5-2018

Minimal Models of Rational Elliptic Curves with non-Trivial Torsio

Alexander J. Barrios
Purdue University

MINIMAL MODELS OF RATIONAL ELLIPTIC CURVES WITH NON-TRIVIAL TORSION

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Alexander J. Barrios

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

May 2018

Purdue University

West Lafayette, Indiana

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF DISSERTATION APPROVAL

Dr. Edray H. Goins, Chair
Department of Mathematics
Dr. Donu V.B. Arapura
Department of Mathematics
Dr. Tong Liu
Department of Mathematics
Dr. Chung Pang Mok
Department of Mathematics

Approved by:
Dr. David Goldberg
Head of the School Graduate Program

To my parents, Miriam and Victor; my brothers, Carlos and Victor Jr.;
and my wife and best friend, Carla.

ACKNOWLEDGMENTS

I would not be where I am today had it not been for the immense support of many people at various stages of my academic career.

I am especially grateful to Edray Goins, who has been my mentor and research advisor since my participation in the Mathematical Sciences Research Institute Undergraduate Program in 2010. Throughout all these years, he has been fundamental in my growth as an individual and mathematician through his exemplary advising, encouragement, generosity, guidance, and patience. I am truly thankful and amazed at how he goes above and beyond for his students, the department, and the community.

I also want to thank my dissertation committee, Donu Arapura, Tong Liu, and Chung Pang Mok for their advice and encouragement throughout the writing of this dissertation. Special thanks to Jamie Weigandt for conversation and for his helpful comments during the writing of this dissertation. I would also like to thank Mike Bennett and Soroosh Yazdani for providing and allowing me to use the data they acquired while investigating good elliptic curves. In addition, I want to thank Alejandra Alvarado, Rodrigo Bañuelos, Steve Bell, Kelly Beranger, Greg Buzzard, Shannon Cassady, Joe Chen, Rachel Davis, Owen Davis, Huimei Delgado, Patrick Devlin, Danielli Donatella, David Goldberg, William Heinzer, Rebecca Lank, Leonard Lipshitz, Kenji Matsuki, Ben McReynolds, Philip Mummert, Dominic Naughton, Deepam Patel, Shaun Ponder, Freydoon Shahidi, Bernd Ulrich, and Mark Ward for their mentoring and support throughout my years in the mathematics department.

As an undergraduate, I was fortunate to participate in three summer programs in mathematics and I am incredibly grateful to Katie Ansaldi, Jason Boynton, Ken Brown, Duane Cooper, Huimei Delgado, Oguz Durumeric, Edray Goins, Ebony Harvey, Kristine Jones, Philip Kutzko, Luis Lomelí, Matt Noonan, Ravi Ramakrishna, Mutiara Sondjaja, and to the many behind the scenes who made these programs possible. Thank you for giving me the motivation to pursue a career in mathematics.

I would also like to thank Johnny Guzman for being a wonderful mentor and role model during my undergraduate studies and for his continued encouragement in the years since.

Additionally, I am appreciative of all the mentors, professors, and teachers I have had throughout this journey, who saw something in me and encouraged me to succeed. Particularly, Marcia Anglin, Cecilia Armesto, E. Carter Burrus Jr., Alvio Dominguez, Tom Goodwillie, Alfredo Granado, Alina Grandal, Christopher Hill, Jeffrey Hoffstein, Giselle Martinez, Jennie Olaguibel-Lundahl, Jill Pipher, Eric Richey, and Richard Schwartz.

I would like to express my thanks and gratitude to the AGEP, MEP, and LSAMP community at Purdue for their years of support and for their shared vision of a more equitable future. Thank you, Ignacio Camarillo, Quincy Clark, Ashlee Colbert, Martha Delaney, Belayneh Desta, Darryl Dickerson, Kathy Dixon, Brittni Echols, Curtis Martin, Maithilee Motlag, Vivek Muralidharar, Keturah Nix, Bonnie Prado, Darryl Reano, Cinthia Sanchez, Carol Stwalley, Elizabeth Suazo Flores, Michelle Visbal, Richard Womack, Virginia Womack, and to the many not listed here who help make your programs a success.

I would also like to thank all my graduate student peers, which include Tyler Billingsley, Jacob Bond, Frankie Chan, Kyle Dahlin, David Daniels, Nicole Eikmeier, Hongshan Li, Reggie McGee, Joan Ponce, Alessio Sammartano, Gabe Sosa, and Razan Taha. Additional thanks to Kate Brubaker, Alessandra Constantini, Tan Dang, Christina Jamroz, Abhishek Parab, and Mark Pengitore for years of friendship, support, and running of our multi-year learning seminar on algebraic geometry.

Special thanks to Sharon Raszap Skorbiansky for being a great friend and running partner. Thank you for motivating me to pursue long-distance running. Prior to entering graduate school, I would not have imagined that I would go on to complete several marathons.

Thank you, Lila Albizu, Nicole Baker-Carson, Dane Bardroff, Matt Carson, Alex Cherin, Cory Colbert, Anthony Hearst, Jared Lafer, Jhon Pereda, Elizabeth Reuter, Andrew Ritchie, Christopher Roemmele, Apollo Roemmele, Alejo Stark, and Lee Zhi for the continued friendship, great conversations, and support throughout the years.

I am eternally grateful for the love and encouragement of my family: Carla Barrios, Carlos Gazabon, Miriam Barrios, Victor Barrios, and Victor Barrios Jr. Their constant support and encouragement have been instrumental in reaching this point in my career. Thank you for helping me achieve this. In addition, I would like to thank my wife Carla Barrios who has stood by me throughout my graduate studies. For her friendship and unconditional love which has kept me going through the ups and downs of graduate school. Words cannot express the gratitude I have for your understanding and support through each step of the way.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SYMBOLS

$a, b, c, d, \ldots$	Integers
$\hat{a},\ \hat{b},\ \hat{c},\ \hat{d}, \ldots$	Factors of $a, b, c, d, \ldots$
a_1, a_2, a_3, a_4, a_6	Coefficients of a Weierstrass model of E
A_T	Invariant c_4 of H_T given in Table E.1
α_T	Invariant c_4 of E_T given in Table D.2
$b_2, b_4, b_6, b_8, c_4, c_6$	Quantities associated to a Weierstrass model of E (see (2.2))
B_T	Invariant c_6 of H_T given in Table E.2
β_T	Invariant c_6 of E_T given in Table D.3
c_p	Local Tamagawa number at p
C_N	Cyclic group of N elements
$\mathcal{C}^{\min}/R_K$	Minimal proper regular model of E/K
$\Delta_E^{\min}$	Minimal discriminant of a rational elliptic curve E
D_T	Discriminant of H_T given in Table E.3
γ_T	Discriminant of E_T given in Table D.4
δ_{u_T}	Polynomial depending on T and u_T in Table 6.2
E	Elliptic Curve
$[E]_K$	K-isomorphism class of E
$E(K)$	Mordell-Weil group of an elliptic curve E defined over a field K
$E(K)_{\text{tors}}$	Torsion subgroup of $E(K)$
E_T	Elliptic curve given by the Weierstrass model in Table D.1
f_p	Exponent appearing at the prime p of the conductor of E
F_P	Frey curve determined by an ABC triple P as defined in Section A
$\mathcal{F}_T$	Database of rational elliptic curves with $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$

$h_{\text{naive}}(E)$	Naive height of an elliptic curve E
H_T	Elliptic curve given by the Weierstrass model in Theorem 4.8
m_p	Number of components of $\bar{\mathcal{C}}_p^{\min}$
N_E	Conductor of E
$\mathcal{N}$	Néron model of E
p, ℓ	Rational prime numbers
$\mathfrak{p}$	Prime ideal
P	An ABC triple
$q(P)$	Quality of an ABC triple P
$\text{rad}(n)$	Product of the distinct prime factors of an integer n
R_K	Integral closure of $\mathbb{Z}$ in K
R_j	The j-th reduced minimal model (see Table 7.1)
$\mathcal{S}$	Database of good elliptic curves
$\sigma_m(E)$	Modified Szpiro ratio of a rational elliptic curve E
$\sigma(E)$	Szpiro ratio of a rational elliptic curve E
T	T is either C_N for $N = 1, \ldots, 10, 12$ or $C_2 \times C_{2m}$ for $m = 1, 2, 3, 4$
u_T	Constant depending on T (see Theorem 5.14)
$v_{\mathfrak{p}}$	The $\mathfrak{p}$-adic valuation on K
$X_1(N)$	Modular Curves
$X_1(2, 2m)$	Modular Curves
$\mathcal{X}_t(T)$	Elliptic curve given by the Weierstrass model in Table 2.1
$\mathcal{Y}_t(T)$	Elliptic curve given by the Weierstrass model in Table 4.1
$\mathbb{Z}_p$	p-adic integers

ABSTRACT

Barrios, Alexander J. PhD, Purdue University, May 2018. Minimal Models of Rational Elliptic Curves with non-Trivial Torsion. Major Professor: Edray H. Goins.

This dissertation concerns the formulation of an explicit modified Szpiro conjecture and the classification of minimal discriminants of rational elliptic curves with non-trivial torsion.

The Frey curve $y^2 = x\,(x+a)\,(x-b)$ is a two-parameter family of elliptic curves which comes equipped with an easily computable minimal discriminant which helped pave the mathematical bridge that led to the proof of Fermat's Last Theorem. In this dissertation, we extend the ideas of the Frey curve by considering two- and three-parameter families of elliptic curves which parameterize all rational elliptic curves with non-trivial torsion subgroup. First, we use these families to give a new proof of a classic result of Frey, Flexor, and Oesterlé which pertains to the primes at which an elliptic curve over a number field can have additive reduction. While our proof gives a weaker variant of the original statement, it is explicit and does not require the Néron model of an elliptic curve. As a consequence of this new proof, we attain our classification of minimal discriminants of rational elliptic curves with non-trivial torsion. In addition, we give necessary and sufficient conditions for when a rational elliptic curve with non-trivial torsion has additive reduction at a given prime. We also study the connection between torsion structure of a rational elliptic curve and the possible reduced minimal models

The second theme of this dissertation concerns the modified Szpiro conjecture, which is equivalent to the *ABC* Conjecture. Roughly speaking, the modified Szpiro conjecture states that certain elliptic curves, known as good elliptic curves, are rare in nature. Masser gave a non-constructive proof which showed that there were infinitely

many good Frey curves. In this dissertation, we give a constructive proof of Masser's assertion. We then extend this result by proving that for each of the fifteen torsion subgroups T allowed by Mazur's Torsion Theorem, there are infinitely many good elliptic curves E with torsion subgroup isomorphic to T. This proof is also constructive and allows for the construction of a database which consists of 13 870 964 good elliptic curves. We provide an analysis of these good elliptic curves to parallel the work done by the ABC@Home project concerning the ABC Conjecture and good ABC triples. The data obtained is then used to formulate an explicit version of the modified Szpiro conjecture. We then show that this explicit formulation allows for the construction of databases of elliptic curves which are exhaustive up to a given conductor.

Lastly, we use the classification of minimal discriminants to study the local data of rational elliptic curves at a given prime via Tate's Algorithm. These results and a study of the naive height of an elliptic curve allow us to prove that there is a lower bound on the modified Szpiro ratio which depends only on the torsion structure of an elliptic curve.

1. INTRODUCTION

> "We live on an island surrounded by a sea of ignorance. As our island of knowledge grows, so does the shore of our ignorance."
>
> - John Archibald Wheeler

1.0.1 Layout of this Dissertation

Chapter 2

This short chapter provides definitions and results which will be assumed in the subsequent chapters. References are provided for the reader.

Chapter 3

In this chapter, we give a succinct survey of the ABC Conjecture. We follow this by introducing the modified Szpiro conjecture and prove the equivalence between the ABC Conjecture and the modified Szpiro conjecture by following an argument due to Oesterlé [1]. Roughly speaking, the modified Szpiro conjecture states that certain elliptic curves, known as good elliptic curves are rare in nature. The goal of this chapter is to study and create a database of good elliptic curves to parallel the work done for good ABC triples by the ABC@Home project [2].

We start by giving an overview of current databases of rational elliptic curves and then construct a new database of rational elliptic curves. This database consists of 130 789 162 rational elliptic curves E with the property that $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$ where $T = C_2 \times C_{2N}$ with $N = 2, 3, 4$. Assuming Theorem 5.14, we show that there is a subset of this database which is exhaustive up to a given naive height.

Next, we give a constructive proof that there are infinitely many good Frey curves. The original proof due to Masser [3] is non-constructive. Building on this constructive result and models of elliptic curves which are studied in Chapter 4, we create a new database consisting of 13 870 964 good elliptic curves. The data obtained is then used to formulate an explicit version of the modified Szpiro conjecture. In Appendix B, we order these good elliptic curves by their modified Szpiro and Szpiro ratios.

Chapter 4

In this chapter, we extend the result of Chapter 3 pertaining to infinitely many good Frey curves. Specifically, we prove that if T is one of the fifteen torsion subgroups allowed by Mazur's Torsion Theorem, then there are infinitely many good elliptic curves E with $E(\mathbb{Q})_{\text{tors}} \cong T$. This proof is constructive and we conclude the chapter with examples.

Chapter 5

In this chapter, we give a new proof of a result due to Frey-Flexor-Oesterlé which does not require use of the Néron model of an elliptic curve. We then consider rational elliptic curves and use the Explicit version of Frey-Flexor-Oesterlé to prove our main result, Theorem 5.14. This Theorem is the classification of minimal discriminants of rational elliptic curves with non-trivial torsion subgroup. As a consequence of this Theorem, we give necessary and sufficient conditions for additive reduction to occur in a rational elliptic curve with non-trivial torsion subgroup.

Chapter 6

In this chapter, we use Theorem 5.14 to study the naive height of a rational elliptic curve. In fact, let T be one of the fifteen torsion subgroups allowed by Mazur's Torsion Theorem. We show that if E is a rational elliptic curve and $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$

with $T \neq C_1, C_2, C_2 \times C_2$, then there is an explicit function that coincides with the naive height of rational elliptic curve E with $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$. Next, we use the results of Chapter 5 to study the local data of an elliptic curve via Tate's Algorithm. These results together with the work on the explicit naive height allow us to prove that there is a lower bound on the modified Szpiro ratio which only depends on the torsion subgroup of a rational elliptic curve.

Chapter 7

In this chapter, we review the reduced minimal model of a rational elliptic curve. It is well known that each rational elliptic curve has a unique reduced minimal model. The classification of minimal discriminants in Chapter 4 relied on a Theorem of Kraus and therefore did not yield a global minimal model in all cases. We give a partial answer in regards to global minimal models by classifying the reduced minimal models of rational elliptic curves with a rational torsion point of order at least 3. This is done by use of the Laska-Kraus-Connell Algorithm and Theorem 5.14.

2. BACKGROUND

In this chapter, we state definitions and results which will be used in this thesis. Unless stated otherwise, the main references for this chapter are [4], [5], and [6].

2.1 Elliptic Curves

An *elliptic curve* is a pair $(E, \mathcal{O})$, where E is a smooth projective curve of genus one and $\mathcal{O} \in E$. The elliptic curve E is defined over a field K if E is defined over K as a curve and $\mathcal{O}$ is a K-rational point on E. The set of K-rational points on E is denoted by $E(K)$ and a result of Poincaré shows that if E is an elliptic curve over K, then the set $E(K)$ is a group with identity $\mathcal{O}$. Mordell and Weil then showed that $E(K)$ is a finitely generated abelian group if K is a number field. The torsion subgroup of $E(K)$ is denoted by $E(K)_{\text{tors}}$. We say E is a rational elliptic curve if E is defined over the rational numbers $\mathbb{Q}$. Mazur proved that the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is one of fifteen possible groups.

Theorem 2.1 (Mazur's Torsion Theorem [7]) *Let E be a rational elliptic curve and let C_N denote the cyclic group of N elements. Then*

$$E(\mathbb{Q})_{tors} \cong \begin{cases} C_N & \text{for } N = 1, 2, \ldots, 10, 12 \\ C_2 \times C_{2N} & \text{for } N = 1, 2, 3, 4. \end{cases}$$

We say that two elliptic curves E and E' are K-isomorphic if there is an isomorphism between E and E' which is defined over K. Now suppose E is an elliptic curve defined over a field K. Then the point $\mathcal{O}$ corresponds to a very ample divisor and therefore via the Riemann-Roch Theorem we obtain an embedding of E into $\mathbb{P}^2_K = \mathrm{Proj}K[X, Y, Z]$. In fact, the K-isomorphic image of E in $\mathbb{P}^2_K$ is given by

$$\mathrm{Proj}K[X, Y, Z] \,/\, \left(Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3\right)$$

with each coefficient $a_i \in K$ and $\mathcal{O}$ corresponding to the homogeneous prime ideal (X, Z). Moreover, every smooth cubic curve in $\mathbb{P}^2_K$ is cut out by an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Henceforth, by an elliptic curve E defined over K we will write E in affine coordinates, i.e., E is given by the *Weierstrass model*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with each $a_i \in K$, and it will be understood that there is an additional point $\mathcal{O} = (0, 1, 0)$ which we call the *point at infinity*. For an elliptic curve E given by the Weierstrass model (2.1), we define the following quantities:

$$\begin{aligned}
&b_2 = a_1^2 + 4a_2 \qquad b_4 = 2a_4 + a_1a_3 \qquad b_6 = a_3^2 + 4a_6\\
&b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\\
&c_4 = b_2^2 - 24b_4 \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6\\
&\Delta = \tfrac{c_4^3 - c_6^2}{1728} \qquad j = \tfrac{c_4^3}{\Delta}
\end{aligned} \tag{2.2}$$

We say Δ is the *discriminant* of E and the assumption that E is smooth is equivalent to $\Delta \neq 0$. The quantity j is known as the *j-invariant* and we call the quantities c_4 and c_6 the *invariants associated to the Weierstrass model* of E. In particular, we have the identity $1728\Delta = c_4^3 - c_6^2$.

The *admissible change of variables* $x \longmapsto u^2x + r$ and $y \longmapsto u^3y + u^2sx + w$ for $u, r, s, w \in K$ and $u \neq 0$ gives a K-isomorphism from E onto an elliptic curve E' whose Weierstrass model arises from the given change of variables on E. Conversely, if E and E' are K-isomorphic and the isomorphism preserves the point at infinity $\mathcal{O}$, then there is an admissible change of variables on E, $x \longmapsto u^2x+r$ and $y \longmapsto u^3y+u^2sx+w$ with $u, r, s, w \in K$ and $u \neq 0$, which gives the Weierstrass model of E'.

Moreover, let Δ', j', c_4', and c_6' denote the quantities attained from the Weierstrass model for E'. Then

$$\Delta' = u^{-12}\Delta, \qquad j' = j, \qquad c_4' = u^{-4}c_4, \qquad c_6' = u^{-6}c_6.$$

2.2 Minimal Discriminant

The main reference for this section is Chapter VII and VIII of [4] and Chapter IV of [5].

2.2.1 Local Definition

Let K be a local field, complete with respect to a discrete valuation v. Let R denote the ring of integers of K and let π be a uniformizer for the unique maximal ideal of R. Now suppose E is an elliptic curve over K given by the Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The admissible change of variables $x \longmapsto u^{-2}x$ and $y \longmapsto u^{-3}y$ leads to a K-isomorphic elliptic curve E' to E with Weierstrass model

$$E' : y^2 + u^{-1}a_1xy + u^{-3}a_3y = x^3 + u^{-2}a_2x^2 + u^{-4}a_4x + u^{-6}a_6.$$

In particular, we can choose u to be divisible by a sufficiently large power of π so that we obtain a Weierstrass model with the property that each coefficient is in R and $v(\Delta) \geq 0$. Since v is discrete, we have that among all Weierstrass equations with coefficients in R, there is one that minimizes the value of $v(\Delta)$.

Definition 2.1 *Let E be an elliptic curve defined over K. A Weierstrass model for E is said to be a* ***minimal Weierstrass model*** *for E at v if $v(\Delta)$ is minimized subject to the condition that each $a_i \in R$. The minimal value of $v(\Delta)$ is called the* ***valuation of the minimal discriminant*** *of E at v.*

Definition 2.2 *Let E be an elliptic curve defined over K. We say E has* ***additive reduction*** *at v if $v(\Delta) > 0$ and $v(c_4) > 0$. If E does not have additive reduction at v, we say E is* ***semistable*** *at v.*

2.2.2 Global Definition

Now let K be a number field and let R denote its ring of integers. Let E be an elliptic curve over K. For each finite prime $\mathfrak{p}$ there is a Weierstrass model

$$y^2 + a_{1,\mathfrak{p}}xy + a_{3,\mathfrak{p}}y = x^3 + a_{2,\mathfrak{p}}x^2 + a_{4,\mathfrak{p}}x + a_{6,\mathfrak{p}}$$

that is a minimal equation for E at $\mathfrak{p}$. That is, $v_{\mathfrak{p}}(a_{j,\mathfrak{p}}) \geq 0$ for each j where $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation.

Definition 2.3 *Let E be an elliptic curve over a number field K. The **minimal discriminant** $\mathcal{D}_{E/K}$ is the (integral) ideal of K given by*

$$\mathcal{D}_{E/K} = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{v_{\mathfrak{p}}(\Delta_{\mathfrak{p}})}$$

where $\Delta_{\mathfrak{p}}$ is the minimal discriminant of a minimal equation for E at $\mathfrak{p}$.

Definition 2.4 *Let E be an elliptic curve over a number field K. A **global minimal model** for E is a Weierstrass model*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E such that each $a_j \in R$ and the discriminant Δ of the equation satisfies $\mathcal{D}_{E/K} = (\Delta)$. If a global minimal model for E exists, we denote the minimal discriminant of E by Δ_E^{min}.

In general, we say E is given by an *integral Weierstrass model* if each $a_i \in R$. If K has class number one, then each elliptic curve over K has a global minimal model [4, Corollary VIII.8.3].

Definition 2.5 *Let E be an elliptic curve over a number field K. The **conductor** of E is the ideal*

$$N_{E/K} = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{f_{\mathfrak{p}}} \text{ where } f_{\mathfrak{p}} = \begin{cases} 0 & \text{if } \mathfrak{p} \nmid \mathcal{D}_{E/K} \\ 1 & \text{if } \mathfrak{p} | \mathcal{D}_{E/K} \text{ and } E \text{ is semistable at } \mathfrak{p} \\ 2 + \delta_{\mathfrak{p}} & \text{if } E \text{ has additive reduction at } \mathfrak{p}. \end{cases}$$

The quantity $\delta_{\mathfrak{p}} = 0$ *if* $\mathfrak{p} \nmid 6$. *If* $\mathfrak{p}$ *has residue characteristic* 2 *or* 3 *and* E *has additive reduction at* $\mathfrak{p}$, *then* $\delta_{\mathfrak{p}}$ *is a measure of the wild ramification in the extension* $K_{\mathfrak{p}}(E[p])/K_{\mathfrak{p}}$ *for* $\mathfrak{p}$ *a a prime lying above the rational prime* p *[5, IV.10].*

2.2.3 Rational Elliptic Curves

We now consider rational elliptic curves and state results which will be used in the subsequent chapters.

Lemma 2.2 *Let* E *be a rational elliptic curve and let* p *be a prime. If* p *divides* $\gcd(c_4, \Delta_E^{min})$, *then* E *has additive reduction at* p. *If* p *does not divide* $\gcd(c_4, \Delta_E^{min})$, *then* E *is semistable at* p. *We say* E *is semistable if* E *is semistable at all primes.*

For a rational elliptic curve E, we consider the conductor N_E of E as the integer

$$N_E = \prod_{p \mid \Delta_E^{\min}} p^{f_p} \text{ where } f_{\mathfrak{p}} = \begin{cases} 1 & \text{if } E \text{ is semistable at } p \\ 2 + \delta_p & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

The quantity $\delta_p = 0$ for each prime $p \geq 5$. In particular, if E is semistable, then $N_E = \operatorname{rad}(\Delta_E^{\min})$ where $\operatorname{rad}(n)$ is the product of the distinct primes dividing n.

Lemma 2.3 *Let* E *be a rational elliptic curve and let* N_E *be its conductor and let* δ_p *as given above. Then* $\delta_2 \leq 6$ *and* $\delta_3 \leq 3$.

Proof [5, IV.10.4]. ■

Lemma 2.4 *Let* K *be a local field, complete with respect to a discrete valuation* v *and let* R *denote its ring of integers. If* E *is an elliptic curve given by an integral Weierstrass model, then any admissible change of variables* $x \longmapsto u^2x + r$ *and* $y \longmapsto u^3y + u^2sx + w$ *used to produce a minimal Weierstrass equation satisfies* $u, r, s, w \in R$.

In particular, if E *is a rational elliptic curve and* $x \longmapsto u^2x + r$ *and* $y \longmapsto u^3y + u^2sx + w$ *is an admissible change of variables which results in a global minimal model for* E, *then* $u, r, s, w \in \mathbb{Z}$.

Definition 2.6 *The rational elliptic curve*

$$F : y^2 = x\,(x + a)\,(x - b)$$

*with a and b relatively prime integers is known as a **Frey curve**. The discriminant of F is $\Delta = (4ab\,(a + b))^2$.*

Lemma 2.5 *Let $F : y^2 = x\,(x + a)\,(x - b)$ be a Frey curve. Then the minimal discriminant of F is $u^{-12}\Delta$ where u is either 1 or 2. Moreover, $u = 2$ if and only if $a \equiv 0 \mod 16$ and $b \equiv 3 \mod 4$. The Frey curve is semistable at all odd primes and semistable at 2 if and only if $u = 2$.*

At the time of its formulation, it was not possible to state the above result as an equivalence. The minimal discriminant being $2^{-12}\Delta$ was proven to hold under the given congruences due to the existence of an integral Weierstrass model for F under these assumptions. An application of a Theorem of Kraus shows that the above is in, fact, an equivalence.

Theorem 2.6 (Kraus, [8]) *Let $\alpha, \beta,$ and γ be integers such that $\alpha^3 - \beta^2 = 1728\gamma$ with $\gamma \neq 0$. Then there exists a rational elliptic curve E given by an integral Weierstrass equation having invariants $c_4 = \alpha$ and $c_6 = \beta$ if and only if the following conditions hold:*

(*i*) $v_3(\beta) \neq 2$;

(*ii*) *either* $\beta \equiv -1 \mod 4$ *or both* $v_2(\alpha) \geq 4$ *and* $\beta \equiv 0$ *or* $8 \mod 32$.

2.3 Reduced Minimal Model

Given a rational elliptic curve, there are infinitely many possible global minimal models. Among these, there is a unique global minimal model known as the reduced minimal model of E.

Definition 2.7 *Let E be a rational elliptic curve. The* ***reduced minimal model*** *of E is given by a Weierstrass model*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

which is a global minimal model for E and satisfies $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$.

Proposition 2.7 ([9, Chapter III]) *The reduced minimal model of rational elliptic curve is unique.*

Following Kraus's Theorem, Connell modified an existing algorithm of Laska's [10] to output the reduced minimal model of a rational elliptic curve, given the invariants c_4 and c_6 associated to a global minimal model of E.

Algorithm 2.8 (Laska-Kraus-Connell Algorithm, [9, 3.2]) *Let E be a rational elliptic curve with invariants c_4 and c_6 associated to a global minimal model of E. Then the coefficients a_i of the reduced minimal model of E are determined from the quantities below:*

$$\begin{array}{ll} b_2 = -c_6 \mod 12 \in \{-5, -4, \ldots, 6\} & b_4 = \frac{b_2^2 - c_4}{24} \\ b_6 = \frac{-b_2^3 + 36b_2b_4 - c_6}{216} & a_1 = b_2 \mod 2 \in \{0, 1\} \\ a_2 = \frac{b_2 - a_1}{4} & a_3 = b_6 \mod 2 \in \{0, 1\} \\ a_4 = \frac{b_4 - a_1a_3}{2} & a_6 = \frac{b_6 - a_3}{4} \end{array}$$

In particular, the quantities $b_6, a_4,$ and a_6 are integers.

2.4 Local Data of a Rational Elliptic Curve

In this section, we assume familiarity with algebraic geometry. We follow the terminology in [6].

Let R be a Dedekind domain with field of fractions K and E an elliptic curve over K. Then there exists a regular arithmetic surface $\mathcal{C}/R$, proper over R, whose generic fiber is isomorphic to E over K. We call $\mathcal{C}/R$ a *proper regular model* for E/K.

In addition, there exists a proper regular model $\mathcal{C}^{\min}/R$ for E/K with the following minimal property:

Let $\mathcal{C}/R$ be any other regular model for E/K. Fix an isomorphism from the generic fiber of $\mathcal{C}$ to the generic fiber of $\mathcal{C}^{\min}$. Then the induced R-birational map $\mathcal{C} \dashrightarrow \mathcal{C}^{\min}$ is an R-isomorphism. We call $\mathcal{C}^{\min}/R$ the *minimal proper regular model* for E/K. It is unique up to unique R-isomorphism.

We define the *Néron model* of E over R to be a scheme $\mathcal{N} \to \operatorname{Spec} R$ which is smooth, separated, and of finite type, with generic fiber isomorphic to E, and that verifies the following universal property: for any smooth scheme X over R, the canonical map $\mathrm{Map}_K(X, \mathcal{N}) \to \mathrm{Map}_K(X_K, E)$ is bijective. In fact, $\mathcal{N}$ is the open subscheme of the minimal proper regular model $\mathcal{C}^{\min}$ associated to E which is made up of points that are smooth over R [6, Theorem 10.2.14].

Now suppose E is a rational elliptic curve and let p be a finite prime. Let $\mathbb{Z}_p$ be the p-adic integers and denote by $\mathcal{C}_p^{\min}$ and $\mathcal{N}_p$ the minimal proper regular model and Néron model over $\mathbb{Z}_{(p)}$, respectively. The special fiber $\bar{\mathcal{N}}_p$ of $\mathcal{N}_p$ is a scheme over the residue field $\mathbb{F}_p$. Since $\bar{\mathcal{N}}_p$ is an algebraic group, we let $\bar{\mathcal{N}}_p^0$ be the connected component of $\bar{\mathcal{N}}_p$ containing the unit element of $\bar{\mathcal{N}}_p$. Similarly, denote by $\bar{\mathcal{C}}_p^{\min}$ the special fiber of $\mathcal{C}_p^{\min}$.

Tate's Algorithm [5, Chapter IV] returns the following local data for each prime p of $\mathbb{Z}$:

1. The reduction type of the special fiber $\bar{\mathcal{C}}_p^{\min}$ over $\bar{\mathbb{F}}_p$. We will use Kodaira symbols to describe the reduction type.

2. m_p: the number of components, defined over $\bar{\mathbb{F}}_p$ and counted without multiplicity, on $\bar{\mathcal{C}}_p^{\min}$.

3. $v_p(\Delta_E^{\min})$: the valuation of the minimal discriminant of E/K with respect to p;

4. f_p: the exponent appearing at the prime p of the conductor of E. This will be computed via Ogg's formula: $f_p = v_p(\Delta_E^{\min}) - m_p + 1$;

5. c_p: the local Tamagawa number at p, i.e., the order of the group of components $\bar{\mathcal{N}_p}(\mathbb{F}_p)\,/\bar{\mathcal{N}_p^0}(\mathbb{F}_p)$. Equivalently, c_p is the number of components of $\bar{\mathcal{C}}_p^{\min}$ which have multiplicity 1 and are defined over $\mathbb{F}_p$.

2.5 Universal Elliptic Curves

Let $N \geq 2$ be an integer. The modular curve $X_1(N)$ (with cusps removed) parameterizes isomorphism classes of pairs (E, P) where E is an elliptic curve and P is a torsion point of order N on E. Two isomorphism classes of pairs (E, P) and (E', P') are isomorphic if there exists an isomorphism $\varphi : E \to E'$ such that $\varphi(P) = P'$ [5]. Now let $m \geq 1$ be an integer. The modular curve $X_1(2, 2m)$ parameterize isomorphism classes of pairs (E, P, Q) where E is a rational elliptic curve and $\langle P, Q\rangle \cong C_2 \times C_{2m}$ and $e(P, mQ) = \zeta_2$ where e_2 is the Weil pairing [4, III.8]. It is well known that the modular curve $X_1(N)$ and $X_1(2, 2m)$ has genus 0 if [11, Proposition 3.7] $N = 2, 3, \ldots, 10, 12$ or $m = 1, 2, 3, 4$. When $N = 4, 5, \ldots, 10, 12$ and $m = 2, 3, 4$ these modular curves are parameterizable by a single parameter t [12, Table 3]. More precisely, for these values of N and M, we consider the abelian groups $T = C_N$ and $T = C_2 \times C_{2m}$. For $t \in \mathbb{P}^1$, define $\mathcal{X}_t$ as the mapping which takes T to the elliptic curve $\mathcal{X}_t(T)$ where the Weierstrass model of $\mathcal{X}_t(T)$ is given in Table 2.1[1]. Then $\mathcal{X}_t(T)$ is a one-parameter family of elliptic curves with the property that if $t \in K$ for some field K, then $\mathcal{X}_t(T)$ is an elliptic curve over K and $T \hookrightarrow \mathcal{X}_t(T)(K)_{\text{tors}}$. The Weierstrass model of $\mathcal{X}_t(T)$ is known as the *universal elliptic curve* over $X_1(N)$ (resp. $X_1(2, 2m)$) if $T = C_N$ (resp. $T = C_2 \times C_{2m}$).

We summarize the above with the following result which will be used in the subsequent chapters.

[1]Our parameterizations differ slightly from [12, Table 3]. We instead use [13, Table 3] which expands the implicit expressions for the parameters b and c in [12, Table 3] to express the universal elliptic curves in terms of a single parameter t.

Table 2.1.: Universal Elliptic Curve $\mathcal{X}_t(T)$

$\mathcal{X}_t(T) : y^2 + (1-g)\,xy - fy = x^3 - fx^2$		
f	g	T
t	0	C_4
t	t	C_5
t^2+t	t	C_6
t^3-t^2	t^2-t	C_7
$2t^3-3t+1$	$\frac{2t^2-3t+1}{t}$	C_8
$t^5-2t^4+2t^3-t^2$	t^3-t^2	C_9
$\frac{2t^5-3t^4+t^3}{(t^2-3t+1)^2}$	$\frac{-2t^3+3t^2-t}{t^2-3t+1}$	C_{10}
$\frac{12t^6-30t^5+34t^4-21t^3+7t^2-t}{(t-1)^4}$	$\frac{-6t^4+9t^3-5t^2+t}{(t-1)^3}$	C_{12}
$4t^2+t$	0	$C_2 \times C_4$
$\frac{-2t^3+14t^2-22t+10}{(t+3)^2(t-3)^2}$	$\frac{-2t+10}{(t+3)(t-3)}$	$C_2 \times C_6$
$\frac{16t^3+16t^2+6t+1}{(8t^2-1)^2}$	$\frac{16t^3+16t^2+6t+1}{2t(4t+1)(8t^2-1)}$	$C_2 \times C_8$

Lemma 2.9 *Let K be a field. If $t \in K$ such that $\mathcal{X}_t(T)$ is an elliptic curve, then $T \subset \mathcal{X}_t(T)(K)_{tors}$. Moreover, if E is an elliptic curve over K, then there is a $t \in K$ such that E is K-isomorphic to $\mathcal{X}_t(T)$.*

3. THE EXPLICIT MODIFIED SZPIRO CONJECTURE

The story of the *ABC* Conjecture begins with the following theorem:

Theorem 3.1 (Mason-Stothers) *Let a, b, c be nonconstant relatively prime complex polynomials in one variable such that $a + b = c$. Then*

$$\max\{\deg a, \deg b, \deg c\} < n_0(abc)$$

where $n_0(f)$ denotes the number of distinct roots of f.

This was first proven by Stothers [14] in 1981, but rediscovered three years later by Mason [15]. The following year, Masser and Oesterlé were discussing Mason's recent paper and the pair came up with the novel idea of reformulating the Mason-Stothers Theorem as a statement pertaining to the integers. In the hours that followed, the *ABC* Conjecture was conceived. In the years since, the literature has been replete with applications of the *ABC* Conjecture, most notably Fermat's Last Theorem which at the time remained unproven. We refer the interested reader to the classic article by Lang [16] as well as the survey article of Martin and Miao [17] to learn more about the numerous applications of the *ABC* Conjecture.

As with Fermat's Last Theorem, the *ABC* Conjecture has also manifested itself in the theory of elliptic curves where it has an equivalent formulation known as the modified Szpiro conjecture. The modified Szpiro conjecture roughly says that for a rational elliptic curve E, it is rare for the inequality

$$N_E^6 < \max\{ c_4^3 \ , c_6^2$$

to hold where N_E is the conductor of E and c_4 and c_6 are the invariants associated with a global minimal model of E. We will say that if an elliptic curve satisfies the above inequality, then it is a *good elliptic curve*.

In the first section, we give a succinct introduction to the ABC Conjecture and state known results which will motivate our study of the modified Szpiro conjecture which begins in section two. In section three, we briefly go over current databases of rational elliptic curves and find all good elliptic curves in Cremona's database which as of this writing consists of all elliptic curves of conductor at most 400 000. In addition, we construct new databases consisting of elliptic curves with $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_{2m}$ where $m = 2, 3, 4$ and summarize the data obtained pertaining to the modified Szpiro conjecture. In section 4 we give a constructive proof that there are infinitely many good Frey curves. In section 5, we use the elliptic curves from section 4 as well as certain models of elliptic curves which will be studied in further detail in chapter 4 to construct a database consisting of 13 870 964 good elliptic curves and conjecture an explicit formulation of the modified Szpiro conjecture based on the data acquired, i.e., what is the smallest real number λ such that $\max\{|c_4^3|, c_6^2\} < N_E^{\lambda}$ holds for all rational elliptic curves E. As an application, we show at the end how the explicit Modified Szpiro conjecture can be used to construct exhaustive databases of elliptic curves up to a given conductor. We note that as of this writing, the 2012 proof of the modified Szpiro conjecture by Mochizuki is still under review. Even if the proof is found to be correct, it does not shed light on the explicit version of the modified Szpiro conjecture.

3.1 The ABC Conjecture

We begin with the following definition which will simplify the statement of the ABC Conjecture.

Definition 3.1 *By an* ***ABC triple*** $P = (a, b, c)$ *we mean a triple of integers* a, b, c *such that* a, b, c *are relatively prime non-zero integers and* $a + b = c$. *The* ***quality*** *of an* ABC *triple* $P = (a, b, c)$ *is the quantity*

$$q(P) = \frac{\log \max\{|a|, |b|, |c|\}}{\log \operatorname{rad}(abc)}$$

where $\mathrm{rad}(n)$ *denotes the product of all distinct primes dividing* n*.*

We say an ABC triple is ***good*** *if* $q(P) > 1$ *and if* a, b, c *are positive, we say that* P *is* ***positive****.*

Proposition 3.2 *The following are equivalent:*

(i) For every $\epsilon > 0$ *there exists a positive constant* κ_ϵ *such that for all ABC triples* $P = (a, b, c)$ *we have*

$$\max\{|a|, |b|, |c|\} \leq \kappa_\epsilon \, \mathrm{rad}(abc)^{1+\epsilon}\,; \tag{3.1}$$

(ii) For every $\epsilon > 0$ *there are finitely many ABC triples* $P = (a, b, c)$ *satisfying*

$$\mathrm{rad}(abc)^{1+\epsilon} < \max\{|a|, |b|, |c|\}\,.$$

(iii) For every $\epsilon > 0$ *there are finitely many ABC triples* $P = (a, b, c)$ *satisfying*

$$q(P) > 1 + \epsilon.$$

We refer to each of these equivalent statements as the ***ABC*** **Conjecture**.

Proof By the previous definition it follows that (ii) and (iii) are equivalent.

$(i \Longrightarrow iii)$ Fix $\epsilon > 0$ and suppose there exists a positive constant κ_ϵ so that (3.1) holds. If $\kappa_\epsilon \leq 1$, then

$$\begin{aligned} \max\{|a|, |b|, |c|\} &\leq \mathrm{rad}(abc)^{1+\epsilon} \\ \Longrightarrow \qquad & \frac{\log \max\{|a|, |b|, |c|\}}{\log \mathrm{rad}(abc)} \leq 1 + \epsilon \end{aligned}$$

and thus (iii) holds. Now suppose $\kappa_\epsilon > 1$ and towards a contradiction, assume that there are infinitely many ABC triples $P = (a, b, c)$ such that $q(P) > 1 + \epsilon$. Taking logarithms in (3.1) yields

$$\begin{aligned} \log \max\{|a|, |b|, |c|\} &\leq \log \kappa_\epsilon + (1 + \epsilon) \log \mathrm{rad}(abc) \\ \Longrightarrow \qquad & q(P) \leq \frac{\log \kappa_\epsilon}{\log \mathrm{rad}(abc)} + 1 + \epsilon. \end{aligned}$$

In particular,

$$1+\epsilon < q(P) \le \frac{\log \kappa_\epsilon}{\log \operatorname{rad}(abc)} + 1 + \epsilon \qquad \Longrightarrow \qquad 0 < q(P) \le \frac{\log \kappa_\epsilon}{\log \operatorname{rad}(abc)}$$

$$\Longrightarrow \qquad \log \max\{|a|,|b|,|c|\} \le \log \kappa_\epsilon$$

which is our desired contradiction since there are finitely many ABC triples satisfying

$$\log \max\{|a|,|b|,|c|\} \le \log \kappa_\epsilon$$

for any fixed constant κ_ϵ.

($iii \Longrightarrow i$) Fix $\epsilon > 0$. Observe that if P is an ABC triple satisfying $q(P) \le 1+\epsilon$, then

$$\log \max\{|a|,|b|,|c|\} \le (1+\epsilon) \log \operatorname{rad}(abc)$$

$$\Longrightarrow \qquad \max\{|a|,|b|,|c|\} \le \operatorname{rad}(abc)^{1+\epsilon}.$$

Now assume that there are finitely many ABC triples P satisfying $q(P) > 1+\epsilon$. In particular, there is a real number $\kappa_\epsilon \ge 1$ such that

$$\frac{\max\{|a|,|b|,|c|\}}{\operatorname{rad}(abc)^{1+\epsilon}} \le \kappa_\epsilon$$

for all $P = (a,b,c)$ satisfying $q(P) > 1+\epsilon$. Since $\max\{|a|,|b|,|c|\} \le \operatorname{rad}(abc)^{1+\epsilon}$ holds for all ABC triples P satisfying $q(P) \le 1+\epsilon$, it follows that (i) holds for all ABC triples. ■

The following lemma shows that the ϵ is necessary for the statement of the ABC Conjecture.

Lemma 3.3 *Let p be an odd prime. Then $\left(1, p^{(p-1)k} - 1, p^{(p-1)k}\right)$ is a good ABC triple for each positive integer k.*

Proof Note that $p^{(p-1)k} - 1 = (p-1)\,P$ where

$$P = \sum_{j=1}^{(p-1)k} p^{j-1}.$$

Since $p \equiv \mp 1 \mod (p \pm 1)$, it follows that $P \equiv 0 \mod (p \pm 1)$. In particular, $P \equiv 0 \mod 4$. Therefore,

$$\operatorname{rad}\left(p^{(p-1)k} - 1\right) = \operatorname{rad}\left(\frac{P}{2}\right) \leq \frac{P}{2} = \frac{p^{(p-1)k} - 1}{2\,(p-1)}. \tag{3.2}$$

Moreover, $\operatorname{rad}\left(\left(p^{(p-1)k} - 1\right) p^{(p-1)k}\right) = p \operatorname{rad}\left(\left(p^{(p-1)k} - 1\right)\right)$ and $\max\left\{1, p^{(p-1)k} - 1, p^{(p-1)k}\right\} = p^{(p-1)k}$ and so we attain

$$\begin{aligned} p^{(p-1)k} - p \operatorname{rad}\left(\left(p^{(p-1)k} - 1\right)\right) &\geq p^{(p-1)k} - \frac{p^{(p-1)k} - 1}{2\,(p-1)} \quad \text{by (3.2)} \\ &= p^{(p-1)k}\left(1 - \frac{p}{2\,(p-1)}\right) + \frac{p}{2\,(p-1)} \\ &> 0. \end{aligned}$$

■

In the special case when $p = 3$ and $k = 1$ we get the ABC triple $P = (1, 8, 9)$ with quality $q(P) \approx 1.2263$. Since there are infinitely many good ABC triples, we have that the ABC Conjecture is equivalent to

$$\limsup q(P) = 1$$

where the lim sup ranges over all ABC triples P. Assuming the ABC Conjecture, Browkin et al. [18] proved that the set of limit points of $q(P)$ as P ranges over all ABC triples is equal to the closed interval $\left[\frac{1}{3}, 1\right]$. Specifically, they proved that given any real number ϵ in the closed interval $\left[\frac{1}{3}, 1\right]$, there is a sequence of ABC triples $\{P_n\}_{n \geq 0}$ such that $\lim_{n \to \infty} q(P_n) = \epsilon$. At the end of section 3.3.2, we present evidence for what the analogous result should be for the modified Szpiro conjecture based on a result which will be proven in chapter 6.

While there are infinitely many good ABC triples, there is strong numerical evidence for the ABC Conjecture being true. The ABC@Home project was a network computing project which began in 2007 with the goal of finding all good ABC triples $P = (a, b, c)$ with $\max\{|a|, |b|, |c|\} < 10^8$. This goal was accomplished in 2011 with the finding of 14 482 065 good ABC triples. The project continued until 2015 with the finding of an additional 9 345 651 good ABC triples with $10^{18} \leq \max\{|a|, |b|, |c|\} < 2^{63}$. Of the 23 827 716 good ABC triples found by the ABC@Home project, only 240 of them have quality greater than 1.4. In fact, $P = (2, 3^{10} \cdot 109, 23^5)$ is the triple with largest known quality $q(P) \approx 1.6299$. As of May 2018, this data is available at Bart de Smit's webpage [2].

The data also gives support for Baker's [19] explicit formulation of the ABC Conjecture,

Conjecture 3.4 (Explicit ABC Conjecture) *Let $P = (a, b, c)$ be an ABC triple. Then*

$$\max\{|a|, |b|, |c|\} \leq \operatorname{rad}(abc)^{1.75}.$$

While this variant does not imply the ABC Conjecture, it does imply Fermat's Last Theorem.

Proposition 3.5 *The explicit ABC Conjecture implies Fermat's Last Theorem.*

Proof Towards a contradiction, suppose Fermat's Last Theorem is false for some exponent $n > 2$. That is, there are relatively prime positive integers a, b, and c such that $a^n + b^n = c^n$. Then

$$c^n = \max\{|a^n|, |b^n|, |c^n|\} \leq \operatorname{rad}(a^n b^n c^n)^{1.75} = \operatorname{rad}(abc)^{1.75} \leq (abc)^{1.75} < c^{5.25}.$$

In particular, $n \leq 5$ which is our desired contradiction since these cases have been known since 1825. ∎

In fact, the data compiled by the ABC@Home project suggests that Baker's exponent of 1.75 may be replaced with 1.63. In section 3, we will study the explicit side of the modified Szpiro conjecture and formulate an explicit modified Szpiro conjecture based on numerical evidence from Cremona's database of rational elliptic curves and further data acquired from rational elliptic curves with non-trivial torsion.

3.2 The Modified Szpiro Conjecture

Let E be a rational elliptic curve with minimal discriminant $\Delta_E^{\min}$. Throughout this section, the invariants c_4 and c_6 will be assumed to be associated with a global minimal model of E so that $1728\Delta_E^{\min} = c_4^3 - c_6^2$. In 1981, Szpiro [20] made the following deep conjecture pertaining to the minimal discriminant and conductor of a rational elliptic curve.

Conjecture 3.6 (Szpiro, 1981) *For every $\epsilon > 0$ there exists a positive constant κ_ϵ such that for all rational elliptic curves E,*

$$\left| \Delta_E^{min} \right| \leq \kappa_\epsilon N_E^{6+\epsilon}.$$

Soon after, it was shown that Szpiro's conjecture implied the Asymptotic Fermat's Last Theorem [4, Proposition VIII.11.2]. After the formulation of the ABC Conjecture, it was shown that the ABC Conjecture implied Szpiro's conjecture. While the converse did not hold, a modification of Szpiro's conjecture resulted in an equivalence with the ABC Conjecture [1]. As with the previous section, we begin with a definition which will simplify our description of the modified Szpiro conjecture.

Definition 3.2 *Let E be a rational elliptic curve with minimal discriminant Δ_E^{min} and associated invariants c_4 and c_6. Define the* ***modified Szpiro ratio*** *$\sigma_m(E)$ and* ***Szpiro ratio*** *$\sigma(E)$ of E to be the quantities*

$$\sigma_m(E) = \frac{\log \max\{|c_4^3|, c_6^2\}}{\log N_E} \qquad \textit{and} \qquad \sigma(E) = \frac{\log |\Delta_E^{min}|}{\log N_E}$$

where N_E is the conductor of E.

We say that E is ***good*** *if $\sigma_m(E) > 6$.*

Lemma 3.7 *For all rational elliptic curves, $\sigma(E) < \sigma_m(E)$.*

Proof Since $1728\Delta_E^{\min} = c_4^3 - c_6^2$, it suffices to show that $\left|\Delta_E^{\min}\right| < \max\{|c_4^3|, c_6^2\}$.

Case I. Suppose $c_4, \Delta_E^{\min} > 0$. Then $\left|\Delta_E^{\min}\right| < 1728 \left|\Delta_E^{\min}\right| + c_6^2 = c_4^3$.

Case II. Suppose $c_4 = 0$. Then $|\Delta_E^{\min}| < 1728\, |\Delta_E^{\min}| = c_6^2$.

Case III. Suppose $c_4 > 0$ and $\Delta_E^{\min} < 0$. Then $|\Delta_E^{\min}| < 1728\, |\Delta_E^{\min}| + c_4^3 = c_6^2$.

Case IV. Suppose $c_4 < 0$. Let $a = \min\{|c_4^3|, c_6^2\}$, $b = \max\{|c_4^3|, c_6^2\}$, and $c = 1728\, |\Delta_E^{\min}|$. Then a, b, c are nonnegative and satisfy $a + b = c$. In particular $\frac{c}{2} < b$ since $a < b$. Hence $|\Delta_E^{\min}| < \max\{|c_4^3|, c_6^2\}$. ■

Proposition 3.8 *The following are equivalent:*

(i) *For every $\epsilon > 0$ there exists a positive constant κ_ϵ such that for all rational elliptic curves E,*

$$\max\{|c_4^3|, c_6^2\} \leq \kappa_\epsilon N_E^{6+\epsilon}; \tag{3.3}$$

(ii) *For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying*

$$N_E^{6+\epsilon} < \max\{|c_4^3|, c_6^2\}.$$

(iii) *For every $\epsilon > 0$ there are finitely many rational elliptic curves E satisfying*

$$\sigma_m(E) > 6 + \epsilon.$$

We refer to each of these equivalent statements as the **modified Szpiro conjecture**. In particular, the modified Szpiro conjecture implies Conjecture 3.6 since $|\Delta_E^{\min}| < \max\{|c_4^3|, c_6^2\}$ for all rational elliptic curves by the proof of Lemma 3.7.

Proof By definition, (ii) and (iii) are equivalent.

$(i \Longrightarrow ii)$ Fix $\epsilon > 0$ and suppose there exists a positive constant κ_ϵ so that (3.3) holds. If $\kappa_\epsilon \leq 1$, then

$$\max\{|c_4^3|, c_6^2\} \leq N_E^{6+\epsilon} \qquad \Longrightarrow \qquad \frac{\log \max\{|c_4^3|, c_6^2\}}{\log N_E} \leq 6 + \epsilon$$

and thus (iii) holds. Now suppose $\kappa_\epsilon > 1$ and towards a contradiction, assume that there are infinitely many rational elliptic curves E satisfying $\sigma_m(E) > 6 + \epsilon$. Taking logarithms in (3.3) yields

$$\log \max\{|c_4^3|, c_6^2\} \leq \log \kappa_\epsilon + (6 + \epsilon) \log N_E \qquad \Longrightarrow \qquad \sigma_m(E) \leq \frac{\log \kappa_\epsilon}{\log N_E} + 6 + \epsilon.$$

In particular,

$$6+\epsilon < \sigma_m(E) \leq \frac{\log \kappa_\epsilon}{\log N_E} + 6 + \epsilon \qquad \Longrightarrow \qquad 0 < \sigma_m(E) \leq \frac{\log \kappa_\epsilon}{\log N_E}$$

$$\Longrightarrow \qquad \log \max \left\{ c_4^3 , c_6^2 \right\} \leq \log \kappa_\epsilon$$

which is our desired contradiction since there are only finitely many elliptic curves satisfying the inequality above for any fixed constant κ_ϵ.

($iii \Longrightarrow i$) Lastly, suppose that for a given $\epsilon > 0$, there are finitely many rational elliptic curves E satisfying $\sigma_m(E) > 6+\epsilon$. In particular, there is a real number $\kappa_\epsilon \geq 1$ such that

$$\frac{\max \left\{ \left| c_4^3 \right| , c_6^2 \right\}}{N_E^{6+\epsilon}} \leq \kappa_\epsilon$$

for all rational elliptic curves E satisfying $\sigma_m(E) > 6+\epsilon$. Since $\max\{\left| c_4^3 \right| , c_6^2\} \leq N_E^{6+\epsilon}$ holds for all rational elliptic curves E satisfying $\sigma_m(E) \leq 6+\epsilon$, it follows that ($i$) holds for all rational elliptic curves. ■

Theorem 3.9 *The modified Szpiro conjecture is equivalent to the ABC Conjecture.*

Proof Assume that the modified Szpiro conjecture is true and let $P = (a, b, c)$ be an ABC triple. Relabeling if necessary, we may assume $1 \leq a < b < c$ so that $c < 2b$. In particular,

$$1 + \frac{c}{2} + \frac{c^2}{4} < a^2 + ab + b^2.$$

By Lemma 2.5, the Frey curve

$$E : y^2 = x\left(x+a\right)\left(x-b\right)$$

has minimal discriminant $\Delta_E^{\min} = u^{-12} \cdot (4abc)^2$ where u is either 1 or 2. The invariants c_4 and c_6 associated to a global minimal model of E have the form

$$c_4 = u^{-4} \cdot 16\left(a^2 + ab + b^2\right) \text{ and } c_6 = u^{-6} \cdot 32\left(b-a\right)\left(a+c\right)\left(b+c\right).$$

Hence c_4 and $\Delta_E^{\min}$ are always positive and therefore $\max\left\{c_4^3, c_6^2, 1728\Delta_E^{\min}\right\} = c_4^3$ since $c_4^3 = c_6^2 + 1728\Delta_E^{\min}$. Applying the modified Szpiro conjecture to E yields

$$\left(1 + \frac{c}{2} + \frac{c^2}{4}\right)^3 < \kappa_\epsilon N_E^{6+\epsilon}$$

for all $\epsilon > 0$. Multiplying by 64 gives

$$c^6 < 64\left(1 + \frac{c}{2} + \frac{c^2}{4}\right)^3 < 64\kappa_\epsilon N_E^{6+\epsilon}$$
$$\Longrightarrow \qquad c < 2\kappa_\epsilon^{1/6} N_E^{1+\epsilon/6}$$

for all $\epsilon > 0$. Since E is semistable at all odd primes it follows that $N_E = 2^j \operatorname{rad}\left(\Delta_E^{\min}\right)$ for some nonnegative integer j. By Lemma 2.3, $j \leq 7$ and therefore $N_E \leq 2^7 \operatorname{rad}(abc)$. Now set $\epsilon' = 6\epsilon$ so that $c < \kappa_{\epsilon'} \operatorname{rad}(abc)^{1+\epsilon'}$ with $\kappa_{\epsilon'} = \kappa_\epsilon^{1/6} 2^{2+\epsilon'}$, which is the ABC Conjecture.

Conversely, assume that the ABC Conjecture is true and let E be a rational elliptic curve with minimal discriminant $\Delta_E^{\min}$ and invariant $j_E \neq 0, 1728$. In particular, the associated invariants c_4 and c_6 are nonzero. Let $d = \gcd\left(c_4^3, c_6^2, \Delta_E^{\min}\right)$, $a = \frac{c_4^3}{d}$, $b = \frac{c_6^2}{d}$, and $c = \frac{1728\Delta_E^{\min}}{d}$. Then (a, b, c) is an ABC triple and by the ABC Conjecture we get that

$$\max\{|a|, b\} \leq \max\{|a|, b, |c|\} \leq \kappa_\epsilon \operatorname{rad}(abc)^{1+\epsilon}$$
$$\Longrightarrow \qquad \max\{ c_4^3, c_6^2 \} \leq \kappa_\epsilon \left(d \operatorname{rad}(abc)\right)^{1+\epsilon}.$$

We claim that $d \operatorname{rad}(abc)$ divides $36c_4c_6N_E$. It is clear that

$$\operatorname{rad}(abc) = \operatorname{rad}\left(6c_4^3c_6^2\Delta_E^{\min} d^{-3}\right)$$

divides $36c_4c_6N_E$. So it suffices to show that for all primes p dividing d, the inequality

$$v_p\left(d \operatorname{rad}\left(6c_4^3c_6^2\Delta_E^{\min} d^{-3}\right)\right) \leq v_p(36c_4c_6N_E)$$

holds. Since p divides d, it follows that p divides both $\Delta_E^{\min}$ and c_4 and therefore E has additive reduction at p by Lemma 2.2. Thus $v_p(N_E) \geq 2$. In particular, we have the following inequalities:

$$v_p\left(d \operatorname{rad}\left(6c_4^3c_6^2\Delta_E^{\min} d^{-3}\right)\right) \leq v_p(d) + 1 \qquad v_p(36c_4c_6) + 2 \leq v_p(36c_4c_6N_E)$$

Hence it suffices to show $v_p(d) + 1 \leq v_p(36c_4c_6) + 2$ for each prime p dividing d. For $p > 3$, we have $v_p(c_4) < 4$ or $v_p(c_6) < 6$ by [4, VII. Remark 1.1]. For $p = 2, 3$,

$v_p(c_4) < 8$ or $v_p(c_6) < 12$ [21, Proposition 3]. Since d is the greatest common divisor of c_4^3 and c_6^2, we observe that

$$v_p(d) = \min\{v_p(c_4^3), v_p(c_6^2)\} \tag{3.4}$$

for each prime p dividing d. In particular, $v_p(d) < 12$ if $p > 3$ and $v_p(d) < 24$ if $p = 2, 3$.

We now verify that $v_p(d) \leq v_p(36c_4c_6) + 1$ for $v_p(d) < 24$. by (3.4), $v_p(d)$ is divisible by 2 or 3, and

$$v_p(c_4) \geq \frac{v_p(d)}{3} \qquad \text{and} \qquad v_p(c_6) \geq \frac{v_p(d)}{2}$$

with equality holding for at least one of them. The table below summarizes all possibilities for $v_p(d) < 24$ and the middle two rows are to be read as follow: at least one of $v_p(c_4)$ or $v_p(c_6)$ is equal to the entry in the table. For instance, if $v_p(d) = 10$, then $v_p(d) = v_p(c_6^2)$ since $3v_p(c_4)$ does not divide 10. Hence $v_p(c_6) = 5$ and since $v_p(c_4^3) > v_p(c_6^2)$ and this implies that $v_p(c_4) \geq 4$. The remaining cases can be checked similarly

$v_p(d) =$	2	3	4	6	8	9	10	12	14	15	16	18	20	21	22
$v_p(c_4) \geq$	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8
$v_p(c_6) \geq$	1	2	2	3	4	5	5	6	7	8	8	9	10	11	11
$v_p(c_4c_6) + 1 \geq$	3	4	5	6	8	9	10	11	13	14	15	16	18	19	20

Thus $\max\{|c_4^3|, c_6^2\} \leq \kappa'_\epsilon (c_4c_6N)^{1+\epsilon}$ with $\kappa'_\epsilon = 36^{1+\epsilon}\kappa_\epsilon$. In particular, we obtain the following three inequalities:

$$\begin{aligned} |c_4|^{2-\epsilon} &\leq \kappa'_\epsilon (c_6N)^{1+\epsilon} \\ |c_6|^{1-\epsilon} &\leq \kappa'_\epsilon (c_4N)^{1+\epsilon} \\ \max\{ c_4^3, c_6^2 &\leq \kappa'_\epsilon (c_4c_6N)^{1+\epsilon}. \end{aligned}$$

Now raise the first inequality to the $2+2\epsilon$ power, raise the second inequality to the $3+3\epsilon$ power, and raise the third inequality to the $1-5\epsilon$ power. Multiplying the resulting inequalities results in

$$
\begin{aligned}
&|c_4|^{4+2\epsilon-2\epsilon^2}\,|c_6|^{3-3\epsilon^2}\max\left\{\left|c_4^3\right|, c_6^2\right\}^{1-5\epsilon} \leq \kappa_\epsilon'^6 N^{6+6\epsilon} c_4^{4+2\epsilon-2\epsilon^2} c_6^{3-3\epsilon^2} \\
\iff &\max\left\{\left|c_4^3\right|, c_6^2\right\}^{1-5\epsilon} \leq \kappa_\epsilon'^6 N^{6+6\epsilon} \\
\iff &\max\left\{\left|c_4^3\right|, c_6^2\right\} \leq \kappa_\epsilon'' N^{(6+6\epsilon)/(1-5\epsilon)} \text{ with } \kappa_\epsilon'' = \kappa_\epsilon'^{6/(1-5\epsilon)}.
\end{aligned}
$$

Now take $\epsilon = \frac{-6+\epsilon'}{6+5\epsilon'} > 0$ so that $\max\{|c_4^3|, c_6^2\} \leq \kappa_{\epsilon'}'' N^{6+\epsilon'}$. This is the modified Szpiro conjecture, which concludes the proof. ■

The proof above varies slightly from that given originally in [1]. The original proof reduces the argument to showing that if the modified Szpiro conjecture is true for semistable Frey curves, then the *ABC* Conjecture is true.

3.3 Database of Modified Szpiro Ratios

As with the *ABC* Conjecture, we could ask whether there are infinitely many good elliptic curves. This question was first considered by Masser [3] who proved that there are infinitely many good Frey curves. This showed, that as with the *ABC* Conjecture, we also have an equivalent formulation of the modified Szpiro conjecture, namely

$$\limsup \sigma_m(E) = 6$$

where the lim sup ranges over all rational elliptic curves E. The main theorem of the next chapter asserts that if T is one of the fifteen possible torsion subgroups allowed by Theorem 2.1, then there are infinitely many good elliptic curves E with $E(\mathbb{Q})_{\text{tors}} \cong T$. In the next section, we will prove a weaker version of this result for elliptic curves with full 2-torsion as well as expand on the history of the existence of infinitely many good curves in the literature.

In this section, we review current databases of elliptic curves with the intention of stating an explicit modified Szpiro conjecture. In addition, we wish to study the behavior of how the modified Szpiro ratio and Szpiro ratio vary as the naive height of elliptic curves increases, akin to how the ABC@Home project studied good ABC triples $P = (a, b, c)$ with $\max\{|a|, |b|, |c|\} < 2^{63}$. To this end, we create a new database consisting of elliptic curves E with $T \hookrightarrow E(\mathbb{Q})$ where $T = C_2 \times C_{2m}$ where $m = 2, 3, 4$. This will allow us to study how the modified Szpiro ratio and Szpiro ratio behave for elliptic curves with a large conductor ($> 10^{20}$).

Nitaj in [22] and [23] studied the case of the explicit Szpiro conjecture and showed that the elliptic curve

$$E_{\text{Nitaj}} : y^2 + xy = x^3 + x^2 + 349410011109107572x - 77542877461830750584255659 2$$

has conductor 2 526 810 and Szpiro ratio $\sigma(E_{\text{Nitaj}}) \approx 8.8119$. At the time, this was the elliptic curve with largest known Szpiro ratio. Recently Bennett and Yazdani [24] found the elliptic curve

$$E_{\text{B-Y}} : y^2 + xy = x^3 - 424151762667003358518x - 6292273164116612928531204122716$$

which has conductor 12 735 814 and Szpiro ratio $\sigma(E_{\text{B-Y}}) \approx 9.01996$.

These findings suggest the following explicit form of the Szpiro conjecture:

Explicit Szpiro Conjecture. For all rational elliptic curves E, $\Delta_E^{\min} < N_E^{9.02}$.

As with the explicit ABC Conjecture, this does not imply Szpiro's conjecture but can be used to tackle problems due to its absolute bound on how the minimal discriminant and conductor are related. In fact, this explicit Szpiro conjecture was used recently by Sadek [25] to study the elliptic curve discrete logarithm problem in cryptography.

While Szpiro's conjecture has been studied on the explicit side, there has been no research on the explicit modified Szpiro conjecture - which is the goal of this section. We begin by computing the modified Szpiro ratios of the previous two elliptic curves. Since $\sigma(E) < \sigma_m(E)$ we know that these are good elliptic curves and in fact, their modified Szpiro ratios are

$$\sigma_m(E_{\text{Nitaj}}) \approx 9.3169 \qquad \text{and} \qquad \sigma_m(E_{\text{B-Y}}) \approx 9.4962.$$

In contrast to the Szpiro ratio, we have found modified Szpiro ratios which exceed 10. In fact, the largest known modified Szpiro ratio is approximately 16.0587. This is the modified Szpiro ratio of the elliptic curve

$$E_{11} : y^2 - y = x^3 + x^2 - 7820x - 263580$$

which has conductor 11, yet its Szpiro ratio is equal to 1 since its $\Delta_E^{\min} = -11$. In Appendix B we order good elliptic curves by their modified Szpiro and Szpiro ratios. At the end of this section, we describe how the elliptic curves in Appendix B were found.

A technique first employed by Nitaj [23] is to check if curves isogenous to a good elliptic curve are also good. In the following example, we demonstrate this technique by considering the isogeny classes of E_{Nitaj} and $E_{\text{B-Y}}$.

Example 3.10 *Let $\mathcal{C}_{Nitaj}$ and $\mathcal{C}_{B\text{-}Y}$ denote the set of $\mathbb{Q}$-isomorphism classes of elliptic curves which are isogenous to E_{Nitaj} and $E_{B\text{-}Y}$, respectively. Then $\mathcal{C}_{Nitaj} = \{[E_1], [E_2], [E_3], [E_4]\}$ and $\mathcal{C}_{B\text{-}Y} = \{[F_1], [F_2]\}$ and computing their modified Szpiro ratio and Szpiro ratio yields:*

	E_1	E_2	E_3	E_4	F_1	F_2
$\sigma(-)$	8.81194	8.46189	8.22578	8.34794	9.01996	8.62243
$\sigma_m(-)$	9.31690	9.14240	8.77950	9.70439	9.49618	9.05540

Remark Each curve in the two isogeny classes above are good, but this is not the case in general. For instance, if $\mathcal{C}$ is the isogeny class of the elliptic curve

$$E_1 : y^2 + xy = x^3 - 2342114817x - 46491207963039,$$

then $\mathcal{C} = \{[E_1], [E_2], [E_3]\}$ has three distinct $\mathbb{Q}$-isomorphism classes and computing the modified Szpiro ratio and Szpiro ratio for these curves returns

	E_1	E_2	E_3
$\sigma(-)$	5.23078	4.76945	4.77440
$\sigma_m(-)$	5.98001	5.35237	7.00531

and therefore only one of the elliptic curves in the isogeny class is good.

3.3.1 Current Databases of Elliptic Curves

Our first step in analyzing good elliptic curves is by considering Cremona's database [26] which, as of May 2018, has an exhaustive list of elliptic curves whose conductor is at most 400 000. For each of these elliptic curves, we have computed their modified Szpiro ratio and Szpiro ratio. This has been done previously by Bennett and Yazdani [24] where they computed the Szpiro ratio of all elliptic curves in Cremona's database, which at the time had an exhaustive list of elliptic curves with conductor at most 230 000. Table 3.1 summarizes our findings for both the modified Szpiro ratio and Szpiro ratio of elliptic curves in Cremona's database,

Table 3.1.: Modified Szpiro and Szpiro Ratios in Cremona's Database

Conductor	1-99999	100000-199999	200000-299999	300000-399999	Total
# of Curves	657 396	624 965	607 003	594 285	2 483 649
$\sigma_m > 6$	30 641	17 903	14 774	12 949	76 267
% w. $\sigma_m > 6$	4.66%	2.86%	2.44%	2.18%	3.07%
$\sigma_m > 7$	7 798	3 621	2 697	2 358	16 474
$\sigma_m > 8$	1 415	474	303	266	2 458
$\sigma_m > 9$	196	43	15	21	275
$\sigma_m > 10$	26	2	0	0	28
$\sigma > 6$	4 061	2 561	2 096	1 861	10 579
$\sigma > 7$	534	272	214	182	1 202
$\sigma > 8$	41	15	10	2	68

In contrast to Cremona's database, the Stein-Watkins database [27] as of May 2018 contains 36 832 795 elliptic curves with conductor at most 10^8. This database is constructed by finding elliptic curves whose minimal discriminant $\Delta_E^{\min}$ satisfies $\Delta_E^{\min} \leq 10^{12}$ and whose conductor is at most 10^8. For each rational elliptic curve which satisfies these conditions, they compute its isogeny class as well as certain twists of representatives in the isogeny class to attain a larger database of elliptic curves which may not satisfy the original assumptions. From this data, they then input more elliptic curves into the database via isogenies and twists. By construction, the Stein-Watkins database does not have an exhaustive list of elliptic curves of conductor at most 10^8 and furthermore misses most good elliptic curves. To illustrate this, we compared Cremona's database to the Stein-Watkins database for elliptic curves of conductor at most 400 000. We found that the Stein-Watkins database has 1 766 993 elliptic curves or roughly 71.2% of all elliptic curves of conductor at most 400 000. Moreover, the Stein-Watkins database for elliptic curves of conductor at most 400 000 contains 14 894 good elliptic curves, of these, only 384 elliptic curves satisfy $\sigma(E) > 6$. For these reasons, we did not pursue a further study of the Stein-Watkins database.

Constructing an exhaustive database of elliptic curves up to a given conductor is difficult and Cremona's achievement[1] is the state of the art in this direction. If we instead focus our attention on the naive height of an elliptic curve, then it is much simpler to create an exhaustive database. This has been done recently in [28], where Balakrishnan et al. considered the collection of elliptic curves $\mathcal{F}_n$ where

$$\mathcal{F}_n = \left\{ [E]_{\mathbb{Q}} \mid E : y^2 = x^3 + a_4 x + a_6,\ a_4, a_6 \in \mathbb{Z},\ \Delta_E \neq 0,\ \max\{4 \left| a_4^3 \right|, 27a_6^2\} \leq n \right\}$$

where $[E]_{\mathbb{Q}}$ denotes the $\mathbb{Q}$-isomorphism class of E. For $n = 2.7 \cdot 10^{10}$, they found that $\#\mathcal{F}_n = 238\,764\,310$. We note that Balakrishnan et al. refer to the quantity $\max\{4\left|a_4^3\right|, 27a_6^2\}$ as the naive height of E which is slightly different than the one defined in this thesis since it does not depend on a global minimal model. While this collection of elliptic curves is significantly larger than the number of elliptic curves found in Cremona's and the Stein-Watkins database, it is insufficient for studying the explicit side of the modified Szpiro conjecture as the following lemma demonstrates.

[1]By Cremona's achievement, we mean the works of Birch, Cremona, Stein, Swinnerton-Dyer, and Wakins whose efforts constructed the exhaustive database of rational elliptic curves up to conductor 400 000.

Lemma 3.11 *If E is a good curve in $\mathcal{F}_n$ where $n = 2.7 \cdot 10^{10}$, then the conductor of E is at most* 301. *In particular, E is in Cremona's database.*

Proof Let $E : y^2 = x^3 + a_4 x + a_6$ be a good curve contained in $\mathcal{F}_n$ of conductor N. Then $N^6 < \max\{|c_4^3|, c_6^2\}$ where c_4 and c_6 are the invariants associated to a global minimal model of E. Since E is contained in $\mathcal{F}_n$ it also satisfies $\{4\,|a_4^3|, 27a_6^2\} \leq n$. Let $\tilde{c}_4$ and $\tilde{c}_6$ denote the invariants associated to the given Weierstrass model of E. Then

$$\tilde{c}_4 = -48a_4 \qquad \text{and} \qquad \tilde{c}_6 = -864a_6.$$

Since E is given by an integral Weierstrass model, it follows that $c_4 = u^{-4}\tilde{c}_6$ and $c_6 = u^{-6}\tilde{c}_6$ for some positive integer u by Lemma 2.4. Therefore,

$$\begin{aligned} N^6 &< \max\{|c_4^3|, c_6^2\} \leq \max\{|\tilde{c}_4^3|, \tilde{c}_6^2\} = 32^2 \cdot 27 \max\{4\,|a_4^3|, 27a_6^2\} \leq 32^2 \cdot 27^2 \cdot 10^9 \\ \implies & \qquad N < 301.19. \end{aligned}$$

■

3.3.2 New Databases of Elliptic Curves

In order to bypass the bottleneck presented by the aforementioned databases in studying the explicit modified Szpiro conjecture, we will focus on elliptic curves E with $E(\mathbb{Q})_{\text{tors}} \hookleftarrow T$ where $T = C_2 \times C_{2m}$ for $m = 2, 3, 4$. Recall that these elliptic curves are parameterized by the curve $\mathcal{X}_t(T)$, as defined in Table 2.1. Recall that the naive height of an elliptic curve E is defined as the quantity

$$h_{\text{naive}}(E) = \frac{1}{12} \log \max\{|c_4^3|, c_6^2\}.$$

We will now show that for elliptic curves E with $T \hookrightarrow E(\mathbb{Q})$ we can create an exhaustive database up to a certain naive height.

By Lemma 2.4 there exists relatively prime integers a and b such that $E_T(a, b)$ is $\mathbb{Q}$-isomorphic to $\mathcal{X}_{b/a}$ where $E_T = E_T(a, b)$ is as defined in Table D.1. By Lemma 2.4 we also have that the discriminant of E_T is $\gamma_T = \gamma_T(a, b)$ and the invariants c_4 and

c_6 of the Weierstrass model for E_T are given by $\alpha_T = \alpha_T(a,b)$ and $\beta_T = \beta_T(a,b)$, respectively. Since γ_T is a square, it follows that $\alpha_T > \beta_T$ from the identity $\alpha_T^3 - \beta_T^2 = 1728\gamma_T$.

Now consider the set of rational numbers

$$S = \left\{ (a,b) \in \mathbb{Z}^2 \mid a,b \neq 0,\ \gcd(a,b) = 1,\ |a|\,,|b| \leq 7000 \right. .$$

It can be verified with SageMath [29] that $\#S = 59\,580\,582$. For each T, we construct the following set:

$$\mathcal{F}_T = \{E_T(a,b)_{\text{reduced}} \mid (a,b) \in S,\ \gamma_T(a,b) \neq 0\}$$

where $E_T(a,b)_{\text{reduced}}$ is the reduced minimal model of $E_T(a,b)$. In other words, the map

$$E_T(a,b)_{\text{reduced}} \longmapsto [E_T(a,b)]$$

is a bijection between $\mathcal{F}_T$ and the set of $\mathbb{Q}$-isomorphism classes of elliptic curves which have a representative $E_T(a,b)$ for $(a,b) \in S$. Note that $\#\mathcal{F} < \#S$ since the $\mathbb{Q}$-rational noncuspidal points of the modular curves $X_1(2,2m)$. Recall that the modular curve $X_1(2,2m)$ (with cusps removed) parameterize isomorphism classes of pairs (E,P,Q) where E is a rational elliptic curve and $\langle P,Q\rangle \cong C_2 \times C_{2m}$ and $e(P,mQ) = \zeta_2$ where e_2 is the Weil pairing. In particular, the $\mathbb{Q}$-isomorphism class of E may contain distinct isomorphism classes of pairs $(E,(P,Q))$. In fact, computing the order of $\mathcal{F}_T$ shows that this is the case,

T	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
$\#\mathcal{F}_T$	49 030 354	47 003 904	34 754 904

Now let u_T and l_T be the real numbers defined in Table 3.2

In order to show that $\mathcal{F}_T$ contains all elliptic curves $E_T(a,b)$ up to a certain naive height, we admit the following result which will be proven in Chapter 5:

Lemma 3.12 *Let $c_{4,T}$ be the invariant associated with a global minimal model of $E_T(a,b)$. Then $u_T^{-4}\alpha_T \leq c_{4,T}$.*

Table 3.2.: The numbers u_T and l_T

T	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
u_T	4	16	64
l_T	3.2433	6.4865	13.5747

Proof This follows automatically from Theorem 5.14. ■

We can now show that $\mathcal{F}_T$ contains an exhaustive list of rational elliptic curves whose naive height is at most l_T. To this end, we will consider the following two sets in the next two results:

$$R_+ = \left\{(x, y) \in \mathbb{R}^2 \mid x, y > 0 \right. \qquad \text{and} \qquad R_- = \left\{(x, y) \in \mathbb{R}^2 \mid x > 0, y < 0 \right. .$$

Lemma 3.13 *Let $\epsilon, \delta \geq 0$ with equality holding for at most one them. Then*

$$\alpha_T(x, y) \leq \begin{cases} \alpha_T(x + \epsilon, y + \delta) & \text{for } T = C_2 \times C_4, C_2 \times C_8 \text{ and } (x, y) \in R_+ \\ \alpha_T(x + \epsilon, y - \delta) & \text{for } T = C_2 \times C_6 \text{ and } (x, y) \in R_-. \end{cases} \tag{3.5}$$

Proof VIa a computer algebra system such as Mathematica [30] it is verified that the partial derivative $\frac{\partial}{\partial x}\alpha_T(x, y) > 0$ on R_+ for each T. Whereas the partial derivative $\frac{\partial}{\partial y}\alpha_T(x, y) > 0$ on R_+ for $T = C_2 \times C_4, C_2 \times C_8$ and the partial derivative $\frac{\partial}{\partial y}\alpha_T(x, y) < 0$ on R_- for $T = C_2 \times C_6$.

By the Mean Value Theorem, we can find P and P' in $R_\pm$ such that

$$\begin{aligned} 0 &< \frac{\partial \alpha_T}{\partial x}(P) = \frac{\alpha_T(x + \epsilon, y \pm \delta) - \alpha_T(x, y \pm \delta)}{\epsilon} \\ 0 &< \pm\frac{\partial \alpha_T}{\delta_T}(P') = \pm\left(\frac{\alpha_T(x, y \pm \delta) - \alpha_T(x, y)}{\delta}\right) \end{aligned}$$

This yields

$$\alpha_T(x + \epsilon, y \pm \delta) - \alpha_T(x, y) = \epsilon\frac{\partial \alpha_T}{\partial x}(P) \pm \delta\frac{\partial \alpha_T}{\partial y}(P') > 0.$$

■

Theorem 3.14 *Let E be an elliptic curve with $T \hookrightarrow E(\mathbb{Q})$. If $h_{naive}(E) \leq l_T$, then E is $\mathbb{Q}$-isomorphic to $E_T(a,b)$ for some $(a,b) \in S$.*

Proof Since $T \hookrightarrow E(\mathbb{Q})$, there exists a rational number t such that E is $\mathbb{Q}$-isomorphic to $\mathcal{X}_t(T)$. We claim that $\mathcal{X}_t(T)$ is $\mathbb{Q}$-isomorphic to the curve $\mathcal{X}_{t_j}(T)$ where t_j is given in Table 3.3.

Table 3.3.: Quantities for Proof of Theorem 3.14

T	j	t_j	u_j	r_j	s_j	w_j	I_j
$C_2 \times C_4$	1	$\frac{-(1+4t)}{4}$	1	0	0	0	$\left(-\infty, -\frac{1}{4}\right)$
	2	$\frac{-(1+4t)}{4(1+8t)}$	$8t+1$	$2\left(4t^2+2\right)$	$4t$	$4t^2\left(4t+1\right)$	$\left(-\frac{1}{4}, -\frac{1}{8}\right)$
	3	$\frac{-t}{1+8t}$	$8t+1$	$2\left(4t^2+2\right)$	$4t$	$4t^2\left(4t+1\right)$	$\left(-\frac{1}{8}, \infty\right)$
$C_2 \times C_6$	1	$\frac{15+t}{-1+t}$	$\frac{t-9}{2(t-3)}$	$\frac{-2(t-5)(t-1)}{(t+3)(t-3)^2}$	$\frac{4(1-t)}{t^2-9}$	$\frac{4(t-5)(t-1)^2}{(t+3)^2(t-3)^3}$	$(-15, 1)$
	2	$\frac{-21+5t}{-1+t}$	$\frac{t-9}{t+3}$	$\frac{4(5-t)(t-1)}{(t+3)^2(t-3)}$	$-\frac{8}{t+3}$	$\frac{16(t-1)(t-5)^2}{(t-3)^2(t+3)^3}$	$\left(1, \frac{21}{5}\right)$
	3	$\frac{-9+5t}{-5+t}$	1	0	0	0	$\left(\frac{9}{5}, 5\right)$
	4	$\frac{-21+t}{-5+t}$	$\frac{t-9}{2(t-3)}$	$\frac{-2(t-5)(t-1)}{(t+3)(t-3)^2}$	$\frac{4(1-t)}{t^2-9}$	$\frac{4(t-5)(t-1)^2}{(t+3)^2(t-3)^3}$	$(5, 21)$
	5	$6-t$	$\frac{t-9}{t+3}$	$\frac{4(5-t)(t-1)}{(t+3)^2(t-3)}$	$-\frac{8}{t+3}$	$\frac{16(t-1)(t-5)^2}{(t-3)^2(t+3)^3}$	$(6, \infty)$
$C_2 \times C_8$	1	$\frac{-(1+2t)}{2}$	$\frac{\left(8t^2+8t+1\right)}{2t(8t^2-1)} \cdot (2t+1)$	$\frac{\left(8t^2+4t+1\right)}{2t(1-8t)^2} \cdot \frac{(2t+1)(4t+1)}{1}$	$\frac{(4t+1)^2}{2t(8t^2-1)}$	$\frac{\left(8t^2+4t+1\right)}{4t^2(8t^2-1)^3} \cdot \frac{(2t+1)^2(4t+1)}{1}$	$\left(-\infty, -\frac{1}{2}\right)$
	2	$\frac{-(1+4t)}{4(1+2t)}$	1	0	0	0	$\left(-\frac{1}{2}, -\frac{1}{4}\right)$
	3	$\frac{-(1+4t)}{8t}$	$\frac{\left(8t^2+8t+1\right)}{2t(8t^2-1)} \cdot (2t+1)$	$\frac{\left(8t^2+4t+1\right)}{2t(1-8t)^2} \cdot \frac{(2t+1)(4t+1)}{1}$	$\frac{(4t+1)^2}{2t(8t^2-1)}$	$\frac{\left(8t^2+4t+1\right)}{4t^2(8t^2-1)^3} \cdot \frac{(2t+1)^2(4t+1)}{1}$	$\left(-\frac{1}{4}, 0\right)$

For each j, let u_j, r_j, s_j, w_j be as given in Table 3.3. The admissible change of variables $x \longmapsto u_j^2 x + r_j$ and $y \longmapsto u_j^3 y + u_j s_j x + w_j$ gives a $\mathbb{Q}$-isomorphism between $\mathcal{X}_t(T)$ and $\mathcal{X}_{t_j}(T)$.

We now claim that if $t < 0$ (resp. $t > 0$), then at least one $t_j > 0$ (resp. $t_j < 0$) for $T = C_2 \times C_4, C_2 \times C_8$ (resp. $T = C_2 \times C_6$).

First, suppose T is $C_2 \times C_4$ or $C_2 \times C_8$. It is easily checked that $t_j > 0$ for $t \in I_j \cap \mathbb{Q}$ where I_j is the open interval given in Table 3.3.

Similarly, if $T = C_2 \times C_6$, then $t_j < 0$ for $t \in I_j \cap \mathbb{Q}$ where I_j is the open interval given in Table 3.3.The claim now follows. By Lemma 2.4, $\mathcal{X}_{b/a}(T)$ is $\mathbb{Q}$-isomorphic to $E_T(a, b)$. Since $E_T(a, -b) = E_T(-a, b)$, we conclude that if E is an elliptic curve with $T \hookrightarrow E(\mathbb{Q})$, then there are relatively prime integers a and b such that E is $\mathbb{Q}$-isomorphic to $E_T(a, b)$ where $a > 0, b > 0$ (resp. $b < 0$) if $T = C_2 \times C_4, C_2 \times C_8$ (resp. $T = C_2 \times C_6$).

Now let u_T be as defined in (3.2) and define $h_T = 12^{-1} \log\left(u_T^{-4} \alpha_T(x, y)^3\right)$. Set

$$
\begin{array}{ll}
S_1 = \{(x, y) \in \mathbb{Z}^2 \mid x > 0, y > 7000\} & S_1' = \{(x, y) \in \mathbb{Z}^2 \mid x > 0, y < -7000\} \\
S_2 = \{(x, y) \in \mathbb{Z}^2 \mid x > 7000, y > 0\} & S_2' = \{(x, y) \in \mathbb{Z}^2 \mid x > 7000, y < 0\} \\
S_3 = \{(x, y) \in \mathbb{Z}^2 \mid x > 7000, y > 7000\} & S_3' = \{(x, y) \in \mathbb{Z}^2 \mid x > 7000, y < -7000\}
\end{array}
$$

In particular, S_3 (resp. S_3') is the union of S_1 and S_2 (resp. S_1' and S_2'). By Lemma 3.13, we have that the minimum value of h_T on S_3 (resp. S_3') occurs on the boundary of S_3 (resp. S_3').

$$
\begin{array}{ll}
h_T|_{S_3'} \geq l_T = \min\{h_T|_{S_1}, h_T|_{S_2}\} & \text{if } T = C_2 \times C_4, C_2 \times C_8 \\
h_T|_{S_3'} \geq l_T = \min\{h_T|_{S_1'}, h_T|_{S_2'} & \text{if } T = C_2 \times C_6.
\end{array}
\tag{3.6}
$$

Now let `alpT` and `uT` be the Mathematica input for $\alpha_T(x, y)$ and u_T, respectively. We then verify that l_T is the value claimed in (3.2) via the Mathematica input:

```
NMinimize[Log[{12^-1Log[10,alpT/uT^4)^3],x>0&&y>7000},{x,y},Integers]
NMinimize[Log[{12^-1Log[10,alpT/uT^4)^3],x>7000&&y>0},{x,y},Integers]
```

for $T = C_2 \times C_4, C_2 \times C_8$ and

```
NMinimize[Log[{12^-1Log[10,alpT/uT^4)^3],x>0&&y<-7000},{x,y},Integers]
NMinimize[Log[{12^-1Log[10,alpT/uT^4)^3],x>7000&&y<0},{x,y},Integers]
```

for $T = C_2 \times C_6$.

Lastly, suppose $h_{\text{naive}}(E_T(a, b)) < l_T$. By the second claim we may assume $(a, b) \in R_+$ if $T = C_2 \times C_4, C_2 \times C_8$ or $(a, b) \in R_-$ if $T = C_2 \times C_6$. Since

$$
12^{-1} \log\left(u_T^{-4} \alpha_T(a, b)^3\right) \leq h_{\text{naive}}(E_T(a, b))
$$

by Lemma 3.12 it follows that $(a, b) \in S$ by (3.6), as desired. ■

Thus $\mathcal{F}_T$ contains an exhaustive list of elliptic curves of naive height at most l_T. In particular,

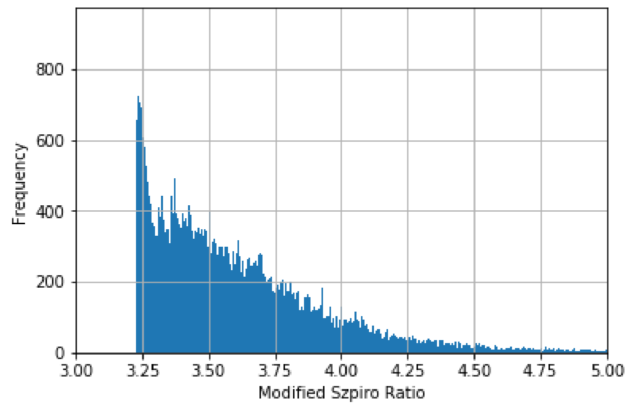
T	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
$\#\{E \in \mathcal{F}_T \mid h_{\text{naive}}(E) < l_T\}$	502 472	701 964	1 106 884

For each elliptic curve E in $\mathcal{F}_T$, we saved the following information into our database: its reduced minimal model, a pair (a, b) in S such that E is $\mathbb{Q}$-isomorphic to $E_T(a, b)$, its naive height, its modified Szpiro ratio, and its Szpiro ratio. The table below summarizes the data obtained on good elliptic curves in $\mathcal{F}_T$.

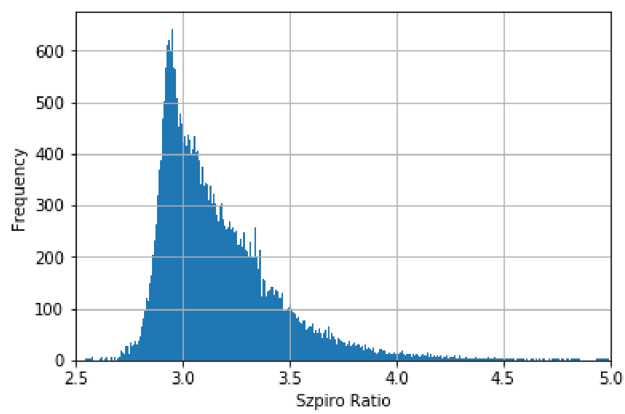
T	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
Max σ_m	8.4797	8.5262	7.3412
Max σ	6.8890	7.2555	6.9407
# of Curves w. $\sigma_m > 6$	915	11 085	7 480
# of Curves w. $\sigma > 6$	79	1 139	967

The above table is insufficient in conveying the information obtained from our database of elliptic curves arising from each $\mathcal{F}_T$. To this end, the next three subsections provide histograms for the naive height, modified Szpiro ratio, and Szpiro ratio of those elliptic curves in $\{E \in \mathcal{F}_T \mid h_{\text{naive}}(E) < l_T\}$ with a bin size of 10 000. At the end of Appendix B we provide further histograms for the naive height, modified Szpiro ratio, and Szpiro ratio of elliptic curves in $\mathcal{F}_T$ with a bin size of 50 000.

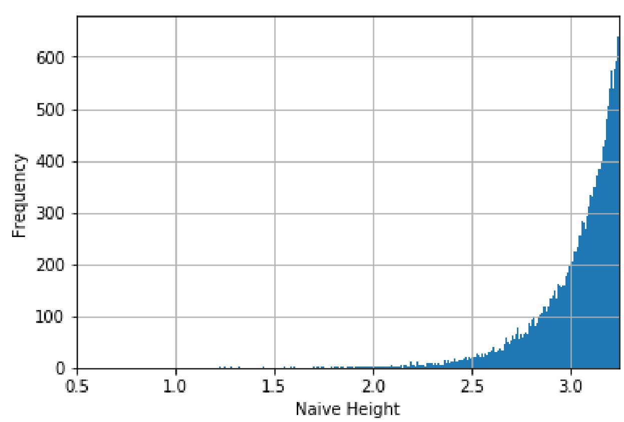
Summary of Data for $\mathcal{F}_{C_2 \times C_4}$



(a) Modified Szpiro Ratio in $\mathcal{F}_{C_2 \times C_4}$



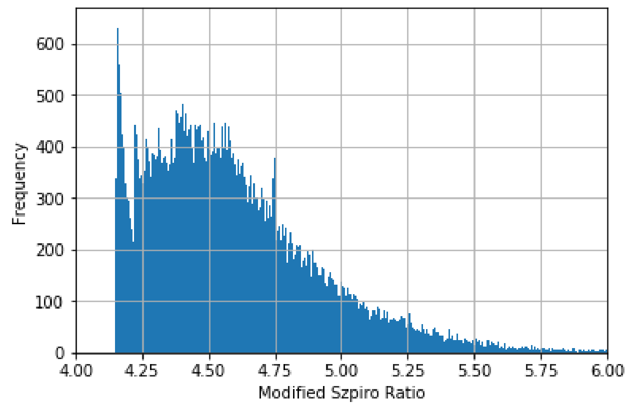
(b) Szpiro Ratio in $\mathcal{F}_{C_2 \times C_4}$



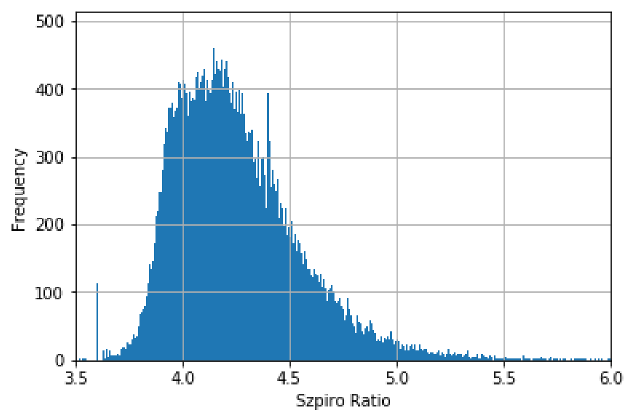
(c) Naive Height in $\mathcal{F}_{C_2 \times C_4}$

Figure 3.1.: Histograms for Exhaustive Subregion of $\mathcal{F}_{C_2 \times C_4}$

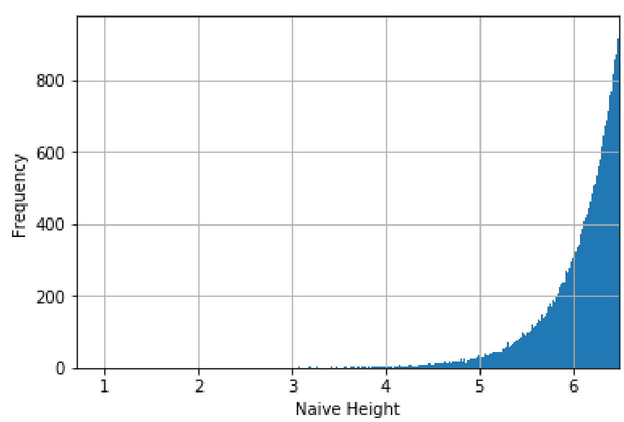
Summary of Data for $\mathcal{F}_{C_2 \times C_6}$



(a) Modified Szpiro Ratio in $\mathcal{F}_{C_2 \times C_6}$



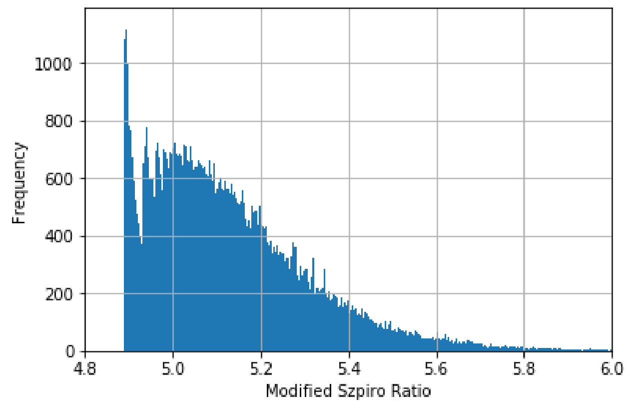
(b) Szpiro Ratio in $\mathcal{F}_{C_2 \times C_6}$



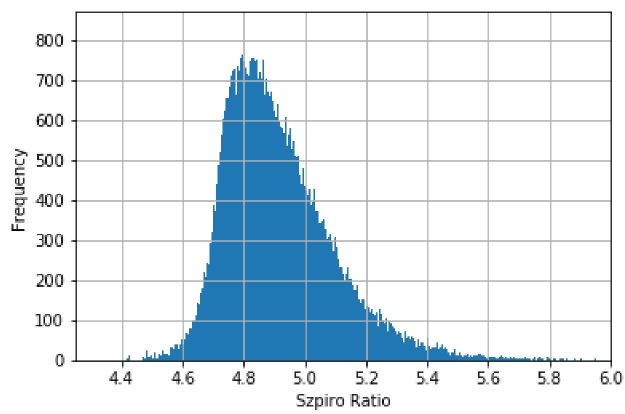
(c) Naive Height in $\mathcal{F}_{C_2 \times C_6}$

Figure 3.2.: Histograms for Exhaustive Subregion of $\mathcal{F}_{C_2 \times C_6}$

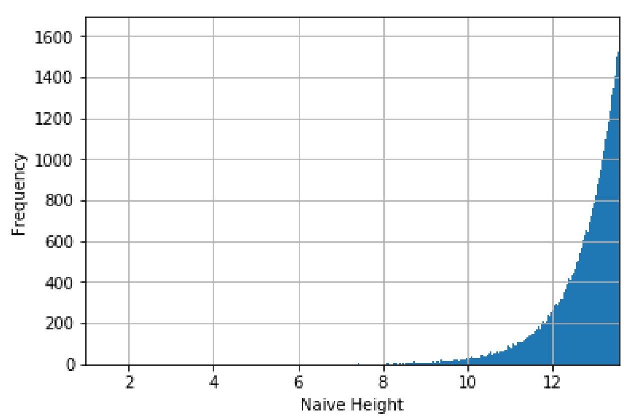
Summary of Data for $\mathcal{F}_{C_2\times C_8}$



(a) Modified Szpiro Ratio in $\mathcal{F}_{C_2\times C_8}$



(b) Szpiro Ratio in $\mathcal{F}_{C_2\times C_8}$



(c) Naive Height in $\mathcal{F}_{C_2\times C_8}$

Figure 3.3.: Histograms for Exhaustive Subregion of $\mathcal{F}_{C_2\times C_8}$

The set $\bigcup_T \mathcal{F}_T$ contains 19 480 distinct good elliptic curves. Of these, 225 occur in Cremona's database. By Nitaj's heuristic, we expect to get more good elliptic curves by considering representatives in the isogeny class of these good elliptic curves. Motivated by the remark following Example 3.10, we consider elliptic curves in $\mathcal{F}_T$ whose modified Szpiro ratio is at least 5.7. In particular, we construct the following set

$$\mathcal{S}^{(1)} = \bigcup_T \{E \in \mathcal{F}_T \mid \sigma_m(E) > 5.7,\ N_E > 400\,000\}\,. \tag{3.7}$$

For each $E \in \mathcal{S}^{(1)}$, we compute its isogeny class and consider those $\mathbb{Q}$-isomorphism classes of elliptic curves which have representatives E with $\sigma_m(E) > 6$. To this end, for a set S of $\mathbb{Q}$-isomorphism classes of elliptic curves, let $\mathcal{I}$ be the map defined by

$$\mathcal{I}(S) = \big\{[E]_{\mathbb{Q}} \mid E \text{ is isogenous to a curve in } S \text{ and } \sigma_m(E) > 6 \quad . \tag{3.8}$$

Returning to the set $\mathcal{S}^{(1)}$ above, we compute the order $\#\mathcal{I}\big(\mathcal{S}^{(1)}\big) = 248\,391$. Since isogenous elliptic curves have the same conductor, we conclude that for each $[E]_{\mathbb{Q}} \in \mathcal{I}\big(\mathcal{S}^{(1)}\big)$, E is not in Cremona's database. Below we give a brief summary of the elliptic curves found in $\mathcal{I}\big(\mathcal{S}^{(1)}\big)$.

# of $[E]_{\mathbb{Q}} \in \mathcal{I}\big(\mathcal{S}^{(1)}\big)$ with $\sigma(E) > 6$	Max σ_m	Max σ	Max h_{naive}	Max N_E
36 315	9.2416	7.8063	18.1118	$1.548 \cdot 10^{36}$

In the next two sections, we develop an efficient way of computing good elliptic curves. Specifically, we will construct additional sets $\mathcal{S}^{(j)}$ and then consider $\mathcal{S} = \bigcup_j \mathcal{S}^{(j)}$. We will then show that $\mathcal{I}(\mathcal{S})$ has 13 870 964 distinct $\mathbb{Q}$-isomorphism classes of elliptic curves whose representatives are good.

We conclude this section by noting that there is a leftward shift in comparing the histograms for the modified Szpiro ratio of $\{E \in \mathcal{F}_T \mid h_{\text{naive}}(E) < l_T\}$ and $\mathcal{F}$. This will be explained in Chapter 6 where we show that the modified Szpiro ratio of an elliptic curve is bounded below by a number depending only on the torsion subgroup of the elliptic curve. Below is the main result which explains the behavior observed in the three histograms.

Theorem 6.6 Let T be one of the fifteen torsion subgroups allowed by Theorem 2.1. If $T \hookrightarrow E(\mathbb{Q})$, then $\sigma_m(E) > l_T$ where l_T is as given below:

T	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
l_T	1	1.5	3	3	3	3	4	4

T	C_9	C_{10}	C_{12}	$C_2 \times C_2$	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
l_T	4.5	4.5	4.8	2	3	4	4.8

This result motivates the following conjecture which is an analogue the aforementioned Theorem by Browkin et al [18]:

Conjecture 3.15 *Assuming the modified Szpiro conjecture, the set of limit points of $\sigma_m(E)$ as E ranges over all elliptic curves is equal to the closed interval $[1, 6]$. Moreover, if T is one of the fifteen torsion subgroups allowed by Theorem 2.1 and l_T is defined in Theorem 6.6, then the set of limit points of $\sigma_m(E)$ as E ranges over all elliptic curves with $T \hookrightarrow E(\mathbb{Q})$ is equal to the closed interval $[l_T, 6]$.*

In Corollary 6.20 we show that 1 is in the set of limit points of $\sigma_m(E)$ as E ranges over all elliptic curves.

3.4 Infinitely Many Good Frey Curves

While Masser [3] proved that there are infinitely many good Frey curves, his proof was non-constructive. Nitaj [22] [23] improved on Masser's result by showing how good ABC triples can be used to construct good elliptic curves, but his approach has to be done one elliptic curve at a time. Our goal in this section and the next chapter is to develop techniques which will allow for the construction of infinitely many good elliptic curves with specified torsion subgroup. Our work is motivated by Lemma 3.3, where fixing an odd prime p results in the explicit family of good ABC triples $\left\{\left(1, p^{(p-1)k} - 1, p^{(p-1)k}\right)\right\}_{k\geq 1}$. The main theorem of this section is based on an unpublished work which is included in Appendix A.

Let $P = (a, b, c)$ be an ABC triple with a even and $b \equiv 1 \bmod 4$. For $T = C_2 \times C_{2m}$ where $m = 1, 2, 3, 4$, let $\mathfrak{A}_T = \mathfrak{A}_T(a, b)$, $\mathfrak{B}_T(a, b)$, $\mathfrak{C}_T = C_T(a, b)$, and $\mathfrak{D}_T = \mathfrak{D}_T(a, b)$ be as defined in Table A.3. Assume further that $a \equiv 0 \mod 3$ if $T = C_2 \times C_6$. Then the elliptic curve $F_T = F_T(a, b)$ given by the Weierstrass model

$$F_T : y^2 = x\,(x - \mathfrak{A}_T)(x + \mathfrak{B}_T)$$

is semistable and satisfies $F_T(\mathbb{Q})_{\text{tors}} \cong T$ by Lemma A.6. Moreover, by Lemma 2.5 the minimal discriminant of F_T is $\Delta_T = (16^{-1}\mathfrak{A}_T\mathfrak{B}_T\mathfrak{C}_T)^2$ and the invariant $c_{4,T} = c_{4,T}(a, b)$ associated with a global minimal model of F_T is

Table 3.4.: The Invariant c_4 of F_T

$c_{4,T}$	T
$a^8 + 60a^6b^2 + 134a^4b^4 + 60a^2b^6 + b^8$	$C_2 \times C_2$
$a^8 + 14a^4b^4 + b^8$	$C_2 \times C_4$
$9a^8 + 228a^6b^2 + 30a^4b^4 - 12a^2b^6 + b^8$	$C_2 \times C_6$
$a^{16} - 8a^{14}b^2 + 12a^{12}b^4 + 8a^{10}b^6 + 230a^8b^8 + 8a^6b^{10} + 12a^4b^{12} - 8a^2b^{14} + b^{16}$	$C_2 \times C_8$

Lemma 3.16 *Let $P = (a, b, c)$ be a good positive ABC triple satisfying $a \equiv 0 \mod 2$, $b \equiv 1 \mod 4$, and $\frac{b}{a} > \theta_T$ where θ_T is as given in Lemma A.2. Assume further that $a \equiv 0 \mod 3$ if $T = C_2 \times C_6$. Then the Frey curve $F_T = F_T(\mathfrak{A}_T, \mathfrak{B}_T)$ is good and $F_T(\mathbb{Q})_{tors} \cong T$.*

Proof By Lemma A.6, $F_T(\mathbb{Q})_{\text{tors}} \cong T$. Since F_T is a Frey curve we have that the invariants c_4 and c_6 associated to a global minimal model of F_T satisfy $\max\{|c_4^3|, c_6^2\} = c_4^3$ since c_4 is always positive. The congruences on a and b imply that $c_4 = c_{4,T}$. It, therefore, suffices to show that $c_{4,T}^3 - N_T^6 > 0$ where N_T is the conductor of F_T. Since F_T is semistable,

$$N_T = \operatorname{rad}(\mathfrak{A}_T\mathfrak{B}_T\mathfrak{C}_T) < \mathfrak{D}_T$$

by Lemma A.4. Note that D_T is positive since $\frac{b}{a} > \theta_T$. Thus

$$\frac{c_{4,T}^3 - N_T^6}{\mathfrak{D}_T(1,t)^6} > \frac{c_{4,T}(1,t)^3 - \mathfrak{D}_T(1,t)^6}{\mathfrak{D}_T(1,t)^6} \text{ for } t = \frac{b}{a} \tag{3.9}$$

Lastly, for each T, the polynomial $c_{4,T}(1,t)^3 - \mathfrak{D}_T(1,t)^6$ is positive on the open interval (θ_T, ∞) from which we conclude that F_T is a good elliptic curve. ■

Theorem 3.17 *For each T, let $P_0^T = (a_0, b_0, c_0)$ be a good positive ABC satisfying $a_0 \equiv 0 \mod 2$, $b_0 \equiv 1 \mod 4$, and $\frac{b_0}{a_0} > \theta_T$ where θ_T is as given in Lemma A.2. Assume further that $a_0 \equiv 0 \mod 3$ if $T = C_2 \times C_6$. For $j \geq 1$, define P_j^T recursively by*

$$P_j^T = (a_j, b_j, c_j) = \left(\mathfrak{A}_T(a_{j-1}, b_{j-1}), \mathfrak{B}_T(a_{j-1}, b_{j-1}), \mathfrak{C}_T(a_{j-1}, b_{j-1})\right).$$

Then for each j, the Frey curve $F_T(a_j, b_j)$ is good and $F_T(a_j, b_j)(\mathbb{Q})_{tors} \cong T$.

Proof By Proposition A.5, $P_j^T = (a_j, b_j, c_j)$ satisfies $a_j \equiv 0 \mod 2$, $b_j \equiv 1 \mod 4$, and $\frac{b_j}{a_j} > \theta_T$ for each j. For $T = C_2 \times C_6$, if $a_0 \equiv 0 \mod 3$, then $a_j \equiv 0 \mod 3$ for each j. Hence P_j^T is a good positive ABC triple for each j by Proposition A.5. Therefore the result follows by Lemma 3.16. ■

In Example A.8 we began with a good ABC triple $P_0 = (a_0, b_0, c_0)$. For each T, we constructed an infinite sequence of good ABC triples $P_j^T = (a_j, b_j, c_j)$. By Theorem 3.17, each Frey curve $F_T(a_j, b_j)(\mathbb{Q})_{\text{tors}}$ is a good elliptic curve with torsion subgroup isomorphic to T. Table 3.5 lists the modified Szpiro and Szpiro ratios of the Frey curves corresponding to P_j^T. Due to computatonal limitations, we could only compute these ratios up to $j = 3$.

The above example illustrates that while we can explicitly write down infinitely many good Frey curves E, it is not necessarily the case that $\sigma(E) > 6$ infinitely many times. Observe that the main ingredient in proving Lemma 3.16 is the inequality

$$N_T^6 < \mathfrak{D}_T^6 < c_{4,T}^3.$$

Table 3.5.: Example of Good Frey Curves

T	$C_2 \times C_2$	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
$\sigma_m(F_T(a_1,b_1))$	6.4204	7.4219	6.7269	6.1985
$\sigma(F_T(a_1,b_1))$	5.9524	6.7268	5.8544	5.4642
$\sigma_m(F_T(a_2,b_2))$	6.1912	6.3124	6.1666	6.0241
$\sigma(F_T(a_2,b_2))$	6.0511	6.1586	5.6515	5.7399
$\sigma_m(F_T(a_3,b_3))$	6.0901	6.0769		
$\sigma(F_T(a_3,b_3))$	6.0656	6.0371		

Therefore, extending Lemma 3.16 to yield $\sigma(F_T) > 6$ would require a proof of the inequality

$$N_T^6 < \mathfrak{D}_T^6 < \left(\frac{\mathfrak{A}_T \mathfrak{B}_T \mathfrak{C}_T}{16}\right)^2 = \Delta_T^{\min}, \tag{3.10}$$

where $\Delta_T^{\min}$ is the minimal discriminant of F_T. However, for a given T the validity of this inequality may be false or result in stricter assumptions on the good ABC triple. As a result, an analog of Theorem 3.17 under the techniques developed in this section is not possible. To illustrate, we demonstrate what occurs for $T = C_2 \times C_2$ and $T = C_2 \times C_4$. For both of these cases, we consider the difference

$$\frac{\left(\frac{\mathfrak{A}_T \mathfrak{B}_T \mathfrak{C}_T}{16}\right)^2 - \mathfrak{D}_T^6}{\mathfrak{D}_T^6} = \frac{(\mathfrak{A}_T(1,t)\,\mathfrak{B}_T(1,t)\,\mathfrak{C}_T(1,t))^2 - 2^8\mathfrak{D}_T(1,t)^6}{2^8\mathfrak{D}_T(1,t)^6}.$$

The polynomial

$$(\mathfrak{A}_T(1,t)\,\mathfrak{B}_T(1,t)\,\mathfrak{C}_T(1,t))^2 - 2^8\mathfrak{D}_T(1,t)^6$$

is never positive for $T = C_2 \times C_2$ and is positive for $T = C_2 \times C_4$ on the interval

$$(-\theta_1, -1) \cup (-1, -\theta_2) \cup (\theta_2, 1) \cup (1, \theta_1) \tag{3.11}$$

where $\theta_1 = \sqrt[4]{\frac{33+\sqrt{65}}{32}}$ and $\theta_2 = \sqrt[4]{\frac{33-\sqrt{65}}{32}}$. In particular, inequality (3.10) never holds for $T = C_2 \times C_2$. For $T = C_2 \times C_4$, we consider the ABC triple $P =$

$(59\,969\,536, 56\,746\,089, 116\,715\,625)$ which is good since $q(P) \approx 1.1035$. Moreover, $56\,746\,089 \equiv 1 \mod 4$ and $\frac{56\,746\,089}{59\,969\,536} \approx 0.94625$ is in the interval (3.11) and so we expect the associated Frey curve to have Szpiro ratio at least 6. Indeed, the elliptic curve $F_T = F_T(59\,969\,536, 56\,746\,089)$ of conductor $\approx 4.97 \cdot 10^{28}$ satisfies

$$\sigma_m(F_T) \approx 6.6211 \qquad \sigma(F_T) \approx 6.3618.$$

Therefore an extension of Theorem 3.17 for infinitely many Frey curves for $T = C_2 \times C_4$ whose Szpiro ratio is at least 6 would require a sequence of good positive ABC triples $P_j = (a_j, b_j, c_j)$ which satisfy the following conditions for each j: $a_j \equiv 2 \mod 4$, $b_j \equiv 1 \mod 4$, and $\frac{b_j}{a_j}$ is in the interval (3.11). The stricter condition that $\frac{b_j}{a_j}$ is in the interval (3.11) for infinitely many j is not satisfied by our sequence $P_j^{C_2 \times C_4}$. Similar conclusions hold for $C_2 \times C_6$ and $C_2 \times C_8$ and therefore we are only interested in constructing good elliptic curves without requiring any assumptions of the Szpiro ratio.

3.5 Database of Good Elliptic Curves

In section 3.3, we analyzed Cremona's database which contains an exhaustive list of elliptic curves of conductor at most 400 000. This analysis showed that Cremona's database has 76 267 good elliptic curves. We then proceeded to construct databases of elliptic curves E with $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$ where $T \cong C_2 \times C_{2m}$ where $m = 2, 3, 4$. This produced a database consisting of 130 789 162 $\mathbb{Q}$-isomorphism classes of elliptic curves. We then considered the subcollection $\mathcal{S}^{(1)}$ as defined in (3.7) which consist of $\mathbb{Q}$-isomorphism classes of elliptic curves whose conductor and modified Szpiro ratio is at least 400 000 and 5.7, respectively. We then considered the set $\mathcal{I}\big(\mathcal{S}^{(1)}\big)$ where $\mathcal{I}$ is as defined in (3.8) and found that its order is 248 391. Now let $\mathcal{S}^{(2)} = \{[E]_{\mathbb{Q}} \mid E$ is in Cremona's Database and $\sigma_m(E) > 6$ so that $\mathcal{S}^{(2)} = \mathcal{I}\big(\mathcal{S}^{(2)}\big)$ since isogenous curves have the same conductor. By Table (3.1), $\#\mathcal{S}^{(2)} = 76\,267$. In particular, the methods of section 3.3 resulted in 324 658 good elliptic curves.

In this section, we will construct additional sets $\mathcal{S}^{(j)}$ with the intention of constructing 13 870 964 good $\mathbb{Q}$-isomorphism classes of elliptic curves. This will be done by using good ABC triples to construct good elliptic curves via the Frey curves F_T of the previous section as well as the elliptic curves $H_T = H_T(a,b)$ which will be studied in further detail in the next chapter. To this end, let

$$\mathcal{A}_n = \left\{(a,b) \in \mathbb{Z}^2 \mid (a,b,a+b) \text{ is a good positive } ABC \text{ triple, } a < b,\ a+b \leq n\right\}.$$

The ABC@Home project showed that $\#\mathcal{A}_{10^{18}} = 14\,482\,065$ and Bart de Smit's webpage [2] as of May 2018 has a file containing all good ABC triples in $\mathcal{A}_{10^{18}}$ available for download. In what follows we will use elements in $\mathcal{A}_n$ for $n \leq 10^{18}$ to construct good elliptic curves. Due to computational limitations, we will restrict ourselves to $\mathcal{A}_{n_j}$ where n_j is as given below

j	1	2	3
n_j	$3 \cdot 10^{12}$	10^{11}	10^{10}
$\#\mathcal{A}_{n_j}$	359 905	116 988	51 689

(3.12)

In the following subsections we use good ABC triples $(a,b) \in \mathcal{A}_{n_j}$ to construct good elliptic curves.

3.5.1 Good Elliptic Curves Arising From F_T

Let $T = C_2 \times C_{2m}$ where $m = 1,2,3,4$ and let $\mathfrak{A}_T = \mathfrak{A}_T(a,b)$, $\mathfrak{B}_T(a,b)$ be as defined in Table A.3. In the previous section, we considered the Frey curve $F_T = F_T(a,b)$, where

$$F_T : y^2 = x\,(x - \mathfrak{A}_T)(x + \mathfrak{B}_T)\,,$$

and proved in Theorem 3.16 that under the assumptions that $(a,b,a+b)$ is a good positive ABC triple satisfying $a \equiv 0 \mod 2$, $b \equiv 1 \mod 4$, and $\frac{b}{a} > \theta_T$ where θ_T is as given in Lemma A.2 we could construct infinitely many good Frey curves under the additional assumption that $a \equiv 0 \mod 3$ whenever $T = C_2 \times C_6$. However, what if we drop the assumptions on a and b? Then $F_T(a,b)$ may still be good if $(a,b,a+b)$ is a good ABC triple. Indeed, for $T = C_2 \times C_2$ we have

$$\sigma_m(F_T(a,b)) \approx \begin{cases} 6.5648 & \text{if } (a,b) = (1,8) \\ 6.1598 & \text{if } (a,b) = (169,343) \end{cases}$$

This motivates the study of $F_T(a,b)$ for $(a,b) \in \mathcal{A}_n$ for some n. In fact, for a pair $(a,b) \in \mathcal{A}_n$ for some n, we will consider the elliptic curves $F_T(a,b)$ and $F_T(-(a+b), a)$. To this end, let

$$n_T = \begin{cases} 10^{10} & \text{if } T = C_2 \times C_8 \\ 3 \cdot 10^{12} & \text{if } T = C_2 \times C_2, C_2 \times C_4, C_2 \times C_6 \end{cases}$$

where n_j is as defined in (3.12). Now consider the set

$$\mathcal{S}_T = \left\{ [E]_{\mathbb{Q}} \mid E \text{ is } \mathbb{Q}\text{-isomorphic to } F_T(a,b) \text{ or } F_T(a, -(a+b)) \text{ for } (a,b) \in \mathcal{A}_{n_T} \right. .$$

By construction, $F_{C_2 \times C_2}(a,b)$ and $F_{C_2 \times C_4}(a,b)$ are isogenous for all $(a,b) \in \mathcal{A}_{n_1}$ and therefore

$$\mathcal{I}(\mathcal{S}_{C_2 \times C_2}) = \mathcal{I}(\mathcal{S}_{C_2 \times C_4}) .$$

In particular, we only compute $\mathcal{S}_{C_2 \times C_2}$ since our goal is to construct the set $\bigcup_T \mathcal{I}(\mathcal{S}_T)$. The following table summarizes the data obtained from $\mathcal{S}_T$ and $\mathcal{I}(\mathcal{S}_T)$

	$\mathcal{S}_{C_2 \times C_2}$	$\mathcal{S}_{C_2 \times C_6}$	$\mathcal{S}_{C_2 \times C_8}$	$\mathcal{I}(\mathcal{S}_{C_2 \times C_2})$	$\mathcal{I}(\mathcal{S}_{C_2 \times C_6})$	$\mathcal{I}(\mathcal{S}_{C_2 \times C_8})$
$\#(-)$	719 768	719 803	103 334	4 777 029	4 961 688	803 659
Max σ_m	8.0503	7.9683	7.1115	8.6852	8.5825	8.0997
Max σ	7.0510	7.4256	6.9407	7.3622	7.5762	7.1800
# w. $\sigma > 6$	110 848	113 765	10 172	852 672	1 215 292	220 938
Max h_{naive}	25.293	25.402	40.000	25.5940	25.7167	40.7743
# w. $\sigma_m > 6$	531 726	580 396	102 364			
Max N_E	$2.5 \cdot 10^{50}$	$1.0 \cdot 10^{51}$	$9.8 \cdot 10^{79}$			

Now let $\mathcal{S}^{(3)} = \bigcup_T \mathcal{S}_T$ and we compute $\#\mathcal{I}(\mathcal{S}^{(3)}) = 10\,542\,376$.

3.5.2 Good Elliptic Curves Arising From H_T

In the following chapter we prove that for each of the fifteen torsion subgroups T allowed by Theorem 2.1, there are infinitely many good elliptic curves T such that $E(\mathbb{Q})_{\text{tors}} \cong T$. For each T except $T = C_5$ let $H_T = H_T(a,b)$ be given by the Weierstrass model

$$H_T : y^2 + xy = x^3 - \frac{A_T - 1}{48}x - \frac{3A_T + 2B_T - 1}{1728}$$

where $A_T = A_T(a,b)$ and $B_T = B_T(a,b)$ are as defined in Table $(E.1)$ and Table $(E.2)$, respectively. In the next chapter, we prove under certain assumptions on a and b, that H_T is given by a global minimal model and $H_T(\mathbb{Q})_{\text{tors}} \cong T$. Following a similar approach to the previous section will then result in an explicit proof that there are infinitely many good elliptic curves with specified torsion. In this section, however, we focus on the specific case of when $T = C_7, C_9, C_{10}, C_{12}, C_2 \times C_8$. For these T let

$$m_T = \begin{cases} 3 \cdot 10^{12} & \text{if } T = C_7 \\ 10^{11} & \text{if } T = C_{10} \\ 10^{10} & \text{if } T = C_9, C_{12}, C_2 \times C_8 \end{cases}$$

where n_j is as defined in (3.12). Now consider the set

$$\mathfrak{S}_T = \begin{cases} \{[E]_{\mathbb{Q}} \mid E \cong H_T(a,b) \text{ or } H_T(b,a) \text{ for } (a,b) \in \mathcal{A}_{m_T} & \text{for } T = C_7, C_9, C_{10} \\ \{[E]_{\mathbb{Q}} \mid E \cong H_T(-a,b) \text{ or } H_T(b,a) \text{ for } (a,b) \in \mathcal{A}_{m_T} & \text{for } T = C_{12} \\ \{[E]_{\mathbb{Q}} \mid E \cong H_T(a,b) \text{ for } (a,b) \in \mathcal{A}_{m_T} & \text{for } T = C_2 \times C_8. \end{cases}$$

The table below summarizes the data pertaining to the isomorphism classes of elliptic curves in $\mathfrak{S}_T$

$\mathfrak{S}_T$	C_7	C_9	C_{10}	C_{12}	$C_2 \times C_8$
$\#\mathfrak{S}_T$	719 810	103 378	233 976	103 378	51 679
Max σ_m	7.2265	6.9232	7.3152	6.9645	7.1098
Max σ	6.9203	6.6725	6.6937	6.6035	6.9407
# of Curves w. $\sigma_m > 6$	663 202	96 216	193 497	102 188	51 679
# of Curves w. $\sigma > 6$	32 295	4 524	14 487	9 335	5 494
Max h_{naive}	24.98	30.00	33.33	40.00	40.00
Max Conductor	$1.4 \cdot 10^{50}$	$1.06 \cdot 10^{60}$	$7.79 \cdot 10^{66}$	$9.82 \cdot 10^{79}$	$9.82 \cdot 10^{79}$

Next we compute $\mathcal{I}(\mathfrak{S}_T)$ for $T \neq C_{12}, C_2 \times C_8$ and find

$\mathcal{I}(\mathfrak{S}_T)$	C_7	C_9	C_{10}
$\#\mathcal{I}(\mathfrak{S}_T)$	1 337 841	291 101	814 414
Max σ_m	9.4006	7.5658	7.6216
Max σ	7.2053	6.8701	7.3306
# of Curves w. $\sigma > 6$	291 618	62 291	176 518
Max h_{naive}	25.3731	30.39	33.60

For $T = C_{12}$ we compute a proper subset of $\mathcal{I}(\mathfrak{S}_T)$ which we denote by $\mathcal{J}(\mathfrak{S}_T)$:

$\#\mathcal{J}(\mathfrak{S}_{C_{12}})$	Max σ_m	Max σ	# of Curves w. $\sigma > 6$	Max h_{naive}
561 584	7.3700	6.8430	150 443	40.41

Lastly, let $\mathcal{S}^{(4)} = \bigcup_T \mathfrak{S}_T$ and we compute $\#\mathcal{I}\big(\mathcal{S}^{(4)}\big) = 3\,056\,619$.

3.5.3 Good Elliptic Curves due to Bennett, Nitaj, and Yazdani

In [22] and [23], Nitaj found 142 good elliptic curves. For each elliptic curve in Nitaj's papers, we computed its $\mathbb{Q}$-isogeny class. This, in turn, provided us with

336 distinct good elliptic curves with conductor at least 400 000. The table below summarizes the data of these 336 good elliptic curves:

Max σ_m	Max σ	# of Curves w. $\sigma > 6$	Max h_{naive}	Max N_E
10.1148	8.8119	315	21.68	$1.18 \cdot 10^{40}$

Building on Nitaj's techniques, Bennett and Yazdani [24] found 25 good elliptic curves with Szpiro ratio at least 8.4861. In addition, Bennett and Yazdani found an additional 1 933 good elliptic curves, of which the aforementioned 25 were the ones with best known Szpiro ratio. For each of these elliptic curves, we also computed their $\mathbb{Q}$-isogeny class. This resulted in 3 253 distinct good elliptic curves with conductor at least 400 000. The table below summarizes the data of these 3 253 good elliptic curves:

Max σ_m	Max σ	# of Curves w. $\sigma > 6$	Max h_{naive}	Max N_E
10.1609	9.0200	3 200	13.7936	$3.80 \cdot 10^{20}$

Let $\mathcal{S}^{(5)}$ be the set of $\mathbb{Q}$-isomorphism classes of the elliptic curves found by Bennett, Nitaj, and Yazdani. Then $\#\mathcal{I}\big(\mathcal{S}^{(5)}\big) = 3\,467$. The intention of these works was to construct good elliptic curves with high Szpiro ratio. Consequently, almost all elliptic curves of conductor at least 400 000 appearing in Appendix B are due to the works of Nitaj and Bennett and Yazdani.

3.5.4 The Explicit Modified Szpiro Conjecture

Let $\mathcal{S} = \bigcup_{j=1}^{5} \mathcal{I}\big(\mathcal{S}^{(j)}\big)$. Then $\mathcal{S}$ contains 13 870 964 $\mathbb{Q}$-isomorphism classes of good elliptic curves from which we create our database of good elliptic curves. For each $[E]_{\mathbb{Q}}$ in $\mathcal{S}$ we save the following information into our database:

N_E	$h_{\text{naive}}(E)$	$[a_1, a_2, a_3, a_4, a_6]_{\text{reduced}}$	$\sigma_m(E)$	$\sigma(E)$	$E(\mathbb{Q})_{\text{tors}}$

where $[a_1, a_2, a_3, a_4, a_6]_{\text{reduced}}$ are the unique invariants of the reduced minimal model of E. That is E is $\mathbb{Q}$-isomorphic to the elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Table 3.6.: Summary of Data of Elliptic Curves in $\mathcal{S}$

T	C_1	C_2	C_3	C_4	C_5
# w. $\sigma_m > 6$	801 523	3 890 675	98 058	2 089 799	69
# w. $\sigma > 6$	304 931	1 248 830	16 824	305 948	18
max σ_m	16.0587	13.3951	9.8648	10.1145	8.5371
max σ	9.0200	8.8119	8.6224	8.5352	8.0067

T	C_6	C_7	C_8	C_9	C_{10}
# w. $\sigma_m > 6$	1 923 692	663 228	209 723	96 221	404 826
# w. $\sigma > 6$	481 403	32 311	26 307	96 221	31 307
max σ_m	9.7672	8.6345	8.2265	6.9232	7.3163
max σ	8.3096	7.3625	7.3403	6.6725	7.0006

T	C_{12}	$C_2 \times C_2$	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
# w. $\sigma_m > 6$	91 037	1 407 167	1 422 306	663 101	109 539
# w. $\sigma > 6$	10 348	299 930	119 765	125 004	11 106
max σ_m	7.8752	9.7559	8.4797	8.5262	7.3412
max σ	6.9035	8.4619	7.4605	7.4256	6.9407

Table 3.6 summarizes the data obtained from our database for each of the fifteen torsion subgroups allowed by Theorem 2.1.

For each of the fifteen torsion subgroups T, we order the elliptic curves in $\mathcal{S}$ by their modified Szpiro and Szpiro ratio. These rankings can be found in Appendix B. The data acquired through this study motivates the following explicit formulation of the modified Szpiro conjecture and Szpiro conjecture

Conjecture 3.18 (The Explicit Modified Szpiro Conjecture) *Let E be an elliptic curve of conductor $N_E > 300\,000$ with $T \hookrightarrow E(\mathbb{Q})$. Then* $\max\{|c_4^3, c_6^2|\} < N_E^{f_T}$ *and* $|\Delta_E^{min}| < N_E^{g_T}$ *where*

T	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
f_T	11	10.2	9.87	10.2	8.54	9.77	8.63	8.23
g_T	9.02	8.82	8.63	8.54	8.01	8.31	7.37	7.35

T	C_9	C_{10}	C_{12}	$C_2 \times C_2$	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
f_T	6.93	7.32	7.88	9.76	8.48	8.53	7.35
g_T	6.68	7.01	6.91	8.47	7.47	7.43	6.95

Corollary 3.19 *Assuming the explicit modified Szpiro conjecture, the database $\mathcal{F}_T$ constructed in section 3.3.2 contains all elliptic curves of conductor at most N_T where*

$$N_T = \begin{cases} 38\,866 & \text{if } T = C_2 \times C_4 \\ 1.334 \cdot 10^9 & \text{if } T = C_2 \times C_6 \\ 1.454 \cdot 10^{22} & \text{if } T = C_2 \times C_8 \end{cases}$$

Proof Suppose E is an elliptic curve with $T \hookrightarrow E(\mathbb{Q})$ and $h_{\text{naive}}(E) = k$. Applying the explicit modified Szpiro conjecture yields

$$\begin{aligned} \frac{1}{12}\log\max\{|c_4^3|, |c_6^2|\} &= k \\ \implies \qquad \max\{|c_4^3|, |c_6^2|\} &= 10^{12k} < N_E^{f_T} \\ \implies \qquad 10^{12k/f_T} &< N_E. \end{aligned}$$

Now let l_T is as defined in 3.2. By Theorem 3.14, $\mathcal{F}_T$ contains an exhaustive list of all elliptic curves up to naive height l_T. The result now follows by taking $k = l_T$ above. ∎

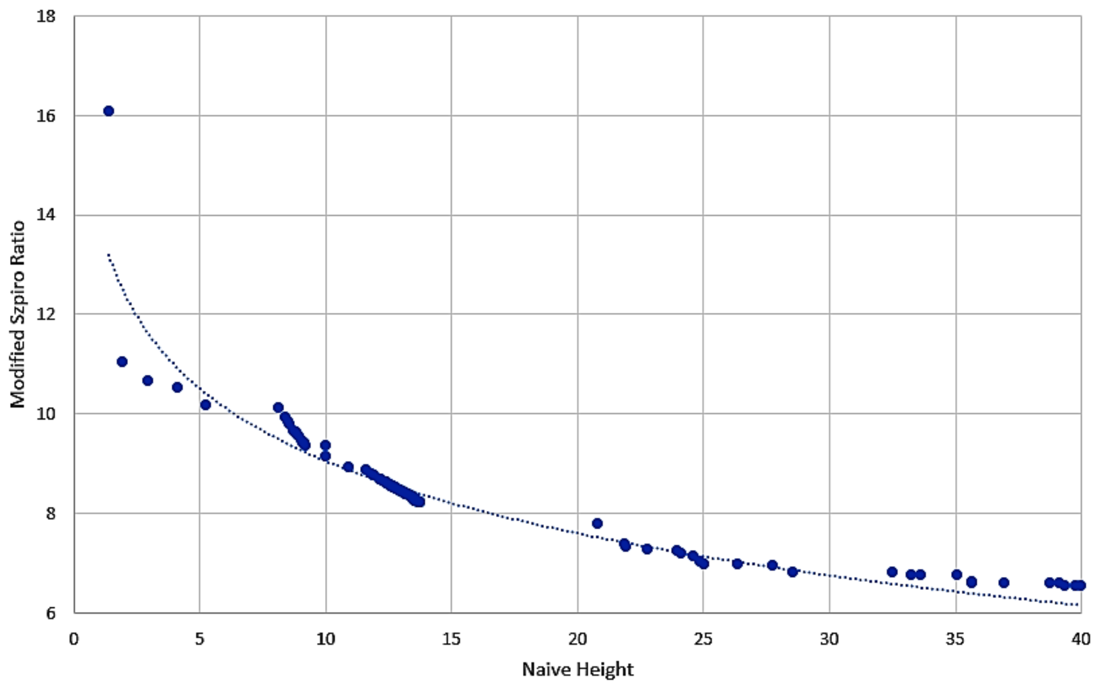
3.5.5 Further Analysis of $\mathcal{S}$

We now consider the following subset of $\mathcal{S}$,

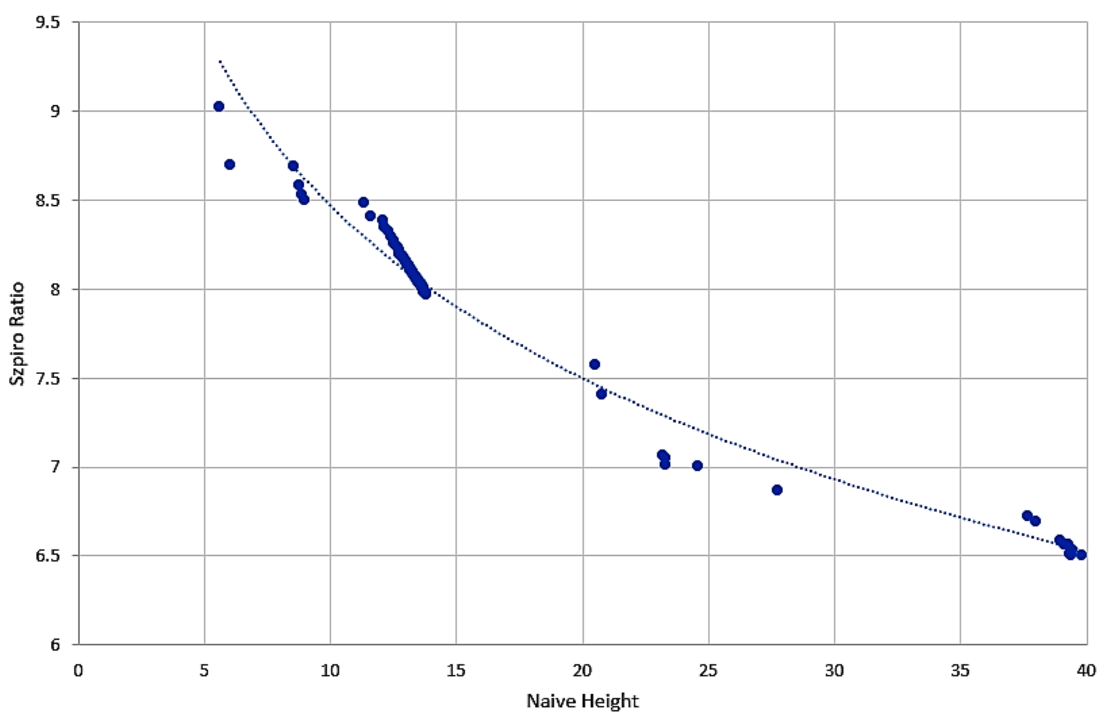
$$\mathcal{S}^{\sigma_m} = \{[E_1]_{\mathbb{Q}}, [E_2]_{\mathbb{Q}}, \dots, [E_n]_{\mathbb{Q}}$$

which satisfies $\sigma_m(E_j) > \sigma_m(E_k) > 6.5$ and $h_{\text{naive}}(E_j) < h_{\text{naive}}(E_k)$ for $j < k$. This determines $\mathcal{S}^{\sigma_m}$ uniquely and similarly we define $\mathcal{S}^{\sigma}$ as the unique subset of $\mathcal{S}$ which satisfies $\sigma(E_j) > \sigma(E_k) > 6.5$ and $h_{\text{naive}}(E_j) < h_{\text{naive}}(E_k)$ for $j < k$. Then $\#\mathcal{S}^{\sigma_m} = 150$ and $\#\mathcal{S}^{\sigma} = 120$. Tables B.1 and B.2 list the approximate conductor, naive height, modified Szpiro ratio, Szpiro ratio, and torsion subgroup of each element in $\mathcal{S}^{\sigma_m}$ and $\mathcal{S}^{\sigma}$, respectively. Figure 3.4 contains the scatter plot of the modified Szpiro ratio (resp. Szpiro ratio) against the naive height for each element in $\mathcal{S}^{\sigma_m}$ (resp. $\mathcal{S}^{\sigma_m}$). In addition, each scatter plot has a logarithmic trendline which acts as a heuristic of expected largest modified Szpiro ratio or Szpiro ratio for a given naive height between 0 and 40. Figure 3.5 consists of histograms for the modified Szpiro ratio, Szpiro ratio, and naive height of elliptic curves in $\mathcal{S}$.

Summary of Data for Elliptic Curves in $\mathcal{S}$

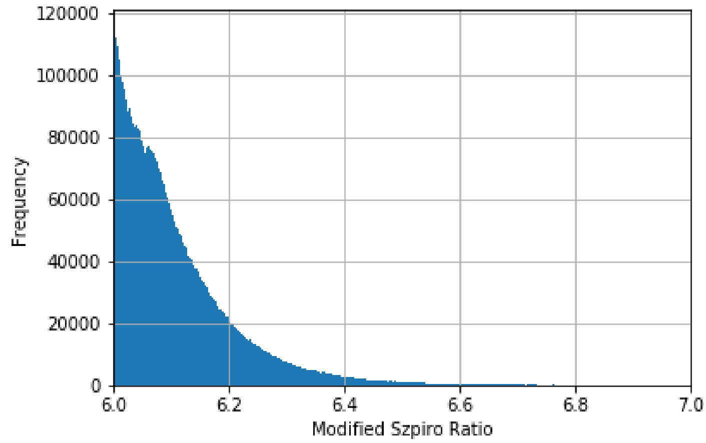


(a) Scatter Plot for $\mathcal{S}^{\sigma_m}$

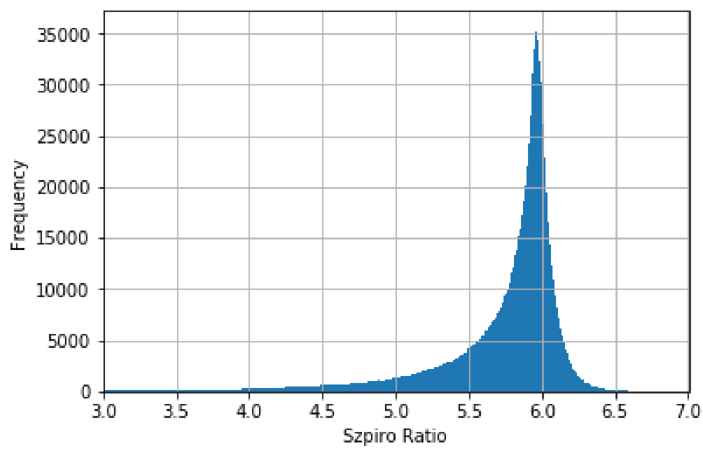


(b) Scatter Plot for $\mathcal{S}^{\sigma}$

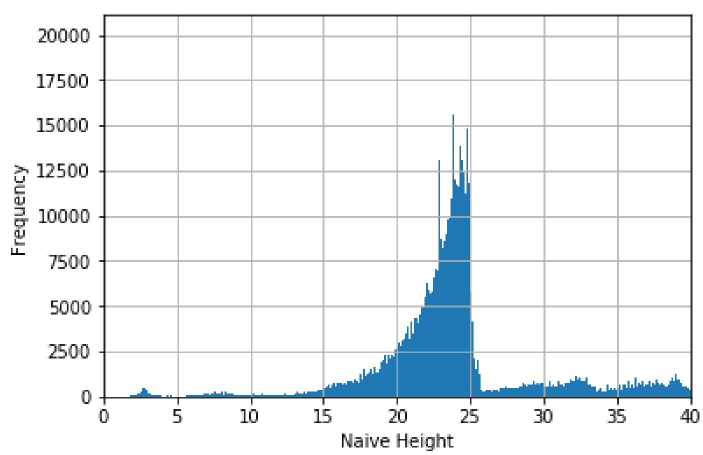
Figure 3.4.: Histograms for Elliptic Curves in $\mathcal{S}^{\sigma}$



(a) Modified Szpiro Ratio for Elliptic Curves in $\mathcal{S}$



(b) Szpiro Ratio for Elliptic Curves in $\mathcal{S}$



(c) Naive Height for Elliptic Curves in $\mathcal{S}$

Figure 3.5.: Histograms for Elliptic Curves in $\mathcal{S}$

4. GOOD ELLIPTIC CURVES WITH SPECIFIED TORSION SUBGROUP

In this chapter we extend the result of Chapter 3.4 by proving the following Theorem.

Theorem 4.1 *For each of the fifteen torsion subgroups T allowed by Theorem 2.1, there are infinitely many elliptic curves E with $E(\mathbb{Q})_{tors} \cong T$.*

While this was proven for $T = C_2 \times C_{2m}$ for $m = 1, 2, 3, 4$, the method relied on results in Appendix A. The result of Appendix A relied on the construction of the ABC triple $(\mathfrak{A}_T(a, b), \mathfrak{B}_T(a, b), \mathfrak{C}_T(a, b))$. Since these ABC triples were constructed via the forgetful map $X_1(2, 2m) \to X(2)$ for $m = 2, 3, 4$, we have that this approach does not work for constructing good elliptic curves E with $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$ where $T \neq C_2 \times C_{2m}$ for $m = 1, 2, 3, 4$. Instead, for each of the fifteen torsion subgroups T, we will first construct modular curves Y_T consisting of isomorphism classes of pairs (E, P) where E is an elliptic curve and P is a torsion point on E. We will then prove that there is a subset of $Y_T(\mathbb{Q})$ consisting of isomorphism classes of pairs (E, P) where E is a rational elliptic curve with $E(\mathbb{Q})_{\text{tors}} \cong T$. We then consider two-parameter families of elliptic curves $H_T = H_T(a, b)$ with the property that the discriminant of H_T is minimal when a and b satisfy certain conditions and show that the isomorphism class of (H_T, P) for P a torsion point on H_T lies in the aforementioned subset of $Y_T(\mathbb{Q})$ which allows us to conclude that $H_T(\mathbb{Q})_{\text{tors}} \cong T$. In section 4, we use the minimal discriminant of H_T as well as the associated invariants c_4 and c_6 to prove that for each T except $T = C_1, C_2, C_5$ we can construct an infinite sequence of good ABC triples. We combine all these results in section 4.4 to prove Theorem 4.1 and conclude the chapter with examples for each T.

4.1 Models of Elliptic Curves

Let T be one of the fifteen torsion subgroups allowed by Theorem 2.1. For $t \in \mathbb{P}^1$, define $\mathcal{Y}_t$ as the mapping which takes T to the elliptic curve $\mathcal{Y}_t(T)$ where the Weierstrass model of $\mathcal{Y}_t(T)$ for $T \neq C_1$ is given in Table 4.1.

a_1	a_2	a_3	a_4	T
0	$-2(t^4-12t^3+6t^2-12t+1)$	0	$(t+1)^8$	C_2
1	0	$\frac{t(t+1)\left(t^2+t+1\right)^3}{\left(t^3+6t^2+3t-1\right)^3}$	0	C_3
1	$\frac{\left(t^2+1\right)^2}{(8t)^2}$	a_2	0	C_4
$1-\frac{t^{20}}{32}$	$-\frac{t^{20}}{32}$	a_2	0	C_5
$\frac{2\left(t^4-4t^3+10t^2-4t+1\right)}{\left(t^2-4t+1\right)^2}$	$\frac{-8t(t-1)^2\left(t^2+1\right)^2}{\left(t^2-4t+1\right)^4}$	a_2	0	C_6
$-t^2-t+1$	$-t\left(t+1\right)^2$	a_2	0	C_7
$\frac{t^4-4t^3-2t^2-4t+1}{\left(t^2+1\right)(t-1)^2}$	$\frac{-t(1+t)^2}{\left(1+t^2\right)^2}$	a_2	0	C_8
$-t^3-2t^2-t+1$	$-t\left(t+1\right)^2\cdot(t^2+t+1)$	a_2	0	C_9
$\frac{2t^3+4t^2-1}{t^2-t-1}$	$\frac{-t(2t+1)(t+1)^3}{\left(t^2-t-1\right)^2}$	a_2	0	C_{10}
$\frac{-t^4-2t^3+2t^2-2t+1}{-t^3(t+1)}$	$\frac{(t-1)\left(t^2-t+1\right)\left(t^2+1\right)}{t^4(t+1)^2}$	a_2	0	C_{12}
0	$t^4-12t^3+6t^2-12t+1$	0	$-8t\left(t-1\right)^4\cdot(t^2+1)$	$C_2\times C_2$
1	$\frac{-t\left(1+t^2\right)}{2(1-t)^4}$	a_2	0	$C_2\times C_4$
$\frac{2t^4-4t^3-4t^2-4t+2}{(t+1)^2\left(t^2-4t+1\right)}$	$\frac{-8t^2(t-1)^2\left(t^2+1\right)}{(t+1)^4\left(t^2-4t+1\right)^2}$	a_2	0	$C_2\times C_6$
$\frac{1+4t-t^4}{(1+t)\left(1+2t-t^2\right)}$	$\frac{t(1-t)\left(1+t^2\right)}{\left(1+2t-t^2\right)^2}$	a_2	0	$C_2\times C_8$

Table 4.1.: The Weierstrass model for $\mathcal{Y}_t(T) : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x$

For $T = C_1$, let

$$\mathcal{Y}_t(C_1) : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

where a_1, a_2, a_3 are as defined in Table 4.1 for $T = C_9$ and

$$a_4 = -5t\,(t+1)\left(t^9 + 9t^8 + 28t^7 + 53t^6 + 61t^5 + 47t^4 + 25t^3 + 8t^2 - 1\right)$$

$$a_6 = -t\,(t+1)\left(\begin{array}{l} t^{15} + 23t^{14} + 162t^{13} + 643t^{12} + 1621t^{11} + \\ 2878t^{10} + 3778t^9 + 3721t^8 + 2719t^7 + 1453t^6 + \\ 608t^5 + 266t^4 + 145t^3 + 65t^2 + 13t - 1 \end{array}\right)$$

For $T \neq C_1$, it is checked via SageMath [29] that the point $(0,0)$ of $\mathcal{Y}_t(T)$ is a point of order N where

$$N = \begin{cases} \frac{1}{2}\,|T| & \text{if } T = C_2 \times C_{2n} \text{ for } n = 1,2,3,4 \\ |T| & \text{otherwise.} \end{cases} \tag{4.1}$$

Now let Y_T be the set consisting of isomorphism classes of pairs (E, P) where each isomorphism class (E, P) contains a representative $(\mathcal{Y}_t(T)\,, (0,0))$ for $T \neq C_1$ and $(\mathcal{Y}_t(C_1)\,, \mathcal{O})$. For each T, we endow the set Y_T with the structure of a modular curve via the rational map $\mathbb{P}^1 \to Y_T$ where t is mapped to the isomorphism class of $(\mathcal{Y}_t(T)\,, P)$ where P is $\mathcal{O}$ or $(0,0)$ if $T = C_1$ or all other T, respectively.

The next three results will aid us in proving that there is a subset of $Y_T(\mathbb{Q})$ consisting of isomorphism classes (E, P) with $E(\mathbb{Q})_{\text{tors}} \cong T$.

Remark When T is clear from context, we will simply write $\mathcal{Y}_t$ in place of $\mathcal{Y}_t(T)$.

Lemma 4.2 *For each T, there exists an embedding $T \hookrightarrow \mathcal{Y}_t(T)(\mathbb{Q})_{tors}$.*

Proof For $T = C_1$ there is nothing to show. For the remaining T, we have by the discussion above that the point $P = (0,0)$ is a torsion point of order N where N is as given in (4.1). Therefore for $T \neq C_2 \times C_{2m}$ for $m = 1,2,3,4$, we have that $T \hookrightarrow \mathcal{Y}_t(T)(\mathbb{Q})$.

Next, assume $T = C_2 \times C_2$. The admissible change of variables $x \longmapsto \frac{1}{a^4}x$ and $y \longmapsto \frac{1}{a^6}y$ gives a $\mathbb{Q}$-isomorphism between the elliptic curve $\mathcal{Y}_t$ and the elliptic curve

$$y^2 = x\left(x - 8ab\left(a^2 + b^2\right)\right)\left(x + (a-b)^4\right)$$

which has $\langle (8ab\,(a^2+b^2)\,,0)\,,(0,0)\rangle \cong C_2 \times C_2$. Thus $T \hookrightarrow \mathcal{Y}_t(\mathbb{Q})$. For the remaining T, let t' be as defined in the table below

T	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
t'	$\frac{t}{2(t-1)^2}$	$\frac{1+8t+t^2}{1+t^2}$	$\frac{1}{2(t-1)}$

Then $\mathcal{Y}_t(T) = \mathcal{X}_{t'}(T)$ where $\mathcal{X}_{t'}(T)$ is as given in Table 2.1. In particular, $T \hookrightarrow \mathcal{Y}_t(T)(\mathbb{Q})$. ■

Lemma 4.3 *Fix $t \in \mathbb{Q}$ and consider the elliptic curve $\mathcal{Y}_t(T)$. Then*

$$\mathcal{Y}_t(C_4) \xrightarrow{\quad 2 \quad} \mathcal{Y}_t(C_2 \times C_4) \xrightarrow{\quad 2 \quad} \mathcal{Y}_t(C_2 \times C_2) \xrightarrow{\quad 2 \quad} \mathcal{Y}_t(C_2)$$

$$\mathcal{Y}_t(C_9) \xrightarrow{\quad 3 \quad} \mathcal{Y}_t(C_3) \xrightarrow{\quad 3 \quad} \mathcal{Y}_t(C_1)$$

where each $\mathcal{Y}_t(T) \xrightarrow{p} \mathcal{Y}_t(T')$ is an isogeny defined over $\mathbb{Q}$ of degree p whose kernel is rational.

Proof In [31], Nitaj completely classified the isogeny class over $\mathbb{Q}$ of a rational elliptic E with $E(\mathbb{Q})_{\text{tors}} \cong C_9$. Our models for $\mathcal{Y}_t(T)$ for $T = C_1, C_3, C_9$ are isomorphic over $\mathbb{Q}$ to the three models given by Nitaj. We omit the proof of the first row, but remark that the proof follows mutandis mutatis to the one given by [31]. Namely, the rational isogeny $\mathcal{Y}_t(T) \xrightarrow{2} \mathcal{Y}_t(T')$ is obtained by applying Vélu's formulas [32] to the elliptic curve $\mathcal{Y}_t(T)$ and its torsion point of order 2, $P = \frac{N}{2}(0,0)$ where N is as in (4.1). ■

Lemma 4.4 *The rational map $f : \mathbb{P}^1 \to \mathbb{P}^1$ defined by $f(t) = \frac{t^2}{(t+1)^2(2t+1)}$ induces a morphism $X_1(10) \to X_1(5)$ with $[(E,P)] \to [(E,2P)]$. In particular, if E is an elliptic curve with a K-torsion point of order 5, then E has a K-rational torsion point of order 10 if and only if E is isomorphic over K to an elliptic curve with Weierstrass equation*

$$y^2 + (1-f(t))\,xy - f(t)\,y = x^3 - f(t)\,x^2 \text{ and } t \in K. \tag{4.2}$$

Proof Since $\mathcal{Y}_t(C_{10}) = \mathcal{X}_{t+1}(C_{10})$, it follows that $\mathcal{Y}_t(C_{10})$ and $X_1(10)$ are isomorphic as modular curves. Therefore the rational map $\eta_1 : \mathbb{P}^1 \to X_1(10)$ defined by $t \longmapsto [(\mathcal{Y}_t(C_{10}), (0,0))]$ is an isomorphism of curves since $X_1(10)$ has genus 0. The universal elliptic curve for $X_1(5)$ is given by

$$\mathcal{X}_t(C_5) : y^2 + (1-t)\,xy - ty = x^3 - tx^2.$$

Consequently, we have an isomorphism of curves $\eta_2 : \mathbb{P}^1 \to X_1(5)$ defined by $t \longmapsto [(\mathcal{X}_t(C_5), (0,0))]$. Let $g = \eta_2 \circ f \circ \eta_1^{-1}$ so that the following diagram commutes.

$$\begin{tikzcd}
\mathbb{P}^1 \arrow[r, "f"] \arrow[d, "\eta_1"] & \mathbb{P}^1 \arrow[d, "\eta_2"] \\
X_1(10) \arrow[r, "g"] & X_1(5)
\end{tikzcd}$$

Then $g([(\mathcal{Y}_t(C_{10}), (0,0))]) = \left[\left(\mathcal{X}_{f(t)}(C_5), (0,0)\right)\right]$. Lastly, writing $\mathcal{Y}_t(C_{10})$ in Tate normal form with respect to $2 \cdot (0,0)$ results is the Weierstrass equation of $\mathcal{X}_{f(t)}(C_5)$. Hence g is a well-defined morphism of curves. ■

Proposition 4.5 *For $T = C_5$, let $t = 2^n$ for some positive integer n. For all other T, let $t = \frac{b}{a}$ where a and b are relatively prime positive integers with $a \equiv 0 \mod 6$. Assume further that $v_2(a)$ is even if $T = C_2, C_4$. Then*

$$\mathcal{Y}_t(T)(\mathbb{Q})_{tors} \cong T.$$

Proof By Lemma 4.2, $T \hookrightarrow \mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}}$ for each T. Consequently, it suffices to show $|\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}}| = |T|$. Observe that for any non-trivial isogeny $\phi : E \to E'$ we have the following equality via the First Isomorphism Theorem:

$$|E'(\mathbb{Q})_{\text{tors}}|\,|E(\mathbb{Q})[\phi]| = |E(\mathbb{Q})_{\text{tors}}|\,[E'(\mathbb{Q})_{\text{tors}} : \phi(E(\mathbb{Q})_{\text{tors}})]\,. \tag{4.3}$$

We now claim that $\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}}$ is not divisible by an odd prime for $T = C_2, C_4$, and $C_2 \times C_2$. By Lemma 4.3, $\mathcal{Y}_t(T)$ for $T = C_2, C_4, C_2 \times C_2$ is 2^k-isogenous to the curve $\mathcal{Y}_t(C_2 \times C_4)$ where k is either 1 or 2. Let $\phi_T : \mathcal{Y}_t(T) \to \mathcal{Y}_t(C_2 \times C_4)$ be the degree 2^k isogeny for $T = C_2, C_4, C_2 \times C_2$. Now let

$$[\mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q})_{\text{tors}} : \phi(\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}})] = l$$

for some integer l. Taking $E = \mathcal{Y}_t(T)$ and $E' = \mathcal{Y}_t(C_2 \times C_4)$ in (4.3), we obtain

$$\frac{2^{k+3}}{l} = |\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}}|$$

since $|\mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q})_{\text{tors}}| = 8$. In particular, $|\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}}|$ is not divisible by an odd prime as claimed. We now prove the Proposition by considering various cases separately.

Case I. By Theorem 2.1, $|\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}}| \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 16\}$. Therefore $\mathcal{Y}_t(T)(\mathbb{Q})_{\text{tors}} \cong T$ for $T = C_7, C_9, C_{10}, C_{12}, C_2 \times C_6, C_2 \times C_8$.

Case II. We now show the Proposition for $T = C_1, C_3$. By [31], we know that the isogeny class over $\mathbb{Q}$ containing an elliptic curve with torsion subgroup isomorphic to C_9, contains exactly 3 isomorphism classes of rational elliptic curves. Therefore by Lemma 4.3 we have that the isogeny class over $\mathbb{Q}$ of $\mathcal{Y}_t(C_9)$ is $\{[\mathcal{Y}_t(C_1)]_{\mathbb{Q}}, [\mathcal{Y}_t(C_3)]_{\mathbb{Q}}, [\mathcal{Y}_t(C_9)]_{\mathbb{Q}}\}$ where $[E]_{\mathbb{Q}}$ denotes the $\mathbb{Q}$-isomorphism class of E. By [33, Proposition 3], $\mathcal{Y}_t(C_9)$ is isogenous over $\mathbb{Q}$ to an elliptic curve with trivial torsion. Since $C_3 \hookrightarrow \mathcal{Y}_t(C_3)(\mathbb{Q})$, it follows that $\mathcal{Y}_t(C_1)(\mathbb{Q})_{\text{tors}}$ is trivial. Now let $\phi : \mathcal{Y}_t(C_3) \to \mathcal{Y}_t(C_1)$ be the 3-isogeny with rational kernel from Lemma 4.3. We claim that

$$3 = |\mathcal{Y}_t(C_3)(\mathbb{Q})[\phi]| = |\mathcal{Y}_t(C_3)(\mathbb{Q})_{\text{tors}}|.$$

Indeed, this follows upon choosing $E = \mathcal{Y}_t(C_3)$ and $E' = \mathcal{Y}_t(C_1)$ in (4.3) since $\mathcal{Y}_t(C_1)(\mathbb{Q})_{\text{tors}}$ is trivial.

Case III. Assume $T = C_2 \times C_4$. By Theorem 2.1, $|\mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q})_{\text{tors}}| \in \{8, 16\}$. In fact, $\mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q})_{\text{tors}}$ is either $C_2 \times C_4$ or $C_2 \times C_8$. Our model for $\mathcal{Y}_t(C_2 \times C_4)$ differs by a linear change of variable in t from the model given in [34], which parametrizes elliptic curves F over $\mathbb{Q}(i)$ having $F(\mathbb{Q}(i))_{\text{tors}} \cong C_4 \times C_4$. Thus $\mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q}(i))_{\text{tors}} \cong C_4 \times C_4$ and therefore $C_2 \times C_8 \not\hookrightarrow \mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q}(i))_{\text{tors}}$. Hence $\mathcal{Y}_t(C_2 \times C_4)(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_4$.

Case IV. Next, assume $T = C_2 \times C_2$. By the claim at the start of the proof, we know that $|\mathcal{Y}_t(C_2 \times C_2)(\mathbb{Q})_{\mathrm{tors}}|$ is not divisible by an odd prime. Consequently, by Theorem 2.1 we have $|\mathcal{Y}_t(C_2 \times C_2)(\mathbb{Q})_{\mathrm{tors}}| \in \{4, 8, 16\}$. In fact, $\mathcal{Y}_t(C_2 \times C_2)(\mathbb{Q})_{\mathrm{tors}}$ is either $C_2 \times C_2, C_2 \times C_4$, or $C_2 \times C_8$. By the proof of Lemma 4.3, $\mathcal{Y}_t$ is $\mathbb{Q}$-isomorphic to the elliptic curve given by the Weierstrass model

$$y^2 = x\left(x - 8ab\left(a^2 + b^2\right)\right)\left(x + (a - b)^4\right)$$

This model satisfies the assumptions of [35, Main Theorem 1] and therefore we have that $\mathcal{Y}_t(C_2 \times C_2)(\mathbb{Q})_{\mathrm{tors}} \cong C_2 \times C_2$ if $8ab\left(a^2 + b^2\right)$ is not a square. If it were a square we would have a nontrivial integer solution to the Diophantine equation $x^4 - y^4 = z^2$ since

$$8ab\left(a^2 + b^2\right) + (a - b)^4 = (a + b)^4 .$$

This contradicts Fermat's Theorem and therefore $\mathcal{Y}_t(C_2 \times C_2)(\mathbb{Q})_{\mathrm{tors}} \cong C_2 \times C_2$.

Case V. Next, assume $T = C_5$. By Theorem 2.1, it suffices to show that $C_{10} \not\hookrightarrow \mathcal{Y}_t(C_5)(\mathbb{Q})_{\mathrm{tors}}$. Observe that $\mathcal{Y}_t(C_5)$ is already in Tate normal form and therefore by Lemma 4.4, it suffices to show that there is no rational number $t = \frac{u}{v}$ with

$$2^{5(4n-1)} = \frac{u^2 v}{(u + v)^2 (2u + v)}. \tag{4.4}$$

Towards a contradiction, suppose this equality holds. Now consider the quantities $u^2 v$ and $(u + v)^2 (2u + v)$ as polynomials in $\mathbb{Z}[u, v, r, s]$ and set

$$\begin{aligned} \mu &= -5u^2 r - 4uvr - v^2 r + 16u^2 s + 36uvs + 22v^2 s \\ \nu &= u^2 r - 8uvs + 2v^2 s \end{aligned}$$

Then

$$\mu u^2 v + \nu (u + v)^2 (2u + v) = 2\left(ru^5 + sv^5\right) \tag{4.5}$$

Without loss of generality, u and v are relatively prime integers and therefore we may find integers r and s such that $ru^5 + sv^5 = 1$. Therefore by (4.5) $d = \gcd\left(u^2 v, (u + v)^2 (2u + v)\right)$ divides 2. If $d = 1$, then $(u + v)^2 (2u + v) = \pm 1$ and $u^2 v = \pm 2^{5(4n-1)}$. By parity considerations on u and v, there are no integers where this holds. If $d = 2$, then $(u+v)^2(2u+v) = \pm 2$ and $u^2 v = 2^{4(5n-1)}$. If u is even, then v is even which is a contradiction since they are relatively prime. Consequently, $u = \pm 1$ which also gives a contradiction. Hence, no such rational numbers exist and we conclude that $\mathcal{Y}_t(C_5)(\mathbb{Q})_{\text{tors}} \cong C_5$.

Case VI. Next, assume $T = C_8$. It suffices to show that $C_2 \times C_2 \not\hookrightarrow \mathcal{Y}_t(C_8)(\mathbb{Q})_{\text{tors}}$ by Theorem 2.1. To show this, we consider the admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ where

$$u_T = \frac{1}{2(a-b)^2(a^2+b^2)} \qquad r_T = -\frac{(a^2-b^2)^2}{4(a^2+b^2)^2} \qquad w_T = \frac{(a-b)^2(a+b)^4}{8(a^2+b^2)^3}$$
$$s_T = -\frac{a^4 - 4a^3b - 2a^2b^2 - 4ab^3 + b^4}{2(a-b)^2(a^2+b^2)}.$$

This admissible change of variables gives a $\mathbb{Q}$-isomorphism between $\mathcal{Y}_t(C_8)$ and the elliptic curve

$$y^2 = x^3 - 2\left(a^8 - 4a^6b^2 - 26a^4b^4 - 4a^2b^6 + b^8\right)x^2 + \left(a^2-b^2\right)^8 x.$$

Let a_2 and a_4 denote the coefficients of this Weierstrass model and observe that

$$a_2^2 - 4a_4 = -256a^4b^4\left(a^2+2ab-b^2\right)\left(a^2-2ab-b^2\right)\left(a^2+b^2\right)^2.$$

Moreover, $C_2 \times C_2 \hookrightarrow \mathcal{Y}_t(C_8)(\mathbb{Q})_{\text{tors}}$ if and only if $a_2^2 - 4a_4$ is a square if and only if $-(a^2+2ab-b^2)(a^2-2ab-b^2)$ is a square. Since $a \equiv 0 \mod 6$ and $b^2 \equiv 1 \mod 4$, we observe that

$$-\left(a^2+2ab-b^2\right)\left(a^2-2ab-b^2\right) \equiv -1 \mod 4. \tag{4.6}$$

Thus $a_2^2 - 4a_4$ is not a square since (4.6) is not congruent to 1 modulo 4. In particular, $C_2 \times C_2 \not\hookrightarrow \mathcal{Y}_t(C_8)(\mathbb{Q})_{\text{tors}}$ which shows that $\mathcal{Y}_t(C_8)(\mathbb{Q})_{\text{tors}} \cong C_8$.

It remains to prove the Proposition for $T = C_2, C_4, C_6, C_8$. To prove these cases we will consider the elliptic curve

$$\begin{aligned}\mathcal{Z}_t(T) : y^2 &= x\left(x^2 + 2m_T x + m_T^2 - n_T^2 d_T\right)\\ &= x\left(x + \left(m_T + n_T\sqrt{d_T}\right)\right)\left(x + \left(m_T - n_T\sqrt{d_T}\right)\right)\end{aligned}$$

Table 4.2.: Quantities for $T = C_2, C_4, C_6$

u_T	r_T	s_T	w_T	T
$-\frac{1}{2(a-b)^2}$	0	$-\frac{1}{2}$	0	C_2
$\frac{1}{8ab}$	$-\frac{\left(a^2+b^2\right)^2}{64a^2b^2}$	$-\frac{1}{2}$	0	C_4
$\frac{1}{\left(a^2-4ab+b^2\right)^2}$	$-\frac{\left(a^2+b^2\right)^2}{\left(a^2-4ab+b^2\right)^2}$	$-\frac{a^4-4a^3b+10a^2b^2-4ab^3+b^4}{\left(a^2-4ab+b^2\right)^2}$	$\frac{\left(a^2+b^2\right)^4}{\left(a^2-4ab+b^2\right)^4}$	C_6

d_T	m_T	n_T	T
$-2ab\left(a^2+b^2\right)$	$-\left(a^4-12a^3b+6a^2b^2-12ab^3+b^4\right)$	$4\left(a-b\right)^2$	C_2
-1	$-\left(a^2-2ab-b^2\right)\left(a^2+2ab-b^2\right)$	$4ab\left(a^2-b^2\right)$	C_4
$ab\left(a^2-ab+b^2\right)$	$-(a^8-4a^7b+4a^6b^2+20a^5b^3-$ $26a^4b^4+20a^3b^5+4a^2b^6-$ $4ab^7+b^8)$	$8ab\left(a-b\right)^3\left(a+b\right)$	C_6

where d_T, m_T, and n_T are as defined in Table 4.2.

Case VII. Next, assume $T = C_2$. Let u_T, r_T, s_T, w_T be as defined in Table 4.2. The admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism between $\mathcal{Y}_t(C_2)$ and $\mathcal{Z}_t(C_2)$. Now observe that the discriminant of the quadratic $x^2 + 2m_T x + m_T^2 - n_T^2 d_T$ is

$$4m_T^2 - 4\left(m_T^2 - n_T^2 d_T\right) = 4d_T n_T^2 = -128ab\left(a^2+b^2\right)(a-b)^4. \tag{4.7}$$

Since a and b are assumed to be positive, the quantity (4.7) is negative and therefore is not a square. In particular, $C_2 \times C_2 \not\hookrightarrow \mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}}$. By the claim at the start of the proof, we know that $|\mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}}|$ is not divisible by an odd prime. Therefore by Theorem 2.1, $\mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}}$ is isomorphic to either C_2, C_4, or C_8. In particular, $\mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}} \cong C_2$ if $\mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}}$ does not contain a point of order 4. We will show this by applying the main theorem of [36]. To apply this Theorem, we first need to verify that m_T and $n_T d_T$ are relatively prime under our assumptions on a and b.

To show this, we consider m_T and $n_T d_T$ as polynomials in $R = \mathbb{Z}[a, b, r, s]$. Let μ'_T and ν'_T be the polynomials defined in Tables E.7 and E.8, respectively. In particular, $\mu'_T, \nu'_T \in R$. Then the we have the identity

$$\mu'_T m_T + \nu'_T n_T d_T = 2^8 \left(ra^9 + sb^9\right). \tag{4.8}$$

Now let a and b be as in the assumption. Then for a given integer $k \geq 1$, we may find integers r and s such that $ra^k + sb^k = 1$. Therefore, by (4.8), $\gcd(m_T, n_T d_T)$ divides 2^8. Since a is even, it follows that $m_T \equiv -b^4 \mod 2$ and so m_T is odd. Hence $\gcd(m_T, n_T d_T) = 1$, and so we may use the main theorem of [36].

Now write $d_T = d'h^2$ with d' squarefree and set $n' = n_T h$. By [36], $C_4 \hookrightarrow \mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}}$ if and only if there exist relatively prime integers u and v satisfying $m_T = u^2 + v^2 d'$ with $n' = 2uv$. Towards a contradiction, we suppose this is the case. Since b is odd, we have that $m_T \equiv -1 \mod 4$ and $n' = 2uv$ implies that exactly one of u or v is even. Therefore $u^2 + v^2 d' \equiv -1 \mod 4$ if and only if u is even and $v^2 d'$ is odd with $d' \equiv -1 \mod 4$. Since $v_2(a)$ is even, we have that d' is even, which is a contradiction. Thus, $\mathcal{Y}_t(C_2)(\mathbb{Q})_{\text{tors}} \cong C_2$.

Case VIII. Next, assume $T = C_4$. Let u_T, r_T, s_T, w_T be as defined in Table 4.2. The admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism between $\mathcal{Y}_t(C_4)$ and $\mathcal{Z}_t(C_4)$. Now observe that the discriminant of the quadratic $x^2 + 2m_T x + m_T^2 - n_T^2 d_T$ is

$$4m_T^2 - 4\left(m_T^2 - n_T^2 d_T\right) = 4d_T n_T^2 = -64a^2b^2\left(a^2 - b^2\right)^2$$

is always negative and therefore is not a square. In particular, $C_2 \times C_2 \not\hookrightarrow \mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}}$. By the claim at the start of the proof, we know that $|\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}}|$ is not divisible by an odd prime. Therefore by Theorem 2.1, $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}}$ is isomorphic to either C_4, or C_8. In particular, $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}} \cong T$ if $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}}$ does not contain a point of order 8. We will show this by applying the main theorem of [36]. To do so, we must first verify that m_T and $n_T d_T$ are relatively prime under our assumptions on a and

b. To this end, consider m_T and $n_T d_T$ as polynomials in $R = \mathbb{Z}[a,b,r,s]$. Let μ'_T and ν'_T be the polynomials defined in Tables E.7 and E.8, respectively. Then

$$\mu'_T m_T + \nu'_T n_T d_T = 2^4 \left(ra^7 + sb^7\right).$$

Now let a and b be as in the assumption. Then for a given integer $k \geq 1$, we may find integers r and s such that $ra^k + sb^k = 1$. Consequently $\gcd(m_T, n_T d_T)$ divides 2^4. But $m_T \equiv -b^4 \mod 2$ and therefore m_T is odd since b is relatively prime to a. In particular, $\gcd(m_T, n_T d_T) = 1$ and so we may use the main theorem of [36]. By [36], $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}} \cong C_8$ if and only if there exist non-zero integers u, v, w such that $m_T = u^4 + v^2 w^2 d_T$, $n_T = 2u^2 vw$, and $2u^2 - v^2 = w^2 d_T$. Towards a contradiction, suppose $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}} \cong C_8$. Then $2ab\left(a^2 - b^2\right) = u^2 vw$ with $m_T = u^4 - v^2 w^2$ for nonzero integers u, v, w. In particular, at least one of u, v, w must be even. Since $m_T \equiv -1 \mod 4$, we verify that $u^4 - v^2 w^2 \equiv -1 \mod 4$ if and only if u is even and $v^2 w^2 \equiv 1 \mod 4$. Since $v_2(a)$ is even, it follows that one of v or w must be even which is a contradiction. Hence $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}} \cong C_4$.

Case IX. Lastly, assume $T = C_6$ and let u_T, r_T, s_T, w_T be as defined in Table 4.2. The admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism between $\mathcal{Y}_t(C_6)$ and $\mathcal{Z}_t(C_6)$. Observe that the discriminant of the quadratic $x^2 + 2m_T x + m_T^2 - n_T^2 d_T$ is

$$4m_T^2 - 4\left(m_T^2 - n_T^2 d_T\right) = 4d_T n_T^2 = 256ab\left(a-b\right)^6\left(a+b\right)^2\left(a^2 - ab + b^2\right)$$

is a square if and only if $ab\left(a^2 - ab + b^2\right)$ is a square. Since a and b are relatively prime, we have that both a and b are relatively prime to $\left(a^2 - ab + b^2\right)$. In particular, $ab\left(a^2 - ab + b^2\right)$ is a square if and only if a, b, and $a^2 - ab + b^2$ are squares. We claim this is not the case. Towards a contradiction, suppose a, b, and $a^2 - ab + b^2$ are squares. Then

$$(X, Y) = \left(\frac{2}{b}\left(a + \sqrt{a^2 - ab + b^2}\right), \frac{2}{b}\sqrt{\frac{a}{b}}\left(2a - b + 2\sqrt{a^2 - ab + b^2}\right)\right)$$

is a rational point on the elliptic curve $y^2 = x^3 - x^2 - 4x + 4$. The Mordell-Weil group of this elliptic curve is isomorphic to $C_2 \times C_4$ and it is equal as a set to

$$\{\mathcal{O}, (4, \pm 6), (\pm 2, 0), (0, \pm 2), (1, 0)\}.$$

Our desired contradiction is now obtained since

$$X = 0 \Longrightarrow a = b;\ Y = 0 \Longrightarrow a = 0 \text{ or } b = 0; \text{ and } X = 4 \Longrightarrow a = b \text{ or } b = 0.$$

Therefore $4d_T n_T^2$ is not a square which is equivalent to $C_2 \times C_2 \not\hookrightarrow \mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}}$. By Theorem 2.1, $\mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}}$ is isomorphic to either C_6, or C_{12}. It suffices to show that $C_{12} \not\hookrightarrow \mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}}$. This is equivalent to showing that $C_4 \not\hookrightarrow \mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}}$. As with the previous two cases, we first show that m_T and $n_T d_T$ are relatively prime. To this end, let μ_T' and ν_T' be the polynomials defined in Tables E.7 and E.8, respectively and consider m_T and $n_T d_T$ as polynomials in $R = \mathbb{Z}[a, b, r, s]$. Then

$$\mu_T' m_T + \nu_T' n_T d_T = 2^7 3 \left(ra^{17} + sb^{17}\right)$$

Now let a and b be as in the assumption. Then for a given integer $k \geq 1$, we may find integers r and s such that $ra^k + sb^k = 1$. Therefore, $\gcd(m_T, n_T d_T)$ divides $2^7 3$ for each T. Since $a \equiv 0 \mod 6$, it follows that $m_T \equiv -b^8 \mod 6$ and so $m_T \equiv -1 \mod 6$. Hence $\gcd(m_T, n_T d_T) = 1$. We may, therefore, use the main theorem of [36].

Let $d_T = d'h^2$ with d' squarefree and set $n' = n_T h$. By [36], $C_4 \hookrightarrow \mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}}$ if and only if there exist relatively prime integers u and v satisfying $m_T = u^2 + v^2 d'$ with $n' = 2uv$. Towards a contradiction, we suppose this is the case. Since d_T is always positive, we have that $u^2 + v^2 d'$ is always positive and therefore $m_T \neq u^2 + v^2 d'$ since m_T is always negative whenever a and b are positive. Thus $C_4 \not\hookrightarrow \mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}}$ and therefore $\mathcal{Y}_t(C_6)(\mathbb{Q})_{\text{tors}} \cong C_6$ which concludes the proof. ∎

Remark If $t = \frac{2209}{18}$, then $\mathcal{Y}_t(C_4)(\mathbb{Q})_{\text{tors}} \cong C_8$, which shows the need for the assumption of $v_2(a)$ being even.

4.2 Elliptic Curves with Minimal Discriminant

Consider the polynomial ring $R = \mathbb{Q}[a, b]$. For each T we define the polynomials $A_T = A_T(a, b)$, $B_T = B_T(a, b)$, $D_T = D_T(a, b)$, and $\hat{D}_T = \hat{D}_T(a, b)$ as given in Tables E.1, E.2, E.3, and E.4, respectively. Our first result can be verified with a computer algebra system.

Lemma 4.6 *For each T, the identity $A_T^3 - B_T^2 = 1728 D_T$ holds in R. Moreover, let μ_T and ν_T be as defined in Tables E.5 and E.6, respectively. Then $\mu_T, \nu_T \in \mathbb{Z}[a, b, r, s]$ and $\mu_T A_T + \nu_T B_T$ is the quantity given in the Table 4.3.*

Table 4.3.: $\mu_T A_T + \nu_T B_T$

$\mu_T A_T + \nu_T B_T$	T
$-2^4 3^{21} (ra^{29} + sb^{29})$	C_1
$2^{22} 3^2 (ra^{19} + sb^{19})$	C_2
$2^4 3^{12} (ra^{29} + sb^{29})$	C_3
$2^{14} 3^2 (ra^{18} + sb^{18})$	C_4
$2^{49} 3^2 5$	C_5
$2^{22} 3^4 (ra^{39} + sb^{39})$	C_6
$2^4 3^2 7 (ra^{19} + sb^{19})$	C_7
$2^{22} 3^2 (ra^{38} + sb^{38})$	C_8

$\mu_T A_T + \nu_T B_T$	T
$2^4 3^4 (ra^{39} + sb^{29})$	C_9
$-2^3 3^2 5 (ra^{29} + sb^{29})$	C_{10}
$2^7 3^4 (ra^{39} + sb^{39})$	C_{12}
$2^{14} 3^2 (ra^{18} + sb^{18})$	$C_2 \times C_2$
$2^6 3^2 (ra^{16} + sb^{16})$	$C_2 \times C_4$
$2^{14} 3^4 (ra^{39} + sb^{39})$	$C_2 \times C_6$
$2^{14} 3^2 (ra^{38} + sb^{38})$	$C_2 \times C_8$

Proposition 4.7 *Let T be one of the fifteen torsion subgroups in Theorem 2.1. For $T \neq C_5$, suppose a and b be relatively prime integers with $a \equiv 0 \mod 6$. Moreover, (i) for $T = C_5$, assume that $b = 2^{n+1}$ for some nonnegative integer n; (ii) for $T = C_{10}$, assume that $a \equiv 0 \mod 5$, and (iii) for $T = C_7$ assume that $a \equiv 0 \mod 7$. Then $A_T = A_T(a, b)$, $B_T = B_T(a, b)$, and $D_T = D_T(a, b)$ are integers with A_T and B_T and*

$$\gcd(A_T, B_T) = \begin{cases} 5 & \text{if } T = C_5 \\ 1 & \text{otherwise.} \end{cases}$$

Proof We proceed by cases.

Case I. For $T = C_5$, let $b = 2^{n+1}$ and observe that

$$A_T = 2^{80n+60} - 3 \cdot 2^{60n+47} + 7 \cdot 2^{40n+31} + 3 \cdot 2^{20n+17} + 1$$
$$B_T = -2^{120n+90} + 9 \cdot 2^{100n+76} - 75 \cdot 2^{80n+60} - 75 \cdot 2^{40n+30} - 9 \cdot 2^{20n+16} - 1$$

Since n is a nonnegative integer, we have that A_T and B_T are integers. Now let $\mu_T = \mu_T(a,b)$ and $\nu_T = \nu_T(a,b)$ be as defined in Tables E.5 and E.6, respectively. Since they are integers we have that $\gcd(A_T, B_T)$ divides $2^{49}3^2 5$ since $\mu_T A_T + \mu_T B_T = 2^{49}3^2 5$ by the previous lemma. The $\gcd(A_T, B_T)$ is not divisible by 2 since A_T and B_T are odd. Moreover, $\gcd(A_T, B_T)$ is not divisible by 3 since

$$A_T \equiv 2^{80n+60} + 2^{40n+31} + 1 \mod 3 = 1 \mod 3.$$

Therefore $\gcd(A_T, \beta_T)\,|5$. Reducing modulo 5 and applying Fermat's Little Theorem, we deduce that

$$A_T \equiv \left(2^{20n+15}\right)^4 + \left(2^{15n+12}\right)^4 + \left(2^{10n+8}\right)^4 + \left(2^{5n+4}\right)^4 + 1 \mod 5 = 0 \mod 5.$$

Similarly,

$$B_T \equiv \left(2^{30n+23}\right)^4 + 4 \cdot \left(2^{20n+19}\right)^4 + \left(2^{5n+4}\right)^4 + 4 \mod 5 = 0 \mod 5.$$

Thus $\gcd(A_T, B_T) = 5$.

Case II. Let $T = C_{10}$. By assumption a is even and so we may write $a = 2\hat{a}$ for some integer $\hat{a}$. Then A_T and D_T are integers since

$$A_T = 256\hat{a}^{12} + 2048\hat{a}^{11}b + 6656\hat{a}^{10}b^2 + 11520\hat{a}^9b^3 + 11520\hat{a}^8b^4 + 6528\hat{a}^7b^5 +$$
$$664\hat{a}^6b^6 - 192\hat{a}^5b^7 - 240\hat{a}^4b^8 - 40\hat{a}^3b^9 + 16\hat{a}^2b^{10} + 8\hat{a}b^{11} + b^{12}$$
$$D_T = \hat{a}^5b^{10}\left(\hat{a}+b\right)^{10}\left(2\hat{a}+b\right)^{10}\left(-4\hat{a}^2 - 2\hat{a}b + b^2\right)^2\left(\hat{a}^2 + 3\hat{a}b + b^2\right).$$

Consequently, B_T is an integer due to the identity $B_T^2 = 1728D_T - A_T^3$. Since a and b are relatively prime, we can find integers r and s such that $ra^{29} + sb^{29} = 1$. In particular, by Lemma 4.6 it follows that $\gcd(A_T, B_T)$ divides $2^3 3^2 5$. By assumption

$a \equiv 0 \mod 30$ and therefore $A_T \equiv b^{12} \mod 30$. In particular, A_T is not divisible by $2, 3$, or 5 and thus $\gcd(A_T, B_T) = 1$.

Case III. Let $T = C_7$. From the definition of A_T, B_T, and D_T it is clear that these quantities are integers. By a similar argument to Case II, it follows that $\gcd(A_T, B_T)$ divides $2^4 3^2 7$. By assumption $a \equiv 0 \mod 42$ and by inspection $A_T \equiv b^6 \mod 42$. In particular, A_T is not divisible by $2, 3$, or 7 and so $\gcd(A_T, B_T) = 1$.

Case IV. Let $T = C_2, C_4, C_2 \times C_2, C_2 \times C_4$. That A_T and B_T are integers follows from their definitions in Tables E.1 and E.2, respectively. By Table E.4, it is clear that D_T is an integer in each of these cases since a is even. A similar argument to the preceding two cases shows that $\gcd(A_T, B_T)$ divides $2^{22} 3^2$. Since a is divisible by 6, we have by inspection that $A_T \equiv b^8 \mod 6$. Consequently A_T is not divisible by 2 or 3 and so $\gcd(A_T, B_T) = 1$.

Case V. For the remaining T, we observe that A_T, B_T, D_T are integers by their definition in Tables E.1, E.2, and E.4, respectively. A similar argument to the above shows that $\gcd(A_T, B_T)$ divides $2^{22} 3^{21}$. Since $a \equiv 0 \mod 6$, $A_T \equiv b^k \mod 6$ for some positive integer k. Hence A_T is not divisible by 2 or 3 and so $\gcd(A_T, B_T) = 1$. ■

Theorem 4.8 *Assume the terminology of Proposition 4.7. For each T, let $H_T = H_T(A_T, B_T)$ be the rational elliptic curve given by*

$$H_T : y^2 + xy + a_{3,T}\, y = x^3 + a_{2,T}\, x^2 - \frac{a_{4,T}}{48} x - \frac{a_{6,T}}{1728} \text{ where} \tag{4.9}$$

$$a_{4,T} = A_T - 1,$$

$$a_{2,T} = a_{3,T} = \begin{cases} 1 & \text{if } T = C_5 \\ 0 & \text{if } T \neq C_5 \end{cases}, \text{ and } a_{6,T} = \begin{cases} 15A_T + 2B_T + 307 & \text{if } T = C_5 \\ 3A_T + 2B_T - 1 & \text{if } T \neq C_5. \end{cases}$$

The invariants of H_T are $c_4 = A_T$ and $c_6 = B_T$. Its discriminant is D_T and it is the minimal discriminant since (4.9) *is the reduced minimal Weierstrass model for H_T. Moreover, for all T except $T = C_5$, H_T is semistable. For $T = C_5$, H_T is semistable away from $p = 5$. Suppose further that $v_2(a)$ is even if $T = C_2, C_4$. Then $H_T(\mathbb{Q})_{tors} \cong T$.*

Proof By Proposition 4.7, A_T, B_T, and D_T are integers. It is verified via the formulas (2.2) that c_4 and c_6 are as claimed and that the discriminant of H_T is D_T. We now claim that H_T is given by an integral Weierstrass model. To this end, it suffices to show that $a_{4,T} \equiv 0 \mod 16$, $a_{4,T} \equiv 0 \mod 3$, $a_{6,T} \equiv 0 \mod 27$, and $a_{6,T} \equiv 0 \mod 64$. We show most of these congruences via Mathematica [30]. We consider the cases $T = C_5$ and $T \neq C_5$.

Case I. For $T = C_5$, let $b = 2^{n+1}$ for some nonnegative integer n and consider $A_T = A_T(1, 2^{n+1})$ and $B_T = B_T(1, 2^{n+1})$. Then

$$a_{4,T} = 2^{80n+60} + 3 \cdot 2^{60n+47} + 7 \cdot 2^{40n+31} + 3 \cdot 2^{20n+17}.$$

In particular, $a_{4,T} \equiv 0 \mod 16$ and $a_{4,T} \equiv 2^{80n} + 2 \cdot 2^{40n} \mod 3$. Since squares modulo 3 are congruent to 1 modulo 3, we conclude that $a_{4,T} \equiv 0 \mod 3$. Next,

$$\begin{aligned} a_{6,T} = -2^{120n+91} + 9 \cdot 2^{100n+77} - 148 \cdot 2^{80n+60} + \\ 45 \cdot 2^{60n+47} + 15 \cdot 2^{40n+32} + 9 \cdot 2^{20n+19} + 2^6 5. \end{aligned}$$

Thus $a_{6,T} \equiv 0 \mod 64$ and

$$a_{6,T} \equiv 25 \cdot 2^{120n} + 18 \cdot 2^{100n} + 18 \cdot 2^{60n} + 6 \cdot 2^{40n} + 18 \cdot 2^{20n} + 23 \mod 27.$$

Since $25 \cdot 2^{120n} + 6 \cdot 2^{40n} \equiv 4 \mod 27$ and $18 \cdot 2^{20n} \equiv 0 \mod 27$ for each nonnegative integer n, it follows that $a_{6,T} \equiv 0 \mod 27$. Hence H_T is given by an integral Weierstrass model. We claim that H_T is a global minimal model for H_T. Indeed, since $\gcd(A_T, B_T) = 5$ by Proposition 4.7 we have that the only fourth power dividing c_4 and c_6 is ± 1. Thus H_T is a global minimal model. By Lemma 2.2, H_T has additive reduction at 5 since 5 divides its discriminant and invariant c_4. Moreover, E_T is semistable at each prime $p \neq 5$. Lastly, let u_T, r_T, s_T, and w_T be as defined in the table E.9. Then the admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism between H_T and $\mathcal{Y}_{b/a}(T)$. Therefore, $H_T(\mathbb{Q})_{\mathrm{tors}} \cong T$ by Proposition 4.5.

Case II. Now suppose $T \neq C_5$ and let `a4T[a,b]` and `a6T[a,b]` be the Mathematica inputs for $a_{4,T} = a_{4,T}(a, b)$ and $a_{6,T} = a_{6,T}(a, b)$, respectively. Write $a = 6k$

for some integer k. Since b is odd and congruent to $\pm 1 \mod 3$, we verify that $a_{4,T} \equiv 0 \mod 16$, $a_{4,T} \equiv 0 \mod 3$, $a_{6,T} \equiv 0 \mod 27$, and $a_{6,T} \equiv 0 \mod 64$ via the Mathematica inputs

```
Table[Mod[a4[6*k,b],16],{k,1,16},{b,1,16,2}]
Table[Mod[a4[6*k,b],3],{k,1,3},{b,1,2}]
Table[Mod[a6[6*k,b],27],{k,1,27},{b,1,27,3}]
Table[Mod[a6[6*k,b],27],{k,1,27},{b,2,27,3}]
Table[Mod[a6[6*k,b],64],{k,1,64},{b,1,64,2}]
```

Hence H_T is given by an integral Weierstrass model for all T. By Proposition 4.7 $\gcd(A_T, B_T) = 1$ and therefore H_T is a global minimal model since there is no fourth power other than 1 dividing $\gcd(c_4, c_6)$. In particular, (4.9) is the reduced minimal model for H_T. Moreover, H_T is semistable.

Next, let u_T, r_T, s_T, and w_T be as defined in the table E.9. Then the admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism between H_T and $\mathcal{Y}_{b/a}(T)$. Therefore, $H_T(\mathbb{Q})_{\text{tors}} \cong T$ by Proposition 4.5. ■

4.3 Sequences of Good ABC Triples

In this section, we will consider $A_T = A_T(a,b)$, $B_T = B_T(a,b)$, $D_T = D_T(a,b)$, and $\hat{D}_T = \hat{D}_T(a,b)$ as polynomials in a and b. Note that for each T except $T = C_5$, A_T^3, B_T^2, D_T, and $\hat{D}_T^6$ are homogenous polynomials in $\mathbb{Q}[a,b]$ of degree n_T where

$$n_T = \begin{cases} 24 & \text{if } T = C_2, C_4, C_7, C_2 \times C_2, C_2 \times C_4 \\ 36 & \text{if } T = C_1, C_3, C_9, C_{10} \\ 48 & \text{if } T = C_6, C_8, C_{12}, C_2 \times C_6, C_2, C_2 \times C_8. \end{cases} \tag{4.10}$$

We will now consider $A_T(1,x)$, $B_T(1,x)$, $D_T(1,x)$, and $\hat{D}_T(1,x)$ as functions from $\mathbb{R} \to \mathbb{R}$ as well as the rational functions $f_T, g_T, h_T : \mathbb{R} \to \mathbb{R}$ as defined below

$$f_T(x) = \begin{cases} \frac{A_T(1,x)^3}{-1728 D_T(1,x)} - x & \text{if } T = C_4, C_8 \\ \frac{B_T(1,x)^2}{1728 D_T(1,x)} - x & \text{for all other } T \text{ except } T = C_1, C_2. \end{cases} \tag{4.11}$$

$$g_T(x) = \begin{cases} -B_T(1,x) - A_T(1,x)\,\hat{D}_T(1,x) & \text{if } T = C_4, C_8 \\ A_T(1,x)^2 + B_T(1,x)\,\hat{D}_T(1,x) & \text{for all other } T \text{ except } T = C_1, C_2. \end{cases} \tag{4.12}$$

$$h_T(x) = \begin{cases} B_T(1,x)^2 - \hat{D}_T(1,x)^6 & \text{if } T = C_2, C_4, C_8 \\ A_T(1,x)^3 - \hat{D}_T(1,x)^6 & \text{for all other } T \end{cases}$$

The following lemma can be verified with a computer algebra system.

Lemma 4.9 *Let $f_T(x)$, $g_T(x)$, and $h_T(x)$ be as defined above. Let δ_T be the largest real root of $f_T(x)$ and for each T let γ_T be given by*

$$\gamma_T = \begin{cases} \textit{largest real root of } A_T(1,x) & \textit{if } T = C_2, C_4, C_8 \\ \textit{largest real root of } D_T(1,x) & \textit{otherwise.} \end{cases}$$

Then $\gamma_T = 1$, if $T = C_2 \times C_2, C_2 \times C_4$ and we have the approximations

$$\delta_T \approx \begin{cases} 43.4033 & \textit{if } T = C_3 \\ 432.43 & \textit{if } T = C_4 \\ 43.3677 & \textit{if } T = C_6 \\ 7.07956 & \textit{if } T = C_7 \\ 12.2476 & \textit{if } T = C_8 \\ 4.75552 & \textit{if } T = C_9 \\ 3.06311 & \textit{if } T = C_{10} \\ 3.89418 & \textit{if } T = C_{12} \\ 432.569 & \textit{if } T = C_2 \times C_2 \\ 4.93645 & \textit{if } T = C_2 \times C_4 \\ 6.00485 & \textit{if } T = C_2 \times C_6 \\ 3.38169 & \textit{if } T = C_2 \times C_8 \end{cases} \quad \textit{and } \gamma_T \approx \begin{cases} 4.41147 & \textit{if } T = C_1, C_3, C_9 \\ 115.382 & \textit{if } T = C_2 \\ 7.59575 & \textit{if } T = C_4 \\ 1.34123 & \textit{if } T = C_5 \\ 3.73205 & \textit{if } T = C_6, C_{12}, C_2 \times C_6 \\ 6.2959 & \textit{if } T = C_7 \\ 4.17101 & \textit{if } T = C_8 \\ 1.61803 & \textit{if } T = C_{10} \\ 2.41421 & \textit{if } T = C_2 \times C_8. \end{cases}$$

Moreover,

(*i*) *For each T except $T = C_1, C_2, C_5$, the functions $f_T(x)$, $g_T(x)$, $-B_T(1,x)$ are positive on the interval (δ_T, ∞);*

(*ii*) *For each T, the functions $h_T(x)$, $A_T(1,x)$, $\hat{D}_T(1,x)$ are positive on the interval (γ_T, ∞);*

(*iii*) *On (γ_T, ∞), the function $D_T(1,x)$ is negative if $T = C_2, C_4, C_8$ and it is positive for the remaining T.*

Corollary 4.10 *For each T except $T = C_5$, let a and b be relatively prime positive integers with $a \equiv 0 \mod 6$ and $\frac{b}{a} > \gamma_T$ where γ_T is as in the previous lemma. Assume further that $a \equiv 0 \mod 5$ (resp. $a \equiv 0 \mod 7$) whenever $T = C_{10}$ (resp. $T = C_7$). Then*

$$\begin{array}{ll} (-1728D_T, A_T^3, B_T^2) & \textit{is a positive } ABC \textit{ triple if } T = C_2, C_4, C_8 \\ (1728D_T, B_T^2, A_T^3) & \textit{is a positive } ABC \textit{ triple for the remaining } T. \end{array}$$

Proof By Lemma 4.6 and Proposition 4.7 it follows that they are ABC triples for each T. Let $t = \frac{b}{a}$ so that $D_T(a,b) = a^{n_T} D_T\left(1, \frac{b}{a}\right)$ where n_T is as given in (4.10). By Lemma 4.9 (iii), the assumption that $\frac{b}{a} > \gamma_T$ allows us to conclude that $-D_T(a,b)$ is positive if $T = C_2, C_4, C_8$ and that $D_T(a,b)$ is positive for the remaining T. By Lemma 4.9 (ii), $A_T(1,x)$ is positive on (γ_T, ∞) and thus $A_T(a,b)$ is positive for all T since $A_T(a,b) = a^{n_T/3} A_T\left(1, \frac{b}{a}\right)$. ■

Proposition 4.11 *Let $P_0 = (a_0, b_0, c_0)$ be a positive ABC triple with $a_0 \equiv 0 \mod 6$ and $\frac{b_0}{a_0} > \delta_T$. For each T except $T = C_1, C_2, C_5$, define $P_n^T = (a_n, b_n, c_n)$ recursively by*

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{pmatrix} = \begin{pmatrix} -1728D_T(a_n, b_n) \\ A_T(a_n, b_n)^3 \\ B_T(a_n, b_n)^2 \end{pmatrix} \textit{if } T = C_4, C_8$$

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{pmatrix} = \begin{pmatrix} 1728D_T(a_n, b_n) \\ B_T(a_n, b_n)^2 \\ A_T(a_n, b_n)^3 \end{pmatrix} \textit{for all other } T.$$

Assume further that $a_0 \equiv 0 \mod 5$ *(resp.* $a_0 \equiv 0 \mod 7$*) whenever* $T = C_{10}$ *(resp.* $T = C_7$*). Then for each* n*, the same congruences above hold for* a_n*,* $\frac{b_n}{a_n} > \delta_T$*, and* $P_n^T = (a_n, b_n, c_n)$ *is a positive ABC triple. Additionally, for* $n \geq 1$*,* $v_2(a_n)$ *is even if* $T = C_4, C_2 \times C_2, C_2 \times C_4$*.*

Proof For each T and any given n we have that the statement on congruences is automatic since $D_T(a_n, b_n) \equiv 0 \mod a_n$. Moreover, by Lemma 4.6 and Proposition 4.7 we deduce that P_n^T is an ABC triple for each n. Now let f_T be as defined in (4.11) and observe that

$$f_T\left(\frac{b_n}{a_n}\right) = \frac{b_{n+1}}{a_{n+1}} - \frac{b_n}{a_n}.$$

By Lemma 4.9, f_T is positive on (δ_T, ∞). Since $\frac{b_0}{a_0} > \delta_T$, it follows that $\frac{b_1}{a_1} > \frac{b_0}{a_0} > \delta_T$ and in fact we obtain an increasing sequence $\left\{\frac{b_n}{a_n}\right\}_n$ of rational numbers. Hence P_n^T is a positive ABC triple by Corollary 4.10.

Lastly, for $T = C_4, C_2 \times C_2, C_2 \times C_4$, observe that $v_2(a_{n+1}) = v_2\left(2^m a_n^k\right)$ where m and k are positive even integers. Hence $v_2(a_n)$ is even for all $n \geq 1$. ■

Lemma 4.12 *For* $T = C_5$*, let* $b = 2^n$ *for some positive integer* n*. Then* $\frac{1}{5}\hat{D}_T(1, b)$ *is a positive integer and* $\mathrm{rad}(D_T(1, b)) \leq \frac{1}{5}\hat{D}_T(1, b)$*. For the remaining* T*, let* (a, b, c) *be a good ABC triple with* a *even and* $\max\{|a|, |b|, |c|\} = |c|$*. Then* $\hat{D}_T(a, b)$ *is an integer and*

$$\mathrm{rad}(D_T(a, b)) < \hat{D}_T(a, b) .$$

Proof We first consider the case when $T = C_5$. By Lemma 4.9 (ii), the quantity $\hat{D}_T(1, b)$ is positive since $b > \gamma_T$. It suffices to show that $\frac{2^{35}}{b^{100}} D_T(1, b)$ is divisible by $2^{10}5^3$ since this would imply that $\frac{1}{5}\hat{D}_T(1, b)$ is an integer and that any prime dividing $D_T(1, b)$ also divides $\frac{1}{5}\hat{D}_T(1, b)$, which is equivalent to the desired inequality. That the quantity is divisible by 2^{10} is clear. By Fermat's Little Theorem we deduce that it is divisible by 5^3 since the quantities $(b^8 - 2b^4 - 4)$, $(b^{16} - 4b^{12} + 16b^8 - 24b^4 + 16)$, and $(b^{16} + 6b^{12} + 16b^8 + 16b^4 + 16)$ are all congruent to 0 modulo 5.

For $T \neq C_5$, we let (a,b,c) be a good ABC triple with $\max\{|a|,|b|,|c|\} = |c|$ and a even. By definition, $\operatorname{rad}(abc) < c$ and by properties of the radical we have that

$$\operatorname{rad}\left(abcd^k\right) = \operatorname{rad}(abcd) \leq \operatorname{rad}(abc)\operatorname{rad}(d) < c\operatorname{rad}(d) \leq cd$$

for any positive integers d and k. Moreover, if 2^k divides a, then $\operatorname{rad}\left(\frac{a}{2^k}\right) \leq \operatorname{rad}(a)$. Using these two statements it is easy to verify by inspection that the claim holds for all T with the possible exception of $T = C_{10}$.

For $T = C_{10}$, we first observe that

$$\operatorname{rad}(D_T(a,b)) \leq \operatorname{rad}(4096 D_T(a,b)) = \operatorname{rad}(Q(a,b)) \text{ where}$$
$$Q(a,b) = ab\,(a+b)\,(a+2b)\left(a^2+6ab+4b^2\right)\left(-a^2-ab+b^2\right)$$

Moreover,

$$\frac{Q(a,b)}{ab\,(a+B)} = (a+2b)\left(a^2+6ab+4b^2\right)\left(-a^2-Ab+b^2\right) \equiv 0 \mod 8$$

and therefore $(a+2b)\,(a^2+6ab+4b^2)\,(-a^2-Ab+b^2) = 8P$ for some P. The result now follows since

$$\begin{aligned}
\operatorname{rad}(Q(a,b)) &= \operatorname{rad}(8ab\,(a+b)\,P) \\
&= \operatorname{rad}(ab\,(a+b)\,P) \text{ since } a \text{ is even} \\
&< |a+b|\operatorname{rad}(P) \\
&\leq |a+b|\,|P| = \hat{D}_T(a,b) \ .
\end{aligned}$$

■

Proposition 4.13 *Assume the statement of Proposition 4.11 with the additional assumption that $P_0 = (a_0, b_0, c_0)$ is a good positive ABC triple. For $T \neq C_1, C_2, C_5$, P_n^T is a good positive ABC triple for each n.*

Proof Fix T and let P_0 be a good positive ABC triple with $\frac{b_0}{a_0} > \delta_T$. By Proposition 4.11, $P_n^T = (a_n, b_n, c_n)$ is a positive ABC triple, a_n is even, and $\frac{b_n}{a_n} > \delta_T$ for each n.

We proceed by induction on n and assume that P_n^T is good. Since $\delta_T > \gamma_T$, we have by Lemma 4.12 that

$$\begin{aligned} \operatorname{rad}(a_{n+1}b_{n+1}c_{n+1}) &= \operatorname{rad}(D_T(a_n,b_n)\,A_T(a_n,b_n)\,B_T(a_n,b_n)) \\ &< \hat{D}_T(a_n,b_n)\,A_T(a_n,b_n)\,|B_T(a_n,b_n)|\,. \end{aligned} \tag{4.13}$$

Recall that the polynomials A_T^3, B_T^2, D_T, and $\hat{D}_T^6$ are of the same homogenous degree n_T. Let $t_n = \frac{b_n}{a_n}$ and observe that

$$c_{n+1} - \hat{D}_T(a_n,b_n)\,A_T(a_n,b_n)\,|B_T(a_n,b_n)| = \begin{cases} a_n^{n_T}\,|B_T(1,t_n)|\,g_T(t_n) & \text{if } T = C_4, C_8 \\ a_n^{n_T}\,A_T(1,t_n)\,g_T(t_n) & \text{for all other } T. \end{cases}$$

Since $t_n > \delta_T$, it follows that $g_T(t_n)$ is positive by Lemma 4.9 and hence the left hand side is positive. Equivalently, $\hat{D}_T(a_n,b_n)\,A_T(a_n,b_n)\,|B_T(a_n,b_n)| < c_{n+1}$. By (4.13), we conclude that $\operatorname{rad}(a_{n+1}b_{n+1}c_{n+1}) < c_{n+1}$ and so P_n^T is a good positive ABC triple for each n, as desired. ■

4.4 Proof of Theorem 4.1

Lemma 4.14 *For each T except $T = C_5$, let $P^T = (a_T, b_T, c_T)$ be a good positive ABC triple with $a_T \equiv 0 \mod 6$ and $\frac{b_T}{a_T} > \gamma_T$ where γ_T is as in Lemma 4.9. Assume further, that $a_T \equiv 0 \mod 5$ (resp. $a_T \equiv 0 \mod 7$) if $T = C_{10}$ (resp. $T = C_7$) and that $v_2(a_T)$ is even if $T = C_2, C_4$. Let H_T be the rational elliptic curve given by the Weierstrass equation (4.9) in Theorem 4.8 with $A_T = A_T(a_T, b_T)$ and $B_T = B_T(a_T, b_T)$. Then H_T is a good semistable elliptic curve with $H_T(\mathbb{Q})_{tors} \cong T$.*

Proof For each T, we have by Theorem 4.8 that H_T is a semistable elliptic curve with $H_T(\mathbb{Q})_{\text{tors}} \cong T$ and that the discriminant $D_T = D_T(a_T, b_T)$ is minimal. Moreover, the invariants c_4 and c_6 associated with a global minimal model of H_T are A_T and B_T, respectively. By Corollary 4.10 we have that

$$\max\{A_T^3, B_T^2\} = \begin{cases} B_T^2 & \text{if } T = C_2, C_4, C_8 \\ A_T^3 & \text{for all other } T. \end{cases}$$

Let n_T be the homogenous degree of A_T^3, B_T^2, and $\hat{D}_T^6$ and let $t = \frac{b_T}{a_T}$. Observe that $h_T(t)$ is positive by Lemma 4.9. Therefore

$$\max\left\{ A_T^3 \right., B_T^2 \quad - \hat{D}_T^6 = a_T^{n_T} h_T(t)$$

is positive by Lemma 4.9. Since H_T is semistable and $D_T \equiv 0 \mod 6$, we have that $\mathrm{rad}(1728 D_T) = N_{H_T}$ where N_{H_T} is the conductor of H_T. Since P^T is a good ABC triple, $N_{H_T} < \hat{D}_T$ by Lemma 4.12 and therefore H_T is good. ■

Theorem 4.1. For $T = C_5$, let $b_n = 2^n$ and set $A_{T,n} = A_T(1, b_n)$ and $B_{T,n} = B_T(1, b_n)$. For the remaining T, let $P_0^T = (a_0, b_0, c_0)$ be a good positive ABC triple satisfying $a_0 \equiv 0 \mod 6$ and $a_0 \equiv 0 \mod 5$ (resp. $A_0 \equiv 0 \mod 7$) if $T = C_{10}$ (resp. $T = C_7$). Assume further the following conditions:

(a) If $T = C_1$, let $\frac{b_0}{a_0} > \delta_{C_9}$. Let $P_n^T = \{(a_n, b_n, c_n)\}_n$ be the sequence of ABC triples associated to $T = C_9$.

(b) If $T = C_2$, let $\frac{b_0}{a_0} > \gamma_T$. Let $P_n^T = \{(a_n, b_n, c_n)\}_n$ be the sequence of ABC triples associated to $T = C_2 \times C_4$.

(c) For the remaining T, let $\frac{b_0}{a_0} > \delta_T$ and let $P_n^T = \{(a_n, b_n, c_n)\}_n$ be the sequence of ABC triples associated to T.

For each T except $T = C_5$, let $A_{T,0} = A_T(a_0, b_0)$ and $B_{T,0} = B_T(a_0, b_0)$, and define $A_{T,n}$ and $B_{T,n}$ recursively by

$$A_{T,n+1} = A_T(a_n, b_n) \text{ and } B_{T,n+1} = B_T(a_n, b_n)\,.$$

For each positive integer n, let $H_{T,n}$ be the rational elliptic curve given by the Weierstrass equation (4.9) in Theorem 4.8 with $A_T = A_{T,n}$ and $B_T = B_{T,n}$. Then each $H_{T,n}$ is a good elliptic curve with $H_{T,n}(\mathbb{Q})_{\mathrm{tors}} \cong T$. Moreover, each H_{T_n} is semistable away from 5 for each T. If $T \neq C_5$, then $H_{T,n}$ is semistable.

Proof By Theorem 4.8, $H_{T,n}$ is the reduced minimal Weierstrass model of $H_{T,n}$ and the invariants c_4 and c_6 are $c_4 = A_{T,n}$ and $c_6 = B_{T,n}$, respectively.

We first consider the case when $T = C_5$. By Theorem 4.8, $H_{T,n}$ has additive reduction at 5 for each n and hence $v_5\big(N_{H_{T,n}}\big) = 2$ where $N_{H_{T,n}}$ denotes the conductor of $H_{T,n}$. In particular, $N_{H_{T,n}} = 5\,\mathrm{rad}(D_T(1,b_n)) \leq \hat{D}_T(1,b_n)$ by Lemma 4.12. By Lemma 4.9, $D_T(1,b_n)$, $A_T(1,b_n)$, and $h_T(b_n)$ are positive for each n and hence $\max\{ A_{T,n}^3 , B_{T,n}^2 = A_{T,n}^3$. In particular, $H_{T,n}$ is a good elliptic curve since $A_{T,n}^3 > \hat{D}_T(1,b_n)^6$ and thus $A_{T,n}^3 > N_{H_{T,n}}^6$ for each n. By Theorem 4.8, $H_{T_n}(\mathbb{Q})_{\mathrm{tors}} \cong C_5$ for each n.

For the remaining T, let P_0^T be a good ABC triple. By Proposition 4.11 and Proposition 4.13 we have that for each P_n^T satisfies the assumptions of Lemma 4.14. Hence each $H_{T,n}$ is a good semistable elliptic curve with $H_{T,n}(\mathbb{Q})_{\mathrm{tors}} \cong T$. ■

Lemma 4.15 *Let E be a good semistable elliptic curve with minimal discriminant $\Delta_E \equiv 0 \mod 6$. Then the ABC triple $(1728\Delta_E, -c_4^3, c_6^2)$ is good.*

Proof Since E is good,

$$N_E^6 < \max\{ c_4^3 , c_6^2 \leq \max\{ c_4^3 , c_6^2, 1728\,|\Delta_E|$$

where N_E is the conductor of E and c_4 and c_6 are the invariants associated with a global minimal model of E. Since E is semistable and $\Delta_E \equiv 0 \mod 6$, $\mathrm{rad}(1728\Delta_E) = N_E$. Now observe that

$$\mathrm{rad}(1728\Delta c_4 c_6) = N_E\,\mathrm{rad}(c_4 c_6) \leq N_E\,|c_4|\,|c_6|\,.$$

It suffices to show that $N_E\,|c_4|\,|c_6| < \max\{|c_4^3|\,, c_6^2\}$ since this would imply that $\mathrm{rad}(1728\Delta c_4 c_6) < \max\{|c_4^3|\,, c_6^2, 1728\,|\Delta_E|\}$.

Case I. Suppose $\max\{|c_4^3|\,, c_6^2\} = |c_4^3|$. Then $N_E < |c_4|^{1/2}$ and $|c_6| < |c_4|^{3/2}$. Thus

$$N_E\,|c_4|\,|c_6| < |c_4|^{1/2}\,|c_4|\,|c_4|^{3/2} = c_4^3 \,.$$

Case II. Suppose $\max\{|c_4^3|\,, c_6^2\} = c_6^2$. Then $N_E < |c_6|^{1/3}$ and $|c_4| < |c_6|^{2/3}$. Hence

$$N_E\,|c_4|\,|c_6| < |c_6|^{1/3}\,|c_6|^{2/3}\,|c_6| = c_6^2$$

which concludes the proof. ■

The following result now follows.

Corollary 4.16 *Assume the statement of Theorem 4.1. Let* $\{H_{T,n}\}_{n\geq 1}$ *be the sequence of good elliptic curves associated to* $T = C_1, C_2$*. Then* $\{(1728D_{T,n}, -A^3_{T,n}, B^2_{T,n}$ *is a sequence of good ABC triples for each* n*.*

Remark The converse to the previous lemma does not hold. Let E be the elliptic curve given by the Weierstrass equation

$$E : y^2 + xy = x^3 - 2342114817x - 46491207963039.$$

The curve E is semistable and its discriminant Δ is minimal. Let c_4 and c_6 be the invariants associated to a global minimal model of E, given explicitly below

$$\Delta = -2^3 3^6 7^3 67^9 127^3,\ c_4 = 19 \cdot 53 \cdot 157 \cdot 251 \cdot 2833,\ c_6 = 13^2 73 \cdot 5651 \cdot 576166333.$$

The positive ABC triple $(-1728\Delta, c_4^3, c_6^2)$ is good and satisfies $\Delta \equiv 0 \mod 6$, yet E is not good since $\max\{c_4^3, c_6^2\} = c_6^2 < N_E^6$. However, E is 3-isogenous to the good elliptic curve

$$F : y^2 + xy = x^3 - 193149169647x - 32672893402475361.$$

4.5 Examples

Recall that for an ABC triple $P = (a, b, c)$ and a rational elliptic curve E, the **quality** $q(P)$ of P and the **modified Szpiro ratio** $\sigma(E)$ of E are defined as

$$q(P) = \frac{\log(\max\{|A|, |B|, |C|\})}{\mathrm{rad}(ABC)} \text{ and } \sigma_m(E) = \frac{\log(\max\{|c_4^3|, |c_6^2|\})}{\log N_E}.$$

where N_E is the conductor of E and c_4 and c_6 are the invariants associated to a global minimal model of E. Moreover, P is a good ABC triple if and only if $q(P) > 1$ and E is a good elliptic curve if and only if $\sigma_m(E) > 6$. Due to computational limitations, it is difficult to find $q(P)$ and $\sigma_m(E)$ for the second term of our sequences since they require the factorization of very large numbers. To bypass this, we use Lemma 4.12 for $T \neq C_5$. We start with the following definition which will be used to bypass the need of factorization of large numbers.

Definition 4.1 *Consider the ABC triple* $P = (1728D_T, B_T^2, A_T^3)$ *and let* $H_T = H_T(A_T, B_T)$ *be the elliptic curve defined in Theorem 4.8. The* ***pseudo quality*** $q'(P)$ *of* P *and the* ***pseudo modified Szpiro ratio*** $\sigma'_m(H_T)$ *of* H_T *are as defined below*

$$q'(P) = \frac{\log(\max\{|A_T^3|, B_T^2, |1728D_T|\})}{\log\ A_T B_T \hat{D}_T} \qquad \textit{and} \qquad \sigma'_m(H_T) = \frac{\log(\max\{|A_T^3|, B_T^2\})}{\log\ \hat{D}_T}$$

Lemma 4.17 *Let* (a, b, c) *be a good ABC triple with* $a \equiv 0 \mod 6$ *and let* $A_T = A_T(a, b)$, $B_T = B_T(a, b)$, $D_T = D_T(a, b)$, *and* $\hat{D}_T = \hat{D}_T(a, b)$. *Let* P *be the ABC triple* $(1728D_T, B_T^2, A_T^3)$ *and let* $H_T = H_T(A_T, B_T)$. *Then*

$$q'(P) < q(P) \qquad \textit{and} \qquad \sigma'_m(H_T) < \sigma_m(H_T)\,.$$

Proof Note that $\mathrm{rad}(1728D_T) = \mathrm{rad}(D_T) = N_{H_T}$ where N_{H_T} is the conductor of H_T. By Lemma 4.12, $N_{H_T} < \hat{D}_T$ and $\mathrm{rad}(1728A_TB_TD_T) < A_TB_T\hat{D}_T$. These two inequalities respectively imply that $\sigma'_m(H_T) < \sigma_m(H_T)$ and $q'(P) < q(P)$. ∎

Remark Whenever we use the pseudo quality or pseudo modified Szpiro ratio, we will place a * by the number, e.g. 6.07^*.

The table below list the initial exceptional ABC triple $P_0^T = (a_0, b_0, c_0)$ for $T \neq C_5$. We also give the approximate values of its quality $q\big(P_0^T\big)$ and the ratio $\frac{b_0}{a_0}$.

T	P_0^T	$q\big(P_0^T\big)$	$\frac{B_0}{A_0}$
$C_1, C_9,\ C_{12}, C_2 \times C_4, C_2 \times C_6, C_2 \times C_8$	$(2^6 3, 47^2, 7^4)$	1.0258	11.505
$C_2, C_4, C_2 \times C_2$	$(2^2 43, 3^5 7^3, 17^4)$	1.0969	484.6
Remaining T	$(2 \cdot 3^4, 5 \cdot 7^4, 23^3)$	1.1090	74.1

Note that for each $T \neq C_1, C_2, C_5$, we have $\frac{b_0}{a_0} > \delta_T$ and in the case of $T = C_1, C_2$ we have $\frac{b_0}{a_0} > \gamma_T$. Let $\left\{P_n^T\right\}_n$ be the sequence of good ABC triples given in Proposition 4.11 associated to T for $T \neq C_1, C_2, C_5$. While a_0 does not satisfy the necessary congruences for some of the triples above, we check that P_1^T is a good ABC triple and so A_1^T satisfies the required congruences of this chapter. Thus we are able to conclude that each P_n^T is a good ABC triple. Moreover, let $H_{T,n}$ denote the exceptional elliptic curve associated to P_n^T as in Theorem 4.1. We also mention that in all examples when $a_{T,0}$ does not satisfy the necessary congruences, we still have that $E_{T,1}(\mathbb{Q})_{\text{tors}} \cong T$.

T	$q(P_1^T)$	$\sigma_m(E_{T,1})$	$q(P_2^T)$	$\sigma_m(E_{T,2})$
C_1	–	6.3029643908	–	6.0000000048*
C_2	–	6.7239778673	–	6.0000000000*
C_3	1.0189474430	6.1016117819	1.0000000000*	6.0000000000*
C_4	1.0036966403	6.1355002205	1.0000000966*	6.0000007851*
C_6	1.0000365997*	6.0759107746	1.0000002115*	6.0000074862*
C_7	1.0042477843	6.1562385739	1.0000000000*	6.0000000000*
C_8	1.0000008631*	6.0747174816	1.0000000000*	6.0000000000*
C_9	1.0011947214	6.0432683528	1.0000000001*	6.0000000048*
C_{10}	1.0048032166	6.1771707434	1.0000000000*	6.0000000000*
C_{12}	1.0008399918	6.0303672474	1.0000000000*	6.0000000000*
$C_2 \times C_2$	1.0036975919	6.1354933081	1.0000001278*	6.0000005612*
$C_2 \times C_4$	1.0010799142	6.0384795691	1.0000000000*	6.0000000001*
$C_2 \times C_6$	1.0008421129	6.0303765948	1.0000000778*	6.0000028021*
$C_2 \times C_8$	1.0000421851	6.0206718011	1.0000000000*	6.0000000000*

Lastly, for $T = C_5$, let $H_{T,n}$ be the sequence of elliptic curves corresponding to $T = C_5$ in Theorem 4.1. Then

n	1	2	3	4	5	6
$\sigma_m(E_n)$	6.2766	6.1155	6.0730	6.0533	6.0420	6.0347

5. CLASSIFICATION OF MINIMAL DISCRIMINANTS

Let E be an elliptic curve over a number field K. Frey [37] proved that if $E(K)$ contains a point of order ℓ for ℓ a prime greater than 3, then E is semistable at all primes $\mathfrak{p}$ of K whose residue field has a characteristic different from ℓ. Flexor and Oesterlé [38] then showed that if $E(K)$ contains a point of order n and E has additive reduction at a prime $\mathfrak{p}$ of K whose residue characteristic does not divide n, then $n \leq 4$. Moreover, if E has additive reduction at at least two primes of K with different residue characteristics then n divides 12.

The proof of these results and their generalizations to abelian varieties [39] require a study of the Néron model of the abelian variety. In this chapter, we give a new effective proof of Frey's and Flexor-Oesterlé's result, but note that for Frey's result, our proof only holds for $\ell = 5, 7$. Let T be one of the fourteen non-trivial torsion subgroups allowed by Mazur's Torsion Theorem. In section one, we show that if $T \neq C_2, C_2 \times C_2$, then there are two-parameter families of elliptic curves which parameterize all elliptic curves over K with $T \hookrightarrow E(K)$. Care must be taken for $T = C_3$ by considering those rational elliptic curves E whose j-invariant is 0 and $T \hookrightarrow E(K)$ separately. For $T = C_2, C_2 \times C_2$, we must assume that K has class number one in order to parameterize elliptic curves with $T \hookrightarrow E(K)$ by a three-parameter family of elliptic curves.

In section two, we use these families of elliptic curves to give an effective proof of Frey's and Flexor-Oesterlé's result. In section three, we restrict our attention to rational elliptic curves and use the effective version of Frey-Flexor-Oesterlé to provide necessary and sufficient conditions for a given polynomial to coincide with the minimal discriminant of a rational elliptic curve with non-trivial torsion. Section 4 is devoted to the proof of the classification of minimal discriminants of rational elliptic curves with non-trivial torsion subgroup. In section 5 we build on the classification of minimal discriminants and provide necessary and sufficient conditions for when additive reduction occurs on a rational elliptic curve with non-trivial torsion. We conclude the chapter with a couple of examples.

5.1 Parameterization of Certain Elliptic Curves with non-Trivial Torsion

Let K be a number field with ring of integers R_K and let E be the elliptic curve given by the Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5.1}$$

where each $a_i \in K$. Suppose further that $P = (a, b) \in E(K)$ is a torsion point of order N. Then the admissible change of variables $x \longmapsto x - a$ and $y \longmapsto y - a$ results in a K-isomorphic elliptic curve with P translated to the origin. In particular, we may assume that $a_6 = 0$ in (5.1) and that $P = (0, 0)$.

5.1.1 Point of Order $N = 2$

First suppose $N = 2$, so that $P = -P$. By [4, III.2.3], $-P = (0, -a_3)$ and so $a_3 = 0$. The change of variables $x \longmapsto u^2x$ and $y \longmapsto u^3y + u^2sx$ with $u = (2a_1)^{-1}$ and $s = -\frac{a_1}{2}$ results in a K-isomorphic elliptic curve given by the Weierstrass model

$$y^2 = x^3 + \left(a_1^4 + 4a_1^2a_2\right)x^2 + 16a_1^4a_4x.$$

As a result, if E is an elliptic curve over K with a torsion point of order 2, we may assume that E is given by the Weierstrass model

$$E : y^2 = x^3 + a_2x^2 + a_4x$$

where each $a_i \in K$. In fact, we may assume that $a_2, a_4 \in R_K$ since the admissible change of variables $x \longmapsto u^{-2}x$ and $y \longmapsto u^{-3}y$ results in the Weierstrass model

$$y^2 = x^3 + a_2u^2x^2 + a_4u^4x.$$

Note that if $a_2^2 - 4a_4$ is a square in K, then $x^2 + a_2 x + a_4 = (x + \alpha)(x + \beta)$ for some $\alpha, \beta \in K$. In particular, we observe that E has full 2-torsion in K if and only if $a_2^2 - 4a_4$ is a square since $(-\alpha, 0)$ is a torsion point of order 2.

Lemma 5.1 *Let K be a number field with class number equal to* 1*. Let E be an elliptic curve over K with a rational torsion point P of order* 2*. Suppose further that E does not have full* 2*-torsion over K. Then E is K-isomorphic to the elliptic curve*

$$E_{C_2}(a, b, d) : y^2 = x^3 + 2ax^2 + \left(a^2 - b^2 d\right) x$$

for some $a, b, d \in R_K$ with $d \neq 1, b \neq 0$ such that $\gcd(a, b)$ *and d are squarefree.*

Proof By the above discussion, we may assume that E is given by the Weierstrass model

$$E : y^2 = x^3 + a_2 x^2 + a_4 x$$

with $a_2, a_4 \in R_K$ and $P = (0, 0)$.

Since $E[2] \not\hookrightarrow E(K)$, we have that $a_2^2 - 4a_4$ is not a square in K. Then

$$x^3 + a_2 x^2 + a_4 x = x\,(x - \theta_1)\,(x - \theta_2)$$

with $\theta_1 = a + b\sqrt{d}$ and $\theta_2 = a - b\sqrt{d}$ for some $a, b, d \in R_K$ with $d \neq 1, b \neq 0$, and d squarefree. Therefore

$$E : y^2 = x^3 + 2ax^2 + \left(a^2 - b^2 d\right) x.$$

Now suppose $\gcd(a, b) = g^2 h$ with h squarefree. Then the admissible change of variables $x \longmapsto g^2 x$ and $y \longmapsto g^3 y$ results in the K-isomorphic elliptic curve

$$y^2 = x^3 + \frac{2ax^2}{g^2} + \frac{(a^2 - b^2 d)}{g^4} x.$$

In particular, we may assume that $\gcd(a, b)$ and d are squarefree, which completes the proof. ∎

Remark If we omit the condition that K has class number equal to 1, the lemma still holds with the omission that the $\gcd(a, b)$ is squarefree.

Lemma 5.2 *Let K be a number field with class number equal to 1. Let E be an elliptic curve over K with a rational torsion point P of order 2. Suppose further that E has full 2-torsion over K. Then E is K-isomorphic to the elliptic curve*

$$E_{C_2\times C_2} = E_{C_2\times C_2}(a,b,d) : y^2 = x^3 + (ad+bd)\,x^2 + abd^2$$

for some $a,b,d \in R_K - \{0\}$ such that $\gcd(a,b) = 1$ and d is squarefree.

Proof By the above discussion, we may assume that E is given by the Weierstrass model

$$E : y^2 = x^3 + a_2x^2 + a_4x$$

with $a_2, a_4 \in R_K$ and $P = (0,0)$.

Since $E[2] \hookrightarrow E(K)$,

$$\begin{aligned} x^3 + a_2x^2 + a_4x &= x\,(x+A)\,(x+B) \\ &= x^3 + (A+B)\,x + ABx \end{aligned}$$

for $A, B \in R_K - \{0\}$. Now suppose that $\gcd(A,B) = g^2d$ with d squarefree. Then the admissible change of variables $x \longmapsto g^2x$ and $y \longmapsto g^3y$ results in the K-isomorphic elliptic curve

$$y^2 = x^3 + \frac{(A+B)}{g}x + \frac{AB}{g^2}x$$

and so we may assume that $\gcd(A,B) = d$. Taking $A = ad$ and $B = bd$ gives the lemma. ∎

Remark If we omit the condition that K has class number equal to 1, the lemma still holds with the omission that $\gcd(a,b) = 1$ and d is squarefree.

5.1.2 Point of Order $N = 3$

Now suppose $N \geq 3$ and once more consider the elliptic curve E over K given by the Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x \tag{5.2}$$

with $P = (0,0)$ the point of order N.

Lemma 5.3 *Let E be given by the Weierstrass model* (5.2) *and $P = (0, 0)$ a torsion point of order N.*

(*i*) *If $N \geq 3$, then $a_3 \neq 0$ and, after a change of coordinates, we can suppose $a_4 = 0$.*

(*ii*) *If $a_3 \neq 0$ and $a_4 = 0$, then P is of order* 3 *if and only if $a_2 = 0$.*

Proof See [40, Lemma 1.1]. ∎

Corollary 5.4 *Let E be an elliptic curve over K with a rational torsion point of order* 3*. If the j-invariant of E is non-zero, then E is K-isomorphic to the elliptic curve*

$$\mathcal{X}_t(C_3) : y^2 + xy + ty = x^3$$

for some $t \in K^*$.

Proof By Lemma 5.3, we may assume that E is given by the Weierstrass model

$$E : y^2 + a_1 xy + a_3 y = x^3.$$

The invariant $c_4 = a_1 \left(a_1^3 - 24a_3\right)$. Since the j-invariant of E is 0 if and only if $c_4 = 0$, we may assume that $a_1 \neq 0$ and $a_1^3 - 24a_3 \neq 0$.

Since $a_1 \neq 0$, the admissible change of variables $x \longmapsto a_1^2 x$ and $y \longmapsto a_1^3 y$ results in the K-isomorphic elliptic curve

$$y^2 + xy + \frac{a_3}{a_1^3} y = x^3$$

and so we may take $t = \frac{a_3}{a_1^3}$ which completes the proof. ∎

5.1.3 Point of Order $N \geq 4$ and Modular Curves

Lemma 5.5 (Tate Normal Form) *Let E be an elliptic curve over K with a rational torsion point of order $N \geq 4$. Then every K-isomorphism class of pairs (E, P) with E an elliptic curve over K and $P \in E(K)$ a torsion point of order n contains a unique model of the form*

$$y^2 + (1 - g)\, xy - fy = x^3 - fx^2 \tag{5.3}$$

with $f, g \in K^{\times}$, $g \in K$.

Proof See [40, Proposition 1.3]. ■

By the proof of the above lemma, we observe that the model is indeed independent of the characteristic of K. Now let $T = C_N$ where $N = 4, \ldots, 10, 12$. For these T, we defined the elliptic curve $\mathcal{X}_t(T)$ in Table 2.1 and its Weierstrass model is (5.3) with f and g as in the lemma. Now assume further that $T = C_N$ as above or $T = C_2 \times C_{2M}$ where $M = 2, 3, 4$. We now restate the result given in the introduction.

Proposition 5.6 *Let E be an elliptic curve over K with $T \hookrightarrow E(K)$. Then there is a $t \in K$ such that E is K-isomorphic to $\mathcal{X}_t(T)$.*

5.1.4 The Elliptic Curves $E_T(a,b)$ and $E_T(a,b,d)$

Let T be one of the fourteen non-trivial torsion subgroups allowed by Theorem 2.1 and let E_T be the elliptic curve defined in Table D.1. Then for $T = C_2, C_2 \times C_2$, $E_T = E_T(a,b,d)$ is the three parameter family of elliptic curves which was the subject of Lemmas 5.1 and 5.2. For $T \neq C_2, C_2 \times C_2$, we show that $E_T = E_T(a,b)$ is K-isomorphic to $\mathcal{X}_{b/a}(T)$. For the following lemma, let α_T, β_T, and γ_T be as defined in Tables D.2, D.3, and D.4, respectively.

Lemma 5.7 *For $T \neq C_2, C_2 \times C_2$, the elliptic curves $\mathcal{X}_{b/a}(T)$ and E_T are K-isomorphic for coprime elements $a, b \in R_K$. Moreover, the discriminant of E_T is γ_T and the invariants c_4 and c_6 of E_T are α_T and β_T, respectively.*

Proof Let

$$u_T = \begin{cases} a & \text{if } T = C_3, C_4, C_5, C_6, C_2 \times C_4 \\ a^2 & \text{if } T = C_7 \\ ab & \text{if } T = C_8 \\ a^3 & \text{if } T = C_9 \\ a\left(a^2 - 3ab + b^2\right) & \text{if } T = C_{10} \\ a\left(-a+b\right)^3 & \text{if } T = C_{12} \\ -9a^2 + b^2 & \text{if } T = C_2 \times C_6 \\ 2b\left(a+4b\right)\left(-a^2+8b^2\right) & \text{if } T = C_2 \times C_8. \end{cases}$$

Then the admissible change of variables $x \longmapsto u_T^{-2}x$ and $y \longmapsto u_T^{-3}y$ gives a K-isomorphism from $\mathcal{X}_{b/a}(T)$ onto $E_T = E_T(a,b)$. It is now verified via the formulas in (2.2) that the discriminant of E_T is γ_T and that the invariants c_4 and c_6 of E_T are α_T and β_T, respectively. ■

5.2 Explicit Flexor-Frey-Oesterlé

We begin by formally stating the results of Frey and Flexor-Oesterlé.

Theorem 5.8 (Frey, [37]) *Let E be an elliptic curve over K. If $E(K)$ contains a point of prime order $\ell > 3$, then E is semistable at all primes $\mathfrak{p}$ of K whose residue characteristic is different from ℓ.*

Theorem 5.9 (Flexor-Oesterlé, [38]) *Let E be an elliptic curve over K. If $E(K)$ contains a point of order N and E has additive reduction at a prime $\mathfrak{p}$ of K whose residue characteristic does not divide N, then $N \leq 4$. Moreover, if E has additive reduction at at least two primes of K with different residue characteristics then N divides 12.*

Now let E_T be as defined in the previous section. In the previous section, we saw that these families of elliptic curves parameterize all elliptic curves over K with

$T \hookrightarrow E(K)$ where T is one of the fourteen non-trivial torsion subgroups allowed by Theorem 2.1. Moreover, the discriminant of E_T is given by γ_T and the invariants c_4 and c_6 are α_T and β_T, respectively. In the following lemma, we consider $\alpha_T, \beta_T, \gamma_T$ as polynomials in $S = \mathbb{Z}[a, b, d, r, s]$.

Lemma 5.10 *Let $\alpha_T, \beta_T, \gamma_T$ be as given in Tables D.2, D.3, and D.4, respectively. For $j = 1, 2, 3$, let $\mu_T^{(j)}, \nu_T^{(j)}$ be as defined in Tables D.5 through D.10. Then for each T, the identity $\alpha_T^3 - \beta_T^2 = 1728\gamma_T$ holds in S and we have the additional identities in S:*

$\mu_T^{(1)}\alpha_T + \nu_T^{(1)}\beta_T$	$\mu_T^{(2)}\alpha_T + \nu_T^{(2)}\gamma_T$	$\mu_T^{(3)}\beta_T + \nu_T^{(3)}\gamma_T$	T
$2^8 3^2 (rb^4d^2 + sa^3)$	$2^{10} (rb^6d^3 + sa^6)$	$2^{12} (rb^8d^4 + sa^7)$	C_2
$2^6 3^3 a^3 (ra^3 + sb^3)$	$2^{15} 3^6 a^3 (ra^9 + sb^9)$	$2^6 3^9 a^4 (ra^9 + sb^9)$	C_3
$2^8 3^2 a^2 (ra^5 + sb^5)$	$2^{12} a^2 (ra^{12} + sb^{11})$	$2^{18} a^3 (ra^{11} + sb^{11})$	C_4
$2^4 3^2 5 (ra^9 + sb^9)$	$5 (ra^{15} + sb^{15})$	$5^3 (ra^{17} + sb^{17})$	C_5
$2^7 3^4 (ra^9 + sb^9)$	$2^4 3^4 (ra^{15} + sb^5)$	$2^9 3^3 (ra^{17} + sb^{17})$	C_6
$2^4 3^2 7 (ra^{19} + sb^{19})$	$7^2 (ra^{31} + sb^{31})$	$7 (ra^{35} + sb^{35})$	C_7
$2^7 3^2 (ra^{18} + sb^{19})$	$2^4 (ra^{30} + sb^{31})$	$2^9 (ra^{34} + sb^{35})$	C_8
$2^4 3^4 (ra^{29} + sb^{29})$	$3^4 (ra^{47} + sb^{47})$	$3^3 (ra^{53} + sb^{53})$	C_9
$2^7 3^2 5 (ra^{29} + sb^{29})$	$2^4 5 (ra^{47} + sb^{47})$	$2^8 5 (ra^{53} + sb^{47})$	C_{10}
$2^7 3^4 (ra^{38} + sb^{39})$	$2^4 3^4 (ra^{62} + sb^{63})$	$2^9 3^3 (ra^{70} + sb^{71})$	C_{12}
$2^5 3^2 d^4 (ra^4 + sb^4)$	$2^4 d^6 (ra^6 + sb^6)$	$2^7 d^8 (ra^8 + sb^8)$	$C_2 \times C_2$
$2^{14} 3^2 (ra^8 + sb^8)$	$2^{16} (ra^{14} + sb^{12})$	$2^{24}(ra^{16} + sb^{16})$	$C_2 \times C_4$
$2^{31} 3^4 (ra^{18} + sb^{19})$	$2^{45} 3^4 (ra^{30} + sb^{31})$	$2^{56} 3^3 (ra^{34} + sb^{35})$	$C_2 \times C_6$
$2^{49} 3^2 (ra^{38} + sb^{38})$	$2^{74} (ra^{62} + sb^{62})$	$2^{90} (ra^{70} + sb^{70})$	$C_2 \times C_8$

In particular, for $T \neq C_2, C_2 \times C_2$ suppose K is a number field with ring of integers R_K and $a, b \in R_K$ such that the principal ideals generated by a and b are coprime.

Then the ideal $(\alpha_T(a,b)+\beta_T(a,b)) \subset \gamma R_K$ *and the ideals* $(\alpha_T(a,b))+(\Delta_T(a,b))$ *and* $(\beta_T(a,b)+\gamma_T(a,b))$ *are contained in the principal ideal* δR_K *where* γ *and* δ *are:*

T	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{12}	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
γ	$6a$	$6a$	30	6	42	6	6	10	6	2	6	2
δ	$6a$	$2a$	5	6	7	2	3	10	6	2	6	2

Proof The identities can be checked with a computer algebra system. For the second statement, note that since the ideals generated by a and b are coprime, it follows that the ideals generated by a^n and b^m are coprime for any positive integers n and m. In particular, there exist $r, s \in R_K$ such that $ra^n + sb^m = 1$ and thus the second claim now follows. ∎

Theorem 5.11 *Let* E *be an elliptic curve over a number field* K *with ring of integers* R_K*. Suppose further that the* j*-invariant of* E *is not* 0 *or* 1728 *and that* $T \hookrightarrow E(K)$ *for one of the* T *in the previous lemma. If* E *has additive reduction at a prime* $\mathfrak{p}$ *of* K*, then the residue characteristic of* $\mathbb{F}_\mathfrak{p} = R_K/\mathfrak{p}$ *is one of the following elements of the set of primes* S*:*

T	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}
S	$\{2,3\} \cup S_a$	$\{2\} \cup S_a$	$\{5\}$	$\{2,3\}$	$\{7\}$	$\{2\}$	$\{3\}$	$\{5\}$

T	C_{12}	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
S	$\{2,3\}$	$\{2\}$	$\{2,3\}$	$\{2\}$

where $S_a = \{p \text{ a prime} \mid p \text{ divides } |R_K/aR_K|\}$ *for some* $a \in R_K$*.*

Proof Let E be an elliptic curve with $T \hookrightarrow E(K)$ and assume that E has additive reduction at a prime $\mathfrak{p}$ of K. By Lemma 5.7, there are coprime elements $a, b \in R_K$ such that E is K-isomorphic to $E_T = E_T(a,b)$. Now let $x \longmapsto u_\mathfrak{p}^2 x + r_\mathfrak{p}$ and $y \longmapsto u_\mathfrak{p}^3 y + s_\mathfrak{p} u_\mathfrak{p}^2 x + t_\mathfrak{p}$ be an admissible change of variables resulting in a minimal equation for E_T at $\mathfrak{p}$. Since E_T is given by an integral Weierstrass model, we have that $u_\mathfrak{p}, s_\mathfrak{p}, r_\mathfrak{p}, t_\mathfrak{p} \in R_{K_\mathfrak{p}}$ by Lemma 2.4 where $R_{K_\mathfrak{p}}$ denotes the ring of integers of $K_\mathfrak{p}$.

Let $\Delta_{\mathfrak{p}}$ denote the minimal discriminant with respect to $\mathfrak{p}$ and let $c_{4,\mathfrak{p}}$ and $c_{6,\mathfrak{p}}$ be the associated invariants so that $1728\Delta_{\mathfrak{p}} = c_{4,\mathfrak{p}}^3 - c_{6,\mathfrak{p}}^2$. Moreover, $\Delta_{\mathfrak{p}} = u_{\mathfrak{p}}^{-12}\gamma_T$ and $c_{4,\mathfrak{p}} = u_{\mathfrak{p}}^{-4}\alpha_T$ are both in $R_{K_{\mathfrak{p}}}$ and by Lemma 5.10, $c_{4,\mathfrak{p}}R_{K_{\mathfrak{p}}} + \Delta_{\mathfrak{p}}R_{K_{\mathfrak{p}}} \subset \alpha_T(a,b)\,R_{K_{\mathfrak{p}}} + \gamma_T(a,b)\,R_{K_{\mathfrak{p}}} \subset \delta R_{K_{\mathfrak{p}}}$ where δ is as in Lemma 5.10. Since E has additive reduction at $\mathfrak{p}$, we have that $v_{\mathfrak{p}}(\Delta_{\mathfrak{p}})\,, v(c_{4,\mathfrak{p}}) > 0$ and therefore $v_{\mathfrak{p}}(\delta) > 0$. In particular, the residue characteristic of $v_{\mathfrak{p}}$ divides δ. This shows all cases claimed except for $T = C_{10}$. Note that if $C_{10} \hookrightarrow E(K)$, then $C_5 \hookrightarrow E(K)$. Therefore $E_{C_{10}}(a,b)$ is K-isomorphic to $E_{C_5}(a',b')$ for two coprime elements $a',b' \in R_K$. In particular, if $E_{C_{10}}$ has additive reduction at a prime $\mathfrak{p}$, it follows that the residue characteristic of $\mathfrak{p}$ is 5. ■

This is Frey's result in the case when $\ell = 5, 7$. To attain Flexor-Oesterlé's result, observe that only for $T = C_3,\ C_4,\ C_6,\ C_{12}$, and $C_2 \times C_6$ is additive reduction possible at two or more distinct valuations with different residue characteristic.

Proof [Proof of Flexor-Oesterlé]Let E be an elliptic curve over K with a rational torsion point of order N. First suppose E has additive reduction at a prime $\mathfrak{p}$ of K whose residue characteristic does not divide N. If ℓ divides N for $\ell > 3$ a prime, we have by Frey's Theorem that the residue characteristic of $\mathfrak{p}$ must divide N. If 6, 8, or 9 divides N, then the residue characteristic of $\mathfrak{p}$ must divide N by Theorem 5.11. Therefore $N \leq 4$ since the only primes dividing N are 2 and 3.

Next, suppose E has additive reduction at at least two primes of K with different residue characteristics. By Frey's Theorem, the only primes dividing N are 2 and 3. By Theorem 5.11, 8 nor 9 divide N and so $N = 1, 2, 3, 4, 6, 12$. ■

5.3 Classification of Minimal Discriminants

In this section, we restrict our attention to rational elliptic curves. As before, let T be one of the fourteen non-trivial torsion subgroups allowed by Theorem 2.1 and let E_T be as given in Table D.1. Then if E is a rational elliptic curve with $T \hookrightarrow E(\mathbb{Q})$ where $T \neq C_2, C_2 \times C_2$, we have that there are relatively prime integers a and b such that E is $\mathbb{Q}$-isomorphic to $E_T = E_T(a,b)$. If $T = C_2$ and E does not have full

2-torsion, then E is $\mathbb{Q}$-isomorphic to $E_T = E_T(a, b, d)$ with $\gcd(a, b)$ and d squarefree integers. For $T = C_2 \times C_2$, E is $\mathbb{Q}$-isomorphic to $E_T = E_T(a, b, d)$ with a and b relatively prime and d squarefree. However, we can assume in this case that a is even as demonstrated in the following lemma.

Lemma 5.12 *Let $T = C_2 \times C_2$ and suppose $T \hookrightarrow E(\mathbb{Q})$. Then there are integers a, b, d with a and b relatively prime, a even, and d a positive squarefree integer.*

Proof By Lemma 5.2, E is $\mathbb{Q}$-isomorphic to

$$E_T : y^2 = x^3 + (ad + bd)\, x^2 + abd^2$$

where a, b, d are integers such that a and b are relatively prime and d is a squarefree integer. By the proof of Lemma 5.2, d may be assumed to be positive. It remains to show that a may be assumed to be even. Observe that if b were even, then we can interchange a and b. So suppose a and b are odd. Then $c = b - a$ is even and the admissible change of variables $x \longmapsto x - ad$ gives a $\mathbb{Q}$-isomorphism from E_T onto the elliptic curve given by the Weierstrass model

$$y^2 = x^3 + (cd - ad)\, x^2 - acd^2 x.$$

This shows that we may assume a to be even. ■

Lemma 5.13 *For $T \neq C_2, C_2 \times C_2$, we have that $E_T(-a, b)$ is $\mathbb{Q}$-isomorphic to $E_T(a, -b)$.*

Proof Let E and E' be rational elliptic curves. Suppose further than the invariants c_4 and c_6 of their Weierstrass model coincide. Then E and E' are $\mathbb{Q}$-isomorphic since they are both $\mathbb{Q}$-isomorphic to the elliptic curve

$$y^2 = x^3 - 27c_4 x - 54c_6.$$

In particular, the invariants c_4 and c_6 of a Weierstrass model determine an elliptic curve up to $\mathbb{Q}$-isomorphism.

Since $\alpha_T(a,b)$ and $\beta_T(a,b)$ are the invariants c_4 and c_6 of the Weierstrass model of $E_T(a,b)$, it suffices to verify by the remark above that the following equalities hold:

$$\alpha_T(-a,b)=\alpha_T(a,-b) \qquad \text{and} \qquad \beta_T(-a,b)=\beta_T(a,-b)\,.$$

This is easily checked via a computer algebra system such as Mathematica [30]. ■

Remark Henceforth, we will assume that a is even in the Weierstrass model of E_T for $T = C_2 \times C_2$. Similarly, we will assume that a is positive in the Weierstrass model of E_T for $T \neq C_2, C_2 \times C_2$.

We now state the main theorem of this section.

Theorem 5.14 *The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is one of the possibilities below*

T	C_2	C_3	C_4	C_5	C_6	C_7	C_8
u_T	$1, 2,$ *or* 4	c^2d	c *or* $2c$	1	1 *or* 2	1	1 *or* 2

T	C_9	C_{10}	C_{12}	$C_2 \times C_2$	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
u_T	1	1 *or* 2	1 *or* 2	1 *or* 2	$1, 2,$ *or* 4	$1, 4,$ *or* 16	$1, 16,$ *or* 64

where

$$a=\begin{cases} c^3d^2e \text{ with } d \text{ and } e \text{ squarefree and } \gcd(d,e)=1 & \text{if } T=C_3 \\ c^2d \text{ with } d \text{ squarefree} & \text{if } T=C_4. \end{cases} \tag{5.4}$$

Moreover, there are necessary and sufficient conditions on a, b, d to determine exactly the value of u_T. Table 5.1 summarizes these necessary and sufficient conditions.

Table 5.1.: Necessary and Sufficient Conditions on u_T

T	Conditions on u_T
C_2	$u_T = 4 \iff v_2(b^2d - a^2) \geq 8$ *with* $v_2(a) = v_2(b) = 1$ *and* $2^{-1}a \equiv 1 \mod 4$. $u_T = 2 \iff$ *either (i)* $u_T \neq 4$, $v_2(b^2d - a^2) \geq 4$ *with* $v_2(a) = v_2(b) = 1$ *and* $d \equiv 1 \mod 4$, *(ii)* $v_2(b) \geq 3$ *and* $a \equiv -1 \mod 4$, *or (iii)* $a = 3b$ *with* b *a squarefree even integer not divisible by* 3. $u_T = 1 \iff$ *The previous conditions are not satisfied.*
C_4	$u_T = 2c \iff v_2(a) \geq 8$ *is even with* $bd \equiv 3 \mod 4$ $u_T = c \iff$ *The previous condition is not satisfied.*
C_6	$u_T = 1 \iff v_2(a+b) < 3$ $u_T = 2 \iff v_2(a+b) \geq 3$
C_8	$u_T = 1 \iff v_2(a) \neq 1$ $u_T = 2 \iff v_2(a) = 1$
C_{10}	$u_T = 1 \iff a$ *is odd.* $u_T = 2 \iff a$ *is even.*
C_{12}	$u_T = 1 \iff a$ *is odd.* $u_T = 2 \iff a$ *is even.*
$C_2 \times C_2$	$u_T = 2 \iff v_2(a) \geq 4$ *and* $bd \equiv 1 \mod 4$. $u_T = 1 \iff$ *The previous condition is not satisfied.*
$C_2 \times C_4$	$u_T = 1 \iff v_2(a) \leq 1$ $u_T = 2 \iff v_2(a) \geq 2$ *and* $v_2(a+4b) < 4$ $u_T = 4 \iff v_2(a) = 2$ *and* $v_2(a+4b) \geq 4$.
$C_2 \times C_6$	$u_T = 1 \iff v_2(a+b) = 0$ $u_T = 4 \iff v_2(a+b) \geq 2$ $u_T = 16 \iff v_2(a+b) = 1$

continued on next page

Table 5.1.: continued

T	*Conditions on u_T*
$C_2 \times C_8$	$u_T = 1 \iff a$ *is odd.*
	$u_T = 16 \iff v_2(a) = 1$
	$u_T = 64 \iff v_2(a) \geq 2$

In Theorem 5.11, we considered elliptic curves whose j-invariant was not 0 or 1728. Consequently, in order to prove Theorem 5.14 as stated we need knowledge of when E_T has j-invariant 0 or 1728. Below we prove a series of easy lemmas which will allow us to distinguish those E_T's whose j-invariant is 0 or 1728.

Lemma 5.15 *Let E be a rational elliptic curve with a rational torsion point of order $N \geq 4$. If E has j-invariant 0, then E is $\mathbb{Q}$-isomorphic to $E_{C_6}(3, -1)$. If E has j-invariant 1728, then E is $\mathbb{Q}$-isomorphic to $E_{C_4}(8, -1)$.*

Proof From (2.2) it is checked that $j = 0$ if and only if $c_4 = 0$. Similarly, $j = 1728$ if and only if $c_6 = 0$. By Proposition 5.6 and Lemma 5.7, E is $\mathbb{Q}$-isomorphic to E_T for some T. We now consider the cases when $j = 0$ and $j = 1728$.

Case I. Suppose $j = 0$. Then the invariant c_4 of E is 0. In particular, it suffices to check when there are integer solutions to the equations $\alpha_T = 0$. By inspection, this only occurs for $T = C_6$ with $a = 3$ and $b = -1$ since we assuming a to be even by Remark 5.3.

Case II. Suppose $j = 1728$. Then the invariant c_6 of E is 0. In particular, it suffices to check when there are integer solutions to the equations $\beta_T = 0$. By inspection, this only occurs for $T = C_4$ with $a = 8$ and $b = -1$ since we assuming a to be even by Remark 5.3. ■

Lemma 5.16 *Let E be a rational elliptic curve with a rational torsion point of order $N = 3$. Then the j-invariant of E is not equal to 1728. Moreover, if the j-invariant of E is 0, then E is $\mathbb{Q}$-isomorphic to either $E_{C_3}(24, 1)$ or*

$$E_{C_3^0}(a) : y^2 + ax = x^3$$

for some cubefree integer a.

Proof By Lemma 5.3, we may assume that E is given by the Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3$$

for some integers a_1 and a_2. Then $c_4 = a_1\left(a_1^3 - 24a_3\right)$ and $c_6 = -a_1^6 + 36a_1^3a_3 - 216a_2^2$. By inspection, $c_6 = 0$ does not have any real solutions and therefore there is no elliptic curve E with a torsion point of order 3 which has j-invariant 1728.

Next, the j-invariant of E is 0 if and only if $c_4 = 0$. In particular, either $a_1 = 0$ or $a_1^3 - 24a_3 = 0$. We consider each of these cases separately.

Case I. Suppose $a_1 \neq 0$. Then E is $\mathbb{Q}$-isomorphic to $E_T(a, b)$ for some relatively prime integers a and b by Corollary 5.4. But then $\alpha_T = a^3\left(a - 24b\right) = 0$. Consequently, $a - 24b = 0$ and so $a = 24b$. Since a and b are relatively prime, we conclude that E is $\mathbb{Q}$-isomorphic to $E_{C_3}(24, 1)$.

Case II. Suppose $a_1 = 0$. Then

$$E : y^2 + a_3x = x^3.$$

We claim that E is $\mathbb{Q}$-isomorphic to $E_{C_3^0}(a)$ where a is the cubefree part of a_3. Indeed, write $a_3 = c^3a$ with a and c positive integers such that a is cubefree. Then the admissible change of variables $x \longmapsto a^2x$ and $y \longmapsto a^3y$ gives a $\mathbb{Q}$-isomorphism from E onto

$$E_{C_3^0}(a) : y^2 + ax = x^3,$$

which concludes the proof. ∎

Corollary 5.17 *For a cubefree integer a, $E_{C_3^0} = E_{C_3^0}(a)$ is a global minimal model for $E_{C_3^0}$. Moreover, $E_{C_3^0}$ has additive reduction at each prime dividing the discriminant.*

Proof Let Δ denote the discriminant of $E_{C_3^0}$ and c_6 the invariant associated to the Weierstrass model of $E_{C_3^0}$. Then

$$\Delta = -3^3a^4 \qquad \text{and} \qquad c_6 = 2^33^3a^2.$$

Observe that for p a prime, $v_p(\Delta) \leq 11$ since a is cubefree. In particular, $E_{C_3^0}$ is a global minimal model for $E_{C_3^0}$. It now follows that $E_{C_3^0}$ has additive reduction at each prime dividing the discriminant. ■

Lemma 5.18 *Let $T = C_2$. Then*

(i) If E_T has j-invariant 0, then it is $\mathbb{Q}$-isomorphic to $E_T(3b, b, -3)$ for b a squarefree integer not divisible by 3.

(ii) If E_T has j-invariant 1728, then it is $\mathbb{Q}$-isomorphic to $E_T(0, b, d)$ for squarefree integers b and d.

Proof (*i*) If E_T has j-invariant 0, then $\alpha_T = 0$. In particular,

$$\alpha_T = 16\left(3b^2d + a^2\right) = 0 \qquad \Longrightarrow \qquad a^2 = -3b^2d.$$

Since $\gcd(a, b)$ and d are squarefree, it follows that $d = -3$ and $a = 3b$ with b a squarefree integer not divisible by 3.

(*ii*) If E_T has j-invariant 1728, then

$$\beta_T = -64a\left(9b^2d - a^2\right) = 0 \qquad \Longrightarrow \qquad a = 0 \text{ or } a^2 = 9b^2d.$$

Since $d \neq 1$, it follows that the latter cannot occur. Consequently, $a = 0$. Now suppose $b = \hat{b}^2 e$ for e a squarefree integer. Then the admissible change of variables $x \longmapsto \hat{b}x$ and $y \longmapsto \hat{b}^3 y$ gives a $\mathbb{Q}$-isomorphism from E_T onto

$$E_T' : y^2 = x^3 - e^2dx.$$

In particular, we may assume b is a squarefree integer which concludes the proof. ■

Lemma 5.19 *Let $T = C_2 \times C_2$. Then the j-invariant of E_T is nonzero. Moreover, if E_T has j-invariant 1728, then E_T is $\mathbb{Q}$-isomorphic to $E_T(2, 1, d)$ for some squarefree integer d.*

Proof Towards a contradiction, suppose the j-invariant of E_T is 0. Then

$$\alpha_T = 16d^2\left(a^2 - ab + b^2\right) = 0.$$

But this is a contradiction since $a^2 - ab + b^2 \neq 0$ for integers a and b.

Next, suppose the j-invariant of E_T is 1728. Then

$$\beta_T = -32\,(a+b)\,(a-2b)\,(2a-b) = 0$$

Since a and b are relatively and a is assumed to be even by Lemma 5.12, we have that $\beta_T = 0$ if and only if $a = \pm 2$ and $b = \pm 1$. The admissible change of variables $x \longmapsto x - 2d$ gives a $\mathbb{Q}$-isomorphism from $E_T(2,1,d)$ onto $E_T(-2,-1,d)$, which concludes the proof. ∎

5.4 Proof of Theorem 5.14

The proof will rely on extensive use of Kraus's Theorem which we recall below:

Lemma 2.6 Let α, β, and γ be integers such that $\alpha^3 - \beta^2 = 1728\gamma$ with $\gamma \neq 0$. Then there exists a rational elliptic curve E given by an integral Weierstrass equation having invariants $c_4 = \alpha$ and $c_6 = \beta$ if and only if the following conditions hold:

(i) $v_3(\beta) \neq 2$;

(ii) either $\beta \equiv -1 \mod 4$ or both $v_2(\alpha) \geq 4$ and $\beta \equiv 0$ or $8 \mod 32$.

The following corollary is automatic by Lemma 2.4 and the definition of an integral Weierstrass model.

Corollary 5.20 *Let E be a rational elliptic curve which is given by an integral Weierstrass model. Let c_4 and c_6 be the invariants associated to this model. If $x \longmapsto u^2x + r$ and $y \longmapsto u^3 + u^2sx + w$ is an admissible change of variables between E and a global minimal model of E, then $\alpha = u^{-4} \cdot c_4$ and $\beta = u^{-6} \cdot c_6$ satisfy the conditions of Theorem 2.6.*

Lemma 5.21 *Let α, β, and γ be integers such that $\alpha^3 - \beta^2 = 1728\gamma$ with $\gamma \neq 0$. If $v_2(\alpha_T) = 4k$ for some integer k and $v_2(\gamma_T) \geq 12k$, then $v_2(\beta_T) = 6k$.*

Proof The assumption implies that 2^{12k} divides α^3 and γ. Then 2^{12k} divides β^2 since $\alpha^3 - 1728\gamma = \beta^2$. Since $2^{-12k} \cdot \alpha^3$ is odd and $2^{-12k} \cdot 1728\gamma$ is even, it follows that $2^{-12k} \cdot \beta^2$ is odd. Therefore $v_2(\beta_T) = 6k$. ∎

Remark By Lemma 5.15, the j-invariant of E_T is not equal to 0 or 1728 for $T \neq C_2, C_3, C_4, C_6$, and $C_2 \times C_2$. Consequently, for these T, we will implicitly assume in the proof of Theorem 5.14 that the j-invariant of E_T is not 0 or 1728.

5.4.1 Proof of Theorem 5.14 for $T = C_5, C_7, C_9$.

Theorem 5.14 for $T = C_5, C_7, C_9$. For $T = C_5, C_7, C_9$, the minimal discriminant of E_T is γ_T.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6 | \beta_T$ and $u_T^{12} | \gamma_T$. In particular, u_T^6 divides $\gcd(\beta_T, \gamma_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\beta_T, \gamma_T)$ divides d_T where

$$d_T = \begin{cases} 5^3 & \text{if } T = C_5 \\ 7 & \text{if } T = C_7 \\ 3^3 & \text{if } T = C_9. \end{cases}$$

In particular, $u_T = 1$ which shows that E_T is a global minimal model for E_T. ∎

5.4.2 Proof of Theorem 5.14 for $T = C_2$

Theorem 5.14 for $T = C_2$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2, 4\}$. Moreover,

(*i*) $u_T = 4 \Longleftrightarrow v_2\left(b^2 d - a^2\right) \geq 8$ with $v_2(a) = v_2(b) = 1$ and $2^{-1}a \equiv 1 \mod 4$.

(ii) either (1) $u_T = 2 \iff u_T \neq 4$, $v_2\left(b^2d - a^2\right) \geq 4$ with $v_2(a) = v_2(b) = 1$ and $d \equiv 1 \mod 4$, (2) $v_2(b) \geq 3$ and $a \equiv -1 \mod 4$, or (3) $a = 3b$ with b a squarefree even integer not divisible by 3.

Otherwise $u_T = 1$.

Proof Recall that the discriminant of E_T is γ_T and the invariants c_4 and c_6 of E_T are α_T and β_T where

$$\alpha_T = 16\left(3b^2d + a^2\right) \qquad \beta_T = -64a\left(9b^2d - a^2\right) \qquad \gamma_T = 64b^2d\left(b^2d - a^2\right)^2.$$

By assumption, a, b, d are integers with $d \neq 1, b \neq 0$ such that $\gcd(a, b)$ and d are squarefree.

First, suppose the j-invariant of E_T is 0. By Lemma 5.18 E_T is $\mathbb{Q}$-isomorphic to $E_T(3b, b, -3)$ for b a squarefree integer not divisible by 3. Then

$$\beta_T = 2^8 3^3 b^3 \qquad \text{and} \qquad \gamma_T = 2^{10} 3^3 b^6.$$

In particular, if b is odd, then $v_p(\gamma_T) < 12$ for all primes p and therefore γ_T is the minimal discriminant of E_T. Now suppose $b = 2\hat{b}$ for some odd squarefree integer $\hat{b}$. The admissible change of variables $x \longmapsto 4x$ and $y \longmapsto 8y$ gives a $\mathbb{Q}$-isomorphism from E_T onto

$$E_T' : y^2 = x^3 + 3\hat{b}x^2 3 + \hat{b}^2 x.$$

Note that the discriminant of E_T' is $u_T^{-12}\gamma_T = 2^4 3^3 \hat{b}^6$ with $u_T = 2$. In particular, $v_p\left(u_T^{-12}\gamma_T\right) < 12$ for each prime p. Thus $u_T^{-12}\gamma_T$ is the minimal discriminant of E_T.

Next, suppose the j-invariant of E_T is 1728. By Lemma 5.18 E_T is $\mathbb{Q}$-isomorphic to $E_T(0, b, d)$ for squarefree integers b and d. Then

$$\alpha_T = 2^4 3 b^2 d \qquad \text{and} \qquad \gamma_T = 2^6 b^6 d^3.$$

In particular, $v_p(\gamma_T) \leq 9$ for each odd prime p and $v_2(\gamma_T) \leq 15$. Now let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$. Then u_T divides 2 since $v_2(\gamma_T) \leq 15$. Towards a contradiction, suppose $u_T = 2$. Then b is even since $v_2(\gamma_T) \geq 12$ if and only if b is even. Write $b = 2\hat{b}$ for $\hat{b}$ an odd squarefree integer. Then

$$u_T^{-4}\alpha_T = 12\hat{b}^2 d \qquad \text{and} \qquad u_T^{-12}\gamma_T = \hat{b}^6 d^3.$$

Since $u_T^{-6}\beta_T = 0$ and $v_2\big(u_T^{-4}\alpha_T\big) \leq 3$, we have by Theorem 2.6 there is no integral Weierstrass model having invariants $c_4 = u_T^{-4}\alpha_T$ and $c_6 = 0$. This contradicts the assumption that $u_T^{-12}\gamma_T$ is the minimal discriminant of E_T.

Next, suppose the j-invariant of E_T is not equal to 0 or 1728. Let $\gcd(a,b) = mn$ such that $\gcd(a,d) = ml$ and $\gcd(b,l) = 1$. In particular, m, n, l are squarefree relatively prime positive integers. Hence

$$a = mnl\tilde{a}, \qquad b = mn\tilde{b}, \text{ and } \qquad d = ml\tilde{d}$$

for some integers $\tilde{a}, \tilde{b}$, and $\tilde{d}$. Then by Lemma 5.10,

$$\begin{array}{lll} \gcd(\alpha_T, \beta_T) & \text{divides} & 2^8 3^2 \gcd(b^4 d^2, a^3) = 2^8 3^2 m^3 n^3 l^2, \\ \gcd(\alpha_T, \gamma_T) & \text{divides} & 2^{10} \gcd(b^6 d^3, a^6) = 2^{10} m^6 n^6 l^3, \\ \gcd(\beta_T, \gamma_T) & \text{divides} & 2^{12} \gcd(b^8 d^4, a^7) = 2^{12} m^7 n^7 l^4. \end{array} \tag{5.5}$$

Next let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^4 | \alpha_T$, $u_T^6 | \beta_T$, and $u_T^{12} | \gamma_T$. We claim that u_T is 1, 2, or 4. To this end, suppose p is an odd prime dividing u_T. If $p > 3$, then u_T^4 divides $m^3 n^3 l^2$ by (5.5). But m, n, l are relatively prime which contradicts the assumption that p^4 divides $m^3 n^3 l^2$. So suppose $p = 3$. By (5.5) we observe that 3 does not divide l since this would imply that 3^4 does not divide $\gcd(\alpha_T, \gamma_T)$. We may therefore assume that 3 divides either m or n.

Case I. Suppose 3 divides u_T and m. Write $a = 3\hat{a}$, $b = 3\hat{b}$,and $d = 3\hat{d}$ for some integers $\hat{a}, \hat{b}, \hat{d}$ with 3 dividing at most one of $\hat{a}$ and $\hat{b}$. In particular,

$$4 \leq v_3(\alpha_T) = v_3\left(9\hat{a}^2 + 81\hat{b}^2\hat{d}\right) = 2 + v_3\left(\hat{a}^2 + 9\hat{b}^2\hat{d}\right)$$

Note that the inequality only holds if $v_3(\hat{a}) > 0$ and so 3 does not divide $\hat{b}$. Since

$$12 \leq v_3(\gamma_T) = v_3\left(27\hat{b}^2\hat{d}\right) + 2v_3\left(27\hat{b}^2\hat{d} - 9\hat{a}^2\right)$$

and $v_3\left(27\hat{b}^2\hat{d} - 9\hat{a}^2\right) = 6$ since $v_3(\hat{a}) > 0$, we conclude that $v_3(\gamma_T) = 9$ which contradict the assumption that 3 divides u_T.

Case II. Suppose 3 divides u_T and n. Write $a = 3\hat{a}$ and $b = 3\hat{b}$ for some integers $\hat{a}$ and $\hat{b}$ with 3 dividing at most one of $\hat{a}$ and $\hat{b}$. Then

$$4 \leq v_3(\alpha_T) = v_3\left(9\hat{a}^2 + 27\hat{b}^2\hat{d}\right) = 2 + v_3\left(\hat{a}^2 + 3\hat{b}^2\hat{d}\right)$$

But this is a contradiction since $v_3\left(\hat{a}^2 + 3\hat{b}^2\hat{d}\right) \leq 1$ with equality if and only if $v_3(\hat{a}) > 0$.

Since u_T is not divisible by odd primes, we conclude that u_T divides 4 by (5.5) since u_T^4 divides $\gcd(\alpha_T, \beta_T)$ and m, n, l are squarefree.

Now suppose $u_T = 4$. Then $v_2(\alpha_T) \geq 8$ and so $v_2(3b^2d + a^2) \geq 4$. For this to occur, we must have either $3b^2d$ and a^2 are both even or are both odd.

Case I. Assume that $3b^2d$ and a^2 are both odd. Now observe that

$$\begin{aligned} 24 \leq v_2(\gamma_T) \quad &\Longrightarrow \quad 9 \leq v_2(b^2d - a^2) \\ 12 \leq v_2(\beta_T) \quad &\Longrightarrow \quad 6 \leq v_2(9b^2d - a^2) \end{aligned}$$

But $9b^2d - a^2 = b^2d - a^2 + 8b^2d \equiv 8b^2d \mod 64$. But this is a contradiction since b^2d is assumed to be odd and therefore $9b^2d - a^2 \not\equiv 0 \mod 64$.

Case II. Assume that $3b^2d$ and a^2 are both even.

Subcase I. Assume further that b is odd and d is even. Write $a = 2\hat{a}$ and $d = 2\hat{d}$ for some integers $\hat{a}$ and $\hat{d}$. Then

$$8 \leq v_2(\alpha_T) = 4 + v_2\left(6b^2\hat{d} + 4\hat{a}^2\right)$$

But then $v_2(\alpha_T) = 5$ since $b^2\hat{d}$ being odd implies that $v_2\left(3b^2\hat{d} + 2\hat{a}^2\right) = 0$. This contradicts the assumption that $u_T = 4$.

Subcase II. Assume further that b and d are both even and write $a = 2\hat{a},\ b = 2\hat{b}$, and $d = 2\hat{d}$ for some integers $\hat{a}, \hat{b}, \hat{d}$ with at most one of $\hat{a}$ and $\hat{b}$ being even. Then

$$\begin{aligned} 8 \leq v_2(\alpha_T) &= 4 + v_2\left(24\hat{b}^2\hat{d} + 4\hat{a}^2\right) \\ &= 6 + v_2\left(6\hat{b}^2\hat{d} + \hat{a}^2\right) \end{aligned}$$

But $v_2\left(6\hat{b}^2\hat{d} + \hat{a}^2\right) \leq 1$ with equality if and only if $v_2(\hat{a}) > 0$. This contradicts the assumption that $u_T = 4$.

Subcase III. Assume further that b is even and d is odd and write $a = 2\hat{a}$ and $b = 2\hat{b}$ for some integers $\hat{a}$ and $\hat{b}$ such that at most one of $\hat{a}$ and $\hat{b}$ is even. Then

$$\begin{aligned} 8 \leq v_2(\alpha_T) &= 4 + v_2\left(12\hat{b}^2 d + 4\hat{a}^2\right) \\ &= 6 + v_2\left(3\hat{b}^2 d + \hat{a}^2\right) \end{aligned}$$

Therefore $v_2\left(3\hat{b}^2 d + \hat{a}^2\right) \geq 2$ and we deduce that $\hat{a}$ and $\hat{b}$ are both odd. Next,

$$24 \leq v_2(\gamma_T) = 12 + 2v_2\left(\hat{b}^2 d - \hat{a}^2\right) \qquad \Longrightarrow \qquad 6 \leq v_2\left(\hat{b}^2 d - \hat{a}^2\right)$$

Now observe that $v_2\left(\hat{b}^2 d - \hat{a}^2\right) \geq 6 \iff v_2(b^2 d - a^2) \geq 8$ which is part of the assumption of (i). Now write $\hat{b}^2 d - \hat{a}^2 = 2^6 k$ for some integer k. Solving for $\hat{a}^2$ yields $\hat{a}^2 = \hat{b}^2 d - 2^6 k$. Since odd squares are congruent to 1 modulo 4, it follows that $d \equiv 1 \mod 4$. Then

$$v_2\left(3\hat{b}^2 d + \hat{a}^2\right) = v_2\left(4\hat{b}^2 d - 2^6 k\right) = 2$$

since $v_2\left(\hat{b}^2 d - 2^4 k\right) = 0$. Consequently, $v_2(\alpha_T) = 8$. Now observe that

$$\begin{aligned} 4^{-6}\beta_T &= -2^{-3}\hat{a}\left(9\hat{b}^2 d - \hat{a}^2\right) \\ &= -2^{-3}\hat{a}\left(8\hat{b}^2 d + 2^6 k\right) \\ &= -\hat{a}\left(\hat{b}^2 d + 2^3 k\right) \end{aligned}$$

is odd since $\hat{a}\hat{b}^2 d$ is odd. Now let c_4 and c_6 denote the invariants associated to a global minimal model of E_T. In particular, c_4 and c_6 satisfy Theorem 2.6. By construction,

$c_4 = 4^{-4}\alpha_T$ and $c_6 = 4^{-6}\beta_T$ and are both odd. Therefore $c_6 \equiv -1 \mod 4$. Since $-\hat{a}\left(\hat{b}^2 d + 2^3 k\right) \equiv -\hat{a}d \mod 4$ it follows that $c_6 \equiv -1 \mod 4$ if and only if $\hat{a} \equiv 1 \mod 4$. It remains to show that $v_3(4^{-6}\beta_T) = v_3(\beta_T) \neq 2$. Observe that

$$9b^2 d - a^2 \equiv -a^2 \mod 9. \tag{5.6}$$

If a is divisible by 3, then $a\,(9b^2 d - a^2) \equiv 0 \mod 27$. This concludes the proof of (i).

Now assume that $u_T = 2$. Observe that 2^4 and 2^6 divide α_T and β_T. The invariants c_4 and c_6 associated with a global minimal model of E_T are $2^{-4}\alpha_T$ and $2^{-6}\beta_T$, respectively. The argument preceding (5.6) shows that $v_3(c_6) \neq 2$. Therefore by Theorem 2.6, either $-c_6 \equiv -1 \mod 4$ or both $v_2(c_4) \geq 4$ and $c_6 \equiv 0$ or $8 \mod 32$. Moreover, the minimal discriminant is $2^{-12}\gamma_T$ and so we get the inequality

$$v_2\left(b^2 d\right) + 2v_2\left(b^2 d - a^2\right) \geq 6.$$

Note that $b^2 d - a^2$ is even if both $b^2 d$ and a^2 are odd or if they are both even. We now proceed by cases.

Case I. Suppose $v_2(b^2 d - a^2) \geq 3$ with $b^2 d$ and a^2 odd. Write $b^2 d - a^2 = 8k$ for some integer k and observe that

$$c_4 = 3b^2 d + a^2 = 3b^2 d - 3a^2 + 4a^2 = 24k + 4a^2.$$

Since c_6 is even, it follows by Theorem 2.6 that $v_2(c_4) \geq 4$. Reducing modulo 16 yields

$$24k + 4a^2 \equiv 4\left(2k + a^2\right) \mod 16$$

which is congruent to 0 modulo 16 if and only if k and a are even, which contradicts the assumptions.

Case II. Suppose $v_2(b^2 d - a^2) \geq 3$ with d and a^2 even and b odd. Write $a = 2\hat{a}$ and $d = 2\hat{d}$ for some integers $\hat{a}$ and $\hat{b}$ so that $2b^2\hat{d} - 4\hat{a} = 8k$. In particular, $b^2\hat{d} - 2\hat{a} = 4k$ which is impossible since $b^2\hat{d}$ is odd.

Case III. Suppose $v_2(b^2d - a^2) \geq 2$ with a and b even. Write $a = 2\hat{a}$ and $b = 2\hat{b}$ for some integers $\hat{a}$ and $\hat{b}$. Moreover, $b^2d - a^2 = 4k$ for some integer k. Since c_6 is even, we have that $v_2(c_4) \geq 4$ by Theorem 2.6. Observe that

$$c_4 = 3b^2d - 3a^2 + 4a^2 \equiv 12k \mod 16$$

and so k must be divisible by 4. Write $k = 4\hat{k}$ for some integer $\hat{k}$ and observe that

$$\begin{aligned} b^2d - a^2 = 4k &\iff 4\hat{b}^2d - 4\hat{a}^2 = 16\hat{k} \\ &\iff \hat{b}^2d - \hat{a}^2 = 4\hat{k}. \end{aligned} \tag{5.7}$$

This only occurs when both $\hat{b}^2d$ and $\hat{a}^2$ are even or they are both odd. We claim that they are both odd. Indeed, if $\hat{a}^2$ and $\hat{b}^2d$ are even, then $\hat{a}$ and d are even and $\hat{b}$ is odd since at most one of $\hat{a}$ and $\hat{b}$ can be even. Write $d = 2\hat{d}$ and $\hat{a} = 2\bar{a}$ for integers $\hat{d}$ and $\bar{a}$ and observe that

$$\hat{b}^2d - \hat{a}^2 = 4\hat{k} \iff 2\hat{b}^2\hat{d} - 4\bar{a}^2 = 4k \iff \hat{b}^2\hat{d} - 2\bar{a}^2 = 2k$$

which is impossible since $\hat{b}^2\hat{d}$ is odd.

Therefore $\hat{b}^2d$ and $\hat{a}^2$ are both odd. We now return to equation (5.7). Since odd squares modulo 4 are 1, we have that $\hat{b}^2d - \hat{a}^2 \equiv d - 1 \mod 4$ and so $\hat{b}^2d - \hat{a}^2 = 4\hat{k}$ if and only if $d \equiv 1 \mod 4$. To summarize we have shown that if $u_T = 2$ and $v_2(b^2d - a^2) \geq 2$ with a and b even, then $v_2(a) = v_2(b) = 1$ and $d \equiv 1 \mod 4$. In fact by the above $v_2(b^2d - a^2) \geq 4$ since k is divisible by 4. It remains to show that $c_6 \equiv 0$ or $8 \mod 32$. Indeed,

$$\begin{aligned} c_6 = -a\left(9b^2d - a^2\right) &= -8\hat{a}\left(9\hat{b}^2d - \hat{a}^2\right) = -8\hat{a}\left(9\hat{b}^2d - 9\hat{a}^2 + 8\hat{a}^2\right) \\ &= -8\hat{a}\left(36\hat{k} + 8\hat{a}^2\right) = -32\hat{a}\left(9\hat{k} + 2\hat{a}^2\right) \equiv 0 \mod 32. \end{aligned}$$

Case IV. Suppose $v_2(b^2d - a^2) = 1$ and $v_2(b^2d) \geq 2$. Note that $v_2(b^2d) \geq 2$ implies that $v_2(b) \geq 1$ since d is squarefree. In particular, a is even. Now write $b^2d - a^2 = 2k$, $a = 2\hat{a}$, and $b = 2\hat{b}$ for some integers $\hat{a}$ and $\hat{b}$ and k an odd integer. Then

$$2k = b^2d - a^2 = 4\hat{b}^2d - 4\hat{a}^2$$

implies that k is even, which contradicts our assumption on k being odd.

Case V. Suppose $v_2(b^2d) \geq 6$. Then $v_2(b) \geq 3$ since d is squarefree and so we write $b = 8\hat{b}$ for some integer $\hat{b}$. We first claim a is odd. Suppose not, then $a = 2\hat{a}$ for some odd integer $\hat{a}$ and we attain

$$b^2d - a^2 = 64\hat{b}^2d - 4\hat{a}^2 = 4\left(16\hat{b}^2d - \hat{a}^2\right)$$

and so $v_2(b^2d - a^2) = 2$. But these are the assumptions of Case III, where we saw that $u_T = 2$ if $v_2(b) = 1$. Therefore $u_T \neq 2$ under the assumptions of Case V with a even. Therefore a is odd, as claimed. Then c_4 is odd and so $c_6 \equiv -1 \mod 4$ by Theorem 2.6. Now observe that

$$c_6 = -a\left(9b^2d - a^2\right) \equiv -a\left(72\hat{b}^2d - a^2\right) \equiv a^3 \mod 4.$$

Therefore $c_6 \equiv -1 \mod 4$ if and only if $a \equiv -1 \mod 4$.

By the above, we have exhausted the possibilities when $u_T = 2, 4$ and so it follows that $u_T = 1$ if (i) and (ii) do not hold. ■

5.4.3 Proof of Theorem 5.14 for $T = C_3$

Theorem 5.14 for $T = C_3$. Let $a = c^3d^2e$ with d, e positive squarefree integers such that $\gcd(d, e) = 1$. Then the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T = c^2d$.

Proof First, suppose E_T has j-invariant 0. Then by Lemma 5.16, $E_T = E_T(24, 1)$. Since $24 = 8 \cdot 3$, it is verified that the minimal discriminant of $E_T(24, 1)$ is $u_T^{-12}\gamma_T$ with $u_T = 4$ which verifies the Theorem.

Next, suppose the j-invariant of E_T is not equal to 0 or 1728. The admissible change of variables $x \longmapsto v^2x$ and $y \longmapsto v^3y$ with $v = c^2d$ results in a $\mathbb{Q}$-isomorphism between E_T and the elliptic curve

$$E_T' : y^2 + cdexy + de^2by = x^3.$$

In particular, E'_T is given by an integral Weierstrass model and its discriminant Δ and invariants c_4 and c_6 are

$$\begin{aligned}
c_4 &= v^{-4}\alpha_T = cd^2e^3\,(a-24b)\\
c_6 &= v^{-6}\beta_T = d^2e^4\left(-a^2+36ab-216b^2\right)\\
\Delta &= v^{-12}\gamma_T = d^4e^8b^3\,(a-27b)\,.
\end{aligned}$$

We claim that E'_T is a global minimal model for E_T. By the assumption on E_T, a and b are relatively prime integers and therefore

$$\gcd(\beta_T,\gamma_T) \qquad \text{divides} \qquad 2^6 3^9 a^4$$

by Lemma 5.10. Since $\gcd(c_6,\Delta) = v^{-6}\gcd(\beta_T,\gamma_T)$ we conclude that $\gcd(c_6,\Delta)$ divides $2^6 3^9 d^2 e^4$. Now let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E'_T and a global minimal model of E_T. Since E'_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6|c_4$ and $u_T^{12}|\Delta$. Therefore u_T^6 divides $2^6 3^9 d^2 e^4$. In particular, $v_p(u_T)=0$ for all primes $p \geq 5$ since d and e are relatively prime squarefree integers.

We now claim that $v_3(u_T)=0$. If this is not the case, we have

$$12 \leq v_3(\Delta) = v_3\left(d^4e^8b^3\right) + v_3(a-27b)\,.$$

First, suppose $v_3(a) > 0$ with $v_3(a) \neq 3$. Then $v_3(a-27b) \leq 3$ and $v_3(d^4e^8b^3) \leq 8$ since a and b are relatively prime and d,e are squarefree and relatively prime. Therefore this case is not possible. Suppose instead that $v_3(a)=3$ and write $a = 27\hat{a}$ for some integer $\hat{a}$. Note that 3 does not divide de and so

$$v_3(c_6) = v_3\left(-3^6a^2 + 3^5 4a\hat{b} - 3^9 8\hat{b}^2\right) = 5 + v_3\left(-3a^2 + 4a\hat{b} - 3^4 8\hat{b}^2\right) = 5$$

since $-3a^2 + 4a\hat{b} - 3^4 8\hat{b}^2 \equiv 4a\hat{b} \mod 3$. It follows that this quantity is not 0 modulo 3 since $a\hat{b}$ is not divisible by 3. But this is our desired contradiction since $v_3(u_T) > 0$ implies that $v_3(c_6) \geq 6$. Next, suppose $v_3(a) = 0$. Then $c_4 \equiv acd^2e^3 \mod 3$ which is nonzero modulo 3 since $a = c^3d^2e$. In particular, we have shown that $v_3(u_T) = 0$.

It remains to show that $v_2(u_T) = 0$. To this end, observe that c_4 is even if and only if a is even. Therefore, if $v_2(u_T) > 0$, then $v_2(a) > 0$ since $v_2(c_4) \geq 4$. But then we have a contradiction since $a - 27b$ is odd and

$$12 \leq v_2(\Delta) = v_2\big(d^4 e^8\big) \leq 8.$$

Hence $v_2(u_T) = 0$ which implies that $|u_T| = 1$. Hence E_T' is a global minimal model for E_T. ■

5.4.4 Proof of Theorem 5.14 for $T = C_4$

Theorem 5.14 for $T = C_4$. Let $a = c^2 d$ with d a positive squarefree integer. Then the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{c, 2c\}$. Moreover, $u_T = 2c$ if and only if $v_2(a) \geq 8$ is even with $bd \equiv 3 \mod 4$.

Proof First, suppose E_T has j-invariant 1728. Then by Lemma 5.15, E_T is $\mathbb{Q}$-isomorphic to $E_T(8, -1)$. Then $a = c^2 d$ with $c = 2$ and $d = 2$. The admissible change of variables $x \longmapsto u_T^2 x$ and $y \longmapsto u_T^3 y$ with $u_T = c$ gives a $\mathbb{Q}$-isomorphism from E_T onto

$$E_T' : y^2 + 4xy + 8y = x^3 + 2x^2.$$

Then the discriminant of $E_T' = -2^{12}$. We claim that the minimal discriminant is -2^{12}. Indeed, if this were not the case, then the only possibility for the minimal discriminant is -1. But this is absurd since there is no rational elliptic curve of conductor 1.

Next, suppose E_T has j-invariant not equal to 0 or 1728. The admissible change of variables $x \longmapsto c^2 x$ and $y \longmapsto c^3 y$ results in a $\mathbb{Q}$-isomorphism between E_T and the elliptic curve

$$E_T' : y^2 + cdxy - cd^2 by = x^3 - bdx^2.$$

In particular, E'_T is given by an integral Weierstrass model and its discriminant Δ and invariants c_4 and c_6 are

$$
\begin{aligned}
c_4 &= c^{-4}\alpha_T = d^2\left(a^2+16ab+16b^2\right)\\
c_6 &= c^{-6}\beta_T = d^3\left(a+8b\right)\left(-a^2-16ab+8b^2\right)\\
\Delta &= c^{-12}\gamma_T = b^4c^2d^7\left(a+16b\right).
\end{aligned}
$$

Since a and b are relatively prime integers, we have that

$$\gcd(\beta_T,\gamma_T) \qquad \text{divides} \qquad 2^{18}a^3$$

by Lemma 5.10. Since $\gcd(c_6,\Delta) = c^{-6}\gcd(\beta_T,\gamma_T)$ we conclude that $\gcd(c_6,\Delta)$ divides $2^{18}d^3$. Now let $x \longmapsto u_T^2x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E'_T and a global minimal model of E_T. Since E'_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6|c_4$ and $u_T^{12}|\Delta$. Therefore u_T^6 divides $2^{18}d^3$. In particular, $v_p(u_T) = 0$ for all odd primes p since d is squarefree. Therefore u_T divides 2^3.

We first claim that $u_T \neq 4, 8$. Towards a contradiction, suppose u_T is 4 or 8. In either case, we have that $v_2(c_4) \geq 8$ and $v_2(c_6) \geq 12$. We show that these inequalities never hold. First, observe that c_4 is even if and only if a is even. But

$$v_2(c_4) = 2v_2(d) + v_2\big(a^2+16ab+16b^2\big) \leq 6$$

whenever a is even with $v_2(a) \neq 2$. So suppose $v_2(a) = 2$ so that $a = 4\hat{a}$ for some odd integer $\hat{a}$. Then

$$
\begin{aligned}
12 \leq v_2(c_6) &= 3v_2(d) + v_2(4\hat{a}+8b) + v_2\big(-16\hat{a}^2-64\hat{a}b+8b^2\big)\\
&= 5 + 3v_2(d) + v_2(\hat{a}+2b) + v_2\big(-2\hat{a}^2-8\hat{a}b+b^2\big)\\
&\leq 8
\end{aligned}
$$

since $v_2(\hat{a}+2b) = v_2(-2\hat{a}^2-8\hat{a}b+b^2) = 0$. This is our desired contradiction and so we conclude that u_T divides 2.

Suppose $u_T = 2$. Then $2^4 | c_4$, $2^6 | c_6$, and $2^{12} | \Delta$. In particular, a is even since c_4 is even if and only if a is even. Since $a = c^2 d$ with d squarefree, we claim that if $v_2(a) \neq 4$, then $v_2(\Delta) \geq 12$ if and only if $v_2(a) = 3, 5$ or $v_2(a) \geq 7$. Indeed,

$$12 \leq v_2(\Delta) = 2v_2(c) + 7v_2(d) + v_2(a + 16b)$$

and note that

$$v_2(c) = \begin{cases} 0 & \text{if } v_2(a) \text{ is odd} \\ \frac{v_2(a)}{2} & \text{if } v_2(a) \text{ is even} \end{cases} \qquad \text{and} \qquad v_2(d) = \begin{cases} 1 & \text{if } v_2(a) \text{ is odd} \\ 0 & \text{if } v_2(a) \text{ is even.} \end{cases}$$

Lastly $v_2(a + 16b) \leq 4$ with equality holding if $v_2(a) > 4$. The claim now follows.

Next, suppose $v_2(a) = 4$. Then by inspection $v_2(c_4) = 4$ and $v_2(c_6) = 6$ since $v_2(d) = 0$. In addition, $v_2(\Delta) \geq 12$ if and only if $v_2(a + 16b) \geq 8$.

Since $u_T = 2$, we have that $2^{-4}c_4$ and $2^{-6}c_6$ satisfy the conclusion of Theorem 2.6. We now show that Theorem 2.6 is satisfied if and only if $v_2(a) \geq 8$ is even with $bd \equiv 3 \mod 4$.

Case I. Suppose $v_2(a) \geq 3$ is odd. In particular, c and d are even and we write $c = 2\hat{c}$ and $d = 2\hat{d}$ for integers $\hat{c}$ and $\hat{d}$. Next, observe that

$$\begin{aligned} 2^{-4}c_4 &= 2^{-4}\left(d^2\left(c^4 d^2 + 16c^2 bd + 16b^2\right)\right) \\ &= 16\hat{c}^4\hat{d}^4 + 32\hat{c}^2\hat{d}^3 b + 4b^2\hat{d}^2 \equiv 4b^2\hat{d}^2 \mod 16 \\ 2^{-6}c_6 &= 2^{-6}\left(d^3\left(c^2 d + 8b\right)\left(-c^4 d^2 - 16c^2 db + 8b^2\right)\right) \\ &= -64\hat{c}^6\hat{d}^6 - 192b\hat{c}^4\hat{d}^5 - 120b^2\hat{c}^2\hat{d}^4 + 8b^3\hat{d}^3 \equiv 0 \mod 4. \end{aligned}$$

Since $2^{-6}c_6 \not\equiv -1 \mod 4$, $v_2(2^{-4}c_4) \geq 4$ by Theorem 2.6. But this is not satisfied since $b^2\hat{d}^2$ is odd.

Case II. Next suppose $v_2(a) = 4$ and $v_2(a + 16b) \geq 8$. Then d is odd and $c = 4\hat{c}$ for some odd integer $\hat{c}$. Write $a + 16b = 2^8 k$ for some integer k and solving for b yields

$$16b = 2^8 k - 16\hat{c}^2 d \Longleftrightarrow b = 16k - \hat{c}^2 d.$$

Then

$$2^{-6}c_6 = \hat{c}^6 d^6 - 528\hat{c}^4 d^5 k - 8448\hat{c}^2 d^4 k^2 + 4096 d^3 k^3 \equiv \hat{c}^6 d^6 \mod 4.$$

Since odd squares are congruent to 1 modulo 4, we have $2^{-6}c_6 \equiv 1 \mod 4$. But then $2^{-6}c_6$ is odd and does not satisfy Theorem 2.6. So this case is not possible.

Case III. Suppose $v_2(a) \geq 8$ is even. Then $c = 16\hat{c}$ for some integers $\hat{c}$ and d, with d odd. Then

$$\begin{aligned} 2^{-6}c_6 &= 2^{-6}\left(d^3\left(16^2\hat{c}^2 d + 8b\right)\left(-16^4\hat{c}^4 d^2 - 16^3\hat{c}^2 db + 8b^2\right)\right) \\ &= -2^{18}\hat{c}^6 d^6 - 2^{13}3b\hat{c}^4 d^5 - 480b^2\hat{c}^2 d^4 + b^3 d^3 \equiv b^3 d^3 \mod 4. \end{aligned}$$

Since bd is odd, we have by Theorem 2.6 that $2^{-6}c_6 \equiv 3 \mod 4$. But this occurs if and only if $bd \equiv 3 \mod 4$. It remains to check that $v_3(2^{-6}c_6) \neq 2$. To verify this, we observe that $v_3(2^{-6}c_6) = 2$ if and only if $2^{-6}c_6 \equiv 0, 18 \mod 27$. Reducing modulo 27, we attain

$$2^{-6}c_6 \equiv 26\hat{c}^6 d^6 + 21b\hat{c}^4 d^5 + 6b^2\hat{c}^2 d^4 + b^3 d^3 \mod 27.$$

Now let `f[c,d,b]` be the Mathematica input for $26\hat{c}^6 d^6 + 21b\hat{c}^4 d^5 + 6b^2\hat{c}^2 d^4 + b^3 d^3$. The Mathematica input

```
Table[Mod[f[c,d,b],27],{c,1,27},{d,1,27},{b,1,27}]
```

verifies that $2^{-6}c_6 \not\equiv 0, 18 \mod 27$. Therefore the minimal discriminant of E_T in terms of γ_T is $(2c)^{-12}\gamma_T$, as claimed.

It now follows that if $v_2(a) \geq 8$ is even with $bd \equiv 3 \mod 4$ does not hold, then E_T' is a global minimal model for E_T, which completes the proof. ∎

5.4.5 Proof of Theorem 5.14 for $T = C_6$

Theorem 5.14 for $T = C_6$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2\}$. Moreover, $u_T = 2$ if and only if $v_2(a + b) \geq 3$.

Proof First, suppose E_T has j-invariant 0. Then by Lemma 5.15 E_T is $\mathbb{Q}$-isomorphic to $E_T(3, -1)$. Then $\gamma_T = -2^4 3^3$ and therefore it is the minimal discriminant of E_T.

Next, suppose the j-invariant of E_T is not equal to 0 or 1728. Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6|\beta_T$ and $u_T^{12}|\gamma_T$. In particular, u_T^6 divides $\gcd(\beta_T, \gamma_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\beta_T, \gamma_T)$ divides $2^9 3^3$. Therefore u_T divides 2.

Suppose $u_T = 2$. Then $2^4|\alpha_T$, $2^6|\beta_T$, and $2^{12}|\gamma_T$. Observe that $\alpha_T \equiv (a+b)^4 \mod 2$. Hence α_T is even if and only if $a+b$ is even. Consequently, a and b are both odd since a and b are relatively prime. Next,

$$12 \leq v_2(\gamma_T) = v_2(a+9b) + 3v_2(a+b)\,. \tag{5.8}$$

We claim that the above inequality holds if and only if $v_2(a+b) \geq 3$. Suppose $v_2(a+b) \leq 2$ so that $a+b \equiv \pm 2, 4 \mod 8$. Since $a+9b \equiv a+b \mod 8$, it follows that $v_2(a+9b) \leq 2$ and so inequality (5.8) does not hold. Now suppose $v_2(a+b) \geq 3$. Then $v_2(a+9b) \geq 3$ since $a+9b \equiv a+b \mod 8$ and therefore $v_2(\gamma_T) \geq 12$. We now claim that if $v_2(a+b) \geq 3$, then $2^{-4}\alpha_T$ and $2^{-6}\beta_T$ are integers.

Since $a+3b$ is even, it suffices to show that

$$a^3 + 9a^2b + 3ab^2 + 3b^3 \equiv 0 \mod 8$$

to show that $v_2(\alpha_T) \geq 4$. Since odd squares are congruent to 1 modulo 8, we conclude that

$$\begin{aligned} a^3 + 9a^2b + 3ab^2 + 3b^3 &\equiv a + 9b + 3a + 3b \mod 8 \\ &\equiv 4\,(a+b) \mod 8 \\ &\equiv 0 \mod 8. \end{aligned}$$

We now conclude that β_T is divisible by 2^6 from the identity $\beta_T^2 = \alpha_T^3 - 1728\gamma_T$. The admissible change of variables $x \longmapsto 4x$ and $y \longmapsto 8y$ gives a $\mathbb{Q}$-isomorphism from E_T onto the elliptic curve E_T' given by the Weierstrass model

$$E_T' : y^2 + \frac{a-b}{2}xy - \frac{ab\,(a+b)}{8}y = x^3 - \frac{b\,(a+b)}{4}x^2.$$

Since $v_3(a+b) \geq 3$, it follows that E_T' is an integral Weierstrass model. By the above, we conclude that it is a global minimal model for E_T whenever $v_3(a+b) \geq 3$.

To recap u_T divides 2 and is exactly 2 if and only if $v_2(a+b) \geq 3$. Consequently, E_T is a global minimal model for E_T if $v_2(a+b) < 3$. ∎

5.4.6 Proof of Theorem 5.14 for $T = C_8$

Theorem 5.14 for $T = C_8$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2\}$. Moreover, $u_T = 2$ if and only if $v_2(a) = 1$.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6 | \beta_T$ and $u_T^{12} | \gamma_T$. In particular, u_T^6 divides $\gcd(\beta_T, \gamma_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\beta_T, \gamma_T)$ divides 2^9. In particular, u_T divides 2.

Suppose $u_T = 2$ so that $2^4 | \alpha_T$, $2^6 | \beta_T$, and $2^{12} | \gamma_T$. Reducing modulo 2, shows

$$\alpha_T \equiv a^8 \mod 2$$

and so α_T is even if and only if a is even. Observe that

$$12 \leq v_2(\gamma_T) = 2v_2(a) + 4v_2(a-2b) + v_2\left(a^2 - 8ab + 8b^2\right) \tag{5.9}$$

We claim that inequality (5.9) holds if and only if $v_2(a) = 1$ or $v_2(a) > 2$. Indeed,

$$v_2\left(a^2 - 8ab + 8b^2\right) = \begin{cases} 2 & \text{if } v_2(a) = 1 \\ 3 & \text{if } v_2(a) > 1 \end{cases}$$

and for $v_2(a-2b)$ we have that $v_2(a-2b) = 1$ if $v_2(a) > 1$ and $v_2(a-2b) \geq 2$ if $v_2(a) = 1$. The claim now follows. By inspection, $v_2(\alpha_T) = 4$ and so $v_2(\beta_T) = 6$ by Lemma 5.21.

This shows that $u_T = 2$ is possible only if a is even and $v_2(a) \neq 2$. Since $2^{-6}\beta_T$ is odd, we have by Theorem 2.6 that $2^{-6}\beta_T \equiv 3 \mod 4$. Now write $a = 2\hat{a}$ for some integer $\hat{a}$ such that $\hat{a}$ is odd or $v_2(\hat{a}) > 1$. Then

$$2^{-6}\beta_T \equiv 2\hat{a}^4 b^8 + b^{12} \mod 4.$$

Since odd squares are congruent to 1 modulo 4, we deduce that $2^{-6}\beta_T \equiv 2\hat{a}^4+1 \mod 4$. In particular,

$$2^{-6}\beta_T \equiv \begin{cases} 3 \mod 4 & \text{if } v_2(\hat{a}) = 0 \\ 1 \mod 4 & \text{if } v_2(\hat{a}) > 1. \end{cases}$$

Hence Theorem 2.6 only holds if and only if $v_2(a) = 1$. It remains to show that $v_3(2^{-6}\beta_T) \neq 2$. To this end we note that $v_3(2^{-6}\beta_T) = 2$ if and only if $2^{-6}\beta_T \equiv 9, 18 \mod 27$. Since $2^{-6}\beta_T$ is in terms of $\hat{a}$ and b, we let `beta[a1,b]` be the Mathematica input for $2^{-6}\beta_T$ with `a1` being the input corresponding to $\hat{a}$. Then the Mathematica input

```
Table[Mod[beta[a1,b],27],{a1,1,27}{b,1,27}]
```

verifies that $v_3(2^{-6}\beta_T) \neq 2$. We conclude that $u_T = 2$ if and only if $v_2(a) = 1$.

Lastly, since u_T divides 2 it follows that if $v_2(a) \neq 1$, then E_T is a global minimal model for E_T. ■

5.4.7 Proof of Theorem 5.14 for $T = C_{10}$

Theorem 5.14 for $T = C_{10}$. The minimal discriminant of $E_T$is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2\}$. Moreover, $u_T = 2$ if and only if a is even.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6|\beta_T$ and $u_T^{12}|\gamma_T$. In particular, u_T^6 divides $\gcd(\beta_T, \gamma_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and

s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\beta_T, \gamma_T)$ divides $2^8 5$. Therefore u_T divides 2.

Suppose $u_T = 2$. Then $2^{-4}|\alpha_T,\ 2^{-6}|\beta_T$, and $2^{-12}|\gamma_T$. Reducing α_T modulo 2 yields $\alpha_T \equiv a^{12} \bmod 2$ and so α_T is even if and only if a is even. Now observe that

$$12 \leq v_2(\gamma_T) = 5v_2(a) + 5v_2(a-2b) + v_2\big(a^2 + 2ab - 4b^2\big) \tag{5.10}$$

It is clear that (5.10) holds if $v_2(a) \geq 2$. So suppose $v_2(a) = 1$. Then $v_2(a-2b) \geq 2$ and so inequality (5.10) holds. By inspection, $v_2(\alpha_T) = 4$ if a is even and consequently $v_2(\beta_T) = 6$ by Lemma 5.21. The admissible change of variables $x \longmapsto 4x$ and $y \longmapsto 8y$ gives a $\mathbb{Q}$-isomorphism from E_T onto the elliptic curve

$$E_T' : y^2 + \frac{a^3 - 2a^2b - 2ab^2 + 2b^3}{2} xy - \frac{a^2b^3\,(a-2b)\,(a-b)\,(a^2 - 3ab + b^2)}{8} = x^3 - \frac{a\,(a-2b)\,(a-b)\,b^3}{4} x^2.$$

In particular, E_T' is given by an integral Weierstrass model if a is even. Therefore E_T' is a global minimal model for E_T if a is even.

Lastly, if a is not even, then E_T is a global minimal model for E_T. ∎

5.4.8 Proof of Theorem 5.14 for $T = C_{12}$

Theorem 5.14 for $T = C_{12}$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2\}$. Moreover, $u_T = 2$ if and only if a is even.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6|\beta_T$ and $u_T^{12}|\gamma_T$. In particular, u_T^6 divides $\gcd(\beta_T, \gamma_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\beta_T, \gamma_T)$ divides $2^9 3^3$. Therefore u_T divides 2.

Suppose $u_T = 2$ so that $2^{-4}|\alpha_T$, $2^{-6}|\beta_T$, and $2^{-12}|\gamma_T$. Then $\alpha_T \equiv a^{16} \mod 2$ and so α_T is even if and only if a is even. Next, observe that

$$v_2(\gamma_T) = 2v_2(a) + 6v_2(A - 2b) + v_2\left(a^2 - 6ab + 6b^2\right) + 3v_2\left(a^2 - 2ab + 2b^2\right).$$

By inspection, we see that a is even if and only if $v_2(\gamma_T) \geq 12$. By inspection, $v_2(\alpha_T) = 4$ and so $v_2(\beta_T) = 6$ by Lemma 5.21. The admissible change of variables $x \longmapsto 4x$ and $y \longmapsto 8y$ gives a $\mathbb{Q}$-isomorphism from E_T onto the elliptic curve $E_T' : y^2 + a_1xy + a_3y = x^3 + a_2x^2$ where

$$\begin{aligned}
a_1 &= -\frac{1}{2}\left(a^4 - 2a^3b - 2a^2b^2 + 8ab^3 - 6b^4\right)\\
a_2 &= \frac{1}{4}b\left(a - 2b\right)\left(a - b\right)^2\left(a^2 - 3ab + 3b^2\right)\left(a^2 - 2ab + 2b^2\right)\\
a_3 &= -\frac{1}{8}ab\left(a - 2b\right)\left(a - b\right)^3\left(a^2 - 3ab + 3b^2\right)\left(a^2 - 2ab + 2b^2\right).
\end{aligned}$$

Since a is even, E_T' is given by an integral Weierstrass model. Therefore E_T' is a global minimal model for E_T if a is even.

Lastly, if a is not even, then E_T is a global minimal model for E_T. ■

5.4.9 Proof of Theorem 5.14 for $T = C_2 \times C_2$

Theorem 5.14 for $T = C_2 \times C_2$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2\}$. Moreover, $u_T = 2$ if and only if $v_2(a) \geq 4$ and $bd \equiv 1 \mod 4$.

Proof First, suppose E_T has j-invariant equal to 1728. By Lemma 5.19, E_T is $\mathbb{Q}$-isomorphic to $E_T(2, 1, d)$. Then $\gamma_T = 64d^6$. Since d is squarefree, we have that $v_p(\gamma_T) \leq 6$ for each odd prime p. In particular, if d is even, γ_T is the minimal discriminant of E_T. Now suppose $d = 2\hat{d}$ for some odd squarefree integer $\hat{d}$ and let $x \longmapsto u_T^2x + r_T$ and $y \longmapsto u_T^3 + u_T^2s_Tx + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^4|\alpha_T$ and $u_T^{12}|\gamma_T$. Since d is even, it follows that u_T divides 2. Towards a contradiction, suppose $u_T = 2$. Then $u_T^{-12}\gamma_T = \hat{d}^6$ and $u_T^{-4}\alpha_T = 12\hat{d}^2$. Since $v_2\left(u_T^{-4}\alpha_T\right) = 2$, we have our desired contradiction. Indeed, by Theorem 2.6 there is no integral Weierstrass model having invariants $c_4 = u_T^{-4}\alpha_T$ and $c_6 = 0$.

Next, suppose E_T does not have j-invariant equal to 1728. Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^6 | \beta_T$ and $u_T^{12} | \gamma_T$. In particular, u_T^6 divides $\gcd(\beta_T, \gamma_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\beta_T, \gamma_T)$ divides $2^7 d^8$. In particular, u_T divides $2d$. Recall that d is a squarefree integer.

We claim that $v_p(u_T) = 0$ for all odd primes. Towards a contradiction, suppose an odd prime p divides u_T. In particular, p divides d and moreover, p^{12} divides γ_T. In particular, $v_p(ab\,(a-b)) \geq 3$ since $\gamma_T = 16a^2b^2d^6\,(a-b)^2$. Since a, b, and $a-b$ are relatively prime, it follows that p divides exactly one of these. If p divides one of a or b, then p does not divide $a^2 - ab + b^2$ which contradicts the assumption that p^4 divides α_T. Therefore p divides $a - b$ and $a^2 - ab + b^2$. But then p divides

$$a^2 - ab + b^2 - (a-b)^2 = ab$$

which is a contradiction. Hence $v_p(u_T) = 0$ for all odd primes.

Consequently u_T divides 4. We claim that $u_T \neq 4$. Towards a contradiction, suppose $u_T = 4$ so that $v_2(\alpha_T) \geq 8$. Note that since $u_T = 4$, we have by Lemma 5.10 that d is even. Since d is squarefree, we deduce

$$8 \leq v_2(\alpha_T) = 6 + v_2\big(a^2 - ab + b^2\big) \tag{5.11}$$

Recall that by Lemma 5.12, a is even. Thus $a^2 - ab + b^2 \equiv -ab + 1 \mod 4$ since $b^2 \equiv 1 \mod 4$. If a and b are odd, then $a^2 - ab + b^2 \equiv 2 - ab \mod 4$. Since $ab \equiv \pm 1 \mod 4$, we conclude that $a^2 - ab + b^2$ is always odd. Therefore inequality (5.11) does not hold.

Now assume $u_T = 2$. Then $2^4|\alpha_T$, $2^6|\beta_T$, and $2^{12}|\gamma_T$. By definition of α_T and β_T, we see that the first two divisibilities are always satisfied. Now observe that

$$12 \leq v_2(\gamma_T) = 4 + 6v_2(d) + 2v_2(a)\,. \tag{5.12}$$

We now consider the cases where d is even or odd.

Case I. Suppose d is even. Since d is squarefree, it follows that $v_2(a) \geq 1$. Since $2^{-6}\beta_T$ is even and

$$2^{-4}\alpha_T = d^2\left(a^2 - ab + b^2\right) \not\equiv 4 \mod 8,$$

we conclude by Theorem 2.6 that there is no integral Weierstrass equation having invariants $c_4 = 2^{-4}\alpha_T$ and $c_6 = 2^{-6}\beta_T$. Therefore d cannot be even.

Case II. Suppose d is odd. Then by (5.12), $v_2(a) \geq 4$. Write $a = 16\hat{a}$ for some integer $\hat{a}$. Then

$$2^{-6}\beta_T = -d^3\left(16\hat{a} + b\right)\left(8\hat{a} - b\right)\left(32\hat{a} - b\right) \equiv -bd \mod 4.$$

By Theorem 2.6, there is an integral Weierstrass model having invariants $c_4 = 2^{-4}\alpha_T$ and $c_6 = 2^{-6}\beta_T$ if and only if $bd \equiv 1 \mod 4$ and $v_3(2^{-6}\beta_T) \neq 2$. Since $v_3(2^{-6}\beta_T) \neq 2$ if and only if $2^{-6}\beta_T \not\equiv 9, 18 \mod 27$, we verify that this indeed the case via the Mathematica input

```
Table[Mod[beta[a1,b],27],{a1,1,27}{b,1,27}]
```

where `beta` and `a1` are the Mathematica inputs for $2^{-6}\beta_T$ and $\hat{a}$, respectively. Hence $u_T = 2$ if and only if $v_2(a) \geq 4$ and $bd \equiv 1 \mod 4$.

Consequently, E_T is a global minimal model for E_T if and only if the above equivalence does not hold. ■

5.4.10 Proof of Theorem 5.14 for $T = C_2 \times C_4$

Theorem 5.14 for $T = C_2 \times C_4$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 2, 4\}$. Moreover, $u_T = 4$ if and only if $v_2(a) = 2$

(i) $u_T = 1$ if and only if $v_2(a) \leq 1$.

(ii) $u_T = 2$ if and only if $v_2(a) \geq 2$ with $v_2(a+4b) < 4$.

(iii) $u_T = 4$ if and only if $v_2(a) = 2$ and $v_2(a+4b) \geq 4$.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^4 | \alpha_T$ and $u_T^6 | \beta_T$. In particular, u_T^4 divides $\gcd(\alpha_T, \beta_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\alpha_T, \beta_T)$ divides $2^{14}3^2$. Therefore u_T divides 8. Note that $\alpha_T \equiv a^4 \mod 2$ and so α_T is even if and only if a is even. Under this assumption, we observe that

$$v_2(\alpha_T) = v_2\left(a^4 + 16a^3b + 80a^2b^2 + 128ab^3 + 256b^4\right) = \begin{cases} 4 & \text{if } v_2(a) = 1 \\ 8 & \text{if } v_2(a) \geq 2. \end{cases} \tag{5.13}$$

Therefore u_T divides 4. Moreover, observe that if $v_2(\alpha_T) = 8$ and $v_2(\gamma_T) \geq 24$, then $v_2(\beta_T) = 12$ by Lemma 5.21. In particular, $4^{-4} \cdot \beta_T$ is odd under these assumptions.

(iii) Suppose $u_T = 4$. Then $4^4 | \alpha_T$, $4^6 | \beta_T$, and $4^{12} | \gamma_T$. By (5.13), $4^4 | \alpha_T$ if and only if $v_2(a) \geq 2$. Then

$$24 \leq v_2(\gamma_T) = 2v_2(a) + 2v_2(a+8b) + 4v_2(a+4b)\,. \tag{5.14}$$

Case I. Suppose $v_2(a) \geq 4$. Then $v_2(\gamma_T) = 2v_2(a) + 14$ and thus inequality (5.14) holds if $v_2(a) \geq 5$. Now assume further that $v_2(a) \geq 5$. Since $v_2(\alpha_T) = 8$, it follows that $v_2(\beta_T) = 12$. In particular, $4^{-6}\beta_T$ is odd and by Theorem 2.6 we must have $4^{-6}\beta_T \equiv -1 \mod 4$. Write $a = 2^5\hat{a}$ for some integer $\hat{a}$ and observe that $4^{-6}\beta_T \equiv b^6 \mod 4$. Hence $4^{-6}\beta_T \equiv 1 \mod 4$ and by Theorem 2.6 we conclude that there is no integral Weierstrass model having invariants $c_4 = 4^{-4}\alpha_T$ and $c_6 = 4^{-6}\beta_T$.

Case II. Suppose $v_2(a) = 3$. Write $a = 8\hat{a}$ for some odd integer $\hat{a}$. Then $v_2(\gamma_T) = 20 + 2v_2(\hat{a}+b)$ and so inequality (5.14) holds if $v_2(\hat{a}+b) \geq 2$. Under this additional assumption, we have that $4^{-4} \cdot \beta_T$ is odd by the discussion following (5.13). By Theorem 2.6 we must have $4^{-6}\beta_T \equiv -1 \mod 4$. But

$$\begin{aligned}4^{-6}\beta_T &\equiv 2\hat{a}^2b^4 + 2\hat{a}b^5 + b^6 \mod 4\\ &\equiv 3 + 2\hat{a}b \mod 4\\ &\equiv 1 \mod 4\end{aligned}$$

since odd squares are congruent to 1 modulo 4 and $2k \equiv 2 \mod 4$ for odd integers k. In particular, there is no integral Weierstrass model having invariants $c_4 = 4^{-4}\alpha_T$ and $c_6 = 4^{-6}\beta_T$.

Case III. Suppose $v_2(a) = 2$. Write $a = 4\hat{a}$ for some odd integer $\hat{a}$. Then $v_2(\gamma_T) = 16 + 4v_2(\hat{a} + b)$ and so inequality (5.14) holds if $v_2(\hat{a} + b) \geq 2$. Under this additional assumption, we have that $4^{-4} \cdot \beta_T$ is odd by the discussion following (5.13). Now write $\hat{a} + b = 4k$ for some integer k. Hence $b = 4k - \hat{a}$ and so

$$\begin{aligned}4^{-4} \cdot \beta_T &\equiv 3\hat{a}^6 \mod 4\\ &\equiv 3 \mod 4.\end{aligned}$$

It remains to show that $v_3(4^{-4} \cdot \beta_T) \neq 2$. Since $v_3(4^{-4} \cdot \beta_T) \neq 2$ if and only $4^{-4} \cdot \beta_T \not\equiv 9, 18 \mod 27$. Now let `c6[x,y]` and `a1` be the Mathematica inputs for $\beta_T(x, y)$ and $\hat{a}$, respectively. Then the Mathematica input

```
Table[Mod[c6[2^2*a1,4*k-a1]/4^6,27],{a1,1,27},{k,1,27}]
```

verifies that $4^{-4} \cdot \beta_T \not\equiv 9, 18 \mod 27$. Hence $u_T = 4$ if and only if $v_2(a) = 2$ and $v_2(a + 4b) \geq 4$.

(ii) Suppose $u_T = 2$. Then $2^4|\alpha_T$, $2^6|\beta_T$, and $2^{12}|\gamma_T$. By (5.13), $2^4|\alpha_T$ if and only if $v_2(a) \geq 1$.

Case I. Suppose $v_2(a) = 2$ with $v_2(a + 4b) \leq 3$. By (5.13), $4^4|\alpha_T$. In fact, since $v_2(a) = 2$, $v_2(a + 4b) = 3$. Then $v_2(\gamma_T) = 20$ and hence $v_2(\beta_T) \geq 6$ by the identity $1728\gamma_T = \alpha_T^3 - \beta_T^2$. By Theorem 2.6, there is an integral Weierstrass model having invariants $c_4 = 2^{-4}\alpha_T$ and $c_6 = 2^{-6}\beta_T$ if and only if $2^{-6}\beta_T \equiv 0, 8 \mod 32$ and

$v_3(2^{-6}\beta_T) \neq 2$. To this end, let $a+4b = 8k$ for some odd integer k and let $a = 8k-4b$. Then $\beta_T(x,y) \equiv 0 \mod 32$. Let `c6[x,y]` be the Mathematica input for $2^{-6}\beta_T$. Then Mathematica input

```
Table[Mod[c6[8*k-4*b,b]/2^6,27],{b,1,27},{k,1,27}]
```

verifies that $v_3(2^{-6}\beta_T) \neq 2$. Thus, there is an integral Weierstrass model having invariants $c_4 = 2^{-4}\alpha_T$ and $c_6 = 2^{-6}\beta_T$.

Case II. Suppose $v_2(a) \geq 3$. By (5.13), $4^4|\alpha_T$ and we note that

$$v_2(\gamma_T) = 2v_2(a) + 2v_2(a+8b) + 4v_2(a+4b) \geq 20$$

and so $v_2(\beta_T) \geq 6$ from the identity $1728\gamma_T = \alpha_T^3 - \beta_T^2$. By Theorem 2.6, there is an integral Weierstrass model having invariants $c_4 = 2^{-4}\alpha_T$ and $c_6 = 2^{-6}\beta_T$ if and only if $2^{-6}\beta_T \equiv 0, 8 \mod 32$ and $v_3(2^{-6}\beta_T) \neq 2$. Set $a = 8\hat{a}$ for some integer $\hat{a}$ and observe that $2^{-6}\beta_T \equiv 0 \mod 32$. Now let `c6[x,y]` be the Mathematica input for $\beta_T(x,y)$. Then Mathematica input

```
Table[Mod[c6[8*a,b]/2^6,27],{a,1,27},{b,1,27}]
```

verifies that $v_3(2^{-6}\beta_T) \neq 2$. Thus, there is an integral Weierstrass model having invariants $c_4 = 2^{-4}\alpha_T$ and $c_6 = 2^{-6}\beta_T$.

Case III. Suppose $v_2(a) = 1$. Then

$$v_2(\gamma_T) = 2v_2(a) + 2v_2(a+8b) + 4v_2(a+4b) = 8$$

and so $v_2(\gamma_T) < 12$. This contradicts the assumption that $u_T = 2$.

Therefore $u_T = 2$ if and only if $v_2(a) \geq 2$ with $v_2(a+4b) \neq 3$.

(*iii*) Since (*i*) and (*ii*) exhaust the possibilities when $v_2(a) \geq 2$ and $u_T \geq 2$, it follows that E_T is a global minimal model for E_T if and only if $v_2(a) \leq 1$. ■

5.4.11 Proof of Theorem 5.14 for $T = C_2 \times C_6$

Theorem 5.14 for $T = C_2 \times C_6$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 4, 16\}$. Moreover,

(i) $u_T = 1$ if and only if $v_2(a+b) = 0$;

(ii) $u_T = 4$ if and only if $v_2(a+b) \geq 2$;

(iii) $u_T = 16$ if and only if $v_2(a+b) = 1$.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^4 | \alpha_T$ and $u_T^6 | \beta_T$. In particular, u_T^4 divides $\gcd(\alpha_T, \beta_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\alpha_T, \beta_T)$ divides $2^7 3$. But u_T^6 divides $\gcd(\beta_T, \gamma_T)$, and so we conclude by Lemma 5.10 that that u_T divides 2^7. Since $\alpha_T \equiv a^8 + b^8 \mod 2$, we deduce that α_T is even if and only if $a+b$ is even.

(i) Suppose $v_2(a+b) = 0$. Then α_T is odd and therefore by the above E_T is a global minimal model for E_T if $v_2(a+b) = 0$. This is the converse of (i).

In what follows we will prove the converse of (ii) and (iii). This will exhaust all possibilities which then gives the forward implication. To prove the converse for (ii) and (iii) we will exhibit a global minimal model which satisfies $u_T^{-4}\alpha_T$ and $u_T^{-6}\beta_T$ as the invariants c_4 and c_6, respectively of the constructed model. Namely, we consider the admissible change of variables $x \longmapsto u_T^2 x$ and $y \longmapsto u_T^3 y$. This gives a $\mathbb{Q}$-isomorphic from E_T onto the elliptic curve

$$E_{u_T} : y^2 - \frac{a_1}{u_T} xy + \frac{2a_3}{u_T^3} y = x^3 + \frac{2a_2}{u_T^2} x^2 \text{ where} \tag{5.15}$$

$$a_1 = 19a^2 - 2ab - b^2$$

$$a_2 = a\,(b-a)^2\,(b-5a)$$

$$a_3 = a\,(b-5a)\,(b-3a)\,(3a+b)\,(b-a)^2\,.$$

We will show for each of the cases below that E_{u_T} is an integral Weierstrass model under the desired assumptions on $a+b$.

(iii) Suppose $v_2(a+b) = 1$. Write $a+b = 2k$ for some odd integer k so that $b = 2k - a$. Then

$$v_2(\gamma_T) = 6 + 2v_2((b-9a)(b-3a)(3a+b)) + 6v_2((b-5a)(b-a)).$$

We claim that $v_2(\gamma_T) \geq 48$. Note that

$$(b-5a)(b-a) = (2k-6a)(2k-2a) = 4\left(k^2 - 4ak + 3a^2\right).$$

Since odd squares are congruent to 0 modulo 8, we deduce

$$k^2 - 4ak + 3a^2 \equiv 4 - 4ak \mod 8.$$

But $4n \equiv 4 \mod 8$ for all odd integers n, and so $(b-5a)(b-a) \equiv 0 \mod 32$. In particular, $v_2((b-5a)(b-a)) \geq 5$. Next,

$$\begin{aligned}(b-9a)(b-3a)(3a+b) &= (2k-10a)(2k-4a)(2k+2a) \\ &= 8\left(k^3 - 6ak^2 + 3a^2k + 10a^3\right).\end{aligned}$$

Since odd squares are congruent to 1 modulo 8, we deduce

$$\begin{aligned}k^3 - 6ak^2 + 3a^2k + 10a^3 &\equiv k - 6a + 3k + 10a \mod 8 \\ &\equiv 4k + 4a \mod 8 \\ &\equiv 0 \mod 8.\end{aligned}$$

Hence $v_2((b-9a)(b-3a)(3a+b)) \geq 6$. In particular, $v_2(\gamma_T) \geq 48$.

Now let $\alpha_T = PQ$ where P is the factor of degree 2 and Q is the factor of degree 6. Then

$$\begin{aligned}P &\equiv -4\left(a^2 - 4ak - k^2\right) \mod 2^5 \\ Q &\equiv -64\left(a^2 + 4ak - k^2\right)^3 \mod 2^{13}.\end{aligned}$$

Since $a^2 \pm 4ak - k^2 \equiv 4 \mod 8$ and $2^{l-1}x \equiv 2^{l-1} \mod 2^l$ for all odd integers x and positive integers l, we have that $P \equiv 16 \mod 32$ and $Q \equiv 2^{12} \mod 2^{13}$. Therefore $v_2(\alpha_T) = 16$ and by Lemma 5.21 we have that $v_2(\beta_T) = 24$. Thus $16^{-4}\alpha_T$ and $16^{-6}\beta_T$

are odd integers. Then $16^{-4}\alpha_T$ and $16^{-6}\beta_T$ are the invariants c_4 and c_6, respectively of the elliptic curve E_{u_T} in (5.15) with $u_T = 16$. We claim that E_{u_T} is given by an integral Weierstrass model. Indeed,

$$\begin{aligned} a_1 &\equiv 3a^2 - 2ab - b^2 \mod 16 \\ &\equiv 3a^2 - 2a\,(2k-a) - (2k-a)^2 \mod 16 \\ &\equiv 4a^2 - 4k^2 \mod 16 \\ &\equiv 0 \mod 16 \text{ since } 4l \equiv 4 \mod 16 \text{ for odd integers } l. \end{aligned}$$

We have already established that $(b-5a)\,(b-a) \equiv 0 \mod 32$. Since $v_2(a+b) = 1$, we have that $a+b \equiv 2 \bmod 4$ which implies that $b-a \equiv 0 \mod 4$. Hence $v_2\big((b-5a)\,(b-a)^2\big) \geq 7$ and so $16^{-3} \cdot 2a_2$ is an integer. Lastly, observe that by the above $(b-a)^2 \equiv 0 \mod 16$. Therefore, to show that $16^{-2} \cdot 2a_3$ is an integer, it suffices to show that $(b-5a)\,(b-3a)\,(3a+b) \equiv 0 \mod 8$. But this is automatic since each factor is even. Therefore E_{u_T} with $u_T = 16$ is a global minimal model for E_T whenever $v_2(a+b) = 1$. This shows the converse of (iii).

(ii) Suppose $v_2(a+b) \geq 2$. Write $a+b = 4k$ for some integer k. Then $b-a = 4k-2a \equiv 2 \mod 4$ since a is odd. Since $b-5a$ and $b-9a$ are congruent to $b-a \mod 4$ we have that $v_2(b-a) = v_2(b-5a) = v_2(b-9a) = 1$. Therefore

$$\begin{aligned} v_2(\gamma_T) &= 6 + 2v_2((b-9a)\,(b-3a)\,(3a+b)) + 6v_2((b-5a)\,(b-a)) \\ &= 20 + 2v_2((b-3a)\,(3a+b)) \end{aligned}$$

Since $(b-3a)\,(3a+b)$ is a difference of odd squares, it follows that it is divisible by 8 which implies that $v_2(\gamma_T) \geq 26$.

As before, let $\alpha_T = PQ$ where P is the factor of degree 2 and Q is the factor of degree 6. Then

$$\begin{aligned} P &\equiv 4a^2 \mod 8 = 4 \mod 8 \\ Q &\equiv 64a^2 \mod 128 = 64 \mod 128. \end{aligned}$$

Therefore $v_2(\alpha_T) = 8$ and so by Lemma 5.21, $v_2(\beta_T) = 24$. In particular, $4^{-4}\alpha_T$ and $4^{-6}\beta_T$ are odd integers and they are the invariants c_4 and c_6, respectively of the

Weierstrass model of E_{u_T} for $u_T = 4$. We claim that E_{u_T} is an integral Weierstrass model. Indeed,

$$a_1 = 19a^2 - 2ab - b^2 = 20a^2 - 16k^2 \equiv 0 \mod 4$$
$$a_2 = a\,(b-a)^2\,(b-5a) \equiv 0 \mod 8$$
$$a_3 = a\,(b-5a)\,(b-3a)\,(b+3a)\,(b-a)^2 \equiv 0 \mod 64.$$

This shows that E_{u_T} is a global minimal model for E_T if $v_2(a+b) \geq 2$. This is the converse of (ii).

Since the converse of (i), (ii), and (iii) exhaust all possibilities for a and b, we get that the forward implication in each holds as well, which concludes the proof. ■

5.4.12 Proof of Theorem 5.14 for $T = C_2 \times C_8$

Theorem 5.14 for $T = C_2 \times C_8$. The minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T \in \{1, 16, 64\}$. Moreover,

(i) $u_T = 1$ if and only if a is odd;

(ii) $u_T = 16$ if and only if $v_2(a) = 1$;

(iii) $u_T = 64$ if and only if $v_2(a) \geq 2$.

Proof Let $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 + u_T^2 s_T x + w_T$ be an admissible change of variables between E_T and a global minimal model of E_T. Since E_T is given by an integral Weierstrass model, we have by Lemma 2.4 that $u_T, s_T, r_T, w_T \in \mathbb{Z}$ and moreover, $u_T^4 | \alpha_T$ and $u_T^6 | \beta_T$. In particular, u_T^4 divides $\gcd(\alpha_T, \beta_T)$. Since a and b are relatively prime, we have that for a fixed positive integer k, there are integers r and s such that $ra^k + sb^k = 1$ and so by Lemma 5.10, $\gcd(\alpha_T, \beta_T)$ divides 2^{12}.

Observe that $\alpha_T \equiv a^{16} \mod 2$. Therefore α_T is even if and only if a is even.

(i) Suppose a is odd so that α_T is odd. Since u_T divides 2^{12}, it follows that E_T is a global minimal model for E_T if a is odd. This shows the converse of (i).

For (ii) and (iii) we will consider the admissible change of variables $x \longmapsto u_T^2 x$ and $y \longmapsto u_T^3 y$ which gives a $\mathbb{Q}$-isomorphism between E_T and the elliptic curve

$$\begin{aligned}
&E_{u_T} : y^2 - \frac{a^4}{u_T}xy + \frac{8a_3}{u_T^3}y = x^3 - \frac{4a_2}{u_T^2}x^2 \text{ where} \\
&a_1 = a^4 + 8a^3b + 24a^2b^2 - 64b^4 \\
&a_2 = ab^2\left(a+2b\right)\left(a+4b\right)^2\left(a^2+4ab+8b^2\right) \\
&a_3 = ab^3\left(a+2b\right)\left(a+4b\right)^3\left(a^2-8b^2\right)\left(a^2+4ab+8b^2\right)
\end{aligned}$$

We will prove the converse of (ii) and (iii) by demonstrating that E_{u_T} is an integral Weierstrass model under the assumptions on a. Note that if a is even, then

$$\begin{aligned}
v_2(\gamma_T) = 8 + 8v_2(a\left(a+2b\right)\left(a+4b\right)) + 2v_2\left(\left(a^2-8b^2\right)\left(a^2+8ab+8b^2\right)\right) \\
+ 4v_2\left(a^2+4ab+8b^2\right)
\end{aligned} \tag{5.16}$$

(ii) Suppose $v_2(a) = 1$. Then

$$\begin{aligned}
4v_2\left(a^2+4ab+8b^2\right) &= 8 \\
2v_2\left(\left(a^2-8b^2\right)\left(a^2+8ab+8b^2\right)\right) &= 8 \\
8v_2(a\left(a+4b\right)) &= 16 \\
8v_2(a+2b) &\geq 16.
\end{aligned}$$

Therefore $v_2(\gamma_T) \geq 56$. Next, we observe that

$$\alpha_T \equiv 2^{16}k^{16} \mod 2^{17}.$$

In particular, $v_2(\alpha_T) = 16$ since k is odd. By Lemma 5.21, $v_2(\beta_T) = 24$. In particular, $16^{-4}\alpha_T$ and $16^{-6}\beta_T$ are odd integers and they are the invariants c_4 and c_6, respectively of the Weierstrass model for E_{u_T} with $u_T = 16$. We claim that E_{u_T} is an integral Weierstrass model. By inspection, $v_2(a_1) \geq 4$, $v_2(a_2) \geq 7$, and $v_2(a_3) \geq 10$. Therefore E_{u_T} is an integral Weierstrass model and therefore it is a global minimal model for E_T when $v_2(a) = 1$. This shows the converse of (ii).

(iii) Suppose $v_2(a) \geq 2$ so that $a = 4k$ for some integer k. Observe that $v_2(\gamma_T) \geq 72$ since

$$\begin{aligned} 12 &= 2v_2\left(\left(a^2 - 8b^2\right)\left(a^2 + 8ab + 8b^2\right)\right) \\ 12 &= 4v_2\left(a^2 + 4ab + 8b^2\right) \\ 24 &= 8v_2(a\,(a + 2b)) \\ 16 &\leq 8v_2(a + 4b) \end{aligned}$$

Next, we compute $\alpha_T \equiv 2^{24}b^{16} \mod 2^{25}$ and so $v_2(\alpha_T) = 24$. By Lemma 5.21 we conclude that $v_2(\beta_T) = 36$. In particular, $2^{-24}\alpha_T$ and $2^{-36}\beta_T$ are odd integers and they are the invariants c_4 and c_6, respectively of the Weierstrass model for E_{u_T} with $u_T = 64$. By inspection, we observe that $v_2(a_1) \geq 6,\ v_2(a_2) \geq 10$, and $v_2(a_3) \geq 15$. Therefore E_{u_T} is an integral Weierstrass model and therefore it is a global minimal model for E_T when $v_2(a) \geq 2$. This shows the converse of (iii).

Since the converse of (i), (ii), and (iii) exhaust all possibilities for a and b, we get that the forward implication in each holds as well, which concludes the proof. ■

5.4.13 Corollaries and Examples

The following two statements were proven in the proof of Theorem 5.14.

Corollary 5.22 *Let c_4 and c_6 be the invariants associated to a global minimal model of E_T. Then c_4 and c_6 are always odd if $T = C_{10}, C_{12}, C_2 \times C_6, C_2 \times C_8$.*

Corollary 5.23 *Let E be a rational elliptic curve with discriminant Δ containing a point of order $3, 5,$ or 7. Then Δ is minimal if and only if $v_p(\Delta) < 12$ or $v_p(c_4) < 4$ for all primes p.*

For an arbitrary elliptic curve, this is only true for primes $p \geq 5$ [4, Remark VII.1.1].

Example 5.24 *The elliptic curve*

$$E : y^2 = x^3 - 1900650154752x + 990015042347311104$$

has torsion subgroup $E(\mathbb{Q})_{tors} \cong C_2 \times C_4$. *The point* $P = (222288, 760596480)$ *has order* 4 *and placing* E *in Tate normal form with respect to* P *results in the elliptic curve*

$$E_{TNF} : y^2 + xy - \frac{4585}{36864}y = x^3 - \frac{4585}{36864}x^2.$$

Now consider the elliptic curve $\mathcal{X}_t(C_4)$. *It is clear if* $t = \frac{4585}{36864}$, *then* $\mathcal{X}_t(C_4)$ *is* E_{TNF}. *Therefore* E *is isomorphic over* $\mathbb{Q}$ *to* $E_{C_4}(36864, 4585)$. *Moreover,* $36864 = 2^{12} \cdot 3^2$ *and* $4585 \equiv 1 \mod 4$. *In particular, in the notation of Theorem 5.14, we have that* $c = 2^6 \cdot 3$ *and hence the minimal discriminant of* E *and associated invariants* c_4 *and* c_6 *are*

$$\begin{aligned}
\Delta_E^{min} &= \left(2^6 \cdot 3\right)^{-12} \Delta_4(36864, 4585) = 2^{16} \cdot 3^2 \cdot 5^4 \cdot 7^4 \cdot 83^2 \cdot 131^4 \\
c_4 &= \left(2^6 \cdot 3\right)^{-4} \alpha_4(36864, 4585) = 2^4 \cdot 274978321 \\
c_6 &= \left(2^6 \cdot 3\right)^{-4} \beta_4(36864, 4585) = -2^6 \cdot 23 \cdot 29 \cdot 47 \cdot 313 \cdot 317 \cdot 1439.
\end{aligned}$$

5.5 Necessary and Sufficient Conditions for Semistability of E_T

Theorem 5.25 *Assume the statement of Theorem 5.14. Assume further that the* j*-invariant of* E_T *is not equal to* 0 *or* 1728. *Then* E_T *with* $T = C_2 \times C_8$ *is semistable and* E_T *is semistable if and only if*

Table 5.2.: Semistablity of E_T

Necessary and Sufficient Conditions for Semistablity of E_T	T
$\gcd(a, bd) = 1$ *and either* $u_T = 4$ *or* $v_2(b) \geq 3$ *with* $a \equiv -1 \mod 4$.	C_2
a *is a cube and* 3 *does not divide* a.	C_3
a *is a square and either* a *is odd or* $v_2(a) \geq 8$ *is even with* $b \equiv 3 \mod 4$.	C_4
$v_5(a + 3b) = 0$.	C_5
$v_3(a) = 0$ *and* $v_2(a + b) \neq 1, 2$.	C_6
$v_7(a + 4b) = 0$.	C_7

continued on next page

Table 5.2.: continued

Necessary and Sufficient Conditions for Semistablity of E_T	T
$v_2(a) \leq 1$.	C_8
$v_3(a+b) = 0$.	C_9
$v_5(a+b) = 0$.	C_{10}
$v_3(a) = 0$.	C_{12}
$d = 1$ *and* $v_2(a) \geq 4$ *with* $b \equiv 1 \mod 4$.	$C_2 \times C_2$
either a *is odd or* $v_2(a) = 2$ *with* $v_2(a+4b) \geq 4$.	$C_2 \times C_4$
$v_3(b) = 0$.	$C_2 \times C_6$

In particular, if for $T = C_2 \times C_6$ *and* $T = C_N$ *where* $N = 5, 7, 8, 9, 10, 12$*, the equivalence above is not satisfied, then* E_T *has additive reduction at* p *where* p *is the prime that appears in the valuation* v_p *above. For the remaining* T *we have the following necessary and sufficient conditions for additive reduction to occur at a prime* p*:*

($T = C_2$*)* E_T *has additive reduction at each prime* p *dividing* $\gcd(a, bd)$*. In addition,* E_T *has additive reduction at* $p = 2$ *if and only if* $u_T = 1$ *or* $v_2\left(b^2 d - a^2\right) \geq 4$ *with* $v_2(a) = v_2(b) = 1$ *and* $d \equiv 1 \mod 4$*.*

($T = C_3$*)* E_T *has additive reduction at all primes dividing* de*. In addition,* E_T *has additive reduction at* 3 *if and only if* $v_3(a) > 0$*.*

($T = C_4$*)* E_T *has additive reduction at all primes dividing* d*. In addition,* E_T *has additive reduction at* 2 *if and only if* a *is even and* $u_T = c$*.*

($T = C_6$*)* E_T *has additive reduction at* 2 *(resp. at* 3*) if and only if* $v_2(a+b) = 1, 2$ *(resp.* $v_3(a) > 0$*).*

($T = C_2 \times C_2$*)* E_T *has additive reduction at all primes dividing* d*. In addition,* E_T *has additive reduction at* 2 *if and only if* ad *is even with* $u_T = 1$*.*

($T = C_2 \times C_4$) *E_T has additive reduction at 2 if and only if $v_2(a+4b) < 4$ with a even.*

Proof We first consider the case when $T \neq C_2, C_3, C_4$, or $C_2 \times C_2$. For these T, let S be the set of primes at which E_T can have additive reduction. By Theorem 5.11, we have:

T	C_5	C_7	C_8	C_9	C_{10}	C_{12}	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
S	$\{5\}$	$\{7\}$	$\{2\}$	$\{3\}$	$\{5\}$	$\{2,3\}$	$\{2\}$	$\{2,3\}$	$\{2\}$

(5.17)

Let u_T be as given in Theorem 5.14. Then the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ and the invariant c_4 associated to a global minimal model of E_T is $u_T^{-4}\alpha_T$. In particular, E_T has additive reduction at a prime p if and only if p divides both $u_T^{-4}\alpha_T$ and $u_T^{-12}\gamma_T$. In what follows we will proceed by cases and reduce $u_T^{-4}\alpha_T$ and $u_T^{-12}\gamma_T$ modulo p for $p \in S$ where S is as given in (5.17).

Suppose $T = C_5$. Then $u_T = 1$ and we verify that

$$\alpha_T \equiv (a+3b)^4 \mod 5 \qquad \text{and} \qquad \gamma_T \equiv 4a^5b^5\,(a+3b)^2 \mod 5.$$

Therefore E_T has additive reduction at 5 if and only if 5 divides $a+3b$.

Suppose $T = C_6$. By Theorem 5.14, u_T is either 1 or 2. Note that $v_3(\alpha_T) = v_3\left(u_T^{-4}\alpha_T\right)$ and $v_3(\gamma_T) = v_3\left(u_T^{-12}\gamma_T\right)$. Therefore E_T has additive reduction at 3 if and only if 3 divides a since

$$\alpha_T \equiv a^4 \mod 3 \qquad \text{and} \qquad \gamma_T \equiv a^3b^6\,(a+b)\left(a^2-ab+b^2\right) \mod 3.$$

It remains to verify that additive reduction occurs at 2 if and only if $v_2(a+b) = 1, 2$.

Case I. Suppose $u_T = 1$. Then $v_2(a+b) < 3$ and we have that

$$\alpha_T \equiv (a+b)^4 \mod 2 \qquad \text{and} \qquad \gamma_T \equiv a^2b^6\,(a+b)^6 \mod 2$$

Since a and b are relatively prime, we conclude that E_T with $u_T = 1$ has additive reduction at 2 if and only if $a+b$ is even. Similarly, E_T with $u_T = 1$ has additive reduction at 3 if and only if 3 divides a.

Case II. Suppose $u_T = 2$ so that $v_2(a+b) \geq 3$. Write $a+b = 8k$ for some integer k. Then $b = 8k - a$ and we have the reduction:

$$u_T^{-4}\alpha_T \equiv a^4 \mod 2 \qquad \text{and} \qquad u_T^{-12}\gamma_T \equiv a^8k^3\left(a+k\right) \mod 2$$

Since $a+b = 8k$, a is odd and therefore E_T with $u_T = 2$ is semistable at 2.

Therefore E_T has additive reduction at 2 if and only if $v_2(a+b) = 1, 2$.

Suppose $T = C_7$. Then $u_T = 1$ and we verify that

$$\alpha_T \equiv \left(a+4b\right)\left(a+2b\right)^7 \mod 7 \qquad \text{and} \qquad \gamma_T \equiv 6a^7b^7\left(a+4b\right)^3\left(a-b\right)^7 \mod 7.$$

It is clear that E_T has additive reduction at 7 if 7 divides $a+4b$. Suppose instead that $a+2b$ is divisible by 7 and $a+4b$ is not divisible by 7. Since a and b are relatively prime, it follows that neither a nor b is divisible by 7. Next, $a - b \equiv -3b \mod 7$ and so it is not divisible by 7. Therefore E_T has additive reduction at 7 if and only if 7 divides $a+4b$.

Suppose $T = C_8$. Then u_T is either 1 or 2.

Case I. Suppose $u_T = 1$ so that $v_2(a) \neq 1$. Then

$$\alpha_T \equiv a^8 \mod 2 \qquad \text{and} \qquad \gamma_T \equiv a^8b^8\left(a+b\right)^8 \mod 2$$

and so E_T has additive reduction at 2 if $v_2(a) > 1$.

Case II. Suppose $u_T = 2$ so that $v_2(a) = 1$. Then $u_T^{-4}\alpha_T \equiv b^8 \mod 2$ and since a is even, b is odd. In particular, E_T is semistable at 2.

We conclude that E_T has additive reduction at 2 if and only if $v_2(a) > 1$.

Suppose $T = C_9$. Then $u_T = 1$ and we verify that

$$\alpha_T = \left(a+b\right)^{12} \mod 3 \qquad \text{and} \qquad \gamma = 2a^9b^9\left(a^2-b^2\right)^9 \mod 3.$$

Therefore E_T has additive reduction at 3 if and only if 3 divides $a+b$.

Suppose $T = C_{10}$. Then u_T is either 1 or 2. Since $v_5(\alpha_T) = v_5\big(u_T^{-4}\alpha_T\big)$ and $v_5(\gamma_T) = v_5\big(u_T^{-12}\gamma_T\big)$, it suffices to consider α_T and γ_T modulo 5. To this end,

$$\alpha_T \equiv \left(a+b\right)^{12} \mod 5 \qquad \text{and} \qquad \gamma_T \equiv a^5b^{10}\left(a+b\right)^6\left(a^{15}+a^{10}b^5+3b^{15}\right) \mod 5.$$

Therefore E_T has additive reduction at 5 if and only if 5 divides $a+b$.

Suppose $T = C_{12}$. Then u_T is either 1 or 2. By Corollary 5.22, $u_T^{-4}\alpha_T$ is always odd and therefore E_T is semistable at 2. Since $v_3(\alpha_T) = v_3\big(u_T^{-4}\alpha_T\big)$ and $v_3(\gamma_T) = v_3\big(u_T^{-12}\gamma_T\big)$, we verify that $\alpha_T \equiv a^{16} \mod 3$. Hence, α_T is divisible by 3 if and only if a is divisible by 3. In particular, if a is divisible by 3, then 3 divides γ_T. Thus E_T has additive reduction at 3 if and only if 3 divides a.

Suppose $T = C_2 \times C_4$. Then u_T is either $1, 2$, or 4.

Case I. Suppose $u_T = 1$ so that $v_2(a) \leq 1$. Then α_T is even if and only if $v_2(a) = 1$ since $\alpha_T \equiv a^4 \mod 2$. But if a is even, then γ_T is even and so we attain that E_T with $u_T = 1$ has additive reduction at 2 if and only if $v_2(a) = 1$.

Case II. Suppose $u_T = 2$ so that $v_2(a) \geq 2$ with $v_2(a+4b) < 4$. Write $a = 4k$ for some integer k. Then $u_T^{-4}\alpha_T$ and $u_T^{-12}\gamma_T$ are divisible by 2 and so we have that E_T with $u_T = 2$ always has additive reduction at 2.

Case III. Suppose $u_T = 4$ so that $v_2(a) = 2$ with $v_2(a+4b) \geq 4$. Write $a + 4b = 16k$ for some integer k. Thus $a = 16k - 4b$ and we have $u_T^{-4}\alpha_T \equiv b^4 \mod 2$. Since b is odd, it follows that E_T with $u_T = 4$ is semistable at 2.

We conclude that E_T has additive reduction at 2 if and only if a is even and $v_2(a+4b) < 4$.

Suppose $T = C_2 \times C_6$. Then u_T is either $1, 4$, or 16. By Corollary 5.22, $u_T^{-4}\alpha_T$ is always odd, and so E_T is semistable at 2. Since $v_3(\alpha_T) = v_3\big(u_T^{-4}\alpha_T\big)$ and $v_3(\gamma_T) = v_3\big(u_T^{-12}\gamma_T\big)$, we verify that $\alpha_T \equiv b^8 \mod 3$. Hence α_T is divisible by 3 if and only if 3 divides b. But if this is the case, 3 also divides γ_T. Thus E_T has additive reduction at 3 if and only if 3 divides b.

Suppose $T = C_2 \times C_8$. Then u_T is either $1, 16$, or 64. By Corollary 5.22, $u_T^{-4}\alpha_T$ is always odd, and so E_T is semistable at all primes.

It remains to show the Theorem for $T = C_2, C_3, C_4, C_2 \times C_2$.

Suppose $T = C_2$. Let $\Delta = u_T^{-12}\gamma_T$ be the minimal discriminant of E_T where u_T is one of the possibilities allowed by Theorem 5.14. Then $c_4 = u_T^{-4}\alpha_T$ is the invariant associated with a global minimal model of E_T. In particular, E has additive reduction at a prime p if and only if p divides $\gcd(\Delta, c_4)$. Since $\gcd(\Delta, c_4)$ divides $\gcd(\alpha_T, \gamma_T)$, it follows that $\gcd(\Delta, c_4)$ divides $2^{10}\gcd(a^6, b^6d^3)$ by Lemma 5.10. In particular, E_T has additive reduction at an odd prime p if and only if p divides a and bd. It remains to check when additive reduction occurs at $p = 2$.

Case I. Suppose $u_T = 1$. Then E_T always has additive reduction at 2.

Case II. Suppose $u_T = 2$. Then $v_2\left(b^2d - a^2\right) \geq 2$ with $v_2(a) = v_2(b) = 1$ and $d \equiv 1 \mod 4$ or $v_2(b) \geq 3$ and $a \equiv -1 \mod 4$.

Subcase I. First suppose $v_2\left(b^2d - a^2\right) \geq 4$ with $v_2(a) = v_2(b) = 1$ and $d \equiv 1 \mod 4$. Write $a = 2\hat{a},\ b = 2\hat{a}$, and $b^2d - a^2 = 16k$ for some odd integers $\hat{a}, \hat{b}$, and an integer k. In particular, $a^2 = b^2d - 16k$ and so

$$u_T^{-4}\alpha_T = 4b^2d - 16k \qquad \text{and} \qquad u_T^{-12}\gamma_T = \frac{1}{64}b^2d\left(16k\right)^2 = 4b^2dk^2.$$

In particular, E_T always has additive reduction at 2.

Subcase II. Suppose $v_2(b) \geq 3$ and $a \equiv -1 \mod 4$ and write $b = 8\hat{b}$. Then

$$u_T^{-4}\alpha_T = 192\hat{b}^2d + a^2 \qquad \text{and} \qquad u_T^{-12}\gamma_T = \hat{b}^2d\left(64\hat{b}^2d - a^2\right)^2.$$

Since $a \equiv -1 \mod 4$, $u_T^{-4}\alpha_T$ is odd and hence E_T is semistable at 2.

Case III. Suppose $u_T = 4$ so that $v_2\left(b^2d - a^2\right) \geq 8$ with $v_2(a) = v_2(b) = 1$ and $2^{-1}a \equiv 1 \mod 4$. Write $b = 2\hat{b}$ for some odd integer $\hat{b}$. Then $4\hat{b}^2d - a^2 = 2^8k$ for some integer k. Then $a^2 = 4\hat{b}^2d - 2^8k$ and

$$u_T^{-4}\alpha_T = \frac{1}{16}\left(16\hat{b}^2d - 2^8k\right) = \hat{b}^2d - 16k \qquad \text{and} \qquad u_T^{-12}\gamma_T = \frac{1}{2^{18}}4\hat{b}^2d\left(2^8k\right)^2 = \hat{b}^2dk^2.$$

Since d is odd under these assumptions, we conclude that E_T is semistable at 2.

Suppose $T = C_3$. Write $a = c^3d^2e$ with d and e relatively prime positive squarefree integers. By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ with $u_T = c^2d$. In particular,

$$u_T^{-4}\alpha_T = cd^2e^3\left(a - 24b\right) \qquad \text{and} \qquad u_T^{-12}\gamma_T = d^4e^8b^3\left(a - 27b\right).$$

In particular, E_T has additive reduction at all primes dividing de. By Lemma 5.10, $\gcd(\alpha_T, \gamma_T)$ divides $2^{15}3^6a^3$. Now suppose a is a cube so that $de = 1$. Then $a = c^3$ and we observe that $u_T^{-12}\gamma_T \equiv -27b^4 \mod c$. Since b is relatively prime to c, it follows that the only prime dividing a at which E_T has additive reduction is 3. We now consider the cases of additive reduction at 2 or 3.

Observe that

$$u_T^{-4}\alpha_T \equiv acd^2e^3 \mod 2 \qquad \text{and} \qquad u_T^{-12}\gamma_T \equiv d^4e^8b^3\left(a+b\right) \mod 2.$$

Therefore $u_T^{-4}\alpha_T$ is even if and only if 2 divides a. Under this assumption, b is odd and therefore $u_T^{-12}\gamma_T$ is even if and only if de is even. But we have already shown that E_T has additive reduction at all primes dividing de.

Next, we compute

$$u_T^{-4}\alpha_T \equiv acd^2e^3 \mod 3 \qquad \text{and} \qquad u_T^{-12}\gamma_T \equiv ad^4e^8b^3 \mod 3.$$

Therefore $u_T^{-4}\alpha_T$ is divisible by 3 if and only if 3 divides a. But if this is so, we conclude that $u_T^{-12}\gamma_T$ is divisible by 3 and therefore E_T has additive reduction at 3 if and only if 3 divides a.

Suppose $T = C_4$. Write $a = c^2d$ for d a positive squarefree integer. Then u_T is either c or $2c$. Then

$$c^{-4}\alpha_T = d^2\left(a^2+16ab+16b^2\right) \qquad \text{and} \qquad c^{-12}\gamma_T = b^4c^2d^7\left(a+16b\right).$$

By Lemma 5.10, $\gcd(\alpha_T, \gamma_T)$ divides $2^{12}a^2$. Therefore, E_T has additive reduction at an odd prime p if and only if p divides d. Next, observe that

$$c^{-4}\alpha_T \equiv a^2d^2 \mod 2 \qquad \text{and} \qquad c^{-12}\gamma_T \equiv ab^4c^2d^7 \mod 2.$$

Then $c^{-4}\alpha_T$ is even if and only if a is even. In particular, E_T with $u_T = c$ has additive reduction at 2 if and only if a is even.

Now suppose $u_T = 2c$ so that $v_2(a) \geq 8$ is even with $bd \equiv 3 \mod 4$. Then $c = 2^4k$ for some integer k and so

$$\left(2c\right)^{-4}\alpha_T = b^2d^2 + 256bd^3k^2 + 4096d^4k^4 \equiv 1 \mod 4$$

since bd is odd. Hence E_T is semistable at 2 if $u_T = 2c$.

We conclude that E_T has additive reduction at all primes dividing d and moreover, E_T has additive reduction at 2 if and only if a is even and $u_T = c$.

Lastly, suppose $T = C_2 \times C_2$. By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. By Lemma 5.10, $\gcd(\alpha_T, \gamma_T)$ divides $2^4 d^6$. Since d divides both α_T and γ_T, we conclude that E_T has additive reduction at an odd prime p if and only if p divides d. Moreover, if $u_T = 1$, both α_T and γ_T are even and hence E_T has additive reduction at 2.

So suppose $u_T = 2$ so that $v_2(a) \geq 4$ and $bd \equiv 1 \mod 4$. Then

$$u_T^{-4}\alpha_T = d^2\left(a^2 - ab + b^2\right) \not\equiv 1 \mod 2.$$

Therefore E_T is semistable at 2.

Thus, E_T has additive reduction at 2 if and only if ad is even with $u_T = 1$ and E_T has additive reduction at an odd prime p if and only if p divides d. ■

Remark If the j-invariant of E_T is 0 or 1728, then Theorem 5.14 classified the minimal discriminants of these elliptic curves. From the identity $1728\Delta_{E_T}^{\min} = c_4^3 - c_6^2$ we conclude that these elliptic curves have additive reduction at all primes dividing the minimal discriminant $\Delta_{E_T}^{\min}$.

Corollary 5.26 *Let E be a rational elliptic curve. If E has additive reduction at three or more primes, then $E(\mathbb{Q})_{tors} \cong C_N$ for $N = 1, \ldots, 4$ or $E(\mathbb{Q})_{tors} \cong C_2 \times C_2$. If E has additive reduction at two primes, then $E(\mathbb{Q})_{tors}$ can be embedded into C_4, C_6, or $C_2 \times C_2$.*

Proof The elliptic curve $y^2 = x^3 + 30$ has additive reduction at the primes $2, 3$, and 5 and has trivial torsion subgroup. The Corollary now holds for the remaining T by Theorem 5.25. ■

Remark The previous corollary does not hold in arbitrary number fields. Indeed, suppose E is an elliptic curve over a number field K with a K-torsion point of order n. If E has additive reduction at two places with distinct residue characteristics, then n divides 12 by Theorem 5.9. In fact, Flexor and Oesterlé proved a stronger statement, namely that under these assumption the order of $E(K)_{\text{tors}}$ divides 12. They also showed that this divisibility condition is sharp since the elliptic curve $y^2 - 2y = x^3$ over $K = \mathbb{Q}(\sqrt{-3})$ has additive reduction at two places and their residue characteristic is 2 and 3. Moreover, $E(K)_{\text{tors}} \cong C_2 \times C_6$.

Example 5.27 *Consider the elliptic curve E given by the Weierstrass equation*

$$E : y^2 = x^3 - 19057987954261048752x + 31955359661403338940204703104.$$

The point $P = (2365794828, 10458914400000)$ is a torsion point of order 12 on E. Placing E in Tate normal form with respect to P yields the Weierstrass equation

$$E_{TNF} : y^2 + \frac{6021}{125}xy - \frac{430408}{1875}y = x^3 - \frac{430408}{1875}x^2.$$

In particular, E_{TNF} is equal to $\mathcal{X}_t(C_{12})$ for some t. Therefore, we solve for t and attain

$$\frac{12t^6 - 30t^5 + 34t^4 - 21t^3 + 7t^2 - t}{(t-1)^4} = \frac{430408}{1875} \text{ and } 1 - \frac{-6t^4 + 9t^3 - 5t^2 + t}{(t-1)^3} = \frac{6021}{125}.$$

Observe that the common rational solution to both equations is $t = \frac{11}{6}$ and so E is isomorphic over $\mathbb{Q}$ to $E_T(6, 11)$ for $T = C_{12}$. Since $v_3(6) > 0$, we have by Theorem 5.25 that E has additive reduction at 3. Moreover, its minimal discriminant is

$$\Delta_{12}^{min} = 2^{-12}\gamma_T(6, 11) = 2^{18} \cdot 3^7 \cdot 5^{12} \cdot 11^{12} \cdot 61 \cdot 67^4 \cdot 73^3.$$

since 6 is even. In particular, a global minimal model of E has associated invariants

$$c_4 = 2^{-4}\alpha_T(6, 11) = 3^2 \cdot 23 \cdot 107 \cdot 227 \cdot 27361 \cdot 320687$$
$$c_6 = 2^{-6}\beta_T(6, 11) = -3^3 \cdot 503 \cdot 769 \cdot 47221 \cdot 18748939480561.$$

6. LOWER BOUNDS ON THE MODIFIED SZPIRO RATIO

Let T be one of the fourteen non-trivial torsion subgroups allowed by Theorem 2.1 and suppose E is a rational elliptic curve with $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$. In the previous chapter, we saw that for $T \neq C_2, C_2 \times C_2, C_3$, there exist relatively prime integers a and b such that E is $\mathbb{Q}$-isomorphic to $E_T = E_T(a,b)$ where E_T is as defined in Table D.1. The same holds for $T = C_3$, so long as the j-invariant of E is non-zero. If instead, E had j-invariant equal to 0, then E is parametrized by the one-parameter family of elliptic curves $E_T = E_T(a)$ where $T = C_3^0$.

For $T = C_2, C_2 \times C_2$ we have similar parameterizations, namely E is $\mathbb{Q}$-isomorphic to $E_T = E_T(a,b,d)$ for some integers a, b, d. We note that in order for E to be $\mathbb{Q}$-isomorphic to E_T for $T = C_2$, E must not have full 2-torsion as demonstrated in Lemma 5.2.

In particular, a study of the elliptic curves E_T is equivalent to a study of all rational elliptic curves with non-trivial torsion. Moreover, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where γ_T is as defined in Table D.4 and u_T is an integer. By Theorem 5.14, we have necessary and sufficient conditions on a and b to determine u_T. In this chapter, we use Theorem 5.14 to explicitly construct the naive height of E_T. Recall that for a rational elliptic curve E, the naive height $h_{\text{naive}}(E)$ of E is defined as

$$h_{\text{naive}}(E) = \frac{1}{12} \log \max\{ c_4^3 , c_6^2$$

where c_4 and c_6 are the invariants associated to a global minimal model of E. By Theorem 5.14, we have that

$$h_{\text{naive}}(E_T) = \frac{1}{12} \log \left(u_T^{-12} \max\{ \alpha_T^3 , \beta_T^2 \} \right) \tag{6.1}$$

where α_T and β_T are as defined in Tables D.2 and D.3, respectively. Our first result is that for $T \neq C_2, C_2 \times C_2$, we can define an explicit function which coincides with the naive height of E_T.

In section 6.3 we revisit the modified Szpiro conjecture and state the main theorem of the chapter. Recall that the modified Szpiro ratio $\sigma_m(E)$ of a rational elliptic curve E is defined as

$$\sigma_m(E) = \frac{\log \max\{|c_4^3|, c_6^2\}}{\log N_E}$$

where N_E is the conductor of E and c_4 and c_6 are the invariants associated to a global minimal model of E. Our main result states that if E is a rational elliptic curve, then there is a lower bound on the modified Szpiro ratio which depends only on the torsion subgroup of E.

In section 6.4, via Tate's Algorithm, we prove stricter upper bounds on the exponent of the conductor of a rational elliptic curve at 2 and 3. These results will allow us to bound the conductor of rational elliptic curves with non-trivial torsion in Section 6.5. We finish in Section 6.6 with the proof of the main theorem.

6.1 Results on Polynomials

Let T be one of the fourteen non-trivial possible torsion subgroups allowed by Theorem 2.1. Let $\alpha_T, \beta_T, \gamma_T$, and δ_T be as defined in Tables D.2, D.3, D.4, and 6.2, respectively.

For $T \neq C_2, C_2 \times C_2$ let

$$m_T = \begin{cases} 12 & \text{if } T = C_3, C_4, C_5, C_6, C_2 \times C_4 \\ 24 & \text{if } T = C_7, C_8, C_2 \times C_6 \\ 36 & \text{if } T = C_9, C_{10} \\ 48 & \text{if } T = C_{12}, C_2 \times C_8. \end{cases} \tag{6.2}$$

It is then verified that we have the following identities:

$$\alpha_T(a,b)^3 = a^{m_T} \alpha_T\left(1, \frac{b}{a}\right)^3 \qquad \beta_T(a,b)^2 = a_T^{m_T} \beta_T\left(1, \frac{b}{a}\right)^2 \tag{6.3}$$

Assume further that $T \neq C_2 \times C_{2M}$ where $M = 2, 3, 4$ and consider $\alpha_T(1, x)$ and $\beta_T(1, x)$ as functions from $\mathbb{R} \to \mathbb{R}$. To this end, set

$$S_T = \{\theta \in \mathbb{R} \mid \ \alpha_T(1,\theta)^3 \ - \beta_T(1,\theta)^2 = 0 \ \ .$$

Now write $S_T = \{\theta_1, \theta_2, \ldots, \theta_n\}$ where $\theta_j < \theta_k$ if $j < k$.

Table 6.1, with a few exception, lists the approximate value up to four decimal places of the θ_j's. For the exceptions, Table 6.1 lists the exact value of θ_j. The following three results are easily verified via compute algebra system:

Lemma 6.1 *For $T = C_N$ with $N \geq 3$, let θ_j be as given in Table 6.1. Then the function $|\alpha_T(1,x)|^3 - \beta_T(1,x)^2$ is nonnegative on the interval I_T where*

$$I_T = \begin{cases} [\theta_1,\theta_2] \cup [\theta_3,\theta_4] & \text{if } T = C_3 \\ [\theta_1,\theta_2] \cup [\theta_3,\infty) & \text{if } T = C_4 \\ [\theta_1,\theta_2] \cup [\theta_3,\theta_4] \cup [\theta_5,\theta_6] \cup [\theta_7,\infty) & \text{if } T = C_5 \\ (-\infty,\theta_1] \cup [\theta_2,\theta_3] \cup [\theta_4,\infty) & \text{if } T = C_6 \\ [\theta_1,\theta_2] \cup [\theta_3,\theta_4] \cup [\theta_5,\theta_6] \cup [\theta_7,\theta_8] \cup [\theta_9,\theta_{10}] \cup [\theta_{11},\infty) & \text{if } T = C_7, C_9 \\ (-\infty,\theta_2] \cup [\theta_3,\theta_4] \cup [\theta_6,\theta_7] \cup [\theta_8,\infty) & \text{if } T = C_8, C_{12} \\ [\theta_1,\theta_2] \cup [\theta_3,\theta_6] \cup [\theta_7,\theta_8] \cup [\theta_9,\infty) & \text{if } T = C_{10} \end{cases}$$

For $T = C_2 \times C_2$, let $m_T = 6$ and observe that

$$\alpha_T(a,b,d)^3 = (ad)^{m_T}\, \alpha_T\left(1, \frac{b}{a}, 1\right)^3 \qquad \beta_T(a,b,d)^2 = (ad)^{m_T}\, \beta_T\left(1, \frac{b}{a}, 1\right)^2. \tag{6.4}$$

Lemma 6.2 *For $T = C_2 \times C_2$, the function $|\alpha_T(1,x,1)|^3 - \beta_T(1,x,1)^2$ is nonnegative on $I_T = \mathbb{R}$.*

Table 6.1.: Roots of $\alpha_T(1,x)^3 - \beta_T(1,x)^2$

T	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7	θ_8	θ_9	θ_{10}	θ_{11}
C_7	-0.2802	-0.1846	0.1588	0	0.7811	0.8419	0.8629	1	4.5685	6.4180	7.2959
C_9	-0.3480	-0.2539	-0.2267	0	0.7418	0.7975	0.8152	1	3.8735	4.9381	5.4115
C_{10}	-0.4873	-0.3479	$\frac{1-\sqrt{5}}{4}$	0	$\frac{3-\sqrt{5}}{2}$	$\frac{1}{2}$	0.7532	0.7948	$\frac{1+\sqrt{5}}{4}$	1	$\frac{3+\sqrt{5}}{2}$
C_8	0	$\frac{2-\sqrt{2}}{4}$	0.1611	0.2062	$\frac{1}{2}$	0.7938	0.8389	$\frac{2+\sqrt{2}}{4}$	1		
C_{12}	0	$\frac{3-\sqrt{3}}{6}$	0.2231	0.2568	$\frac{1}{2}$	0.7432	0.7769	$\frac{3+\sqrt{3}}{6}$	1		
C_5	-0.2119	-0.1130	$\frac{11-5\sqrt{5}}{2}$	0	4.7183	8.8512	$\frac{11+5\sqrt{5}}{2}$				
C_6	-1	-0.1994	-0.1303	$-\frac{1}{9}$	0						
C_3	0	$\frac{1}{27}$	0.0654	0.4913							
C_4	-0.2246	-0.08660	$-\frac{1}{16}$	0							

For $T = C_2$, set

$$\hat{\alpha}_T(a, B) = 16\left(a^2 + 3B\right) \qquad \hat{\beta}_T(a, B) = -64a\left(-a^2 + 9B\right)$$

In particular, $\hat{\alpha}_T(a, B) = \alpha_T(a, b, d)$ and $\hat{\beta}(a, B) = \beta_T(a, b, d)$ with $B = b^2 d$. Let $m_T = 6$ and observe that

$$a^{m_T}\hat{\alpha}_T\left(1, \frac{B}{a^2}\right)^3 = \hat{\alpha}_T(a, B)^3 \qquad a^{m_T}\hat{\beta}_T\left(1, \frac{B}{a^2}\right)^2 = \hat{\beta}_T(a, B)^2 . \tag{6.5}$$

Then

$$\begin{aligned} S_T &= \left\{\theta \in \mathbb{R} \mid \hat{\alpha}_T(1, \theta)^3 - \hat{\beta}_T(1, \theta)^2 = 0\right\} \\ &= \{\theta_1, \theta_2, \theta_3\} \end{aligned}$$

where $\theta_1 \approx -4.0860$, $\theta_2 = 0$, and $\theta_3 = 1$.

Lemma 6.3 *For $T = C_2$, the function $|\hat{\alpha}_T(1, x)|^3 - \hat{\beta}_T(1, x)^2$ is nonnegative on the interval $I_T = (-\infty, \theta_1] \cup [0, \infty)$.*

6.2 Explicit Naive Height

In the following Proposition, let I_T^C denote the complement of I_T in $\mathbb{R}$.

Proposition 6.4 *Let c_4 and c_6 be the invariants associated to a global minimal model of E_T. Set*

$$A = \begin{cases} a^2 & \text{if } T = C_2 \\ a & \text{otherwise} \end{cases}, \qquad B = \begin{cases} b^2 d & \text{if } T = C_2 \\ b & \text{otherwise.} \end{cases},$$

and $I_T = \mathbb{R}$ for $T = C_2 \times C_{2M}$ for $M = 1, 2, 3, 4$. Then

$$\max\left\{\left|c_4^3\right|, c_6^2\right\} = \begin{cases} \left|c_4^3\right| & \text{if } \frac{B}{A} \in I_T \\ c_6^2 & \text{if } \frac{B}{A} \in I_T^C. \end{cases} \tag{6.6}$$

Proof By Theorem 5.14, $c_4 = u_T^{-4}\alpha_T$ and $c_6 = u_T^{-6}\beta_T$ where u_T is a positive integer uniquely determined by a and b. Hence

$$\max\left\{\left|c_4^3\right|, c_6^2\right\} = u_T^{-12}\max\left\{\left|\alpha_T^3\right|, \beta_T^2\right\} = u_T^{-12}a^{m_T}\max\left\{\left|\alpha_T\left(1, \frac{b}{a}\right)\right|^3, \beta_T\left(1, \frac{b}{a}\right)^2\right\}.$$

Now suppose $T = C_N$ where $N \geq 3$. Then

$$u_T^{-12} \max\{\alpha_T^3, \beta_T^2\} = u_T^{-12} a^{m_T} \max\left\{ \alpha_T\left(1, \frac{b}{a}\right)^3, \beta_T\left(1, \frac{b}{a}\right)^2 \right\}$$

by (6.3). By Lemma 6.1, $|\alpha_T(1,x)|^3 \geq \beta_T(1,x)^2$ if and only if $x \in I_T$, which gives (6.6).

For $T = C_2$, observe that

$$u_T^{-12} \max\{\alpha_T^3, \beta_T^2\} = u_T^{-12} a^{m_T} \max\left\{ \hat{\alpha}_T\left(1, \frac{B}{A}\right)^3, \hat{\beta}_T\left(1, \frac{B}{A}\right)^2 \right\}$$

by (6.5). By Lemma 6.3, $|\hat{\alpha}_T(1,x)|^3 \geq \hat{\beta}_T(1,x)^2$ if and only if $x \in I_T$, which gives (6.6).

Next, Suppose $T = C_2 \times C_2$. Then

$$u_T^{-12} \max\{\alpha_T^3, \beta_T^2\} = u_T^{-12} (ad)^{m_T} \max\left\{ \alpha_T\left(1, \frac{b}{a}, 1\right)^3, \beta_T\left(1, \frac{b}{a}, 1\right)^2 \right\}$$

by (6.4). By Lemma 6.2, $|\alpha_T(1,x,1)|^3 \geq \beta_T(1,x,1)^2$ for all $x \in I_T = \mathbb{R}$, which gives (6.6). In particular, $\max\{|c_4^3|, c_6^2\} = |c_4^3|$.

Lastly, assume $T = C_2 \times C_{2M}$ for $M = 2, 3, 4$. Since $C_2 \times C_2 \hookrightarrow E_T$, it follows that E_T is $\mathbb{Q}$-isomorphic to $E_{C_2 \times C_2}(a,b,d)$ for some integers a, b, d. By the above, we conclude that $\max\{|c_4^3|, c_6^2\} = |c_4^3|$. ■

By Theorem 5.14, $c_4 = u_T^{-4}\alpha_T$ and $c_6 = u_T^{-6}\beta_T$ where u_T is a positive integer uniquely determined by a and b and in the case of $T = C_2, C_2 \times C_2$, u_T is uniquely determined by a, b, and d. Now let

$$S_T = \left\{ \frac{b}{a} \in \mathbb{Q} \mid \gcd(a,b) = 1 \text{ and } \Delta_T(a,b) \neq 0 \right\}$$

For $T \neq C_2, C_2 \times C_2$ we can construct a function $\hat{u}_T : S_T \to \mathbb{Q}$ such that $\hat{u}_T(a,b) = u_T^{-12}$. Now define $\hat{f}_T : S_T \to \mathbb{Q}$ by

$$\hat{f}_T\left(\frac{b}{a}\right) = \begin{cases} \alpha_T(a,b)^3 & \text{if } \frac{b}{a} \in I_T \\ \beta_T(a,b)^2 & \text{if } \frac{b}{a} \in I_T^C. \end{cases}$$

Corollary 6.5 *For $T \neq C_2, C_2 \times C_2$, there is an explicitly defined function $f_T : S_T \to \mathbb{R}$ such that*

$$f_T\left(\frac{b}{a}\right) = h_{naive}(E_T(a,b))\,.$$

Proof Let $\hat{f}_T, \hat{u}_T : \mathbb{Q} \to \mathbb{Q}$ be as defined above. Define $f_T\left(\frac{b}{a}\right) = \frac{1}{12}\log\left(\hat{u}_T\left(\frac{b}{a}\right)\hat{f}_T\left(\frac{b}{a}\right)\right)$. Then

$$\begin{aligned} f_T\left(\frac{b}{a}\right) &= \frac{1}{12}\log\left(\hat{u}_T\left(\frac{b}{a}\right)\max\left\{\alpha_T(a,b)^3\;, \beta_T(a,b)^2\right\}\right) \\ &= \frac{1}{12}\log\max\left\{c_4^3\;, c_6^2\right\} \end{aligned}$$

by the definition of $\hat{u}_T\left(\frac{b}{a}\right)$, $\hat{f}_T\left(\frac{b}{a}\right)$ and the proof of 6.4. ■

6.3 Lower Bounds on the Modified Szpiro Ratio

Let

$$l_T = \begin{cases} 1 & \text{if } T = C_1 \\ 1.5 & \text{if } T = C_2 \\ 2 & \text{if } T = C_3, C_4, C_2 \times C_2 \\ 3 & \text{if } T = C_5, C_6, C_2 \times C_4 \\ 4 & \text{if } T = C_7, C_8, C_2 \times C_6 \\ 4.5 & \text{if } T = C_9, C_{10} \\ 4.8 & \text{if } T = C_{12}, C_2 \times C_8. \end{cases} \tag{6.7}$$

We may now state the main theorem of this chapter:

Theorem 6.6 *Let T be one of the fifteen torsion subgroups allowed by Theorem 2.1 and let l_T be as given in* (6.7)*. If E is a rational elliptic curve with $T \hookrightarrow E(\mathbb{Q})_{tors}$, then $\sigma_m(E) \geq l_T$.*

The proof of this result will be given in section 6.6. The main step is to bound the conductor. This will be done in the next two sections. Namely, we will prove a series of lemmas in the next section which relies on Tate's Algorithm. These results will then allow us to bound the conductor in section 6.5. Once these results are proven, the proof of Theorem 6.6 is done in section 6.6.

6.4 Tate's Algorithm and the Conductor of E_T

In Section 2.4, we reviewed the terminology pertaining to the local data of a rational elliptic curve. In this section, we will use Tate's Algorithm to establish upper bounds on the conductor of an elliptic curve at the primes 2 and 3 under certain conditions. For the reader's benefit, we restate the quantities which are obtained from Tate's Algorithm.For each prime p of $\mathbb{Z}$, Tate's Algorithm [5, Chapter IV] returns the following local data:

1. The reduction type of the special fiber $\bar{\mathcal{C}}_p^{\min}$ over $\bar{\mathbb{F}}_p$. We will use Kodaira symbols to describe the reduction type.

2. m_p: the number of components, defined over $\bar{\mathbb{F}}_p$ and counted without multiplicity, on $\bar{\mathcal{C}}_p^{\min}$.

3. $v_p\bigl(\Delta_E^{\min}\bigr)$: the valuation of the minimal discriminant of E/K with respect to p;

4. f_p: the exponent appearing at the prime p of the conductor of E. This will be computed via Ogg's formula: $f_p = v_p\bigl(\Delta_E^{\min}\bigr) - m_p + 1$;

5. c_p: the local Tamagawa number at p, i.e., the order of the group of components $\bar{\mathcal{N}}_p(\mathbb{F}_p)\,/\bar{\mathcal{N}}_p^0(\mathbb{F}_p)$. Equivalently, c_p is the number of components of $\bar{\mathcal{C}}_p^{\min}$ which have multiplicity 1 and are defined over $\mathbb{F}_p$.

Theorem 6.7 (Ogg's Formula, [5, 4.11.1]) *Let E be a rational elliptic curve with minimal discriminant Δ_E^{min}. For p a prime, let f_p denote the exponent of the conductor at p and let m_p be as defined above. Then*

$$v_p\bigl(\Delta_E^{min}\bigr) = f_p + m_p - 1$$

In particular, $f_p \leq v_p(\Delta_E^{min})$ for each prime.

Remark From this point onward, we assume familiarity with Tate's Algorithm and follow the Algorithm as outlined in [5, Chapter IV].

Proposition 6.8 *Let $T = C_3$ and consider the elliptic curve E_T. If p does not divide $\Delta_{E_T}^{min}$, then $m_p = 1$, $f_p = 0$, and $c_p = 1$. Moreover, E_T has multiplicative reduction of type I_n where $n = v_p\left(\Delta_{E_T}^{min}\right)$ if and only if p divides b or $(a - 27b)$.*

Now suppose E has additive reduction at p. If p divides d, then E has reduction type IV at p and $m_p = c_p = 3$ and

	$p \neq 3$	$p = 3$ *and* $v_3(a) = 2$	$p = 3$ *and* $v_3(a) \equiv 2 \mod 3$ *with* $v_3(a) \neq 2$
f_p	2	4	5
$v_p(\Delta)$	4	6	7

If p divides e, then E has reduction type IV^* at p and $m_p = 7$, $c_p = 3$, and

	$p \neq 3$	$p = 3$ *and* $v_3(a) = 1$	$p = 3$ *and* $v_3(a) \equiv 1 \mod 3$ *with* $v_3(a) \neq 1$
f_p	2	3	5
$v_p(\Delta)$	8	9	11

Now suppose 3 divides a with $v_3(a) \equiv 0 \mod 3$. Write $a = 27\hat{a}$ and set $n = v_3(\hat{a} - b)$. If $n = 0$, then reduction at 3 is type II if and only if $v_3(2b^2d^2e^4 - bcd^2e^3 + 1) = 1$. Otherwise, reduction type at 3 is type III. If type II, then $m_3 = c_4 = 1$ and $f_3 = v_3(\Delta) = 3$. If type III, then $m_3 = c_3 = 2$, $v_3(\Delta) = 3$, and $f_3 = 2$.

Lastly,

n	*Type*	m_3	f_3	$v_3(\Delta)$	c_3
1	II	1	4	4	1
2	IV	3	3	5	1 *or* 3
$3 + \tilde{n},\ \tilde{n} \geq 0$	$I_{\tilde{n}}^*$	$\tilde{n} + 5$	2	$6 + \tilde{n}$	2 *or* 4

Proof The rational elliptic curve

$$E_T' : y^2 + cdexy + bde^2y = x^3$$

is a global minimal model for the elliptic curve E_T by Theorem 5.14. In particular, the minimal discriminant of E_T is

$$\Delta_{E_T}^{\min} = b^3d^4e^8\left(c^3d^2e - 27b\right)$$

Now let p be a prime. The admissible change of variables $x \longmapsto x+p$ and $y \longmapsto y$ gives a $\mathbb{Q}$-isomorphism from E'_T onto the elliptic curve

$$E_T^{(1)} : y^2 + cdexy + \left(bde^2 + cdep\right) y = x^3 + 3px^2 + 3p^2 + p^3. \qquad (6.8)$$

Now let b_2, b_4, b_6, b_8 be as in (2.2). Then

$$b_2 = c^2d^2e^2 + 12p \qquad b_6 = b^2d^2e^4 + 2bcd^2e^3p + c^2d^2e^2p^2 + 4p^3$$
$$b_8 = p\left(3b^2d^2e^4 + 3bcd^2e^3p + c^2d^2e^2p^2 + 3p^3\right)$$

In what follows, a_1, a_2, a_3, a_4, a_6 will refer to the coefficients of the Weierstrass model for $E_T^{(1)}$.

Case I. Suppose $p \nmid \Delta_{E_T}^{\min}$. Then E_T has good reduction at p and the reduction type is I_0. Consequently, $m_p = 1$, $f_p = 0$, and $c_p = 1$.

Case II. Suppose that $p|\Delta_{E_T}^{\min}$ and that E_T has multiplicative reduction at p. By Theorem 5.25, p divides b or $c^3d^2e - 27b$. Otherwise, E_T would have additive reduction at p. The Weierstrass model for $E_T^{(1)}$ satisfies the condition that p divides a_3, a_4, a_6 and so we may proceed with Step 2 of Tate's Algorithm. Since p does not divide cde, it follows that p does not divide b_2. By Tate's Algorithm, the reduction type at p is Type I_n where $n = v_p\left(\Delta_{E_T}^{\min}\right)$.

Case III. Suppose p divides d. By Theorem 5.25, E_T has additive reduction at p. Then $p|b_2, p^2|a_6, p^3|b_8$. But $p^3 \nmid b_6$ since de is relatively prime to b. Now observe that for an indeterminate T,

$$T^2 + \frac{bde^2 + cdep}{p}T - \frac{p^3}{p^2} = T^2 + \left(b\hat{d}e^2 + c\hat{d}ep\right)T - p \equiv T\left(T + b\hat{d}e^2\right) \mod p$$

with $d = \hat{d}p$. In particular, $\mathbb{F}_p$ is the splitting field of the polynomial $T\left(T + b\hat{d}e^2\right)$. We conclude by Tate's Algorithm that E_T has reduction type IV at p and thus $m_p = c_p = 3$ and $f_p = v_p\left(\Delta_{E_T}^{\min}\right) - 2$.

Subcase I. Suppose $p \neq 3$. Then $v_p\left(\Delta_{E_T}^{\min}\right) = 4$ and thus $f_p = 2$.

Subcase II. Suppose $p = 3$ and $v_3(a) = 2$. Then 3 divides d and we have that $v_3\left(\Delta_{E_T}^{\min}\right) = 6$. Thus $f_3 = 4$.

Subcase III. Suppose $p = 3$ and $v_3(a) \equiv 2 \mod 3$ with 3 dividing c. In particular, 3 divides d. Then $v_3\left(\Delta_{E_T}^{\min}\right) = 7$ and so $f_3 = 5$.

Case IV. Suppose p divides e. By Theorem 5.25, E_T has additive reduction at p. Now observe that p divides b_2, a_1, a_2, p^2 divides a_6, a_3, a_4, and p^3 divides b_6, b_8, a_6. Consequently, Tate's Algorithm runs through Step 6. Now consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{3p}{p}T^2 + \frac{3p^2}{p^2}T + \frac{p^3}{p^3} \\ &\equiv (T+1)^3 \mod p. \end{aligned}$$

Since this polynomial has a triple root over $\mathbb{F}_p$, Tate's Algorithm skips to Step 8. To proceed, we consider the admissible change of variables $x \longmapsto x + p^2$ and $y \longmapsto y$ which gives a $\mathbb{Q}$-isomorphism from E_T' onto

$$E_T^{(2)} : y^2 + cdexy + \left(bde^2 + cdep^2\right) y = x^3 + 3p^2x^2 + 3p^4x + p^6.$$

Let a_j' correspond to the coefficients of the Weierstrass model for $E_T^{(2)}$. Then $p^2|a_2', p^3|a_4'$, and $p^4|a_6'$. Now consider the polynomial

$$T^2 + \frac{bde^2 + cdep^2}{p^2}T - \frac{p^6}{p^4} = T^2 + \left(bd\hat{e}^2 + cd\hat{e}p^2\right)T - p^2.$$

Viewed as a polynomial in $\mathbb{F}_p$, we observe that $\mathbb{F}_p$ is its splitting field since

$$T^2 + \left(bd\hat{e}^2 + cd\hat{e}p^2\right)T - p^2 \equiv T\left(T + bd\hat{e}^2\right) \mod p.$$

By Tate's Algorithm we conclude that E_T has reduction type IV^* at p and moreover $m_p = 7$, $f_p = v_p\left(\Delta_{E_T}^{\min}\right) - 6$, and $c_p = 3$.

Subcase I. Suppose $p \neq 3$. Then $v_p\left(\Delta_{E_T}^{\min}\right) = 8$ and so $f_p = 2$.

Subcase II. Suppose $p = 3$ and $v_3(a) = 1$. Then 3 divides e and we have that $v_3\left(\Delta_{E_T}^{\min}\right) = 9$. Thus $f_3 = 3$.

Subcase III. Suppose $p = 3$ and $v_3(a) \equiv 1 \mod 3$ with 3 dividing c. In particular, 3 divides e. Then $v_3\left(\Delta_{E_T}^{\min}\right) = 11$ and so $f_3 = 5$.

Case V. Suppose $p = 3$ and $v_3(a) \equiv 0 \mod 3$. Then $c = 3\hat{c}$ for some integer $\hat{c}$ and 3 does not divide de. Now consider the admissible change of variables $x \longmapsto x - 1$ and $y \longmapsto y + bde^2$ which gives a $\mathbb{Q}$-isomorphism from E_T' onto

$$E_T^{(3)} : x^3 + cdexy + de\left(3be - c\right)y = x^3 - 3x^2 + \left(3 - bcd^2e^3\right)x + bcd^2e^3 - 2b^2d^2e^4 - 1.$$

Let a_j'' denote the coefficients of $E_T^{(3)}$. Then 3 divides a_3'' and a_4''. Note that

$$a_6'' = bcd^2e^3 - 2b^2d^2e^4 - 1 \equiv 0 \mod 3$$

since $b^2d^2e^2$ is square not divisible by 3. Now compute the quantities $b_2'', b_4'', b_6'', b_8''$ for $E_T^{(3)}$ via the formulas in (2.2). Then

$$b_2'' = 9\hat{c}^2d^2e^2 - 12 \qquad b_6'' = \left(bde^2 - 3\hat{c}de - 2\right)\left(bde^2 - 3\hat{c}de + 2\right)$$
$$b_8'' = 3 + 9b\hat{c}d^2e^3 - 9\hat{c}^2d^2e^2 - 3b^2d^2e^4.$$

Note that 3 divides b_2''.

Subcase I. Suppose $v_3(a) \geq 6$. Then $v_3\left(\Delta_{E_T}^{\min}\right) = 3$. Then

$$a_6'' \equiv 7b^2d^2e^4 - 1 \mod 9.$$

By Tate's Algorithm, E_T has reduction type II if and only if $a_6'' \not\equiv 0 \mod 9$. If this is the case, then $m_3 = c_3 = 1$ and $f_3 = 3$. Now suppose $a_6'' \equiv 0 \mod 9$. Then $bde^2 \equiv \pm 2 \mod 9$. In particular, $b^2d^2e^4 \equiv 4 \mod 9$ and so $b^2d^2e^4 = 4 + 9k$ for some integer k. Now observe that since 3 divides $\hat{c}$ we attain

$$b_8'' \equiv 3 - 3b^2d^2e^4 \mod 27 = 3 - 3\,(4 + 9k) \mod 27 = -9 \mod 27.$$

Thus we have that if $a_6'' \equiv 0 \mod 9$, then E_T has reduction type III at 3. In particular, $m_3 = c_3 = f_3 = 2$.

Subcase II. Suppose $v_3(a) = 3$. Then $c = 3\hat{c}$ with $\hat{c}$ an odd integer. Then

$$c^3d^2e - 27b = 27\left(\hat{c}^3d^2e - b\right)$$

Set $\hat{n} = v_3(\hat{c}^3d^2e - b)$ so that $v_3\left(\Delta_{E_T}^{\min}\right) = 3 + \hat{n}$. We now consider the following cases: (i) $\hat{n} = 0$, (ii) $\hat{n} = 1$, (iii) $\hat{n} = 2$, and (iv) $\hat{n} \geq 3$.

(i) Suppose $\hat{n} = 0$. Since $f_p \leq v_3\left(\Delta_{E_T}^{\min}\right)$ we note that the only possibilities with $f_p \geq 2$ are Type II or Type III. Moreover, Type II occurs if and only if $a_6'' \not\equiv 0 \mod 9$. If this is the case, then $m_3 = c_3 = 1$ and $f_3 = 3$. Otherwise, E_T has reduction type III at 3 with $m_3 = c_3 = f_3 = 2$.

(ii) Suppose $\hat{n} = 1$. Then $b = \hat{c}^3d^2e - 3k$ for some integer k not divisible by 3. Now observe that

$$\begin{aligned} a_6'' &= 3\hat{c}^4d^4e^4 - 9\hat{c}d^2e^3k - 2\left(\hat{c}^6d^4e^2 - 6\hat{c}^3d^2ek + 3k^2\right)d^2e^4 - 1 \\ &= 3\hat{c}^4d^4e^4 - 9\hat{c}d^2e^3k - 2\hat{c}^6d^6e^6 + 12\hat{c}^3d^4e^5k - 3d^2e^4k^2 - 1 \\ &\equiv 8 \pm 3 \mod 9 \neq 0 \mod 9 \end{aligned} \tag{6.9}$$

since $3l^2 \equiv 3 \mod 9$, $-2l^6 \equiv 7 \mod 9$, and $12l \equiv \pm 3 \mod 9$ for all l not divisible by 3. Thus E_T has reduction type II at 3 and in particular $m_3 = c_3 = 1$ and $f_3 = 4$.

(iii) Suppose $\hat{n} = 2$. Then $b = \hat{c}^3d^2e - 9k$ for some integer k not divisible by 3. Then

$$a_6'' \equiv 8 + 3\hat{c}^4d^4e^4 + 7\hat{c}^6d^6e^6 \mod 9 = 0 \mod 9$$

since $3l^4 \equiv 3 \mod 9$ and $7l^6 \equiv 7 \mod 9$ for integers l not divisible by 3. Next, we consider b_8'' and observe that

$$b_8'' \equiv 3 + 18\hat{c}^2d^2e^2 + 9\hat{c}^4d^4e^4 + 24\hat{c}^6d^6e^6 \mod 27 = 0 \mod 27$$

since $18l^2 \equiv 18 \mod 27$, $9l^2 \equiv 9 \mod 27$, and $24l^6 \equiv 24 \mod 27$ for integers l which are not divisible by 3. Next, we consider b_6'' and observe that

$$b_6'' \equiv 23 + 9\hat{c}^2d^2e^2 + 21\hat{c}^4d^4e^4 + \hat{c}^6d^6e^6 + 9\hat{c}^3d^4e^5k \mod 27 = 9\hat{c}^3d^4e^5k \mod 27$$

since $23 + 9l^2 + 21l^4 + l^6 \equiv 0 \mod 27$. Moreover, $\hat{c}dek$ is not divisible by 3 and therefore we conclude that b_6'' is not divisible by 27. By Tate's Algorithm, we conclude that E_T has reduction type IV at 3. In particular, $m_3 = f_3 = 3$. Lastly, consider the polynomial

$$T^2 + \frac{a_3''}{3}T - \frac{a_6''}{9} = T^2 + de\left(be - \hat{c}\right)T - \frac{3b\hat{c}d^2e^3 - 2b^2d^2e^4 - 1}{9}.$$

Now observe that

$$\begin{aligned} 3b\hat{c}d^2e^3 - 2b^2d^2e^4 - 1 &= -1 + 3\hat{c}^4d^4e^4 - 2\hat{c}^6d^6e^6 - 27\hat{c}d^2e^3k + 36\hat{c}^3d^4e^5k - 162d^2e^4k^2 \\ &\equiv 9\hat{c}^3d^4e^5k \mod 27. \end{aligned}$$

Since $de\,(be-\hat{c}) = -\hat{c}de + \hat{c}^3d^3e^3 - 9de^2k \equiv 0 \mod 3$, we have that

$$T^2 + \frac{a_3''}{3}T - \frac{a_6''}{9} \equiv T^2 + \hat{c}^3d^4e^5k \mod 3.$$

But $\hat{c}^3d^4e^5k$ is square modulo 3 if and only if $\hat{c}^3d^4e^5k \equiv 1 \mod 3$. If this congruence holds, then $\mathbb{F}_3$ is the splitting field of this polynomial and therefore by Tate's Algorithm, $c_3 = 3$ if and only if $\hat{c}^3d^4e^5k \equiv 1 \mod 3$. Otherwise $c_3 = 1$.

(iv) Suppose $\hat{n} = 3 + n$ for some integer $n \geq 0$. Then $b = \hat{c}^3d^2e - 27k$ for some integer k satisfying $v_3(k) = n$. Proceeding as above shows that 9 divides a_6'' and 81 divides b_8''. We now show that b_6'' is divisible by 27. Indeed,

$$b_6'' \equiv -4 + 9\hat{c}^2d^2e^2 - 6\hat{c}^4d^4e^4 + \hat{c}^6d^6e^6 \mod 27 = 0 \mod 27$$

since $-4 + 9l^2 - 6l^4 + l^6 \equiv 0 \mod 27$ for integers l not divisible by 3. To proceed through Tate's algorithm we must satisfy further divisibility conditions, which are not satisfied by the coefficients of the Weierstrass model for $E_T^{(3)}$. To this end, consider the admissible change of variables $x \longmapsto x$ and $y \longmapsto y - \hat{c}dex$ from $E_T^{(3)}$ onto

$$\begin{aligned} E_T^{(4)} : & y^2 - 9\hat{c}dexy + 3de\,(be-\hat{c})\,y = x^3 - \left(18\hat{c}^2d^2e^2 + 3\right)x^2 + \\ & \left(15b\hat{c}d^2e^3 - 18\hat{c}^2d^2e^2 + 3\right)x - 2b^2d^2e^4 + 3b\hat{c}d^2e^3 - 1. \end{aligned}$$

Let $\hat{a}_j$ denote the coefficients of the Weierstrass model for $E_T^{(4)}$. Observe that 3 divides $\hat{a}_1$ and $\hat{a}_2$. We claim that 9 divides $\hat{a}_3$ and $\hat{a}_4$ and that 27 divides $\hat{a}_6$. Indeed,

$$\begin{aligned} \hat{a}_3 &\equiv cde\left(6 + 3\hat{c}^2d^2e^2\right) \mod 9 = 0 \mod 9 \\ \hat{a}_4 &\equiv 3 + 6\hat{c}^4d^4e^4 \mod 9 = 0 \mod 9 \\ \hat{a}_6 &\equiv -1 + 3\hat{c}^4d^4e^4 - 2\hat{c}^6d^6e^6 \mod 27 = 0 \mod 27 \end{aligned}$$

since $3l^2 \equiv 3 \mod 9$, $6l^4 \equiv 6 \mod 9$, and $3l^4 - 2l^6 \equiv 1 \mod 27$ for integers l not divisible by 3.

Now consider the polynomial

$$P(T) = T^3 + \frac{\hat{a}_2}{3}T^2 + \frac{\hat{a}_4}{9}T + \frac{\hat{a}_6}{27}.$$

The discriminant of this polynomial is

$$\begin{aligned}\mathrm{Disc}(P) &= 3^{-6}\cdot\left(-4\hat{a}_2^3\hat{a}_6+\hat{a}_2^2\hat{a}_4^2-4\hat{a}_4^3-27\hat{a}_6^2+18\hat{a}_2\hat{a}_4\hat{a}_6\right)\\ &\equiv \hat{c}^9d^{10}e^{11}k+\frac{236\hat{c}^8d^8e^8-328\hat{c}^{10}d^{10}e^{10}+92\hat{c}^{12}d^{12}e^{12}}{3} \mod 3.\end{aligned}$$

But $236l^8-328l^{10}+92l^{12}$ is divisible by 9 for all integers l. Thus $\mathrm{Disc}(P)\equiv \hat{c}^9d^{10}e^{11}k \mod 3$. In particular, $P(T)$ has distinct roots over an algebraic closure of $\mathbb{F}_3$ if and only if k is not divisible by 3. Equivalently, $v_3(k)=n=0$. By Tate's Algorithm, if this is the case, then E_T has reduction type I_0^*, $m_3=5$, $f_3=3$, and $c_3=1+\#\{\alpha\in\mathbb{Q}_3 \mid P(\alpha)=0\}$.

Now suppose n is positive. Then we may write $b=\hat{c}^3d^2e-81k$ for some integer k satisfying $v_3(k)=n-1$. Then $P(T)$ does not have distinct roots and in fact

$$P(T)\equiv T^3+2T^2+\left(\hat{c}^2d^2e^2+\frac{1+5\hat{c}^4d^4e^4}{3}\right)T+\frac{3\hat{c}^4d^4e^4-2\hat{c}^6d^6e^6-1}{27} \mod 3.$$

Since $P(T)$ does not have distinct roots over an algebraic closure of $\mathbb{F}_3$, it follows that either $P(T)$ has a double root or a triple root over an algebraic closure of $\mathbb{F}_3$. Suppose $P(T)$ had a triple root over an algebraic closure of $\mathbb{F}_3$. Then $P(T)\equiv(T-\lambda)^3 \mod 3$ for some λ in an algebraic closure of $\mathbb{F}_3$. In particular, $P(T)\equiv T^3+2\lambda^3$. Since the coefficient of $P(T)$ modulo 3 is 2, we conclude that $P(T)$ does not have a triple root over an algebraic closure of $\mathbb{F}_3$.

Since $n=v_3\left(\Delta_{E_T}^{\min}\right)-6$, we conclude by Tate's Algorithm that E_T has reduction type I_n^* at 3 and moreover, $m_3=v_3\left(\Delta_{E_T}^{\min}\right)-1$ and $f_3=2$. Lastly, $c_3=2$ or 4. This concludes the proof. ∎

Example 6.9 *Let $T=C_3$ and let $E_1=E_T(27,-8)$ and $E_2(27,-17)$. Then*

$$v_3\left(\Delta_{E_1}^{min}\right)=3+v_3(1+8)=5 \qquad \text{and} \qquad v_3\left(\Delta_{E_2}^{min}\right)=3+v_3(1+17)=5.$$

By Proposition 6.8, the reduction type at 3 is Type II for both E_1 and E_2. Next we compute the local Tamagawa number at 3. With notation as in part (iii) of the proof of Proposition 6.8, we saw that $c_3=3$ if and only if $\hat{c}^3d^4e^5k\equiv 1 \mod 3$ where $c=3\hat{c}$

and $b = \hat{c}^3 d^2 e - 9k$. *Since* $de = 1$ *for both* E_1 *and* E_2 *we observe that* $k = 1$ *for* E_1 *and* $k = 2$ *for* E_2. *In particular, since* $\hat{c}^3 d^4 e^5 k = k$, *we conclude that* $c_3 = 3$ *for* E_1 *and* $c_3 = 1$ *for* E_2.

Lemma 6.10 *Let* $T = C_4$. *If* $u_T = c$, *then* $v_p(N_T) \leq 2$ *for all odd primes* p. *Moreover, if* $v_2(a) \leq 2$, *then* $v_p(N_T) \leq 6$.

Proof Since we are assuming $u_T = c$, we have by Theorem 5.14 that a global minimal model for E_T is

$$E_T' : y^2 + cdxy - cd^2by = x^3 - bdx^2$$

with $a = c^2 d$ for d a positive squarefree integer. Moreover, the minimal discriminant of E_T is

$$\Delta_{E_T}^{\min} = b^4 c^2 d^7 \left(c^2 d + 16b\right)$$

For $p \geq 5$ a prime, it is true that $v_p(N_T) \leq 2$. So it suffices to show that the inequality holds for $p = 3$ to prove the first claim. If E_T is semistable at 3, then $v_3(N_T) \leq 1$. So suppose E_T has additive reduction at 3. By Theorem 5.25, E_T has additive reduction at 3 if and only if 3 divides d. We may, therefore, assume that $d = 3\hat{d}$ with $\hat{d}$ a positive integer not divisible by 3. We now consider Tate's Algorithm for E_T at the prime 3. To this end, consider the admissible change of variables $x \longmapsto x$ and $y \longmapsto y - 2cdx + 2bcd^2$ which gives a $\mathbb{Q}$-isomorphism from E_T' onto

$$E_T^{(1)} : y^2 - 3cdxy + 3bcd^2 y = x^3 - \left(2c^2 d^2 - bd\right) x^2 + 4bc^2 d^3 x - 2b^2 c^2 d^4$$

Now let a_j be the coefficient of the Weierstrass model for $E_T^{(1)}$. Since 3 divides d, we have that 3 divides a_1 and a_2, 9 divides a_3 and a_4, and 81 divides a_6. Now we compute the b_j as given in (2.2),

$$b_2 = d\left(c^2 d - 4b\right), \qquad b_6 = b^2 c^2 d^4, \qquad b_8 = -b^3 c^2 d^5.$$

Now observe that the assumption of d being divisible by 3 implies that 3 divides b_2, 27 divides b_6 and b_8. Thus Tate's Algorithm runs through Step 6. Next, we consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{a_2}{3} + \frac{a_4}{9} + \frac{a_6}{27} = T^3 + \left(6c^2\hat{d}^2 - b\hat{d}\right)T^2 + 12bc^2\hat{d}^3T + 6b^2c^2\hat{d}^4 \\ &\equiv T^3 - b\hat{d}T^2 \mod 3 = T^2\left(T - b\hat{d}\right) \mod 3. \end{aligned}$$

Since $b\hat{d}$ is not divisible by 3, we have that $P(T)$ over $\mathbb{F}_3$ has a double root at 0 and a simple root at $b\hat{d}$. Now let

$$n = v_3\left(\Delta_{E_T}^{\min}\right) - 6 = 1 + 2v_3(c)$$

since $v_3\left(\Delta_{E_T}^{\min}\right) = 7+2v_3(c)$. By Tate's Algorithm, we conclude that E_T has reduction Type I_n^* at 3. Moreover, $m_3 = n+5$, $f_3 = 2$, and c_3 is either 2 or 4. Hence $v_p(N_T) \leq 2$ for all odd primes p.

It remains to show that if $u_T = c$ and $v_2(a) \leq 2$, then $v_2(N_T) \leq 6$. By Theorem 5.25, E_T additive reduction occurs at 2 with $u_T = c$ if and only if a is even. So it suffices to consider the cases $v_2(a) = 1$ and $v_2(a) = 2$.

Case I. Suppose $v_2(a) = 1$. Then $d = 2\hat{d}$ for some odd integer $\hat{d}$ and c is odd. Since d is even, we note that 2 divides a_1 and a_2, 4 divides a_3 and a_4, and 8 divides a_6. Moreover, 2 divides b_2 and 8 divides both b_6 and b_8. In particular, Tate's Algorithm runs through Step 6. Now consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{a_2}{2} + \frac{a_4}{4} + \frac{a_6}{8} = T^3 - \left(4c^2\hat{d}^2 - b\hat{d}\right)T^2 + 8bc^2\hat{d}^3T - 4b^2c^2\hat{d}^4 \\ &\equiv T^3 - b\hat{d}T^2 \mod 2 = T^2\left(T - b\hat{d}\right) \mod 2. \end{aligned}$$

Since $b\hat{d}$ is odd it follows that $P(T)$ has a double root at 0 over $\mathbb{F}_2$ and a simple root at $b\hat{d}$. Now observe that $v_2\left(\Delta_{E_T}^{\min}\right) = 8$. Since the double root of $P(T)$ over $\mathbb{F}_2$ occurs at 0 we may proceed to the subprocedure of Step 7 in Tate's Algorithm. Indeed, 4 does not divide a_2, but 8 and 32 divide a_4 and a_6, respectively. Next we consider the polynomial

$$\begin{aligned} Y^2 + \frac{a_3}{4}Y - \frac{a_6}{16} &= Y^2 + 3bc\hat{d}^2 Y - 2b^2c^2\hat{d}^4 \\ &\equiv Y^2 + bc\hat{d}^2 Y \mod 2 = Y\left(Y + bc\hat{d}^2\right) \mod 2. \end{aligned}$$

Since $bc\hat{d}$ is odd, we have that this polynomial is $Y(Y+1)$ over $\mathbb{F}_2$. Since it has distinct roots over $\mathbb{F}_2$, we conclude by Tate's Algorithm that the reduction type at 2 is Type I_1^* and moreover $m_2 = 6$, $f_p = 3$, and $c_2 = 4$.

Case II. Suppose $v_2(a) = 2$. Then $c = 2\hat{c}$ for some odd integer $\hat{c}$ and d is odd. In particular, $v_2\left(\Delta_{E_T}^{\min}\right) = 4$. By Ogg's Formula we conclude that $f_p \leq 4$ which concludes the proof. ■

Lemma 6.11 *Let $T = C_6$. Then $v_p(N_T) \leq 2$ for all p.*

Proof By Theorem 5.25, E_T is semistable at all primes $p \geq 5$. Consequently, $v_p(N_T) \leq 1$ for all primes $p \geq 5$. By Proposition 6.8, $v_2(N_T) \leq 2$ since E_T is $\mathbb{Q}$-isomorphic to $E_{C_3}(a', b')$ for some relatively prime integers a' and b'. It remains to show that $v_3(N_T) \leq 2$. To this end, we assume E_T has additive reduction at 3. By Theorem 5.25, E_T has additive reduction at 3 if and only if 3 divides a. By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. Moreover, $u_T = 2$ if and only if $v_2(a+b) \geq 3$. We will now prove the Lemma by considering the cases $u_T = 1$ and $u_T = 2$ separately.

Case I. Suppose $u_T = 1$. Then E_T is a global minimal model for E_T. We now consider the cases $v_3(a) = 1$, $v_3(a) = 2$, and $v_3(a) > 2$ separately.

Subcase I. Suppose $v_3(a) = 1$. Then $a = 3\hat{a}$ for some integer $\hat{a}$ not divisible by 3. In particular, $v_3\left(\Delta_{E_T}^{\min}\right) = 3$. The admissible change of variables $x \longmapsto x$ and $y \longmapsto y + 3$ gives a $\mathbb{Q}$-isomorphism from E_T onto

$$\begin{aligned} E_T^{(1)} : y^2 + (a-b)\,xy + \left(6 - a^2b - ab^2\right) y = \\ x^3 - \left(ab + b^2\right) x^2 + (3b - 3a)\,x + 3a^2b + 3ab^2 - 9. \end{aligned}$$

Let $a_j^{(1)}$ denote the coefficients of $E_T^{(1)}$. Observe that 3 divides $a_3^{(1)}, a_4^{(1)}$, and $a_6^{(1)}$. Now let $b_j^{(1)}$ be as given in (2.2) for the Weierstrass model of $E_T^{(1)}$. Then

$$b_2^{(1)} = a^2 - 6ab - 3b^2 \qquad b_8^{(1)} = -a^5b^3 - 3a^4b^4 - 3a^3b^5 - a^2b^6.$$

Since $a = 3\hat{a}$ we observe that 3 divides $b_2^{(1)}$ and 9 divides $a_6^{(1)}$. However,

$$b_8^{(1)} \equiv 18\hat{a}^2b^6 \mod 27 = 18 \mod 27$$

since $18l^2 \equiv 18 \mod 27$ for integers l not divisible by 3. Therefore 27 does not divide $b_8^{(1)}$ and by Tate's Algorithm, we conclude that E_T has reduction Type III at 3. In particular, $m_3 = 2,\ f_3 = 2$, and $c_3 = 2$.

Before proceeding to the next two subcases, we will consider a new translation of E_T. Let $x \longmapsto x$ and $y \longmapsto y + (a-b)\,x - a^2b - ab^2$ be an admissible change of variables from E_T onto

$$\begin{aligned} E_T^{(2)} : y^2 + (3a-3b)\,xy - \left(3a^2b + 3ab^2\right) y = x^3 + \left(3ab - 2a^2 - 3b^2\right) x^2 \\ + \left(4a^3b - 4ab^3\right) x - 2a^4b^2 - 4a^3b^3 - 2a^2b^4. \end{aligned}$$

Let $a_j^{(2)}$ denote the coefficients the Weierstrass model for $E_T^{(2)}$ and we compute the $b_j^{(2)}$ as given in (2.2):

$$\begin{aligned} b_2^{(2)} &= a^2 - 6ab - 3b^2 \qquad b_6^{(2)} = a^4b^2 + 2a^3b^3 + a^2b^4 \\ b_8^{(2)} &= -a^5b^3 - 3a^4b^4 - 3a^3b^5 - a^2b^6. \end{aligned}$$

Observe that if $v_3(a) \geq 2$, then 3 divides $a_1^{(2)},\ a_2^{(2)}$, and $b_2^{(2)}$, 9 divides $a_3^{(2)}$ and $a_4^{(2)}$, and 27 divides $a_6^{(2)},\ b_6^{(2)}$, and $b_8^{(2)}$. Consequently, if $v_3(a) \geq 2$, then Tate's Algorithm runs through Step 6. Let $a = 9\hat{a}$ for some integer $\hat{a}$ and consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{a_2^{(2)}}{3}T^2 + \frac{a_4^{(2)}}{9}T + \frac{a_6^{(2)}}{27} \\ &= T^3 + \left(9\hat{a}b - 9\hat{a}^2 - b^2\right) T^2 + \left(324\hat{a}^3b - 4\hat{a}b^3\right) T - 486\hat{a}^4b^2 - 108\hat{a}^3b^3 - 6\hat{a}^2b^4 \\ &\equiv T^3 - b^2T^2 + 2\hat{a}b^3T \mod 3 = T\left(T^2 + 2T + 2\hat{a}b\right) \mod 3. \end{aligned}$$

Subcase II. Suppose $v_3(a) = 2$ and let $a = 9\hat{a}$ for some integer $\hat{a}$ not divisible by 3. Then $v_3\left(\Delta_{E_T}^{\min}\right) = 6 + v_3(\hat{a} + b)$. In what follows we let $n = v_3(\hat{a} + b)$.

First, assume $n = 0$. Then $\hat{a}+b \equiv 1, 2 \mod 3$. But this only occurs if $\hat{a} \equiv b \mod 3$. In particular, $2\hat{a}b^3 \equiv 2 \mod 3$. Moreover, $P(T) \equiv T^3 + 2T^2 + T \mod 3$ which has distinct roots over an algebraic closure of $\mathbb{F}_3$. Indeed, the discriminant of the polynomial is congruent to $\hat{a}^3 b^9 + \hat{a}^2 b^{10} \mod 3$. Since $\hat{a} \equiv b \mod 3$, we get that the discriminant is $2 \mod 3$ and therefore has distinct roots. Therefore the reduction type is I_0^* at 3 and $m_3 = 5$, $f_3 = 2$, and $c_3 = 1 + \#\left\{\alpha \in \mathbb{F}_3 \mid P(\alpha) \equiv 0 \mod 3\right\} = 2$.

Next, assume $n > 0$. Then $\hat{a} \equiv -b \mod 3$. Then $2\hat{a}b \equiv 1 \mod 3$ and so $P(T) \equiv T\left(T+1\right)^2 \mod 3$. Therefore $P(T)$ has a double root over $\mathbb{F}_3$ and by Tate's Algorithm, we conclude that E_T has reduction Type I_n^* at 3. Moreover $m_3 = v_3\left(\Delta_{E_T}^{\min}\right) - 1$ and $f_3 = 2$. Lastly, c_3 is 2 or 4.

Subcase III. Suppose $v_3(a) > 2$. Then 3 divides $\hat{a}$ and we observe that $P(T) \equiv T^2\left(T+2\right) \mod 3$. Therefore $P(T)$ has a double root over $\mathbb{F}_3$. By Tate's Algorithm, we conclude that E_T has reduction Type $I_{\hat{n}}^*$ at 3 where $\hat{n} = v_3\left(\Delta_{E_T}^{\min}\right) - 6$. In particular, $f_3 = 2$ and $m_3 = v_3\left(\Delta_{E_T}^{\min}\right) - 1$. Lastly, c_3 is either 2 or 4.

Case II. Suppose $u_T = 2$. Then $v_2(a + b) \geq 3$. Let $a + b = 8k$ for some integer k so that $b = 8k - a$. Note that a and k are relatively prime since a and b are relatively prime. By the proof of Theorem 5.14, a global minimal model for E_T is

$$E_T' : y^2 + (a - 4k)\,xy + ak\,(a - 8k)\,y = x^3 + 2k\,(a - 8k)\,x^2.$$

Moreover, the minimal discriminant of E_T is

$$\Delta_{E_T}^{\min} = a^2 k^3 \left(9k - a\right)\left(a - 8k\right)^6.$$

Since E_T has additive reduction at 3 if and only if $v_3(a) > 0$, we have that if E_T has additive reduction at 3, then

$$v_3\left(\Delta_{E_T}^{\min}\right) = 2v_3(a) + v_3(9k - a)\,.$$

Henceforth we will assume $v_3(a) > 0$. Now consider the admissible change of variables $x \longmapsto x$ and $y \longmapsto y + (a-k)\,x + ak\,(a-8k)$ which gives a $\mathbb{Q}$-isomorphism between E'_T and the elliptic curve

$$E_T^{(3)} : y^2 + 3\,(a-4k)\,xy + 3ak\,(a-8k)\,y = x^3 - 2\left(a^2 - 9ak + 24k^2\right)x^2 - \\ 4ak\,(a-8k)\,(a-4k)\,x - 2a^2k^2\,(a-8k)^2\,.$$

Let $a_j^{(3)}$ denote the coefficients the Weierstrass model for $E_T^{(3)}$ and we compute the $b_j^{(3)}$ as given in (2.2):

$$b_2^{(3)} = a^2 - 48k^2 \qquad b_6^{(3)} = a^2k^2\,(a-8k)^2 \qquad b_8^{(3)} = 2a^2k^3\,(a-8k)^3$$

Now observe that

$$\begin{array}{lll} v_3\left(a_1^{(3)}\right) = 1 & v_3\left(a_2^{(3)}\right) = 1 & v_3\left(a_3^{(3)}\right) = 1 + v_3(a) \\ v_3\left(a_4^{(3)}\right) = v_3(a) & v_3\left(a_6^{(3)}\right) = 2v_3(a) & v_3\left(b_2^{(3)}\right) = 1 \\ v_3\left(b_6^{(3)}\right) = 2v_3(a) & v_3\left(b_8^{(3)}\right) = 2v_3(a) & \end{array}$$

Subcase I. Suppose $v_3(a) = 1$ so that $v_3\left(\Delta_{E_T}^{\min}\right) = 3$. Then $v_3\left(b_8^{(3)}\right) = 2$ and by Tate's Algorithm we conclude that E_T has reduction Type III at 3. Thus $m_3 = f_3 = c_3 = 2$.

Subcase II. Suppose $v_3(a) \geq 2$ so that $a = 9\hat{a}$ for some integer $\hat{a}$. Now consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{a_2^{(3)}}{3}T^2 + \frac{a_4^{(3)}}{9}T + \frac{a_6^{(3)}}{27} \\ &= T^3 - 2\left(3\hat{a}^2 - 27\hat{a}k + 8k^2\right)T^2 - 4\hat{a}k\,(9\hat{a}-8k)\,(9\hat{a}-4k)\,T - 6\hat{a}^2k^2\,(9\hat{a}-8k)^2 \\ &\equiv T^3 - 16k^2T^2 - 128\hat{a}k^3T \mod 3 = T\left(T^2 + 2T + \hat{a}k\right) \bmod 3 \end{aligned}$$

since $k^2 \equiv 1 \mod 3$. We now consider two additional cases (a) $v_3(a) = 2$ and (b) $v_3(a) > 2$.

(a) Suppose $v_3(a) = 2$. Then $\hat{a}$ is odd and

$$v_3\left(\Delta_{E_T}^{\min}\right) = 6 + v_3(k - \hat{a})\,.$$

Let $n = v_3(k - \hat{a})$. We first assume $n = 0$ so that $k - \hat{a} \equiv 1, 2 \mod 3$. This occurs when $\hat{a} \equiv -k \mod 3$. In particular, $\hat{a}k \equiv 1 \mod 3$. Therefore $P(T) \equiv T^3 + 2T^2 + T \mod 3$. But we already saw in Case I that this polynomial has distinct roots over $\mathbb{F}_3$. Therefore by Tate's Algorithm, E_T has reduction Type I_0^* at 3. In particular, $m_3 = 5$, $f_3 = c_3 = 2$.

Now assume $n > 0$. Then $k - \hat{a} \equiv 0 \mod 3$ and so $\hat{a} \equiv k \mod 3$. Thus $\hat{a}k \equiv 1 \mod 3$ from which we attain the congruence $P(T) \equiv T\,(T+1)^2 \mod 3$. In particular, $P(T)$ has a double root over $\mathbb{F}_3$ and by Tate's Algorithm we conclude that E_T has reduction type I_n^* since $n = v_3\big(\Delta_{E_T}^{\min}\big) - 6$. In particular, $m_3 = v_3\big(\Delta_{E_T}^{\min}\big) - 1$ and $f_3 = 2$. Moreover, c_3 is 2 or 4.

(*b*) Suppose $v_3(a) > 2$. Then $v_3\big(\Delta_{E_T}^{\min}\big) = 2 + 2v_3(a)$. Then $\hat{a} \equiv 0 \mod 3$ and therefore $P(T) \equiv T^2\,(T+2) \mod 3$. Therefore $P(T)$ has a double root over $\mathbb{F}_3$. By Tate's Algorithm, we conclude that E_T has reduction Type $I_{\hat{n}}^*$ where $\hat{n} = v_3\big(\Delta_{E_T}^{\min}\big) - 6$. In particular, $f_3 = 2$ and $m_3 = v_3\big(\Delta_{E_T}^{\min}\big) - 1$. Lastly, c_3 is either 2 or 4. ■

Lemma 6.12 *Let $T = C_8$ and let j be 0 or 1. If $v_2(a) = 2 + j$, then $v_2(N_T) \leq 6 + j$.*

Proof Since $v_2(a) = 2, 3$, we have by Theorem 5.14 that $u_T = 1$. Therefore E_T is a global minimal model for E_T. In particular, γ_T is the minimal discriminant of E_T. Since $v_2(a) \geq 2$, we observe that

$$v_2(\gamma_T) = 7 + 2v_2(a)\,.$$

Now consider the admissible change of variables $x \longmapsto x$ and

$$y \longmapsto y - \left(a^2 - 4ab + 2b^2\right) x - a^3b^3 + 3a^2b^4 - 2ab^5.$$

This gives a $\mathbb{Q}$-isomorphism between E_T and the elliptic curve

$$
\begin{aligned}
&E'_T : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ where}\\
&a_1 = -3a^2 + 12ab - 6b^2\\
&a_2 = -2a^4 + 16a^3b - 41a^2b^2 + 35ab^3 - 10b^4\\
&a_3 = -3a^3b^3 + 9a^2b^4 - 6ab^5\\
&a_4 = -4a^5b^3 + 28a^4b^4 - 64a^3b^5 + 56a^2b^6 - 16ab^7\\
&a_6 = -2a^6b^6 + 12a^5b^7 - 26a^4b^8 + 24a^3b^9 - 8a^2b^{10}.
\end{aligned}
$$

We now use (2.2) to compute

$$
\begin{aligned}
b_2 &= a^4 - 8a^3b + 16a^2b^2 - 4ab^3 - 4b^4\\
b_6 &= a^6b^6 - 6a^5b^7 + 13a^4b^8 - 12a^3b^9 + 4a^2b^{10}\\
b_8 &= -a^8b^8 + 9a^7b^9 - 33a^6b^{10} + 63a^5b^{11} - 66a^4b^{12} + 36a^3b^{13} - 8a^2b^{14}.
\end{aligned}
$$

Since $v_2(a) \geq 2$, we observe that

$$
\begin{array}{lll}
v_3(a_1) = 1 & v_3(a_2) = 1 & v_3(a_3) = v_2(a) + 1\\
v_3(a_4) = 4 + v_2(a) & v_3(a_6) = 3 + 2v_2(a) & v_3(b_2) = 2\\
v_3(b_6) = 2 + 2v_2(a) & v_3(b_8) = 3 + 2v_2(a) &
\end{array}
$$

In particular, Tate's Algorithm runs through Step 6. Now let $a = 4\hat{a}$ for some integer $\hat{a}$ and consider the polynomial

$$
\begin{aligned}
P(T) &= T^3 + \frac{a_2}{2}T^2 + \frac{a_4}{4}T + \frac{a_6}{8}\\
&\equiv T^3 - 5b^4T^2 \mod 2 = T^2\,(T+1) \mod 2
\end{aligned}
$$

since $-5b^4$ is odd. Since this polynomial has a double root, we proceed to the subprocedure of Step 7 in Tate's Algorithm.

Now suppose $v_2(a) = 2$. Then $v_2(\gamma_T) = 11$. By the subprocedure of Step 7, we observe that $f_2 = 11 - k$ with $k \geq 5$. In particular, $f_2 \leq 6$.

If $v_2(a) = 3$, then $v_2(\gamma_T) = 13$. It suffices to show that E_T does not have reduction Type I_1^* at 2. Indeed, if this is the case, then $f_2 = 13 - k$ for $k \geq 6$ which implies that $f_2 \leq 7$. To this end, we observe that E_T has reduction Type I_1^* at 2 if and only if

$$Y^2 + \frac{a_3}{4} Y - \frac{a_6}{16} \mod 2 \tag{6.10}$$

has distinct roots over an algebraic closure of $\mathbb{F}_2$. But $4^{-1}a_3$ and $16^{-1}a_6$ are both even and therefore (6.10) is congruent to $Y^2 \mod 2$. This concludes the proof. ■

Lemma 6.13 *Let $T = C_9$. Then $v_3(N_T) \leq 3$.*

Proof By Theorem 5.25, E_T has additive reduction at 3 if and only if $a + b = 3k$ for some nonzero integer k. By Theorem 5.14, E_T is a global minimal model for E_T and therefore the minimal discriminant is γ_T. Note that

$$\gamma_T = 3^5 a^9 (3k-2a)^9 (3k-a)^9 \left(a^2 - 3ak + 3k^2\right)^3 \left(3k^3 - 9ak^2 + 6a^2k - a^3\right).$$

Consequently, $v_3(\gamma_T) = 5$ since a and k are not divisible by 3. Now consider the admissible change of variables $x \longmapsto x$ and $y \longmapsto y + 3$ which gives a $\mathbb{Q}$-isomorphic from E_T onto the elliptic curve

$$\begin{aligned}
&E_T' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ where}\\
&a_1 = 3\left(a^3 - 5a^2k + 12ak^2 - 9k^3\right)\\
&a_2 = 3a(2a-3k)(3k-a)^2\left(a^2 - 3ak + 3k^2\right)\\
&a_3 = 3\left(2a^9 - 21a^8k + 87a^7k^2 - 180a^6k^3 + 189a^5k^4 - 81a^4k^5 + 2\right)\\
&a_4 = 9\left(9k^3 - 12k^2 + 5a^2k - a^3\right)\\
&a_6 = 9\left(-2a^9 + 21a^8k - 87a^7k^2 + 180a^6k^3 - 189a^5k^4 + 81a^4k^5 - 1\right)
\end{aligned}$$

We now use (2.2) to compute

$$\begin{aligned}
b_2 &= 3\left(11a^6 - 114a^5k + 495a^4k^2 - 1134a^3k^3 + 1458a^2k^4 - 972ak^5 + 243k^6\right)\\
b_6 &= 9a^8(3k-2a)^2(3k-a)^4\left(a^2 - 3ak + 3k^2\right)^2\\
b_8 &= 27a^9(2a-3k)^3(3k-a)^6\left(a^2 - 3ak + 3k^2\right)^3.
\end{aligned}$$

In particular, 3 divides b_2, 9 divides a_6, and 27 divides b_8. However, 27 does not divide b_6 since a and k are not divisible by 3. By Tate's Algorithm, we conclude that

E_T has reduction Type IV at 3. Moreover, $f_3 = m_3 = c_3 = 3$. We note that $c_3 = 3$ since the polynomial

$$T^2 + \frac{a_3}{3}T - \frac{a_6}{9} \equiv T^2 + \left(2a^9 + 2\right)T + 2a^9 + 1 \mod 3$$
$$\equiv \begin{cases} T\left(T+1\right) \mod 3 & \text{if } a \equiv 1 \mod 3 \\ \left(T+1\right)\left(T+2\right) \mod 3 & \text{if } a \equiv 2 \mod 3 \end{cases}$$

has distinct roots over $\mathbb{F}_3$. ■

Lemma 6.14 *Let $T = C_2 \times C_2$ and suppose d is odd. If $v_2(a) = 1, 2, 3$, then $v_2(N_T) \leq 5$.*

Proof Since $v_2(a) = 1, 2, 3$, we have by Theorem 5.14 that E_T is a global minimal model for E_T. Thus

$$\Delta_{E_T}^{\min} = \gamma_T = 16a^2b^2d^6\left(a-b\right)^2$$

is the minimal discriminant of E_T. The admissible change of variables $x \longmapsto x+2$ and $y \longmapsto y + x + 6$ gives a $\mathbb{Q}$-isomorphism from E_T onto F where F is given by the Weierstrass model

$$F : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ where}$$

$$a_1 = 2 \qquad a_2 = ad + bd + 5 \qquad a_3 = 12$$
$$a_4 = d\left(abd + 4a + 4b\right) \qquad a_6 = 2\left(abd^2 + 2ad + 2bd - 14\right)$$

We now use (2.2) to compute

$$b_2 = 4\left(ad + bd + 6\right) \qquad b_6 = 8\left(bd + 2\right)\left(ad + 2\right)$$
$$b_8 = -a^2b^2d^4 + 24abd^2 + 32ad + 32bd + 48.$$

Observe that each a_j and b_j is even since a is even and bd is odd.

Case I. First assume $v_2(a) = 1$. Observe that

$$b_8 \equiv -a^2b^2d^4 \mod 8 = 4 \mod 8 \tag{6.11}$$

since bd is odd. Thus 8 does not divide b_8. Since 4 divides a_6, we have by Tate's Algorithm that E_T has reduction type III at 2 and $m_2 = c_2 = 2$. Since bd is odd, $v_2\left(\Delta_{E_T}^{\min}\right) = 6$ and so $f_2 = 5$.

Case II. Next, assume $v_2(a) = 2$. Then by (6.11), 8 divides b_8. Since 8 divides b_6, Tate's Algorithm continues to Step 6. By inspection, 4 divides a_3 and a_4. Now write $a = 4\hat{a}$ for some odd integer $\hat{a}$. Since $2^n k \equiv 2^n \mod 2^{n+1}$ holds for all positive integers n and odd integers k, we have

$$\begin{aligned} a_4 &\equiv 4\hat{a}bd^2 + 4bd \mod 8 \equiv 0 \mod 8 \\ a_6 &\equiv 8\hat{a}bd^2 + 4bd + 4 \mod 16 = 12 + 4bd \mod 16 \\ &\equiv \begin{cases} 0 \mod 16 & \text{if } bd \equiv 1 \mod 4 \\ 8 \mod 16 & \text{if } bd \equiv 3 \mod 4. \end{cases} \end{aligned}$$

In particular, 8 divides a_4 and a_6. Next, we consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{a_2}{2}T^2 + \frac{a_4}{4}T + \frac{a_6}{8} \\ &\equiv T^3 + \frac{bd+1}{2}T^2 + \frac{12+4bd}{8} \mod 2 \\ &\equiv \begin{cases} T^2(T+1) & \text{if } bd \equiv 1 \mod 4 \\ (T+1)(T^2+T+1) & \text{if } bd \equiv 3 \mod 4. \end{cases} \end{aligned}$$

Subcase I. Suppose $bd \equiv 1 \mod 4$. Then $P(T)$ has a double root over $\mathbb{F}_2$. Moreover, $a_2 \equiv 2 \mod 4$ and 16 divides a_6. In particular, the polynomial

$$Y^2 + \frac{a_3}{4}Y - \frac{a_6}{16} \equiv Y^2 + Y + k \mod 2$$

where k is either 0 or 1 has distinct roots over an algebraic closure of $\mathbb{F}_2$. By Tate's Algorithm, E_T has reduction type I_1^*. Moreover, $m_2 = 6$ and $f_2 = 3$ since $v_2\left(\Delta_{E_T}^{\min}\right) = 8$. Lastly, c_2 is either 2 or 4 with $c_2 = 4$ if and only if $k = 0$. Note that $k = 0$ if and only if $a_6 \equiv 0 \mod 32$. Observe that

$$a_6 \equiv 8\hat{a}bd^2 + 4bd + 20 \mod 32 = \begin{cases} 8\hat{a}d - 8 \mod 32 & \text{if } bd \equiv 1 \mod 8 \\ 8\hat{a}d + 8 \mod 32 & \text{if } bd \equiv 5 \mod 8. \end{cases}$$

From this we see that $k = 0$ if and only if either (i) $bd \equiv 1 \mod 8$ and $\hat{a}d \equiv 1 \mod 4$ or (ii) $bd \equiv 5 \mod 8$ and $\hat{a}d \equiv 3 \mod 4$.

Subcase II. Suppose $bd \equiv 3 \mod 4$. Then $P(T)$ has distinct roots over an algebraic closure of $\mathbb{F}_2$. Hence by Tate's Algorithm, E_T has reduction type I_0^* at 2. Moreover, $m_2 = 5$ and $c_2 = 2$. Since $v_2\left(\Delta_{E_T}^{\min}\right) = 8$, $f_2 = 4$.

Case III. Lastly, assume $v_2(a) = 3$. The admissible change of variables $x \longmapsto x + 4$ and $y \longmapsto y + x + 12$ gives a $\mathbb{Q}$-isomorphism from E_T onto F' where F' is given by the Weierstrass model

$$F' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \text{ where}$$

$$\begin{array}{lll} a_1' = 2 & a_2' = ad + bd + 11 & a_3' = 24 \\ a_4' = abd^2 + 8ad + 8bd + 24 & & a_6' = 4\left(abd^2 + 4ad + 4bd - 20\right). \end{array}$$

We now use (2.2) to compute

$$\begin{array}{ll} b_2' = 4\left(ad + bd + 12\right) & b_6' = 16\left(bd + 4\right)\left(ad + 4\right) \\ b_8' = -a^2b^2d^4 + 96abd^2 + 256ad + 256bd + 768. & \end{array}$$

Now observe that a_1' and b_2' are even, 8 divides a_3'. Now observe that

$$a_4' \equiv abd^2 + 8bd + 8 \mod 16 = 8 \mod 16$$
$$a_6' \equiv 16bd + 16 \mod 16 = 0 \mod 32.$$

Indeed, for an odd integer k, the congruences $2^n k \equiv 2^n \mod 2^{n+1}$ holds for all positive integers n. From this, it follows that $abd^2 \equiv 8 \mod 16$ since $v_2(a) = 3$. In particular, Tate's Algorithm runs through Step 6. Now consider the polynomial

$$\begin{aligned} P(T) &= T^3 + \frac{a_2'}{2}T^2 + \frac{a_4'}{4}T + \frac{a_6'}{8} \\ &\equiv T^2\left(T + \frac{bd-1}{2}\right) \mod 2 \\ &\equiv \begin{cases} T^3 \mod 2 & \text{if } bd \equiv 1 \mod 4 \\ T^2\left(T+1\right) \mod 2 & \text{if } bd \equiv 3 \mod 4. \end{cases} \end{aligned}$$

Subcase I. Suppose $bd \equiv 1 \mod 4$. Then 4 divides a_2' and we have that the polynomial $P(T)$ has a triple root over $\mathbb{F}_2$. Thus Tate's Algorithm continues to Step 8. Since the polynomial

$$Y^2 + \frac{a_3'}{4}Y - \frac{a_6'}{16} \equiv Y^2 \mod 2$$

we have that Tate Algorithm goes to Step 9. By Tate's Algorithm, we conclude that E_T has reduction type III^* at 2. Moreover, $m_2 = 8$, $c_2 = 2$, and $f_2 = 3$ since $v_2(\Delta_{E_T}^{\min}) = 10$.

Subcase II. Suppose $bd \equiv 3 \mod 4$. Then $P(T)$ has a double root over $\mathbb{F}_2$ and Tate's Algorithm continues to the subprocedure of Step 7. Since 4 does not divide a_2' we may proceed with the Weierstrass for F'. Next, the polynomial

$$Y^2 + \frac{a_3'}{4}Y - \frac{a_6'}{16} \equiv Y^2 \mod 2$$

has a double root over $\mathbb{F}_2$. Next, we claim that $a_6' \equiv 0 \mod 64$. To this end, write $bd = 3 + 4k$ for some integer k since $bd \equiv 3 \mod 4$. Then

$$a_6' \equiv 16 + 16bd \mod 64 = 16 + 16\,(3 + 4k) \mod 64 = 0 \mod 64.$$

In particular, the polynomial

$$\frac{a_2'}{2}X^2 + \frac{a_4'}{8}X + \frac{a_6'}{32} \equiv X\,(X+1) \mod 2$$

has distinct roots over $\mathbb{F}_2$. By Tate's Algorithm, we conclude that E_T has reduction type I_2^* at 2. Moreover, $m_2 = 7$, $c_2 = 4$, and $f_2 = 4$ since $v_2(\Delta_{E_T}^{\min}) = 10$. This concludes the proof. ∎

Example 6.15 *Let $T = C_2 \times C_2$ and consider the following elliptic curves:*

$$E_1 = E_T(20, 7, 13) \qquad E_2 = E_T(52, 11, 3)$$
$$E_3 = E_T(76, 11, 3) \qquad E_4 = E_T(40, 7, 11)\,.$$

We now use Lemma 6.14 to compute the local data at 2 of each E_j. Observe that $v_2(a) = 2$ for E_1, E_2, E_3 and $v_2(a) = 3$ for E_4. By the proof of Lemma 6.14 we *conclude that* E_4 *has reduction type* III^* *at* 2. *Moreover,* $m_2 = 8$, $c_2 = 2$, *and* $f_2 = 3$.

For E_1 *we note that* $bd \equiv 3 \mod 4$ *and so* E_1 *has reduction type* I_0^* *at* 2. *Moreover,* $m_2 = 5$, $c_2 = 2$, *and* $f_2 = 4$. *Both* E_2 *and* E_3 *satisfy* $bd \equiv 1 \mod 4$ *and so reduction type at* 2 *is* I_1^*. *Moreover,* $m_2 = 6$ *and* $f_2 = 3$. *It remains to compute the Tamagawa number at* 2. *For both* E_2 *and* E_3 *we have that* $bd \equiv 1 \mod 8$. *Since* $13 \cdot 3 \equiv 3 \mod 4$, *we have by the proof of Lemma 6.14 that* $c_2 = 2$ *for* E_2. *Similarly,* $19 \cdot 3 \equiv 1 \mod 4$ *and so* $c_2 = 4$ *for* E_3.

6.5 Upper Bound on the Conductor of E_T

Throughout this section, N_T will denote the conductor of E_T. For each T, we have by Theorem 5.14 that the minimal discriminant of E_T is $u_T^{-12}\gamma_T$. For each u_T, we let δ_T be as given in Table 6.2.

Table 6.2.: The Polynomials δ_{u_T}

T	u_T	δ_{u_T}
C_2	1	$2^7 3b^2d\,(b^2d - a^2)$
	2	$6b^2d\,(b^2d - a^2)$
	4	$\frac{3}{1024}b^2d\,(b^2d - a^2)$
C_3	c^2d	$3bd^2e^4\,(c^3d^2e - 27b)$
C_4	c	$4bc^2d^4\,(16b + c^2d)$
	$2c$	$3bc^2d^4\,(b + 16c^2d)$
C_5	1	$ab\,(a^2 + 11ab - b^2)$
C_6	1	$ab(a + b)\,(a + 9b)$
	2	$\frac{1}{64}ab\,(a + b)\,(a + 9b)$
C_7	1	$ab\,(a - b)\,(a^3 + 5a^2b - 8ab^2 + b^3)$
C_8	1	$ab(a - 2b)\,(a - b)\,(a^2 - 8ab + 8b^2)$

continued on next page

Table 6.2.: *continued*

T	u_T	δ_{u_T}
	2	$\frac{1}{16}ab\,(a-2b)\,(a-b)\,(a^2-8ab+8b^2)$
C_9	1	$ab\,(a-b)\,(a^2-ab+b^2)\,(a^3+3a^2b-6ab^2+b^3)$
C_{10}	1	$ab(a-2b)\,(a-b)\,(a^2+2ab-4b^2)(a^2-3ab+b^2)$
	2	$\frac{1}{16}ab\,(2b-a)\,(a-b)\,(a^2+2ab-4b^2)\,(a^2-3ab+b^2)$
C_{12}	1	$ab\,(a-2b)\,(a-b)\,(a^2-6ab+6b^2)\,(a^2-2ab+2b^2)\,(a^2-3ab+3b^2)$
	2	$\frac{1}{16}ab\,(a-2b)\,(a-b)\,(a^2-2ab+2b^2)\,(a^2-3ab+3b^2)\,(a^2-6ab+6b^2)$
$C_2\times C_2$	1	$144abd^3\,(a-b)$
	2	$\frac{9}{8}abd^3\,(b-a)$
$C_2\times C_4$	1	$8ab\,(a+4b)\,(a+8b)$
	2	$\frac{1}{2}ab\,(a+4b)\,(a+8b)$
	4	$\frac{1}{256}ab\,(a+4b)\,(a+8b)$
$C_2\times C_6$	1	$a\,(b-9a)\,(b-3a)\,(3a+b)\,(b-5a)\,(b-a)$
	4	$\frac{1}{64}a\,(a-b)\,(3a-b)\,(5a-b)\,(9a-b)\,(3a+b)$
	16	$\frac{1}{1024}a\,(b-9a)\,(b-3a)\,(3a+b)\,(b-5a)\,(b-a)$
$C_2\times C_8$	1	$2ab\,(a+2b)\,(a+4b)\,(a^2-8b^2)\,(a^2+8ab+8b^2)\,(a^2+4ab+8b^2)$
	16	$\frac{1}{512}ab\,(a+2b)\,(a+4b)\,(a^2-8b^2)\,(a^2+4ab+8b^2)\,(a^2+8ab+8b^2)$
	64	$\frac{1}{16384}ab\,(a+2b)\,(a+4b)\,(a^2-8b^2)\,(a^2+4ab+8b^2)\,(a^2+8ab+8b^2)$

We show that if the minimal discriminant of E_T is $u_T^{-12}\gamma_T$, then $N_T \leq |\delta_{u_T}|$.

Proposition 6.16 *Suppose $u_T^{-12}\gamma_T$ is the minimal discriminant of E_T. Then $N_T \leq |\delta_{u_T}|$ where δ_{u_T} is as given in Table 6.2.*

We will consider most cases separately in the following subsections.

6.5.1 Proof of Proposition 6.16 for $T = C_2$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either $1, 2$, or 4. By Theorem 5.25, E_T has additive reduction at each prime p dividing $\gcd(a, bd)$. Moreover, E_T has additive reduction at $p = 2$ if and only if $u_T = 1$ and $v_2(b^2d - a^2) \geq 4$ with $v_2(a) = v_2(b) = 1$, $d \equiv 1 \mod 4$, and $u_T \neq 4$.

Case I. Suppose $u_T = 1$. Then each prime dividing the minimal discriminant divides

$$\delta_{u_T} = 2^7 3 b^2 d \left(b^2 d - a^2\right)$$

Suppose E_T has additive reduction at an odd prime p. Then p divides $\gcd(a, bd)$. In particular, $v_p(\delta_{u_T}) \geq 2$. If $p \geq 5$, then $v_p(N_T) \leq 2$ which shows that $v_p(N_T) \leq v_p(\delta_{u_T})$.

Now suppose 3 divides $\gcd(a, bd)$.

Subcase I. Suppose 3 does not divide b. Then 3 divides d and we attain $v_3(\gamma_T) = 3$ and by Theorem 6.7 we have that $v_3(N_T) \leq 3$. Since $v_3(\delta_{u_T}) = 3$ it follows that $v_3(N_T) \leq v_3(\delta_{u_T})$.

Subcase II. Suppose 3 divides b. Then $v_3(\delta_{u_T}) \geq 5$ and so $v_3(N_T) \leq v_3(\delta_{u_T})$ since $v_3(N_T) \leq 5$.

If $b^2 d\left(b^2 d - a^2\right)$ is even, then $v_2(\delta_{u_T}) \geq 8$ and so $v_2(N_T) \leq v_2(\delta_{u_T})$ since $v_2(N_T) \leq 8$. So suppose $b^2 d\left(b^2 d - a^2\right)$ is odd. Then $v_2(\gamma_T) = 6$ and therefore $v_2(N_T) \leq 6$ by Theorem 6.7. This shows that $N_T \leq |\delta_{u_T}|$ in the case when $u_T = 1$.

Case II. Suppose $u_T = 2$. By Theorem 5.14 we have that either $v_2(b) \geq 3$ with $a \equiv -1 \mod 4$ or $v_2(b^2d - a^2) \geq 4$ with $v_2(a) = v_2(b) = 1$ and $d \equiv 1 \mod 4$.

Subcase I. First suppose $v_2(b) \geq 3$. Then $b = 8\hat{b}$ and the minimal discriminant of E_T is

$$u_T^{-12}\gamma_T = \hat{b}^2 d \left(64\hat{b}^2 d - a^2\right)^2.$$

In particular, each prime dividing the minimal discriminant divides

$$\begin{aligned} \delta_{u_T} &= 6 b^2 d \left(b^2 d - a^2\right) \\ &= 2^7 3 \hat{b}^2 d \left(64\hat{b}^2 d - a^2\right) \end{aligned}$$

By Theorem 5.25, E_T is semistable at 2. Consequently $v_2(N_T) \leq 1$. Now suppose E_T has additive reduction at an odd prime. By Theorem 5.25, p must divide $\gcd(a, bd)$. In particular, $v_p(\delta_{u_T}) \geq 2$. Since $v_p(N_T) \leq 2$ for $p \neq 3$, it follows that $v_p(N_T) \leq v_p(\delta_{u_T})$ for each odd prime $p \neq 3$. Now suppose E_T has additive reduction at 3. Then 3 divides $\gcd(a, bd)$. If 3 divides b, then $v_3(\delta_{u_T}) \geq 5$ and so $v_3(N_T) \leq v_3(\delta_{u_T})$. So suppose 3 divides d but not b. Then $v_3\big(u_T^{-12}\gamma_T\big) = 3$ since d is squarefree. By Theorem 6.7 we have that $v_3(N_T) \leq 3$. Consequently, $v_3(N_T) \leq v_3(\delta_{u_T})$ and so $N_T \leq |\delta_{u_T}|$ under the assumptions of this subcase.

Subcase II. Now suppose $v_2(b^2d - a^2) \geq 4$. Write $b^2d = 16k + a^2$ for some integer k and let $a = 2\hat{a}$ for some odd integer $\hat{a}$. Then the minimal discriminant is

$$u_T^{-12}\gamma_T = 16k^2\left(\hat{a}^2 + 4k\right)$$

In particular, every prime dividing the minimal discriminant divides

$$\begin{aligned}\delta_{u_T} &= 6b^2d\left(b^2d - a^2\right)\\ &= 2^7 3k\left(\hat{a}^2 + 4k\right)\end{aligned}$$

By Theorem 5.25, E_T has additive reduction at each odd prime dividing $\gcd(a, bd)$. Equivalently, E_T has additive reduction at each odd prime p dividing $\gcd(\hat{a}, k)$. If this is the case, then $v_p(\delta_{u_T}) \geq 2$. Consequently, if $p \geq 5$, then $v_p(N_T) \leq v_p(\delta_{u_T})$ since $v_p(N_T) \leq 2$. Now suppose $p = 3$. From Case I above, we observe that $v_3\big(u_T^{-12}\gamma_T\big) = 3$ if 3 does not divide b since $v_3(\gamma_T) = v_3\big(u_T^{-12}\gamma_T\big) = 3$. Therefore by Theorem 6.7 we have that $v_3(N_T) \leq 3$. Next suppose 3 divides b. Then $v_3(k) = v_3(\hat{a}^2 + 4k) = 2$ and so $v_3(\delta_{u_T}) = 5$ and therefore $v_3(N_T) \leq v_3(\delta_{u_T})$ since $v_3(N_T) \leq 5$.

By Theorem 5.25, E_T has additive reduction at 2. If $k\left(\hat{a}^2 + 4k\right)$ is odd, then $v_2\big(u_T^{-12}\gamma_T\big) = 4$ and so $v_2(N_T) \leq 4$ by Theorem 6.7. But $v_2(\delta_{u_T}) = 7$ and so $v_2(N_T) \leq v_2(\delta_{u_T})$. Lastly, if $k\left(\hat{a}^2 + 4k\right)$ is even, then $v_2(\delta_{u_T}) \geq 8$ which implies $v_2(N_T) \leq v_2(\delta_{u_T})$ since $v_2(N_T) \leq 8$.

Case III. Suppose $u_T = 4$. Then $v_2(b^2d - a^2) = 256k$ for some integer k and $a = 2\hat{a}$ for some odd integer $\hat{a}$. Write $b^2d = 256k + 4\hat{a}^2$. Then the minimal discriminant is

$$u_T^{-12}\gamma_T = k^2\left(\hat{a}^2 + 64k\right)$$

and each prime dividing the minimal discriminant divides

$$\begin{aligned}\delta_{u_T} &= \frac{3}{1024}b^2d\left(b^2d-a^2\right)\\ &= 3k\left(\hat{a}^2+64k\right)\end{aligned}$$

By Theorem 5.25 is semistable at 2 and therefore $v_2(N_T) \leq 1$. Moreover, E_T has additive reduction at an odd prime p if and only if p divides $\gcd(a, bd)$ which is equivalent to p dividing $\gcd(\hat{a}, k)$. If this is the case, then $v_p(\delta_{u_T}) \geq 2$. If $p \neq 3$, then $v_p(N_T) \leq v_p(\delta_{u_T})$. So it remains to show this inequality for $p = 3$. From Case I above, we observe that $v_3\left(u_T^{-12}\gamma_T\right) = 3$ if 3 does not divide b since $v_3(\gamma_T) = v_3\left(u_T^{-12}\gamma_T\right)$. Therefore by Theorem 6.7 we have that $v_3(N_T) \leq 3$. But if 3 does not divide b, then $v_3(k) = v_3(\hat{a}^2 + 64k) = 1$ and so $v_3(\delta_{u_T}) = 3$ which shows that $v_3(N_T) \leq v_3(\delta_{u_T})$. If 3 divides b, then $v_3(k) = v_3(\hat{a}^2 + 64k) = 2$ and so $v_3(\delta_{u_T}) = 5$ and therefore $v_3(N_T) \leq v_3(\delta_{u_T})$ since $v_3(N_T) \leq 5$. This concludes the proof. ∎

6.5.2 Proof of Proposition 6.16 for $T = C_3, C_5, C_7, C_9$

Proof Suppose $T = C_3$. Then the minimal discriminant of E_T is

$$\Delta_{E_T}^{\min} = b^3d^4e^8\left(c^3b^2e - 27b\right)$$

with $a = c^3d^2e$ where d and e are positive squarefree integers. Since

$$\delta_{u_T} = 3bd^2e^4\left(c^3d^2e - 27b\right)$$

it is clear that each prime p dividing $\Delta_{E_T}^{\min}$ divides δ_{u_T}. In particular, if E_T is semistable, then $N_T \leq |\delta_{u_T}|$.

Now suppose E_T has additive reduction at a prime $p \neq 3$. By Proposition 6.8, $v_p(N_T) \leq 2$ for each $p \neq 3$. By Theorem 5.25, E_T has additive reduction at a prime $p \neq 3$ if and only if p divides de. In particular, $p^2 | \delta_{u_T}$ and so $v_p(N_T) \leq v_p(\delta_{u_T})$ for each prime $p \neq 3$.

Now suppose E_T has additive reduction at $p = 3$. By Theorem 5.25, this occurs if and only if a is divisible by 3.

Case I. Suppose 3 divides e. Then $v_3(\delta_{u_T}) \geq 6$. But $v_3(N_T) \leq 5$ by Lemma 2.3 and so $v_3(N_T) \leq v_3(\delta_{u_T})$.

Case II. Suppose 3 divides d. Then $v_3(\delta_{u_T}) \geq 5$ and so $v_3(N_T) \leq v_3(\delta_{u_T})$ by Lemma 2.3.

Case III. Suppose 3 divides c. Then $v_3(\delta_{u_T}) \geq 4$. But if $v_3(a) = 3$, then $v_3(N_T) \leq 4$ by Proposition 6.8. If $v_3(a) \geq 4$, then $v_3(\delta_{u_T}) \geq 5$ and so we conclude that in either case $v_3(N_T) \leq v_3(\delta_{u_T})$.

By the above we conclude that $v_p(N_T) \leq v_p(\delta_{u_T})$ for all primes p and therefore $N_T \leq |\delta_{u_T}|$.

Suppose $T = C_5$. Then the minimal discriminant of E_T is γ_T and so $u_T = 1$. Moreover, it is clear that each prime dividing

$$\delta_{u_T} = ab\left(a^2 + 11ab - b^2\right)$$

divides γ_T. By Theorem 5.25, the only prime at which E_T can have additive reduction is 5 and so $v_p(N_T) \leq v_p(\delta_{u_T})$ for each prime $p \neq 5$. In particular, E_T has additive reduction at 5 if and only if $v_5(a + 3b) > 0$. So suppose $a + 3b = 5k$ for some integer k. Then $a = 5k - 3b$ and we verify that

$$\delta_{u_T} = 25b\,(3b - 5k)\left(b^2 - bk - k^2\right)$$

In particular, $v_5(\delta_{u_T}) \geq v_5(N_T) = 2$. Consequently, $N_T \leq |\delta_{u_T}|$.

Suppose $T = C_7$. Then the minimal discriminant of E_T is γ_T and so $u_T = 1$. Moreover, it is clear that each prime dividing

$$\delta_{u_T} = ab\,(a - b)\left(a^3 + 5a^2b - 8ab^2 + b^3\right)$$

divides γ_T. By Theorem 5.25, the only prime at which E_T can have additive reduction is 7 and so $v_p(N_T) \leq v_p(\delta_{u_T})$ for each prime $p \neq 7$. In particular, E_T has additive reduction at 7 if and only if $v_7(a + 4b) > 0$. Now let $a + 4b = 7k$ for some integer k. Then $a = 7k - 4b$ and we verify that

$$\delta_{u_T} = 49b\,(4b - 7k)\,(5b - 7k)\left(b^3 - 7bk^2 + 7k^3\right)$$

Thus $v_7(\delta_{u_T}) \geq v_7(N_T) = 2$. Consequently, $N_T \leq |\delta_{u_T}|$.

Lastly, suppose $T = C_9$. Then the minimal discriminant of E_T is γ_T and so $u_T = 1$. Moreover, it is clear that each prime dividing

$$\delta_{u_T} = ab\,(a-b)\left(a^2 - ab + b^2\right)\left(a^3 + 3a^2b - 6ab^2 + b^3\right)$$

divides γ_T. By Theorem 5.25, the only prime at which E_T can have additive reduction is 3 and so $v_p(N_T) \leq v_p(\delta_{u_T})$ for each prime $p \neq 3$. Furthermore, E_T has additive reduction at 3 if and only if $v_3(a+b) > 0$. Let $a + b = 3k$ for some integer k so that $a = 3k - b$. Then

$$\delta_{u_T} = 27b\,(b-3k)\,(2b-3k)\left(b^2 - 3bk + 3k^2\right)\left(b^3 - 3b^2k + 3k^3\right)$$

In particular, $v_3(\delta_{u_T}) \geq 3$. But by Lemma 6.13, $v_3(N_T) \leq 3$ and so $v_3(N_T) \leq v_3(\delta_{u_T})$. Thus $N_T \leq |\delta_{u_T}|$, which concludes the proof. ■

6.5.3 Proof of Proposition 6.16 for $T = C_4$

Proof Let $a = c^2 d$ with d a positive squarefree integer. By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either c or $2c$. Moreover, $u_T = 2c$ if and only if $v_2(a) \geq 8$ is even and $bd \equiv 3 \mod 4$.

Case I. Suppose $u_T = c$. Then the minimal discriminant of E_T is

$$\Delta_{E_T}^{\min} = u_T^{-12}\gamma_T = b^4 c^2 d^7 \left(16b + c^2 d\right)$$

Therefore each prime dividing $\Delta_{E_T}^{\min}$ divides

$$\delta_{u_T} = 4bc^2 d^4 \left(16b + c^2 d\right)$$

By Theorem 5.25, E_T has additive reduction at an odd prime p if and only if p divides d. But if this is the case, we have $v_p(\delta_{u_T}) \geq 4$. By Lemma 6.10 $v_p(N_T) \leq 2$ for all odd primes p. Thus $v_p(N_T) \leq v_p(\delta_T)$ for all odd primes p.

Now suppose E_T has additive reduction at 2. It follows by Theorem 5.25 that a is even.

Subcase I. Suppose $v_2(a) \leq 2$. Then $v_2(\delta_{u_T}) \geq 6$ and by Lemma 6.10 we have that $v_2(N_T) \leq 6$. Thus $v_2(N_T) \leq v_2(\delta_{u_T})$.

Subcase II. Suppose $v_2(a) \geq 3$. Then $v_2(\delta_{u_T}) \geq 8$ and therefore $v_2(N_T) \leq v_2(\delta_{u_T})$ by Lemma 2.3.

We conclude that if $u_T = c$, then $N_T \leq |\delta_{u_T}|$.

Case II. Suppose $u_T = 2c$ for some integer $\hat{c}$. Then $v_2(a) \geq 8$ is even and $bd \equiv 3 \mod 4$. In particular, $c = 2^4\hat{c}$ and observe that

$$\Delta_{E_T}^{\min} = u_T^{-12}\gamma_T = b^4\hat{c}^2d^7\left(b + 16\hat{c}^2d\right)$$

Consequently, each prime p dividing $\Delta_{E_T}^{\min}$ divides

$$\delta_{u_T} = 3bc^2d^4\left(b + 16c^2d\right)$$

By Theorem 5.25, E_T is semistable at 2 and so $v_2(N_T) \leq 1$. Moreover, E_T has additive reduction at an odd prime p if and only if p divides d. Since $v_p(\delta_{u_T}) \geq 4$ for each odd prime p we conclude that $v_p(N_T) \leq v_p(\delta_{u_T})$ for each odd prime $p \neq 3$ by Lemma 2.3. For $p = 3$, we observe that $v_3(\delta_{u_T}) \geq 5$ and thus $v_3(N_T) \leq v_3(\delta_{u_T})$.

We conclude that if $u_T = 2c$, then $N_T \leq |\delta_{u_T}|$. ■

6.5.4 Proof of Proposition 6.16 for $T = C_6$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. Moreover, $u_T = 2$ if and only if $v_2(a+b) \geq 3$.

Case I. Suppose $u_T = 1$. Then each prime dividing γ_T divides

$$\delta_{u_T} = ab(a+b)(a+9b)\,.$$

By Theorem 5.25, the only primes at which E_T can have additive reduction are 2 and 3. By Lemma 6.11, $v_p(N_T) \leq 2$ for all primes and so it suffices to check that $v_p(\delta_{u_T}) \geq 2$ if E_T has additive reduction at $p = 2, 3$. Indeed, E_T has additive reduction at 2 if and only if $v_2(a+b) = 1, 2$. In particular, $a + 9b$ is also even and we have $v_2(\delta_{u_T}) \geq 2$. Now suppose E_T has additive reduction at 3. This occurs if and only if

3 divides a. But then 3 divides $a + 9b$ and so $v_3(\delta_{u_T}) \geq 2$. Therefore $N_T \leq |\delta_{u_T}|$ if $u_T = 1$.

Case II. Suppose $u_T = 2$. Then $a + b = 8k$ and so $b = 8k - a$. Then

$$\Delta_{E_T}^{\min} = 2^{-12}\gamma_T = a^2k^3(9k-a)(a-8k)^6 \,.$$

In particular, each prime p dividing $\Delta_{E_T}^{\min}$ divides

$$\begin{aligned} \delta_{u_T} &= \frac{1}{64}ab\,(a+b)\,(a+9b) \\ &= -ak(9k-a)(a-8k)\,. \end{aligned}$$

By Theorem 5.25, E_T is semistable at 2 and additive reduction at 3 occurs if and only if 3 divides a. As before we observe that $v_3(\delta_T) \geq 2$ under these assumptions.

From the previous two cases, we conclude that $N_T \leq |\delta_{u_T}|$ for each u_T. ■

6.5.5 Proof of Proposition 6.16 for $T = C_8$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. Moreover, $u_T = 2$ if and only if $v_2(a) = 1$.

Case I. Suppose $u_T = 1$. It is automatic that each prime dividing γ_T divides

$$\delta_{u_T} = ab(a-2b)(a-b)\left(a^2 - 8ab + 8b^2\right)$$

By Theorem 5.25, E_T can only have additive reduction at 2. In fact, E_T has additive reduction at 2 if and only if $v_2(a) > 1$.

Subcase I. Suppose $v_2(a) = 2 + j$ where j is either 0 or 1. Then $v_2(\delta_{u_T}) \geq 6 + j$. By Lemma 6.12, $v_2(N_T) \leq 6 + j$ and so $v_2(N_T) \leq v_2(\delta_{u_T})$ which implies that $N_T \leq |\delta_{u_T}|$ for $u_T = 1$.

Subcase II. Suppose $v_2(a) \geq 4$. Then $v_2(\delta_{u_T}) \geq 8$ and $v_2(N_T) \leq 8$ by Lemma 2.3. Thus $N_T \leq |\delta_{u_T}|$ for $u_T = 1$.

Case II. Suppose $u_T = 2$. Then $v_2(a) = 1$ and by Theorem 5.25 we have that E_T is semistable. Let $a = 2\hat{a}$ for some odd integer $\hat{a}$ and observe that

$$\Delta_{E_T}^{\min} = 2^{-12}\gamma_T = \frac{1}{16}b^8\hat{a}^2(b-2\hat{a})^8(b-\hat{a})^4\left(2b^2 - 4b\hat{a} + \hat{a}^2\right)$$

Note that this is an integer since $b-\hat{a}$ is even. In particular, each prime p dividing $\Delta_{E_T}^{\min}$ divides

$$\begin{aligned}\delta_{u_T} &= \frac{1}{16}ab\,(a-2b)\,(a-b)\left(a^2-8ab+8b^2\right)\\ &= \hat{a}b(b-2\hat{a})(b-\hat{a})\left(2b^2-4b\hat{a}+\hat{a}^2\right).\end{aligned}$$

Since E_T is semistable, $\operatorname{rad}\left(\Delta_{E_T}^{\min}\right)=N_T$ and therefore $N_T\leq|\delta_{u_T}|$ for $u_T=2$. ■

6.5.6 Proof of Proposition 6.16 for $T=C_{10}$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. Moreover, $u_T=2$ if and only if a is even. Moreover, E_T can only have additive reduction at 5 by Theorem 5.25. In fact, E_T has additive reduction at 5 if and only if 5 divides $a+b$.

Case I. Suppose $u_T=1$. Then each prime dividing γ_T divides

$$\delta_{u_T}=ab(a-2b)(a-b)\left(a^2+2ab-4b^2\right)\left(a^2-3ab+b^2\right).$$

If E_T is semistable, then $N_T\leq|\delta_{u_T}|$. So suppose E_T has additive reduction at 5. Then $a+b=5k$ and setting $a=5k-b$ we observe that

$$\delta_{u_T}=25b(b-5k)(2b-5k)(3b-5k)\left(b^2-5k^2\right)\left(b^2-5bk+5k^2\right).$$

Thus $v_5(\delta_{u_T})\geq 2$ from which we conclude that $N_T\leq|\delta_{u_T}|$ if $u_T=1$.

Case II. Suppose $u_T=2$. Then $a=2\hat{a}$ for some integer $\hat{a}$ and we compute

$$\Delta_{E_T}^{\min}=2^{-12}\gamma_T=\hat{a}^5b^{10}(b-2\hat{a})^{10}(b-\hat{a})^5\left(b^2-\hat{a}b-\hat{a}^2\right)\left(b^2-6\hat{a}b+4\hat{a}^2\right)^2.$$

In particular, each prime dividing $\Delta_{E_T}^{\min}$ divides

$$\begin{aligned}\gamma_{u_T} &= \frac{1}{16}ab\,(2b-a)\,(a-b)\left(a^2+2ab-4b^2\right)\left(a^2-3ab+b^2\right)\\ &= \hat{a}b(b-2\hat{a})(b-\hat{a})\left(b^2-\hat{a}b-\hat{a}^2\right)\left(b^2-6\hat{a}b+4\hat{a}^2\right).\end{aligned}$$

It remains to consider the case when E_T has additive reduction at 5. To this end suppose $a+b=5j$ so that $b=5j-2\hat{a}$. Then

$$\gamma_{u_T} = 25\hat{a}(5j-4\hat{a})(5j-3\hat{a})(5j-2\hat{a})\left(5j^2-5j\hat{a}+\hat{a}^2\right)\left(5j^2-10j\hat{a}+4a^2\right)$$

and so $v_5(\delta_{u_T}) \geq 2$. Hence $N_T \leq |\delta_{u_T}|$ if $u_T = 2$, which concludes the proof. ■

6.5.7 Proof of Proposition 6.16 for $T = C_{12}$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. Moreover, $u_T = 2$ if and only if a is even. Since $C_6 \hookrightarrow E_T$, there exist relatively prime integers a' and b' such that $E_{C_{12}}(a,b)$ is $\mathbb{Q}$-isomorphic to $E_{C_6}(a',b')$. Therefore by Lemma 6.11, $v_p(N_T) \leq 2$ for each prime p.

Case I. Suppose $u_T = 1$. Then a is odd and each prime dividing γ_T divides

$$\delta_{u_T} = ab\,(a-2b)\,(a-b)\left(a^2-6ab+6b^2\right)\left(a^2-2ab+2b^2\right)\left(a^2-3ab+3b^2\right)$$

Therefore $v_p(N_T) \leq v_p(\delta_{u_T})$ for each prime $p \neq 3$. This inequality holds for $p = 3$ since E has additive reduction at 3 implies that 3 divides a by Theorem 5.25 and so $v_3(\delta_{u_T}) \geq 3$. Thus $N_T \leq |\delta_{u_T}|$ if $u_T = 1$.

Case II. Suppose $u_T = 2$. Then a is even and so $a = 2\hat{a}$ for some integer $\hat{a}$. Then

$$\begin{aligned}\Delta_{E_T}^{\min} = 2^{-12}\gamma_T = \hat{a}^2 b^{12}\,(b-2\hat{a})^{12}\,(b-\hat{a})^6\left(3b^2-6\hat{a}b+2\hat{a}^2\right)\\ \left(b^2-2\hat{a}b+2\hat{a}^2\right)^3\left(3b^2-6\hat{a}b+4\hat{a}^2\right)^4.\end{aligned}$$

In particular, each prime dividing $\Delta_{E_T}^{\min}$ divides

$$\begin{aligned}\delta_{u_T} &= \frac{1}{16}ab\,(a-2b)\,(a-b)\left(a^2-2ab+2b^2\right)\left(a^2-3ab+3b^2\right)\left(a^2-6ab+6b^2\right)\\ &= \hat{a}b\,(b-2\hat{a})\,(b-\hat{a})\left(3b^2-6\hat{a}b+2\hat{a}^2\right)\left(b^2-2\hat{a}b+2\hat{a}^2\right)\left(3b^2-6\hat{a}b+4\hat{a}^2\right)\end{aligned}$$

It suffices to show that $v_3(\delta_{u_T}) \geq 2$ if E_T has additive reduction at 3. But this is clear since E_T has additive reduction at 3 if and only if 3 divides a which is equivalent to 3 dividing $\hat{a}$. Therefore 27 divides δ_{u_T} from which we conclude that $N_T \leq |\delta_{u_T}|$ if $u_T = 2$. ■

6.5.8 Proof of Proposition 6.16 for $T = C_2 \times C_2$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either 1 or 2. By Theorem 5.25, E_T has additive reduction at all primes dividing d. Moreover, it has additive reduction at 2 if and only if ad is even and $u_T = 1$. Recall that by Lemma 5.12, we may assume a is even.

Case I. Suppose $u_T = 1$. Then every prime dividing the minimal discriminant divides

$$\delta_{u_T} = 2^4 3^2 abd^3 \left(a - b\right).$$

If E_T is semistable at a prime p, then $v_p(N_T) \leq v_p(\delta_{u_T})$. So suppose E_T has additive reduction at a prime $p \neq 2, 3$. Then $v_p(N_T) = 2$ and we note that $v_p(\delta_T) \geq 3$ since p divides d. Now suppose $p = 3$. Then $v_3(\delta_{u_T}) \geq 5$ since 3 divides d. But $v_3(N_T) \leq 5$ and so $v_3(N_T) \leq v_3(\delta_{u_T})$.

Now suppose $p = 2$. Then E_T has additive reduction at 2 if and only if ad is even. Recall that by Lemma 5.12, we may assume that a is even. Thus if d were even, we have $v_2(\delta_{u_T}) \geq 8$. Since $v_2(N_T) \leq 8$ we conclude that $v_2(N_T) \leq v_2(\delta_{u_T})$. So it remains to consider the case where d is odd. We now show that $v_2(N_T) \leq v_2(\delta_{u_T})$ also holds in the case when d is odd by considering two subcases.

Subcase I. Suppose $v_2(a) = j$ for $1 \leq j \leq 3$. Then $v_2(\delta_{u_T}) \geq 5$ and $v_2(N_T) \leq 5$ by Lemma 6.14.

Subcase II. Suppose $v_2(a) \geq 4$. Then $v_2(\delta_{u_T}) \geq 8$, but $v_2(N_T) \leq 8$ which concludes the case when $u_T = 1$.

Case II. Suppose $u_T = 2$. Then $v_2(a) \geq 4$ and $bd \equiv 1 \mod 4$. Then $a = 16\hat{a}$ and the minimal discriminant of E_T is

$$u_T^{-12}\gamma_T = \hat{a}^2 b^2 d^6 \left(b - 16\hat{a}\right).$$

In particular, each prime dividing the minimal discriminant divides

$$\begin{aligned} \delta_{u_T} &= \frac{9}{8} abd^3 \left(b - a\right) \\ &= 2 \cdot 3^2 \hat{a} bd^3 \left(b - 16\hat{a}\right). \end{aligned}$$

By Theorem 5.25, E_T is semistable at 2 and has additive reduction at an odd prime p if and only if p divides d. If $p \neq 3$, then $v_p(\delta_{u_T}) \geq 3$, but $v_p(N_T) \leq 2$. Lastly, if $p = 3$, then $v_3(\delta_{u_T}) \geq 5$. Since $v_3(N_T) \leq 5$, we conclude that $N_T \leq |\delta_{u_T}|$ in the case when $u_T = 2$. ■

6.5.9 Proof of Proposition 6.16 for $T = C_2 \times C_4$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either $1, 2$, or 4. By Theorem 5.25, E_T is semistable at all primes except possibly 2. Consequently, $v_p(N_T) \leq 1$ for all primes $p \neq 2$. Moreover, E_T has additive reduction at 2 if and only if $1 \leq v_2(a + 4b) \leq 3$.

By Proposition 5.7, E_T is $\mathbb{Q}$-isomorphic to $\mathcal{X}_{b/a}(C_2 \times C_4)$. From the Weierstrass equation of $\mathcal{X}_t$ in Table 2.1, it is clear that $\mathcal{X}_{b/a}(C_2 \times C_4) = \mathcal{X}_{t'}(C_4)$ where

$$t' = 4\left(\frac{b}{a}\right)^2 + \frac{b}{a} = \frac{4b^2 + ab}{a^2}.$$

Case I. Suppose $u_T = 1$ so that $v_2(a) \leq 1$. Then each prime dividing γ_T divides

$$\delta_{u_T} = 2^3 ab\,(a + 4b)\,(a + 8b)\,.$$

If a is odd, then E_T is semistable and so $N_T \leq |\delta_{u_T}|$. So suppose $v_2(a) = 1$. Then $v_2(\delta_{u_T}) = 6$. We claim that $v_2(N_T) \leq 6$. To this end, write $a = 2\hat{a}$ for some odd integer $\hat{a}$. Then

$$t' = \frac{2b^2 + \hat{a}b}{2\hat{a}^2}.$$

In particular, E_T is $\mathbb{Q}$-isomorphic to $E_{C_4}(2\hat{a}, 2b^2 + \hat{a}b)$ since $2\hat{a}$ is relatively prime to $2b^2 + \hat{a}b$. Since $v_2(2\hat{a}) = 1$, we conclude by Lemma 6.10 that $v_2(N_T) \leq 6$. Consequently, $N_T \leq |\delta_{u_T}|$ holds for $u_T = 1$.

Case II. Suppose $u_T = 2$ and $v_2(a) \geq 3$. Then $a = 8\hat{a}$ for some integer $\hat{a}$ and we have that

$$u_T^{-12}\gamma_T = 256\hat{a}^2 b^4\,(\hat{a} + b)^2\,(2\hat{a} + b)^4\,.$$

In particular, each prime dividing $u_T^{-12}\gamma_T$ divides

$$\begin{aligned}\delta_{u_T} &= \frac{1}{2}ab\,(a+4b)\,(a+8b)\\ &= 128\hat{a}b\,(\hat{a}+b)\,(2\hat{a}+b)\,.\end{aligned}$$

It follows that $v_2(\delta_{u_T}) \geq 8$ and so $v_2(N_T) \leq v_2(\delta_{u_T})$.

Case III. Suppose $u_T = 2$ and $v_2(a+4b) = 3$. Then $v_2(a) = 2$ and hence $a = 4\hat{a}$ for some odd integer $\hat{a}$. Since $a + 4b = 8k$ for some odd integer k, we attain that $a = 8k - 4b$. In particular, the minimal discriminant is

$$u_T^{-12}\gamma_T = 256b^4k^4\left(b^2-4k^2\right)^2.$$

Moreover, every prime dividing the minimal discriminant divides

$$\begin{aligned}\delta_{u_T} &= \frac{1}{2}ab\,(a+4b)\,(a+8b)\\ &= -64bk\left(b^2-4k^2\right).\end{aligned}$$

Thus $v_2(\delta_{u_T}) = 6$ since bk is odd. We claim that $v_2(N_T) \leq 6$. To this end, observe that

$$t' = \frac{bk}{2\,(b-2k)^2}$$

Therefore E_T is $\mathbb{Q}$-isomorphic to the elliptic curve $E_{C_4}\left(2\,(b-2k)^2, bk\right)$. Since bk is relatively prime to $2\,(b-2k)$, we have that $v_2\left(2\,(b-2k)^2\right) = 1$ we conclude by Lemma 6.10 that $v_2(N_T) = 3$.

Case III. Suppose $u_T = 4$ so that $a + 4b = 16k$ for some integer k. Then by Theorem 5.25, E_T is semistable at all primes and therefore $v_p(N_T) \leq 1$ for all primes p. The minimal discriminant of E_T is

$$u_T^{-12}\gamma_T = b^4k^4\left(b^2-16k^2\right)^2.$$

Therefore each prime dividing the minimal discriminant divides

$$\begin{aligned}\delta_{u_T} &= -\frac{1}{256}ab\,(a+4b)\,(a+8b)\\ &= bk\left(16k^2-b^2\right)\end{aligned}$$

and so $N_T \leq |\delta_{u_T}|$, which concludes the proof. ∎

6.5.10 Proof of Proposition 6.16 for $T = C_2 \times C_6$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either $1, 4$, or 16. By Theorem 5.25, E_T is semistable at all primes except possibly 3. Moreover, E_T has additive reduction at 3 if and only if b is divisible by 3. In particular, $v_p(N_T) \leq 1$ for all primes $p \neq 3$ and $v_3(N_T) \leq 2$ by Lemma 6.11. Indeed, since $C_6 \hookrightarrow E_T$, we have that E_T is $\mathbb{Q}$-isomorphic to $E_{C_6}(a', b')$ for some relatively prime integers a' and b'.

Case I. Suppose $u_T = 1$. Then $a + b$ is odd and we observe that each prime dividing the minimal discriminant γ_T divides

$$\delta_{u_T} = a\,(b-9a)\,(b-3a)\,(3a+b)\,(b-5a)\,(b-a)\,.$$

Moreover, if 3 divides b, it is clear that $v_3(\delta_{u_T}) \geq 2$. Consequently, $N_T \leq |\delta_{u_T}|$.

Case II. Suppose $u_T = 4$. Then $v_2(a+b) \geq 2$ and we write $a + b = 4k$ for some nonzero integer k. Then $a = 4k - b$ and we observe that

$$u_T^{-12}\gamma_T = 4\,(5b-18k)^2\,(3b-10k)^6\,(b-6k)^2\,(b-4k)^6\,(b-3k)^2\,(b-2k)^6\,.$$

In particular, each prime dividing the minimal discriminant divides

$$\begin{aligned}\delta_{u_T} &= \frac{1}{64}a\,(a-b)\,(3a-b)\,(5a-b)\,(9a-b)\,(3a+b)\\ &= (5b-18k)\,(3b-10k)\,(b-6k)\,(b-4k)\,(b-3k)\,(b-2k)\,.\end{aligned}$$

We note that if 3 divides b, then $v_3(\delta_{u_T}) \geq 3$ and so $N_T \leq |\delta_{u_T}|$.

Case III. Suppose $u_T = 16$. Then $v_2(a+b) = 1$. Write $a = 2k - b$ for some odd integer k. In the proof of Theorem 5.14, we established that

$$v_2((b-5a)\,(b-a)) \geq 5 \qquad v_2((b-9a)\,(b-3a)\,(3a+b)) \geq 6.$$

Consequently,

$$\delta_{u_T} = \frac{1}{1024}a\,(b-9a)\,(b-3a)\,(3a+b)\,(b-5a)\,(b-a)$$

is an integer and each prime dividing the minimal discriminant divides δ_{u_T}. Lastly, E_T can only have additive reduction at 3, which occurs exactly when 3 divides b. If this is the case, then $v_3(\delta_{u_T}) \geq 2$ and so $N_T \leq |\delta_{u_T}|$ which concludes the proof. ∎

6.5.11 Proof of Proposition 6.16 for $T = C_2 \times C_8$

Proof By Theorem 5.14, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either $1, 16$, or 64. By Theorem 5.25, E_T is semistable. Therefore $v_p(N_T) \leq 1$ for all primes p.

Case I. Suppose $u_T = 1$. Then a is odd and each prime dividing γ_T divides

$$\delta_{u_T} = 2ab\left(a+2b\right)\left(a+4b\right)\left(a^2-8b^2\right)\left(a^2+8ab+8b^2\right)\left(a^2+4ab+8b^2\right).$$

Thus $N_T \leq |\delta_{u_T}|$ for $u_T = 1$.

Case II. Suppose $u_T = 16$ so that $a = 2\hat{a}$ for an odd integer $\hat{a}$. Then

$$u_T^{-12}\gamma_T = \hat{a}^8 b^8\left(\hat{a}+b\right)^8\left(\hat{a}+2b\right)^8\left(\hat{a}^2+2\hat{a}b+2b^2\right)^4\left(\hat{a}^4+4\hat{a}^3b-8\hat{a}b^3-4b^4\right)^2.$$

In particular, each prime dividing the minimal discriminant divides

$$\begin{aligned}\delta_{u_T} &= \frac{1}{512}ab\left(a+2b\right)\left(a+4b\right)\left(a^2-8b^2\right)\left(a^2+4ab+8b^2\right)\left(a^2+8ab+8b^2\right)\\ &= \hat{a}k\left(\hat{a}+b\right)\left(\hat{a}+2b\right)\left(\hat{a}^2+2\hat{a}b+2b^2\right)\left(\hat{a}^4+4\hat{a}^3b-8\hat{a}b^3-4b^4\right)\end{aligned}$$

Thus $N_T \leq |\delta_{u_T}|$ for $u_T = 16$.

Case III. Suppose $u_T = 64$ so that $a = 4\hat{a}$ for a nonzero integer $\hat{a}$. Then

$$\begin{aligned}u_T^{-12}\gamma_T &= \frac{1}{16384}ab\left(a+2b\right)\left(a+4b\right)\left(a^2-8b^2\right)\left(a^2+4ab+8b^2\right)\left(a^2+8ab+8b^2\right)\\ &= \hat{a}^8b^8\left(\hat{a}+b\right)^8\left(2\hat{a}+b\right)^8\left(2\hat{a}^2+2\hat{a}b+b^2\right)^4\left(b^4+4\hat{a}b^3-8\hat{a}^3b-4\hat{a}^4\right)^2.\end{aligned}$$

Therefore each prime dividing the minimal discriminant divides

$$\delta_{u_T} = \hat{a}b\left(\hat{a}+b\right)\left(2\hat{a}+b\right)\left(2\hat{a}^2+2\hat{a}b+b^2\right)\left(b^4+4\hat{a}b^3-8\hat{a}^3b-4\hat{a}^4\right).$$

This shows that $N_T \leq |\delta_{u_T}|$, which concludes the proof. ■

6.6 Proof of Theorem 6.6

For the reader's convenience, we recall the quantities m_T and l_T defined earlier in the chapter:

$$l_T = \begin{cases} 1 & \text{if } T = C_1 \\ 1.5 & \text{if } T = C_2 \\ 2 & \text{if } T = C_3, C_4, C_2 \times C_2 \\ 3 & \text{if } T = C_5, C_6, C_2 \times C_4 \\ 4 & \text{if } T = C_7, C_8, C_2 \times C_6 \\ 4.5 & \text{if } T = C_9, C_{10} \\ 4.8 & \text{if } T = C_{12}, C_2 \times C_8 \end{cases} \quad \text{and } m_T = \begin{cases} 6 & \text{if } T = C_2, C_2 \times C_2 \\ 12 & \text{if } T = C_3, C_4, C_5, C_6, C_2 \times C_4 \\ 24 & \text{if } T = C_7, C_8, C_2 \times C_6 \\ 36 & \text{if } T = C_9, C_{10} \\ 48 & \text{if } T = C_{12}, C_2 \times C_8. \end{cases} \tag{6.12}$$

Lemma 6.17 *Let δ_{u_T} be as defined in Table 6.2. For $T = C_2$, let $B = b^2 d$. Then we have the following equalities:*

$$\begin{array}{rcll} |\delta_{u_T}(a,B)|^{l_T} & = & a^{m_T} \ \delta_{u_T}\big(1, \frac{B}{a^2}\big)^{\ l_T} & \textit{if } T = C_2 \\ |\delta_{u_T}(c,d,e,b)|^{l_T} & = & (cde)^{m_T} \ \delta_{u_T}\big(1,1,1, \frac{b}{c^3d^2e}\big)^{\ l_T} & \textit{if } T = C_3 \\ |\delta_{u_T}(c,d,b)|^{l_T} & = & (cd)^{m_T} \ \delta_{u_T}\big(1,1, \frac{b}{c^2d}\big)^{\ l_T} & \textit{if } T = C_4 \\ |\delta_{u_T}(a,b,d)|^{l_T} & = & (ad)^{m_T} \ \delta_{u_T}\big(1, \frac{b}{a}, 1\big)^{\ l_T} & \textit{if } T = C_2 \times C_2 \\ |\delta_{u_T}(a,b)|^{l_T} & = & a^{\ m_T}\delta_{u_T}\big(1, \frac{b}{a}\big)^{\ l_T} & \textit{for the remaining } T. \end{array}$$

Proof For $T \neq C_2, C_9, C_{10}, C_{12}, C_2 \times C_8$, it is easily verified that the equalities hold with the omission of the absolute value, which gives the lemma in these cases.

We now show by cases that equality holds for these remaining T

Case I. Suppose $T = C_2$. Then we check via a computer algebra system that the following equality holds:

$$\left(\delta_{u_T}(a,B)^{l_T}\right)^2 = \quad a^{m_T}\delta_{u_T}\left(\left(1, \frac{B}{a^2}\right)^{l_T}\right)^2.$$

In particular, the equality in the lemma holds.

Case II. Suppose $T = C_9, C_{10}$. Then via a computer algebra system, we verify that

$$\left(\delta_{u_T}(a,b)^{l_T}\right)^2 = \quad a^{m_T}\delta_{u_T}\left(\left(1,\frac{b}{a}\right)^{l_T}\right)^2.$$

This gives the lemma in this case as well.

Case III. Suppose $T = C_{12}, C_2 \times C_8$. As before, via a computer algebra system, it is verified that

$$\left(\delta_{u_T}(a,b)^{l_T}\right)^5 = \quad a^{m_T}\delta_{u_T}\left(\left(1,\frac{b}{a}\right)^{l_T}\right)^5$$

holds. This concludes the proof. ■

6.6.1 The Polynomials $\hat{\alpha}$, $\hat{\beta}$ for $T = C_2$, C_3, C_4, and $C_2 \times C_2$

In section 6.1, we established that for $T \neq C_2, C_2 \times C_2$ the following equalities hold

$$\alpha_T(a,b)^3 = a^{12}\alpha_T\left(1,\frac{b}{a}\right)^3 \qquad \beta_T(a,b)^2 = a_T^{12}\beta_T\left(1,\frac{b}{a}\right)^2. \tag{6.13}$$

Now suppose $T = C_3$ so that $a = c^3d^2e$ with d and e relatively prime positive squarefree integers. Let $\hat{\alpha}_T = \hat{\alpha}_T(c,d,e,b)$ and $\hat{\beta}_T = \hat{\beta}_T(c,d,e,b)$ such that $\hat{\alpha}_T(c,d,e,b) = \alpha_T(c^3d^2e,b)$ and $\hat{\beta}_T(c,d,e,b) = \beta_T(c^3d^2e,b)$.

Similarly for $T = C_4$, write $a = c^2d$ for d a positive squarefree integer Now let $\hat{\alpha}_T = \hat{\alpha}_T(c,d,b)$ and $\hat{\beta}_T = \hat{\beta}_T(c,d,b)$ such that $\hat{\alpha}_T(c,d,b) = \alpha_T(c^2d,b)$ and $\hat{\beta}_T(c,d,b) = \beta_T(c^2d,b)$.

Consequently, (6.13) yields the following equalities

$$\begin{aligned}
\hat{\alpha}_T(c,d,e,b)^3 &= (c^3d^2e)^{12}\,\hat{\alpha}_T\left(1,1,1,\tfrac{b}{c^3d^2e}\right)^3 && \text{if } T = C_3\\
\hat{\beta}_T(c,d,e,b)^2 &= (c^3d^2e)^{12}\,\hat{\beta}_T\left(1,1,1,\tfrac{b}{c^3d^2e}\right)^2 && \text{if } T = C_3\\
\hat{\alpha}_T(c,e,b)^3 &= (c^2d)^{12}\,\hat{\alpha}_T\left(1,1,\tfrac{b}{c^2d}\right)^3 && \text{if } T = C_4\\
\hat{\beta}_T(c,e,b)^2 &= (c^2d)^{12}\,\hat{\beta}_T\left(1,1,\tfrac{b}{c^2d}\right)^2 && \text{if } T = C_4
\end{aligned}$$

By Theorem 5.14 the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where $u_T = c^2d$. Therefore

$$u_T^{-12}\alpha_T(a,b)^3 = (cde)^{12}\,\hat{\alpha}_T\left(1,1,1,\frac{b}{c^3d^2e}\right)^3$$
$$u_T^{-12}\beta_T(a,b)^2 = (cde)^{12}\,\hat{\beta}_T\left(1,1,1,\frac{b}{c^3d^2e}\right)^2.$$

For $T = C_4$, the minimal discriminant of E_T is $u_T^{-12}\gamma_T$ where u_T is either c or $2c$. In particular,

$$c^{-12}\alpha_T(a,b)^3 = (cd)^{12}\,\hat{\alpha}_T\left(1,1,\frac{b}{c^2d}\right)^3$$
$$c^{-12}\beta_T(a,b)^2 = (cd)^{12}\,\hat{\beta}_T\left(1,1,\frac{b}{c^2d}\right)^2.$$

For $T = C_2$, we set $B = b^2d$ so that $\hat{\alpha}_T(a,B) = \alpha_T(a,b,d)$ and $\hat{\beta}(a,B) = \beta_T(a,b,d)$. Then

$$\alpha_T(a,b,d)^3 = a^{m_T}\hat{\alpha}_T\left(1,\frac{B}{a^2}\right)^3 \qquad \beta_T(a,b,d)^2 = a^6\hat{\beta}_T\left(1,\frac{B}{a^2}\right)^2$$

Lastly, for $T = C_2 \times C_2$ we saw that

$$\alpha_T(a,b,d)^3 = (ad)^6\,\alpha_T\left(1,\frac{b}{a},1\right)^3 \qquad \beta_T(a,b,d)^2 = (ad)^6\,\beta_T\left(1,\frac{b}{a},1\right)^2.$$

6.6.2 Real-Valued Functions

Let $u_T^{-12}\gamma_T$ be the minimal discriminant of E_T where u_T is as given in Theorem 5.14.For each u_T we define a real valued function $\varphi_{u_T} : \mathbb{R} \to \mathbb{R}$ given by

$$\varphi_{u_T}(x) = \begin{cases} u_T^{-12}\max\left\{\hat{\alpha}_T(1,x)^3\ ,\hat{\beta}_T(1,x)^2\right\} & \text{if } T = C_2 \\ u_T^{-12}\max\left\{\hat{\alpha}_T(1,1,1,x)^3\ ,\hat{\beta}_T(1,1,1,x)^2\right\} & \text{if } T = C_3 \\ u_T^{-12}\max\left\{\hat{\alpha}_T(1,1,x)^3\ ,\hat{\beta}_T(1,1,x)^2\right\} & \text{if } T = C_4 \\ u_T^{-12}\max\left\{\hat{\alpha}_T(1,x,1)^3\ ,\hat{\beta}_T(1,x,1)^2\right\} & \text{if } T = C_2 \times C_2 \\ u_T^{-12}\max\{\alpha_T(1,x)^3\ ,\beta_T(1,x)^2 & \text{otherwise.} \end{cases}$$

Next, define $\psi_{u_T} : \mathbb{R} \to \mathbb{R}$ by

$$\psi_{u_T}(x) = \begin{cases} \varphi_{u_T}(x)^2 - |\delta_{u_T}(1,x)|^3 & \text{if } T = C_2 \\ \varphi_{u_T}(x) - |\delta_{u_T}(1,1,1,x)|^{l_T} & \text{if } T = C_3 \\ \varphi_{u_T}(x) - |\delta_{u_T}(1,1,x)|^{l_T} & \text{if } T = C_4 \\ \varphi_{u_T}(x) - |\delta_{u_T}(1,x,1)|^{l_T} & \text{if } T = C_2 \times C_2 \\ \varphi_{u_T}(x)^2 - |\delta_{u_T}(1,x)|^{2l_T} & \text{if } T = C_9, C_{10} \\ \varphi_{u_T}(x)^5 - |\delta_{u_T}(1,x)|^{5l_T} & \text{if } T = C_{12}, C_2 \times C_8 \\ \varphi_{u_T}(x) - |\delta_{u_T}(1,x)|^{l_T} & \text{otherwise.} \end{cases} \tag{6.14}$$

Lemma 6.18 *Let* ψ_{u_T} *be as defined in* (6.14)*. Then* ψ_{u_T} *is nonnegative. Moreover, if* ψ_{u_T} *has a root, then the root is irrational. In particular, for* $x \in \mathbb{Q}$ *we have the following inequalities:*

$$\begin{aligned} |\delta_{u_T}(1,1,1,x)|^{l_T} &< \varphi_{u_T}(x) \quad \textit{if } T = C_3 \\ |\delta_{u_T}(1,1,x)|^{l_T} &< \varphi_{u_T}(x) \quad \textit{if } T = C_4 \\ |\delta_{u_T}(1,x,1)|^{l_T} &< \varphi_{u_T}(x) \quad \textit{if } T = C_2 \times C_2 \\ |\delta_{u_T}(1,x)|^{l_T} &< \varphi_{u_T}(x) \quad \textit{if otherwise.} \end{aligned}$$

Proof For each u_T, let `psiuT[x]` be the Mathematica input [30] for ψ_{u_T}. Then the following Mathematica inputs

`Reduce[psiuT[x]>=0,x,Reals]`	if $T = C_2 \times C_4$ and $u_T = 2$
`Reduce[psiuT[x]>0,x,Reals]`	otherwise

return `True` which verifies that ψ_{u_T} is nonnegative. Now suppose $T = C_2 \times C_4$ with $u_T = 2$. Then solving $\psi_{u_T}(x) = 0$ gives the solution set

$$\left\{-3 \pm \sqrt{5}, 1 \pm \sqrt{5}\right\}.$$

In particular, $\psi_{u_T}(x)$ is positive for all rational numbers x. Now observe that if n, m, and k are positive real numbers such that $n^k < m^k$, then $n < m$. From this, the last claim now follows. ∎

6.6.3 Proof of Theorem 6.6

We are now ready to prove Theorem 6.6.

Theorem 6.6. Let T be one of the fifteen torsion subgroups allowed by Theorem 2.1 and let l_T be as given in (6.7). If E is a rational elliptic curve with j-invariant $\neq 0, 1728$, then $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$, then $\sigma_m(E) \geq l_T$ where l_T is as given in (6.12).

Proof Let E be a rational elliptic curve with conductor N_E. By Theorem 6.7, $N_E \leq \ \Delta_E^{\min}\ $. Let c_4 and c_6 be the invariants associated to a global minimal model of E so that $1728\Delta_E^{\min} = c_4^3 - c_6^2$. From this, we obtain that $\ \Delta_E^{\min}\ < \max\{|c_4^3|, c_6^2\}$. In particular, $\sigma_m(E) > 1$ for all rational elliptic curves E.

Now suppose T is one of the fourteen non-trivial torsion subgroups allowed by Theorem 2.1. If $T \hookrightarrow E(\mathbb{Q})_{\text{tors}}$, then E is $\mathbb{Q}$-isomorphic to E_T for some integers a and b (and d in the case $T = C_2, C_2 \times C_2$). So it suffices to prove that $\sigma_m(E_T) \geq l_T$. Let c_4 and c_6 be the invariants associated with a global minimal model of E_T. By Theorem 5.14, $c_4 = u_T^{-4}\alpha_T$ and $c_6 = u_T^{-6}\beta_T$. In particular,

$$\max\{\ c_4^3\ , c_6^2\ = u_T^{-12}\max\{\ \alpha_T^3\ , \beta_T^2\ .$$

For $T = C_2$, let $B = b^2 d$. As we saw in the proof of Proposition 6.4,

$$\max\{\ \alpha_T^3\ , \beta_T^2\ = \begin{cases} a^{m_T}\max\Big\{\ \hat{\alpha}_T\big(1, \frac{B}{a^2}\big)^3\ , \hat{\beta}_T\big(1, \frac{B}{a^2}\big)^2\Big\} & \text{if } T = C_2 \\ (ad)^{m_T}\max\Big\{\ \alpha_T\big(1, \frac{b}{a}, 1\big)^3\ , \beta_T\big(1, \frac{b}{a}, 1\big)^2\Big\} & \text{if } T = C_2 \times C_2 \\ a^{m_T}\max\Big\{\ \alpha_T\big(1, \frac{b}{a}\big)^3\ , \beta_T\big(1, \frac{b}{a}\big)^2\Big\} & \text{otherwise.} \end{cases}$$

It suffices to show the existence of a number y_T such that $N_T < |y_T|^{l_T} < \max\{|c_4^3|, c_6^2\}$. Indeed, this would imply

$$\begin{aligned} \log N_T < l_T \log|y| &< \log\max\{\ c_4^3\ , c_6^2 \\ \implies \qquad \frac{l_T \log|y|}{\log N_T} &< \frac{\log\max\{|c_4^3|, c_6^2\}}{\log N_T} = \sigma_m(E_T)\,. \end{aligned}$$

Since $\frac{\log|y|}{\log N_T} > 1$ it follows that $l_T < \sigma_m(E_T)$. We now show this by cases.

Case I. Suppose $T = C_2$. Then

$$\varphi_{u_T}\left(\frac{B}{a^2}\right) = u_T^{-12} \max\left\{ \hat{\alpha}_T\left(1, \frac{B}{a^2}\right)^3, \hat{\beta}_T\left(1, \frac{B}{a^2}\right)^2 \right\}.$$

By Lemmas 6.17 and 6.18,

$$\begin{aligned} & \delta_{u_T}\left(1, \frac{B}{a^2}\right)^{1.5} < \varphi_{u_T}\left(\frac{B}{a^2}\right) \\ \Longrightarrow \quad & a^6 \ \delta_{u_T}\left(1, \frac{B}{a^2}\right)^{1.5} < a^6 \varphi_{u_T}\left(\frac{B}{a^2}\right) \\ \Longleftrightarrow \quad & |\delta_{u_T}(a, B)|^{1.5} < \max\{ c_4^3, c_6^2 \}. \end{aligned}$$

By Proposition 6.16, $N_T \leq |\delta_{u_T}(a, B)|^{1.5}$. Consequently, $\sigma_m(E_T) > 1.5$.

Case II. Suppose $T = C_3$. Then

$$\varphi_{u_T}\left(\frac{b}{c^3 d^2 e}\right) = u_T^{-12} \max\left\{ \hat{\alpha}_T\left(1, 1, 1, \frac{b}{c^3 d^2 e}\right)^3, \hat{\beta}_T\left(1, 1, 1, \frac{b}{c^3 d^2 e}\right)^2 \right\}.$$

By Lemmas 6.17 and 6.18,

$$\begin{aligned} & \delta_{u_T}\left(1, 1, 1, \frac{b}{c^3 d^2 e}\right)^2 < \varphi_{u_T}\left(\frac{b}{c^3 d^2 e}\right) \\ \Longrightarrow & (cde)^{12} \ \delta_{u_T}\left(1, 1, 1, \frac{b}{c^3 d^2 e}\right)^2 < (cde)^{12} \varphi_{u_T}\left(\frac{b}{c^3 d^2 e}\right) \\ \Longleftrightarrow & |\delta_{u_T}(c, d, e, b)|^2 < \max\{ c_4^3, c_6^2 \}. \end{aligned}$$

By Proposition 6.16, $N_T \leq |\delta_{u_T}(c, d, e, b)|^2$. Consequently, $\sigma_m(E_T) > 2$.

Case III. Suppose $T = C_4$. Then

$$\varphi_{u_T}\left(\frac{b}{c^2 d}\right) = u_T^{-12} \max\left\{ \hat{\alpha}_T\left(1, 1, \frac{b}{c^2 d}\right)^3, \hat{\beta}_T\left(1, 1, \frac{b}{c^2 d}\right)^2 \right\}.$$

By Lemmas 6.17 and 6.18,

$$\begin{aligned} & \delta_{u_T}\left(1, 1, \frac{b}{c^2 d}\right)^2 < \varphi_{u_T}\left(\frac{b}{c^2 d}\right) \\ \Longrightarrow & (cd)^{12} \ \delta_{u_T}\left(1, 1, \frac{b}{c^2 d}\right)^2 < (cd)^{12} \varphi_{u_T}\left(\frac{b}{c^2 d}\right) \\ \Longleftrightarrow & |\delta_{u_T}(c, d, b)|^2 < \max\{ c_4^3, c_6^2 \}. \end{aligned}$$

By Proposition 6.16, $N_T \leq |\delta_{u_T}(c,d,b)|^2$. Consequently, $\sigma_m(E_T) > 2$.

Case IV. Suppose $T = C_2 \times C_2$. Then

$$\varphi_{u_T}\left(\frac{b}{a}\right) = u_T^{-12} \max\left\{ \hat{\alpha}_T\left(1, \frac{b}{a}, 1\right)^3, \hat{\beta}_T\left(1, \frac{b}{a}, 1\right)^2 \right\}.$$

By Lemmas 6.17 and 6.18,

$$\begin{aligned} & \delta_{u_T}\left(1, \frac{b}{a}, 1\right)^2 < \varphi_{u_T}\left(\frac{b}{a}\right) \\ \Longrightarrow \quad & (ad)^6 \, \delta_{u_T}\left(1, \frac{b}{a}, 1\right)^2 < (ad)^6 \, \varphi_{u_T}\left(\frac{b}{a}\right) \\ \Longleftrightarrow \quad & |\delta_{u_T}(a,b,d)|^2 < \max\{ c_4^3, c_6^2 \}. \end{aligned}$$

By Proposition 6.16, $N_T \leq |\delta_{u_T}(a,b,d)|^2$. Consequently, $\sigma_m(E_T) > 2$.

Now let $T \neq C_2, C_3, C_4, C_2 \times C_2$. Then

$$\varphi_{u_T}\left(\frac{b}{a}\right) = u_T^{-12} \max\left\{ \alpha_T\left(1, \frac{b}{a}\right)^3, \beta_T\left(1, \frac{b}{a}\right)^2 \right\}.$$

By Lemmas 6.17 and 6.18,

$$\begin{aligned} & \delta_{u_T}\left(1, \frac{b}{a}\right)^{l_T} < \varphi_{u_T}\left(\frac{b}{a}\right) \\ \Longrightarrow \quad & a^{m_T} \, \delta_{u_T}\left(1, \frac{b}{a}\right)^{l_T} < a^{m_T} \varphi_{u_T}\left(\frac{b}{a}\right) \\ \Longleftrightarrow \quad & |\delta_{u_T}(a,b)|^{l_T} < \max\{ c_4^3, c_6^2 \}. \end{aligned}$$

By Proposition 6.16, $N_T \leq |\delta_{u_T}(a,b)|^{l_T}$. Consequently, $\sigma_m(E_T) > l_T$ which concludes the proof. ∎

The Theorem automatically implies the following corollary.

Corollary 6.19 *Let E be a rational elliptic curve such that $\sigma_m(E) \leq 1.5$. Then $E(\mathbb{Q})_{tors}$ is trivial.*

Now let n be a positive integer and consider the elliptic curve E_n given by the Weierstrass model

$$E_n : Y^2 + y = x^3 + nx.$$

Using (2.2), we compute

$$c_4 = -48n, \qquad c_6 = -216, \qquad \Delta_n = -\left(64n^3 + 27\right).$$

In particular, E_n is a global minimal model for E_n. Indeed, suppose $x \longmapsto u^2x + r$ and $y \longmapsto u^3y + u^2sx + w$ were an admissible change of variables between E_n and a global minimal model of E. Then by 2.4 $u, r, s, w \in \mathbb{Z}$ since E_n is given by an integral Weierstrass model. But then u^4 divides $\gcd(c_4, c_6)$. But this only occurs when $|u| = 1$. Thus E_n is a global minimal model for E_n.

Corollary 6.20 *If Δ_n is squarefree, then the elliptic curve E_n has trivial torsion subgroup for each positive integer n. Moreover, there are infinitely many n's such that Δ_n is squarefree and in particular,*

$$\lim_{n\to\infty,\ \Delta_n \ \textit{squarefree}} \sigma_m(E_n) = 1.$$

Proof Let N_{E_n} denote the conductor of E_n. If Δ_n is squarefree, then n is not divisible by 3. Moreover, since Δ_n is odd we have that these assumption imply that $\gcd(216, \Delta_n) = 1$ and so E_n is semistable. In particular, $N_{E_n} = \Delta_n$. Since

$$\Delta_n = -\left(4n+3\right)\left(16n^2 - 12n + 9\right)$$

is not divisible by some square of a linear polynomial in n with integral coefficient, we have by the main Theorem of [41] that there infinitely many n such that Δ_n is squarefree. To this end, it is easy to verify via Calculus that the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \frac{3\log(48x)}{\log(64x^3 + 27)}$$

is differentiable on $[1, \infty)$ and is monotonically decreasing. Moreover,

$$\lim_{x\to\infty} f(x) = 1.$$

Consequently,

$$\lim_{n\to\infty,\ \Delta_n \ \text{squarefree}} \sigma_m(E_n) = \lim_{n\to\infty,\ \Delta_n \ \text{squarefree}} \frac{3\log(48n)}{\log(64n^3 + 27)} = 1.$$

It remains to show that $E(\mathbb{Q})_{\text{tors}}$ is trivial whenever Δ_n is squarefree. Since $f(x)$ is monotonically decreasing, we have that for any positive integer j such that Δ_{n+j} is squarefree the inequality

$$\sigma_m(E_n) < \sigma_m(E_{n+j})$$

holds. Moreover, for each $x \geq 36$, $f(x) < 1.5$ and so by Corollary 6.19 $E_n(\mathbb{Q})_{\text{tors}}$ is trivial if $n \geq 36$ and Δ_n is squarefree. For $n < 36$, we verify via SageMath [29] that $E_n(\mathbb{Q})_{\text{tors}}$ is trivial. ∎

As a direct consequence of this corollary we have that 1 is in the set of limit points of $\sigma_m(E)$ where E ranges over all rational elliptic curves E.

7. CLASSIFICATION OF REDUCED MINIMAL MODELS

The goal of this chapter is to classify the reduced minimal models of rational elliptic curves with $T \hookrightarrow E(\mathbb{Q})$ where $T = C_N$ for $N = 3, \ldots, 10, 12$ or $T = C_2 \times C_8$. As in the previous two chapters, we will consider the elliptic curves $E_T = E_T(a, b)$ which parameterize all rational elliptic curves with $T \hookrightarrow E(\mathbb{Q})$. We recall, that for $T = C_3$, we need to consider those curves E which have j-invariant 0 separately. In section 1, we give a brief review of the reduced minimal model as well as a couple of results which will ease the use of the Laska-Kraus-Connell Algorithm in our setting. In section 2, we state the main theorem and in section 3 we provide its proof by considering each T separately. The proof relies on computer verification via Mathematica [30]. The reader is referred to Appendix C which contains a review of the Mathematica commands `Table` and `Mod` which we will use in the course of proving the main theorem. We conclude the chapter with examples.

7.1 Reduced Minimal Models and Torsion

Let E be a rational elliptic curve. As we saw in Chapter 2.3, E is $\mathbb{Q}$-isomorphic to a unique elliptic curve R known as the **reduced minimal model** of E. Recall that the reduced minimal model of E is an elliptic curve R which is $\mathbb{Q}$-isomorphic to E and whose Weierstrass model

$$R : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

has the property that R is a global minimal model for E and $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. Moreover, if c_4 and c_6 are the invariants associated with a global minimal model of E, then the Laska-Kraus-Connell Algorithm (Algorithm 2.8) computes the a_i's of the Weierstrass model of R:

$$\begin{aligned} b_2 &= -c_6 \mod 12 \in \{-5,-4,\ldots,6\} & b_4 &= \tfrac{b_2^2-c_4}{24} \\ b_6 &= \tfrac{-b_2^3+36b_2b_4-c_6}{216} & a_1 &= b_2 \mod 2 \in \{0,1\} \\ a_2 &= \tfrac{b_2-a_1}{4} & a_3 &= b_6 \mod 2 \in \{0,1\} \\ a_4 &= \tfrac{b_4-a_1a_3}{2} & a_6 &= \tfrac{b_6-a_3}{4} \end{aligned} \tag{7.1}$$

In particular, the quantities a_j and b_j are integers.

Table 7.1.: The Reduced Minimal Models R_j for $1 \le j \le 12$ where $R_j : y^2 + a_1xy + a_3y = x^3 + a_2x^2 - \frac{A}{48}x - \frac{B}{1728}$

j	a_1	a_2	a_3	A	B
1	0	0	0	c_4	$2c_6$
2	0	0	1	c_4	$2c_6 + 216$
3	0	-1	0	$c_4 - 16$	$2(-6c_4 + c_6 + 32)$
4	0	-1	1	$c_4 - 16$	$2(-6c_4 + c_6 + 248)$
5	0	1	0	$c_4 - 16$	$2(6c_4 + c_6 - 32)$
6	0	1	1	$c_4 - 16$	$2(6c_4 + c_6 + 184)$
7	1	0	0	$c_4 - 1$	$3c_4 + 2c_6 - 1$
8	1	0	1	$c_4 + 23$	$3c_4 + 2c_6 + 431$
9	1	-1	0	$c_4 - 9$	$-9c_4 + 2c_6 + 27$
10	1	-1	1	$c_4 + 15$	$-9c_4 + 2c_6 + 459$
11	1	1	0	$c_4 - 25$	$15c_4 + 2c_6 - 125$
12	1	1	1	$c_4 - 1$	$15c_4 + 2c_6 + 307$

Now suppose we run the Laska-Kraus-Connell Algorithm for an elliptic curve E with invariants c_4 and c_6 associated to a global minimal model of E. We show that computing a_1, a_2, and a_3 uniquely determines a_4 and a_6 in terms of c_4 and c_6.

In particular, there are exactly 12 possible reduced minimal models R_j for E with $j = 1, 2, \ldots, 12$. Table 7.1 gives the 12 possible Weierstrass models of R_j.

Lemma 7.1 *Let R be a rational elliptic curve given by the global minimal model*

$$R : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. Then a_4 and a_6 are uniquely determined by the invariants c_4 and c_6 of the Weierstrass model for R. In particular, there are 12 *possible reduced minimal models and they coincide with the ones given in Table 7.1.*

Proof Let $S_j : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where a_1, a_2, a_3 are as given in Table 7.1 for R_j. Computing the invariants c_4 and c_6 of the model of S_j yields

$$c_4 = \begin{cases} -48a_4 & \text{if } j = 1 \\ -48a_4 & \text{if } j = 2 \\ -16\,(3a_4 - 1) & \text{if } j = 3 \\ -16\,(3a_4 - 1) & \text{if } j = 4 \\ -16\,(3a_4 - 1) & \text{if } j = 5 \\ -16\,(3a_4 - 1) & \text{if } j = 6 \\ -\,(48a_4 - 1) & \text{if } j = 7 \\ -\,(48a_4 + 23) & \text{if } j = 8 \\ -3\,(16a_4 - 3) & \text{if } j = 9 \\ -3\,(16a_4 + 5) & \text{if } j = 10 \\ -\,(48a_4 - 25) & \text{if } j = 11 \\ -\,(48a_4 - 1) & \text{if } j = 12 \end{cases} \quad \text{and } c_6 = \begin{cases} -864a_6 & \text{if } j = 1 \\ -216\,(4a_6 + 1) & \text{if } j = 2 \\ -32\,(9a_4 + 27a_6 - 2) & \text{if } j = 3 \\ -8\,(36a_4 + 108a_6 + 19) & \text{if } j = 4 \\ -32\,(-9a_4 + 27a_6 + 2) & \text{if } j = 5 \\ -8\,(-36a_4 + 108a_6 + 35) & \text{if } j = 6 \\ -\,(-72a_4 + 864a_6 + 1) & \text{if } j = 7 \\ -\,(-72a_4 + 864a_6 + 181) & \text{if } j = 8 \\ -27\,(8a_4 + 32a_6 - 1) & \text{if } j = 9 \\ -27\,(8a_4 + 32a_6 + 11) & \text{if } j = 10 \\ -\,(-360a_4 + 864a_6 + 125) & \text{if } j = 11 \\ -\,(-360a_4 + 864a_6 + 161) & \text{if } j = 12 \end{cases}$$

For each j, solving for a_4 and a_6 in terms of c_4 and c_6 allows us to verify that $a_4 = -\frac{A}{48}$ and $a_6 = -\frac{B}{1728}$ for A and B as given in Table 7.1 in terms of c_4 and c_6. Hence $R_j = S_j$ for each j. ■

As a result, given a rational elliptic curve E with invariants c_4 and c_6 associated to a global minimal model of E, the reduced minimal model is uniquely determined upon computing a_1, a_2, and a_3. The next result simplifies the computation of a_3 in the Laska-Kraus-Connell Algorithm:

Lemma 7.2 *Let E be a rational elliptic curve E with invariants c_4 and c_6 associated to a global minimal model of E and let R be the reduced minimal model of E. Let b_2 and b_4 be as in* (7.1)*. If these quantities are known, then the invariant a_3 of R is*

$$a_3 = \begin{cases} 0 & \textit{if } -b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16 \\ 1 & \textit{if } -b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16 \end{cases}$$

Proof Observe that $a_3 \equiv b_6 \mod 2 \in \{0, 1\}$ and

$$b_6 = \frac{-b_2^3 + 36b_2b_4 - c_6}{216}.$$

In particular, $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 8$ since $216 = 8 \cdot 27$. Thus b_6 is even if and only if $-b_2^3 + 36b_2b_4 - c_6$ is divisible by 16. ■

7.2 Classification of Reduced Minimal Models

Let c_4 and c_6 be the invariants associated to a global minimal model of $E_T = E_T(a, b)$ for some integers a and b. By Theorem 5.14 we have necessary and sufficient conditions on a and b so that $c_4 = u_T^{-4}\alpha_T(a, b)$ and $c_6 = u_T^{-6}\beta_T(a, b)$ for u_T as defined in Theorem 5.14. The following Theorem gives necessary and sufficient conditions on a and b for E_T to be $\mathbb{Q}$-isomorphic to R_j for some j for $T = C_N$ where $N = 3, \ldots, 10, 12$ or $T = C_3^0, C_2 \times C_8$. Recall that E_T with $T = C_3$ parameterizes all rational elliptic curves E with non-zero j-invariant such that $C_3 \hookrightarrow E(\mathbb{Q})$. Whereas E_T for $T = C_3^0$, parameterizes all rational elliptic curves E with j-invariant 0 such that $C_3 \hookrightarrow E(\mathbb{Q})$. With this terminology, we now state the main Theorem of this chapter.

Theorem 7.3 *Let $T = C_N$ where $N = 3, \ldots, 10, 12$ or $T = C_3^0, C_2 \times C_8$. Then the reduced minimal model of E_T for $T = C_{10}, C_2 \times C_8$ is R_7. For the remaining T, Table 7.2 lists the necessary and sufficient conditions on a and b for R_j to be the reduced minimal model of E_T.*

Table 7.2.: Necessary and Sufficient Conditions for R_j

T	Conditions to determine R_j
C_3	$R_1 \iff a \equiv 0 \mod 6$ *and* $3 \nmid v_2(a)$
	$R_2 \iff a \equiv 0 \mod 6$ *and* $3 \vert v_2(a)$
	$R_5 \iff a \equiv \pm 2 \mod 6$*and* $3 \nmid v_2(a)$
	$R_6 \iff a \equiv \pm 2 \mod 6$ *and* $3 \vert v_2(a)$
	$R_7 \iff a \equiv \pm 1 \mod 6$ *and b is even*
	$R_8 \iff a \equiv \pm 1 \mod 6$ *and b is odd*
	$R_9 \iff a \equiv 3 \mod 6$ *and b is odd*
	$R_{10} \iff a \equiv 3 \mod 6$ *and b is even*
C_3^0	$R_1 \iff$ *a is even*
	$R_2 \iff$ *a is odd*
C_4	$R_1 \iff$ *$u_T = c$, a is even, and either $3 \nmid ab\,(a+b)$ or $v_3(a)$ is odd*
	$R_3 \iff$ *$u_T = c$, a is even, and either $3 \vert\,(a+b)$ or $v_3(a) > 0$ is even with $bd \equiv 1, 4 \mod 6$*
	$R_5 \iff$ *$u_T = c$, a is even, and either $3 \vert b$ or $v_3(a) > 0$ is even with $bd \equiv 2, 5 \mod 6$*
	$R_7 \iff$ *one of the following holds: (i) a is odd and either $3 \vert b$ or $v_3(a) > 0$ is even with $bd \equiv 2, 5 \mod 6$ or (ii) $u_T = 2c$, $bd \equiv 7, 15 \mod 16$, and either $3 \vert b$ or $v_3(a) > 0$ is even with $bd \equiv 11 \mod 12$*
	$R_8 \iff$ *$u_T = 2c$, $bd \equiv 3, 11 \mod 16$, and either $3 \vert b$ or $v_3(a) > 0$ is even with $bd \equiv 11 \mod 12$*
	$R_9 \iff$ *$u_T = 2c$, $bd \equiv 3, 11 \mod 16$, and either $3 \nmid ab\,(a+b)$ or $v_3(a)$ is odd*

continued on next page

Table 7.2.: continued

T			Conditions to determine R_j
	R_{10}	$\Longleftrightarrow$	*one of the following holds:* (i) a *is odd and either* $3 \nmid ab\,(a+b)$ *or* $v_3(a)$ *is odd or* (ii) $u_T = 2c$, $bd \equiv 7, 15 \mod 16$, *and either* $3 \nmid ab\,(a+b)$ *or* $v_3(a)$ *is odd*
	R_{11}	$\Longleftrightarrow$	$u_T = 2c$, $bd \equiv 3, 11 \mod 16$, *and either* $3 \mid (a+b)$ *or* $v_3(a) > 0$ *with* $bd \equiv 7 \mod 12$
	R_{12}	$\Longleftrightarrow$	*one of the following holds:* (i) a *is odd and either* $3 \mid (a+b)$ *or* $v_3(a) > 0$ *is even with* $bd \equiv 1, 4 \mod 6$ *or* (ii) $u_T = 2c$, $bd \equiv 7, 15 \mod 16$, *and either* $3 \mid (a+b)$ *or* $v_3(a) > 0$ *with* $bd \equiv 7 \mod 12$
C_5	R_4	$\Longleftrightarrow$	$ab \equiv \pm 1 \mod 6$
	R_6	$\Longleftrightarrow$	$ab \equiv 3 \mod 6$
	R_7	$\Longleftrightarrow$	$ab \equiv 0 \mod 6$
	R_{12}	$\Longleftrightarrow$	$ab \equiv \pm 2 \mod 6$
C_6	R_1	$\Longleftrightarrow$	$a \equiv 3 \mod 6$ *with* $v_2(a+b) = 1, 2$
	R_5	$\Longleftrightarrow$	$a \equiv \pm 1 \mod 6$ *with* $v_2(a+b) = 1, 2$
	R_7	$\Longleftrightarrow$	$a \equiv \pm 1 \mod 6$ *with* $v_2(a+b) \neq 1, 2, 3$
	R_8	$\Longleftrightarrow$	*either* $a \equiv \pm 2 \mod 6$ *or* $a \equiv \pm 1 \mod 6$ *with* $v_2(a+b) = 3$
	R_9	$\Longleftrightarrow$	*either* $a \equiv 0 \mod 6$ *or* $a \equiv 3 \mod 6$ *with* $v_2(a+b) = 3$
	R_{10}	$\Longleftrightarrow$	$a \equiv 3 \mod 6$ *with* $v_2(a+b) \neq 1, 2, 3$
C_7	R_7	$\Longleftrightarrow$	$a + b \equiv \pm 1 \mod 3$
	R_{10}	$\Longleftrightarrow$	$a + b \equiv 0 \mod 3$
C_8	R_3	$\Longleftrightarrow$	$a \equiv 0 \mod 12$
	R_5	$\Longleftrightarrow$	$a \equiv \pm 4 \mod 12$
	R_7	$\Longleftrightarrow$	$a \equiv \pm 1, \pm 2, \pm 5 \mod 12$
	R_{12}	$\Longleftrightarrow$	$a \equiv \pm 3, 6 \mod 12$

continued on next page

Table 7.2.: continued

T	Conditions to determine R_j		
C_9	R_7	$\iff$	$a+b \equiv \pm 1 \mod 3$
	R_{10}	$\iff$	$a+b \equiv 0 \mod 3$
C_{12}	R_7	$\iff$	$a \equiv \pm 1, \pm 2, \pm 5 \mod 12$
	R_8	$\iff$	$a \equiv \pm 4 \mod 12$
	R_9	$\iff$	$a \equiv 0 \mod 12$
	R_{10}	$\iff$	$a \equiv \pm 3, 6 \mod 12$

7.3 Proof of Theorem 7.3

The proof relies on computer verification via Mathematica [30] and we refer the reader to Appendix C which reviews the Mathematica inputs `Mod` and `Table`. In what follows the Mathematica inputs `c4[a,b]` and `c6[a,b]` will refer to $c_4 = u_T^{-4}\alpha_T(a,b)$ and $c_6 = u_T^{-6}\beta_T(a,b)$ where T will be known from context. Moreover, for each T we will compute $-c_6 \mod 12$ and $-b_2^3 + 36b_2b_4 - c_6 \mod 16$ via the Mathematica inputs `Mod` and `Table`. The Mathematica input `V[a,b]` will correspond to $-b_2^3 + 36b_2b_4 - c_6$ where b_2 and b_4 are as defined in the Laska-Kraus-Connell Algorithm (7.1). For $T = C_3$, we will prove most of the result directly, but for the remaining T, we will use Mathematica to compute the congruences in the Laska-Kraus-Connell Algorithm.

The proof of the Theorem follows the same structure for each case presented below. Namely, we first compute $-c_6 \mod 12$ from which we deduce b_2, a_1, and a_2 as defined in the Laska-Kraus-Connell Algorithm. Next we use Lemma 7.2 to compute a_3, namely checking the congruence $-b_2^3 + 36b_2b_4 - c_6 \mod 16$. This will conclude the proof of each case since by Lemma 7.1, the reduced minimal model is uniquely determined by a_1, a_2, and a_3.

7.3.1 Proof of Theorem 7.3 for $T = C_3$

Theorem 7.3 for $T = C_3$. The reduced minimal model of E_T is

$$\begin{array}{cccl}
(i) & R_1 & \Longleftrightarrow & a \equiv 0 \mod 6 \text{ and } 3 \nmid v_2(a) \\
(ii) & R_2 & \Longleftrightarrow & a \equiv 0 \mod 6 \text{ and } 3 | v_2(a) \\
(iii) & R_5 & \Longleftrightarrow & a \equiv \pm 2 \mod 6 \text{ and } 3 \nmid v_2(a) \\
(iv) & R_6 & \Longleftrightarrow & a \equiv \pm 2 \mod 6 \text{ and } 3 | v_2(a) \\
(v) & R_7 & \Longleftrightarrow & a \equiv \pm 1 \mod 6 \text{ and } b \text{ is even} \\
(vi) & R_8 & \Longleftrightarrow & a \equiv \pm 1 \mod 6 \text{ and } b \text{ is odd} \\
(vii) & R_9 & \Longleftrightarrow & a \equiv 3 \mod 6 \text{ and } b \text{ is odd} \\
(viii) & R_{10} & \Longleftrightarrow & a \equiv 3 \mod 6 \text{ and } b \text{ is even}
\end{array}$$

Proof By the proof of Theorem 5.14 the invariants c_4 and c_6 associated to a global minimal model of $E_T(a, b)$ are

$$c_4 = cd^2e^3 (a - 24b) \qquad \text{and} \qquad c_6 = -d^2e^4 \left(a^2 - 36ab + 216b^2\right)$$

where $a = c^3d^2e$ with d and e relatively prime squarefree positive integers. Consequently $-c_6 \equiv c^6d^6e^6 \mod 12$. Note that it suffices to prove the converse of statements (i) through $(viii)$ since these exhausts all possibilities for a and b.

Case I. Suppose $a \equiv 0 \mod 6$. Then $-c_6 \equiv 0 \mod 6$ and therefore $b_2 = a_1 = a_2 = 0$. We now consider,

$$-b_2^3 + 36b_2b_4 - c_6 \equiv 8b^2d^2e^4 \mod 16$$

since $a \equiv 0 \mod 6$. By Lemma 7.2,

$$a_3 = \begin{cases} 0 & \text{if } de \text{ is even} \\ 1 & \text{if } de \text{ is odd} \end{cases} \qquad \Longleftrightarrow \qquad a_3 = \begin{cases} 0 & \text{if } 3 \nmid v_2(a) \\ 1 & \text{if } 3 | v_2(a) \end{cases}$$

since $3 | v_2(a)$ if and only if de is odd. This shows the converse of (i) and (ii).

Case II. Suppose $a \equiv \pm 2 \mod 6$. Then $a^2 = c^6d^4e^2 \equiv 4 \mod 12$ and therefore

$$-c_6 = 4d^2e^4 \mod 12.$$

Since de is not divisible by 3 it follows that $-c_6 \equiv 4 \mod 12$ since $4k^2 \equiv 4 \mod 12$ for all integers k not divisible by 3. Therefore $b_2 = 4$ and thus $a_1 = 0$ and $a_2 = 1$. Since $a \equiv \pm 2 \mod 6$, it follows that 2 divides cde and so

$$-b_2^3 + 36b_2b_4 - c_6 \equiv 8b^2d^2e^4 \mod 16$$

and so by Lemma 7.2,

$$a_3 = \begin{cases} 0 & \text{if } de \text{ is even} \\ 1 & \text{if } de \text{ is odd} \end{cases} \quad \Longleftrightarrow \quad a_3 = \begin{cases} 0 & \text{if } 3 \nmid v_2(a) \\ 1 & \text{if } 3 | v_2(a) \end{cases}$$

This shows the converse of (iii) and (iv).

Case III. Suppose $a \equiv \pm 1 \mod 6$. Then $a^2 = c^6d^4e^2 \equiv 1 \mod 12$. Thus

$$-c_6 \equiv d^2e^4 \mod 12.$$

Since $de \equiv \pm 1 \mod 6$ we have $-c_6 \equiv 1 \mod 12$. Hence $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. We now compute

$$\begin{aligned} -b_2^3 + 36b_2b_4 - c_6 &= \frac{1 - 3c^4d^4e^4}{2} + 36bcd^2e^3 + 216b^2d^2e^4 - 36bc^3d^4e^5 + c^6d^6e^6 \\ &= \frac{1 - 3k^4}{2} + 36l\left(1 - k^2\right) + k^6 + 216b^2d^2e^4 \end{aligned}$$

where $k = cde$ and $l = bcd^2e^3$. Since $a \equiv \pm 1 \mod 6$, we have that k is odd. Using Mathematica, we verify that

$$\frac{1 - 3k^4}{2} + 36l\left(1 - k^2\right) + k^6$$

is divisible by 16 via the input

```
Table[Mod[(1-3*k^4)/2+36*l*(1-k^2)+k^6,16],{k,1,16,2},{l,0,16}]
```

Therefore

$$-b_2^3 + 36b_2b_4 - c_6 \equiv 8b^2d^2e^4 \mod 16.$$

By Lemma 7.2,

$$a_3 = \begin{cases} 0 & \text{if } b^2d^2e^4 \text{ is even} \\ 1 & \text{if } b^2d^2e^4 \text{ is odd} \end{cases} \quad \Longleftrightarrow \quad a_3 = \begin{cases} 0 & \text{if } b \text{ is even} \\ 1 & \text{if } b \text{ is odd} \end{cases}$$

This shows the converse of (v) and (vi).

Case IV. Lastly, suppose $a \equiv 3 \mod 6$. Then $a \equiv \pm 3 \mod 12$ and so $a^2 = c^6 d^4 e^2 \equiv 9 \mod 12$. Thus

$$-c_6 \equiv 9d^2e^4 \mod 12 = 9 \mod 12.$$

since $de \equiv \pm 1, \pm 3 \mod 12$ implies that $d^2e^4 \equiv 1, 9 \mod 12$. Hence $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. Then

$$\begin{aligned} -b_2^3 + 36b_2b_4 - c_6 &= \frac{9c^4d^4e^4 - 27}{2} - 36bcd^2e^3\left(3 + c^2d^2e^2\right) + c^6d^6e^6 + 216b^2d^2e^2 \\ &= \frac{9k^4 - 27}{2} - 36l\left(3 + k^2\right) + k^6 + 216b^2d^2e^2 \end{aligned}$$

where $k = cde$ and $l = bcd^2e^3$. Since $a \equiv 3 \mod 6$, it follows that k is odd. We now verify that

$$\frac{9k^4 - 27}{2} - 36l\left(3 + k^2\right) + k^6 \tag{7.2}$$

is not divisible by 16 via the Mathematica input

```
Table[Mod[(9*k^4-27)/2-36*l*(3+k^2)+k^6,16],{k,1,16,2},{l,0,16}]
```

In fact, through Mathematica we see that expression (7.2) is congruent to8 modulo 16. Therefore

$$-b_2^3 + 36b_2b_4 - c_6 \equiv 8 + 8b^2d^2e^2 \mod 16$$

and so

$$a_3 = \begin{cases} 0 & \text{if } b^2d^2e^4 \text{ is odd} \\ 1 & \text{if } b^2d^2e^4 \text{ is even} \end{cases} \qquad \iff \qquad a_3 = \begin{cases} 0 & \text{if } b \text{ is odd} \\ 1 & \text{if } b \text{ is even} \end{cases}$$

which concludes the converse of (vii) and $(viii)$. This concludes the proof since we have exhausted all possibilities for a and b. ∎

7.3.2 Proof of Theorem 7.3 for $T = C_3^0$

Theorem 7.3 for $T = C_3^0$. The reduced minimal model of E_T is

(i) $R_0 \iff a$ is even $\qquad (ii)$ $R_1 \iff a$ is odd.

Proof By Lemma 5.16, we may assume that

$$E_T : y^2 + ay = x^3$$

for some cubefree integer a. In particular, E_T is a global minimal model for E by Corollary 5.17. Thus the invariants c_4 and c_6 associated to a global minimal model of E are $c_4 = 0$ and $c_6 = -216a^2$. Thus $-c_6 \equiv 0 \mod 12$ and so $b_2 = a_1 = a_2 = 0$. The Theorem now follows since

$$-b_2^3 + 36b_2b_4 - c_6 = -c_6 \equiv 8a^2 \mod 16 = \begin{cases} 0 & \text{if } a \text{ is even} \\ 8 & \text{if } a \text{ is odd.} \end{cases}$$

∎

7.3.3 Proof of Theorem 7.3 for $T = C_4$

Theorem 7.3 for $T = C_4$. Let $a = c^2d$ for d a positive squarefree integer and let u_T be as given in Theorem 5.14.

(a) If $u_T = c$, the reduced minimal model of E_T is

(i) $R_1 \iff a$ is even and either $3 \nmid ab\,(a+b)$ or $v_3(a)$ is odd

(ii) $R_3 \iff a$ is even and either $3 |\,(a+b)$ or $v_3(a) > 0$ is even with $bd \equiv 1, 4 \mod 6$

(iii) $R_5 \iff a$ is even and either $3|b$ or $v_3(a) > 0$ is even with $bd \equiv 2, 5 \mod 6$

(iv) $R_7 \iff a$ is odd and either $3|b$ or $v_3(a) > 0$ is even with $bd \equiv 2, 5 \mod 6$

(v) $R_{10} \iff a$ is odd and either $3 \nmid ab\,(a+b)$ or $v_3(a)$ is odd

(vi) $R_{12} \iff a$ is odd and either $3 |\,(a+b)$ or $v_3(a) > 0$ is even with $bd \equiv 1, 4 \mod 6$

(b) If $u_T = 2c$, the reduced minimal model of E_T is

$$
\begin{array}{llcl}
(i) & R_7 & \Longleftrightarrow & bd \equiv 7, 15 \mod 16 \text{ and either } 3|b \text{ or } v_3(a) > 0 \text{ is even with} \\
 & & & bd \equiv 11 \mod 12 \\
(ii) & R_8 & \Longleftrightarrow & bd \equiv 3, 11 \mod 16 \text{ and either } 3|b \text{ or } v_3(a) > 0 \text{ is even with} \\
 & & & bd \equiv 11 \mod 12 \\
(iii) & R_9 & \Longleftrightarrow & bd \equiv 3, 11 \mod 16 \text{ and either } 3 \nmid ab\,(a+b) \text{ or } v_3(a) \text{ is odd} \\
(iv) & R_{10} & \Longleftrightarrow & bd \equiv 7, 15 \mod 16 \text{ and either } 3 \nmid ab\,(a+b) \text{ or } v_3(a) \text{ is odd} \\
(v) & R_{11} & \Longleftrightarrow & bd \equiv 3, 11 \mod 16 \text{ and either } 3|\,(a+b) \text{ or } v_3(a) > 0 \text{ with} \\
 & & & bd \equiv 7 \mod 12 \\
(vi) & R_{12} & \Longleftrightarrow & bd \equiv 7, 15 \mod 16 \text{ and either } 3|\,(a+b) \text{ or } v_3(a) > 0 \text{ with} \\
 & & & bd \equiv 7 \mod 12
\end{array}
$$

Proof By Theorem 5.14, the invariants associated with a global minimal model of $E_T = E_T(a, b)$ are $c_4 = u_T^{-4}\alpha_T(a, b)$ and $c_6 = u_T^{-6}\beta_T(a, b)$ where u_T is either c or $2c$. Moreover, $u_T = 2c$ if and only if $v_2(a) \geq 8$ is even and $bd \equiv 1 \mod 4$. It suffices to show the converse of each statement to prove the Theorem, as this will exhaust all possibilities for a and b.

(a) First, assume $u_T = c$. Then

$$c_4 = d^2\left(a^2 + 16ab + 16b^2\right) \qquad \text{and} \qquad c_6 = d^3\left(a + 8b\right)\left(-a^2 - 16ab + 8b^2\right).$$

Thus

$$-c_6 \equiv 8b^3d^3 + c^6d^6 \mod 12.$$

Case I. Suppose a is even and 3 does not divide $ab\,(a+b)$. Note that if k is an even integer not divisible by 3, then $k^6 \equiv 4 \mod 12$. Hence $-c_6 \equiv 8b^3d^3 + 4 \mod 12$ from which we deduce

$$-c_6 \equiv \begin{cases} 0 \mod 12 & \text{if } bd \equiv 1 \mod 3 \\ 8 \mod 12 & \text{if } bd \equiv 2 \mod 3. \end{cases} \tag{7.3}$$

We claim that $bd \equiv 1 \mod 3$. Indeed, since c is not divisible by 3 we have that $c^2 \equiv 1 \mod 3$. Then

$$a + b = c^2d + b \equiv d + b \mod 3. \tag{7.4}$$

Towards a contradiction, suppose $bd \equiv 2 \mod 3$ so that exactly one of b or d is congruent to 2 modulo 3. This is a contradiction, since then $a + b \equiv 0 \mod 3$ which contradicts our assumption. Hence $-c_6 \equiv 0 \bmod 12$ and so $b_2 = a_1 = a_2 = 0$. Now observe that

$$-b_2^3 + 36b_2b_4 - c_6 = -c_6 \equiv 8b^2c^2d^4 + 8bc^4d^5 + c^6d^6 \mod 16 \tag{7.5}$$

Since 2 divides cd, we conclude that $-c_6 \equiv 0 \mod 16$ and so $a_3 = 0$.

Case II. Suppose a is even and $v_3(a)$ is odd. Thus 3 divides d and so $-c_6 \equiv 0 \mod 12$ which implies $b_2 = a_1 = a_2 = 0$. Since cd is even, we have from (7.5) that $-c_6 \equiv 0 \mod 16$ and so $a_3 = 0$ which concludes the converse of (i).

Case III. Suppose a is even and 3 divides $a + b$. Since 3 does not divide cd, we infer that $-c_6 \equiv 8b^3d^3 + 4 \mod 12$. Since $a + b$ is divisible by 3, we deduce that $bd \equiv 2 \mod 3$ from congruence (7.4). Indeed, towards a contradiction, note that if $bd \equiv 1 \mod 3$, then $b, d \equiv 1 \mod 3$ which implies that 3 does not divide $a + b$. Therefore $-c_6 \equiv 8 \mod 12$ by (7.3). Hence $b_2 = -4$ and so $a_1 = 0$ and $a_2 = -1$. Reducing modulo 16, we attain

$$\begin{aligned}-b_2^3 + 36b_2b_4 - c_6 &\equiv 8b^2c^2d^4 + 6c^4d^4 + 8bc^4d^5 + c^6d^6 \mod 16\\ &\equiv 0 \mod 16\end{aligned}$$

since 2 divides cd. Therefore $a_3 = 0$.

Case IV. Suppose a is even, $v_3(a) > 0$ is even, and $bd \equiv 1, 4 \mod 6$. Since $v_3(a)$ is even, 3 only divides c. Therefore $-c_6 \equiv 8b^3d^3 \mod 12$. Since $8k^3 \equiv 8 \mod 12$ for $k \equiv 1, 4 \mod 6$ we deduce that $-c_6 \equiv 8 \mod 12$. It follows that $b_2 = -4$ and so $a_1 = 0$ and $a_2 = -1$. Reducing modulo 16, we attain

$$\begin{aligned}-b_2^3 + 36b_2b_4 - c_6 &\equiv 8b^2c^2d^4 + 6c^4d^4 + 8bc^4d^5 + c^6d^6 \mod 16\\ &\equiv 0 \mod 16\end{aligned}$$

since 2 divides cd. Therefore $a_3 = 0$ which concludes the converse of (ii).

Case V. Suppose a is even and 3 divides b. Then $-c_6 \equiv 4 \mod 12$ and so $b_2 = 4$. Consequently, $a_1 = 0$ and $a_2 = 1$. Then $a_3 = 0$ since

$$\begin{aligned} -b_2^3 + 36b_2b_4 - c_6 &\equiv 8b^2c^2d^4 + 10c^4d^4 + 8bc^4d^5 + c^6d^6 \mod 16 \\ &\equiv 0 \mod 16 \end{aligned}$$

since 2 divides cd.

Case VI. Suppose a is even, $v_3(a) > 0$ is even, and $bd \equiv 2, 5 \mod 6$. Then $-c_6 \equiv 8b^3d^3 \mod 12$ since 3 divides c. Moreover, $-c_6 \equiv 4 \mod 12$ since $8k^4 \equiv 4 \mod 12$ for $k \equiv 2, 5 \mod 6$. Hence $b_2 = 4$ and so $a_1 = 0$ and $a_2 = 1$. Lastly, $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ since 2 divides cd. Consequently, $a_3 = 0$ which concludes the converse of (iii).

Case VII. Suppose a is odd and 3 divides b. In particular,

$$\begin{aligned} -c_6 &\equiv 8b^3d^3 + c^6d^6 \mod 12 \\ &\equiv 1 \mod 12 \end{aligned}$$

since $k^6 \equiv 1 \mod 12$ for odd integers k not divisible by 3. Hence $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. Then

$$-b_2^3 + 36b_2b_4 - c_6 = \frac{1 - 3k^4}{2} - 24l^2 - 64l^3 - 24lk^2 + 120l^2k^2 + 24lk^4 + k^6$$

with $k = cd$ and $l = bd$. Since k is odd, we verify via the Mathematica input

```
Table[Mod[(1-3*k^4)/2-24*l^2-64*l^3-24*l*k^2+120*l^2*k^2+
24*l*k^4+k^6,16],{k,1,16,2},{l,1,16}]
```

that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$. Hence $a_3 = 0$.

Case VIII. Suppose a is odd and $v_3(a) > 0$ is even with $bd \equiv 2, 5 \mod 6$. Since $v_3(a) > 0$ is even, it follows that c is divisible by 3. We now observe that $k^6 \equiv 9 \mod 12$ for odd integers k divisible by 3 and $8l^3 \equiv 4 \mod 12$ for integers $l \equiv 2, 5 \mod 6$. In particular,

$$\begin{aligned} -c_6 &\equiv 8b^3d^3 + c^6d^6 \mod 12 \\ &\equiv 1 \mod 12 \end{aligned}$$

and so $b_2 = 1$. Consequently, $a_1 = 1$ and $a_2 = 0$. Since $b_2 = 1$, we observe that the proof above for Case VII follows identically to show that $-b_2^3+36b_2b_4-c_6 \equiv 0 \mod 16$. Hence $a_3 = 0$ which concludes the converse of (iv).

Case IX. Suppose a is odd and 3 does not divide $ab\,(a+b)$. Since 3 does not divide $a+b$, it follows that $a \equiv b \mod 3$. Since $a = c^2 d$, we have that $c^2 \equiv 1 \mod 3$ and so $a \equiv d \mod 3$. Hence $bd \equiv 1 \mod 3$ and so $8b^3d^3 \equiv 8 \mod 12$. Since $c^6d^6 \equiv 1 \mod 12$ we conclude that $-c_6 \equiv 9 \mod 12$ and so $b_2 = -3$. Thus $a_1 = 1$ and $a_2 = -1$. Then

$$-b_2^3 + 36b_2b_4 - c_6 = \frac{9k^4-27}{2} + 72l^2 - 64l^3 + 72lk^2 + 120l^2k^2 + 24lk^4 + k^6$$

with $k = cd$ and $l = bd$. Since k is odd, we verify via the Mathematica input

```
Table[Mod[(9*k^4-27)/2+72*l^2-64*l^3+72*l*k^2+120*l^2*k^2+
24*l*k^4+k^6,16],{k,1,16,2},{l,1,16}]
```

that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$. Hence $a_3 = 1$.

Case X. Suppose a is odd and $v_3(a)$ is odd. Since $v_3(a)$ is odd, 3 divides d and so $8b^3d^3 \equiv 0 \mod 12$. Moreover, $c^6d^6 \equiv 9 \mod 12$ since cd is an odd integer divisible by 3. Thus $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. Since $b_2 = -3$, we observe that the proof above for Case IX follows identically to show that $-b_2^3+36b_2b_4-c_6 \equiv 8 \mod 16$. Thus $a_3 = 1$ which concludes the converse of (v).

Case XI. Suppose a is odd and $3|\,(a+b)$. Since 3 divides $a+b$, it follows that $a \equiv -b \mod 3$. Moreover, $a = c^2d \equiv d \mod 3$ since c is not divisible by 3. Thus $d \equiv -b \mod 3$ and so $bd \equiv 2 \mod 3$. Therefore $8b^3d^3 \equiv 4 \mod 12$. Since cd is odd and not divisible by 3, we have $c^6d^6 \equiv 1 \mod 12$ and so $-c_6 \equiv 5 \mod 12$. Hence $b_2 = 5$ and so $a_1 = a_2 = 1$. Next, we compute

$$-b_2^3 + 36b_2b_4 - c_6 = \frac{125-15k^4}{2} - 120l^2 - 64l^3 - 120lk^2 + 120l^2k^2 + 24lk^4 + k^6$$

with $k = cd$ and $l = bd$. Since k is odd, we verify via the Mathematica input

```
Table[Mod[(125-15*k^4)/2-120*l^2-64*l^3-120*l*k^2+120*l^2*k^2+
24*l*k^4+k^6,16],{k,1,16,2},{l,1,16}]
```

that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$. Hence $a_3 = 1$.

Case XII. Suppose a is odd and $v_3(a) > 0$ is even with $bd \equiv 1, 4 \mod 6$. Since $v_3(a) > 0$ is even, we have that 3 divides c. In particular, $c^6 d^6 \equiv 9 \mod 12$. The assumption that $bd \equiv 1, 4 \mod 6$ implies that $8b^3d^3 \equiv 8 \mod 12$ and so $-c_6 \equiv 5 \mod 12$. Hence $b_2 = 5$ and so $a_1 = a_2 = 1$. Since $b_2 = 5$, we observe that the proof above for case XI follows identically to show that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$. Thus $a_3 = 1$ which concludes the converse of (vi).

(b) Now suppose $v_2(a) \geq 8$ and $bd \equiv 3 \mod 4$ so that $u_T = 2c$ by Theorem 5.14. In what follows, we let $a = 2^8c^2d$ and assume $bd \equiv 3 \mod 4$. In particular,

$$c_4 = d^2 \left(a^2 + 16ab + 16b^2\right) 2^{-4} = d^2 \left(b^2 + ab + 16^{-1} \cdot a^2\right)$$
$$c_6 = -d^3 (a + 8b) \left(a^2 + 16ab - 8b^2\right) \cdot 2^{-6} = -d^3 \left(8^{-1} \cdot a + b\right) \left(8^{-1} \cdot a^2 + 2ab - b^2\right)$$

Thus $-c_6 \equiv 11b^3d^3 + 4c^6d^6 \mod 12$ and so

$$-c_6 \equiv \begin{cases} 11b^3d^3 \mod 12 & \text{if } 3 | cd \\ 11b^3d^3 + 4 \mod 12 & \text{if } 3 \nmid cd \end{cases}$$

Since $bd \equiv 3 \mod 4$, bd is congruent to either $3, 7, 11$, or 15 modulo 16. Similarly, bd is congruent to either $3, 7$, or 11 modulo 12. In particular, if $v_3(a) > 0$ is even, then bd is not divisible by 3 and so the only possibilities for bd modulo 12 are $7, 11$. The conditions on a and b in the converse of statements (i) through (vi) exhaust all possibilities satisfying $v_2(a) \geq 8$ and $bd \equiv 3 \mod 4$.

Case I. Suppose 3 divides b. We claim that $-c_6 \equiv 1 \mod 12$. Since $bd \equiv 3 \mod 4$, it follows that exactly one of b or d is congruent to 1 (resp. 3) modulo 4.

Subcase I. Assume that $b \equiv 1 \mod 4$ and $d \equiv 3 \mod 4$. Since 3 divides b, it follows that $b \equiv 9 \mod 12$. Then $11b^3d^3 \equiv 9 \mod 12$ and so $-c_6 \equiv 1 \mod 4$ since 3 does not divide cd.

Subcase II. Assume that $b \equiv 3 \mod 4$ and $d \equiv 1 \mod 4$. Since 3 divides b, it follows that $b \equiv 3 \mod 12$. Then $11b^3d^3 \equiv 9 \mod 12$ and so $-c_6 \equiv 1 \mod 4$ since 3 does not divide cd.

From the claim, we conclude that $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. Then

$$-b_2^3 + 36b_2b_4 - c_6 \equiv \frac{1-3b^2d^2}{2} + 15b^3d^3 \mod 16 \qquad (7.6)$$
$$\equiv \frac{1-3k^2}{2} + 15k^3 \mod 16$$

with $k = bd$. Since k is odd, we observe via the Mathematica input

```
Table[Mod[(1-3*k^2)/2+15*k^3,16],{k,1,16,2}]
```

that

$$-b_2^3 + 36b_2b_4 - c_6 \equiv \begin{cases} 0 \mod 16 & \text{if } bd \equiv 7, 15 \mod 16 \\ 8 \mod 16 & \text{if } bd \equiv 3, 11 \mod 16 \\ 14 \mod 16 & \text{if } bd \equiv 1, 5, 9, 13 \mod 16 \end{cases}$$

Since bd is never congruent to $1, 5, 9, 13$ modulo 16, we conclude that $a_3 = 0$ if $bd \equiv 7, 15 \mod 16$ and $a_3 = 1$ if $bd \equiv 3, 11 \mod 16$. This concludes the first half of the converse of (i) and (ii).

Case II. Suppose $v_3(a) > 0$ is even with $bd \equiv 11 \mod 12$. In particular, 3 divides c and so $-c_6 \equiv 11b^3d^3 \mod 12$. Hence $-c_6 \equiv 1 \mod 12$. In particular, $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. Since $b_2 = 1$, we note that $-b_2^3 + 36b_2b_4 - c_6$ is congruent to the quantity (7.6). Therefore $a_3 = 0$ if $bd \equiv 7, 15 \mod 16$ and $a_3 = 1$ if $bd \equiv 3, 11 \mod 16$. This concludes the converse of (i) and (ii).

Case III. Suppose 3 does not divide $ab\,(a+b)$. Since 3 does not divide $ab\,(a+b)$, we have that bd is congruent to 7 or 11 modulo 12. We claim that $bd \equiv 7 \mod 12$. Towards a contradiction, suppose $bd \equiv 11 \mod 12$. Then $b \equiv -d \mod 12$ and observe that $a \equiv 4d \mod 12$ since $c^2 \equiv 4 \mod 12$. Hence

$$a + b \equiv 4d - d \mod 12 = 3d \mod 12$$

which contradicts the assumption that 3 does not divide $a+b$. Therefore $bd \equiv 7 \mod 12$ as claimed and it follows that $-c_6 \equiv 9 \mod 12$ since $11b^3d^3 \equiv 5 \mod 12$. Thus $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. Then

$$\begin{aligned} -b_2^3 + 36b_2b_4 - c_6 &\equiv \frac{9b^2d^2 - 27}{2} + 15b^3d^3 \mod 16 \\ &\equiv \frac{9k^2 - 27}{2} + 15k^3 \mod 16 \end{aligned}$$

with $k = bd$. Since k is odd, we observe via the Mathematica input

```
Table[Mod[(9*k^2-27)/2+15*k^3,16],{k,1,16,2}]
```

that

$$-b_2^3 + 36b_2b_4 - c_6 \equiv \begin{cases} 0 \mod 16 & \text{if } bd \equiv 3, 11 \mod 16 \\ 6 \mod 16 & \text{if } bd \equiv 1, 5, 9, 13 \mod 16 \\ 8 \mod 16 & \text{if } bd \equiv 7, 15 \mod 16. \end{cases} \tag{7.7}$$

Since $bd \equiv 3 \mod 4$, we see that (7.7) is either $0 \mod 16$ or $8 \mod 16$. In particular, $a_3 = 0$ if $bd \equiv 3, 11 \mod 16$ and $a_3 = 1$ if $bd \equiv 7, 15 \mod 16$.

Case IV. Suppose $v_3(a)$ is odd. Then 3 divides d and therefore $bd = 3k$ for some integer k. Since $bd \equiv 3 \mod 4$, it follows that $k \equiv 1 \mod 4$ and so

$$-c_6 \equiv 11 \cdot (3k)^3 \mod 12 = 9 \mod 12.$$

Hence $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. Since $b_2 = -3$, we note that $-b_2^3 + 36b_2b_4 - c_6$ is congruent to the quantity (7.7). Therefore $a_3 = 0$ if $bd \equiv 3, 11 \mod 16$ and $a_3 = 1$ if $bd \equiv 7, 15 \mod 16$. This concludes the converse of (iii) and (iv).

Case V. Suppose 3 divides $a+b$. Then $a \equiv -b \mod 3$ since $a \equiv d \mod 3$. We first claim that $bd \equiv 11 \mod 12$. Suppose instead $bd \equiv 7 \mod 12$. Since $bd \equiv 3 \mod 4$, we have to consider the two subcases arising from $b \equiv -d \mod 4$.

Subcase I. Suppose $b \equiv 1 \mod 4$ and $d \equiv 3 \mod 4$. Then b is congruent to 1 or 5 modulo 12 and d is congruent to 7 or 11 modulo 12 since bd is not divisible by 3. Since $bd \equiv 7 \mod 12$, it follows that either $b \equiv 1 \mod 12$ and $d \equiv 7 \mod 12$ or $b \equiv 5 \mod 12$ and $d \equiv 11 \mod 12$. For both of these cases, it follows that $a+b$ is not congruent to 0 modulo 3, which contradicts our assumption.

Subcase II. Suppose $b \equiv 3 \mod 4$ and $d \equiv 1 \mod 4$. Then b is congruent to 7 or 11 modulo 12 and d is congruent to 1 or 5 modulo 12 since bd is not divisible by 3. Since $bd \equiv 7 \mod 12$, it follows that either $b \equiv 7 \mod 12$ and $d \equiv 1 \mod 12$ or $b \equiv 11 \mod 12$ and $d \equiv 5 \mod 12$. For both of these cases, it follows that $a+b$ is not congruent to 0 modulo 3, which contradicts our assumption.

Therefore $bd \equiv 11 \mod 12$ and so $-c_6 \equiv 5 \mod 12$ since $11b^3d^3 \equiv 1 \mod 12$. Hence $b_2 = 5$ and so $a_1 = a_2 = 1$. Next, we compute

$$\begin{aligned} -b_2^3 + 36b_2b_4 - c_6 &\equiv \frac{125 - 15b^2d^2}{2} + 15b^3d^3 \mod 16 \\ &\equiv \frac{125 - 15k^2}{2} + 15k^3 \mod 16 \end{aligned}$$

with $k = bd$. Since k is odd, we check via the Mathematica input

```
Table[Mod[(125-15*k^2)/2+15*k^3,16],{k,1,16,2}]
```

that

$$-b_2^3 + 36b_2b_4 - c_6 \equiv \begin{cases} 0 \mod 16 & \text{if } bd \equiv 3, 11 \mod 16 \\ 6 \mod 16 & \text{if } bd \equiv 1, 5, 9, 13 \mod 16 \\ 8 \mod 16 & \text{if } bd \equiv 7, 15 \mod 16. \end{cases} \tag{7.8}$$

Since $bd \equiv 3 \mod 4$, we see that (7.8) is either $0 \mod 16$ or $8 \mod 16$. In particular, $a_3 = 0$ if $bd \equiv 3, 11 \mod 16$ and $a_3 = 1$ if $bd \equiv 7, 15 \mod 16$.

Case VI. Suppose $v_3(a) > 0$ is even with $bd \equiv 7 \mod 12$. Then 3 divides c and therefore $-c_6 \equiv 11b^3d^3 \mod 12$. Since $bd \equiv 7 \mod 12$, it follows that $-c_6 \equiv 5 \mod 12$ and so $b_2 = 5$ and $a_1 = a_2 = 1$. Since $b_2 = 5$, $-b_2^3 + 36b_2b_4 - c_6$ is congruent to the quantity (7.8) and so $a_3 = 0$ if $bd \equiv 3, 11 \mod 16$ and $a_3 = 1$ if $bd \equiv 7, 15 \mod 16$ which concludes the converse of (v) and (vi).

This concludes the proof of the Theorem since as remarked at the start, it sufficed to show the converse for each statement as this would exhaust all possibilities for a and b. ∎

7.3.4 Proof of Theorem 7.3 for $T = C_5$

Theorem 7.3 for $T = C_5$. The reduced minimal model of E_T is

(i)	R_4	$\Longleftrightarrow$	$ab \equiv \pm 1 \mod 6$	(ii)	R_6	$\Longleftrightarrow$	$ab \equiv 3 \mod 6$
(iii)	R_7	$\Longleftrightarrow$	$ab \equiv 0 \mod 6$	(iv)	R_{12}	$\Longleftrightarrow$	$ab \equiv \pm 2 \mod 6$

Proof Observe that

$$-c_6 \equiv a^6 + 6a^5b + 3a^4b^2 + 3a^2b^4 + 6ab^5 + b^6 \mod 12.$$

Case I. Suppose $ab \equiv \pm 1 \mod 6$. Since $k^2 \equiv 1 \mod 12$ and $6k \equiv 6 \mod 12$ for $k \equiv \pm 1 \mod 6$, we have that

$$-c_6 \equiv a^6 + b^6 + 6 \mod 12.$$

Since $ab \equiv \pm 1 \mod 6$ implies $a, b \equiv \pm 1 \mod 6$, it follows that $-c_6 \equiv 8 \mod 12$ and therefore $b_2 = -4$. Hence $a_1 = 0$ and $a_2 = -1$. Since a and b are odd, we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the Mathematica input

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16,2}]
```

Thus $a_3 = 1$. This shows the converse of (i).

Case II. Suppose $ab \equiv 3 \mod 6$. Since $6k \equiv 6 \mod 12$ and $3k^2 \equiv 3 \mod 12$ for $k \equiv 3 \mod 6$, it follows that

$$-c_6 \equiv a^6 + b^6 + 6 \mod 12.$$

Since a and b are relatively prime, we may assume without loss of generality that $a \equiv 3 \mod 6$ and $b \equiv \pm 1 \mod 6$. Then

$$-c_6 \equiv 9 + 1 + 6 \mod 12 = 4 \mod 12$$

and therefore $b_2 = 4$. Thus $a_1 = 0$ and $a_2 = 1$. Since a and b are odd, we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the Mathematica input

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16,2}]
```

Hence $a_3 = 1$ and the converse of (ii) holds.

Case III. Suppose $ab \equiv 0 \mod 6$ so that

$$-c_6 \equiv a^6 + b^6 \mod 12.$$

First, suppose $a \equiv 0 \mod 6$ so that $b \equiv \pm 1 \mod 6$. Then $-c_6 \equiv 1 \mod 12$. Next, we assume without loss of generality that a is even and b is divisible by 3. Then $-c_6 \equiv 1 \mod 12$ which allow us to conclude that $b_2 = 1$. Hence $a_1 = 1$ and $a_2 = 0$. We then verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ by considering the cases a is even (resp. odd) and b is odd (resp. even) in Mathematica via the inputs

```
Table[Mod[V[a,b],16],{a,2,16,2},{b,1,16,2}]
Table[Mod[V[a,b],16],{a,1,16,2},{b,0,16,2}]
```

Thus $a_3 = 0$ and the converse of (iii) holds.

Case IV. Suppose $ab \equiv \pm 2 \mod 6$. Then

$$-c_6 \equiv a^6 + b^6 \mod 12$$

and without loss of generality, we may assume $a \equiv \pm 2 \mod 6$ and $b \equiv \pm 1 \mod 6$ so that $-c_6 \equiv 5 \mod 12$ and so $b_2 = 5$. Hence $a_1 = a_2 = 1$. Next, we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the Mathematica input

```
Table[Mod[V[a,b],16],{a,2,16,2},{b,1,16,2}]
Table[Mod[V[a,b],16],{a,1,16,2},{b,0,16,2}]
```

Thus $a_3 = 1$ and the converse of (iv) holds.

This concludes the proof since we have exhausted all possibilities for a and b. ■

7.3.5 Proof of Theorem 7.3 for $T = C_6$

Theorem 7.3 for $T = C_6$. The reduced minimal model of E_T is

$$\begin{array}{llll} (i) & R_1 & \Longleftrightarrow & a \equiv 3 \mod 6 \text{ with } v_2(a+b) = 1,2 \\ (ii) & R_5 & \Longleftrightarrow & a \equiv \pm 1 \mod 6 \text{ with } v_2(a+b) = 1,2 \\ (iii) & R_7 & \Longleftrightarrow & a \equiv \pm 1 \mod 6 \text{ with } v_2(a+b) \neq 1,2,3 \\ (iv) & R_8 & \Longleftrightarrow & \text{either } a \equiv \pm 2 \mod 6 \text{ or } a \equiv \pm 1 \mod 6 \text{ with } v_2(a+b) = 3 \\ (v) & R_9 & \Longleftrightarrow & \text{either } a \equiv 0 \mod 6 \text{ or } a \equiv 3 \mod 6 \text{ with } v_2(a+b) = 3 \\ (vi) & R_{10} & \Longleftrightarrow & a \equiv 3 \mod 6 \text{ with } v_2(a+b) \neq 1,2,3 \end{array}$$

Proof By Theorem 5.14, the invariants associated with a global minimal model of $E_T(a,b)$ are $c_4 = u_T^{-4}\alpha_T(a,b)$ and $c_6 = u_T^{-6}\beta_T(a,b)$ where

$$u_T = \begin{cases} 1 & \text{if } v_2(a+b) < 3 \\ 2 & \text{if } v_2(a+b) \geq 3 \end{cases}$$

First assume $u_T = 1$ so that $v_2(a+b) < 3$.

Case I. Suppose $a \equiv 3 \mod 6$ and $v_2(a+b) = 1,2$. In particular, $a = 3+6k$ for some odd integer k and b is odd. Then $-c_6 \equiv 0 \mod 12$ as is checked via the Mathematica input

```
Table[Mod[-c6[3+6*k,b],12],{k,1,12},{b,1,12,2}]
```

Hence $b_2 = a_1 = a_2 = 0$. Next we check that $-c_6 \equiv 0 \mod 16$ via the Mathematica input

```
Table[Mod[V[3+6*k,b],16],{k,1,16},{b,1,16,2}]
```

Hence $a_3 = 0$ which concludes the converse of (i).

Case II. Suppose $a \equiv \pm 1 \mod 6$ and $v_2(a+b) = 1,2$. Then $a = \pm 1 + 6k$ for some integer k and b is odd. From the Mathematica input

```
Table[Mod[-c6[1+6*k,b],12],{k,1,12},{b,1,12,2}]
Table[Mod[-c6[-1+ 6*k,b],12],{k,1,12},{b,1,12,2}]
```

we conclude that $-c_6 \equiv 4 \mod 12$ and so $b_2 = 4$. Consequently, $a_1 = 0$ and $a_2 = 1$. Next we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the Mathematica input

```
Table[Mod[V[1+6*k,b],16],{k,1,16},{b,1,16,2}]
Table[Mod[V[-1+6*k, b],16],{k,1,16},{b,1,16,2}]
```

Hence $a_3 = 0$ which concludes the converse of (ii).

Case III. Suppose $a \equiv \pm 1 \mod 6$ and b is even. In particular, $v_2(a+b) = 0$. Then $a = \pm 1 + 6k$ for some integer k and we check that $-c_6 \equiv 1 \mod 12$ from the Mathematica input

```
Table[Mod[-c6[1+6*k,b],12],{k,1,12},{b,2,12,2}]
Table[Mod[-c6[-1+6*k,b],12],{k,1,12},{b,2,12,2}]
```

Hence $b_2 = a_1 = 1$ and $a_2 = 0$. Next we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the Mathematica input

```
Table[Mod[V[1+6*k,b],16],{k,1,16},{b,2,16,2}]
Table[Mod[V[-1+6*k,b],16],{k,1,16},{b,2,16,2}]
```

Hence $a_3 = 0$.

Case IV. Suppose $a \equiv \pm 2 \mod 6$ so that b is odd. Then $a = \pm 2 + 6k$ for some integer k and we verify that $-c_6 \equiv 1 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[2+6*k,b],12],{k,1,12},{b,1,12,2}]
Table[Mod[-c6[-2+6*k,b],12],{k,1,12},{b,1,12,2}]
```

Hence $b_2 = a_1 = 1$ and $a_2 = 0$. Then we check that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ from the Mathematica input

```
Table[Mod[V[2+6*k,b],16],{k,1,16},{b,1,16,2}]
Table[Mod[V[-2+6*k,b],16],{k,1,16},{b,1,16,2}]
```

Thus $a_3 = 1$.

Case V. Suppose $a \equiv 0 \mod 6$ so that b is odd. Then $a = 6k$ for some integer k and we verify that $-c_6 \equiv 9 \mod 12$ from the Mathematica input

```
Table[Mod[-c6[6*k,b],12],{k,1,12},{b,1,12,2}]
```

Hence $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. We now check that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ by the Mathematica input

```
Table[Mod[V[6*k,b],16],{k,1,16},{b,1,16,2}]
```

Hence $a_3 = 0$.

Case VI. Suppose $a \equiv 3 \mod 6$ and b is even. In particular, $v_3(a+b) = 0$. Then $a = 3+6k$ for some integer k and we verify that $-c_6 \equiv 9 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[3+6*k,b],12],{k,1,12},{b,2,12,2}]
```

Hence $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. Then $a_3 = 1$ since $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ which is verified by the Mathematica input

```
Table[Mod[V[3+6*k,b],16],{k,1,16},{b,2,16,2}]
```

Now assume that $u_T = 2$ so that $v_2(a+b) \geq 3$.

Case I. Suppose $a \equiv \pm 1 \mod 6$ and b is odd. Then $a = \pm 1 + 6k$ and $a + b = 8l$ for some integer k and l. In particular, $b = 8l \mp 1 - 6k$. Since b is odd it follows that either l and k are both even or are both odd. Then $-c_6 \equiv 1 \mod 12$ is verified via the Mathematica inputs

```
Table[Mod[-c6[1+6*k,8*l-1-6*k],12],{l,1,12,2},{k,1,12,2}]
Table[Mod[-c6[1+6*k,8*l-1-6*k],12],{l,2,12,2},{k,2,12,2}]
Table[Mod[-c6[-1+6*k,8*l+1-6*k],12],{l,1,12,2},{k,1,12,2}]
Table[Mod[-c6[-1+6*k,8*l+1-6*k],12],{l,2,12,2},{k,2,12,2}]
```

Hence $b_2 = a_1 = 1$ and so $a_2 = 0$. Now we consider two subcases corresponding to whether l is even or odd.

Subcase I. Suppose l is even so that $v_2(a+b) \geq 4$. We verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the Mathematica inputs

```
Table[Mod[V[1+6*k,8*l-1-6*k],16],{l,2,16,2},{k,2,16,2}]
Table[Mod[V[-1+6*k,8*l+1-6*k],16],{l,2,16,2},{k,2,16,2}]
```

Thus $a_3 = 0$ and this concludes the converse of (iii).

Subcase II. Suppose l is odd so that $v_2(a+b) = 3$. We verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the Mathematica inputs

```
Table[Mod[V[1+6*k,8*l-1-6*k],16],{l,1,16,2},{k,1,16,2}]
Table[Mod[V[-1+6*k,8*l+1-6*k],16],{l,1,16,2},{k,1,16,2}]
```

Hence $a_3 = 1$ and this concludes the converse of (iv).

Case II. Suppose $a \equiv 3 \mod 6$ with b odd such that $v_2(a+b) \geq 3$. Then $a = 3+6k$ and $a + b = 8l$ for some integers l and k. In particular, $b = 8l - 6k - 3$. Then $-c_6 \equiv 9 \mod 12$ as is verified via the Mathematica input

```
Table[Mod[-c6[3+6*k,8*l-6*k-3],12],{k,1,12},{l,1,12}]
```

Hence $b_2 = -3$ and so $a_1 = 1$ and $a_2 = -1$. Lastly we consider the two subcases corresponding to whether l is even or odd.

Subcase I. Suppose l is odd so that $v_2(a+b) = 3$. We then verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the Mathematica input

```
Table[Mod[V[3+6*k,8*l-6*k-3],16],{l,1,16,2},{k,1,16}]
```

Hence $a_3 = 0$ and this concludes the converse of (v).

Subcase II. Suppose l is even so that $v_2(a+b) \geq 4$. We then verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the Mathematica input

```
Table[Mod[V[3+6*k,8*l-6*k-3],16],{l,2,16,2},{k,1,16}]
```

Thus $a_3 = 1$ which concludes the converse of (vi).

The Theorem now follows since we have exhausted all possibilities for a and b. ■

7.3.6 Proof of Theorem 7.3 for $T = C_7, C_9$

Theorem 7.3 for $T = C_7, C_9$. The reduced minimal model of E_T is

(i) $R_7 \iff a + b \equiv \pm 1 \mod 3$ (ii) $R_{10} \iff a + b \equiv 0 \mod 3$

Proof Let T be C_7 or C_9.

Case I. Suppose $a + b \equiv \pm 1 \mod 3$. Then $a + b = \pm 1 + 3k$ for some integer k and so $b = \pm 1 + 3k - a$. If k is odd, we note that $a + b$ is even and thus a and b are both odd since they are relatively prime. In this case, we verify that $-c_6 \equiv 1 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[a,1+3*k-a],12],{a,1,12,2},{k,1,12,2}]
Table[Mod[-c6[a,-1+3*k-a],12],{a,1,12,2},{k,1,12,2}]
```

Next, we consider the case when k is even and verify that $-c_6 \equiv 1 \mod 12$ holds in this case as well via the Mathematica input

```
Table[Mod[-c6[a,1+3*k-a],12],{a,1,12},{k,2,12,2}]
Table[Mod[-c6[a,-1+3*k-a],12],{a,1,12},{k,2,12,2}]
```

Therefore $b_2 = 1$. Hence $a_1 = 1$ and $a_2 = 0$.

We now verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ by considering the two subcases: (1) a is odd and (2) a is even and b is odd. The verification is done in Mathematica for these two subcases via the inputs:

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16}]
Table[Mod[V[a,b],16],{a,0,16,2},{b,1,16,2}]
```

Hence $a_3 = 0$ from which the converse of (i) follows.

Case II. Suppose $a + b \equiv 0 \mod 3$. Then $a + b = 3k$ for some integer k so that $b = 3k - a$. Since a and b are relatively prime, we observe that if a is even, then k is odd. We then verify that $-c_6 \equiv 9 \mod 12$ via the Mathematica inputs:

```
Table[Mod[-c6[a,3*k-a],12],{a,2,12,2},{k,1,12,2}]
Table[Mod[-c6[a,3*k-a],12],{a,1,12,2},{k,1,12}]
```

Hence $b_2 = -3$ from which we attain $a_1 = 1$ and $a_2 = -1$. We then verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16}]
Table[Mod[V[a,b],16],{a,0,16,2},{b,1,16,2}]
```

Thus $a_3 = 1$ and so the converse of (ii) holds.

The Theorem thus holds since we have exhausted all possibilities for a and b. ■

7.3.7 Proof of Theorem 7.3 for $T = C_8$

Theorem 7.3 for $T = C_8$. The reduced minimal model of E_T is

(i)	R_3	$\iff$	$a \equiv 0 \mod 12$	(ii)	R_5	$\iff$	$a \equiv \pm 4 \mod 12$
(iii)	R_7	$\iff$	$a \equiv \pm 1, \pm 2, \pm 5 \mod 12$	(iv)	R_{12}	$\iff$	$a \equiv \pm 3, 6 \mod 12$

Proof By Theorem 5.14, the invariants associated with a global minimal model of $E_T(a,b)$ are $c_4 = u_T^{-4}\alpha_T(a,b)$ and $c_6 = u_T^{-6}\beta_T(a,b)$ where

$$u_T = \begin{cases} 1 & \text{if } v_2(a) \neq 1 \\ 2 & \text{if } v_2(a) = 1 \end{cases}$$

In particular, $u_T = 2$ if and only if $a \equiv \pm 2, 6 \mod 12$.

Case I. Suppose $a \equiv 0 \mod 12$ so that $a = 12k$ for some integer k. Then b is odd and not divisible by 3 and we verify that $-c_6 \equiv 8 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[12*k,b],12],{k,1,12},{b,1,12,3}]
Table[Mod[-c6[12*k,b],12],{k,1,12},{b,2,12,3}]
```

Hence $b_2 = -4$ so that $a_1 = 0$ and $a_2 = -1$. Therefore $a_3 = 0$ since $-b_2^3+36b_2b_4-c_6 \equiv 0 \mod 16$ as is checked via the Mathematica input

```
Table[Mod[V[12*k,b],16],{k,1,16},{b,1,16}]
```

This concludes the converse of (i).

Case II. Suppose $a \equiv \pm 4 \mod 12$. Then $a = \pm 4 + 12k$ for some integer k and b is odd. Moreover, $b_2 = 4$ since $-c_6 \equiv 4 \mod 12$ as is checked via the Mathematica input

```
Table[Mod[-c6[4+12*k,b],12],{k,1,12},{b,1,12,2}]
Table[Mod[-c6[-4+12*k,b],12],{k,1,12},{b,1,12,2}]
```

In particular, $a_1 = 0$ and $a_2 = 1$. Then $a_3 = 0$ since $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ as is checked via the Mathematica input

```
Table[Mod[V[4+12*k,b],16],{k,1,16},{b,1,16,2}]
Table[Mod[V[-4+12*k,b],16],{k,1,16},{b,1,16,2}]
```

This concludes the converse of (ii).

Case III. Suppose $a \equiv \pm 1, \pm 5 \mod 12$. Then $a \equiv \pm 1 \mod 6$ and we write $a = \pm 1 + 6k$ for some integer k. We now verify that $-c_6 \equiv 1 \mod 12$ via the Mathematica

```
Table[Mod[-c6[1+6*k,b],12],{k,1,12},{b,1,12}]
Table[Mod[-c6[-1+6*k,b],12],{k,1,12},{b,1,12}]
```

In particular, $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. It then follows that $a_3 = 0$ since $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ as is checked via the Mathematica input

```
Table[Mod[V[1+6*k,b],16],{k,1,16},{b,1,16}]
Table[Mod[V[-1+6*k,b],16],{k,1,16},{b,1,16}]
```

Case IV. Suppose $a \equiv \pm 3 \mod 12$. Then $a \equiv 3 \mod 6$ and so $a = 3 + 6k$ for some integer k. In particular, $b \equiv \pm 1 \mod 3$ and so we verify that $-c_6 \equiv 5 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[3+6*k,b],12],{k,1,12},{b,1,12,3}]
Table[Mod[-c6[3+6*k,b],12],{k,1,12},{b,2,12,3}]
```

Hence $b_2 = 5$ and so $a_1 = a_2 = 1$. Next we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the Mathematica input

```
Table[Mod[V[3+6*k,b],16],{k,1,16},{b,1,16}]
```

In particular, $a_3 = 1$.

We now assume that $u_T = 2$ and consider the remaining cases, namely $a \equiv \pm 2, 6 \mod 12$.

Case I. Suppose $a \equiv \pm 2 \mod 12$. Then $a = \pm 2 + 12k$ for some integer k and b is odd. Then $-c_6 \equiv 1 \mod 12$ as is verified via the Mathematica input

```
Table[Mod[-c6[2+12*k,b],12],{k,1,12},{b,1,12,2}]
Table[Mod[-c6[-2+12*k,b],12],{k,1,12},{b,1,12,2}]
```

Hence $b_2 = a_1 = 1$ and $a_2 = 0$. Then $a_3 = 0$ since $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ which is verified via the Mathematica input

```
Table[Mod[V[2+4*k,b],16],{k,1,16},{b,1,16,2}]
```

This concludes the converse of (iii).

Case II. Suppose $a \equiv 6 \mod 12$ so that $a = 6 + 12k$ for some integer k and $b \equiv \pm 1 \mod 5$. Then $-c_6 \equiv 5 \mod 12$ as is verified via the Mathematica input

```
Table[Mod[-c6[6+12*k,b],12],{k,1,12},{b,1,12,6}]
Table[Mod[-c6[6+12*k,b],12],{k,1,12},{b,5,12,6}]
```

Hence $b_2 = 5$ and so $a_1 = 1$ and $a_2 = 1$. Lastly, we verify that $a_3 = 1$ since $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ as is verified via the Mathematica input

```
Table[Mod[V[6+12*k,b],16],{k,1,16},{b,1,16,2}]
```

This concludes the converse of (iv).

The Theorem now follows since we have exhausted all possibilities for a and b. ■

7.3.8 Proof of Theorem 7.3 for $T = C_{10}$

Theorem 7.3 for $T = C_{10}$. The reduced minimal model of E_T is R_7.

Proof By Theorem 5.14, the invariants associated with a global minimal model of $E_T(a, b)$ are $c_4 = u_T^{-4}\alpha_T(a, b)$ and $c_6 = u_T^{-6}\beta_T(a, b)$ where

$$u_T = \begin{cases} 1 & \text{if } a \text{ is odd} \\ 2 & \text{if } a \text{ is even.} \end{cases}$$

Case I. Suppose a is odd. From the Mathematica input

```
Table[Mod[-c6[a,b],12],{a,1,12,2},{b,1,12}]
```

we conclude that $-c_6 \equiv 1 \mod 12$. Note that the above input does return $-c_6 \equiv 9 \mod 12$ which occurs only when 3 divides $\gcd(a, b)$ which is not possible since a and b are assumed to be relatively prime. Hence $b_2 = 1$ and therefore $a_1 = 1$ and $a_2 = 0$. From the Mathematica input

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16}]
```

we conclude that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$. Therefore $a_3 = 1$.

Case II. Suppose a is even and write $a = 2k$ for some integer k. Then $u_T = 2$ and we verify that $-c_6 \equiv 1 \mod 12$ from the Mathematica input

```
Table[Mod[-c6[2*k,b],12],{k,1,12,2},{b,1,12,2}]
```

As before, we note that the above input does return $-c_6 \equiv 9 \mod 12$ which occurs only when 3 divides $\gcd(a,b)$. Hence $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. Next we verify that $a_3 = 1$ since the Mathematica input

```
Table[Mod[V[2*k,b],16],{k,1,16,2},{b,1,16,2}]
```

verifies that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$.

This concludes the proof since we have exhausted all possibilities for a. ■

7.3.9 Proof of Theorem 7.3 for $T = C_{12}$

Theorem 7.3 for $T = C_{12}$. The reduced minimal model of E_T is

(i)	R_7	$\Longleftrightarrow$	$a \equiv \pm1, \pm2, \pm5 \mod 12$	(ii)	R_8	$\Longleftrightarrow$	$a \equiv \pm4 \mod 12$
(iii)	R_9	$\Longleftrightarrow$	$a \equiv 0 \mod 12$	(iv)	R_{10}	$\Longleftrightarrow$	$a \equiv \pm3, 6 \mod 12$

Proof By Theorem 5.14, the invariants associated with a global minimal model of $E_T(a,b)$ are $c_4 = u_T^{-4}\alpha_T(a,b)$ and $c_6 = u_T^{-6}\beta_T(a,b)$ where

$$u_T = \begin{cases} 1 & \text{if } a \text{ is odd} \\ 2 & \text{if } a \text{ is even.} \end{cases}$$

We first assume that $u_T = 1$ and consider the cases where $a \equiv \pm1, \pm3, \pm5 \mod 12$.

Case I. Suppose $a \equiv \pm1, \pm5 \mod 12$. Then $a \equiv \pm1 \mod 6$ and so $a = \pm1 + 6k$ for some integer k. We then verify that $-c_6 \equiv 1 \mod 12$ in Mathematica via the input

```
Table[Mod[-c6[1+6*k,b],12],{k,1,12},{b,1,12}]
Table[Mod[-c6[-1+6*k,b],12],{k,1,12},{b,1,12}]
```

Hence $b_2 = 1$ which implies that $a_1 = 1$ and $a_2 = 0$. Next we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the input

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16}]
```

We note that the congruence holds for all odd integers a. In particular, $a_3 = 0$.

Case II. Suppose $a \equiv \pm 3 \mod 12$. Then $a \equiv 3 \mod 6$ so that $a = 3 + 6k$ for some integer k. We verify that $-c_6 \equiv 9 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[3+6*k,b],12],{k,1,12},{b,1,12}]
```

Thus $b_2 = -3$ and consequently $a_1 = 1$ and $a_2 = -1$. We then verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the input

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16}]
```

Hence $a_3 = 1$.

Now assume that $u_T = 2$ so that $a \equiv 0, \pm 2, \pm 4, 6 \mod 12$.

Case I. Suppose $a \equiv \pm 2, \pm 4 \mod 12$. Then $a \equiv \pm 2 \mod 6$ and so $a = \pm 2 + 6k$ for some integer k. Since b is odd we verify that $-c_6 \equiv 1 \mod 12$ via the Mathematica inputs

```
Table[Mod[-c6[2+6*k,b],12],{k,1,12}, {b,1,12,2}]
Table[Mod[-c6[-2+6*k,b],12],{k,1,12}, {b,1,12,2}]
```

Thus $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$.

Subcase I. Suppose $a \equiv \pm 2 \mod 12$. Then $a \equiv \pm 2, \pm 6 \mod 16$. In particular, $a \equiv \pm 2 \mod 8$.

We verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$ via the input

```
Table[Mod[V[a,b],16],{a,2,16,4},{b,1,16,2}]
```

Note that `{a,2,16,4}` refers to the case where $a \equiv \pm 2 \mod 8$ since its considers $a \equiv 2, 6, 10, 14 \mod 16$. In particular, $a_3 = 0$ which concludes the converse of (i).

Subcase II. Suppose $a \equiv \pm 4 \mod 12$. Then $a \equiv 0 \mod 4$ and we verify that $-b_2^3 + 36b_2b_4 - c_6 \equiv 8 \mod 16$ via the input

```
Table[Mod[V[a,b],16],{a,4,16,4},{b,1,16,2}]
```

Hence $a_3 = 1$ which concludes the converse of (ii).

Case III. Suppose $a \equiv 0 \mod 6$ so that $a = 6k$ for some integer k. Then b is odd and we verify that $-c_6 \equiv 9 \mod 12$ via the Mathematica input

```
Table[Mod[-c6[6*k,b],12],{k,1,12},{b,1,12,2}]
```

Therefore $b_2 = -3$ and consequently $a_1 = 1$ and $a_2 = -1$. Lastly, we conclude that

$$-b_2^3+36b_2b_4-c_6 \equiv \begin{cases} 0 \mod 16 & \text{if } k \text{ is even} \\ 8 \mod 16 & \text{if } k \text{ is odd} \end{cases} \quad \Longleftrightarrow \quad a_3 = \begin{cases} 0 & \text{if } a \equiv 0 \mod 12 \\ 1 & \text{if } a \equiv 6 \mod 12 \end{cases}$$

from the Mathematica input

```
Table[Mod[V[6*k,b],16],{k,2,16,2},{b,1,16,2}]
```

This concludes the converse of (iii) and (iv) and therefore the Theorem now follows since we have exhausted all possibilities for a and b. ■

7.3.10 Proof of Theorem 7.3 for $T = C_2 \times C_8$

Theorem 7.3 for $T = C_2 \times C_8$. The reduced minimal model of E_T is R_7.

Proof By Theorem 5.14, the invariants associated with a global minimal model of $E_T(a,b)$ are $c_4 = u_T^{-4}\alpha_T(a,b)$ and $c_6 = u_T^{-6}\beta_T(a,b)$ where

$$u_T = \begin{cases} 1 & \text{if } v_2(a) = 0 \\ 16 & \text{if } v_2(a) = 1 \\ 64 & \text{if } v_2(a) \geq 2 \end{cases}$$

Case I. We first assume that $u_T = 1$ so that a is odd. From the Mathematica input

```
Table[Mod[-c6[a,b],12],{a,1,12,2},{b,1,12}]
```

we conclude that $-c_6 \equiv 1 \mod 12$. Note that the above input does return $-c_6 \equiv 9 \mod 12$ which occurs only when 3 divides $\gcd(a,b)$ which is not possible since a and b are assumed to be relatively prime. Hence $b_2 = 1$ and therefore $a_1 = 1$ and $a_2 = 0$. From the Mathematica input

```
Table[Mod[V[a,b],16],{a,1,16,2},{b,1,16}]
```

we conclude that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$. Therefore $a_3 = 1$.

Case II. Next, assume $u_T = 16$ so that $a = 2k$ for some odd integer k. Then $-c_6 \equiv 1 \mod 12$ from the Mathematica input

```
Table[Mod[-c6[2*k,b],12],{k,1,12,2},{b,1,12,2}]
```

Hence $b_2 = 1$ and so $a_1 = 1$ and $a_2 = 0$. Next we verify that $a_3 = 1$ since the Mathematica input

```
Table[Mod[V[2*k,b],16],{k,1,16,2},{b,1,16,2}]
```

verifies that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$.

Case III. Lastly, assume $u_T = 64$ so that $a = 4k$ for some integer k. Then $-c_6 \equiv 1 \mod 12$ is verified from the Mathematica input

```
Table[Mod[-c6[4*k,b],12],{k,1,12},{b,1,12,2}]
```

and so $b_2 = a_1 = 1$ and $a_2 = 0$. Finally, $a_3 = 0$ since the Mathematica input

```
Table[Mod[V[4*k,b],16],{k,1,16},{b,1,16,2}]
```

verifies that $-b_2^3 + 36b_2b_4 - c_6 \equiv 0 \mod 16$. ■

7.4 Examples

Example 7.4 *The reduced minimal model of the elliptic curve $E_T(5^3, 14)$ for $T = C_3$ is*

$$y^2 + xy = x^3 + 22x - 4$$

Example 7.5 *Let E be the elliptic curve in Example 5.27. Then as noted, E is $\mathbb{Q}$-isomorphic to the elliptic curve $E_T(6, 11)$ for $T = C_{12}$. Since $6 \equiv 6 \mod 12$, we have by Theorem 7.3 that the reduced minimal model of E is given by*

$$R_{10} : y^2 + xy + y = x^3 - x^2 - \frac{c_4 + 15}{48} - \frac{-9c_4 + 2c_6 + 459}{1728} \text{ with}$$
$$\frac{c_4 + 15}{48} = 919077351189287 \text{ and } \frac{-9c_4 + 2c_6 + 459}{1728} = -1070178552446727956131$$

APPENDICES

A. GOOD *ABC* TRIPLES

Introduction

The ABC Conjecture [1] of Masser and Oesterlé states that for each $\epsilon > 0$, there exists finitely many relatively prime positive integers a, b, c satisfying $a + b = c$ and $\operatorname{rad}(abc)^{1+\epsilon} < c$ where $\operatorname{rad}(n)$ denotes the product over all the distinct prime factors of n. By an ABC triple we mean a triple $P = (a, b, c)$ where a, b, c are relatively prime positive integers such that $a + b = c$. We say an ABC triple $P = (a, b, c)$ is good if $\operatorname{rad}(abc) < c$. Following ideas of Frey [42, §1], we associate to an ABC triple P an elliptic curve $F_P : y^2 = x\,(x - a)\,(x + b)$. This elliptic curve is known as a Frey curve and its Mordell-Weil group contains $F_P[2] \cong C_2 \times C_2$. Therefore by Theorem 2.1, the torsion subgroup $E_P(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_{2N}$ where $N = 1, 2, 3, 4$. Let $T = C_2 \times C_{2N}$ be one of these four groups. In this appendix we associate to each T a sequence of good ABC triples $\{P_n^T\}_n$ and prove:

Theorem A.1 *Let T be one of $C_2 \times C_{2N}$ where $N = 1, 2, 3, 4$. Then for each T, there is a sequence of good ABC triples $\{P_n^T\}_n$ such that the Frey curve $F_{P_n^T}$ has torsion subgroup isomorphic to T for each $n \geq 1$.*

Certain Polynomials

In this section we establish a series of technical results which will ease the proofs in the sections that are to follow. Let $T = C_2 \times C_{2N}$ where $N = 1, 2, 3, 4$. For each T let $\mathfrak{A}_T = \mathfrak{A}_T(a, b)$, $\mathfrak{B}_T = \mathfrak{B}_T(a, b)$, $\mathfrak{C}_T = \mathfrak{C}_T(a, b)$, $\mathfrak{D}_T = \mathfrak{D}_T(a, b)$, $\mathfrak{A}_T^r = \mathfrak{A}_T^r(a, b)$, $\mathfrak{B}_T^r = \mathfrak{B}_T^r(a, b)$, $\mathfrak{C}_T^r = \mathfrak{C}_T^r(a, b)$, $U_T = U_T(a, b, r, s)$, $V_T = V_T(a, b, r, s)$, and $W_T = W_T\,(a, b, r, s)$ be the polynomials in $R = \mathbb{Z}[a, b, r, s]$ defined in Table A.3.

For a fixed T, the polynomials $\mathfrak{A}_T$, $\mathfrak{B}_T$, $\mathfrak{C}_T$, and $\mathfrak{D}_T$ are homogenous polynomials in a and b of the same degree m_T. In particular, we have the equalities

$$\begin{aligned} a^{m_T}\mathfrak{A}_T\big(1,\tfrac{b}{a}\big) &= \mathfrak{A}_T(a,b) & \qquad a^{m_T}\mathfrak{B}_T\big(1,\tfrac{b}{a}\big) &= \mathfrak{B}_T(a,b) \\ a^{m_T}\mathfrak{C}_T\big(1,\tfrac{b}{a}\big) &= \mathfrak{C}_T(a,b) & \qquad a^{m_T}\mathfrak{D}_T\big(1,\tfrac{b}{a}\big) &= \mathfrak{D}_T(a,b)\,. \end{aligned}$$

The first result can be verified via a computer algebra system and we note that we are considering $\mathfrak{A}_T(1,t)\,,\ \mathfrak{B}_T(1,t)\,,\ \mathfrak{C}_T(1,t)\,,\ \mathfrak{D}_T(1,t)$ as functions from $\mathbb{R}$ to $\mathbb{R}$.

Lemma A.2 *For $T = C_2 \times C_{2N}$ with $N = 1, 2, 3, 4$, let $f_T, g_T : \mathbb{R} \to \mathbb{R}$ be the function in the variable t defined in Table A.3. Let θ_T be the greatest real root of $f_T(t)$. The (approximate) value of θ_T is found in Table A.3. Then for each T,*

1. $\mathfrak{A}_T + \mathfrak{B}_T = \mathfrak{C}_T$;

2. $U_T\mathfrak{B}_T + V_T\mathfrak{C}_T = W_T$;

3. $f_T\big(\frac{b}{a}\big) = \frac{\mathfrak{B}_T(a,b)}{\mathfrak{A}_T(a,b)} - \frac{b}{a}$;

4. $g_T(t) = \mathfrak{C}_T(1,t) - \mathfrak{D}_T(1,t)$;

5. $f_T(t)\,, g_T(t)\,,\ \mathfrak{A}_T(1,t)\,,\ \mathfrak{B}_T(1,t)\,,\ \mathfrak{C}_T(1,t)\,,\ \mathfrak{D}_T(1,t) > 0$ *for* $t > \theta_T$;

6. *For* $T = C_2 \times C_{2N}$ *for* $N = 1, 2$, $f_T(t)\,, g_T(t)\,,\ \mathfrak{A}_T(1,t)\,,\ \mathfrak{B}_T(1,t)\,,\ \mathfrak{C}_T(1,t)$, $\mathfrak{D}_T(1,t) > 0$ *for* t *in* $(0,1)$.

   In particular, $\mathfrak{A}_T \in 4R$.

[

Good ABC Triples]Good ***ABC*** Triples

Definition A.1 *By an ABC triple, we mean a triple $P = (a, b, c)$ such that a, b, and c are relatively prime positive integers with $a + b = c$. We say $P = (a, b, c)$ is good if* $\operatorname{rad}(abc) < c$.

Lemma A.3 *For each $T = C_2 \times C_{2N}$, let $P = (a, b, a+b)$ be an ABC triple with a even and $\frac{b}{a} > \theta_T$ where θ_T is as defined in Lemma A.2. Suppose further that $a \equiv 0 \mod 3$ if $N = 3$. Then $(\mathfrak{A}_T, \mathfrak{B}_T, \mathfrak{C}_T)$ is an ABC triple with $\mathfrak{A}_T \equiv 0 \mod 16$, $\mathfrak{B}_T \equiv 1 \mod 4$, and $\frac{\mathfrak{B}_T}{\mathfrak{A}_T} > \theta_T$. Moreover, if $N = 3$, then $\mathfrak{A}_T \equiv 0 \mod 3$.*

Proof Since a and b are relatively prime, there exist integers r and s such that $ra^n + sb^n = 1$, for any positive integer n. Therefore, by lemma A.2, $\gcd(\mathfrak{B}_T, \mathfrak{C}_T)$ divides 32 if $N \neq 3$ and $\gcd(\mathfrak{B}_T, \mathfrak{C}_T)$ divides 48 if $N = 3$. Since a is even and $a \equiv 0 \mod 3$ when $N = 3$, we conclude that $\gcd(\mathfrak{B}_T, \mathfrak{C}_T) = 1$. By lemma A.2 we also have that $\mathfrak{A}_T + \mathfrak{B}_T = \mathfrak{C}_T$ for each T and therefore $(\mathfrak{A}_T, \mathfrak{B}_T, \mathfrak{C}_T)$ is an ABC triple. Since a is even it is easily verified that $\mathfrak{A}_T \equiv 0 \mod 16$. Similarly, when $N = 3$, $\mathfrak{A}_T \equiv 0 \mod 3$ since $a \equiv 0 \mod 3$. It easily checked that for each T, $\mathfrak{B}_T \equiv b^{2k} \mod 4$ for some integer k. Since b is odd, it follows that $\mathfrak{B}_T \equiv 1 \mod 4$. Now observe that

$$f_T\left(\frac{b}{a}\right) = \frac{\mathfrak{B}_T\left(1, \frac{b}{a}\right)}{\mathfrak{A}_T\left(1, \frac{b}{a}\right)} - \frac{b}{a} = \frac{\mathfrak{B}_T(a,b)}{\mathfrak{A}_T(a,b)} - \frac{b}{a}.$$

Since $\frac{b}{a} > \theta_T$, we have by Lemma A.2 that $f_T\left(\frac{b}{a}\right)$ is positive and therefore $\frac{\mathfrak{B}_T}{\mathfrak{A}_T} > \frac{b}{a} > \theta_T$. ■

Lemma A.4 *Let $P = (a, b, a+b)$ be a good ABC triple and assume the statement of Lemma A.3. Then $(\mathfrak{A}_T, \mathfrak{B}_T, \mathfrak{C}_T)$ is a good ABC triple.*

Proof Since a is assumed to be even, we have that $\operatorname{rad}(2^n ax) = \operatorname{rad}(ax)$ for some integer x. Therefore

$$\operatorname{rad}(\mathfrak{A}_T) = \operatorname{rad}(\mathfrak{A}_T^r), \qquad \operatorname{rad}(\mathfrak{B}_T) = \operatorname{rad}(\mathfrak{B}_T^r), \qquad \operatorname{rad}(\mathfrak{C}_T) = \operatorname{rad}(\mathfrak{C}_T^r).$$

Since $(a, b, a+b)$ is a good ABC triple, we have that $\operatorname{rad}(ab(a+b)) < a+b$. From this and the fact that $\operatorname{rad}\left(xy^k\right) = \operatorname{rad}(xy) \leq xy$ for positive integers k, x, y, we have that for each T, we attain

$$\operatorname{rad}(\mathfrak{A}_T\mathfrak{B}_T\mathfrak{C}_T) = \operatorname{rad}(\mathfrak{A}_T^r\mathfrak{B}_T^r\mathfrak{C}_T^r) < |\mathfrak{D}_T|.$$

Since $\frac{b}{a} > \theta_T$, $\mathfrak{D}_T\big(1, \frac{b}{a}\big)$ is positive by Lemma A.2. In particular, $\mathfrak{D}_T$ is positive since $a^{m_T}\mathfrak{D}_T\big(1, \frac{b}{a}\big) = \mathfrak{D}_T$ where m_T is the homogenous degree of $\mathfrak{D}_T$. Now observe that

$$\mathfrak{C}_T - \mathrm{rad}(\mathfrak{A}_T\mathfrak{B}_T\mathfrak{C}_T) > \mathfrak{C}_T - \mathfrak{D}_T = a^{m_T}\left(\mathfrak{C}_T\left(1, \frac{b}{a}\right) - \mathfrak{D}_T\left(1, \frac{b}{a}\right)\right) > 0$$

where the positivity follows from Lemma A.2. Hence $(\mathfrak{A}_T, \mathfrak{B}_T, \mathfrak{C}_T)$ is a good ABC triple since $\mathrm{rad}(\mathfrak{A}_T\mathfrak{B}_T\mathfrak{C}_T) < \mathfrak{C}_T$. ■

Proposition A.5 *Let (a_0, b_0, c_0) be a good ABC triple with a_0 even. For each T define the triple P_j^T recursively by*

$$P_j^T(a_{j+1}, b_{j+1}, c_{j+1}) = (\mathfrak{A}_T(a_j, b_j)\,, \mathfrak{B}_T(a_j, b_j)\,, \mathfrak{C}_T(a_j, b_j))\,.$$

Assume further that $\frac{b_0}{a_0} > \theta_T$ and that $b_0 \equiv 0 \mod 3$ if $T = C_2 \times C_6$. Then for each $j \geq 1$, P_j^T is a good ABC triple with $a_j \equiv 0 \mod 16$, $b_j \equiv 1 \mod 4$, and $\frac{b_j}{a_j} > \theta_T$. Additionally, if $T = C_2 \times C_6$, then $a_j \equiv 0 \mod 3$.

Proof This follows automatically from Lemmas A.3 and A.5. ■

Frey Curves

Let $P = (a, b, c)$ be an ABC triple. Let $F_P = F_P(a, b)$ be the Frey curve given by the Weierstrass model

$$F_P : y^2 = x\,(x - a)\,(x + b)\,.$$

Lemma A.6 *Let (a, b, c) be an ABC triple which satisfies the assumptions of Lemma A.3. Then for each T, the Frey curve F_P with $P = (\mathfrak{A}_T, \mathfrak{B}_T, \mathfrak{C}_T)$ has torsion subgroup $F_P(\mathbb{Q})_{tors} \cong T$.*

Proof Let $\mathcal{X}_t(T)$ be as defined in Table 2.1 for $T = C_2 \times C_6, C_2 \times C_8$ and let $\mathcal{Y}_t(T)$ be as defined in Table 4.1 for $T = C_2 \times C_2, C_2 \times C_4$. In addition, let u_T, r_T, s_T, w_T, and t_T be as defined in Table A.2. We now proceed by cases.

Case I. Suppose $T = C_2 \times C_8$. Then the admissible change of variables $x \longmapsto u_T^2x + r_T$ and $y \longmapsto u_T^3y + u_T^2s_Tx + w_T$ gives a $\mathbb{Q}$-isomorphism from F_P onto $\mathcal{X}_{t_T}(T)$.

In particular, $C_2 \times C_8 \subset F_P(\mathbb{Q})_{\text{tors}}$ by Lemma 2.9. By Theorem 2.1 we conclude that $F_P(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_8$.

Case II. Suppose $T = C_2 \times C_6$. Then the admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism from F_P onto $\mathcal{X}_{t_T}(T)$. In particular, $C_2 \times C_6 \subset F_P(\mathbb{Q})_{\text{tors}}$ by Lemma 2.9. By Theorem 2.1 we conclude that $F_P(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_6$.

Case III. Suppose $T = C_2 \times C_4$. Then the admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism from F_P onto $\mathcal{Y}_{t_T}(T)$. In particular, $C_2 \times C_4 \subset F_P(\mathbb{Q})_{\text{tors}}$ by Lemma 4.2. Note that in the proof of Proposition 4.5 for $T = C_2 \times C_4$, the only assumptions on a and b used was that they were relatively prime. Consequently, we get that $F_P(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_4$.

Case IV. Suppose $T = C_2 \times C_2$. Then the admissible change of variables $x \longmapsto u_T^2 x + r_T$ and $y \longmapsto u_T^3 y + u_T^2 s_T x + w_T$ gives a $\mathbb{Q}$-isomorphism from F_P onto $\mathcal{Y}_{t_T}(T)$. In particular, $C_2 \times C_2 \subset F_P(\mathbb{Q})_{\text{tors}}$ by Lemma 4.2. Note that in the proof of Proposition 4.5 for $T = C_2 \times C_2$, the only assumptions on a and b used was that they were relatively prime. Consequently, we get that $F_P(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_2$ which concludes the lemma. ■

Theorem A.7 (Barrios-Tillman-Watts) *Let $T = C_2 \times C_{2N}$ for $N = 1, 2, 3, 4$ and consider the sequence of exceptional ABC triples P_j^T defined in Proposition A.5. Then for each $j \geq 1$, the Frey curve $F_{P_j^N}$ determined by P_j^T has torsion subgroup $F_{P_j^N}(\mathbb{Q})_{tors} \cong C_2 \times C_{2N}$.*

Proof In Proposition A.5, we saw that each P_j^T satisfies the assmptions of Lemma A.3. Consequently, the Theorem follows from Lemma A.6. ■

Examples

Recall that for a positive ABC triple $P = (a, b, c)$, the quality of P is given by

$$q(P) = \frac{\log(c)}{\log(\text{rad}(abc))}.$$

In particular, P is a good ABC triple is equivalent to $q(P) > 1$.

Example A.8 *For $T = C_2 \times C_2, C_2 \times C_4$, let $P_0 = (2^5, 7^2, 3^4)$. Then P_0 is a good ABC triple since $q(P) \approx 1.1757$. By Proposition A.5, this good ABC triple results in two distinct infinite sequences of good ABC triples P_j^T for $T = C_2 \times C_2, C_2 \times C_6$.*

For $T = C_2 \times C_6$, let $P_0 = (2^4 3^3, 17^3 61, 5^3 7^4)$. Then P_0 is a good ABC triple since $q(P) \approx 1.0261$. Moreover, $\frac{17^3 61}{2^4 3^3} > \theta_T$. By Proposition A.5, this good ABC triple results in an infinite sequence of good ABC triples P_j^T.

For $T = C_2 \times C_8$, let $P_0 = (2^2, 11^2, 5^3)$. Then P_0 is a good ABC triple since $q(P) \approx 1.0272$. Moreover, $\frac{121}{4} > \theta_T$. By Proposition A.5, this good ABC triple results in an infinite sequence of good ABC triples P_j^T.

Table A.1 gives gives a_1 and b_1 of $P_j^T = (a_j, b_j, c_j)$ as well as the quality $q\bigl(P_j^T\bigr)$ for $j = 1, 2, 3$. We note that the values of a_j and b_j are not given for $j \geq 2$ due to the size of these quantities. For $T = C_2 \times C_6, C_2 \times C_8$, we only compute $q\bigl(P_j^T\bigr)$ for $j = 1, 2$ due to computational limitations.

Table A.1.: Table for Example A.8

T	a_1	b_1	$q\bigl(P_1^T\bigr)$	$q\bigl(P_2^T\bigr)$	$q\bigl(P_3^T\bigr)$
$C_2 \times C_2$	$2^5 11^2 14657$	$3^8 13^4$	1.0755	1.0324	1.015
$C_2 \times C_4$	$2^{12} 7^4$	$3^8 17^2$	1.2425	1.0531	1.0130
$C_2 \times C_6$	$2^{16} 3^9 17^3 61$	$5^9 7^{12} 11 \cdot 27127$	1.1211	1.0278	–
$C_2 \times C_8$	$2^{12} 11^8$	$7 \cdot 31 \cdot 503 \cdot 1951 \cdot 14657^2$	1.0331	1.0040	–

Table of Polynomials

Table A.2.: Admissible Change of Variables for Lemma A.6

T	u_T	r_T	s_T	w_T	t_T
$C_2 \times C_2$	a^2	0	0	0	$\frac{b}{a}$
$C_2 \times C_4$	$2\left(a-b\right)^2$	$-2ab\left(a-b\right)^2$	$\left(a-b\right)^2$	$-2ab\left(a-b\right)^2\left(a^2+b^2\right)$	$\frac{b}{a}$
$C_2 \times C_6$	$9a^2-b^2$	$-4a^2\left(a+b\right)\left(-3a+b\right)$	$5a^2-b^2$	$36a^6-40a^4b^2+4a^2b^4$	$\frac{9a+b}{a+b}$
$C_2 \times C_8$	$\frac{1}{2a(a+b)(b^2-2ab-a^2)}$	$\frac{ab\left(a^2+b^2\right)}{(a+b)^2(b^2-2ab-a^2)}$	$\frac{a^4+4a^3b-b^4}{2a(a+b)(b^2-2ab-a^2)}$	$\frac{ab^2\left(a^2+b^2\right)^2}{(a+b)^3(b^2-2ab-a^2)^2}$	$\frac{a}{2(b-a)}$

Table A.3.: Polynomials For Appendix A

T	$C_2 \times C_2$	$C_2 \times C_4$	$C_2 \times C_6$	$C_2 \times C_8$
$\mathfrak{A}_{\mathfrak{T}}$	$8ab(a^2+b^2)$	$(2ab)^2$	$16a^3b$	$(2ab)^4$
$\mathfrak{B}_{\mathfrak{T}}$	$(a-b)^4$	$(a^2-b^2)^2$	$(a+b)^3(b-3a)$	$(a^4-6a^2b^2+b^4)(a^2+b^2)^2$
$\mathfrak{C}_{\mathfrak{T}}$	$(a+b)^4$	$(a^2+b^2)^2$	$(3a+b)(b-a)^3$	$(a^2-b^2)^4$
$\mathfrak{D}_{\mathfrak{T}}$	b^4-a^4	b^4-a^4	$(b^2-a^2)(b^2-9a^2)$	$(a^4-6a^2b^2+b^4)(b^4-a^4)$
$\mathfrak{A}^r_T$	$ab(a^2+b^2)$	ab	ab	ab
$\mathfrak{B}^r_T$	$(a-b)$	a^2-b^2	$(a+b)(b-3a)$	$(a^4-6a^2b^2+b^4)(a^2+b^2)$
$\mathfrak{C}^r_T$	$a+b$	a^2+b^2	$(3a+b)(b-a)$	a^2-b^2
f_T	$\frac{(1-t)^4}{8t(1+t^2)}-t$	$\frac{\left(1-t^2\right)^2}{(2at)^2}-t$	$\frac{(1+t)^3(t-3)}{16t}-t$	$\frac{\left(1-6t^2+t^4\right)\left(1+t^2\right)^2}{(2t)^4}-t$
g_T	$4t^3+6t^2+4t+2$	$2t^2+2$	$4t^2+8t-12$	$2t^6+6t^4-10t^2+2$
θ_T	1	1	4.87517	3.17374
U_T	$5a^3r+20a^2br+29ab^2r+$ $16b^3r+16a^3s+29a^2bs+$ $20ab^2s+5b^3s$	a^2r+2b^2r+ $2a^2s+b^2s$	$-54a^3r+144a^2br-117ab^2r+$ $24b^3r-8a^3s+$ $6a^2bs-b^3s$	$4a^6r-15a^4b^2r+20a^2b^4r-$ $10b^6r-10a^6s+$ $20a^4b^2s-15a^2b^4s+4b^6s$
V_T	$-5a^3r+20a^2br-29ab^2r+$ $16b^3r+16a^3s-$ $29a^2bs+20ab^2s-5b^3s$	$-a^2r+2b^2r+$ $2a^2s-b^2s$	$54a^3r+144a^2br+$ $117ab^2r+24b^3r-$ $8a^3s-6a^2bs+b^3s$	$-4a^6r+15a^4b^2r+44a^2b^4r+$ $26b^6r+26a^6s+$ $44a^4b^2s+15a^2b^4s-4b^6s$
W_T	$32\left(ra^7+sb^7\right)$	$4\left(ra^6+sb^6\right)$	$48\left(ra^7+sb^7\right)$	$16\left(ra^{14}+sb^{14}\right)$

B. TABLES OF GOOD ELLIPTIC CURVES

Elliptic Curves in $\mathcal{S}^{\sigma_m}$

Let $\mathcal{S}^{\sigma_m}$ and $\mathcal{S}$ be as defined in Section 3.5.5. Tables B.1 and B.2 list data pertaining to elliptic curves in these sets. The Weierstrass models of these elliptic curves are not included due to their length, but will be made available upon request.

Table B.1.: Elliptic Curves E_j in $\mathcal{S}^{\sigma_m}$

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
1	1.04	1.3936	16.0587	1	C_1
2	2.08	1.9143	11.0293	3.5	C_1
3	3.33	2.9593	10.6692	6.8123	C_2
4	4.73	4.1427	10.5204	4.7602	C_2
5	6.23	5.2735	10.1609	5.3004	C_1
6	9.67	8.1514	10.1145	4.9403	C_4
7	10.15	8.39	9.921	4.9901	C_2
8	10.37	8.5009	9.8371	5.0117	C_2
9	10.52	8.574	9.7838	5.0254	C_2
10	10.85	8.7395	9.6684	5.0552	C_2
11	10.95	8.7908	9.634	5.064	C_2
12	10.99	8.8125	9.6196	5.0677	C_2
13	11.13	8.8826	9.574	5.0795	C_2
14	11.16	8.8971	9.5647	5.0819	C_2
15	11.22	8.9235	9.548	5.0862	C_2
16	11.43	9.0294	9.4822	5.1031	C_2

continued on next page

Table B.1.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
17	11.61	9.1212	9.4272	5.1173	C_2
18	11.64	9.1357	9.4186	5.1195	C_2
19	11.65	9.1403	9.4159	5.1202	C_2
20	11.69	9.162	9.4032	5.1235	C_2
21	11.79	9.2133	9.3736	5.1311	C_2
22	12.81	9.9851	9.3529	7.0748	C_2
23	13.11	9.9851	9.1382	6.9123	C_2
24	14.67	10.9168	8.9271	6.9383	C_2
25	15.67	11.6026	8.8847	8.1963	C_2
26	16.15	11.8411	8.7994	8.1314	C_2
27	16.37	11.9521	8.7615	8.1025	C_2
28	16.78	12.1595	8.6932	8.0505	C_2
29	16.85	12.1906	8.6833	8.043	C_2
30	16.95	12.2419	8.667	8.0306	C_2
31	17.13	12.3338	8.6384	8.0088	C_2
32	17.24	12.3867	8.6223	7.9965	C_2
33	17.26	12.3981	8.6188	7.9938	C_2
34	17.3	12.4193	8.6124	7.989	C_2
35	17.43	12.4805	8.594	7.975	C_2
36	17.48	12.509	8.5856	7.9685	C_2
37	17.61	12.5723	8.567	7.9544	C_2
38	17.65	12.5914	8.5614	7.9502	C_2
39	17.68	12.6047	8.5576	7.9472	C_2
40	17.72	12.6252	8.5516	7.9427	C_2
41	17.78	12.6579	8.5423	7.9356	C_2

continued on next page

Table B.1.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
42	17.83	12.6833	8.535	7.9301	C_2
43	17.84	12.6892	8.5333	7.9288	C_2
44	17.94	12.7362	8.5201	7.9187	C_2
45	17.96	12.7476	8.5169	7.9162	C_2
46	18	12.7688	8.5109	7.9117	C_2
47	18.06	12.7989	8.5026	7.9054	C_2
48	18.13	12.83	8.494	7.8988	C_2
49	18.15	12.8433	8.4903	7.896	C_2
50	18.25	12.8907	8.4774	7.8862	C_2
51	18.31	12.9218	8.469	7.8798	C_2
52	18.32	12.9277	8.4674	7.8786	C_2
53	18.35	12.9436	8.4631	7.8753	C_2
54	18.37	12.9542	8.4603	7.8731	C_2
55	18.41	12.9731	8.4552	7.8693	C_2
56	18.42	12.9747	8.4548	7.869	C_2
57	18.42	12.9763	8.4544	7.8687	C_2
58	18.48	13.0073	8.4461	7.8624	C_2
59	18.52	13.026	8.4412	7.8586	C_2
60	18.54	13.0375	8.4382	7.8563	C_2
61	18.54	13.0386	8.4379	7.8561	C_2
62	18.58	13.0587	8.4326	7.8521	C_2
63	18.63	13.0823	8.4264	7.8474	C_2
64	18.7	13.1179	8.4172	7.8404	C_2
65	18.72	13.1293	8.4143	7.8381	C_2
66	18.76	13.1484	8.4093	7.8344	C_2

continued on next page

Table B.1.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
67	18.77	13.1505	8.4088	7.834	C_2
68	18.79	13.1617	8.4059	7.8318	C_2
69	18.83	13.1822	8.4007	7.8278	C_2
70	18.85	13.1928	8.398	7.8257	C_2
71	18.87	13.2034	8.3953	7.8237	C_2
72	18.9	13.2148	8.3924	7.8215	C_2
73	18.95	13.2402	8.386	7.8166	C_2
74	18.96	13.2461	8.3845	7.8155	C_2
75	18.99	13.2646	8.3799	7.8119	C_2
76	19.02	13.2772	8.3767	7.8095	C_2
77	19.05	13.2931	8.3727	7.8065	C_2
78	19.06	13.2972	8.3717	7.8057	C_2
79	19.14	13.3359	8.3621	7.7984	C_2
80	19.18	13.3564	8.3571	7.7946	C_2
81	19.22	13.3755	8.3524	7.791	C_2
82	19.24	13.3888	8.3491	7.7885	C_2
83	19.24	13.3891	8.3491	7.7885	C_2
84	19.27	13.4003	8.3463	7.7864	C_2
85	19.28	13.4082	8.3444	7.785	C_2
86	19.31	13.4204	8.3415	7.7827	C_2
87	19.31	13.4215	8.3412	7.7825	C_2
88	19.33	13.4318	8.3387	7.7806	C_2
89	19.35	13.442	8.3362	7.7787	C_2
90	19.4	13.4674	8.3301	7.7741	C_2
91	19.42	13.4788	8.3274	7.772	C_2

continued on next page

Table B.1.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
92	19.43	13.4827	8.3264	7.7713	C_2
93	19.44	13.4847	8.326	7.7709	C_2
94	19.55	13.491	8.2794	8.0307	C_2
95	19.58	13.5031	8.2766	8.0282	C_2
96	19.61	13.5188	8.2729	8.025	C_2
97	19.64	13.5342	8.2694	8.0218	C_2
98	19.65	13.5411	8.2678	8.0204	C_2
99	19.66	13.5449	8.2669	8.0196	C_2
100	19.68	13.555	8.2646	8.0175	C_2
101	19.69	13.5607	8.2633	8.0163	C_2
102	19.72	13.5734	8.2603	8.0137	C_2
103	19.73	13.5811	8.2586	8.0122	C_2
104	19.74	13.5855	8.2576	8.0113	C_2
105	19.74	13.5861	8.2574	8.0111	C_2
106	19.75	13.5892	8.2567	8.0105	C_2
107	19.77	13.5969	8.255	8.0089	C_2
108	19.79	13.6072	8.2526	8.0069	C_2
109	19.8	13.6122	8.2515	8.0058	C_2
110	19.85	13.6374	8.2458	8.0007	C_2
111	19.88	13.652	8.2425	7.9978	C_2
112	19.89	13.6592	8.2409	7.9964	C_2
113	19.9	13.6622	8.2402	7.9958	C_2
114	19.91	13.6716	8.2381	7.9939	C_2
115	19.94	13.6853	8.235	7.9912	C_2
116	19.96	13.6933	8.2332	7.9895	C_2

continued on next page

Table B.1.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
117	19.98	13.7054	8.2305	7.9871	C_2
118	19.99	13.7079	8.2299	7.9867	C_2
119	20.01	13.7182	8.2276	7.9846	C_2
120	20.02	13.7251	8.2261	7.9832	C_2
121	20.03	13.7296	8.2251	7.9823	C_2
122	20.05	13.7417	8.2224	7.98	C_2
123	20.06	13.7446	8.2218	7.9794	C_2
124	20.09	13.7573	8.219	7.9769	C_2
125	32.05	20.7895	7.7831	7.405	C_2
126	35.53	21.852	7.3805	5.7173	C_6
127	35.8	21.9098	7.3444	6.4075	C_4
128	37.54	22.7925	7.286	5.4236	C_6
129	39.66	23.952	7.247	6.428	C_2
130	40.29	24.1201	7.184	4.4724	C_2
131	41.35	24.5769	7.1315	7.0026	C_1
132	42.38	24.8519	7.0363	5.1039	C_2
133	42.94	25.0177	6.9916	4.711	C_2
134	43.1	25.0359	6.9714	5.8854	C_4
135	45.39	26.367	6.9705	6.7577	C_1
136	47.94	27.7515	6.9464	6.8701	C_1
137	50.21	28.5603	6.8255	6.6845	C_2
138	57.18	32.5053	6.8218	6.1759	C_2
139	59.01	33.2702	6.7659	6.3336	C_6
140	59.73	33.633	6.7575	6.3286	C_2
141	62.34	35.0898	6.7543	6.6107	C_6

continued on next page

Table B.1.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
142	64.58	35.6548	6.6252	6.0727	C_2
143	64.76	35.6692	6.6095	6.4893	C_2
144	67.18	36.9559	6.6011	6.5522	C_6
145	70.54	38.7635	6.5939	6.5253	C_8
146	71.28	39.1547	6.5913	6.5376	$C_2 \times C_2$
147	72.05	39.3702	6.5573	6.506	C_2
148	72.94	39.7962	6.5475	6.5031	C_2
149	73.39	39.9817	6.5375	6.1138	C_2
150	74.82	40.7383	6.534	6.2822	C_2

Elliptic Curves in $\mathcal{S}$

Table B.2.: Elliptic Curves E_j in $\mathcal{S}$

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
1	7.11	5.6226	9.4962	9.02	C_1
2	7.95	6.0451	9.1245	8.6989	C_1
3	11.22	8.5426	9.1332	8.689	C_2
4	11.7	8.7812	9.0055	8.5793	C_2
5	11.92	8.8921	8.9495	8.5313	C_2
6	12.07	8.9652	8.9138	8.5007	C_2
7	15.67	11.3498	8.6911	8.4834	C_2
8	16.15	11.5883	8.6116	8.41	C_2

continued on next page

Table B.2.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
9	16.9	12.0705	8.573	8.3864	C_2
10	16.9	12.162	8.638	8.3502	C_2
11	17.37	12.309	8.5023	8.3209	C_2
12	17.59	12.42	8.4708	8.2916	C_2
13	17.74	12.493	8.4504	8.2727	C_2
14	17.59	12.5115	8.5332	8.2568	C_2
15	17.94	12.5912	8.4236	8.2479	C_2
16	18.01	12.6275	8.4138	8.2388	C_2
17	18.07	12.6585	8.4055	8.2311	C_2
18	18.17	12.7099	8.3919	8.2185	C_2
19	18.22	12.7316	8.3862	8.2132	C_2
20	18.07	12.7501	8.4663	8.1972	C_2
21	18.41	12.8297	8.3608	8.1896	C_2
22	18.44	12.8425	8.3575	8.1866	C_2
23	18.46	12.8546	8.3544	8.1837	C_2
24	18.49	12.866	8.3515	8.181	C_2
25	18.57	12.9065	8.3413	8.1715	C_2
26	18.62	12.9326	8.3347	8.1654	C_2
27	18.64	12.9407	8.3327	8.1636	C_2
28	18.65	12.9484	8.3308	8.1618	C_2
29	18.71	12.9769	8.3236	8.1552	C_2
30	18.78	13.0137	8.3145	8.1467	C_2
31	18.85	13.05	8.3056	8.1385	C_2
32	18.87	13.0593	8.3034	8.1363	C_2
33	18.92	13.0811	8.2981	8.1314	C_2

continued on next page

Table B.2.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
34	18.94	13.0931	8.2951	8.1287	C_2
35	19.02	13.1324	8.2857	8.1199	C_2
36	19.04	13.1451	8.2826	8.1171	C_2
37	19.05	13.1481	8.2819	8.1164	C_2
38	19.1	13.1712	8.2764	8.1113	C_2
39	19.11	13.1792	8.2745	8.1095	C_2
40	19.16	13.2041	8.2686	8.1041	C_2
41	19.18	13.211	8.2669	8.1026	C_2
42	19.19	13.2155	8.2659	8.1016	C_2
43	19.22	13.2306	8.2623	8.0983	C_2
44	19.26	13.2523	8.2572	8.0935	C_2
45	19.27	13.256	8.2563	8.0927	C_2
46	19.29	13.2668	8.2538	8.0904	C_2
47	19.31	13.2771	8.2514	8.0881	C_2
48	19.32	13.2821	8.2502	8.0871	C_2
49	19.33	13.2886	8.2487	8.0857	C_2
50	19.35	13.2979	8.2466	8.0837	C_2
51	19.41	13.3291	8.2393	8.077	C_2
52	19.46	13.3552	8.2333	8.0714	C_2
53	19.48	13.3632	8.2315	8.0697	C_2
54	19.5	13.371	8.2297	8.068	C_2
55	19.51	13.3753	8.2287	8.0671	C_2
56	19.53	13.3867	8.2261	8.0647	C_2
57	19.55	13.3995	8.2232	8.062	C_2
58	19.58	13.4116	8.2205	8.0595	C_2

continued on next page

Table B.2.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
59	19.61	13.4272	8.2169	8.0562	C_2
60	19.64	13.4426	8.2135	8.053	C_2
61	19.65	13.4496	8.2119	8.0515	C_2
62	19.66	13.4533	8.211	8.0507	C_2
63	19.68	13.4635	8.2088	8.0486	C_2
64	19.69	13.4691	8.2075	8.0474	C_2
65	19.72	13.4819	8.2046	8.0448	C_2
66	19.73	13.4896	8.2029	8.0432	C_2
67	19.74	13.494	8.2019	8.0423	C_2
68	19.74	13.4946	8.2018	8.0422	C_2
69	19.75	13.4976	8.2011	8.0415	C_2
70	19.77	13.5054	8.1994	8.0399	C_2
71	19.79	13.5157	8.1971	8.0378	C_2
72	19.8	13.5207	8.196	8.0368	C_2
73	19.85	13.5459	8.1904	8.0316	C_2
74	19.88	13.5605	8.1872	8.0286	C_2
75	19.89	13.5676	8.1856	8.0272	C_2
76	19.9	13.5707	8.185	8.0265	C_2
77	19.9	13.572	8.1847	8.0263	C_2
78	19.91	13.58	8.1829	8.0246	C_2
79	19.94	13.5937	8.1799	8.0218	C_2
80	19.96	13.6018	8.1782	8.0202	C_2
81	19.98	13.6138	8.1755	8.0178	C_2
82	19.99	13.6163	8.175	8.0173	C_2
83	20.01	13.6266	8.1727	8.0152	C_2

continued on next page

Table B.2.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
84	20.02	13.6335	8.1712	8.0138	C_2
85	20.03	13.638	8.1703	8.0129	C_2
86	20.05	13.6501	8.1677	8.0105	C_2
87	20.06	13.6531	8.167	8.0099	C_2
88	20.09	13.6658	8.1643	8.0073	C_2
89	20.11	13.6786	8.1615	8.0048	C_2
90	20.13	13.6894	8.1592	8.0026	C_2
91	20.14	13.6906	8.1589	8.0024	C_2
92	20.14	13.6919	8.1587	8.0021	C_2
93	20.16	13.7021	8.1565	8.0001	C_2
94	19.98	13.7054	8.2305	7.9871	C_2
95	19.99	13.7079	8.2299	7.9867	C_2
96	20.01	13.7182	8.2276	7.9846	C_2
97	20.02	13.7251	8.2261	7.9832	C_2
98	20.03	13.7296	8.2251	7.9823	C_2
99	20.05	13.7417	8.2224	7.98	C_2
100	20.06	13.7446	8.2218	7.9794	C_2
101	20.09	13.7573	8.219	7.9769	C_2
102	20.14	13.7822	8.2135	7.972	C_2
103	20.14	13.7834	8.2132	7.9717	C_2
104	20.16	13.7936	8.211	7.9697	C_2
105	32.05	20.5156	7.6806	7.5762	C_2
106	32.05	20.7895	7.7831	7.405	C_2
107	38.91	23.1808	7.1498	7.0676	C_2
108	38.91	23.2766	7.1793	7.0497	C_2

continued on next page

Table B.2.: *continued*

j	$\log N_{E_j}$	$h_{\text{naive}}(E_j)$	$\sigma_m(E_j)$	$\sigma(E_j)$	T
109	39.37	23.2866	7.0985	7.0151	C_2
110	41.35	24.5769	7.1315	7.0026	C_1
111	47.94	27.7515	6.9464	6.8701	C_1
112	66.42	37.6628	6.8043	6.7205	C_4
113	66.42	37.9637	6.8587	6.6912	C_2
114	70.54	38.9732	6.6296	6.585	C_2
115	70.54	39.1164	6.654	6.5667	C_2
116	71.28	39.2668	6.6102	6.566	C_2
117	71.28	39.4515	6.6413	6.5353	C_2
118	72.05	39.3455	6.5532	6.5085	C_2
119	72.05	39.3702	6.5573	6.506	C_2
120	72.94	39.7962	6.5475	6.5031	C_2

Best Known Modified Szpiro and Szpiro Ratios

The tables that follow give the best known modified Szpiro and Szpiro ratios of elliptic curves. As before, the Weierstrass models of these elliptic curves is not given but will be provided upon request. Each table has a column "By" which refers to where the given elliptic curve originated from. By "C" we refer to elliptic curves found in Cremona's database,"N" refers to elliptic curves found by Nitaj, "B-Y" refers to elliptic curves found by Bennett and Yazdani, and "Ba" refers to elliptic curves found by the author.

Table B.3.: Best Known Modified Szpiro Ratios

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	T	By
1	1.0414	1.3936	16.0587	1	C_1	C
2	1.1461	1.2794	13.3951	3.8385	C_2	C
3	1.1761	1.2539	12.7942	2.2171	C_2	C
4	2.0828	1.9143	11.0293	3.5	C_1	C
5	1.4771	1.3521	10.984	3.323	C_2	C
6	1.6532	1.4925	10.8333	3.3088	C_2	C
7	1.2788	1.1418	10.7152	1	C_1	C
8	3.3284	2.9593	10.6692	6.8123	C_2	C
9	4.7253	4.1427	10.5204	4.7602	C_2	C
10	3.0856	2.6873	10.4507	5.9897	C_2	C
11	3.0065	2.6116	10.4239	6.0767	C_1	C
12	1.3222	1.1439	10.3816	1.6392	C_2	C
13	4.3376	3.7425	10.3536	4.9188	C_1	C
14	3.6425	3.134	10.3249	4.2314	C_2	C
15	3.7386	3.2063	10.2914	4.37	C_2	C
16	2.3222	1.9912	10.2894	2.3927	C_2	C
17	1.8751	1.6034	10.2615	3.6272	C_2	C

continued on next page

Table B.3.: *continued*

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	T	By
18	1.9912	1.7019	10.2565	4.7559	C_2	C
19	1.1461	0.9785	10.2445	5.465	C_2	C
20	2.7559	2.351	10.2371	3.392	C_2	C
21	6.228	5.2735	10.1609	5.3004	C_1	B-Y
22	5.2027	4.3951	10.1373	7.8574	C_1	C
23	4.3733	3.6867	10.116	7.0314	C_1	C
24	9.671	8.1514	10.1145	4.9403	C_4	N
25	5.2025	4.3813	10.1058	4.8739	C_2	C
26	3.2874	2.7653	10.0944	7.4446	C_2	C
27	3.8055	3.1978	10.0838	6.7104	C_2	C
28	3.0453	2.5589	10.0832	4.6301	C_2	C
29	3.69	3.0923	10.0561	5.9294	C_1	C
30	3.4849	2.905	10.0032	5.3061	C_1	C

Table B.4.: Best Known Szpiro Ratios

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	T	By
1	7.105	5.6226	9.4962	9.02	C_1	B-Y
2	3.1106	2.577	9.9413	8.9037	C_1	C
3	3.9782	3.2011	9.6561	8.8431	C_1	C
4	5.4462	4.2596	9.3855	8.8333	C_1	C
5	6.4026	4.971	9.3169	8.8119	C_2	N
6	3.9863	3.2727	9.8517	8.8016	C_2	C
7	3.601	2.9082	9.6914	8.7924	C_1	C
8	4.514	3.5735	9.4999	8.7827	C_1	C

continued on next page

Table B.4.: *continued*

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	T	By
9	2.9335	2.4104	9.8601	8.7573	C_1	C
10	7.9501	6.0451	9.1245	8.6989	C_1	B-Y
11	11.224	8.5426	9.1332	8.689	C_2	N
12	10.4331	8.0134	9.2169	8.6622	C_2	B-Y
13	7.105	5.3616	9.0554	8.6224	C_3	B-Y
14	6.8797	5.2096	9.0869	8.6169	C_2	N
15	8.219	6.1795	9.0223	8.6107	C_1	B-Y
16	8.7857	6.5548	8.9529	8.5966	C_1	N
17	11.7011	8.7812	9.0055	8.5793	C_2	N
18	8.3838	6.2619	8.9629	8.5593	C_1	B-Y
19	10.9102	8.252	9.0762	8.5458	C_2	B-Y
20	4.4553	3.4397	9.2646	8.5387	C_1	C
21	11.5576	8.6875	9.02	8.5373	C_2	B-Y
22	11.5576	8.6874	9.02	8.5373	C_2	B-Y
23	7.1015	5.3205	8.9904	8.5352	C_4	N
24	8.7583	6.509	8.9181	8.5318	C_2	N
25	11.923	8.8921	8.9495	8.5313	C_2	N
26	5.1083	3.9073	9.1788	8.5253	C_2	C
27	3.5877	2.8155	9.4172	8.5175	C_1	C
28	4.9911	3.8121	9.1653	8.5167	C_1	C
29	5.3607	4.1073	9.1944	8.5157	C_1	C
30	8.5674	6.3538	8.8994	8.5045	C_1	B-Y

Best σ_m and σ by Torsion Subgroup

Table B.5.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_1$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	1.0414	1.3936	16.0587	1	C
2	2.0828	1.9143	11.0293	3.5	C
3	1.2788	1.1418	10.7152	1	C
4	3.0065	2.6116	10.4239	6.0767	C
5	4.3376	3.7425	10.3536	4.9188	C
6	6.228	5.2735	10.1609	5.3004	B-Y
7	5.2027	4.3951	10.1373	7.8574	C
8	4.3733	3.6867	10.116	7.0314	C
9	3.69	3.0923	10.0561	5.9294	C
10	3.4849	2.905	10.0032	5.3061	C

Table B.6.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_1$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	7.105	5.6226	9.4962	9.02	B-Y
2	3.1106	2.577	9.9413	8.9037	C
3	3.9782	3.2011	9.6561	8.8431	C
4	5.4462	4.2596	9.3855	8.8333	C
5	3.601	2.9082	9.6914	8.7924	C
6	4.514	3.5735	9.4999	8.7827	C
7	2.9335	2.4104	9.8601	8.7573	C
8	7.9501	6.0451	9.1245	8.6989	B-Y
9	8.219	6.1795	9.0223	8.6107	B-Y
10	8.7857	6.5548	8.9529	8.5966	N

Table B.7.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_2$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	1.1461	1.2794	13.3951	3.8385	C
2	1.1761	1.2539	12.7942	2.2171	C
3	1.4771	1.3521	10.984	3.323	C
4	1.6532	1.4925	10.8333	3.3088	C
5	3.3284	2.9593	10.6692	6.8123	C
6	4.7253	4.1427	10.5204	4.7602	C
7	3.0856	2.6873	10.4507	5.9897	C
8	1.3222	1.1439	10.3816	1.6392	C
9	3.6425	3.134	10.3249	4.2314	C
10	3.7386	3.2063	10.2914	4.37	C

Table B.8.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_2$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	6.4026	4.971	9.3169	8.8119	N
2	3.9863	3.2727	9.8517	8.8016	C
3	11.224	8.5426	9.1332	8.689	N
4	10.4331	8.0134	9.2169	8.6622	B-Y
5	6.8797	5.2096	9.0869	8.6169	N
6	11.7011	8.7812	9.0055	8.5793	N
7	10.9102	8.252	9.0762	8.5458	B-Y
8	11.5576	8.6875	9.02	8.53729	B-Y
9	11.5576	8.6874	9.02	8.53728	B-Y
10	8.7583	6.509	8.9181	8.5318	N

Table B.9.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_3$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	6.7052	5.5121	9.8648	5.3502	B-Y
2	5.5836	4.4626	9.5907	3.7718	C
3	3.8519	2.9978	9.3392	7.0964	C
4	5.9966	4.6322	9.2696	5.3561	N
5	6.3505	4.9031	9.265	6.9488	B-Y
6	6.3505	4.9031	9.265	2.3163	B-Y
7	6.228	4.7964	9.2416	7.6215	B-Y
8	4.6378	3.5545	9.1969	3.1264	C
9	10.2284	7.8202	9.1747	8.063	B-Y
10	3.8837	2.9497	9.1141	7.3068	C

Table B.10.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_3$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	7.105	5.3616	9.0554	8.6224	B-Y
2	9.7512	7.1087	8.748	8.3541	B-Y
3	8.0593	5.8611	8.727	8.3072	B-Y
4	5.1896	3.7988	8.784	8.1606	C
5	8.7857	6.4368	8.7918	8.1579	N
6	6.932	5.0013	8.6578	8.1254	B-Y
7	8.004	5.6807	8.5168	8.1117	B-Y
8	10.2284	7.8202	9.1747	8.063	B-Y
9	9.74	6.7933	8.3696	8.0483	N
10	12.8001	9.0919	8.5236	8.0005	B-Y

Table B.11.: Best σ_m for $E(\mathbb{Q})_{\mathrm{tors}} \cong C_4$

Rank	$\log N_E$	$h_{\mathrm{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	9.671	8.1514	10.1145	4.9403	N
2	3.6933	3	9.7475	4.4081	C
3	4.1483	3.3112	9.5784	5.7275	C
4	1.8921	1.4995	9.5102	4.2522	C
5	5.0217	3.8794	9.2705	3.8597	C
6	10.5741	8.1514	9.2506	8.0676	B-Y
7	4.7278	3.6419	9.2437	3.7546	C
8	1.7993	1.3825	9.2197	2.7955	C
9	12.0691	9.2659	9.2129	7.5614	N
10	1.1761	0.8961	9.1433	1	C

Table B.12.: Best σ for $E(\mathbb{Q})_{\mathrm{tors}} \cong C_4$

Rank	$\log N_E$	$h_{\mathrm{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	7.1015	5.3205	8.9904	8.5352	N
2	15.6709	11.0439	8.4569	8.2502	B-Y
3	16.574	11.6508	8.4355	8.2391	B-Y
4	12.9722	9.2662	8.5717	8.1874	B-Y
5	10.0461	7.096	8.4761	8.1453	B-Y
6	12.2037	8.6077	8.464	8.1074	B-Y
7	13.317	9.2474	8.3329	8.0884	B-Y
8	11.6474	8.1202	8.3661	8.0878	B-Y
9	12.8363	8.9223	8.3409	8.087	B-Y
10	10.5741	8.1514	9.2506	8.0676	B-Y

Table B.13.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_5$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	13.3832	9.5211	8.5371	7.3009	B-Y
2	11.8831	8.449	8.5321	6.2449	N
3	13.7441	9.6366	8.4138	5.4948	N
4	8.5927	6.0068	8.3887	8.0067	B-Y
5	9.5534	6.6564	8.3612	7.5939	N
6	7.3134	5.045	8.2779	6.7144	N
7	1.0414	0.7169	8.2605	5	C
8	13.7715	9.4136	8.2027	7.5004	N
9	11.641	7.947	8.192	6.9278	B-Y
10	11.5493	7.8442	8.1503	7.2499	B-Y

Table B.14.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_5$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	8.5927	6.0068	8.3887	8.0067	B-Y
2	9.5534	6.6564	8.3612	7.5939	N
3	13.7715	9.4136	8.2027	7.5004	N
4	13.9764	9.0574	7.7766	7.4436	N
5	7.0098	4.66	7.9774	7.3561	B-Y
6	11.6205	7.6857	7.9367	7.3437	B-Y
7	13.3832	9.5211	8.5371	7.3009	B-Y
8	11.5493	7.8442	8.1503	7.2499	B-Y
9	12.5761	7.8386	7.4795	7.2223	B-Y
10	15.2647	10.1548	7.983	7.1909	N

Table B.15.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_6$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	1.9542	1.5906	9.7672	3.9766	C
2	5.1083	3.8883	9.1342	7.3124	C
3	7.2107	5.4243	9.0271	5.6695	N
4	5.4979	4.094	8.9357	7.0766	C
5	5.5854	4.1459	8.9072	8.3096	C
6	4.1096	3.0464	8.8955	5.6309	C
7	3.6789	2.691	8.7775	5.2711	C
8	2.7993	2.0453	8.7675	3.7427	C
9	5.376	3.9205	8.7511	6.4273	C
10	5.5854	4.0716	8.7477	7.8873	C

Table B.16.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_6$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	5.5854	4.1459	8.9072	8.3096	C
2	5.5854	4.0716	8.7477	7.8873	C
3	5.5774	3.9221	8.4385	7.8611	C
4	7.2107	5.1233	8.5262	7.6868	N
5	15.0308	9.7856	7.8125	7.5729	N
6	6.7336	4.515	8.0463	7.5699	N
7	5.1083	3.5879	8.4284	7.5161	C
8	32.0533	20.2606	7.5851	7.4877	Ba
9	32.0533	20.3147	7.6053	7.4784	Ba
10	5.5774	3.8209	8.2209	7.474	C

Table B.17.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_7$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	2.9335	2.1108	8.6345	6.6196	C
2	8.3071	5.3759	7.7658	5.4996	N
3	17.2439	10.8613	7.5584	7.3625	N
4	18.966	11.7054	7.4061	6.7331	B-Y
5	8.0805	4.9865	7.4052	6.3564	N
6	17.8125	10.9867	7.4016	6.6911	N
7	16.8791	10.3484	7.3571	6.4517	N
8	16.1434	9.866	7.3338	7.1062	N
9	11.296	6.9	7.33	5.7148	B-Y
10	15.828	9.6244	7.2967	6.4658	N

Table B.18.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_7$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	17.2439	10.8613	7.5584	7.3625	N
2	16.1434	9.866	7.3338	7.1062	N
3	22.1241	13.0172	7.0605	6.9203	Ba
4	41.3549	24.0542	6.9798	6.9015	Ba
5	31.529	18.3693	6.9914	6.8898	Ba
6	30.5304	17.5546	6.8999	6.8019	Ba
7	36.9497	21.2101	6.8883	6.8004	Ba
8	32.5831	18.9757	6.9885	6.7945	Ba
9	26.4268	15.2317	6.9165	6.7652	Ba
10	19.15	11.0648	6.9336	6.7645	N

Table B.19.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_8$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	1.1761	0.8063	8.2265	5.5659	C
2	3.7568	2.5057	8.0036	5.2881	C
3	6.0392	3.964	7.8765	7.3403	Ba
4	5.6389	3.6912	7.855	7.0385	Ba
5	5.4264	3.5049	7.7508	4.9534	C
6	4.1996	2.696	7.7037	5.6891	C
7	13.5995	8.7096	7.6852	5.6546	N
8	11.5099	7.3698	7.6836	6.7376	N
9	5.6894	3.6276	7.6513	7.0911	Ba
10	2.3222	1.4648	7.5695	4.7718	C

Table B.20.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_8$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	6.0392	3.964	7.8765	7.3403	Ba
2	11.2638	7.0332	7.4928	7.0962	Ba
3	5.6894	3.6276	7.6513	7.0911	N
4	5.6389	3.6912	7.855	7.0385	Ba
5	22.1795	13.2545	7.1712	7.0305	Ba
6	16.8025	10.2792	7.3412	6.9995	Ba
7	10.8492	6.5354	7.2286	6.8817	N
8	23.8054	13.9792	7.0467	6.8343	Ba
9	27.446	15.8907	6.9478	6.8297	Ba
10	9.9853	5.9207	7.1153	6.8203	N

Table B.21.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_9$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	22.2722	12.8496	6.9232	6.2785	Ba
2	47.9415	27.6277	6.9153	6.5242	Ba
3	8.8598	5.0701	6.8671	5.1416	Ba
4	45.392	25.8181	6.8254	6.6725	Ba
5	40.5668	23.066	6.8231	5.7852	Ba
6	25.8537	14.6733	6.8106	5.5363	Ba
7	25.8546	14.6736	6.8105	5.5362	Ba
8	31.8033	17.8476	6.7342	6.3266	Ba
9	30.6628	17.1762	6.722	5.5376	Ba
10	30.6632	17.1764	6.7219	5.5375	Ba

Table B.22.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_9$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	45.392	25.8181	6.8254	6.6725	Ba
2	46.0298	25.5196	6.653	6.5844	Ba
3	41.9014	23.1685	6.6351	6.5424	Ba
4	38.4149	21.4147	6.6895	6.5378	Ba
5	47.9415	27.6277	6.9153	6.5242	Ba
6	34.3046	18.8048	6.5781	6.4836	Ba
7	47.4918	26.3517	6.6584	6.4834	Ba
8	51.9158	28.2517	6.5302	6.4679	Ba
9	40.6088	22.6083	6.6808	6.452	Ba
10	40.3045	22.0003	6.5502	6.4517	Ba

Table B.23.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_{10}$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	14.1479	8.6258	7.3163	7.0006	Ba
2	14.1479	8.6246	7.3152	6.686	Ba
3	2.7559	1.6564	7.2124	5.8239	C
4	17.7436	10.622	7.1837	5.1316	Ba
5	23.9438	13.9711	7.0019	5.8695	Ba
6	17.7436	10.321	6.9801	5.954	Ba
7	8.5358	4.9615	6.9751	5.7738	Ba
8	20.9924	12.1684	6.9559	4.9759	Ba
9	39.3827	22.5171	6.861	6.1057	Ba
10	23.9438	13.67	6.851	6.2848	Ba

Table B.24.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_{10}$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	14.1479	8.6258	7.3163	7.0006	Ba
2	44.8544	25.2964	6.7676	6.6937	Ba
3	14.1479	8.6246	7.3152	6.686	Ba
4	44.8544	25.2268	6.749	6.6402	Ba
5	50.2119	28.1464	6.7266	6.6219	Ba
6	57.1791	31.8115	6.6762	6.6105	Ba
7	50.2119	27.8946	6.6664	6.6018	Ba
8	50.6744	28.1466	6.6653	6.5959	Ba
9	43.2765	24.0527	6.6695	6.5649	Ba
10	42.3074	23.5139	6.6694	6.5631	Ba

Table B.25.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_{12}$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	16.4632	10.8042	7.8752	6.4694	Ba
2	6.8059	4.3028	7.5866	6.1696	Ba
3	5.192	3.1899	7.3727	5.2997	C
4	11.2702	6.8354	7.2781	6.9035	Ba
5	12.1426	7.3229	7.2369	6.5351	Ba
6	8.9416	5.3242	7.1453	5.2472	Ba
7	8.014	4.7655	7.1358	5.2583	Ba
8	8.5442	5.067	7.1164	5.322	Ba
9	14.8786	8.8097	7.1053	6.7731	Ba
10	11.1158	6.5582	7.0798	6.556	Ba

Table B.26.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_{12}$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	11.2702	6.8354	7.2781	6.9035	Ba
2	14.8786	8.8097	7.1053	6.7731	Ba
3	22.5087	12.7648	6.8053	6.6692	Ba
4	39.044	21.9509	6.7465	6.6631	Ba
5	30.9516	17.4563	6.7678	6.6489	Ba
6	30.4164	17.4477	6.8836	6.6315	Ba
7	40.815	22.8596	6.721	6.6242	Ba
8	39.481	22.1265	6.7252	6.6178	Ba
9	8.8844	5.1638	6.9746	6.6108	Ba
10	62.3421	34.5759	6.6554	6.6035	Ba

Table B.27.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_2$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	4.7253	3.8417	9.7559	6.8759	C
2	9.671	7.8504	9.7409	7.1539	N
3	1.1761	0.9529	9.7228	4.4341	C
4	10.1481	8.089	9.5651	7.0996	B-Y
5	10.37	8.1999	9.4888	7.0761	B-Y
6	10.5161	8.2729	9.4403	7.0611	B-Y
7	5.2025	4.0802	9.4115	6.7955	C
8	10.8471	8.4384	9.3353	7.0287	B-Y
9	10.9498	8.4898	9.3041	7.0191	B-Y
10	10.9932	8.5115	9.291	7.0151	B-Y

Table B.28.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_2$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	6.4026	4.8779	9.1424	8.4619	N
2	10.7537	7.724	8.6192	8.3121	N
3	15.6709	11.3016	8.6542	8.31	B-Y
4	6.8797	5.1165	8.9245	8.2912	N
5	16.8956	11.9317	8.4744	8.2778	B-Y
6	11.7928	8.4825	8.6316	8.2572	N
7	11.224	8.5423	9.1329	8.245	N
8	16.148	11.5402	8.5758	8.2417	B-Y
9	7.1015	5.2274	8.8331	8.2196	N
10	17.3727	12.1702	8.4064	8.2153	B-Y

Table B.29.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_4$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	4.7278	3.3408	8.4797	5.7351	C
2	4.7592	3.3399	8.4215	6.6384	C
3	7.539	5.1921	8.2644	6.9951	N
4	12.2528	8.3861	8.2131	7.218	N
5	5.0879	3.4491	8.1348	6.7562	C
6	4.6308	3.1374	8.13	5.3121	C
7	13.1559	8.6871	7.9239	7.4605	N
8	13.1516	8.6558	7.8979	7.4051	N
9	5.6389	3.6902	7.8531	6.2239	C
10	11.2638	7.3329	7.8122	7.0216	N

Table B.30.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_4$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	13.1559	8.6871	7.9239	7.4605	N
2	13.1516	8.6558	7.8979	7.4051	N
3	12.2528	8.3861	8.2131	7.218	N
4	11.2638	7.3329	7.8122	7.0216	N
5	22.1795	13.3086	7.2005	7.017	Ba
6	31.6677	18.7487	7.1045	6.9989	Ba
7	7.539	5.1921	8.2644	6.9951	N
8	9.9853	6.11	7.3428	6.992	N
9	31.6677	18.6731	7.0759	6.9248	Ba
10	28.2863	16.5874	7.037	6.9087	Ba

Table B.31.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_6$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	7.2107	5.1233	8.5262	6.8473	N
2	8.0892	5.4227	8.0444	6.3285	Ba
3	5.0712	3.3891	8.0196	5.6586	C
4	12.542	8.3282	7.9683	6.7848	N
5	4.1611	2.7581	7.9541	5.9662	C
6	1.9542	1.2897	7.9191	5.0234	C
7	14.5536	9.5391	7.8653	6.4214	Ba
8	6.7336	4.41	7.8591	7.2555	N
9	4.2986	2.8126	7.8515	5.4686	C
10	7.3646	4.8077	7.8337	6.3186	N

Table B.32.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_6$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	32.0533	20.1472	7.5426	7.4256	Ba
2	15.0308	9.7777	7.8061	7.3401	N
3	6.7336	4.41	7.8591	7.2555	N
4	22.5824	13.7778	7.3213	7.1742	Ba
5	12.0649	7.6128	7.5719	7.1615	N
6	17.1442	10.5259	7.3675	7.1208	N
7	11.1071	6.8536	7.4046	7.113	Ba
8	31.111	18.6111	7.1786	7.0744	Ba
9	24.3925	15.0043	7.3814	7.0626	Ba
10	9.6698	5.9515	7.3857	7.042	Ba

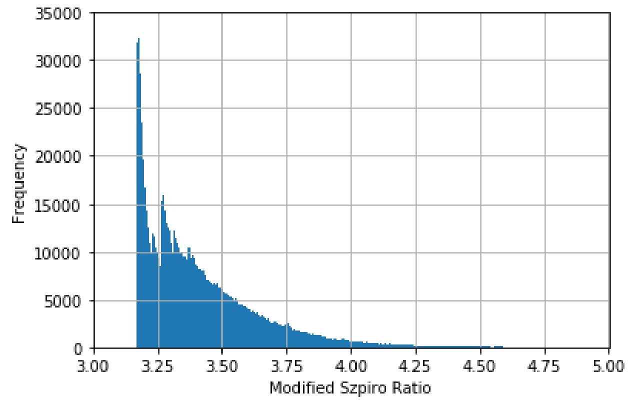
Table B.33.: Best σ_m for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_8$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	16.8025	10.2792	7.3412	6.6577	Ba
2	13.8562	8.3466	7.2284	6.5386	Ba
3	15.086	8.9404	7.1115	5.8465	Ba
4	22.1795	13.1411	7.1098	6.9407	Ba
5	17.6296	10.4426	7.108	5.8551	Ba
6	5.4264	3.2038	7.0851	5.6864	Ba
7	7.045	4.1548	7.0771	6.3162	Ba
8	10.9852	6.4212	7.0144	5.7357	Ba
9	22.9852	13.3984	6.995	6.3868	Ba
10	17.4688	10.1638	6.9819	6.5084	Ba

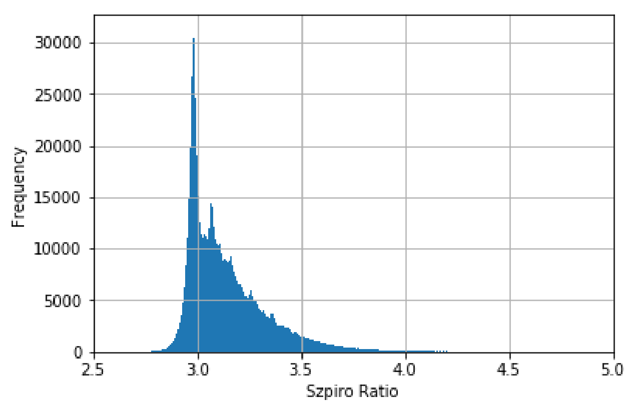
Table B.34.: Best σ for $E(\mathbb{Q})_{\text{tors}} \cong C_2 \times C_8$

Rank	$\log N_E$	$h_{\text{naive}}(E)$	$\sigma_m(E)$	$\sigma(E)$	By
1	22.1795	13.1411	7.1098	6.9407	Ba
2	27.446	15.8296	6.921	6.7363	Ba
3	16.5597	9.5532	6.9227	6.7266	Ba
4	27.0283	15.5744	6.9147	6.7124	Ba
5	22.0659	12.681	6.8963	6.7024	Ba
6	17.1056	9.8012	6.8758	6.6777	Ba
7	66.4215	37.3617	6.7499	6.6662	Ba
8	16.8025	10.2792	7.3412	6.6577	Ba
9	24.4226	13.9132	6.8362	6.6574	Ba
10	16.5906	9.4403	6.8282	6.628	Ba

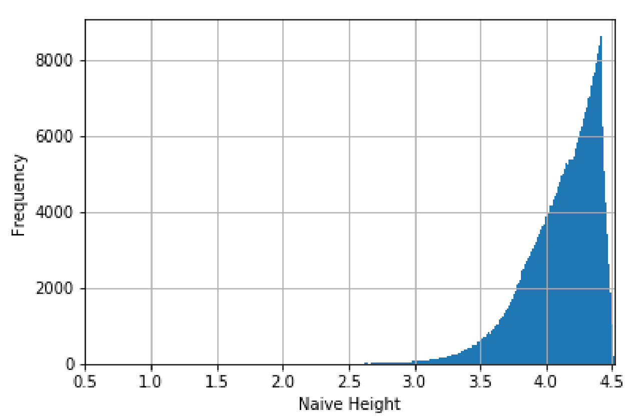
Summary of Data for $\mathcal{F}_{C_2 \times C_4}$



(a) Modified Szpiro Ratio in $\mathcal{F}_{C_2 \times C_4}$



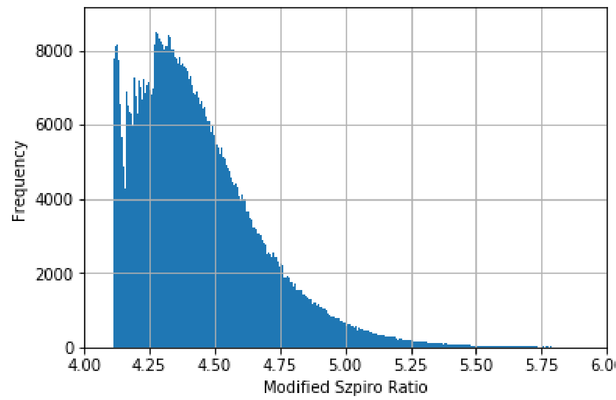
(b) Szpiro Ratio in $\mathcal{F}_{C_2 \times C_4}$



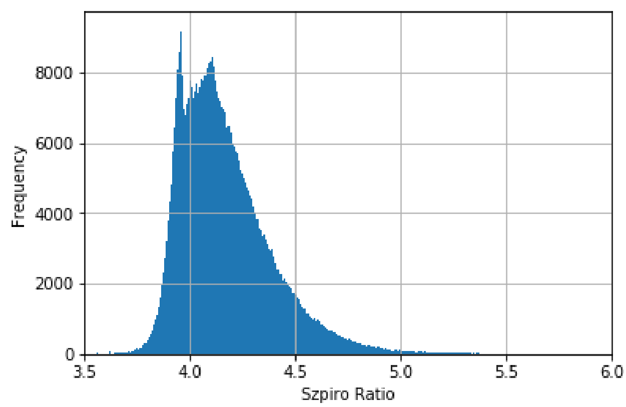
(c) Naive Height in $\mathcal{F}_{C_2 \times C_4}$

Figure B.1.: Histograms for $\mathcal{F}_{C_2 \times C_4}$

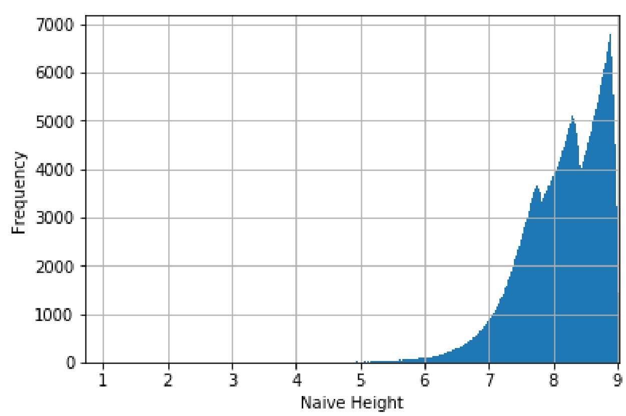
Summary of Data for $\mathcal{F}_{C_2 \times C_6}$



(a) Modified Szpiro Ratio in $\mathcal{F}_{C_2 \times C_6}$



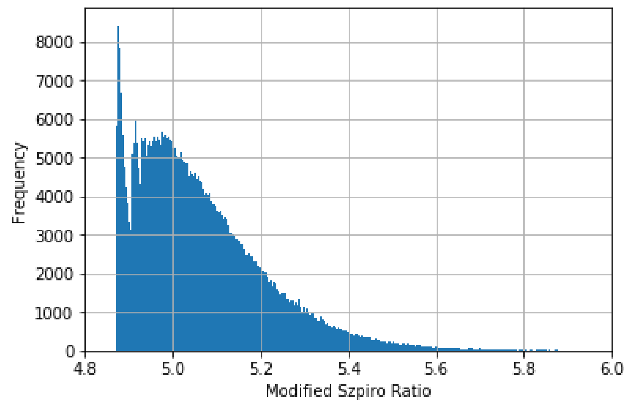
(b) Szpiro Ratio in $\mathcal{F}_{C_2 \times C_6}$



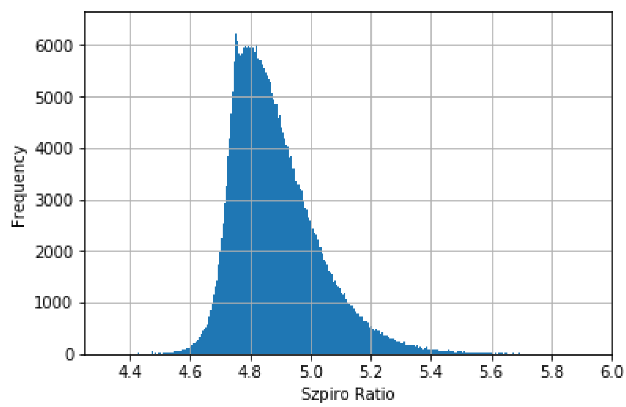
(c) Naive Height in $\mathcal{F}_{C_2 \times C_6}$

Figure B.2.: Histograms for $\mathcal{F}_{C_2 \times C_6}$

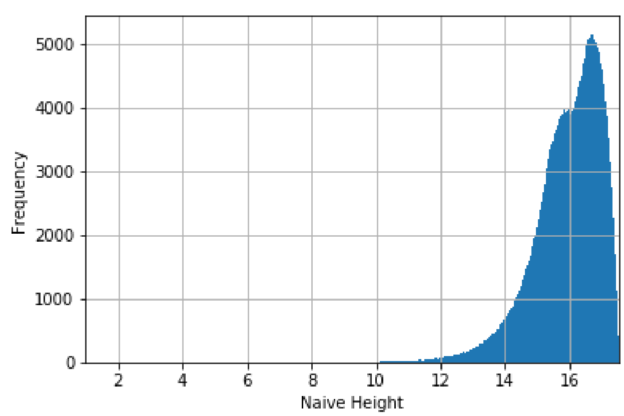
Summary of Data for $\mathcal{F}_{C_2 \times C_8}$



(a) Modified Szpiro Ratio in $\mathcal{F}_{C_2 \times C_8}$



(b) Szpiro Ratio in $\mathcal{F}_{C_2 \times C_8}$



(c) Naive Height in $\mathcal{F}_{C_2 \times C_8}$

Figure B.3.: Histograms for $\mathcal{F}_{C_2 \times C_8}$

C. REVIEW OF MATHEMATICA COMMANDS

To illustrate, $5 \equiv 1 \mod 4$ can be verified via the Mathematica input `Mod[5,4]` which outputs `1`. Now suppose we want to compute via Mathematica the congruence $k^2 \mod 8$ for $1 \leq k \leq 8$. Then the input

```
Table[Mod[k^2,16],{k,1,8}]
```

outputs

```
{1,4,1,0,1,4,1,0}
```

where the j-th entry refers to $j^2 \mod 8$. Indeed, the sixth entry is 4 and which agrees with $6^2 \equiv 4 \mod 8$. From this we see the classic fact that an odd square is congruent to 1 mod 8. This can be checked more efficiently via the input

```
Table[Mod[k^2,16],{k,1,8,2}]
```

which outputs

```
{1,1,1,1}
```

Namely, the j-th entry in this set corresponds to $(2j-1)^2 \mod 8$.

To check the different possibilities of $a^2 + b^2 \mod 4$ for $1 \leq a \leq 4$ and $1 \leq b \leq 3$, we use the input

```
Table[Mod[a^2+b^2,4],{a,1,4},{b,1,3}]
```

which outputs

```
{{2,1,2},{1,0,1},{2,1,2},{1,0,1}}
```

In particular, the set is an output of four sets consisting of three integers. Viewing this output as the matrix

$$A = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$$

we have the interpretation that the $a_{j,k}$ entry of A is interpretted as $j^2 + k^2 \equiv a_{j,k} \mod 4$. Indeed, $a_{2,1} = 1$ which verifies $2^2 + 1^2 \equiv 1 \mod 4$. Lastly, we consider consider $a^2 + b^2 \mod 8$ where $1 \leq a, b \leq 8$ with a even and b odd. Then the input

```
Table[Mod[a^2+b^2,8],{a,2,8,2},{b,1,8,2}]
```

outputs

```
{{5,5,5,5},{1,1,1,1},{5,5,5,5},{1,1,1,1}}
```

As before, let

$$A = \begin{pmatrix} 5 & 5 & 5 & 5 \\ 1 & 1 & 1 & 1 \\ 5 & 5 & 5 & 5 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

and we observe that for $a_{j,k}$ in A we have $(2j)^2 + (2k-1)^2 \equiv a_{j,k} \mod 8$. Indeed, $a_{2,3} = 1$ which corresponds to $4^2 + 5^2 \equiv 1 \mod 8$.

D. E_T AND ITS ASSOCIATED QUANTITIES

Table D.1.: Weierstrass Model of E_T

where $E_T : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$

a_1	a_2	a_3	a_4	T
0	$2a$	0	$a^2 - b^2d$	C_2
0	0	a	0	C_3^0
a	0	a^2b	0	C_3
a	$-ab$	$-a^2b$	0	C_4
$a-b$	$-ab$	$-a^2b$	0	C_5
$a-b$	$-ab-b^2$	$-a^2b-ab^2$	0	C_6
a^2+ab-b^2	$a^2b^2-ab^3$	$a^4b^2-a^3b^3$	0	C_7
$-a^2+4ab-2b^2$	$-a^2b^2+3ab^3-2b^4$	$-a^3b^3+3a^2b^4-2ab^5$	0	C_8
$a^3+ab^2-b^3$	$(a^4b^2-2a^3b^3+$ $2a^2b^4-ab^5)$	$(a^7b^2-2a^6b^3+$ $2a^5b^4-a^4b^5)$	0	C_9

continued on next page

Table D.1.: *continued*

a_1	a_2	a_3	a_4	T
$(a^3-2a^2b-2ab^2+2b^3)$	$-a^3b^3+3a^2b^4-2ab^5$	$(-a^6b^3+6a^5b^4-12a^4b^5+9a^3b^6-2a^2b^7)$	0	C_{10}
$(-a^4+2a^3b+2a^2b^2-8ab^3+6b^4)$	$(a^7b-9a^6b^2+36a^5b^3-83a^4b^4+119a^3b^5-106a^2b^6+54ab^7-12b^8)$	$(-a^{11}b+12a^{10}b^2-66a^9b^3+219a^8b^4-485a^7b^5+748a^6b^6-812a^5b^7+611a^4b^8-304a^3b^9+90a^2b^{10}-12ab^{11})$	0	C_{12}
0	$ad+bd$	0	abd^2	$C_2\times C_2$
a	$-ab-4b^2$	$-a^2b-4ab^2$	0	$C_2\times C_4$
$-19a^2+2ab+b^2$	$(-10a^4+22a^3b-14a^2b^2+2ab^3)$	$(90a^6-198a^5b+116a^4b^2+4a^3b^3-14a^2b^4+2ab^5)$	0	$C_2\times C_6$
$(-a^4-8a^3b-24a^2b^2+64b^4)$	$(-4a^6b^2-56a^5b^3-320a^4b^4-960a^3b^5-1536a^2b^6-1024ab^7)$	$(8a^9b^3+144a^8b^4+1024a^7b^5+3328a^6b^6+2048a^5b^7-21504a^4b^8-77824a^3b^9-114688a^2b^{10}-65536ab^{11})$	0	$C_2\times C_8$

Table D.2.: The Polynomials α_T

α_T	T
$16\,(3b^2d + a^2)$	C_2
$a^3\,(a - 24b)$	C_3
$a^2\,(a^2 + 16ab + 16b^2)$	C_4
$(a^4 + 12a^3b + 14a^2b^2 - 12ab^3 + b^4)$	C_5
$(a + 3b)\,(a^3 + 9a^2b + 3ab^2 + 3b^3)$	C_6
$(a^2 - ab + b^2)\,(a^6 + 5a^5b - 10a^4b^2 - 15a^3b^3 + 30a^2b^4 - 11ab^5 + b^6)$	C_7
$(a^8 - 16a^7b + 96a^6b^2 - 288a^5b^3 + 480a^4b^4 - 448a^3b^5 + 224a^2b^6 - 64ab^7 + 16b^8)$	C_8
$(a^3 - 3ab^2 + b^3)\,(a^9 - 9a^7b^2 + 27a^6b^3 - 45a^5b^4 + 54a^4b^5 - 48a^3b^6 + 27a^2b^7 - 9ab^8 + b^9)$	C_9
$(a^{12} - 8a^{11}b + 16a^{10}b^2 + 40a^9b^3 - 240a^8b^4 + 432a^7b^5 - 256a^6b^6 - 288a^5b^7 + 720a^4b^8 - 720a^3b^9 + 416a^2b^{10} - 128ab^{11} + 16b^{12})$	C_{10}
$(a^4 - 6a^3b + 12a^2b^2 - 12ab^3 + 6b^4)\,(a^{12} - 18a^{11}b + 144a^{10}b^2 - 684a^9b^3 + 2154a^8b^4 - 4728a^7b^5 + 7368a^6b^6 - 8112a^5b^7 + 6132a^4b^8 - 3000a^3b^9 + 864a^2b^{10} - 144ab^{11} + 24b^{12})$	C_{12}
$16d^2\,(a^2 - ab + b^2)$	$C_2 \times C_2$
$a^4 + 16a^3b + 80a^2b^2 + 128ab^3 + 256b^4$	$C_2 \times C_4$
$(21a^2 - 6ab + b^2)\,(6861a^6 - 2178a^5b - 825a^4b^2 + 180a^3b^3 + 75a^2b^4 - 18ab^5 + b^6)$	$C_2 \times C_6$

continued on next page

Table D.2.: *continued*

α_T	T
$(a^{16} + 32a^{15}b + 448a^{14}b^2 + 3584a^{13}b^3 + 17664a^{12}b^4 + 51200a^{11}b^5 + 51200a^{10}b^6 - 237568a^9b^7 - 1183744a^8b^8 - 1900544a^7b^9 + 3276800a^6b^{10} + 26214400a^5b^{11} + 72351744a^4b^{12} + 117440512a^3b^{13} + 117440512a^2b^{14} + 67108864ab^{15} + 16777216b^{16})$	$C_2 \times C_8$

Table D.3.: The Polynomials β_T

β_T	T
$-64a\,(9b^2d - a^2)$	C_2
$a^4\,(-a^2 + 36ab - 216b^2)$	C_3
$a^3\,(a + 8b)\,(-a^2 - 16ab + 8b^2)$	C_4
$-\,(a^2 + b^2)\,(a^4 + 18a^3b + 74a^2b^2 - 18ab^3 + b^4)$	C_5
$-\,(a^2 + 6ab - 3b^2)\,(a^4 + 12a^3b + 30a^2b^2 + 36ab^3 + 9b^4)$	C_6
$-(a^{12} + 6a^{11}b - 15a^{10}b^2 - 46a^9b^3 + 174a^8b^4 - 222a^7b^5 + 273a^6b^6 - 486a^5b^7 + 570a^4b^8 - 354a^3b^9 + 117a^2b^{10} - 18ab^{11} + b^{12})$	C_7
$-\,(a^4 - 8a^3b + 16a^2b^2 - 16ab^3 + 8b^4)\,(a^8 - 16a^7b + 96a^6b^2 - 288a^5b^3 + 456a^4b^4 - 352a^3b^5 + 80a^2b^6 + 32ab^7 - 8b^8)$	C_8

continued on next page

Table D.3.: *continued*

β_T	T
$-(a^{18} - 18a^{16}b^2 + 42a^{15}b^3 + 27a^{14}b^4 - 306a^{13}b^5 + 735a^{12}b^6 - 1080a^{11}b^7 + 1359a^{10}b^8 - 2032a^9b^9 + 3240a^8b^{10} - 4230a^7b^{11} + 4128a^6b^{12} - 2970a^5b^{13}1359a^{10}b^8 - 570a^3b^{15} + 135a^2b^{16} - 18ab^{17} + b^{18})$	C_9
$-(a^2 - 2ab + 2b^2)(a^4 - 2a^3b + 2b^4)(a^4 - 2a^3b - 6a^2b^2 + 12ab^3 - 4b^4)(a^8 - 6a^7b + 4a^6b^2 + 48a^5b^3 - 146a^4b^4 + 176a^3b^5 - 104a^2b^6 + 32ab^7 - 4b^8)$	C_{10}
$-(a^8 - 12a^7b + 60a^6b^2 - 168a^5b^3 + 288a^4b^4 - 312a^3b^5 + 216a^2b^6 - 96ab^7 + 24b^8)(a^{16} - 24a^{15}b + 264a^{14}b^2 + 8208a^{12}b^4 - 27696a^{11}b^5 + 70632a^{10}b^6 - 138720a^9b^7 + 211296a^8b^8 - 248688a^7b^9 + 222552a^6b^{10} - 146304a^5b^{11} + 65880a^4b^{12} - 17136a^3b^{13} + 1008a^2b^{14} + 576ab^{15} - 72b^{16})$	C_{12}
$-32d^3(a+b)(a-2b)(2a-b)$	$C_2 \times C_2$
$-(a^2 + 8ab - 16b^2)(a^2 + 8ab + 8b^2)(a^2 + 8ab + 32b^2)$	$C_2 \times C_4$
$-(183a^4 - 36a^3b - 30a^2b^2 + 12ab^3 - b^4)(393a^4 - 156a^3b + 30a^2b^2 - 12ab^3 + b^4)(759a^4 - 228a^3b - 30a^2b^2 + 12ab^3 - b^4$	$C_2 \times C_6$
$-(a^8 + 16a^7b + 96a^6b^2 + 256a^5b^3 - 256a^4b^4 - 4096a^3b^5 - 12288a^2b^6 - 16384ab^7 - 8192b^8)(a^8 + 16a^7b + 96a^6b^2 + 256a^5b^3 + 128a^4b^4 - 1024a^3b^5 - 3072a^2b^6 - 4096ab^7 - 2048b^8)(a^8 + 16a^7b + 96a^6b^2 + 256a^5b^3 + 512a^4b^4 + 2048a^3b^5 + 6144a^2b^6 + 8192ab^7 + 4096b^8)$	$C_2 \times C_8$

Table D.4.: The Polynomials γ_T

γ_T	T
$64b^2d\,(b^2d-a^2)^2$	C_2
$a^8b^3\,(a-27b)$	C_3
$a^7b^4\,(a+16b)$	C_4
$(ab)^5\,(-a^2-11ab+b^2)$	C_5
$a^2b^6\,(a+9b)\,(a+b)^3$	C_6
$(ab)^7\,(-a+b)^7\,(a^3+5a^2b-8ab^2+b^3)$	C_7
$a^2b^8\,(a-2b)^4\,(a-b)^8\,(a^2-8ab+8b^2)$	C_8
$(ab)^9\,(-a+b)^9\,(a^2-ab+b^2)^3\,(a^3+3a^2b-6ab^2+b^3)$	C_9
$a^5b^{10}\,(a-2b)^5\,(a-b)^{10}\,(a^2+2ab-4b^2)\,(a^2-3ab+b^2)^2$	C_{10}
$a^2b^{12}\,(a-2b)^6\,(a-b)^{12}\,(a^2-6ab+6b^2)\,(a^2-2ab+2b^2)^3\,(a^2-3ab+3b^2)^4$	C_{12}
$16a^2b^2d^6\,(a-b)^2$	$C_2 \times C_2$
$a^2b^4\,(a+8b)^2\,(a+4b)^4$	$C_2 \times C_4$
$(2a)^6\,(-9a+b)^2\,(-3a+b)^2\,(3a+b)^2\,(-5a+b)^6\,(-a+b)^6$	$C_2 \times C_6$
$(2ab)^8\,(a+2b)^8\,(a+4b)^8\,(a^2-8b^2)^2\,(a^2+8ab+8b^2)^2\,(a^2+4ab+8b^2)^4$	$C_2 \times C_8$

Table D.5.: The Polynomials $\mu_T^{(1)}$

$\mu_T^{(1)}$	T
$48b^2dr - 4a^2r + 108as$	C_2
$a^2r - 12abr - 72b^2r + 15552a^2s - 124416abs$	C_3
$-a^3r - 22a^2br - 88ab^2r + 144b^3r + 51968a^3s + 413696a^2bs - 212992ab^2s$	C_4
$-3121a^5r - 56475a^4br - 239450a^3b^2r - 22800a^2b^3r - 236305ab^4r + 33663b^5r + 33663a^5s + 236305a^4bs - 22800a^3b^2s + 239450a^2b^3s - 56475ab^4s + 3121b^5s$	C_5
$-10a^5r - 177a^4br - 936a^3b^2r - 1494a^2b^3r - 702ab^4r + 1215b^5r + 1670139a^5s + 15348366a^4bs + 31389282a^3b^2s + 27054648a^2b^3s - 9760581ab^4s - 5183190b^5s$	C_6
$-86718a^{11}r - 538213a^{10}br + 1184537a^9b^2r + 4196345a^8b^3r - 14193432a^7b^4r + 16599205a^6b^5r - 20778709a^5b^6r + 38254845a^4b^7r - 42322212a^3b^8r + 23351603a^2b^9r - 6305919ab^{10}r + 575487b^{11}r - 63181a^{11}s - 693257a^{10}bs + 204867a^9b^2s + 6273544a^8b^3s - 12066603a^7b^4s + 10691961a^6b^5s - 18844497a^5b^6s + 31181840a^4b^7s - 23670877a^3b^8s + 8967083a^2b^9s - 1492111ab^{10}s + 86718b^{11}s$	C_7
$-73848a^{11}r + 1685380a^{10}br - 15738648a^9b^2r + 79535073a^8b^3r - 243082192a^7b^4r + 472307520a^6b^5r - 593480800a^5b^6r + 470894488a^4b^7r - 205849824a^3b^8r + 17561360a^2b^9r + 20674464ab^{10}r - 4013912b^{11}r + 7939456a^{10}s - 129476608a^9bs + 852553728a^8b^2s - 3040530432a^7b^3s + 6517843968a^6b^4s - 8762834944a^5b^5s + 7329972224a^4b^6s - 3378085888a^3b^7s + 343171072a^2b^8s + 334233600ab^9s - 66846720b^{10}s$	C_8

continued on next page

Table D.5.: *continued*

$\mu_T^{(1)}$	T
$-1226439a^{17}r - 244494a^{16}br + 22022128a^{15}b^2r - 47126079a^{14}b^3r - 42424647a^{13}b^4r + 366718037a^{12}b^5r - 828596070a^{11}b^6r + 1160606676a^{10}b^7r - 1437637049a^9b^8r + 2208303306a^8b^9r - 3536970804a^7b^{10}r + 4488727213a^6b^{11}r - 4177124136a^5b^{12}r + 2820215667a^4b^{13}r - 1355696806a^3b^{14}r + 433546551a^2b^{15}r - 80947617ab^{16}r + 6344929b^{17}r - 1509634a^{17}s - 1969182a^{16}bs + 25088703a^{15}b^2s - 32212634a^{14}b^3s - 83911401a^{13}b^4s + 367882251a^{12}b^5s - 671480020a^{11}b^6s + 822495528a^{10}b^7s - 1065165066a^9b^8s + 1797411572a^8b^9s - 2734457013a^7b^{10}s + 3077148984a^6b^{11}s - 2487390935a^5b^{12}s + 1445707773a^4b^{13}s - 580111959a^3b^{14}s + 148685480a^2b^{15}s - 21093957ab^{16}s + 1226439b^{17}s$	C_9
$-6523389056a^{17}r + 63087926272a^{16}br - 165987178496a^{15}b^2r - 361329740800a^{14}b^3r + 3070640097280a^{13}b^4r - 6455127277568a^{12}b^5r + 451386679296a^{11}b^6r + 25113889800192a^{10}b^7r - 59895333888000a^9b^8r + 78301390315520a^8b^9r - 75429907677184a^7b^{10}r + 70609949360128a^6b^{11}r - 68357168144384a^5b^{12}r + 54456447795200a^4b^{13}r - 29922586787840a^3b^{14}r + 10435287187456a^2b^{15}r - 2082858074112ab^{16}r + 180193591296b^{17}r - 397080a^{17}s + 4270002a^{16}bs - 13736234a^{15}b^2s - 15544820a^{14}b^3s + 218902960a^{13}b^4s - 556182675a^{12}b^5s + 249618296a^{11}b^6s + 1779966128a^{10}b^7s - 4995435080a^9b^8s + 7030769520a^8b^9s - 6911468520a^7b^{10}s + 6352978528a^6b^{11}s - 6234485776a^5b^{12}s + 5216995960a^4b^{13}s - 3016234040a^3b^{14}s + 1099023280a^2b^{15}s - 227714752ab^{16}s + 20338184b^{17}s$	C_{10}

continued on next page

Table D.5.: *continued*

$\mu_T^{(1)}$	T
$-16368060a^{23}r + 568385154a^{22}br - 9292716576a^{21}b^2r + 95397960970a^{20}b^3r - 691561164324a^{19}b^4r + 3772371497316a^{18}b^5r - 16102752845712a^{17}b^6r + 55195394708001a^{16}b^7r - 154610209756152a^{15}b^8r + 358140590212680a^{14}b^9r - 691273485740880a^{13}b^{10}r + 1116410011234272a^{12}b^{11}r - 1510188566936400a^{11}b^{12}r + 1707700080266136a^{10}b^{13}r - 1605685037888160a^9b^{14}r + 1243597792375008a^8b^{15}r - 781293500284464a^7b^{16}r + 388281466111320a^6b^{17}r - 145974139946496a^5b^{18}r + 37767414705048a^4b^{19}r - 4955293945584a^3b^{20}r - 403876566288a^2b^{21}r + 248899583808ab^{22}r - 22193079192b^{23}r + 969115570560a^{22}s - 29786348215296a^{21}bs + 431949361665024a^{20}b^2s - 3940658270263296a^{19}b^3s + 25421425703700480a^{18}b^4s - 123488879453485056a^{17}b^5s + 469378490732181504a^{16}b^6s - 1431289906739159040a^{15}b^7s + 3559957206093600768a^{14}b^8s - 7300614514238742528a^{13}b^9s + 12423346938386251776a^{12}b^{10}s - 17589066612647067648a^{11}b^{11}s + 20703296540531515392a^{10}b^{12}s - 20171476151052189696a^9b^{13}s + 16128249993599827968a^8b^{14}s - 10429451637581611008a^7b^{15}s + 5323789523146530816a^6b^{16}s - 2054130396901539840a^5b^{17}s + 546612033833533440a^4b^{18}s - 75080393883648000a^3b^{19}s - 5221551522447360a^2b^{20}s + 3637025974517760ab^{21}s - 330638724956160b^{22}s$	C_{12}
$-8a^2rd^2 + 8abrd^2 + 22b^2rd^2 + 22a^2sd^2 + 8absd^2 - 8b^2sd^2$	$C_2 \times C_2$
$-a^4r - 16a^3br - 80a^2b^2r - 128ab^3r + 704b^4r + 3325952a^4s + 26476544a^3bs + 92274688a^2b^2s - 109051904ab^3s - 218103808b^4s$	$C_2 \times C_4$

continued on next page

Table D.5.: *continued*

$\mu_T^{(1)}$	T
$1067140860516356259150a^{11}r - 7855741476134969920515a^{10}br + 1112066596613535372 0a^9b^2r + 1393922940386917949 19a^8b^3r - 540263313122077393 56a^7b^4r + 120256452301199224 50a^6b^5r - 181009134664662650 4a^5b^6r - 2546027300012804 82a^4b^7r + 2076856849993946 22a^3b^8r - 40223459978629695a^2b^9r + 3369402100004256ab^{10}r - 986943723233349b^{11}r + 209691261a^{10}s - 49111434a^9bs - 28026945a^8b^2s + 13520952a^7b^3s - 2963502a^6b^4s + 670356a^5b^5s + 14670a^4b^6s - 52776a^3b^7s + 11649a^2b^8s - 1050ab^9s + 35b^{10}s$	$C_2 \times C_6$

continued on next page

Table D.5.: *continued*

$\mu_T^{(1)}$	T
$-13209a^{22}r - 581196a^{21}br - 11576762a^{20}b^2r - 137600720a^{19}b^3r - 1077037264a^{18}b^4r - 5710255296a^{17}b^5r - 19612356744a^{16}b^6r - 32139665664a^{15}b^7r + 67579970048a^{14}b^8r + 654116311040a^{13}b^9r + 2539506890752a^{12}b^{10}r + 7576036622336a^{11}b^{11}r + 20926819385344a^{10}b^{12}r + 49766416842752a^9b^{13}r + 71499449008128a^8b^{14}r - 49546029170688a^7b^{15}r - 594695737573376a^6b^{16}r - 1737832804646912a^5b^{17}r - 3062535049707520a^4b^{18}r - 3577238700163072a^3b^{19}r - 2727157029666816a^2b^{20}r - 1234538286022656ab^{21}r - 251783498694656b^{22}r - 4224226142835961757696a^{22}s - 165696923878975044845568a^{21}bs - 2928262563368869124112384a^{20}b^2s - 30728246454371888213786624a^{19}b^3s - 210455806101560524244254720a^{18}b^4s - 955383687919928815025913856a^{17}b^5s - 2615499513803006279998767104a^{16}b^6s - 1743245925865610951226556416a^{15}b^7s + 20125305744387565039248211968a^{14}b^8s + 112064008174291341614038122496a^{13}b^9s + 376984063943539642166721642496a^{12}b^{10}s + 1091821942697524503459231956992a^{11}b^{11}s + 2927852105445251608192013565952a^{10}b^{12}s + 6033158092096936875735195320320a^9b^{13}s + 4986521647937652009843159990272a^8b^{14}s - 18971909987788747557810909216768a^7b^{15}s - 92616736137948046779718066765824a^6b^{16}s - 215727345747674278873189085872128a^5b^{17}s - 325514539284174435175029450735616a^4b^{18}s - 332698126411126193945151212093440a^3b^{19}s - 223927143829335898781277111713792a^2b^{20}s - 89935724884063234281283925311488ab^{21}s - 16351949978920588051142531874816b^{22}s$	$C_2 \times C_8$

Table D.6.: The Polynomials $\mu_T^{(2)}$

$\mu_T^{(2)}$	T
$20b^4d^2r + 36b^4d^2s - 4a^2b^2dr - 84a^2b^2ds + 64a^4s$	C_2
$a^5b^3r - 3a^4b^4r - 72a^3b^5r - 1728a^2b^6r - 41472ab^7r - 995328b^8r + 23887872a^8s + 573308928a^7bs + 13759414272a^6b^2s + 2972033482752a^5b^3s$	C_3
$4096a^{10}s - 65536a^9bs + 983040a^8b^2s - 14680064a^7b^3s + 3271557120a^6b^4s + 14a^5b^4r + 209a^4b^5r - 224a^3b^6r + 240a^2b^7r - 256ab^8r + 256b^9r$	C_4
$1461113a^6b^5r + 16210516a^5b^6r + 72975a^4b^7r + 6900a^3b^8r + 650a^2b^9r + 60ab^{10}r + 5b^{11}r + 5a^{11}s - 60a^{10}bs + 650a^9b^2s - 6900a^8b^3s + 72975a^7b^4s - 16210516a^6b^5s + 1461113a^5b^6s$	C_5
$-14a^5b^6r - 180a^4b^7r - 555a^3b^8r - 644a^2b^9r - 192ab^{10}r + 144b^{11}r + 1296a^{11}s - 15552a^{10}bs + 147744a^9b^2s - 1321920a^8b^3s + 11605680a^7b^4s - 101243520a^6b^5s + 37105834644a^5b^6s + 112064430042a^4b^7s + 112339252836a^3b^8s + 37494993069a^2b^9s$	C_6

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$1651723461a^{16}b^{7}r - 3053281690a^{15}b^{8}r - 36782602949a^{14}b^{9}r + 204185576679a^{13}b^{10}r - 489777156547a^{12}b^{11}r + 679075714135a^{11}b^{12}r - 582586779859a^{10}b^{13}r + 306736145405a^{9}b^{14}r - 91184305523a^{8}b^{15}r + 11718436003a^{7}b^{16}r + 14216370a^{6}b^{17}r + 1993320a^{5}b^{18}r + 277585a^{4}b^{19}r + 38024a^{3}b^{20}r + 4998a^{2}b^{21}r + 588ab^{22}r + 49b^{23}r + 49a^{23}s - 196a^{22}bs + 1470a^{21}b^{2}s - 8624a^{20}b^{3}s + 53361a^{19}b^{4}s - 324576a^{18}b^{5}s + 1980874a^{17}b^{6}s + 1785698469a^{16}b^{7}s - 669951077a^{15}b^{8}s - 47015940877a^{14}b^{9}s + 197639682387a^{13}b^{10}s - 386355913895a^{12}b^{11}s + 434312001991a^{11}b^{12}s - 293599696103a^{10}b^{13}s + 115624987021a^{9}b^{14}s - 23374293686a^{8}b^{15}s + 1651723461a^{7}b^{16}s$	C_7
$-357458640a^{15}b^{8}r + 8158710360a^{14}b^{9}r - 80486629680a^{13}b^{10}r + 462999914325a^{12}b^{11}r - 1751207521180a^{11}b^{12}r + 4629708846410a^{10}b^{13}r - 8841897565516a^{9}b^{14}r + 12392459288439a^{8}b^{15}r - 12779259296936a^{7}b^{16}r + 9595977477844a^{6}b^{17}r - 5108730463880a^{5}b^{18}r + 1828677484739a^{4}b^{19}r - 394956635884a^{3}b^{20}r + 38913849610a^{2}b^{21}r + 4ab^{22}r + b^{23}r + 16a^{22}s + 256a^{21}bs + 2560a^{20}b^{2}s + 20992a^{19}b^{3}s + 156160a^{18}b^{4}s + 1104896a^{17}b^{5}s + 7614976a^{16}b^{6}s + 51758080a^{15}b^{7}s + 253102534400a^{14}b^{8}s - 4072815337472a^{13}b^{9}s + 29609435103232a^{12}b^{10}s - 128858517192704a^{11}b^{11}s + 374187054964736a^{10}b^{12}s - 764274088935424a^{9}b^{13}s + 1126470388744192a^{8}b^{14}s - 1207848547123200a^{7}b^{15}s + 935574791454720a^{6}b^{16}s - 510806411182080a^{5}b^{17}s + 186695700971520a^{4}b^{18}s - 41033505177600a^{3}b^{19}s + 4103350517760a^{2}b^{20}s$	C_8

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$135940809738a^{26}b^{9}r - 1197869037753a^{25}b^{10}r + 3444842282078a^{24}b^{11}r + 4319052282096a^{23}b^{12}r -$ $70147771315344a^{22}b^{13}r + 293881449824863a^{21}b^{14}r - 778251598529082a^{20}b^{15}r + 1507584524451618a^{19}b^{16}r -$ $2259713081490952a^{18}b^{17}r + 2690669861053062a^{17}b^{18}r - 2574037510631457a^{16}b^{19}r +$ $1980590869755400a^{15}b^{20}r - 1215922719878304a^{14}b^{21}r + 584638476988131a^{13}b^{22}r - 212901000346933a^{12}b^{23}r +$ $55337356929966a^{11}b^{24}r - 9153972031890a^{10}b^{25}r + 722876226613a^{9}b^{26}r + 221626935a^{8}b^{27}r +$ $41538420a^{7}b^{28}r + 7747650a^{6}b^{29}r + 1431756a^{5}b^{30}r + 259767a^{4}b^{31}r + 45360a^{3}b^{32}r + 7290a^{2}b^{33}r +$ $972ab^{34}r + 81b^{35}r + 81a^{35}s + 972a^{33}b^{2}s - 2268a^{32}b^{3}s + 13122a^{31}b^{4}s - 51516a^{30}b^{5}s +$ $229230a^{29}b^{6}s - 976860a^{28}b^{7}s + 4221639a^{27}b^{8}s + 167381260189a^{26}b^{9}s - 1300117919226a^{25}b^{10}s +$ $2915104871124a^{24}b^{11}s + 8130665525060a^{23}b^{12}s - 77449748892573a^{22}b^{13}s + 282997179822048a^{21}b^{14}s -$ $678447127755680a^{20}b^{15}s + 1202177287983873a^{19}b^{16}s - 1652749612061232a^{18}b^{17}s + 1803034382276282a^{17}b^{18}s -$ $1574131566464940a^{16}b^{19}s + 1097930005064271a^{15}b^{20}s - 604854624173645a^{14}b^{21}s + 257183219777592a^{13}b^{22}s -$ $81080661044868a^{12}b^{23}s + 17678879503103a^{11}b^{24}s - 2336592015435a^{10}b^{25}s + 135940809738a^{9}b^{26}s$	C_9

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$80a^{35}r + 640a^{34}br + 3840a^{33}b^2r + 17280a^{32}b^3r + 70400a^{31}b^4r + 252160a^{30}b^5r + 865280a^{29}b^6r + 2746880a^{28}b^7r + 8584960a^{27}b^8r + 25350400a^{26}b^9r - 2563220086223360a^{25}b^{10}r + 54979529333143552a^{24}b^{11}r - 526149425435931904a^{23}b^{12}r + 2886354545496600576a^{22}b^{13}r - 9317700507739463680a^{21}b^{14}r + 12524062806426669056a^{20}b^{15}r + 37526459513442967552a^{19}b^{16}r - 276924418747316404224a^{18}b^{17}r + 904141487155400359936a^{17}b^{18}r - 2007153798077220782080a^{16}b^{19}r + 3332232900147818070016a^{15}b^{20}r - 4289724827745625047040a^{14}b^{21}r + 4347007463178515251200a^{13}b^{22}r - 3480826810741329756160a^{12}b^{23}r + 2192991654130713886720a^{11}b^{24}r - 1073935756083393986560a^{10}b^{25}r + 400010603983479504896a^9b^{26}r - 109330524929536294912a^8b^{27}r + 20635259529401991168a^7b^{28}r - 2397561310842716160a^6b^{29}r + 128886268460269568a^5b^{30}r - 1937958058a^{25}b^{10}s + 44106528930a^{24}b^{11}s - 449145105934a^{23}b^{12}s + 2640364756878a^{22}b^{13}s - 9340127711501a^{21}b^{14}s + 15868363193038a^{20}b^{15}s + 23880468530480a^{19}b^{16}s - 252189535314019a^{18}b^{17}s + 905292287648353a^{17}b^{18}s - 2139595441384566a^{16}b^{19}s + 3738627331975331a^{15}b^{20}s - 5034910005668975a^{14}b^{21}s + 5315826222776635a^{13}b^{22}s - 4420936311943345a^{12}b^{23}s + 2885113801233555a^{11}b^{24}s - 1460022911673739a^{10}b^{25}s + 560710964362165a^9b^{26}s - 157675900137377a^8b^{27}s + 30554780273479a^7b^{28}s - 3637289208623a^6b^{29}s + 199914824158a^5b^{30}s + 2275a^4b^{31}s + 705a^3b^{32}s + 190a^2b^{33}s + 40ab^{34}s + 5b^{35}s$	C_{10}

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$-49718144749484a^{35}b^{12}r+232323272762586a^{34}b^{13}r-5253044943025512a^{33}b^{14}r+76626192763896468a^{32}b^{15}r-810976464047842164a^{31}b^{16}r+6639085466284932633a^{30}b^{17}r-43762438506515101516a^{29}b^{18}r+238695067779834414912a^{28}b^{19}r-1098595757448248655870a^{27}b^{20}r+4329139817203307331233a^{26}b^{21}r-14768392172533907022336a^{25}b^{22}r+43986951267804663608451a^{24}b^{23}r-115138632200530400748294a^{23}b^{24}r+266197601531211986912067a^{22}b^{25}r-545635956895028247508128a^{21}b^{26}r+994211332301352513076269a^{20}b^{27}r-1613158401983939932878534a^{19}b^{28}r+2332710506855274908328180a^{18}b^{29}r-3006256651053801903331064a^{17}b^{30}r+3449862065404583082697137a^{16}b^{31}r-3519129440477374261342020a^{15}b^{32}r+3182440893651242926347585a^{14}b^{33}r-2541819871432653481975260a^{13}b^{34}r+1784065389804294788426676a^{12}b^{35}r-1093245840399015710680454a^{11}b^{36}r+579948252449981036552259a^{10}b^{37}r-263421158563387896634296a^{9}b^{38}r+100977116501666342967055a^{8}b^{39}r-32037412819049278147602a^{7}b^{40}r+8187983788098497233011a^{6}b^{41}r-1619818427808312190440a^{5}b^{42}r+232739976265175255439a^{4}b^{43}r-21606150474937395198a^{3}b^{44}r+972645292454212926a^{2}b^{45}r+72ab^{46}r+9b^{47}r+1296a^{46}s+31104a^{45}bs+404352a^{44}b^{2}s+3794688a^{43}b^{3}s+28926720a^{42}b^{4}s+191165184a^{41}b^{5}s+1141641216a^{40}b^{6}s+6340239360a^{39}b^{7}s+33426908928a^{38}b^{8}s+169846377984a^{37}b^{9}s+840955924224a^{36}b^{10}s+4089770901504a^{35}b^{11}s+$	C_{12}

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$3418213735184992128 0a^{34}b^{12}s - 14134395338321665674 24a^{33}b^{13}s + 28464543958050971020800a^{32}b^{14}s -$	
$3718218649305514796789 76a^{31}b^{15}s + 354004206333026730784128 0a^{30}b^{16}s -$	
$2617024222233152556071731 2a^{29}b^{17}s + 1562713241347168292519976 96a^{28}b^{18}s -$	
$77416498369243570191151104 0a^{27}b^{19}s + 3243053051767478191464972288a^{26}b^{20}s -$	
$11650794867793457881658007552a^{25}b^{21}s + 36278354590060146057865469952a^{24}b^{22}s -$	
$98705273805123939297653391360a^{23}b^{23}s + 236104644886102925025811292160a^{22}b^{24}s -$	
$498818510124601337767823376384a^{21}b^{25}s + 933906611382150544483520839680a^{20}b^{26}s -$	
$1552955430323882715756646367232a^{19}b^{27}s + 2296424646224773452794836942848a^{18}b^{28}s -$	
$3020814689098839654019052077056a^{17}b^{29}s + 3532824024687139570047929548800a^{16}b^{30}s -$	
$3667672791881656351666146902016a^{15}b^{31}s + 3371663350681204956256505364480a^{14}b^{32}s -$	
$2734751659907662343591183253504a^{13}b^{33}s + 1947558048184436275999397117952a^{12}b^{34}s -$	
$1209954150911156533289086353408a^{11}b^{35}s + 650304906814703435748637409280a^{10}b^{36}s -$	
$299085017209056132788096335872a^{9}b^{37}s + 116025052981461016220679536640a^{8}b^{38}s -$	
$37236114047895929905238507520a^{7}b^{39}s + 9622241072881021483814486016a^{6}b^{40}s -$	
$1923932760132995187933708288a^{5}b^{41}s + 279296629359036081968775168a^{4}b^{42}s -$	
$26188016321639618162196480a^{3}b^{43}s + 1190364378256346280099840a^{2}b^{44}s$	

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$-a^2b^2rd^4 + ab^3rd^4 + b^4rd^4 + a^4sd^4 + a^3bsd^4 - a^2b^2sd^4$	$C_2 \times C_2$
$65536a^{10}s - 1048576a^9bs + 11534336a^8b^2s - 109051904a^7b^3s + 49777999872a^6b^4s + 826244333568a^5b^5s + 5010079350784a^4b^6s + 13400297963520a^3b^7s + 13400297963520a^2b^8s - a^4b^4r - 16a^3b^5r - 80a^2b^6r - 128ab^7r + 256b^8r$	$C_2 \times C_4$

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$1159487207440931318587186950000000a^{23}r - 8447490799074846955863340497000000a^{22}br +$	$C_2 \times C_6$
$26892338858158823522672033894400000a^{21}b^2r - 48801352126301672047814422958400000a^{20}b^3r +$	
$54909961081503776257405980640320000a^{19}b^4r - 38377900570008945395516797085472000a^{18}b^5r +$	
$14684480406193246211222514490890240a^{17}b^6r - 602945496113482431033900709575168a^{16}b^7r -$	
$2415740388326299448657596156444416a^{15}b^8r + 1250195086306264625681978184165504a^{14}b^9r -$	
$254009176402672471049497862074368a^{13}b^{10}r - 13083105087436681320966340867584a^{12}b^{11}r +$	
$21048861437882954247444412193280a^{11}b^{12}r - 5777001839116907514835780425984a^{10}b^{13}r +$	
$858992325710048558720447993856a^{9}b^{14}r - 75424819625032918583275605504a^{8}b^{15}r +$	
$3670771113284685051390164352a^{7}b^{16}r - 76165362610162885325210688a^{6}b^{17}r +$	
$1548198221776504750080a^{5}b^{18}r + 149091454557867737088a^{4}b^{19}r + 13337691771434434560a^{3}b^{20}r +$	
$1060175499780685824a^{2}b^{21}r + 68398419340689408ab^{22}r + 2849934139195392b^{23}r + 2077898720832a^{22}s -$	
$13915584294912a^{21}bs + 40444178248704a^{20}b^{2}s - 65148459648000a^{19}b^{3}s + 62258221814528a^{18}b^{4}s -$	
$33628348661760a^{17}b^{5}s + 6640256596992a^{16}b^{6}s + 3327522388992a^{15}b^{7}s - 2665599371904a^{14}b^{8}s +$	
$696379846656a^{13}b^{9}s - 11237499904a^{12}b^{10}s - 43105029120a^{11}b^{11}s + 13228720896a^{10}b^{12}s - 2037547008a^{9}b^{13}s +$	
$180900864a^{8}b^{14}s - 8825856a^{7}b^{15}s + 183872a^{6}b^{16}s$	

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$-5468332800a^{38}b^{8}r - 415593292800a^{37}b^{9}r - 15030479470080a^{36}b^{10}r - 344100833832960a^{35}b^{11}r - 5592686650920960a^{34}b^{12}r - 68551099577057280a^{33}b^{13}r - 656343498163491840a^{32}b^{14}r - 5008067352183767040a^{31}b^{15}r - 30704354570055680000a^{30}b^{16}r - 150511255454179000320a^{29}b^{17}r - 573881950573021429760a^{28}b^{18}r - 1555929403601156833280a^{27}b^{19}r - 1888132798986019405824a^{26}b^{20}r + 7717110566856438054912a^{25}b^{21}r + 61095914222890459332608a^{24}b^{22}r + 233022209870668794691584a^{23}b^{23}r + 587657523485329298817024a^{22}b^{24}r + 892459771859284885766144a^{21}b^{25}r - 674948483590980653547 52a^{20}b^{26}r - 5328738987803352399609856a^{19}b^{27}r - 19595879758491599859875840a^{18}b^{28}r - 46496786977289389819822080a^{17}b^{29}r - 83442754583810282828595200a^{16}b^{30}r - 118338659068201711790194688a^{15}b^{31}r - 134092511287375736042684416a^{14}b^{32}r - 120744678224713067758878720a^{13}b^{33}r - 84814185809480583699496960a^{12}b^{34}r - 44907905473431710245847040a^{11}b^{35}r - 16881975148941598611472384a^{10}b^{36}r - 4018724156477866734780416a^{9}b^{37}r - 455465682313752933826560a^{8}b^{38}r - 32171710228725760a^{7}b^{39}r + 31164557577682944a^{6}b^{40}r - 28217866415243264a^{5}b^{41}r + 23292054322806784a^{4}b^{42}r - 16888498602639360a^{3}b^{43}r + 10133099161583616a^{2}b^{44}r - 4503599627370496ab^{45}r + 1125899906842624b^{46}r + 188894659314785808547 84a^{46}s - 604462909807314587353088a^{45}bs + 10880332376531662572355584a^{44}b^{2}s - 145071098353755500964741120a^{43}b^{3}s + 1600617785169769027310977024a^{42}b^{4}s-$	$C_2 \times C_8$

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$1551293611729492156982965043 2a^{41}b^5s + 1370631737246281973114874101 76a^{40}b^6s -$ $1131941423421569588860886712320a^{39}b^7s - 128202192321766651449122969104007823360a^{38}b^8s -$ $904936230680926574279560656913701850316 8a^{37}b^9s-$ $30411862796020542886477205208942736152985 6a^{36}b^{10}s-$ $647191124339636825662250760199358159781888 0a^{35}b^{11}s-$ $977840987154710441980073235153824628971929 60a^{34}b^{12}s-$ $111367308873684626318224429482522822706200576 0a^{33}b^{13}s-$ $989428095167691806658742767906297016140326502 4a^{32}b^{14}s-$ $698548146514267205283629970942330597704005058 56a^{31}b^{15}s-$ $394047267484903131618111870057848227204347985920 0a^{30}b^{16}s-$ $175659894706144974357121624883372143758639366144 0a^{29}b^{17}s-$ $592249124952604474220595915061488182610096029696 0a^{28}b^{18}s-$ $128841002966851945138843171770524157993716673413 12a^{27}b^{19}s-$ $130554023795660380326688045553138678615688557363 2a^{26}b^{20}s+$ $138101460629513081128382907275976679344108608684032a^{25}b^{21}s+$ $727484777709777833704171169482074666167896821989376a^{24}b^{22}s+$	

continued on next page

Table D.6.: *continued*

$\mu_T^{(2)}$	T
$230774018913329483973660294999072166241681426664652 8a^{23}b^{23}s+$ $4840517021008719277765021076048926429377710457356288a^{22}b^{24}s+$ $4891299921051587670064779306132381998804388550803456a^{21}b^{25}s-$ $9573970703780937240253245296790007811630879050039296a^{20}b^{26}s-$ $63115994956408238622608203426368443578619572214824960a^{19}b^{27}s-$ $186235340570633649499433765896022865374958192227778560a^{18}b^{28}s-$ $390749559434433282076411640256653476809546403267215360a^{17}b^{29}s-$ $637704495109758341157263306211255428756198779781120000a^{16}b^{30}s-$ $832107916162387386428333005213704808321837905613946880a^{15}b^{31}s-$ $872430152610318870467796283767747778947391298564259840a^{14}b^{32}s-$ $728960325597312339660762511302987781069285619914506240a^{13}b^{33}s-$ $475773162755630149680658854560967585141177378605629440a^{12}b^{34}s-$ $234182892392296341539904339869543890462590784524779520a^{11}b^{35}s-$ $81833714080566324441172355375993143946921092243783680a^{10}b^{36}s-$ $18101640876857678502005292198716915497646812456550400a^{9}b^{37}s-$ $1905435881774492473895293915654412157647032890163200a^{8}b^{38}s$	

Table D.7.: The Polynomials $\mu_T^{(3)}$

$\mu_T^{(3)}$	T
$-15ab^4d^2r + 7a^3b^2dr + 81b^4d^2s - 153a^2b^2ds + 64a^4s$	C_2
$a^4b^3r - 18a^3b^4r - 135a^2b^5r - 972ab^6r - 5832b^7r - 1259712a^7s - 45349632a^6bs - 1360488960a^5b^2s + 764050599936a^4b^3s$	C_3
$1991a^4b^4r + 32824a^3b^5r + 15936a^2b^6r + 7680ab^7r + 4096b^8r - 262144a^8s + 6291456a^7bs - 119537664a^6b^2s + 2097152000a^5b^3s + 1206617374720a^4b^4s$	C_4
$246553002a^6b^5r + 2733893761a^5b^6r - 4703250a^4b^7r - 391500a^3b^8r - 31125a^2b^9r - 2250ab^{10}r - 125b^{11}r - 125a^{11}s + 2250a^{10}bs - 31125a^9b^2s + 391500a^8b^3s - 4703250a^7b^4s - 2733893761a^6b^5s + 246553002a^5b^6s$	C_5
$-492a^5b^6r - 5737a^4b^7r - 12802a^3b^8r - 9309a^2b^9r - 1024ab^{10}r + 512b^{11}r - 13824a^{11}s + 248832a^{10}bs - 3110400a^9b^2s + 33841152a^8b^3s - 344134656a^7b^4s + 3369682944a^6b^5s + 3392204039415a^5b^6s + 10152372291606a^4b^7s + 10143558801891a^3b^8s + 3379639518108a^2b^9s$	C_6

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$2497745017a^{16}b^{7}r - 4638275503a^{15}b^{8}r - 55595615706a^{14}b^{9}r + 309249758202a^{13}b^{10}r - 742980340662a^{12}b^{11}r + 1031980431804a^{11}b^{12}r - 887347384140a^{10}b^{13}r + 468689078146a^{9}b^{14}r - 140068984929a^{8}b^{15}r + 18222532679a^{7}b^{16}r - 7825398a^{6}b^{17}r - 984312a^{5}b^{18}r - 119805a^{4}b^{19}r - 13818a^{3}b^{20}r - 1449a^{2}b^{21}r - 126ab^{22}r - 7b^{23}r - 7a^{23}s + 42a^{22}bs - 357a^{21}b^{2}s + 2450a^{20}b^{3}s - 16905a^{19}b^{4}s + 112896a^{18}b^{5}s - 744898a^{17}b^{6}s + 2763834966a^{16}b^{7}s - 1516600104a^{15}b^{8}s - 69252613309a^{14}b^{9}s + 295155166705a^{13}b^{10}s - 579797539293a^{12}b^{11}s + 653546063793a^{11}b^{12}s - 442629420023a^{10}b^{13}s + 174559653789a^{9}b^{14}s - 35325644769a^{8}b^{15}s + 2497745017a^{7}b^{16}s$	C_7
$-119249442224a^{15}b^{8}r + 2722451995528a^{14}b^{9}r - 26865300956912a^{13}b^{10}r + 154593891786433a^{12}b^{11}r - 584928886998832a^{11}b^{12}r + 1546968127236956a^{10}b^{13}r - 2955573214633416a^{9}b^{14}r + 4144069533901166a^{8}b^{15}r - 4275154708619032a^{7}b^{16}r + 3211545554074660a^{6}b^{17}r - 1710478368646136a^{5}b^{18}r + 612521782775953a^{4}b^{19}r - 132346657237000a^{3}b^{20}r + 13045044762288a^{2}b^{21}r + 48ab^{22}r + 8b^{23}r - 512a^{22}s - 12288a^{21}bs - 172032a^{20}b^{2}s - 1859584a^{19}b^{3}s - 17326080a^{18}b^{4}s - 147210240a^{17}b^{5}s - 1178099712a^{16}b^{6}s - 9057189888a^{15}b^{7}s + 142930775568384a^{14}b^{8}s - 2283576016142336a^{13}b^{9}s + 16544909149077504a^{12}b^{10}s - 71857205116600320a^{11}b^{11}s + 208392253473456128a^{10}b^{12}s - 425268114202558464a^{9}b^{13}s + 626432068129652736a^{8}b^{14}s - 671411975535722496a^{7}b^{15}s + 519919277044137984a^{6}b^{16}s - 283816411615199232a^{5}b^{17}s + 103722160664608768a^{4}b^{18}s - 22795895942676480a^{3}b^{19}s + 2279589594267648a^{2}b^{20}s$	C_8

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$743422717107a^{26}b^{9}r - 6554079892458a^{25}b^{10}r + 18867078014386a^{24}b^{11}r + 23541974848140a^{23}b^{12}r - 383736209556210a^{22}b^{13}r + 1608819916214036a^{21}b^{14}r - 4262805722241693a^{20}b^{15}r + 8262058761845874a^{19}b^{16}r - 12390869419414560a^{18}b^{17}r + 14762974445910216a^{17}b^{18}r - 14132815125206085a^{16}b^{19}r + 10883287134688772a^{15}b^{20}r - 6688012543537092a^{14}b^{21}r + 3219702449893584a^{13}b^{22}r - 1174411230071765a^{12}b^{23}r + 305971891726518a^{11}b^{24}r - 50805179205795a^{10}b^{25}r + 4042940003106a^{9}b^{26}r - 420689133a^{8}b^{27}r - 71799696a^{7}b^{28}r - 11974149a^{6}b^{29}r - 1930392a^{5}b^{30}r - 295488a^{4}b^{31}r - 41634a^{3}b^{32}r - 5103a^{2}b^{33}r - 486ab^{34}r - 27b^{35}r - 27a^{35}s - 486a^{33}b^{2}s + 1134a^{32}b^{3}s - 8019a^{31}b^{4}s + 32562a^{30}b^{5}s - 159003a^{29}b^{6}s + 714420a^{28}b^{7}s - 3272238a^{27}b^{8}s + 910868506242a^{26}b^{9}s - 7081073425530a^{25}b^{10}s + 15909499292454a^{24}b^{11}s + 44130104332141a^{23}b^{12}s - 421559307462828a^{22}b^{13}s + 1541542193234256a^{21}b^{14}s - 3697476241545988a^{20}b^{15}s + 6554376796322943a^{19}b^{16}s - 9014101041990114a^{18}b^{17}s + 9836940643865847a^{17}b^{18}s - 8590749567811218a^{16}b^{19}s + 5993704020941199a^{15}b^{20}s - 3302944535378860a^{14}b^{21}s + 1404828612017796a^{13}b^{22}s - 443026943934204a^{12}b^{23}s + 96627463762711a^{11}b^{24}s - 12774910752324a^{10}b^{25}s + 743422717107a^{9}b^{26}s$	C_9

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$-1868060897658518568 96a^{17}r + 1786731211079968096256a^{16}br - 4614882747586788720640a^{15}b^2r - 1049203448659310411 7760a^{14}b^3r + 8651905697634334277 6320a^{13}b^4r - 1793155164126968262 16448a^{12}b^5r + 7228712307962148814848a^{11}b^6r + 7076706081645025820 67200a^{10}b^7r - 16701384878787349341 79840a^9b^8r + 2172685189713796037345280a^8b^9r - 2090514177979220423081984a^7b^{10}r + 1959225750253128598421504a^6b^{11}r - 1894409563379611562147840a^5b^{12}r + 1503828456720647019560960a^4b^{13}r - 823277785206301838 54080a^3b^{14}r + 286182079237632804519936a^2b^{15}r - 56960126329285819498496ab^{16}r + 4915887687818868162560b^{17}r - 16369376293696a^{17}s + 176225237848436a^{16}bs - 568187696377956a^{15}b^2s - 635925848701000a^{14}b^3s + 9036606027723200a^{13}b^4s - 23023965604314003a^{12}b^5s + 10471528296790328a^{11}b^6s + 73427984102451632a^{10}b^7s - 206755326094107000a^9b^8s + 291506483368630000a^8b^9s - 286802766107346904a^7b^{10}s + 263536784536337184a^6b^{11}s - 258602328438533744a^5b^{12}s + 216633410165921240a^4b^{13}s - 125439243143043800a^3b^{14}s + 45772666697705776a^2b^{15}s - 9496380366202816ab^{16}s + 848650629916376b^{17}s$	C_{10}

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$514152485812875408896000a^{12}b^{23}s+324487140345044826972160a^{11}b^{24}s-159148768462304237871104a^{10}b^{25}s+$ $59358798092707037642752a^{9}b^{26}s - 16243369822325679063040a^{8}b^{27}s + 3069057270089532571648a^{7}b^{28}s -$ $356919297437569908736a^{6}b^{29}s + 19202686280542453760a^{5}b^{30}s - 994361678361384a^{23}r +$ $34537447522698396a^{22}br - 564800263882811072a^{21}b^{2}r + 5799617430905287148a^{20}b^{3}r -$ $42053436599237437688a^{19}b^{4}r + 229455255151657063288a^{18}b^{5}r - 979710987860835208544a^{17}b^{6}r +$ $3359049555143464506059a^{16}b^{7}r - 9411715159675695936968a^{15}b^{8}r + 21807330919646551992504a^{14}b^{9}r -$ $42103542324766720534800a^{13}b^{10}r + 68016419864405208829072a^{12}b^{11}r - 92033144582077101472272a^{11}b^{12}r +$ $104099750495192568629880a^{10}b^{13}r - 97909713946869134073120a^{9}b^{14}r + 75853504478373601484736a^{8}b^{15}r -$ $47669925330939830900112a^{7}b^{16}r + 23698383769556659974312a^{6}b^{17}r - 8912601895212571273344a^{5}b^{18}r +$ $2306959559333364391848a^{4}b^{19}r - 302941515444215921424a^{3}b^{20}r - 24619780364093859312a^{2}b^{21}r +$ $15206916128744691648ab^{22}r - 1356484235117005656b^{23}r + 68342622644379096023040a^{22}s -$ $2075027973925122511994880a^{21}bs + 29784162716312354720317440a^{20}b^{2}s -$ $269365222624223317354610688a^{19}b^{3}s + 1724783100305731845247991808a^{18}b^{4}s -$ $8324730435042894880568770560a^{17}b^{5}s + 31466444802631826586733117440a^{16}b^{6}s -$ $95489059634593478602383163392a^{15}b^{7}s + 236509279770324069718273032192a^{14}b^{8}s -$ $483260436524245427429264326656a^{13}b^{9}s + 819769221896596302664273231872a^{12}b^{10}s-$	C_{12}

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$115748825883770160266246671564 8a^{11}b^{11}s + 1359266156909836031123490078720a^{10}b^{12}s -$ $1321745022211116130151411220480a^9b^{13}s + 1055068935735288752103852343296a^8b^{14}s -$ $681337351781554081029842534400a^7b^{15}s + 347405390599236200649222782976a^6b^{16}s -$ $133921329657195413883794227200a^5b^{17}s + 35610523516972769977609224192a^4b^{18}s -$ $4887726408522637739210833920a^3b^{19}s - 340581382878689565503127552a^2b^{20}s +$ $23695829249455809697834598 4ab^{21}s - 21541662954050736088940544b^{22}s$	
$-14a^3b^2rd^5 + 21a^2b^3rd^5 - 3ab^4rd^5 - 2b^5rd^5 - 2a^5sd^5 - 3a^4bsd^5 + 21a^3b^2sd^5 - 14a^2b^3sd^5$	$C_2 \times C_2$
$-7a^4r - 112a^3br - 560a^2b^2r - 896ab^3r + 3648b^4r + 79500918390784a^4s + 597945346949120a^3bs +$ $2082887339868160a^2b^2s - 2471152383426560ab^3s - 4942304766853120b^4s$	$C_2 \times C_4$

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$9642417549363246076218279572770 6110a^{11}r - 7280251384013347139256984351598 7667a^{10}br +$	$C_2 \times C_6$
$2284179509045724028436488749879240a^9b^2r + 1262641373610858816863956463058 9948a^8b^3r -$	
$5122027699081132006964731192061652a^7b^4r + 1169849478607363242590175225026190a^6b^5r -$	
$1805040418735966458529821086580 96a^5b^6r - 2066221270266162000280871929794 0a^4b^7r +$	
$1931194970458851513481471557696 6a^3b^8r - 3973162685655024420019519132755a^2b^9r +$	
$3590172354467888655030948717 36ab^{10}r - 1204247097651547315375986081 6b^{11}r + 341065560834a^{10}s -$	
$75948034914a^9bs - 45044753445a^8b^2s + 21649124016a^7b^3s - 4759891200a^6b^4s + 1066738284a^5b^5s +$	
$25749130a^4b^6s - 84517152a^3b^7s + 18599158a^2b^8s - 1675290ab^9s + 55843b^{10}s$	

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$-29482290307a^{22}r - 1297220773508a^{21}br - 25840982312838a^{20}b^2r - 307195659349040a^{19}b^3r - 2405233271827120a^{18}b^4r - 12758836467214656a^{17}b^5r - 43865950094664092a^{16}b^6r - 72129738551681920a^{15}b^7r + 149895391933595392a^{14}b^8r + 1460121843166099456a^{13}b^9r + 5678867869324891136a^{12}b^{10}r + 16956890635869298688a^{11}b^{11}r + 46848098821667364864a^{10}b^{12}r + 111466954531910811648a^9b^{13}r + 160625815629332135936a^8b^{14}r - 108689960558544551936a^7b^{15}r - 1327236622236242149376a^6b^{16}r - 3890145381061612273664a^5b^{17}r - 6872949362645096464384a^4b^{18}r - 8051733316297543385088a^3b^{19}r - 6162086147086746648576a^2b^{20}r - 2804677970136336957440ab^{21}r - 576734585557400682496b^{22}r - 272355207634798474196597421087553016665216a^{22}s - 10595773793131767512608155828550057005678592 0a^{21}bs- 186237626147569939480688323242766638938220134 4a^{20}b^2s- 1946789659744684777531144688489507070963980697 6a^{19}b^3s- 13294217506248906310558920823465475167438136934 4a^{18}b^4s- 60197084073215661471342651267877521696037745459 2a^{17}b^5s- 164303935627212902572193314101581417625778808422 4a^{16}b^6s- 107641323235016860183889423376395909834306958131 2a^{15}b^7s+ 127260882246669870927846394064967203088459848744 96a^{14}b^8s+$	$C_2 \times C_8$

continued on next page

Table D.7.: *continued*

$\mu_T^{(3)}$	T
$706505759089947479257762111686739063358556985098 24a^{13}b^{9}s+$	
$2375480823633521665023842710186118207712004732354 56a^{12}b^{10}s+$	
$6878532029620530881437412443487643323686000430940 16a^{11}b^{11}s+$	
$1842897987370625141370869670901744247908723186466 816a^{10}b^{12}s+$	
$3790693029674710240125205754039133421925191424933 888a^{9}b^{13}s+$	
$3113205490582616382081489792811480477641330317590 528a^{8}b^{14}s-$	
$1198460847644276738712089978282746439270216524365 8240a^{7}b^{15}s-$	
$5830784892753149171696364372073087985821528473416 4992a^{6}b^{16}s-$	
$1356752210069058695391635008436077378234079250984 46848a^{5}b^{17}s-$	
$2046146176835813425483432794078197924632746689088 71680a^{4}b^{18}s-$	
$2090665321422592990643262923622492124629232920612 04480a^{3}b^{19}s-$	
$1406916899995939417644362867657051843223390964395 54048a^{2}b^{20}s-$	
$5650193346922404682946915902471733818843110744417 8944ab^{21}s-$	
$1027307881258619033263075618631224330698747408075 9808b^{22}s$	

Table D.8.: The Polynomials $\nu_T^{(1)}$

$\nu_T^{(1)}$	T
$ar + 9s$	C_2
$r + 13824s$	C_3
$-ar - 14br + 49664as + 53248bs$	C_4
$-3121a^3r - 37749a^2br - 47287ab^2r + 32943b^3r + 32943a^3s + 47287a^2bs - 37749ab^2s + 3121b^3s$	C_5
$-10a^3r - 117a^2br - 264ab^2r - 21b^3r + 1659771a^3s + 5514156a^2bs + 2101707ab^2s + 1727730b^3s$	C_6
$-86718a^7r - 364777a^6br + 1133629a^5b^2r + 207018a^4b^3r - 2955183a^3b^4r + 4298504a^2b^5r - 2871141ab^6r + 574479b^7r - 64189a^7s - 560847a^6bs + 718620a^5b^2s + 1121491a^4b^3s - 2631622a^3b^4s + 2876111a^2b^5s - 971803ab^6s + 86718b^7s$	C_7
$-73848a^7r + 1094596a^6br - 5800312a^5b^2r + 14437473a^4b^3r - 18445448a^3b^4r + 11363504a^2b^5r - 3161552ab^6r + 1003496b^7r + 7938304a^6s - 65988608a^5bs + 197447680a^4b^2s - 279629824a^3b^3s + 181594112a^2b^4s - 50135040ab^5s + 16711680b^6s$	C_8
$-1226439a^{11}r - 244494a^{10}br + 14663494a^9b^2r - 31422897a^8b^3r + 15865380a^7b^4r + 47235375a^6b^5r - 130399407a^5b^6r + 194946777a^4b^7r - 193299969a^3b^8r + 118928988a^2b^9r - 42901371ab^{10}r + 6343633b^{11}r - 1510930a^{11}s - 1969182a^{10}bs + 16007571a^9b^2s - 22838418a^8b^3s - 1302489a^7b^4s + 54123471a^6b^5s - 107773143a^5b^6s + 141696162a^4b^7s - 112816116a^3b^8s + 55235591a^2b^9s - 13735323ab^{10}s + 1226439b^{11}s$	C_9

continued on next page

Table D.8.: *continued*

$\nu_T^{(1)}$	T
$-6523394816a^{11}r + 36994300928a^{10}br - 18010251264a^9b^2r - 302904093696a^8b^3r + 858196842496a^7b^4r - 817070891008a^6b^5r - 229401274368a^5b^6r + 1337582452736a^4b^7r - 1579436670976a^3b^8r + 1021496098816a^2b^9r - 340520927232ab^{10}r + 450483978 24b^{11}r - 397080a^{11}s + 2681682a^{10}bs - 3009506a^9b^2s - 19641244a^8b^3s + 70821144a^7b^4s - 83204219a^6b^5s - 2224452a^5b^6s + 111722144a^4b^7s - 146547004a^3b^8s + 102963784a^2b^9s - 36591584ab^{10}s + 5084456b^{11}s$	C_{10}
$-16368060a^{15}r + 371968434a^{14}br - 3847011768a^{13}b^2r + 24165879634a^{12}b^3r - 103545204444a^{11}b^4r + 321344545212a^{10}b^5r - 746902049904a^9b^6r + 1323272770545a^8b^7r - 1797785532156a^7b^8r + 1864752259596a^6b^9r - 1453384657128a^5b^{10}r + 825155421456a^4b^{11}r - 324026619960a^3b^{12}r + 81998905176a^2b^{13}r - 13343938848ab^{14}r + 1849423272b^{15}r + 969115560192a^{14}s - 18156961741824a^{13}bs + 155918883916800a^{12}b^2s - 817402574997504a^{11}b^3s + 2927986683346944a^{10}b^4s - 7582944748345344a^9b^5s + 14624630199465984a^8b^6s - 21278142234943488a^7b^7s + 23353733793871872a^6b^8s - 19082362286407680a^5b^9s + 11270047067504640a^4b^{10}s - 4567054883880960a^3b^{11}s + 1179066424688640a^2b^{12}s - 192872589557760ab^{13}s + 27553227079680b^{14}s$	C_{12}
$-2ard + brd + asd - 2bsd$	$C_2 \times C_2$
$-a^2r - 8abr - 8b^2r + 3178496a^2s + 3407872abs + 13631488b^2s$	$C_2 \times C_4$

continued on next page

Table D.8.: *continued*

$\nu_T^{(1)}$	T
$2816715912781053150a^7r - 1254131753648366115a^6br - 1545439567640961 60a^5b^2r + 1064545240018402 89a^4b^3r + 10949518510656462a^3b^4r - 11176427563268121a^2b^5r + 2178807569806500ab^6r - 988683184988 37b^7r + 550293a^6s + 28530a^5bs - 31431a^4b^2s + 1332a^3b^3s + 3039a^2b^4s - 630ab^5s + 35b^6s$	$C_2 \times C_6$
$-13209a^{14}r - 369852a^{13}br - 4391066a^{12}b^2r - 28456368a^{11}b^3r - 103820176a^{10}b^4r - 159393216a^9b^5r + 332251768a^8b^6r + 2379693952a^7b^7r + 4934706432a^6b^8r - 3132680192a^5b^9r - 48406967296a^4b^{10}r - 141552214016a^3b^{11}r - 216685813760a^2b^{12}r - 178459344896ab^{13}r - 614706544464b^{14}r - 422423120938554254950 4a^{14}s - 98109062399219778715648a^{13}bs - 952994287212899115991040a^{12}b^2s - 4980425767936924227469312a^{11}b^3s - 13625349992275086646706176a^{10}b^4s - 7054168672681066932207616a^9b^5s + 88895768193351959432921088a^8b^6s + 342950041455456735822086144a^7b^7s + 383060208270845052681453568a^6b^8s - 147014293131875324099611852 8a^5b^9s - 766057686543793048661681766 4a^4b^{10}s - 1679767480842554002879650201 6a^3b^{11}s - 20736222902468481529923239936a^2b^{12}s - 13972613507378432172607143936ab^{13}s - 3992175287822409192173469696b^{14}s$	$C_2 \times C_8$

Table D.9.: The Polynomials $\nu_T^{(2)}$

$\nu_T^{(2)}$	T
$r - 27s$	C_2
$-r - 2641807540224s$	C_3
$-3052404736a^2s - 3271557120abs - 14ar - 209br$	C_4
$1461113a^3r + 17671629a^2br + 22127943ab^2r - 15439276b^3r - 15439276a^3s - 22127943a^2bs + 17671629ab^2s - 1461113b^3s$	C_5
$14a^3r + 180a^2br + 555ab^2r + 420b^3r - 36224549460a^3s - 119729917530a^2bs - 45681487380ab^2s - 37494993069b^3s$	C_6
$1651723461a^7r + 6857059076a^6br - 22067823869a^5b^2r - 3248119070a^4b^3r + 57189936895a^3b^4r - 84018038727a^2b^5r + 57050372330ab^6r - 11617337047b^7r + 1797773049a^7s + 10043071381a^6bs - 15073102331a^5b^2s - 18470724580a^4b^3s + 47078968860a^3b^4s - 53760723268a^2b^5s + 18419123303ab^6s - 1651723461b^7s$	C_7
$357458640a^7r - 5299041240a^6br + 28085457840a^5b^2r - 69925413045a^4b^3r + 89362321300a^3b^4r - 55069807950a^2b^5r + 15319961076ab^6r - 4864231201b^7r - 252753342464a^6s + 2053135073280a^5bs - 6091527290880a^4b^2s + 8589703249920a^3b^3s - 5577148661760a^2b^4s + 1538756444160ab^5s - 512918814720b^6s$	C_8

continued on next page

Table D.9.: *continued*

$\nu_T^{(2)}$	T
$135940809738a^{11}r + 25598249889a^{10}br - 1626465048703a^9b^2r + 3500083359540a^8b^3r - 1787889845574a^7b^4r - 5230525891968a^6b^5r + 14512383231975a^5b^6r - 21736721436858a^4b^7r + 21599815477017a^3b^8r - 13333181337024a^2b^9r + 4830058660002ab^{10}r - 721696816069b^{11}r + 167399411965a^{11}s + 206398597377a^{10}bs - 17555482249538a^9b^2s + 2526272748477a^8b^3s + 98500469859a^7b^4s - 5909026191759a^6b^5s + 11813801740728a^5b^6s - 15592292477658a^4b^7s + 12444052772988a^3b^8s - 6106261985777a^2b^9s + 1520947157007ab^{10}s - 135940809738b^{11}s$	C_9
$2563220161187840a^{11}r - 13968006543081472a^{10}br + 5327782651953152a^9b^2r + 116168139132796928a^8b^3r - 318388519501234176a^7b^4r + 294262118199066624a^6b^5r + 94265044361019392a^5b^6r - 496376897921875968a^4b^7r + 578260619281563648a^3b^8r - 370238528900038656a^2b^9r + 122476544722468864ab^{10}r - 16110783557533696b^{11}r + 1937958058a^{11}s - 13099200002a^{10}bs + 14754771174a^9b^2s + 95825559486a^8b^3s - 346217668107a^7b^4s + 407632781458a^6b^5s + 9657861042a^5b^6s - 546163721061a^4b^7s + 717685125501a^3b^8s - 504856113082a^2b^9s + 179778279400ab^{10}s - 24989352181b^{11}s$	C_{10}

continued on next page

Table D.9.: *continued*

$\nu_T^{(2)}$	T
$4971814474984a^{15}r - 112999725362970a^{14}br + 1168830739218648a^{13}b^2r - 7343265583001516a^{12}b^3r + 31468492602978204a^{11}b^4r - 97673466621205245a^{10}b^5r + 227054091232077972a^9b^6r - 402323545115665200a^8b^7r + 546669605121641658a^7b^8r - 567113536226054841a^6b^9r + 442071357364683744a^5b^{10}r - 251021779116423657a^4b^{11}r + 98586726114168570a^3b^{12}r - 24951348855850266a^2b^{13}r + 4060457805627432ab^{14}r - 562873433133225b^{15}r - 341821177056668161536a^{14}s + 5930688024820473200064a^{13}bs - 47966277684559872983O4a^{12}b^2s + 239679333284098424832OOa^{11}b^3s - 825955236473370624000000a^{10}b^4s + 207316942235906935947264a^9b^5s - 389873305193352589541376a^8b^6s + 555930773740283971239936a^7b^7s - 600594843978775747952640a^6b^8s + 484913713195925990277120a^5b^9s - 284005838463998846828544a^4b^{10}s + 114550000317686681174016a^3b^{11}s - 29539502215498659004416a^2b^{12}s + 4822077921177328680960ab^{13}s - 688868274453904097280b^{14}s$	C_{12}
$r + s$	$C_2 \times C_2$
$-48838475776a^2s - 52344913920abs - 209379655680b^2s + r$	$C_2 \times C_4$

continued on next page

Table D.9.: *continued*

$\nu_T^{(2)}$	T
$-2546259355819186485495511095Oa^7r + 118777605662199113463689723 97a^6br + 1189213989266646788761412244a^5b^2r - 1005207914850882587506206945a^4b^3r - 8113716297596377573799895 0a^3b^4r + 1042727476456200319446541 95a^2b^5r - 216438570907701394302448 56ab^6r + 11903225285197892952962 73b^7r - 45196737a^6s - 2348046a^5bs + 2579745a^4b^2s - 108900a^3b^3s - 249495a^2b^4s + 51714ab^5s - 2873b^6s$	$C_2 \times C_6$

continued on next page

Table D.9.: *continued*

$\nu_T^{(2)}$	T
$21360675a^{14}r + 598098900a^{13}br + 7105419630a^{12}b^2r + 46125499920a^{11}b^3r + 168938921040a^{10}b^4r + 262905854400a^9b^5r - 525880005420a^8b^6r - 3855997905600a^7b^7r - 8098291873600a^6b^8r + 4753938481920a^5b^9r + 78224096273280a^4b^{10}r + 231185841843200a^3b^{11}r + 357941121199104a^2b^{12}r + 299403873079296ab^{13}r + 106046375330816b^{14}r + 5007898484920598628455657030140559936a^{14}s + 113111585205681976299370114517859904128a^{13}bs + 1081810658298515302955461525659986165 76a^{12}b^2s + 5589730666671771855132770931325272064 00a^{11}b^3s + 1513074075212618936814440705289596436480a^{10}b^4s + 735636348883540733212981861822507253760a^9b^5s - 1002519976014885983150131176297610608 6400a^8b^6s - 38187953589942464485684602072145802035200a^7b^7s - 41664506532417970681005602359703890821120a^6b^8s + 16663638206683774289984569749629797662 7200a^5b^9s + 85662209863306181135383200253332387004 4160a^4b^{10}s + 18710725651012847116952906105547018102 37440a^3b^{11}s + 23058405014637935794016835419552132943 05280a^2b^{12}s + 155275351978156800815684923548028863774 7200ab^{13}s + 44364386279473371661624263870865389649 9200b^{14}s$	$C_2 \times C_8$

Table D.10.: The Polynomials $\nu_T^{(3)}$

$\nu_T^{(3)}$	T
$64b^2dr - 7a^2r + 729as$	C_2
$ar - 27br + 803232681984as - 6112404799488bs$	C_3
$1991a^2r + 48752abr + 262600b^2r + 1242201849856a^2s + 9342896046080abs - 4826469498880b^2s$	C_4
$-246553002a^5r - 4459764775a^4br - 18886000075a^3b^2r - 1670746025a^2b^3r - 18639447075ab^4r + 2789018761b^5r + 2789018761a^5s + 18639447075a^4bs - 1670746025a^3b^2s + 18886000075a^2b^3s - 4459764775ab^4s + 246553002b^5s$	C_5
$-492a^5r - 8689a^4br - 45748a^3b^2r - 72846a^2b^3r - 40752ab^4r + 41751b^5r + 3424447441143a^5s + 30395059879392a^4bs + 61798659475842a^3b^2s + 52797620229732a^2b^3s - 19165211345313ab^4s - 10138918554324b^5s$	C_6
$-2497745017a^{11}r - 15343684633a^{10}br + 35253684339a^9b^2r + 119805998182a^8b^3r - 417369430378a^7b^4r + 495797505553a^6b^5r - 612871701330a^5b^6r + 1127680956200a^4b^7r - 1265252918778a^3b^8r + 708207103362a^2b^9r - 194452169109ab^{10}r + 182834314119b^{11}r - 2758970190a^{11}s - 20586723093a^{10}bs + 17880417165a^9b^2s + 158150760545a^8b^3s - 325690559471a^7b^4s + 272311306414a^6b^5s - 486043044305a^5b^6s + 855286820288a^4b^7s - 665504579057a^3b^8s + 255559137926a^2b^9s - 42818879820ab^{10}s + 2497745017b^{11}s$	C_7

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$-119249442224a^{11}r + 2722451995528a^{10}br - 25434307650224a^{9}b^{2}r + 128602436604641a^{8}b^{3}r - 393299188780688a^{7}b^{4}r + 764729717232800a^{6}b^{5}r - 961663949889696a^{5}b^{6}r + 763668309331080a^{4}b^{7}r - 334225413090016a^{3}b^{8}r + 28682328199056a^{2}b^{9}r + 33560716714144ab^{10}r - 6522522381000b^{11}r + 142998505291776a^{10}s - 2283079366868992a^{9}bs + 14832517487001600a^{8}b^{2}s - 52442485339717632a^{7}b^{3}s + 111819244662423552a^{6}b^{4}s - 149846949476958208a^{5}b^{5}s + 125078510577385472a^{4}b^{6}s - 57557969004396544a^{3}b^{7}s + 5841031272595456a^{2}b^{8}s + 5698973985669120ab^{9}s - 1139794797133824b^{10}s$	C_8
$-743422717107a^{17}r - 136724561505a^{16}br + 13356423201884a^{15}b^{2}r - 28767381691398a^{14}b^{3}r - 25362400906164a^{13}b^{4}r + 222821830879885a^{12}b^{5}r - 505438041369924a^{11}b^{6}r + 709950711325941a^{10}b^{7}r - 879763065782232a^{9}b^{8}r + 1348861323871773a^{8}b^{9}r - 2160649630918044a^{7}b^{10}r + 2747361223975454a^{6}b^{11}r - 2563658421472068a^{5}b^{12}r + 1736573973789912a^{4}b^{13}r - 838212815164505a^{3}b^{14}r + 269641567050804a^{2}b^{15}r - 50791368120732ab^{16}r + 4045364893248b^{17}r - 910853714778a^{17}s - 1116676789704a^{16}bs + 15029127264852a^{15}b^{2}s - 19839960363847a^{14}b^{3}s - 48921280770273a^{13}b^{4}s + 218833175805216a^{12}b^{5}s - 401439535456706a^{11}b^{6}s + 491972245843248a^{10}b^{7}s - 635220039813597a^{9}b^{8}s + 1072797339438948a^{8}b^{9}s - 1637059053494439a^{7}b^{10}s + 1847465038159380a^{6}b^{11}s - 1496687033357461a^{5}b^{12}s + 871593129545376a^{4}b^{13}s - 350355428676498a^{3}b^{14}s + 89936659308748a^{2}b^{15}s - 12774910752324ab^{16}s + 743422717107b^{17}s$	C_9

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$-64000a^{35}r - 768000a^{34}br - 6144000a^{33}b^2r - 37120000a^{32}b^3r - 192000000a^{31}b^4r -$ $873984000a^{30}b^5r - 3655168000a^{29}b^6r - 14183424000a^{28}b^7r - 52216320000a^{27}b^8r -$ $182996480000a^{26}b^9r - 1868060903852684328 96a^{25}b^{10}r + 4028404286244986667008a^{24}b^{11}r -$ $387584713910920252006 40a^{23}b^{12}r + 2138330276182784596869 12a^{22}b^{13}r - 6953228510208479265751 04a^{21}b^{14}r +$ $953343811607995315175424a^{20}b^{15}r + 272509235332852192382156 8a^{19}b^{16}r -$ $205259516983966909104128 00a^{18}b^{17}r + 674330547026805646691205 12a^{17}b^{18}r -$ $150297810397113118755651584a^{16}b^{19}r + 250299186878437613843251200a^{15}b^{20}r -$ $323060122443600693841100800a^{14}b^{21}r + 328108894130074193213521920a^{13}b^{22}r -$ $263246072736192209354752000a^{12}b^{23}r + 166137415856662951409745920a^{11}b^{24}r -$ $81484169452699769790005248a^{10}b^{25}r + 30391704623466003273089024a^9b^{26}r -$ $8316605349030747680276480a^8b^{27}r + 1571357322285840676683776a^7b^{28}r -$ $182742680288035793272832a^6b^{29}r + 9831775375637736325120a^5b^{30}r - 16369376293696a^{25}b^{10}s +$ $372657753372788a^{24}b^{11}s - 3796008138530516a^{23}b^{12}s + 22323464260126904a^{22}b^{13}s -$ $79007289775340552a^{21}b^{14}s + 134390205194709853a^{20}b^{15}s + 20130612638999774 8a^{19}b^{16}s -$ $2131931915948864296a^{18}b^{17}s + 7657931561269819694a^{17}b^{18}s - 18106747938657159502a^{16}b^{19}s +$ $31650453432592374684a^{15}b^{20}s - 42638946291038299175a^{14}b^{21}s + 45032466428146755880a^{13}b^{22}s -$	C_{10}

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$3746318178732955 2815a^{12}b^{23}s + 24455963173246494200a^{11}b^{24}s - 12379669014942376318a^{10}b^{25}s + 4755671645243917014a^{9}b^{26}s - 1337694844845958268a^{8}b^{27}s + 259289334276684392a^{7}b^{28}s - 30873869573192771a^{6}b^{29}s + 1697301253462252a^{5}b^{30}s - 1710000a^{4}b^{31}s - 407500a^{3}b^{32}s - 81000a^{2}b^{33}s - 12000ab^{34}s - 1000b^{35}s$	

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$-994361678361384a^{35}b^{12}r + 464697876630350004a^{34}b^{13}r - 10508436749972114472a^{33}b^{14}r +$ $153304057489341554436a^{32}b^{15}r - 1622685426039561423444a^{31}b^{16}r + 13285694009843709851152a^{30}b^{17}r -$ $87584565720091128837792a^{29}b^{18}r + 477770966470923889075563a^{28}b^{19}r - 2199199487176117989715524a^{27}b^{20}r +$ $8667201261284151617392220a^{26}b^{21}r - 29570674041752794789068884a^{25}b^{22}r +$ $88085172134101901356095558a^{24}b^{23}r - 230595684416307250810869912a^{23}b^{24}r +$ $533194510692480840506930034a^{22}b^{25}r - 1093040438097001336031752400a^{21}b^{26}r +$ $1991883819085641619315707119a^{20}b^{27}r - 3232322823443378670472960000a^{19}b^{28}r +$ $4674674692935495914661729044a^{18}b^{29}r - 6025178187906808120809334120a^{17}b^{30}r +$ $6915114344100464423291223077a^{16}b^{31}r - 7054840759199949738966497088a^{15}b^{32}r +$ $6380684170568918252142630388a^{14}b^{33}r - 5096913122167999701114687922a^{13}b^{34}r +$ $3577910363913311263289797988a^{12}b^{35}r - 2192771886097903374749263088a^{11}b^{36}r +$ $1163382521172332872746670444a^{10}b^{37}r - 528496820608243474999110566a^{9}b^{38}r +$ $202616078013384474145449311a^{8}b^{39}r - 64293695532983266599516044a^{7}b^{40}r +$ $16434206440862402404259722a^{6}b^{41}r - 3251619402411507822996400a^{5}b^{42}r + 467268756138680789785122a^{4}b^{43}r -$ $43384669509645725494488a^{3}b^{44}r + 1953337298568488154000a^{2}b^{45}r + 96ab^{46}r + 8b^{47}r - 13824a^{46}s - 497664a^{45}bs -$ $9455616a^{44}b^{2}s - 126406656a^{43}b^{3}s - 1337720832a^{42}b^{4}s - 11956875264a^{41}b^{5}s - 94062477312a^{40}b^{6}s-$	C_{12}

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$670154342400a^{39}b^7s - 4415821443072a^{38}b^8s - 27345281163264a^{37}b^9s - 161147485974528a^{36}b^{10}s -$	
$912732334276608a^{35}b^{11}s + 68342617636200614449152a^{34}b^{12}s - 289513947244809283950182 4a^{33}b^{13}s +$	
$5960516709338758783512 5760a^{32}b^{14}s - 7944930129353499294521425 92a^{31}b^{15}s +$	
$77057095017944161845646 66368a^{30}b^{16}s - 57943820970822561654302687232a^{29}b^{17}s +$	
$351464905594685769810014453760a^{28}b^{18}s - 1766448538678514101677101383680a^{27}b^{19}s +$	
$7498841465637925802045972840448a^{26}b^{20}s - 27271982013210574646351790440448a^{25}b^{21}s +$	
$85884290260854852043487334334464a^{24}b^{22}s - 236116816261431365858260273201152a^{23}b^{23}s +$	
$570236169544426262064815241854976a^{22}b^{24}s - 1215414642750586311535127740809216a^{21}b^{25}s +$	
$2294072155947124025454128747249664a^{20}b^{26}s - 3843209414297520857164263176798208a^{19}b^{27}s +$	
$5721975283186102571857991478804480a^{18}b^{28}s - 7573900419393270452787532171051008a^{17}b^{29}s +$	
$8907920454548497138840554405101568a^{16}b^{30}s - 9295514920391708325193035200593920a^{15}b^{31}s +$	
$8584928851056391271780092784148480a^{14}b^{32}s - 6992159697594140347508412641181696a^{13}b^{33}s +$	
$4997875118429031181275432373714944a^{12}b^{34}s - 3115117923485726617303706480148480a^{11}b^{35}s +$	
$1678997311292040033411815234863104a^{10}b^{36}s - 774067846136366314622201955876864a^{9}b^{37}s +$	
$300897330615830505499724743704576a^{8}b^{38}s - 96727590041000821695885663535104a^{7}b^{39}s +$	
$25027949280853287597863092617216a^{6}b^{40}s - 5009007916045593013486199242752a^{5}b^{41}s+$	

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$7276061021871294842340775034888a^4b^{42}s - 6824398823843273192976364333392a^3b^{43}s + 3101999465383305996807438336a^2b^{44}s$	
$-56a^2rd^2 + 56abrd^2 + 114b^2rd^2 + 114a^2sd^2 + 56absd^2 - 56b^2sd^2$	$C_2 \times C_2$
$-7a^6b^4r - 168a^5b^5r - 1512a^4b^6r - 6272a^3b^7r - 11136a^2b^8r - 3072ab^9r + 4096b^{10}r - 16777216a^{10}s + 402653184a^9bs - 6039797760a^8b^2s + 73014444032a^7b^3s + 787117181501444a^6b^4s + 1242018642657280a^5b^5s + 7422047084871680a^4b^6s + 19769219067412480a^3b^7s + 19769219067412480a^2b^8s$	$C_2 \times C_4$

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$115896562708900714713194732225100000000a^{23}r - 844095822080142199852436714448390000000a^{22}br +$	$C_2 \times C_6$
$268611615330761530370823787595174400000a^{21}b^2r - 487219006384630829626386966797313000000a^{20}b^3r +$	
$547883533385549676717145062756186960000a^{19}b^4r - 382626678931988042720449314234041227200a^{18}b^5r +$	
$146206720002675150700017153571422132480a^{17}b^6r - 58909735460074727064567807518197668848a^{16}b^7r -$	
$24096883167542463851700957777628957056a^{15}b^8r + 12448062205827660635408001393919452864a^{14}b^9r -$	
$2525404616397107674675177651598504448a^{13}b^{10}r - 1308664123283433359836979094728142 72a^{12}b^{11}r +$	
$2094543847587436951417938778488841088a^{11}b^{12}r - 574866242352719044245963287765942 40a^{10}b^{13}r +$	
$85576585300072067497171331064936 96a^9b^{14}r - 7534265009620658944953083000250 24a^8b^{15}r +$	
$368494284139820121290351105203 20a^7b^{16}r - 77077164057566690936318840524 8a^6b^{17}r -$	
$451925976016757080247500 8a^5b^{18}r - 354489855885377808629760a^4b^{19}r - 2500427336153714550374 4a^3b^{20}r -$	
$1505859600204618006528a^2b^{21}r - 70039981404865953792ab^{22}r - 1945555039024054272b^{23}r +$	
$40958565386368a^{22}s - 276777107970432a^{21}bs + 801242730916672a^{20}b^2s - 1286746889804544a^{19}b^3s +$	
$1224602945218240a^{18}b^4s - 657765694942848a^{17}b^5s + 127855167499072a^{16}b^6s + 65925228864000a^{15}b^7s -$	
$52117158883904a^{14}b^8s + 13524629594496a^{13}b^9s - 196934480960a^{12}b^{10}s - 842855461632a^{11}b^{11}s +$	
$257698159168a^{10}b^{12}s - 39637223808a^9b^{13}s + 3516988864a^8b^{14}s - 171549696a^7b^{15}s + 3573952a^6b^{16}s$	

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$-7547466318592a^{38}b^{8}r-573607440212992a^{37}b^{9}r-20744148420490752a^{36}b^{10}r-474851872457060352a^{35}b^{11}r-$	$C_2 \times C_8$
$7716346963107721216a^{34}b^{12}r - 94555931444454834176a^{33}b^{13}r - 904995026209050385408a^{32}b^{14}r -$	
$6901972611098746486784a^{31}b^{15}r - 42288386590880977043456a^{30}b^{16}r - 207111075522872124178432a^{29}b^{17}r -$	
$788638755350000561192960a^{28}b^{18}r - 2132837051351474349277184a^{27}b^{19}r -$	
$2560352545095225114361856a^{26}b^{20}r + 10730930423342858025041920a^{25}b^{21}r +$	
$84217518907636637373825024a^{24}b^{22}r + 320161760068857947207237632a^{23}b^{23}r +$	
$804815189323712985909166080a^{22}b^{24}r + 1214743256353369647600369664a^{21}b^{25}r -$	
$1212514146406447845516247 04a^{20}b^{26}r - 7359581220954699571960741888a^{19}b^{27}r -$	
$26904851365096257990466469888a^{18}b^{28}r - 63630408468415338731226005504a^{17}b^{29}r -$	
$113877160508411866915826302976a^{16}b^{30}r - 161070161485115439404845891584a^{15}b^{31}r -$	
$182009225905637768545641168896a^{14}b^{32}r - 163409773404178933786456621056a^{13}b^{33}r -$	
$114418011007965219707057864704a^{12}b^{34}r - 60372579036592320802164047872a^{11}b^{35}r -$	
$22609525504287417823972556800a^{10}b^{36}r - 5359918179973563018905649152a^{9}b^{37}r -$	
$604750050361867484035809280a^{8}b^{38}r + 4598632616382431232a^{7}b^{39}r - 35280777268355399 68a^{6}b^{40}r +$	
$247078734556613836 8a^{5}b^{41}r - 1538542222700445696a^{4}b^{42}r + 819655132181430272a^{3}b^{43}r -$	
$351280770934898688a^{2}b^{44}r + 108086391056891904ab^{45}r - 18014398509481984b^{46}r-$	

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$1237940039285380274899124224a^{46}s + 5942112188569825319515796 2752a^{45}bs -$	
$1544949169028154583074107031552a^{44}b^2s + 2883905115519221888404999792 2304a^{43}b^3s -$	
$43306113630296886928631123253 6576a^{42}b^4s + 55637184844016988431690303683 95264a^{41}b^5s -$	
$635561981436427375028402086079 36512a^{40}b^6s + 66273280440171924402008242258 3394304a^{39}b^7s -$	
$69722933797427074324120821335461625728073 7280a^{38}b^8s-$	
$494365194609977047609588954591079090016653 14816a^{37}b^9s-$	
$16682885224223955447656026868420911104683671 55200a^{36}b^{10}s-$	
$35637680465850268956548353920475845731861726 756864a^{35}b^{11}s-$	
$54032378022062506420006911296294037859794753 5785984a^{34}b^{12}s-$	
$61734466951777453036460177525917947811270337 05463808a^{33}b^{13}s-$	
$55008913151349334090915944931316098900857417 497575424a^{32}b^{14}s-$	
$38944375397770771863087038044986553954944784 7902445568a^{31}b^{15}s-$	
$22027046336482959645072358544074151040122108 34470076416a^{30}b^{16}s-$	
$98463287948918597697240078901653793011334693 57925466112a^{29}b^{17}s-$	
$33306592755874578734163371108514569847432153 448067366912a^{28}b^{18}s-$	
$72885762126340861738598788631914877288264412 164098359296a^{27}b^{19}s-$	

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$9606526784233455207362546421299779964308201339086700544a^{26}b^{20}s+$	
$7699350090197714860860415164672053183474912113956560056832a^{25}b^{21}s+$	
$4080897831276003399161411283815995794539347174060531384320a^{24}b^{22}s+$	
$12987303914285252639189428769843208079022872037149821108224a^{23}b^{23}s+$	
$27330147428607447522493161377877427756698540078735393030144a^{22}b^{24}s+$	
$27859088163139464825203731160630465813637379155495653212160a^{21}b^{25}s-$	
$53176441906558351807996221970283901642081665809588844232704a^{20}b^{26}s-$	
$354378339887966243188345680044198475773536512442753506869248a^{19}b^{27}s-$	
$1048280712172191846264710659700495434357042909225002425384960a^{18}b^{28}s-$	
$2202382718577005287161357369741389766677848842279534939078656a^{17}b^{29}s-$	
$3597498070603163665522498461676744103280004644804697977257984a^{16}b^{30}s-$	
$4697239153056342730977244861764409268621141438980582442795008a^{15}b^{31}s-$	
$4927261593121478474220886543240362462855809016380794253344768a^{14}b^{32}s-$	
$4118491668266634594476974449713249024752970648722506690592768a^{13}b^{33}s-$	
$2688754491995638583299664671675277468021268599701693901307904a^{12}b^{34}s-$	
$1323693826838758062298434159060167759139628976885676380258304a^{11}b^{35}s-$	

continued on next page

Table D.10.: *continued*

$\nu_T^{(3)}$	T
$4626099682858657476707729069470785743636111958231256211128 32a^{10}b^{36}s-$ $10233498694537058258517196408877619495974312740621456611737 6a^{9}b^{37}s-$ $10772103888986377114228627798818546837867697621706796433408a^{8}b^{38}s$	

E. H_T AND ITS ASSOCIATED QUANTITIES

Table E.1.: The Polynomials A_T

A_T	T
$(a^3-3a^2b-6ab^2-b^3)(a^9-225a^8b-855a^7b^2-1866a^6b^3-2844a^5b^4-3123a^4b^5-2265a^3b^6-981a^2b^7-234ab^8-b^9)$	C_1
$a^8-120a^7b+540a^6b^2-840a^5b^3+1094a^4b^4-840a^3b^5+540a^2b^6-120ab^7+b^8$	C_2
$(a^3-3a^2b-6ab^2-b^3)(a^3+3a^2b-b^3)(a^6+12a^5b+69a^4b^2+88a^3b^3+24a^2b^4-6ab^5+b^6)$	C_3
$(a^4-8a^3b+2a^2b^2+8ab^3+b^4)(a^4+8a^3b+2a^2b^2-8ab^3+b^4)$	C_4
$\frac{1}{2^{20}}(b^{80}-384b^{60}+14336b^{40}+393216b^{20}+1048576)$	C_5
$(a^4+4a^3b-6a^2b^2+4ab^3+b^4)(a^{12}-12a^{11}b+78a^{10}b^2-188a^9b^3+111a^8b^4+264a^7b^5-444a^6b^6+264a^5b^7+$ $111a^4b^8-188a^3b^9+78a^2b^{10}-12ab^{11}+b^{12})$	C_6
$(a^2+ab+b^2)(a^6+11a^5b+30a^4b^2+15a^3b^3-10a^2b^4-5ab^5+b^6)$	C_7
$a^{16}-8a^{14}b^2-228a^{12}b^4+968a^{10}b^6+2630a^8b^8+968a^6b^{10}-228a^4b^{12}-8a^2b^{14}+b^{16}$	C_8
$(a^3+3a^2b-b^3)(a^9+9a^8b+27a^7b^2+48a^6b^3+54a^5b^4+45a^4b^5+27a^3b^6+9a^2b^7-b^9)$	C_9

continued on next page

Table E.1.: *continued*

A_T	T
$\frac{1}{16}(a^{12} + 16a^{11}b + 104a^{10}b^2 + 360a^9b^3 + 720a^8b^4 + 816a^7b^5 + 416a^6b^6 - 96a^5b^7 - 240a^4b^8 - 80a^3b^9 + 64a^2b^{10} + 64ab^{11} + 16b^{12})$	C_{10}
$(a^4 - 2a^3b - 2ab^3 + b^4)(a^{12} - 6a^{11}b + 12a^{10}b^2 - 14a^9b^3 + 3a^8b^4 + 12a^7b^5 - 24a^6b^6 + 12a^5b^7 + 3a^4b^8 - 14a^3b^9 + 12a^2b^{10} - 6ab^{11} + b^{12})$	C_{12}
$a^8 + 60a^6b^2 + 134a^4b^4 + 60a^2b^6 + b^8$	$C_2 \times C_2$
$(a^4 - 2a^3b + 2a^2b^2 + 2ab^3 + b^4)(a^4 + 2a^3b + 2a^2b^2 - 2ab^3 + b^4)$	$C_2 \times C_4$
$(a^4 - 2a^3b + 6a^2b^2 - 2ab^3 + b^4)(a^{12} - 6a^{11}b + 6a^{10}b^2 + 10a^9b^3 + 15a^8b^4 - 36a^7b^5 + 84a^6b^6 - 36a^5b^7 + 15a^4b^8 + 10a^3b^9 + 6a^2b^{10} - 6ab^{11} + b^{12})$	$C_2 \times C_6$
$a^{16} - 8a^{14}b^2 + 12a^{12}b^4 + 8a^{10}b^6 + 230a^8b^8 + 8a^6b^{10} + 12a^4b^{12} - 8a^2b^{14} + b^{16}$	$C_2 \times C_8$

Table E.2.: The Polynomials B_T

B_T	T
$-(a^{18} + 522a^{17}b - 8433a^{16}b^2 - 56382a^{15}b^3 - 174843a^{14}b^4 - 433494a^{13}b^5 - 1084008a^{12}b^6 - 2541474a^{11}b^7 - 4836168a^{10}b^8 - 7036328a^9b^9 - 7787457a^8b^{10} - 6599304a^7b^{11} - 4265121a^6b^{12} - 2050470a^5b^{13} - 692973a^4b^{14} - 148722a^3b^{15} - 17154a^2b^{16} - 504ab^{17} + b^{18})$	C_1

continued on next page

Table E.2.: *continued*

B_T	T
$-(a^4-12a^3b+6a^2b^2-12ab^3+b^4)(a^8+264a^7b-996a^6b^2+1848a^5b^3-1978a^4b^4+1848a^3b^5-996a^2b^6+264ab^7+b^8)$	C_2
$-(a^6+12a^5b+15a^4b^2-20a^3b^3-30a^2b^4-6ab^5+b^6)(a^{12}+6a^{11}b+48a^{10}b^2+428a^9b^3+1899a^8b^4+3636a^7b^5+3030a^6b^6+720a^5b^7-288a^4b^8-58a^3b^9+48a^2b^{10}+6ab^{11}+b^{12})$	C_3
$-(a^2-2ab-b^2)(a^2+2ab-b^2)(a^8+132a^6b^2-250a^4b^4+132a^2b^6+b^8)$	C_4
$-\frac{1}{2^{30}}(b^4-2b^2+2)(b^4+2b^2+2)(b^{16}-2b^{14}+2b^{12}-4b^8+8b^4-16b^2+16)(b^{16}+2b^{14}+2b^{12}-4b^8+8b^4+16b^2+16)(b^{80}-576b^{60}+75776b^{40}+589824b^{20}+1048576)$	C_5
$-(a^8-4a^7b+4a^6b^2+20a^5b^3-26a^4b^4+20a^3b^5+4a^2b^6-4ab^7+b^8)(a^{16}-8a^{15}b+24a^{14}b^2-568a^{13}b^3+2684a^{12}b^4-4776a^{11}b^5+2344a^{10}b^6+4840a^9b^7-8826a^8b^8+4840a^7b^9+2344a^6b^{10}-4776a^5b^{11}+2684a^4b^{12}-568a^3b^{13}+24a^2b^{14}-8ab^{15}+b^{16})$	C_6
$-(a^{12}+18a^{11}b+117a^{10}b^2+354a^9b^3+570a^8b^4+486a^7b^5+273a^6b^6+222a^5b^7+174a^4b^8+46a^3b^9-15a^2b^{10}-6ab^{11}+b^{12})$	C_7
$-(a^8-4a^6b^2-26a^4b^4-4a^2b^6+b^8)(a^{16}-8a^{14}b^2+540a^{12}b^4-2104a^{10}b^6-5050a^8b^8-2104a^6b^{10}+540a^4b^{12}-8a^2b^{14}+b^{16})$	C_8
$-(a^{18}+18a^{17}b+135a^{16}b^2+570a^{15}b^3+1557a^{14}b^4+2970a^{13}b^5+4128a^{12}b^6+4230a^{11}b^7+3240a^{10}b^8+2032a^9b^9+1359a^8b^{10}+1080a^7b^{11}+735a^6b^{12}+306a^5b^{13}+27a^4b^{14}-42a^3b^{15}-18a^2b^{16}+b^{18})$	C_9

continued on next page

Table E.2.: *continued*

B_T	T
$-\frac{1}{64}(a^2+2ab+2b^2)(a^4+6a^3b+6a^2b^2-4ab^3-4b^4)(a^4+6a^3b+12a^2b^2+8ab^3+2b^4)(a^8+10a^7b+32a^6b^2+40a^5b^3+14a^4b^4+8a^2b^6-4b^8)$	C_{10}
$-(a^8-4a^7b+4a^6b^2-4a^5b^3-2a^4b^4-4a^3b^5+4a^2b^6-4ab^7+b^8)(a^{16}-8a^{15}b+24a^{14}b^2-40a^{13}b^3+44a^{12}b^4-24a^{11}b^5-32a^{10}b^6+88a^9b^7-114a^8b^8+88a^7b^9-32a^6b^{10}-24a^5b^{11}+44a^4b^{12}-40a^3b^{13}+24a^2b^{14}-8ab^{15}+b^{16})$	C_{12}
$-(a^4+6a^2b^2+b^4)(a^4-12a^3b+6a^2b^2-12ab^3+b^4)(a^4+12a^3b+6a^2b^2+12ab^3+b^4)$	$C_2\times C_2$
$-(a^2-2ab-b^2)(a^2+2ab-b^2)(a^4+b^4)(a^4+6a^2b^2+b^4)$	$C_2\times C_4$
$-(a^8-4a^7b+4a^6b^2-28a^5b^3+22a^4b^4-28a^3b^5+4a^2b^6-4ab^7+b^8)(a^8-4a^7b+4a^6b^2-4a^5b^3-2a^4b^4-4a^3b^5+4a^2b^6-4ab^7+b^8)(a^8-4a^7b+4a^6b^2+20a^5b^3-26a^4b^4+20a^3b^5+4a^2b^6-4ab^7+b^8)$	$C_2\times C_6$
$-(a^8-4a^6b^2-26a^4b^4-4a^2b^6+b^8)(a^8-4a^6b^2-2a^4b^4-4a^2b^6+b^8)(a^8-4a^6b^2+22a^4b^4-4a^2b^6+b^8)$	$C_2\times C_8$

Table E.3.: The Polynomials D_T

D_T	T
$-ab(a+b)(a^2+ab+b^2)^3(a^3+6a^2b+3ab^2-b^3)^9$	C_1
$-\frac{1}{2}ab(a-b)^4(a+b)^{16}(a^2+b^2)$	C_2
$-(ab)^3(a+b)^3(a^2+ab+b^2)^9(a^3+6a^2b+3ab^2-b^3)^3$	C_3

continued on next page

Table E.3.: *continued*

D_T	T
$-\frac{1}{4}b^2a^2(a-b)^2(a+b)^2(a^2+b^2)^8$	C_4
$\frac{1}{2^{35}}b^{100}(b^8-2b^4-4)(b^{16}-4b^{12}+16b^8-24b^4+16)(b^{16}+6b^{12}+16b^8+16b^4+16)$	C_5
$(a+b)^2(ab)^3(a-b)^6(a^2-ab+b^2)(a^2-4ab+b^2)^4(a^2+b^2)^{12}$	C_6
$-(ab)^7(a+b)^7(a^3+8a^2b+5ab^2-b^3)$	C_7
$-(ab)^4(a-b)^{16}(a+b)^{16}(a^2-2ab-b^2)(a^2+2ab-b^2)(a^2+b^2)^2$	C_8
$-(ab)^9(a+b)^9(a^2+ab+b^2)^3(a^3+6a^2b+3ab^2-b^3)$	C_9
$\left(\frac{1}{4096}\right)a^5b^{10}(a+2b)^5(a+b)^{10}(a^2+6ab+4b^2)(a^2+ab-b^2)^2$	C_{10}
$(ab)^{12}(a+b)^2(a-b)^6(a^2-4ab+b^2)(a^2+b^2)^3(a^2-ab+b^2)^4$	C_{12}
$\left(\frac{1}{4}\right)(ab)^2(a-b)^8(a+b)^8(a^2+b^2)^2$	$C_2\times C_2$
$\left(\frac{1}{16}\right)(ab)^4(a-b)^4(a+b)^4(a^2+b^2)^4$	$C_2\times C_4$
$(ab)^6(a+b)^4(a-b)^{12}(a^2-4ab+b^2)^2(a^2-ab+b^2)^2(a^2+b^2)^6$	$C_2\times C_6$
$(ab)^8(a-b)^8(a+b)^8(a^2-2ab-b^2)^2(a^2+2ab-b^2)^2(a^2+b^2)^4$	$C_2\times C_8$

Table E.4.: The Polynomials $\hat{D}_T$

$\hat{D}_T$	T
$(a+b)(a^2+ab+b^2)(-a^3-6a^2b-3ab^2+b^3)$	C_1, C_3, C_9
$(a+b)(-a+b)(a^2+b^2)$	$C_2, C_4, C_2\times C_2, C_2\times C_4$
$\frac{1}{2^9 5}(b^8-2b^4-4)(b^{16}-4b^{12}+16b^8-24b^4+16)(b^{16}+6b^{12}+16b^8+16b^4+16)$	$C_5 6$
$(a+b)(-a+b)(a^2+b^2)(a^2-ab+b^2)(a^2-4ab+b^2)$	$C_6, C_{12}, C_2\times C_6$
$(a+b)(-a^3-8a^2b-5ab^2+b^3)$	C_7
$(a+b)(-a+b)(a^2-2ab-b^2)(a^2+2ab-b^2)(a^2+b^2)$	$C_8, C_2\times C_8$
$\frac{1}{8}(a+b)(a+2b)(a^2+6ab+4b^2)(-a^2-ab+b^2)$	C_{10}

Table E.5.: The Polynomials μ_T

μ_T	T
$-114130130479a^{17}r + 1879115953389a^{16}br + 16153551884991a^{15}b^2r + 55924236165662a^{14}b^3r + 141543993170631a^{13}b^4r + 349960470393840a^{12}b^5r + 837732735445061a^{11}b^6r + 1677524536313028a^{10}b^7r + 2590462038128166a^9b^8r + 3033318243388525a^8b^9r + 2707700169632052a^7b^{10}r + 1839634739518686a^6b^{11}r + 930071439811837a^5b^{12}r + 331173637331595a^4b^{13}r + 74493869821257a^3b^{14}r + 9004572709072a^2b^{15}r + 269171877150ab^{16}r - 533493693b^{17}r + 533493693a^{17}s + 278241269931a^{16}bs - 4625267532424a^{15}b^2s - 27911319845583a^{14}b^3s - 81733628093217a^{13}b^4s - 200130199006987a^{12}b^5s - 503449029251016a^{11}b^6s - 1165691591034717a^{10}b^7s - 2148524674558036a^9b^8s - 2999858097459078a^8b^9s - 3177872505023688a^7b^{10}s - 2573564131084052a^6b^{11}s - 1583462122040823a^5b^{12}s - 719314025130417a^4b^{13}s - 226783462679054a^3b^{14}s - 44900351509017a^2b^{15}s - 4633366624314ab^{16}s - 1061786394386b^{17}s$	C_1
$-24090947a^{11}r + 485642118a^{10}br - 1833566112a^9b^2r + 4021108998a^8b^3r - 5922733858a^7b^4r + 7097059764a^6b^5r - 5972936796a^5b^6r + 4084023444a^4b^7r - 1892608403a^3b^8r + 514528710a^2b^9r - 31233420ab^{10}r - 123930b^{11}r - 123930a^{11}s - 31233420a^{10}bs + 514528710a^9b^2s - 1892608403a^8b^3s + 4084023444a^7b^4s - 5972936796a^6b^5s + 7097059764a^5b^6s - 5922733858a^4b^7s + 4021108998a^3b^8s - 1833566112a^2b^9s + 485642118ab^{10}s - 24090947b^{11}s$	C_2

continued on next page

Table E.5.: *continued*

μ_T	T
$-35154907a^{17}r - 202968591a^{16}br - 1812357657a^{15}b^2r - 15460281946a^{14}b^3r - 74774519625a^{13}b^4r - 177010427664a^{12}b^5r - 145839060655a^{11}b^6r + 172229805180a^{10}b^7r + 480796864254a^9b^8r + 395661570505a^8b^9r + 104012269368a^7b^{10}r - 27178558650a^6b^{11}r - 11598276815a^5b^{12}r + 4408967415a^4b^{13}r + 1750560345a^3b^{14}r + 57702256a^2b^{15}r + 721638ab^{16}r - 3229353b^{17}r + 3229353a^{17}s + 55620639a^{16}bs + 393035960a^{15}b^2s + 3167583105a^{14}b^3s + 22130117955a^{13}b^4s + 85428229229a^{12}b^5s + 145658752152a^{11}b^6s + 24139828863a^{10}b^7s - 262167622540a^9b^8s - 357219306846a^8b^9s - 163228989744a^7b^{10}s + 5645656744a^6b^{11}s + 18303633069a^5b^{12}s - 2440094445a^4b^{13}s - 2407000670a^3b^{14}s - 135348369a^2b^{15}s - 9364914ab^{16}s - 1533206b^{17}s$	C_3
$93983a^{10}r - 966168a^8b^2r + 1729162a^6b^4r - 1052844a^4b^6r + 128591a^2b^8r + 1020b^{10}r + 1020a^{10}s + 128591a^8b^2s - 1052844a^6b^4s + 1729162a^4b^6s - 966168a^2b^8s + 93983b^{10}s$	C_4
$3272605696b^{100} - 1894986547200b^{80} + 257107479756800b^{60} - 7834020347904400b^{40} + 25982009520160768Ob^{20} + 1184411517626351616$	C_5

continued on next page

Table E.5.: *continued*

μ_T	T
$682119803a^{23}r - 919193900a^{22}br + 17459253962a^{21}b^2r - 205653618960a^{20}b^3r + 900104856528a^{19}b^4r - 1354020329592a^{18}b^5r - 1778236419126a^{17}b^6r + 10085409866076a^{16}b^7r - 15863389091982a^{15}b^8r + 6907877049952a^{14}b^9r + 14152590910268a^{13}b^{10}r - 26842553969624a^{12}b^{11}r + 16625970593916a^{11}b^{12}r + 4521465435816a^{10}b^{13}r - 15447859427652a^9b^{14}r + 11086657189440a^8b^{15}r - 2697140213877a^7b^{16}r - 1085042438964a^6b^{17}r + 965263679738a^5b^{18}r - 278063951000a^4b^{19}r + 38772818876a^3b^{20}r - 3413180976a^2b^{21}r + 688548858ab^{22}r - 57731100b^{23}r - 57731100a^{23}s + 688548858a^{22}bs - 3413180976a^{21}b^2s + 38772818876a^{20}b^3s - 278063951000a^{19}b^4s + 965263679738a^{18}b^5s - 1085042438964a^{17}b^6s - 2697140213877a^{16}b^7s + 11086657189440a^{15}b^8s - 15447859427652a^{14}b^9s + 4521465435816a^{13}b^{10}s + 16625970593916a^{12}b^{11}s - 26842553969624a^{11}b^{12}s + 14152590910268a^{10}b^{13}s + 6907877049952a^9b^{14}s - 15863389091982a^8b^{15}s + 10085409866076a^7b^{16}s - 1778236419126a^6b^{17}s - 1354020329592a^5b^{18}s + 900104856528a^4b^{19}s - 205653618960a^3b^{20}s + 17459253962a^2b^{21}s - 919193900ab^{22}s + 682119803b^{23}s$	C_6
$575487a^{11}r + 6305919a^{10}br + 23351603a^9b^2r + 42322212a^8b^3r + 38254845a^7b^4r + 20778709a^6b^5r + 16599205a^5b^6r + 14193432a^4b^7r + 4196345a^3b^8r - 1184537a^2b^9r - 538213ab^{10}r + 86718b^{11}r - 86718a^{11}s - 1492111a^{10}bs - 8967083a^9b^2s - 23670877a^8b^3s - 31181840a^7b^4s - 18844497a^6b^5s - 10691961a^5b^6s - 12066603a^4b^7s - 6273544a^3b^8s + 204867a^2b^9s + 693257ab^{10}s - 63181b^{11}s$	C_7

continued on next page

Table E.5.: *continued*

μ_T	T
$-2831841a^{22}r + 327794784a^{20}b^2r - 13441903864a^{18}b^4r + 9358164944a^{16}b^6r + 349776251370a^{14}b^8r + 598346451208a^{12}b^{10}r + 260177870716a^{10}b^{12}r - 42177388712a^8b^{14}r - 15008226033a^6b^{16}r + 2050586840a^4b^{18}r - 44679196a^2b^{20}r + 3767064b^{22}r + 3767064a^{22}s - 44679196a^{20}b^2s + 2050586840a^{18}b^4s - 15008226033a^{16}b^6s - 42177388712a^{14}b^8s + 260177870716a^{12}b^{10}s + 598346451208a^{10}b^{12}s + 349776251370a^8b^{14}s + 9358164944a^6b^{16}s - 13441903864a^4b^{18}s + 327794784a^2b^{20}s - 2831841b^{22}s$	C_8
$6344929a^{17}r + 80947617a^{16}br + 433546551a^{15}b^2r + 1355696806a^{14}b^3r + 2820215667a^{13}b^4r + 4177124136a^{12}b^5r + 4488727213a^{11}b^6r + 3536970804a^{10}b^7r + 2208303306a^9b^8r + 1437637049a^8b^9r + 1160606676a^7b^{10}r + 828596070a^6b^{11}r + 366718037a^5b^{12}r + 42424647a^4b^{13}r - 47126079a^3b^{14}r - 22022128a^2b^{15}r - 244494ab^{16}r + 1226439b^{17}r - 1226439a^{17}s - 21093957a^{16}bs - 148685480a^{15}b^2s - 580111959a^{14}b^3s - 1445707773a^{13}b^4s - 2487390935a^{12}b^5s - 3077148984a^{11}b^6s - 2734457013a^{10}b^7s - 1797411572a^9b^8s - 1065165066a^8b^9s - 822495528a^7b^{10}s - 671480020a^6b^{11}s - 367882251a^5b^{12}s - 83911401a^4b^{13}s + 32212634a^3b^{14}s + 25088703a^2b^{15}s + 1969182ab^{16}s - 1509634b^{17}s$	C_9

continued on next page

Table E.5.: *continued*

μ_T	T
$-5450595200a^{17}r - 118263203840a^{16}br - 1110096237568a^{15}b^2r - 5946924160000a^{14}b^3r - 20135061882880a^{13}b^4r - 44774922321920a^{12}b^5r - 64885773967360a^{11}b^6r - 56146674941952a^{10}b^7r - 17430776832000a^9b^8r + 18463829319680a^8b^9r + 26213937479680a^7b^{10}r + 17575902085120a^6b^{11}r + 11086826151936a^5b^{12}r + 6294386769920a^4b^{13}r + 804605788160a^3b^{14}r - 1615886417920a^2b^{15}r - 980432977920ab^{16}r - 180193591296b^{17}r + 397080a^{17}s + 9230718a^{16}bs + 93107690a^{15}b^2s + 538146080a^{14}b^3s + 1976767720a^{13}b^4s + 4808646995a^{12}b^5s + 7735882352a^{11}b^6s + 7715115160a^{10}b^7s + 3488016520a^9b^8s - 1601855760a^8b^9s - 3443143320a^7b^{10}s - 2471518896a^6b^{11}s - 1479630160a^5b^{12}s - 941873560a^4b^{13}s - 242009480a^3b^{14}s + 195567200a^2b^{15}s + 157390496ab^{16}s + 33657080b^{17}s$	C_{10}

continued on next page

Table E.5.: *continued*

μ_T	T
$59801425a^{23}r - 498478732a^{22}br + 1763578126a^{21}b^2r - 3833741424a^{20}b^3r + 5712942624a^{19}b^4r - 5662023912a^{18}b^5r + 2506276614a^{17}b^6r + 2695845756a^{16}b^7r - 7891460802a^{15}b^8r + 8937869408a^{14}b^9r - 7508885252a^{13}b^{10}r + 5561847368a^{12}b^{11}r - 6692907948a^{11}b^{12}r + 8535806280a^{10}b^{13}r - 8973743052a^9b^{14}r + 4990776816a^8b^{15}r + 475494897a^7b^{16}r - 4710102372a^6b^{17}r + 5977463950a^5b^{18}r - 4698460024a^4b^{19}r + 2560049188a^3b^{20}r - 929362368a^2b^{21}r + 191919774ab^{22}r - 16368060b^{23}r - 16368060a^{23}s + 191919774a^{22}bs - 929362368a^{21}b^2s + 2560049188a^{20}b^3s - 4698460024a^{19}b^4s + 5977463950a^{18}b^5s - 4710102372a^{17}b^6s + 475494897a^{16}b^7s + 4990776816a^{15}b^8s - 8973743052a^{14}b^9s + 8535806280a^{13}b^{10}s - 6692907948a^{12}b^{11}s + 5561847368a^{11}b^{12}s - 7508885252a^{10}b^{13}s + 8937869408a^9b^{14}s - 7891460802a^8b^{15}s + 2695845756a^7b^{16}s + 2506276614a^6b^{17}s - 5662023912a^5b^{18}s + 5712942624a^4b^{19}s - 3833741424a^3b^{20}s + 1763578126a^2b^{21}s - 498478732ab^{22}s + 59801425b^{23}s$	C_{12}
$93983a^{10}r + 966168a^8b^2r + 1729162a^6b^4r + 1052844a^4b^6r + 128591a^2b^8r - 1020b^{10}r - 1020a^{10}s + 128591a^8b^2s + 1052844a^6b^4s + 1729162a^4b^6s + 966168a^2b^8s + 93983b^{10}s$	$C_2 \times C_2$
$395a^8r + 430a^4b^4r - 13b^8r - 13a^8s + 430a^4b^4s + 395b^8s$	$C_2 \times C_4$

continued on next page

Table E.5.: *continued*

μ_T	T
$77229967a^{23}r - 559400692a^{22}br + 1934924194a^{21}b^2r - 3847800240a^{20}b^3r + 6362709936a^{19}b^4r - 3330327288a^{18}b^5r - 27997244046a^{17}b^6r + 88725852372a^{16}b^7r - 175472596662a^{15}b^8r + 187429833680a^{14}b^9r - 170779788116a^{13}b^{10}r + 116573201816a^{12}b^{11}r - 159390898500a^{11}b^{12}r + 184171173912a^{10}b^{13}r - 189082516596a^9b^{14}r + 111669989328a^8b^{15}r - 43675377441a^7b^{16}r + 2754240132a^6b^{17}r + 5945187250a^5b^{18}r - 4581750856a^4b^{19}r + 2455843612a^3b^{20}r - 877585152a^2b^{21}r + 178839426ab^{22}r - 15102660b^{23}r - 15102660a^{23}s + 178839426a^{22}bs - 877585152a^{21}b^2s + 2455843612a^{20}b^3s - 4581750856a^{19}b^4s + 5945187250a^{18}b^5s + 2754240132a^{17}b^6s - 43675377441a^{16}b^7s + 111669989328a^{15}b^8s - 189082516596a^{14}b^9s + 184171173912a^{13}b^{10}s - 159390898500a^{12}b^{11}s + 116573201816a^{11}b^{12}s - 170779788116a^{10}b^{13}s + 187429833680a^9b^{14}s - 175472596662a^8b^{15}s + 88725852372a^7b^{16}s - 27997244046a^6b^{17}s - 3330327288a^5b^{18}s + 6362709936a^4b^{19}s - 3847800240a^3b^{20}s + 1934924194a^2b^{21}s - 559400692ab^{22}s + 77229967b^{23}s$	$C_2 \times C_6$
$898107a^{22}r - 3299040a^{20}b^2r + 8611016a^{18}b^4r + 35391632a^{16}b^6r - 233604750a^{14}b^8r - 132897944a^{12}b^{10}r - 214250660a^{10}b^{12}r + 59575864a^8b^{14}r + 2488299a^6b^{16}r - 4302472a^4b^{18}r + 1256708a^2b^{20}r - 105672b^{22}r - 105672a^{22}s + 1256708a^{20}b^2s - 4302472a^{18}b^4s + 2488299a^{16}b^6s + 59575864a^{14}b^8s - 214250660a^{12}b^{10}s - 132897944a^{10}b^{12}s - 233604750a^8b^{14}s + 35391632a^6b^{16}s + 8611016a^4b^{18}s - 3299040a^2b^{20}s + 898107b^{22}s$	$C_2 \times C_8$

Table E.6.: The Polynomials ν_T

ν_T	T
$53235520769a^{11}r+111843861183a^{10}br-504030111156a^9b^2r-2531536786203a^8b^3r-5979244668579a^7b^4r-9579118186629a^6b^5r-10889855965245a^5b^6r-8400858961140a^4b^7r-4095789366321a^3b^8r-1204415466302a^2b^9r-127747430442ab^{10}r-533493693b^{11}r+533493693a^{11}s-121878999819a^{10}bs-43716685003a^9b^2s+1083341919852a^8b^3s+3839862083094a^7b^4s+7824467368461a^6b^5s+11104286433957a^5b^6s+10998756063243a^4b^7s+7203713774874a^3b^8s+3034055120643a^2b^9s+722013862806ab^{10}s+61187011810b^{11}s$	C_1
$13657789a^7r-65207070a^6br+101536650a^5b^2r-133583730a^4b^3r+102581797a^3b^4r-66556110a^2b^5r+14868540ab^6r-123930b^7r-123930a^7s+14868540a^6bs-66556110a^5b^2s+102581797a^4b^3s-133583730a^3b^4s+101536650a^2b^5s-65207070ab^6s+13657789b^7s$	C_2
$-26651851a^{11}r-145094157a^{10}br+63348984a^9b^2r+2839989297a^8b^3r+7392585681a^7b^4r+6405656391a^6b^5r+296390535a^5b^6r-2109182580a^4b^7r-692959401a^3b^8r+38326138a^2b^9r+721638ab^{10}r-3229353b^{11}r+3229353a^{11}s+36244521a^{10}bs+146504657a^9b^2s-472577688a^8b^3s-3661950546a^7b^4s-5918085159a^6b^5s-2295484983a^5b^6s+1512531063a^4b^7s+1017308274a^3b^8s+8507403a^2b^9s-9364914ab^{10}s+6969850b^{11}s$	C_3
$-53473a^6r+132450a^4b^2r-61129a^2b^4r+1020b^6r+1020a^6s-61129a^4b^2s+132450a^2b^4s-53473b^6s$	C_4
$3351148232704b^{60}-1297045763653632b^{40}+51992606342643712b^{20}+1159078769722392576$	C_5

continued on next page

Table E.6.: *continued*

ν_T	T
$342381179a^{15}r - 2267578176a^{14}br - 6570128418a^{13}b^2r + 57698482892a^{12}b^3r - 120333533178a^{11}b^4r + 54119037948a^{10}b^5r + 142846493010a^9b^6r - 276592045944a^8b^7r + 167051195475a^7b^8r + 33007126988a^6b^9r - 118432373154a^5b^{10}r + 65892347832a^4b^{11}r - 11647576732a^3b^{12}r - 1351758744a^2b^{13}r + 457624458ab^{14}r - 57731100b^{15}r - 57731100a^{15}s + 457624458a^{14}bs - 1351758744a^{13}b^2s - 11647576732a^{12}b^3s + 65892347832a^{11}b^4s - 118432373154a^{10}b^5s + 33007126988a^9b^6s + 167051195475a^8b^7s - 276592045944a^7b^8s + 142846493010a^6b^9s + 54119037948a^5b^{10}s - 120333533178a^4b^{11}s + 57698482892a^3b^{12}s - 6570128418a^2b^{13}s - 2267578176ab^{14}s + 342381179b^{15}s$	C_6
$574479a^7r + 2871141a^6br + 4298504a^5b^2r + 2955183a^4b^3r + 207018a^3b^4r - 1133629a^2b^5r - 364777ab^6r + 86718b^7r - 86718a^7s - 971803a^6bs - 2876111a^5b^2s - 2631622a^4b^3s - 1121491a^3b^4s + 718620a^2b^5s + 560847ab^6s - 64189b^7s$	C_7
$-40580577a^{14}r - 136517412a^{12}b^2r + 5100183710a^{10}b^4r + 10398531868a^8b^6r + 3526086071a^6b^8r - 863018408a^4b^{10}r - 29610940a^2b^{12}r + 3767064b^{14}r + 3767064a^{14}s - 29610940a^{12}b^2s - 863018408a^{10}b^4s + 3526086071a^8b^6s + 10398531868a^6b^8s + 5100183710a^4b^{10}s - 136517412a^2b^{12}s - 40580577b^{14}s$	C_8

continued on next page

Table E.6.: *continued*

ν_T	T
$6343633a^{11}r + 42901371a^{10}br + 118928988a^9b^2r + 193299969a^8b^3r + 194946777a^7b^4r + 130399407a^6b^5r + 47235375a^5b^6r - 15865380a^4b^7r - 31422897a^3b^8r - 14663494a^2b^9r - 244494ab^{10}r + 1226439b^{11}r - 1226439a^{11}s - 13735323a^{10}bs - 55235591a^9b^2s - 112816116a^8b^3s - 141696162a^7b^4s - 107773143a^6b^5s - 54123471a^5b^6s - 1302489a^4b^7s + 22838418a^3b^8s + 16007571a^2b^9s + 1969182ab^{10}s - 1510930b^{11}s$	C_9
$-21802357760a^{11}r - 298634321920a^{10}br - 1615259717632a^9b^2r - 4456911294464a^8b^3r - 6606908653568a^7b^4r - 4627575914496a^6b^5r - 72345935872a^5b^6r + 2082365374464a^4b^7r + 1105711464448a^3b^8r - 375794827264a^2b^9r - 620045795328ab^{10}r - 180193591296b^{11}r + 1588320a^{11}s + 24216312a^{10}bs + 146933864a^9b^2s + 461020768a^8b^3s + 795901216a^7b^4s + 695579052a^6b^5s + 135672736a^5b^6s - 255080848a^4b^7s - 188721936a^3b^8s + 15423168a^2b^9s + 90074176ab^{10}s + 33657440b^{11}s$	C_{10}
$59791057a^{15}r - 259397448a^{14}br + 486409386a^{13}b^2r - 613091684a^{12}b^3r + 390087786a^{11}b^4r - 9426516a^{10}b^5r - 511385850a^9b^6r + 522470208a^8b^7r - 600862695a^7b^8r + 195927724a^6b^9r + 237104778a^5b^{10}r - 567458664a^4b^{11}r + 556386844a^3b^{12}r - 358099992a^2b^{13}r + 126447534ab^{14}r - 16368060b^{15}r - 16368060a^{15}s + 126447534a^{14}bs - 358099992a^{13}b^2s + 556386844a^{12}b^3s - 567458664a^{11}b^4s + 237104778a^{10}b^5s + 195927724a^9b^6s - 600862695a^8b^7s + 522470208a^7b^8s - 511385850a^6b^9s - 9426516a^5b^{10}s + 390087786a^4b^{11}s - 613091684a^3b^{12}s + 486409386a^2b^{13}s - 259397448ab^{14}s + 59791057b^{15}s$	C_{12}
$-53473a^6r - 132450a^4b^2r - 61129a^2b^4r - 1020b^6r - 1020a^6s - 61129a^4b^2s - 132450a^2b^4s - 53473b^6s$	$C_2 \times C_2$

continued on next page

Table E.6.: *continued*

ν_T	T
$-181a^4r - 13b^4r - 13a^4s - 181b^4s$	$C_2 \times C_4$
$75902863a^{15}r - 266406072a^{14}br + 512604294a^{13}b^2r - 651100796a^{12}b^3r - 81817626a^{11}b^4r - 2576280204a^{10}b^5r + 5107433130a^9b^6r - 9218890368a^8b^7r + 6096091335a^7b^8r - 3455358764a^6b^9r + 264746742a^5b^{10}r - 572882136a^4b^{11}r + 547880356a^3b^{12}r - 343459368a^2b^{13}r + 118428786ab^{14}r - 15102660b^{15}r - 15102660a^{15}s + 118428786a^{14}bs - 343459368a^{13}b^2s + 547880356a^{12}b^3s - 572882136a^{11}b^4s + 264746742a^{10}b^5s - 3455358764a^9b^6s + 6096091335a^8b^7s - 9218890368a^7b^8s + 5107433130a^6b^9s - 2576280204a^5b^{10}s - 81817626a^4b^{11}s - 651100796a^3b^{12}s + 512604294a^2b^{13}s - 266406072ab^{14}s + 75902863b^{15}s$	$C_2 \times C_6$
$750651a^{14}r - 1476084a^{12}b^2r - 3459730a^{10}b^4r - 24403124a^8b^6r - 977293a^6b^8r - 1177736a^4b^{10}r + 834020a^2b^{12}r - 105672b^{14}r - 105672a^{14}s + 834020a^{12}b^2s - 1177736a^{10}b^4s - 977293a^8b^6s - 24403124a^6b^8s - 3459730a^4b^{10}s - 1476084a^2b^{12}s + 750651b^{14}s$	$C_2 \times C_8$

Table E.7.: The Polynomials μ'_T

μ'_T	T
$-288a^4br + 584a^3b^2r - 608a^2b^3r + 584ab^4r - 256b^5r - 256a^5s + 584a^4bs - 608a^3b^2s + 584a^2b^3s - 288ab^4s$	C_2
$20a^2br - 16b^3r - 16a^3s + 20ab^2s$	C_4

continued on next page

Table E.7.: *continued*

μ'_T	T
$2288a^7b^2r - 6704a^6b^3r + 6280a^5b^4r + 712a^4b^5r - 7048a^3b^6r + 6368a^2b^7r - 1536ab^8r - 384b^9r - 384a^9s - 1536a^8bs + 6368a^7b^2s - 7048a^6b^3s + 712a^5b^4s + 6280a^4b^5s - 6704a^3b^6s + 2288a^2b^7s$	C_6

Table E.8.: The Polynomials ν'_T

ν'_T	T
$36a^3r - 433a^2br + 230ab^2r - 457b^3r - 457a^3s + 230a^2bs - 433ab^2s + 36b^3s$	C_2
$-5a^3r + 29ab^2r - 29a^2bs + 5b^3s$	C_4
$286a^7r - 1124a^6br + 1051a^5b^2r + 5842a^4b^3r - 7062a^3b^4r + 4942a^2b^5r + 1677ab^6r - 1372b^7r + 1372a^7s - 1677a^6bs - 4942a^5b^2s + 7062a^4b^3s - 5842a^3b^4s - 1051a^2b^5s + 1124ab^6s - 286b^7s$	C_6

Table E.9.: The values of u_T, r_T, s_T, and w_T

u_T	r_T	s_T	w_T	T
a^{-3}	$\left(-\frac{1}{12}\right)\cdot\left(a^{-6}\cdot(a^6-6a^5b-15a^4b^2-14a^3b^3-6a^2b^4+b^6-1)\right)$	$\left(\frac{1}{2}\right)\cdot\left(a^{-3}\cdot(-a^3+a^2b+2ab^2+b^3+1)\right)$	$\left(-\frac{1}{24}\right)\cdot\left(a^{-9}\cdot(-a^9-5a^8b-25a^7b^2-60a^6b^3-80a^5b^4-61a^4b^5-27a^3b^6-5a^2b^7+2ab^8+b^9+a^3-a^2b-2ab^2-b^3)\right)$	C_1
$2\cdot a^{-2}$	$\left(\frac{1}{3}\right)\cdot\left(a^{-4}\cdot(2a^4-24a^3b+12a^2b^2-24ab^3+2b^4+1)\right)$	$\left(\frac{1}{2}\right)\cdot\left(2\cdot a^{-2}\right)$	0	C_2
a^{-3}	$\left(-\frac{1}{12}\right)\cdot\left(a^{-6}\cdot(-a^3+3a^2b+6ab^2+b^3-1)\cdot(-a^3+3a^2b+6ab^2+b^3+1)\right)$	$\left(-\frac{1}{2}\right)\cdot\left(a^{-3}\cdot(-a^3+3a^2b+6ab^2+b^3-1)\right)$	$\left(\frac{1}{24}\right)\cdot\left(a^{-9}\cdot(-a^9-3a^8b-57a^7b^2-186a^6b^3-120a^5b^4+159a^4b^5+213a^3b^6+69a^2b^7+6ab^8+b^9+a^3-3a^2b-6ab^2-b^3)\right)$	C_3
$\left(\frac{1}{4}\right)\cdot\left((ab)^{-1}\right)$	$\left(-\frac{1}{192}\right)\cdot\left(b^{-2}\cdot a^{-2}\cdot(a^4+18a^2b^2+b^4-1)\right)$	$\left(-\frac{1}{8}\right)\cdot\left(b^{-1}\cdot a^{-1}\cdot(4ab-1)\right)$	$\left(-\frac{1}{384}\right)\cdot\left(b^{-2}\cdot a^{-2}\cdot(2a^4-12a^2b^2+2b^4+1)\right)$	C_4
1	$\left(-\frac{1}{12288}\right)\cdot\left(b^{40}-192b^{20}-4096\right)$	$\left(\frac{1}{64}\right)\cdot\left(b^{20}\right)$	$\left(-\frac{1}{786432}\right)\cdot\left(b^{60}-224b^{40}-10240b^{20}-262144\right)$	C_5

continued on next page

Table E.9.: *continued*

u_T	r_T	s_T	w_T	T
$2\cdot(a^2-4ab+b^2)^{-2}$	$\left(-\frac{1}{3}\right)\cdot\left((a^2-4ab+b^2)^{-4}\cdot(a^8-16a^7b+52a^6b^2-112a^5b^3+166a^4b^4-112a^3b^5+52a^2b^6-16ab^7+b^8-1)\right)$	$(-1)\cdot(a^2-4ab+b^2)^{-2}\cdot(a^4-4a^3b+10a^2b^2-4ab^3+b^4-1)$	$\left(\frac{1}{3}\right)\cdot\left((a^2-4ab+b^2)^{-6}\cdot(a^{12}-8a^{11}b+6a^{10}b^2-40a^9b^3+335a^8b^4-848a^7b^5+1172a^6b^6-848a^5b^7+335a^4b^8-40a^3b^9+6a^2b^{10}-8ab^{11}+b^{12}-a^4+4a^3b-10a^2b^2+4ab^3-b^4)\right)$	C_6
a^{-2}	$\left(-\frac{1}{12}\right)\cdot\left(a^{-4}\cdot(a^4-6a^3b-9a^2b^2-2ab^3+b^4-1)\right)$	$\left(\frac{1}{2}\right)\cdot\left(a^{-2}\cdot(-a^2+ab+b^2+1)\right)$	$\left(-\frac{1}{24}\right)\cdot\left(a^{-6}\cdot(-a^6-5a^5b-20a^4b^2-25a^3b^3-12a^2b^4-ab^5+b^6+a^2-ab-b^2)\right)$	C_7
$(a-b)^{-2}\cdot(a^2+b^2)^{-1}$	$\left(-\frac{1}{12}\right)\cdot\left((a-b)^{-4}\cdot(a^2+b^2)^{-2}\cdot(a^8-12a^7b+20a^6b^2+12a^5b^3+22a^4b^4+12a^3b^5+20a^2b^6-12ab^7+b^8-1)\right)$	$\left(-\frac{1}{2}\right)\cdot\left((a-b)^{-2}\cdot(a^2+b^2)^{-1}\cdot(a^4-4a^3b-2a^2b^2-4ab^3+b^4-1)\right)$	$\left(\frac{1}{24}\right)\cdot\left((a-b)^{-6}\cdot(a^2+b^2)^{-3}\cdot(a^{12}-4a^{11}b+18a^{10}b^2+12a^9b^3-17a^8b^4-264a^7b^5-4a^6b^6-264a^5b^7-17a^4b^8+12a^3b^9+18a^2b^{10}-4ab^{11}+b^{12}-a^4+4a^3b+2a^2b^2+4ab^3-b^4)\right)$	C_8

continued on next page

Table E.9.: *continued*

u_T	r_T	s_T	w_T	T
a^{-3}	$\left(-\frac{1}{12}\right)\cdot a^{-6}\cdot(a^6-6a^5b-15a^4b^2-14a^3b^3-6a^2b^4+b^6-1)$	$\left(\frac{1}{2}\right)\cdot a^{-3}\cdot(-a^3+a^2b+2ab^2+b^3+1)$	$\left(-\frac{1}{24}\right)\cdot a^{-9}\cdot(-a^9-5a^8b-25a^7b^2-60a^6b^3-80a^5b^4-61a^4b^5-27a^3b^6-5a^2b^7+2ab^8+b^9+a^3-a^2b-2ab^2-b^3)$	C_9
$2\cdot a^{-1}\cdot(-a^2-ab+b^2)^{-1}$	$\left(-\frac{1}{12}\right)\cdot a^{-2}\cdot(-a^2-ab+b^2)^{-2}\cdot(a^6-4a^5b-28a^4b^2-40a^3b^3-12a^2b^4+8ab^5+4b^6-4)$	$\left(-\frac{1}{2}\right)\cdot a^{-1}\cdot(-a^2-ab+b^2)^{-1}\cdot(-a^3+4ab^2+2b^3-2)$	$\left(\frac{1}{24}\right)\cdot a^{-3}\cdot(-a^2-ab+b^2)^{-3}\cdot(-a^9-8a^8b-40a^7b^2-130a^6b^3-240a^5b^4-224a^4b^5-72a^3b^6+32a^2b^7+32ab^8+8b^9+4a^3-16ab^2-8b^3)$	C_{10}
$b^{-3}\cdot(a+b)^{-1}$	$\left(-\frac{1}{12}\right)\cdot b^{-6}\cdot(a+b)^{-2}\cdot(a^8-4a^7b+4a^6b^2-4a^5b^3-2a^4b^4+8a^3b^5-8a^2b^6+8ab^7+b^8-1)$	$\left(-\frac{1}{2}\right)\cdot b^{-3}\cdot(a+b)^{-1}\cdot(-a^4+2a^3b-2a^2b^2+2ab^3+b^4-1)$	$\left(\frac{1}{24}\right)\cdot b^{-9}\cdot(a+b)^{-3}\cdot(-a^{12}+6a^{11}b-14a^{10}b^2+22a^9b^3-21a^8b^4+12a^7b^5+12a^6b^6-36a^5b^7+45a^4b^8-34a^3b^9+18a^2b^{10}-2ab^{11}+b^{12}+a^4-2a^3b+2a^2b^2-2ab^3-b^4)$	C_{12}

continued on next page

Table E.9.: *continued*

u_T	r_T	s_T	w_T	T
$2\cdot a^{-2}$	$\left(-\frac{1}{3}\right)\cdot a^{-4}\cdot(a^4-12a^3b+6a^2b^2-12ab^3+b^4-1)$	$\left(\frac{1}{2}\right)\cdot 2\cdot a^{-2}$	0	$C_2\times C_2$
$(a-b)^{-2}$	$\left(-\frac{1}{12}\right)\cdot(a-b)^{-4}\cdot(a^4-6a^3b+6a^2b^2-6ab^3+b^4-1)$	$\left(-\frac{1}{2}\right)\cdot(a-b)^{-2}\cdot(-a+b-1)\cdot(-a+b+1)$	$\left(\frac{1}{24}\right)\cdot(a-b)^{-4}\cdot(a^4+6a^2b^2+b^4-1)$	$C_2\times C_4$
$2\cdot(a+b)^{-2}\cdot(a^2-4ab+b^2)^{-1}$	$\left(-\frac{1}{3}\right)\cdot(a+b)^{-4}\cdot(a^2-4ab+b^2)^{-2}\cdot(a^8-4a^7b-8a^6b^2+20a^5b^3-2a^4b^4+20a^3b^5-8a^2b^6-4ab^7+b^8-1)$	$(-1)\cdot(a+b)^{-2}\cdot(a^2-4ab+b^2)^{-1}\cdot(a^4-2a^3b-2a^2b^2-2ab^3+b^4-1)$	$\left(\frac{1}{3}\right)\cdot(a+b)^{-6}\cdot(a^2-4ab+b^2)^{-3}\cdot(a^{12}-6a^{11}b+10a^{10}b^2-6a^9b^3-17a^8b^4+44a^7b^5-116a^6b^6+44a^5b^7-17a^4b^8-6a^3b^9+10a^2b^{10}-6ab^{11}+b^{12}-a^4+2a^3b+2a^2b^2+2ab^3-b^4)$	$C_2\times C_6$
$a^{-1}\cdot(a+b)^{-1}\cdot(-a^2-2ab+b^2)^{-1}$	$\left(-\frac{1}{12}\right)\cdot a^{-2}\cdot(a+b)^{-2}\cdot(-a^2-2ab+b^2)^{-2}\cdot(a^8+12a^7b+20a^6b^2-2a^4b^4-12a^3b^5-4a^2b^6+b^8-1)$	$\left(-\frac{1}{2}\right)\cdot a^{-1}\cdot(a+b)^{-1}\cdot(-a^2-2ab+b^2)^{-1}\cdot(-a^4-4a^3b+b^4-1)$	$\left(\frac{1}{24}\right)\cdot a^{-3}\cdot(a+b)^{-3}\cdot(-a^2-2ab+b^2)^{-3}\cdot(-a^{12}-4a^{11}b-20a^{10}b^2-32a^9b^3+3a^8b^4+8a^7b^5+24a^6b^6-32a^5b^7-3a^4b^8-4a^3b^9-4a^2b^{10}+b^{12}+a^4+4a^3b-b^4)$	$C_2\times C_8$

Index

REFERENCES

REFERENCES

[1] Joseph Oesterlé. Nouvelles approches du "théorème" de Fermat. *Astérisque*, (161-162):Exp. No. 694, 4, 165–186 (1989), 1988. Séminaire Bourbaki, Vol. 1987/88.

[2] Bart de Smit. *ABC-triples*, 2018. `http://www.math.leidenuniv.nl/ desmit/abc/`.

[3] D. W. Masser. Note on a conjecture of Szpiro. *Astérisque*, (183):19–23, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[4] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[5] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[6] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[7] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[8] Alain Kraus. Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.*, 54(1):75–80, 1989.

[9] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[10] Michael Laska. An algorithm for finding a minimal Weierstrass equation for an elliptic curve. *Math. Comp.*, 38(157):257–260, 1982.

[11] David A. Cox and Walter R. Parry. Torsion in elliptic curves over $k(t)$. *Compositio Math.*, 41(3):337–354, 1980.

[12] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[13] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.

[14] W. W. Stothers. Polynomial identities and Hauptmoduln. *Quart. J. Math. Oxford Ser. (2)*, 32(127):349–370, 1981.

[15] R. C. Mason. Equations over function fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 149–157. Springer, Berlin, 1984.

[16] Serge Lang. Old and new conjectured Diophantine inequalities. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):37–75, 1990.

[17] Greg Martin and Winnie Miao. *abc* triples. *Funct. Approx. Comment. Math.*, 55(2):145–176, 2016.

[18] J. Browkin, M. Filaseta, G. Greaves, and A. Schinzel. Squarefree values of polynomials and the *abc*-conjecture. In *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*, volume 237 of *London Math. Soc. Lecture Note Ser.*, pages 65–85. Cambridge Univ. Press, Cambridge, 1997.

[19] Alan Baker. Experiments on the *abc*-conjecture. *Publ. Math. Debrecen*, 65(3-4):253–260, 2004.

[20] Arnaud Beauville Lucien Szpiro. *Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux*. Société Mathématique de France, Paris, 1981. Astérisque No. 86 (1981) (1981).

[21] Siman Wong. On the density of elliptic curves. *Compositio Math.*, 127(1):23–54, 2001.

[22] Abderrahmane Nitaj. Algorithms for finding good examples for the *abc* and Szpiro conjectures. *Experiment. Math.*, 2(3):223–230, 1993.

[23] Abderrahmane Nitaj. Détermination de courbes elliptiques pour la conjecture de Szpiro. *Acta Arith.*, 85(4):351–376, 1998.

[24] Michael A. Bennett and Soroosh Yazdani. A local version of Szpiro's conjecture. *Exp. Math.*, 21(2):103–116, 2012.

[25] Mohammad Sadek. Discrete logarithms and mordell-weil groups. Cryptology ePrint Archive, Report 2013/660, 2013. https://eprint.iacr.org/2013/660.

[26] The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2013.

[27] William A. Stein and Mark Watkins. A database of elliptic curves—first report. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 267–275. Springer, Berlin, 2002.

[28] Jennifer S. Balakrishnan, Wei Ho, Nathan Kaplan, Simon Spicer, William Stein, and James Weigandt. Databases of elliptic curves ordered by height and distributions of Selmer groups and ranks. *LMS J. Comput. Math.*, 19(suppl. A):351–370, 2016.

[29] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.1)*, 2017. http://www.sagemath.org.

[30] Wolfram Research, Inc. Mathematica, Version 11.2. Champaign, IL, 2017.

[31] Abderrahmane Nitaj. Isogenous of the elliptic curves over the rationals. *J. Comput. Math.*, 20(4):337–348, 2002.

[32] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[33] Raymond Ross. Minimal torsion in isogeny classes of elliptic curves. *Trans. Amer. Math. Soc.*, 344(1):203–215, 1994.

[34] Andrej Dujella and Mirela Jukić Bokun. On the rank of elliptic curves over $\mathbf{Q}(i)$ with torsion group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. *Proc. Japan Acad. Ser. A Math. Sci.*, 86(6):93–96, 2010.

[35] Ken Ono. Euler's concordant forms. *Acta Arith.*, 78(2):101–123, 1996.

[36] De Rong Qiu and Xian Ke Zhang. Explicit classification for torsion subgroups of rational points of elliptic curves. *Acta Math. Sin. (Engl. Ser.)*, 18(3):539–548, 2002.

[37] Gerhard Frey. Some remarks concerning points of finite order on elliptic curves over global fields. *Ark. Mat.*, 15(1):1–19, 1977.

[38] M. Flexor and J. Oesterlé. Sur les points de torsion des courbes elliptiques. *Astérisque*, (183):25–36, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[39] A. Silverberg and Yu. G. Zarhin. Semistable reduction and torsion subgroups of abelian varieties. *Ann. Inst. Fourier (Grenoble)*, 45(2):403–420, 1995.

[40] Houria Baaziz. Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points. *Math. Comp.*, 79(272):2371–2386, 2010.

[41] P. Erdös. Arithmetical properties of polynomials. *J. London Math. Soc.*, 28:416–425, 1953.

[42] Gerhard Frey. Elliptic curves and solutions of $A - B = C$. In *Séminaire de Théorie des Nombres, Paris 1985–86*, volume 71 of *Progr. Math.*, pages 39–51. Birkhäuser Boston, Boston, MA, 1987.

VITA

VITA

Alexander J. Barrios was born in Miami, FL. After graduating from Hialeah High School in 2007, he attended Miami Dade College. In the summer of 2008, he participated in the Math Alliance Research Experience for Undergraduates at the University of Iowa. Through this experience, he received his first exposure to modern mathematics and went on to receive an A.A. in Mathematics in May 2009. He continued his education at Brown University where he received a B.S. in Mathematics in May 2011. During the summer of 2009 and 2010, he participated in the Cornell Summer Math Institute and the Mathematical Sciences Research Institute Undergraduate Program, respectively. Both summer programs were instrumental in his development as a mathematician and led him to pursue doctoral work in number theory at Purdue University, where he began as a graduate student in the fall of 2011. In his time in graduate school, he has had an active role mentoring high school, undergraduate, and graduate students through Purdue Science Bound, the Louis Stokes Alliance for Minority Participation program (LSAMP), Alliance for Graduate Education and the Professoriate (AGEP), Association for Women in Mathematics (AWM), and the Minority Engineering Program (MEP). He has also been the lead instructor for the MEP summer programs for grade 6-12 students since 2014.