The Dissertation Committee for Francisco Xavier Portillo-Bobadilla
Certifies that this is the approved version of the following dissertation:

COMPUTATIONS ON AN EQUATION OF THE BIRCH AND SWINNERTON-DYER TYPE

Committee:

Felipe Voloch, Supervisor

Fernando Rodriguez-Villegas

John Tate

Douglas Ulmer

Jeffrey Vaaler

COMPUTATIONS ON AN EQUATION OF THE BIRCH AND SWINNERTON-DYER TYPE

by

FRANCISCO XAVIER PORTILLO-BOBADILLA, B.S.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

August 2004

I would like to dedicate this thesis to my parents and my *abuelitos*.

Acknowledgments

I would like to thank mainly to my family, who always encourage me and show its support in many different ways, and to my professors, who were very patient and supportive, especially Felipe Voloch and Javier Elizondo. Also, thanks to John Tate for his valuable help in understanding my problem thesis better.

Gracias to my Mom and Dad for giving me all their strength and youth, and also courage and education to succeed in many aspects of my life.

To my brothers: Miguel, Tobías, Alán y Juanito for their examples and love. And, for all the good time, we have shared.

Also, I would like to thank to the many people that have been close to me in some way or another: Laura, to my abuelitos Gloria y Tobías, to mis tías y tíos: Silvia, Armando, Esperanza, Agustín, Chepis, Regino, Gregorio, Pilar, Paco, Mari, etc...

To mis primos also...

And gracias también to my friends, especialmente a la “camarilla” de los “bolivares” y al compa de Tucson. Y a Steve, Iza, Rolando y Mari de Austin y San Marcos, Texas.

Y desde luego, a mi querida Magdalena con mucho amor!

COMPUTATIONS ON AN EQUATION OF THE BIRCH AND SWINNERTON-DYER TYPE

Publication No. ____________________

Francisco Xavier Portillo-Bobadilla, Ph.D.
The University of Texas at Austin, 2004

Supervisor: Felipe Voloch

Let us assume that $E/\mathbb{Q}$ is an elliptic curve of level N and rank equal to 1. Let q be a prime that does not divide the conductor. We study conjecture 4 of B. Mazur and J. Tate in [MT87]. This conjecture relates to the Birch and Swinnerton-Dyer problem in the q-adic case. We produce a lot of numerical evidence towards the conjecture. We also propose a refinement of the conjecture in the rank 1 case in section 2.3.

Table of Contents

List of Tables

Chapter 1

Introduction

B. Mazur and J. Tate in *Refined Conjectures of the Birch and Swinnerton-Dyer Type* postulated a series of conjectures of the BSD-type in terms of finite layers. The hope was to find "functions with adelic type domains of definition and ranges of values" for which the q-adic L functions were only a component, as expressed by Yuri Manin [Man].

In the present work, we show computational evidence related to those conjectures. Our approach is completely experimental and we focus in the special case of elliptic curves with Mordell-Weil rank 1. We concentrate our attention in conjecture 4 in [MT87]. We start by defining the analytic and arithmetic ingredients, then we will present our results and computations.

Our computations are mainly divided in two parts, one which matches the language and ideas in [MT87] and a second part which can be thought as a curiosity in the computation of the arithmetic side or the g function.

Chapter 2

Mazur-Tate Conjecture for rank 1

2.1 Analytic Side

Assume E is an elliptic curve over $\mathbb{Q}$ with conductor N. Consider a Néron differential ω for E. (i.e. a regular differential which extends to a differential on the Néron model of E over $\mathbb{Z}$ and is not zero in the special fiber). Such ω is unique up to sign. Then, by the Néron lattice Λ_E we understand the "periods" $\int_\gamma \omega \in \mathbb{C}$, where γ runs through loops in $E(\mathbb{C})$.

Now, there is a unique pair of positive real numbers Ω_E^+ and Ω_E^- such that one of the two conditions holds:

1. $\Lambda_E = \Omega_E^+\mathbb{Z} + \Omega_E^- i\mathbb{Z}$
2. $\Lambda_E \subset \Omega_E^+\mathbb{Z} + \Omega_E^- i\mathbb{Z}$ is the sub-lattice generated by the complex numbers $a\Omega_E^+ + b\Omega_E^- i$ such that $a - b \equiv 0 \pmod 2$.

In the first case, we will just simply say that Λ_E is rectangular or that we are on the rectangular case, otherwise, we will just say that we are on the non-rectangular case.

Let f be the modular form associated to E, and let a/b be a rational number. We define the modular elements by:

$$2\pi \int_0^\infty f(a/b + it)dt = \Omega_E^+[a/b]_E^+ + \Omega_E^-[a/b]_E^- i. \tag{2.1}$$

If E_1 and E_2 are two elliptic curves in the same isogeny class, we have that:

$$[a/b]_{E_1}^\pm = \Omega_{E_2}^\pm / \Omega_{E_1}^\pm [a/b]_{E_2}^\pm \tag{2.2}$$

Denote $R(E_1, E_2, \pm) = \Omega_{E_2}^\pm / \Omega_{E_1}^\pm$. In our computations, we are going to be concerned only with the plus symbols $(+)$; so from now on, we denote $R(E_1, E_2, +)$ simply by $R(E_1, E_2)$. Also, most of the time the curve E will be clear from the context, so we will simply write Ω^+ and $[a/b]^+$ for Ω_E^+ and $[a/b]_E^+$.

If w is the real period of E, then the value Ω_E^+ is a period in the rectangular case, or half a period in the non-rectangular case. Hence, if w_1 and w_2 are the real periods of E_1 and E_2, respectively; we have the following cases:

$$R(E_2, E_1) = \begin{cases} w_2/w_1 & \text{if } \Delta_{E_1}\Delta_{E_2} > 0 \\ 2w_2/w_1 & \text{if } \Delta_{E_1} < 0 \text{ and } \Delta_{E_2} > 0 \\ \frac{1}{2}w_2/w_1 & \text{if } \Delta_{E_1} > 0 \text{ and } \Delta_{E_2} < 0 \end{cases} \tag{2.3}$$

where Δ_{E_1} and Δ_{E_2} are the discriminants of E_1 and E_2, respectively. Notice that Λ_E is rectangular, if and only if, the discriminant of E is positive.

Hence, to compute the modular elements for all the elliptic curves in an isogeny class, it suffices to compute them for only one curve $\tilde{E}$, and then calculate the ratio $R(\tilde{E}, \_)$ for all the other curves in the class.

For convenience, we use the Strong Weil Curves, as listed in [Cre97], of each class to compute the modular elements. If E is an elliptic curve, we denote E_S the Strong Weil Curve in the class of E.

Definition 2.1.1. For a prime $q \nmid N$ and an elliptic curve E with $rank(E) > 1$ we define the following "multiplicative" modular element:

$$l(q) = \prod_{a=1}^{q-1} a^{[a/q]^+} (\bmod q) \tag{2.4}$$

The values $[a/q]^+$ are integers for $q \nmid N$ if $rank(E) > 1$ [Man72], so the "multiplicative" modular elements are well defined.

Sometimes, it simplifies notation to consider the global multiplicative modular element:

$$l = (l(q))_q \in \prod_{q \nmid N} \mathbb{F}_q^* \tag{2.5}$$

(i.e. l has projection $l(q)$ at the q-coordinate for $q \nmid N$).

2.2 Arithmetic side

Let E_0 be the points of good reduction everywhere in E. Let P, P' be points on E and Q in E_0. For $q \nmid N$ prime, consider the quantity:

$$g(P, Q, P', q) = \frac{d(P' + P)d(P' + Q)}{d(P')d(P' + P + Q)} \ (\bmod q) \tag{2.6}$$

where $d(T)$ is the denominator of the x-coordinate of a point T.

This quantity is well defined (as element of $\mathbb{F}_q^*$) if all the d's are different from zero (mod q). In such a case, we say that the value $g(P, Q, P', q)$ is a good value.

Lemma 2.2.1. *If $Q \in E_0$ and $n_q = \#(E(\mathbb{F}_q))$, then the good values of $g(P, n_q Q, P', q)$ depend only on P and Q.*

Proof. See [MT87], page 733. □

Corollary 2.2.2. *There is a bi-multiplicative function*

$$\hat{g} : E \times E_0 \to \prod_{q \nmid N} \mathbb{F}_q^* \tag{2.7}$$

given by $\hat{g}(P, Q) = g(P, n_q Q, P', q)$ at the q-coordinate ($q \nmid N$) and for some $P' \in E$, assuming there is a P' such that 2.6 is well defined.

Proof. For simplicity, we denote $Q_q = n_q Q$. Now, $g(P_1 + P_2, Q_q, P', q) = g(P_1, Q_q, P', q) g(P_2, Q_q, P' + P_1, q)$ follows directly from the identity:

$$\begin{aligned} &\frac{d(P' + Q_q) d(P' + P_1 + P_2)}{d(P') d(P' + P_1 + P_2 + Q_q)} = \\ &\qquad \frac{d(P' + P_1) d(P' + Q_q)}{d(P' + P_1 + Q_q) d(P')} \frac{d(P' + P_1 + P_2) d(P' + P_1 + Q_q)}{d(P' + P_1 + P_2 + Q_q) d(P' + P_1)} \end{aligned} \tag{2.8}$$

So, taking $P'' = P' + P_1$, in the last fraction of the equation, we obtain:

$$g(P_1 + P_2, Q_q, P', q) = g(P_1, Q_q, P', q) g(P_2, Q_q, P'', q) \tag{2.9}$$

But, since $g(P_2, Q_q, P'', q) = g(P_2, Q_q, P', q)$ does not depend on the choice of P' or P'', we obtain the proposition, provided all terms are well defined.

The only problem with this proof is when $P' + P_1 \in E_q$, in this case $d(P' + P_1)$ will be divisible by q. To avoid this situation, we can take P_2 in place of P_1 and vice-versa. Again, if we also have $P' + P_2 \in E_q$, we conclude that $P_1 \equiv P_2 \bmod q$.

In this case, we can change P' so that the right hand side has no vanishing denominators

But, then all the quantities on 2.8 will be well defined.

So, the function is multiplicative in the first coordinate.

The multiplicativity in the second coordinate follows from the formal symmetry $g(P, Q_q, P', q) = g(Q_q, P, P', q)$. Suppose Q, $Q' \in E_0$, then:

$$\begin{aligned} g(P, Q_q + Q'_q, P', q) =& g(Q_q + Q'_q, P, P', q) \\ =& g(Q_q, P, P', q) g(Q'_q, P, P' + Q_q, q) \\ =& g(P, Q_q, P', q) g(P, Q'_q, P' + Q_q, q) \end{aligned} \tag{2.10}$$

But, multiplicativity follows because $g(P, Q'_q, P' + Q_q, q)$ does not depend on P' by lemma 2.2.1. □

Remark 2.2.1. Notice $\hat{g}(O, Q) = \hat{1} \in \prod_{q \nmid N} \mathbb{F}_q^*$. Now, if T is a point of order m, then: $g(T, Q_q, P', q)^m = g([m]T, Q_q, P', q) = g(O, Q_q, P', q) = 1$, but then the number $g(T, Q_q, P', q)$ will be an m-root mod q for almost all prime q. Hence, $g(T, Q_q, P', q) = \pm 1$ if m is even, or $g(T, Q_q, P', q) = 1$ if m is odd. I still wonder if $\hat{g}(T, Q) = \hat{1} \in \prod_{q \nmid N} \mathbb{F}_q^*$ for every torsion point T. I believe this is the case, because the experimental evidence have shown that the value $g(P, Q_q, P', q)$ does not depend on the generator P of the free part of E. We know that the set of all possible generators is $P + E_{tors}$. So, if for a torsion point T $g(T, Q_q, P', q) = -1$, then we must have also that $\hat{g}(P + T, Q) = -\hat{g}(P, Q)$.

2.3 Mazur-Tate conjecture

Assume E is an elliptic curve of rank 1. We use similar notation as in the previous section. Let E_0 be the everywhere good reduction points of E, and let E_q be fiber of the Néron model of E at q. Denote $E_{ns}(\mathbb{F}_q)$ the non-singular points of $E \pmod q$. Set $N_q := E_q/E_{ns}(\mathbb{F}_q)$ the group of conected components in the fiber.

We would like to compute the order of the cokernel of the natural projection:

$$\phi : E \to \prod_{q \in \wp} N_q \tag{2.11}$$

where q ranges through the set of all primes $\wp$.

By looking at the following exact commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_0 & \longrightarrow & E & \longrightarrow & E/E_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_{q\in\wp} E_{ns}(\mathbb{F}_q) & \longrightarrow & \prod_{q\in\wp} E_q & \longrightarrow & \prod_{q\in\wp} N_q & \longrightarrow & 0
\end{array}$$

we obtain the following formula for the order of the cokernel:

$$\#(coker(\phi)) = \frac{C}{\#(E/E_0)} \tag{2.12}$$

where $C = \#\left(\prod_{q\in\wp} N_q\right) = \prod_{q\in\wp} c_q$ and $c_q = |N_q|$ are the Tamagawa numbers.

Denote E_{tors} the torsion of E. We can explicitly compute the order $\#(E/E_0)$ as the product $\frac{ru}{v}$, where u is the order of torsion in E, v the order of the torsion in E_0, and

$$r = \min\{j : jP + R \in E_0 \text{ and } R \in E_{tors}\} \tag{2.13}$$

and P is any generator of E modulo torsion.

Conjecture 2.3.1. *Case rank* 1 *at good reduction primes.*

Let E *be a curve of rank* 1*, let* P *be a generator of* E *(modulo torsion), and let* Q *be a generator of* E_0 *(modulo torsion), then:*

$$l^{uv} = \hat{g}(P,Q)^{|\text{Ш}||coker(\phi)|} \tag{2.14}$$

where $|\text{Ш}|$ *is the order of the Tate-Shafarevich group.*

This conjecture is slightly stronger than Mazur and Tate conjecture, since they have an extra ζ u-power root of unit in the right side. The computational evidence suggest that such a root of unit is in fact 1, so we don't include it in the formula.

Now, if we exponentiate the above equation by u/v, we obtain the equation:

$$l^{u^2} = \hat{g}(P,Q)^{\frac{C|\text{Ш}|}{r}} \tag{2.15}$$

which in some way looks more like the classical BSD.

2.4 Testing

We tested the above conjecture for the first 300 elliptic curves in the Cremona database [Cre97]. All these cases have trivial Tate-Shafarevich group. The computations of the modular symbols was possible thanks to the program *modsym.gp* by B. Bernardi, B. Perrin-Riou and W. Stein [BPRin] written for running in the Pari Calculator [BC]. Those programs solve the linear algebra to compute the modular symbols as explained in [Man72] and [Cre97].

However, we must point out that the program *modsym.gp* gives the right modular symbols $[a/q]^+$ up to a multiplication by a constant. So, in order to have the correct modular symbols, we just have to determine the constant. Thanks to John Tate who suggested to compute explicitly the integral and to Fernando Rodriguez-Villegas who explained how to get the approximation, we were able to fix this situation. Hence, to correct the value $[a/b]^+$, we assume the aproximation:

$$[a/b]^+ \approx \left(\sum_{i=1}^{\infty} \frac{a_n}{n} cos\left(2\pi n \left(\frac{a}{b}\right)\right)\right) /\Omega^+ \tag{2.16}$$

formally equal to the real part of the integral 2.1. Here, the a_n values are the coefficients of the Fourier expansion of the normalized modular form associated to E. We compare our computations with the ones obtained by *modsym.gp*, to determine the constant. Once this constant is determined, we don't have to use the integral for computing more modular symbols, since this constant is independent from a and b.

We may point out that the above series is equal to $[a/b]^+$ if integration term by term is possible and that we don't have an estimate of the error of this approximation, but we are looking for differences of 0.49 or smaller. In practice, we use the information that we have about the values $[a/b]^+$ computed from *modsym.gp* to say if the series in 2.16 was a good approximation to $[a/b]^+$. What we did was to check many values of $[a/b]^+$. More specifically, for $b = q$ a prime not dividing N. We computed the values $[j/q]^+$ using *modsym.gp* for $1 < j < q - 1$ and we kept the results in a vector with $q - 1$ rational entries. Now , we also approximated the integrals by computing

$$\left(\sum_{i=1}^{\infty} \frac{a_n}{n} cos\left(2\pi n \left(\frac{j}{q}\right)\right)\right) /\Omega^+ \tag{2.17}$$

up to the first $10,000$ terms. We rounded those values to the closest integers, and we also put the results in another vector with $q-1$ entries. If the computation is good enough, these two vectors are multiples of one another. Notice that if the value of any of the integrals in 2.17 differs badly from the actual value, then the vector obtained from the integrals won't be a multiple of the vector with the values $[j/q]^+$ from the program *modsym.gp*. Now, once these vectors are determined, we will have the needed constant.

If we want, we can also double check our results by taking another prime and computing the constant again.

The corrected output from *modsym.gp* for the 300 curves was kept in a big file. This allows to speed up our testing. Also, we computed the g function using some routines that we wrote in Pari. and stored the output in another file.

Now, the following tables contain the information necessary to test 2.3.1.

2.4.1 Tables

Table 1

This table lists all the strong Weil curves up to level 320 with the generators of E and E_0. In this table, N is the conductor, L is the letter type and # is the number type. In the last two columns, we have vectors with points on E and E_0. Those points are the generators for the groups E and E_0, respectively. The first point in each vector is of infinite order. The other points are torsion points.

Table 2.1: Generators of E and E_0.

Table of generators for E and E_0.					
N	L	#	equation	E	E_0
37	1	1	[0, 0, 1, -1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
43	1	1	[0, 1, 1, 0, 0]	[[0, 0, 1]]	[[0, 0, 1]]
53	1	1	[1, -1, 1, 0, 0]	[[0, 0, 1]]	[[0, 0, 1]]
57	1	1	[0, -1, 1, -2, 2]	[[2, -2, 1]]	[[1, -1, 1]]
58	1	1	[1, -1, 0, -1, 1]	[[0, 1, 1]]	[[1, -1, 1]]
61	1	1	[1, 0, 0, -2, 1]	[[1, -1, 1]]	[[1, -1, 1]]
65	1	1	[1, 0, 0, -1, 0]	[[-1, 1, 1], [0, 0, 1]]	[[-1, 1, 1], [0, 0, 1]]
77	1	1	[0, 0, 1, 2, 0]	[[2, 3, 1]]	[[0, 0, 1]]
79	1	1	[1, 1, 1, -2, 0]	[[0, 0, 1]]	[[0, 0, 1]]
82	1	1	[1, 0, 1, -2, 0]	[[0, -1, 1], [1, -1, 1]]	[[0, -1, 1]]
83	1	1	[1, 1, 1, 1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
88	1	1	[0, 0, 0, -4, 4]	[[2, -2, 1]]	[[1, 1, 1]]
89	1	1	[1, 1, 1, -1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
91	1	1	[0, 0, 1, 1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
91	2	1	[0, 1, 1, -7, 5]	[[-1, 3, 1], [1, 0, 1]]	[[-1, 3, 1], [1, 0, 1]]
92	2	1	[0, 0, 0, -1, 1]	[[1, -1, 1]]	[[0, 1, 1]]
99	1	1	[1, -1, 1, -2, 0]	[[0, 0, 1], [-1, 0, 1]]	[[0, 0, 1]]
101	1	1	[0, 1, 1, -1, -1]	[[-1, 0, 1]]	[[-1, 0, 1]]
102	1	1	[1, 1, 0, -2, 0]	[[-1, 2, 1], [0, 0, 1]]	[[1, -1, 1]]
106	2	1	[1, 1, 0, -7, 5]	[[2, -3, 1]]	[[1, -1, 1]]
112	1	1	[0, 1, 0, 0, 4]	[[0, 2, 1], [-2, 0, 1]]	[[-1, -2, 1]]
117	1	1	[1, -1, 1, 4, 6]	[[0, 2, 1], [2, 3, 1]]	[[0, 2, 1]]
118	1	1	[1, 1, 0, 1, 1]	[[0, 1, 1]]	[[-1, 0, 1]]
121	2	1	[0, -1, 1, -7, 10]	[[4, 5, 1]]	[[2, 0, 1]]
122	1	1	[1, 0, 1, 2, 0]	[[1, 1, 1]]	[[0, -1, 1]]
123	1	1	[0, 1, 1, -10, 10]	[[1, -2, 1], [-1, 4, 1]]	[[1, -2, 1]]
123	2	1	[0, -1, 1, 1, -1]	[[1, 0, 1]]	[[1, 0, 1]]
124	1	1	[0, 1, 0, -2, 1]	[[1, -1, 1], [0, 1, 1]]	[[1, -1, 1]]
128	1	1	[0, 1, 0, 1, 1]	[[0, 1, 1], [-1, 0, 1]]	[[0, 1, 1]]
129	1	1	[0, -1, 1, -19, 39]	[[1, 4, 1]]	[[3, -1, 1]]
130	1	1	[1, 0, 1, -33, 68]	[[2, -5, 1], [-1, 10, 1]]	[[2, -5, 1]]
131	1	1	[0, -1, 1, 1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
135	1	1	[0, 0, 1, -3, 4]	[[4, -8, 1]]	[[2, 2, 1]]
136	1	1	[0, 1, 0, -4, 0]	[[-2, 2, 1], [0, 0, 1]]	[[-1, -2, 1]]
138	1	1	[1, 1, 0, -1, 1]	[[0, 1, 1], [-2, 1, 1]]	[[-1, -1, 1]]
141	1	1	[0, 1, 1, -12, 2]	[[-3, 4, 1]]	[[-4, -2, 1]]
141	4	1	[0, -1, 1, -1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
Continued ...					

Table 2.1: (continued)

Table of generators for E and E_0. (continued)					
N	L	#	equation	E	E_0
142	1	1	[1, -1, 1, -12, 15]	[[1, 1, 1]]	[[-2, 31, 8]]
142	2	1	[1, 1, 0, -1, -1]	[[-1, 1, 1]]	[[-1, 1, 1]]
143	1	1	[0, -1, 1, -1, -2]	[[4, 6, 1]]	[[2, -1, 1]]
145	1	1	[1, -1, 1, -3, 2]	[[0, 1, 1], [1, -1, 1]]	[[0, 1, 1], [1, -1, 1]]
148	1	1	[0, -1, 0, -5, 1]	[[-1, 2, 1]]	[[0, -1, 1]]
152	1	1	[0, 1, 0, -1, 3]	[[-1, 2, 1]]	[[-2, -1, 1]]
153	1	1	[0, 0, 1, -3, 2]	[[0, 1, 1]]	[[1, -1, 1]]
153	2	1	[0, 0, 1, 6, 27]	[[5, 13, 1]]	[[3, -9, 1]]
154	1	1	[1, -1, 0, -29, 69]	[[2, 3, 1], [-6, 3, 1]]	[[3, -3, 1]]
155	1	1	[0, -1, 1, 10, 6]	[[2, 5, 1], [0, 2, 1]]	[[2, 5, 1]]
155	3	1	[0, -1, 1, -1, 1]	[[1, 0, 1]]	[[1, 0, 1]]
156	1	1	[0, -1, 0, -5, 6]	[[1, -1, 1], [2, 0, 1]]	[[-2, -2, 1]]
158	1	1	[1, -1, 1, -9, 9]	[[-1, 4, 1]]	[[22, -7, 8]]
158	2	1	[1, 1, 0, -3, 1]	[[0, 1, 1]]	[[1, 0, 1]]
160	1	1	[0, 1, 0, -6, 4]	[[0, 2, 1], [1, 0, 1]]	[[10, -1, 8], [1, 0, 1]]
162	1	1	[1, -1, 0, -6, 8]	[[2, -2, 1], [1, 1, 1]]	[[-1, -3, 1]]
163	1	1	[0, 0, 1, -2, 1]	[[1, 0, 1]]	[[1, 0, 1]]
166	1	1	[1, 1, 0, -6, 4]	[[0, 2, 1]]	[[1, -1, 1]]
170	1	1	[1, 0, 1, -8, 6]	[[0, 2, 1], [1, -1, 1]]	[[2, -1, 1]]
171	2	1	[0, 0, 1, 6, 0]	[[2, 4, 1]]	[[0, -1, 1]]
172	1	1	[0, 1, 0, -13, 15]	[[2, -1, 1], [1, 2, 1]]	[[2, -1, 1]]
175	1	1	[0, -1, 1, 2, -2]	[[2, 2, 1]]	[[1, -1, 1]]
175	2	1	[0, -1, 1, -33, 93]	[[-3, 12, 1]]	[[3, -4, 1]]
176	3	1	[0, -1, 0, 3, 1]	[[1, 2, 1]]	[[0, -1, 1]]
184	1	1	[0, -1, 0, 0, 1]	[[0, 1, 1]]	[[1, -1, 1]]
184	2	1	[0, -1, 0, -4, 5]	[[2, -1, 1]]	[[1, -1, 1]]
185	1	1	[0, 1, 1, -156, 700]	[[4, 12, 1]]	[[7, -1, 1]]
185	2	1	[0, -1, 1, -5, 6]	[[0, 2, 1]]	[[2, -1, 1]]
185	3	1	[1, 0, 1, -4, -3]	[[3, 2, 1], [-1, 0, 1]]	[[3, 2, 1], [-1, 0, 1]]
189	1	1	[0, 0, 1, -3, 0]	[[-1, 1, 1]]	[[0, -1, 1]]
189	2	1	[0, 0, 1, -24, 45]	[[-3, 9, 1], [3, 0, 1]]	[[-3, 9, 1], [3, 0, 1]]
190	1	1	[1, -1, 1, -48, 147]	[[13, -47, 1]]	[[754240, -1900091, 262144]]
190	2	1	[1, 1, 0, 2, 2]	[[1, 2, 1]]	[[-1, 1, 1]]
192	1	1	[0, -1, 0, -4, -2]	[[3, 2, 1], [-1, 0, 1]]	[[3, 2, 1], [-1, 0, 1]]
Continued ...					

Table 2.1: (continued)

Table of generators for E and E_0. (continued)					
N	L	#	equation	E	E_0
196	1	1	[0, -1, 0, -2, 1]	[[0, 1, 1]]	[[-1, -1, 1]]
197	1	1	[0, 0, 1, -5, 4]	[[1, 0, 1]]	[[1, 0, 1]]
198	1	1	[1, -1, 0, -18, 4]	[[-1, 5, 1], [-4, 2, 1]]	[[21, -103, 1]]
200	2	1	[0, 1, 0, -3, -2]	[[-1, 1, 1], [-2, 0, 1]]	[[2, 2, 1]]
201	1	1	[0, -1, 1, 2, 0]	[[1, 1, 1]]	[[0, -1, 1]]
201	2	1	[1, 0, 0, -1, 2]	[[-1, 2, 1]]	[[1, 1, 1]]
201	3	1	[1, 1, 0, -794, 8289]	[[16, -7, 1]]	[[16, -7, 1]]
203	2	1	[1, 1, 1, 0, -2]	[[2, 2, 1]]	[[1, -2, 1]]
205	1	1	[1, -1, 1, -22, 44]	[[-1, 8, 1], [2, 1, 1]]	[[-1, 8, 1], [3, -2, 1]]
207	1	1	[1, -1, 1, -5, 20]	[[0, 4, 1], [-3, 1, 1]]	[[1, -5, 1]]
208	1	1	[0, -1, 0, 8, -16]	[[4, 8, 1]]	[[13, 46, 1]]
208	2	1	[0, -1, 0, -16, 32]	[[4, -4, 1]]	[[1, 4, 1]]
209	1	1	[0, 1, 1, -27, 55]	[[-5, 9, 1], [1, 5, 1]]	[[13, -46, 1]]
210	4	1	[1, 1, 0, -3, -3]	[[-1, 1, 1], [-2, 1, 1]]	[[-1, 1, 1]]
212	1	1	[0, -1, 0, -4, 8]	[[2, -2, 1]]	[[1, 2, 1]]
214	1	1	[1, 0, 0, -12, 16]	[[0, 4, 1]]	[[6, -25, 8]]
214	2	1	[1, 0, 1, 1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
214	3	1	[1, 0, 1, -193, 1012]	[[11, 10, 1]]	[[8, -4, 1]]
215	1	1	[0, 0, 1, -8, -12]	[[6, 12, 1]]	[[4, -5, 1]]
216	1	1	[0, 0, 0, -12, 20]	[[-2, 6, 1]]	[[89, 839, 1]]
218	1	1	[1, 0, 0, -2, 4]	[[4, 6, 1], [0, 2, 1]]	[[6, 11, 8]]
219	1	1	[0, -1, 1, -6, 8]	[[2, -1, 1]]	[[2, -1, 1]]
219	2	1	[0, 1, 1, 3, 2]	[[2, 4, 1], [0, 1, 1]]	[[2, 4, 1]]
219	3	1	[1, 1, 0, -82, -305]	[[-6, 7, 1], [10, -5, 1]]	[[-6, 7, 1]]
220	1	1	[0, 1, 0, -45, 100]	[[-5, -15, 1], [15, 55, 1]]	[[4576, -9738, 2197]]
224	1	1	[0, 1, 0, 2, 0]	[[1, 2, 1], [0, 0, 1]]	[[1, 2, 1]]
225	1	1	[0, 0, 1, 0, 1]	[[1, 1, 1]]	[[-1, 0, 1]]
225	5	1	[0, 0, 1, -75, 256]	[[-5, 22, 1]]	[[138, 55, 27]]
226	1	1	[1, 0, 0, -5, 1]	[[-2, 3, 1], [2, -1, 1]]	[[-2, 13, 8]]
Continued ...					

Table 2.1: (continued)

Table of generators for E and E_0. (continued)					
N	L	#	equation	E	E_0
228	2	1	[0, -1, 0, 3, 9]	[[3, -6, 1]]	[[10, -29, 8]]
229	1	1	[1, 0, 0, -2, -1]	[[-1, 1, 1]]	[[-1, 1, 1]]
232	1	1	[0, -1, 0, 8, -4]	[[2, 4, 1]]	[[1, -2, 1]]
234	3	1	[1, -1, 0, -3, 5]	[[1, 1, 1], [-2, 1, 1]]	[[-1, -2, 1]]
235	1	1	[1, 1, 1, -5, 0]	[[-2, 3, 1]]	[[0, 0, 1]]
236	1	1	[0, -1, 0, -1, 2]	[[1, 1, 1]]	[[2, -2, 1]]
238	1	1	[1, 0, 0, -60, 16]	[[-4, 16, 1], [-8, 4, 1]]	[[448368568432, -42753352118559, 49836032]]
238	2	1	[1, -1, 0, 2, 0]	[[1, 1, 1], [0, 0, 1]]	[[1, 1, 1]]
240	3	1	[0, -1, 0, 4, 0]	[[1, 2, 1], [0, 0, 1]]	[[1, 2, 1]]
242	1	1	[1, 0, 0, 3, 1]	[[0, 1, 1]]	[[-2, -3, 8]]
243	1	1	[0, 0, 1, 0, -1]	[[1, 0, 1]]	[[1, 0, 1]]
244	1	1	[0, 0, 0, 1, 6]	[[-1, 2, 1]]	[[2, 4, 1]]
245	1	1	[0, 0, 1, -7, 12]	[[7, 17, 1]]	[[1, -3, 1]]
245	3	1	[0, -1, 1, -65, -204]	[[12, 24, 1]]	[[1230, -506, 125]]
246	4	1	[1, 1, 0, -66, 180]	[[3, 3, 1], [4, -2, 1]]	[[5, 0, 1]]
248	1	1	[0, 1, 0, 0, 1]	[[0, 1, 1]]	[[-1, -1, 1]]
248	3	1	[0, 0, 0, 1, -1]	[[1, 1, 1]]	[[2, -3, 1]]
249	1	1	[1, 1, 1, -55, 134]	[[4, -3, 1]]	[[4, -3, 1]]
249	2	1	[1, 1, 0, 2, 1]	[[0, 1, 1]]	[[0, 1, 1]]
252	2	1	[0, 0, 0, -12, 65]	[[-2, 9, 1], [-5, 0, 1]]	[[41171784, -733675159, 94818816]]
254	1	1	[1, 0, 0, -22, 36]	[[-4, 10, 1], [4, 2, 1]]	[[116, -167, 64]]
254	3	1	[1, -1, 0, -5, -3]	[[-1, 1, 1]]	[[-1, 1, 1]]
256	1	1	[0, 1, 0, -3, 1]	[[0, -1, 1], [1, 0, 1]]	[[0, -1, 1]]
256	2	1	[0, 0, 0, -2, 0]	[[-1, 1, 1], [0, 0, 1]]	[[-1, 1, 1]]
258	1	1	[1, 1, 0, 3, -3]	[[2, 3, 1]]	[[1, -2, 1]]
258	3	1	[1, 0, 1, -15, 22]	[[5, -12, 1]]	[[30, -104, 27]]
262	1	1	[1, 0, 0, 1, 25]	[[-2, 5, 1]]	[[-4942, -9225, 2744]]
262	2	1	[1, -1, 0, -2, 2]	[[1, 0, 1]]	[[1, 0, 1]]
265	1	1	[1, -1, 1, -138, 656]	[[6, 1, 1], [7, -4, 1]]	[[6, 1, 1], [7, -4, 1]]
269	1	1	[0, 0, 1, -2, -1]	[[-1, 0, 1]]	[[-1, 0, 1]]
272	1	1	[0, 1, 0, -8, 4]	[[-2, 4, 1], [2, 0, 1]]	[[3, -4, 1]]
272	2	1	[0, 0, 0, -11, -6]	[[-1, 2, 1], [-3, 0, 1]]	[[6, 12, 1]]
Continued …					

Table 2.1: (continued)

Table of generators for E and E_0. (continued)					
N	L	#	equation	E	E_0
273	1	1	[0, -1, 1, -26, 68]	[[11, 31, 1]]	[[1, -7, 1]]
274	1	1	[1, 0, 0, -7, 9]	[[2, -3, 1]]	[[-26, 15, 8]]
274	2	1	[1, -1, 0, -2846, 59156]	[[31, -15, 1]]	[[31, -15, 1]]
274	3	1	[1, -1, 0, -2, 0]	[[-1, 1, 1], [0, 0, 1]]	[[-1, 1, 1]]
275	1	1	[1, -1, 1, 20, 22]	[[8, 21, 1], [4, 10, 1]]	[[8, 21, 1]]
277	1	1	[1, 0, 1, 0, -1]	[[1, 0, 1]]	[[1, 0, 1]]
278	1	1	[1, 0, 0, -1, 9]	[[2, -5, 1]]	[[148, 215, 64]]
280	1	1	[0, -1, 0, -1, 5]	[[1, 2, 1]]	[[4, 7, 1]]
280	2	1	[0, 0, 0, -412, 3316]	[[-18, 70, 1]]	[[-23844365889629004780557695, -146026589415587201590421981, 1816504686805930915452625]]
282	2	1	[1, 1, 1, -15, 21]	[[3, -6, 1], [-5, 2, 1]]	[[-65064, 75319, 13824]]
285	1	1	[1, 0, 0, 19, 0]	[[1, 4, 1], [0, 0, 1]]	[[5103, -23220, 343]]
285	2	1	[1, 1, 0, 2, -17]	[[6, 13, 1], [2, -1, 1]]	[[6, 13, 1]]
286	2	1	[1, 1, 1, 13, 177]	[[19, -98, 1]]	[[-5052188869623392, -6615903343401659, 1144707943923712]]
286	3	1	[1, 1, 0, -33, 61]	[[1, 5, 1]]	[[3, -2, 1]]
288	1	1	[0, 0, 0, 3, 0]	[[1, 2, 1], [0, 0, 1]]	[[2, -7, 8]]
288	2	1	[0, 0, 0, -21, -20]	[[-3, 4, 1], [-1, 0, 1], [5, 0, 1]]	[[420, -715, 64]]
289	1	1	[1, -1, 1, -199, 510]	[[-12, 38, 1], [30, 129, 1]]	[[-12, 38, 1]]
290	1	1	[1, -1, 0, -70, -204]	[[-5, 4, 1], [-4, 2, 1]]	[[-5, 4, 1]]
291	3	1	[1, 1, 1, -3, 0]	[[0, -1, 1], [1, -1, 1]]	[[0, -1, 1]]
294	7	1	[1, 0, 1, 2, 32]	[[1, 5, 1], [-3, 1, 1]]	[[6, 13, 1]]
296	1	1	[0, -1, 0, -9, 13]	[[1, 2, 1]]	[[4, -5, 1]]
296	2	1	[0, -1, 0, -33, 85]	[[3, 2, 1]]	[[4, 1, 1]]
297	1	1	[0, 0, 1, -81, 290]	[[15, 49, 1]]	[[1, -15, 1]]
297	2	1	[1, -1, 1, 1, 0]	[[0, 0, 1]]	[[0, 0, 1]]
297	3	1	[1, -1, 0, 12, -19]	[[4, 7, 1]]	[[20, -99, 1]]
Continued ...					

Table 2.1: (continued)

Table of generators for E and E_0. (continued)					
N	L	#	equation	E	E_0
298	1	1	[1, 0, 0, -19, 33]	[[2, 1, 1]]	[[-12, -381, 64]]
298	2	1	[1, -1, 0, 1, -1]	[[1, 0, 1]]	[[1, 0, 1]]
300	4	1	[0, -1, 0, -13, 22]	[[7, -15, 1], [2, 0, 1]]	[[324, -497, 64]]
302	1	1	[1, 1, 1, -230, 1251]	[[33, 159, 1], [1, 31, 1]]	[[4810366, -1101641, 551368]]
302	3	1	[1, -1, 1, 0, 3]	[[1, 1, 1]]	[[-2, 11, 8]]
303	1	1	[0, 1, 1, -197, -208]	[[-2, 13, 1]]	[[1046333508, 1767647804, 67419143]]
303	2	1	[0, 1, 1, -6, 2]	[[0, 1, 1]]	[[2, -2, 1]]
304	1	1	[0, 1, 0, 0, -76]	[[10, 32, 1]]	[[187, 2564, 1]]
304	3	1	[0, -1, 0, -8, 16]	[[0, 4, 1]]	[[-3, 2, 1]]
304	6	1	[0, 1, 0, -21, 31]	[[3, 2, 1]]	[[2, 1, 1]]
306	2	1	[1, -1, 0, -27, -27]	[[-3, 6, 1], [6, -3, 1]]	[[7, -13, 1]]
308	1	1	[0, -1, 0, -21, 49]	[[7, -14, 1]]	[[26, 17, 8]]
309	1	1	[1, 0, 0, -6, 9]	[[3, -6, 1]]	[[5, 8, 1]]
310	2	1	[1, 0, 0, -106, 420]	[[-4, 30, 1], [8, 6, 1]]	[[5948280296, -8759749391, 1204550144]]
312	2	1	[0, -1, 0, -3, 0]	[[-1, 1, 1], [0, 0, 1]]	[[4, -6, 1]]
312	6	1	[0, 1, 0, 5, 14]	[[-1, 3, 1], [-2, 0, 1]]	[[5754, 38998, 9261]]
314	1	1	[1, -1, 0, 13, -11]	[[6, 13, 1]]	[[1, 1, 1]]
315	2	1	[1, -1, 1, -23, -34]	[[-2, 1, 1], [-3, 1, 1]]	[[-2, 1, 1]]
316	2	1	[0, 0, 0, -7, -2]	[[-1, 2, 1]]	[[-2, -2, 1]]
318	3	1	[1, 1, 0, 7, -9]	[[5, 11, 1]]	[[1, 0, 1]]
318	4	1	[1, 1, 1, -12, 45]	[[1, 5, 1]]	[[-5948841000, 2569385943, 1151022592]]
320	2	1	[0, 0, 0, -8, 8]	[[1, -1, 1], [2, 0, 1]]	[[1, -1, 1]]
320	6	1	[0, 1, 0, -5, -5]	[[-2, 1, 1], [-1, 0, 1]]	[[-2, 1, 1]]
The end					

Table 2

This last table contains the quantities needed for testing Mazur and Tate conjecture. N is the conductor, L is the letter type, # is the number type, r is as in section 3, u is the order of the torsion, v is the order of the torsion in E_0 and C is the product of Tamawaga numbers.

Table 2.2: Table of values for conjecture.

Table of values for r conjecture.

N	L	#	r	u	v	C
37	1	1	1	1	1	1
43	1	1	1	1	1	1
53	1	1	1	1	1	1
57	1	1	2	1	1	2
58	1	1	2	1	1	2
61	1	1	1	1	1	1
65	1	1	1	2	2	1
65	1	2	2	2	1	4
77	1	1	2	1	1	2
79	1	1	1	1	1	1
82	1	1	1	2	1	2
82	1	2	1	2	1	2
83	1	1	1	1	1	1
88	1	1	4	1	1	4
89	1	1	1	1	1	1
91	1	1	1	1	1	1
91	2	1	1	3	3	1
91	2	2	3	3	1	9
91	2	3	9	1	1	9
92	2	1	3	1	1	3
99	1	1	1	2	1	2
99	1	2	2	2	1	4
101	1	1	1	1	1	1
102	1	1	2	2	1	4
102	1	2	2	2	1	4
106	2	1	2	1	1	2

Continued ...

Table 2.2: (continued)

Table of values for conjecture. (continued)						
N	L	#	r	u	v	C
112	1	1	2	2	1	4
112	1	2	4	2	1	8
117	1	1	1	4	1	4
117	1	2	2	4	1	8
117	1	3	4	2	1	8
117	1	4	2	2	1	4
118	1	1	2	1	1	2
121	2	1	2	1	1	2
121	2	2	2	1	1	2
122	1	1	2	1	1	2
123	1	1	1	5	1	5
123	1	2	5	1	1	5
123	2	1	1	1	1	1
124	1	1	1	3	1	3
124	1	2	3	1	1	3
128	1	1	1	2	1	2
128	1	2	2	2	1	4
129	1	1	2	1	1	2
130	1	1	1	6	1	6
130	1	2	2	6	1	24
130	1	3	3	2	1	6
130	1	4	6	2	1	24
131	1	1	1	1	1	1
135	1	1	6	1	1	6
136	1	1	2	2	1	4
136	1	2	2	2	1	4
138	1	1	2	2	1	4
138	1	2	1	2	1	2
141	1	1	7	1	1	7
141	4	1	1	1	1	1
142	1	1	9	1	1	9
142	2	1	1	1	1	1
143	1	1	2	1	1	2
145	1	1	1	2	2	1
Continued ...						

Table 2.2: (continued)

Table of values for conjecture. (continued)						
N	L	#	r	u	v	C
145	1	2	2	2	1	4
148	1	1	3	1	1	3
152	1	1	4	1	1	4
153	1	1	2	1	1	2
153	2	1	4	1	1	4
153	2	2	4	3	1	12
154	1	1	2	2	1	4
154	1	2	1	2	1	2
155	1	1	1	5	1	5
155	1	2	5	1	1	5
155	3	1	1	1	1	1
156	1	1	3	2	1	6
156	1	2	3	2	1	6
158	1	1	8	1	1	8
158	2	1	2	1	1	2
160	1	1	2	2	2	2
160	1	2	4	2	1	8
162	1	1	2	3	1	6
162	1	2	6	1	1	6
163	1	1	1	1	1	1
166	1	1	2	1	1	2
170	1	1	2	2	1	4
170	1	2	4	2	1	16
171	2	1	2	1	1	2
171	2	2	2	3	1	6
171	2	3	2	3	3	2
172	1	1	1	3	1	3
172	1	2	3	1	1	3
175	1	1	2	1	1	2
175	1	2	2	5	1	10
175	2	1	4	1	1	4
175	2	2	4	1	1	4
175	2	3	4	1	1	4
176	3	1	2	1	1	2
Continued ...						

Table 2.2: (continued)

Table of values for conjecture. (continued)

N	L	#	r	u	v	C
176	3	2	6	1	1	6
184	1	1	2	1	1	2
184	2	1	2	1	1	2
185	1	1	2	1	1	2
185	2	1	2	1	1	2
185	3	1	1	2	2	1
185	3	2	2	2	1	4
189	1	1	3	1	1	3
189	2	1	1	3	3	1
189	2	2	3	3	1	9
189	2	3	1	1	1	1
190	1	1	22	1	1	22
190	2	1	2	1	1	2
192	1	1	1	2	2	1
192	1	2	2	4	1	8
192	1	3	1	4	1	4
192	1	4	4	2	1	8
196	1	1	3	1	1	3
196	1	2	1	1	1	1
197	1	1	1	1	1	1
198	1	1	4	2	1	8
198	1	2	2	4	1	16
198	1	3	1	2	1	2
198	1	4	4	2	1	16
200	2	1	2	2	1	4
200	2	2	4	2	1	8
201	1	1	2	1	1	2
201	2	1	3	1	1	3
201	3	1	1	1	1	1
203	2	1	2	1	1	2
205	1	1	1	4	2	2
205	1	2	2	4	1	8
205	1	3	4	2	1	8
205	1	4	2	4	1	8

Continued ...

Table 2.2: (continued)

Table of values for conjecture. (continued)						
N	L	#	r	u	v	C
207	1	1	2	2	1	4
207	1	2	4	2	1	8
208	1	1	4	1	1	4
208	1	2	12	1	1	12
208	1	3	4	1	1	4
208	2	1	4	1	1	4
209	1	1	2	3	1	6
209	1	2	6	1	1	6
210	4	1	1	2	1	2
210	4	2	2	4	1	16
210	4	3	1	2	1	2
210	4	4	2	2	1	4
212	1	1	3	1	1	3
214	1	1	7	1	1	7
214	2	1	1	1	1	1
214	3	1	2	1	1	2
215	1	1	2	1	1	2
216	1	1	12	1	1	12
218	1	1	2	3	1	6
218	1	2	6	1	1	6
219	1	1	1	1	1	1
219	2	1	1	3	1	3
219	2	2	3	1	1	3
219	3	1	1	2	1	2
219	3	2	1	2	1	2
220	1	1	3	6	1	18
220	1	2	3	6	1	18
220	1	3	1	2	1	2
220	1	4	1	2	1	2
224	1	1	1	2	1	2
224	1	2	2	2	1	4
225	1	1	2	1	1	2
225	1	2	2	1	1	2
225	5	1	12	1	1	12
Continued . . .						

Table 2.2: (continued)

Table of values for conjecture. (continued)

N	L	#	r	u	v	C
225	5	2	12	1	1	12
226	1	1	3	2	1	6
226	1	2	3	2	1	6
228	2	1	6	1	1	6
229	1	1	1	1	1	1
232	1	1	2	1	1	2
234	3	1	2	2	1	4
234	3	2	2	2	1	8
235	1	1	3	1	1	3
236	1	1	3	1	1	3
238	1	1	14	2	1	28
238	1	2	28	2	1	56
238	2	1	1	2	1	2
238	2	2	2	2	1	4
240	3	1	1	2	1	2
240	3	2	2	4	1	16
240	3	3	2	2	1	4
240	3	4	4	2	1	8
242	1	1	4	1	1	4
242	1	2	12	1	1	12
243	1	1	1	1	1	1
243	1	2	1	3	1	3
244	1	1	3	1	1	3
245	1	1	6	1	1	6
245	3	1	4	1	1	4
245	3	2	12	1	1	12
245	3	3	36	1	1	36
246	4	1	2	2	1	4
246	4	2	2	2	1	4
248	1	1	2	1	1	2
248	3	1	2	1	1	2
249	1	1	1	1	1	1
249	2	1	1	1	1	1
252	2	1	12	2	1	24

Continued ...

Table 2.2: (continued)

Table of values for conjecture. (continued)

N	L	#	r	u	v	C
252	2	2	6	2	1	12
254	1	1	3	3	1	9
254	1	2	3	3	1	9
254	1	3	1	1	1	1
254	3	1	1	1	1	1
256	1	1	1	2	1	2
256	1	2	1	2	1	2
256	2	1	1	2	1	2
256	2	2	1	2	1	2
258	1	1	2	1	1	2
258	3	1	10	1	1	10
262	1	1	11	1	1	11
262	2	1	1	1	1	1
265	1	1	1	2	2	1
265	1	2	2	2	1	4
269	1	1	1	1	1	1
272	1	1	2	2	1	4
272	1	2	2	2	1	4
272	2	1	2	2	1	4
272	2	2	2	4	1	8
272	2	3	2	4	2	4
272	2	4	2	4	1	8
273	1	1	6	1	1	6
274	1	1	7	1	1	7
274	2	1	1	1	1	1
274	3	1	1	2	1	2
274	3	2	1	2	1	2
275	1	1	1	4	1	4
275	1	2	2	4	1	8
275	1	3	4	2	1	8
275	1	4	2	2	1	4
277	1	1	1	1	1	1
278	1	1	8	1	1	8
280	1	1	4	1	1	4

Continued ...

Table 2.2: (continued)

Table of values for conjecture. (continued)						
N	L	#	r	u	v	C
280	2	1	60	1	1	60
282	2	1	8	2	1	16
282	2	2	4	2	1	8
285	1	1	5	2	1	10
285	1	2	10	2	1	20
285	2	1	1	2	1	2
285	2	2	2	2	1	4
286	2	1	26	1	1	26
286	3	1	2	1	1	2
288	1	1	2	2	1	4
288	1	2	4	2	1	8
288	2	1	2	4	1	8
288	2	2	1	2	1	2
288	2	3	4	4	1	16
288	2	4	2	2	1	8
289	1	1	1	4	1	4
289	1	2	1	4	1	4
289	1	3	2	2	1	4
289	1	4	2	2	1	4
290	1	1	1	2	1	2
290	1	2	2	2	1	8
291	3	1	1	2	1	2
291	3	2	1	2	1	2
294	7	1	4	2	1	16
294	7	2	8	2	1	32
296	1	1	4	1	1	4
296	2	1	2	1	1	2
297	1	1	6	1	1	6
297	2	1	1	1	1	1
297	3	1	3	1	1	3
298	1	1	9	1	1	9
298	2	1	1	1	1	1
300	4	1	6	2	1	12
300	4	2	6	2	1	12
Continued ...						

Table 2.2: (continued)

Table of values for conjecture. (continued)						
N	L	#	r	u	v	C
302	1	1	3	5	1	15
302	1	2	15	1	1	15
302	3	1	5	1	1	5
303	1	1	14	1	1	14
303	2	1	4	1	1	4
304	1	1	4	1	1	4
304	1	2	20	1	1	20
304	3	1	4	1	1	4
304	6	1	2	1	1	2
306	2	1	2	2	1	4
306	2	2	1	2	1	4
306	2	3	2	6	1	12
306	2	4	1	6	1	12
308	1	1	6	1	1	6
309	1	1	5	1	1	5
310	2	1	4	6	1	24
310	2	2	2	6	1	12
310	2	3	12	2	1	24
310	2	4	6	2	1	12
312	2	1	2	2	1	4
312	2	2	2	2	1	4
312	6	1	6	2	1	12
312	6	2	12	2	1	24
314	1	1	2	1	1	2
315	2	1	1	2	1	2
315	2	2	2	4	1	16
315	2	3	4	2	1	8
315	2	4	4	2	1	16
316	2	1	3	1	1	3
318	3	1	2	1	1	2
318	4	1	22	1	1	22
320	2	1	1	2	1	2
320	2	2	1	4	1	8
320	2	3	1	2	1	2
Continued ...						

Table 2.2: (continued)

Table of values for conjecture. (continued)						
N	L	#	r	u	v	C
320	2	4	2	2	1	8
320	6	1	1	2	1	2
The end						

Note about tables

The only interesting part in computing the tables above was the computation of the subgroup E_0 and, as a consequence, the value v. The generators of E were available in [Cre97] or at Cremona's extensive databases [Cre03]. The torsion points of E are easily computed by Pari.

Now, in order to compute generators for E_0, we created a simple function called *onerons*, such that giving a point $P \in E$, the *onerons* function outputs the smallest integer k such that $kP \in E_0$. We called this value the order of Néron of P in E, and we denote it as $o(P)$.

We use the following algorithms to compute E_0 and v.

Algorithm 2.4.1. Computation of generators of E_0.

The main idea is to use the free group L generated by the generators of E. In other words, the group of expressions

$$aP + \sum_{i=1}^{t} b_i R_i \tag{2.18}$$

where P is a generator of the free part and the points R_i are generators of the torsion. Now, we know that the torsion part has at most two generators. So, in the worst case, we are working with an abelian group isomorphic to $\mathbb{Z}^3$.

Now, if L_0 is the subgroup of all linear expressions such that $aP + \sum_{i=1}^{t} b_i R_i \in E_0$, then a basis for L_0 will be a set of generators for E_0.

The generators of L_0 are obtained by using the next algorithm 2.4.2 and the *onerons* function.

Algorithm 2.4.2. Given a finitely generated free abelian group F and a subgroup H of maximal rank in F. We would like to compute a basis for H, assuming we have a basis for F and an algorithm to determine if an element $x \in F$ belongs to H.

Assume $\{f_1, f_2, \ldots, f_r\}$ is a basis for F. Denote o_i to the smallest positive integer such that $o_i f_i \in H$. Let $I_i = [0, o_i] \bigcap \mathbb{Z}$ and $B_i = I_1 \times \cdots \times I_i$. Let $F_i =< f_1, f_2, \ldots, f_i >$ for $1 \leq i \leq r$, and set: $H_i = F_i \bigcap H$.

Now, we construct a basis for H_{i+1} from a basis $\{h_1, h_2, \ldots, h_i\}$ of H_i as follows: Set $u_{i+1} = gcd(o_{i+1}, o_1 o_2 \cdots o_i)$, then take as h_{i+1} any element in $(cu_{i+1} f_{i+1} + B_i) \bigcap H$, where $c \geq 1$ is minimum such that

$$(cu_{i+1} f_{i+1} + B_i) \bigcap H \neq \emptyset \tag{2.19}$$

We will start the algorithm with $h_1 = o_1 f_1$.

Algorithm 2.4.3. Algorithm for computing $v = \#(E_0 / < Q_0 >)$ with Q_0 of infinite order.

Let $E_0 =< S, T_0 >$ where T_0 is the torsion part in B_0 and S is a generator of the free part. Then, if r is the minimal integer such that $Q_0 - rS$

is a torsion, the representatives of $E_0/<Q_0>$ are the elements: $sS+R$, with $0<s\leq r$ and $R\in T_0$. Hence, $v=r|T_0|$.

To obtain r, let v be the order of the torsion, w the number of torsion points with good reduction, set $m=v/w$. Then, starting from r=1, compute $m(Q_0-rS)$, until $m(Q_0-rS)=O$. Such an r is the one we want.

Chapter 3

The g function

3.1 Extending the g function.

Easy testings on curves of composite conductor N show that we cannot extend the function $\hat{g}$ to $E \times E$. The main problem is that the function $g(P_1, n_q P_2, P', q)$ with P_1, P_2, $P' \in E$ and $q \nmid N$ is not well defined depending only on P_1 and P_2. In other words, it is not independent of the point P'.

Instead, we observed that the number of good values of $g(P_1, n_q P_2, P', q)$, fixing P_1, P_2 and q but varying P', is bounded; and such a bound does not depend on q.

In fact, if $V(P_1, n_q P_2, q)$ is the set of distinct values of $g(P_1, n_q P_2, P', q)$ and r is chosen as in the previous section, we observed from our computations that:

$$|V(P_1, n_q P_2, q)| \leq r \tag{3.1}$$

for all $q \nmid N$.

We conjecture the following statement that we will assume true for the remaining of the thesis. We have not proved it, but our computations of the g function seems to suggest that it is true.

Conjecture 3.1.1. *Given P_1, P_2, and P' points in E, and Q a point of E_0, then $g(P_1, n_qP_2, P', q) = g(P_1, n_qP_2, P' + Q, q)$ if both side of the equations are good values.*

This conjecture is saying that $g(P_1, n_qP_2, P', q)$ depends only on P' modulo E_0. So, for P_1 and P_2 fixed, we will have at most $\#(E/E_0) = r\frac{u}{v}$ different values in $V(P_1, n_qP_2, q)$.

Now, the next conjecture says a little more about the torsion.

Conjecture 3.1.2. *Let P be a generator of E modulo torsion and P_1, $P_2 \in E$. Then, for every $1 \leq i \leq r$ and $R \in E_{tors}$, there is a $j \in \mathbb{Z}$ with $1 \leq j \leq r$ such that: $g(P_1, n_qP_2, iP + R, q) = g(P_1, n_qP_2, jP, q)$ for every prime q not dividing the conductor N, where the two sides are well defined.*

Notice that the last two conjectures would impply that $|V(P_1, n_qP_2, q)| \leq r$.

Now, instead of extending $\hat{g}$ to $E \times E$, we can construct a map:

$$\tilde{g} : E \times E \to \prod_{q \nmid N} (\mathbb{F}_q^*)^r \tag{3.2}$$

given by

$$\tilde{g}(P_1, P_2) = (g(P_1, n_qP_2, P, q), g(P_1, n_qP_2, 2P, q), \ldots, g(P_1, n_qP_2, rP, q)). \tag{3.3}$$

Now, in order to get an equation of the BSD-type, we take the product of all these values. (i.e. We compose $\tilde{g}$ coordinate by coordinate with the product maps

$$\pi_q^r : (\mathbb{F}_q^*)^r \to F_q^* \tag{3.4}$$

$$(u_1, \ldots, u_r) \to \prod_{i=1}^{r} u_i \tag{3.5}$$

Denote $\pi^r = (\pi_q^r)_{q \nmid N}$ the product map over all the q's.

We state the following weak conjecture.

Conjecture 3.1.3. *For P_1 and P_2 points in E. There exist integer exponents s and w depending on P_1 and P_2 such that*

$$l^s = \pi^r \circ \tilde{g}(P_1, P_2)^w \tag{3.6}$$

Now, if we set $\breve{g} = \pi^r \circ \tilde{g}(P_1, P_2)$, then for $P \in E$ and $Q \in E_0$, we have $\breve{g}(P, Q) = \hat{g}^r(P, Q)$.

The main result that we obtain after computing multiple values of the function $\tilde{g}(P_1, P_2)$ in several elliptic curves is the following conjecture.

Conjecture 3.1.4. *Let E be an elliptic curve with conductor N and rank 1. Let P a generator of E modulo torsion and r as above. Set $P_q = n_q P$. For $q \nmid N$ and d a divisor of r. Set $a = r/d$, then the function $g(dP, dP_q, P', q)$ takes up to a different values. Those values satisfy the formula:*

$$\left(\prod_{i=1}^{a} g_i(dP, dP_q, iP, q) \right)^w = l(q)^{ds} \tag{3.7}$$

for some integers w and s that does not depend on d.

In the following section, I will explain how this conjecture relates to Mazur and Tate and how combining with it, we obtain a more precise description of the exponents in the above conjecture. In order to explain it, we need some technical formulas.

3.2 Multiplicative Formulas

Now, let g the function defined in 2.6. Then, we have the following propositions.

Proposition 3.2.1. *For P_1, P_2, P, Q_1, Q_2, Q, and P' in E, and $q \nmid N$; then, we have the identities (if both sides of the equation are well defined in $\mathbb{F}_q^*$):*

1. $g(P, Q_1 + Q_2, P', q) = g(P, Q_1, P', q)g(P, Q_2, P' + Q_1, q)$

2. $g(P_1 + P_2, Q, P', q) = g(P_1, Q, P', q)g(P_2, Q, P' + P_1, q)$

Proof. These identities follow by simple cancellation. We just write down the proof of the first one (the second one is identical, replacing P's by Q's and vice-versa):

$$\frac{d(P'+P)d(P'+Q_1+Q_2)}{d(P')d(P'+P+Q_1+Q_2)} = \frac{d(P'+P)d(P'+Q_1)}{d(P')d(P'+P+Q_1)}\frac{d(P'+Q_1+P)d(P'+Q_1+Q_2)}{d(P'+Q_1)d(P'+P+Q_1+Q_2)} \tag{3.8}$$

□

Now, for convenience, we write $g(P, Q, P')$ instead of $g(P, Q, P', q)$. Although, we understand this function depends also on $q \nmid N$.

In fact, the reader may notice that the identity used in the proof is the same as the one used before to prove that $\hat{g}$ is a bi-multiplicative function.

An easy corollary to this proposition is the following:

Proposition 3.2.2. *Having the same notation as in the previous proposition and $n \in \mathbb{Z}$, these product formulas are true:*

1. $g(P, nQ, P') = \prod_{i=0}^{n-1} g(P, Q, P' + iQ)$

2. $g(nP, Q, P') = \prod_{i=0}^{n-1} g(P, Q, P' + iP)$

Proof. It follows by induction from 3.2.1:

$$\begin{aligned} g(P, nQ, P') =& g(P, Q, P')g(P, (n-1)Q, P') \\ =& \hat{g}(P, Q, P') \prod_{i=1}^{n-1} g(P, Q, P' + iQ) \\ =& \prod_{i=0}^{n-1} g(P, Q, P' + iQ) \end{aligned} \tag{3.9}$$

The base of induction is 3.2.1.

□

Now, these two propositions in conjunction with 3.1.1 and 3.1.2 imply that the image of g (as a function in $E \times n_q E \times E$) in the coordinate $\mathbb{F}_q^*$ is completely determined by the values $g(P, P_q, iP, q)$ where i is an integer modulo r. In other words, any element in the image of g in $\mathbb{F}_q^*$ can be decomposed as a product of those r values. Now, let's use the above identities to justify some of the identities in the last conjecture of the previous section.

Proposition 3.2.3. *1. If $gcd(n_q, r) = 1$, then 3.1.1 implies lemma 2.2.1. Also, in this case $g(P, n_q Q, P) = g(Q, n_q P, P)$.*

2. *If* $gcd(n_q, r) = d > 1$*, then we have the identity:* $g(dP, n_qQ, P) = g(Q, n_qP, P)^d$*.*

Proof. These proposition follows from a series of simple observations.

Let $P \in E$ and $Q = rP$, with r as in 2.2.1. Then, from 3.2.3 we have:

$$g(P, n_qQ, P) = \prod_{i=0}^{r-1} g(P, n_qP, P + in_qP) \tag{3.10}$$

So, if $gcd(n_q, r) = 1$, we can arrange the product, so that:

$$g(P, n_qQ, P) = \prod_{i=0}^{r-1} g(P, n_qP, P + iP) = g(Q, n_qP, P) \tag{3.11}$$

Now, notice also that this identity proves that $g(P, n_qQ, P)$ does not depend on the choice of P. In fact, we change P by any other point in the curve $P' = mP + R$ where $R \in E_{tors}$ and $m \in \mathbb{Z}$, this will be just a shifting by $m - 1$ of the index i in the middle term of the formula above. But, since the quantity $g(P, n_qP, P')$ depends only on P' modulo E_0, the product after the shifting gives the same value.

Note 3.2.1. The only condition, on which we want to be careful is in having all the g functions well defined. This may be a problem for small primes q, because in that case n_q may be small in comparison with r and therefore, we may have a lot of bad values for $g(P, n_qQ, P + iP)$, and the products in 3.2.3 won't be properly computed. But, for q sufficiently large, so that $r << n_q$, all these formulas will hold nicely. For the same reason, it seems that in the conjectures of B. Mazur and J. Tate in [MT87], we should be careful also when q is a small prime, since we may encounter anomalies or problems in the definition of the g function. Basically, the obvious case, is when a prime q divides the denominator $d(P)$ for every point $P \in E$.

If $gcd(n_q, r) = d$, we obtain

$$g(P, n_q Q, P) = \left(\prod_{i=0}^{r/d-1} g(P, n_q P, P + idP) \right)^d \tag{3.12}$$

Unfortunately, this equation is not enough to prove that $g(P, n_q Q, P')$ does not depend on P'. We know that 2.2.1 is true, and we have plenty of evidence in favor of conjecture 3.1.1. So, it is a reasonable question to see if the first part of the proposition holds in general.

The second part of the proposition is obtained as follows:

$$g(dP, n_q Q, P) = \left(\prod_{i=0}^{r/d-1} g(dP, n_q P, P + idP) \right)^d \tag{3.13}$$

$$= g(rP, n_q P, P)^d \tag{3.14}$$

$$= g(Q, n_q P, P)^d \tag{3.15}$$

□

Now, from the proof of the second identity in the above proposition, it is not very clear that that $g(dP, n_q Q, P')$ does not depend on the choice of P'. The following lemma proves it.

Lemma 3.2.4. *$g(Q, n_q P, P')$ does not depend on the choice of P'.*

Proof. This is clear, assuming 3.1.1 and the following identity:

$$\frac{g(P, n_q P, P)}{g(P, n_q P, P + Q)} = \frac{g(Q, n_q P, P)}{g(Q, n_q P, P + P)} \tag{3.16}$$

This identity is proved as usual by simple comparison and cancellations. In fact, this equation shows that this lemma is equivalent to 3.1.1 □

One last comment ending this section is that if we can prove 3.1.1 by elementary methods, and if it implies 2.2.1, then we would have obtained an elementary way of explaining the properties of the g function.

3.3 De-constructing the g function

In this section, we will assume also 3.1.1. We will give some multiplicativity identities to study the values $g(mP, tP_q, sP)$ with $0 \leq s < r$ and $P_q = n_q P$, and P a generator of the free part of E.

The following proposition goes towards this direction. We denote $g(Q, P_q)$ to the value $g(rP, P_q, sP)$.

Proposition 3.3.1. *Let m be an integer. Let $a \equiv m \pmod r$ with $0 \leq a < r$. Set $e = (m-a)/r$. We have the following decompositions:*

1. $g(mP, P_q, P') = g(Q, P_q)^e g(aP, P, P')$
2. *If* $gcd(a, n_q) = 1$, *then* $g(P, mP_q, P') = \hat{g}(P, Q_q)^e g(P, aP, P')$.

Proof. The first computation is as follows:

$$\begin{aligned} g(mP, P_q, P') &= \prod_{i=0}^{m-1} g(P, P_q, P' + iP) && (3.17) \\ &= \left(\prod_{i=0}^{r-1} g(P, P_q, P + iP) \right)^e \prod_{i=0}^{a-1} g(P, P_q, P' + iP) && (3.18) \\ &= g(Q, P_q)^e g(aP, P_q, P') && (3.19) \end{aligned}$$

The second is a corollary of the below proposition. □

We have the more general result of part two.

Proposition 3.3.2. *Let $d = gcd(n_q, r)$ and let m an integer. Chose $m \equiv a$ (mod r/d) and set $e = d(m-a)/r$. Then,*

$$g(P, mP_q, P') = \left(\prod_{i=0}^{r/d-1} g(P, P_q, P' + idP)\right)^e g(P, aP_q, P') \tag{3.20}$$

Proof. This is prove as follows:

$$\begin{aligned} g(P, mP_q, P') &= \prod_{i=0}^{m-1} g(P, P_q, P + iP_q) & (3.21) \\ &= \left(\prod_{j=0}^{e-1} \prod_{i=jr/d}^{(j+1)r/d-1} g(P, P_q, P + iP_q)\right) \prod_{i=m-a}^{m-1} g(P, P_q, P + iP_q) & (3.22) \\ &= \left(\prod_{i=0}^{r/d-1} g(P, P_q, P + iP_q)\right)^e \prod_{i=0}^{a} g(P, P_q, P + iP_q) & (3.23) \end{aligned}$$

Now, since $gcd(\frac{r}{d}, \frac{n_q}{d}) = 1$, we can arrange indexes, so that, we obtain the identity:

$$\prod_{i=0}^{r/d-1} g(P, P_q, P + iP_q) = \prod_{j=0}^{r/d-1} g(P, P_q, P' + jdP) \tag{3.24}$$

This proves the proposition. □

Now, the second part of 3.3.1 follows from 3.3.2, when $d = 1$. In such a case, we obtain:

$$g(P, mP_q, P') = g(P, rP_q, P')^e g(P, aP_q, P') \tag{3.25}$$

Note that the above proposition is a generalization of 3.2.3. We summarize this discussion in the following lemma, which is a kind of commutativity property.

Lemma 3.3.3. *If $gcd(n_q, r) = d$ and if Q is a generator of E_0 and $Q_q = n_q Q$, then:*

$$g(Q, P_q, P')^d = g(P, Q_q, P')^d = (\hat{g}(P, Q)^d)_q \tag{3.26}$$

Here, the third term is the q-coordinate of $\hat{g}(P, Q)^d$.

Proof. Since, we assume that the torsion is insignificant for the g function, we have that $g(Q, dP_q, P') = g(rP, dP_q, P')$ and also $g(dP, Q_q, P') = g(dP, rP_q, P')$. The lemma follows if we apply 3.3.2 to $g(dP, rP_q, P')$. Thus,

$$\begin{aligned} g(P, rP_q, P')^d =& g(dP, rP_q, P') && (3.27)\\ =& \left(\prod_{i=0}^{r/d-1} g(dP, P_q, P' + idP)\right)^d && (3.28)\\ =& g(rP, P_q, P')^d && (3.29) \end{aligned}$$

Note that this also follows from 3.2.3. □

We state a refinement or generalization of part c) of conjecture 3.1.4. This is also a generalization of 3.1.1

Conjecture 3.3.4. *Let $ab = r$ with a, $b \in \mathbb{Z}$. Then, the functions: $g(P, bP_q, P')$ and $g(bP, P_q, P')$ take up to a different values. Moreover, if $P' - P'' \in E_0$, then $g(P, bP_q, P') = g(P, bP_q, P'')$ and $g(bP, P_q, P') = g(bP, P_q, P'')$.*

Now, if the above lemma is true, then we can take the values $g(bP, bP_q, P + iP)$ as representatives of the different values of $g(bP, bP_q, P')$.

Hence, we can state our last conjecture, using similar notation as in section 3:

Conjecture 3.3.5. *Let P be a generator of E. Let $ab = r$ with a,$b \in \mathbb{Z}$. For $q \nmid N$, we have*

$$\left(\prod_{i=0}^{a-1} g(bP, bP_q, P + iP)\right)^{\frac{C|Ш|}{r}} = l(q)^{u^2 b} \tag{3.30}$$

I am still not sure if 2.3.1 implies 3.3.5.

But, at least in the case when $gcd(n_q, r)$ divides b, the equivalence follows from the commutativity property 3.3.3. In that case, the identity:

$$g(rP, bP, P) = \prod_{i=0}^{a-1} g(bP, bP_q, P + iP) \tag{3.31}$$

together with

$$g(bP, rP_q, P) = (g(P, Q))_q^b \tag{3.32}$$

gives the equivalence.

3.3.1 Tables with multiple values

These are some of the tables as an example of the computations of multiples values for g. We tabulate the values of the clases $g(P, P_q, iP, q)$ for $1 \le i \le r$ and $3 \le q \le 100$ with $gcd(q, N) = 1$. For $q \mid N$, we just put a row of zeros. Also, if q divides always to at least one of the denominators of $g(P, P_q, iP+Q, q)$ for any shift of Q, we just write a 0 (In practice, we create a function that computed $g(P, P_q, iP + jQ, q)$ varying j until certain limit, if the value of $g(P, P_q, iP + jQ, q)$ was not well defined for every j tested, we return a 0).

Curve: $e = [0, 0, 1, -1, 0]$
N = 37 L = 1 # = 1 r = 1

Table 3.1: Multiple values for $37A1$.

Table of multiple values of g.	
q	1 P
3	1
5	4
7	2
11	4
13	4
17	2
19	17
23	8
29	25
31	14
37	0
41	1
43	16
47	18
53	10
59	26
61	20
67	19
71	10
73	69
79	2
83	12
89	49
97	22
The end	

Curve: $e = [0, 1, 1, 0, 0]$
N = 43 L = 1 # = 1 r = 1

Table 3.2: Multiple values for $43A1$.

Table of multiple values of g.	
q	1 P
3	1
5	4
7	4
11	5
13	3
17	13
19	7
23	8
29	5
31	7
37	7
41	16
43	0
47	16
53	24
59	49
61	3
67	33
71	43
73	49
79	2
83	63
89	68
97	64
The end	

Curve: $e = [0, -1, 1, -2, 2]$
N = 57 L = 1 # = 1 r = 2

Table 3.3: Multiple values for $57A1$.

Table of multiple values of g.		
q	1 P	2 P
3	0	0
The end		

Table 3.3: (continued)

Table of multiple values of g.		
q	1 P	2 P
5	1	4
7	1	4
11	4	9
13	10	10
17	2	4
19	0	0
23	12	12
29	16	16
31	2	2
37	28	28
41	23	23
43	23	36
47	9	1
53	25	25
59	15	15
61	57	47
67	37	37
71	50	50
73	71	16
79	36	36
83	33	33
89	80	80
97	11	11
The end		

Curve: $e = [0, 0, 0, -4, 4]$
N = 88 L = 1 # = 1 r = 4

Table 3.4: Multiple values for $88A1$.

Table of multiple values of g.				
q	1 P	2 P	3 P	4 P
3	1	1	1	1
5	4	1	1	1
7	2	1	1	2
11	0	0	0	0
13	4	3	3	4
17	9	9	9	9
19	7	7	7	7
23	1	6	1	13
29	16	6	6	16
31	8	2	8	16
37	34	27	34	16
41	36	21	21	36
43	17	25	25	17
47	12	12	12	12
53	9	9	9	9
59	15	48	1	48
61	27	47	47	27
67	10	36	40	36
71	25	24	29	24
73	67	49	49	67
79	18	72	72	18
83	27	25	25	27
89	87	44	87	11
97	75	43	9	43
The end				

Curve: $e = [0, 1, 1, 13, 42]$
N = 91 L = 2 # = 2 r = 3

Table 3.5: Multiple values for $91B2$.

Table of multiple values of g.			
q	1 P	2 P	3 P
3	1	1	1
The end			

Table 3.5: (continued)

Table of multiple values of g.			
q	1 P	2 P	3 P
5	1	1	1
7	0	0	0
11	4	4	4
13	0	0	0
17	2	2	2
19	7	7	7
23	4	4	4
29	24	24	24
31	16	16	16
37	36	36	36
41	25	25	25
43	41	41	41
47	2	2	2
53	10	10	10
59	51	51	51
61	58	58	58
67	14	14	14
71	64	64	64
73	8	8	8
79	52	52	52
83	11	11	11
89	57	57	57
97	1	1	1
The end			

Curve: $e = [0, 1, 1, -117, -1245]$
N = 91 L = 2 # = 3 r = 9

Table 3.6: Multiple values for $91B3$.

Table of multiple values of g.									
q	1 P	2 P	3 P	4 P	5 P	6 P	7 P	8 P	9 P
3	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	0	0
7	0	0	0	0	0	0	0	0	0
11	9	1	1	9	4	1	1	1	4
13	0	0	0	0	0	0	0	0	0
17	15	15	9	4	15	15	4	9	15
19	9	9	9	9	9	9	9	9	9
23	6	18	18	6	2	18	18	18	2
29	16	1	1	16	24	1	1	1	24
31	9	9	9	9	9	9	9	9	9
37	27	27	27	27	27	27	27	27	27
41	36	1	1	36	25	1	1	1	25
43	9	9	9	9	9	9	9	9	9
47	21	21	21	21	21	21	21	21	21
53	28	28	28	28	28	28	28	28	28
59	5	5	28	9	5	5	9	28	5
61	57	57	57	57	57	57	57	57	57
67	54	54	54	54	54	54	54	54	54
71	10	10	12	64	10	10	64	12	10
73	2	2	2	2	2	2	2	2	2
79	76	76	76	76	76	76	76	76	76
83	7	7	7	7	7	7	7	7	7
89	80	4	4	80	87	4	4	4	87
97	61	61	61	61	61	61	61	61	61
The end									

Curve: $e = [0, 1, 0, -40, 84]$
N = 112 L = 1 # = 2 r = 4

Table 3.7: Multiple values for $112A2$.

Table of multiple values of g.				
q	1 P	2 P	3 P	4 P
3	1	1	1	1
The end				

Table 3.7: (continued)

Table of multiple values of g.				
q	1 P	2 P	3 P	4 P
5	1	4	4	1
7	0	0	0	0
11	5	5	5	5
13	12	9	9	12
17	16	16	16	16
19	5	1	1	5
23	8	8	8	8
29	9	9	9	9
31	18	18	18	18
37	36	36	36	36
41	25	25	25	25
43	9	9	9	9
47	28	28	28	28
53	36	36	36	36
59	36	26	26	36
61	56	41	41	56
67	65	65	65	65
71	30	30	30	30
73	9	9	9	9
79	21	21	21	21
83	3	12	12	3
89	87	87	87	87
97	35	35	35	35
The end				

Curve: $e = [1, 0, 1, 112, -4194]$
N = 130 L = 1 # = 4 r = 6

Table 3.8: Multiple values for $130A4$.

Table of multiple values of g.						
q	1 P	2 P	3 P	4 P	5 P	6 P
3	1	0	0	1	0	0
5	0	0	0	0	0	0
7	4	4	4	4	4	4
11	4	4	4	4	4	4
13	0	0	0	0	0	0
17	4	4	4	4	4	4
19	9	9	9	9	9	9
23	16	16	16	16	16	16
29	25	25	25	25	25	25
31	10	10	10	10	10	10
37	16	16	16	16	16	16
41	40	40	40	40	40	40
43	21	21	21	21	21	21
47	8	8	8	8	8	8
53	10	10	10	10	10	10
59	53	53	53	53	53	53
61	15	15	15	15	15	15
67	25	25	25	25	25	25
71	19	19	19	19	19	19
73	2	2	2	2	2	2
79	36	36	36	36	36	36
83	16	16	16	16	16	16
89	67	67	67	67	67	67
97	16	16	16	16	16	16
The end						

Curve: $e = [0, 1, 1, -12, 2]$
N = 141 L = 1 # = 1 r = 7

Table 3.9: Multiple values for $141A1$.

Table of multiple values of g.							
q	1 P	2 P	3 P	4 P	5 P	6 P	7 P
3	0	0	0	0	0	0	0
The end							

Table 3.9: (continued)

Table of multiple values of g.							
q	1 P	2 P	3 P	4 P	5 P	6 P	7 P
5	4	1	4	1	1	1	1
7	4	4	1	4	4	1	4
11	9	9	1	9	9	9	1
13	10	4	12	10	12	4	10
17	15	15	13	15	15	15	13
19	5	6	7	5	7	6	5
23	2	18	18	2	2	1	2
29	25	22	22	25	25	24	25
31	25	25	20	20	25	25	16
37	33	1	33	16	1	1	16
41	10	8	8	10	10	31	10
43	6	6	6	6	6	6	6
47	0	0	0	0	0	0	0
53	17	52	47	17	47	52	17
59	28	16	28	49	16	16	49
61	12	47	47	12	12	57	12
67	14	14	9	14	14	14	9
71	3	3	27	3	3	27	3
73	3	3	49	49	3	3	46
79	50	50	55	50	50	55	50
83	40	40	28	40	40	28	40
89	81	81	9	81	81	81	9
97	64	64	61	61	64	64	93
The end							

Curve: $e = [1, -1, 1, -9, 9]$
N = 158 L = 1 # = 1 r = 8

Table 3.10: Multiple values for $158A1$.

Table of multiple values of g.								
q	1 P	2 P	3 P	4 P	5 P	6 P	7 P	8 P
3	1	1	1	1	1	1	1	1
5	4	1	1	1	4	1	4	1
7	2	1	2	2	1	2	1	2
11	4	9	4	5	5	4	9	4
13	1	4	1	1	4	1	4	1
17	9	9	8	2	15	15	2	8
19	1	1	6	4	5	5	4	6
23	6	13	13	6	9	6	6	9
29	25	25	25	25	25	25	25	25
31	19	28	28	19	7	19	19	7
37	16	16	16	16	16	16	16	16
41	21	21	21	21	21	21	21	21
43	10	10	10	10	10	10	10	10
47	24	2	24	24	2	24	2	24
53	10	29	29	10	47	10	10	47
59	15	48	15	15	48	15	15	48
61	19	20	20	19	5	19	19	5
67	23	23	14	25	56	56	25	14
71	18	1	18	18	1	18	1	18
73	69	69	69	69	69	69	69	69
79	0	0	0	0	0	0	0	0
83	70	41	70	31	31	70	41	70
89	4	16	1	16	4	1	64	1
97	24	6	24	24	6	24	24	6
The end								

Curve: $e = [0, -1, 0, -72, 496]$
N = 208 L = 1 # = 2 r = 12

Table 3.11: Multiple values for $208A2$.

Table of multiple values of g.												
q	1 P	2 P	3 P	4 P	5 P	6 P	7 P	8 P	9 P	10 P	11 P	12 P
3	1	1	1	1	1	1	1	1	1	1	1	1
5	4	4	1	4	4	4	1	4	4	4	1	4
The end												

Table 3.11: (continued)

Table of multiple values of g.												
q	1 P	2 P	3 P	4 P	5 P	6 P	7 P	8 P	9 P	10 P	11 P	12 P
7	2	4	2	1	2	4	2	1	2	4	2	1
11	1	4	4	1	1	4	4	1	1	4	4	1
13	0	0	0	0	0	0	0	0	0	0	0	0
17	13	13	1	13	13	13	1	13	13	13	1	13
19	4	6	16	4	11	16	16	11	4	16	6	4
23	12	12	12	12	12	12	12	12	12	12	12	12
29	5	5	5	5	5	5	5	5	5	5	5	5
31	20	1	20	20	1	20	20	1	20	20	1	20
37	33	26	21	26	33	26	21	26	33	26	21	26
41	20	39	39	20	20	39	39	20	20	39	39	20
43	25	16	25	13	11	9	25	4	25	9	11	13
47	27	8	27	2	27	8	27	2	27	8	27	2
53	28	6	6	28	28	6	6	28	28	6	6	28
59	17	9	9	17	17	9	9	17	17	9	9	17
61	47	5	5	47	47	5	5	47	47	5	5	47
67	17	35	1	17	59	1	1	59	17	1	35	17
71	50	54	58	54	50	54	58	54	50	54	58	54
73	3	3	3	3	3	3	3	3	3	3	3	3
79	64	72	64	64	72	64	64	72	64	64	72	64
83	9	9	9	9	9	9	9	9	9	9	9	9
89	8	8	8	8	8	8	8	8	8	8	8	8
97	12	12	12	12	12	12	12	12	12	12	12	12
The end												

Chapter 4

Mazur-Tate conjecture for $|S| > 1$.

4.1 Mazur and Tate for multiple primes

In this section, we present computational evidence related to the Mazur-Tate conjecture for the case $S = \{q_1, q_2, \ldots, q_n\}$ where q_1,...,q_n are primes of good reduction at E.

The left hand side of the equation is defined in the obvious way.

Definition 4.1.1. Set $m_S = q_1 \cdots q_n$. Then, the modular element in this case is:

$$l(S) = \prod_{a \in (\mathbb{Z}/m_S\mathbb{Z})^*} a^{[a/m_S]^+} \tag{4.1}$$

Now, we also generalize the definition of the g function.

Definition 4.1.2. If we set $n_S = n_{q_1} \cdots n_{q_n}$ and $Q = n_S Q$, then the g function is given by

$$g(P, Q_S, m_S) = \frac{d(P' + P)d(P' + Q_S)}{d(P')d(P' + P + Q_S)} \pmod{m_S} \tag{4.2}$$

Of course, we have again that this function is bi-multiplicative and satisfies the identities and properties of the previous chapters. We won't go over those details again here.

Now, to simplify notation, denote $g(S) = g(P, Q_S, m_S)$. We have the following proposition:

Proposition 4.1.1. *If $T \subset S$, then*

$$g(S) = g(T)^{n_S/n_T} \ \textit{(mod } n_T\textit{)} \tag{4.3}$$

Proof. This is straightforward:

$$g(P, n_S Q, m_T) = g(P, (n_S/n_T) n_T Q, m_T) = g(P, n_T Q, m_T)^{n_S/n_T} \qquad \square$$

Hence, for computing $g(S)$, we only need to get $g(q_i)$ for $1 \leq i \leq n$ and to solve the system of congruences:

$$x \equiv g(q_i)^{n_S/n_T} \pmod{q_i} \tag{4.4}$$

If we have all the values of g already computed, this is trivially done.

Now, to define the right hand side of the Mazur-Tate conjecture, we need the elementary proposition:

Proposition 4.1.2. *For $M \mid N$ such that $gcd(M, N/M) = 1$, the map:*

$$y_{\{M,N\}} : (\mathbb{Z}/M\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^* \tag{4.5}$$

given by

$$a \to b^{\phi(N/M)} \tag{4.6}$$

where $b \in (\mathbb{Z}/N\mathbb{Z})^*$, $b \equiv a$ (mod M) and ϕ is the phi of Euler function is well defined

Proof. Let b_1,$b_2 \in (\mathbb{Z}/N\mathbb{Z})^*$ such that $b_1 \equiv b_2 \pmod{M}$. Assume $b_1 = b_2 + kM$. We would like to prove that: $b_1^{\phi(N/M)} \equiv b_2^{\phi(N/M)} \pmod{N}$.

Now, clearly $b_1^{\phi(N/M)} \equiv b_2^{\phi(N/M)} \pmod{N/M}$. So, we just need to see:

$$\begin{aligned} b_1^{\phi(N/M)} =& (b_2 + kM)^{\phi(N/M)} & (4.7) \\ =& b_2^{\phi(N/M)} + kM(b_2^{\phi(N/M)} + \text{other terms}) & (4.8) \end{aligned}$$

So, $b_1^{\phi(N/M)} \equiv b_2^{\phi(N/M)} \pmod{M}$ and hence the proposition follow because $gcd(M, N/M) = 1$.

□

Definition 4.1.3. We define the right hand side of the equation or the Capital G function as:

$$G(S) = \prod_{T \subset S} y_{\{T,S\}}(g(T))^{(-1)^{(1+\#(T))}} \tag{4.9}$$

where $y_{\{T,S\}} = y_{\{m_T,m_S\}}$.

Now, to compute $G(S)$ we can use the following:

Proposition 4.1.3. *The following congruence is true:*

$$G(S) \equiv g(q_i)^{e(q_i,S)} \ (\textit{mod } q_i) \tag{4.10}$$

where

$$e(q_i, S) = \sum_{q_i \in T \subset S} (-1)^{(1+\#(T))}(n_T/n_{q_i})\phi(m_S/m_T) \tag{4.11}$$

Proof. If $q_i \in T$, then from the following congruences:

$$g(T) \equiv g(q_i)^{n_T/n_{q_i}} \pmod{q_i} \tag{4.12}$$

and

$$y_{\{T,S\}}(g(T)) \equiv b^{\phi(m_S/m_T)} \pmod{m_S} \tag{4.13}$$

for $b \equiv g(T) \pmod{m_T}$, we obtain that:

$$y_{\{T,S\}}(g(T)) \equiv g(q_i)^{(n_T/n_{q_i})\phi(m_S/m_T)} \pmod{q_i} \tag{4.14}$$

If $q_i \notin T$, then $y_{\{T,S\}}(g(T)) \equiv 1 \pmod{q_i}$, because the map $y_{\{T,S\}}$ implies to raise to the power $\phi(m_S/m_T)$ which is divided by $q_i - 1$.

Hence, the proposition follows from splitting $G(S)$ as the product:

$$\prod_{q \in T \subset S} y_{\{T,S\}}(g(T))^{(-1)^{(1+\#(T))}} \prod_{q \notin T \subset S} y_{\{T,S\}}(g(T))^{(-1)^{(1+\#(T))}} \tag{4.15}$$

The last term in the product is trivial, so:

$$\begin{aligned} G(S) &= \prod_{q \in T \subset S} y_{\{T,S\}}(g(T))^{(-1)^{(1+\#(T))}} \pmod{q_i} && (4.16)\\ &= \prod_{q \in T \subset S} \left(g(q_i)^{(n_T/n_{q_i})\phi(m_S/m_T)}\right)^{(-1)^{(1+\#(T))}} \pmod{q_i} && (4.17)\\ &= g(q_i)^{e(q_i,S)} \pmod{q_i} && (4.18) \end{aligned}$$

□

In order to compute efficiently the values $e(q_i, S)$, we will have to introduce some symmetric functions. Let I_k be the set of integers from 1 to $k \in \mathbb{Z}$. Denote $Per(i, n)$ the set of all 1-1 increasing maps $\sigma : I_i \to I_n$. Now, assume that we have n-variables X_i for $1 \leq i \leq n$. Thus, denote:

$$X_\sigma = \prod_{j=1}^{i} X_{\sigma(j)} \tag{4.19}$$

for $\sigma \in Per(i, n)$.

Also, let $X = \prod_{j=1}^{n} X_j$ and $\hat{X}_\sigma = X/X_\sigma$.

For $(X, Y) \in \mathbb{A}^n \times \mathbb{A}^n$, define the following "bi-symmetric" function:

$$\partial^n(X, Y) = \sum_{i=1}^{n} (-1)^i \sum_{\sigma \in Per(i,n)} X_\sigma \hat{Y}_\sigma \tag{4.20}$$

Also, given $(X, Y) \in \mathbb{A}^n \times \mathbb{A}^n$ with $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$, define the map:

$$s_i : \mathbb{A}^n \times \mathbb{A}^n \to \mathbb{A}^{n-1} \times \mathbb{A}^{n-1} \tag{4.21}$$

given by

$$((X_1, \ldots, X_n), (Y_1, \ldots, Y_n)) \to ((X_1, \ldots \hat{X}_i \ldots, X_n), (Y_1, \ldots \hat{Y}_i \ldots, Y_n)) \tag{4.22}$$

where $(X_1, \ldots \hat{X}_i \ldots, X_n)$ means that we exclude the X_i coordinate from the vector $(X_1, \ldots, X_n)$.

Using this notation, we have the following identity:

$$e(q_i, S) = \partial^{n-1} \circ s_i(\vec{q}, \vec{n}) \tag{4.23}$$

where $\vec{q} = (q_1 - 1, \ldots, q_n - 1)$ and $\vec{n} = (n_{q_1}, \ldots, n_{q_n})$.

We summarize our methods to compute $G(S)$ in the following algorithm:

Algorithm 4.1.1. Algorithm to compute $G(S)$.

1. Compute the values $g(q_i)$ for all $q_i \in S$.

2. Compute the functions s_i and evaluate $s_i((\vec{q}, \vec{n}))$.

3. Calculate the symmetric function ∂^{n-1} and evaluate at $s_i((\vec{q}, \vec{n})$.

4. Solve the congruences:

$$X \equiv g(q_i)^{\partial^{n-1} \circ s_i(\vec{q},\vec{n})} \pmod{q_i} \tag{4.24}$$

Using the above algorithm, we can test for the Mazur and Tate conjecture in the case:

Conjecture 4.1.4. *Mazur-Tate for many primes.*

The following identity is also true:

$$l(S)^{uv} = G(S)^{|Ш||coker(\phi)|} \tag{4.25}$$

Here, ϕ is the function in section 3 (It is not the ϕ of Euler).

We tested this conjecture for the first 300 curves in Cremona tables [Cre97] and for all the combinations of two primes $3 \leq q_1 < q_2 \leq 50$.

My last comment is that if we can prove something like proposition 4.1.3 for the function $l(S)$ (i.e. to get $l(S)$ in terms of congruences involving powers of $l(q_i)$ for $q_i \in S$), we may be able to prove that Mazur and Tate for a single prime implies the proposition for many primes. I don't know if that is possible, but it sounds like a reasonable question.

Chapter 5

A computation with non-trivial Tate Shafarevich group

The main problem to test 2.3.1, when we have a non-trivial Tate-Shafarevich group arises from the fact that the conductor N is big enough in those cases to slow down our computations. In fact, the elliptic curve of rank 1 having non-trivial Tate Shafarevich group and smallest conductor has $N = 1610$, and it is given by the equation:

$$y^2 + xy + y = x^3 - x^2 - 8587x - 304111 \tag{5.1}$$

This conductor is about 5 times higher than the curve with biggest conductor in the tables in 2.4.1. In practice, this means a lot of computing time. Everytime, we tried to solve the linear algebra of the modular symbols, using the function *ellsym(e,1)* in *modsym.gp*, we had to Shut down the process after a several days of getting nothing. Also, we attempted to use the aproximations

1. $$[a/b]^+ \approx \left(\sum_{i=1}^{INDEX} \frac{a_n}{n} cos\left(2\pi n\left(\frac{a}{b}\right)\right)\right)/\Omega^+ \tag{5.2}$$

2. $$[a/b]^+ \approx \left(lim_{y\to 0} \sum_{i=1}^{INDEX} \frac{a_n}{n} e^{-2y\pi n} cos\left(2\pi n\left(\frac{a}{b}\right)\right)\right)/\Omega^+ \tag{5.3}$$

(Suggested by Fernando Rodriguez-Villegas and John Tate)

We use different values for $INDEX$ and y, but the changes made the approximations differ badly, and we were not confident about the results. Hence, we insisted in computing the linear algebra of the modular symbols. This time, we took the simple tactic of "divide and conquer". So, instead of running the whole function *ellsym(e,1)*, we computed each of the proceses inside of this function, separetely. We didn't change the algorithm, nor the sequel in which it was computed, but the machine worked better having just a simple task to perform. Finally, we were able to compute the linear algebra, after a couple of days.

The important information of these computations was recorded in a 296×3456 matrix, which represented the linear combinations of 3456 G-symbols (for $G = \Gamma_0(1610)$) in terms of 296 generators. (See Cremona's book to read about G-symbols [Cre97]) We noticed that all the entries were divisible by 4, which impplies that the values $[a/b]^+$ (obtain with the program *modsym.gp* will be also divisible by 4. Hence, the actual values $[a/b]^+$ are in the range:

$$[a/b]^+ \in D\ (Prog(a/b) - 2, Prog(a/b) + 2) \tag{5.4}$$

where D is the constant that we want to compute as in section 2.4 and $Prog(a/b)$ represents the value $[a/b]^+$ obtained from the program.

To compute D, we took the primes $q =$ 11,13 and calculate the vectors $([i/q]^+)_{i=1}^{q-1}$. Using the series approximation 5.3 with $INDEX = 20,000$ and $y = .00002$, we obtained after rounding the following vectors:

$q = 11$

$(4, 3, -3, -4, -1, -1, -4, -3, 3, 4)$

$q = 11$

$(11, 4, -3, -5, 3, -11, -11, 3, -5, -3, 4, 11)$

And, using the information of the matrix, the values were:

$q = 11$

$(4, 4, -4, -4, 0, 0, -4, -4, 4, 4)$

$q = 13$

$(12, 4, -4, -4, 4, -12, -12, 4, -4, -4, 4, 12)$

From, these computations, we conclude that $D = 1$, and that the approximation of the series was among the aceptable interval:

$$([a/b]^+ - 2, [a/b]^+ + 2) \tag{5.5}$$

5.0.1 Tables with Big Shafarevich

To check for the conjecture, we had to compute the values u, v, r and C as mention in section 2.4, and also the generators of E_0.

The following tables show this computations for the elliptic curves with $rank(E) = 1$, and $|Ш| > 1$ as listed in the file *allbigsha.1-8000* in John Cremona's Web site [Cre03]. The generators of E were obtained from the file *allgens.1-8000*, also in John Cremona's Web Site.

Table 5.1: Table of generators for E and E_0 with $|\text{Ш}| > 1$.

Table of generators for E and E_0.				
N	L	#	E	E_0
1610	6	3	[[6996, 11413, 64], [-426, 209, 8]]	[[6996, 11413, 64], [-426, 209, 8]]
2184	13	5	[[675, 13530, 1], [-225, 0, 1]]	[[675, 13530, 1], [-225, 0, 1]]
2478	7	3	[[31511, 5361297, 1], [-38234, 19113, 8]]	-too long
2574	10	3	[[705, 1045, 1], [-2810, 1405, 8]]	[[705, 1045, 1]]
3192	14	3	[[501, 10776, 1], [-75, 0, 1]]	[[501, 10776, 1], [-75, 0, 1]]
3210	3	3	[[705, 17659, 1], [-858, 425, 8]]	[[1333287293276172, 6898592146675675, 5843671777728], [-858, 425, 8]]
3990	1	3	[[-49, 26, 1], [-394, 197, 8]]	[[-49, 26, 1]]
4074	12	5	[[58120, 13919050, 1], [-25090, 12545, 8]]	[[405866978020555778714802890, 455511379629292197988483573, 27136016283106337310000], [-25090, 12545, 8]]
4080	31	3	[[370909, 9761928, 343], [-341, 0, 1]]	[[370909, 9761928, 343], [-341, 0, 1]]
4305	13	5	[[73044, 463263, 64], [-4482, 2241, 8]]	[[73044, 463263, 64], [-4482, 2241, 8]]
4641	1	3	[[415, 7532, 1], [-730, 361, 8]]	[[415, 7532, 1], [-730, 361, 8]]
4680	7	3	[[626, 13804, 1], [-158, 0, 1]]	[[626, 13804, 1]]
4830	20	3	[[-39, 20, 1], [-314, 153, 8]]	[[-98565048, 51284241, 2515456]]
5190	16	3	[[332616, 3947487, 512], [-2306, 1153, 8]]	-too long
5208	12	3	[[867, 19686, 1], [-289, 0, 1]]	[[115883770636473031736813880518355 1, -113719407069855930754639905829034 93478, 1203368627147188426589813 3], [-289, 0, 1]]
6006	30	5	[[404102, 85009439, 8], [-76098, 38049, 8]]	-too long
6090	14	3	[[-58, 30, 1], [-466, 229, 8]]	[[-61789254, 31520551, 1061208]]
6150	14	7	[[26122, 2403776, 1], [-87474, 43733, 8]]	[[948898368439098, -240700091016804049, 13600574603]]
6160	4	3	[[151, 390, 1], [-74, 0, 1]]	[[30685294770, -1973025331984, 7414875], [-74, 0, 1]]
The end				

Table 5.1: (continued)

Table of generators for E and E_0.				
N	L	#	E	E_0
6162	17	3	[[-132823880, 66411955, 175616]]	[[-132823880, 66411955, 175616]]
6195	5	3	[[91005, 1250634, 125], [-2522, 1257, 8]]	[[91005, 1250634, 125], [-2522, 1257, 8]]
6390	10	3	[[8867, 823634, 1], [-5114, 2557, 8]]	[[-175554015, 87775592, 274625]]
6402	11	4	[[61, 479, 1], [29, 179, 1]]	[[1476153690, 8232165727, 132651000]]
6450	42	3	[[436, 1592, 1], [-1714, 853, 8]]	[[436, 1592, 1]]
6510	20	3	[[1338, 48081, 1], [-546, 273, 8]]	[[162824298, 2726911537, 474552]]
6630	20	3	[[-355, 183, 1], [-2842, 1417, 8]]	[[-6432326405050, 3136888458861, 18108570376]]
6930	6	3	[[385, -184, 1], [3078, -1539, 8]]	[[385, -184, 1]]
7230	14	2	[[-15, 8, 1], [-122, 57, 8]]	[[-334740, 153357, 21952]]
7230	22	3	[[374, 3428, 1], [-1346, 673, 8]]	-too long
7320	17	3	[[243, 2934, 1], [-81, 0, 1]]	[[243, 2934, 1], [-81, 0, 1]]
7392	6	2	[[1569, 2492, 27], [-29, 0, 1]]	[[1569, 2492, 27], [-29, 0, 1]]
7410	20	3	[[132372, 5793189, 64]]	[[8548440, 112295545, 13824]]
7770	26	5	[[29022, 497049, 8], [3486, -1743, 1]]	[[1227274346684092301280, -272123045660263521628423, 24979031175168000]]
7770	26	6	[[1146157038, -507700151279, 5832], [-55778, 27889, 8]]	[[1146157038, -507700151279, 5832]]
7854	11	3	[[-179, 91, 1], [-1434, 713, 8]]	[[-7519808315716716302723751482, 3713797364587613770490123653, 41952075357784943090604808]]
7854	42	6	[[360, 4650, 1], [2430, -1215, 8]]	[[188238063715170, -7859023165871417, 112678587000]]
7896	5	3	[[838, 19932, 1], [-251, 0, 1]]	[[78445849488963, -1253368286693360, 123729330087], [-251, 0, 1]]
The end				

We exclude the generators of E_0 for a few curves above, because the points were too long to fit nicely in the above table. For instance, for the curve of conductor 2478, we have that the generator of the free part of E_0 is:

[842054006666670826638927695671868489512953328311197160300068661612819268763034128794281565604762661943041870322921206090830496523064514855496059707209069601293999191273452004696009992220045825219413135000460364179697256222353428966712989383434680481143277998605537569704650039089600419973937204713990589271973304 62,

$-$72625904691053859777684646251608153029759554683249950923730959200359012996898502103037135131992005351174927357983660438571727087618395325229486618546542909736320058785265099712321530756160296839987577501932494414984216744370829498163732490116217327226991308991696971892887507699025268191404341606298322631566188 3263,

878361397212657694740728735061656523356678553488941505898038703965260791747417364734543669010722966215622681253559211334600694743207940350780762397538642357181860072596685716481505695269324253097067002250981769157420452061544697255590058931898010653688913077270723299699789212524090288083017615687438297021623 2]

The next table is like the second table in 2.4.1; except that now we add the equation of the curve, the order of the cokernel of ϕ and the order $|Ш|$.

Table 5.2: Table of values for conjecture with $|Ш| > 1$.

Table of values for conjecture.									
N	L	#	e	$\|Ш\|$	r	u	v	C	coker(ϕ)
1610	6	3	[1, -1, 1, -8587, -304111]	4	1	2	2	1	1
2184	13	5	[0, 1, 0, -151424, -22730400]	4	1	2	2	2	2
2478	7	3	[1, 1, 1, -68511744, -218299350495]	4	7	2	2	7	1
The end									

Table 5.2: (continued)

Table of values for conjecture.									
N	L	#	e	|Ш|	r	u	v	C	coker(ϕ)
2574	10	3	[1, -1, 0, -370656, -86764370]	4	1	2	1	2	1
3192	14	3	[0, -1, 0, -17024, -849300]	4	1	2	2	1	1
3210	3	3	[1, 1, 1, -34240, -2452915]	4	2	2	2	2	1
3990	1	3	[1, 1, 0, -7108, -233642]	4	1	2	1	2	1
4074	12	5	[1, 0, 0, -29506624, -61694252620]	4	2	2	2	8	4
4080	31	3	[0, 1, 0, -348160, -79187020]	4	1	2	2	2	2
4305	13	5	[1, 0, 0, -941360, -351624105]	4	1	2	2	2	2
4641	1	3	[1, 1, 1, -24752, -1509184]	4	1	2	2	1	1
4680	7	3	[0, 0, 0, -74883, -7887202]	4	1	2	1	2	1
4830	20	3	[1, 1, 1, -4491, -117711]	4	3	2	1	6	1
5190	16	3	[1, 0, 0, -249120, -47879478]	4	3	2	2	3	1
5208	12	3	[0, 1, 0, -249984, -48191328]	4	3	2	2	3	1
6006	30	5	[1, 0, 0, -271443794, -1721367884082]	4	4	2	1	32	4
6090	14	3	[1, 0, 1, -10098, -391382]	4	3	2	1	6	1
6150	14	7	[1, 0, 1, -358668001, -2614520347102]	4	2	2	1	16	4
6160	4	3	[0, 0, 0, -16427, -810374]	4	2	2	2	2	1
6162	17	3	[1, 0, 0, -1715733, -865156065]	9	1	1	1	1	1
6195	5	3	[1, 1, 1, -297360, -62536458]	4	1	2	2	1	1
6390	10	3	[1, -1, 0, -1226880, -522753080]	4	1	2	1	2	1
6402	11	4	[1, 1, 1, 508, -2551]	4	2	4	1	8	1
6450	42	3	[1, 0, 1, -137601, -19657652]	4	1	2	1	2	1
6510	20	3	[1, 0, 0, -13901, -631995]	4	2	2	1	4	1
6630	20	3	[1, 1, 1, -377310, -89363493]	4	3	2	1	12	2
6930	6	3	[1, -1, 0, -443520, 113799816]	4	1	2	1	2	1
7230	14	2	[1, 1, 1, -645, -6573]	4	3	2	1	6	1
7230	22	3	[1, 0, 0, -81210, -8907828]	4	12	2	1	48	2
7320	17	3	[0, 1, 0, -19520, -1056240]	4	1	2	2	2	2
7392	6	2	[0, 1, 0, -2464, -47908]	4	1	2	2	1	1
7410	20	3	[1, 0, 0, -208136, -36744390]	9	2	1	1	2	1
7770	26	5	[1, 0, 0, -9114581, -10592163939]	9	2	2	1	8	2
7770	26	6	[1, 0, 0, -145833331, -677861695189]	9	1	2	1	4	2
7854	11	3	[1, 1, 1, -95794, -11451745]	4	5	2	1	10	1
7854	42	6	[1, 0, 0, 83356, -53367660]	4	2	2	1	8	2
7896	5	3	[0, -1, 0, -189504, -31689252]	4	2	2	2	2	1
The end									

Our testing was for the first curve in the above tables, and for primes not dividing 1610 and smaller than 100.

The results as shown in *Pari* were as follows:

$l = [Mod(1,3), 0, 0, Mod(4,11), Mod(3,13), Mod(1,17), Mod(5,19), 0,$ $Mod(20,29), Mod(20,31), Mod(33,37), Mod(10,41), Mod(17,43), Mod(12,47),$ $Mod(42,53), Mod(12,59), Mod(47,61), Mod(56,67), Mod(40,71), Mod(55,73),$ $Mod(44,79), Mod(40,83), Mod(2,89), Mod(61,97)]$

$g = [0, 0, 0, Mod(4,11), Mod(3,13), 0, Mod(5,19), 0, Mod(20,29), Mod(20,31),$ $Mod(33,37), Mod(10,41), Mod(17,43), Mod(12,47), Mod(42,53), Mod(12,59),$ $Mod(47,61), Mod(56,67), Mod(40,71), Mod(55,73), Mod(44,79), Mod(40,83),$ $Mod(2,89), Mod(61,97)]$

From the above results, we can see that the equation $l(q) = g(q)$ must be satisfied for almost all q.

This is a little sharper than the predicted equation $l(q)^4 = g(q)^4$ in the conjecture 2.3.1 (since $u = v = 2$ and $|Ш| = 4$).

Bibliography

[BC] K. Belabas and H. Cohen. Program Pari-2/gp. `http://pari.math.u-bordeaux.fr/`.

[BPRin] B. Bernardi and B. Perrin-Riou. `http://modular.fas.harvard.edu/tables/modsym.gp`. Version for Pari-2 by W. Stein.

[Cre97] J.E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second ed. edition, 1997.

[Cre03] J.E. Cremona. `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`. 7 April 2003.

[Man72] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk. SSSR. Ser. Mat.*, 36:19–66, 1972.

[MT87] B. Mazur and J. Tate. Refined Conjectures of the Birch and Swinnerton-Dyer Type. *Duke Math. J.*, 54:711–750, 1987.

Vita

Francisco Xavier Portillo-Bobadilla was born in Mexico City, on March 27, 1974, son of Olga Yolanda Bobadilla Hernández and Francisco Javier Portillo Ruíz. During his high-school years, he was a student in the *Colegio de Ciencias y Humanidades - Sur*. In 1994, he entered to *La Facultad de Ciencias* in *La Universidad Nacional Autónoma de México*, where he received his B.S degree in Mathematics in August of 1996. Then, he moved to Austin, TX, where he entered to graduate school in September of the same year.

Permanent address: Cerro Zempoala # 14
Colonia Hermosillo
Coyoacán, México 04240

This dissertation was typeset with LaTeX[‡] by the author.

[‡]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.