Hasse-Weil inequality and primality tests in the context of curves of genus 2

Ruíz Duarte, Eduardo

Hasse-Weil Inequality and Primality Tests in the context of Curves of Genus 2

Eduardo Ruíz Duarte

This research is financially supported by the Mexican government through the *Consejo Nacional de Ciencia y Tecnología* (CONACyT, CVU-440153).

ISBN 978-94-034-0700-5 (printed version)
ISBN 978-94-034-0699-2 (electronic version)

rijksuniversiteit
groningen

Hasse-Weil Inequality and Primality Tests in the context of Curves of Genus 2

Proefschrift

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. E. Sterken
en volgens besluit van het College voor Promoties.

De openbare verdediging zal plaatsvinden op

vrijdag 25 mei 2018 om 14.30 uur

door

Eduardo Ruíz Duarte

geboren op 3 november 1984
te Baja California, México

Promotores
Prof. J. Top
Prof. H. Waalkens

Beoordelingscommissie
Prof. P. Beelen
Prof. J-C. Lario
Prof. T. Müller

Contents

To my mother María G. Duarte.

Acknowledgement

First of all I would like to thank my supervisor Prof. Dr. Jaap Top. His passion for mathematics made this survey fun & full of interesting questions. Thank you Jaap for your patience and shared knowledge. You made me understand the importance of rigour when doing and writing mathematics.

Cristina Tapia, one of the main characters on this stage. Your patience, spontaneity & intelligence, always makes me feel peaceful, fun, calm & curious (even in difficult times). You showed me how to be a better man, bringing balance & happiness to my life. Thank you for your ∞ love and laughs. I love you too.

To my family, my mother María Duarte, who is always supporting me and loving me, I love you too. To Gloria Duarte, who taught me how to read & write very early in my life, I am very grateful for that. To Miguel Duarte, he has always supported me since I have memory, giving me good tips in life & trusting me. To Carlos Duarte, who has been a motivation to do science. To Ernesto Duarte, whose heart & humour is big. Also to my *sisters* Atenea Duarte & Aranza Duarte, I am proud of you, I like having a talented artist in my family to show off & a very smart cousin. Also thanks to Maria Elena Corona for being so close to my family.

Thanks to my new friends in Groningen. Jesús Barradas, Hildeberto Jardón & Adrián de la Parra for being there since the beginning of this journey, for being good friends. Also I would like to thank Ane Anema, Marc Noordman & Max Kronberg, for the nice discussions regarding my thesis and also for the fun when enjoying general mathematics. Also thanks to the people who made this a more interesting experience: María, Mauricio, Rodolfo, Nuria, Pablo, Sheviit, Paulina, Alain, Leonel, Beatriz, Alejandro, Pamela, Herson, Mónica, Enis, Estela, Ineke and Venustiano.

To my best friends Rommel Sánchez Verdejo & Omar Lara Salazar who always make me laugh. But must important, you make me think too.

To my reading committee which includes Prof. Dr. Peter Beelen, Prof. Dr. Joan Carles Lario and Prof. Dr. Tobias Müller for taking the time to read and suggest ideas for this thesis.

Special thanks to Prof. Dr. Marius van der Put, Prof. Dr. Michael Stoll, Prof. Dr. Cayetano De Lella, Prof. Dr. Lenny Taelman, Prof. Dr. Holger Waalkens, Prof. Dr. Octavio Páez Osuna, Dr. Robin de Jong, Dr. Arthemy Kiselev, Dr. Elisa Lorenzo García, Dr. Steffen Müller & Dr. Maarten Derickx who where open to my questions during my Ph.D. To CONACyT México, for my grant (CVU-440153).

Introduction

This thesis discusses some attempts to extend specific results and applications dealing with elliptic curves, to the case of curves of genus 2.

The first question is to extend Manin's elementary proof of the Hasse inequality (genus 1) [Man56] to genus 2.
Recall that the Hasse-Weil inequality states that the number of points of a genus g curve over a finite field $\mathbb{F}_q$ of cardinality q is $q+1-t$ where $|t| \leq 2g\sqrt{q}$. The special case $g = 1$ of this result was originally proven by Hasse in the 1930's and it is called the Hasse inequality.
In Chapter 1 we revisit Manin's proof of the Hasse inequality. Although the proof has already been revisited (see for example [Soo13]), we rearranged and simplified the argument even further. We also added (although well-known) a less elementary proof of the Hasse inequality in order to make a comparison and appreciate the elementariness of Manin's argument.

The main idea to prove the Hasse inequality for an elliptic curve $E/\mathbb{F}_q$ is to obtain a formula for the degree d_n of the sum $F + [n]$ of the Frobenius map $F\colon E \to E$ that raises every coordinate of a point on E to the q-th power, and the *multiplication by* n map defined by $[n](P) = nP$ (by convention $d_n = 0$ if $F + [n]$ is the zero map).
Manin restricted himself to an elliptic curve E given by an equation $y^2 = x^3 + Ax + B$. In particular this means he ignored the case that q is a power of 2, and also for q a power of 3, he did not describe all possible elliptic curves. Taking a variable x over $\mathbb{F}_q$ and y in an extension of $\mathbb{F}_q(x)$ with $y^2 = x^3 + Ax + B$, Manin's idea can be described as follows. The point $(x, y) \in E$ yields

$$\mathfrak{Q}_n := (F + [n])(x, y) = (x^q, y^q) + [n](x, y) \in E.$$

If $\mathfrak{Q}_n$ is non-trivial, then the x-coordinate of $\mathfrak{Q}_n$ is a rational function $\frac{\alpha_n(x)}{\beta_n(x)}$

with $\alpha_n(x), \beta_n(x) \in \mathbb{F}_q[x]$ coprime polynomials. The degree of the polynomial $\alpha_n(x)$ is in fact d_n and Manin uses this to show that d_n satisfies the recurrence formula $d_{n+1} + d_{n-1} = 2d_n + 2$. As Cassels correctly remarked in his review [Cas56], Manin's argument relies on the assumption that $\deg(\alpha_n(x)) > \deg(\beta_n(x))$ and Manin did not comment on this assumption. Various authors after this either provided proofs of Manin's assumption, or worked out the details of Cassels' suggestion on how one might avoid the assumption in the argument. In this thesis, by an elementary observation we present a very short and simple new proof of the claim $\deg \alpha_n(x) > \deg \beta_n(x)$, compared with previous proofs (e.g. [GL66, Chapter 10, Lemma 3], [Cha88, Lemma 8.6], [Kna92, Theorem 10.8] or [Soo13, Lemma 5.3.1]).
Clearly $d_0 = q$ and it can be shown that $d_{-1} = \#E(\mathbb{F}_q)$. Further, since d_n satisfies a second order recursion formula, we obtain that

$$d_n = n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q.$$

From the observation that $d_n \geq 0$ and that it cannot be zero for two consecutive integers n, it follows that the discriminant of the quadratic polynomial $x^2 + (q + 1 - \#E(\mathbb{F}_q))x + q$ is ≤ 0, which shows the Hasse inequality.
Chapter 1 is a preamble to the proof of the Hasse-Weil inequality for genus 2 presented in Chapter 3.

In Chapter 2 we essentially do technical work. Starting from a genus 2 curve $\mathcal{H}$ with equation $y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ over a field k, we construct and explore the function field of the associated Jacobian variety $\mathcal{J}$ and of the Kummer surface $\mathcal{K}$. The function field $k(\mathcal{K})$ may be used to give us a geometric interpretation of our proof of the Hasse-Weil inequality for genus 2 presented in Chapter 3.
We obtain $k(\mathcal{J})$ through an explicit affine open subset of $\mathcal{J}$ using the so called *Mumford representation* of the points of $\mathcal{J}$. This representation is popular in the cryptographic literature and is also used in most symbolic algebra software like MAGMA or SAGE to do arithmetic in $\mathcal{J}(k)$ (see [Can87]). Further, using this representation, we describe some families of functions in $k(\mathcal{J})$ that will be used in subsequent chapters. Moreover, we introduce and study a specific function $\kappa_4 \in k(\mathcal{J})$ directly related to the Kummer surface $\mathcal{K}$, and we compute the poles of this function. The same κ_4 was used by Flynn, see [Fly93, Equation (6)] but here more details on its construction and properties are presented. The function κ_4 will be fundamental in our proof of the Hasse-Weil inequality for genus 2 *à la Manin*.

In Chapter 3, we answer the first question of this thesis: we mimic Manin's

proof of the Hasse inequality and obtain a proof for the Hasse-Weil inequality for all hyperelliptic curves $\mathcal{H}/\mathbb{F}_q$ of genus 2 given by an equation $y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. The idea is to construct an integer analogous to d_n as it appears in Manin's original proof. The strategy is to first embed $\mathcal{H}$ in its Jacobian $\mathcal{J}$ via the map $P \mapsto [P - \infty]$. The image of this map is denoted $\Theta \subset \mathcal{J}$. Next, introduce the curve $\Theta_n \subset \mathcal{J}$ as the image of $\Theta \cong \mathcal{H}$ under $F + [n]$ where F is the q-th power Frobenius map and $[n]$ the *multiplication by n* map on $\mathcal{J}$ (the special case where $F + [n]$ is the zero map, so that Θ_n is not a curve, is in fact simpler and it is treated separately). Assuming that Θ_n is a curve, we assign an intersection number δ_n to the pair of curves Θ_n and Θ.
To mimic Manin's approach, we use the rational function κ_4 obtained in Chapter 2. This allows us to describe the proposed intersection number in a much more elementary way. We restrict κ_4 to Θ_n, thus obtaining a rational map $\mathcal{H} \to \mathbb{P}^1$. Provided this map is not constant, its degree is related to the intersection number δ_n.

We obtain the second order recurrence formula $\delta_{n-1} + \delta_{n+2} = 2\delta_n + 4$. Unfortunately the proof we found for this requires the interpretation of δ_n as an intersection number. To have a proof of the Hasse-Weil inequality in the spirit of Manin, an argument relying on the interpretation of δ_n in terms of degrees of rational maps is preferred, but we did not find such.
After showing that $\delta_0 = 2q$ and $\delta_{-1} = q + 1 + \#\mathcal{H}(\mathbb{F}_q)$ we obtain the formula $\delta_n = 2n^2 + (q + 1 - \#\mathcal{H}(\mathbb{F}_q))n + 2q$. With this, our proof of the Hasse-Weil inequality for genus 2 can be completed similar to Manin's original argument. In conclusion, our proof relies on some theory of Abelian surfaces and on some intersection theory, making it less elementary than Manin's proof for genus 1, but still quite accessible for graduate students.

As a matter of a personal experience, our first attempt to get δ_n, was to experiment with elements of $\mathcal{J}(\mathbb{F}_q(\mathcal{J})) \cong \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{J}, \mathcal{J})$. We did this since Manin worked with elements of $E(\mathbb{F}_q(E)) \cong \mathrm{Mor}_{\mathbb{F}_q}(E, E)$. Using $\mathrm{Mor}_{\mathbb{F}_q}(\mathcal{J}, \mathcal{J})$, resulted in a very complicated situation due to the difficulty in the representation of its objects. The more successful approach to define a sequence δ_n and prove a recursive formula for it, was found after experimenting with $\mathcal{J}(\mathbb{F}_q(\mathcal{H})) \cong \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$.

In Chapter 4 we consider a second question. The idea is to extend methods of primality testing using elliptic curves to hyperelliptic curves. A framework for such tests using elliptic curves is given in the master's thesis of Wieb Bosma

[Bos85] and more recently in a paper [ASSW16] by Abatzoglou, Silverberg, Sutherland, and Wong. An explicit example where such elliptic curves methods are applied to Mersenne numbers $M_p := 2^p - 1$ is given in a paper by Benedict Gross [Gro05]. He uses the rank 1 elliptic curve $E : y^2 = x^3 - 12x$. Gross observes that when $q \equiv 7 \bmod 24$ is prime, the point $P := (-2, 4)$ is not divisible by 2 in $E(\mathbb{F}_q)$ and the latter group is cyclic of order $q + 1$. Using this, he proves that M_p is prime if and only if $2^k P \in E(\mathbb{Q})$ is a well defined point modulo M_p for $1 \leq k \leq p - 1$ and $2^{p-1} P = (0, 0)$. This result by Gross can be implemented as an algorithm using recursive doubling of P in E.

We begin with primality tests using conics before discussing elliptic curves and (Jacobians of) genus 2 curves. Note that a paper by Hambleton [Ham12] discusses Pell conics for primality testing. Here for the sake of motivation, we start using some specific conics to do primality tests, namely the ones given as the zeros of $xy - 1$ and $x^2 + y^2 - 1$.
We interpret Pépin's test for Fermat numbers $\mathcal{F}_n := 2^{2^n} + 1$ geometrically, in terms of a group structure on the conic $\mathfrak{h}$ given by $xy = 1$. For the ring $R := \mathbb{Z}/(\mathcal{F}_n)$, the group $\mathfrak{h}(R)$ has order 2^{2^n} if and only if $\mathcal{F}_n$ is prime. Further if $\mathcal{F}_n$ is prime, we have that $R^\times$ is cyclic. A primality test based on this is obtained by choosing an $(\alpha, \frac{1}{\alpha}) \in \mathfrak{h}(R)$ where $\alpha \notin (\mathbb{Z}/(\mathcal{F}_n))^{\times 2}$ and then repeatedly doubling it in the group $\mathfrak{h}(R)$. It turns out that $\mathcal{F}_n$ is prime if and only if we obtain the point $(-1, -1) \in \mathfrak{h}(R)$ of order two after doubling $2^n - 1$ times.

Similarly, we show how to do primality tests for certain integers of the form $\mathcal{A}_{m,n} := m2^n - 1 \equiv \pm 2 \bmod 5$ where $m < 2^n - 2 + \frac{2}{2^n}$. We use the group structure of the conic $\mathfrak{C} : x^2 + y^2 - 1$ over $\mathbb{Z}/(\mathcal{A}_{m,n})$. The strategy is to square recursively the point $(\frac{3}{5}, \frac{4}{5}) \in \mathfrak{C}(\mathbb{Z}/(\mathcal{A}_{m,n}))$ (which is not a square in the multiplicative group $\mathfrak{C}(\mathbb{Z}/(\mathcal{A}_{m,n}))$). We obtain the point $(0, \pm 1) \in \mathfrak{C}(\mathbb{Z}/(\mathcal{A}_{m,n}))$ of order 4 at the $m - 2$ iteration if and only if $\mathcal{A}_{m,n}$ is prime.

After the examples with conics, we continue with a primality test using the elliptic curve $E_t : y^2 = x^3 - (t^2 + 1)x$ where $t \in \mathbb{Z}$. We show that if $p \equiv 3 \bmod 4$ is prime then E_t defines a supersingular elliptic curve over $\mathbb{F}_p$, and the point $(-1, t)$ is not divisible by 2 in $E_t(\mathbb{F}_p)$. Moreover, if $t^2 + 1$ is not a square in $\mathbb{F}_p$ then $E_t(\mathbb{F}_p)$ is cyclic and we obtain a primality test for integers of the form $m2^n - 1$ where $4m < 2^n$. The primality test is done using a reasoning analogous to the one given by Gross, that is, multiplying by two the point $m(-1, t)$ recursively in E_t.

So far, we have described primality tests using group varieties as $\mathbb{Z}$-modules.

As shown in [Bos85], the $\mathrm{End}(E)$-module structure of an elliptic curve E can be used to design a primality test algorithm. Denomme and Savin in [DS08] use elliptic curves with j-invariants 0 and 1728 as cyclic $\mathbb{Z}[\zeta_3]$-modules and $\mathbb{Z}[i]$-modules respectively to obtain primality tests for certain integer sequences. In particular, using a specific elliptic curve E with j-invariant 1728, they develop a primality test for Fermat numbers $\mathcal{F}_n$. Their test consists of the recursive multiplication by $[1+i] \in \mathrm{End}(E) \cong \mathbb{Z}[i]$ of certain point $Q \in E$ modulo $\mathcal{F}_n$, expecting some point of order 2 at a specific step of the iteration. We make variations on their arguments and in this way obtain primality tests for integers of the form $\mathcal{S}_{p,n} := p^2 16^n + 1$ where $p \equiv \pm 1 \bmod 10$ is prime and $p < 2^n$. A key ingredient to extend their setting is the observation that if $\mathcal{S}_{p,n}$ is prime, $pE(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong \mathbb{Z}[i]/(1+i)^{4n}$ as $\mathbb{Z}[i]$-modules. We show that when $\mathcal{S}_{p,n}$ is prime, a certain point $Q \in E(\mathbb{F}_{\mathcal{S}_{p,n}})$ that was also used by Denomme and Savin in their setting, has the property $pQ \notin [1+i]E(\mathbb{F}_{\mathcal{S}_{p,n}})$. Therefore, iterating the point pQ by recursive *multiplication by* $[1+i]$, leads to a primality test for $\mathcal{S}_{p,n}$, similar to the test for the integers $\mathcal{F}_n$ described by Denomme and Savin. Note that whereas heuristic arguments predict that only finitely many Fermat numbers are prime, the same kind of heuristics applied to, e.g., $\mathcal{S}_{11,n} = 121 \cdot 16^n + 1$ suggests that there may be infinitely many primes of this form.

Finally we focus on an open question stated in [ASSW16, Remark 4.13] related to designing a deterministic primality test using genus 2 curves. We partially answer this question using the Jacobian variety $\mathcal{J}$ of the genus 2 curve $\mathcal{H} : y^2 = x^5 + h$ as a $\mathbb{Z}[\sqrt{5}]$-module (where $h \in \mathbb{Z}$). Note that the curve $\mathcal{H}$ has the automorphism given by $(x, y) \mapsto (\zeta_5 x, y)$ where ζ_5 is a complex primitive fifth root of unity. This automorphism of $\mathcal{H}$ extends to an automorphism of $\mathcal{J}$, which we use to obtain the endomorphism $[\sqrt{5}] \in \mathrm{End}(\mathcal{J}) \cong \mathbb{Z}[\zeta_5]$ observing that $1 + 2\zeta_5 + 2\zeta_5^4 = \sqrt{5}$.
Our method is able to find primes of the form $\lambda_n := 4 \cdot 5^n - 1$ using the curve $\mathcal{H}$ when $\gcd(\lambda_n, h) = 1$. We use the recursive *multiplication by* $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$ of a divisor in $\mathcal{J}$ modulo λ_n similarly as in the previous tests.
We first show that when λ_n is prime, $4\mathcal{J}(\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}[\sqrt{5}]/(\sqrt{5}^{2n})$ as $\mathbb{Z}[\sqrt{5}]$-modules. Further, we construct recursively a sequence of divisors in $\mathcal{J}$ modulo λ_n, similarly to the previous elliptic tests using $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$. This sequence must be of certain form at each step and finish with a specific divisor of $\mathcal{J}$ to infer that λ_n is prime.

An explicit example of this method is implemented using MAGMA. The curve

$\mathcal{H} : y^2 = x^5 + 10$ is used with the initial divisor $4[(-1, 3) - \infty] \in \mathcal{J}$, to which repeatedly the map $[\sqrt{5}]$ is applied. In this example we detected the primes of the form λ_n where $1 < n < 5000$. To be specific, we obtained primes λ_n for all $n \in \{3, 9, 13, 15, 25, 39, 69, 165, 171, 209, 339, 2033\}$.

As we mentioned, we only *partially* solved the open question in [ASSW16] since we did not prove that if λ_n is prime, the divisor $[(-1, 3) - \infty] \in \mathcal{J}(\mathbb{F}_{\lambda_n})$ is not in $[\sqrt{5}]\mathcal{J}(\mathbb{F}_{\lambda_n})$.

Note that faster tests can be developed to check the primality of λ_n, but here we focus on the use of an Abelian surface for primality testing purposes for the first time [ASSW16].

As we will see in Chapter 4, the proofs and correctness of the elliptic and hyperelliptic methods exposed here for primality testing, depend deeply on the Hasse-Weil inequality which is the subject of the earlier chapters.

Chapter 1

Hasse inequality *à la* Manin revisited

In this chapter we recall the Hasse inequality for elliptic curves as in [Man56] (for the english translation we refer to [Man60]). This proof is elementary and it was revisited for example in [GL66, Chapter 10], [Kna92, Section X.3], [Cha95], and [CST14]. These revisions include:

- a missing argument in the original proof pointed out by Cassels (see [Cas56]);
- a modern treatment of the original argument;
- the generalization of Manin's reasoning to any finite field of any characteristic.

We present here more simplifications to the existing proofs of the result by Manin. The chapter is meant to be a preamble to Chapter 3, where we provide a similar proof inspired by Manin's ideas for the new case of hyperelliptic curves of genus 2.

Before starting the elementary proof of the Hasse inequality, the first section is a non-elementary one in order to appreciate Manin's argument. The non-elementary proof intends to lead us to the same fundamental idea exploited by Manin in his proof of the Hasse inequality. This fundamental idea is that if $E/\mathbb{F}_q$ is an elliptic curve and $\phi, [n] \in \mathrm{End}(E)$ are the q-th Frobenius and the multiplication by $n \in \mathbb{Z}$ maps respectively, then $\deg(\phi + [n]) =$

$n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q \geq 0$ for all $n \in \mathbb{Z}$. We fix by convention that $\deg([0]) = 0$ for the special situation $\phi = -[n]$.

Both proofs rely on the quadratic polynomial in n describing $\deg(\phi + [n])$. With a small extra argument, the non-negativity of this quadratic polynomial at any real number can be showed, implying the Hasse inequality. The non-elementary proof is short and explicit, using some modern theory of algebraic curves. Standard references for the necessary background may be found in mainly [Sil86] and sometimes [Har77]. The elementary proof in the subsequent section is more accessible for students since it does not need any of these references.

1.1 A non-elementary proof of the Hasse inequality

In this section we construct a quadratic polynomial in n representing the degree of the sum of the Frobenius endomorphism and the multiplication by n map on an elliptic curve: $\deg(\phi + [n])$. This is what Manin did in [Man56]. But here we will use some algebraic geometry.
The purpose of this first part is to appreciate the elementariness of Manin's proof which is discussed in Section 1.2. All results of the present section are standard and well known; references are, e.g., [Sil86] and [Was08].

1.1.1 First ideas

Formally, an elliptic curve E/k is a non-singular, projective, algebraic curve of genus one with a distinguished k-rational point that we denote by ∞. These curves are Abelian varieties of dimension one and their locus $E \setminus \{\infty\}$ can be given by the affine equation $y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6$ (see [Sti09, Proposition 6.1.2]). If $\mathrm{char}(k) \notin \{2, 3\}$, there is a *simpler* equation called the *short Weierstrass model* of E, namely $y^2 = x^3 + \alpha x + \beta$ where $\alpha, \beta \in k$. This model is obtained by a projective linear change of coordinates that preserves ∞. Similarly if $\mathrm{char}(k) = 3$, a projective linear change of coordinates leads to the equation $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$.
The specific model of E presented here for odd and even characteristic will be used in the following section.
As discussed in the introduction, Hasse's result is the following theorem.

Theorem 1.1.1. *Let $E/\mathbb{F}_q$ be an elliptic curve, then*

$$\left|\#E(\mathbb{F}_q) - (q+1)\right| \leq 2\sqrt{q}. \tag{1.1}$$

This is equivalent to the statement that $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$.

Definition 1.1.2. *An isogeny $\gamma : E_1 \to E_2$ of elliptic curves over k is a non-constant morphism that induces a homomorphism of groups $E_1(\overline{k}) \to E_2(\overline{k})$. We define* $\deg \gamma = [k(E_1) : \gamma^* k(E_2)]$ *where $\gamma^* : k(E_2) \to k(E_1)$ is the map given by $F \mapsto F \circ \gamma$.*

The fact that $k(E_1)/\gamma^* k(E_2)$ is a finite extension can be seen in [Har77, II,6.8]. We say that an isogeny γ is separable if the field extension $k(E_1)/\gamma^* k(E_2)$ is separable (otherwise inseparable).
The importance of separability is illustrated in the next definition and the subsequent lemma and proposition.

Definition 1.1.3. *Let $\gamma : E_1 \to E_2$ be a non-zero isogeny of elliptic curves and take $P \in E_1$. Let $t_{\gamma(P)} \in k(E_2)$ be a uniformizer at $\gamma(P) \in E_2$. We define the ramification index of γ at P by $e_\gamma(P) := ord_P(\gamma^* t_{\gamma(P)})$.*

Lemma 1.1.4. *Let $\gamma : E_1 \to E_2$ be a non-zero isogeny of elliptic curves and $Q \in E_2$, then* $\deg \gamma = \sum_{P \in \gamma^{-1}(Q)} e_\gamma(P)$.

Proof. [Sil86, Chapter II,§2, Proposition 2.6]. □

Proposition 1.1.5. *Let $\gamma : E_1 \to E_2$ be a separable isogeny, then*

$$\deg \gamma = \#Ker(\gamma).$$

Proof. Since the E_j have genus 1 and since the map γ is separable, this follows from [Sil86, II, 5.9]) and [Sil86, II, 2.6] and [Sil86, III, 4.10(a)]. □

Denote by $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ the endomorphism ring of E. So the elements of $\mathrm{End}(E)$ are the zero map, and all isogenies of E to itself. $\mathrm{End}(E)$ is a ring with ring operations given by $\circ$ and $+$.

From the previous proposition we can say something interesting about the number of points of $E/\mathbb{F}_q$.
Let $E/\mathbb{F}_q$ be an elliptic curve and let $[n], \phi \in \mathrm{End}(E)$ denote the multiplication by n map and the q-Frobenius map $(x, y) \mapsto (x^q, y^q)$. The map ϕ induces a purely inseparable extension of fields $\mathbb{F}_q(E)/\phi^* \mathbb{F}_q(E)$ of degree q (see [Sil86,

II, Proposition 2.11]). However, the map $\phi - [1]$ is separable (see [Sil86, III, Corollary 5.5]). Therefore, since $\phi(P) = P$ if and only if $P \in E(\mathbb{F}_q)$ we have that $\operatorname{Ker}(\phi - [1]) = E(\mathbb{F}_q)$, hence, by Proposition 1.1.5:

$$\deg(\phi - [1]) = \#E(\mathbb{F}_q). \tag{1.2}$$

Our goal is to calculate $\deg(\phi + [n])$ for all n.

1.1.2 Dual isogeny

For this non-elementary proof we will use the *dual isogeny* of an isogeny $\gamma : E_1 \to E_2$, which is an isogeny $\hat{\gamma} : E_2 \to E_1$.
The existence and construction of the dual isogeny uses machinery from algebraic geometry. We only state and cite the theorem that guarantees the existence and construction of $\hat{\gamma}$. Before the theorem, we define the pullback of γ in order to understand how the theorem exhibits the construction of $\hat{\gamma}$.

Recall that $\mathrm{Div}^0(E)$ is the free group consisting of finite $\mathbb{Z}$-linear formal sums of points of E of the form $n_1P_1 + n_2P_2 + \cdots + n_mP_m$ such that $\sum_{1 \le i \le m} n_i = 0$.

Let $\gamma : E_1 \to E_2$ be a non-constant isogeny, then the pullback of γ is defined as:

$$\gamma^* : \mathrm{Div}^0(E_2) \to \mathrm{Div}^0(E_1)$$
$$\sum n_i P_i \mapsto \sum n_i \Big(\sum_{Q \in \gamma^{-1}(P_i)} e_\gamma(Q) Q \Big).$$

Theorem 1.1.6. *Let $\gamma : E_1 \to E_2$ be a non-constant isogeny. Then there exists a unique isogeny $\hat{\gamma} : E_2 \to E_1$ such that $\gamma \circ \hat{\gamma} = [\deg \gamma]$.*
Further, consider the maps $\rho_i : E_i \to \mathrm{Div}^0(E_i)$ given by $P \mapsto P - \infty$ and the "sum maps" $\sigma_i : \mathrm{Div}^0(E_i) \to E_i$ given by $\sum n_i P_i \mapsto \sum [n_i] P_i$. We have that $\hat{\gamma} := \sigma_1 \circ \gamma^* \circ \rho_2$, that is, $\hat{\gamma}$ is the composition of:

$$E_2 \xrightarrow{\rho_2} \mathrm{Div}^0(E_2) \xrightarrow{\gamma^*} \mathrm{Div}^0(E_1) \xrightarrow{\sigma_1} E_1. \tag{1.3}$$

Proof. See [Sil86, Chapter III, Theorem 6.1]. □

Useful properties of the dual isogeny are:

- $\gamma \circ \hat{\gamma}$ equals multiplication by $\deg \gamma$ on E_2 and $\hat{\gamma} \circ \gamma$ equals multiplication by $\deg \gamma$ on E_1,

- $\hat{\hat{\gamma}} = \gamma$,
- $\widehat{\gamma \circ \eta} = \hat{\eta} \circ \hat{\gamma}$,
- $\widehat{\gamma + \eta} = \hat{\gamma} + \hat{\delta}$.

The last property is the hardest to verify, see [Sil86, Chapter III, Theorem 6.2] for details.

In the case $E_1 = E_2 = E$, one extends the notion 'dual isogeny' to all of $\mathrm{End}(E)$ by defining $\widehat{[0]} = [0]$. Note that with this extension, the properties mentioned above hold for all $\gamma, \eta \in \mathrm{End}(E)$.

Lemma 1.1.7. *Let $\gamma \in End(E)$, then $\gamma + \hat{\gamma} = [1] + [\deg \gamma] - [\deg([1] - \gamma)]$.*

Proof. The properties of the dual isogeny imply

$$[\deg([1]-\gamma)] = ([1]-\gamma)\circ\widehat{([1]-\gamma)} = ([1]-\gamma)\circ([1]-\hat{\gamma}) = [1]-(\hat{\gamma}+\gamma)+[\deg\gamma],$$

where we used the evident equality $\widehat{[1]} = [1]$. □

Corollary 1.1.8. *Let $\phi \in \mathrm{End}(E)$ be the q-Frobenius isogeny, then $\phi + \hat{\phi} = [1 + q - \#E(\mathbb{F}_q)]$.*

Proof. Using Lemma 1.1.7, since $\deg \phi = q$ ([Sil86, II, Proposition 2.11]) we have that $\deg([1] - \phi) = \deg(\phi - [1]) = \#E(\mathbb{F}_q)$ as we saw in (1.2) above. Therefore $\phi + \hat{\phi} = [1 + q - \#E(\mathbb{F}_q)]$. □

Theorem 1.1.9. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then, $d(n) := \deg(\phi + [n]) = n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q \geq 0$ for all $n \in \mathbb{Z}$.*

Proof. Using Lemma 1.1.7 and Corollary 1.1.8 and the properties of the dual isogeny, and the fact that $\deg \phi = q$, one finds

$$\begin{aligned}
[\deg(\phi + [n])] &= (\phi + [n]) \circ \widehat{(\phi + [n])} = (\phi + [n]) \circ (\hat{\phi} + [n]) \\
&= \phi \circ \hat{\phi} + \phi \circ [n] + [n] \circ \hat{\phi} + [n] \circ [n] \\
&= [\deg \phi] + (\phi + \hat{\phi}) \circ [n] + [n^2] \\
&= [n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q].
\end{aligned}$$

Note that from row two to three, we used that $[n]$ is in the center of $\mathrm{End}(E)$ for all $n \in \mathbb{Z}$, which is obvious since γ is an homomorphism of groups.

Finally, $\deg(\phi + [n]) \geq 0$ since $\phi + [n]$ is either $[0]$ or non-constant. □

Corollary 1.1.10 (Hasse inequality)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve, then*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Proof. Consider the polynomial $d(x) := x^2 + x(q + 1 - \#E(\mathbb{F}_q)) + q$. By Theorem 1.1.9 we know that $d(n) \geq 0$ for all $n \in \mathbb{Z}$. We claim that $d(x) \geq 0$ for all $x \in \mathbb{R}$.

To prove the claim, suppose that there is $x \in \mathbb{R}$ such that $d(x) < 0$. Then, there are two real zeros $\alpha < \beta$ of $d(x)$. Since $d(n) \geq 0$ for $n \in \mathbb{Z}$, there are no integers in the open interval (α, β), hence $0 < \beta - \alpha \leq 1$. Suppose that $\beta - \alpha = 1$, then α and β are consecutive integers. So, we have that $\phi - [\alpha] = [0]$ and $\phi - [\beta] = [0]$. Then, subtracting these isogenies we obtain that $[0] = (\phi - [\alpha]) - (\phi - [\beta]) = [1]$ which is absurd. Therefore $0 < \beta - \alpha < 1$, but this is also absurd since $(\beta - \alpha)^2$ is the discriminant of $d(x)$, which is an integer.

As $d(x) \geq 0$ for all $x \in \mathbb{R}$, the discriminant Δ_d of d is non-positive. This means $(q + 1 - \#E(\mathbb{F}_q))^2 - 4q \leq 0$, and therefore $|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$. □

1.2 Elementary proof of the Hasse-inequality revisited

In this section we prove Theorem 1.1.9 essentially following Manin's argument, so, using only elementary techniques. The proof will be done for $E/\mathbb{F}_q$ with q odd. This allows us to use the model $y^2 = x^3 + a_2x^2 + a_4x + a_6$ introduced in the previous section. We do not include the elementary proof for even characteristic (which is included in Soomro's PhD thesis and also in [CST14]). However, we simplified some arguments presented in [Soo13]. Recall that Hasse's theorem is the following.

Theorem 1.2.1. *Let $\mathbb{F}_q$ be a finite field of cardinality q, and let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$\left|\#E(\mathbb{F}_q) - (q + 1)\right| \leq 2\sqrt{q}$$

This is equivalent to the assertion that $\#E(\mathbb{F}_q) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$.

Recall that an elliptic curve E is a projective non-singular algebraic curve of genus 1 equipped with a distinguished rational point that we denote as $\infty \in E$. Any elliptic curve E is an Abelian variety with the distinguished point as the identity element of E.

1.2.1 Degree of endomorphisms of elliptic curves

The definition of *isogeny* given in 1.1.2 in the previous section needed to be very general for the proof to work. In the present proof, a much more down to earth definition suffices, which we motivate using the following observations. We know that a morphism between elliptic curves sending the identity element to the identity element is an homomorphism of groups (see [Sil86, III, Proposition 4.8]). Further, a non-constant morphism of curves is surjective; this is since a projective variety is complete and therefore, its image under a morphism is also complete. Furthermore, since E is smooth, any rational map of the form $\gamma : E \to C$ where C is a complete variety, is a morphism. Said this, we have a new definition of isogeny which will be enough for this section (compare [Was08, Section 12.2] for a similar approach):

Definition 1.2.2. *An isogeny of elliptic curves E_1, E_2 over k is a non-constant rational map $\gamma : E_1 \to E_2$ sending ∞ to ∞.*

This definition of isogeny will let us find explicitly the shape of the rational functions expressing $\gamma : E_1 \to E_2$. This will be done using the geometry and group structure of E_1 and E_2 assuming that both are given by Weierstrass equations. The following proof can be found in [Was08, Chapter 2, §2.9].

Lemma 1.2.3. *Let E_1/k and E_2/k be elliptic curves given by $y^2 = f_j(x)$ for $j \in \{1, 2\}$ respectively, so the f_j are cubic polynomials. Let $\gamma : E_1 \to E_2$ be an isogeny, then the affine form of γ is given explicitly as:*

$$\gamma(x, y) = \left(\frac{u_1(x)}{u_2(x)}, y\frac{v_1(x)}{v_2(x)}\right). \tag{1.4}$$

Here $u_i, v_i \in k[x]$ and $\gcd(u_1, u_2) = 1 = \gcd(v_1, v_2)$.

Proof. Using affine coordinates we have that $\gamma(x, y) = (r(x, y), s(x, y))$ for certain r, s in the function field $k(E_1) = k(x, y) = k(x) + k(x)y$, a quadratic extension of the rational function field $k(x)$. Therefore $r(x, y) = \rho_1(x) + \rho_2(x)y$ and $s(x, y) = \sigma_1(x) + \sigma_2(x)y$ for certain rational functions ρ_j, σ_j. Moreover since γ is a homomorphism one has in particular $\gamma \circ [-1] = [-1] \circ \gamma$. Written in coordinates this means $\rho_1(x) + \rho_2(x)y = \rho_1(x) - \rho_2(x)y$ and $\sigma_1(x) + \sigma_2(x)y = -\sigma_1(x) + \sigma_2(x)y$. As a consequence $\rho_2 = 0 = \sigma_1$. The lemma follows immediately from this. □

Now, to calculate the degree of γ, we state an elementary observation concerning the rational function field which will be useful for the subsequent propositions. The same observation is also stated and proven in [Soe13, Lemma 6.2].

Lemma 1.2.4. *Consider the rational function field $k(x)$ and let $\alpha, \beta \in k[x]$ be relatively prime and not both constant. Then*

$$[k(x) : k\big(\tfrac{\alpha(x)}{\beta(x)}\big)] = \max\{\deg \alpha(x), \deg \beta(x)\}.$$

Proof. We know that $[k(x) : k\big(\frac{\alpha(x)}{\beta(x)}\big)] = \deg(m(T))$ where $m(T) \in k\big(\frac{\alpha(x)}{\beta(x)}\big)[T]$ is the minimal polynomial of x over $k(\frac{\alpha(x)}{\beta(x)})$. We claim that this minimal polynomial (up to a multiplicative constant in $k(\frac{\alpha}{\beta})$) equals $\mu(T) := \beta(T)\frac{\alpha(x)}{\beta(x)} - \alpha(T)$. Clearly $\mu(x) = 0$ so we need to check that $\mu(T)$ is irreducible in $k(\frac{\alpha}{\beta})[T]$. Put $\gamma := \frac{\alpha(x)}{\beta(x)}$.

We have that $\mu(T) \in k[T][\gamma] \cong k[\gamma][T]$, therefore μ is linear as a polynomial in γ. As by assumption $\gcd(\alpha(x), \beta(x)) = 1$ in $k[x]$, it follows that μ is irreducible in $k[T][\gamma] = k[\frac{\alpha(x)}{\beta(x)}][T] \cong k[\frac{\alpha(x)}{\beta(x)}, T]$. Moreover, this implies that $\mu(T) \in k(\frac{\alpha(x)}{\beta(x)})[T]$ is also irreducible as a polynomial in T (Gauß' lemma). With this we conclude $m(T) = \mu(T)$ (up to a multiplicative constant), hence

$$\deg m(T) = \deg \mu(T) = \max\{\deg \alpha(x), \deg \beta(x)\}.$$

□

See [Sti09, Theorem 1.4.11] for a more general result of the previous lemma.

Now, we combine the previous two lemmas with $E := E_1 = E_2$ to calculate for $\gamma \in \operatorname{End}(E)$ the value $\deg \gamma$ explicitly.

Proposition 1.2.5. *Let E/k be an elliptic curve given by the equation $y^2 = f(x)$ for some cubic polynomial f. Take a non-constant $\gamma \in \operatorname{End}(E)$. Then $\gamma(x, y) = (\frac{\alpha(x)}{\beta(x)}, y\rho(x))$ where $\rho(x) \in k(x)$ and $\alpha, \beta \in k[x]$ satisfy $\gcd(\alpha, \beta) = 1$. Moreover $\deg \gamma = \max\{\deg \alpha(x), \deg \beta(x)\}$.*

Proof. The formula for γ follows from Lemma 1.2.3. Using Definition 1.1.2 one has

$$\deg \gamma = [k(x, y) : \gamma^* k(x, y)] = [k(x, y) : k(\tfrac{\alpha(x)}{\beta(x)}, y\rho(x))].$$

Consider the tower of field extensions:

$$\begin{tikzcd}
k(\frac{\alpha(x)}{\beta(x)}, y\rho(x)) \arrow[r, hook] & k(x, y) \\
k(\frac{\alpha(x)}{\beta(x)}) \arrow[u, hook, "2"'] \arrow[r, hook] & k(x) \arrow[u, hook, "2"']
\end{tikzcd}$$

To see that the vertical arrows indeed define quadratic extensions, first observe that the $[-1]$ map on E induces an automorphism of $k(x, y)$ with $x \mapsto x$ and $y \mapsto -y$. Hence this automorphism is the identity when restricted to the fields $k(\frac{\alpha}{\beta}) \subset k(x)$. Moreover it sends y to $-y$ and $y\rho$ to $-y\rho$. So the vertical arrows define extensions of degree at least 2.
Since $y^2 = f(x)$ and $y^2\rho(x)^2 = f\big(\frac{\alpha(x)}{\beta(x)}\big)$ due to the equation defining E, we conclude that indeed $y\rho$ resp. y define quadratic extensions.
As a consequence

$$2[k(x) : k(\tfrac{\alpha(x)}{\beta(x)})] = [k(x, y) : k(\tfrac{\alpha(x)}{\beta(x)})] = 2[k(x, y) : k(\tfrac{\alpha(x)}{\beta(x)}, y\rho(x))] = 2\deg\gamma.$$

Hence Lemma 1.2.4 implies $\deg\gamma = \max\{\deg\alpha(x), \deg\beta(x)\}$. □

Note that in [Was08, Section 12.2] the formula for $\deg\gamma$ proven above is in fact used as the definition of the degree of a (non-constant) isogeny.
The next proposition is the most important result of this section. It is motivated by a comment by Cassels (see [Cas56]) on Manin's proof. Other proofs of the same proposition can be found, e.g., in [GL66, Chapter 10, Lemma 3] and [Cha88, Lemma 8.6]; a different proof extending the result to finite fields of arbitrary characteristic is given in [Soo13, Lemmas 5.3.1, 5.4.2, 5.4.6]. We remark here that the proof presented below also extends without any difficulty to characteristic 2.

Proposition 1.2.6. *Let E/k be an elliptic curve in Weierstrass form. Consider $\gamma \in \mathrm{End}(E)$ given by $(x, y) \mapsto (\frac{\alpha(x)}{\beta(x)}, y\rho(x))$ with $\gcd(\alpha, \beta) = 1$ and $\rho(x) \in k(x)$ and γ non-constant. Then $\deg\gamma = \deg\alpha(x)$.*

Proof. We need to prove that $\max\{\deg\alpha(x), \deg\beta(x)\} = \deg\alpha(x)$. In fact we show that $\deg\alpha(x) > \deg\beta(x)$ which is equivalent to $\frac{\alpha(x)}{\beta(x)} \notin \mathcal{O}_\infty \subset k(x, y) \cong k(E)$.
Let $\pi \in k(E)$ be a uniformizer at ∞, so $\pi\mathcal{O}_\infty = \mathfrak{m}_\infty$ (the unique maximal ideal of $\mathcal{O}_\infty$). Then $x = u\pi^{-2}$ for some $u \in k[E]^*$ and:

$$v_\infty(\tfrac{\alpha(x)}{\beta(x)}) = \deg\alpha(x)v_\infty(x) - \deg\beta(x)v_\infty(x) = -2\deg\alpha(x) + 2\deg\beta(x).$$

Since $\gamma(\infty) = \infty$ we have that $v_\infty(\frac{\alpha(x)}{\beta(x)}) < 0$. This shows $\deg\beta(x) < \deg\alpha(x)$. Hence, by Lemma 1.2.5 indeed $\deg\gamma = \deg\alpha(x)$. □

1.2.2 Proof of the Hasse inequality

Let $E/\mathbb{F}_q$ be an elliptic curve given by the equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Let $\phi, [n] \in \mathrm{End}(E)$ be the q-Frobenius map and the multiplication by n endomorphisms. In this section we derive, using only elementary means as in the original result by Manin, a polynomial expression in n for $\deg(\phi + n)$.

Let $\mathbb{F}_q(E) \cong \mathbb{F}_q(x, y)$ be the function field of E and consider the map:

$$\begin{aligned} \Upsilon : \mathrm{Mor}_{\mathbb{F}_q}(E, E) &\to E(\mathbb{F}_q(E)) \\ \psi &\mapsto \big(\rho_1(x) + \rho_2(x)y, \sigma_1(x) + \sigma_2(x)y\big) \end{aligned} \tag{1.5}$$

where $\psi \in \mathrm{Mor}_{\mathbb{F}_q}(E, E)$ is given by $\psi(x, y) = \big(\rho_1(x)+\rho_2(x)y, \sigma_1(x)+\sigma_2(x)y\big)$ (compare the proof of Lemma 1.2.3) for certain $\rho_j, \sigma_j \in \mathbb{F}_q(x)$. It is evident that Υ is an isomorphism of groups (see e.g. [Soo13, Chapter 5, Section 5.2]). This Υ allows us to work with $\mathrm{Mor}_{\mathbb{F}_q}(E, E)$ instead of with $E(\mathbb{F}_q(E))$; this is illustrated in the proposition below. As a remark, the next proposition was stated and proved originally by Manin completely elementary in terms of a point in $E^{\text{TW}}(\mathbb{F}_q(t))$ where E^{TW} denotes the quadratic twist of E defined using the extension $\mathbb{F}_q(E) \supset \mathbb{F}_q(t)$. The elementary argument given below directly uses (1.5).

Proposition 1.2.7. *Let $E/\mathbb{F}_q$ be an elliptic curve given in Weierstrass form $y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x)$ with q odd. Then* $\deg(\phi - [1]) = \#E(\mathbb{F}_q)$.

Proof. First, by the Lemma 1.2.3 we know that $\phi - [1] : E \to E$ is of the form $(x, y) \mapsto (\frac{\alpha(x)}{\beta(x)}, y\rho(x))$ in which $\alpha, \beta \in \mathbb{F}_q[x]$ are coprime (note $\phi - 1$ is non-constant since $\deg([1]) = 1 \neq q = \deg(\phi)$. Further by Lemma 1.2.6 it suffices to show $\deg \alpha(x) = \#E(\mathbb{F}_q)$.

Consider $\Upsilon(\phi) = (x^q, yf(x)^{(q-1)/2}) \in E(\mathbb{F}_q(E))$ and $\Upsilon([1]) = (x, y) \in E(\mathbb{F}_q(E))$. Using the addition $\oplus$ on $E(\mathbb{F}_q(E))$ we have that:

$$(x^q, yf(x)^{\frac{q-1}{2}}) \oplus (x, -y) = (\tfrac{\alpha(x)}{\beta(x)}, y\rho(x)) \in E(\mathbb{F}_q(E)).$$

Hence before cancellations, $\frac{\alpha(x)}{\beta(x)}$ is given by:

$$\begin{aligned} \tfrac{\alpha(x)}{\beta(x)} &:= \big(\tfrac{y^q+y}{x^q-x}\big)^2 - (x^q + x) - a_2 = \tfrac{f(x)^q+f(x)(2f(x)^{(q-1)/2}+1)}{(x^q-x)^2} - (x^q + x) - a_2 \\ &= \tfrac{f(x)^q+f(x)(2f(x)^{(q-1)/2}+1)-(x^q+x)(x^q-x)^2-a_2(x^q-x)^2}{(x^q-x)^2}. \end{aligned}$$

The numerator in the last given expression has degree $2q + 1$.
To simplify notation let $\mu(x) := f(x)^q + f(x)(2f(x)^{\frac{q-1}{2}} + 1)$, so that

$$\tfrac{\alpha(x)}{\beta(x)} = \tfrac{\mu(x)-(x^q+x-a_2)\prod_{\xi\in\mathbb{F}_q}(x-\xi)^2}{\prod_{\xi\in\mathbb{F}_q}(x-\xi)^2}. \tag{1.6}$$

We proceed to count the common factors of the numerator and denominator of the right hand side of (1.6), and thereby find the degree of α.
To do this counting, we evaluate $\mu(x) = f(x)^q + f(x)(2f(x)^{(q-1)/2} + 1)$ at $x = a \in \mathbb{F}_q$. Take $b \in \mathbb{F}_{q^2}$ such that $b^2 = f(a)$, so that $(a, b) \in E$. We will distinguish three possibilities.
Case $b \notin \mathbb{F}_q$: In this case, $f(a)^{(q-1)/2} = -1$ and $a^q = a$. Hence $\mu(a) = f(a)^q - f(a) = 0$. Further, $\frac{\partial\mu}{\partial x} = (f(x)^{(q-1)/2} + 1)f'(x)$ which is also zero at $x = a$, hence a is a double zero of μ and $(x-a)^2$ divides both the numerator and the denominator of the right hand side of (1.6). An easy counting argument tells us that the number of cancellations of this type is exactly $2q + 2 - (\#E(\mathbb{F}_q) + \#E[2](\mathbb{F}_q))$.
Case $b \in \mathbb{F}_q^*$: In this case, $f(a)^{(q-1)/2} = 1$ and $a^q = a$. Hence $\mu(a) = 4f(a) \neq 0$, and no cancellation occurs in this case.

Case $b = 0$: In this case, $f(a)^{(q-1)/2} = 0$ and $a^q = a$. Hence, $\mu(a) = f(a) = 0$ is a single zero of $\mu(x)$ since $f(x)$ is separable. The total number of cancellations or this type is $\#E[2](\mathbb{F}_q) - 1$ (the -1 because of the point $\infty \in E$).

Combining these cases one finds

$$\deg\alpha(x) = 2q+1-\big(2q + 2 - (\#E(\mathbb{F}_q) + \#E[2](\mathbb{F}_q)) - \#E[2](\mathbb{F}_q)\big)+1 = \#E(\mathbb{F}_q).$$

□

Denote $d_n := \deg(\phi + [n])$, where we write $\deg([0]) = 0$ by convention.
We give details about the curve E^{TW} used by Manin in his original elementary proof.

As before, let $E/\mathbb{F}_q$ be an elliptic curve given by $y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x)$. Consider the curve $E^{\text{TW}}/\mathbb{F}_q(t)$ given by $f(t)y^2 = x^3 + a_2x^2 + a_4x + a_6$. The curve E^{TW} is the quadratic twist of $E/\mathbb{F}_q(t)$ corresponding to the extension $\mathbb{F}_q(t,s) \supset \mathbb{F}_q(t)$, where $s^2 = f(t)$ (see [Soo13, Section 2.6]). In particular $E^{\text{TW}} \cong E$ over $\mathbb{F}_q(t,s) \cong \mathbb{F}_q(E)$. An explicit isomorphism is given by:

$$\begin{aligned} \varsigma : E &\xrightarrow{\sim} E^{\text{TW}} \\ (u, v) &\longmapsto (u, \tfrac{v}{s}). \end{aligned}$$

Observe that if $\gamma \in \operatorname{End}(E) \subset \operatorname{Mor}_{\mathbb{F}_q}(E, E)$ corresponds via the isomorphism Υ to the point $\left(\frac{\alpha(t)}{\beta(t)}, s\rho(t)\right) \in E(\mathbb{F}_q(t,s)) \cong E(\mathbb{F}_q(E))$, then its corresponding point in E^{TW} is given by $\varsigma\left(\frac{\alpha(t)}{\beta(t)}, s\rho(t)\right) = \left(\frac{\alpha(t)}{\beta(t)}, \rho(t)\right) \in E^{\text{TW}}(\mathbb{F}_q(t))$. Hence we can also calculate $\deg \gamma = \deg \alpha(t)$ using the arithmetic of $E^{\text{TW}}(\mathbb{F}_q(t))$. This is the approach used by Manin; in particular he defined and showed properties of the numbers d_n in terms of points in $E^{\text{TW}}(\mathbb{F}_q(t))$.

Note that the q-Frobenius point $\Upsilon(\phi) = (t^q, sf(t)^{(q-1)/2}) \in E(\mathbb{F}_q(E))$ corresponds to $(t^q, f(t)^{(q-1)/2}) \in E^{\text{TW}}(\mathbb{F}_q(t))$. Moreover, the identity map $(t,s) \in E(\mathbb{F}_q(E))$ corresponds to $(t,1) \in E^{\text{TW}}(\mathbb{F}_q(t))$.
Note that E^{TW} is not in Weierstrass form, so the group law has a small variation (see [Soo13, Section 5.3]).

Lemma 1.2.8. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $d_n := \deg(\phi+[n])$ satisfies $2d_n + 2 = d_{n-1} + d_{n+1}$ for all $n \in \mathbb{Z}$.*

Proof. This can be shown quite elementary, although somewhat elaborate. It requires Proposition 1.2.6. Manin did it in odd characteristics by working explicitly with the points $\varsigma(\Upsilon(\phi + n)) \in E^{\text{TW}}(\mathbb{F}_q(t))$, manipulating the rational functions that define their coordinates. He considered all the cases where these points add up $\infty \in E^{\text{TW}}$ and showed the recursion formula with explicit calculation.
For the original proof see [Man56, Pages 675-678, "Основная Лемма"]. For a modern treatment see [Cha95, Pages 226 and 229-231, *"Basic identity"*]. Further, a small reduction in the proof and the extension of the proof to characteristic two can be found in [Soo13, Lemma 5.3.4]. □

With this lemma, we state the main theorem which is the same as Theorem 1.1.9.

Theorem 1.2.9. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $d_n = \deg(\phi + [n]) = n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q \geq 0$ for all $n \in \mathbb{Z}$.*

Proof. The proof follows by induction using the previous Lemma 1.2.8 twice (positive n and negative n).
We have that $d_{-1} = \#E(\mathbb{F}_q)$ by Proposition 1.2.7 and $d_0 = \deg \phi = \deg x^q = q$ which is the basis step. Suppose that the formula holds for two consecutive values $n-1, n$. Then, by Lemma 1.2.8:

$$\begin{aligned} d_{n+1} &= 2d_n - d_{n-1} + 2 \\ &= 2(n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q) - \\ &\quad ((n-1)^2 + (q + 1 - \#E(\mathbb{F}_q))(n-1) + q) + 2 \\ &= (n+1)^2 + (n+1)(q + 1 - \#E(\mathbb{F}_q)) + q. \end{aligned}$$

Therefore, the theorem holds for $n, n+1$. The induction is similar in the other direction. □

Now we state again the Hasse inequality.

Corollary 1.2.10 (Hasse inequality)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$|q+1-\#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Proof. Use the same proof as for Corollary 1.1.10. But here, use Theorem 1.2.9. □

As we saw, in this section we used very little algebraic geometry to prove the Hasse inequality.

Chapter 2

Jacobian and Kummer varieties function fields

In this chapter we construct and explore the function fields of the Jacobian $\mathcal{J}$ and of the Kummer surface $\mathcal{K}$ associated to a genus 2 curve $\mathcal{H}$ over a field k. This is done in terms of Mumford coordinates, which are used in many computer algebra systems such as MAGMA, sage, PARI. We define, in terms of these coordinates, some interesting symmetric functions in $k(\mathcal{J})$ used in Chapter 3 for our proof of the Hasse-Weil inequality for genus 2 *à la* Manin. Furthermore, we introduce and calculate two infinite families of symmetric functions σ_n and ρ_n in $k(\mathcal{J})$ recursively in terms of these coordinates. These families of functions facilitate the explicit computation of $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$ for the genus 2 curve $y^2 = x^5 + h$ presented in Chapter 4 for primality testing purposes.
Finally, we introduce a codimension 1 subvariety $\Theta \subset \mathcal{J}$ such that $\Theta \cong \mathcal{H}$. We construct a specific basis of the Riemann-Roch space $\mathcal{L}(2\Theta) \subset k(\mathcal{J})$. An element of this basis will be important for the proof of the Hasse-Weil inequality for genus 2.

2.1 The Jacobian $\mathcal{J}$ of a genus 2 curve and its function field

Here we construct $k(\mathcal{J})$ using Mumford coordinates which we briefly recall. Further we find equations for an affine variety $\mathcal{J}^{\mathrm{Aff}} \subset \mathbb{A}^4$ birational to $\mathcal{J}$.

Let k be a field with $\mathrm{char}(k) \neq 2$. We consider a complete, smooth curve $\mathcal{H}$ of genus 2 over k corresponding to an equation

$$y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = f(x) \tag{2.1}$$

where $f(x) \in k[x]$ is a separable polynomial. This is the canonical form of hyperelliptic curves of genus 2 in odd characteristic having a unique k-rational point at infinity $\infty \in \mathcal{H}(k)$. The point ∞ is fixed by the hyperelliptic involution $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$ given by $(x, y) \mapsto (x, -y)$. For details about this canonical form see [CF96, Chapter 1]. Denote by $\mathcal{J}$ the Jacobian variety associated to $\mathcal{H}$.

The geometry of $\mathcal{J}$ can be thought of as follows. Consider $\mathcal{H} \times \mathcal{H}$ and take $\sigma \in \mathrm{Aut}(\mathcal{H} \times \mathcal{H})$ where $\sigma(P_1, P_2) = (P_2, P_1)$ for $P_1, P_2 \in \mathcal{H}$. More precisely, let $P_i := (x_i, y_i) \in \mathcal{H}$, we have that σ permutes $x_1 \leftrightarrow x_2$ and $y_1 \leftrightarrow y_2$ with (x_1, y_1, x_2, y_2) the generic point of $\mathcal{H} \times \mathcal{H}$. Consider the quotient $\mathrm{Sym}^2(\mathcal{H}) := (\mathcal{H} \times \mathcal{H})/\sigma$, that is, the identification of the points $(P_1, P_2) \leftrightarrow (P_2, P_1)$ in $\mathcal{H} \times \mathcal{H}$. The elements of $\mathrm{Sym}^2(\mathcal{H})$ are denoted by $\{P_1, P_2\}$, that is unordered 2-tuples. The map $\mathrm{Sym}^2(\mathcal{H}) \to \mathrm{Pic}^0(\mathcal{H} \otimes \overline{k})$ given by $\{P_1, P_2\} \mapsto [P_1 + P_2 - 2\infty]$ contracts the curve $\{\{P, \mathfrak{t}(P)\}\colon P \in \mathcal{H}\}$ to one point, and is injective everywhere else. Hence, after *blowing down*) the mentioned curve in $\mathrm{Sym}^2(\mathcal{H})$ one obtains a variety birational to $\mathcal{J}$ (see also [Mil86, Proposition 3.2]). The formal procedure of *blowing down* is described, e.g., in [CF96, Chapter 2, Appendix I].

The previous construction of $\mathcal{J}$ gives us details about the geometry of $\mathcal{J}$, however, we also require an algebraic description of $\mathcal{J}(k)$ as a group. In the next chapter (Section 3.2.1), we give details of the isomorphism $\mathcal{J}(k) \cong \mathrm{Pic}^0(\mathcal{H}/k)$.

Denote $G_k := \mathrm{Gal}(\overline{k}/k)$, where $\overline{k} := k^{sep}$. Then we have

$$\mathcal{J}(k) = \mathcal{J}(\overline{k})^{G_k} \cong \mathrm{Pic}^0(\mathcal{H} \otimes_k \overline{k})^{G_k} \overset{(!)}{=} \mathrm{Pic}^0(\mathcal{H}/k) = \mathrm{Div}^0(\mathcal{H}/k)/\sim . \tag{2.2}$$

Here $\sim$ is linear equivalence of divisors defined over k, namely $D_1 \sim D_2$ if and only if $D_1 - D_2 = \mathrm{div}(f)$ for some $f \in k(\mathcal{H})$.

We also show in the next chapter that the elements of $\mathcal{J}(k)$ can be represented by divisor classes of the form $[P + Q - 2\infty]$ or $[R - \infty]$. Being defined over k means in the first case that P, Q are fixed by G_k and therefore either $P, Q \in \mathcal{H}(k)$ or $P, Q \in \mathcal{H}(\ell)$ with ℓ a quadratic extension of k, and then P, Q are conjugate over k. In the other case $R \in \mathcal{H}(k)$.

2.1.1 Mumford coordinates and $k(\mathcal{J})$

In this section, we use Mumford coordinates to describe the generic point of $\mathcal{J}$ and the function field of $\mathcal{J}$. The Mumford representation of the elements of $\mathcal{J}(k) \cong \mathrm{Pic}^0(\mathcal{H})$ is ubiquitous in the theory of hyperelliptic Jacobians, and it is very much used in applications of this theory in, e.g., cryptography.

Definition 2.1.1 (Mumford Representation)**.** *Let $\mathcal{H}/k$ be a hyperelliptic curve of genus 2 given by the equation $y^2 = x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0 = f(x)$ and let $\mathfrak{D} := [(\alpha_1, \beta_1) + (\alpha_2, \beta_2) - 2\infty] \in \mathcal{J}(k)$. We represent $\mathfrak{D}$ by the unique pair $\langle u, v\rangle$ where $u, v \in k[x]$ explicitly by the following cases:*

- *Case $\alpha_1 \neq \alpha_2$ (general case):*
  $u(x) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2$ *and* $v(x) = \frac{\beta_1-\beta_2}{\alpha_1-\alpha_2}x + \frac{\alpha_1\beta_2-\alpha_2\beta_1}{\alpha_1-\alpha_2}$
- *Case $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$ with $\beta_1 \neq 0$:*
  $u(x) = (x - \alpha_1)^2$ *and* $v(x) = \frac{f'(\alpha_1)}{2\beta_1}x - \frac{f'(\alpha_1)}{2\beta_1}\alpha_1 + \beta_1$
- *Case $\alpha_1 = \alpha_2$ and $\beta_1 = -\beta_2$:*
  $u(x) = 1$ *and* $v(x) = 0$.

If $\mathfrak{D} := [(\alpha, \beta) - \infty] \in \mathcal{J}(k)$, we represent $\mathfrak{D}$ using $u(x) = x - \alpha$ and $v(x) = \beta$.

The previous definition says that u, v have coefficients in k. This is clear from the description of k-rational divisors as given at the end of the previous section.

The following lemma yields a property of Mumford coordinates:

Lemma 2.1.2. *Let $\mathcal{H}$ be a genus 2 curve defined by $y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = f(x)$. If $\langle u, v\rangle$ are the Mumford coordinates of a point in $\mathcal{J}(k)$ then $u \mid f - v^2$.*
Moreover if $u \in \overline{k}[x]$ is monic of degree ≤ 2, $v \in \overline{k}[x]$ has $\deg(v) < \deg(u)$ and $u \mid f - v^2$, then $\langle u, v\rangle$ is the Mumford representation of a point in $\mathcal{J}(\overline{k})$.

Proof. In case of the zero point we have $u(x) = 1$ and $v(x) = 0$ and then the lemma follows trivially.
In case $\langle u, v\rangle = \langle x - \alpha, \beta\rangle$ for some point $(\alpha, \beta) \in \mathcal{H}(k)$ we have $f(\alpha) - \beta^2 = 0$ hence indeed $x - \alpha \mid f(x) - \beta^2$.
If the point corresponds to $[(\alpha_1, \beta_1) + (\alpha_2, \beta_2) - 2\infty]$ and $\alpha_1 \neq \alpha_2$ then $f - v^2$ clearly has α_1 and α_2 as zeros, settling this case.
Finally, starting from $[(\alpha_1, \beta_1) + (\alpha_1, \beta_1) - 2\infty]$ with $\beta_1 \neq 0$ then both $f - v^2$ and its derivative $f' - \frac{f'(\alpha_1)}{\beta_1}v$ have a zero at $x = \alpha_1$, which again implies $u \mid f - v^2$.

To show the last statement of the lemma, the case that $\deg(u) \leq 1$ is obvious. If $\deg(u) = 2$ and u is separable, then the two zeros $\alpha_1 \neq \alpha_2$ of u are also zeros of $f - v^2$. Hence $v(\alpha_j)^2 = f(\alpha_j)$ and $(\alpha_j, v(\alpha_j)) \in \mathcal{H}(\overline{k})$ for $j = 1, 2$. Then $\langle u, v\rangle$ represents the point $[(\alpha_1, v(\alpha_1)) + (\alpha_2, v(\alpha_2)) - 2\infty] \in \mathcal{J}(\overline{k})$.
The last case is if $\deg(u) = 2$ and u is non-separable. Here u has a double zero, say at α and $u(x) = (x - \alpha)^2 \mid f - v^2$. Hence $v(\alpha)^2 = f(\alpha)$ and $2v'(\alpha)v(\alpha) = f'(\alpha)$. We have that $v(\alpha) \neq 0$ since otherwise f would have a multiple zero at α. By assumption $\deg v < \deg u = 2$, so v equals its own first order Taylor expansion around α, i.e., $v = v(\alpha) + v'(\alpha)(x - \alpha)$. A direct verification shows that $\langle u, v\rangle$ equals the Mumford representation of $[2(\alpha, v(\alpha)) - 2\infty] \in \mathcal{J}(\overline{k})$. □

With this lemma we proceed to construct the locus $\mathcal{J}^{\text{Aff}} \subset \mathbb{A}^4$ consisting of the points in general position in $\mathcal{J}$ namely $[(x_1, y_1) + (x_2, y_2) - 2\infty] \in \mathcal{J}$ with $x_1 \neq x_2$, using the Mumford representation. The variety $\mathcal{J}^{\text{Aff}}$ will be useful to find generators of the function field of $\mathcal{J}$.
We use the Mumford coordinates to embed $\mathcal{J}^{\text{Aff}}$ in $\mathbb{A}^4$ as an intersection of two hypersurfaces . Let $\mathfrak{D} := [(x_1, y_1) + (x_2, y_2) - 2\infty] \in \mathcal{J}(k)$ be the generic point. Consider the symmetric functions $A := x_1 + x_2$, $B := x_1x_2$, $C := \frac{y_1 - y_2}{x_1 - x_2}$ and $D := \frac{x_1y_2 - x_2y_1}{x_1 - x_2}$. We have that $\mathfrak{D}$ is represented by $\langle u(x), v(x)\rangle = \langle x^2 - Ax + B, Cx + D\rangle$ and by Lemma 2.1.2:

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 - (Cx + D)^2 \equiv 0 \bmod x^2 - Ax + B.$$

Solving this congruence yields the equations of two hypersurfaces in $\mathbb{A}^4$, namely:

$$\begin{aligned} A^4 - AC^2 + B^2 - 2CD + a_4(A^3 - 2AB) + a_3(A^2 - B) + a_2A - 3A^2B + a_1 &= 0, \\ -A^3B + BC^2 - D^2 + 2AB^2 - a_4(A^2B - B^2) - a_3AB - a_2B + a_0 &= 0. \end{aligned}$$

These two equations in A, B, C, D define an embedding in $\mathbb{A}^4$ of the locus of the points of $\mathcal{J}$ in general position. Denote by $\mathcal{J}^{\text{Aff}} \subset \mathbb{A}^4$ this embedded affine variety. Then $k(\mathcal{J}^{\text{Aff}}) = k(\mathcal{J})$. We proceed to show that this function field equals $k(A, B, C, D)$ and that the relations between A, B, C, D are generated by the two given ones.

In $\mathcal{H} \times \mathcal{H}$ consider the four curves $\infty \times \mathcal{H}$ and $\mathcal{H} \times \infty$ and the two graphs of the identity map and of the hyperelliptic involution $\mathfrak{t}$. The complement of these four curves is an affine surface we denote $(\mathcal{H} \times \mathcal{H})^{\text{Aff}}$; it is birational to

$\mathcal{H} \times \mathcal{H}$ hence $k((\mathcal{H} \times \mathcal{H})^{\mathtt{Aff}}) = k(x_1, x_2, y_1, y_2)$. Here the x_i are independent variables and $y_i^2 = f(x_i)$. There is a well-defined morphism

$$(\mathcal{H} \times \mathcal{H})^{\mathtt{Aff}} \to \mathcal{J}^{\mathtt{Aff}}$$

given by $((\alpha_1, \beta_1), (\alpha_2, \beta_2)) \mapsto [(\alpha_1, \beta_1) + (\alpha_2, \beta_2) - 2\infty]$. The map σ introduced earlier restricts to $(\mathcal{H} \times \mathcal{H})^{\mathtt{Aff}}$ and it interchanges the two elements in each fiber of the given morphism. Hence $k(\mathcal{J}) = k(\mathcal{J}^{\mathtt{Aff}})$ is isomorphic to the subfield of $k(x_1, x_2, y_1, y_2)$ consisting of all elements fixed by σ^*. Clearly $k(A, B, C, D)$ is contained in this subfield and it remains to show $k(A, B, C, D) = k(x_1, x_2, y_1, y_2)^{\sigma^*}$ and to find the relations between A, B, C, D.

We have that $[k(\mathcal{H} \times \mathcal{H}) : k(x_1, x_2)] = 4$. The involution σ^* restricts to an involution (which we also denote by σ^*) on $k(x_1, x_2)$. Its fixed field is clearly $k(A, B)$, since x_1, x_2 are the zeros of $X^2 - AX + B \in k(A, B)[X]$.

Now, consider the following diagram describing inclusions of function fields.

$$\begin{tikzcd}
k(x_1, x_2, y_1, y_2)^{\sigma^*} \arrow[r, hook, "2"] & k(x_1, x_2, y_1, y_2) \\
k(A, B) \arrow[u, hook] \arrow[r, hook, "2"] & k(x_1, x_2). \arrow[u, hook, "4"']
\end{tikzcd}$$

It shows that $[k(x_1, x_2, y_1, y_2)^{\sigma^*} : k(A, B)] = 4$. The equation

$$A^4 - AC^2 + B^2 - 2CD + a_4(A^3 - 2AB) + a_3(A^2 - B) + a_2 A - 3A^2 B + a_1 = 0$$

implies $D \in k(A, B, C)$. Expressing D as a rational function in A, B, C, the remaining relation

$$-A^3 B + BC^2 - D^2 + 2AB^2 - a_4(A^2 B - B^2) - a_3 AB - a_2 B + a_0 = 0$$

shows that $[k(A, B, C, D) : k(A, B)] \leq 4$.

Consider the extension of $k(A, B, C, D)$ given by $k(A, B, C, D)(x_1 - x_2)$. We have that $x_1 - x_2$ is a zero of $X^2 - (A^2 + 4B) \in k(A, B, C, D)[X]$ and $x_1 - x_2 \in k(x_1, x_2, y_1, y_2)$ is not fixed by σ^*, therefore $x_1 - x_2 \notin k(A, B, C, D)$. This means that $[k(A, B, C, D)(x_1 - x_2) : k(A, B, C, D)] = 2$.

Moreover,

$$x_1 = \frac{A + (x_1 - x_2)}{2} \qquad x_2 = \frac{A - (x_1 - x_2)}{2}$$
$$y_1 = D + x_1 C \qquad y_2 = D + x_2 C.$$

This shows that $k(x_1, x_2, y_1, y_2) = k(A, B, C, D)(x_1 - x_2)$ and

$$k(\mathcal{J}) \cong k(x_1, x_2, y_1, y_2)^{\sigma^*} = k(A, B, C, D).$$

Moreover, the argument shows that $[k(A, B, C, D) : k(A, B)] = 4$ which means that the two relations obtained for C, D in terms of A, B generate the prime ideal defining the affine variety in $\mathbb{A}^4$ birational to $\mathcal{J}^{\text{Aff}}$.

To end this section we present an example of how to use the previous Lemma and discussion to do symbolic computations with elements of $\mathcal{J}$. The following code constructs the generic point of $\mathcal{J}/\mathbb{Q}(\zeta_5)$ in Mumford coordinates using MAGMA. We do it for the Jacobian $\mathcal{J}$ of $\mathcal{H} : y^2 = x^5 + h$, considered over the 5-th cyclotomic field. We extend the element of $\mathrm{Aut}(\mathcal{H})$ given by $(x, y) \mapsto (\zeta_5 x, y)$ to an automorphism ζ_5 of $\mathcal{J}$ and construct the *multiplication by* $\sqrt{5}$ endomorphism, that is, $[\sqrt{5}] \in \mathrm{End}(\mathcal{J}) \cong \mathbb{Z}[\zeta_5]$ (see [CF96, Chapter 5, Section 2]). We will see more details in Chapter 4. The code below obtains formulas in terms of Mumford coordinates for the action of $[\sqrt{5}]$ on the generic point of $\mathcal{J}$. This is done noting that $\zeta_5 + \zeta_5^4 = \frac{-1+\sqrt{5}}{2} \in \mathrm{End}(\mathcal{J}) \cong \mathbb{Z}[\zeta_5]$.

```
> Q<z> := CyclotomicField(5);
> K<h> := RationalFunctionField(Q);
> MumCoef<d,c,b,a> := PolynomialRing(K, 4);
> MumPol<X> := PolynomialRing(MumCoef);
> jaceqs := (X^5+h - (c*X+d)^2)   mod (X^2-a*X+b);
> FFJ<D,C,B,A> := FieldOfFractions(quo<MumCoef | Coefficients(jaceqs)>);
> H := HyperellipticCurve(Polynomial([FFJ|h,0,0,0,0,1]));
> J := Jacobian(H);
> gp   := elt<J | Polynomial([B,-A,1]), Polynomial([D,C]), 2>;
> gpz1 := elt<J | Polynomial([z^2*B,-z*A,1]), Polynomial([D,C/z]),2>;
> gpz4 := elt<J | Polynomial([z^(-2)*B,-(z^-1)*A,1]), Polynomial([D,C/(z^-1)]),2>;
> gp;
(x^2 - A*x + B, C*x + (-1/2*A^2 + 2*B)/(A^4 - 3*B*A^2 + B^2)*C^3 + (1/2*A^5 -
    7/2*B*A^3 + 9/2*B^2*A + 2*h)/(A^4 - 3*B*A^2 + B^2)*C, 2)
> gpz1;
(x^2 - z*A*x + z^2*B, (-z^3 - z^2 - z - 1)*C*x + (-1/2*A^2 + 2*B)/(A^4 - 3*B*A^2
    + B^2)*C^3 + (1/2*A^5 - 7/2*B*A^3 + 9/2*B^2*A + 2*h)/(A^4 - 3*B*A^2 +
    B^2)*C, 2)
> sq5 := 2*(gpz1+gpz4)+gp;
Time: 179.180
```

In the next section we reduce the number of Mumford coordinates defining $k(\mathcal{J})$. Further we find some interesting symmetric functions in terms of these coordinates which will be used in subsequent chapters.

2.2 $k(\mathcal{J})$ with three generators and some interesting symmetric functions

In the previous section we saw that $D = \frac{x_1y_2 - x_2y_1}{x_1 - x_2} \in k(A, B, C)$ using the equations that define $\mathcal{J}^{\mathrm{Aff}}$. We show for $\delta := x_1y_2 + x_2y_1$, that:

$$k(A, B, \delta) = k(A, B, C, D) \cong k(\mathcal{J}) \tag{2.3}$$

which is convenient in certain situations to get compact formulas for some symmetric functions in $\mathcal{J}$.

It is clear that the function δ is invariant under σ^*. Consider the following diagram where the numbers represent the degrees of the field extensions, as explained in the previous section:

$$\begin{tikzcd}
k(A,B,C,D) \arrow[r, hook, "2"] & k(x_1,y_1,x_2,y_2) \\
k(A,B,\delta) \arrow[u, hook, "1?"'] & \\
k(A,B) \arrow[u, hook, "4?"'] \arrow[uu, hook, bend left, "4"] \arrow[uur, hook, "8"] \arrow[r, hook, "2"] & k(x_1,x_2) \arrow[uu, hook, "4"']
\end{tikzcd}$$

To infer that $[k(A, B, \delta) : k(A, B)] = 4$, the following proposition suffices together with the previous diagram.

Proposition 2.2.1. *The minimal polynomial of $\delta := x_1y_2 + x_2y_1$ over $k(x_1, x_2)$ where $y_i^2 = x_i^5 + a_4x_i^4 + a_3x_i^3 + a_2x_i^2 + a_1x_i + a_0 =: f(x_i)$, has degree 4.*

Proof. Let $\mathcal{B} = \{1, y_1, y_2, y_1y_2\}$ be a basis of $k(x_1, x_2)(y_1, y_2)$ as a vector space over $k(x_1, x_2)$. Consider the matrix that represents in its columns the coefficients in $k(x_1, x_2)$ using the basis $\mathcal{B}$ to represent powers of δ, namely $\delta^0, \delta^1, \delta^2, \delta^3$.

$$M = \begin{pmatrix} 1 & 0 & x_1^2 f(x_2) + x_2^2 f(x_1) & 0 \\ 0 & x_2 & 0 & 3x_1^2x_2 f(x_2) + f(x_1)x_2^3 \\ 0 & x_1 & 0 & 3x_2^2x_1 f(x_1) + f(x_2)x_1^3 \\ 0 & 0 & 2x_1x_2 & 0 \end{pmatrix}$$

A direct calculation shows that the determinant of this matrix is nonzero i.e. this matrix has rank 4.

It is easy to see that $[k(x_1, x_2, \delta) : k(A, B, \delta)] = 2$. Hence the above diagram implies $k(\mathcal{J}) = k(A, B, \delta)$ and that $[k(A, B, \delta) : k(A, B)] = 4$, from which the result follows. □

Remark. We can go further and calculate explicitly the minimal polynomial of δ. The column vector for δ^4 in terms of the basis $\mathcal{B}$ is given by:

$$b = \begin{pmatrix} x_1^4 f(x_2)^2 + 6x_1^2x_2^2 f(x_1)f(x_2) + f(x_1)^2 x_2^4 \\ 0 \\ 0 \\ 4x_1^3x_2 f(x_2) + 4x_1x_2^3 f(x_1). \end{pmatrix}$$

By the previous proposition we can solve the system $M\alpha = b$, where $\alpha = (\alpha_0, \alpha_2, \alpha_3, \alpha_4)^T$, and $\alpha_i \in k(A,B) \subset k(x_1,x_2)$. We obtain:

$$\begin{aligned} \alpha_0 &= -(f(x_1)^2x_2^4 + x_1^4 f(x_2)^2) + 2x_1^2x_2^2 f(x_1)f(x_2) \\ \alpha_1 &= 0 \\ \alpha_2 &= 2x_2^2 f(x_1) + 2x_1^2 f(x_2) \\ \alpha_3 &= 0. \end{aligned}$$

Note that each α_i is symmetric. Writing α_0 and α_2 in terms of $A = x_1 + x_2$, $B = x_1x_2$, we obtain

$$\begin{aligned} \alpha_0 :=& -A^6B^4 - 2a_4A^5B^4 + 2a_0A^5B^2 + 6A^4B^5 + (-2a_3 - a_4^2)A^4B^4 + 2a_1A^4B^3 \\ &+ 2a_0a_4A^4B^2 - a_0^2A^4 + 10a_4A^3B^5 - 2a_3a_4A^3B^4 + (-10a_0 + 2a_1a_4)A^3B^3 \\ &+ 2a_0a_3A^3B^2 - 2a_0a_1A^3B - 9A^2B^6 + (10a_3 + 4a_4^2)A^2B^5 \\ &+ (-10a_1 - a_3^2)A^2B^4 + (-8a_0a_4 + 2a_1a_3)A^2B^3 - a_1^2A^2B^2 + 4a_0^2A^2B \\ &- 8a_4AB^6 + 8a_3a_4AB^5 + (8a_0 - 8a_1a_4)AB^4 - 8a_0a_3AB^3 + 8a_0a_1AB^2 \\ &+ 4B^7 - 8a_3B^6 + (8a_1 + 4a_3^2)B^5 - 8a_1a_3B^4 + 4a_1^2B^3 \\ \alpha_2 :=& 2A^3B^2 + 2A^2B^2a_4 - 6AB^3 + 2AB^2a_3 - 4B^3a_4 + 2A^2a_0 + 2ABa_1 \\ &+ 4B^2a_2 - 4Ba_0 \end{aligned}$$

where the $a_i \in k$ are the coefficients of the polynomial f defining the hyperelliptic curve. By Proposition 2.2.1 we know that $P(X) := X^4 - \alpha_2X^2 - \alpha_0 \in k(A,B)[X]$ is irreducible, and $P(\delta) = 0$.

2.2.1 Useful functions in $k(\mathcal{J})$

In this section, in terms of the generators A, B, C, D of the function field $k(\mathcal{J})$ we introduce some useful functions in $k(\mathcal{J})$. These will be used in the next chapters.

Let $\mathcal{H}/k$ be a hyperelliptic curve given by $y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Define the following functions in $k(\mathcal{J})$ (verifying that the different expressions indeed define the same function is just a direct computation).

$$\begin{aligned} s_1 :&= a_1 + a_2A + a_3(A^2 - B) + a_4(A^3 - 2AB) + A^4 - B(3A^2 - B) \\ &= \tfrac{f(x_1)-f(x_2)}{x_1-x_2}, \\[2ex] s_2 :&= 2a_0 + a_1A + a_2(A^2 - 2B) + a_3(A^3 - 3AB) + a_4(A^4 - 4A^2B + 2B^2) \\ &\quad + A^5 + 5AB^2 - 5A^3B \\ &= f(x_1) + f(x_2), \\[2ex] s_3 :&= \frac{s_2 - C^2(A^2 - 4B)}{2} \\ &= y_2y_1, \\[2ex] s_4 :&= a_0 + a_1A + a_2(A^2 - B) + a_3(A^3 - 2AB) + a_4(A^4 - B(3A^2 - B)) \\ &\quad + A(A^2 - 3B)(A^2 - B) \\ &= \tfrac{x_1f(x_1)-x_2f(x_2)}{x_1-x_2}, \\[2ex] \rho_0 &:= 2D + AC = y_1 + y_2, \\ \rho_1 &:= A^2C + AD - 2BC = x_1y_1 + x_2y_2, \\ \sigma_1 &:= AD + 2BC = x_1y_2 + x_2y_1 = \delta. \end{aligned} \tag{2.4}$$

In the following two lemmas we describe recursively two infinite families of symmetric functions in terms of the Mumford coordinates A, B, C, D, namely $\rho_n = x_1^ny_1 + x_2^ny_2 \in k(\mathcal{J})$ and $\sigma_n = x_1^ny_2 + x_2^ny_1 \in k(\mathcal{J})$. We are interested in $\sigma_n, \rho_n \in k(\mathcal{J})$ since they can be used in Chapter 4 to derive formulas describing certain elements of End($\mathcal{J}$). In particular this makes MAGMA implementations shorter.

Lemma 2.2.2. *Let $\rho_n := x_1^ny_1 + x_2^ny_2 \in k(\mathcal{J})$, then we have the recursion formula $\rho_n = A\rho_{n-1} - B\rho_{n-2}$. Moreover, as was noted in (2.4), $\rho_0 = 2D + AC$ and $\rho_1 = A^2C + AD - 2BC$.*

Proof. Recall $A = x_1 + x_2$ and $B = x_1x_2$. We have $Ax_1 - B = x_1^2$ and $Ax_2 - B = x_2^2$ and hence

$$\begin{aligned} A\rho_{n-1} - B\rho_{n-2} &= A(x_1^{n-1}y_1 + x_2^{n-1}y_2) - B(x_1^{n-2}y_1 + x_2^{n-2}y_2) \\ &= x_1^{n-2}(Ax_1 - B)y_1 + x_2^{n-2}(Ax_2 - B)y_2 \\ &= x_1^{n-2}x_1^2y_1 + x_2^{n-2}x_2^2y_2 = \rho_n. \end{aligned}$$

□

Lemma 2.2.3. *Let $\sigma_n := x_1^n y_2 + x_2^n y_1 \in k(\mathcal{J})$, then $\sigma_n = A\sigma_{n-1} - B\sigma_{n-2}$ and $\sigma_0 = 2D + AC$ and $\sigma_1 = AD + 2BC$.*

Proof. The proof is similar to the previous lemma. □

Note that we can express D in terms of A, B, C using the functions $s_1, s_2, s_4 \in k(A, B)$ and $s_3 \in k(A, B, C)$ defined in (2.4), namely:

$$D = \tfrac{x_1y_2 - x_2y_1}{x_1 - x_2} = \frac{C(s_2 + s_3 - s_4)}{s_1}. \tag{2.5}$$

2.3 Kummer surface and its function field

Let $\mathcal{H}/k$ be a hyperelliptic curve of genus 2 given by $y^2 = f(x)$ with f of degree 5, and let $\mathcal{J}/k$ be the associated Jacobian variety. Previously we described $k(\mathcal{J})$ as the function field of $\mathrm{Sym}^2(\mathcal{H})$. That is, as the field of invariants $k(\mathrm{Sym}^2(\mathcal{H})) = k(\mathcal{H} \times \mathcal{H})^{\sigma^*} \subset k(\mathcal{H} \times \mathcal{H})$. Moreover, we obtained $k(\mathcal{J}) \cong k(A, B, \delta)$ by Proposition 2.2.1. Further, using Equation (2.5) we have $k(A, B, \delta) = k(A, B, C)$.

We now discuss the subfield of $k(\mathcal{J})$ obtained by taking the invariants under the $[-1]$ map.

Consider the hyperelliptic involution $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$, given by $\mathfrak{t}(x_0, y_0) = (x_0, -y_0)$. This automorphism can be extended naturally to $\mathcal{J}$, namely as

$$[(x_1, y_1) + (x_2, y_2) - 2\infty] \mapsto [(x_1, -y_1) + (x_2, -y_2) - 2\infty].$$

Since $(x_1, -y_1) + (x_2, -y_2) - 2\infty \sim -(x_1, y_1) - (x_2, y_2) + 2\infty$, this is exactly the $[-1]$ map on $\mathcal{J}$.

We are interested in the field of invariants $k(\mathcal{J})^{[-1]^*} \subset k(\mathcal{J})$. This is related to the Kummer surface of $\mathcal{J}$ as we will now recall.

The Kummer surface $\mathcal{K}$ associated to $\mathcal{J}$ is obtained by the desingularization of the quotient $\mathcal{J}/[-1]$. This means that $\mathcal{K}$ is the surface resulting from the identification of *opposite points in* $\mathcal{J}$ with its $\binom{6}{2}+1=16$ singularities blown up. These singularities correspond to the elements of $\mathcal{J}[2]$ which are invariant under $[-1]$. So now, consider the induced automorphism $[-1]^* \in \mathrm{Aut}(k(\mathcal{J}))$. Since $\mathcal{K}$ is birational to $\mathcal{J}/[-1]$, the function field of $\mathcal{K}$ equals the subfield of $k(\mathcal{J})$ consisting of all invariants under $[-1]^*$, so

$$k(\mathcal{K}) = k(\mathcal{J})^{[-1]^*} = k(A,B,C)^{[-1]^*} = k(A,B,\delta)^{[-1]^*}.$$

Clearly $k(A,B) \subset k(A,B,C)^{[-1]^*}$. Recall that $[k(A,B,C) : k(A,B)] = 4$, hence as $[-1]^*$ has order 2 we have $[k(A,B,C) : k(A,B,C)^{[-1]^*}] = 2$ and $[k(A,B,C)^{[-1]^*} : k(A,B)] = 2$. To get an explicit generator for the extension $k(\mathcal{K})$ over $k(A,B)$, note that $s_3 = y_1y_2$ is invariant under $[-1]^*$ and $s_3 \notin k(A,B)$. Therefore $k(\mathcal{K}) = k(\mathcal{J})^{[-1]^*} \cong k(A,B,s_3)$. In fact we have that $k(A,B,s_3) = k(A,B,C^2)$ since $C^2 = \frac{2s_3-s_2}{4B-A^2}$ and $s_2 = f(x_1)+f(x_2) \in k(A,B)$. In the next section we describe the minimal polynomial of s_3 and of C^2 over $k(A,B)$. Moreover, we present a singular surface birational to $\mathcal{K}$ explicitly similar to what we did for $\mathcal{J}$ in Section 2.1.1.

2.3.1 A singular surface birational to $\mathcal{K}$

Here we introduce a surface $\mathcal{K}_s$ which is birational to the Kummer surface $\mathcal{K}$. Recall that $k(\mathcal{K}) \cong k(A,B,\delta)^{[-1]^*} = k(A,B,y_1y_2)$.

As before, we assume the hyperelliptic curve $\mathcal{H}$ of genus 2 over k to be given by $y^2 = x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0 = f(x)$. We have that $f(x) \in k[x]$ factors in $\bar{k}[x]$ as $f(x) = \prod_{i=1}^{5}(x-\alpha_i)$ with $\alpha_i \in \bar{k}$. Then

$$\begin{aligned}(y_1y_2)^2 = f(x_1)f(x_2) &= \prod_{i=1}^{5}(x_1-\alpha_i)(x_2-\alpha_i)\\ &= \prod_{i=1}^{5}(x_1x_2-(x_1+x_2)\alpha_i+\alpha_i^2) \qquad (2.6)\\ &= \prod_{i=1}^{5}(B-A\alpha_i+\alpha_i^2) =: \kappa(A,B)\end{aligned}$$

where $A = x_1 + x_2$ and $B = x_1 x_2$ as usual. Since $\kappa(A, B) = f(x_1)f(x_2)$, it is clear that $\kappa(A, B) \in k[A, B]$. A direct calculation shows

$$\begin{aligned}\kappa(A, B) :=& a_0A^5 + a_1A^4B + a_0a_4A^4 + a_2A^3B^2 + (-5a_0 + a_1a_4)A^3B\\ &+ a_0a_3A^3 + a_3A^2B^3 + (a_2a_4 - 4a_1)A^2B^2 + (a_1a_3 - 4a_0a_4)A^2B\\ &+ a_0a_2A^2 + a_4AB^4 + (a_3a_4 - 3a_2)AB^3 + (5a_0 - 3a_1a_4 + a_2a_3)AB^2\\ &+ (a_1a_2 - 3a_0a_3)AB + a_0a_1A + B^5 + (a_4^2 - 2a_3)B^4\\ &+ (2a_1 - 2a_2a_4 + a_3^2)B^3 + (2a_0a_4 - 2a_1a_3 + a_2^2)B^2\\ &+ (a_1^2 - 2a_0a_2)B + a_0^2.\end{aligned}$$

Formula (2.6) says

$$s_3^2 = \kappa(A, B) \tag{2.7}$$

which implies that $T^2 - \kappa(A, B) \in k(A, B)[T]$ is the minimal polynomial of s_3 over $k(A, B)$. Taking A, B, s_3 as coordinates in $\mathbb{A}^3$, we define the affine surface $\mathcal{K}_s \subset \mathbb{A}^3$ as the zeros of the equation $s_3^2 = \kappa(A, B)$. By construction $\mathcal{K}_s$ is birational to $\mathcal{K}$.

As described in detail in [vGT06, Section 4.3], we discuss some of the geometry of $\mathcal{K}_s$. From Equation (2.7) one sees that the map $(A, B, s_3) \mapsto (A, B)$ realizes $\mathcal{K}_s$ as a double cover of $\mathbb{A}^2$ branched over the lines $B - \alpha_i A + \alpha_i^2 = 0$ for $i = 1, \dots, 5$. These lines are tangent to the parabola with equation $A^2 = 4B$. The affine tangency points are $(2\alpha_i, \alpha_i^2) \in \mathbb{A}^2$.

Since $k(A, B, s_3) = k(A, B, C^2)$, we can also describe $k(\mathcal{K})$ using the minimal polynomial of C^2 over $k(A, B)$. One verifies that $C^2 = \frac{s_2 - 2s_3}{A^2 - 4B}$ is a zero of

$$T^2 - \frac{2s_2}{A^2 - 4B}T + \frac{{s_2}^2 - 4\kappa(A, B)}{(A^2 - 4B)^2} \in k(A, B)[T].$$

To end this chapter, in the next section we discuss the curve $\Theta \subset \mathcal{J}$ isomorphic to $\mathcal{H}$, given as the image of the map $\mathcal{H} \to \mathcal{J}$ defined by $P \mapsto [P - \infty]$. Since $\mathcal{J}$ has dimension 2, we have that Θ is a codimension 1 subvariety of $\mathcal{J}$ and we can regard it as a divisor on $\mathcal{J}$. Further, we will construct a function $\kappa_4 \in k(\mathcal{J})$ having $\Theta \subset \mathcal{J}$ as a pole of order 2 and no other poles. We will see that a basis of the Riemann Roch space $\mathcal{L}(2\Theta)$ realizes the Kummer Surface of $\mathcal{J}$ in $\mathbb{P}^3$. The function κ_4 in the constructed basis of $\mathcal{L}(2\Theta)$ will be important to prove the Hasse-Weil inequality for genus 2 in the next chapter.

2.4 The divisor $\Theta \in \mathrm{Div}(\mathcal{J})$ and $\mathcal{L}(2\Theta) \subset k(\mathcal{J})$

Let $\mathcal{H}/k$ be a hyperelliptic curve of genus 2 given by $y^2 = f(x)$ where f has degree 5. Let $Q \in \mathcal{H}(k)$. The image of $\mathcal{H}$ in its Jacobian $\mathcal{J}$ translated over $[\infty - Q]$ is given by the image of the injective map:

$$\begin{aligned} \iota^Q : \mathcal{H} &\to \mathcal{J} \\ P &\mapsto [P - Q]. \end{aligned}$$

This map has the following universal property:
Given an Abelian variety $\mathcal{A}/k$ and any $\mu \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{A})$ such that $\mu(Q) = 0 \in \mathcal{A}$, there exists a unique $\gamma \in \mathrm{Hom}(\mathcal{J}, \mathcal{A})$, such that the following diagram commutes (see Chapter III, Proposition 6.1 [Mil08]):

$$\begin{tikzcd} \mathcal{H} \arrow[r, "\iota^Q"] \arrow[dr, "\mu"'] & \mathcal{J} \arrow[d, "\gamma"] \\ & \mathcal{A} \end{tikzcd} \tag{2.8}$$

where γ is defined with the property $\mu = \gamma \circ \iota^Q$.
In our case we have the point $\infty \in \mathcal{H}$, so we fix the embedding $\iota := \iota^\infty \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$. The image of the curve $\mathcal{H}$ in $\mathcal{J}$ will be defined as $\Theta := \iota(\mathcal{H})$ and is called the *Theta divisor* of $\mathcal{J}$. The word *divisor* is coined since Θ has codimension 1 in $\mathcal{J}$, therefore $\Theta \in \mathrm{Div}(\mathcal{J})$.

Now we examine functions in $k(\mathcal{J})$ having Θ as a pole. Let $\mathcal{H}/k$ be a hyperelliptic curve of genus 2 given by the equation $Y^2 = f(X)$ with $\deg f = 5$. In previous sections we saw that $\mathfrak{D} := [(x_1, y_1) + (x_2, y_2) - 2\infty] \in \mathcal{J}$ is represented in Mumford coordinates by four symmetric rational functions $A, B, C, D \in k(\mathcal{J})$.
Recall that the Mumford representation of the generic point $\mathfrak{D}$ is given by two polynomials in $k(\mathcal{J})[x]$, namely $\langle x^2 - Ax + B, Cx + D\rangle$. These functions were presented in previous sections, in fact they are given by:

$$A = x_1 + x_2, B = x_1 x_2, C = \tfrac{y_1 - y_2}{x_1 - x_2} \text{ and } D = \tfrac{x_2 y_1 - x_1 y_2}{x_1 - x_2}. \tag{2.9}$$

It is easy to see that the functions $\{1, A, B\} = \{1, x_1 + x_2, x_1 x_2\} \subset \mathcal{L}(2\Theta)$ since every point of Θ is of the form $[P + \infty - 2\infty]$ and x_i has pole order 2 at ∞ in each component of $\mathcal{H} \times \mathcal{H}$. Further, these functions linearly independent but $\dim_k \mathcal{L}(2\Theta) = 2^g = 4$ as we will see in this section. Hence, for a basis of $\mathcal{L}(2\Theta)$ one more function is needed. The first candidate is C since Θ belongs to the pole divisor of C. However, $C \in \mathcal{L}(3\Theta) \setminus \mathcal{L}(2\Theta)$, as we will show below, that is, Θ is the only pole of $C \in k(\mathcal{J})$, and its order is 3. First we introduce notation below to prove this.

Notation 2.4.1. *Let V/k be a smooth and irreducible variety, P a codimension 1 subvariety of V and $F \in k(V)$ a function on V. The order of vanishing of F at P is denoted by $ord_P^V(F)$.*

Proposition 2.4.2. $C \in \mathcal{L}(3\Theta) \setminus \mathcal{L}(2\Theta)$

Proof. Let $k(\mathcal{H}) =: k(x, y)$ be the function field of the hyperelliptic curve $\mathcal{H}$, where $y^2 = f(x)$ and f of degree 5. Let $P := (x, y) \in \mathcal{H}$ be the generic point of $\mathcal{H}$ and consider C as a function in $k(\mathcal{H} \times \mathcal{H}) =: k(x_1, y_1, x_2, y_2)$ where $y_j^2 = f(x_j)$. Note that $k(\mathcal{J}) = k(\mathrm{Sym}^2(\mathcal{H})) \subset k(\mathcal{H} \times \mathcal{H})$ as we showed in previous sections.
Consider the function $C_P \in k(\mathcal{H} \times \mathcal{H}) = k(\mathcal{H})(\mathcal{H})$ as a rational map in a variable Q, fixing the generic point P, namely:

$$\begin{aligned} &C_P : \mathcal{H} \longrightarrow \mathbb{P}^1 \\ &\qquad Q \mapsto \tfrac{\rho_1(Q)}{\rho_2(Q)} := \tfrac{y_1(P)-y_2(Q)}{x_1(P)-x_2(Q)}. \end{aligned} \tag{2.10}$$

Since P is generic and $y_1(P) = y, x_1(P) = x$ are constant we have that $\rho_1, \rho_2 \in k(x, y)(\mathcal{H})$. One has $\mathrm{ord}_\infty^{\mathcal{H}}(\rho_1) = -5$ since the y-coordinate function on $\mathcal{H}$ has a pole at ∞ of order 5. Similarly $\mathrm{ord}_\infty^{\mathcal{H}}(\rho_2) = -2$. Hence:

$$\mathrm{ord}_\infty^{\mathcal{H}}(C_P) = \mathrm{ord}_\infty^{\mathcal{H}}(\tfrac{\rho_1}{\rho_2}) = -3.$$

Further, symmetrically, $\mathrm{ord}_{\mathcal{H}\times\{\infty\}}^{\mathcal{H}\times\mathcal{H}}(C) = -3$.
This calculation implies that if we see C as a function in $k(\mathrm{Sym}^2(\mathcal{H}))$ and we define $\theta : \mathcal{H} \to \mathrm{Sym}^2(\mathcal{H})$ given by $\theta(P) = \{P, \infty\}$ then $\mathrm{ord}_{\mathrm{Im}(\theta)}^{\mathrm{Sym}^2(\mathcal{H})}(C) = -3$.
Finally for $C \in k(\mathcal{J}) = k(\mathrm{Sym}^2(\mathcal{H}))$ since $\Theta \cong \mathrm{Im}(\theta)$, from the birationality of $\mathrm{Sym}^2(\mathcal{H}) \dashrightarrow \mathcal{J}$ (see the previous section) we deduce that $\mathrm{ord}_\Theta^{\mathcal{J}}(\frac{y_1-y_2}{x_1-x_2}) = \mathrm{ord}_\Theta^{\mathcal{J}}(C) = -3$. □

Naively, one could think that C has other poles than Θ, that is, $C \notin \mathcal{L}(n\Theta)$ and invalidate the previous proof. This is since another possible pole of $C \in k(\mathcal{J})$ could be $\Delta := \{[2R - 2\infty] : R \in \mathcal{H}\}$. However

$$C \cdot \tfrac{y_1+y_2}{y_1+y_2} |_\Delta = \tfrac{f(x_1)-f(x_2)}{(y_1+y_2)(x_1-x_2)} |_\Delta = \tfrac{s_1(A,B)}{y_1+y_2} |_\Delta = \tfrac{f'(X)}{2Y}$$

which implies that C is defined at almost all points of Δ. Further, C is also not defined at $\{\{R, \mathrm{t}(R)\} : R \in \mathcal{H}\} \subset \mathrm{Sym}^2(\mathcal{H})$ which is the canonical class of

$\mathrm{Sym}^2(\mathcal{H})$. This class in $\mathrm{Sym}^2(\mathcal{H})$ is blown down to the identity point $[0] \in \mathcal{J}$ (see [CF96]). Hence it does not give a codimension 1 subvariety of $\mathcal{J}$ and therefore not a pole of C. With this we have that $C \in \mathcal{L}(3\Theta) \setminus \mathcal{L}(2\Theta)$.
An obvious consequence of $C \in \mathcal{L}(3\Theta) \setminus \mathcal{L}(2\Theta)$ is that $\mathrm{ord}_\Theta^{\mathcal{J}}(C^2) = -6$, therefore $C^2 \in \mathcal{L}(6\Theta)$.

Now to simplify notation we look at another function in $k(\mathcal{J}) \cong k(A, B, C, D)$. We claim that there is a polynomial $\rho(A, B) \in k[A, B]$ such that the function $C^2 - \rho(A, B) \in \mathcal{L}(2\Theta)$. Moreover, we show in the next proposition that given such $\rho(A, B)$, the set $\{1, A, B, C^2 - \rho(A, B)\}$ forms a basis of $\mathcal{L}(2\Theta)$.

Proposition 2.4.3. *Let $\mathcal{H}/k$ be a hyperelliptic curve of genus 2 given by the equation $y^2 = x^5 + a_4x^4 + a_3x^3 + a_3x^2 + a_1x + a_0 = f(x)$ and let $A := x_1 + x_2, B := x_1x_2, C := \frac{y_1-y_2}{x_1-x_2} \in k(\mathcal{J})$.*
Let $\Theta \in Div(\mathcal{J})$ and put $\rho(A, B) := A^3 - AB + a_4A^2 + a_3A + a_2 \in k[A, B]$ then $\kappa_4 := C^2 - \rho(A, B) \in \mathcal{L}(2\Theta)$ and $\{1, A, B, \kappa_4\}$ is a basis of $\mathcal{L}(2\Theta)$.

Proof. As we saw in the previous proposition, $\mathrm{ord}_\Theta^{\mathcal{J}}(C^2) = -6$. We show that $\mathrm{ord}_\Theta^{\mathcal{J}}(C^2 - \rho(A, B)) = -2$.
Using the identities in (2.4) we have that:

$$C^2 = \frac{s_2(A, B) - 2s_3(A, B, C)}{A^2 - 4B} = \frac{f(x_1) + f(x_2) - 2y_1y_2}{(x_1 - x_2)^2}. \tag{2.11}$$

A similar reasoning as in the Proposition 2.4.2, here applied to (2.11) shows

$$\begin{aligned} \mathrm{ord}_\Theta^{\mathcal{J}}(y_1y_2) &= \mathrm{ord}_{\mathcal{H}\times\{\infty\}}^{\mathcal{H}\times\mathcal{H}}(y_1y_2) = -5, \\ \mathrm{ord}_\Theta^{\mathcal{J}}(x_1^n + x_2^n) &= \mathrm{ord}_{\mathcal{H}\times\{\infty\}}^{\mathcal{H}\times\mathcal{H}}(x_1^n + x_2^n) = -2n. \end{aligned} \tag{2.12}$$

Note that the term with most negative order at Θ in the numerator of (2.11) is $x_1^5 + x_2^5$. Hence $\mathrm{ord}_\Theta^{\mathcal{J}}(x_1^5 + x_2^5) = -10$ and the denominator of (2.11) satisfies $\mathrm{ord}_\Theta^{\mathcal{J}}(A^2 - 4B) = -4$.
We proceed to show that the numerator of $C^2 - \rho(A, B)$ has order -6 at Θ to infer that $\mathrm{ord}_\Theta^{\mathcal{J}}(C^2 - \rho(A, B)) = -2$ which is equivalent to $C^2 - \rho(A, B) \in \mathcal{L}(2\Theta)$. Note that we do not care about the term y_1y_2 in the equation (2.11) since its order at Θ is low enough (-5).

Recall that $\rho(A, B) = A^3 - AB + a_4A^2 + a_3A + a_2 \in k[A, B]$. It is easy to see that $\mathrm{ord}_\Theta\left(C^2 - \left(A^3 - AB + a_4A^2\right)\right) = -2$. The other two terms in $\rho(A, B)$ do not have any effect the order at Θ; they were chosen to simplify the lower degree terms:

$$\begin{aligned}\kappa_4 &= C^2 - \rho(A,B)\\ &= \tfrac{2a_0+a_1(x_1+x_2)+2a_2x_1x_2+a_3x_1x_2(x_1+x_2)+2a_4(x_1x_2)^2+(x_1x_2)^2(x_1+x_2)-2y_1y_2}{(x_1-x_2)^2}\\ &=: \frac{F_0(A,B)-2s_3(A,B,C)}{A^2-4B} \in k(\mathcal{J}).\end{aligned} \tag{2.13}$$

Similar to the calculation for C^2 one verifies that κ_4 has no other poles, so indeed $\kappa_4 \in \mathcal{L}(2\Theta)$.

To show the linear independence of $\{1, A, B, \kappa_4\}$, note that the minimal polynomial of $C^2 = \frac{f(x_1)+f(x_2)-2y_1y_2}{(x_1-x_2)^2} = \frac{s_2-2s_3}{A^2-4B}$ over $k(A,B)$ has degree 2, in fact is given by:

$$X^2 - \tfrac{2s_2}{A^2-4B}X + \tfrac{s_2^2-4\kappa(A,B)}{(A^2-4B)} \in k(A,B)[X]$$

where $\kappa(A,B) = f(x_1)f(x_2)$ (see Section 2.3.1 for details). Hence $C^2 \notin k(A,B)$ and therefore also $\kappa_4 \notin k(A,B)$. In particular κ_4 is linearly independent of $\{1, A, B\}$. Independence of $1, A, B$ is evident.

Finally to show that $\dim_k(\mathcal{L}(2\Theta)) = 4$, we use the Theorem of Riemann-Roch for Abelian varieties applied to $n\Theta \in \mathrm{Div}(\mathcal{J})$ (see [Mum74, Chapter III, §16]), namely:

$$\dim_k(\mathcal{L}(n\Theta)) = h_0(2\Theta) = \deg(n\Theta) = \tfrac{(n\Theta)^g}{g!}.$$

We are interested in $g = 2$, hence $\dim_k(\mathcal{L}(n\Theta)) = \frac{n^2\Theta\bullet\Theta}{2} = n^2$ since $\Theta \bullet \Theta = 2$ by the adjunction formula (or see Lemma 3.4.3 for an elementary deduction of this). With this we have that $\mathcal{L}(2\Theta)$ has dimension $2^2 = 4$ and $\{1, A, B, \kappa_4\}$ is a basis. □

Chapter 3

Hasse-Weil inequality *à la* Manin for genus 2

In this chapter we prove the genus 2 case of the Hasse-Weil inequality using elementary arguments that mimic as close as possible the elementary proof obtained by Manin in the genus 1 case. The difference with the genus 1 case is that we will require some theory of Abelian surfaces since the proof will rely on the Jacobian variety $\mathcal{J}$ of the genus 2 curve $\mathcal{H}$.

3.1 From elliptic curves to hyperelliptic curves

Before we expose the general idea for the proof of the Hasse-Weil theorem for genus 2 we will arrange Manin's proof in such a way that we can compare it with the new genus 2 scenario.

3.1.1 General idea for genus 1

Recall that in Chapter 1 the Hasse inequality for an elliptic curve $E/\mathbb{F}_q$ given by a Weierstrass equation $Y^2 = f(X)$, was obtained in an elementary way. Let $\phi, [n] \in \mathrm{End}_{\mathbb{F}_q}(E)$ be the q-th power Frobenius map and the multiplication by n map, respectively. Basically we proved that when $\psi_n := \phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(E)$ is non-trivial then it is of the form $(x, y) \mapsto \left(\frac{u_1(x)}{u_2(x)}, y\frac{v_1(x)}{v_2(x)}\right)$, (see Lemma 1.2.3), with $u_1, u_2, v_1, v_2 \in \mathbb{F}_q[x]$ such that $\gcd(u_1, u_2) = 1$. The Hasse inequality follows from:

$$\deg(\psi_n) = \deg(u_1) = n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q \geq 1. \tag{3.1}$$

Here $\deg(\psi_n) = [\mathbb{F}_q(E) : \psi_n^*\mathbb{F}_q(E)]$ is the degree of ψ_n and $\deg(u_1)$ is the degree of the polynomial $u_1 \in \mathbb{F}_q[x]$.

The Leftmost equality (3.1) follows from the inequality $\deg(u_1) > \deg(u_2)$ (see Lemma 1.2.6). The fact that $\deg(u_1) = \deg(\psi_n)$, is an elementary observation (see Section 1.2.1, Lemmas 1.2.4 and 1.2.5).

The Rightmost part of the equality (3.1) is shown by induction on n, observing that $\psi_{n+1} = \psi_n + [1] \in \mathrm{End}_{\mathbb{F}_q}(E)$ where $[1]$ is the identity map. Let $\mathbb{F}_q(x, y) \cong \mathbb{F}_q(E)$ where $y^2 = f(x)$. Using that $\mathrm{Mor}_{\mathbb{F}_q}(E, E) \cong E(\mathbb{F}_q(E))$ we define the following function for the isogeny $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(E, E)$ given by $(x, y) \mapsto (\frac{u_1(x)}{u_2(x)}, y\frac{v_1(x)}{v_2(x)})$:

$$d_n := \begin{cases} \deg(u_1) & \text{if } \psi_n \text{ is non-trivial;} \\ 0 & \text{otherwise.} \end{cases}$$

These equalities, led by a somewhat elaborate but elementary computation, give us the recursion relation $d_{n-1} + d_{n+1} = 2d_n + 2$ from which the formula $n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q$ for d_n is easily deduced.

Finally the non-negativity of $d_n = n^2 + (q+1-\#E(\mathbb{F}_q))n + q$ yields that the discriminant of this quadratic polynomial in n is non-positive, implying the Hasse inequality.

The above sketch is phrased in terms of elements $\psi_n \in \mathrm{End}_{\mathbb{F}_q}(E)$, however, Manin did not mention this endomorphism ring in his original proof. To obtain the translation from our perspective to his, consider the Weierstrass equation of E given by $Y^2 = f(X)$.

Define $P_n := P_0 + n \cdot (x, y)$ as a point in $E(\mathbb{F}_q(x, y)) \cong \mathrm{Mor}_{\mathbb{F}_q}(E, E)$ where $y^2 = f(x)$; by definition $P_n = (\phi + [n])(x, y) = \big(\frac{u_1(x)}{u_2(x)}, y\frac{v_1(x)}{v_2(x)}\big)$, so $P_0 = (x^q, yf(x)^{\frac{q-1}{2}})$ is the "q-Frobenius point". Now, $E : Y^2 = f(X)$ is isomorphic over $\mathbb{F}_q(x, y)$ to $E^{\text{TW}} : f(x)Y^2 = f(X)$. Note that the curve E^{TW} is the quadratic twist of $E/\mathbb{F}_q(x)$ by the non-square $f(x) \in \mathbb{F}_q(x)$.

An explicit isomorphism $E \xrightarrow{\sim} E^{\text{TW}}$ is given by $(a, b) \mapsto (a, \frac{b}{y})$; this means that P_n is mapped to $\big(\frac{u_1(x)}{u_2(x)}, \frac{v_1(x)}{v_2(x)}\big) \in E^{\text{TW}}(\mathbb{F}_q(x))$ where $u_1, u_2, v_1, v_2 \in \mathbb{F}_q[x]$.

Particularly under this isomorphism, the q-Frobenius point $P_0 \in E(\mathbb{F}_q(x, y))$ is mapped to $(x^q, f(x)^{\frac{q-1}{2}}) \in E^{\text{TW}}(\mathbb{F}_q(x))$.

Manin formulated the proof completely in terms of the group $E^{\text{TW}}(\mathbb{F}_q(x))$.

To interpret d_n more geometrically, let $\pi_1 : E \to \mathbb{P}^1$ be the double cover of $\mathbb{P}^1$ by E, so $\pi_1(x, y) = x$, then $\deg(\pi_1) = 2$. Also consider $\psi_n(x, y) = \left(\frac{u_1(x)}{u_2(x)}, y\frac{v_1(x)}{v_2(x)}\right)$ and the following diagram:

$$\begin{tikzcd}
E \arrow[r, "\psi_n"] \arrow[dr, "\pi_1 \circ \psi_n"'] & E \arrow[d, "\pi_1"] \\
 & \mathbb{P}^1
\end{tikzcd} \tag{3.2}$$

Here $\frac{\deg(\pi_1 \circ \psi_n)}{2} = \deg \psi_n = \deg(u_1) = d_n$.
Note that as before $\deg u_1$ means the degree of u_1 as a polynomial in x, not deg as a function in $\mathbb{F}_q(E)$.

3.1.2 General idea for genus 2

Now we define an analogous integer d_n for the genus 2 case such that it satisfies some polynomial behavior, and use it to prove the Hasse-Weil inequality for genus 2. To achieve this we do arithmetic with points in the Jacobian variety $\mathcal{J}$, as $\mathcal{H}$ does not have a natural group structure. More precisely, where in the elliptic curve case the group $\mathrm{Mor}_{\mathbb{F}_q}(E, E) \cong E(\mathbb{F}_q(E))$ was used, here we use $\mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J}) \cong \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$.

We are interested in $\mathcal{H}(\mathbb{F}_q)$ so, to work with $\mathcal{H}$ in $\mathcal{J}$ we use the theta divisor Θ of $\mathcal{J}$. This Θ is the image of the Abel-Jacobi map $\iota : \mathcal{H} \to \mathcal{J}$ given by $P \mapsto [P - \infty]$. Note that $\mathcal{H} \cong \Theta \subset \mathcal{J}$ is an irreducible subvariety of codimension 1. This means that Θ can be regarded as an ample[1] Weil divisor.

Now we construct our geometrical scenario. Let $\mathcal{H}/\mathbb{F}_q$ be a genus 2 curve given by the affine equation $y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = f(x)$. Let ∞ be the unique point at infinity on $\mathcal{H}$ and consider the Jacobian $\mathcal{J}$ of $\mathcal{H}$. Take $\phi, [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$, where as before ϕ denotes the q-th power Frobenius map and let $\Phi_n := \phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$. Consider the following diagram (the maps and notations used in the lower part of it will be explained below). The

[1] The basis of $\mathcal{L}(4\Theta)$ defines a projective embedding of $\mathcal{J} \hookrightarrow \mathbb{P}^{15}$, see [CF96]

diagram is analogous to the diagram (3.2):

$$\begin{tikzcd}
 & \mathcal{J} \arrow[dr, "\Phi_n:=\phi+[n]"] & \\
\mathcal{H} \arrow[ur, "\iota"] \arrow[rr, "\psi_n"] \arrow[ddrr, "\Psi_n"'] & & \mathcal{J} \arrow[d, dotted, "2:1"', "\kappa"] \arrow[dd, dotted, bend left, "\kappa_4"] \\
 & & \mathcal{K}_s \arrow[d, dotted, "\pi"] \\
 & & \mathbb{P}^1
\end{tikzcd} \tag{3.3}$$

The most important thing about this diagram is the map Ψ_n. The behavior of the degree of Ψ_n for every n will let us prove the Hasse-Weil inequality for genus 2. The calculation of its degree is the whole purpose of this chapter. We sketch in this section how this is done, and we formalize it later. But first, we proceed to describe the diagram (3.3).

The map κ is a rational 2:1 map. It sends points in the Jacobian to points in a variety $\mathcal{K}_s \subset \mathbb{P}^3$ described in the previous chapter, which is birational to the Kummer surface associated to $\mathcal{H}$. Recall that this variety consists of the identification of pairs of points $D, -D \in \mathcal{J}$. In other words, $\mathcal{K}_s$ is the quotient of $\mathcal{J}$ by $[-1] \in \mathrm{Aut}(\mathcal{J})$ where $[-1]$ is the automorphism obtained from the hyperelliptic involution in $\mathrm{Aut}(\mathcal{H})$. The variety $\mathcal{K}_s$ is a singular variety with 16 singular points corresponding to $\kappa(\mathcal{J}[2])$; note that the points of $\mathcal{J}$ fixed by $[-1]$ are precisely the 2-torsion points of $\mathcal{J}$.

The rational map κ can be described explicitly by four symmetric even functions $\{\kappa_1, \kappa_2, \kappa_3, \kappa_4\}$ on $\mathcal{J}$ that realize $\mathcal{K}_s$ as a surface in $\mathbb{P}^3$. This will be described in the following sections justified by the Lefschetz embedding theorem.
By the previous chapter we have that as that as a vector space $\dim_{\mathbb{F}_q}(\mathcal{L}(2\Theta)) = 4$, in fact $\mathcal{L}(2\Theta) = \langle\{\kappa_1, \kappa_2, \kappa_3, \kappa_4\}\rangle$. These functions on $\mathcal{J}$ are defined for the generic point $[(x_1, y_1) + (x_2, y_2) - 2\infty] \in \mathcal{J}$ as:

$$\kappa_1 := 1, \kappa_2 := x_1 + x_2, \kappa_3 := x_1 x_2, \kappa_4 := \tfrac{F_0(x_1,x_2) - 2y_1y_2}{(x_1-x_2)^2} \in \mathbb{F}_q(\mathcal{J})$$

where

$$F_0 := 2a_0 + a_1\kappa_2 + 2a_2\kappa_3 + a_3\kappa_2\kappa_3 + 2a_4\kappa_3^2 + \kappa_3^2\kappa_2. \tag{3.4}$$

By construction $\kappa_i : \mathcal{J} \cdots \to \mathbb{P}^1$ factors over $\mathcal{K}_s$. With this we proceed to sketch the calculation of $\deg \Psi_n$.

Consider the group $\mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J}) \cong \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$ where the addition of morphisms is induced by the addition on $\mathcal{J}$.
The q-th Frobenius action $\mathrm{Fr}_{\mathcal{H}}$ on $\mathcal{H}$ in $\mathcal{J}$ yields $\Phi := \iota \circ \mathrm{Fr}_{\mathcal{H}} = \phi \circ \iota$. Now, since $\iota, \Phi \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ we define $\psi_n := \Phi + n \cdot \iota = \Phi + ([n] \circ \iota) \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$.

Now suppose that $\psi_n(\mathcal{H}) \not\subset \Theta$, hence ψ_n is non-constant because $\psi_n(\infty) \in \Theta$. Therefore the map $\Psi_n = \kappa_4 \circ \psi_n$ is also non-constant. This will be shown by considering the poles of κ_4. We will conclude that if $(x, y) \in \mathcal{H}$ is the generic point, $\Psi_n : \mathcal{H} \to \mathbb{P}^1$ is given by the rational map $(x, y) \mapsto \kappa_4(\psi_n(x, y)) := \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)} \in \mathbb{F}_q(x)$ where $\mu_{1,n}, \mu_{2,n} \in \mathbb{F}_q[x]$ are coprime. Therefore we measure $\deg \Psi_n$ through the polynomial degree $\deg \mu_{1,n}$ since we will show that $\deg \mu_{1,n} > \deg \mu_{2,n}$. With this, we will get information about $\#\mathcal{H}(\mathbb{F}_q)$ for every n as we explain below.

Note that $\psi_n(\infty) = [0] \in \Theta \subset \mathcal{J}$ and Θ is exactly where $\kappa_4 \in \mathcal{L}(2\Theta) \subset \mathbb{F}_q(\mathcal{J})$ has a double pole. So, if $n \neq 0$ and $\psi_n(\mathcal{H}) \subset \Theta$ we have that $\Psi_n : \mathcal{H} \to \mathbb{P}^1$ is the constant map ∞, therefore we say that $\deg \Psi_n = 0$ in this case. For the case $n = 0$, namely $\psi_0 = \Phi = \iota \circ \mathrm{Fr}_{\mathcal{H}}$, we will prove separately that "$\deg \Phi_0 = 2q$" since $\kappa_4(\psi_0(x, y))$ is not well defined. In the remaining situation $\psi_n(\mathcal{H}) \not\subset \Theta$, the map $\Psi_n : \mathcal{H} \to \mathbb{P}^1$ is non-constant and fully determined by $\kappa_4(\psi_n(x, y)) \in \mathbb{F}_q(x)$. Now define δ_n as follows:

$$\delta_n := \begin{cases} 2q & \text{if } n = 0; \\ \deg \kappa_4(\psi_n(x, y)) = \deg \mu_{1,n} = \frac{\deg \Psi_n}{2} & \text{if } \psi_n(\mathcal{H}) \not\subset \Theta; \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

We will show the equalities involved in this definition later. Similarly to d_n in the elliptic case, we show that δ_n satisfies a second order recurrence relation. As a consequence δ_n is given by an explicit quadratic polynomial in n. The non-positiveness of its discriminant will entail the Hasse-Weil for genus 2 .

To understand δ_n geometrically, define $\pi : \mathcal{H} \to \mathbb{P}^1$ by $\pi(x, y) = x$ and consider the following diagram:

$$\begin{tikzcd}
\mathcal{H} \arrow[r, "\psi_n"] \arrow[d, "\pi"'] \arrow[rd, "\Psi_n"'] & \mathcal{J} \arrow[d, dotted, "\kappa_4"] \\
\mathbb{P}^1 \arrow[r, dotted, "\rho_n"'] & \mathbb{P}^1
\end{tikzcd} \tag{3.6}$$

Here ρ_n is the rational map defined by $x \mapsto \kappa_4(\psi_n(x,y)) = \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)}$ and $\Psi_n = \rho_n \circ \pi$. By definition, δ_n is the degree of the morphism ρ_n and therefore $2\delta_n$ is the degree of Ψ_n as asserted in the definition of δ_n.
Using this scenario, to prove the Hasse-Weil inequality for genus 2 we adapt Manin's ideas as we describe below.

Let $T := q + 1 - \#\mathcal{H}(\mathbb{F}_q)$ and recall that $\Phi_n := \phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$, then we will show that:

$$2\delta_n = \deg \Psi_n \ = 2\Theta \bullet {\Phi_n}^*\Theta = 2(2n^2 + Tn + 2q).$$

Here $\bullet$ denotes the intersection number $D_1 \bullet D_2$ of divisors D_1, D_2 on $\mathcal{J}$. The ideas behind these equalities are, first of all, the observation that deg Ψ_n equals the number of points counted with multiplicity in the preimage $\Psi_n^{-1}(\infty)$. Observing that $\kappa_4 \in \mathbb{F}_q(\mathcal{J})$ has only a pole of order 2 at the curve $\Theta \cong \mathcal{H}$ and no other poles, we will show that $\deg \Psi_n$ is 2 times the degree of $2\Theta \bullet \Phi_n^*\Theta$. If $\Phi_n(\Theta) \not\subset \Theta$, this last number is explicitly computed by $\deg \mu_{1,n}(x)$ as a polynomial in $\mathbb{F}_q[x]$ since Ψ_n is defined by $\kappa_4(\psi_n(x,y)) = \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)} \in \mathbb{F}_q(x)$, $\deg \mu_{1,n} > \deg \mu_{2,n}$ and κ_4 has Θ as its only double pole. If $\Phi_n(\Theta) \subset \Theta$ is a non-constant curve in $\mathcal{J}$, we will use a translation of $\Phi_n(\Theta)$ invariant under $[-1] \in \mathrm{End}(\mathcal{J})$ to proceed similarly.

The remaining equality $\Theta \bullet {\Phi_n}^*\Theta \ = 2n^2 + Tn + 2q$ relies on a second order recurrence relation for δ_n similar to the one that Manin obtained for genus 1. We will deduce that $2\delta_n + 4 = \delta_{n-1} + \delta_{n+1}$ using δ_{-1}, δ_0 and δ_1. After induction we obtain the aforementioned polynomial describing δ_n. Since $\delta_n \geq 0$ regardless of $\psi_n(\mathcal{H})$ being contained in Θ or not, one deduces that the discriminant of the polynomial $2x^2 + Tx + 2q \in \mathbb{Z}[x]$ is non-positive. This implies the Hasse-Weil inequality for genus 2.

3.2 Construction of $\mathcal{J}$ and an interesting family of curves $\Theta_n \subset \mathcal{J}$

In this section we construct our basic objects of this chapter. First we recall the construction of $\mathcal{J}$ using divisors of a genus 2 hyperelliptic curve $\mathcal{H} : Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ over $\mathbb{F}_q$ and linear equivalence. Moreover, we will show how to represent its elements in a compact way using the Mumford representation of the elements of $\mathrm{Pic}^0(\mathcal{H}) \cong \mathcal{J}$.

After constructing $\mathcal{J}$, a geometrical interpretation of $\mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ will be given In fact we show that $\mathcal{J}(\mathbb{F}_q(\mathcal{H})) \cong \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ where $\mathbb{F}_q(\mathcal{H})$ is the function field of $\mathcal{H}$. Using this we construct points $\mathcal{L}_n \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$ corresponding to certain morphisms $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$, which are closely related to the q-th Frobenius and the multiplication by n endomorphisms of $\mathcal{J}$ as we sketched in the previous section. The points $\mathcal{L}_n$ yield curves $\Theta_n := \mathrm{Im}(\psi_n) \subset \mathcal{J}$. These curves can be seen as elements of $\mathrm{Div}(\mathcal{J})$ since they have codimension 1 in $\mathcal{J}$. In order to work with $\mathcal{H}$ using the geometry of $\mathcal{J}$, we work with the curve $\Theta \subset \mathcal{J}$ which is isomorphic to $\mathcal{H}$ as we saw in the previous chapter. The intersection number $\Theta \bullet \Theta_n$ will be of our interest as we will see in the rest of the chapter.

A reason why we work with the curves $\Theta = \iota(\mathcal{H})$ and $\Theta_n = \psi_n(\mathcal{H})$ in $\mathrm{Div}(\mathcal{J})$ and not directly with the maps $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is because divisors will let us work geometrically to get information on $\#\mathcal{H}(\mathbb{F}_q)$ for every n. We will deduce a quadratic polynomial in n describing $\deg(\Psi_n)$ using some intersection theory on $\Theta, \Theta_n \in \mathrm{Div}(\mathcal{J})$. Finally, as we saw in the beginning of this chapter, the behavior of the discriminant of the quadratic polynomial describing $\deg(\Psi_n)$ will have as a consequence the Hasse-Weil inequality for genus 2.

3.2.1 Definition of $\mathcal{J}(k)$ via $\mathrm{Pic}^0(\mathcal{H})$ and its elements

Recall that we are working with points in the Jacobian $\mathcal{J}/k$ of a hyperelliptic curve $\mathcal{H}/k$ of genus 2 with one distinguished point ∞. Let $\overline{k} := k^{sep}$ be a separable closure of k.

It is well known that the Abelian variety $\mathcal{J}$ can be embedded in $\mathbb{P}^{15}$ (see [Fly90]) and sometimes in $\mathbb{P}^8$ (see [Gra90]); this suggests that it may not be a good idea to work with the points of these models of $\mathcal{J}$. Therefore we will use divisor classes on $\mathcal{H}$ modulo linear equivalence over k, we recall this below.

Consider the group $\mathrm{Pic}^0(\mathcal{H}) := \mathrm{Div}^0(\mathcal{H})/\sim$ where $D_1 \sim D_2$ if and only if $D_1 - D_2 = (g) \in \mathrm{Div}^0(\mathcal{H})$ for some $g \in \overline{k}(\mathcal{H})$. We have that $\mathrm{Pic}^0(\mathcal{H}) \cong \mathcal{J}(\overline{k})$ as groups by a result due to Abel and Jacobi over $\mathbb{C}$. Over $\overline{k}$ this isomorphism also holds using the Lefschetz principle. We are interested in $\mathcal{J}(k)$, so we proceed to sketch the construction of it. A more detailed algebraic treatment of this for hyperelliptic curves is presented in [Mum84] and in an analytic way in [ACGH13].

The isomorphism $\mathrm{Pic}^0(\mathcal{H}) \cong \mathcal{J}(\overline{k})$ is a consequence of the surjectivity of the linear extension to degree 0 divisors of the usual Abel-Jacobi map $P \mapsto [P - \infty]$ that embeds $\mathcal{H}$ into $\mathcal{J}$. The linearly extended Abel-Jacobi map is naturally a homomorphism $\alpha : \mathrm{Div}^0(\mathcal{H}) \to \mathcal{J}$ whose kernel consists of all principal divisors $(g) \in \mathrm{Div}^0(\mathcal{H})$, where $g \in \overline{k}(\mathcal{H})^*$ (see [Sil94] III,2.6). These principal divisors in $\mathrm{Ker}(\alpha)$ are exactly characterized by $\sim$, that is, they are the divisors "indistinguishable" under α. Therefore $\mathrm{Div}^0(\mathcal{H})/\mathrm{Ker}(\alpha) \cong \mathcal{J}(\overline{k})$ as groups.

Now, we are interested in the divisor classes representing $\mathcal{J}(k) \subset \mathcal{J}(\overline{k})$. There are two distinct natural choices for a definition of $\mathcal{J}(k)$: the first one is to take $G_k = \mathrm{Gal}(\overline{k}/k)$ and consider the G_k-invariants in $\mathrm{Div}^0(\mathcal{H})/\mathrm{Ker}(\alpha)$, and their image under the Abel-Jacobi map,

$$\left(\mathrm{Div}^0(\mathcal{H})/\mathrm{Ker}(\alpha)\right)^{G_k} \longrightarrow \mathcal{J}.$$

The other choice is to take $\mathrm{Div}^0(\mathcal{H})(k)$, the group of G_k-invariant divisors on $\mathcal{H}$ of degree 0, and take the quotient by the principal divisors (g) with $g \in k(\mathcal{H})^*$. The image under the Abel-Jacobi map

$$\left(\mathrm{Div}^0(\mathcal{H})\right)^{G_k} / \left(k(\mathcal{H})^*\right) \longrightarrow \mathcal{J}$$

is the alternative choice.

For general curves and fields the two choices can be different. However for curves of genus 2 they coincide, as is explained, e.g., in [PS97, Section 3]. The justification of $\mathrm{Pic}^0(\mathcal{H})(k) \cong \mathcal{J}(k)$ is relevant since we will work with the Jacobian of $\mathcal{H}$ over a non-perfect field $k := \mathbb{F}_q(\mathcal{H})$, using divisors classes.

Now we show how representatives of the divisor classes in $\mathrm{Pic}^0(\mathcal{H})(k)$ look like.
For genus 2, if $\infty \in \mathcal{H}(k)$ (our case), $[D] \in \mathrm{Pic}^0(\mathcal{H})(k)$ can be represented by $[P + Q - 2\infty]$ or $[R - \infty]$. In other words, if $D \in \mathrm{Div}^0(\mathcal{H})$, there is an effective

$D_0 \in \mathrm{Div}(\mathcal{H})$ such that $D \sim D_0 - k\infty$ with $\deg(D_0) = k \leq g = 2$.
To show this, let $D := D_1 - D_2 \in \mathrm{Div}^0(\mathcal{H})$ with D_1, D_2 effective. Further, suppose that there are no pairs of points in the supports of D_1 and D_2 related by the hyperelliptic involution $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$ (if there are, use that $P + \mathfrak{t}(P) - 2\infty \sim 0$).
The first case is for $D = P_1 - P_2$ where $P_i \in \mathcal{H}$. If $P_2 = \infty$ we are done. Suppose that $P_2 \neq \infty$, if $P_1 \neq \infty$ we have that $P_1 - P_2 \sim P_1 + \mathfrak{t}(P_2) - 2\infty$ since $P_2 + \mathfrak{t}(P_2) - 2\infty \sim 0$. For $P_1 = \infty$ we have that $P_1 - P_2 = \infty - P_2 \sim \mathfrak{t}(P_2) - \infty$.

Now suppose that $D = D_1 - D_2 \in \mathrm{Div}^0(\mathcal{H})$ with $\deg D_i \geq 2$ and D_i effective. Recall that the Theorem of Riemann-Roch guarantees the existence of a function with prescribed poles and zeroes when the number of the required zeros is at most $2g - 2$. More precisely, it says in our genus 2 case that for $\mathfrak{D} \in \mathrm{Div}(\mathcal{H})$ we have that $\dim \mathcal{L}(\mathfrak{D}) = \deg \mathfrak{D} - 1 + \dim \mathcal{L}(\omega_{\mathcal{H}} - \mathfrak{D})$.
Take $F \in \mathcal{L}(D_1 - D_2 + 2\infty)$ with $F \neq 0$ (this vector space has at least dimension 1 by Riemann-Roch since $\deg(D_1 - D_2 + 2\infty) = 2$, so, this F exists). Note that $(F) \neq Q - \infty$ for $Q \in \mathcal{H}$ as $\deg D_i \geq 2$ (and also $Q - \infty$ is not principal). Therefore $(F) = D_0 - D_1 + D_2 - 2\infty$ and $D' := D + 2\infty + (F) = D_1 - D_2 + 2\infty + (F) = D_0$ has degree 2 and is effective. Hence $D_0 - 2\infty \sim D_1 - D_2 = D$ if and only if $D = D_1 - D_2 \in [D_0 - 2\infty]$.

Now, for the divisors $[P + Q - 2\infty]$ we have that P, Q are affine points of $\mathcal{H}$ (not related by the hyperelliptic involution $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$), and moreover since we want the divisor $P + Q$ to be fixed by the absolute Galois group of k, either both points are defined over k or they are conjugate over k and their coordinates generate a quadratic extension of k.
For the second form $[R - \infty]$ we have that $R \in \mathcal{H}$ is k-rational. A special case is $R = \infty$ which describes the zero point in $\mathcal{J}(k)$.
Note that the formal addition of the representatives of divisor classes in $\mathrm{Pic}^0(\mathcal{H})(k)$ remains *reduced* to these cases modulo $\sim$, by the previous discussion.

A handy way to represent the reduced representants of elements of $\mathrm{Pic}^0(\mathcal{H})(k)$ in order to do arithmetic with them, is the Mumford representation [Mum84]. Let $P := (x_P, y_P)$, $Q := (x_Q, y_Q)$ and $R := (x_R, y_R) \in \mathcal{H}$. We encode the divisor classes $[P + Q - 2\infty]$ and $[R - \infty]$ in a unique way. For the first case this representation consists of two polynomials $\langle u(t), v(t) \rangle$ where $u \in k[t]$ is monic and quadratic and satisfies $u(x_P) = u(x_Q) = 0$. The polynomial v has degree at most 1 and is determined by $v(x_P) = y_P$ and $v(x_Q) = y_Q$. A divisor class $[R - \infty]$ is represented as $\langle t - x_R, y_R \rangle$. Moreover we represent $[0]$ as $\langle 1, 0 \rangle$. Addition between divisor classes using Mumford representation was studied in the general setting for hyperelliptic curves of genus g by Cantor in [Can87]. Cantor's algorithm is very practical although there are ways to improve it if the genus g is fixed (see for example [CL12, DO14]).

We use Mumford representation $\langle u(t), v(t)\rangle \in \mathcal{J}(k)$ to do explicit arithmetic in $\mathcal{J}$. For the theory we will use the usual divisor class representation $[P + Q - 2\infty]$, $[P - \infty]$ or $[0]$.

3.2.2 Morphisms as points

In this small section, we show how to treat the Abelian group $\mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ as the group of points on the Jacobian of $\mathcal{H}$ over the function field $k(\mathcal{H})$. We do this since in the rest of this chapter we study a family of morphisms $\psi_n \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ by doing arithmetic with the associated points $\mathcal{L}_n \in \mathcal{J}(k(\mathcal{H}))$. It will turn out that the Mumford representation comes in very handy here.

The set $\mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ has a natural Abelian group structure using pointwise addition of morphisms by means of the addition $\oplus$ on $\mathcal{J}$.
To be precise, let $\alpha, \beta \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$, we define for every $P \in \mathcal{H}$ the addition of morphisms as $(\alpha + \beta)(P) := \alpha(P) \oplus \beta(P) \in \mathcal{J}$, therefore $\alpha + \beta \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$. For the inverse $-\alpha$, consider the $[-1]$-map on the Jacobian, which is obtained from the hyperelliptic involution $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$. We define $-\alpha := [-1] \circ \alpha$. Finally the neutral element is given by the map $\{P \mapsto [0]\} \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$. With these definitions, the Abelian group structure of $\mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ follows from the Abelian group structure of $\mathcal{J}$. The following lemma allows us to work with the elements of $\mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ as points of $\mathcal{J}(k(\mathcal{H}))$.

Lemma 3.2.1. *Let $\mathcal{H}/k$ be a hyperelliptic curve of genus g. Consider its associated Jacobian variety $\mathcal{J}$, then $\mathcal{J}(k(\mathcal{H})) \cong \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ as Abelian groups.*

Proof. This is a special case of a much more general fact. Namely; if $V \subset \mathbb{P}^N$ is a projective variety and C a smooth irreducible curve over k, then:

$$\begin{aligned} \Upsilon : V(k(C)) &\to \mathrm{Mor}_k(C, V) \\ (\alpha_0 : \ldots : \alpha_N) &\mapsto \{P \mapsto (\alpha_0(P) : \ldots : \alpha_N(P))\} \end{aligned} \tag{3.7}$$

is a bijection. This general fact follows from [Sil86] (II,2.1).
In the special case of this lemma we have that $C := \mathcal{H}$ and $V := \mathcal{J}$ (which indeed is a projective variety; e.g., it can be embedded in $\mathbb{P}^{4^g-1}$ as can be seen in [CF96] for $g = 2$ and in [Mum66] for the general case). The group isomorphism follows from the bijection (3.7) and the Abelian group structure on $\mathcal{J}(k(\mathcal{H}))$. □

3.2.3 The family of curves $\Theta_n \subset \mathcal{J}$ via $\phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$

Recall the diagram (2.8) in Section 2.4 that we used to construct $\Theta \subset \mathcal{J}$. Using that diagram we construct similarly the curves Θ_n. Fix $\mathcal{A} := \mathcal{J}$ and consider the q-th Frobenius action $\mathrm{Fr}_{\mathcal{H}} \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{H})$ on the coordinates of the points in $\mathcal{H}$. Take $\Phi := \iota \circ \mathrm{Fr}_{\mathcal{H}}, \iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$. Since $\mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is an Abelian group we define $\psi_n := \Phi + n \cdot \iota$ for $n \in \mathbb{Z}$.

Using the diagram (2.8), assume that ψ_n is non-constant. Let $\Phi_n := \phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$ where ϕ is the q-th Frobenius endomophism, then we have the following commutative diagram:

$$\begin{tikzcd}
\mathcal{H} \arrow[r, "\iota"] \arrow[dr, "\psi_n"'] & \mathcal{J} \arrow[d, "\Phi_n"] \\
 & \mathcal{J}.
\end{tikzcd} \tag{3.8}$$

We have that $\psi_n = \Phi_n \circ \iota = (\phi + [n]) \circ \iota$ is uniquely determined by $\Phi_n \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$ (see Section 2.4 for details). We define the curves $\Theta_n := \psi_n(\mathcal{H}) \subset \mathcal{J}$. These curves Θ_n can be regarded as divisors in $\mathrm{Div}(\mathcal{J})$ since they have codimension 1 in $\mathcal{J}$.

We have been emphasizing previously the constraint on $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ to be *non-constant*. This is motivated by some special cases where $\Phi = -n \cdot \iota$ and therefore $\psi_n = 0$. This also means that the curve $\Theta_0 = -[n](\Theta) \subset \mathcal{J}$ for some n and $[n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$. We give an example of this situation below.

Example 3.2.2. *($\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is the zero map)*

Consider the hyperelliptic curve $Y^2 = X^5 + 5X$ over $\mathbb{F}_{7^2}$. An explicit computation of ψ_7 shows that this is the map that sends every point of $\mathcal{H}$ to $[0] \in \mathcal{J}$. This is because $\Phi, -7\iota \in \mathrm{Mor}_{\mathbb{F}_{7^2}}(\mathcal{H}, \mathcal{J})$ are the same morphism, where $\Phi(x, y) = [(x^{7^2}, y^{7^2}) - \infty]$. We check this with MAGMA:

```
> p := 7;
> F := FiniteField(p^2);
> P<x> := PolynomialRing(F);
> f := x^5 + 5*x;
> H := HyperellipticCurve(f);
> FH<X,Y> := FunctionField(H);
> HE := BaseExtend(H,FH);
> JE := Jacobian(HE);
> M<t> := PolynomialRing(FH);
> q := p^2;
> Phi := JE![t-X^q, Y^q];
> GPt := JE![t-X,   Y];
> -7*GPt;
```

```
(x + 6*X^49, (X^120 + X^116 + 5*X^112 + 6*X^108 + X^92 + X^88 + 5*X^84 +
6*X^80 + 5*X^64 + 5*X^60 + 4*X^56 + 2*X^52 + 6*X^36 + 6*X^32 + 2*X^28 +
X^24)*Y, 1)
> Phi;
(x + 6*X^49, (X^120 + X^116 + 5*X^112 + 6*X^108 + X^92 + X^88 + 5*X^84 +
6*X^80 + 5*X^64 + 5*X^60 + 4*X^56 + 2*X^52 + 6*X^36 + 6*X^32 + 2*X^28 +
X^24)*Y, 1)
> Phi+7*GPt;
(1, 0, 0)
```

therefore $\psi_7 := \Phi + 7\iota \in \mathrm{Mor}_{\mathbb{F}_{7^2}}(\mathcal{H}, \mathcal{J})$ is the zero map.

This situation is in some sense exceptional since in this example, $\mathcal{J}$ is isogenous to the square of a supersingular elliptic curve. To be more precise, $\mathcal{J} \sim E_S \times E_S$ and the ground field has p^2 elements. In this case the characteristic polynomial of Frobenius $\phi \in \mathrm{End}_{\mathbb{F}_{7^2}}(\mathcal{J})$ is given by $\chi_\phi(X) := (X + 7)^4$ which is the main reason of this behavior.
The general construction of these curves having Jacobian isogenous to a square of a supersingular elliptic curve was achieved by Moret-Bailly in [MB81].

In the next proposition we calculate the number of points of $\mathcal{H}/\mathbb{F}_q$ assuming that there is an $n \in \mathbb{Z}$ such that $\psi_n = (\phi + [n]) \circ \iota = 0$. In particular the proposition implies the Hasse-Weil inequality under this additional assumption. It turns out that this is an exceptional case, and we will deal with it in a combinatorial way. Later, in Subsection 3.4.2 we treat the general case, assuming that $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is non-constant for all n. This general case is treated in a more geometric way.

Proposition 3.2.3. *Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2, given by an equation $y^2 = f(x)$ with f of degree 5. Let $\mathcal{J}$ be the Jacobian of $\mathcal{H}$ and $\iota\colon \mathcal{H} \to \mathcal{J}$ the map $P \mapsto [P - \infty]$. Suppose that there is an $n \in \mathbb{Z}$ such that $\psi_n = (\phi + [n]) \circ \iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is constant. Then q is a perfect square and $\#\mathcal{H}(\mathbb{F}_q) = q + 1 + 4n = q + 1 \pm 4\sqrt{q}$.*

Proof. First, we show that if $\psi_n = (\phi + [n]) \circ \iota$ is constant, then $\phi = -[n]$.

We have that $\psi_n = (\phi + [n]) \circ \iota$ is constant and $0 \in \mathrm{Im}\psi_n$, hence $\psi_n = 0$; this is equivalent to $(\phi + [n])(\Theta) = 0$ since $\Theta = \iota(\mathcal{H})$.
Moreover, Θ generates $\mathcal{J}$, that is $\mathcal{J} = \{D_1 + D_2 \ : \ D_1, D_2 \in \Theta\}$. So if any $\varphi \in \mathrm{End}(\mathcal{J})$ is zero on Θ then it is the zero map. Hence we have $\phi = -[n] \in \mathrm{End}(\mathcal{J})$.
Note that $\phi = -[n]$ implies $q^2 = \deg(\phi) = \deg([-n]) = n^4$, hence $q = n^2$, so q is a perfect square and $n = \pm\sqrt{q}$ (depending on the sign of n).

Now we proceed to count $\#\mathcal{H}(\mathbb{F}_q)$. Using that $\phi = -[n]$ we have that:

$$\#\mathcal{J}(\mathbb{F}_q) = \#\mathrm{Ker}(\phi - [1]) = \#\mathrm{Ker}(-[n+1]) = (n+1)^4. \tag{3.9}$$

(Here we used that $n+1$ is not a multiple of $\mathrm{char}(\mathbb{F}_q)$). Moreover, an easy counting argument (see [CF96, Chapter 8,§2]) shows:

$$\#\mathcal{J}(\mathbb{F}_q) = \frac{\#\mathcal{H}(\mathbb{F}_q)^2 + \#\mathcal{H}(\mathbb{F}_{q^2})}{2} - q. \tag{3.10}$$

Consider the quadratic twist of $\mathcal{H}$ denoted by $\mathcal{H}^{\text{TW}}$ and its Jacobian $\mathcal{J}^{\text{TW}}$. We have that:

$$\#\mathcal{J}^{\text{TW}}(\mathbb{F}_q) = \mathrm{Ker}(\phi + [1]) = \mathrm{Ker}(-[n] + 1) = (n-1)^4 \tag{3.11}$$

Similarly as in (3.10) and using that $\#\mathcal{H}(\mathbb{F}_q) + \#\mathcal{H}^{\text{TW}}(\mathbb{F}_q) = 2q + 2 = 2n^2 + 2$ and $\mathcal{H}^{\text{TW}}(\mathbb{F}_{q^2}) \cong \mathcal{H}(\mathbb{F}_{q^2})$, we have that:

$$\begin{aligned} \#\mathcal{J}^{\text{TW}}(\mathbb{F}_q) &= \frac{\#\mathcal{H}^{\text{TW}}(\mathbb{F}_q)^2 + \#\mathcal{H}(\mathbb{F}_{q^2})}{2} - q \\ &= \frac{(2n^2 + 2 - \#\mathcal{H}(\mathbb{F}_q))^2 + \#\mathcal{H}(\mathbb{F}_{q^2})}{2} - q = (n-1)^4 \end{aligned} \tag{3.12}$$

Subtracting (3.12) from (3.10) yields:

$$\begin{aligned} \#\mathcal{H}(\mathbb{F}_q)^2 - (2n^2 + 2 - \#\mathcal{H}(\mathbb{F}_q))^2 &= 2\big((n+1)^4 - (n-1)^4\big) \\ &= 16n(n^2+1), \end{aligned} \tag{3.13}$$

which can be rewritten as $\#\mathcal{H}(\mathbb{F}_q) = n^2 + 4n + 1 = q + 1 \pm 4\sqrt{q}$. □

Applying Proposition 3.2.3 to $\mathcal{H} : y^2 = x^5 + 5x$ over $\mathbb{F}_{7^2}$ (see Example 3.2.2) which has the property $\psi_7 = 0$, give us $\#\mathcal{H}(\mathbb{F}_{7^2}) = 49{+}1{+}4{\cdot}7 = 78$. Moreover, if we calculate its quadratic twist $\mathcal{H}^{\text{TW}}$ we have that $\psi^{\text{TW}}_{-7} \in \mathrm{Mor}_{\mathbb{F}_{7^2}}(\mathcal{H}^{\text{TW}}, \mathcal{J}^{\text{TW}})$ is trivial, hence $\#\mathcal{H}^{\text{TW}}(\mathbb{F}_{7^2}) = 49 + 1 - 4 \cdot 7 = 22$.

Now we associate to every curve $\Theta_n \subset \mathcal{J}(\mathbb{F}_q)$ a point $\mathcal{L}_n \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$. We do this to look at the coefficients that define $\mathcal{L}_n$ in its Mumford representation which are functions in $\mathbb{F}_q(\mathcal{H})$. These coefficients will be shown to encode explicit information about $\#\mathcal{H}(\mathbb{F}_q)$.

Definition 3.2.4. *Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 and $(x, y) \in \mathcal{H}(\mathbb{F}_q(\mathcal{H}))$ its generic point. We define the following point in $\mathcal{J}(\mathbb{F}_q(\mathcal{H}))$:*

$$\mathcal{L}_n := \Phi_n(\iota(x, y)) = \psi_n(x, y) = [(x^q, yf(x)^{\frac{q-1}{2}}) - \infty] \oplus n[(x, y) - \infty]$$

where n denotes the multiplication by $n \in \mathbb{Z}$ in $\mathrm{End}(\mathcal{J})$.

With this definition we now characterize easily the inverse $-\mathcal{L}_n$ in $\mathcal{J}$.

Lemma 3.2.5. *Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 with one point at infinity and $\mathcal{J}$ its Jacobian. Let $P := (x, y) \in \mathcal{H}(\mathbb{F}_q(\mathcal{H}))$ be the generic point of $\mathcal{H}$, then $-\mathcal{L}_n = \psi_n(x, -y) \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$.*

Proof. Let $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$ be the hyperelliptic involution, then:

$$\begin{aligned} -\mathcal{L}_n &= -\psi_n(x, y) = -\phi([(x, y) - \infty]) - n[(x, y) - \infty] \\ &= [\mathfrak{t}(x^q, y^q) - \infty] + n[\mathfrak{t}(x, y) - \infty] \\ &\sim [(x^q, -y^q) - \infty] + n[(x, -y) - \infty] = \psi_n(x, -y). \end{aligned}$$ □

The point $\mathcal{L}_n \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$ is completely determined by ψ_n using Lemma 3.2.1, since (using notation as in the proof of 3.2.1) $\Upsilon(\mathcal{L}_n) = \psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$.

3.3 Even functions in $\mathbb{F}_q(\mathcal{J})$ and the map $\Psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathbb{P}^1)$

Let $(x, y) \in \mathcal{H}$ be the generic point. In this section we look at the even functions in $\mathcal{J}$. We built already in Proposition 2.4.3 a set of generators for them, namely $\{\kappa_1, \kappa_2, \kappa_3, \kappa_4\} \subset \mathbb{F}_q(\mathcal{J})$. These generators form a basis of the vector space $\mathcal{L}(2\Theta) \subset \mathcal{L}(4\Theta)$ as we saw in the previous chapter, further, the basis defines a map $\mathcal{J} \cdots \to \mathbb{P}^3$ with image a surface $\mathcal{K}_s \subset \mathbb{P}^3$. This surface is birational to the Kummer surface associated to $\mathcal{H}$. The map $\mathcal{J} \to \mathcal{K}_s$ will be denoted κ. The map κ is defined over $\mathbb{F}_q$ and given by $D \mapsto [\kappa_1(D) : \kappa_2(D) : \kappa_3(D) : \kappa_4(D)]$. The projective coordinate corresponding $\kappa_4(\mathcal{L}_n) = \kappa_4(\psi_n(x, y)) \in \mathbb{P}^1(\mathbb{F}_q(\mathcal{H}))$ will be associated to a rational map Ψ_n whose degree is of our main interest. The morphism $\Psi_n : \mathcal{H} \to \mathbb{P}^1$ is defined as $(x, y) \mapsto \kappa_4(\mathcal{L}_n)$. Moreover, the degree of the map Ψ_n will define the integer δ_n already mentioned at the beginning of this chapter. The integer $\deg(\Psi_n)$ will be expressed as the degree of some rational function, since we will show that $\kappa_4(\mathcal{L}_n) \in \mathbb{F}_q(x)$.

Our goal is to show that $\deg \kappa_4(\mathcal{L}_n)$ is given by a quadratic polynomial in n. The discriminant turns out to be negative and a consequence of this is the Hasse-Weil inequality for genus 2.

We start by motivating the analysis of the points $\mathcal{L}_{\pm 1} \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$, evaluating them with the even function $C^2 := \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \in \mathbb{F}_q(\mathcal{J})$. This will allow us to obtain a formula for $\#\mathcal{H}(\mathbb{F}_q)$ for every hyperelliptic curve of genus g encoded in the degree of the numerator of $C^2(\mathcal{L}_{\pm 1})$. Note that we have shown already that $C^2 \in \mathcal{L}(6\Theta) \subset \mathbb{F}_q(\mathcal{J})$ (see Proposition 2.4.2). After this we use the "better" function $\kappa_4 \in \mathcal{L}(2\Theta)$ compared to C^2 constructed in Proposition 3.16. This function has smaller pole order at Θ and we use it to also to obtain information of $\#\mathcal{H}(\mathbb{F}_q)$ as well, via $\kappa_4(\mathcal{L}_{\pm 1})$. This will give us the step induction to obtain the degree of $\kappa_4(\mathcal{L}_n)$ as a quadratic polynomial in n.

Consider the point $\mathcal{L}_{-1} \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$, that is, the point related to the morphism $\psi_{-1} = \Phi - \iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ via Lemma 3.2.1. Note that $\#\psi_{\text{-}1}^{-1}([0]) = \#\mathcal{H}(\mathbb{F}_q)$. This is since if $(x_0, y_0) \in \mathcal{H}(\overline{\mathbb{F}}_q)$, we have that:

$$\psi_{\text{-}1}(x_0, y_0) = [({x_0}^q, {y_0}^q) + (x_0, -y_0) - 2\infty] \in \mathcal{J}(\overline{\mathbb{F}}_q).$$

Therefore $\psi_{\text{-}1}(x_0, y_0) = [0]$ if and only if $[({x_0}^q, {y_0}^q) - \infty] \sim [(x_0, y_0) - \infty]$ if and only if $({x_0}^q, {y_0}^q) = (x_0, y_0) \in \mathcal{H}(\mathbb{F}_q)$.
With this observation, an interesting proposition arises for a hyperelliptic curve of genus g.

Proposition 3.3.1. *Let $\mathcal{H}$ be a hyperelliptic curve given by the equation $Y^2 = f(X)$ for some separable polynomial f. Let g be the genus of $\mathcal{H}$ and suppose $\mathcal{H}$ has only one rational point at infinity. Consider the function field $\mathbb{F}_q(\mathcal{H}) \cong \mathbb{F}_q(x, y)$ where $y^2 = f(x)$.*
Let $\langle t^2 + \alpha(x)t + \beta(x), \gamma(x, y)t + \delta(x, y)\rangle$ be the Mumford representation of $\mathcal{L}_{\text{-}1}$ then $\gamma^2 \in \mathbb{F}_q(x)$ and considered as a rational function in the variable x one has $\deg \gamma^2 = (2g - 1)q + \#\mathcal{H}(\mathbb{F}_q) - 1$.

Proof. The Mumford representation of $\mathcal{L}_{-1}$ is given by two polynomials in $\mathbb{F}_q(\mathcal{H})[t]$, namely:

$$\begin{aligned} \mathcal{L}_{\text{-}1} = \psi_{\text{-}1}(x, y) &= [\Phi(x, y) - \infty] \oplus [(x, -y) - \infty] \\ &= [(x^q, y^q) + (x, -y) - 2\infty] \\ &= \langle t^2 - (x^q + x)t + x^{q+1}, \tfrac{y^q + y}{x^q - x} t + \tfrac{xy^q + x^q y}{x^q - x}\rangle. \end{aligned}$$

Therefore $\gamma(x, y) = \frac{y^q + y}{x^q - x} \in \mathbb{F}_q(\mathcal{H})$, and:

$$\begin{aligned} \gamma(x, y)^2 = \Big(\frac{y^q + y}{x^q - x}\Big)^2 &= \Big(\frac{y(f(x)^{\frac{q-1}{2}} + 1)}{x^q - x}\Big)^2 \\ &= \frac{f(x)(f(x)^{\frac{q-1}{2}} + 1)^2}{(x^q - x)^2} \in \mathbb{F}_q(x). \end{aligned} \tag{3.14}$$

Since f is separable we have $\deg f(x) = 2g + 1$. Therefore the degree of the numerator of γ^2 before cancellations is given by $(2g + 1)q$. We proceed to count the cancellations to get the final degree.

Since $\gamma^2 \in \mathbb{F}_q(x) \subset \mathbb{F}_q(x,y) \cong \mathbb{F}_q(\mathcal{H})$ is a function from $\mathcal{H}$ to $\mathbb{P}^1$ we evaluate this function at $x = \alpha \in \mathbb{F}_q$ and check whether $(\alpha, \beta) \in \mathcal{H}(\mathbb{F}_q)$ (meaning that $f(\alpha)$ is zero or is a square in $\mathbb{F}_q^*$) or neither. Using the equation (3.14) we have that $\beta^2 = f(\alpha)$ and if $f(\alpha) \neq 0$ then $f(\alpha)^{\frac{q-1}{2}} = \pm 1 \in \mathbb{F}_q$ (Euler's criterion). The sign depends on the conditions $\beta \in \mathbb{F}_q^*$ or $\beta \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ for $+1$ and -1 respectively. This leaves us three possible cases for cancellations using the numerator of the equation (3.14).

Case $\beta \notin \mathbb{F}_q$:
If this holds, then $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, hence $(f(\alpha)^{\frac{q-1}{2}} + 1)^2 = 0$ since $f(\alpha)$ is not a quadratic residue in $\mathbb{F}_q$. Therefore the numerator of (3.14) has the factor $x - \alpha$ which cancels with a factor $(x - \alpha)$ in the denominator since $\alpha \in \mathbb{F}_q$. Moreover, $(x - \alpha)$ cancels twice since both $(x^q - x)^2$ and $(f(x)^{\frac{q-1}{2}} + 1)^2$ are squares. The factor $(x - \alpha)$ does not have higher multiplicity as follows from the factorization of the denominator. With this we have a cancellation at all the points $(\alpha, \beta) \in \mathcal{H}$ such that $\alpha \in \mathbb{F}_q$ and $\beta \notin \mathbb{F}_q$. There are exactly $2q+1-(\#\mathcal{H}(\mathbb{F}_q)+\#\mathcal{W}(\mathbb{F}_q))$ such points, where $\mathcal{W}(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-rational affine Weierstrass points. This follows from an easy counting argument.

Case $\beta \in \mathbb{F}_q^*$:
In this case $f(\alpha)^{\frac{q-1}{2}} = 1$ and $\alpha \in \mathbb{F}_q$, hence the numerator of (3.14) is given by $4f(\alpha) \neq 0$. So there is no cancellation here.

Case $\beta = 0$:
Here the factor $(f(x)^{\frac{q-1}{2}} + 1)^2$ in the numerator is not divisible by $(x - \alpha)$, but the factor $f(x)$ is exactly once (note that f is separable). So this results in $\#\mathcal{W}(\mathbb{F}_q)$ cancellations.

Combining the above cases one obtains for the degree of γ^2, viewed as a rational function (i.e., as a map $\mathbb{P}^1 \to \mathbb{P}^1$) that

$$\begin{aligned}\deg \gamma^2 &= \deg \left(\frac{y^q + y}{x^q - x}\right)^2 \\ &= (2g+1)q - \big(2q + 1 - (\#\mathcal{H}(\mathbb{F}_q) + \#\mathcal{W}(\mathbb{F}_q)) + \#\mathcal{W}(\mathbb{F}_q)\big) \\ &= (2g-1)q + \#\mathcal{H}(\mathbb{F}_q) - 1.\end{aligned}$$

□

Proposition 3.3.2. *Let $\mathcal{H}$ be as in Proposition 3.3.1, and consider the Mumford representation $\langle t^2 + \alpha(x)t + \beta(x), \gamma(x,y)t + \delta(x,y)\rangle$ of $\mathcal{L}_1$.*
Then $\deg \gamma^2 = (2g+1)q - \#\mathcal{H}(\mathbb{F}_q) + 1$

Proof. The proof is analogous to the proof of Proposition 3.3.1 but in this case using $\gamma = \frac{y^2 - y}{x^q - x}$. □

Example: The curve $\mathcal{H}$ over $\mathbb{F}_5$ given by $y^2 = x^9 - x^3 + x + 1$ has genus 4 and $\#\mathcal{H}(\mathbb{F}_5) = 7$. We illustrate Propositions 3.3.1 and 3.3.2 by explicitly computing the rational functions γ^2. The propositions state that these have degrees $(2 \cdot 4 - 1) \cdot 5 + 7 - 1 = 41$ and $(2 \cdot 4 + 1) \cdot 5 - 7 + 1 = 39$, respectively.

```
> q := 5; F := FiniteField(q);
> P<x> := PolynomialRing(F);
> H := HyperellipticCurve(x^9 + x^3 + x + 1); #H;
7
> g := Genus(H);g;
4
> FH<X,Y> := FunctionField(H);
> HE := BaseExtend(H,FH);
> JE := Jacobian(HE);
> M<t> := PolynomialRing(FH);
> Lminus1 := JE![t-X,Y] - JE![t-X^q,Y^q];
> Lplus1  := JE![t-X,Y] + JE![t-X^q,Y^q];
> gamma_m1 := Coefficient(Lminus1[2],1);
> gamma_p1 := Coefficient(Lplus1[2] ,1);
> FH!gamma_m1^2;
(X^41 + 2*X^40 + 2*X^39 + X^38 + X^37 + 4*X^36 + 4*X^35 + 2*X^34 + X^33 +
X^32 + X^31 + 3*X^30 + X^29 + 3*X^28 + 3*X^27 + 4*X^26 + X^25 + 2*X^23 +
4*X^22 + 4*X^20 + 4*X^19 + 4*X^18 + 4*X^15 + 3*X^14 + 3*X^13 + 4*X^12 + X^11
+ 2*X^9 + X^8 + 2*X^6 + X^5 + 4*X^4 + 4*X^3 + 4*X^2 + 2*X + 1)/(X^6 + 2*X^5
+ 2*X^4 + X^3 + 4*X^2)
> FH!gamma_p1^2;
(X^39 + 3*X^38 + 2*X^37 + 4*X^36 + X^35 + X^34 + 4*X^33 + 3*X^32 + X^31 +
4*X^30 + X^29 + 2*X^28 + X^27 + 2*X^26 + 3*X^25 + X^24 + X^23 + 3*X^21 +
4*X^20 + 2*X^19 + 2*X^16 + 2*X^15 + 2*X^14 + 4*X^13 + 2*X^12 + 3*X^11 +
3*X^10 + 3*X^8 + 2*X^7 + X^6 + 2*X^4 + 2*X^2 + 3*X + 1)/(X^4 + 3*X^3 + 2*X^2
+ 4*X + 4)
> (2*g-1)*q+(#H-1);
41
> (2*g+1)*q-(#H-1);
39
```

Proposition 3.3.1 applies to all hyperelliptic curves of genus g with one point at infinity. Now we have the full setting to prove the Hasse-Weil inequality for genus 2.

But before doing so, we introduce a geometrical interpretation of the current situation. Consider the already known functions in $\mathbb{F}_q(\mathcal{J})$ given by:

$$\kappa_1 := 1, \kappa_2 := A, \kappa_3 := B, \kappa_4 := C^2 - \rho(A,B) = C^2 - A^3 + AB - a_4 A^2 - a_3 A - a_2$$

which as shown in Proposition 2.4.3 forms a basis of $\mathcal{L}(2\Theta)$. Consider the map:

$$\begin{aligned} \kappa : \mathcal{J} &\dashrightarrow \mathbb{P}^3 \\ \langle t^2 - At + B, tC + D\rangle &\mapsto [\kappa_1 : \kappa_2 : \kappa_3 : \kappa_4] \end{aligned}$$

We define the surface $\mathcal{K}_s := \mathrm{Im}(\kappa) \subset \mathbb{P}^3$.

As we sae in the previous chapter, $k(\mathcal{K}_s) \cong k(A, B, C^2) = k(A, B, \kappa_4)$. Further, the variety $\mathcal{K}_s$ is birational to the Kummer surface associated to $\mathcal{H}$. This is because the points of $\mathcal{K}_s$ are obtained by identifying any point $P \in \mathcal{J}$ with its "negative" $-P$. This is seen by observing that every κ_i is symmetric and even, and moreover the subfield of $k(\mathcal{J}) = k(A, B, C)$ consisting of all even functions is generated by A, B, and C^2. In particular $\kappa_i(D) = \kappa_i(-D)$ for every $D \in \mathcal{J}$, $i = 1, \dots, 4$.

Recall that $\Phi_n := \phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$. We have the following situation.

$$\begin{tikzcd}
 & \mathcal{J} \arrow[dr, "\Phi_n"] & \\
\mathcal{H} \arrow[ur, "\iota"] \arrow[rr, "\psi_n"] \arrow[ddrr, "\Psi_n"'] & & \mathcal{J} \arrow[d, dotted, "2:1"', "\kappa"] \arrow[dd, dotted, bend left, "\kappa_4"] \\
 & & \mathcal{K}_s \arrow[d, dotted, "\pi"] \\
 & & \mathbb{P}^1
\end{tikzcd} \tag{3.15}$$

Here κ_4 is seen as a rational map to $\mathbb{P}^1$. We introduce the map $\Psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathbb{P}^1)$ given by $(x, y) \mapsto \kappa_4(\psi_n(x, y))$.

The above diagram suggests that the next step is to study κ_4 in the same way that we studied $C^2 \circ \psi_{\pm 1}$ in Proposition 3.3.1, that is $\kappa_4 \circ \psi_{\pm 1}$. Finally, with this we study the degree of $\kappa_4 \circ \psi_n$ through the map Ψ_n to get the fundamental lemmas and prove our final result.

Proposition 3.3.3. *Let $\mathcal{H}$ be a hyperelliptic curve of genus 2 given by $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = f(X)$. Let $(x, y) \in \mathcal{H}(\mathbb{F}_q(\mathcal{H}))$ be* *the generic point of $\mathcal{H}$. Then $\kappa_4(\mathcal{L}_{-1}) \in \mathbb{F}_q(x)$ and considered as a rational function in the variable x, $\deg \kappa_4(\mathcal{L}_{-1}) = \deg \kappa_4(\psi_{-1}(x,y)) = \#\mathcal{H}(\mathbb{F}_q) + q + 1$.*

Proof. Recall that in Proposition 3.3.1 we calculated the point $\mathcal{L}_{-1}$ which is:

$$\mathcal{L}_{-1} = \psi_{-1}(x,y) = [(x^q, yf(x)^{\frac{q-1}{2}}) + (x,-y) - 2\infty] \in \mathcal{J}(\mathbb{F}_q(\mathcal{H})).$$

The present proof is analogous to the one for Proposition 3.3.1. Consider $\kappa_4(\mathcal{L}_{-1}) = \kappa_4(\psi_{-1}(x,y))$

$$\frac{x^{3q+2}+x^{2q+3}+2a_4x^{2q+2}+a_3(x^{2q+1}+x^{q+2})+2a_2x^{q+1}+a_1(x^q+x)+2a_0+2f(x)^{\frac{q+1}{2}}}{(x^q-x)^2}. \quad (3.16)$$

In particular $\kappa_4(\mathcal{L}_{-1}) \in \mathbb{F}_q(x) \subset \mathbb{F}_q(\mathcal{H})$. Let ν and η be the numerator and denominator of 3.16 respectively before cancellations. We have that before cancellations, $\deg(\eta) = 2q$, in fact every $\alpha \in \mathbb{F}_q$ is a double root of η. Further, the highest exponent in the numerator is $3q+2$ since $f(x)^{\frac{q+1}{2}}$ has degree $\frac{5(q+1)}{2}$, therefore $\deg(\nu) = 3q+2$ before cancellations.
With this we have that after cancellations $\deg(\kappa_4(\mathcal{L}_{-1})) = 3q+2-\deg(\gcd(\nu,\eta))$. Since $\kappa_4(\mathcal{L}_{-1}) = \kappa_4(\psi_{-1}(x,y))$ is a function on the curve $\mathcal{H}$, that is $\kappa_4(\mathcal{L}_{-1}) \in \mathbb{F}_q(\mathcal{H}) \subset \mathbb{F}_q(\mathcal{J})$, the common factors $(x-\alpha)$ of ν and η occur at the points $(\alpha,\beta) \in \mathcal{H}$ such that $\alpha \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$ or $\beta \in \mathbb{F}_q^* \setminus \mathbb{F}_{q^2}^*$ or $\beta = 0$. Hence, we have three possible cases for cancellations:

Case $\beta \in \mathbb{F}_q^*$:
In this case $(\alpha,\beta) \in \mathcal{H}(\mathbb{F}_q)$ and therefore $f(\alpha)$ is a square in $\mathbb{F}_q^*$. Hence $f(\alpha)^{\frac{q-1}{2}} = 1$. Moreover, $\alpha^q = \alpha$ and $\beta^q = \beta$. Using this, the last term of $\nu(\alpha)$ is $2f(\alpha)^{\frac{q+1}{2}} = 2f(\alpha)f(\alpha)^{\frac{q-1}{2}}$. Therefore $2f(\alpha)^{\frac{q+1}{2}} = 2f(\alpha)$ and

$$\nu(\alpha) = 4f(\alpha).$$

Since $\beta \neq 0$ there are no cancellations for this case.

Case $\beta = 0$:
We have that $f(\alpha) = 0$ and $\alpha^q = \alpha$, so the numerator of (3.16) is $2f(\alpha) = 0$. Therefore $\nu(x)$ and $\eta(x)$ share the linear factor $x - \alpha$ with multiplicity one or two. The multiplicity in fact equals one since $\frac{d}{dx}\nu(x) \mid_\alpha = 4f'(\alpha) \neq 0$ as $f(x)$ does not have repeated roots.

Case $\beta \notin \mathbb{F}_q$:

In this case $f(\alpha)$ is nonzero and is not a square in $\mathbb{F}_q^*$. Therefore $f(\alpha)^{\frac{q-1}{2}} = -1$ by Euler's criterion. Moreover $\alpha^q = \alpha$ and $\nu(\alpha)$ is in this case

$$2(\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) - 2f(\alpha) = 0.$$

To find the multiplicity of α as a zero of $\nu(x)$, we calculate the derivative of $\nu(x)$ at α:

$$\begin{aligned}\frac{d}{dx}\nu(x)\mid_\alpha &= 2\alpha^{3q+1}+3\alpha^{2q+2}+4a_4\alpha^{2q+1}+a_3(\alpha^{2q}+2\alpha^{q+1})+2a_2\alpha^q+a_1-f'(\alpha)\\ &= 5\alpha^4 + 4a_4\alpha^3 + 3a_3\alpha^2 + 2a_2\alpha + a_1 - f'(\alpha)\\ &= f'(\alpha) - f'(\alpha).\\ &= 0\end{aligned}$$

This tells us that the factor $(x-\alpha)^2$ appears in ν and then it cancels with the denominator.

Combining the cases, one concludes $\deg(\gcd(\nu(x), \eta(x))) = 2q + 1 - \#\mathcal{H}(\mathbb{F}_q)$ and therefore $\deg(\kappa_4(\mathcal{L}_{-1})) = \deg(\kappa_4(\psi_{-1}(x, y))) = q + 1 + \#\mathcal{H}(\mathbb{F}_q)$. □

Proposition 3.3.4. *Assume the hypotheses of the Proposition 3.3.3, then:*

$$\deg(\kappa_4(\mathcal{L}_1)) = \deg(\kappa_4(\psi_1(x, y))) = 3(q + 1) - \#\mathcal{H}(\mathbb{F}_q).$$

Proof. An explicit calculation of $\mathcal{L}_1 \in \mathcal{J}(\mathbb{F}_q(\mathcal{H}))$ shows that:

$$\kappa_4(\mathcal{L}_1) = \frac{x^{3q+2}+x^{2q+3}+2a_4x^{2q+2}+a_3(x^{2q+1}+x^{q+2})+2a_2x^{q+1}+a_1(x^q+x)+2a_0-2f(x)^{\frac{q+1}{2}}}{(x^q-x)^2}$$

Note that $\kappa_4(\mathcal{L}_1)$ differs from (3.16) just at the sign of the last term of the numerator, namely $2f(x)^{\frac{q+1}{2}}$. An analogous argument as the one given above proves the proposition. □

If we compare the last Proposition 3.3.3, with Proposition 3.3.1 with $g = 2$, we have that $\deg(C^2(\psi_{-1}(x, y))) - \deg(\kappa_4(\psi_{-1}(x, y)) = 2q - 2$. This difference on the degree is the main reason of why is less complicated to work with κ_4 even when computing and experimenting.

We proceed to show an important (and almost trivial at this point) property of $\kappa_4(\mathcal{L}_n)$ for $n \neq 0$. This property will be used to measure the degree of the associated map $\Psi_n(x, y) = \kappa_4(\psi_n(x, y))$ in terms of a polynomial degree in one variable.

Proposition 3.3.5. *Assume the hypotheses of the Proposition 3.3.3. Let $n \neq 0$ and let $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ be non-constant. If $(x, y) \in \mathcal{H}$ is the generic point, then $\kappa_4(\mathcal{L}_n) \in \mathbb{F}_q(x) \subset \mathbb{F}_q(\mathcal{H})$.*

Proof. In Proposition 2.4.3 we built $\kappa_4 \in \mathcal{L}(2\Theta)$ explicitly as the function in $\mathbb{F}_q(\mathcal{J})$ given by:

$$\kappa_4 := \frac{2a_0+a_1(x_1+x_2)+2a_2x_1x_2+a_3x_1x_2(x_1+x_2)+2a_4(x_1x_2)^2+(x_1x_2)^2(x_1+x_2)-2y_1y_2}{(x_1-x_2)^2}.$$

Let $[-1] \in \mathrm{Aut}(\mathcal{J})$ be the inversion map on the group variety $\mathcal{J}$. It is induced by the hyperelliptic involution $\mathfrak{t} \in \mathrm{Aut}(\mathcal{H})$. We see that κ_4 is invariant under the field automorphism $[-1]^* : \mathbb{F}_q(\mathcal{J}) \to \mathbb{F}_q(\mathcal{J})$, that is, $[-1]^*(\kappa_4) = \kappa_4$. Particularly by Lemma 3.2.5 $\kappa(\mathcal{L}_n) = \kappa(-\mathcal{L}_n)$, which means

$$\kappa_4(\psi_n(x, y)) = \kappa_4(\psi_n(x, -y)) \in \mathbb{F}_q(\mathcal{H}) \cong \mathbb{F}_q(x, y).$$

Writing $\kappa_4(\psi_n(x, y)) = \frac{\nu(x)+\beta(x)y}{\eta(x)}$ for certain rational functions $\nu(x), \beta(x), \eta(x)$, it follows that $\beta(x) = 0$ and $\kappa_4(\mathcal{L}_n) \in \mathbb{F}_q(x) \subset \mathbb{F}_q(x, y)$. □

We have shown that when $\Theta_n \not\subset \Theta$ (recall that Θ_n is the image of $\mathcal{H}$ in $\mathcal{J}$ under the composition $(\phi + [n]) \circ \iota$), we have that $\kappa_4(\mathcal{L}_n) := \frac{\nu(x)}{\eta(x)} \in \mathbb{F}_q(x)$. Further, we show in the next lemma that in this case $\deg \kappa_4(\mathcal{L}_n) = \max\{\deg \nu(x), \deg \eta(x)\} = \deg \nu(x)$. With this, the degree of $\Psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathbb{P}^1)$ is determined by the degree of the numerator of $\kappa_4(\mathcal{L}_n)$ as a polynomial in x: namely, $\Psi_n(x, y) = \kappa_4(\psi_n(x, y)) = \frac{\nu(x)}{\eta(x)} \in \mathbb{F}_q(x)$. Calculating this degree for all n is the analog for genus two of what Manin did for genus one. In both cases it leads to a proof of the Hasse-Weil inequality.

Lemma 3.3.6. *Assume the hypotheses of the previous Proposition 3.3.5. Let $\kappa_4(\mathcal{L}_n) = \kappa_4(\psi_n(x, y)) = \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)} \in \mathbb{F}_q(x)$ with $\gcd(\mu_{1,n}, \mu_{2,n}) = 1$. Then $\deg \kappa_4(\psi_n(x, y)) = max\,\{\deg \mu_{1,n}, \deg \mu_{2,n}\,\} = \deg \mu_{1,n}$.*

Proof. To simplify notation denote $u := \mu_{1,n}$ and $t := \mu_{2,n}$. Recall that $\kappa_4(\mathcal{L}_n) \in \mathbb{F}_q(x, y) \cong \mathbb{F}_q(\mathcal{H})$ is a function on the curve $\mathcal{H}$ where $y^2 = f(x)$ is the defining equation of $\mathcal{H}$. To show that the degree of the numerator of $\kappa_4(\mathcal{L}_n) = \kappa_4(\psi_n(x, y))$ is higher than the degree of its denominator, we just need to calculate the order of $\kappa_4(\mathcal{L}_n) = \kappa_4(\psi_n(x, y)) \in \mathbb{F}_q(\mathcal{H})$ at $\infty \in \mathcal{H}$ and check its sign.

Let $\mathcal{O}_\infty \subset \mathbb{F}_q(\mathcal{H})$ be the ring of regular functions at $\infty \in \mathcal{H}$. Consider a uniformizer $\pi \in \mathbb{F}_q(\mathcal{H})$ at $\infty \in \mathcal{H}$, that is, $\pi\mathcal{O}_\infty = m_\infty$ where m_∞ is the maximal ideal of $\mathcal{O}_\infty$. Therefore $x = \mathfrak{u}\pi^{-2} \in \mathbb{F}_q(\mathcal{H})$ for a unit $\mathfrak{u} \in \mathbb{F}_q[\mathcal{H}]$, hence

$$\mathrm{ord}_\infty^{\mathcal{H}}(\tfrac{\nu(x)}{\eta(x)}) = \deg u \cdot \mathrm{ord}_\infty^{\mathcal{H}}(x) - \deg t \cdot \mathrm{ord}_\infty^{\mathcal{H}}(x) = -2\deg u + 2\deg t.$$

Further, we have that $\infty \in \Theta$ and $\kappa_4 \in \mathcal{L}(2\Theta) \subset \mathbb{F}_q(\mathcal{J})$ (i.e. Θ is a double pole of κ_4 in $\mathcal{J}$), therefore, $\kappa_4(\mathcal{L}_n) \in \mathbb{F}_q(\mathcal{H}) \subset \mathbb{F}_q(\mathcal{J})$ is not regular at $\infty \in \mathcal{H}$, that is $\kappa_4(\mathcal{L}_n) \notin \mathcal{O}_\infty$ if and only if $0 > \mathrm{ord}_\infty^{\mathcal{H}}(\frac{u(x)}{t(x)}) = -2\deg u + 2\deg t$ if and only if $\deg u > \deg t$. □

With this we have that if $n \neq 0$ and ψ_n is non-constant and $(x, y) \in \mathcal{H}$ is the generic point, then $\deg \Psi_n = \deg(\kappa_4 \circ \psi_n) = 2\deg u(x) = 2\deg \mu_{1,n}$. The "2" is because x as a function $\mathcal{H} \to \mathbb{P}^1$ has degree 2; the last 'deg' denotes degree as a polynomial in x.

3.4 Computing $\deg \Psi_n$ explicitly

Suppose that $\psi_n(\mathcal{H}) \not\subset \Theta$. The purpose of this section is to finally compute the degree of the rational function $\kappa_4(\mathcal{L}_n) = \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)}$ for every $n \in \mathbb{Z}$, that is, we obtain $\deg \mu_{1,n}(x)$ (as a polynomial) by the previous Lemma 3.3.6. This will tell us $\deg \Psi_n$. This calculation will be done in terms of a second order recurrence formula for $\delta_n := \frac{\deg \Psi_n}{2} = \deg \nu(x)$ similar to the one Manin found for the genus 1 case. In order to find an expression for this degree we will require some machinery from the theory of Abelian varieties.

First, we define the intersection multiplicity (number) between the curves Θ_n and Θ in $\mathcal{J}$ and prove its relation with δ_n. We also define and deduce the self intersection number of Θ in $\mathcal{J}$. Moreover we deduce the intersection of $\mathrm{Im}\psi_0 = \Theta_0$ with Θ (we cannot use κ_4 as before since $\Theta_0 \subset \Theta$) using a linear equivalent divisor Θ_0' in order to use explicitly κ_4 and obtain δ_0.

Finally, an important theorem that we use to obtain $\deg \Psi_n$ comes from a general result in algebraic geometry, the *Theorem of the Cube* (see Chapter III §10 [Mum74]). This theorem is very general and usually is stated for schemes using invertible sheaves. However, we relax the theory since we are working with $\mathcal{J}$, which is an Abelian variety and therefore smooth. So, we switch the language of invertible sheaves $\mathscr{L} \in \mathrm{Pic}(\mathcal{J})$ to Weil divisors $\mathcal{L} \in \mathrm{Div}(\mathcal{J})/\sim$ since both groups are isomorphic in this case (see Chapter II, Proposition 6.15 and Corollary 6.16 [Har77]).

As a remark, the theory of Abelian varieties for $\mathcal{J}/k$ using divisors $\mathrm{Div}(\mathcal{J})(k)$ works for any k with a separable closure k^{sep}. This was justified in the Section 3.2.1 obtaining $\mathcal{J}(k)$ via the invariants of $\mathcal{J}$ under $G_k = \mathrm{Gal}(\overline{k}/k)$.

3.4.1 Intersection theory on $\mathcal{J}$ and δ_n

Definition 3.4.1. *Let $D_1, D_2 \in Div(\mathcal{J})$. By $D_1 \bullet D_2$ we denote the intersection number of the divisors D_1 and D_2 on the surface $\mathcal{J}$.*

As a matter of formality we briefly explain in the next paragraph what "*intersection number*" means, for more details see [Har77, Appendix C or Chapter V]. In what follows we will be mostly interested in $\Theta_n \bullet \Theta$. We will show in Lemma 3.4.2 that this number is related to the degree of the rational function $\kappa_4(\psi_n(x, y)) \in \mathbb{F}_q(x)$.

When $D_1, D_2 \in \mathrm{Div}(\mathcal{J})$ are irreducible curves intersecting transversally, $D_1 \bullet D_2 = |D_1 \cap D_2|$. The general situation is different, let D_1 and D_2 be two curves in $\mathcal{J}$ with no common irreducible components. Take $P \in D_1 \cap D_2$ and consider local equations describing the curves D_1 and D_2 in $\mathcal{J}$ at P, namely γ_1 and γ_2. Consider the local ring $\mathcal{O}_{\mathcal{J},P}$ of $\mathcal{J}$ at P, that is $k[U]_{\mathfrak{m}_P}$ where U is an affine neighborhood of P and $\mathfrak{m}_P \subset k[U]$ is the maximal ideal corresponding to P. Then $\mathcal{O}_{\mathcal{J},P}/(\gamma_1, \gamma_2)$ is the ring that best describes the intersection of D_1 and D_2 at P in $\mathcal{J}$. Namely, $D_1 \bullet D_2 := \sum_{P \in D_1 \cap D_2} \dim_k\big(\mathcal{O}_{\mathcal{J},P}/(\gamma_1, \gamma_2)\big)$ (see [Har77, Chapter V, Proposition 1.4]). This number is finite since these quotient rings are local Artinian over k and hence finite dimensional over k.

The next lemma shows the expected relation between $\Theta_n \bullet \Theta$ and δ_n. This will allow us to show that $\delta_0 = 2q$ and $\Theta \bullet \Theta = 2$ using κ_4.

Lemma 3.4.2. *Suppose that* $\mathrm{Im}\psi_n = \Theta_n \not\subset \Theta$. *Let* $\Phi_n := \phi + [n] \in \mathrm{End}(\mathcal{J})$, *then*

$$2\Theta_n \bullet \Theta = \deg \Psi_n = 2\Phi_n^* \Theta \bullet \Theta.$$

Proof. Let $(x, y) \in \mathcal{H}$ be generic. Since $\mathrm{Im}\psi_n = \Theta_n \not\subset \Theta$ we have that $\Psi_n(x, y) = \kappa_4(\psi_n(x, y)) \in \mathbb{F}_q(x)$ by Lemma 3.3.6. Further, $\kappa_4 \in \mathbb{F}_q(\mathcal{J})$ has divisor $D - 2\Theta$ for some effective divisor $D \in \mathrm{Div}(\mathcal{J})$. Therefore $\deg \Psi_n = \deg\big((\kappa_{4|\Theta_n})^* \infty\big) = 2\Theta_n \bullet \Theta$ which shows the first equality.

For the second equality, note that $\Phi_n^{-1}(\Theta) = \{D \in \mathcal{J} : \Phi_n(D) \in \Theta\}$ and Θ is the locus where κ_4 has a pole (in fact a double pole). Since $\deg(\Psi_n) =$

$\deg(\kappa_4 \circ \Phi_{n|\Theta})$ we conclude $\deg \Psi_n = 2\Phi_n^{-1}(\Theta) \bullet \Theta$. Applying [Ful84, Lemma 1.7.1], this equals $2\Phi_n^* \Theta \bullet \Theta$. □

Note that since $\delta_n = \frac{\deg \Psi_n}{2} = \deg \kappa_4(\psi_n(x,y))$ by Lemma 3.3.6, the previous lemma implies that $\delta_{-1} = q + 1 + \#\mathcal{H}(\mathbb{F}_q)$ and $\delta_1 = 3(q+1) - \#\mathcal{H}(\mathbb{F}_q)$ using Propositions 3.3.3 and 3.3.4 respectively.

We will show soon how to deal with the cases where $\Theta_n \subset \Theta$ using a linear equivalent divisor $\Theta_n' \in \mathrm{Div}(\mathcal{J})$.

We now prove in the next lemma that $\Theta \bullet \Theta = 2$. This number is the intersection number of Θ with Θ' where $\Theta \sim \Theta'$. A divisor Θ' can be regarded as a translation of Θ in $\mathcal{J}$. This number will be useful to compute $\Theta_n \bullet \Theta$. The following lemmas use the known fact that the intersection number of two divisors is invariant under translation since they are linearly equivalent (see [Har77, Chapter V. Theorem 1.1] and [BL13, Corollary 2.5.4]).

To see the intuition of why we want the intersection number $\Theta_n \bullet \Theta$, for $n \in \mathbb{Z}$, think about $n = -1$. The integer $\Theta_{-1} \bullet \Theta$ is directly related with $\#\mathcal{H}(\mathbb{F}_q)$ since it counts (with multiplicities) the number of solutions $D \in \Theta \subset \mathcal{J}$ such that $\psi_{-1}(D) = 0$ if and only if $\phi(D) = D$ where $\phi \in \mathrm{End}(\mathcal{J})$ is the q-th Frobenius. Note that the divisors (on $\mathcal{H}$, so points in $\mathcal{J}$) considered here are the ones in $\Theta \cong \mathcal{H}$ and $\Theta \subset \mathcal{J}$. Therefore we are counting points in $\mathcal{H} \cong \Theta$.

Lemma 3.4.3. *Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ and consider its Jacobian $\mathcal{J}$. Let $\mathrm{Im}\,\iota = \Theta \subset \mathcal{J}$, then $\Theta \bullet \Theta = 2$.*

Proof. Let $(w, 0) \in \mathcal{H}(\overline{\mathbb{F}_q})$ be a Weierstrass point and consider $\iota_w \in \mathrm{Mor}(\mathcal{H}, \mathcal{J})$ given by $P \mapsto [P + (w,0) - 2\infty]$. Let $(x,y) \in \mathcal{H}$ be the generic point. We have that $\Theta' := \mathrm{Im}\ \iota_w \subset \mathcal{J}$ is a translation of Θ, and therefore $\Theta' \sim \Theta$ in $\mathrm{Div}(\mathcal{J})$. Hence $\Theta \bullet \Theta = \Theta' \bullet \Theta = \deg \kappa_4(\iota_w(x,y))$. We have that $\kappa_4(\iota_w(x,y))$ is well defined since $\Theta' \not\subset \Theta$ and κ_4 only has a double pole at Θ. By an analog argument used in the previous Lemma 3.4.2, we have that $\Theta \bullet \Theta = \deg \kappa_4(\iota_w(x,y))$. Note that $\iota_w(x,y) = [(x,y) + (w,0) - 2\infty]$, therefore:

$$\begin{aligned}\kappa_4(\iota_w(x,y)) &= \tfrac{2a_0+a_1(x+w)+2a_2xw+a_3(x+w)xw+2a_4(xw)^2+(x+w)(xw)^2}{(x-w)^2} \\ &= \tfrac{a_1+a_3xw+(xw)^2}{(x-w)} + \tfrac{2a_2xw+(xw)^2+2a_0}{(x-w)^2}\end{aligned} \tag{3.17}$$

We see explicitly that $\deg \kappa_4(\iota_w(x,y)) = 2$. Note that when $w = 0$, the degree is taken as the degree of the denominator which has highest degree. □

Note that the previous lemma can be showed also using the *adjunction formula* ([Har77, Chapter V §1, 1.5]) but here we show how to obtain these intersection numbers using κ_4.

Using an analogous argument we calculate $\Theta_0 \bullet \Theta$ as we see in the next lemma, justifying the definition of δ_0 in (3.5).

Lemma 3.4.4. *Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = f(x)$ and consider its Jacobian $\mathcal{J}$. Let* $\operatorname{Im} \psi_0 = \Theta_0 \subset \Theta \subset \mathcal{J}$*, then $\delta_0 = \Theta_0 \bullet \Theta = 2q$.*

Proof. Let $(x,y) \in \mathcal{H}$ be generic. By a similar argument in the previous Lemma 3.4.3 we translate Θ_0 by $(w,0) \in \mathcal{H}(\overline{\mathbb{F}_q})$ using the map $\psi_{0,w}(x,y) := [(x^q, yf(x)^{\frac{q-1}{2}}) + [(w,0) - 2\infty]$. Let $\Theta_0' := \operatorname{Im} \psi_{0,w}$, we calculate $\Theta_0 \bullet \Theta = \Theta_0' \bullet \Theta$ as the degree of:

$$\begin{aligned}\kappa_4(\psi_{0,w}(x,y)) &= \frac{2a_0+a_1(x^q+w)+2a_2x^qw+a_3(x^q+w)x^qw+2a_4(x^qw)^2+(x^q+w)(x^qw)^2}{(x^q-w)^2}\\ &= \frac{a_1+a_3x^qw+(x^qw)^2}{(x^q-w)} + \frac{2a_2x^qw+(x^qw)^2+2a_0}{(x^q-w)^2}.\end{aligned} \tag{3.18}$$

This rational function has clearly degree $2q$, therefore $\Theta_0 \bullet \Theta = 2q$. □

In summary, with the previous Propositions 3.3.4 and 3.3.3, we know that $\delta_{-1} = \Theta_{-1} \bullet \Theta = q + 1 + \#\mathcal{H}(\mathbb{F}_q)$ and $\delta_1 = \Theta_1 \bullet \Theta = 3(q+1) - \#\mathcal{H}(\mathbb{F}_q)$. Further, using 3.4.2 we justified $\delta_0 = \Theta_0 \bullet \Theta = 2q$ and also that $\Theta \bullet \Theta = 2$.

Finally we state an important result from the theory of Abelian varieties. Let $(\mathcal{A}, \oplus)$ be an Abelian variety.
For every non-empty $I \subseteq \{1,2,3\}$ define the map $\pi_I : \mathcal{A} \times \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ by $\pi_I(x_1,x_2,x_2) = \bigoplus_{i \in I} x_i$. For example, for $\{2,3\}$ we have $\pi_{23}(x_1,x_2,x_2) = x_2 \oplus x_3 \in \mathcal{A}$.
Consider the pullbacks $\pi_I^* : \operatorname{Div}(\mathcal{A}) \to \operatorname{Div}(\mathcal{A} \times \mathcal{A} \times \mathcal{A})$. We state the following fundamental result.

Theorem 3.4.5 (Theorem of the Cube on Abelian varieties)**.** *Let $\mathcal{A}$ be an Abelian variety and $\mathcal{L} \in Div(\mathcal{A})$. Consider the divisor $\mathfrak{D} \in Div(\mathcal{A} \times \mathcal{A} \times \mathcal{A})$*

given by:

$$\begin{aligned}\mathfrak{D} :&= \pi_{123}^*\mathcal{L} - \pi_{12}^*\mathcal{L} - \pi_{13}^*\mathcal{L} - \pi_{23}^*\mathcal{L} + \pi_1^*\mathcal{L} + \pi_2^*\mathcal{L} + \pi_3^*\mathcal{L} \\ &= - \sum_{I \subseteq \{1,2,3\}} (-1)^{\#I} \pi_I^*(\mathcal{L})\end{aligned}$$

then $\mathfrak{D} \sim 0$.

Proof. An elegant and compact proof over $\mathbb{C}$ using that $\mathfrak{D}$ is the divisor of an explicit θ function when $\mathcal{L}$ is effective, is found in [HS13] (Theorem A.7.2.1). The algebraic proof there follows from the Lefschetz principle. Other proofs can be found in [Mil08] using the *Seesaw principle.* □

The next corollary is a handy tool for the main result of this chapter.

Corollary 3.4.6. *Let* $\mathcal{A}$ *be an Abelian variety,* $\alpha, \beta, \gamma \in \mathrm{End}_k(\mathcal{A})$ *and* $\mathcal{L} \in$ *Div*$(\mathcal{A})$*, then :*

$$\mathfrak{E} := (\alpha+\beta+\gamma)^*\mathcal{L} - (\alpha+\beta)^*\mathcal{L} - (\alpha+\gamma)^*\mathcal{L} - (\beta+\gamma)^*\mathcal{L} + \alpha^*\mathcal{L} + \beta^*\mathcal{L} + \gamma^*\mathcal{L} \sim 0$$

in Div$(\mathcal{A})$

Proof. Put

$$\begin{aligned}\varrho : \mathcal{A} &\to \mathcal{A} \times \mathcal{A} \times \mathcal{A} \\ X &\mapsto (\alpha(X), \beta(X), \gamma(X))\end{aligned} \tag{3.19}$$

Let $\mathfrak{D}$ be as in Theorem 3.4.5. It is easy to see that $\varrho^*(\mathfrak{D}) = \mathfrak{E}$, that is, the inverse image of $\mathfrak{D}$ under ϱ is $\mathfrak{E}$. Therefore $\mathfrak{E} \sim 0$ by Theorem 3.4.5 □

3.4.2 Proof of the Hasse-Weil inequality for genus 2

In this section we show that the degree of Ψ_n is given by an explicit quadratic polynomial in the variable n. The proof uses the Theorem of the cube described in the previous section. Finally we use this polynomial to infer the Hasse-Weil inequality for genus 2.

We recall the full setting for the definition of δ_n now using Lemma 3.3.6.

Definition 3.4.7. *Let* $\mathcal{H}/\mathbb{F}_q$ *be a hyperelliptic curve of genus* 2 *with one point at infinity and* $\mathcal{J}$ *its Jacobian. Let* $\phi, [n] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$ *be the Frobenius and the multiplication by n endomorphisms. Consider the inclusion* $\iota : \mathcal{H} \to \mathcal{J}$*. Put*

$\psi_n := (\phi + [n]) \circ \iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$. *Using the diagram (3.15) we have that* Ψ_n *is the map given by* $(x, y) \mapsto \kappa_4(\psi_n(x, y)) = \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)}$. *We define:*

$$\delta_n := \begin{cases} \deg \kappa_4(\psi_n(x, y)) = \deg \mu_{1,n} = \frac{\deg \Psi_n}{2} & \textit{if } \psi_n(\mathcal{H}) \not\subset \Theta; \\ 2q & \textit{if } n = 0; \\ 0 & \textit{otherwise.} \end{cases}$$

Theorem 3.4.8. *Suppose that* $\mathrm{Im}\psi_j = \Theta_j \not\subset \Theta$ *for* $j \in \{n-1, n, n+1\}$, *then:*

$$\delta_{n-1} + \delta_{n+1} = 2\delta_n + 4. \tag{3.20}$$

Moreover, for any n *we have* $\Theta_n \bullet \Theta = 2n^2 + n(q + 1 - \#\mathcal{H}(\mathbb{F}_q)) + 2q$ *and this equals* δ_n *provided* $n = 0$ *or* $\Theta_n \not\subset \Theta$.

Proof. Using Corollary 3.4.6, let $\mathcal{L} := \Theta \in \mathrm{Div}(\mathcal{J})$ and take $\alpha := \phi + [n], \beta = [1], \gamma := -[1] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$. Let $\Phi_m := \phi + [m]$, then in this case the Corollary of the theorem of the cube (3.4.6) says:

$$2\Phi_n^*\Theta - \Phi_{n+1}^*\Theta - \Phi_{n-1}^*\Theta + 2\Theta \sim 0,$$

or equivalently:

$$2\Phi_n^*\Theta + 2\Theta \sim \Phi_{n-1}^*\Theta + \Phi_{n+1}^*\Theta. \tag{3.21}$$

Intersecting both sides of the equivalence with Θ proves the first part of the theorem. To be more precise, we use Lemma 3.4.2 together with Lemma 3.4.3 to deduce $2\delta_n + 4 = \delta_{n-1} + \delta_{n+1}$.

Now, for the explicit value of δ_n in case it equals $\Theta_n \bullet \Theta$, we proceed to prove by induction that:

$$\Theta_n \sim n(n-1)\Theta + n\Theta_1 + (1-n)\Theta_0. \tag{3.22}$$

Note that intersecting both divisors in the previous equivalence with Θ, using the known values of δ_0, δ_{-1} and δ_1 we see that it yields the desired polynomial formula in n for $\Theta_n \bullet \Theta$.

Recall that $\Theta_0 := \mathrm{Im}\psi_0 = \Phi_0(\Theta) \subset \mathcal{J}$ is the divisor that corresponds to the image of $\phi \circ \iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$, that is, the Frobenius action on the points of Θ.

The argument we give here to prove (3.22) is completely analogous to the proof of Proposition 10.13 in [Mil08]; we give a few more details.

Clearly (3.22) is satisfied for $n = 0$ and $n = 1$. Furthermore by (3.21) we have $\Theta_{n+1} - 2\Theta_n + \Theta_{n-1} \sim 2\Theta$. Hence if we assume $\Theta_n \sim n(n-1)\Theta + (n)\Theta_1 + (1-n)\Theta_0$ and $\Theta_{n-1} \sim (n-1)(n-2)\Theta + (n-1)\Theta_1 + (1-(n-1))\Theta_0$, it follows that

$$\begin{aligned}\Theta_{n+1} &\sim 2\Theta_n - \Theta_n + 2\Theta \\ &\sim (n+1)n\Theta + (n+1)\Theta_1 + (1-(n+1))\Theta_0.\end{aligned} \tag{3.23}$$

Completely similarly, if (3.22) is assumed for $n+2$ and for $n+1$, then it follows for n. This finishes the induction proof of (3.22) and we are ready to calculate $\delta_n = \Theta_n \bullet \Theta$.
Finally, we know that $\Theta \bullet \Theta = 2$, $\delta_1 = \Theta_1 \bullet \Theta = 3(q+1) - \#\mathcal{H}(\mathbb{F}_q)$ and $\delta_0 = \Theta_0 \bullet \Theta = 2q$ by the Lemma 3.4.3, Proposition 3.3.4 and Lemma 3.4.4 respectively. Therefore, using the linear relation of the divisors in (3.22):

$$\begin{aligned}\Theta_n \bullet \Theta &= n(n-1)\Theta \bullet \Theta + n\Theta_1 \bullet \Theta + (1-n)\Theta_0 \bullet \Theta \\ &= 2n(n-1) + n(3(q+1) - \#\mathcal{H}(\mathbb{F}_q)) + 2q(1-n) \\ &= 2n^2 + n(q+1-\#\mathcal{H}(\mathbb{F}_q)) + 2q.\end{aligned} \tag{3.24}$$

□

Corollary 3.4.9 (Hasse-Weil for $g = 2$). *Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve with one rational point at infinity and char$(\mathbb{F}_q) \neq 2$, then:*

$$|q + 1 - \#\mathcal{H}(\mathbb{F}_q)| \leq 4\sqrt{q}. \tag{3.25}$$

Proof. Consider the polynomial in n appearing in (3.24) in the previous Theorem 3.4.8. The polynomial has the form $\delta(x) := 2x^2 + Tx + 2q$ with $T := q + 1 - \#\mathcal{H}(\mathbb{F}_q)$. Its discriminant is

$$\Delta_\delta := T^2 - 16q.$$

We want to prove that $\Delta_\delta \leq 0$ since that would imply that $|T| \leq 4\sqrt{q}$, which is exactly the statement of the Hasse-Weil inequality for $g = 2$.

We already proved in Proposition 3.2.3 that if $n \in \mathbb{Z}$ exists such that $\psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is constant, then $\psi_n = 0$, $q = n^2$ is a perfect square and $\#\mathcal{H}(\mathbb{F}_q) = q + 1 \pm 4\sqrt{q}$. Hence from the existence of such n, the Hasse-Weil inequality over $\mathbb{F}_q$ for the curve in question follows. So from now on we will suppose that ψ_n is non-constant for every $n \in \mathbb{Z}$. By Theorem 3.4.8 this implies that $\delta(n) = \Theta \bullet \Theta_n$ for all $n \in \mathbb{Z}$.

We proceed to show first that $\Theta \bullet \Theta_n > 0$ for all $n \in \mathbb{Z}$. A fast and not very elementary argument for that uses that the divisor Θ is ample, hence by the Nakai-Moishezon criterion for ampleness on surfaces, its intersection number with any curve is positive. However, we now present a more elementary proof of the fact that $\Theta \bullet \Theta_n > 0$. In Lemma 3.4.4 we showed that $\Theta \bullet \Theta_0 = 2q > 0$. The remaining cases are the following:

Case $\psi_n(\mathcal{H}) \not\subset \Theta$ for all $n \in \mathbb{Z} \setminus \{0\}$: In this case $\delta(n) = \delta_n = \frac{\deg \Psi_n}{2}$ for all $n \in \mathbb{Z} \setminus \{0\}$, hence $\delta(n) > 0$ for all $n \in \mathbb{Z}$.

Case $\psi_n(\mathcal{H}) \subset \Theta$ for some $n \in \mathbb{Z} \setminus \{0\}$: Here $\psi_n : \mathcal{H} \to \mathcal{J}$ is given by $P \mapsto [(\mathfrak{x}(P), \mathfrak{y}(P)) - \infty]$ for some $\mathfrak{x}, \mathfrak{y} \in \mathbb{F}_q(\mathcal{H})$. Let $(w, 0) \in \mathcal{H}(\mathbb{F}_{q^k})$ be a Weierstrass point on $\mathcal{H}$ (defined over some extension of $\mathbb{F}_q$ of degree k). Consider its associated 2-torsion point $\iota(w, 0) = [(w, 0) - \infty] \in \mathcal{J}$. Further, consider the morphisms $W, \psi_n \in \mathrm{Mor}_{\mathbb{F}_{q^k}}(\mathcal{H}, \mathcal{J})$ where W is given by the constant map $P \mapsto [(w, 0) - \infty]$.
Let $\psi_n^w(x, y) := (\psi_n + W)(x, y) = [(\mathfrak{x}(x, y), \mathfrak{y}(x, y)) + (w, 0) - 2\infty]$, we have that $\Theta_n^w := \psi_n^w(\mathcal{H}) \not\subset \Theta$ and $\Theta_n^w \in \mathrm{Div}(\mathcal{J})$ is clearly a translation of Θ_n by a 2-torsion point, so $\Theta_n^w \sim \Theta_n$ (see [BL13, Corollary 2.5.4]). Moreover, let $[-1] \in \mathrm{Aut}(\mathcal{J})$, we have that $\kappa_4([-1]\psi_n^w(P)) = \kappa_4(\psi_n^w(P))$ by Proposition 3.3.5 and the fact that $W(P) = [-1]W(P) = [(w, 0) - \infty]$. This means that Θ_n^w is symmetric with respect to $[-1]$, therefore $\kappa_4(\psi_n^w(x, y)) \in \mathbb{F}_{q^k}(x)$, which is well defined since $\Theta_n^w \not\subset \Theta$ and $\kappa_4 \in \mathcal{L}(2\Theta)$. Now, let $\Psi_n^w : \mathcal{H} \to \mathbb{P}^1$ be the induced map by $\kappa_4(\psi_n^w(x, y)) = \frac{\mu_{1,n}^w(x)}{\mu_{2,n}^w(x)}$ (analogous to Diagram (3.15)) which is non-constant, then:

$$\Theta_n \bullet \Theta = \Theta_n^w \bullet \Theta = \deg \frac{\Psi_n^w}{2} = \max\{\deg \mu_{1,n}^w, \deg \mu_{2,n}^w\} > 0.$$

The leftmost equality follows from the fact that the intersection number is invariant under linear equivalence (see [Har77, Chapter V. Theorem 1.1]). The middle and rightmost equalities are justified analogous to Lemma 3.4.2. The inequality follows from the fact that $\kappa_4(\psi_n^w(x, y))$ is non-constant and well defined.

Now we show that $\delta(x)$ is non-negative for all $x \in \mathbb{R}$ hence, it has non-positive discriminant.
Suppose that the Hasse-Weil inequality for genus 2 is false. This is equivalent to the statement $\Delta_\delta > 0$. In this case $\delta(x)$ has two different real zeros $\alpha < \beta$.

We have that Δ_δ in terms of α and β is given by:

$$\Delta_\delta = 4(\alpha - \beta)^2 = T^2 - 16q.$$

The integer Δ_δ is assumed to be positive, so we conclude $4(\alpha - \beta)^2 \geq 1$. Moreover, recall $\delta(n) > 0$ for every $n \in \mathbb{Z}$. Since for any $x_0 \in (\alpha, \beta)$ we have that $\delta(x_0) < 0$, it follows that (α, β) contains no integers. This implies that $\beta - \alpha < 1$ and then $1 \leq 4(\alpha - \beta)^2 < 4$.
So we have just three situations for positive discriminant: $T^2 - 16q \in \{1, 2, 3\}$. Each of these possibilities results in a contradiction as we will see below.

Case $T^2 - 16q = 3$: Consider the parabola Π given by of $x^2 - 16y = 3$. We are interested in the integer points $(T, q) =: (x, y)$ of Π.
Since $16y = x^2 - 3$, we have that $x \in \mathbb{Z}$ must be odd, namely $x = 2k + 1$ for $k \in \mathbb{Z}$. If we substitute $x = 2k+1$ in the equation of Π we get $8y+1 = 2(k^2+k)$ which obviously does not have integer solutions. ※

Case $T^2 - 16q = 2$: This is similar to the previous case since the integer solutions for the parabola $16y = x^2 - 2$ must have $x = 2k$ with $k \in \mathbb{Z}$. Therefore $8y + 1 = 2k^2$ which also does not have integer solutions. ※

Case $T^2 - 16q = 1$: Again we consider the parabola Π given by the locus of $16y = x^2 - 1$. Here we have that the integer solutions $(x, y) \in \Pi$ must have x coordinate odd, namely $x = 2k + 1$.
We substitute $x = 2k + 1$ in the equation and we get that $4y = k^2 + k$. So $k^2 + k \equiv 0 \bmod 4$, therefore we have two subcases for k.

(i) $k = 4w$ with $w \in \mathbb{Z}$: then $y = 4w^2 + w$ and one obtains the integral point $(8w + 1, 4w^2 + w) \in \Pi$. We will show that this integer point in Π cannot be of the form (T, q) with q the cardinality of a finite field $\mathbb{F}_q$ and $T = q + 1 - \#\mathcal{H}(\mathbb{F}_q)$ for some genus 2 curve $\mathcal{H}/\mathbb{F}_q$.

(ii) $k = 4w + 3$ with $w \in \mathbb{Z}$: Here one obtains $y = 4w^2 + 7x + 3$ hence we find the integral point $(8w + 7, 4w^2 + 7w + 3) \in \Pi$. We will prove that no pair $(T = 8w + 7, q = 4w^2 + 7w + 3) \in \Pi$ is possible for a genus 2 hyperelliptic curve $\mathcal{H}/\mathbb{F}_q$.

Subcase (i): $T = 8w + 1 = q + 1 - \#\mathcal{H}(\mathbb{F}_q)$, $q = 4w^2 + w = p^n$.

Since p is the only prime dividing $q = w(4w+1)$ and since $\gcd(w, 4w+1) = 1$, it follows that $w = \pm 1$ or $4w + 1 = \pm 1$. We proceed to check all possibilities.

If $4w+1=+1$ then $w=0$ and $q=0$ which is not possible.
If $4w+1=-1$ then $w=-\frac{1}{2}$ which is absurd since w is an integer.
If $w=+1$ then $q=5$ and $T=9$. However $9=5+1-\#\mathcal{H}(\mathbb{F}_5)$ is impossible since a curve cannot have less than 0 points.
If $w=-1$ then $q=3$ and $T=-7$. However a hyperelliptic curve $\mathcal{H}/\mathbb{F}_3$ has at most $2\cdot 3+2$ rational points, hence $T\geq 3+1-8=-4$.

Subcase (ii): $T=8w+7=q+1-\#\mathcal{H}(\mathbb{F}_q)$, $q=4w^2+7w+3=p^n$

Again p is the only prime dividing $q=4w^2+7w+3=(w+1)(4w+3)$. Moreover these two factors are coprime since $4(w+1)-(4w+3)=1$. Therefore one of the factors must be ± 1. Again we check all possibilities
If $w+1=1$ then $q=3$ and $T=7$. However any curve $C/\mathbb{F}_3$ has at least 0 rational points, hence $T=3+1-\#C(\mathbb{F}_3)\leq 4$.
If $w+1=-1$ then $q=5$ and $T=-9$. Any hyperelliptic $\mathcal{H}/\mathbb{F}_5$ satisfies $\#\mathcal{H}(\mathbb{F}_5)\leq 2\cdot(5+1)$, hence $T\geq 6-12=-6$.
The case $4w+3=1$ is impossible since w is assumed to be an integer.
Finally, $4w+3=-1$ leads to $q=0$ which is absurd.

This shows that the assumption $\Delta_\delta=T^2-16q>0$ leads to a contradiction. As a consequence $|T|\leq 4\sqrt{q}$ which is precisely the Hasse-Weil inequality for genus 2. □

Chapter 4

Geometric primality tests using curves of genus $0, 1$ & 2

Here we revisit and generalize some geometric techniques behind deterministic primality testing for some integer sequences using curves of genus 0 and 1 over finite rings. Subsequently we develop a similar primality test using the Jacobian of a genus 2 curve.

This chapter is mainly inspired by a lecture at the *Intercity Seminar* [Top15] given by Jaap Top, *"Lucas-Lehmer revisited"*. Also a paper by B.H. Gross was relevant for this topic: in this paper [Gro05] he was the first to use an elliptic curve for constructing a deterministic primality test for numbers of the form $2^p - 1$ (Mersenne numbers).

We begin with the simplest case, namely conics. Conics are going to be a motivation for all subsequent primality tests discussed in the present chapter. After a rather trivial first example, we describe the usage of the unit circle to identify primes of the form $m2^n - 1$ where $m < 2^n - 2 - \frac{2}{2^n}$ is odd. The observation that makes the methods work is that over any finite field $\mathbb{F}$ considered, the conics $\mathfrak{C}$ we use have the structure of a group variety over $\mathbb{F}$ and we have good estimates for $\#\mathfrak{C}(\mathbb{F})$.

After the case of conics, we describe the usage of elliptic curves $E_t : y^2 = x^3 - (t^2 + 1)x$ for primality testing of integers of the same form as before, namely $m2^n - 1$. Here we demand the odd integer m to satisfy $4m < 2^n$.

Again the group structure and size of $E_t(\mathbb{F})$ for $\mathbb{F}$ certain finite fields is used for designing a primality test. In [DS08] Denomme and Savin use complex multiplication on elliptic curves to develop primality tests for several sequences of integers. Variants and generalizations of this were obtained by Gurevich and Kunyavskiĭ in [GK12], by Tsumura [Tsu11], and by Wong [Won13]. As one of their examples, Denomme and Savin used a quadratic twist of $E : y^2 = x^3 - x$ to do a primality test on Fermat numbers using the $\mathrm{End}_{\mathbb{Q}(i)}(E)$-module structure of E. Here we extend their setting from Fermat integers to integers of the form $p^2 16^n + 1$ where $p \equiv \pm 1 \bmod 10$ and $p < 4^n$.

Finally, with this, we focus our attention to an open question stated by Abatzoglou, Silverberg, Sutherland and Wong in [ASSW16, Remark 4.13]. This question asks about the design of a potential primality test using Jacobians of genus 2 curves. We develop a method to identify primes of the form $4 \cdot 5^n - 1$ using the Jacobian $\mathcal{J}$ of the genus 2 curve $\mathcal{H} : y^2 = x^5 + h$ as a cyclic $\mathrm{End}_{\mathbb{Q}(\sqrt{5})}(\mathcal{J})$-module. We emphasize that efficient primality tests for integers $4 \cdot 5^n - 1$ may exist, but here we state a result to work with these integers using an Abelian variety of dimension 2.

4.1 Motivation: Primality testing *à la* Lucas and conics

It is well known that a necessary condition (but not sufficient) for a number $n \in \mathbb{N}$ to be prime is that for all $a \in \mathbb{N}$ such that $2 \leq a < n$ the congruence $a^{n-1} \equiv 1 \bmod n$ holds. This *Little Theorem* by Fermat can be used as a *test* for compositeness calculating the congruence for several a. We infer that n is composite if for some a, the congruence does not hold. When the congruence holds for many choices of a the number n is said to be *probably prime.* The computation of this congruence can be done quite fast using modular repeated squaring.

Unfortunately there is a problem with this *Fermat test*, there are infinitely many composite numbers such as $m = 561$ satisfying $a^{m-1} \equiv 1 \bmod m$ for all a such that $(m, a) = 1$. These numbers are known as *Carmichael numbers.* Even though Carmichael numbers are rarer than prime numbers (see [EM56]) other extensions of this test were developed to deal with this, like Miller-Rabin or Solovay-Strassen which are more common in practice. In order to turn this *Fermat test* into a primality testing algorithm, Édouard Lucas stated the following theorem:

Theorem 4.1.1. *[Lucas, 1876] Let $a, n \in \mathbb{Z}$ be such that $a^{n-1} \equiv 1 \bmod n$ and $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$ for all primes $p \mid (n-1)$. Then n is prime.*

Proof. Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $k = \#\langle a \rangle$. Since $a^{n-1} \equiv 1 \bmod n$, we have $k \mid n-1$. Further, we have that $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$ for all $p \mid (n-1)$, hence $k = n-1$. With this we have that $\#(\mathbb{Z}/n\mathbb{Z})^\times = n-1$ and then n is prime. □

This elementary theorem is used by several deterministic primality tests.
A problem for potential algorithms that could arise from this theorem is that it requires the prime divisors of $n-1$. This is very difficult in general, but for example, if we restrict our algorithms to potential prime numbers of the form $k2^n + 1$ or $2^{2^n} + 1$ this theorem can be applied effectively. Also, another less difficult problem when using Theorem 4.1.1 is that in case of n being prime, we need to find a correct $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ that satisfies the hypotheses of Theorem 4.1.1. This "*problem*" means that when n is prime then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic, so we need an $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ that generates this cyclic group (of units of $\mathbb{Z}/n\mathbb{Z}$). The existence of this a satisfying Theorem 4.1.1 is a classical result by Gauß exposed in the article 57 from *Disquisitiones* where he calls them *primitive roots modulo n*, see [Gau86]. Gauß proved that such a exists but finding it in general is a different problem.
The main motivation for primality testing using geometrical tools can be obtained from the following theorem for Mersenne numbers $M_n := 2^n - 1$.

Theorem 4.1.2. *[Lucas-Lehmer] Consider the sequence $a_0 := 4, a_{i+1} := a_i^2 - 2$. Let $n > 2$. $M_n := 2^n - 1$ is prime if and only if $a_{n-2} \equiv 0 \bmod M_n$.*

This result is classical and many proofs of it can be found in the literature. We sketch a proof that uses properties of an Abelian group variety given by a Pell conic, namely:

$$G := \{(x, y) \in \mathbb{A}^2 : x^2 - 3y^2 = 1\}.$$

The group variety structure is defined by

$$G \times G \to G \ : \quad ((x_1, y_1), (x_2, y_2)) \mapsto (x_1x_2 + 3y_1y_2, x_1y_2 + x_2y_1).$$

The element a_j in the sequence of Theorem 4.1.2 is exactly 2 times the x coordinate of the j^{th} recursive doubling of the point $(2, 1) \in G \bmod M_n$, in other words $a_j = 2 \cdot x(2^j(2, 1)) \bmod M_n$. When M_n is prime and $n > 2$, one first shows that $\#G(\mathbb{F}_{M_n}) = 2^n$ and that this group contains only one element of order 2. As a result, the group is cyclic. Next, one shows that the point $(2, 1)$ is not the double of some other point in $G(\mathbb{F}_{M_n})$ and therefore $(2, 1)$ generates this group. It follows that $2^{n-2}(2,1) \in G(\mathbb{F}_{M_n})$ has order 4. It is easy to see that any point of order 4 has x-coordinate equal to 0, and therefore $a_{n-2} = 0$. For the converse, assume that $a_{n-2} \equiv 0 \bmod M_n$. Take a prime divisor $\ell | M_n$. The assumption implies that $2^{n-2}(2,1)$ has order 4 in $G(\mathbb{F}_\ell)$. Hence $(2,1)$ has order 2^n in that group, and one concludes $2^n \leq \#G(\mathbb{F}_\ell) \leq \ell + 1$. It follows that $\ell = M_n$ and hence M_n is prime.

In the following sections we explore a geometrical perspective of the *Lucasian* primality tests arising from these ideas using algebraic groups from conics, elliptic curves and finally from Jacobians of genus 2 curves. It is important to mention that a formal treatment of primality test algorithms using Pell conics exists (see [Ham12]). We begin with two specific conics (a hyperbola and a unit circle) in order to get the motivation for the next parts.

4.1.1 Fermat primes and the rational curve $xy = 1$

We denote Fermat numbers by $\mathcal{F}_n := 2^{2^n} + 1$.
Consider the conic $\mathfrak{H} \subset \mathbb{A}^2$ given by the zeros of $xy - 1$. This is in fact the standard model of the group variety $\mathbb{G}_m$; the group structure is given by

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2, y_1y_2), \quad (x, y)^{-1} = (y, x), \quad \text{and} \quad \mathbb{1} := (1, 1).$$

For any commutative ring $\mathcal{R}$ the group

$$\mathfrak{H}(\mathcal{R}) := \{(a, b) \in \mathbb{A}^2 : a, b \in \mathcal{R}, ab = 1\}$$

is isomorphic to $\mathcal{R}^\times$, the group of units in the ring $\mathcal{R}$. Our interest is in the group $\mathfrak{H}(\mathbb{Z}/\mathcal{F}_n\mathbb{Z}) \cong (\mathbb{Z}/\mathcal{F}_n\mathbb{Z})^\times$ since it has order 2^{2^n} if and only if $\mathcal{F}_n$ is prime. Moreover, if $\mathcal{F}_n$ is prime, this group is cyclic.

.

Proposition 4.1.3. *Let $\mathcal{F}_n$ be prime with $n > 0$. $Q := (\alpha, \frac{1}{\alpha})$ generates $\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$ if and only if $\alpha \notin \mathbb{F}_{\mathcal{F}_n}^{\times 2}$.*

Proof. Consider the Euler's totient function φ. Suppose that Q generates $\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$. Since $\#\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n}) = \varphi(\mathcal{F}_n) = 2^{2^n}$, there is no $R \in \mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$ such that $R^2 = Q$ (otherwise Q is not a generator). This is equivalent to say that $x^2 = \alpha$ has no solutions over $\mathbb{F}_{\mathcal{F}_n}$, hence α is not a square.
For the converse, if α is not a square in $\mathbb{F}_{\mathcal{F}_n}^\times$ then there is no $R \in \mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$ with $R^2 = Q$. Since $\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$ is cyclic of order 2^{2^n} we have that Q generates $\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$. □

With this, we obtain *Pépin's* test for Fermat primes naturally.

Corollary 4.1.4. *Let $\alpha \in (\mathbb{Z}/\mathcal{F}_n\mathbb{Z})^\times$ be a non-square.*
$\mathcal{F}_n$ is prime iff the sequence $x_0 = \alpha$, $x_{i+1} = x_i^2$ has $x_{2^n-1} \equiv -1 \bmod \mathcal{F}_n$.

Proof. Let $\mathcal{F}_n$ be prime, then $\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$ is cyclic of order $\mathcal{F}_n - 1 = 2^{2^n}$.
The sequence above is equivalent to the first coordinate of a recursive squaring in $\mathfrak{H}$ of the point $Q := (\alpha, \frac{1}{\alpha})$, that is, x_i is the first coordinate of Q^{2^i}. Since α is not a square in $\mathbb{F}_{\mathcal{F}_n}$ we have that $\mathfrak{H}(\mathbb{F}_{\mathcal{F}_n})$ is generated by Q by the previous proposition. With this we have that Q has order 2^{2^n} and $T := Q^{2^{2^n-1}}$ has order 2, hence $T = (-1, -1)$ since this is the only point of order 2. This is equivalent to $x_{2^n-1} \equiv -1 \bmod \mathcal{F}_n$.

For the converse, if $x_{2^n-1} \equiv -1 \bmod \mathcal{F}_n$ then $x_{2^n} \equiv 1 \bmod \mathcal{F}_n$. This means that the order of $Q := (\alpha, \frac{1}{\alpha}) \in \mathfrak{H}(\mathbb{Z}/\mathcal{F}_n\mathbb{Z})$ divides $\mathcal{F}_n - 1 = 2^{2^n}$. Further the order of Q does not divide $\frac{\mathcal{F}_n-1}{2}$ (since $x_{2^n-1} \equiv -1 \bmod \mathcal{F}_n$), hence $Q \in \mathfrak{H}(\mathbb{Z}/\mathcal{F}_n\mathbb{Z})$ has order 2^{2^n}. Is equivalent to say that $2^{2^n} \mid \#\mathfrak{H}(\mathbb{Z}/\mathcal{F}_n\mathbb{Z}) = \varphi(\mathcal{F}_n)$. This implies that $\varphi(\mathcal{F}_n) = \mathcal{F}_n - 1$ hence $\mathcal{F}_n$ is prime. □

To put Corollary 4.1.4 in practice, it is useful to find a fixed $\alpha \in \mathbb{Z}$ such that α is not a square modulo $\mathcal{F}_n$ for $n > 0$. This potential α can be found using the Jacobi symbol. For example, $\alpha = 3$ works, as is seen as follows. Since $n > 0$, $\mathcal{F}_n$ is odd and $\mathcal{F}_n \not\equiv 3 \bmod 4$ and $\mathcal{F}_n \equiv 2 \bmod 3$. Therefore $\left(\frac{3}{\mathcal{F}_n}\right) = \left(\frac{\mathcal{F}_n}{3}\right) = \left(\frac{2}{3}\right) = -1$, hence $\alpha \notin (\mathbb{Z}/\mathcal{F}_n\mathbb{Z})^{\times 2}$.

A similar computation shows that for $n > 1$ we can use $\alpha = 5$ to do primality test on $\mathcal{F}_n$. Further, we can use $\alpha = 10$, but it requires a little bit more to show that $\left(\frac{10}{\mathcal{F}_n}\right) = -1$. A proof runs as follows. Observe

$$\left(\frac{10}{\mathcal{F}_n}\right) = \left(\frac{5}{\mathcal{F}_n}\right)\left(\frac{2}{\mathcal{F}_n}\right) = -\left(\frac{2}{\mathcal{F}_n}\right).$$

We have to show that $\left(\frac{2}{\mathcal{F}_n}\right) = \prod \left(\frac{2}{f_i}\right) = 1$ where $\mathcal{F}_n = \prod f_i$ is the prime factorization of $\mathcal{F}_n$. Using Gauss' Lemma on quadratic residues, we have that $\left(\frac{2}{p}\right) = -1$ iff $p \equiv 3$ or $5 \bmod 8$. Hence, $\left(\frac{2}{\mathcal{F}_n}\right) = 1$ if $\#\{f_j \mid \mathcal{F}_n : f_j \equiv 3, 5 \bmod 8\}$ is even. We proceed to show that there are no primes in the factorization of $\mathcal{F}_n$ that are 3 or 5 mod 8.
Let $f \mid \mathcal{F}_n$ be a prime divisor, then $2^{2^n} \equiv -1 \bmod f$, hence, squaring the last congruence we have that the order of 2 modulo f is 2^{n+1}. Hence $f \equiv$

1 mod 2^{n+1} which implies that $f \equiv 1 \bmod 8$ for $n > 1$ for every prime divisor of $\mathcal{F}_n$. Hence, $\left(\frac{2}{\mathcal{F}_n}\right) = 1$ and $\left(\frac{10}{2}\right) = -1$.

We remark as a consequence of the equality $\left(\frac{2}{\mathcal{F}_n}\right) = 1$ that if α works as the initial point in Pépin's test, then so does 2α.

We show a sample code using the computer algebra system MAGMA of a typical implementation of this test.
We test $\mathcal{F}_{15} = 2^{32768} + 1$, which has $\approx 10,000$ decimal digits.

```
> IsFermatPrime := function(n)
function> xi := 3; Fn := 2^(2^n)+1; R := Integers(Fn);
function>       for n := 1 to 2^n-1 do
function|for>             xi := R!xi^2;
function|for>   end for;
function> return xi eq R!-1;
function> end function;
> time IsFermatPrime(15);
false
Time: 784.000
```

Pepin's test is the fastest deterministic primality test known for $\mathcal{F}_n$, but due to the fact that the size of $\mathcal{F}_n$ increases very rapidly with n, only a few of them can be tested in reasonable time. According to the *Proth Search Project* (http://www.prothsearch.com/fermat.html), it is unknown (January 2018) whether $\mathcal{F}_{33}$ is prime or not (2.6 billion decimal digits).

4.1.2 Primes of the form $m2^n - 1$ with $m < 2^n$ odd and the conic $x^2 + y^2 - 1$

In this section we set the stage for a primality test applied to certain integers of the form $\mathcal{A}_{m,n} := m2^n - 1$ (with $m, n \in \mathbb{Z}_{>0}$). We use (an algebraic group structure on) the conic $\mathfrak{C} \subset \mathbb{A}^2$ given by the zeros of $x^2 + y^2 - 1$.
The group law for $\mathfrak{C}$ is written multiplicatively, and it is defined for $(x_1, y_1), (x_2, y_2) \in \mathfrak{C}$ by $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$ and $(x, y)^{-1} = (x, -y)$. The neutral element of $\mathfrak{C}$ is $\mathbb{1} := (1, 0)$.
Observe that the group operation of $\mathfrak{C}$ is motivated by the usual multiplication of complex numbers $x + yi \in \mathbb{C}$. Further, the inverses in $\mathfrak{C}$ reflect complex conjugation (on the subgroup $\mathbb{S} = \{z \ : \ |z| = 1\} \subset \mathbb{C}^\times$ indeed complex conjugation and taking inverses coincide). This observation can be extended to a more algebraic description of the groups discussed here, e.g.,

$$\mathfrak{C}(\mathbb{Z}/n\mathbb{Z}) \cong \{a + bi \in (\mathbb{Z}[i]/(n))^\times : a^2 + b^2 \equiv 1 \bmod n\}. \tag{4.1}$$

We will show some lemmas allowing us to use $\mathfrak{C}(\mathbb{Z}/\mathcal{A}_{m,n}\mathbb{Z})$ for a primality

testing algorithm applicable to certain integers of the form $\mathcal{A}_{m,n}$.
First we state the next easy lemma to discard trivially composite numbers of the form $\mathcal{A}_{m,n}$.

Lemma 4.1.5. *The integer $\mathcal{A}_{m,n} = m2^n - 1$ is divisible by 3 if one of the following conditions holds:*

- $m \equiv 2 \bmod 3$ *and* $n \equiv 1 \bmod 2$*;*
- $m \equiv 1 \bmod 3$ *and* $n \equiv 0 \bmod 2$.

Further, $\mathcal{A}_{m,n} = m2^n - 1$ is divisible by 5 if one of the following conditions holds:

- $m \equiv 1 \bmod 5$ *and* $n \equiv 0 \bmod 4$*;*
- $m \equiv 2 \bmod 5$ *and* $n \equiv 3 \bmod 4$*;*
- $m \equiv 3 \bmod 5$ *and* $n \equiv 1 \bmod 4$*;*
- $m \equiv 4 \bmod 5$ *and* $n \equiv 2 \bmod 4$.

Proof. This is clear analyzing the period of the map $n \mapsto 2^n \bmod 3$ and of the map $n \mapsto 2^n \bmod 5$. □

Now we show some properties of the group $\mathfrak{C}(\mathbb{F}_p)$.

Lemma 4.1.6. *If $p \equiv 3 \bmod 4$ is prime then $\mathfrak{C}(\mathbb{F}_p)$ is a cyclic group of order $p+1$.*

Proof. Since $p \equiv 3 \bmod 4$ we have that p is prime in $\mathbb{Z}[i]$ and therefore $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$. As a consequence the multiplicative group $(\mathbb{Z}[i]/(p))^\times \cong \mathbb{F}_{p^2}^\times$ is cyclic. Since $\mathfrak{C}(\mathbb{F}_p)$ is isomorphic to a subgroup of $(\mathbb{Z}[i]/(p))^\times$ (compare (4.1)), we have that $\mathfrak{C}(\mathbb{F}_p)$ is cyclic.

It remains to show that $\#\mathfrak{C}(\mathbb{F}_p) = p + 1$, which is done by a well known argument we recall here.

Consider the lines through $\mathbb{1} = (1, 0) \in \mathfrak{C}$ with slope $\sigma \in \mathbb{F}_p$, namely $y = \sigma(x - 1)$. If we intersect such a line with $\mathfrak{C}$, an intersection point (x, y) satisfies $x^2 + \sigma^2(x - 1)^2 = 1$. Hence $x = \frac{\sigma^2-1}{\sigma^2+1}$ or $x = 1$. For the first solution, since $p \not\equiv 1 \bmod 4$ we have that $\sigma^2 + 1 \neq 0$, hence the slope σ can have all the different p values in $\mathbb{F}_p$ obtaining p points of $\mathfrak{C}(\mathbb{F}_p)$. The additional point in $\mathfrak{C}$ is $\mathbb{1}$, the "base" point of our lines intersecting $\mathfrak{C}$. Hence, $\#\mathfrak{C}(\mathbb{F}_p) = p + 1$. □

An important remark about the group $\mathfrak{C}(\mathbb{Z}/n\mathbb{Z})$ is that if $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ is the prime factorization of n, then $\mathfrak{C}(\mathbb{Z}/n\mathbb{Z}) \cong \mathfrak{C}(\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \ldots \times \mathfrak{C}(\mathbb{Z}/p_r^{k_r}\mathbb{Z})$. This follows from the Chinese remainder theorem. As a consequence, for $r > 1$ we have that $\mathfrak{C}(\mathbb{Z}/p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}\mathbb{Z})$ is non-cyclic because every factor $\mathfrak{C}(\mathbb{Z}/p_r^{k_r})$ contains the element $(0, 1)$ which has order 2 (case $p_r = 2$) or order 4 (case $p_r > 2$).

The following lemma identifies important points in $\mathfrak{C}$ that will be used in our primality test algorithm.

Lemma 4.1.7. *Let $p > 2$ be prime. The only point order 2 in $\mathfrak{C}(\mathbb{F}_p)$ is $(-1, 0)$ and there are only two points of order 4 given by $(0, \pm 1)$.*

Proof. Suppose that $T := (a, b)$ is a point of order 2. Using the group law we have that $a^2 - b^2 = 1$, $2ab = 0$ and $a^2 + b^2 = 1$. It follows that $a^2 = 1$ and $b = 0$. Since $T \neq \mathbb{1}$, this implies $T = (-1, 0)$ which indeed has order 2.

Suppose that $U := (z, w) \in \mathfrak{C}(\mathbb{F}_p)$ has order 4. Then we have that U^2 has order 2, therefore

$$U^2 = \left(z^2 - w^2, 2zw\right) = (-1, 0)$$

Using that $z^2 + w^2 = 1$ and $U \neq \mathbb{1}$ it follows that $U = (0, \pm 1)$, and indeed these points have order 4. □

Now fix the point $Q := (\frac{3}{5}, \frac{4}{5}) \in \mathfrak{C}$. The following easy lemma tells us for which p the point Q is a square in $\mathfrak{C}(\mathbb{F}_p)$.

Lemma 4.1.8. *Let $p > 5$ be prime. $Q := (\frac{3}{5}, \frac{4}{5})$ is a square in $\mathfrak{C}(\mathbb{F}_p)$ if and only if $p \equiv \pm 1 \bmod 5$.*

Proof. Using the group law on $\mathfrak{C}$ we have that Q is a square in $\mathfrak{C}(\mathbb{F}_p)$ if and only if the system of equations given by $x^2 - y^2 = \frac{3}{5}$, $2xy = \frac{3}{5}$ and $x^2 + y^2 = 1$ has a solution $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$. Adding the first and the third equations we obtain $x^2 = \frac{4}{5}$. There is a solution to this equation if and only if $5 \in \mathbb{F}_p^{\times 2}$. Quadratic reciprocity implies that this holds if and only if $p \equiv \pm 1 \bmod 5$. Furthermore, if this congruence holds then taking $x \in \mathbb{F}_p$ with $x^2 = \frac{4}{5}$ one easily checks that $(x, \frac{x}{2}) \in \mathfrak{C}(\mathbb{F}_p)$ squared is Q. □

Remark: We will test primality of certain integers of the form $\mathcal{A}_{m,n}$ using the point $Q := (\frac{3}{5}, \frac{4}{5}) \in \mathfrak{C}(\mathbb{Z}/\mathcal{A}_{m,n}\mathbb{Z})$ together with Lemma 4.1.8.

We require that 5 is not a square modulo $\mathcal{A}_{m,n}$. For any integer N with $\gcd(N, 10) = 1$ one has that 5 is a quadratic residue mod N if and only if every prime that divides N is congruent to $\pm 1 \mod 5$. In our case, if $\mathcal{A}_{m,n} := m2^n - 1$ happens to be ± 2 modulo 5 and $n > 0$, then clearly $\gcd(\mathcal{A}_{m,n}, 10) = 1$ and the reasoning above shows that 5 is not a quadratic residue modulo $\mathcal{A}_{m,n}$.

Lemma 4.1.9. *Let $\mathcal{A}_{m,n} := m2^n - 1$ be an integer, m odd and $n \geq 1$ such that one of the following conditions on m and n hold:*

(i) $m \equiv 1 \bmod 5$ *and* $n \equiv 3$ *or* $2 \bmod 4$*;*

(ii) $m \equiv 2 \bmod 5$ *and* $n \equiv 2$ *or* $1 \bmod 4$*;*

(iii) $m \equiv 3 \bmod 5$ *and* $n \equiv 0$ *or* $3 \bmod 4$*;*

(iv) $m \equiv 4 \bmod 5$ *and* $n \equiv 1$ *or* $0 \bmod 4$*.*

Then $\mathcal{A}_{m,n} \equiv \pm 2 \bmod 5$ and 5 is not a square modulo $\mathcal{A}_{m,n}$.

Proof. This is a direct calculation using the period of the map $n \mapsto 2^n \mod 5$. □

With this we get the following deterministic primality test algorithm for certain integers $\mathcal{A}_{m,n} := m2^n - 1$.

Theorem 4.1.10. *Let m, n be positive integers such that $n > 1$, $m < 2^n - 2 + \frac{2}{2^n}$ is odd, and $\mathcal{A}_{m,n} := m2^n - 1 \equiv \pm 2 \bmod 5$. Define coprime integers α, β as follows. Take $Q := (\frac{3}{5}, \frac{4}{5}) \in \mathfrak{C}(\mathbb{Q})$ and let $\frac{\alpha}{\beta}$ be the x-coordinate of Q^m. Then β is a unit modulo $\mathcal{A}_{m,n}$. Define the sequence $x_0 := \frac{\alpha}{\beta}$, $x_{i+1} = 2x_i^2 - 1$.*
We have that $\mathcal{A}_{m,n}$ is prime if and only if $x_{n-2} \equiv 0 \bmod \mathcal{A}_{m,n}$.

Proof. Note that $p = 5$ is the only prime appearing in the denominator of the coordinates of Q. The formula for multiplication in $\mathfrak{C}$ then shows that the only prime that can possibly appear in a coordinate of Q^a for an integer a, is again $p = 5$. Hence β is (up to sign) a power of 5, so by assumption it is a unit modulo $\mathcal{A}_{m,n}$. As a consequence, all $x_j \bmod \mathcal{A}_{m,n}$ are well defined.

Suppose that $\mathcal{A}_{m,n}$ is prime. Note that the x_j given above are the x-coordinates of certain powers of $Q^m \in \mathfrak{C}(\mathbb{F}_{\mathcal{A}_{m,n}})$, namely $x_j = x((Q^m)^{2^j})$.
Since $n > 1$ we have that $\mathcal{A}_{m,n} \equiv 3 \bmod 4$, hence $\mathfrak{C}(\mathbb{F}_{\mathcal{A}_{m,n}})$ is cyclic of order $m2^n$ by Lemma 4.1.6. By assumption $\mathcal{A}_{m,n} \equiv \pm 2 \bmod 5$, hence by Lemma 4.1.8 Q is not a square in $\mathfrak{C}(\mathbb{F}_{\mathcal{A}_{m,n}})$.
With this, since m is odd, we have that Q^m generates the 2-Sylow-subgroup of $\mathfrak{C}(\mathbb{F}_{\mathcal{A}_{m,n}})$. Hence $(Q^m)^{2^{n-2}}$ has order four in $\mathfrak{C}(\mathbb{F}_{\mathcal{A}_{m,n}})$, and therefore $x_{n-2} \equiv 0 \bmod \mathcal{A}_{m,n}$ by Lemma 4.1.7.

For the converse suppose that $x_{n-2} \equiv 0 \bmod \mathcal{A}_{m,n}$ and assume $\mathcal{A}_{m,n}$ is composite. Let $\mathfrak{s} \mid \mathcal{A}_{m,n}$ be a proper prime divisor of $\mathcal{A}_{m,n}$ with the property $\mathfrak{s}^2 \leq \mathcal{A}_{m,n}$. Then $x_{n-2} \equiv 0 \bmod \mathfrak{s}$. Hence $(\bar{Q}^m)^{2^{n-2}} \in \mathfrak{C}(\mathbb{F}_\mathfrak{s})$ is of the form $(0, \pm 1)$, by Lemma 4.1.7. This last point has order 4 in $\mathfrak{C}(\mathbb{F}_\mathfrak{s})$ and therefore $\bar{Q}^m$ has order 2^n. Further, we have that $\mathfrak{s} \leq \sqrt{\mathcal{A}_{m,n}} = \sqrt{m2^n - 1}$, implying that $2^n \leq \#\mathfrak{C}(\mathbb{F}_\mathfrak{s}) \leq \mathfrak{s} + 1 \leq \sqrt{m2^n - 1} + 1$.
As a consequence $2^n + \frac{2}{2^n} - 2 \leq m$, contradicting the hypotheses. ※Hence $\mathcal{A}_{m,n}$ is prime. □

The proof of this theorem guarantees the primality of $\mathcal{A}_{m,n}$ starting on a certain n with respect to a fixed m. In the next subsection, we provide an example of a primality test algorithm for a sequence of numbers of the form $\mathcal{A}_{m,n}$ using Theorem 4.1.10.

4.1.3 Example: Finding primes via the conic method

Consider the integers of the form $\mathcal{A}_{7,n} = 7 \cdot 2^n - 1$. Theorem 4.1.10 says that we have a conclusive primality test for $\mathcal{A}_{7,n}$ when the inequality $7 < 2^n - 2 + \frac{2}{2^n}$ holds. This means that we can test starting from $n \geq 4$ (note that $\mathcal{A}_{7,2} = 3^3$ and $\mathcal{A}_{7,3} = 5 \cdot 11$).
Since $7 \equiv 2 \bmod 5$ and $7 \equiv 1 \bmod 3$, it is easy to see that $\mathcal{A}_{7,2k}$ and $\mathcal{A}_{7,4k+3}$ are divisible by 3 and 5 respectively (see Lemma 4.2.4). This means that all the primes of the form $\mathcal{A}_{7,n}$ must have $n = 4k + 1$. Further, we can use $Q = (\frac{3}{5}, \frac{4}{5}) \in \mathfrak{C}(\mathbb{Z}/\mathcal{A}_{7,4k+1}\mathbb{Z})$ to do a primality test since $\mathcal{A}_{7,4k+1} \equiv -2 \bmod 5$, and by Lemma 4.2.6 we have that 5 is not a square modulo $\mathcal{A}_{7,4k+1}$.
With this, we implement a primality test algorithm for the sequence $\mathcal{A}_{7,4k+1}$ for all $k > 1$.

Let $Q = (\frac{3}{5}, \frac{4}{5}) \in \mathfrak{C}(\mathbb{Q})$, then Q^7 can be calculated with the group law, or also as $Q^7 = (\cos(7\cos^{-1}(\frac{3}{5})), \sin(7\sin^{-1}(\frac{4}{5}))) = (\frac{76443}{78125}, \frac{16124}{78125})$. We use the sequence presented in Theorem 4.1.10:

$$x_0 := \frac{76443}{78125}, x_{i+1} := 2x_i^2 - 1 \bmod \mathcal{A}_{7,n}.$$

We have to check that $x_{n-2} \equiv 0 \bmod \mathcal{A}_{7,n}$ to infer that $\mathcal{A}_{7,n}$ is prime ($n-2$ steps), otherwise composite.
For example using *MAGMA*, we checked that the number $7 \cdot 2^{70209} - 1$ is prime which has ≈ 21,500 decimal digits.

```
> primetest7 := function(n)
R := Integers(7*2^n -1);  xi := R!(76443/78125);
 for i:=1 to n-2 do
```

```
   xi := R!(2*xi^2 -1);
 end for;
return xi eq 0;
end function;
primetest7(70209);
true
```

Running this for $n = 4, \ldots, 5000$, one finds that the only integers in this range such that $\mathcal{A}_{7,n}$ is prime, are the integers $n \in \{5, 9, 17, 21, 29, 45, 177\}$. This took less than half a minute on a standard laptop.

Similarly, a faster program can be done in GP/PARI. In this case we do it for $13 \cdot 2^n - 1$. Primes of this form can only occur when the exponent is of the form $n = 4k + 3$ for some integer k, as we will see in the next section. The code is:

```
{
p = 13;
for (k=3, 100,
xi = (1064447283/1220703125) ;
        for (i=1, (4*k+3) - 2,
                xi = (2*xi^2  - 1) % (p*2^(4*k+3) - 1);
             );
                if (xi == 0,
                printf("at n=%d IS prime\n", 4*k+3),
                            printf("at n=%d NOT prime\n", 4*k+3)
           );
    );
}
```

4.2 Primality testing with genus 1 curves

In the first subsection here, we construct a primality test using properties of supersingular elliptic curves without using the complex multiplication of its endomorphism ring; later we will use the complex multiplication as well.
For the first part we use recursive doubling of points similar to the primality test algorithm proposed by B.H. Gross for Mersenne primes, but now for certain integers of the form $m2^n - 1$.
Additionally we will extend a test presented by Denomme and Savin in [DS08] from Fermat numbers to integers of the form $p^2 16^n + 1$ where $p \equiv \pm 1 \bmod 10$ and $p < 4^n$. The idea behind the test by Denomme and Savin is to use an endomorphism of degree 2 arising from the complex multiplication of an elliptic curve E of j-invariant 1728, namely $(1 + i) \in \mathrm{End}(E)$. Their method is to recursively apply this map on a specific point to prove that a Fermat number is prime using the same principle given by Theorem 4.1.2. They use

the $\mathbb{Z}[i]$-module structure of the elliptic curve E obtained by the action of $\mathbb{Z}[i]$ on the Abelian group given by the rational points of the elliptic curve E.

4.2.1 Primality testing with supersingular elliptic curves

In this subsection we provide a family of elliptic curves that will lead to primality tests for certain integers of the form $\mathcal{A}_{m,n} := m2^n - 1$. The following proposition is a key part for the design of a primality test algorithm of $\mathcal{A}_{m,n}$.

Proposition 4.2.1. *Let $p > 3$ be a prime number such that $p \equiv 3 \bmod 4$ and $t \in \mathbb{F}_p$. The equation $y^2 = x^3 - (t^2+1)x = f_t(x)$ over $\mathbb{F}_p$ defines a supersingular elliptic curve $E_t/\mathbb{F}_p$ and the point $(-1, t)$ is not divisible by 2 in $E_t(\mathbb{F}_p)$.*

Proof. The first claim can be proved directly. First, since $p \equiv 3 \bmod 4$, we have that $t^2 \neq -1$ for all $t \in \mathbb{F}_p$. Hence E_t indeed defines an elliptic curve. The fact that it is supersingular is well known, compare [Sil86, V Example 4.5]. For convenience we provide an alternative argument. Let $w \in \{1, 3\}$ be the number of $\mathbb{F}_p$-rational zeros of $f_t(x)$ and let $x_0 \in \mathbb{F}_p$ be such that $f_t(x_0) \neq 0$. We have that $f_t(-x_0) = -f_t(x_0)$, hence using $p \equiv 3 \bmod 4$, one concludes $f_t(x_0)$ is a square over $\mathbb{F}_p$ if and only if $f_t(-x_0)$ is not a square over $\mathbb{F}_p$ (this is because $-1 \notin \mathbb{F}_p^2$). Hence, the number of points of $E_t(\mathbb{F}_p)$ is given by twice the aforementioned squares $f_t(x_i)$ for all $x_i \in \mathbb{F}_p$ such that $f_t(x_i) \neq 0$. The value $\#E_t(\mathbb{F}_p)$ is given by counting these x_i which are $\frac{p-w}{2} \cdot 2$ and adding the number of Weierstrass points given by $w + 1$. Hence $\#E_t(\mathbb{F}_p) = p + 1$ for all $t \in \mathbb{F}_p$ and $E_t/\mathbb{F}_p$ is supersingular.

To prove that $(-1, t)$ is not divisible by two, in other words that there is no $Q \in E_t(\mathbb{F}_p)$ such that $2Q = (-1, t)$, consider the multiplication- by-2 map given by $2 \in \mathrm{End}_{\mathbb{F}_p}(E)$. It is equivalent to show that $(-1, t) \notin 2E_t(\mathbb{F}_p)$. The 2-descent homomorphism δ (see [Sil86] Chapter X, §4 Prop. 4.9 for details) is useful here since $\mathrm{Ker}(\delta) = 2E_t(\mathbb{F}_p)$. We proceed to construct δ for $E_t(\mathbb{F}_p)$ and apply it to $(-1, t)$. This construction will be done in two cases depending on $t^2 + 1$ being a square or not in $\mathbb{F}_p$.

Let $t^2 + 1 \notin \mathbb{F}_p^2$ and consider the ring $\mathfrak{R}_t := \mathbb{F}_p[X]/(f_t(X))$. Since $t^2 + 1$ is not a square, $f_t(X)$ defines only one affine $\mathbb{F}_p$-rational Weierstrass point in $E_t(\mathbb{F}_p)$, namely $(0, 0)$. Hence $\mathfrak{R}_t \cong \mathbb{F}_p \times \mathbb{F}_p[\xi]/(\xi^2 - (t^2+1))$. Let $P := (\alpha, \beta) \in E_t(\mathbb{F}_p)$. Since $X \in \mathfrak{R}_t$ satisfies the equation $f_t(X) = 0$, the 2-descent homomorphism of $E_t(\mathbb{F}_p)$ in this case is given by:

$$\begin{aligned}\delta : E_t(\mathbb{F}_p) &\to \mathfrak{R}_t^\times/\mathfrak{R}_t^{\times 2}\\ P &\mapsto \begin{cases} 1 & \text{if } P = \infty\\ [-(t^2+1) - X] & \text{if } P = (0,0)\\ [\alpha - X] & \text{otherwise,}\end{cases}\end{aligned} \tag{4.2}$$

compare [ST15, § 3.5].
Since $\mathrm{Ker}(\delta) = 2E_t(\mathbb{F}_q)$ we have that $(-1,t)$ is divisible by 2 if and only if $-1 - X$ is in $\mathfrak{R}_t^{\times 2}$. However it is not a square since its image -1 in $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ is nontrivial.

The other case is when $\lambda^2 = t^2 + 1 \in \mathbb{F}_p^2$, hence $f_t(X)$ splits in $\mathbb{F}_p[X]$ and $\mathfrak{R}_t \cong \mathbb{F}_p[X]/(X) \times \mathbb{F}_p[X]/(X+\lambda) \times \mathbb{F}_p[X]/(X-\lambda) \cong \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$. The 2-descent map $\delta : E_t(\mathbb{F}_p) \to \mathfrak{R}_t^\times/\mathfrak{R}_t^{\times 2}$ in this case applied to $(-1,t)$ again yields in the first factor -1 which is nontrivial. This shows that $(-1,t) \notin 2E_t(\mathbb{F}_p)$ in all cases. □

Now we need to know when E_t is cyclic, this will depend on the base field of E_t. This is important in order to establish for which integers our primality testing algorithm will be useful.

Lemma 4.2.2. *Let $p \equiv 3 \bmod 4$ be prime and $t \in \mathbb{F}_p$ such that $t^2 + 1 \notin ({\mathbb{F}_p}^\times)^2$. Consider the elliptic curve E_t given by $y^2 = x^3 - (t^2+1)x$, then $E_t(\mathbb{F}_p)$ is cyclic.*

Proof. Consider the multiplication by $p+1$ map, that is $p{+}1 \in \mathrm{End}(E_t)$. We have that $\mathrm{Ker}(p{+}1) = E_t(\overline{\mathbb{F}}_p)[p{+}1] \cong \mathbb{Z}/(p{+}1)\mathbb{Z}\times\mathbb{Z}/(p{+}1)\mathbb{Z}$. By Proposition 4.2.1 $\#E_t(\mathbb{F}_p) = p{+}1$, hence $E_t(\mathbb{F}_p) \leq E_t(\overline{\mathbb{F}}_p)[p{+}1]$. With this, for $1 \leq \alpha \leq \beta$ we have that $E_t(\mathbb{F}_p) \cong \mathbb{Z}/\alpha\mathbb{Z} \times \mathbb{Z}/\beta\mathbb{Z}$ such that $\alpha \mid \beta$ and $\alpha \cdot \beta = p + 1$.
Now we show that $\alpha \mid p - 1$.
We look at the $\alpha-$torsion. We have that $\mathbb{Z}/\alpha\mathbb{Z} \times \mathbb{Z}/\alpha\mathbb{Z} \leq \mathbb{Z}/\alpha\mathbb{Z} \times \mathbb{Z}/\beta\mathbb{Z} \cong E_t(\mathbb{F}_p)$, this means that $E_t(\mathbb{F}_p) \supset \mathrm{Ker}(\alpha)$. Using the surjectivity of the Weil pairing (see [Sil86], III, Corollary 8.1.1) there must be $P, Q \in E_t(\mathbb{F}_p)$ with $(P,Q) = \omega_\alpha$ where $\omega_\alpha \in \overline{\mathbb{F}}_p$ is a α^{th} root of unity. Using the fact that the Weil pairing is Galois invariant (see [Sil86],III, Proposition 8.1), for any $\sigma \in \mathrm{Gal}(\mathbb{F}_p(\omega_\alpha)/\mathbb{F}_p)$ we have that $(P^\sigma, Q^\sigma) = (P,Q)^\sigma$, hence ω_α is invariant under σ. This means that $\omega_\alpha \in \mathbb{F}_p^\times$, which implies that $\alpha \mid \#\mathbb{F}_p^\times$ hence $\alpha \mid p{-}1$. Now we have that $\alpha \mid p + 1$ and $\alpha \mid p - 1$ hence $\alpha \mid 2$. This means that if $\alpha = 2$ then $E_t(\mathbb{F}_p)$ has full two-torsion. But this is not the case since $t^2 + 1$ is not a square and $p \equiv 3$ mod 4. Hence $\alpha = 1$ and $E_t(\mathbb{F}_p)$ is cyclic. □

Corollary 4.2.3. *Let $m \geq 1$ be an odd integer and suppose that $\mathcal{A}_{m,n} := m2^n - 1$ is prime with $n > 1$. Take $t \in \mathbb{F}_{\mathcal{A}_{m,n}}$ such that $t^2 + 1$ is not a square and consider the elliptic curve $E_t/\mathbb{F}_{\mathcal{A}_{m,n}}$. Then the point $m(-1, t)$ generates the 2-Sylow subgroup of $E_t(\mathbb{F}_{\mathcal{A}_{m,n}})$.*

Proof. Since $n > 1$ we have that $\mathcal{A}_{m,n} \equiv 3 \bmod 4$. Using Lemma 4.2.2 and $t^2 + 1 \notin {\mathbb{F}_{\mathcal{A}_{m,n}}}^2$, the group $E_t(\mathbb{F}_{\mathcal{A}_{m,n}})$ is cyclic and has $m2^n$ points. By Proposition 4.2.1 the point $(-1, t)$ is not divisible by 2 and since m is odd, $m(-1, t)$ has order 2^n. □

The following simple lemma will be used to discard some trivial small divisors of $\mathcal{A}_{m,n}$ for every $n > 0$ and $m > 2$. This lemma will make the proof of the main Theorem of this section shorter.

Lemma 4.2.4. *The number $\mathcal{A}_{m,n} = m2^n - 1$ is divisible by 3 if and only if one of the following conditions holds:*

- $m \equiv 2 \bmod 3$ *and* $n \equiv 1 \bmod 2$*;*
- $m \equiv 1 \bmod 3$ *and* $n \equiv 0 \bmod 2$.

Further, $\mathcal{A}_{m,n} = m2^n - 1$ is divisible by 5 if and only if one of the following conditions holds:

- $m \equiv 1 \bmod 5$ *and* $n \equiv 0 \bmod 4$*;*
- $m \equiv 2 \bmod 5$ *and* $n \equiv 3 \bmod 4$*;*
- $m \equiv 3 \bmod 5$ *and* $n \equiv 1 \bmod 4$*;*
- $m \equiv 4 \bmod 5$ *and* $n \equiv 2 \bmod 4$.

Proof. This is clear analyzing the period of 2^n mod 3 and mod 5. □

With this we are ready to formulate the statement that will lead us to a primality testing algorithm for $\mathcal{A}_{m,n}$.

Theorem 4.2.5. *Let $m \geq 1$ be odd and $n > 1$ be such that $\mathcal{A}_{m,n} := m2^n - 1$ is not divisible by 3 or 5 (see Lemma 4.2.4) and $4m < 2^n$. Consider $t \in \mathbb{Z}$ such that the Jacobi symbol $\left(\frac{t^2+1}{\mathcal{A}_{m,n}}\right) = -1$. Take $(\frac{\alpha}{\beta}, \frac{\gamma}{\delta}) := m(-1, t) \in E_t(\mathbb{Q})$ and define the sequence:*

$$x_0 := \tfrac{\alpha}{\beta}, \quad x_{i+1} := \tfrac{(x_i^2 + t^2 + 1)^2}{4(x_i^3 - (t^2+1)x_i)} \mod \mathcal{A}_{m,n}.$$

Then $\mathcal{A}_{m,n}$ is prime if and only if x_i is well defined for every $0 \leq i \leq n - 1$ and $x_{n-1} \equiv 0 \bmod \mathcal{A}_{m,n}$.

Proof. Suppose that $\mathcal{A}_{m,n}$ is prime. Observe that x_i equals the x-coordinate of the point $m2^i(-1,t) \in E_t(\mathbb{F}_{\mathcal{A}_{m,n}})$. Since $2^n > 4m$ we have that $n > 2$, hence $\mathcal{A}_{m,n} \equiv 3 \bmod 4$. By Lemma 4.2.2 using that $t^2+1 \notin \mathbb{F}^2_{\mathcal{A}_{m,n}}$ we have that $E_t(\mathbb{F}_{\mathcal{A}_{m,n}})$ is cyclic. By Corollary 4.2.1, the point $(-1,t)$ is not divisible by 2 and $\#E_t(\mathbb{F}_{\mathcal{A}_{m,n}}) = m2^n$, hence since m is odd $m(-1,t)$ has order 2^n by Corollary 4.2.3. This means that $x_{n-1} = x(2^{n-1}(\frac{\alpha}{\beta},\frac{\gamma}{\delta}))$ equals the x-coordinate of the unique $\mathbb{F}_{\mathcal{A}_{m,n}}$-rational point of order 2 in $E_t(\mathbb{F}_{\mathcal{A}_{m,n}})$, namely $(0,0)$. The fact that x_i is well defined for $0 \leq i \leq n-1$ also follows from the reasoning above.

For the converse suppose that $\mathcal{A}_{m,n}$ is not prime. Also suppose that the x_i modulo $\mathcal{A}_{m,n}$ are well defined for $0 \leq i \leq n-1$ and that $x_{n-1} \equiv 0 \bmod \mathcal{A}_{m,n}$. Take $\ell \mid \mathcal{A}_{m,n}$ the smallest prime divisor of $\mathcal{A}_{m,n}$. Since $\left(\frac{t^2+1}{\mathcal{A}_{m,n}}\right) = -1$, it follows that $t^2+1 \neq 0$ in $\mathbb{F}_\ell$. Moreover ℓ is odd hence E_t defines an elliptic curve over $\mathbb{F}_\ell$.

With this we have that the point $2^{n-1}m(-1,t) \in E_t(\mathbb{F}_\ell)$ has x-coordinate 0 by assumption, so this point equals $(0,0)$ which has order 2. Hence $m(-1,t) \in E_t(\mathbb{F}_\ell)$ has order 2^n. Since $\mathcal{A}_{m,n}$ is not divisible by 3 or 5 we have that $\ell > 5$. Further $\ell \leq \sqrt{\mathcal{A}_{m,n}}$ and $m(-1,t)$ generates a subgroup of order 2^n in $E_t(\mathbb{F}_\ell)$. Furthermore by the Hasse inequality and the fact that $\ell > 5$ we have $\#E_t(\mathbb{F}_\ell) \leq (\sqrt{\ell}+1)^2 < 2\ell$, hence:

$$2^n \leq \#E_t(\mathbb{F}_\ell) < 2\ell \leq 2\sqrt{\mathcal{A}_{m,n}} = 2\sqrt{m2^n-1}.$$

Since $4m < 2^n$ it follows that $4^n \leq 4m2^n - 4 < 2^{2n} - 4 = 4^n - 4$ which is absurd. This contradiction shows that $\mathcal{A}_{m,n}$ must be prime. □

The algorithm in the previous theorem uses the recursive iteration of a degree 4 map (multiplication by 2). In the next section we will define a primality test for other integers using a map of degree 2.

4.2.2 Example: Finding primes via the elliptic supersingular method

We show an example algorithm for $\mathcal{A}_{13,n}$ using Theorem 4.2.5.

First note that $\mathcal{A}_{13,n}$ is divisible by 3 or 5 when $n \equiv 0,1,2 \bmod 4$ by Lemma 4.2.6. Hence, the only non-trivial case to do a primality test is with the integers $13 \cdot 2^{4k+3} - 1$. To apply the previous theorem we need that $4m = 4 \cdot 13 < 2^n = 2^{4k+3}$, which indeed holds for every $k \geq 1$.

Now we need to choose our elliptic curve E_t according to Lemma 4.2.2, so we need a $t \in \mathbb{Z}$ such that $\left(\frac{t^2+1}{\mathcal{A}_{13,4k+3}}\right) = -1$. We state the following technical result as a lemma for this example:

Lemma 4.2.6. *Let $\mathcal{A}_{m,n} := m2^n - 1$ be an integer, $m \geq 1$ and $n > 1$ such that one of the following conditions on m and n hold:*

(i) $m \equiv 1 \bmod 5$ *and* $n \equiv 3$ *or* $2 \bmod 4$

(ii) $m \equiv 2 \bmod 5$ *and* $n \equiv 2$ *or* $1 \bmod 4$

(iii) $m \equiv 3 \bmod 5$ *and* $n \equiv 0$ *or* $3 \bmod 4$

(iv) $m \equiv 4 \bmod 5$ *and* $n \equiv 1$ *or* $0 \bmod 4$

Then $\mathcal{A}_{m,n} \equiv \pm 2 \bmod 5$ and therefore 5 is not a square modulo $\mathcal{A}_{m,n}$.

Proof. This is a direct calculation using the period of 2^n modulo 5. □

The above Lemma 4.2.6 part (iii) allows us to use the curve E_t for $t = 2$ to check precisely $\mathcal{A}_{13,4k+3}$ since $m = 13 \equiv 3 \bmod 5$, hence $t^2 + 1 = 5$ is not a square modulo $\mathcal{A}_{13,4k+3}$, for every $k \in \mathbb{N}$.
With this, consider the curve E_2 given by $y^2 = x^3 - 5x$.
The x-coordinate of the point $13(-1, 2) \in E_2(\mathbb{Q})$ can be computed instantly with a computer algebra software and is given by:

$$x_0 = -\frac{38867230505264472384304448711791072932034380121}{20648248720215880190543854206835397627372795209}.$$

A computer program can be easily implemented to check the primality of $\mathcal{A}_{13,4k+3}$ returning "composite" when the denominator of x_j for $0 \leq j \leq 4k + 2$ is not a unit modulo $\mathcal{A}_{13,4k+3}$ and returning "prime" when $x_{4k+2} \equiv 0 \bmod \mathcal{A}_{13,4k+3}$. A similar analysis can be done using these results for other sequences $\mathcal{A}_{m,n}$.

4.2.3 Primality testing using CM by $\mathbb{Z}[i]$ on elliptic curves

Now we propose a primality test for integers of the form $\mathcal{S}_{p,n} := p^2 16^n + 1$ with $p \equiv \pm 1 \bmod 10$ prime and $p < 2^n$. For the iteration step in the primality test we will use an endomorphism of an elliptic curve E with j-invariant 1728. The resulting algorithm is similar to the one in the previous section but now using a degree 2 endomorphism which is computationally better.

We chose these integers since $p^2 16^n + 1$ is prime in $\mathbb{Z}$ if and only if its Gaussian factor $p4^n + i$ (and its conjugate of course) is prime in $\mathbb{Z}[i]$. We did not choose $p^2 4^n + 1$ since this integer is divisible by 5 for n odd.

For the integers $\mathcal{S}_{p,n}$, it is not immediate how to adapt a primality test as proposed in the previous section.
In the previous section we implicitly used the $\mathbb{Z}$-module structure of the elliptic curve E_t, that is, we used the action of $\mathbb{Z} \subset \operatorname{End}(E_t)$ on E_t. Here we will use the action of $\mathbb{Z}[i]$ on E for our primality testing purposes.

Let $p \equiv 1 \bmod 4$ and consider the elliptic curve $E/\mathbb{F}_p$ given by $y^2 = x^3 - x$. Take $\xi \in \mathbb{F}_p$ such that $\xi^2 = -1$. The action of $i \in \mathbb{Z}[i]$ on $E(\mathbb{F}_p)$ is defined as the "multiplication by i" map:

$$\begin{aligned} i \colon E(\mathbb{F}_p) &\to E(\mathbb{F}_p), \\ (x, y) &\mapsto (-x, \xi y). \end{aligned} \tag{4.3}$$

The map i is clearly an element of $\operatorname{Aut}(E) \subset \operatorname{End}(E)$ and $E(\mathbb{F}_p)$ obtains the structure of $\mathbb{Z}[i]$-module using the ring homomorphism

$$\begin{aligned} \mathbb{Z}[i] &\to \operatorname{End}(E) \\ a + bi &\mapsto a{+}b{\circ}i. \end{aligned} \tag{4.4}$$

We will use the next theorem for the rest of this section. It has an interesting history related to the last entry in Gauß' *Tagebuch* (July 7^{th}, 1814), discovered by Felix Klein in 1897 and published in *Math. Annalen 1903* [Kle03]. Gauß conjectured a way of calculating the number of points over $\mathbb{F}_p$ of a curve birational to the elliptic curve with j-invariant 1728 where $p \equiv 1 \bmod 4$. Gustav Herglotz was the first to prove Gauß's conjecture in 1921. Here we show another elementary proof using modern language (first proved in [Her21] and more general in [Kob12] and [Ire90]). The subsequent corollary is precisely the conjecture predicted by Gauß.
For the rest of this text we will denote the composition of endomorphisms as $ab := a \circ b$ using the previously defined homomorphism in (4.4).

Theorem 4.2.7. *Let $p \equiv 1 \bmod 4$ be a prime and let $E/\mathbb{F}_p$ be given by $y^2 = x^3 - x$. Consider the p^{th} Frobenius endomorphism ϕ_p and the identity map $\mathbb{1}$. We have that* $\operatorname{End}(E) = \mathbb{Z}[i]$ *and $\phi_p = a + bi \in \operatorname{End}(E)$ satisfies $a^2 + b^2 = p$ and $(2 + 2i) \mid \big(\phi_p - \mathbb{1}\big)$.*

Proof. We already saw that $\mathbb{Z}[i] \subseteq \operatorname{End}(E)$. Since $p \not\equiv 3 \bmod 4$ we have that E is not supersingular (see Proposition 4.2.1 and take $t = 0$), hence $\operatorname{End}(E)$ is contained in the ring of integers of an imaginary quadratic field and then

$\mathrm{End}(E) = \mathbb{Z}[i]$. Moreover $p = \deg(\phi_p) = a^2 + b^2$.

Note that $2 + 2i \in \mathrm{End}(E)$ is a separable map since $p \nmid \deg(2 + 2i) = 8$. We proceed to analyze its kernel since $2 + 2i \mid \phi_p - \mathbb{1}$ if and only if $\mathrm{Ker}(2 + 2i) \subset \mathrm{Ker}(\phi_p - \mathbb{1}) = E(\mathbb{F}_p)$.
Let $P \in E(\mathbb{F}_p)$, we have that $(2 + 2i)P = (1 + i)2P$, hence, if $Q \in \mathrm{Ker}(1 + i)$ is non-trivial, we have that:

$$\mathrm{Ker}(2 + 2i) = E[2](\mathbb{F}_p) \cup [2]^{-1}(Q)$$

Note that $Q = (0, 0)$ generates $\mathrm{Ker}(1 + i) \subset E(\mathbb{F}_p)$. Computing the tangent lines to $E/\mathbb{F}_p$ that contain Q, one obtains:

$$[2]^{-1}(Q) = \{(\xi, \pm(1 - \xi)), (-\xi, \pm(1 + \xi))\}.$$

Since $p \equiv 1 \bmod 4$ we have that $\xi \in \mathbb{F}_p$ and the four points in $[2]^{-1}(Q)$ are fixed by ϕ_p. Trivially the other four points $\{(0, 0), (1, 0), (-1, 0), \infty\}$ in $\mathrm{Ker}(2 + 2i)$ are fixed by ϕ_p, hence $\mathrm{Ker}(2 + 2i) \subset \mathrm{Ker}(\phi_p - \mathbb{1})$ and the result follows. □

This theorem gives a lot of information of the Frobenius endomorphism of E and the precise answer to Gauß' last entry in his *Tagebuch* which we will use soon.

Corollary 4.2.8. *Let $p \equiv 1 \bmod 4$ and consider the elliptic curve $E/\mathbb{F}_p$ given by $y^2 = x^3 - x$, then $\#E(\mathbb{F}_p) = p + 1 - 2\alpha$ where $p = \alpha^2 + \beta^2$ and if $p \equiv 1 \bmod 8$ then $\alpha \equiv 1 \bmod 4$, otherwise $\alpha \equiv 3 \bmod 4$.*

Proof. We have that $\#E(\mathbb{F}_p) = \deg(\phi_p - \mathbb{1}) = \deg(\alpha + \beta i - 1)$, hence

$$\#E(\mathbb{F}_p) = \alpha^2 + \beta^2 + 1 - 2\alpha = p + 1 - 2\alpha.$$

Theorem 4.2.7 shows $2 + 2i \mid \alpha - 1 + \beta i$, hence α is odd and β is even. Further we have that $8 \mid \#\mathrm{Ker}(\phi_p - \mathbb{1}) = \deg(\phi_p - \mathbb{1}) = (\alpha - 1)^2 + \beta^2$ since $\mathrm{Ker}(2 + 2i) \subset \mathrm{Ker}(\phi_p - \mathbb{1}) = E(\mathbb{F}_p)$ by the same theorem.
With this, since $\alpha^2 + \beta^2 = p$ we have that

$$p + 1 - 2\alpha \equiv 0 \bmod 8. \tag{4.5}$$

This implies the result. □

We illustrate the corollary with the following example.
Consider the elliptic curve $E/\mathbb{F}_{37}$ given by $y^2 = x^3 - x$. We have that $37 \equiv 5 \bmod 8$. By the previous corollary, $37 = \alpha^2 + \beta^2$, $\alpha \equiv 3 \bmod 4$ and

β even, hence $\alpha^2 + \beta^2 = 1 + 36$, $\alpha = -1$, and $\#E(\mathbb{F}_{37}) = 37 + 1 - 2(-1) = 40$.

The following proposition will be used to tell us the structure of $E(\mathbb{F}_{\mathcal{S}_{p,n}})$ as an abstract group, given that $\mathcal{S}_{p,n}$ is prime.

Proposition 4.2.9. *Let p be a prime such that $p \equiv 1 \bmod 8$ and $p - 1$ is a square. Consider the elliptic curve $E : y^2 = x^3 - x$, then $p = (\alpha - i)(\alpha + i)$ in $\mathbb{Z}[i]$, $\#E(\mathbb{F}_p) = \alpha^2$ and $E(\mathbb{F}_p) \cong \mathbb{Z}/(\alpha) \times \mathbb{Z}/(\alpha)$ as Abelian groups.*

Proof. We have that $p - 1 = \alpha^2$ for some $\alpha \in \mathbb{Z}$, hence $p = (\alpha + i)(\alpha - i)$ in $\mathbb{Z}[i]$. Using Theorem 4.2.7, since $p \equiv 1 \bmod 8$ we have that $\#E(\mathbb{F}_p) = p + 1 - 2 = \alpha^2$.

Let $\phi_p \in \mathrm{End}(E) = \mathbb{Z}[i]$ be the p^{th} power of Frobenius. The previous calculation shows that $\mathrm{Tr}(\phi_p) = 2$. Further $\deg \phi_p = p = \alpha^2 + 1 = (\alpha + i)(\alpha - i)$, hence (after possibly changing the sign of α) the Frobenius endomorphism is given by $\phi_p = \alpha i + 1$. With this, if $P \in E(\mathbb{F}_p)$ we have that $P = \phi_p(P) = (\alpha i + 1)(P)$. Hence $\alpha P = \infty$ and $P \in E[\alpha] \cong \mathbb{Z}/(\alpha) \times \mathbb{Z}/(\alpha)$. Since $\#E(\mathbb{F}_p) = \alpha^2$ we conclude that $E(\mathbb{F}_p) \cong \mathbb{Z}/(\alpha) \times \mathbb{Z}/(\alpha)$. □

Now we present two corollaries that describe particular properties of the group $E(\mathbb{F}_{\mathcal{S}_{p,n}})$ (again, provided $\mathcal{S}_{p,n}$ is prime). These corollaries will be used to extend the structure of $E(\mathbb{F}_{\mathcal{S}_{p,n}})$ to a cyclic $\mathbb{Z}[i]$-module in the subsequent proposition.

Corollary 4.2.10. *Let $\mathcal{S}_{p,n} := p^2 16^n + 1$ be prime and $n > 0$. Consider the elliptic curve $E/\mathbb{F}_{\mathcal{S}_{p,n}}$ given by $y^2 = x^3 - x$, then $\#E(\mathbb{F}_{\mathcal{S}_{p,n}}) = p^2 16^n$.*

Proof. Immediate from Proposition 4.2.9. □

Corollary 4.2.11. *Let $\mathcal{S}_{p,n} := p^2 16^n + 1$ be prime with p odd and $n > 0$. Consider the elliptic curve $E : y^2 = x^3 - x$, then $E(\mathbb{F}_{\mathcal{S}_{p,n}})$ has full p-torsion, that is $E[p] \subset E(\mathbb{F}_{\mathcal{S}_{p,n}})$.*

Proof. Again, this is a direct consequence of Proposition 4.2.9. □

The next proposition provides the group $pE(\mathbb{F}_{\mathcal{S}_{p,n}})$ with the structure of a cyclic $\mathbb{Z}[i]$-module.

Proposition 4.2.12. *Let $\mathcal{S}_{p,n} := p^2 16^n + 1$ be prime such that p is odd and $n > 0$. Consider the elliptic curve $E/\mathbb{F}_{\mathcal{S}_{p,n}}$ given by $y^2 = x^3 - x$, then $pE(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong \mathbb{Z}[i]/(1 + i)^{4n})$ as cyclic $\mathbb{Z}[i]$-modules.*

Proof. Since $n > 0$ we know by Lemma 4.2.10 that $\#pE(\mathbb{F}_{\mathcal{S}_{p,n}}) = 16^n$ and $pE(\mathbb{F}_{\mathcal{S}_{p,n}})$ is a finitely generated $\mathrm{End}(E)$-module with $\mathrm{End}(E) = \mathbb{Z}[i]$. Further, $\mathbb{Z}[i]$ is a PID and by the structure theorem for finitely generated modules over a PID there exists a finite sequence of ideals $(1) \neq (z_1) \supseteq (z_2) \supseteq \ldots \supseteq (z_t)$ of $\mathbb{Z}[i]$, for some $t \in \mathbb{N}$, such that

$$pE(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong \mathbb{Z}[i]/(z_1) \oplus \mathbb{Z}[i]/(z_2) \oplus \ldots \oplus \mathbb{Z}[i]/(z_t). \tag{4.6}$$

This sequence of ideals implies that $z_1 \mid z_2 \mid \ldots \mid z_t$. Let $\mathcal{N}\colon \mathbb{Z}[i] \to \mathbb{Z}$ be the norm map. Each direct summand has cardinality $\mathcal{N}(z_j) = z_j\bar{z_j}$ and $\mathcal{N}(z_j) \mid 16^n$. Thus for every j one concludes $\mathcal{N}(z_j) = 2^{m_j}$ for some power $m_j > 0$. Hence $(z_j) = ((1+i)^{m_j}) \subset \mathbb{Z}[i]$. This implies, using $m_j > 0$ for all j, that the $1+i$-torsion in $\bigoplus \mathbb{Z}[i]/(z_j)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^t$.
Note that $\deg(1+i) = 2$, hence $t = 1$ and $pE(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong \mathbb{Z}[i]/((1+i)^{4n})$, proving the result. □

Now we know that if $\mathcal{S}_{p,n}$ is prime, $pE(\mathbb{F}_{\mathcal{S}_{p,n}})$ is a cyclic $\mathbb{Z}[i]$-module. We need a generator of this $\mathbb{Z}[i]$-module to apply ideas as used in the previous sections. Similarly to [DS08], we use the quadratic twist of E given by the curve E_{30} : $30y^2 = x^3 - x$, but now we will do a primality test on $\mathcal{S}_{p,n}$ instead of Fermat numbers. Assuming $\mathcal{S}_{p,n}$ is prime, the curve E_{30} is isomorphic to $E : y^3 = x^3 - x$ over $\mathbb{F}_{\mathcal{S}_{p,n}}$ if and only if $\left(\frac{30}{\mathcal{S}_{p,n}}\right) = 1$. The following simple lemma will tell us for which p the element 30 is a square in $\mathbb{F}_{\mathcal{S}_{p,m}}$.

Lemma 4.2.13. *Let* $p \equiv \pm 1 \bmod 10$ *and* $\mathcal{S}_{p,n} := p^2 16^n + 1$ *be prime, then* $E_{30}(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong E(\mathbb{F}_{\mathcal{S}_{p,n}})$

Proof. We have to show that 30 is a square modulo $\mathcal{S}_{p,n}$. This is a direct application of the properties of the Legendre symbol, using that $\mathcal{S}_{p,n} \equiv 2 \bmod 5$ and $\mathcal{S}_{p,n} \equiv 2 \bmod 3$ and $\mathcal{S}_{p,n} \equiv 1 \bmod 8$; these properties imply

$$\left(\frac{30}{\mathcal{S}_{p,n}}\right) = \left(\frac{5}{\mathcal{S}_{p,n}}\right)\left(\frac{3}{\mathcal{S}_{p,n}}\right)\left(\frac{2}{\mathcal{S}_{p,n}}\right) = (-1)(-1)(1) = 1. \tag{4.7}$$

□

The curve E_{30} was chosen since the point $p(5,2)$ turns out to be a generator of the cyclic $\mathbb{Z}[i]$-module $pE_{30}(\mathbb{F}_{\mathcal{S}_{p,n}})$. We proceed to prove this.

Lemma 4.2.14. *Let* $p \equiv \pm 1 \bmod 10$ *be prime and consider* $Q := p(5,2) \in pE_{30}(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong \mathbb{Z}[i]/((1+i)^{4n})$. *The point* Q *generates the* $\mathbb{Z}[i]$*-submodule* $\mathbb{Z}[i]/((1+i)^{4n})$ *of* $E_{30}(\mathbb{F}_{\mathbb{F}_{\mathcal{S}p,n}})$

Proof. Since p is odd, we just need to show that $(5,2)$ is not in the image of $(1+i)$. This is the same as saying that $(1+i)(X,Y) = (X,Y) + (-X, \xi Y) = (5,2)$ has no $\mathbb{F}_{\mathcal{S}_{p,n}}$-rational solution.
We proceed to calculate $(1+i)(X,Y)$ explicitly. Consider the endomorphism $1+i \in \mathrm{End}(E_{30})$ where $E_{30} : 30y^2 = x^3 - x$. The slope between (X,Y) and $i(X,Y) = (-X, \xi Y)$ is $\lambda := \frac{(1-\xi)Y}{2X}$. A quick computation shows that

$$(1+i)(X,Y) = (30\lambda^2, \lambda(X - 30\lambda^2) - Y) = (\tfrac{\xi(1-X^2)}{2X}, -\tfrac{(1+\xi)(X^2+1)Y}{4X^2}). \tag{4.8}$$

We have that $(5,2) \in E_{30}(\mathbb{F}_{\mathcal{S}_{p,n}})$ is not in the image of $1+i \in \mathrm{End}(E_{30})$ (divisible by $1+i$) if and only if the solutions of the equations below for X and Y are not $\mathbb{F}_{\mathcal{S}_{p,n}}$-rational:

$$(1+i)(X,Y) = (30\lambda^2, \lambda(X - 30\lambda^2) - Y) = (5,2)$$

If we look at the equation $30\lambda^2 = 5$, it means that 5 must be a square modulo $\mathcal{S}_{p,n}$ since 30 is by Lemma 4.2.13. By the proof of that lemma we have that $\left(\frac{5}{\mathcal{S}_{p,n}}\right) = -1$ so there is no such $\mathbb{F}_{\mathcal{S}_{p,n}}$-rational point (X,Y), hence $(5,2)$ is not divisible by $1+i$. Therefore $p(5,2)$ generates $\mathbb{Z}[i]/((1+i)^{4n})$ and the generated submodule has cardinality $2^{4n} = 16^n$. □

Now we state the main theorem of this section. This theorem will lead us to a conclusive deterministic primality test algorithm for integers of the form $\mathcal{S}_{p,n} = p^2 16^n + 1$.

Theorem 4.2.15. *Consider the integer* $\mathcal{S}_{p,n} := p^2 16^n + 1$ *where* $p \equiv \pm 1 \bmod 10$ *is prime, and* $p < 2^n$. *Let* E_{30} *be the elliptic curve* $30y^2 = x^3 - x$ *and consider the point* $Q := p(5,2) \in E_{30}(\mathbb{Q}(i))$ *(which is a* $\mathbb{Z}[i]$*-module).*
Then $\mathcal{S}_{p,n}$ *is prime if and only if* $(1+i)^{4n-1}Q = (0,0) \bmod (p4^n + i)$.

Proof. Suppose that the congruence holds and $\mathcal{S}_{p,n}$ is not prime. Take $k \mid \mathcal{S}_{p,n}$ the smallest prime divisor of $\mathcal{S}_{p,n}$, hence $k \leq \sqrt{p^2 16^n + 1}$. Further we have that $p^2 16^n + 1 \equiv 0 \bmod k$ if and only if $(p4^n)^2 \equiv -1 \bmod k$. This means that -1 is a square in $\mathbb{F}_k$ and then $k = \pi\overline{\pi}$ with $\pi \in \mathbb{Z}[i]$ Gaussian prime.
Now, since $\pi \mid p^2 16^n + 1 = (p4^n + i)(p4^n - i)$ without loss of generality, assume that $\pi \mid p4^n + i$. Let $\mathcal{N}$ be the Gaussian norm. Since $\pi\overline{\pi} = k \leq \sqrt{\mathcal{S}_{p,n}}$ we have that:

$$\mathcal{N}(\pi) < \sqrt{\mathcal{N}(p4^n + i)} = \sqrt{\mathcal{S}_{p,n}} \tag{4.9}$$

Further, the discriminant of E_{30} is $(2^2 \cdot 3 \cdot 5)^2$ and it is easy to see that $p^2 16^n + 1$ is not divisible by $2, 3$ or 5. Hence, $E_{30}(\mathbb{Z}[i]/(\pi))$ defines an elliptic curve.

Furthermore, $(1+i)^{4n-1}Q \equiv (0,0) \bmod \pi$ in $E_{30}(\mathbb{Z}[i]/(\pi))$ if and only if $(1+i)^{4n}Q = \infty \bmod \pi$. This means that $Q = p(5,2)$ generates a $\mathbb{Z}[i]$-submodule of $E_{30}(\mathbb{Z}[i]/(\pi))$ of size 16^n. With this we get the following inequalities using the Hasse inequality and the inequality in (4.9):

$$16^n \leq \#E_{30}(\mathbb{Z}[i]/(\pi)) \leq (\sqrt{\mathcal{N}(\pi)}+1)^2 < (\sqrt[4]{\mathcal{S}_{p,n}}+1)^2. \tag{4.10}$$

This implies that $4^n - 1 < \sqrt[4]{p^2 16^n + 1}$ and then $\frac{(4^n-1)^4-1}{16^n} < p^2$. Since $p < 2^n$ by hypothesis this implies that $\frac{(4^n-1)^4-1}{16^n} < 4^n$, hence $0 \leq n < \varepsilon$ with $\varepsilon \approx 0.91 < 1$ which is absurd since $n \geq 1$. $\divideontimes$. We conclude that $\mathcal{S}_{p,n}$ is prime.

Suppose that $\mathcal{S}_{p,n}$ is prime, then Q generates $pE_{30}(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong \mathbb{Z}[i]/((1+i)^{4n})$ by Lemma 4.2.14. Further $(0,0)$ is the only non-trivial point in the $(1+i)$-torsion of $E_{30}(\mathbb{F}_{\mathcal{S}_{p,n}})$, hence $(1+i)^{4n-1}Q = (0,0) \bmod p4^n + i$ since $E_{30}(\mathbb{F}_{\mathcal{S}_{p,n}}) \cong E_{30}(\mathbb{Z}[i]/(p4^n+i))$. □

The same theorem can be stated as an algorithm.

Corollary 4.2.16. *Consider the integer* $\mathcal{S}_{p,n} := p^2 16^n + 1$ *such that* p *is prime,* $p \equiv \pm 1 \bmod 10$ *and* $p < 2^n$. *Let* $(x_0, y_0) := p(5,2) \in E_{30}(\mathbb{Q}(i))$ *and consider the sequence:*

$$x_{j+1} = \frac{i(1-x_j^2)}{2x_j} \quad \bmod p4^n + i$$

$\mathcal{S}_{p,n}$ *is prime if and only if* x_j *is well defined for all* $j < 4n$ *and* $x_{4n-1} \equiv 0 \bmod p4^n + i$

Proof. This is equivalent to Theorem 4.2.15. The sequence is the recursive multiplication by $(1+i)$ starting with the x coordinate of the point $p(5,2) \in E_{30}$. This formula was deduced in Equation (4.8). □

4.2.4 Example: Finding primes via the elliptic CM method

In order to implement the previous corollary as a primality test algorithm for $\mathcal{S}_{p,n}$, note that we can test these integers starting from $n > \frac{\log(p)}{\log(2)}$.
Consider the ring $\mathbb{Z}/(\mathcal{S}_{p,n})$. We have that $i := p \cdot 4^n$ and $i^2 = -1$ in $\mathbb{Z}/(\mathcal{S}_{p,n})$. Take the curve $E_{30} : 30y^2 = x^3 - x$. The curve $E' : y^2 = x^3 - 900x$ is isomorphic fo E_{30} under the change of variables $(x,y) \mapsto (30x, 900y)$. The initial value of the iteration is x_0 from $(x_0, y_0) = p(5,2)$. We calculate it in E' as $p(30 \cdot 5, 900 \cdot 2)$ and its x coordinate divided by 30 will be our x_0.
We show the primes $\mathcal{S}_{p,n} = p^2 16^n + 1$ with this technique where $p \equiv \pm 1 \bmod 10$, $p \leq 101$ and $\frac{\log p}{\log 2} < n \leq 2000$ using a GP/PARI implementation.

p	$\approx \frac{\log p}{\log 2}$	n values where $\mathcal{S}_{p,n} = p^2 16^n + 1$ is prime $\frac{\log p}{\log 2} < n \leq 2000$
11	3.45943	$11, 21, 24, 57, 66, 80, 183, 197, 452, 1982$
19	4.24792	$7, 9, 25, 78, 142, 646$
29	4.85798	$6, 19, 33, 36, 86, 103, 326, 352$
31	4.95419	$5, 65, 142, 148, 196, 1154$
41	5.35755	$12, 18, 48, 81, 113, 305, 620, 1098$
59	5.88264	$9, 19, 33, 46, 121, 264, 904, 1365, 1858$
61	5.93073	$11, 259, 361, 415, 427, 594$
71	6.14974	$12, 21, 33, 36, 49, 70, 82, 85, 91, 111, 114, 129, 147, 255$
79	6.30378	$13, 17, 19, 81, 375, 1027, 1562, 1785$
89	6.47573	$39, 41, 47, 65, 71, 99, 299, 909, 1901$
101	6.65821	$8, 202, 238, 1484$

4.3 Primality testing using real multiplication on hyperelliptic Jacobians of dimension 2

In this last part we identify primes of the form $\lambda_n := 4 \cdot 5^n - 1$ using the Jacobian of a hyperelliptic curve of genus 2. This will be done similarly to what was done in the previous section using complex multiplication on an elliptic curve.

This section is motivated by an open question stated by Abatzoglou, Silverberg, Sutherland and Wong in [ASSW16] (Remark 4.13) asking for a primality test algorithm using higher dimensional Abelian varieties such as Jacobians of genus 2 curves. We will use the Jacobian $\mathcal{J}$ of the hyperelliptic curve $y^2 = x^5 + h$ where $h \in \mathbb{Z}$ to partially answer this question. We begin with the structure of $\operatorname{End}(\mathcal{J})$.

Proposition 4.3.1. *Let $h \neq 0$ be an integer and $\mathcal{H} : y^2 = x^5 + h$ a hyperelliptic curve of genus 2 over $\mathbb{Q}$. Consider the Jacobian of $\mathcal{H}$ denoted by $\mathcal{J}$. We have that $\operatorname{End}(\mathcal{J}) = \mathbb{Z}[\zeta]$ where ζ is a primitive fifth root of unity.*

Proof. Let $\zeta^* \in \operatorname{Aut}(\mathcal{H})$ be the automorphism $\zeta^*(x_0, y_0) = (\zeta x_0, y_0) \in \mathcal{H}$ where ζ is a primitive fifth root of unity. The action of ζ^* on $\mathcal{H}$ is naturally extended to the Jacobian which implies that $\zeta^* \in \operatorname{End}(\mathcal{J})$. As ζ^* generates a subring $\cong \mathbb{Z}[\zeta] \subset \operatorname{End}(\mathcal{J})$ and $\mathcal{J}$ is a simple Abelian variety over $\overline{\mathbb{Q}}$ (see [CF96], Chapter 15) , and moreover $\mathbb{Z}[\zeta]$ is integrally closed, we have that $\operatorname{End}(\mathcal{J}) = \mathbb{Z}[\zeta]$. □

Remark: We will use $\mathcal{J}$ and End($\mathcal{J}$) to test whether $\lambda_n = 4 \cdot 5^n - 1$ is prime. Note that $3 \mid \lambda_{2k}$, so we will only test λ_n when n is odd.

Let λ_n be prime. We proceed to deduce the group structure of $\mathcal{J}(\mathbb{F}_{\lambda_n})$. First we state and prove two easy lemmas that will tell us the structure of $\mathcal{J}[2](\mathbb{F}_{\lambda_n})$.

Lemma 4.3.2. *Let $\mathcal{H}$ be the hyperelliptic curve given by $y^2 = x^5 + h$ and let $\lambda_n := 4 \cdot 5^n - 1$ be prime, then there is only one $\mathbb{F}_{\lambda_n}$-rational point in $\mathcal{H}$ of the form $(\alpha, 0)$ for some $\alpha \in \mathbb{F}_{\lambda_n}$*

Proof. This follows from Fermat's little theorem. We have that 5 and $\lambda_n - 1 = 2(2 \cdot 5^n - 1)$ are coprime, hence, the map $x \mapsto x^5$ is invertible over $\mathbb{F}_{\lambda_n}$, hence, $x^5 = -h$ has only one solution in $\mathbb{F}_{\lambda_n}$. □

We calculate explicitly the $\mathbb{F}_{\lambda_n}$-rational zero α of $x^5 + h \in \mathbb{F}_{\lambda_n}[x]$ as follows: by the proof of the previous lemma it is easy to see that there is a $d \in \mathbb{Z}$ such that the map $x \mapsto (x^d)^5$ defined over $\mathbb{F}_{\lambda_n}$ is the identity map. By Fermat's little theorem, this d satisfies $5d \equiv 1 \bmod (\lambda_n - 1)$ and $\lambda_n - 1 = 4 \cdot 5^n - 2$. To calculate d, let $N = 2 \cdot 5^n - 1$ and consider $\lambda_n - 1 = 2N$. Using the Chinese Remainder Theorem we evaluate 5^{-1} with the isomorphism $\tau : \mathbb{Z}/2N\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, using the fact that $5^{-1} \equiv 2 \cdot 5^{n-1} \bmod N$ and 5 is odd. Hence, $\tau(5^{-1}) = (1, 2 \cdot 5^{n-1}) = (1, 0) + (0, 2 \cdot 5^{n-1})$ and therefore:

$$d = 5^{-1} = \tau^{-1}(1,0) + \tau^{-1}(0, 2 \cdot 5^{n-1}) = N + 2 \cdot 5^{n-1} = 12 \cdot 5^{n-1} - 1.$$

Using this we have that $x^{5d} = x$ in $\mathbb{F}_{\lambda_n}$, and particularly if:

$$\alpha = (-h)^d \tag{4.11}$$

we have that $\alpha^5 = -h$ in $\mathbb{F}_{\lambda_n}$.

Observe that the zeros of $x^5 + h$ are given by $\zeta^j \alpha$ for $0 \leq j \leq 4$ and ζ a fifth root of unity. Therefore by the previous lemma $\zeta \notin \mathbb{F}_{\lambda_n}$ and

$$\begin{aligned} x^5 + h &= \prod_{j=0}^{4} (x - \zeta^j \alpha) \\ &= (x - \alpha)(x^2 - \alpha(\zeta + \zeta^4)x + \alpha^2)(x^2 - \alpha(\zeta^2 + \zeta^3)x + \alpha^2). \end{aligned} \tag{4.12}$$

In order to deduce the structure of the 2-torsion of $\mathcal{J}$, the following lemma tells us the field extension of $\mathbb{F}_{\lambda_n}$ where ζ lives and this will give us directly the structure of the 2-torsion of $\mathcal{J}$. In fact, the following lemma implies that the Polynomial (4.12) is defined over $\mathbb{F}_{\lambda_n}[x]$.

Lemma 4.3.3. *Let $n > 0$ and suppose $\lambda_n := 4 \cdot 5^n - 1$ is prime. Consider the field $\mathbb{F}_{\lambda_n}$. Let ζ be a primitive fifth root of unity, then $\zeta \in \mathbb{F}_{\lambda_n^2}$ and $\zeta^{\lambda_n} = \zeta^{-1}$.*

Proof. This is immediate by observing that $\lambda_n^2 \equiv 1 \bmod 5$, using that the unit group of a finite field is cyclic. □

Observe that we can factorize explicitly $x^5 + h \in \mathbb{F}_{\lambda_n}[x]$ as follows: Note that over $\mathbb{Q}(\zeta)$ using the 5-th cyclotomic polynomial, $\zeta + \zeta^4 = \frac{-1+\sqrt{5}}{2}$ and $\zeta^2 + \zeta^3 = \frac{-1-\sqrt{5}}{2}$. Further, if λ_n is prime we know that n is odd and one can check easily that $\sqrt{5} \equiv 2 \cdot 5^{(n+1)/2} \bmod \lambda_n$. Furthermore, note that $\frac{1}{2} \equiv 2 \cdot 5^n \bmod \lambda_n$. Hence, using (4.12), the root α in (4.11), and the previous congruences, we obtain the explicit factorization of $x^5 + h \in \mathbb{F}_{\lambda_n}[x]$.

With this, we deduce easily the structure of $\mathcal{J}[2](\mathbb{F}_{\lambda_n})$ in the next corollary.

Corollary 4.3.4. *Let $n > 0$ and suppose λ_n is prime. Consider the hyperelliptic curve $\mathcal{H}/\mathbb{F}_{\lambda_n}$ given by $y^2 = x^5 + h$. Then $\mathcal{J}[2](\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.*

Proof. We know that $\mathcal{J}[2](\mathbb{F}_{\lambda_n}) \subset \mathcal{J}$ consists of divisor classes $D - 2\infty$ where D consists of pairs of Weierstrass points of $\mathcal{H}$ and D is fixed under the action of the absolute Galois group of $\mathbb{F}_{\lambda_n}$. By the previous discussion we know that all the Weierstrass points of $\mathcal{H}$ are of the form $(\zeta^j \alpha, 0)$ for $0 \leq j \leq 4$, with $\alpha \in \mathbb{F}_{\lambda_n}$ satisfying $\alpha^5 + h = 0$. Further, only two Weierstrass points are defined over $\mathbb{F}_{\lambda_n}$ by Lemma 4.3.2, namely $(\alpha, 0)$ and ∞. The other four lie in a quadratic extension of $\mathbb{F}_{\lambda_n}$ since ζ lies there by Lemma 4.3.3. Let $\rho_k := \zeta^k \alpha$ be a zero of $x^5 + h$, then Lemma 4.3.2 shows that the only conjugate of ρ_k is ρ_{-k} (if $5 \nmid k$). Hence there are two pairs of conjugate Weierstrass points plus two ordered pairs of $\mathbb{F}_{\lambda_n}$-rational Weierstrass points:

$$\mathcal{J}[2](\mathbb{F}_{\lambda_n}) = \{\{(\rho_1, 0), (\rho_4, 0)\}, \{(\rho_2, 0), (\rho_3, 0)\}, \{(\rho_0, 0), \infty\}, \{\infty, \infty\}\}$$

Therefore $\mathcal{J}[2](\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. □

Proposition 4.3.5. *Let $\mathcal{H}$ be the hyperelliptic curve given by $y^2 = x^5 + h$ and suppose $\lambda_n := 4 \cdot 5^n - 1$ is prime and $n > 0$. Then $\#\mathcal{J}(\mathbb{F}_{\lambda_n}) = 16 \cdot 5^{2n}$ and $\mathcal{J}(\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(\lambda_n + 1) \times \mathbb{Z}/(\lambda_n + 1) = \mathbb{Z}/(4 \cdot 5^n) \times \mathbb{Z}/(4 \cdot 5^n)$*

Proof. First we calculate the zeta function of $\mathcal{H}$. We refer to an old paper by Tate and Shafarevich [TS67] where they proved that the numerator of the zeta function of the curve $\mathcal{C}/\mathbb{F}_p$ given by $y^e = x^f + \delta$ can be described explicitly when $m = \operatorname{lcm}(e, f) | p^k + 1$ for some k. In our case $p = \lambda_n = 4 \cdot 5^n - 1$, $m = 10$ and $k = 1$. By [TS67] the numerator of the zeta-function of $\mathcal{H}/\mathbb{F}_{\lambda_n}$ is in this

case given by $\lambda_n^2 T^4 + 2\lambda_n T^2 + 1$ which tells us the characteristic polynomial $\chi_{\mathcal{J}}(T)$ of Frobenius of $\mathcal{J}$ equals $T^4 + 2\lambda_n T + \lambda_n^2 = (T^2 + \lambda_n)^2$. With this $\#\mathcal{J}(\mathbb{F}_{\lambda_n}) = \chi_{\mathcal{J}}(1) = 16 \cdot 5^{2n}$.
For the structure of $\mathcal{J}(\mathbb{F}_{\lambda_n})$, using that $\chi_{\mathcal{J}}(T) = (T^2 + \lambda_n)^2$ and $\lambda_n \equiv 3 \bmod 4$, by Theorem 3.2 (iii) in [Xin96], we have that $\mathcal{J}(\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(\frac{4 \cdot 5^n}{2^a}) \times \mathbb{Z}/(\frac{4 \cdot 5^n}{2^b}) \times \mathbb{Z}/(2^{a+b})$ with $0 \leq a, b \leq 2$. Further, by the previous Lemma 4.3.4, $\mathcal{J}[2](\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Hence $a = b = 0$ and $\mathcal{J}(\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(4 \cdot 5^n) \times \mathbb{Z}/(4 \cdot 5^n)$. □

Lemma 4.3.6. *Let $\mathcal{H}$ be the hyperelliptic curve $y^2 = x^5 + h$ and take $\lambda_n := 4 \cdot 5^n - 1$ prime. Then $\sqrt{5} \in \mathrm{End}_{\mathbb{F}_{\lambda_n}}(\mathcal{J})$*

Proof. By Proposition 4.3.1 we have that $\mathrm{End}(\mathcal{J}) = \mathbb{Z}[\zeta]$ with ζ a primitive fifth root of unity. Using the fifth cyclotomic polynomial we have that $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$. Consider $\rho := \zeta + \zeta^4$, then $\rho^2 = \zeta^3 + \zeta^2 + 2 = 1 - (\zeta + \zeta^4) = 1 - \rho$. With this we have that $\rho^2 + \rho = 1$ if and only if $4(\rho^2 + \rho) + 1 = 5$ if and only if $(2\rho + 1)^2 = 5$. With this $2(\zeta + \zeta^4) + 1$ is a square root of 5 in $\mathrm{End}(\mathcal{J})$. It is defined over $\mathbb{F}_{\lambda_n}$ since the Frobenius automorphism interchanges ζ and ζ^4 by Lemma 4.3.3. □

Proposition 4.3.7. *Suppose λ_n is prime and consider the hyperelliptic curve $\mathcal{H}/\mathbb{F}_{\lambda_n}$ given by $y^2 = x^5 + h$, then $4\mathcal{J}(\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}[\sqrt{5}]/(\sqrt{5}^{2n})$ as $\mathbb{Z}[\sqrt{5}]$-modules.*

Proof. By Proposition 4.3.5 we have $4\mathcal{J}(\mathbb{F}_{\lambda_n}) \cong \mathbb{Z}/(5^n) \times \mathbb{Z}/(5^n)$. This is a $\mathbb{Z}[\sqrt{5}]$ module with $\sqrt{5} \in \mathrm{End}_{\mathbb{F}_{\lambda_n}}(\mathcal{J})$ acting as $2(\zeta + \zeta^4) + 1$. Moreover $\sqrt{5}^{2n}$ acts trivially. Since $\mathbb{Z}[\sqrt{5}]/(5^n) \cong \mathbb{Z}/(5^n) \times \mathbb{Z}/(5^n)$, the module is necessarily cyclic since otherwise it would contain too many elements of order 5. □

4.3.1 Computation of $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$

We use the Mumford representation for elements of $\mathcal{J}$ and briefly recall this here. Details and proofs of correctness and uniqueness are given in classical texts such as [Mum84, Can87]. We fix our curve $\mathcal{H} : y^2 = x^5 + h$ and its Jacobian $\mathcal{J}$.
Any point in $\mathcal{J}$ is represented by a divisor $D - 2\infty$ on $\mathcal{H}$, with D a sum of two points. In case $D = (x_1, y_1) + (x_2, y_2)$, then define polynomials $u(x) = (x - x_1)(x - x_2)$ and $v(x)$ of degree ≤ 1 such that $v(x_i) = y_i$. Then

$$v(x)^2 \equiv x^5 + h \bmod u(x). \tag{4.13}$$

Note that the pair u, v determines the divisor D. In case $D = (x_1, y_1) + \infty$ put $u(x) = x - x_1$ and $v = y_1$, and if $D = 2\infty$ put $u = 1$ and $v = 0$. So in all cases the pair u, v determines D.

For the generic point $\mathfrak{g} := (x_1, y_1) + (x_2, y_2) - 2\infty \in \mathcal{J}$, the coefficients of $u(x) = x^2 - \alpha x + \beta$ and $v(x) = \gamma x + \delta$ are given by the symmetric functions $\alpha = x_1 + x_2, \beta = x_1 x_2, \gamma = \frac{y_1 - y_2}{x_1 - x_2}, \delta = \frac{x_2 y_1 - x_1 y_2}{x_1 - x_2}$. The congruence (4.13) yields defining equations for an affine part of $\mathcal{J}$ under this representation as we calculated in Chapter 2, Section 2.1.1 as the intersection of two hypersurfaces in $\mathbb{A}^4$.

With this representation, the points of $\mathcal{J}$ will be denoted by $\langle u(x), v(x) \rangle$. Cantor in [Can87] developed a useful algorithm to do arithmetic in $(\mathcal{J}, \oplus)$ using this representation; in fact as he explains, his method generalizes to every hyperelliptic Jacobian of genus g.

Now we show how to construct the $\sqrt{5}$ endomorphism acting on the generic point $\mathfrak{g} \in \mathcal{J}(\mathbb{Q}(\sqrt{5})) \subset \mathcal{J}(\mathbb{Q}(\zeta))$. Further, we will show how to deal with the exceptional case when the image of $\sqrt{5}$ corresponds to an *exceptional element* (not generic) of the form $(\sigma, \rho) - \infty \in \mathcal{J}$.

By Lemma 4.3.6 we have that $\eta := \zeta + \zeta^4 = \frac{-1+\sqrt{5}}{2}$. We know that ζ^i acts on the points of $\mathcal{H}$ by multiplication on their x coordinate. This action is naturally extended to $\mathcal{J}$, namely ζ^i maps $\mathfrak{g}$ to $(\zeta^i x_1, y_1) + (\zeta^i x_2, y_2) - 2\infty$. With this we evaluate the image of the generic point under $\eta \in \mathrm{End}(\mathcal{J})$ explicitly:

$$\eta(\mathfrak{g}) = (\zeta x_1, y_1) + (\zeta x_2, y_2) - 2\infty \oplus (\zeta^4 x_1, y_1) + (\zeta^4 x_2, y_2) - 2\infty. \quad (4.14)$$

Let $u(x) = x^2 - \alpha x + \beta$ and $v(x) = \gamma x + \delta$ be the polynomials representing the generic point $\mathfrak{g}$ of $\mathcal{J}$ in Mumford representation and let $\mathfrak{G} := \langle u(x), v(x) \rangle \in \mathcal{J}$. The Mumford representation of (4.14) is given by the resulting divisor below which can be calculated explicitly using Cantor's addition:

$$\mathfrak{G}_\eta := \eta(\mathfrak{G}) = \langle x^2 - \zeta\alpha x + \zeta^2\beta, \zeta^4(\gamma x + \delta) \rangle \oplus \langle x^2 - \zeta^4\alpha x + \zeta^3\beta, \zeta(\gamma x + \delta) \rangle.$$

Then $\sqrt{5}\mathfrak{G} = 2\mathfrak{G}_\eta + \mathfrak{G}$ using again Cantor's addition since $\eta = \frac{-1+\sqrt{5}}{2}$. The polynomials u_η and v_η defining the resulting divisor $\mathfrak{G}_\eta$ will have coefficients in $\mathbb{Z}[\eta]$ by Lemma 4.3.6.

For the case of multiplication by $\sqrt{5}$ acting on an exceptional element of the form $\hat{\mathfrak{G}} := \langle x - x_0, y_0 \rangle$, we calculate

$$\begin{aligned}\hat{\mathfrak{G}}_\eta := \eta\hat{\mathfrak{G}} &= \langle x - \zeta x_0, y_0 \rangle \oplus \langle x - \zeta^4 x_0, y_0 \rangle \\ &= \langle x^2 - (\zeta + \zeta^4) x_0 x + x_0^2, y_0 \rangle \\ &= \langle x^2 - \eta x_0 x + x_0^2, y_0 \rangle.\end{aligned}$$

Similarly to the previous case, we calculate the explicit formula for $\sqrt{5}$ in this exceptional case using Cantor's addition by $\sqrt{5}\hat{\mathfrak{G}} = 2\hat{\mathfrak{G}}_\eta + \hat{\mathfrak{G}}$.

The remaining case is if the resulting element of $\mathcal{J}$ under $\sqrt{5} \in \mathrm{End}(\mathcal{J})$ is exceptional (not generic), that is, $\mathfrak{D}_0 \in \mathcal{J}$ and $\sqrt{5}\mathfrak{D}_0 = \langle x - \sigma, \rho \rangle$ or $\sqrt{5}\mathfrak{D}_0 = \langle 1, 0 \rangle$. This can be managed in several ways. For example, fix a divisor $\mathfrak{D}_c \in \mathcal{J}$ such that $\sqrt{5}\mathfrak{D}_c$ is not an *exceptional element* of $\mathcal{J}$. Calculate $\mathfrak{L} := \sqrt{5}(\mathfrak{D}_0 + \mathfrak{D}_c)$ and if $\mathfrak{L}$ results again in an exceptional divisor repeat this procedure with a different $\mathfrak{D}_c$. Hence using Cantor's addition, we obtain $\sqrt{5}\mathfrak{D}_0 = \mathfrak{L} - \sqrt{5}\mathfrak{D}_c = \langle x - \sigma, \rho \rangle$. If $\mathfrak{L} = \sqrt{5}\mathfrak{D}_c$, it means that $\mathfrak{D}_0 \in \mathrm{Ker}(\sqrt{5})$ and $\sqrt{5}\mathfrak{D}_0 = \langle 1, 0 \rangle$ is the identity.
Now we are ready to formulate the main theorem of this section.

Theorem 4.3.8. *Let $n > 1$ be an odd integer and let $\lambda_n := 4 \cdot 5^n - 1$. Consider the hyperelliptic curve $\mathcal{H}/\mathbb{Q}(\sqrt{5})$ given by $y^2 = x^5 + h$ such that $\gcd(\lambda_n, h) = 1$. Suppose $\mathfrak{F} \in \mathcal{J}(\mathbb{Q}(\sqrt{5}))$ is given and consider the sequence of divisors $\mathfrak{D}_0 := 4\mathfrak{F}$, $\mathfrak{D}_i := \sqrt{5}\mathfrak{D}_{i-1} = \langle u_i(x), v_i(x) \rangle$ with its coefficients reduced in $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]/(2 \cdot 5^{\frac{n+1}{2}}\sqrt{5} - 1) \cong \mathbb{Z}/(\lambda_n)$.
If $\mathfrak{D}_j$ is well defined and $\neq \langle 1, 0 \rangle$ for $j \leq 2n - 1$ and $\mathfrak{D}_{2n} = \langle 1, 0 \rangle$ then λ_n is prime and $\overline{\mathfrak{F}} \notin [\sqrt{5}]\mathcal{J}(\mathbb{F}_{\lambda_n})$ for $[\sqrt{5}] \in \mathrm{End}_{\mathbb{F}_{\lambda_n}}(\mathcal{J})$.*

Proof. Suppose that $\mathfrak{D}_j = \langle u_j(x), v_j(x) \rangle$ is well defined for $0 \leq j \leq 2n - 1$, $\mathfrak{D}_{2n} = \langle 1, 0 \rangle$ and λ_n is not prime. Take the smallest prime divisor $k \mid \lambda_n$, hence $k \leq \sqrt{4 \cdot 5^n - 1}$. Since 2 or 5 do not divide λ_n we have that $k \neq 2, 5$. Moreover since $k \mid \lambda_n \nmid h$ it follows that $\mathcal{J}$ has good reduction at k. Finally, since in $\mathbb{F}_k$ we have $5 = 1/(4 \cdot 5^{n-1})$ and n is odd, it follows that $\sqrt{5} \in \mathbb{F}_k$. Consider the group $\mathcal{J}(\mathbb{F}_k)$ which, by the argument above, is a $\mathbb{Z}[\sqrt{5}]$-module. The assumption on $\mathfrak{D}_j$ implies that $\mathfrak{D}_j$ is well defined for $0 \leq j \leq 2n-1$ in $\mathcal{J}(\mathbb{F}_k)$. Moreover $\mathfrak{D}_0$ generates a $\mathbb{Z}[\sqrt{5}]$-submodule of $\mathcal{J}(\mathbb{F}_k)$ of size 5^{2n}. Further, $\#\mathcal{J}(\mathbb{F}_k) \leq (\sqrt{k}+1)^4 \leq (\sqrt[4]{4 \cdot 5^n - 1}+1)^4$ by the Hasse-Weil inequality. Hence

$$5^{2n} \leq \#\mathcal{J}(\mathbb{F}_k) \leq (\sqrt[4]{4 \cdot 5^n - 1} + 1)^4.$$

Since $n > 1$, this inequality is false ⨳. Therefore λ_n is prime.
It follows that $\overline{\mathfrak{F}} \notin [\sqrt{5}]\mathcal{J}(\mathbb{F}_{\lambda_n})$ by the existence of the sequence of $\mathfrak{D}_n$ in the hypothesis and the cardinality of $4\mathcal{J}(\mathbb{F}_{\lambda_n})$. □

To implement Theorem 4.3.8 as an algorithm we need a fixed h and an explicit $\mathfrak{F} \in \mathcal{J}$. Optionally, a proof that if λ_n is prime then $\overline{\mathfrak{F}} \notin [\sqrt{5}]\mathcal{J}(\mathbb{F}_{\lambda_n})$ where $[\sqrt{5}] \in \mathrm{End}_{\mathbb{F}_{\lambda_n}}(\mathcal{J})$. This proof would make the above result into an if and only if criterion. If λ_n is prime and $\overline{\mathfrak{F}} \in [\sqrt{5}]\mathcal{J}(\mathbb{F}_{\lambda_n})$, we will reach the identity in $4\mathcal{J}(\mathbb{F}_{\lambda_n})$ under recursive multiplication by $\sqrt{5}$ in less than $2n$ steps. However we can use the previous theorem even that this $\mathfrak{F}$ is not available to find primes when the sequence in the previous theorem can be constructed.

4.3.2 Example: Finding primes via the hyperelliptic Jacobian RM method

Let $h := 10$, that is, $\mathcal{H} : y^2 = x^5 + 10$. We chose the divisor $\mathfrak{F} := (-1, 3) - \infty \in \mathcal{J}$ (in Mumford representation $\langle x + 1, 3\rangle$). In this case

$$\mathfrak{D}_0 = 4\mathfrak{F} = \langle x^2 + \tfrac{9678206}{70644025}x + \tfrac{117106201}{70644025}, \tfrac{3088313263561}{7125156361500}x + \tfrac{22033622417431}{7125156361500}\rangle$$

regarded as polynomials in $\mathbb{Z}/(\lambda_n)[x]$.

Using Theorem 4.3.8 we tested primality of λ_n for $1 < n < 5000$ using the above choice of $h, \mathfrak{F}$. Only for $n \in \{3, 9, 13, 15, 25, 39, 69, 165, 171, 209, 339, 2033\}$, the integer λ_n was found to be prime. But there could be gaps in this list since we did not prove that our choice of $\mathfrak{F}$ is "not divisible by" $\sqrt{5}$ when λ_n is prime. However, a different computation tells us that in fact this list is complete, so we conjecture that for $h = 10$, our divisor $\mathfrak{F}$ turns Theorem 4.3.8 into a practical deterministic primality test. If our choice of $\mathfrak{F}$ turns out to be divisible by $\sqrt{5}$, to make a practical use of Theorem 4.3.8 and generate the sequence $\{\lambda_n\}$ of primes without gaps, future work will be to find the correct h and $\mathfrak{F}$. An idea to do this is to fix h and suppose that λ_n is prime. Then one could descend through the isogeny $\sqrt{5} \in \mathrm{End}_{\mathbb{F}_{\lambda_n}}(\mathcal{J})$ explicitly and find the correct $\mathfrak{F} \in \mathcal{J}(\mathbb{F}_{\lambda_n}) \setminus [\sqrt{5}]\mathcal{J}(\mathbb{F}_{\lambda_n})$. Another idea is to solve the $\sqrt{5}$ isogeny map equated with a choice of $\mathfrak{F} \in \mathcal{J}$ and show that no solutions over $\mathbb{Z}/(\lambda_n)$ exist for $n > 1$.

Appendix:

$\sqrt{5} \in \mathrm{End}_{\mathbb{Q}(\sqrt{5})}(\mathcal{J})$ for $\mathcal{H} : y^2 = x^5 + h$ in MAGMA

This code is though to be seen using the digital version of this document. Please go to http://www.rug.nl and search for this Ph.D. thesis in order to copy it and paste it for testing.

```
// MAGMA implementation of multiplication by Square root of 5 Endomorphism for the Jacobian of the curve y^2 = x^5 + h.
// This is a Square root of 5 - rational map, so it can be modified to work with any field where 5 is a square.
// Eduardo Ruiz Duarte

Sq5 := function(D)
F := BaseField(Parent(D));
d := Sqrt(F!5);
h := F!-Evaluate(DefiningEquation(Curve(Parent(D))), [0,0,1]);
P<A,B,C> := PolynomialRing(F,3);
R<x> := PolynomialRing(F);
J := Parent(D);

a :=F!-Coefficient(D[1],1);
b :=F! Coefficient(D[1],0);
c :=F! Coefficient(D[2],1);

vec := [a,b,c];

An := -2*A^17*B^3*h^2 - 48*A^16*B*h^3 + 27*A^15*B^4*h^2 + 2*A^14*B^3*C^2*h^2 + 644*A^14*B^2*h^3 - 204*A^13*B^5*h^2 + 48*A^13*B*C^2*h^3 - 64*A^13*h^4 + A^12*B^8*h - 25*A^12*B^4*C^2*h^2 - 3472*A^12*B^3*h^3 + 1033*A^11*B^6*h^2 -
       632*A^11*B^2*C^2*h^3 + 32*A^11*B*h^4 - 47/2*A^10*B^9*h + 178*A^10*B^5*C^2*h^2 + 9452*A^10*B^4*h^3 - A^9*B^8*C^2*h - 3212*A^9*B^7*h^2 + 3184*A^9*B^3*C^2*h^3 + 3328*A^9*B^2*h^4 + 603/4*A^8*B^10*h - 864*A^8*B^6*C^2*h^2 -
       13776*A^8*B^5*h^3 + 576*A^8*B*C^2*h^4 + 192*A^8*h^5 - 1/8*A^7*B^13 + 45/2*A^7*B^9*C^2*h + 5605*A^7*B^8*h^2 - 7640*A^7*B^4*C^2*h^3 - 15008*A^7*B^3*h^4 - 785/2*A^6*B^11*h + 2406*A^6*B^7*C^2*h^2 + 10928*A^6*B^6*h^3 -
       4544*A^6*B^2*C^2*h^4 - 2432*A^6*B*h^5 - 1/2*A^5*B^14 - 253/2*A^5*B^10*C^2*h - 4940*A^5*B^9*h^2 + 8936*A^5*B^5*C^2*h^3 + 24608*A^5*B^4*h^4 + 1/8*A^4*B^13*C^2 + 444*A^4*B^12*h - 3221*A^4*B^8*C^2*h^2 - 4472*A^4*B^7*h^3 +
       11232*A^4*B^3*C^2*h^4 + 6784*A^4*B^2*h^5 + 19/4*A^3*B^15 + 238*A^3*B^11*C^2*h + 1353*A^3*B^10*h^2 - 4984*A^3*B^6*C^2*h^3 - 13952*A^3*B^5*h^4 + 128*A^3*B*C^2*h^5 + 256*A^3*h^6 + 5/8*A^2*B^14*C^2 - 178*A^2*B^13*h +
       1520*A^2*B^9*C^2*h^2 + 184*A^2*B^8*h^3 - 9040*A^2*B^4*C^2*h^4 - 5888*A^2*B^3*h^5 - 51/16*A*B^16 - 112*A*B^12*C^2*h + 806*A*B^11*h^2 + 1376*A*B^7*C^2*h^3 - 1520*A*B^6*h^4 - 512*A*B^2*C^2*h^5 - 512*A*B*h^6 - 9/2*B^15*C^2 -
       129/2*B^14*h + 16*B^10*C^2*h^2 + 256*B^9*h^3 - 192*B^5*C^2*h^4 - 192*B^4*h^5;
Ad :=  A^14*B^4*h^2 - 32*A^13*B^2*h^3 - 2*A^12*B^5*h^2 + 256*A^12*h^4 + 192*A^11*B^3*h^3 - 29*A^10*B^6*h^2 - 2560*A^10*B*h^4 + 2*A^9*B^9*h + 112*A^9*B^4*h^3 + 56*A^8*B^7*h^2 + 9696*A^8*B^2*h^4 - 13/2*A^7*B^10*h - 3112*A^7*B^5*h^3 +
       512*A^7*h^5+ 399*A^6*B^8*h^2-16736*A^6*B^3*h^4- 51/2*A^5*B^11*h + 7752*A^5*B^6*h^3 - 2560*A^5*B*h^5 + A^4*B^14 - 1438*A^4*B^9*h^2 + 11936*A^4*B^4*h^4 + 251/2*A^3*B^12*h - 6184*A^3*B^7*h^3 + 3328*A^3*B^2*h^5 - 9/2*A^2*B^15 +
       1317*A^2*B^10*h^2 - 1760*A^2*B^5*h^4 + 256*A^2*h^6 - 261/2*A*B^13*h + 304*A*B^8*h^3 - 128*A*B^3*h^5 + 81/16*B^16 - 18*B^11*h^2 + 16*B^6*h^4;

Bn := 16*A^17*B*h^3 - A^16*B^4*h^2 - 212*A^15*B^2*h^3 + 5*A^14*B^5*h^2 - 16*A^14*B*C^2*h^3 + 64*A^14*h^4 + A^13*B^4*C^2*h^2 + 1152*A^13*B^3*h^3 + 26*A^12*B^6*h^2 + 200*A^12*B^2*C^2*h^3 - 704*A^12*B*h^4 - 9/2*A^11*B^9*h - 4*A^11*B^5*C^2*h^2 - 3396*A^11*B^4*h^3 -
      255*A^10*B^7*h^2 - 984*A^10*B^3*C^2*h^3 + 3872*A^10*B^2*h^4 + 165/4*A^9*B^10*h - 32*A^9*B^6*C^2*h^2 + 6048*A^9*B^5*h^3 - 32*A^9*B*C^2*h^4 - 192*A^9*h^5 + 9/2*A^8*B^9*C^2*h + 714*A^8*B^8*h^2 + 2452*A^8*B^4*C^2*h^3 - 13536*A^8*B^3*h^4 - 277/2*A^7*B^11*h +
      240*A^7*B^7*C^2*h^2 - 6392*A^7*B^6*h^3 + 1024*A^7*B*h^5 - 3/8*A^6*B^14 - 147/4*A^6*B^10*C^2*h - 735*A^6*B^9*h^2 - 3368*A^6*B^5*C^2*h^3 + 28016*A^6*B^4*h^4 + 206*A^5*B^12*h - 563*A^5*B^8*C^2*h^2 + 2056*A^5*B^7*h^3 + 1472*A^5*B^3*C^2*h^4 + 640*A^5*B^2*h^5 +
      15/8*A^4*B^15 + 193/2*A^4*B^11*C^2*h - 41*A^4*B^10*h^2 + 2668*A^4*B^6*C^2*h^3 - 28352*A^4*B^5*h^4 + 384*A^4*B*C^2*h^5 - 256*A^4*h^6 + 3/8*A^3*B^14*C^2 - 113*A^3*B^13*h + 442*A^3*B^9*C^2*h^2 + 3424*A^3*B^8*h^3 - 4624*A^3*B^4*C^2*h^4 - 5888*A^3*B^3*h^5 -
      13/8*A^2*B^16 - 365/4*A^2*B^12*C^2*h + 257*A^2*B^11*h^2 - 960*A^2*B^7*C^2*h^3 + 9712*A^2*B^6*h^4 - 1600*A^2*B^2*C^2*h^5 - 256*A^2*B*h^6 - 3/2*A*B^15*C^2 - 23/2*A*B^14*h + 72*A*B^10*C^2*h^2 - 2488*A*B^9*h^3 + 3136*A*B^5*C^2*h^4 + 3136*A*B^4*h^5 + 9/16*B^17 +
      21*B^13*C^2*h + 139*B^12*h^2 - 448*B^8*C^2*h^3 - 304*B^7*h^4 + 256*B^3*C^2*h^5 + 256*B^2*h^6;
Bd := A^14*B^4*h^2 - 32*A^13*B^2*h^3 - 2*A^12*B^5*h^2 + 256*A^12*h^4 + 192*A^11*B^3*h^3 - 29*A^10*B^6*h^2 - 2560*A^10*B*h^4 + 2*A^9*B^9*h + 112*A^9*B^4*h^3 + 56*A^8*B^7*h^2 + 9696*A^8*B^2*h^4 - 13/2*A^7*B^10*h - 3112*A^7*B^5*h^3 + 512*A^7*h^5 + 399*A^6*B^8*h^2 -
      16736*A^6*B^3*h^4 - 51/2*A^5*B^11*h + 7752*A^5*B^6*h^3 - 2560*A^5*B*h^5 + A^4*B^14 - 1438*A^4*B^9*h^2 + 11936*A^4*B^4*h^4 + 251/2*A^3*B^12*h - 6184*A^3*B^7*h^3 + 3328*A^3*B^2*h^5 - 9/2*A^2*B^15 + 1317*A^2*B^10*h^2 - 1760*A^2*B^5*h^4 + 256*A^2*h^6 -
      261/2*A*B^13*h + 304*A*B^8*h^3 - 128*A*B^3*h^5 + 81/16*B^16 - 18*B^11*h^2 + 16*B^6*h^4;

Cn := 1/5*d*A^27*B^5*C*h^3 + 308/5*d*A^26*B^3*C*h^4 - 34/5*d*A^25*B^6*C*h^3 + 1216/5*d*A^25*B*C*h^5 - 1/5*d*A^24*B^5*C^3*h^3 - 6472/5*d*A^24*B^4*C*h^4 + 132*d*A^23*B^7*C*h^3 - 308/5*d*A^23*B^3*C^3*h^4 - 24336/5*d*A^23*B^2*C*h^5 + 1/10*d*A^22*B^10*C*h^2 +
      33/5*d*A^22*B^6*C^3*h^3 + 62412/5*d*A^22*B^5*C*h^4 - 1216/5*d*A^22*B*C^3*h^5 - 768/5*d*A^22*C*h^6 - 7223/5*d*A^21*B^8*C*h^3 + 6232/5*d*A^21*B^4*C^3*h^4 + 216864/5*d*A^21*B^3*C*h^5 + 117/20*d*A^20*B^11*C*h^2 - 626/5*d*A^20*B^7*C^3*h^3 - 73312*d*A^20*B^6*C*h^4 +
      25264/5*d*A^20*B^2*C^3*h^5 + 2240*d*A^20*B*C*h^6 - 1/10*d*A^19*B^10*C^3*h^2 + 48522/5*d*A^19*B^9*C*h^3 - 57276/5*d*A^19*B^5*C^3*h^4 - 1119488/5*d*A^19*B^4*C*h^5 + 256/5*d*A^19*C^3*h^6 - 104*d*A^18*B^12*C*h^2 + 6593/5*d*A^18*B^8*C^3*h^3 +
      1464156/5*d*A^18*B^7*C*h^4 - 229952/5*d*A^18*B^3*C^3*h^5 - 40064/5*d*A^18*B^2*C*h^6 - 7/80*d*A^17*B^15*C*h - 119/20*d*A^17*B^11*C^3*h^2 - 218133/5*d*A^17*B^10*C*h^3 + 319524/5*d*A^17*B^6*C^3*h^4 + 3592464/5*d*A^17*B^5*C*h^5 + 3648/5*d*A^17*B*C^3*h^6 +
      4352/5*d*A^17*C*h^7 + 7511/10*d*A^16*B^13*C*h^2 - 41887/5*d*A^16*B^9*C^3*h^3 - 4155276/5*d*A^16*B^8*C*h^4 + 1185008/5*d*A^16*B^4*C^3*h^5 - 153664/5*d*A^16*B^3*C*h^6 + 443/80*d*A^15*B^16*C*h + 1963/20*d*A^15*B^12*C^3*h^2 + 696154/5*d*A^15*B^11*C*h^3 -
      242332*d*A^15*B^7*C^3*h^4 - 6939952/5*d*A^15*B^6*C*h^5 - 103488/5*d*A^15*B^2*C^3*h^6 - 86016/5*d*A^15*B*C*h^7 + 7/80*d*A^14*B^15*C^3*h - 16602/5*d*A^14*B^14*C*h^2 + 35178*d*A^14*B^10*C^3*h^3 + 8292816/5*d*A^14*B^9*C*h^4 - 3682624/5*d*A^14*B^5*C^3*h^5 +
      1896768/5*d*A^14*B^4*C*h^6 - 1792/5*d*A^14*C^3*h^7 - 949/16*d*A^13*B^17*C*h - 3208/5*d*A^13*B^13*C^3*h^2 - 1603171/5*d*A^13*B^12*C*h^3 + 3239664/5*d*A^13*B^8*C^3*h^4 + 6252048/5*d*A^13*B^7*C*h^5 + 805632/5*d*A^13*B^3*C^3*h^6 + 557824/5*d*A^13*B^2*C*h^7 +
      1/80*d*A^12*B^20*C - 109/20*d*A^12*B^16*C^3*h + 52257/5*d*A^12*B^15*C*h^2 - 518686/5*d*A^12*B^11*C^3*h^3 - 10743456/5*d*A^12*B^10*C*h^4 + 1323936*d*A^12*B^6*C^3*h^5 - 8325888/5*d*A^12*B^5*C*h^6 + 3072*d*A^12*B*C^3*h^7 + 1024/5*d*A^12*C*h^8 +
      10271/40*d*A^11*B^18*C*h + 50723/20*d*A^11*B^14*C^3*h^2 + 2553413/5*d*A^11*B^13*C*h^3 - 5910976/5*d*A^11*B^9*C^3*h^4 + 690672*d*A^11*B^8*C*h^5 - 3209728/5*d*A^11*B^4*C^3*h^6 - 1710336/5*d*A^11*B^3*C*h^7 + 99/320*d*A^10*B^21*C + 2151/40*d*A^10*B^17*C^3*h -
      93387/4*d*A^10*B^16*C*h^2 + 1078094/5*d*A^10*B^12*C^3*h^3 + 6953208/5*d*A^10*B^11*C*h^4 - 5195616/5*d*A^10*B^7*C^3*h^5 + 21556736/5*d*A^10*B^6*C*h^6 - 768/5*d*A^10*B^2*C^3*h^7 + 44032/5*d*A^10*B*C*h^8 - 1/80*d*A^9*B^20*C^3 - 20489/40*d*A^9*B^19*C*h -
      143063/20*d*A^9*B^15*C^3*h^2 - 2503679/5*d*A^9*B^14*C*h^3 + 6470872/5*d*A^9*B^10*C^3*h^4 - 16365984/5*d*A^9*B^9*C*h^5 + 7713856/5*d*A^9*B^5*C^3*h^6 + 3501312/5*d*A^9*B^4*C*h^7 + 2048/5*d*A^9*C^3*h^8 - 121/32*d*A^8*B^22*C - 15857/80*d*A^8*B^18*C^3*h +
      677709/20*d*A^8*B^17*C*h^2 - 1454286/5*d*A^8*B^13*C^3*h^3 + 1270708/5*d*A^8*B^12*C*h^4 - 2742496/5*d*A^8*B^8*C^3*h^5 - 34085632/5*d*A^8*B^7*C*h^6 - 243712/5*d*A^8*B^3*C^3*h^7 - 482304/5*d*A^8*B^2*C*h^8 - 103/320*d*A^7*B^21*C^3 + 31121/80*d*A^7*B^20*C*h +
      69012/5*d*A^7*B^16*C^3*h^2 + 1123937/5*d*A^7*B^15*C*h^3 - 2627588/5*d*A^7*B^11*C^3*h^4 + 19237056/5*d*A^7*B^10*C*h^5 - 2344128*d*A^7*B^6*C^3*h^6 - 1323776*d*A^7*B^5*C*h^7 - 37888/5*d*A^7*B*C^3*h^8 - 4096*d*A^7*C*h^9 + 479/40*d*A^6*B^23*C +
      22833/80*d*A^6*B^19*C^3*h - 119693/4*d*A^6*B^18*C*h^2 + 1015729/5*d*A^6*B^14*C^3*h^3 - 5018208/5*d*A^6*B^13*C*h^4 + 8793264/5*d*A^6*B^9*C^3*h^5 + 30290176/5*d*A^6*B^8*C*h^6 + 437248/5*d*A^6*B^4*C^3*h^7 + 1115136/5*d*A^6*B^3*C*h^8 + 1111/320*d*A^5*B^22*C^3 +
      23283/80*d*A^5*B^21*C*h - 74901/5*d*A^5*B^17*C^3*h^2 + 19771*d*A^5*B^16*C*h^3 - 358456*d*A^5*B^12*C^3*h^4 - 10588992/5*d*A^5*B^11*C*h^5 + 10547904/5*d*A^5*B^7*C^3*h^6 + 9256448/5*d*A^5*B^6*C*h^7 + 169984/5*d*A^5*B^2*C^3*h^8 + 172032/5*d*A^5*B*C*h^9 -
      471/40*d*A^4*B^24*C - 6883/80*d*A^4*B^20*C^3*h + 166009/10*d*A^4*B^19*C*h^2 - 109313/5*d*A^4*B^15*C^3*h^3 + 2098348/5*d*A^4*B^14*C*h^4 - 5809616/5*d*A^4*B^10*C^3*h^5 - 11683328/5*d*A^4*B^9*C*h^6 + 61696*d*A^4*B^5*C^3*h^7 - 233472/5*d*A^4*B^4*C*h^8 +
      4096/5*d*A^4*C^3*h^9 - 1351/160*d*A^3*B^23*C^3 - 76881/80*d*A^3*B^22*C*h + 35323/5*d*A^3*B^18*C^3*h^2 - 151804/5*d*A^3*B^17*C*h^3 + 1657112/5*d*A^3*B^13*C^3*h^4 + 2067584/5*d*A^3*B^12*C*h^5 - 4265792/5*d*A^3*B^8*C^3*h^6 - 5609984/5*d*A^3*B^7*C*h^7 -
      191488/5*d*A^3*B^3*C^3*h^8 - 249856/5*d*A^3*B^2*C*h^9 + 1881/320*d*A^2*B^25*C - 5421/40*d*A^2*B^21*C^3*h - 21057/4*d*A^2*B^20*C*h^2 - 29962*d*A^2*B^16*C^3*h^3 + 318012/5*d*A^2*B^15*C*h^4 + 839232/5*d*A^2*B^11*C^3*h^5 - 1024/5*d*A^2*B^10*C*h^6 -
      821504/5*d*A^2*B^6*C^3*h^7 - 958464/5*d*A^2*B^5*C*h^8 - 16384/5*d*A^2*B*C^3*h^9 - 16384/5*d*A^2*C*h^10 + 81/40*d*A*B^24*C^3 + 48717/80*d*A*B^23*C*h - 8412/5*d*A*B^19*C^3*h^2 - 72417/5*d*A*B^18*C*h^3 + 38432/5*d*A*B^14*C^3*h^4 + 214832/5*d*A*B^13*C*h^5 -
      73472/5*d*A*B^9*C^3*h^6 - 115712/5*d*A*B^8*C*h^7 - 53248/5*d*A*B^4*C^3*h^8 - 53248/5*d*A*B^3*C*h^9 - 513/320*d*B^26*C + 2187/10*d*B^22*C^3*h + 2061/4*d*B^21*C*h^2 - 8552/5*d*B^17*C^3*h^3 - 12948/5*d*B^16*C*h^4 + 22528/5*d*B^12*C^3*h^5 + 19776/5*d*B^11*C*h^6 -
      11264/5*d*B^7*C^3*h^7 - 11264/5*d*B^6*C*h^8;
Cd := A^25*B^6*h^3 - 48*A^24*B^4*h^4 - 6*A^23*B^7*h^3 + 768*A^23*B^2*h^5 + 480*A^22*B^5*h^4 - 4096*A^22*h^6 - 32*A^21*B^8*h^3 - 10752*A^21*B^3*h^5 + 3*A^20*B^11*h^2 - 456*A^20*B^6*h^4 + 73728*A^20*B*h^6 + 203*A^19*B^9*h^3 + 51408*A^19*B^4*h^5 - 87/4*A^18*B^12*h^2 -
      11244*A^18*B^7*h^4 - 573952*A^18*B^2*h^6 + 966*A^17*B^10*h^3 - 26256*A^17*B^5*h^5 - 12288*A^17*h^7 - 129/4*A^16*B^13*h^2 + 42660*A^16*B^8*h^4 + 2522624*A^16*B^3*h^6 + 3*A^15*B^16*h - 7822*A^15*B^11*h^3 - 723360*A^15*B^6*h^5 + 159744*A^15*B*h^7 +
      1239/2*A^14*B^14*h^2 + 52464*A^14*B^9*h^4 - 6851328*A^14*B^4*h^6 - 51/2*A^13*B^17*h + 5388*A^13*B^12*h^3 + 3342672*A^13*B^7*h^5 - 847104*A^13*B^2*h^7 - 3783/4*A^12*B^15*h^2 - 704364*A^12*B^10*h^4 + 11822720*A^12*B^5*h^6 - 12288*A^12*h^8 + 579/16*A^11*B^18*h +
      82158*A^11*B^13*h^3 - 7249392*A^11*B^8*h^5 + 2325504*A^11*B^3*h^7 + A^10*B^21 - 12099/2*A^10*B^16*h^2 + 1972080*A^10*B^11*h^4 - 12835328*A^10*B^6*h^6 + 98304*A^10*B*h^8 + 1227/4*A^9*B^19*h - 300951*A^9*B^14*h^3 + 8637264*A^9*B^9*h^5 - 3439872*A^9*B^4*h^7 -
      39/4*A^8*B^22 + 110025/4*A^8*B^17*h^2 - 2646732*A^8*B^12*h^4 + 8383872*A^8*B^7*h^6 - 276480*A^8*B^2*h^8 - 23337/16*A^7*B^20*h + 454166*A^7*B^15*h^3 - 5436528*A^7*B^10*h^5 + 2550528*A^7*B^5*h^7 - 4096*A^7*h^9 + 583/16*A^6*B^23 - 45762*A^6*B^18*h^2 +
      1722120*A^6*B^13*h^4 - 3004352*A^6*B^8*h^6 + 304128*A^6*B^3*h^8 + 41163/16*A^5*B^21*h - 310965*A^5*B^16*h^3 + 1514304*A^5*B^11*h^5 - 748800*A^5*B^6*h^7 + 12288*A^5*B*h^9 - 4077/64*A^4*B^24 + 33018*A^4*B^19*h^2 - 424848*A^4*B^14*h^4 + 483328*A^4*B^9*h^6 -
      89088*A^4*B^4*h^8 - 15525/8*A^3*B^22*h + 72254*A^3*B^17*h^3 - 143088*A^3*B^12*h^5 + 64512*A^3*B^7*h^7 - 4096*A^3*B^2*h^9 + 3159/64*A^2*B^25 - 14985/2*A^2*B^20*h^2 + 22344*A^2*B^15*h^4 - 18048*A^2*B^10*h^6 + 3072*A^2*B^5*h^8 + 7047/16*A*B^23*h - 1809*A*B^18*h^3
      + 2256*A*B^13*h^5 - 768*A*B^8*h^7 - 729/64*B^26 + 243/4*B^21*h^2 - 108*B^16*h^4 + 64*B^11*h^6;

an := Evaluate(An,vec);
ad := Evaluate(Ad,vec);
bn := Evaluate(Bn,vec);
bd := Evaluate(Bd,vec);
cn := Evaluate(Cn,vec);
cd := Evaluate(Cd,vec);

aa := an/ad;
bb := bn/bd;
cc := cn/cd;

// We can deduce D by A,B,C in <x^2 + Ax + B, Cx + D>
sigma1 :=(1/2)*(2*h - aa^5 - 5*aa*bb^2 + 5*aa^3*bb - cc^2 *(aa^2 - 4*bb));
DD := cc*(h  - aa^5 - 5*aa*bb^2 + 5*aa^3*bb + sigma1  +  aa*(aa^2-3*bb)*(aa^2-bb))/(aa^4 -bb*(3*aa^2 - bb));
Rdiv := J![x^2 + aa*x + bb, cc*x+DD ];
return Rdiv;
end function;

// We test H:y^2 = x^5 + 10 using the divisor,  D:=2*<x+1,3>
// We calculate the multiplication by d:=SQ5 twice and compare it with 5*D

Q<d> := QuadraticField(5);
P<X> := PolynomialRing(Q);
J := Jacobian(HyperellipticCurve(X^5 + 10));
D0 := J![X+1,3];
printf "Divisor D to test\n";
D := 2*D0;
D;
printf "Square root of 5 acting on D\n";
Ds5 := Sq5(D);
Ds5;
printf "Square root of 5 acting two times on D\n";
D5 := Sq5(Ds5);
D5;
printf "Is 5*D the same as twice the action of square root of 5 on D? %o\n", D5 eq 5*D;
```

Summary

The Hasse-Weil inequality asserts that a curve C of genus g defined over a finite field $\mathbb{F}_q$ of cardinality q, satisfies $|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}$. Here $\#C(\mathbb{F}_q)$ denotes the number of elements in the finite set $C(\mathbb{F}_q)$ consisting of the $\mathbb{F}_q$-rational points on C. In this thesis, first we extend the ideas of an elementary proof of this inequality for elliptic curves, originally invented by Yu.I. Manin, to hyperelliptic curves of genus 2. We obtain similar lemmas compared to the genus 1 elementary proof, entailing the Hasse-Weil inequality for curves of genus 2 provided that an $\mathbb{F}_q$-rational Weierstrass point is present in the curve. Our proof uses some intersection theory on the Jacobian of the genus 2 curve, making the proof not quite as elementary as Manin's one.

Further as a second part of this thesis, we provide applications of curves of genus 1 and 2 to primality testing. We use the group structure of an elliptic curve and the Jacobian of a genus 2 curve over finite rings.

In the first chapter we discuss and revisit the original proof of the Hasse inequality for elliptic curves by Manin. This proof has been revisited before, however we reduce some of the proofs of the lemmas involved using elementary observations. Moreover, we rearrange the lemmas in order to obtain a more compact proof of the Hasse inequality *à la* Manin.

In the second chapter we discuss and construct the Jacobian and the Kummer surface associated to a hyperelliptic curve $\mathcal{H}/\mathbb{F}_q$ of genus 2 using Mumford coordinates. We explore their function fields using these coordinates which are ubiquitous in cryptography and most computer algebra systems such as MAGMA or SAGE. This chapter also introduces certain functions on the Kummer surface and on the Jacobian of $\mathcal{H}$ which are used in subsequent chapters.

The third chapter is dedicated to the proof of the Hasse-Weil inequality for genus 2, mimicking Manin's ideas. The proof relies on the Jacobian of the curve, since the original proof for genus 1 uses the group structure of the elliptic curve over its function field. In our new proof we use the Jacobian of

the genus 2 curve over the function field of the curve.

Finally, in the fourth chapter we discuss various algorithms for primality testing using curves of genus 0, 1 and 2. We first discuss primality tests using conics, namely the unit circle and a hyperbola. Further, inspired by authors like W. Bosma, A. Silverberg, R. Denomme and G. Savin, we extend some of their deterministic primality tests using elliptic curves E as $\mathrm{End}(E)$-modules. We illustrate these tests by applying them to some infinite families of integer sequences.

Using the previous ideas for primality testing with elliptic curves, we partially answer an open question stated by A. Abatzoglou, A. Silverberg, A. V. Sutherland and A. Wong. They asked about the potential design of a deterministic primality test using an Abelian surface. We provide an algorithm to detect primes in some sequence of integers $\{\lambda_n\}$ using the Jacobian $\mathcal{J}$ of a hyperelliptic curve $\mathcal{H}$ of genus 2 as an $\mathrm{End}(\mathcal{J})$-module. The proposed algorithm using the algebraic group $\mathcal{J}$, conjecturally detects composite numbers in the sequence, that is why we say that the open question is *partially* solved.

The algorithm is tested using MAGMA where an explicit endomorphism of $\mathcal{J}$ was implemented, finding several primes in the sequence $\{\lambda_n\}$.

Future work is to extend our proof of the Hasse-Weil inequality, for example to characteristic 2. Moreover, we used an embedding of the curve into its Jacobian using a rational Weierstrass point of the curve in order to mimic Manin's proof. An open question is to adapt this proof when such a point is not present in the curve.

For the primality testing, future work is to convert our primality test using genus 2 curves to a deterministic test. To do this, an explicit descent map of the *multiplication by* $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$ is required, where $\mathcal{J}$ is the Jacobian of the curve $y^2 = x^5 + h$. Some of the lemmas in Chapter 4 may be useful to build such a descent map.

Resumen

La desigualdad de Hasse-Weil afirma que una curva C de género g sobre un campo finito $\mathbb{F}_q$ de cardinalidad q, satisface $|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}$. Aquí $\#C(\mathbb{F}_q)$ denota el número de elementos en el conjunto finito $C(\mathbb{F}_q)$ que consiste de puntos $\mathbb{F}_q$-racionales de C. En esta tesis, primero extendemos las ideas de una demostración elemental de esta desigualdad para curvas elípticas, originalmente inventada por Yu. I. Manin, a curvas hiperelípticas de género 2. Obtenemos lemas similares comparados con la demostración elemental de género 1 que implican la desigualdad de Hasse-Weil para curvas de género 2 cuando ésta tiene un punto de Weierstrass $\mathbb{F}_q$-racional. Nuestra demostración usa un poco de teoría de intersección en la Jacobiana de la curva de género 2, haciéndo la demostración no tan elemental como la prueba de Manin

Más adelante, en la segunda parte de esta tesis, proveemos aplicaciones de curvas de género 1 y 2 a pruebas de primalidad. Usamos la estructura de grupo de una curva elíptica y la Jacobiana de una curva de género 2 sobre anillos finitos.

En el primer capítulo discutimos y retomamos la demostración original de la desigualdad de Hasse para curvas elípticas hecha por Manin. Esta demostración ya ha sido retomada antes, sin embargo hemos reducido algunas demostraciones de los lemas involucrados usando observaciones elementales. También reacomodamos los lemas de tal manera que obtuvimos una version más compacta de la demostración de la desigualdad de Hasse *à la* Manin.

En el segundo capítulo discutimos y construimos la Jacobiana y superficie de Kummer asociada a una curva hiperelíptica $\mathcal{H}/\mathbb{F}_q$ de género 2 usando coordenadas de Mumford. Exploramos sus campos de funciones usando estas coordenadas que son ubicuas en criptografía y en la mayoría de los sistemas de álgebra computacionales como MAGMA o SAGE. Este capítulo también introduce ciertas funciones interesantes en la superficie de Kummer y en la Jacobiana de $\mathcal{H}$, las cuales son usadas en capitulos siguientes.

El tercer capítulo es dedicado a la demostración de la desigualdad de Hasse-Weil para género 2, imitando las ideas de Manin. La prueba se basa en la Jacobiana de la curva, ya que la prueba original para género 1 usa la estructura de grupo de la curva elíptica sobre su campo de funciones. En nuestra nueva demostración usamos la Jacobiana de la curva de género 2 sobre el campo de funciones de la curva.

Finalmente, en el cuarto capítulo discutimos varios algoritmos para pruebas de primalidad usando curvas de género 0, 1 y 2. Comenzamos discutiendo algoritmos de primalidad usando cónicas, precisamente la circunferencia unitaria y una hipérbola. Además, inspirados por autores como W. Bosma, A. Silverberg, R. Denomme y G. Savin, extendimos algunos algoritmos de primalidad determinísticos usando curvas elípticas E como $\mathrm{End}(E)$-módulos. Aquí ilustramos estos algoritmos aplicándolos a algunas familias infinitas de sucesiones de enteros.

Usando las ideas previas para pruebas de primalidad con curvas elípticas, respondimos parcialmente una pregunta abierta de A. Abatzoglou, A. Silverberg, A.V. Sutherland y A. Wong. Ellos se preguntaron sobre el diseño potencial de una prueba de primalidad determinística usando una superficie Abeliana. Nosotros proveemos un algoritmo que detecta primos en cierta sucesión de enteros $\{\lambda_n\}$ usando la Jacobiana $\mathcal{J}$ de una curva hiperelíptica $\mathcal{H}$ de género 2 como un $\mathrm{End}(\mathcal{J})$-módulo. El algoritmo propuesto usando el grupo algebraico $\mathcal{J}$, conjecturalmente detecta enteros compuestos en la sucesión, esta es la razón por la que decimos que respondimos *parcialmente* la pregunta abierta.

El algoritmo fue probado usando MAGMA, donde un endomorfismo explícito de $\mathcal{J}$ fue implementado, encontrando varios números primos en la sucesión $\{\lambda_n\}$.

El trabajo futuro es extender nuestra demostración de la desigualdad de Hasse-Weil a característica 2. Además, usamos un encaje de la curva en su Jacobiana usando un punto de Weierstrass racional, de tal manera que podamos imitar la demostración de Manin. Una pregunta abierta es la adaptación de nuestra demostración cuando dicho punto no está presente en la curva.

Para las pruebas de primalidad, el trabajo futuro es convertir nuestra prueba de primalidad que usa curvas de género 2 en una prueba determinística. Para hacer esto, un mapeo de descenso explícito de la *multiplicacion por* $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$ es requerido, donde $\mathcal{J}$ es la Jacobiana de la curva $y^2 = x^5 + h$. Algunos de los lemas en el Capítulo 4 podrían ser útiles para construir este mapeo de descenso.

Samenvatting

De Hasse-Weil-ongelijkheid stelt dat een kromme C van geslacht g gedefinieerd over een eindig lichaam $\mathbb{F}_q$ van cardinaliteit q, voldoet aan $|\#C(\mathbb{F}_q) - q - 1| \leq 2q\sqrt{q}$. Hierin is $\#C(\mathbb{F}_q)$ het aantal elementen van de eindige verzameling $C(\mathbb{F}_q)$ van $\mathbb{F}_q$-rationale punten op C. In deze scriptie breiden we eerst de ideeën van een elementair bewijs van deze ongelijkheid voor elliptische krommen, oorspronkelijk uitgevonden door Yu.I. Manin, naar hyperelliptische krommen van geslacht 2. We krijgen vergelijkbare lemma's als in het elementaire bewijs voor geslacht 1, met als conclusie de Hasse-Weil-ongelijkheid voor krommen van geslacht 2, onder de aanname dat een $\mathbb{F}_q$-rationaal Weierstrasspunt aanwezig is op de kromme. Ons bewijs maakt gebruik van doorsnijdingstheorie op de Jacobiaan van de geslacht 2-kromme, waardoor het bewijs niet precies zo elementair is als dat van Manin.

Verder als tweede deel van deze thesis geven we toepassingen van krommen van geslacht 1 en 2 op priemgetaltests. We gebruiken de groepsstructuur van een elliptische kromme en de Jacobiaan van een geslacht 2-kromme over eindige ringen.

In het eerste hoofdstuk bespreken en herzien we het originele bewijs van de Hasse-ongelijkheid voor ellitische krommen door Manin. Dit bewijs is al eerder herzien, maar we reduceren enkele bewijzen van de lemma's met behulp van elementaire observaties. Daarnaast herschikken we de lemma's zodat we een compacter bewijs verkrijgen van de Hasse-ongelijkheid *á la* Manin.

In het tweede hoofdstuk bespreken en construeren we de Jacobiaan en het Kummeroppervlak behorend bij een hyperelliptische kromme $\mathcal{H}/\mathbb{F}_q$ van geslacht 2 met behulp van Mumfordcoördinaten. We onderzoeken hun functielichamen met behulp van deze coördinaten, die veelvuldig voorkomen in cryptografie en in de meeste computeralgebrasystemen zoals MAGMA en SAGE. Dit hoofdstuk introduceert ook bepaalde functies op het Kummeroppervlak en op de Jacobiaan van $\mathcal{H}$ die we in de volgende hoofdstukken zullen gebruiken.

Het derde hoofdstuk is toegewijd aan het bewijs van de Hasse-Weil-ongelijkheid voor geslacht 2, analoog aan Manin's ideeën. Het bewijs berust op de Jacobiaan van de kromme, aangezien het originele bewijs voor geslacht 1 van de groepsstructuur van de elliptische kromme over zijn functielichaam gebruik maakt. In ons nieuwe bewijs gebruiken we de Jacobiaan van de geslacht 2-kromme over het functielichaam van de kromme.

Ten slotte, in het laatste hoofdstuk, bespreken we verschillende algoritmes voor priemgetaltests, gebruik makend van krommen van geslacht 0, 1 en 2. Als eerste bespreken we priemgetaltests met behulp van kegelsneden, namelijk de eenheidscirkel en een hyperbool. Verder, geïnspireerd door auteurs als W. Bosma, A. Silverberg, R. Denomme en G. Savin, breiden we enkele van hun deterministische priemgetaltests uit, gebruik makend van elliptische krommen E als $\mathrm{End}(E)$-modulen. We illustreren deze tests door ze toe te passen op enkele oneindige families van rijen van gehele getallen.

Met behulp van de voorgaande ideeën voor priemgetaltests met elliptische krommen, beantwoorden we gedeeltelijk een open vraag geformuleerd door A. Abatzoglou, A. Silverberg, A.V. Sutherland and A. Wong. Zij vroegen naar het potentiële ontwerp van een deterministische priemgetaltest die gebruik maakt van een Abels oppervlak. We geven een algoritme dat priemgetallen detecteert in bepaalde rijen van gehele getallen $\{\lambda_n\}$ met behulp van de Jacobiaan $\mathcal{J}$ van een hyperelliptische kromme $\mathcal{H}$ van geslacht 2 als een $\mathrm{End}(\mathcal{J})$-moduul. Het voorgestelde algoritme, gebruik makend van de algebraïsche groep $\mathcal{J}$, detecteert vermoedelijk samengestelde getallen in de rij; om deze reden zeggen we dat de open vraag *gedeeltelijk* is beantwoord.

Het algoritme is getest met behulp van MAGMA, waar een expliciet endomorfisme van $\mathcal{J}$ is geïmplementeerd. We vinden meerdere priemen in de rij $\{\lambda_n\}$.

Toekomstig werk is om ons bewijs van de Hasse-Weil-ongelijkheid uit te breiden, bijvoorbeeld naar karakteristiek 2. Daarnaast hebben we een imbedding van de kromme in zijn Jacobiaan met behulp van een rationaal Weierstrasspunt gebruikt om Manin's bewijs na te bootsen. Een open vraag is om dit bewijs aan te passen wanneer zo'n punt niet aanwezig is in de kromme.

Voor de priemgetaltests is er toekomstig werk in het omzetten van onze priemgetaltest met geslacht 2-krommen naar een deterministische test. Om dit te doen is een expliciete afdalingsafbeelding van de *vermenigvuliging met* $[\sqrt{5}] \in \mathrm{End}(\mathcal{J})$ noodzakelijk, waar $\mathcal{J}$ de Jacobiaan is van de kromme $y^2 = x^5 + h$. Enkele van de lemma's in Hoofdstuk 4 zijn mogelijk nuttig voor het construeren van zo'n afdalingsafbeelding.

Biography

Eduardo Ruíz Duarte was born on November 3rd, 1984 in Tijuana, Mexico. He obtained his bachelor's and master's degrees in mathematics from the National Autonomous University of Mexico (UNAM). From 2014 to 2018 he was a PhD student in mathematics at the University of Groningen under the supervision of Prof. Jaap Top.

He maintains a website at http://ff2.nl and a blog at http://b3ck.blogspot.nl which gathers some of his informal interests in mathematics and computer science.

Bibliography

[ACGH13] Enrico Arbarello, Maurizio Cornalba, Phillip Griffiths, and Joseph Daniel Harris. *Geometry of algebraic curves*, volume 1. Springer Science & Business Media, 2013.

[Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. I. *Math. Z.*, 19(1):153–206, 1924.

[ASSW16] Alexander Abatzoglou, Alice Silverberg, Andrew Sutherland, and Angela Wong. A framework for deterministic primality proving using elliptic curves with complex multiplication. *Mathematics of Computation*, 85(299):1461–1483, 2016.

[BL13] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302. Springer Science & Business Media, 2013.

[Bos85] Wieb Bosma. Primality testing using elliptic curves. Master thesis, http://www.math.ru.nl/~bosma/pubs/PRITwEC1985.pdf, 1985.

[Can87] David G Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of computation*, 48(177):95–101, 1987.

[Can94] David G Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Journal fur die reine und angewandte Mathematik*, 447:91–146, 1994.

[Cas56] J.W.S. Cassels. Revision: On cubic congruences to a prime modulus. *http://www.ams.org/mathscinet-getitem?mr=81308*, 1956.

[CF96] J.W.S. Cassels and E. Victor Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge University Press, 1996.

[Cha88] JS Chahal. Equations over finite fields. In *Topics in Number Theory*, pages 147–162. Springer, 1988.

[Cha95] Jasbir S. Chahal. Manin's proof of the Hasse inequality revisited. *Nieuw Arch. Wisk. (4)*, 13(2):219–232, 1995.

[CL11] Craig Costello and Kristin Lauter. Group law computations on jacobians of hyperelliptic curves. In *Selected Areas in Cryptography*, pages 92–117. Springer, 2011.

[CL12] Craig Costello and Kristin Lauter. Group law computations on jacobians of hyperelliptic curves. In *Selected Areas in Cryptography*, pages 92–117. Springer, 2012.

[CST14] Jasbir S Chahal, Afzal Soomro, and Jaap Top. A supplement to manin's proof of the hasse inequality. *Rocky Mountain Journal of Mathematics*, 44(5):1457–1470, 2014.

[DO14] Eduardo Ruiz Duarte and Octavio Páez Osuna. Explicit endomorphism of the jacobian of a hyperelliptic curve of genus 2 using base field operations. *Studia Scientiarum Mathematicarum Hungarica*, 2014.

[DS08] Robert Denomme and Gordan Savin. Elliptic curve primality tests for fermat and related primes. *Journal of Number Theory*, 128(8):2398–2412, 2008.

[EM56] P Erdös and Amer Math Monthly. On pseudoprimes and carmichael numbers. *Publ. Math. Debrecen*, 4(1956):201–206, 1956.

[EMM02] L Hernández Encinas, Alfred J Menezes, and J Munoz Masqué. Isomorphism classes of genus-2 hyperelliptic curves over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):57–65, 2002.

[FH10] Farideh Firoozbakht and Maximilian F Hasler. Variations on euclidś formula for perfect numbers. *Journal of Integer Sequences*, 13(2):3, 2010.

[Fly90] Eugene Victor Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 107, pages 425–441. Cambridge Univ Press, 1990.

[Fly93] EV Flynn. The group law on the jacobian of a curve of genus 2. *J. reine angew. Math*, 439:45–69, 1993.

[Ful84] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].* Springer-Verlag, Berlin, 1984.

[Gau86] Carl Friedrich Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[GH14] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry.* John Wiley & Sons, 2014.

[GHM08] Steven D Galbraith, Michael Harrison, and David J Mireles Morales. Efficient hyperelliptic arithmetic using balanced representation for divisors. In *Algorithmic number theory*, pages 342–356. Springer, 2008.

[GK09] Alexander Gurevich and Boris Kunyavskii. Primality testing through algebraic groups. *Archiv der Mathematik*, 93(6):555, 2009.

[GK12] Alexander Gurevich and Boris Kunyavskii. Deterministic primality tests based on tori and elliptic curves. *Finite Fields and Their Applications*, 18(1):222–236, 2012.

[GL62] A. O. Gel′fond and Ju. V. Linnik. *Ѐлементарные методы в аналитическоĭтеории чисел.* Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1962.

[GL65] A. O. Gel′fond and Yu. V. Linnik. *Elementary methods in analytic number theory.* Translated by Amiel Feinstein. Revised and edited by L. J. Mordell. Rand McNally & Co., Chicago, Ill., 1965.

[GL66] Aleksandr O Gel'fond and Yuri V Linnik. Elementary methods in the analytic theory of numbers. translated from the russian by de brown. translation edited by in sneddon. international series of monographs in pure and applied mathematics, vol. 92, 1966.

[GLM65] Aleksandr Osipovich Gelfond, Yuri Vladimirovich Linnik, and Louis Joel Mordell. *Elementary methods in analytic number theory.* Rand McNally Chicago, 1965.

[Gra90] David Grant. Formal groups in genus two. *J. reine angew. Math*, 411(96):121, 1990.

[Gro05] Benedict H Gross. An elliptic curve test for Mersenne primes. *Journal of Number Theory*, 110(1):114–119, 2005.

[GS05] Pierrick Gaudry and Éric Schost. Modular equations for hyperelliptic curves. *Mathematics of Computation*, 74(249):429–454, 2005.

[GS12] Pierrick Gaudry and Éric Schost. Genus 2 point counting over prime fields. *Journal of Symbolic Computation*, 47(4):368–400, 2012.

[Ham12] Samuel A. Hambleton. Generalized Lucas-Lehmer tests using Pell conics. *Proc. Amer. Math. Soc.*, 140(8):2653–2661, 2012.

[Har77] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977.

[Has36] Helmut Hasse. Zur Theorie der abstrakten elliptischen Funktionenkörper I,II,III. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung. *J. Reine Angew. Math.*, 175:55–62, 1936.

[HC14] Huseyin Hisil and Craig Costello. Jacobian coordinates on genus 2 curves. In *Advances in Cryptology–ASIACRYPT 2014*, pages 338–357. Springer, 2014.

[Her21] Gustav Herglotz. Zur letzten eintragung im gaussschen tagebuch. *Ber. Verhandl. Sächs. Akad. Wiss. Math.-Phys. Kl*, 73:271–276, 1921.

[HS13] Marc Hindry and Joseph H Silverman. *Diophantine geometry: an introduction*, volume 201. Springer Science & Business Media, 2013.

[Ire90] K Ireland. M. rosen a classical introduction to modern number theory vol. 84 of graduate texts in mathematics, 1990.

[Kan84] Ernst Kani. On castelnuovo's equivalence defect. *J. reine angew. Math*, 352:24–70, 1984.

[Kle03] Felix Klein. Gauß' wissenschaftliches Tagebuch 1796–1814. *Math. Ann.*, 57(1):1–34, 1903.

[Kna92] Anthony W Knapp. *Elliptic curves*, volume 40. Princeton University Press, 1992.

[Kob12] Neal I Koblitz. *Introduction to elliptic curves and modular forms*, volume 97. Springer Science & Business Media, 2012.

[Lan82] Serge Lang. *Introduction to Algebraic and Abelian Functions.* Springer New York, New York, NY, 1982.

[Lan05] Tanja Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 15(5):295–328, 2005.

[Lan12] Serge Lang. *Introduction to algebraic and abelian functions*, volume 89. Springer Science & Business Media, 2012.

[Lem99] Franz Lemmermeyer. Elliptische Kurven I. *ftp://ftp.math.tu-berlin.de/pub/Lehre/Algebra/Algebra2.WS00/Skripte/ell_curv.ps*, 1999.

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves.* Oxford graduate texts in mathematics. Oxford University Press, 2002.

[Man56] Yu. I. Manin. On cubic congruences to a prime modulus. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 20:673–678, 1956.

[Man60] Yu. I. Manin. On cubic congruences to a prime modulus. *Amer. Math. Soc. Transl. (2)*, 13:1–7, 1960.

[MB81] Laurent Moret-Bailly. Familles de courbes et de variétés abéliennes sur p1,ii. *Sém. sur les pinceaux de courbes de genre au moins deux (ed. L. Szpiro). Astériques*, 86, 1981.

[Mil86] James S Milne. Jacobian varieties. *Arithmetic geometry*, pages 167–212, 1986.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[MT10a] Stephen Meagher and Jaap Top. Twists of genus three curves over finite fields. *Finite Fields and Their Applications*, 16(5):347–368, 2010.

[MT10b] Stephen Meagher and Jaap Top. Twists of genus three curves over finite fields. *Finite fields and their applications*, 6(5):3–4, 2010.

[Mum66] David Mumford. On the equations defining abelian varieties. i. *Inventiones mathematicae*, 1(4):287–354, 1966.

[Mum74] David Mumford. *Abelian varieties*, volume 5. Oxford University Press, USA, 1974.

[Mum84] David Mumford. *Tata Lectures on Theta II.* Birkhäuser, 1984.

[OD12] M. Joye O. Diao. Unified addition formulæ for hyperelliptic curve cryptosystems. 2012.

[Poo96] Bjorn Poonen. Computational aspects of curves of genus at least 2. In *Algorithmic number theory*, pages 283–306. Springer, 1996.

[PS97] Bjorn Poonen and Edward F Schaefer. Explicit descent for jacobians of cyclic covers of the projective line. *Journal fur die Reine und Angewandte Mathematik*, 488:141–188, 1997.

[Sev26] Francesco Severi. *Trattato di geometria algebrica*, volume 1. N. Zanichelli, 1926.

[SH94] Igor Rostislavovich Shafarevich and Kurt Augustus Hirsch. *Basic algebraic geometry*, volume 2. Springer, 1994.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2nd edition, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994.

[Sil14] Alice Silverberg. Some remarks on primality proving and elliptic curves. *Adv. in Math. of Comm.*, 8(4):427–436, 2014.

[Soe13] M.M.J Soeten. Hasse′s theorem on elliptic curves. *Rijksuniversiteit Groningen, http://irs.ub.rug.nl/dbi/51c960652a4b7*, 2013.

[Soo13] Muhammad Afzal Soomro. *Algebraic curves over finite fields.* Rijksuniversiteit Groningen, 2013.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[Sti09] H. Stichtenoth. *Algebraic Function Fields and Codes.* Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2009.

[SV04] Tanush Shaska and Helmut Völklein. Elliptic subfields and automorphisms of genus 2 function fields. In *Algebra, arithmetic and geometry with applications*, pages 703–723. Springer, 2004.

[Top89] Jaap Top. Hecke L-series related with algebraic cycles or with Siegel modular forms. (PhD Thesis) http://www.math.rug.nl/~top/Thesis1989.pdf, 1989.

[Top15] Jaap Top. Lucas-Lehmer revisited. Intercity Seminar, University of Groningen, http://www.math.leidenuniv.nl/~desmit/ic/2015.html, 2015.

[TS67] J. T. Tate and I. R. Shafarevich. The rank of elliptic curves. *Dokl. Akad. Nauk SSSR*, 175:770–773, 1967.

[Tsu11] Yu Tsumura. Primality tests for $2^p \pm 2^{(p+1)/2} + 1$ using elliptic curves. *Proc. Amer. Math. Soc.*, 139(8):2697–2703, 2011.

[vGT06] Bert van Geemen and Jaap Top. An isogeny of $K3$ surfaces. *Bull. London Math. Soc.*, 38(2):209–223, 2006.

[Was08] Lawrence C Washington. *Elliptic curves: number theory and cryptography.* CRC press, 2008.

[Wei40] André Weil. Sur les fonctions algébriques à corps de constantes fini. *CR Acad. Sci. Paris*, 210(1940):592–594, 1940.

[Won13] Angela Wong. Primality test using elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-7})$. University of California, Irvine, Ph.D. Thesis: https://search.proquest.com/docview/1417083574?accountid=11219, 2013.

[Xin96] Chaoping Xing. On supersingular abelian varieties of dimension two over finite fields. *Finite Fields Appl.*, 2(4):407–421, 1996.