Algebraic curves over finite fields

Soomro, Muhammad Afzal

Rijksuniversiteit Groningen

Algebraic curves over finite fields

Proefschrift

ter verkrijging van het doctoraat in de
Wiskunde en Natuurwetenschappen
aan de Rijksuniversiteit Groningen
op gezag van de
Rector Magnificus, dr. E. Sterken,
in het openbaar te verdedigen op
maandag 10 juni 2013
om 09.00 uur

door

Muhammad Afzal Soomro

geboren op 15 januari 1985
te Larkana, Pakistan

Promotor:	Prof. dr. J. Top
Beoordelingscommissie:	Prof. dr. J.S. Chahal
	Prof. dr. F. Hess
	Prof. dr. C. Ritzenthaler

ISBN: 978-90-367-6269-4 (printed version)
ISBN: 978-90-367-6268-7 (electronic version)

Algebraic curves over finite fields

Muhammad Afzal Soomro

rijksuniversiteit
groningen

This PhD project was carried out at the Johann Bernoulli Institute according to the requirements of the Graduate School of Science (Faculty of Mathematics and Natural Sciences, University of Groningen, the Netherlands).

Funding was provided to me as a PhD student from QUEST, the Quaid-e-awam University of Engineering, Science and Technology, Nawabshah, Sindh, Pakistan using a HEC (Higher Education Commission) grant.

Contents

Chapter 1

Introduction

Algebraic curves over finite fields is a fascinating topic in number theory and algebraic geometry. Moreover, it has applications in different fields such as cryptography, coding theory. Namely, such curves can be used to construct error-correcting codes (see, e.g., [31]), and also for devising secure protocols for data communication (see, e.g., [18]).

By a curve we mean a smooth geometrically irreducible curve. Let C be a curve of genus g over a finite field $\mathbb{F}_q$. Triggered by the applications, mathematicians such as Ihara, Serre, Vladut and Drin'feld studied the maximal number of points on such curves. The maximal number of rational points for a fixed finite field and genus is

$$N_q(g) = \max\{\#C(\mathbb{F}_q) : C \text{ is a curve over } \mathbb{F}_q \text{ of genus } g\}.$$

An explicit formula for $N_q(1)$ follows from results of Deuring and Waterhouse [34]. Jean-Pierre Serre in [23] determined $N_q(2)$. For higher genera it is unknown whether a formula for $N_q(g)$ exists. Concerning $N_q(3)$, T. Ibukiyama [10] proved

$$N_{p^{2n}}(3) = p^{2n} + 1 + 6p^n$$

whenever p is prime and $n \geq 1$ is odd. Serre calculated $N_q(3)$ for $q \leq 25$. Moreover he stated the conjecture that a real constant ϵ exists such that

$$N_q(3) \geq q + 1 + 6\sqrt{q} - \epsilon$$

for all q. J. Top in [30] extended Serre's table to all $q \leq 100$. Moreover he proved Serre's conjecture for the case q is a power of 3. J-F. Mestre proved Serre's conjecture for q a power of 7. The general case is still open.

In 1991, Gerard van der Geer and Marcel van der Vlugt [32] started a table of $N_q(g)$ for $g \leq 50$ and q a small power 2 or 3. In 2005, this was embedded in a larger project of determining $N_q(g)$ for all $g \leq 50$ and many small prime powers q. This project is moderated by Gerard van der Geer, Everett Howe, Kristin Lauter and Christophe Ritzenthaler. All the results on $N_q(g)$ are gathered on the website `www.manypoints.org`. The tables are still incomplete. The work of this present thesis project has added a lot of data to this website for cases $g \leq 5$.

1.1 Upper bound

Let C be a curve of genus g over a finite field $\mathbb{F}_q$, where $q = p^n$ for p a prime number an $n \geq 1$ and integer. A point on the curve C is said to be $\mathbb{F}_{q^m}$-rational if it is defined over $\mathbb{F}_{q^m}$; if it is defined over $\mathbb{F}_q$, then it is called rational point. The zeta function of a curve C over finite field $\mathbb{F}_q$ is defined as

$$Z_C(t) := \exp\left(\sum_{m=1}^{\infty} \frac{\#C(\mathbb{F}_{q^m})t^m}{m}\right).$$

In 1948 A. Weil in his book [35] published a proof of the fact that

$$Z_C(t) = \frac{P_1(t)}{(1-t)(1-qt)}$$

for a polynomial $P_1(t) \in 1 + t\mathbb{Z}[t]$ of degree $2g$. Substituting $t = q^{-s}$ for $s \in \mathbb{C}$, the function $\zeta(s) := Z_C(q^{-s})$ has its zeros on the line

$$\frac{1}{2} + i\mathbb{R} \subseteq \mathbb{C}.$$

This is the Riemann Hypothesis for curves over finite fields. Writing

$$P_1(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$$

for $\alpha_i \in \mathbb{C}$, it means that all α_i have absolute value $\sqrt{q}$. From the definition of the zeta-function and the properties above, it follows that

$$\#C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{2g} \alpha_i,$$

so the Riemann-hypothesis implies

$$-2g\sqrt{q} = -\sum_{i=1}^{2g} |\alpha_i| \leq \#C(\mathbb{F}_q) - q - 1 \leq \sum_{i=1}^{2g} |\alpha_i| = 2g\sqrt{q},$$

i.e.,

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

E. Artin's thesis (1921) contains the "Riemann-hypothesis for the zeta function of a hyperelliptic curves over $\mathbb{F}_q$". However, no proof appears. F.K. Schmidt's thesis (1931) extends this to arbitrary curves over finite fields. In particular this implies the conjecture that

$$N_q(g) \leq q + 1 + 2g\sqrt{q}.$$

H. Hasse settled the special case of genus one in 1933, so he showed in particular

$$N_q(1) \leq q + 1 + 2\sqrt{q}.$$

A. Weil proved the general case in 1942/1948. It is called Hasse-Weil bound. An interesting survey of the history of this "Riemann hypothesis for the zeta function of curves over finite fields" was written by Peter Roquette [19, 20, 21]. An improvement by J-P. Serre is from 1982/83 [34], and reads

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

This is a nontrivial improvement. For example, taking $g = 5$ and $q = 41$ then Weil's result states $N_{41}(5) \leq 106$ while Serre's improvement shows $N_{41}(5) \leq 102$. This general bound is now called Hasse-Weil-Serre bound.

The curve C has an Abelian variety associated to it. It is called Jacobian variety of C and denoted by $\mathrm{Jac}(C)$; this is a principally polarised Abelian variety of dimension g. Let $\mathrm{T}_l(\mathrm{Jac}(C))$ be the Tate module of $\mathrm{Jac}(C)$ where l is prime different from p. Then the characteristic polynomial $P_C(t)$ of the $\mathbb{F}_q$-Frobenius Frob_q acting on $\mathrm{T}_l(\mathrm{Jac}(C))$ is a degree $2g$ monic polynomial in $\mathbb{Z}[t]$. The α_i in $P_1(t)$ in zeta function of curves over finite fields have another interpretation in terms of the Tate module of the $\mathrm{Jac}(C)$. The following holds (see [28]).

Proposition 1.1.1 (Tate)**.** The $\mathbb{F}_q$-Frobenius Frob_q acting semi-simply on $\mathrm{T}_l(\mathrm{Jac}(C))$ and has eigenvalues $\alpha_1, \ldots, \alpha_{2g}$.

The polynomial $P_C(t)$ is the reciprocal polynomial to the polynomial $P_1(t)$ in the zeta function of curves over finite fields. The number of rational points on C is completely determined by the action of Frob_q on $\mathrm{T}_l(\mathrm{Jac}(C))$. Denote the trace of Frob_q by t. Since the trace is the sum of roots of the eigenvalues, we can write

$$\#C(\mathbb{F}_q) = q + 1 - t.$$

Generally, the Riemann hypothesis for Abelian varieties over finite fields implies that for an Abelian variety A the polynomial $P_A(t)$ lies in $\mathbb{Z}[t]$; it has degree twice the dimension of A, and its complex roots lie on the circle $|z| = \sqrt{q}$. The polynomial $P_A(t)$ contains more information.

Theorem 1.1.2 (Tate)**.** Let A and B be Abelian varieties over $\mathbb{F}_q$. Then $P_A(t) = P_B(t)$ if and only if A and B are isogenous over $\mathbb{F}_q$.

1.2 Maximal Curves

Definition 1.2.1. A curve is called maximal if the number of rational points attains the Hasse-Weil-Serre bound, i.e.,

$$\#C(\mathbb{F}_q) = q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

The following proposition shows that $C/\mathbb{F}_q$ can not be maximal if the genus is large with respect to q.

Proposition 1.2.2. Suppose that $C/\mathbb{F}_q$ is a maximal curve. Then $g \leq q$.

Proof. Y. Ihara in [11] showed that

$$N_q(g) \leq q + 1 + \lfloor \frac{\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g}{2} \rfloor.$$

If $C/\mathbb{F}_q$ has genus g and is maximal, then

$$g\lfloor 2\sqrt{q} \rfloor \leq \frac{\sqrt{(8q+1)g^2 + 4(q^2-q)g} - g}{2},$$

hence

$$g\lfloor 2\sqrt{q} \rfloor \leq \sqrt{2q + \frac{1}{4} + \frac{q^2-q}{g}} - \frac{1}{2}.$$

Now assume $g \geq q$. Then

$$\sqrt{2q + \frac{1}{4} + \frac{q^2 - q}{g}} - \frac{1}{2} \leq \sqrt{3q - \frac{3}{4}},$$

which yields a contradiction. □

Example 1.2.3. Take $q = 41$ and $g = 5$. Then the Hasse-Weil-Serre bound equels 102 while Ihara's bound is 140. So here the Hasse-Weil-Serre bound is much better.

Increasing the genus in this case, for all $g \leq 21$ the Hasse-Weil-Serre bound in better, and for $g = 22$ both bounds are 306. For $g \geq 23$ the Ihara bound is better. In particular, this indicates that the bound given in Proposition 1.2.2 is not the best possible.

The classical example of a maximal curve is the Hermitian curve H over $\mathbb{F}_{q^2}$. The curve H is the curve in $\mathbb{P}^2$ given by the equation

$$Y^q Z + Y Z^q = X^{q+1}.$$

This curve has genus $q(q-1)/2$ and $\#H(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq = q^3 + 1$.

Suppose we have a curve C over $\mathbb{F}_q$ of genus g and a surjective morphism $\phi : C \longrightarrow D$ defined over $\mathbb{F}_q$. If $C/\mathbb{F}_q$ is maximal, then so is $D/\mathbb{F}_q$. Namely, maximality is equivalent to the statement that the set $\{\alpha_1, \ldots, \alpha_{2g}\}$ equals $\{\alpha, \bar{\alpha}\}$ with $\alpha + \bar{\alpha} = \lfloor \sqrt{4q} \rfloor$. The eigenvalues of Frobenius corresponding to $D/\mathbb{F}_q$ are a subset closed under complex conjugation of those of $C/\mathbb{F}_q$, and this implies the assertion.

Vice versa, suppose that one has surjective morphisms

$$\phi_i : C \longrightarrow D_i,$$

defined over $\mathbb{F}_q$, and that

$$\bigoplus_i \phi_i^* H^0(D_i, \Omega^1_{D_i}) \simeq H^0(C, \Omega^1_C).$$

Then the sum of induced morphisms

$$\mathrm{Jac}(\phi_i) : \mathrm{Jac}(D_i) \longrightarrow \mathrm{Jac}(C)$$

of group varieties, i.e.,

$$\sum_{i=1}^{n} \mathrm{Jac}(\phi_i) : \mathrm{Jac}(D_1) \times \cdots \times \mathrm{Jac}(D_n) \longrightarrow \mathrm{Jac}(C)$$

defines an isogeny. Therefore if t_i denotes the trace of Frobenius of $D_i/\mathbb{F}_q$, then

$$\#C(\mathbb{F}_q) = q + 1 + \sum_{i=1}^{n} t_i.$$

In particular if the curves $D_1, \ldots, D_n$ are maximal then the curve C is maximal. For example, the curve $\tilde{D}$ of genus 7 given by the equations

$$\begin{cases} y^2 = x^5 + x, \\ z^2 = x^5 - x \end{cases}$$

See Example 4.2.5 for more details.

Definition 1.2.4. A curve C over $\mathbb{F}_q$ is called "good" if the number of rational points on the curve is within 10 percent of the Hasse-Weil-Serre bound.

For example, taking $g = 5$ and $q = 41$ as above, a good curve of genus over $\mathbb{F}_{41}$ would be a curve $C/\mathbb{F}_{41}$ of genus 5 with $\#C(\mathbb{F}_{41}) \geq 92$. At present we do not know any good curve $C/\mathbb{F}_{41}$ of genus 5.

Chapter 2

Elliptic curves with many points over small fields

We denote by $N_q(1)$ the maximal number of rational points that an elliptic curve E over a finite field $\mathbb{F}_q$ of cardinality q can have. This is the special case $g = 1$ of more general notation $N_q(g)$ for the maximal number of rational points that a curve over $\mathbb{F}_q$ of genus g can have. A result of Deuring and Waterhouse (see [34, Thm. 4.1]); for an exposition see also [23, p. 15-16]) states that

$$N_q(1) = \begin{cases} q+m & \text{if } q = p^e \ \& \ e \geq 5 \text{ is odd } \& \ p|m; \\ q+m+1 & \text{otherwise.} \end{cases}$$

Here p is the characteristic of $\mathbb{F}_q$ and $m = \lfloor 2\sqrt{q} \rfloor$ is the largest integer less than or equal to $2\sqrt{q}$.

In this chapter we present, for many small q, a maximal elliptic curve, i.e., elliptic curve over $\mathbb{F}_q$ attaining this bound. More precisely this is done for every $q = p^n$ with $p \leq 19$ a prime number and $1 < n \leq 5$ and also for all $q = p \leq 97$ a prime number. The examples were computed using the computer algebra packages Maple, Magma and the free mathematics software system Sage. The results obtained below were used to complete the data for $g = 1$ in the tables maintained on the website `http://www.manypoints.org`.

2.1 The prime fields

Over $\mathbb{F}_2$ the equation $y^2+y = x^3+x$ defines an elliptic curve with $N_2(1) = 5$ rational points. For odd prime numbers p, we search over equations $y^2 = x^3 + ax + b$ satisfying $4a^3 + 27b^2 \neq 0$ in order to find an example with

$N_p(1) = p + 1 + \lfloor 2\sqrt{p} \rfloor$ rational points. Using Maple this is very simple for small p. The result is given in the following table.

p	$N_p(1)$	Elliptic Curve
2	5	$y^2 + y = x^3 + x$
3	7	$y^2 = x^3 + 2x + 1$
5	10	$y^2 = x^3 + 3x$
7	13	$y^2 = x^3 + 3$
11	18	$y^2 = x^3 + x + 3$
13	21	$y^2 = x^3 + 4$
17	26	$y^2 = x^3 + 3x$
19	28	$y^2 = x^3 + 8$
23	33	$y^2 = x^3 + x + 11$
29	40	$y^2 = x^3 + 4x$
31	43	$y^2 = x^3 + 3$
37	50	$y^2 = x^3 + 2x$
41	54	$y^2 = x^3 + 2x + 4$
43	57	$y^2 = x^3 + 9$
47	61	$y^2 = x^3 + x + 38$
53	68	$y^2 = x^3 + x$
59	75	$y^2 = x^3 + 2x + 22$
61	77	$y^2 = x^3 + 6x + 29$
67	84	$y^2 = x^3 + 1$
71	88	$y^2 = x^3 + x + 9$
73	91	$y^2 = x^3 + 5$
79	97	$y^2 = x^3 + 3$
83	102	$y^2 = x^3 + 2x + 19$
89	108	$y^2 = x^3 + x + 8$
97	117	$y^2 = x^3 + 2$

2.2 Fields of cardinality p^2

To find examples of elliptic curves over $\mathbb{F}_{p^2}$ having $N_{p^2}(1) = p^2 + 1 + 2p$ rational points, we use the following lemma.

Lemma 2.2.1. Suppose $E/\mathbb{F}_q$ is an elliptic curve. Then

$$\#E(\mathbb{F}_{q^2}) = q^2 + 1 + 2q \Leftrightarrow \#E(\mathbb{F}_q) = q + 1.$$

Proof. (Compare [26, Chapter V, § 2] and [33, Chapter 4,§ 3].) Let $\#E(\mathbb{F}_q) =$

$q+1-a$. Write $X^2 - aX + q = (X-\alpha)(X-\beta)$ with $\alpha, \beta \in \mathbb{C}$. Then

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$$

for all $n \geq 1$. So in particular one has $\#E(\mathbb{F}_{q^2}) = q^2 + 1 - \alpha^2 - \beta^2$. This implies

$$\begin{aligned} \#E(\mathbb{F}_{q^2}) = q^2 + 1 + 2q \quad &\Leftrightarrow \quad \alpha^2 + \beta^2 = -2q \\ &\Leftrightarrow \quad \alpha^2 + \beta^2 + 2\alpha\beta = 0 \\ &\Leftrightarrow \quad (\alpha+\beta)^2 = 0 \\ &\Leftrightarrow \quad \alpha + \beta = 0 \\ &\Leftrightarrow \quad \#E(\mathbb{F}_q) = q+1, \end{aligned}$$

which proves the lemma. □

More generally, any elliptic curve over $\mathbb{F}_q$, having precisely $q+1$ rational points, will have $q^n + 1 + 2q^{n/2}$ rational points over the field $\mathbb{F}_{q^n}$ whenever $n \equiv 2 \pmod 4$.

To have explicit examples, first note that for $p = 2$ the equation $y^2 + y = x^3$ defines an elliptic curve with exactly $3 = p + 1$ rational points over $\mathbb{F}_2$. Next, for every prime number $p \equiv 5 \pmod 6$ the equation $y^2 = x^3 + 1$ defines an elliptic curve with precisely $p + 1$ rational points over $\mathbb{F}_p$ (This is well-known; compare, e.g., [27, Exerc. IV-4.10]). Similarly (see [27, Exerc. IV-4.8]) for every prime number $p \equiv 3 \pmod 4$ the equation $y^2 = x^3 + x$ defines an elliptic curve whose number of rational points over $\mathbb{F}_p$ equals $p + 1$.

With these remarks we have examples for every prime $\not\equiv 1 \pmod{12}$. In particular, we have such a curve for all $p \leq 19$ except $p = 13$. One has $\#E(\mathbb{F}_{13}) = 14$ for the elliptic curve $E:\ y^2 = x^3 + x + 4$.

This discussion is summarized in the following table.

p	$N_{p^2}(1)$	Elliptic Curve
2	9	$y^2 + y = x^3$
3	16	$y^2 = x^3 + x$
5	36	$y^2 = x^3 + 1$
7	64	$y^2 = x^3 + x$
11	144	$y^2 = x^3 + x$
13	196	$y^2 = x^3 + x + 4$
17	324	$y^2 = x^3 + 1$
19	400	$y^2 = x^3 + x$

Alternatively, one may extend the argument as follows, using [25, Prop. 2.3.1]. The elliptic curve E given by $y^2 = x^3 + 4x^2 + 2x$ has an endomorphism ϕ satisfying $\phi^2 = -2$. As a consequence, E defines a supersingular elliptic

curve in every odd characteristic p such that -2 is not a square modulo p, i.e., $p \equiv 5, 7 \pmod 8$. Similarly, $E : y^2 = x^3 - 35x + 98$ has an endomorphism ψ satisfying $\psi^2 + \psi + 2 = 0$. So E is supersingular in every characteristics p such that the polynomial $X^2 + X + 2 \in \mathbb{F}_p[X]$ is irreducible, i.e., for $p \equiv 3, 5, 6 \pmod 7$. In particular $\#E(\mathbb{F}_p) = p + 1$ for such p.

Combining the curves given here, only for primes $p \equiv 1, 25, 121 \pmod{168}$ we did not present an explicit elliptic curve over $\mathbb{F}_p$ with $p + 1$ points. The smallest such prime is 193.

2.3 Fields of cardinality p^3

We used two methods for finding elliptic curves $E/\mathbb{F}_{p^3}$ with $\#E(\mathbb{F}_{p^3}) = N_{p^3}(1) = p^3 + 1 + \lfloor 2p\sqrt{p} \rfloor$.

2.3.1 Using curves over $\mathbb{F}_p$

If $E/\mathbb{F}_p$ satisfies $\#E(\mathbb{F}_p) = p + 1 + a$, then

$$\#E(\mathbb{F}_{p^3}) = p^3 + 1 + a^3 - 3pa.$$

So if a satisfies

$$a^3 - 3pa = \lfloor 2p\sqrt{p} \rfloor,$$

this reduces the problem of finding a maximal elliptic curve over $\mathbb{F}_{p^3}$ to the problem of finding one with $p + 1 + a$ points over $\mathbb{F}_p$.

This works for $p \in \{2, 3, 5, 11, 17\}$, with $a = -1, -2, -2, -3, -4$, respectively. For $p \in \{7, 13, 19\}$ this method does not work, since in that case the equation $a^3 - 3pa = \lfloor 2p\sqrt{p} \rfloor$ has no solution in $a \in \mathbb{Z}$ satisfying $|a| \leq 2\sqrt{p}$. We return to this equation $a^3 - 3pa - \lfloor 2p\sqrt{p} \rfloor = 0$ in Section 2.7.

2.3.2 Using a family with j-invariant j

Let $j_0 \in \overline{\mathbb{F}}_q$. There exists an elliptic curve over $\mathbb{F}_q(j_0)$ whose j-invariant is equal to j_0. It is given by the equation

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}, \tag{2.1}$$

provided $j_0 \neq 0, 1728$(see [26, Chap.III, Prop.1.4]). We searched for elliptic curves with many points in this form (2.1). This made the search much more efficient; because, every j-invariant $\neq 0, 1728$ occurs in this family only once. Our algorithm searches $j_0 \in \mathbb{F}_{p^3}^* \backslash \{1728\}$ such that the curve given by (2.1)

has $p^3 + 1 \pm \lfloor 2p\sqrt{p} \rfloor$ rational points. Once this is found, Lemma 2.4.1 or Lemma 2.4.2 below explains how to obtain a curve with $p^3 + 1 + \lfloor 2p\sqrt{p} \rfloor$ rational points, if necessary.

Write $\mathbb{F}_{p^3} = \mathbb{F}_p[\alpha]$ in which α satisfies $g(\alpha) = 0$ for a monic irreducible $g \in \mathbb{F}_p[X]$ of degree 3. Note that if E is defined over $\mathbb{F}_{p^3}$, then the p-power Frobenius map defines an isomorphism $E(\mathbb{F}_{p^3}) \cong E^{(p)}(\mathbb{F}_{p^3})$. Here $E^{(p)}$ denotes the elliptic curve obtained from E by raising the coefficients of its equation to the power p. In particular, in an equation involving α the number of points does not depend on which zero of g in $\mathbb{F}_p[\alpha]$ is taken.

p	$N_{p^3}(1)$	Elliptic Curve	Minimal Polynomial of α
2	14	$y^2 + xy + y = x^3 + 1$	
3	38	$y^2 = x^3 + 2x^2 + 2x$	
5	148	$y^2 = x^3 + x + 2$	
7	381	$y^2 = x^3 + \alpha^2$	$X^3 + 6X^2 + 4$
11	1404	$y^2 = x^3 + x + 4$	
13	2291	$y^2 = x^3 + \alpha^2 x + \alpha^{75}$	$X^3 + 2X + 11$
17	5054	$y^2 = x^3 + x + 4$	
19	7025	$y^2 = x^3 + \alpha^2 x + \alpha^9$	$X^3 + 4X + 17$

Here we give some simple Magma code for checking the number of points of the elliptic curves in the above table. We illustrate this for the case $p = 7$. First we define the field extension using an irreducible polynomial in $\mathbb{F}_5[X]$ and then we find the number of points on the specified elliptic curve over the obtained field.

```
Fp:=GF(7);
P<X>:=PolynomialRing(Fp);
Fp3<alpha>:=ext<Fp|X^3+6*X^2+4>;
#EllipticCurve([Fp3|0,alpha^2]);
```

2.4 Fields of cardinality p^4

If an elliptic curve E over a finite field $\mathbb{F}_q$ satisfies $\#E(\mathbb{F}_q) = q + 1$, then, by the same calculation as is done in Lemma 2.2.1, one can prove that $\#E(\mathbb{F}_{q^4}) = q^4 + 1 - 2q^2$. Using the following two lemmas one can see that the "quadratic twist" E^{tw} of E over $\mathbb{F}_{q^4}$ satisfies $\#E^{\mathrm{tw}}(\mathbb{F}_{q^4}) = q^4 + 1 + 2q^2 = N_{q^4}(1)$.

Lemma 2.4.1. Suppose q is odd, and let $C/\mathbb{F}_q$ be the hyperelliptic curve corresponding to an equation $y^2 = f(x)$ with $f \in \mathbb{F}_q[X]$ square free. Suppose

$\alpha \in \mathbb{F}_q^*$ is not a square. Define the hyperelliptic curve $C^{\mathrm{tw}}/\mathbb{F}_q$ corresponding to the equation $\alpha y^2 = f(x)$. Then

$$\#C(\mathbb{F}_q) + \#C^{\mathrm{tw}}(\mathbb{F}_q) = 2q + 2. \tag{2.2}$$

Proof. Let $x_0 \in \mathbb{F}_q$; If $f(x_0) = 0$, then this contributes one point $(x_0, 0)$ to both curves. If $f(x_0) \in \mathbb{F}_q^{*^2}$, then this contributes 2 points to C and 0 points to C^{tw}. If $f(x_0) \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*^2}$, then this contributes 0 points to C and 2 points to C^{tw}.

Finally, consider points at infinity. If f has odd degree, then both C and C^{tw} have one rational point at infinity. If f has even degree and leading coefficient in $\mathbb{F}_q^{*^2}$, then C has 2 points at infinity, but C^{tw} has no point at infinity. In the remaining case C^{tw} has 2 points at infinity and C has none. Therefore $\#C(\mathbb{F}_q) + \#C^{\mathrm{tw}}(\mathbb{F}_q) = 2q + 2$. □

For instance, take an elliptic curve $E : y^2 = x^3 + Ax^2 + Bx + C$ over a finite field $\mathbb{F}_q$ of odd characteristic. If $\#E(\mathbb{F}_q) = q + 1$, then $\#E(\mathbb{F}_{q^4}) = q^4 + 1 - 2q^2$. We take a nonsquare $\alpha \in \mathbb{F}_{q^4}^*$ and write another elliptic curve $E^{\mathrm{tw}} : \alpha y^2 = x^3 + Ax^2 + Bx + C$, equivalently $y^2 = x^3 + \alpha Ax^2 + \alpha^2 Bx + \alpha^3 C$. Since

$$\#E(\mathbb{F}_{q^4}) + \#E^{\mathrm{tw}}(\mathbb{F}_{q^4}) = 2q^4 + 2,$$

by using Lemma 2.4.1, this implies

$$\#E^{\mathrm{tw}}(\mathbb{F}_{q^4}) = q^4 + 1 + 2q^2.$$

Hence E^{tw} is the required maximal elliptic curve over $\mathbb{F}_{q^4}$.

Lemma 2.4.2. Suppose $q = 2^n$. Furthermore, assume that

$$E/\mathbb{F}_q : y^2 + (a_1 x + a_3)y = f(x),$$

with $f(x)$ monic of degree 3, defines an elliptic curve over $\mathbb{F}_q$. Write $\mathbb{F}_{q^2} = \mathbb{F}_q(\beta)$, where β satisfies the irreducible polynomial $X^2 + X + a$ for some $a \in \mathbb{F}_q$. Then

$$E^{\mathrm{tw}} : \eta^2 + (a_1\xi + a_3)\eta = f(\xi) + a(a_1\xi + a_3)^2$$

defines an elliptic curve over $\mathbb{F}_q$ which is over $\mathbb{F}_q(\beta)$ isomorphic to E and satisfies

$$\#E(\mathbb{F}_q) + \#E^{\mathrm{tw}}(\mathbb{F}_q) = 2q + 2.$$

Proof. The map

$$(\xi, \eta) \mapsto (\xi, \eta + a_1\beta\xi + a_3\beta)$$

defines an isomorphism $E^{\mathrm{tw}} \cong E$ over $\mathbb{F}_q(\beta)$. In particular, this shows that E^{tw} is an elliptic curve.

It remains to show the assertion on the number of points. Take $x_0 \in \mathbb{F}_q$; let $a_1x_0 + a_3 = \lambda$ and $f(x_0) = \delta$. So with $y_0, \eta_0 \in \overline{\mathbb{F}}_q$ one finds $(x_0, y_0) \in E$ iff

$$y_0^2 + \lambda y_0 + \delta = 0, \tag{2.3}$$

and $(x_0, \eta_0) \in E^{\mathrm{tw}}$ iff

$$\eta_0^2 + \lambda\eta_0 + \delta + a\lambda^2 = 0. \tag{2.4}$$

For each $x_0 \in \mathbb{F}_q$, we have one of the following four cases.

1. $\delta = 0$ and $\lambda = 0$;
2. $\delta = 0$ and $\lambda \neq 0$;
3. $\delta \neq 0$ and $\lambda = 0$;
4. $\delta \neq 0$ and $\lambda \neq 0$.

We consider these cases one by one.

1. $\delta = 0$ and $\lambda = 0$: In this case we obtain one rational point, namely $(x_0, 0)$, on both E and E^{tw}.

2. $\delta = 0$ and $\lambda \neq 0$: In this case the equations (2.3) and (2.4) imply

$$y_0^2 + \lambda y_0 = 0, \tag{2.5}$$

$$\eta_0^2 + \lambda\eta_0 = a\lambda^2. \tag{2.6}$$

Clearly (2.5) has precisely 2 solutions, namely $y_0 = 0$ and $y_0 = \lambda$ in $\mathbb{F}_q$. The equation (2.6) has no solution $\eta_0 \in \mathbb{F}_q$, since if η_0 were a solution, then η_0/λ would be a zero of $X^2 + X + a = 0$, contradicting the fact that the polynomial $X^2 + X + a$ is irreducible over $\mathbb{F}_q$.

3. $\delta \neq 0$ and $\lambda = 0$: In this case the equations (2.3) and (2.4) become

$$y_0^2 = \delta,$$

$$\eta_0^2 = \delta.$$

Since 2^{th}-power Frobenius $\mathrm{Fr}_2 : \mathbb{F}_q \to \mathbb{F}_q$ is an automophism, we get precisely one rational point on each curve.

4. $\delta \neq 0$ and $\lambda \neq 0$: In this case equations (2.3) and (2.4) reduce to

$$y_0^2 + \lambda y_0 = \delta, \tag{2.7}$$

$$\eta_0^2 + \lambda \eta_0 = \delta + a\lambda^2. \tag{2.8}$$

Both equations (2.7) and (2.8) can not simultaneously have solutions in $\mathbb{F}_q$, since if y_0 and η_0 were solutions of these equations in $\mathbb{F}_q$, then $(y_0+\eta_0)/\lambda \in \mathbb{F}_q$ would be a zero of $X^2 + X + a = 0$.

Suppose the equation (2.7) has no solution in $\mathbb{F}_q$; then it has 2 solutions in $\mathbb{F}_{q^2} = \mathbb{F}_q(\beta)$. Let $\tilde{y}_0 = y_1 + y_2\beta$, where $y_1, y_2 \in \mathbb{F}_q$ and $y_2 \neq 0$, be one of the solutions of the equation (2.7) in $\mathbb{F}_q(\beta)$. Hence,

$$(y_1 + y_2\beta)^2 + \lambda(y_1 + y_2\beta) = \delta,$$

which can be written, by using that $\beta^2 = \beta + a$, as

$$y_1{}^2 + y_2{}^2\beta + y_2{}^2 a + y_1\lambda + y_2\beta\lambda = \delta. \tag{2.9}$$

Comparing coefficients of β shows

$$y_2{}^2 + \lambda y_2 = 0.$$

Since $y_2 \neq 0$, this implies $y_2 = \lambda$. Hence, equation (2.9) gives

$$y_1{}^2 + \lambda y_1 = \delta + a\lambda^2.$$

Therefore y_1, and also $y_1 + \lambda$, is a solution of the equation (2.8) in $\mathbb{F}_q$. In this case, we see that if E does not have any point over $\mathbb{F}_q$ with x-coordinate x_0, then E^{tw} will have two such points. Vice versa, if (2.7) would have a solution in $\mathbb{F}_q$, then it has 2 such solutions. Since (2.7) and (2.8) cannot simultaneously have a solution, we now have that (2.8) has no solution in $\mathbb{F}_q$. Hence in this case E has two rational points with x-coordinates x_0, and E^{tw} has none.

Consequently, for all $x_0 \in \mathbb{F}_q$,

$$\#\{P \in E(\mathbb{F}_q) | x(P) = x_0\} + \#\{P \in E^{\mathrm{tw}}(\mathbb{F}_q) | \xi(P) = x_0\} = 2.$$

Finally, both the curves have one point at infinity. Therefore $\#E(\mathbb{F}_q) + \#E^{\mathrm{tw}}(\mathbb{F}_q) = 2q + 2$. Hence the lemma follows. □

Remark 2.4.3. The curve $E^{\mathrm{tw}}/\mathbb{F}_q$ is the "quadratic twist" of E corresponding to the class in $H^1\left(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}, \mathrm{Aut}_{\overline{\mathbb{F}}_q}(E)\right)$ of the cocycle defined by

$\mathrm{Fr}_q \mapsto [-1]$, where $\mathrm{Fr}_q \in \mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}$ denotes the q^{th}-power Frobenius automorphism. See [26, Chapter X] and [17] for more details on this. In Section 2.6 below we consider the question whether E^{tw} can be isomorphic to E over the ground field. Note that Lemma 2.4.2 implies that a necessary condition in the case of $\mathbb{F}_q$, to have $E \cong E^{\text{tw}}$, is that $\#E(\mathbb{F}_q) = q + 1$.

For instance, for $q = p$ odd we have the curves over $\mathbb{F}_p$, with precisely $p + 1$ rational points, in Section 2.2. Take a curve $E : y^2 = x^3 + x$, having $\#E(\mathbb{F}_3) = 4$, and $\alpha \in \mathbb{F}_{3^4}$, satisfying $X^4+2X^3+2 = 0$. Since $X^8+2X^6+2 \in \mathbb{F}_3[X]$ is irreducible, this means that α is not square in $\mathbb{F}_{3^4}$. Then the elliptic curve $E^{\text{tw}} : \alpha y^2 = x^3 + x$, equivalently $y^2 = x^3 + \alpha^2 x$, is the required curve, i.e., $\#E^{\text{tw}}(\mathbb{F}_{3^4}) = 100 = N_{3^4}(1)$.

For $q = 2$, the curve $E : y^2 + y = x^3$ has $\#E(\mathbb{F}_2) = 3$. Write $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$ in which α is a zero of $X^4 + X + 1 \in \mathbb{F}_2[X]$. Since $X^2 + X + \alpha^3$ is irreducible over $\mathbb{F}_{2^4}$, then

$$E^{\text{tw}} : y^2 + y = x^3 + \alpha^3$$

is the required elliptic curve, i.e., $\#E^{\text{tw}}(\mathbb{F}_{2^4}) = 25 = N_{2^4}(1)$. This curve E^{tw} is isomorphic to E over $L = \mathbb{F}_{2^4}(\beta)$, where β is a root of $X^2 + X + \alpha^3$. This discussion is summarized in the following table.

p	$N_{p^4}(1)$	Elliptic Curve	Minimal Polynomial of α
2	25	$y^2 + y = x^3 + \alpha^3$	$X^4 + X + 1$
3	100	$y^2 = x^3 + \alpha^2 x$	$X^4 + 2X^3 + 2$
5	676	$y^2 = x^3 + \alpha^3$	$X^4 + 4X^2 + 4X + 2$
7	2500	$y^2 = x^3 + \alpha^2 x$	$X^4 + 5X^2 + 4X + 3$
11	14884	$y^2 = x^3 + \alpha^2 x$	$X^4 + 8X^2 + 10X + 2$
13	28900	$y^2 = x^3 + \alpha^2 x + 4\alpha^3$	$X^4 + 3X^2 + 12X + 2$
17	84100	$y^2 = x^3 + \alpha^3$	$X^4 + 7X^2 + 10X + 3$
19	131044	$y^2 = x^3 + \alpha^2 x$	$X^4 + 2X^2 + 11X + 2$

2.5 Fields of cardinality p^5

We searched for elliptic curves over $\mathbb{F}_{p^5}$ with $N_{p^5}(1)$ points using the two methods also described in Sections 2.3.1 and 2.3.2.

The first method reduces the problem of finding a maximal curve over $\mathbb{F}_{p^5}$ to the problem of finding one with $p + 1 + a$ points over $\mathbb{F}_p$, where

$$a^5 - 5pa^3 + 5p^2a = \begin{cases} \lfloor 2p^2\sqrt{p} \rfloor - 1 & \text{if } p \mid \lfloor 2p^2\sqrt{p} \rfloor; \\ \lfloor 2p^2\sqrt{p} \rfloor & \text{otherwise.} \end{cases}$$

This method works for $p \in \{2, 3, 11\}$, with, respectively, $a = 1, 1, 2$. For $p \in \{5, 7, 13, 17, 19\}$ this method does not work.

The elliptic curves in the following table were found by using the mathematics software systems Sage and Magma.

p	$N_{p^5}(1)$	Elliptic Curve	Minimal Polynomial of z
2	44	$y^2 + xy + y = x^3 + x^2 + x$	
3	275	$y^2 = x^3 + 2x^2 + x + 1$	
5	3237	$y^2 = x^3 + \alpha^{97}x + 1$	$X^5 + 4X + 3$
7	17066	$y^2 = x^3 + x + \alpha^{601}$	$X^5 + X + 4$
11	161854	$y^2 = x^3 + x + 1$	
13	372512	$y^2 = x^3 + \alpha x + \alpha^{333760}$	$X^5 + 4X + 11$
17	1422241	$y^2 = x^3 + 5x^2 + \alpha^{1351944}x + \alpha^{198311}$	$X^5 + X + 14$
19	2479247	$y^2 = x^3 + 5x^2 + \alpha^{508237}x + \alpha^{1608725}$	$X^5 + 5X + 17$

To verify these results for $p \in \{5, 7, 13, 17, 19\}$, one may use a simple Magma program similar to the one presented in Section 2.3.

2.6 Quadratic twists of an elliptic curve

Let E/K be an elliptic curve over a field K. A twist of E is an elliptic curve E^{tw}/K that is isomorphic to E over a separable closure of K. Two such twists are considered equal if they are isomorphic over K. We denote the set of twists by $\mathrm{Twist}(E/K)$. The elements of $\mathrm{Twist}(E/K)$ are in one-to-one correspondence with the classes in $H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right)$ [26, § X.2].

Remark 2.6.1. Note that we consider elliptic curves, i.e., pairs $(E, O)/K$, where E is a curve of genus one and $O \in E(K)$, and we consider $\mathrm{Aut}_{\bar{K}}(E)$, i.e., the group of isomorphisms from E to E that send O to O. The set of twists over K we consider are denoted as $\mathrm{Twist}((E, O)/K)$ in Silverman's book [26].

The set of quadratic twists of E, i.e.,

$$QT(E) = \left\{E^{\mathrm{tw}}/K \text{ elliptic curve} \mid \exists\ L/K \mathrm{of\,deg}\, 2 \text{ s.t. } E^{\mathrm{tw}} \cong_L E\right\} /_{\cong_K}$$

is a subset of $\mathrm{Twist}(E/K)$; this subset of quadratic twists corresponds to the image of $H^1\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right)$ in the set $H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right)$, under the map induced by the inclusion $< -1 > \subset \mathrm{Aut}_{\bar{K}}(E)$. Here $< -1 >=$

$\{\mathrm{id}, -1\}$ is the subgroup of $\mathrm{Aut}_{\bar{K}}(E)$ generated by the -1 map. Here we consider the question whether E^{tw} can be isomorphic to E over the ground field. In other words, when does E^{tw} correspond to the trivial element in $H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right)$, assuming that it comes from a nontrivial element in $H^1\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right) = \mathrm{Hom}\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right)$.

Proposition 2.6.2. Suppose that $\mathrm{Aut}_{\bar{K}}(E)$ is abelian, which means we exclude the case $j(E) = 0$ in $\mathrm{char}(K) \in \{2, 3\}$. Then the map

$$i : H^1\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right) \longrightarrow H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right)$$

is injective except in the case when $\mathrm{char}(K) \notin \{2, 3\}$, $j(E) = 12^3$ and $\mathrm{G}_{\bar{K}/K}$ acts nontrivially on $\mathrm{Aut}_{\bar{K}}(E)$.

Proof. We have the following long exact sequence of groups.

$$\begin{array}{l} 1 \longrightarrow H^0\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right) \longrightarrow H^0\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \pi \\ \longrightarrow H^0\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) \longrightarrow H^1\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i \\ \longrightarrow H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right) \longrightarrow H^1\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) \end{array}$$

Note that $H^0\left(\mathrm{G}_{\bar{K}/K}, < -1 >\right) =< -1 >$. By [26, Chap. III, Cor. 10.2], we have the following automorphism groups of an elliptic curve.

1. $\mathrm{Aut}_{\bar{K}}(E) = \mathbb{Z}/2\mathbb{Z}$, when $j(E) \neq 0, 12^3$;
2. $\mathrm{Aut}_{\bar{K}}(E) = \mathbb{Z}/4\mathbb{Z}$, when $j(E) = 12^3$ and $\mathrm{char}(K) \notin \{2, 3\}$;
3. $\mathrm{Aut}_{\bar{K}}(E) = \mathbb{Z}/6\mathbb{Z}$, when $j(E) = 0$ and $\mathrm{char}(K) \notin \{2, 3\}$.

We consider each case separately.

1. Since $\#\mathrm{Aut}_{\bar{K}}(E) = 2$, the Galois group $\mathrm{G}_{\bar{K}/K}$ acts trivially on $\mathrm{Aut}_{\bar{K}}(E)$. Therefore, $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) = 1$. Hence, the map i is injective. This proves the proposition in this case.

2. First, suppose $\mathrm{G}_{\bar{K}/K}$ acts trivially on $\mathrm{Aut}_{\bar{K}}(E) \cong \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$. Again, here we see $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) = 2$. Hence, the first four groups in the above long exact sequence have the following orders, respectively.

$$1 \longrightarrow 2 \longrightarrow 4 \xrightarrow{\pi} 2 \longrightarrow$$

This implies that π is surjective, and, therefore, i is injective. The proposition follows.

Now, suppose $\mathrm{G}_{\bar{K}/K}$ acts nontrivially on $\mathrm{Aut}_{\bar{K}}(E)$. If $\rho \in \mathrm{G}_{\bar{K}/K}$ acts nontrivially on $\mathrm{Aut}_{\bar{K}}(E)$, then we must have

$$\begin{aligned}\rho(0) &= 0;\\ \rho(1) &= 3;\\ \rho(2) &= 2;\\ \rho(3) &= 1.\end{aligned}$$

Therefore, $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right) = 2$. Now, the action of ρ on

$$\frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>} = \{\{0,2\},\{1,3\}\}$$

is

$$\begin{aligned}\rho(\{0,2\}) &= \{0,2\},\\ \rho(\{1,3\}) &= \{1,3\}.\end{aligned}$$

This implies that $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) = 2$. Hence, the first four groups in the long exact sequence have the following orders, respectively.

$$1 \longrightarrow 2 \longrightarrow 2 \xrightarrow{\pi} 2 \longrightarrow$$

This implies that π is the zero map, and, therefore, i is not injective. In fact $\#\mathrm{Ker}(i) = 2$. The proposition follows in this case.

3. First, if $\mathrm{G}_{\bar{K}/K}$ acts trivially on $\mathrm{Aut}_{\bar{K}}(E) \cong \mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$, then $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right) = 6$ and $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) = 3$. The first four groups in the long exact sequence have the following orders, respectively.

$$1 \longrightarrow 2 \longrightarrow 6 \xrightarrow{\pi} 3 \longrightarrow$$

This implies that π is surjective; therefore, because the sequence is exact, i is injective.

Now, suppose $\mathrm{G}_{\bar{K}/K}$ acts nontrivially on $\mathrm{Aut}_{\bar{K}}(E)$. If $\rho \in \mathrm{G}_{\bar{K}/K}$ acts nontrivially on $\mathrm{Aut}_{\bar{K}}(E)$, then we must have

$$\begin{aligned}\rho(0) &= 0;\\ \rho(1) &= 5;\\ \rho(2) &= 4;\\ \rho(3) &= 3;\\ \rho(4) &= 2;\\ \rho(5) &= 1.\end{aligned}$$

Therefore, also in this case, $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\bar{K}}(E)\right) = 2$. Now, the action of ρ on

$$\frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>} = \{\{0,3\},\{1,4\},\{2,5\}\}$$

is

$$\begin{aligned}\rho(\{0,3\}) &= \{0,3\},\\ \rho(\{1,4\}) &= \{2,5\};\\ \rho(\{2,5\}) &= \{1,4\}.\end{aligned}$$

This implies that $\#H^0\left(\mathrm{G}_{\bar{K}/K}, \frac{\mathrm{Aut}_{\bar{K}}(E)}{<-1>}\right) = 1$. The first four groups in the above long exact sequence have the following orders, respectively.

$$1 \longrightarrow 2 \longrightarrow 2 \xrightarrow{\pi} 1 \longrightarrow$$

Therefore, we see that π is surjective, and, hence, i is injective. This completes the proof of the proposition. □

Example 2.6.3. Take

$$E/\mathbb{Q} : y^2 = x^3 - x.$$

Then

$$\mathrm{Aut}_{\bar{\mathbb{Q}}}(E) \cong \{\pm 1, \pm\iota\},$$

where $\iota : E \to E$ is defined by $(x,y) \mapsto (-x, \sqrt{-1}y)$ for a fixed choice of $\sqrt{-1} \in \bar{\mathbb{Q}}$.

For $d \in \mathbb{Q}^*$ write

$$E^{(d)} : y^2 = x^3 - d^2x.$$

Then $E^{(d)}$ is a twist of $E/\mathbb{Q}$, since $\psi_d : E \to E^{(d)}$ defined as

$$\psi_d(x,y) = (dx, d\sqrt{d}y).$$

defines an isomorphism.

If $\rho \in \mathrm{G}_{\bar{\mathbb{Q}}/\mathbb{Q}}$, then

$$({}^{\rho}\psi_d)^{-1} \circ \psi_d = \begin{cases} 1 & \text{if } \rho(\sqrt{d}) = \sqrt{d}; \\ -1 & \text{if } \rho(\sqrt{d}) = -\sqrt{d}. \end{cases}$$

So $E^{(d)}$ corresponds to the cocycle class of

$$\rho \mapsto \frac{\rho(\sqrt{d})}{\sqrt{d}} \in \mathrm{Aut}_{\bar{\mathbb{Q}}}(E).$$

In case $d = -1$, this cocycle is a coboundary, since

$$\frac{\rho(\sqrt{-1})}{\sqrt{-1}} = ({}^{\rho}\iota)^{-1} \circ \iota.$$

So $E^{(-1)} \cong E$ over $\mathbb{Q}$, which is, of course, evident from the equation.

Example 2.6.4. Take q a power of an odd prime, and

$$E/\mathbb{F}_q : y^2 = x^3 - x.$$

The Galois group $\mathrm{G}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}$ acts nontrivially on $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(E) \Leftrightarrow \sqrt{-1} \notin \mathbb{F}_q \Leftrightarrow q \equiv 3 \mod (4)$. For $d \in \mathbb{F}_q^*$, define $E^{(d)}/\mathbb{F}_q$ as before. This defines a quadratic twist as in Example 2.6.3.

If d is not a square and $q \equiv 1 \mod (4)$, then $E^{(d)}$ defines the (unique) nontrivial quadratic twist of $E/\mathbb{F}_q$. If d is not a square and $q \equiv 3 \mod (4)$, then $-d$ is a square, and $E^{(d)} = E^{(-d)} \cong E$ ove $\mathbb{F}_q$. So for $q \equiv 3 \mod (4)$, a nontrivial quadratic twist of $E/\mathbb{F}_q$ does not exists.

Example 2.6.5. Take

$$E/\mathbb{F}_2 : y^2 + y = x^3.$$

Then $j(E)$=0. First, we find $\mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)$. By using the formulae given in [26, Table 3.1] one finds all 24 automorphisms. They are described as

$$\Phi_{u,r,t} : E \longrightarrow E$$

$$\Phi_{u,r,t} : (x, y) \mapsto (u^2x + r, u^3y + u^2r^2x + t),$$

where $u \in \mathbb{F}_4^*, r \in \mathbb{F}_4$ and $t^2 + t + r^3 = 0$. Note that with $r \in \mathbb{F}_4$ one has $r^3 = 1$ if $r \neq 0$ and $r^3 = 0$ for $r = 0$. In particular for given r the two possibilities for t are in $\mathbb{F}_4 \backslash \mathbb{F}_2$ when $r \neq 0$ and in $\mathbb{F}_2$ otherwise.

$$\mathrm{Aut}_{\overline{\mathbb{F}}_2}(E) = \left\{ \Phi_{u,r,t} | u \in \mathbb{F}_4, r \in \mathbb{F}_4^* \text{ and } t^2 + t + r^3 = 0 \right\}.$$

By [17, Prop. 9] we see that there is a bijection between the set

$$H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)\right)$$

and the set of Frobenius conjugacy classes of $\mathrm{Aut}_{\overline{\mathbb{F}}_2}$, i.e.,

$$H^1\left(\mathrm{G}_{\bar{K}/K}, \mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)\right) \cong \{C_{u,r,t}\},$$

where $C_{u,r,t}$ runs over the Frobenius conjugacy classes of $\mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)$, i.e.,

$$C_{u,r,t} = \left\{\Phi^{-1}_{\tilde{u},\tilde{r},\tilde{t}}\Phi_{u,r,t}\Phi_{\tilde{u}^2,\tilde{r}^2,\tilde{t}^2} | \tilde{u} \in \mathbb{F}_4, \tilde{r} \in \mathbb{F}_4^* \text{ and } \tilde{t} \in \mathbb{F}_{16} \text{ satisfies } \tilde{t}^2 + \tilde{t} + \tilde{r}^3 = 0\right\}.$$

The identity in $\mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)$ is $\Phi_{1,0,0}$, and the inverse of an element $\Phi_{u,r,t} \in \mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)$ is $\Phi_{u^2,ur,t+r^3}$. We compute the class $C_{1,0,0}$, the conjugacy class of identity.

$$\begin{aligned} C_{1,0,0} &= \left\{\Phi_{u,r,t}\Phi_{1,0,0}\Phi_{u^2,r^2,t^2} | u, r \text{ and } t \text{ are as above}\right\} \\ &= \left\{\Phi_{u^2,ur^2+r,ur}\right\}. \end{aligned}$$

So the identity class $C_{1,0,0}$ consists of the following automorphisms.

$u\backslash r$	0	1	ω	ω^2
1	$\Phi_{1,0,0}$	$\Phi_{1,0,1}$	$\Phi_{1,1,\omega}$	$\Phi_{1,1,\omega^2}$
ω	$\Phi_{\omega^2,0,0}$	$\Phi_{\omega^2,\omega^2,\omega}$	$\Phi_{\omega^2,\omega^2,\omega^2}$	$\Phi_{\omega^2,0,1}$
ω^2	$\Phi_{\omega,0,0}$	$\Phi_{\omega,\omega,\omega^2}$	$\Phi_{\omega,0,1}$	$\Phi_{\omega,\omega,\omega}$

Here, ω is the primitive cube root of unity in $\mathbb{F}_4$. Since $-1 = \Phi_{1,0,1}$ is in this class, the elliptic curve $E/\mathbb{F}_2$ has no quadratic twist.

Now, if we consider E over $\mathbb{F}_4$, then the action of $\mathrm{G}_{\overline{\mathbb{F}}_4/\mathbb{F}_4}$ on $\mathrm{Aut}_{\overline{\mathbb{F}}_4}(E)$ is trivial. Here $C_{1,0,0} = \{\Phi_{1,0,0}\}$, so $\mathrm{Fr} \mapsto -1 = \Phi_{1,0,1}$ defines a nontrivial cocycle class. The corresponding twist is given by

$$E^{\mathrm{tw}} : y^2 + y = x^3 + \omega,$$

since

$$\psi : (x, y) \mapsto (x, y + \tau),$$

with $\tau \in \mathbb{F}_4$ satisfying $\tau^2 + \tau + \omega = 0$, defines an isomorphism $\psi : E \to E^{\mathrm{tw}}$, and

$$({}^{\mathrm{Fr}}\psi)^{-1} \circ \psi = -1.$$

2.7 The polynomial $X^3 - 3nX - \lfloor n\sqrt{4n} \rfloor$

In Section 2.3, one method for finding a maximal elliptic curve over $\mathbb{F}_{p^3}$ was to find an elliptic curve over $\mathbb{F}_p$ having $p + 1 + a$ rational points, with a satisfying $a^3 - 3pa = \lfloor p\sqrt{4p} \rfloor$. In this section we consider the polynomial

$$f(X) = X^3 - 3nX - \lfloor n\sqrt{4n} \rfloor \in \mathbb{Z}[X]$$

and study its zeros in $\mathbb{Z}$.

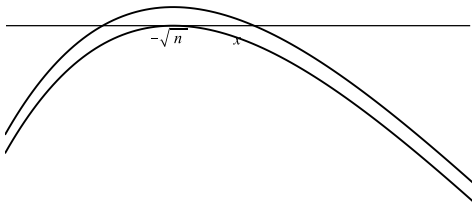
Proposition 2.7.1. For infinitely many $n \in \mathbb{Z}_{>0}$ the above polynomial $f(X)$ has a zero $b \in \mathbb{Z}$ with $|b| \leq 2\sqrt{n}$.

Proof. First note that

$$f(0) = 0 \Leftrightarrow \lfloor n\sqrt{4n} \rfloor = 0 \Leftrightarrow 4n^3 < 1.$$

Since $n > 0$, this is impossible. Hence 0 cannot be zero of the polynomial f, for all $n \in \mathbb{Z}_{>0}$.

Note that $X^3 - 3nX - n\sqrt{4n} = (X + \sqrt{n})^2(X - 2\sqrt{n})$. We will look for an integer zero of $f(X)$ close to $-\sqrt{n}$. Suppose $a \in \mathbb{Z}_{<0}$ and write $a^2 - n = t$. Note that by choosing $a \in \mathbb{Z}$ within distance 1 from $-\sqrt{n}$, it is guaranteed that $1 - 2\sqrt{n} < t < 1 + 2\sqrt{n}$. We assume a is chosen in this way. We will show that if t satisfies the stronger inequalities $t^4 \leq t + n = a^2$, then indeed $f(a) = 0$.



Observe that

$$\begin{aligned} f(a) &= a^3 - 3a(a^2 - t) - \lfloor 2(a^2 - t)\sqrt{a^2 - t} \rfloor \\ &= -2a^3 + 3at - \lfloor \sqrt{(2a^3 - 3at)^2 + 3a^2t^2 - 4t^3} \rfloor. \end{aligned}$$

This implies that $f(a) = 0 \Leftrightarrow$

$$\lfloor \sqrt{(2a^3 - 3at)^2 + 3a^2t^2 - 4t^3} \rfloor = -2a^3 + 3at.$$

The above equation is equivalent to the following system of inequalities.

1. $3a^2t^2 - 4t^3 \geq 0$;
2. $2a^3 - 3at \leq 0$;
3. $(2a^3 - 3at)^2 + 3a^2t^2 - 4t^3 < (-2a^3 - 3at + 1)^2$.

Using $a^2 - n = t$, we see that the first inequality is equivalent to $t = 0$ or $t \leq 3n$. Since we assume $t < 1 + 2\sqrt{n}$ and since $1 + 2\sqrt{n} \leq 3n$ holds for all $n \geq 1$, this condition is fulfilled. The second inequality is equivalent to $t \leq 2n$. For $n \geq 2$ we have $1+2\sqrt{n} \leq 2n$, so for such n, the condition $t \leq 2n$ holds. Moreover, $n = 1$ is a square so then we have $t = 0$. Hence condition 2 holds for all n. The third inequality can be written as

$$4a^3 - 4t^3 + 3a^2t^2 - 6at - 1 < 0. \tag{2.10}$$

Rewriting the inequality (2.10) as

$$4a^3 \left(1 - \frac{t^3}{a^3} + \frac{3t^2}{4a} - \frac{3t}{2a^2} - \frac{1}{4a^3}\right) < 0, \tag{2.11}$$

this means (since a is negative)

$$1 - \frac{t^3}{a^3} + \frac{3t^2}{4a} - \frac{3t}{2a^2} - \frac{1}{4a^3} > 0. \tag{2.12}$$

By taking $a = -\lceil \sqrt{n} \rceil$ we have $-a - 1 < \sqrt{n} \leq -a$, hence $0 \leq t < 2\sqrt{n} + 1$. Moreover we assume $t > 0$ since the case $t = 0$ is already dealt with. Since the two terms $-t^3/a^3$ and $-1/4a^3$ are positive in the left-hand-side of the inequality (2.12), this means that the inequality (2.11) is certainly true if

$$1 + \frac{3t^2}{4a} - \frac{3t}{2a^2} \geq 0.$$

Assume $n \leq 10$ so that $a \leq -4$. This implies that the function

$$x \mapsto \frac{3x^2}{4a} - \frac{3x}{2a^2} + 1$$

attains positive values at $x = 0$ and $x = \sqrt{-a}$. Hence this quadratic function is positive for all t such that $0 \leq t \leq \sqrt{-a}$, implies (2.12) for such t. This proves that $f(a) = 0$. The zero given here satisfies

$$|a| = \lceil \sqrt{n} \rceil \leq 2\sqrt{n},$$

which proves the proposition. In fact similar reasoning applies for $t < 0$, provided $t > -\sqrt{-a}$.

□

Remark 2.7.2. Although Proposition 2.7.1 shows the existence of a zero of $f(X)$ in $[-2\sqrt{n}, 0] \cap \mathbb{Z}$ for infinitely many n, our application asks a zero for n a prime number. We do not know whether a similar result holds in that case. In fact, the Proposition 2.7.1 shows that $-b \in \mathbb{Z}_{<0}$ is a zero of $X^3 - 3nX - \lfloor n\sqrt{4n} \rfloor$, for every $n \in \mathbb{Z}$ in the interval $[b^2 - \sqrt{b}, b^2 + \sqrt{b}]$. Denoting the set of integers in this interval by S_b and $\mathbb{S} = \bigcup_{b \geq 1} S_b$, one has that $\sum_{s \in \mathbb{S}} \frac{1}{s}$ converges whereas $\sum_{p \text{ prime}} \frac{1}{p}$ diverges. So in this sense the set $\mathbb{S}$ is much smaller then the set of prime numbers.

Remark 2.7.3. At the 1912 International Congress of Mathematicians (ICM), Edmund Landau listed four basic problems about prime numbers. One of the problem was as follows.

Are there infinitely many primes of the form $m^2 + 1$?

This is still unsolved problem. If this were true, then we would have a zero of $f(X)$ for infinitely many primes n. For primes of the form $m^2 + 1$, the method in Proposition 2.7.1 always gives a zero of the polynomial $f(X)$, namely, $-|m|$.

2.8 The polynomial $X^5 - 5nX^3 + 5n^2X - \lfloor n^2\sqrt{4n} \rfloor$

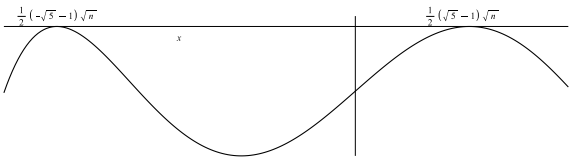
In our attempt to find elliptic curves $E/\mathbb{F}_p$ which are maximal over $\mathbb{F}_{p^5}$, we needed that (cf. Section 2.5) $a := p + 1 - \#E(\mathbb{F}_p)$ was a zero of

$$f(X) = X^5 - 5nX^3 + 5n^2X - \lfloor n^2\sqrt{4n} \rfloor$$

for $n = p$ a prime number. Similar to the situation in Section 2.7, this leads to the question whether $f(X)$ has a zero $a \in \mathbb{Z}$ satisfying $|a| \leq 2\sqrt{n}$.

Observe that

$$X^5 - 5nX^3 + 5n^2X - n^2\sqrt{4n} = (X - a\sqrt{n})(X^2 + \sqrt{n}X - n)^2.$$



The zeros of the latter polynomial are $2\sqrt{n}$ (a simple zero) and $\frac{\pm\sqrt{5}-1}{2} \cdot \sqrt{n}$ (two double zeros). If n is a square, then $2\sqrt{n}$ is a zero as

required. Reasoning as in the previous section we see that if $a \in \mathbb{Z}$ is a "very good" approximation to one of $\frac{\sqrt{5}-1}{2}\sqrt{n}$ or $\frac{-\sqrt{5}-1}{2}\sqrt{n}$, then $f(a) = 0$ and $|a| \leq 2\sqrt{n}$.

Examples: For $n := 3$, we get $\frac{\sqrt{5}-1}{2}\sqrt{3} \approx 1.070466$, and indeed $a = 1$ is a zero of $f(X)$.

For $n := 6$, we get $\frac{-\sqrt{5}-1}{2}\sqrt{6} \approx -3.963357$, and indeed $a = -4$ is a zero of $f(X)$.

For $n := 10$, we get $\frac{\sqrt{5}-1}{2}\sqrt{10} \approx 1.954395$, and indeed $a = 2$ is a zero of $f(X)$.

For $n := 1241$, we get $\frac{-\sqrt{5}-1}{2}\sqrt{1241} \approx -56.999826$, and indeed $a = -57$ is a zero of $f(X)$.

For $n := 1042399$, we get $\frac{-\sqrt{5}-1}{2}\sqrt{1042399} \approx 630.999990$, and indeed $a = 631$ is a zero of $f(X)$.

Chapter 3

Genus Two

3.1 Introduction

A formula for the maximal number of points $N_q(2)$ that a genus 2 curve $C/\mathbb{F}_q$ can have was found by Serre [22, 23]; see also [24].

In this short chapter we recall a method described in a paper by Howe, Leprévost, and Poonen [9] to find an explicit equation of a genus two curve with many points from an equation of an elliptic curve with many points. We illustrate this by giving an example. We also provide Magma code for the calculations.

An immediate consequence of [9, Corollary 6] is the following.

Proposition 3.1.1. Suppose q is a power of an odd prime p, and $E/\mathbb{F}_q$ is an elliptic curve with $\#E(\mathbb{F}_q) = q + 1 + t$ and $j(E) \neq 0, 1728$. Then there exists an explicit $C/\mathbb{F}_q$ of genus 2, such that

$$\#C(\mathbb{F}_q) = q + 1 + 2t.$$

Propositions 3 and 4 in the same paper [9] explain how to find an equation for C in terms of a Weierstrass equation for E. For convenience of the reader we also present this here.

We consider two cases, as in the proof presented in [9, Corollary 6].

Case 1. Suppose $j(E) \notin \mathbb{F}_p$. Then in this case the curve F in Proposition 3 is $E^{(p)}$, obtained by raising the coefficients of the equation of E to the power p. The curves E and $E^{(p)}$ are isogenous. Suppose $E/\mathbb{F}_q : y^2 = f(x)$ and α_i are zeros of $f(x)$ in its splitting field. Then the isomorphism $\psi : E[2] \to F[2]$ is just p-th power Frobenius, i.e.,

$$\psi : (\alpha_i, 0) \mapsto (\alpha_i^p, 0).$$

Now Proposition 4 gives us an explicit equation of C.

Case 2. Suppose $j(E) \in \mathbb{F}_p$. Then there exists $E_0/\mathbb{F}_p$ with $j(E) = j(E_0)$. Then the curve E is a twist of E_0. Since $\mathrm{Aut}(E_0) = \{\pm 1\}$ this means that E is a quadratic twist of E_0. We discussed this in Section 2.6. If $E_0 : y^2 = f(x)$, with $f \in \mathbb{F}_p[X]$ monic, then E can be given as

$$E : dy^2 = f(x),$$

for some $d \in \mathbb{F}_q$.

In this case the curve F in Proposition 3 is again E. Since the $\mathrm{Aut}(E) = \{\pm 1\}$, this implies that any non-trivial automorphism $\psi : E[2] \to E[2]$ cannot be the restriction of an automorphism of E. Now if we find this automorphism ψ then by using Proposition 4 we can find the curve C.

If f has three zeros in $\mathbb{F}_q$, then

$$E[2] = \{O, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}.$$

Therefore, ψ is just any non-trivial permutation of the points.

If f has exactly one zero say α_1 in $\mathbb{F}_q$, then

$$E[2] = \{O, (\alpha_1, 0), (\alpha_2, 0), (\alpha_2^p, 0)\}.$$

Therefore,

$$\psi : (\alpha_i, 0) \mapsto (\alpha_i^p, 0).$$

If f has no zero in $\mathbb{F}_q$, equivalently, no zero in $\mathbb{F}_p$, then

$$E[2] = \{O, (\alpha, 0), (\alpha^p, 0), (\alpha^{p^2}, 0)\}.$$

Therefore, ψ just raises the power of coordinates of points to the power p.

Remark 3.1.2. If $f \in \mathbb{F}_p[x]$ a cubic polynomial, then

- f has no zero in $\mathbb{F}_p \Rightarrow$ if f has one zero in $\mathbb{F}_q$, then it has 3 zeroes in $\mathbb{F}_q$;
- f has one zero in $\mathbb{F}_p \Rightarrow$ if $2 \nmid [\mathbb{F}_q : \mathbb{F}_p]$ then f has one zero in $\mathbb{F}_q$, or if $2 \mid [\mathbb{F}_q : \mathbb{F}_p]$, then f has 3 zeroes in $\mathbb{F}_q$;
- f has 3 zeroes in $\mathbb{F}_p \Rightarrow f$ has 3 zeroes in $\mathbb{F}_q$.

3.2 Example

In the table in Section 2.5 we have

$$E/\mathbb{F}_{5^5}: \quad y^2 = x^3 + \alpha^{97}x + 1,$$

where α satisfies an irreducible polynomial $X^5 + 4X + 3$ in $\mathbb{F}_5[X]$. The number of points on this curve is 3237, so in this case $t = 111$; therefore, we require a curve of genus two with 3348 points. Note that the $j(E) = \alpha^{1324} \notin \mathbb{F}_5$. So this is Case 1 in the above discussion.

In the following Magma code we first find the splitting field of $f = x^3 + a^{97}x + 1$; note that in the code we have $a = \alpha$. Then we find roots of f in the splitting field. The roots of f^p are just the p-th power of the roots of f. By using these roots we define a_1, b_1, a_2, b_2, A and B, as they are defined in Proposition 4 in the paper [9]. Then we find the polynomial h, and we define the hyperellitic curve C by this polynomial, which is the required curve of genus two, with the required number of points.

```
p:=5;
Fp:=GF(p);
P<X>:=PolynomialRing(Fp);
k<a>:=ext<Fp|X^5+4*X+3>;
P1<x>:=PolynomialRing(k);
f:=x^3+a^97*x+1;
K<b>:=ext<k|f>;
P2<Y>:=PolynomialRing(K);
alpha:=[Roots(f, K)[1][1],Roots(f, K)[2][1],Roots(f, K)[3][1]];
beta:=[alpha[1]^p,alpha[2]^p,alpha[3]^p];
a1:=(alpha[3]-alpha[2])^2/(beta[3]-beta[2])+(alpha[2]-alpha[1])\
^2/(beta[2]-beta[1])+(alpha[1]-alpha[3])^2/(beta[1]-beta[3]);
b1:=(beta[3]-beta[2])^2/(alpha[3]-alpha[2])+(beta[2]-beta[1])\
^2/(alpha[2]-alpha[1])+(beta[1]-beta[3])^2/(alpha[1]-alpha[3]);
a2:=alpha[1]*(beta[3]-beta[2])+alpha[2]*(beta[1]-beta[3])+alpha[3]*\
(beta[2]-beta[1]);
b2:=beta[1]*(alpha[3]-alpha[2])+beta[2]*(alpha[1]-alpha[3])+beta[3]*\
(alpha[2]-alpha[1]);
D:=Discriminant(f); A:=D^p*a1/a2; B:=D*b1/b2;
h0:=-(A*(alpha[2]-alpha[1])*(alpha[1]-alpha[3])*Y^2+B*(beta[2]-\
beta[1])*(beta[1]-beta[3]))*(A*(alpha[3]-alpha[2])*(alpha[2]-alpha[1]\
)*Y^2+B*(beta[3]-beta[2])*(beta[2]-beta[1]))*(A*(alpha[1]-alpha[3])*\
(alpha[3]-alpha[2])*Y^2+B*(beta[1]-beta[3])*(beta[3]-beta[2]));
h1:=Polynomial(k,h0);
Poly<x1>:=PolynomialRing(k);
h:=0;
```

```
for i in [0..6] do
    h:=h+Coefficient(h1,i)*x1^i;
end for;
C:=HyperellipticCurve(h);
n:=#C;
print "The curve is y1^2=",h1,"\n and the number of points on this\
curve is",n,"\n The genus of this curve is",Genus(C);
```

Chapter 4

Curves of higher genus with many points

In this chapter we consider some special curves of genus ≥ 4 over $\mathbb{F}_q$, with q odd. All curves considered have a large automorphism group.

4.1 Some curves admitting a platonic map

Let X be a curve defined over $\mathbb{C}$ and $\phi : X \to \mathbb{P}^1$ be a rational function. A point $z \in X$ is called a critical point if $\phi'(z) = 0$, and $w \in \mathbb{P}^1(\mathbb{C})$ is called a critical value if $w = \phi(z)$ for some critical point $z \in X$. We call ϕ a Belyĭ map if its set of critical values is contained in $\{0, 1, \infty\}$. In his thesis [8] Maxim Hendriks has listed all pairs (X, G) where $X/\mathbb{C}$ is curve of genus ≤ 15 and G is a subgroup of $\mathrm{Aut}(X)$, such that the quotient map $X \to X/G$ is actually a Belyĭ map. This condition implies that $X/G \cong \mathbb{P}^1$; the resulting morphism $X \to \mathbb{P}^1$ is called a platonic map. Any such curve can be defined over some number field. In this section we decompose the Jacobians of some curves admitting such a platonic maps, as given in his thesis [8]. We consider reduction modulo primes to obtain curves over finite fields.

4.1.1 Curves of genus 4

We first study the curve C in $\mathbb{P}^3$ given by the equations

$$XY + ZW = 0,$$
$$X^3 + Z^3 = Y^3 + W^3.$$

This corresponds to the curve denoted by $R_{4,3}$ in [8], on page $172 - 173$.

Remark 4.1.1. Up to a linear isomorphism, this example is the same as the one denoted by $(A-1)(2)$ in the paper [14].

Proposition 4.1.2. The curve C, in every characteristic $\neq 2, 3$, is a smooth curve of genus 4. Its automorphism group contains the elements

$$\phi_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega^2 \end{pmatrix}, \phi_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \phi_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

in PGL(4). Here ω is a root of unity of order 3. The subgroup generated by ϕ_1, ϕ_2 and ϕ_3 has order 72.

Proof. We check the smoothness of the curve C at all points with $W = 0$. The points are $(1, 0, -\xi, 0)$ and $(0, 1, \xi, 0)$, where $\xi^3 = 1$. These points are smooth if the characteristic is not 3. The affine equations of C corresponding to $W = 1$ are

$$xy + z = 0,$$

$$x^3 - z^3 = y^3 + 1,$$

that can be written as $x^3(1 - y^3) = y^3 + 1$. The derivatives of this equation with respect to x is

$$3x^2 - 3x^2y^3 = 0$$

and with respect to y is

$$-3x^3y^2 = 3y^2.$$

These equations will have a simultaneous solution only if the characteristic is 2 or 3. Hence, the curve is smooth except when the characteristic is 2 or 3. To verify that C has genus 4, observe that C is a complete intersection of a quadratic and a cubic surface in $\mathbb{P}^3$, so [7, Chapter 2, Exercise 8.4(g)] implies that the genes equals 4.

Now we prove that the order of the group generated by ϕ_1, ϕ_2 and ϕ_3 is 72. Let G be the subgroup of PGL(4) generated by ϕ_1, ϕ_2 and ϕ_2. The action of G on the 4 points $e_1 = (1, 0, 0, 0), e_2 = (0, 1, 0, 0), e_3 = (0, 0, 1, 0), e_4 = (0, 0, 0, 1) \in \mathbb{P}^3$ yields

$$\psi : G \twoheadrightarrow H \subset S_4$$

where H is generated by the permutations $(1, 2)$ and $(1, 4)(2, 3)$. The subgroup

$$V_4 = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

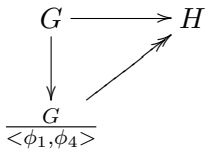
is normal in S_4. We see that $V_4 \subset H$ since conjugating $(1,4)(2,3)$ by $(1,2)$ we get $(1,3)(2,4)$. Therefore V_4 is normal in H, and the image of

$$H \to H/V_4$$

has order 2, so $\#H = 2 \times 4 = 8$. Note that ϕ_1 and

$$\phi_4 := \phi_3\phi_1\phi_3 = \begin{pmatrix} \omega^2 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

are in $\ker(\psi)$. The subgroup $< \phi_1, \phi_4 >= \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is normal in G. The quotient group $G/ < \phi_1, \phi_4 >$ is generated by the images of ϕ_2 and ϕ_3. We have the following diagram.



It is easy to verify that $G/ < \phi_1, \phi_4 > \longrightarrow H$ is an isomorphism. Therefore, $\#G = 9 \times 8 = 72$. This completes the proposition.

□

Theorem 4.1.3. Let k be a field of characteristic $\neq 2, 3$. Over k, the Jacobian of C is isogenous to $E_1^2 \times E_2^2$, where E_1 is the elliptic curve corresponding to

$$E_1 : y_1^2 = x_1^3 - 51x_1 + 142;$$

$$E_2 : y_2^2 = x_2^3 + 21x_2 - 26.$$

Moreover, E_1 is isogenous to the quadratic twist by -3 of E_2.

Proof. The affine equation of C corresponding to $X = 1$ (i.e, in terms of the affine coordinated $z = Z/X$ and $w = W/X$)

$$1 + z^3 = -(zw)^3 + w^3,$$

which may also be written as

$$w^3 = \frac{1 + z^3}{1 - z^3}.$$

Note that $y = -zw$. On this model the automorphism ϕ_1 is given by $\phi_1(z, w) = (\omega z, \omega^2 w)$. We find the quotient curve D of C by ϕ_1. The invariant functions under the action of ϕ_1 are generated by $\eta := z^3$ and $\xi := wz$, which satisfy

$$\xi^3 = w^3 z^3 = \frac{1+z^3}{1-z^3} z^3 = \frac{1+\eta}{1-\eta}\eta.$$

This is rewritten as

$$\eta^2 + \eta = \xi^3 - \eta\xi^3,$$

or

$$4\eta^2 + 4(1+\xi^3)\eta = 4\xi^3,$$

i.e.,

$$(2\eta + 1 + \xi^3)^2 = \xi^6 + 6\xi^3 + 1.$$

So using $\eta_1 := 2\eta + \xi^3 + 1$, the quotient curve D is given by the equation

$$\eta_1^2 = \xi^6 + 6\xi^3 + 1,$$

which is clearly a hyperelliptic curve of genus 2. And the quotient map $\phi : C \to D$ is given by $\phi(z, w) = (\xi = zw, \eta_1 = 2z^3 + z^3w^3 + 1)$. The pull-backs of the regular 1-forms $d\xi/\eta_1$ and $\xi d\xi/\eta_1$ on D under ϕ are $(1 - z^3)dw/2z^2$ and $w(1 - z^3)dw/2z^2$, respectively.

Furthermore, to get other regular 1-forms on C, we use the composition of the automorphism ϕ_3 and the map ϕ

$$C \xrightarrow{\phi_3} C \xrightarrow{\phi} D.$$

On our affine model of C the automorphism ϕ_3 is given by $\phi_3(z, w) = (-z, 1/w)$. Therefore,

$$(\phi \circ \phi_3)^*(d\xi_1/\eta_1) = \phi_3^*((1 - z^3)dw/2z^2) = -w^2(1 + z^3)dw/2z$$

and

$$(\phi \circ \phi_3)^*(\xi_1 d\xi_1/\eta_1) = \phi_3^*(w(1 - z^3)dw/2z^2) = -w(1 + z^3)dw/2z.$$

Here ϕ^* represent the map induced by ϕ on 1-forms. These 1-forms

$$\frac{(1-z^3)dw}{2z^2}, \quad \frac{w(1-z^3)dw}{2z^2},$$
$$\frac{-w^2(1+z^3)dw}{2z}, \quad \frac{-w(1+z^3)dw}{2z}$$

are linearly independent on C; therefore

$$\mathrm{Jac}(C) \sim \mathrm{Jac}(D) \times \mathrm{Jac}(D),$$

with the isogeny defined over k (see 1.2).

We now consider the curves D. We have two involution on D, namely,

$$\rho_1 : (\xi, \eta_1) \mapsto (1/\xi, \eta_1/\xi^3), \qquad \rho_2 : (\xi, \eta_1) \mapsto (1/\xi, -\eta_1/\xi^3).$$

Now we find the quotient curve of D by ρ_1 and ρ_2. Firstly, the functions on D which are invariant under ρ_1 are generated by $\xi_2 := \xi + 1/\xi$ and $\eta_2 := \eta_1(1 + 1/\xi^3)$, which satisfy

$$\begin{aligned}
\eta_2^2 &= \eta^2(1 + 1/\xi^3)^2 = (\xi^3 + 6 + 1/\xi^3)(\xi^3 + 2 + 1/\xi^3) \\
&= \big((\xi + 1/\xi)^3 - 3(\xi + 1/\xi) + 6\big)\big((\xi + 1/\xi)^3 - 3(\xi + 1/\xi) + 2\big) \\
&= (\xi_2^3 - 3\xi_2 + 6)(\xi_2^3 - 3\xi_2 + 2) \\
&= (\xi_2^3 - 3\xi_2 + 6)(\xi_2 - 1)^2(\xi_2 + 2).
\end{aligned}$$

Replacing η_2 by $\tilde{\eta}_2 = \eta_2/(\xi_2 - 1)$ yields the equation

$$\tilde{\eta}_2 = (\xi_2^3 - 3\xi_2 + 6)(\xi_2 + 2).$$

This clearly defines an elliptic curve over k, which by using the coordinates $x_1 := (3\xi_2 + 10)/(\xi_2 + 2)$ and $y_1 := 4\tilde{\eta}_2/(\xi_2 + 2)^2$ is put in Weierstrass form

$$E_1 : y_1^2 = x_1^3 - 51x_1 + 142.$$

Secondly, to find the quotient curve of D by ρ_2, we see the functions on D which are invariant under ρ_2 are generated by $\xi_3 := \xi + 1/\xi$ and $\eta_3 := \eta_1(1 - 1/\xi^3)$, which satisfy

$$\eta_3^2 = (\xi_3^3 - 3\xi_3 + 6)(\xi_3^3 - 3\xi_3 - 2) = (\xi_3^3 - 3\xi_3 + 6)(\xi_3 + 1)^2(\xi_3 - 2).$$

Replacing η_3 by $\tilde{\eta}_3 = \eta_3/(\xi_3 + 1)$ yields

$$\tilde{\eta}_3 = (\xi_3^3 - 3\xi_3 + 6)(\xi_3 - 2).$$

This is clearly an elliptic curve, which by using the coordinates $x_2 := (3\xi_3 + 2)/(\xi_3 - 2)$ and $y_2 := 8\tilde{\eta}_3/(\xi_3 - 2)^2$ is put in Weierstrass form

$$E_2 : y_2^2 = x_2^3 + 21x_2 - 26.$$

To prove that $D \sim E_1 \times E_2$, we use the following theorem given in [12].

Theorem 4.1.4 (Theorem B, [12])**.** Given a curve X, let $G \leq \mathrm{Aut}(X)$ be a finite group such that $G = H_1 \cup H_2 \cup \cdots \cup H_m$ where the subgroups H_i satisfy $H_i \cap H_j = \{1_G\}$ if $i \neq j$. Then we have the following isogeny relation

$$J_X^{m-1} \times J_{X/G}^{g} \sim J_{X/H_1}^{h_1} \times \cdots \times J_{X/H_m}^{h_m}$$

where $g = |G|$ and $h_i = |H_i|$ and $J^n = J \times \cdots \times J$ (n times).

Since the composition of ρ_1 and ρ_2 is the hyperelliptic involution, we have $< \rho_1, \rho_2 > \cong (\mathbb{Z}/2\mathbb{Z})^2$. The quotient of D by $< \rho_1\rho_2 >$ is $\mathbb{P}^1$, and its Jacobian variety is zero dimensional. Therefore

$$\mathrm{Jac}(D) \sim E_1 \times E_2.$$

Hence

$$\mathrm{Jac}(C) \sim E_1^2 \times E_2^2,$$

with the isogeny defined over k.

Now we show that the curve E_1 is isogenous to the quadratic twist by -3 of E_2. Note that $(3, 4)$ is a point of order three on E_1. Let T be the subgroup of E_1 generated by this point. We use the method given in [29] to find the quotient curve E_1/T. Using the substitution

$$x_1 \mapsto x_1 + 3,$$

we get the equation of E_1 in the form

$$y_1^2 = x_1^3 + 9(x_1 - 4/3)^2.$$

Therefore the quotient curve E_1/T is given by the equation

$$s^2 = t^3 - 243(t - 72)^2,$$

where $t := (18y_1^2 - 9x_1^3 - 54x_1^2 + 288)/x_1$ and $s := -27y_1(x_1^3 + 48x_1 - 128)/x_1^3$. Again by using $t_1 := (t - 81)/9$ and $s_1 := s/27$, we can write

$$s_1^2 = t_1^3 + 189t_1 + 702.$$

The quadratic twist by -3 of this curve is E_2. This completes the proof of the theorem. □

Corollary 4.1.5. Let E_1 is defined over a field $\mathbb{F}_q$ of characteristic not equal to 2,3. If a_q is the trace of elliptic curve E_1, then

(1) $\#C(\mathbb{F}_q) = q + 1 - 2a_q - 2\left(\frac{-3}{q}\right)a_q$.

(2) The C reaches Hasse-Weil-Serre bound iff E_1 does and $q \equiv 1 \pmod 6$.

The j-invariant of E_1 is

$$\frac{3^3 \cdot 17^3}{2}.$$

So in particular, in characteristic 0 the curve E_1 has no complex multiplication (CM curves have algebraic integral j-invariant). By result of Elkies [4], there are infinitely many primes, such that $E_1 \pmod p$ is supersingular. For each of them, the curve C is maximal over $\mathbb{F}_{p^n}$ whenever $n \equiv 2 \pmod 4$. Indeed, given such a prime p, we have $p > 3$ and hence $\#E_1(\mathbb{F}_p) = p + 1$. This implies (see 2.2) that $E_1/\mathbb{F}_{p^n}$ is maximal whenever $n \equiv 2 \pmod 4$. Moreover, in this case $p^n \equiv 1 \pmod 6$, so part (2) of the Corollary 4.1.5 implies that $C/\mathbb{F}_{p^n}$ is maximal. The smallest such primes are

$$\{17, 71, 251, 647, 847, 827, 1889, 3527, 3617, 4409\}.$$

A search among prime numbers $p < 4 \cdot 10^6$ did not result in any example for which $p \equiv 1 \pmod 6$ and $\#E_1(\mathbb{F}_p) = p + 1 + \lfloor\sqrt{4p}\rfloor$.

The prime number $p = 1069$ is $\equiv 1 \pmod 6$, and

$$\#E_1(\mathbb{F}_{1069}) = 1069 + \lfloor 2\sqrt{1069}\rfloor,$$

only one below the Hasse bound. Hence

$$\#C(\mathbb{F}_{1069}) = 1069 + 4\lfloor 2\sqrt{1069}\rfloor - 3,$$

just 4 below the Hasse-Weil-Serre bound.

Now we study the curve C_1 in $\mathbb{P}^3$ given by the equations

$$X_1^2 + X_2^2 + X_3^2 = 0$$
$$X_1X_2X_3 + X_4^3 = 0.$$

This corresponds to the curve denoted by $R_{4,1}$ in [8], on page 170.

Theorem 4.1.6. Let k be the field of characteristic $\neq 2, 3$. Over k the curve C_1 is smooth. Its genus is 4, and the Jacobian of C_1 splits into four elliptic curves of j-invariant 0.

Proof. First we check the smoothness of the curve at all points with $X_4 = 0$. The points are $(0, 1, \pm\sqrt{-1}, 0), (1, 0, \pm\sqrt{-1}, 0)$ and $(1, \pm\sqrt{-1}, 0, 0)$. These points are smooth if the characteristic $\neq 2$. Now we need to consider points with $X_4 \neq 0$. Because of the second equation of curve, for each such point we have $X_1 \neq 0$. So we need only consider the affine equations of C_1 corresponding to $X_1 = 1$. Therefore in affine coordinates (i.e., in terms of the affine coordinates $x_2 = X_2/X_1, x_3 = X_3/X_1$ and $x_4 = X_4/X_1$) we have the equations

$$1 + x_2^2 + x_3^2 = 0$$
$$x_2 x_3 + x_4^3 = 0.$$

This curve is singular if the characteristic is 3 (for example, the point $(x_2, x_3, x_4) = (1, 2, 1)$ is a singular point). The rank of the matrix

$$\left(\frac{\partial F_i}{\partial x_j}\right) = \begin{pmatrix} x_2 & x_3 & 0 \\ x_3 & x_2 & 3x_4^2 \end{pmatrix}$$

is 2 for all points on the curve in all characteristics$\neq 2, 3$. Hence the curve is smooth in all characteristics except 2 and 3.

Using $x_2 = -x_4^3/x_3$, the remaining equation of the curve is $1 + x_4^6/x_3^2 + x_3^2 = 0$, which yields

$$x_4^6 + x_3^4 + x_3^2 = 0. \tag{4.1}$$

Note that we we have an automorphism $\phi(x_3, x_4) = (x_3, \omega x_4)$. The invariant functions under the action of ϕ are generated by x_3 and $s := x_4^3$. Therefore the quotient curve of C_1 by ϕ is

$$s^2 + x_3^4 + x_3^2 = 0.$$

The function field of the quotient curve is also generated by $x = 1/x_3$ and $y = s/x_3^2$ satisfying

$$x^2 + y^2 + 1 = 0.$$

Hence this is a rational curve. So the curve C_1 is a cyclic, degree 3 cover of a rational curve. Since only 6 points with $X_4 = 0$, given above, are fixed points of ϕ, the Hurwitz formula shows that the genus of C_1 is 4.

Now we prove that the Jacobian of C_1 splits, upto isogeny over k, in 4 elliptic curves of j-invariant 0. On the affine model of C_1 we have an automorphism $\phi_1(x_3, x_4) = (x_3, -x_4)$, and the invariant functions on C_1 under the action of ϕ_1 are generated by x_3 and $s_1 := x_4^2$. Therefore the quotient curve D_1 of C_1 by ϕ_1 is given by the equation

$$s_1^3 + x_3^4 + x_3^2 = 0.$$

By the substitution $s_1 = t_2x_3$, we get the above equation in the form $t_2^3x_3 + x_3^2 + 1 = 0$, which can be written as

$$(2x_3 + t_2^3)^2 = t_2^6 - 4.$$

So using $s_2 := 2x_3 + t_2^3$, we obtain

$$s_2^2 = t_2^6 - 4.$$

Hence D_1 is a hyperelliptic curve of genus 2. The pull-backs of the regular 1-forms dt_2/s_2 and t_2dt_2/s_2 on D_1 are $x_4^2dx_3/3x_3$ and $x_4^4dx_3/3x_3^2$ on C_1, respectively.

Now we consider the curve D_1. It has an automorphism ψ_1 given by $\psi_1(t_2, s_2) = (-t_2, s_2)$. The invariant functions D_1 under the action of ψ_1 are generated by s_2 and $\tau_1 := t_2^2$. The quotient curve E_1 of D_1 by ψ_1 given by equation

$$s_2^2 = \tau_1^3 - 4,$$

which is indeed an elliptic curve of j-invariant 0. The pull-back of the regular 1-form $d\tau_1/s_2$ on E_1 is $2t_2dt_2/s_2$ on D_1. Now we find the other quotient curve E_2 of D_1 by an automorphism $\psi_2(t_2, s_2) = (-t_2, -s_2)$. The invariant functions on D_1 under the action of ψ_2 are generated by $\tilde{t}_2 := t_2^2$ and $\tilde{s}_2 := s_2t_2$, which satisfy

$$\tilde{s}_2^2 = s_2^2t_2^2 = t_2^8 - 4t_2^2 = \tilde{t}_2^4 - 4\tilde{t}_2$$

Using new coordinates $s_3 := \tilde{s}_2/2\tilde{t}_2^2$ and $\tau_2 := -1/\tilde{t}_2$, we get the equation of E_2 in the form

$$s_3^2 = \tau_2^3 + 1/4,$$

which is also an elliptic curve of j-invariant 0. The pull-back of the regular 1-form $d\tau_2/s_3$ on E_2 is $4dt_2/s_2$ on D_1. Since the pullbacks of regular 1-forms from E_1 and E_2 are independent over D_1, this implies, over k,

$$\mathrm{Jac}(D_1) \sim E_1 \times E_2.$$

Furthermore, on the affine model (4.1) we have another automorphism $\phi_2(x_3, x_4) = (-x_3, x_4)$. We find the quotient curve D_2 of C_1 by ϕ_2. The invariant functions under the action of ϕ_2 are generated by x_4 and $t_3 := x_3^2$. Hence the quotient curve D_2 is given by the equation

$$x_4^6 + t_3^2 + t_3 = 0.$$

This can be written as

$$((2t_3+1)/x_4^3)^2 = 1/x_4^6 - 4.$$

So, using the new coordinates $s_4 := (2t_3+1)/x_4^3$ and $\tau_3 := 1/x_4$, the above can be written as

$$s_4^2 = \tau_3^6 - 4,$$

which shows $D_1 = D_2$. Using

$$C_1 \to D_2 = D_1 \to E_1$$

one obtains the differential $-x_4 dx_3/3(x_3^3 + x_3)$ on C_1, which is independent from the two differentials on C_1 already obtained. This means that, upto isogeny over k, $\mathrm{Jac}(C_1)$ contains a subvariety $E_1^2 \times E_2$.

Next, we see that we have an automorphism ϕ_3 on C_1 which interchanges X_1 and X_3. On the affine model (4.1) the automorphism ϕ_3 is given by $\phi_3(x_3, x_4) = (1/x_3, x_4/x_3)$. We find the quotient curve of C_1 by ϕ_3. The invariant functions under the action of ϕ_3 are generated by $t_5 := x_3 + 1/x_3$ and $s_5 := x_4(1 + 1/x_3)$, which satisfy

$$\begin{aligned} x_4^6(1+1/x_3)^6 &= (-x_3^4 - x_3^2)(1+1/x_3)^6 \\ &= -(x_4^4 + 1/x_4^4) - 6(x_4^3 + 1/x_4^3) - 16(x_4^2 + 1/x_4^2) \\ &\quad - 26(x_4 + 1/x_4) - 30. \end{aligned}$$

In the new coordinate s_5 and t_5, this is written as

$$\begin{aligned} s_5^6 &= -t_5(t_5^3 + 6t_5^2 + 12t_5 + 8) \\ &= -t_5(t_5+2)^3. \end{aligned}$$

Let $\xi = t_5 + 2$, then

$$s_5^6 = \xi^3(2 - \xi).$$

By dividing through by ξ^6, we get

$$\frac{s_5^6}{\xi^6} = \frac{2}{\xi^3} - \frac{1}{\xi^2}$$

Let $s_5/\xi = \eta_1$ and $1/\xi = \xi_1$. Therefore,

$$\eta_1^6 = 2\xi_1^3 - \xi_1^2.$$

Let $\xi_1 = \xi_2\eta_1^3$. Then the above equation yields

$$\frac{1}{\xi_2^3} = 2\eta_1^3 - \frac{1}{\xi_2}.$$

Again let $\xi_3 = 1/\xi_2$. Then by dividing ξ_3^3 the above equation can be written as

$$1 = 2\frac{\eta_1^3}{\xi_3^3} - \frac{1}{\xi_3^2}.$$

Again by using $X = 2\eta_1/\xi_3$ and $Y = 2/\xi_3$ we get

$$Y^2 = X^3 - 4.$$

This defined the elliptic curve E_1. The pull-back of the 1-form dX/Y on E_1 is $(x_3+1)(1-x_3)x_3dx_3/3(x_3^4+x_3^2)$. Since the 4 pull-backs to C_1 are linearly independent over k, this shows that

$$\mathrm{Jac}(C_1) \sim E_1^3 \times E_2.$$

□

Corollary 4.1.7. Over $\mathbb{F}_q$, $\gcd(6,q) = 1$, write $\#E_1(\mathbb{F}_q) = q + 1 - a_1$ and $\#E_2(\mathbb{F}_q) = q + 1 - a_2$. Then

$$\#C_1(\mathbb{F}_q) = q + 1 - 3a_1 - a_2.$$

Recall that we call a curve over a finite field good if the number of rational points on the curve is within 10 percent of the Hasse-Weil-Serre bound. This curve C_1 provides an example of a good curve over some finite fields; for example,

$$\begin{aligned}
\#C_1(\mathbb{F}_{11^5}) &= 161052\\
\#C_1(\mathbb{F}_{13^5}) &= 373350\\
\#C_1(\mathbb{F}_{17^5}) &= 1419858\\
\#C_1(\mathbb{F}_{19^5}) &= 2467824.
\end{aligned}$$

Corollary 4.1.8. Let $\mathbb{F}_q$ be the finite field with characteristics $\neq 2, 3$. If $q \equiv 5 \pmod 6$, then the curve $C_1/\mathbb{F}_{q^n}$ is maximal whenever $n \equiv 2 \pmod 4$.

Proof. Let $\mathbb{F}_p$ be the prime field of characteristic relatively prime to 6. The elliptic curves E of j-invariant 0 over $\mathbb{F}_p$ can be given by an equation of the form

$$y^2 = x^3 + c,$$

where $c \in \mathbb{F}_p^*$. This curve has $p+1$ rational points whenever $p \equiv 5 \pmod 6$ (cf. [23, Exercise 4.10]). This implies (see 2.2) that $E/\mathbb{F}_{p^m}$ is maximal whenever $m \equiv 2 \pmod 4$. Hence, using Corollary 4.1.7, the curve $C_1/\mathbb{F}_{p^m}$ will also be maximal.

Write $q = p^f$. The assumption $q \equiv 5 \pmod 6$ implies that $p \equiv 5 \pmod 6$ and f is odd integer. Since $q^n = p^{nf}$ and $n \pmod 4 = nf \pmod 4$, this proves the corollary. □

4.1.2 Curves of genus 5

In this section we study two examples of genus 5 curves. Our first example is the curve C_2 in $\mathbb{P}^4$ given by

$$\begin{gathered} X_1^2 + X_3^2 + X_4^2 = 0 \\ X_1X_2 + X_5^2 = 0, \\ X_2^2 - X_3^2 + X_4^2 = 0. \end{gathered}$$

If one replaces X_4 by $\sqrt[4]{-1}X_4$, this corresponds to the curve denoted by $R_{5,1}$ in [8], on page 175.

Theorem 4.1.9. Let k be the field of characteristic $\neq 2$. Over k the curve C_2 is smooth. Its genus is 5, and the Jacobian of C_2 splits (upto isogeny, over some extension of k) into 5 elliptic curves. From these elliptic curves, three have j-invariant 1728 and two have complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ (hence with j-invariant 8000).

Proof. First we check the smoothness of the curve C_2 at all points with $X_5 = 0$. The points are $(0, \pm\sqrt{-2}, \pm\sqrt{-1}, 1, 0), (\pm\sqrt{-2}, 0, \pm 1, 1, 0)$. These points are smooth if the characteristic $\neq 2$. So we need to consider points with $X_5 \neq 0$. Because of the second equation of the curve, for each such point we have $X_1 \neq 0$. So we need only consider the affine equations of C_2 corresponding to $X_1 = 1$. Therefore in affine coordinates (i.e., in terms of the affine coordinates $x_2 = X_2/X_1, x_3 = X_3/X_1$, $x_4 = X_4/X_1$ and $x_5 = X_5/X_1$), using $x_2 = -x_5^2$, we have the equations

$$\begin{gathered} 1 + x_3^2 + x_4^2 = 0 \\ x_5^4 - x_3^2 + x_4^2 = 0. \end{gathered}$$

The rank of the matrix

$$\left(\frac{\partial F_i}{\partial x_j}\right) = \begin{pmatrix} 2x_3 & 2x_4 & 0 \\ -4x_3 & 0 & 4x_5^3 \end{pmatrix}$$

is 2 for all points on the curve in all the characteristics except 2. Hence the curve is smooth in all characteristic except 2.

Now, by subtracting and adding the equations, we write these affine equations of C_2 in the form

$$2x_4^2 = x_5^4 + 1$$
$$2x_3^2 = x_5^4 - 1.$$

Hence the curve C_2 is a fibre product of two curves of genus one. We treat fibre products in the next section. For the proof of remaining parts of this theorem see Proposition 4.2.1 and Example 4.2.4. □

Corollary 4.1.10. Let $\mathbb{F}_q$ be finite field with odd characteristic. If $q \equiv 7 \pmod 8$, then $C_2/\mathbb{F}_{q^n}$ is maximal whenever $n \equiv 2 \pmod 4$.

Proof. The condition $q \equiv 7 \pmod 8$ implies that the elliptic curves with j-invariant 1728 and with j-invariant 8000 are both supersingular. Hence so is $\mathrm{Jac}(C_2)$ over $\mathbb{F}_q$. From Example 4.2.4 we see that over the prime field $\mathbb{F}_p \subset \mathbb{F}_q$ we have

$$\mathrm{Jac}(C_2) \sim E_1^2 \times E_2 \times \mathrm{Jac}(D_2),$$

where $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 + x$ and D_2 is the genus 2 curve with equation $y^2 = x^5 - x$. Note that since $q \equiv 7 \pmod 8$, also $p \equiv 7 \pmod 8$. Using [5, Theorem 9] one obtains that the eigenvalues of Frob_p on the Tate module of $\mathrm{Jac}(D_2)$ are $\pm\sqrt{-p}$, each with multiplication 2. Since $\pm\sqrt{-p}$ are also the eigenvalues of Frob_p on $\mathrm{T}_l E_j$ $(j = 1, 2)$, one finds

$$\#C_2(\mathbb{F}_{p^n}) = p^n + 1 - 5(\sqrt{-p})^n - 5(-\sqrt{-p})^n$$

for $p \equiv 7 \pmod 8$. This implies the corollary. □

This curve also gives some examples of good curves. For example,

$$\#C_2(\mathbb{F}_{11^2}) = 216$$
$$\#C_2(\mathbb{F}_{17^2}) = 376$$
$$\#C_2(\mathbb{F}_{11^5}) = 161052$$
$$\#C_2(\mathbb{F}_{17^5}) = 1409304$$
$$\#C_2(\mathbb{F}_{19^5}) = 2476100.$$

Now we study the curve C_3 in $\mathbb{P}^4$ given by the equations

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0$$
$$X_1^2 + \lambda X_3^2 - X_4^2 - \lambda X_5^2 = 0$$
$$X_2^2 - X_3^2 + \lambda X_4^2 - \lambda X_5^2 = 0,$$

where λ satisfies $\lambda^2 + \lambda - 1$. This corresponds to the curve denoted by $R_{5,3}$ in [8], on page $176 - 177$.

Theorem 4.1.11. Let k be a field of characteristic $\neq 2, 5$ containing λ. Then the curve C_3 over k is smooth, and $\mathrm{Jac}(C_3) \sim E^5$, with

$$E : (2 - \lambda)y^2 = x^3 + 5x^2 + 5x.$$

Proof. First we check the smoothness of the curve C_3 at all points with $X_5 = 0$. The points are $(\pm\sqrt{1-\lambda} : \pm\sqrt{-\lambda - 1} : \pm\sqrt{-1} : 1, 0)$. These points are smooth if the characteristic $\neq 2$. So we need to consider points with $X_5 \neq 0$. Therefore in affine coordinates (i.e., in terms of the affine coordinates $x_1 := X1/X_5, x_2 = X_2/X_5, x_3 = X_3/X_5$ and $x_4 = X_4/X_5$) the equations are

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1 = 0$$
$$x_1^2 + \lambda x_3^2 - x_4^2 - \lambda = 0$$
$$x_2^2 - x_3^2 + \lambda x_4^2 - \lambda = 0.$$

Now the rank of the matrix

$$\left(\frac{\partial F_i}{\partial x_j}\right) = \begin{pmatrix} 2x_1 & 2x_2 & 2x_3 & 2x_4 \\ 2x_1 & 0 & 2\lambda x_3 & -2x_4 \\ 0 & 2x_2 & -2x_3 & 2\lambda x_4 \end{pmatrix}$$

is 3 for all points on C_3 unless either $2 = 0$ or $\lambda = 2$, and the latter only happens when the characteristic is 5. Therefore the curve C_3 is smooth in characteristics $\neq 2, 5$.

Now we prove that $\mathrm{Jac}(C_3)$ splits into the products of 5 copies of E. Let $(x_1, x_2, x_3, x_4, x_5)$ be a point on C_3. The curve C_3 has five automorphisms ψ_i which send x_i to $-x_i$. The quotient curve of C_3 by ψ_i is just projection to $\mathbb{P}^3$ given by deleting the variable X_i. We can find the equations of the quotient curves of C_3 by ψ_i by eliminating X_i from the equations of C_3. Therefore it is easy to check that the quotients of C_3 by ψ_i are the Y_i's. Following are the defining polynomials of the Y_i's.

$Y_1 : (X_2^2 - X_3^2 + \lambda X_4^2 - \lambda X_5^2, X_2^2 - (\lambda - 1)X_3^2 + 2X_4^2 + (\lambda + 1)X_5^2)$

$Y_2 : (X_1^2 - \lambda X_3^2 - X_4^2 - \lambda X_5^2, X_1^2 + 2X_3^2 - (\lambda - 1)X_4^2 + (\lambda + 1)X_5^2)$

$Y_3 : ((\lambda - 1)X_1^2 + \lambda X_2^2 + (\lambda + 1)X_4^2 + 2\lambda X_5^2, X_1^2 + 2X_2^2 + (\lambda + 1)X_4^2 - (\lambda - 1)X_5^2)$

$Y_4 : (2X_1^2 - X_2^2 + (\lambda + 1)X_3^2 - (\lambda - 1)X_5^2, \lambda X_1^2 + (\lambda - 1)X_2^2 + (\lambda + 1)X_3^2 + 2\lambda X_5^2)$

$Y_5 : ((\lambda + 1)X_1^2 - \lambda X_2^2 + 2\lambda X_3^2 + (\lambda - 1)X_4^2, \lambda X_1^2 + (\lambda - 1)X_2^2 + (\lambda - 1)X_3^2 + 2\lambda X_4^2)$

Now we check the independence of the pull-backs of regular 1-form of Y_i on C_3. With the help of Magma [1] we find the basis of regular 1-forms $\{\omega_i\}$ of C_3.

$$\begin{aligned}
\omega_1 &:= \frac{x_2x_3dx_4}{x_4^4+(2\lambda+1)x_4^2+1},\\
\omega_2 &:= \frac{x_1x_3dx_4}{x_4^4+(\lambda+2)x_4^2+\lambda+1},\\
\omega_3 &:= \frac{x_1x_2dx_4}{x_4^4+(\lambda+1)x_4^2+\lambda},\\
\omega_4 &:= \frac{x_1x_2x_3dx_4}{x_4^6+2(\lambda+1)x_4^4+2(\lambda+1)x_4^2+1},\\
\omega_5 &:= \frac{x_1x_2x_3x_4dx_4}{x_4^6+2(\lambda+1)x_4^4+2(\lambda+1)x_4^2+1}.
\end{aligned}$$

The pull-backs of regular 1-form on Y_i are, for $i = 1, 2, 3, 4, 5$, respectively, $\lambda\omega_1/4$, $-\lambda\omega_2/4, (\lambda-1)\omega_3/4, (\lambda-1)\omega_4/4$ and $(\lambda-1)\omega_5/4$. The pull-backs are constant multiples of the linearly independent 1-forms on C_3. Hence, if $E_i = \mathrm{Jac}(Y_i)$, then

$$\mathrm{Jac}(C_3) \sim E_1 \times \cdots \times E_5.$$

Now we prove that the E_i's are isogenous to E. Magma, using a point on Y_j over $\mathbb{Q}(\sqrt{-1}, \sqrt{\lambda+1})$ over which the map ramifies, finds an equation for E_i over $\mathbb{Q}(\lambda) = \mathbb{Q}(\sqrt{5})$. Denote these curves by $\tilde{E}_i$,

$$\begin{aligned}
\tilde{E}_1 :&\quad y^2 = x^3+x^2+\lambda^3x = x(x+\lambda)(x+1-\lambda)\\
\tilde{E}_2 :&\quad y^2 = x(x+\lambda)(x+1+\lambda)\\
\tilde{E}_3 :&\quad y^2 = x^3+\lambda^2x^2-\lambda x = x(x-\lambda)(x+1)\\
\tilde{E}_4 :&\quad y^2 = x(x+\lambda)(x-\lambda^3)\\
\tilde{E}_5 :&\quad y^2 = x^3-2\lambda^2x^2-2\lambda^3x+\lambda^3 = x(x+\lambda)(x+1+\lambda)
\end{aligned}$$

Note that $\tilde{E}_2 = \tilde{E}_5$. Both E_i and $\tilde{E}_i$ are isomorphic over an extension field of $\mathbb{Q}(\lambda)$. Moreover the j-invariant of these curves is $2^{11} \notin \{0, 1728\}$. This implies E_i and $\tilde{E}_i$ are quadratic twists. By construction, E_i has good reduction except possibly at the primes $(\sqrt{5})$ and (2). This is also true for $\tilde{E}_i$; in fact, these curves have good reduction at $(\sqrt{5})$ as well. Over $\mathbb{Q}$ a model of the elliptic curve with j-invariant 2^{11} is $\tilde{E} : y^2 = x^3+5x^2+5x$. This curve has bad reduction only at 2 and 5. So $E_i/\mathbb{Q}(\sqrt{5})$ has an equation

$$dy^2 = x^3+5x^2+5x,$$

and since the reduction of E_i is good away from $(2), (\sqrt{5}) = (2\lambda + 1)$, this implies

$$d \in \{1, -1, \lambda, -\lambda, 2, -2, 2\lambda, -2\lambda, 2\lambda + 1, \lambda(2\lambda + 1), -(2\lambda + 1), -\lambda(2\lambda + 1), 2(2\lambda + 1), 2\lambda(2\lambda + 1), -2(2\lambda + 1), -2\lambda(2\lambda + 1)\}.$$

We count the number of rational points on $E^{(d)} : dy^2 = x^3 + 5x^2 + 5x$ and Y_i over finite fields. This yields that for all d except $d = \lambda(2\lambda + 1) = 2 - \lambda$ we find prime p such that

$$\#Y_i(\mathbb{F}_p) \neq \#E^{(d)}(\mathbb{F}_p).$$

The following table gives some values of (q, λ) for which $\#Y_i(\mathbb{F}_q) \neq \#E^{(d)}(\mathbb{F}_q)$.

q	d
9	$1, -1, 2, -2, 2\lambda + 1, -2(2\lambda + 1)$
289	λ
29	$-2\lambda(2\lambda + 1)$

Hence, $E_i \sim E^{(2-\lambda)}$. This completes the theorem. □

Corollary 4.1.12. With q such that $\gcd(10, q) = 1$ and $\lambda \in \mathbb{F}_q$ satisfying $\lambda^2 + \lambda = 1$, write $E : (2-\lambda)y^2 = x^3 + 5x^2 + 5x$ over $\mathbb{F}_q$ and $\#E(\mathbb{F}_q) = q + 1 - t$. Then

$$\#C_3(\mathbb{F}_q) = q + 1 - 5t.$$

Remark 4.1.13. Over $\mathbb{F}_q$, because of the bound $\#C(\mathbb{F}_q) \geq q + 1 - \lfloor 2\sqrt{q} \rfloor > 0$ for genus one curve C, the Y_j have a rational point and hence $\mathrm{Jac}(Y_i) \sim E_i \sim E$ over $\mathbb{F}_q$.

Remark 4.1.14. Over $\mathbb{Q}(\sqrt{5})$, the equation of E can be written as

$$(2 - \lambda)y^2 = x(x + \lambda + 2)(x - \lambda - 3).$$

So all points of order 2 on E are rational. In particular, over $\mathbb{F}_q$ it follows that

$$\#C_3(\mathbb{F}_q) = 5 \cdot \#E(\mathbb{F}_q) - 4q - 4 \equiv 0 \pmod 4.$$

And the maximal number of rational points on a curve of genus 5 over $\mathbb{F}_{q^2}$ is $q^2 + 1 + 5q \equiv 2 + q \pmod 4$ since q is odd. Hence C_3 will never be maximal over $\mathbb{F}_{q^2}$.

This curve C_3 also gives some examples of good curves. For example,

$$\begin{aligned}\#C_3(\mathbb{F}_{79}) &= 160\\ \#C_3(\mathbb{F}_{11^4}) &= 15672\\ \#C_3(\mathbb{F}_{11^5}) &= 160672.\end{aligned}$$

Also $\#C_3(\mathbb{F}_q) = 0$ for $q \in \{9, 19, 49, 59\}$.

4.2 Fibre products of curves of genus one

Let $\mathbb{F}_q$ be a finite field of odd characteristic. Suppose we have two genus one curves having equations of the form

$$\begin{aligned}E_1 &: y^2 = f(x),\\ E_2 &: y^2 = g(x).\end{aligned}$$

over $\mathbb{F}_q$. Here we assume that $f(x)$ and $g(x)$ are polynomials of degree 3 or 4, and f is not a constant multiple of g. The curve E_1 and E_2 are considered as degree 2 covers of $\mathbb{P}^1$ via $(x, y) \mapsto x$. Then the fibre product $C = E_1 \times_{\mathbb{P}^1} E_2$ is defined by the affine equations

$$\begin{cases} y^2 &= f(x)\\ z^2 &= g(x)\end{cases}$$

Proposition 4.2.1.

$$\mathrm{Jac}(C) \sim \mathrm{Jac}(E_1) \times \mathrm{Jac}(E_2) \times \mathrm{Jac}(D),$$

where D is the curve given by the equation $y^2 = f(x)g(x)$.

This can be proven in several ways; for example, it follows from Theorem 4.1.4 with the group $G \subset \mathrm{Aut}(C)$ generated by $\sigma_1 : (x, y, z) \mapsto (x, -y, z)$ and $\sigma_2 : (x, y, z) \mapsto (x, y, -z)$. We can also prove it by calculating the pull-backs of regular 1-forms to C.

Note that genus of D is given by (using $h(x) := \gcd(f(x), g(x)) \in \mathbb{F}_q[x]$)

$$\mathrm{Genus}(D) = \left\lfloor \frac{\deg(f) + \deg(g) - 2\deg(h) - 1}{2} \right\rfloor :$$

If the $\deg(h) = 3$ the $\mathrm{Genus}(D) = 0$. Since $\dim(\mathrm{Jac}(X)) = \mathrm{Genus}(X)$ for any curve X, it follows that

Corollary 4.2.2. $\text{Genus}(C) = \left\lfloor \frac{\deg(f)+\deg(g)-2\deg(h)+3}{2} \right\rfloor$.

Using the maps of degree 2 from C to each of the genus one curves, i.e.,

$$\begin{array}{ccc} C & \xrightarrow{2:1} & E_1 \\ {\scriptstyle 2:1}\downarrow & & \\ E_2 & & \end{array}$$

it is clear that

$$\#C(\mathbb{F}_q) \leq \min\{2\#E_2(\mathbb{F}_q), 2\#E_2(\mathbb{F}_q)\}.$$

Here we present examples of such fibre products genus 4 and 5 with many points produced by fibre product of elliptic curves having many points. Our motivation to study such fibre products was the observation that several genus 4 examples on `manypoints.org` found by E. Howe are of this type.

Example 4.2.3. Take the following elliptic curves (in characteristic $\neq 2, 3$).

$$\begin{aligned} E_1 &: \ s^2 = t^3 + 1, \\ E_2 &: \ r^2 = t^3 - 1. \end{aligned}$$

The fibre product of these elliptic curves is a smooth curve C of genus 4 in $\mathbb{P}^3$, given by the equations of the elliptic curves E_1 and E_2. From the above discussion we see that

$$\text{Jac}(C) \sim E_1 \times E_2 \times \text{Jac}(D),$$

where the curve D is given by

$$u^2 = t^6 - 1.$$

Now we find the quotient curve of D by the automorphism ρ_1 on D which sends (t, u) to $(-t, -u)$. The functions on D which are invariant under ρ_1 are generated by $u_1 := tu, t_1 := t^2$ which satisfy

$$u_1^2 = t^2u^2 = t^8 - t^2 = t_1^4 - t_1.$$

Again by using $u_2 := u_1/t_1^2$ and $t_2 := -1/t_1$ we get the equation of the quotient in the form

$$u_2^2 = t_2^3 + 1.$$

Hence the quotient of D by ρ_1 is isomorphic to E_1.

We also have another automorphism ρ_2 on D which sends (t, u) to $(-t, u)$. The functions on D which are invariant under ρ_2 are generated by $t_2 := t^2$ and $u_2 := u$. Then we can see the quotient of D by ρ_2 is the curve isomorphic to E_2. Now the composition of ρ_1 and ρ_2 is hyperelliptic involution; hence, $< \rho_1, \rho_2 > \cong (\mathbb{Z}/2\mathbb{Z})^2$. Therefore by using Theorem 4.1.4, we have

$$\mathrm{Jac}(D) \sim E_1 \times E_2.$$

Consequently, $\mathrm{Jac}(C) \cong E_1^2 \times E_2^2$. These elliptic curves E_1 and E_2 are supersingular over $\mathbb{F}_q$ whenever $q \equiv 5 \pmod 6$. If $p \equiv 5 \pmod 6$ is prime number, then $\#E_j(\mathbb{F}_p) = p + 1$; hence the eigenvalues of Frob_p on $\mathrm{T}_l E_j$ are $\pm\sqrt{-p}$. As a consequence, $\#C(\mathbb{F}_{p^n}) = p^n + 1 - 4(\sqrt{-p})^n - 4(-\sqrt{-p})^n$. In particular, for $n \equiv 2 \pmod 4$ the curve $C/\mathbb{F}_{p^n}$ is maximal.

Consider the two curves of genus one

$$C_1 : s^2 = f(t),$$
$$C_2 : r^2 = g(t),$$

degree of f is 3 or 4, and degree of g is 4 with $\gcd(f, g) = 1$. Then C given by

$$\begin{cases} s^2 &= f(t) \\ r^2 &= g(t) \end{cases}$$

has genus 5 and

$$\mathrm{Jac}(C) \sim \mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2) \times \mathrm{Jac}(D),$$

where D is given by the equation $u^2 = f(t)g(t)$, as was shown in Proposition 4.2.1.

Example 4.2.4. Take the following two curves of genus one.

$$C_1 : \ 2s^2 = t^4 + 1,$$
$$C_2 : \ 2r^2 = t^4 - 1.$$

The fibre product of these curves is the curve C, given by the equations of curves C_1 and C_2. The degree two map $(t, s) \mapsto (2t^2, 4st)$ maps C_1 to the elliptic curve $E_1 : y^2 = x^3 + 4x$ and C_2 to the elliptic curve $E_2 : y^2 = x^3 - 4x$. Hence $\mathrm{Jac}(C_i) \sim E_i$. We have

$$\mathrm{Jac}(C) \sim \mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2) \times \mathrm{Jac}(D) \sim E_1 \times E_2 \times \mathrm{Jac}(D).$$

It remains to split the Jacobian of curve the D given by equation

$$u^2 = t^8 - 1.$$

In fact over some extension field, D can by given $\eta^2 = \xi^8 + 1$, and in this form it is studied in [13], proving ([13, Proposition 2]) that its Jacobian is isogenous to the product of one elliptic curve with j-invariant 1728 and two elliptic curves with j-invariant 8000.

It is easy to see that the quotient of D by the automorphism $\sigma : (t, u) \mapsto (-t, u)$ is the elliptic curve isogenous to the elliptic curve given by the equation $y^2 = x^3 - x$. This curve is isogenous to E_1. Now we find the quotient curve $\tilde{D}$ of D by $\tau(t, u) \mapsto (-t, -u)$. The invariant functions under the action of τ are generated by $t_1 := t^2$ and $u_1 := ut$ which satisfy

$$u^2t^2 = t^{10} - t^2.$$

In new coordinates it is written as

$$u_1^2 = t_1^5 - t_1.$$

Using [5, Theorem 9] one obtains that if $p \equiv 7 \pmod 8$ then the eigenvalues of Frob_p on the Tate module of $\mathrm{Jac}(\tilde{D})$ are $\pm\sqrt{-p}$, each with multiplicity 2. Since $q = p^n$ and the eigenvalue of Frob_p on $\mathrm{T}_l E_1$ and $\mathrm{T}_l E_2$ are $\pm\sqrt{-p}$ for $p \equiv 7 \pmod 8$, it implies that if $q \equiv 7 \pmod 8$, then $\mathrm{Jac}(C)$ is supersingular, and $C/\mathbb{F}_{q^2}$ is maximal.

Example 4.2.5. This is an example of maximal curves of genus 7. Take the following two curves of genus two.

$$D_1 : \ y^2 = x^5 + x,$$
$$D_2 : \ z^2 = x^5 - x.$$

The fibre product of these curves is denoted by $\tilde{D}$, and it is given by the equations of the curves D_1 and D_2. The Genus of the curve $\tilde{D}$ is 7 and

$$\mathrm{Jac}(\tilde{D}) \sim \mathrm{Jac}(D_1) \times \mathrm{Jac}(D_2) \times \mathrm{Jac}(D),$$

where the curve D is isomorphic to the curve given by the equation

$$s^2 = t^8 - 1.$$

Since $\mathrm{Jac}(D) \sim \mathrm{Jac}(D_2) \times E$, where E is the elliptic curve given by the equation $y^2 = x^3 - x$, we obtain

$$\mathrm{Jac}(\tilde{D}) \sim \mathrm{Jac}(D_1) \times \mathrm{Jac}(D_2)^2 \times E.$$

Now by using [5, Theorem 9] one obtains that if $p \equiv 7 \pmod 8$ then the eigenvalues of Frob_p on the Tate module of $\mathrm{Jac}(D_1)$ and $\mathrm{Jac}(D_2)$ are $\pm\sqrt{-p}$; each with multiplicity 2. Also the eigenvalue of Frob_p on $\mathrm{T}_l E_1$ are $\pm\sqrt{-p}$ for $p \equiv 7 \pmod 8$. Therefore one obtains

$$\#\tilde{D}(\mathbb{F}_{p^n}) = p^n + 1 - 7(\sqrt{-p})^n - 7(-\sqrt{-p})^n.$$

Consequently, the curve $\tilde{D}$ is maximal over $\mathbb{F}_{p^n}$ whenever $p \equiv 7 \pmod 8$ and $n \equiv 2 \pmod 4$.

4.3 Good curves of genus 4

In the following table we present some examples of good genus 4 curves over $\mathbb{F}_q$. In Chapter 2 we have obtained equations of maximal elliptic curves. By translating the x-coordinate and then taking a fibre product, we obtain genus 4 curves with 2 copies of the given elliptic curves in their Jacobian. we then adjust the translation in order to make the number of points on the genus 4 curves as high as possible. The discription of $a \in \mathbb{F}_q$ is the same as given in Chapter 2.

$\#\mathbb{F}_q$	Equations of curve C	$\#C(\mathbb{F}_q)$
5^3	$y^2 = x^3 + x + 2$, $z^2 = (x+2)^3 + (x+2) + 2 - z^2$	196
7^3	$y^2 = x^3 + a^2$, $z^2 = (x + a^1 1)^3 + a^2$	454
11^3	$y^2 = x^3 + x + 4$, $z^2 = (x + a^{49})^3 + (x + a^{49}) + 4$	1580
13^3	$y^2 = x^3 + a^2x + a^{75}$, $z^2 = (x + a^{323})^3 + a^2(x + a^{323}) + a^{75}$	2510
17^3	$y^2 = x^3 + x + 4$, $z^2 = (x + a^{657})^3 + (x + a^{657}) + 4$	5414
19^3	$y^2 = x^3 + a^2x + a^9 - y^2$, $z^2 = (x + a^{2830})^3 + a^2(x + a^{2830}) + a^9$	7470
3^5	$y^2 = x^3 + 2x^2 + x + 1$, $z^2 = (x + a^{11})^3 + 2(x + a^{11})^2 + x + a^{11} + 1$	338
19^3	$y^2 = x^3 + a^2x + a^9 - y^2$, $z^2 = (x + a^{2830})^3 + a^2(x + a^{2830}) + a^9$	7470
3^5	$y^2 = x^3 + 2x^2 + x + 1$, $z^2 = (x + a^{11})^3 + 2(x + a^{11})^2 + x + a^{11} + 1$	338
5^5	$y^2 = x^3 + a^{97}x + 1$, $z^2 = (x + a^{906})^3 + a^{97}(x + a^{906}) + 1$	3522
7^5	$y^2 = x^3 + x + a^{601}$, $z^2 = (x + a^{1698})^3 + (x + a^{1698}) + a^{601}$	17780
11^5	$y^2 = x^3 + x + 1$, $z^2 = (x + a^{27101})^3 + (x + a^{27101}) + 1$	164072
13^5	$y^2 = x^3 + ax + a^{333760}$, $z^2 = (x + a^{6410})^3 + a(x + a^{6410}) + a^{333760}$	375698
17^5	$y^2 = x^3 + 5x^2 + a^{1351944}x + a^{198311}$, $z^2 = (x + a^{1247700})^3 + 5(x + a^{1247700})^2 + a^{1351944}(x + a^{1247700}) + a^{198311}$	1422542
19^5	$y^2 = x^3 + 5x^2 + a^{508237}x + a^{1608725}$, $z^2 = (x + a^{2085476})^3 + 5(x + a^{2085476})^2 + a^{508237}(x + a^{2085476}) + a^{1608725}$	2481878

4.4 Good curves of genus 5

In the following table we present some good curves of genus 5. With the help of Magma, we counted points on curves of genus 5 given in the thesis of Maxim Hendriks [8] and on some of their twists. Note ζ_i is a primitive ith root of unity in $\mathbb{F}_q$, and the minimal polynomial of a is the Conway polynomial (used in Magma by default for the construction of $\mathbb{F}_{p^n}$ using FiniteField(p, n) or its synonyms). To obtain such a polynomial using Magma, simply use the following command.

```
F<a>:=GF(p,n);
MinimalPolynomial(a);
```

$\#\mathbb{F}_q$	$\#C(\mathbb{F}_q)$	Equations of curve C
5^2	64	$X_3^2 + X_4^2 + X_5^2 = 0$, 64
13^2	280	$X_1^2 + (\zeta_3 - 1)X_3^2 + (\zeta_3^2 - 1)X_5^2 = 0,$
17^2	448	$X_2^2 + (\zeta_3^2 - 1)X_3^2 + (\zeta_3 - 1)X_5^2 = 0.$
7^4	2696	$X_3^2 + X_4^2 + X_5^2 = 0,$
19^3	7352	$aX_1^2 + (\zeta_3 - 1)X_3^2 + (\zeta_3^2 - 1)X_5^2 = 0,$
		$X_2^2 + (\zeta_3^2 - 1)X_3^2 + (\zeta_3 - 1)X_5^2 = 0.$
5^4	712	$aX_3^2 + X_4^2 + X_5^2 = 0,$
7^5	17280	$X_1^2 + (\zeta_3 - 1)aX_3^2 + (\zeta_3^2 - 1)X_5^2 = 0,$
		$X_2^2 + (\zeta_3^2 - 1)aX_3^2 + (\zeta_3 - 1)X_5^2 = 0.$
5^5	3536	$X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0,$
13^5	377296	$X_1^2 + X_2^2 + X_3^2 - X_4^2 - X_5^2 = 0,$
17^5	1426584	$X_2^2 - X_3^2 - ix_4^2 + iX_5^2 = 0.$
5^3	192	$X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0,$
13^3	2496	$aX_1^2 + X_2^2 + X_3^2 - X_4^2 - X_5^2 = 0,$
17^3	5384	$X_2^2 - X_3^2 - ix_4^2 + iX_5^2 = 0.$
11^3	1536	$X_1^2 + X_2^2 + aX_3^2 + X_4^2 + X_5^2 = 0,$
11^5	161280	$X_1^2 - (\zeta_5^3 + \zeta_5^2 + 1)aX_3^2 - X_4^2 + (\zeta_5^3 + \zeta_5^2 + 1)X_5^2 = 0$
		$X_2^2 - aX_3^2 - (\zeta_5^3 + \zeta_5^2 + 1)X_4^2 + (\zeta_5^3 + \zeta_5^2 + 1)X_5^2 = 0.$
7^3	384	$aX_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0,$
		$aX_1^2 - (\zeta_5^3 + \zeta_5^2 + 1)X_3^2 - X_4^2 + (\zeta_5^3 + \zeta_5^2 + 1)X_5^2 = 0,$
		$X_2^2 - X_3^2 - (\zeta_5^3 + \zeta_5^2 + 1)X_4^2 + (\zeta_5^3 + \zeta_5^2 + 1)X_5^2 = 0.$
19^4	131912	$aX_2^2 + X_3^2 + X_4^2 + X_5^2 = 0,$
		$X_1^2 + aX_2^2 + X_3^2 - X_4^2 - X_5^2 = 0,$
		$aX_2^2 - X_3^2 - ix_4^2 + iX_5^2 = 0.$
11^4	15247	$X_1^2 + \zeta_3 X_4 X_5 = 0, X_1 X_2 + X_3 X_5 = 0, X_1 X_3 - \zeta_3 X_2 X_4 = 0,$
		$X_1 X_4^2 + X_2^2 X_3 + X_5^3 = 0, X_1 X_5^2 - X_2 X_3^2 - \zeta_3 X_4^3 = 0$
19^5	2485456	$X_1^2 + \zeta_3 X_4 X_5 = 0, X_1 X_2 + X_3 X_5 = 0, X_1 X_3 - \zeta_3 X_2 X_4 = 0,$
		$X_1 X_4^2 + X_2^2 X_3 + X_5^3 = 0, X_1 X_5^2 - X_2 X_3^2 - \zeta_3 X_4^3 = 0$

Chapter 5

An elementary proof of Hasse's theorem

5.1 Introduction

Let $q = p^e$, for a prime number p and an integer $e \geq 1$. Suppose $E/\mathbb{F}_q$ is an elliptic curve.

Theorem 5.1.1 (Hasse)**.** If N_q denotes the number of rational points of $E/\mathbb{F}_q$, then

$$|N_q - q - 1| \leq 2\sqrt{q}.$$

This is well-known; proofs are presented in e.g., [26, 33]. An elementary proof, for the case $p \neq 2, 3$, was provided by Manin in [16]; see also [2], [3] and [6] which in particular includes the easy observation that manin's argument also works in characteristic 3. The aim of this chapter is to compare this elementary proof to the other ones. As a result, we are able to show how Manin's elementary proof extends to the case of finite fields of characteristic 2. We describe this for ordinary elliptic curves in Section 5.4.1 and for supersingular elliptic curves in Section 5.4.2. For convenience we also recall Manin's proof in Section 5.3.

5.2 Interpreting Manin's proof

Suppose $q = p^e$ and $p \neq 2$. Let $E/\mathbb{F}_q$ be given by an equation

$$E: \ y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Consider

$$E^{\mathrm{tw}}: \ f(t)y^2 = x^3 + ax^2 + bx + c. \tag{5.1}$$

The curve E^{tw} is a quadratic twist of $E/\mathbb{F}_q(t)$ [26, Chapter X, § 2]; see also Section 2.6 of this thesis. The two curves E and E^{tw} are isomorphic over $K = \mathbb{F}_q(t, s)$, where $s^2 = f(t)$. The isomorphism is defined as follows:

$$E^{\mathrm{tw}} \longrightarrow E$$

$$(x, y) \mapsto (x, sy).$$

It is easy to see that the points $Q = (t, 1)$ and $P_0 = (x_0, y_0) = (t^q, f(t)^{(q-1)/2})$ are in $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. We define

$$P_n = P_0 + nQ, \quad \forall\ n \in \mathbb{Z}.$$

If P_n is not the point at infinity O, set $P_n = (x_n, y_n)$. We write $x_n = f_n/g_n$, where $f_n, g_n \in \mathbb{F}_q[t]$, with $\gcd(f_n, g_n) = 1$. We get a well-defined function

$$d : \mathbb{Z} \to \ \{0, 1, 2, 3, ...\}$$

given by

$$d(n) = d_n = \begin{cases} 0 & \text{if } P_n = O; \\ \deg(f_n) & \text{otherwise.} \end{cases}$$

We now explain how one may interpret P_n and Q. The group $E(K)$ consists, apart from the point at infinity O, of points $(x(t, s),\ y(t, s))$, such that $x(t, s)$ and $y(t, s)$ are in the function field K over $\mathbb{F}_q$ of the curve with equation

$$s^2 = f(t). \tag{5.2}$$

Moreover

$$y(t, s)^2 = f\left(x(t, s)\right).$$

Since (5.2) defines the curve $E/\mathbb{F}_q$, this means that such a point corresponds to a morphism defined over $\mathbb{F}_q : (t, s) \mapsto (x(t, s), y(t, s))$ from E to E. Hence $E(K) \cong \mathrm{Mor}_{\mathbb{F}_q}(E, E)$ (Note that the addition on E yields a group structure on $\mathrm{Mor}_{\mathbb{F}_q}(V, E)$, for any variety $V/\mathbb{F}_q$). By composing with the isomorphism $E^{\mathrm{tw}}(K) \cong E(K)$ one obtains

$$E^{\mathrm{tw}}(K) \cong \mathrm{Mor}_{\mathbb{F}_q}(E, E),$$

given explicitly by

$$(x(t,s), y(t,s)) \mapsto [(t,s) \mapsto (x(t,s), sy(t,s))]\,.$$

We consider the subfield $\mathbb{F}_q(t) \subset \mathbb{F}_q(t,s)$ and ask the question: which elements $\psi \in \mathrm{Mor}_{\mathbb{F}_q}(E,E)$ corresponds to the subgroup $E^{\mathrm{tw}}(\mathbb{F}_q(t)) \subseteq E^{\mathrm{tw}}(K)$?

Lemma 5.2.1.

$$E^{\mathrm{tw}}(\mathbb{F}_q(t)) \cong \Psi = \{\psi \in \mathrm{Mor}_{\mathbb{F}_q}(E,E) \mid [-1] \circ \psi = \psi \circ [-1]\}.$$

Proof. Suppose a point $(x(t), y(t)) \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$; the corresponding morphism $\psi \in \mathrm{Mor}_{\mathbb{F}_q}(E,E)$ sends (t,s) to $(x(t), sy(t))$. Since

$$([-1] \circ \psi)(t,s) = [-1](x(t), sy(t)) = (x(t), -sy(t))$$

and

$$(\psi \circ [-1])(t,s) = (\psi)(t,-s) = (x(t), -sy(t)),$$

it follows that $[-1] \circ \psi = \psi \circ [-1]$. This proves $\psi \in \Psi$.

Now suppose $\phi \in \mathrm{Mor}_{\mathbb{F}_q}(E,E)$, satisfying $[-1] \circ \phi = \phi \circ [-1]$, maps a point (t,s) on E to $(x(t,s), y(t,s))$. By the isomorphisms $\mathrm{Mor}_{\mathbb{F}_q}(E,E) \cong E(K)$ and $E(K) \cong E^{\mathrm{tw}}(K)$, we get the point $P = (x(t,s), \frac{y(t,s)}{s}) \in E^{\mathrm{tw}}(K)$ corresponding to ϕ.

The action of the Galois group $G_{K/\mathbb{F}_q(t)} = \{id, \rho\}$ on K is determined by $t^\rho = t,\ s^\rho = -s$, and the fixed field of Galois group is $\mathbb{F}_q(t)$.

The assumption $[-1] \circ \phi = \phi \circ [-1]$ means that $((x(t,s), -y(t,s)) = (x(t,-s), y(t,-s))$. This implies that the point P is fixed by the action of the Galois group, and $P \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$. This proves that elements of Ψ indeed correspond to points in the subgroup $E^{\mathrm{tw}}(\mathbb{F}_q(t))$ of $E^{\mathrm{tw}}(K)$.

□

It is easy to see that q^{th}-power Frobenius $\phi_q \in \mathrm{End}_{\mathbb{F}_q}(E)$ is in Ψ. So by Lemma 5.2.1, ϕ_q corresponds to a point in $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. Since $\phi_q : (t,s) \mapsto (t^q, s^q) = (t^q, sf(t)^{(q-1)/2})$, this yields the point P_0 introduced by Manin. In fact, not just ϕ_q but the whole group $\mathrm{End}_{\mathbb{F}_q}(E) \subseteq \Psi$. Since $\mathrm{End}_{\mathbb{F}_q}(E)$ is torsion free, in particular ϕ_q and hence P_0 is an element of infinite order. Similarly, the identity endomorphism, $\mathrm{id} \in \mathrm{End}_{\mathbb{F}_q}(E) \subseteq \Psi$, yields a point of infinite order of $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. Since $\mathrm{id} : (t,s) \mapsto (t,s)$, this is the point $Q = (t,1)$ which Manin uses.

Proposition 5.2.2. The group $E^{\mathrm{tw}}(\mathbb{F}_q(t))$ and $\mathrm{End}_{\mathbb{F}_q}(E)$ have the same rank.

In case the Frobenius endomorphism ϕ_q equals multiplication by an integer (which happens precisely when q is square and $\#(E(\mathbb{F}_q) = (\sqrt{q} \pm 1)^2)$ this rank is 4. In all other cases it equals 2.

Proof. Notice that we have a group homomorphism:

$$\Psi \longrightarrow E(\mathbb{F}_q)$$

$$\psi \mapsto \psi(O).$$

The kernel of this homomorphism is

$$\{\psi \in \Psi | \psi(O) = O\} = \mathrm{End}_{\mathbb{F}_q}(E).$$

Since the group $E(\mathbb{F}_q)$ is finite and $\Psi \cong E^{\mathrm{tw}}(\mathbb{F}_q(t))$, this implies that $\mathrm{rank}(E^{\mathrm{tw}}(\mathbb{F}_q(t)) = \mathrm{rank}(\mathrm{End}_{\mathbb{F}_q}(E))$. The remaining assertions of the proposition follows from [34, Theorem 4.1]. □

Except in the case of a supersingular elliptic curve E with $\#E(\mathbb{F}_q) = (\sqrt{q} \pm 1)^2$, the two endomorphisms id and ϕ_q are linearly independent which implies that Q and P_0 generate a rank 2 subgroup of $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. Indeed, id and ϕ_q generate the subring $\mathbb{Z}[\phi_q] \subseteq \mathrm{End}_{\mathbb{F}_q}(E)$ and ϕ_q satisfies $\phi_q^2 - a_q\phi_q + q = 0$, where $a_q = q + 1 - N_q$. The condition on $\#E(\mathbb{F}_q)$ implies $a_q^2 - 4q < 0$, hence $\mathbb{Z} + \mathbb{Z}\phi_q = \mathbb{Z}[\phi_q] \cong \mathbb{Z}[X]/(X^2 - a_qX + q)$, which has rank 2 over $\mathbb{Z}$.

Example 5.2.1. Consider $E : y^2 = x^3 - x$ over $\mathbb{F}_9$. In this case $\phi_q = [-3]$ and $\#E(\mathbb{F}_9) = 16 = (\sqrt{9} + 1)^2$. By Proposition 5.2.2 this implies that $E^{\mathrm{tw}}(\mathbb{F}_9(t))$ has rank 4. We present 4 independent points by first giving 4 independent elements in $\mathrm{End}_{\mathbb{F}_9}(E)$ in the following table.

Indep. elements of $\mathrm{End}_{\mathbb{F}_9}(E)$	Corresponding points on $E^{\mathrm{tw}}(\mathbb{F}_9(t))$
id	$(t, 1)$
ϕ_3	$(t^3, t^3 - t)$
$\rho : (x, y) \mapsto (-x, \sqrt{-1}y)$	$(-t, \sqrt{-1})$
$\rho\phi_3$	$(-t^3, \sqrt{-1}(t^3 - t))$

We set $\Theta_n = \phi_q + [n]$ and get a well-defined function

$$\tilde{d} : \mathbb{Z} \to \{0, 1, 2, 3, ...\}$$

given by

$$\tilde{d}(n) = \tilde{d}_n = \begin{cases} 0 & \text{if } \Theta_n = 0 \\ \deg(\Theta_n) & \text{otherwise.} \end{cases}$$

Lemma 5.2.3. With notation as above, for every integer n one has $d_n = \tilde{d}_n$.

To prove this lemma we use "dual isogenies". For more detail see [26, Section III.4].

Definition 5.2.4 (The Dual Isogeny)**.** Let $\phi : E_1 \to E_2$ be an isogeny of degree m. The dual isogeny to ϕ is the unique isogeny

$$\hat{\phi} : E_2 \to E_1 \quad \text{satisfying} \quad \hat{\phi} \circ \phi = [m].$$

Theorem 5.2.5. Let $\phi : E_1 \to E_2$ be an isogeny.
(a) Let $m = \deg(\phi)$. Then $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2.
(b) Let $\lambda : E_1 \to E_2$ be another isogeny. Then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.
(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.
(d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.
(e) $\deg \hat{\phi} = \deg \phi$.
(f) $\hat{\hat{\phi}} = \phi$.

Proof. See [26, Chapter 3, Theorem 6.2]. □

Proof of Lemma 5.2.3. In Section 5.3, we will see that d_n satisfies the following properties.

(1) $d_0 = q$,

(2) $d_{-1} = N_q$ (see Lemma (5.3.3)),

(3) $d_{n-1} + d_{n+1} = 2d_n + 2$. (see Lemma (5.3.4))

To prove the theorem it suffices that we prove that $\tilde{d}_n$ also satisfies the above properties. This is shown as follows.

(1) $\tilde{d}_0 = \deg(\phi_q) = q$.

(2) $\tilde{d}_{-1} = \deg(\phi_q - 1) = N_q$(see [26, Chapter 5]).

(3) Here we use the properties of dual isogeny;

$$\begin{aligned} d_{n-1} + d_{n+1} &= (\phi_q + n - 1)(\widehat{\phi_q + n} - 1) + (\phi_q + n + 1)(\widehat{\phi_q + n} + 1) \\ &= (\phi_q + n - 1)(\hat{\phi}_q + n - 1) + (\phi_q + n + 1)(\hat{\phi}_q + n + 1) \\ &= 2\phi_q\hat{\phi}_q + 2n(\phi_q + \hat{\phi}_q) + 2n^2 + 2 \\ &= 2(\hat{\phi}_q + n)(\phi_q + n) + 2 = 2\tilde{d}_n + 2. \end{aligned}$$

This proves the Lemma 5.2.3. □

5.3 Recapitulation of details of Manin's proof

In Manin's proof, E^{tw} is considered as an elliptic curve over $\mathbb{F}_q(t)$. Since E^{tw} is not in the standard Weierstrass form, there will be modifications in the usual addition and duplication formulae.

(*i*) If $O \neq P_j = (x_j, y_j) \in E^{\text{tw}}(\mathbb{F}_q(t))$ and $P_1 \neq \pm P_2$, then

$$x(P_1 + P_2) = f(t)\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - (x_1 + x_2) \tag{5.3}$$

(*ii*) If $P = (x, y) \in E^{\text{tw}}(\mathbb{F}_q(t))$ and $y \neq 0$, then

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \tag{5.4}$$

Now we present the properties of d_n.

Lemma 5.3.1. If $P_n = (x_n, y_n) \neq O$, write $x_n = f_n(t)/g_n(t)$ with $f_n(t), g_n(t) \in \mathbb{F}_q[t]$. Then $\deg(f_n) > \deg(g_n)$.

Proof. Suppose $\tau = 1/t$ and view E^{tw} over $\mathbb{F}_q((\tau))$. We change coordinates as follows:

$$\xi = \tau x \text{ and } \eta = y.$$

In these new coordinates the equation for E^{tw} is

$$(1 + a\tau + b\tau^2 + c\tau^3)\eta^2 = \xi^3 + a\tau\xi^2 + b\tau^2\xi + c\tau^3.$$

By reduction modulo τ, we obtain the curve

$$\bar{E}^{tw}/\mathbb{F}_q : \ \eta^2 = \xi^3.$$

We have an exact sequence of abelian groups (see [26, Chapter VII, Prop: 2.1])

$$0 \to E_1^{\text{tw}}\left(\mathbb{F}_q((\tau))\right) \to E_0^{\text{tw}}\left(\mathbb{F}_q((\tau))\right) \xrightarrow{mod\ \tau} \tilde{E}_{ns}^{tw}(\mathbb{F}_q) \to 0,$$

where $E_0^{tw}\left(\mathbb{F}_q((\tau))\right)$ is the group of points in $E^{\text{tw}}(\mathbb{F}_q((\tau)))$ whose reduction modulo τ is in $\bar{E}_{ns}^{tw}(\mathbb{F}_q)$, the group of non-singular points of $\bar{E}^{tw}$. Moreover, $E_1^{\text{tw}}(\mathbb{F}_q((\tau)))$ is the kernel of the reduction modulo τ.

Let $P = (f/g, y) \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$, where f and g are polynomials. We denote by $v(f/g)$ the valuation of f/g seen as an element of $\mathbb{F}_q((\tau))$. We know that $v(f/g) = v(f) - v(g)$ and if $f \in \mathbb{F}_q[t]$ then $v(f) = -\deg(f)$. Namely, if $f = a_d t^d + \cdots + a_0$ with $a_d \neq 0$, then

$$\begin{aligned} f &= a_d\tau^{-d} + \cdots + a_0 \\ &= \tau^{-d}(a_d + a_{d-1}\tau + \cdots + a_0\tau^d). \end{aligned}$$

Since $v(\tau^{-d}) = -d$ and $a_d + a_{d-1}\tau + \cdots + a_0\tau^d \in \mathbb{F}_q[[\tau]]^*$, we have $v(f) = -d = -\deg(f)$.

In new coordinates ξ, η, the point $P = (\tau f/g, y) \in E^{\mathrm{tw}}(\mathbb{F}_q(t)) \subset E^{\mathrm{tw}}(\mathbb{F}_q((\tau)))$. Note that

$$\begin{aligned} P \in E_0^{tw}(\mathbb{F}_q((\tau))) &\Leftrightarrow v\left(\frac{f}{tg}\right) \leq 0 \\ &\Leftrightarrow \deg(f) > \deg(g). \end{aligned}$$

Clearly the points $P = (t^q, f(t)^{(q-1)/2})$ and $Q = (t, 1)$ are in the group $E_0^{tw}(\mathbb{F}_q((\tau)))$ for all q. Therefore, $P_n = P_0 + nQ \in E_0^{tw}(\mathbb{F}_q((\tau)))$. This proves the lemma. □

Corollary 5.3.2. If $P_n \neq O$ then $d_n > 0$, $\forall\ n \in \mathbb{Z}$.

The following lemma gives the connection between N_q and d_n.

Lemma 5.3.3.

$$d_{-1} = N_q.$$

Proof. We compute d_{-1}. By the addition formula (5.3)

$$\begin{aligned} x(P_{-1}) &= x(P_0 - Q) \\ &= \frac{f(t)\left[f(t)^{(q-1)/2} + 1\right]^2}{(t^q - t)^2} - a - (t^q + t) \\ &= \frac{f(t)^q + 2f(t)^{(q+1)/2} + f(t) - a(t^q - t)^2 - (t^{3q} - t^{2q+1} - t^{q+2} + t^3)}{(t^q - t)^2} \\ &= \frac{t^{2q+1} + \text{ a polynomial of lower degree}}{(t^q - t)^2}. \end{aligned}$$

We can write

$$t^q - t = \prod_{\alpha \in \mathbb{F}_q} (t - \alpha).$$

Therefore,

$$d_{-1} = 2q + 1 - \#\{\text{Cancellations of degree one factors}\}.$$

Now we count $\#\{\text{Cancellations of degree one factors}\}$. Suppose

$$f(t)\left[f(t)^{(q-1)/2} + 1\right]^2 = N(t).$$

We have

$$x(P_{-1}) = \frac{N(t) - a\prod_{\alpha\in\mathbb{F}_q}(t-\alpha)^2 - (t_q - t)\prod_{\alpha\in\mathbb{F}_q}(t-\alpha)^2}{\prod_{\alpha\in\mathbb{F}_q}(t-\alpha)^2},$$

so $t - \alpha$ cancels (from both numerator and denominator) if and only if $N(\alpha) = 0$. For $t = \alpha \in \mathbb{F}_q$, if $f(\alpha) = 0$, then we have one cancellation. From equality

$$f(\alpha)^{(q-1)/2} = \begin{cases} -1 & \text{if } f(\alpha) \neq 0 \text{ is a non-square} \\ 1 & \text{if } f(\alpha) \neq 0 \text{ is a square,} \end{cases}$$

we see for $f(\alpha) \neq 0$ non-square we have a double cancellation. Also, if $f(\alpha) \neq 0$ is a square, there is no cancellation. Therefore

$$\begin{aligned} d_{-1} &= 1 + 2q - \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\} - 2 \cdot \#\{\alpha \in \mathbb{F}_q | f(\alpha) \neq 0, \neq \square\} \\ &= 1 + 2 \cdot \{\alpha \in \mathbb{F}_q\} - \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\} - 2 \cdot \#\{\alpha \in \mathbb{F}_q | f(\alpha) \neq 0, \neq \square\} \\ &= 1 + 2 \cdot \#\{\alpha \in \mathbb{F}_q | f(\alpha) \neq 0, = \square\} + \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\} \\ &= N_q. \end{aligned}$$

This proves the lemma. □

Lemma 5.3.4. The integers d_n satisfy the identity

$$d_{n-1} + d_{n+1} = 2d_n + 2.$$

Proof. Here we follow the exposition of Manin's proof as given by Chahal in his Nieuw Archief paper [2]. Note that at some minor points, our argument slightly simplifies Chahal's treatment.

Take P_{n-1}, P_n and P_{n+1}. We consider the following two cases.

Case 1: One of P_{n-1}, P_n and P_{n+1} is O. By definition, $P_n = P_{n-1} + Q = P_{n+1} - Q$, for every $n \in \mathbb{Z}$.

(*i*) If $P_n = O$, then $P_{n-1} = -(t,1)$ and $P_{n+1} = (t,1)$. Therefore, $d_{n-1} = 1$ and $d_{n+1} = 1$. The lemma follows.

(*ii*) If $P_{n-1} = O$, then $P_n = (t,1)$ and $P_{n+1} = 2(t,1)$. By the duplication formula (5.4),

$$x(P_{n+1}) = \frac{t^4 - 2bt^2 - 8ct + b^2 - 4ac}{4t^3 + 4at^2 + 4bt + 4c}. \tag{5.5}$$

We can write this as

$$x(P_{n+1}) = \frac{\frac{df(t)}{dt} - (4a+2t)f(t)}{4f(t)}.$$

Since $f(t)$ does not have multiple roots, we have (5.5) in lowest form and $d_{n+1} = 4$. This proves the lemma.

(*iii*) If $P_{n+1} = O$, then the same argument proves the the lemma in this case.

Case 2: None of P_{n-1}, P_n and P_{n+1} is O. Recall that we introduced the notation $P_i = (f_i/g_i, y_i)$ whenever $P_i \neq O$, where $f_i, g_i \in \mathbb{F}_q[t]$ are coprime, and $y_i \in \mathbb{F}_q(t)$. By the addition formula (5.3), applied to $P_{n-1} = P_n - Q$, one has

$$\begin{aligned}
\frac{f_{n-1}}{g_{n-1}} &= \frac{-(tg_n + f_n)(tg_n - f_n)^2 - ag_n(tg_n - f_n)^2 + f(t)g_n^3(1+y_n)^2}{g_n(tg_n - f_n)^2} \\
&= \frac{(tg_n + f_n)(bg_n + tf_n) + 2g_n(af_n + cg_n) + 2f(t)g_n^2 y_n}{(tg_n - f_n)^2} \\
&= \frac{R}{(tg_n - f_n)^2},
\end{aligned} \tag{5.6}$$

say. Replacing y_n by $-y_n$ in the formula above, one obtains $x(-P_n - Q) = x(-P_{n+1}) = x(P_{n+1})$. Therefore,

$$\begin{aligned}
\frac{f_{n+1}}{g_{n+1}} &= \frac{-(tg_n + f_n)(tg_n - f_n)^2 - ag_n(tg_n - f_n)^2 + f(t)g_n^3(1-y_n)^2}{g_n(tg_n - f_n)^2} \\
&= \frac{(tg_n + f_n)(bg_n + tf_n) + 2g_n(af_n + cg_n) - 2f(t)g_n^2 y_n}{(tg_n - f_n)^2} \\
&= \frac{S}{(tg_n - f_n)^2},
\end{aligned} \tag{5.7}$$

say.

Remark 5.3.5. The assumption $P_{n\pm1} \neq O$ is equivalent to $P_n \neq \pm Q$, or $x(P_n) = f_n/g_n \neq t$. Since in Case 2 above $P_n \neq O$, this means $x(P_n) = f_n/g_n \neq t$, i.e., $f_n \neq tg_n$.

Suppose $P_n \neq O$, so that coprime polynomials f_n and $g_n \in \mathbb{F}_q[t]$ exist with $x(P_n) = f_n/g_n$. Put $y_n := y(P_n)$ as above. Then

$$f(t)y_n^2 = \frac{f_n^3}{g_n^3} + a\frac{f_n^2}{g_n^2} + b\frac{f_n}{g_n} + c,$$

hence $(f(t)g_n^2y_n)^2 \in \mathbb{F}_q[t]$, which implies $f(t)g_ny_n \in \mathbb{F}_q[t]$. Therefore, R and S are also polynomials. Moreover, f_{n-1}/g_{n-1} and f_{n+1}/g_{n+1} are in lowest form; by multiplying them, we get

$$\begin{aligned}\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n - f_n)^4} &= \frac{(tf_n - bg_n)^2 - 4cg_n\left[(t+a)g_n + f_n\right]}{(tg_n - f_n)^2} \\ &= \frac{T}{(tg_n - f_n)^2},\end{aligned} \tag{5.8}$$

say. If we show that, up to a non-zero constant,

$$g_{n-1}g_{n+1} = (tg_n - f_n)^2, \tag{5.9}$$

up to the same constant, then

$$f_{n-1}f_{n+1} = (tf_n - ag_n)^2 - 4cg_n\left[(t+a)g_n + f_n\right].$$

Using Lemma 5.3.1, it follows that the right-hand-side of this expression has the same degree as $t^2f_n^2$. Hence we get

$$\begin{aligned}d_{n-1} + d_{n+1} &= \deg(f_{n-1}f_{n+1}) \\ &= \deg(t^2f_n^2) \\ &= 2d_n + 2.\end{aligned}$$

Now we prove (5.9). It follows from the second equality in (5.8) that $(tg_n - f_n)^2 \mid RS$. Write $(tg_n - f_n)^2 = R_1S_1$ for certain $R_1, S_1 \in \mathbb{F}_q[t]$ such that $R_1 \mid R$ and $S_1 \mid S$. Since

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R}{(tg_n - f_n)^2} = \frac{R}{R_1S_1} = \frac{R/R_1}{S_1},$$

we get $g_{n-1} \mid S_1$. Similarly, we get $g_{n+1} \mid R_1$. Therefore,

$$g_{n-1}g_{n+1} \mid (tg_n - f_n)^2.$$

The equality (5.9) will follow if we prove that also

$$(tg_n - f_n)^2 \mid g_{n-1}g_{n+1}. \tag{5.10}$$

Suppose (5.10) is not true, then an irreducible polynomial $\lambda(t) \in \mathbb{F}_q[t]$ exists such that $v_\lambda((tg_n - f_n)^2) > v_\lambda(g_{n-1}g_{n+1})$, where v_λ is valuation on $\mathbb{F}_q(t)$ corresponding to $\lambda(t)$. We claim that λ and the valuation v_λ have the following properties.

(*a*) $v_\lambda((tg_n - f_n)^2) > 0$;

(*b*) $\lambda \nmid g_n$;

(*c*) $v_\lambda(T) > 0$;

(*d*) $v_\lambda(R) > 0$ and $v_\lambda(S) > 0$.

Property (*a*) is immediate from the assumption

$$v_\lambda((tg_n - f_n)^2) - v_\lambda(g_{n-1}g_{n+1}) > 0.$$

Since $v_\lambda((tg_n - f_n)^2) > 0$ by Property (*a*), the condition $\lambda \mid g_n$ would imply $\lambda \mid tg_n - (tg_n - f_n) = f_n$, violating the fact that g_n and f_n are coprime; hence, Property (*b*) follows.
To see Property (*c*), note that (5.8) implies

$$v_\lambda(f_{n-1}f_{n+1}) - v_\lambda(g_{n-1}g_{n+1}) = v_\lambda(T) - v_\lambda((tg_n - f_n)^2);$$

hence,

$$v_\lambda(T) - v_\lambda(f_{n-1}f_{n+1}) = v_\lambda((tg_n - f_n)^2) - v_\lambda(g_{n-1}g_{n+1}),$$

which by our assumption is strictly positive. This implies that $v_\lambda(T) > 0$.
Finally, to prove Property (*d*), note that we already saw that $(tg_n - f_n)^2 \mid RS$; hence, Property (*a*) implies that $\lambda \mid RS$. Therefore $\lambda \mid R$ or $\lambda \mid S$. Suppose $\lambda \nmid R$, then from (5.6), we get

$$v_\lambda(g_{n-1}) - v_\lambda(f_{n-1}) = v_\lambda((tg_n - f_n)^2) > 0.$$

Since $\gcd(f_{n-1}, g_{n-1}) = 1$, this implies $v_\lambda(f_{n-1}) = 0$; hence, the equality above reduces to

$$v_\lambda(g_{n-1}) = v_\lambda((tg_n - f_n)^2).$$

From (5.8), we now deduce

$$v_\lambda(f_{n+1}) - v_\lambda(g_{n+1}) = v_\lambda(T) > 0.$$

Since the polynomials f_{n+1} and g_{n+1} are co-prime, it follows that $v_\lambda(g_{n+1}) = 0$. Therefore,

$$v_\lambda(g_{n+1}g_{n-1}) = v_\lambda((tg_n - f_n)^2),$$

contradicting our initial assumption. Hence, indeed $\lambda \mid R$. An analogous argument shows that $\lambda \mid S$. Indeed, if $\lambda \nmid S$, then (5.7) shows

$$v_\lambda(g_{n+1}) - v_\lambda(f_{n+1}) = v_\lambda((tg_n - f_n)^2) > 0,$$

which implies $v_\lambda(f_{n+1}) = 0$ and $v_\lambda(g_{n+1}) = v_\lambda((tg_n - f_n)^2)$. Again applying (5.8) shows in this case that

$$v_\lambda(f_{n-1}) - v_\lambda(g_{n-1}) = v_\lambda(T) > 0$$

and $v_\lambda(g_{n-1}) = 0$. Therefore,

$$v_\lambda(g_{n+1}g_{n-1}) = v_\lambda((tg_n - f_n)^2),$$

which is a contradiction. This finishes the proof of the Properties $(a), (b), (c)$ and (d).

Properties (a) and (d) imply that the valuations at λ of

$$f(t)g_n^3(1 - y_n)^2 = S + (tg_n + f_n)(tg_n - f_n)^2 + ag_n(tg_n - f_n)^2$$

and of

$$f(t)g_n^3(1 + y_n)^2 = R + (tg_n + f_n)(tg_n - f_n)^2 + ag_n(tg_n - f_n)^2$$

are both positive, as is seen by considering the right-hand-side. Also, $v_\lambda((1-y_n)^2)$ and $v_\lambda((1+y_n)^2)$ can not both be positive: since $(1-y_n)+(1+y_n) = 2$ and the characteristic is not equal to 2, this would yield a contradiction. If we suppose $v_\lambda((1-y_n)^2) \leq 0$, then $v_\lambda(f(t)) > 0$ since $v_\lambda(f(t)g_n^3(1-y_n)^2) > 0$. Similarly, if $v_\lambda((1 + y_n)^2) \leq 0$, it follows that $v_\lambda(f(t)) > 0$. So we conclude in all cases that $\lambda \mid f$.

By computing modulo $(tg_n - f_n)$ one clearly has $f_n \equiv tg_n \mod (tg_n - f_n)$; hence,

$$T \equiv \left[(t^2g_n - bg_n)^2 - 4cg_n((t-a)g_n + tg_n)\right] \mod (tg_n - f_n),$$

i.e.,

$$T \equiv g_n^2(t^4 - 2bt^2 - 8ct - 4ac + b^2) \mod (tg_n - f_n).$$

Properties $(a), (b)$, and (c) therefore show

$$\lambda \mid (t^4 - 2bt^2 - 8ct - 4ac + b^2) = \delta(t),$$

say. A calculation reveals that the resultant of δ and f equals the square of the discriminant of f, which is nonzero constant in $\mathbb{F}_q$. Since the resultant is an $\mathbb{F}_q[t]$- linear combination of f and δ, this contradicts the fact that f and δ are divisible by λ. So the lemma follows in this case. □

Remark 5.3.6. Note that the polynomial δ, appearing in the proof above, is precisely the numerator appearing in the formula for $x(2P)$.

From the above identity, we obtain that the function d_n can be expressed as a polynomial in n, as follows.

Lemma 5.3.7. The function d_n satisfies

$$d_n = n^2 + a_q n + q.$$

Proof. This follows by induction on n, using the Lemmas 5.3.4 and 5.3.3. □

Proof of Hasse's theorem. Consider the quadratic polynomial

$$d(x) = x^2 + a_q x + q.$$

Assume that Hasse's theorem were false for $E/\mathbb{F}_q$. This is equivalent to the statement $a_q^2 - 4q > 0$, which implies that $d(x)$ has two zeroes. Suppose $x_1 < x_2$ are two zeroes of the above polynomial. Note that the quadratic function $d(x)$ is negative at all values x between x_1 and x_2. By Lemma 5.3.7 and the definition of the number d_n, $d(x)$ takes non-negative values at all integers x. In particular, this implies that the interval (x_1, x_2) does not contain any integer. Hence taking $n = \lfloor x_1 \rfloor$ (the largest integer $\leq x_1$), we have

$$n \leq x_1 < x_2 \leq n + 1. \tag{5.11}$$

It is not possible that both $x_1, x_2 \in \mathbb{Z}$ since this would imply

$$n(n+1) = x_1 x_2 = q,$$

contradicting the fact that $n(n+1)$ in even and q is odd. As a consequence,

$$0 < x_2 - x_1 < 1.$$

This is impossible since $a_q^2 - 4q = (x_1 - x_2)^2$ is assumed to be a positive integer. Therefore,

$$a_q^2 - 4q \leq 0.$$

This completes the proof of Hasse's theorem. □

5.4 In Characteristic two

In the case of odd characteristic we saw that the main theorem followed from the Lemmas 5.3.1, 5.3.3 and 5.3.4. The same line of reasoning will be applied in characteristic two, with suitable adaptations. Suppose $q = 2^e$, for $e \in \mathbb{Z}$ and $e > 0$. Let $E/\mathbb{F}_q$ be an elliptic curve. To keep the formulas from becoming too lengthy, we will treat the two cases, namely ordinary and supersingular, separately.

5.4.1 The ordinary case

Suppose the elliptic curve $E/\mathbb{F}_q$ has non-zero $j-$invariant. The equation of such a curve can be given as

$$E : y^2 + xy = x^3 + ax^2 + b = f(x),$$

where $b \neq 0$ [26, See Appendix A]. The quadratic twist of $E/\mathbb{F}_q(t)$ associated to the quadratic extension $K = \mathbb{F}_q(t, s)$ with $s^2 + ts = t^3 + at^2 + b$ is

$$E^{\text{tw}} : y^2 + txy = t^2 f(x) + x^2 f(t).$$

Note that $t^2 f(x) + x^2 f(t) = t^2 x^3 + t^3 x^2 + bx^2 + bt^2$. The two curves E^{tw} and E are isomorphic over K. The isomorphism is given as follows:

$$\begin{aligned} E &\longrightarrow E^{\text{tw}} \\ (x, y) &\mapsto (x, sx + ty). \end{aligned}$$

The addition and duplication formula on E^{tw} are as follows.
(i) If $O \neq P_j = (x_j, y_j) \in E^{\text{tw}}(\mathbb{F}_q(t))$ and $P_1 \neq \pm P_2$, then

$$x(P_1 + P_2) = \frac{1}{t^2}\left[\left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + t\left(\frac{y_1 + y_2}{x_1 + x_2}\right) + t^3 + b\right] + x_1 + x_2. \quad (5.12)$$

(ii) If $O \neq P = (x, y) \in E^{\text{tw}}(\mathbb{F}_q(t))$, then

$$x(2P) = \frac{x^4 + b}{x^2}. \quad (5.13)$$

We will now explain a correspondence between points on $E^{\text{tw}}(\mathbb{F}_q(t))$ and morphisms in $\text{Mor}_{\mathbb{F}_q}(E, E)$, as we did in the odd characteristic case. By doing so, we can find points on $E^{\text{tw}}(\mathbb{F}_q(t))$ and then repeat Manin's method.

The group $E(K)$ consists, apart from the point O, of points

$$(x(t,s),\, y(t,s))$$

with coordinates in the function field K over $\mathbb{F}_q$ of the curve with equation

$$s^2 + ts = f(t). \tag{5.14}$$

Moreover

$$y(t,s)^2 + x(t,s)y(t,s) = f\left(x(t,s)\right).$$

Since (5.14) defines the curve $E/\mathbb{F}_q$, this means that a point $(x,y) \in E(K)$ corresponds to a morphism in $\mathrm{Mor}_{\mathbb{F}_q}(E,E)$, sending (t,s) to $(x(t,s), y(t,s))$, as in the odd characteristic case. Therefore $E(K) \cong \mathrm{Mor}_{\mathbb{F}_q}(E,E)$. The composition of the isomorphisms $E^{\mathrm{tw}}(K) \cong E(K)$ and $E(K) \cong \mathrm{Mor}_{\mathbb{F}_q}(E,E)$ implies that

$$E^{\mathrm{tw}}(K) \cong \mathrm{Mor}_{\mathbb{F}_q}(E,E)$$

$$(x(t,s), y(t,s)) \mapsto \left[(t,s) \mapsto (x(t,s), \frac{y(t,s) + sx(t,s)}{t})\right].$$

The analogue of Lemma 5.2.1 is the following.

Lemma 5.4.1. Restricted to the subgroup $E^{\mathrm{tw}}(\mathbb{F}_q(t)) \subset E^{\mathrm{tw}}(K)$, the above isomorphism defines

$$E^{\mathrm{tw}}(\mathbb{F}_q(t)) \cong \Psi = \{\psi \in \mathrm{Mor}_{\mathbb{F}_q}(E,E) | [-1] \circ \psi = \psi \circ [-1]\}.$$

Proof. Suppose a point $(x(t), y(t)) \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$, and the corresponding morphism in $\mathrm{Mor}_{\mathbb{F}_q}(E,E)$ is ψ, which sends (t,s) to $(x(t), (y(t) + sx(t))/t)$. Since

$$([-1] \circ \psi)(t,s) = [-1](x(t), \frac{y(t) + sx(t)}{t}) = (x(t), x(t) + \frac{y(t) + sx(t)}{t})$$

and

$$(\psi \circ [-1])(t,s) = (\psi)(t, t+s) = (x(t), \frac{y(t) + (t+s)x(t)}{t}),$$

which shows $[-1] \circ \psi = \psi \circ [-1]$. This proves that $\psi \in \Psi$.

Suppose $\phi \in \mathrm{Mor}_{\mathbb{F}_q}(E,E)$, satisfying $[-1] \circ \phi = \phi \circ [-1]$, maps a point (t,s) on E to $(x(t,s), y(t,s))$. The corresponding point in $E^{\mathrm{tw}}(K)$ is

$$Q = (x(t,s), sx(t,s) + ty(t,s)).$$

The action of the Galois group $G_{K/\mathbb{F}_q(t)} = \{id, \rho\}$ on K is determined by $t^\rho = t,\ s^\rho = t + s$, and the fixed field of $G_{K/\mathbb{F}_q(t)}$ is $\mathbb{F}_q(t)$.

The assumption $\phi \in \Psi$ translates into

$$(x(t,s), x(t,s)+y(t,s)) = (x(t,t+s), y(t,t+s)).$$

This says exactly that the point Q is fixed by the action of the Galois group. This proves that elements of Ψ indeed correspond to points in the subgroup $E^{\mathrm{tw}}(\mathbb{F}_q(t))$ of $E^{\mathrm{tw}}(K)$. □

The identity map on E via the isomorphism becomes the point

$$Q = (t, 0)$$

on $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. The q^{th}-power Frobenius map on E becomes the point

$$P_0 = (x_0, y_0) = (t^q, st^q + ts^q)$$

on $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. Note that by construction the point $P_0 \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$; equivalently, $st^q + ts^q \in \mathbb{F}_q(t)$. We define

$$P_n = P_0 + nQ, \quad \forall\ n \in \mathbb{Z}.$$

Suppose $P_n = (x_n, y_n)$ and write $x_n = f_n/g_n$, where $f_n, g_n \in \mathbb{F}_q[t]$ with $\gcd(f_n, g_n) = 1$. We get a well-defined function

$$d : \mathbb{Z} \to \ \{0, 1, 2, 3, ...\},$$

given by

$$d(n) = d_n = \deg(f_n).$$

The analogue of Lemma 5.3.1 is the following.

Lemma 5.4.2. If $P_n = (x_n, y_n) \neq O$, write $x_n = f_n(t)/g_n(t)$ with $f_n(t), g_n(t) \in \mathbb{F}_q[t]$. Then $\deg(f_n) > \deg(g_n)$.

Proof. Suppose $\tau = 1/t$ and view E^{tw} over $\mathbb{F}_q((\tau))$. On $\mathbb{F}_q((\tau))$, and therefore on its subfield $\mathbb{F}_q(t)$, we use the valuation v corresponding to τ (this is described in more detail in the proof of Lemma 5.3.1). We change coordinates as follows:

$$\xi = \tau^2 x \text{ and } \eta = \tau^4 y.$$

In these new coordinates the equation for E^{tw} is

$$\eta^2 + \tau\xi\eta = \xi^3 + \tau\xi^2 + b\tau^4\xi^2 + b\tau^6.$$

The reduction modulo τ of this equation is the curve

$$\bar{E}^{tw}/\mathbb{F}_q : \ \eta^2 = \xi^3.$$

Since $E_0^{\mathrm{tw}}(\mathbb{F}_q((\tau)))$ is the subgroup of points in $E^{\mathrm{tw}}(\mathbb{F}_q((\tau)))$ whose reduction modulo τ is in $\bar{E}_{ns}^{tw}(\mathbb{F}_q)$, it is easy to see that $E_0^{\mathrm{tw}}(\mathbb{F}_q((\tau)))$ consists of the point O at infinity and all points which, in the (ξ,η) coordinate, satisfy $v(\xi) \leq 0$. In the (x,y) coordinates this means $2 + v(x) \leq 0$. So a point $(x,y) \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$ is in $E_0^{\mathrm{tw}}(\mathbb{F}_q((\tau)))$ precisely when, writing x as a quotient of polynomial in t,

$$\deg(\mathrm{numer}(x)) \geq \deg(\mathrm{denom}(x)) + 2.$$

The above discussion implies that the point $P_0 \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$, but $Q \notin E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$. Using formula (5.13) we obtain

$$x(2Q) = \frac{t^4 + b}{t^2}.$$

Clearly, this implies $2Q \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$. Therefore, if n is even, then

$$P_n = P_0 + nQ \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t)).$$

So for n even the lemma is true.

If n is odd, then write $P_n = P_{n-1} + Q$. Since $n-1$ is even, the above argument implies that $P_{n-1} \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$.

We claim that if a point $P \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$, then

$$\deg(\mathrm{numer}(x(P+Q))) = \deg(\mathrm{denom}(x(P+Q))) + 1.$$

This is obvious when $P = O$. Hence assume $P \neq O$ and write $P = (f/g, y)$ for polynomial $f, g \in \mathbb{F}_q[t]$. By addition formula (5.12), we get

$$x(P+Q) = \frac{g^2y + t^2fg + tf^2}{f^2 + g^2t^2}.$$

Since the assumption $P \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ means $\deg(g) \leq \deg(f) - 2$, this implies that the degree of the denominator of the given expression for $x(P+Q)$ is $\deg(f^2)$. Now we find the degree of the numerator of in the same expression. The point P satisfies the equation of E^{tw}, and this can be written as

$$(g^2y)^2 + tfg(g^2y) + t^2f^3g + bt^2g^4 + t^3f^2g^2 + bf^2g^2 = 0. \tag{5.15}$$

This implies $g^2y \in \mathbb{F}_q[t]$. We now show that (5.15) implies that the polynomial $g^2y \in \mathbb{F}_q[t]$ has strictly smaller degree than tf^2. Since $\deg(g) \leq \deg(f) - 2$, this implies

$$\deg(g^2y) < \deg(tf^2).$$

Namely, if not, then the first term in the left-hand-side of (5.15) would have strictly larger degree than any of the other terms, which is impossible. It follows that the degree of $g^2y + t^2fg + tf^2$ is $\deg(tf^2)$. Hence, our claim follows.

The above claim proves the lemma for n odd. Consequently, the lemma is true for all $n \in \mathbb{Z}$.

□

Lemma 5.4.3.

$$d_{-1} = N_q.$$

Proof. By the addition formula (5.12)

$$\begin{aligned} x(P_{-1}) &= x(P_0 - Q) \\ &= \frac{1}{t^2}\left[\left(\frac{st^q + ts^q + t^2}{t^q + t}\right)^2 + t\left(\frac{st^q + ts^q + t^2}{t^q + t}\right) + t^3 + b\right] + t^q + t \\ &= \frac{t^{2q+1} + t^{q+2} + t^{q+1} + st^q + ts^q}{(t^q + t)^2}. \end{aligned} \tag{5.16}$$

We claim that $st^q + ts^q$ is a polynomial in t of degree $(3q+2)/2$, this would imply that the degree of numerator of $x(P_{-1})$ is $2q+1$.

Note that $st^q + ts^q$ belongs to $\mathbb{F}_q(t) \subset K = \mathbb{F}_q(E)$. Moreover, $st^q + ts^q$ has no poles outside the point at infinity O, because s and t have a pole of order 3 and 2, respectively, at O and no other poles. Therefore $st^q + ts^q \in \mathbb{F}_q[t]$(otherwise it would have poles outside O).

Suppose v is the valuation on K corresponding to O. Therefore $v(st^q + ts^q) = -3q - 2$, because $v(t) = -2$ and $v(s) = -3$. Since the non-zero polynomial $f \in \mathbb{F}_q[t]$ has valuation $v(f) = -2\deg_t(f)$, it follows that

$$\deg_t(st^q + ts^q) = \frac{3q+2}{2} < 2q + 1.$$

Consequently, the numerator in (5.16) has degree $2q+1$, and

$$d_{-1} = 2q + 1 - \#\{\text{Cancellations of degree one factors}\}.$$

We now count $\#\{\text{Cancellations of degree one factors}\}$. Write

$$N(t) = t^{2q+1} + t^{q+2} + t^{q+1} + st^q + ts^q \in \mathbb{F}_q[t],$$

for numerator of (5.16). Since $(t^q+t)^2 = \prod_{t_0 \in \mathbb{F}_q}(t+t_0)^2$, we need to examine which $t_0 \in \mathbb{F}_q$ are zeroes of $N(t)$, and if they are, whether the multiplicity

of such a zero is 1 or ≥ 2. To evaluate $N(t)$ at $t_0 \in \mathbb{F}_q$, pick $s_0 \in \overline{\mathbb{F}}_q$ such that $Q_0 = (t_0, s_0) \in E(\overline{\mathbb{F}}_q)$. Then

$$N(t_0) = t_0^2 + s_0 t_0 + t_0 s_0^q.$$

The fact that $N(t) \in \mathbb{F}_q[t]$ implies that this value is independent of the choice of s_0.

(i) If Q_0 is a $\mathbb{F}_q$-rational point, then $N(t_0) = t_0^2$; hence,

$$N(t_0) = 0 \Leftrightarrow t_0 = 0.$$

(ii) If Q_0 is not $\mathbb{F}_q$-rational, then $s_0^q \neq s_0$. Since s_0 satisfies

$$s_0^2 + t_0 s_0 = f(t_0),$$

this implies s_0^q is the conjugate of s_0, i.e., $s_0^q = s_0 + t_0$. Therefore, $N(t_0) = t_0^2 + s_0 t_0 + t_0(s_0 + t_0) = 0$.

It follows that we get a cancellation $t_0 \in \mathbb{F}_q$ in (5.16) if $t_0 = 0$ or t_0 is not the x-coordinate of a rational point (x-CRP).

To see whether we have a single or a double cancellation at such t_0, we need to compute $N'(t_0)$. To this end, first extend the derivative d/dt on $\mathbb{F}_q(t)$ to a derivative on $K = \mathbb{F}_q(t, s)$. Since $s^2 + ts = f(t)$, this means we have to define s' such that $2s \cdot s' + s't + s = f'(t)$, i.e., $s' = (f'(t) + s)/t$. As a consequence,

$$\begin{aligned} \frac{dN}{dt} &= t^{2q} + t^q + s' t^q + s^q \\ &= t^{2q} + t^{q+1} + t^q + s t^{q-1} + s^q. \end{aligned}$$

For $t_0 = 0$, we have $s_0 = b^{q/2}$; hence, $N'(0) = b^{q/2} \neq 0$. We get one cancellation. For non-zero $t_0 \in \mathbb{F}_q$ such that t_0 is not an x-CRP, we have $N'(t_0) = t_0 + s_0 + s_0 + t_0 = 0$. This implies that we get two cancellation. Hence,

$$d_{-1} = 2q + 1 - 1 - 2 \cdot \#\{t_0 \in \mathbb{F}_q | 0 \neq t_0 \neq \text{x-CRP}\}.$$

Since

$$q = 1 + \#\{t_0 \in \mathbb{F}_q | 0 \neq t_0 = \text{x-CRP}\} + \#\{t_0 \in \mathbb{F}_q | 0 \neq t_0 \neq \text{x-CRP}\},$$

this implies

$$d_{-1} = 2 + 2 \cdot \#\{t_0 \in \mathbb{F}_q | 0 \neq t_0 = \text{x-CRP}\} = N_q.$$

This proves the lemma. □

Lemma 5.4.4. The integers d_n satisfy the identity

$$d_{n-1} + d_{n+1} = 2d_n + 2.$$

Proof. Take P_{n-1}, P_n and P_{n+1}. We consider the following two cases.

Case 1: One of P_{n-1}, P_n and P_{n+1} is O.

(i) If $P_n = O$, then $P_{n-1} = -(t, 0)$, and $P_{n+1} = (t, 0)$. Hence $d_{n-1} = 1$ and $d_{n+1} = 1$. The lemma follows.

(ii) If $P_{n-1} = O$, then $P_n = (t, 0)$ and $P_{n+1} = 2(t, 0)$. By the duplication formula (5.13), we have

$$x(P_{n+1}) = \frac{t^4 + b}{t^2}.$$

This is in lowest form, since $b \neq 0$; therefore, $d_{n+1} = 4$. Hence, the lemma follows in this situation.

(iii) If $P_{n+1} = O$, then the same argument proves the lemma.

Case 2: None of P_{n-1}, P_n and P_{n+1} is O. Recall our notation, i.e., $P_i = (f_i/g_i, y_i)$ whenever $P_i \neq O$, where $f_i, g_i \in \mathbb{F}_q[t]$. By the addition formula (5.12), applied to $P_{n-1} = P_n - Q$, one has

$$\begin{aligned} \frac{f_{n-1}}{g_{n-1}} &= \frac{tf_n(tg_n + f_n) + tf_n g_n + g_n^2 y_n}{(tg_n + f_n)^2} \\ &= \frac{R}{(tg_n + f_n)^2}, \end{aligned} \tag{5.17}$$

say. Replacing P_n by $-P_n$ is the same as replacing y_n by $y + tf/g$, in the formula above. One obtains in this way

$$\begin{aligned} \frac{f_{n+1}}{g_{n+1}} &= \frac{tf_n(tg_n + f_n) + g_n^2 y_n}{(tg_n + f_n)^2} \\ &= \frac{S}{(tg_n + f_n)^2}, \end{aligned} \tag{5.18}$$

say. Since $g_n^2 y_n$ is a polynomial, also R and S are in $\mathbb{F}_q[t]$. By multiplying the expressions (5.17) and (5.18), we get

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n + f_n)^4} = \frac{t^2 f_n^2 + bg_n^2}{(tg_n + f_n)^2} = \frac{T}{(tg_n + f_n)^2}, \tag{5.19}$$

say. If we show that, up to a non-zero constant,

$$g_{n-1}g_{n+1} = (tg_n + f_n)^2, \tag{5.20}$$

then, upto the same constant,

$$f_{n-1}f_{n+1} = t^2 f_n^2 + bg_n^2.$$

Using Lemma 5.4.2, it follows that the degree of the right-hand-side of this expression is $\deg(t^2 f_n^2)$. Hence, we get

$$\begin{aligned} d_{n-1} + d_{n+1} &= \deg(f_{n-1}f_{n+1}) \\ &= \deg(t^2 f_n^2) \\ &= 2d_n + 2. \end{aligned}$$

Now we prove (5.20). It follows from the second equality of (5.19) that $(tg_n + f_n)^2 \mid RS$. Suppose $(tg_n + f_n)^2 = R_1 S_1$ for certain $R_1,\ S_1 \in \mathbb{F}_q[t]$ such that $R_1 \mid R$ and $S_1 \mid S$. Since

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R}{(tg_n + f_n)^2} = \frac{R}{R_1 S_1} = \frac{R/R_1}{S_1},$$

we get $g_{n-1} \mid S_1$. Similarly, we get $g_{n+1} \mid R_1$. Therefore

$$g_{n-1}g_{n+1} \mid (tg_n + f_n)^2.$$

The equality (5.20) will follow if we prove that also

$$(tg_n + f_n)^2 \mid g_{n-1}g_{n+1}. \tag{5.21}$$

Suppose (5.21) is not true, then an irreducible polynomial $\lambda(t) \in \mathbb{F}_q[t]$ exists such that $v_\lambda((tg_n + f_n)^2) > v_\lambda(g_{n-1}g_{n+1})$, where v_λ is valuation on $\mathbb{F}_q[t]$ corresponding to λ. We claim that λ and the valuation v_λ have the following properties.

(*a*) $v_\lambda((tg_n + f_n)^2) > 0$;

(*b*) $\lambda \nmid g_n$;

(*c*) $v_\lambda(T) > 0$;

(*d*) $v_\lambda(R) > 0$ and $v_\lambda(S) > 0$.

These properties can be proved using exactly the same reasoning we used in the proof of Lemma 5.3.4.

Properties (*a*) and (*d*) imply that the valuations at λ of

$$g_n^2(y_n + tf_n/g_n) = R + tf_n(tg_n + f_n)$$

and of

$$g_n^2 y_n = S + t f_n (t g_n + f_n).$$

are both positive, as is seen by considering the right-hand-side. This and Property (b) imply that $v_\lambda(y_n + t f_n/g_n) > 0$ and $v_\lambda(y_n) > 0$. It follows that $v_\lambda(t f_n/g_n) > 0$; hence, $v_\lambda(t f_n) > 0$, and therefore, because of (c), $v_\lambda(b g_n) > 0$, contradicting (b) since $b \neq 0$. This contradiction proves the lemma in this case. □

Hasse's inequality, for an elliptic curve $E/\mathbb{F}_q$ with $q = 2^e$ and $j(E) \neq 0$, follows by combining the Lemmas 5.4.2, 5.4.3 and 5.4.4. The argument is the same as the one presented on page 67, except for one detail: to see why $x_1, x_2 \in \mathbb{Z}$ leads to a contradiction, note that it would imply

$$n(n+1) = x_1 x_2 = q = 2^e$$

in this case. As a consequence, $e = 1$ and either $x_2 = -1$ or $x_1 = 1$. If $x_2 = -1$, this would mean $0 = d(-1) = d_{-1} = \#E(\mathbb{F}_q) > 0$, a contradiction. Furthermore, note that when $q = 2$ we have

$$x(P_1) = \frac{t^4 + at^2 + b}{t^3 + t};$$

hence, $3 \leq d_1 \leq 4$, so $d(1) \neq 0$ in this case.

Alternatively, note that $d(x)$ cannot be 0 at two consecutive integers since it would imply $d_m = d_{m+1} = 0$ for some $m \in \mathbb{Z}$. Using Lemma 5.4.2 this implies $P_m = P_{m+1} = O$, which is absurd since $P_{m+1} = P_m + Q$.

5.4.2 The supersingular case

Suppose as before $q = 2^e$ with $e \geq 1$, and assume that the elliptic curve $E/\mathbb{F}_q$ has $j-$invariant 0; this is equivalent to E being a supersingular elliptic curve. The equation of such a curve can be given as

$$E : y^2 + ay = x^3 + bx + c = f(x),$$

where $a \neq 0$, and note that a^3 is the discriminant [26, Appendix A](note the misprint in the Second Edition; the formula as presented in the original First Edition are correct). The quadratic twist of $E/\mathbb{F}_q(t)$ associated to the quadratic extension $K = \mathbb{F}_q(t, s)$ with $s^2 + as = f(t)$ is

$$E^{\mathrm{tw}} : y^2 + ay = f(x) + f(t).$$

Note that $f(x) + f(t) = x^3 + bx + t^3 + bt$. The two curves E^{tw} and E are isomorphic over K. The isomorphism is given as follows:

$$E \longrightarrow E^{\text{tw}}$$
$$(x, y) \mapsto (x, s + y).$$

The addition and duplication formula on E^{tw} are the usual ones (compare [26, Section III.2])

(i) If $O \neq P_j = (x_j, y_j) \in E^{\text{tw}}(\mathbb{F}_q(t))$, and $P_1 \neq \pm P_2$, then

$$x(P_1 + P_2) = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2. \tag{5.22}$$

(ii) If $O \neq P = (x, y) \in E^{\text{tw}}(\mathbb{F}_q(t))$, then

$$x(2P) = \frac{x^4 + b^2}{a^2}. \tag{5.23}$$

Just as we saw in the odd characteristic case and in the case of ordinary curves in characteristic 2, we have isomorphism between the groups $E(K)$ and $\text{Mor}_{\mathbb{F}_q}(E, E)$. By composing this isomorphism with the isomorphism between E^{tw} and E we get the following isomorphism

$$E^{\text{tw}}(K) \cong \text{Mor}_{\mathbb{F}_q}(E, E),$$

$$(x(t, s), y(t, s)) \mapsto [(t, s) \mapsto (x(t, s), s + y(t, s)]\,.$$

Lemma 5.4.5. Restricted to the subgroup $E^{\text{tw}}(\mathbb{F}_q(t)) \subset E^{\text{tw}}(K)$, the above isomorphism defines

$$E^{\text{tw}}(\mathbb{F}_q(t)) \cong \Psi = \{\psi \in \text{Mor}_{\mathbb{F}_q}(E, E) | [-1] \circ \psi = \psi \circ [-1]\}.$$

Proof. This is completely analogous to the cases we already discussed. Note that here $[-1] : E \to E$ is given by $(x, y) \mapsto (x, y + a)$. □

The identity map on E via the isomorphism of Lemma 5.4.5 becomes the point

$$Q = (t, 0)$$

on $E^{\text{tw}}(\mathbb{F}_q(t))$. The point corresponding to q^{th}-power Frobenius is

$$P_0 = (x_0, y_0) = (t^q, s + s^q)$$

on $E^{\mathrm{tw}}(\mathbb{F}_q(t))$. Note that by construction the point P_0 is $\mathbb{F}_q(t)$-rational, equivalently $s + s^q \in \mathbb{F}_q(t)$. We define

$$P_n = P_0 + nQ, \quad n \in \mathbb{Z}.$$

Suppose $P_n = (x_n, y_n)$ and write $x_n = f_n/g_n$, where $f_n, g_n \in \mathbb{F}_q[t]$, with $\gcd(f_n, g_n) = 1$. We get a well-defined function

$$d : \mathbb{Z} \to \{0, 1, 2, 3, ...\}$$

given by

$$d(n) = d_n = \begin{cases} 0 & \text{if } P_n = 0; \\ \deg(f_n) & \text{otherwise.} \end{cases}$$

In this case, the analogue of Lemma 5.3.1 is the following.

Lemma 5.4.6. If $P_n = (x_n, y_n) \neq O$, write $x_n = f_n(t)/g_n(t)$ with $f_n(t), g_n(t) \in \mathbb{F}_q[t]$. Then $\deg(f_n) > \deg(g_n)$.

Proof. Suppose $\tau = 1/t$ and view E^{tw} over $\mathbb{F}_q((\tau))$. On $\mathbb{F}_q((\tau))$, and therefore on its subfield $\mathbb{F}_q(t)$, we use the valuation v corresponding to the place with uniformizer τ. So in particular for $g \in \mathbb{F}_q[t]$ one has $v(g) = -\deg(g)$. We change coordinates as follows:

$$\xi = \tau^2 x \text{ and } \eta = \tau^3 y.$$

The equation of E^{tw} in these new coordinates is

$$\eta^2 + a\tau^3\eta = \xi^3 + b\tau^4\xi + \tau^3 + b\tau^5.$$

The reduction modulo τ of this equation is the curve

$$\bar{E}^{tw}/\mathbb{F}_q : \ \eta^2 = \xi^3.$$

It is easy to see that a point $(x, y) \in E^{\mathrm{tw}}(\mathbb{F}_q(t))$ is in $E_0^{\mathrm{tw}}(\mathbb{F}_q((\tau)))$ precisely when, writing x as a quotient of polynomial in t,

$$\deg(\mathrm{numer}(x)) \geq \deg(\mathrm{denom}(x)) + 2.$$

In particular, it follows that the point $P_0 \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$, and $Q \notin E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$. Using formula (5.23) we obtain

$$x(2Q) = \frac{t^4 + b^2}{a^2}.$$

This implies that $2Q \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$. Therefore, if n is even, then

$$P_n = P_0 + nQ \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t)).$$

So for n even the lemma is true.

If n is odd, then write $P_n = P_{n-1} + Q$. Since $n-1$ is even, the above argument implies that $P_{n-1} \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$.

We claim that if a point $P \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$, then

$$\deg(\mathrm{numer}(x(P+Q))) = \deg(\mathrm{denom}(x(P+Q))) + 1.$$

This is obvious when $P = O$. Hence assume $P \neq O$ and write $P = (f/g, y)$ for polynomial $f, g \in \mathbb{F}_q[t]$. By the addition formula (5.22), we get

$$x(P+Q) = \frac{tf^2 + t^2fg + bfg + btg^2 + ag^2y}{f^2 + g^2t^2}.$$

Since the assumption $P \in E_0^{\mathrm{tw}}(\mathbb{F}_q(t))$ means $\deg(g) \leq \deg(f)-2$, this implies that the degree of the denominator of the given expression for $x(P+Q)$ is $\deg(f^2)$. Now we find the degree of the numerator of in the same expression. The point P satisfies the equation of E^{tw}, and this can be written as

$$(g^2y)^2 + tg^2(g^2y) + f^3g + bfg^3 + t^3g^4 + btg^4 = 0. \tag{5.24}$$

This implies $g^2y \in \mathbb{F}_q[t]$. We now show that (5.24) implies that the polynomial $g^2y \in \mathbb{F}_q[t]$ has strictly smaller degree than tf^2. Namely, if this were false, then the inequality $\deg(g) \leq \deg(f) - 2$ would imply that all but the first nonzero terms in (5.24) have degree strictly smaller than $\deg((g^2y)^2)$. Clearly this would contradict (5.24). It follows that the degree of $tf^2 + t^2fg + bfg + btg^2 + ag^2y$ is $\deg(tf^2)$. Hence, our claim follows.

The above claim proves the lemma for n odd. Consequently, the lemma is true for all $n \in \mathbb{Z}$.

□

Lemma 5.4.7.

$$d_{-1} = N_q.$$

Proof. We compute d_{-1}. By the addition formula (5.22)

$$\begin{aligned} x(P_{-1}) &= (t^q, s + s^q) + (t, a) \\ &= \frac{t^{2q+1} + t^{q+2} + b(t^q + t) + a(s^q + s) + a^2}{(t^q + t)^2} \end{aligned} \tag{5.25}$$

We claim that $s+s^q \in \mathbb{F}_q(t)$ is a polynomial in t of degree $3q/2$, and therefore the degree of numerator of the expression given above equals $2q+1$.

As a function on E, $s+s^q$ has no poles outside the point at infinity, O, because s has only one pole of order 3 at O. Therefore $s+s^q \in \mathbb{F}_q[t]$(otherwise it would have poles outside O).

Suppose v is the valuation on $\mathbb{F}_q(E)$ corresponding to O. Then $v(s+s^q) = -3q$. Since a nonzero polynomial $g \in \mathbb{F}_q[t] \subseteq \mathbb{F}_q(E)$ satisfies $v(g) = -3\deg_t(g)$, it follows that

$$\deg_t(s+s^q) = \frac{3q}{2} < 2q+1.$$

Consequently,

$$d_{-1} = 2q+1 - \#\{\text{Cancellations of degree one factors}\}.$$

Write

$$N(t) = t^{2q+1} + t^{q+2} + b(t^q+t) + a(s^q+s) + a^2,$$

for the numerator in (5.25). Since $(t^q+t)^2 = \prod_{t_0 \in \mathbb{F}_q}(t+t_0)^2$, we need to examine which $t_0 \in \mathbb{F}_q$ are zeroes of $N(t)$, and if they are, whether the multiplicity of such a zero is 1 or ≥ 2.

Let $t = t_0 \in \mathbb{F}_q$. Pick $s_0 \in \overline{\mathbb{F}}_q$ such that $Q_0 = (t_0, s_0) \in E(\overline{\mathbb{F}}_q)$. Then

$$N(t_0) = a(s_0^q + s_0) + a^2.$$

(i) If Q_0 is a rational point of $E/\mathbb{F}_q$, then

$$N(t_0) = a^2 \neq 0.$$

(ii) If Q_0 is not rational, then $s_0^q \neq s_0$. Since s_0 satisfies

$$s_0^2 + as_0 = f(t_0),$$

s_0^q is the conjugate of s_0, i.e., $s_0^q = s_0 + a$. It follows that $N(t_0) = a(s_0 + a + s_0) + a^2 = 0$.

Therefore, we get a cancellation at $t_0 \in \mathbb{F}_q$ iff t_0 is not an x-CRP.

To calculate the derivative of $N(t)$, we first extent the derivative d/dt to $\mathbb{F}_q(t,s)$. Since $s^2 + as = t^3 + bt + c$, the extension is given by

$$as' = t^2 + b.$$

As a consequence,

$$\frac{dN}{dt} = t^{2q} + b + t^2 + b = t^{2q} + t^2.$$

It follows that we have two cancellations for every $t_0 \in \mathbb{F}_q$, which is not an x-CRP. Consequently,

$$d_{-1} = 2q + 1 - 2 \cdot \#\{t_0 \in \mathbb{F}_q | t_0 \neq \text{x-CRP}\}.$$

On the other hand

$$q = \#\{t_0 \in \mathbb{F}_q | t_0 = \text{x-CRP}\} + \#\{t_0 \in \mathbb{F}_q | t_0 \neq \text{x-CRP}\}.$$

Therefore,

$$d_{-1} = 1 + 2 \cdot \#\{t_0 \in \mathbb{F}_q | t_0 = \text{x-CRP}\} = N_q,$$

since if t_0 is the x-coordinate of $(t_0, s_0) \in E(\mathbb{F}_q)$, then also $(t_0, s_0 + a) \in E(\mathbb{F}_q)$. This proves the lemma. □

Lemma 5.4.8. The integers d_n satisfies the identity

$$d_{n-1} + d_{n+1} = 2d_n + 2.$$

Proof. Take P_{n-1}, P_n and P_{n+1}. We consider the following two cases.
Case 1: One of P_{n-1}, P_n and P_{n+1} is O.

(i) If $P_n = O$, then $P_{n-1} = -(t, 0)$ and $P_{n+1} = (t, 0)$. Hence $d_{n-1} = 1$ and $d_{n+1} = 1$. So the lemma follows in this case.

(ii) If $P_{n-1} = O$, then $P_n = (t, 0)$ and $P_{n+1} = 2(t, 0)$. By the duplication formula (5.23)

$$x(P_{n+1}) = \frac{t^4 + b^2}{a^2},$$

hence $d_{-1} = 0$, $d_n = 1$ and $d_{n+1} = 4$. So also in this case the lemma follows.

(iii) If $P_{n+1} = O$, then the same reasoning proves the lemma.

Case 2: Now assume that none of P_{n-1}, P_n and P_{n+1} is O, then by the addition formula (5.22)

$$x(P_{n-1}) = \frac{f_{n-1}}{g_{n-1}} = \frac{(tf_n + bg_n)(tg_n + f_n) + ag_n^2(y_n + a)}{(tg_n + f_n)^2} = \frac{R}{(tg_n + f_n)^2}, \tag{5.26}$$

say. Also

$$x(P_{n+1}) = \frac{f_{n+1}}{g_{n+1}} = \frac{(tf_n + bg_n)(tg_n + f_n) + ag_n^2 y_n}{(tg_n + f_n)^2} = \frac{S}{(tg_n + f_n)^2}, \tag{5.27}$$

say. Note that R and S are in $\mathbb{F}_q[t]$. By multiplying the expression of $x(P_{n-1})$ and $x(P_{n+1})$, we get

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n+f_n)^4} = \frac{t^2f_n^2+b^2g_n^2+a^2g_n(tg_n+f_n)}{(tg_n+f_n)^2} = \frac{T}{(tg_n+f_n)^2}, \tag{5.28}$$

say. If we show that, up to a non-zero constant,

$$g_{n-1}g_{n+1} = (tg_n+f_n)^2, \tag{5.29}$$

then, upto the same constant,

$$f_{n-1}f_{n+1} = t^2f_n^2+b^2g_n^2+a^2g_n(tg_n+f_n).$$

Hence, by comparing degrees and using Lemma 5.4.6, it follows that

$$\begin{aligned} d_{n-1}+d_{n+1} &= \deg(t^2f_n^2) \\ &= 2d_n+2. \end{aligned}$$

Now we prove (5.29). It follows from (5.28) that $(tg_n+f_n)^2 \mid RS$. Write $(tg_n+f_n)^2 = R_1S_1$, where $R_1,\ S_1 \in \mathbb{F}_q[t]$ and $R_1 \mid R,\ S_1 \mid S$. Since

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R}{(tg_n+f_n)^2} = \frac{R}{R_1S_1} = \frac{R/R_1}{S_1},$$

it follows that $g_{n-1} \mid S_1$. Similarly, $g_{n+1} \mid R_1$, so $g_{n-1}g_{n+1} \mid (tg_n+f_n)^2$. The equality (5.29) will hold if we prove that also

$$(tg_n+f_n)^2 \mid g_{n-1}g_{n+1}. \tag{5.30}$$

Suppose (5.30) is not true. Then a irreducible polynomial $\lambda(t) \in \mathbb{F}_q[t]$ exists such that $v_\lambda((tg_n-f_n)^2) > v_\lambda(g_{n-1}g_{n+1})$. This v_λ is valuation on $\mathbb{F}_q(t)$ corresponding to $\lambda(t)$. We claim that λ and the valuation v_λ have the following properties.

(a) $v_\lambda((tg_n+f_n)^2) > 0$;

(b) $\lambda \nmid g_n$;

(c) $v_\lambda(T) > 0$;

(d) $v_\lambda(R) > 0$ and $v_\lambda(S) > 0$.

These properties can be proved using exactly the same reasoning we used in the proof of Lemma 5.3.4.

Properties (a) and (d) imply that the valuations at λ of

$$ag_n^2(Y_n + a) = R + (tf_n + bg_n)(tg_n + f_n)$$

and of

$$ag_n^2 Y_n = S + (tf_n + bg_n)(tg_n + f_n).$$

are both positive, as is seen by considering the right-hand-side. This fact and Property (b) imply that $v_\lambda(y_n + a) > 0$ and $v_\lambda(y_n) > 0$. It follows that $v_\lambda(a) > 0$, contradiction $a \neq 0$. This proves the lemma in this case. □

Hasse's inequality, for supersingular elliptic curve $E/\mathbb{F}_q$ with $q = 2^e$, follows by combining the Lemmas 5.4.6, 5.4.7 and 5.4.8. The argument is the same as the one presented in the end of the case of ordinary elliptic curve. This complete elementary proof of Hasse's theorem in all characteristics.

Remark 5.4.9. Note that, regardless of the characteristic, in the definition of the number d_n two cases are distinguished: $P_n = O$ and $P_n \neq O$.

Furthermore, the following holds.

Proposition 5.4.10. Suppose $\mathbb{F}_q$ is an arbitrary finite field of cardinality q. Let $E/\mathbb{F}_q$ be an elliptic curve, and define $(d_n)_{n\in\mathbb{Z}}$ as in sections 5.2, 5.4.1 and 5.4.2. The following statements are equivalent.

(1) $d_n = 0$

(2) $P_n = O$

(3) $\phi_q = [-n]$

(4) $\mathrm{rank}(E^{\mathrm{tw}}(\mathbb{F}_q(t))) = 4$ and $\#E(\mathbb{F}_q = q + 2n + 1$

Proof. It is to easy to the equivalence of (1), (2) and (3); we show the equivalence of (3) and (4).

(3) ⇒ (4). We know that

$$\mathrm{rank}(E^{\mathrm{tw}}(\mathbb{F}_q(t))) = \mathrm{rank}(\mathrm{End}_{\mathbb{F}_q}(E)).$$

Furthermore, $\#E(\mathbb{F}_q) = \deg(\phi_q - [1]) = \deg[-n-1] = n^2+2n+1 = q+2n+1$ since $q = \deg(\phi_q) = \deg([-n]) = n^2$. In particular this implies that $E/\mathbb{F}_q$ is supersingular. Hence $\mathrm{rank}(\mathrm{End}_{\mathbb{F}_q}(E)) = 4$. $\mathrm{End}_{\mathbb{F}_q}(E)$ is the subring of

$\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ consisting of all endomorphisms commuting with ϕ_q. Since here $\phi_q = [-n]$, it follows that

$$\mathrm{End}_{\mathbb{F}_q}(E) = \mathrm{End}_{\bar{\mathbb{F}}_q}(E).$$

This proves (4).

(4) $\Rightarrow$ (3). From $\mathrm{rank}(E^{\mathrm{tw}}(\mathbb{F}_q(t))) = 4$ it follows that $\mathrm{End}_{\mathbb{F}_q}(E)$ has rank 4. This implies that

$$\mathrm{End}_{\mathbb{F}_q}(E) \otimes \mathbb{Q} = \mathrm{End}_{\bar{\mathbb{F}}_q}(E) \otimes \mathbb{Q},$$

hence ϕ_q commutes with every endomorphism. The center of the quaternion ring $\mathrm{End}_{\mathbb{F}_q}(E)$ consists of $\mathbb{Z}$, hence $\phi_q = [m] \in \mathbb{Z}$. It follows

$$q - 2m + 1 = \#E(\mathbb{F}_q) = q + 2n + 1,$$

so $\phi_q = [-n]$. □

5.5 Magma

In this section we will illustrate Manin's proof and our extension of it to all characteristic, using the Magma algebra system [1]. More precisely, we provide Magma-code that takes a "random" elliptic curve E over a "random" finite field $\mathbb{F}_q$, and then defines $E^{\mathrm{tw}}/\mathbb{F}_q(t)$ and the points P_0, Q on it. The values d_n and, in particular, $d_{-1} = \#E(\mathbb{F}_q)$ can be found using Magma.

We do this in the three cases

1. Odd characteristic,
2. Characteristic two and E ordinary,
3. Characteristic two and E supersingular,

separately. In the first two cases, isomorphisms between a curve E^{tw} as given in the preceding section, and a curve given in the usual Weierstrass form are needed. Note that in the last case, E^{tw} is already a Weierstrass equation.

5.5.1 Odd characteristic

```
n:=Random(1,5);
rn:=Random(2,7);
p:=NthPrime(rn);
```

```
q:=p^n;
Fq<g>:=GF(q);
a:=Random(Fq); b:=Random(Fq); c:=Random(Fq);
E0:=EllipticCurve([Fq|0,a,0,b,c]);
Fqt<t>:=FunctionField(Fq);
R<Y>:=PolynomialRing(Fqt);
K<s>:=quo<R|(Y^2-(t^3+a*t^2+b*t+c))>;
P2<x,y,z>:=ProjectiveSpace(K,2);
Ctw:=Curve(P2,(t^3+a*t^2+b*t+c)*y^2*z-(x^3+a*x^2*z+b*x*z^2+c*z^3));
O:=Ctw![0,1,0];
Etw, phi:=EllipticCurve(Ctw,O);
Q:=Ctw![t,1,1];
P0:=Ctw![t^q,s^(q-1),1];
d:= function(m);
      Pm:=Inverse(phi)(phi(P0)+m*phi(Q));
      if Pm[3] eq 0
      then return 0;
      else return Degree(Numerator(Fqt!(Pm[1]/Pm[3])));
      end if;
    end function;
d(-1); #E0;
d(15);
for l:=1 to 10
    do print(d(l-1)+d(l+1)-2*d(l)-2);
end for;
```

5.5.2 Characteristics two and E ordinary

```
n:=Random(1,12);
q:=2^n;
Fq<g>:=GF(q);
a:=Random(Fq); b:=Random(Fq);
E0:=EllipticCurve([Fq|1,a,0,0,b]);
Fqt<t>:=FunctionField(Fq);
R<Y>:=PolynomialRing(Fqt);
K<s>:=quo<R|(Y^2+t*Y+(t^3+a*t^2+b))>;
P2<x,y,z>:=ProjectiveSpace(K,2);
Ctw:=Curve(P2,(y^2*z+t*x*y*z+t^2*x^3+t^3*x^2*z+b*x^2*z+b*t^2*z^3));
O:=Ctw![0,1,0];
Etw, phi:=EllipticCurve(Ctw,O);
Q:=Ctw![t,0,1];
P0:=Ctw![t^q,s*t^q+t*s^q,1];
d:= function(m);
      Pm:=Inverse(phi)(phi(P0)+m*phi(Q));
      return Degree(Numerator(Fqt!(Pm[1]/Pm[3])));
```

```
    end function;
d(-1); #E0;
d(15);
for l:=1 to 10
    do print(d(l-1)+d(l+1)-2*d(l)-2);
end for;
```

5.5.3 Characteristics two and E supersingular

```
n:=Random(1,12);
q:=2^n;
Fq<g>:=GF(q);
a:=Random(Fq); b:=Random(Fq); c:=Random(Fq);
E0:=EllipticCurve([Fq|0,0,a,b,c]);
Fqt<t>:=FunctionField(Fq);
R<Y>:=PolynomialRing(Fqt);
K<s>:=quo<R|(Y^2+a*Y+(t^3+b*t+c))>;
Etw:=EllipticCurve([K|0,0,a,b,t^3+b*t]);
Q:=Etw![t,0,1];
P0:=Etw![t^q,s^q+s,1];
d:= function(m);
      Pm:=P0+m*Q;
      if Pm[3] eq 0
      then return 0;
      else return Degree(Numerator(Fqt!(Pm[1]/Pm[3])));
      end if;
    end function;
d(-1); #E0;
d(15);
for l:=1 to 10
    do print(d(l-1)+d(l+1)-2*d(l)-2);
end for;
```

Samenvatting

In dit proefschrift geven we constructies van krommen met veel punten over een eindig lichaam. Het maximale aantal punten dat een kromme van geslacht g gedefinieerd over een eindig lichaam van cardinaliteit q kan hebben, wordt als $N_q(g)$ genoteerd.

In het eerste hoofdstuk geven we een historisch overzicht van resultaten betreffende $N_q(g)$. We noemen een kromme C over het eindige lichaam $\mathbb{F}_q$ "goed" als het aantal rationale punten binnen 10% van de Hasse-Weil-Serre grens ligt. Dat wil zeggen:

$$\#C(\mathbb{F}_q) > \frac{9}{10}\left(q + 1 + g\lfloor\sqrt{4q}\rfloor\right),$$

waarbij g het geslacht van de kromme C is.

In het tweede hoofdstuk beschouwen we het geval van de elliptische krommen (geslacht 1 krommen met een aangewezen rationaal punt). Uit werk van Deuring (1941) en van Waterhouse (1969) volgt een algemene formule voor $N_q(1)$. We geven voor q klein, expliciete geslacht 1 krommen met $N_q(1)$ punten erop. In Sectie 2.6 beantwoorden we de vraag: onder welke omstandigheden zijn een elliptische kromme en een kwadratische twist daarvan isomorf over het grondlichaam? Bovendien bestuderen we in de twee laatste secties van dit hoofdstuk de nulpunten in $\mathbb{Z}$ van de veeltermen

$$X^3 - 3nX - \lfloor n\sqrt{4n}\rfloor,$$
$$X^5 - 5nX^3 + 5n^2X - \lfloor n^2\sqrt{4n}\rfloor.$$

Deze veeltermen komen voor in een van de methoden voor het vinden van maximale elliptische krommen.

In het derde hoofdstuk behandelen we het geval van krommen met geslacht twee. Jean-Pierre Serre vond in 1985 een expliciete formule voor $N_q(2)$. In dit korte hoofdstuk gebruiken we een methode beschreven in een publicatie van Howe, Leprévost en Poonen (2000) waarmee in veel gevallen een expliciete vergelijking van een geslacht twee kromme met $N_q(2)$ punten erop

kan worden gevonden, uitgaande van een elliptische kromme die $N_q(1)$ punten bevat.

In het vierde hoofdstuk beschouwen we krommen met een hoger geslacht en met een grote groep van automorfismen. Maxim Hendriks (2013) gaf in zijn proefschrift modellen van krommen die een zogeheten platonische afbeelding toelaten. Door de Jacobiaan van deze krommen te ontbinden en door ze te reduceren modulo priemgetallen, vinden we een heleboel voorbeelden van maximale en van goede krommen. We geven bovendien in dit hoofdstuk een flink aantal voorbeelden van maximale en van goede krommen van hoger geslacht, die verkregen zijn als vezelproduct van twee krommen van geslacht 1. We geven twee tabellen met goede krommen. De eerste bevat voorbeelden van goede krommen met geslacht vier, verkregen als vezelproduct van elliptische krommen die $N_q(1)$ punten bevatten. De tweede tabel bevat voorbeelden van goede krommen die met behulp van het proefschrift van Maxim Hendriks zijn gevonden.

In het vijfde hoofdstuk tenslotte, breiden we een elementair bewijs gevonden door Yuri I. Manin (1956), uit naar een meer algemene situatie. Dit betreft het klassieke resultaat van Helmut Hasse (1933) dat zegt dat voor een elliptische kromme E over het eindige lichaam $\mathbb{F}_q$ geldt dat

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

Summary

In this thesis we propose constructions of curves with many points over a finite field. The maximal number of points that a curve of genus g over a finite field with cardinality q can have is denoted $N_q(g)$.

In the first chapter we give a small historical survey of results on $N_q(g)$. We call a curve over $\mathbb{F}_q$ "good" if the number of rational points is within 10% of Hasse-Weil-Serre bound. That means

$$\#C(\mathbb{F}_q) > \frac{9}{10}(q + 1 + g\lfloor\sqrt{4q}\rfloor),$$

where g denotes the genus of the curve.

In the second chapter we consider the case of elliptic curves (genus one curves with a rational point). A general formula for $N_q(1)$ follows from a result of Deuring (1941) and of Waterhouse (1969); we find explicit curves reaching $N_q(1)$ points for small q. In Section 2.6, we answer the question: when are an elliptic curve and its quadratic twist isomorphic over the ground field? Moreover, in the last two sections of this chapter we study the zeros in $\mathbb{Z}$ of the polynomials

$$X^3 - 3nX - \lfloor n\sqrt{4n}\rfloor,$$
$$X^5 - 5nX^3 + 5n^2X - \lfloor n^2\sqrt{4n}\rfloor.$$

These polynomial play a role in one of the methods for finding maximal elliptic curves.

In the third chapter we consider the case of curves of genus two. Jean-Pierre Serre in 1985 found an explicit formula for $N_q(2)$; in this short chapter we recall a method described in a paper by Howe, Leprévost, and Poonen (2000) which in many cases can be used to find an explicit equation of a genus two curve with $N_q(2)$ points from an equation of an elliptic curve with $N_q(1)$ points.

In the fourth chapter we consider curves of higher genus with large automorphism group. Maxim Hendriks (2013) has given models of curves

admitting so-called platonic maps in his thesis. By decomposing the Jacobian of these curves and reducing them modulo primes we obtain lots of examples of maximal and good curves. Moreover, in this chapter we give lots of examples of maximal and good curves of higher genus obtained as the fibre products of genus one curves. We give two tables of good curves. The first table contains examples of good curves of genus 4 obtained as the fibre products of elliptic curves with $N_q(1)$ points, and the second table contains examples of good curves obtained using the thesis of Maxim Hendriks.

Finally, in the fifth chapter we extend an elementary proof due to Yuri I. Manin (1956) of the classical result of Helmut Hasse (1933) stating that for an elliptic curve E over the finite field $\mathbb{F}_q$ one has

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

Acknowledgements

This dissertation would not have been possible without the help that I received from many people. I would like to take this opportunity to thank some of them.

First and foremost, I would like to thank my supervisor Jaap Top for the support, guidance he provided, and the patience he showed throughout the completion of this dissertation. I consider myself fortunate to have such a supervisor.

I would also like to thank my reading committee members Prof. J.S. Chahal, Prof. F. Hess and Prof. C. Ritzenthaler for their time in reading the manuscript and for their valuable suggestions.

I thank the participants/organisers of Intercity Number Theory Seminar for the inspiring talks.

I learned a lot from Sir Basat Kumar when I was in Degree college Larkana. And I believe I would not have been writing this acknowledgement if I had not met him. I would like to thank Sir Kumar for his support.

I would also like to thank PhD-students and staff members of JBI for creating a lively environment. I learned a lot of interesting things during the discussions of our lunch group. I would like to thank Fiaz, Bas and Harsh very much for their help at the early stage of my Ph.D. I would also like to thank Ane for being so helpful.

I would like to thank two couples Fiaz-Raheela and Sasanka-Divya for their endless support. For me, they were like a family in Groningen. I have experienced unforgettable moments with them. Moreover, I specially thank Sasanka for his help in making the cover page.

I would also like to thank all my friends who I met in Groningen, especially Arefin, Omer and Zaman, with whom I have spent great time.

I thank Q.U.E.S.T. for the financial support for this project.

Finally, I thank my family and friends back in Larkana for their love and encouragement, specially my father who every Saturday revived me with his encouraging discussions.

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Jasbir S. Chahal. Manin's proof of the Hasse inequality revisited. *Nieuw Arch. Wisk. (4)*, 13(2):219–232, 1995.

[3] Jasbir S. Chahal and Brian Osserman. The Riemann hypothesis for elliptic curves. *Amer. Math. Monthly*, 115(5):431–442, 2008.

[4] Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[5] Eisaku Furukawa, Mitsuru Kawazoe, and Tetsuya Takahashi. Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In *Selected areas in cryptography*, volume 3006 of *Lecture Notes in Comput. Sci.*, pages 26–41. Springer, Berlin, 2004.

[6] A. O. Gel'fond and Yu. V. Linnik. *Elementary methods in the analytic theory of numbers*. Translated from the Russian by D. E. Brown. Translation edited by I. N. Sneddon. International Series of Monographs in Pure and Applied Mathematics, Vol. 92. Pergamon Press, Oxford, 1966.

[7] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[8] Maxim Hendriks. Platonic maps of low genus. Ph.D. thesis, TU/e, 2013.

[9] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.

[10] Tomoyoshi Ibukiyama. On rational points of curves of genus 3 over finite fields. *Tohoku Math. J. (2)*, 45(3):311–329, 1993.

[11] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[12] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[13] Tetsuo Kodama, Jaap Top, and Tadashi Washio. Maximal hyperelliptic curves of genus three. *Finite Fields Appl.*, 15(3):392–403, 2009.

[14] Izumi Kuribayashi and Akikazu Kuribayashi. On automorphism groups of compact Riemann surfaces of genus 4. *Proc. Japan Acad. Ser. A Math. Sci.*, 62(2):65–68, 1986.

[15] Izumi Kuribayashi and Akikazu Kuribayashi. Automorphism groups of compact Riemann surfaces of genera three and four. *J. Pure Appl. Algebra*, 65(3):277–292, 1990.

[16] Yu. I. Manin. On cubic congruences to a prime modulus. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 20:673–678, 1956.

[17] Stephen Meagher and Jaap Top. Twists of genus three curves over finite fields. *Finite Fields and their Appl.*, 16:347–368, 2010.

[18] V. Kumar Murty, editor. *Algebraic curves and cryptography*, volume 58 of *Fields Institute Communications*. American Mathematical Society, Providence, RI, 2010.

[19] Peter Roquette. The Riemann hypothesis in characteristic p, its origin and development. I. The formation of the zeta-functions of Artin and of F. K. Schmidt. *Mitt. Math. Ges. Hamburg*, 21(2):79–157, 2002. Hamburger Beiträge zur Geschichte der Mathematik.

[20] Peter Roquette. The Riemann hypothesis in characteristic p, its origin and development. II. The first steps by Davenport and Hasse. *Mitt. Math. Ges. Hamburg*, 23(2):5–74, 2004.

[21] Peter Roquette. The Riemann hypothesis in characteristic p, its origin and development. III. The elliptic case. *Mitt. Math. Ges. Hamburg*, 25:103–176, 2006.

[22] Jean-Pierre Serre. Nombres de points des courbes algébriques sur $\mathbf{F}_q$. In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983.

[23] Jean-Pierre Serre. Rational points on curves over finite fields. Unpublished notes by F.Q. Gouvêa of lectures at Harvard. 1985.

[24] V. Shabat. Curves with many points. Ph.D. thesis, Amsterdam, 2001.

[25] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[26] Joseph H. Silverman. *The arithmetic of elliptic curves. Graduate Text in Mathematics 106*. Springer- Verlag, New York, second edition, 2009.

[27] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[28] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[29] Jaap Top. Descent by 3-isogeny and 3-rank of quadratic fields. In *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., pages 303–317. Oxford Univ. Press, New York, 1993.

[30] Jaap Top. Curves of genus 3 over small finite fields. *Indag. Math. (N.S.)*, 14(2):275–283, 2003.

[31] Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin. *Algebraic geometric codes: basic notions*, volume 139 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2007.

[32] Gerard van der Geer and Marcel van der Vlugt. Tables of curves with many points. *Math. Comp.*, 69(230):797–810, 2000.

[33] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[34] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[35] André Weil. *Variétés abéliennes et courbes algébriques.* Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.