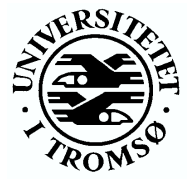

A DISSERTATION FOR THE DEGREE OF DOCTOR SCIENTIARUM

Factorisation patterns of division polynomials of elliptic curves defined over a finite field

Hugues Verdure

June 2003

Department of Mathematics and Statistics
Faculty of Science
University of Tromsø
Norway

Author: Hugues Verdure

Publisher: Institutt for matematikk og statistikk, Universitetet i Tromsø, 9037 Tromsø, Norge

ISBN: 82-92461-42-6

Aknowledgments

Ceci est peut-être la partie la plus importante et la plus difficile de ma thèse, et je ne sais pas comment résoudre ce problème. Comble pour un matheux, je tente de le faire sans ordre précis :

Tusen takk til Loren, min veileder, Ragnar, Ben og Andrei,

Tusen takk til Johan og Kristian som har akseptert å komme til Tromsø i dag,

Mille mercis à Papa, Maman, Luc et Marc. Vous m'avez toujours soutenu par tous les moyens, mêmes si vous n'étiez pas toujours ravis,

Tusen takk til Tormod, Cathrine, Eirik, Hilja, Ida, Geir, Kurt.

Tusen takk til Ane, Pans, Anja, Feico, Per. En spesiell takk til Tom som fikk den glimrende ideen å disputere i dag også.

Tusen takk til dykkerne fra SUT,

Mille mercis à mes amis français, Christophe et Delphine, Benjamin et Stéphanie, Boud,

Mille mercis à F. Morain, P. Gaudry, J.J. Risler, Z. Mebkhout et A. Arabia,

Arigatai Takakazu,

Наконец, Мария; Спосибо большое тебе! Вез тебя, я никогда не мог
быполнять эти последние месяца. Я тебя люблю.

Contents

Chapter 1

Introduction

In the middle of the 1980's, Victor Miller [Mil86] and Neal Koblitz [Kob87b] independently proposed building cryptosystems with elliptic curves defined over finite fields. Since then, modern cryptography uses these curves. Almost everything that was able to be done in "traditional" public-key cryptography is implementable with elliptic curves over finite fields. But a big advantage of elliptic curve cryptosystems is the size of the keys used. For example, to realize a secure RSA with the traditional method, we need keys of size 2048 bits, whereas for identical security, keys of size just 210 bits are sufficient in elliptic curve cryptography. This however does not increase the speed. Moreover, the implementation of the arithmetic of elliptic curves is almost as easy as arithmetic over finite fields. Thus elliptic curve cryptography has every reason to be popular: easy to implement, and as secure as traditional cryptography, but with work spaces of much less size, i.e. we need less resources.

This cryptography being promised a beautiful future, research has then begun to look at its possible weaknesses and strengths in order to avoid the former and make use of the latter. The security of elliptic curves cryptosystems is based on the fact that the elliptic curve discrete logarithm problem is believed to be hard. But in 1993, Alfred Menezes, Tatsuaki Okamoto and Scott Vanstone [MOV93] proved that in the case of supersingular curves, the elliptic curve discrete logarithm problem can be reduced in polynomial time to the discrete logarithm problem in a small extension of the base field, which renders cryptography based on such curves more vulnerable to an attack. So, unless we definitely want to use such curves, these should be avoided in cryptography. In the same manner, in 1998-99, Takakazu Satoh and Kiyomichi Araki [SA99] and Nigel Smart [Sma99] on the one hand, and Igor Semaev [Sem98] on the other hand, independently proved that another class of curves should be avoided, the so-called anomalous curves, that is elliptic curves of trace 1 defined over a prime finite field. Indeed in that case, the group of rational points is isomorphic to the base field and is therefore automatically cyclic. By using p-adic numbers, formal groups and formal logarithms, we can then solve the elliptic curve discrete logarithm problem in linear time.

It is not known whether cyclicity is a problem for cryptography, but in the particular case mentioned above, it is, since it is isomorphic to the base field. But the cyclicity can also be an advantage. In 1991, Burton Kaliski [Kal91] presented a method of constructing one-way permutations that uses elliptic curves. The fact that it is one-way relies once again on the difficulty of the

elliptic curve discrete logarithm problem (and thus anomalous and supersingular curves should be avoided). The construction requires that both a curve and one of its quadratic twists are cyclic.

As we have just seen in the two last examples, the cyclicity of the group of rational points of an elliptic curve defined over a finite field can both be an advantage and a drawback. It is therefore important to study it. One natural method to study it is to look at the l-torsion for some prime number l small compared to the size of the base field, since the non-cyclicity can just come from l-torsion for prime numbers l of maximal size close to the square root of the size of the base field. These l-torsion points, or more accurately their x-coordinates, are explicitly given by the roots of the l-th division polynomial of the curve. We are going to study these division polynomials, or more precisely their factorisations into irreducible factors over the base field.

This has another point of interest: for cryptographical purposes, some elliptic curves are more secure than other ones, and this depends on the cardinality of the group of rational points. And these division polynomials are one of the keys in Schoof's algorithm for counting the number of points on an elliptic curve defined over a finite field. Schoof uses them to find the trace of the Frobenius endomorphism modulo l for small l. An improvement due to Elkies uses not the l-th division polynomial itself, but one of its factors of small degree, and it is therefore natural once again to study the possible factorisations of these polynomials, as well as the probabilities of obtaining such a factorisation.

This dissertation is organized in the following way: we will first give some theoretical background on the notions that we will use afterwards. We freely use the notation in Joseph Silverman's book [Sil86], which will be our reference book for the basic theory of elliptic curves. We begin by talking about lattices and elliptic curves over $\mathbb{C}$ (chapter 2), since it appears to be the best way to introduce division polynomials and modular curves, notions that we then define and use on elliptic curves defined over finite fields. Thereafter come elliptic curves over finite fields (chapter 3). Even if the following concepts are not specific to elliptic curves over finite fields, we will define there the Frobenius endomorphism, the Weil pairing and quadratic twists, which are three important aspects of this dissertation. To conclude this background session, we will come back more precisely to two cryptographical points mentioned above, namely the algorithms of Schoof and SEA, and the one-way permutation of Kaliski (chapter 4).

The dissertation in itself begins with the study of 2 and 3-torsion points of elliptic curves over finite fields (chapter 5). We begin by looking thoroughly at polynomials of degree 3 defined over finite fields of characteristic greater than 4 since two such polynomials will be central in the forthcoming study. We also prove an extension of a theorem of Pellet (theorem 11) that will be of great importance later. We continue by studying the cyclicity of the group of rational points generally, and to this purpose, we use a result of Schoof (theorem 13). Finally, after some computations, we arrive at criteria allowing us to distinguish when the group of rational points are 2 or 3-cyclic or not. Jean-Pierre Serre [Ser72] established them already in 1972, but we give here a new and original proof.

We then come to the central part of this dissertation, namely the study of the possible factorisations of division polynomials into irreducible factors over the base field (chapter 6). The study of the degrees of the irreducible factors of the l-th division polynomials is in fact equivalent to the study of the degrees of the extensions of the x-coordinates of points of l-torsion, which in turn is equivalent, up to a possible factor 2, to the study of the degrees of the extensions on which l-torsion points are defined. The degrees of these extensions are given by the action of the Frobenius endomorphism on the $\mathbb{F}_l$-vector space of l-torsion points. In the case where l is equal to the characteristic p of the field of definition of the curve, the study of the Frobenius is quite simple, since this action is given by a scalar, namely the trace of Frobenius. This is what we treat first. In the case where l is not equal to p, then the study is more subtile. We divide the study into two subcases again. When all l-torsion points are defined over the same extension, then the action of the Frobenius endomorphism may be difficult to describe, but the wanted degrees are of course easy to find. Here we use quadratic twists to possibly find the factor 2 mentioned above. When the l-torsion points are defined over different extensions, then we use the Weil pairing to describe the action of the Frobenius endomorphism on l-torsion points. this enables us to find eigenvalues of this endomorphism, and we thus reach our goal.

In the third part, we prove a result similar to a theorem proved by René Schoof [Sch95] on modular polynomials. In the case when the base field is a finite field of odd characteristic, the determinant of the l-th division polynomial is either always a quadratic residue or not, depending only on l and the characteristic of the base field (chapter 7). The result is reached by counting the number of irreducible factors of the l-th division polynomials and then by

using Pellet's theorem mentioned above. We manage to link the 2-valuations of the degrees of the extensions on which the l-torsion points are defined, of q, of $l-1$ or l^2-1, so that we can exclude some cases of factorisation types. This property will prevent us from deciding on the l-cyclicity of an elliptic curve just by looking at the quadratic residuacity of this determinant.

The final part of this dissertation is dedicated to a partial study of the asymptotic probabilities for obtaining certain patterns of factorisation for division polynomials (chapter 8). By using some results on modular curves on finite fields that give an estimate on the number of elliptic curves having rational l-torsion points and non-cyclic rational l-torsion subgroups respectively, we will give a complete answer for these probabilities when the division polynomials have a linear factor, and then, using the two previous parts, when $l = 3$. We will conclude by giving a conjecture à la Sato-Tate concerning the asymptotic probabilities in the general case, a conjecture which will be based on certain facts, and we then discuss the consequences of this conjecture for the elliptic Kummer theory.

In an appendix, we give some examples of factorisations, as well as some computations that have been made to check our conjecture.

Notation

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{F}_q$ are respectively the natural integers, the integers, the rational numbers, the real numbers, the complex numbers, and the finite field with q elements. The same symbols used with a star indicate that we remove the zero element.

If a and b are in $\mathbb{Z}$, then $a \vee b$ and $a \wedge b$ are respectively the lowest common multiple and greatest common divisor of a and b.

If a, b, n are integers, then $a \equiv b\ [n]$ means that a is congruent to b modulo n.

If $\mathcal{S}$ is a set and $\mathcal{T}$ is a subset of $\mathcal{S}$, then we denote by $\mathcal{T} \subset \mathcal{S}$. If the inclusion is strict, then it is denoted by $\mathcal{T} \subsetneq \mathcal{S}$. Moreover, the complement of $\mathcal{T}$ in $\mathcal{S}$ is denoted by $\mathcal{S} \backslash \mathcal{T}$.

v_2 is the common 2-valuation on $\mathbb{N}^*$.

If A and B are two groups (respectively two fields) and A is a subgroup (respectively a subfield) of B, then $[A : B]$ is the index of B in A. Moreover, if both are fields, and A is a Galois extension of B, then the Galois group of the extension A/B is denoted by $Gal(A : B)$.

If $\mathbb{K}$ is a field, then $\overline{K}$ is the algebraic closure of $\mathbb{K}$. Moreover, $\mathbb{P}^1(\mathbb{K})$ is the projective line.

If $\mathcal{S}$ is a set and $\approx$ is an equivalence relation on this set, then the quotient set is denoted by $\mathcal{S}/_{\approx}$. In particular, if $\mathcal{S}$ is a set of elliptic curves defined over $\mathbb{F}_q$, then $\mathcal{S}/_{\approx_{\mathbb{F}_q}}$ is the quotient of $\mathcal{S}$ and the equivalence relation "being

isomorphic over $\mathbb{F}_q$". In the same way, if B is a subgroup of a group A, then $B/_A$ is the quotient group, and if A acts on a set $\mathcal{U}$, then $\mathcal{U}/_A$ and ${}_A\backslash\mathcal{U}$ are the sets of left and right cosets respectively when defined.

Let $\mathbb{K}$ be a field and $P(X)$ be a polynomial over $\mathbb{K}$. Let $d_1, \ldots, d_n \in \mathbb{N}^*$, $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$ and $a \in \mathbb{K}$. Then P is of type $(a, (d_1, \alpha_1), \ldots, (d_n, \alpha_n))$ if for every $1 \leqslant i \leqslant n$, there exist α_i monic irreducible polynomials $P_{i,1}, \ldots, P_{i,\alpha_i}$ of degree d_i such that

$$P(X) = a \prod_{i=1}^{n} \prod_{j=1}^{\alpha_i} P_{i,j}(X).$$

Alternatively, we say that the pattern of P is $(a, (d_1, \alpha_1), \ldots, (d_n, \alpha_n))$. Sometimes, the a is not written.

If $z \in \mathbb{C}$, then $\overline{z}$, $\Re(z)$ and $\Im(z)$ are respectively the complex conjugate, the real and imaginary part of z respectively.

If R is a commutative ring with unit, then $M_2(R)$, $GL_2(R)$ and $SL_2(R)$ are respectively the ring of 2×2 matrices its subgroup of invertible elements, and its special linear group.

If E is an elliptic curve defined over a field $\mathbb{K}$ by a Weierstrass equation

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

then the element $[0, 1, 0] \in E(\mathbb{K}) \subset \mathbb{P}^1(\mathbb{K})$ is denoted by $\mathcal{O}$ and is the neutral element.

Chapter 2

Lattices and elliptic curves over $\mathbb{C}$

In this chapter, we are going to introduce lattices over $\mathbb{C}$, elliptic functions, and more particularly the Weierstrass $\wp$-function. This special function will allow us to establish an explicit link between elliptic curves defined over $\mathbb{C}$ and lattices. Even if the rest of this dissertation deals primarily with elliptic curves defined over finite fields, we begin with a chapter on complex elliptic curves. Historically, it is more accurate, but it will also be much easier to introduce the two important notions of division polynomial and modular polynomial, notions that will be extended to finite fields afterwards. We will not recall the elementary theory of elliptic curves (Weierstrass form, reduced form, elliptic invariants, group law, formal group...). The reader can refer to [Sil86].

2.1 Lattices

Definition 1 *A lattice in $\mathbb{C}$ is a $\mathbb{Z}$-submodule of rank 2 of $\mathbb{C}$.*

Definition 2 *Let Λ be a lattice in $\mathbb{C}$. An elliptic function relative to Λ is a meromorphic function $f(z)$ on $\mathbb{C}$ such that*

$$\forall z \in \mathbb{C}\ , \forall \lambda \in \Lambda\ , f(z+\lambda) = f(z).$$

Note that the only elliptic functions relative to a lattice Λ that are holomorphic are immediately constant because of the double cyclicity and Liouville's theorem. Here are our main examples of elliptic functions:

Definition 3 *Let Λ be a lattice in $\mathbb{C}$. The Weierstrass $\wp$-function relative to Λ is defined by*

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \left[\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right].$$

In order to link lattices in $\mathbb{C}$ to elliptic curves over $\mathbb{C}$, we will also need the following functions:

Definition 4 *Let Λ be a lattice in $\mathbb{C}$. Let $k \in \mathbb{N}^*$. The Eisenstein series of weight $2k$ relative to Λ is defined by*

$$G_{2k}(\Lambda) = \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \lambda^{-2k}.$$

Theorem 1 *Let Λ be a lattice in $\mathbb{C}$. Then*

1. *The Eisenstein series G_{2k} relative to Λ converges absolutely for any $k > 1$,*
2. *The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on any compact subset of $\mathbb{C}\backslash\Lambda$. It defines a meromorphic function over $\mathbb{C}$ with a double pole at any point of Λ and no other pole,*
3. *The Weierstrass $\wp$-function is an even elliptic function , and its derivative*
$$\wp'(z,\Lambda) = -2\sum_{\lambda\in\Lambda}\frac{1}{(z-\lambda)^3}$$
is an odd elliptic function,
4. *Any elliptic function relative to Λ is a rational combination of $\wp(z,\Lambda)$ and $\wp'(z,\Lambda)$.*

Proof: See [Sil86]

□

We will now describe the relation between lattices, the Weierstrass $\wp$-functions and elliptic curves, by giving a differential equation satisfied by the Weierstrass $\wp$-function.

Definition 5 *Let Λ be a lattice in $\mathbb{C}$. Then*
$$g_2(\Lambda) = 60G_4(\Lambda)$$
and
$$g_3(\Lambda) = 140G_6(\Lambda).$$

Theorem 2 *Let Λ be a lattice in $\mathbb{C}$. Then*

1. *The polynomial*
$$f(X) = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$$
is separable, and thus its discriminant $\Delta(\Lambda) = g_2^3(\Lambda) - 27g_3^2(\Lambda)$ is never zero,
2.
$$\forall z \in \mathbb{C}\backslash\Lambda,\ \wp'(z,\Lambda)^2 = f(\wp(z,\Lambda)),$$

3. *Let $E_\Lambda \subset \mathbb{P}^1(\mathbb{C})$ be the elliptic curve defined by*
$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$
Let $\mathbb{T}_\Lambda = \mathbb{C}/\Lambda$ be the complex torus relative to Λ. Then
$$\begin{array}{rccc} \Phi_\Lambda : & \mathbb{T}_\Lambda & \longrightarrow & E_\Lambda \\ & z & \longmapsto & [\wp(z,\Lambda), \wp'(z,\Lambda), 1] \\ & 0 & \longmapsto & [0,1,0] \end{array}$$
is a complex analytic isomorphism of complex Lie groups,
4. *The addition formula for the Weierstrass $\wp$-function is given by:*
$$4\left[\wp(u)+\wp(v)+\wp(u+v)\right] = \left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2$$
if $u \neq v$ and
$$4\left[\wp(2u)+2\wp(u)\right] = \left(\frac{\wp''(u)}{\wp'(u)}\right)^2 = \frac{\left(6\wp(u)^2 - \frac{1}{2}g_2(\Lambda)\right)^2}{4\wp(u)^3 - g_2(\Lambda)\wp(u) - g_3(\Lambda)}.$$

Proof: See [Sil86], [Web95].

□

We can thus construct an elliptic curve from a lattice. The converse is true:

Theorem 3 *Let $E/\mathbb{C}$ be an elliptic curve defined by a Weierstrass equation $E : y^2 = 4x^3 + Ax + B$. Then, up to homothety, there exists a unique lattice Λ in $\mathbb{C}$ such that*
$$\Phi_\Lambda : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$
is a complex analytic isomorphism of complex Lie groups.

Proof: See [Sil86]

□

2.2 Division polynomials

We want to study the torsion points on elliptic curves. For elliptic curves over $\mathbb{C}$, that is rather trivial, since the m-torsion subgroup is always isomorphic to $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$, but it may look quite different over a non-algebraically-closed field. The first way to study torsion is to look at division polynomials, which give a complete description of the x-coordinates of these torsion points. We will here use the Weierstrass $\wp$- function, as done in [Web95] to define these polynomials. Afterwards, we will give a more modern description of these polynomials.

Let E be an elliptic curve over $\mathbb{C}$ defined by the Weierstrass equation

$$E : y^2 = 4x^3 - ax - b.$$

Let Λ be a lattice in $\mathbb{C}$ such that $\Phi_\Lambda : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ is an isomorphism. Let (ω_1,ω_2) be a $\mathbb{Z}$-basis of Λ. Let $n \in \mathbb{N}^*$. Consider

$$f_n(u) = \wp(nu) - \wp(u).$$

This is an elliptic function for Λ, and its poles are of the form

$$u_p = \frac{\nu_1\omega_1 + \nu_2\omega_2}{n}, \quad (\nu_1,\nu_2) \in \mathbb{N}^2$$

except for $n = 1$. In the same way, the zeros of f are the points

$$u_z = \frac{\nu_1\omega_1 + \nu_2\omega_2}{n \pm 1} \notin \Lambda, \ (\nu_1,\nu_2) \in \mathbb{N}^2$$

if $n \neq 1$. We then introduce the function

$$\Theta_n(u) = n^2 \prod_{\substack{0 \leqslant \nu_1,\nu_2 < n \\ (\nu_1,\nu_2) \neq (0,0)}} \left[\wp(u) - \wp\left(\frac{\nu_1\omega_1 + \nu_2\omega_2}{n}\right)\right].$$

Using the fact that $\wp$ is even and that

$$\wp'(u)^2 = 4\left[\wp(u) - \wp\left(\frac{\omega_1}{2}\right)\right]\left[\wp(u) - \wp\left(\frac{\omega_2}{2}\right)\right]\left[\wp(u) - \wp\left(\frac{\omega_1+\omega_2}{2}\right)\right]$$

we get that

$$\Theta_n(u) = \begin{cases} (P_n(\wp(u)))^2 & \text{if } n \text{ is odd} \\ (\wp'(u)P_n(\wp(u)))^2 & \text{if } n \text{ is even,} \end{cases}$$

where P_n is a polynomial in one variable of degree $\frac{n^2-1}{2}$ if n is odd and $\frac{n^2-4}{2}$ if n is even and such that the leading coefficient is n when n is odd, and $-\frac{n}{2}$ when n is even. Let $Q_n(X,Y) = P_n(X)$ if n is odd and $Q_n(X,Y) = YP_n(X)$ if n is even.

Then, comparing the zeroes and poles of the function

$$\frac{\Theta_n(u)f_n(u)}{Q_{n-1}(\wp(u),\wp'(u))\,Q_{n+1}(\wp(u),\wp'(u))},$$

we can deduce that

$$\begin{aligned} \wp(nu) &= \wp(u) - \frac{Q_{n+1}(\wp(u)\wp'(u))\,Q_{n-1}(\wp(u),\wp'(u))}{Q_n(\wp(u),\wp'(u))^2} \\ &= \frac{\wp(u)Q_n(\wp(u),\wp'(u))^2 - Q_{n+1}(\wp(u)\wp'(u))\,Q_{n-1}(\wp(u),\wp'(u))}{Q_n(\wp(u),\wp'(u))^2} \end{aligned}$$

Moreover, it is easy to compute by using the addition formula for the Weierstrass $\wp$-function, that

$$Q_1(X,Y) = 1,$$

$$Q_2(X,Y) = -Y,$$

$$Q_3(X,Y) = 3X^4, -\tfrac{3}{2}aX^2 - 3bX - \tfrac{a^2}{16},$$

$$Q_4(X,Y) = Y\left(-2X^6 + \tfrac{5}{2}aX^4 + 10bX^3 + \tfrac{5}{8}a^2X^2 + \tfrac{1}{2}abX + b^2 - \tfrac{a^3}{32}\right).$$

Finally, we find a recursion formula:

$$Q_{2n+1}(X,Y) = Q_{n+2}(X,Y)Q_n^3(X,Y) - Q_{n+1}^3(X,Y)Q_{n-1}(X,Y),$$

$$YQ_{2n}(X,Y) = -Q_n(X,Y)\left(Q_{n+2}(X,Y)Q_{n-1}^2(X,Y) - Q_{n+1}^2(X,Y)Q_{n-2}(X,Y)\right).$$

In a similar way, we find that

$$\begin{aligned} \wp'(nu) &= \frac{Q_{n+2}(\wp(u),\wp'(u))Q_{n-1}^2(\wp(u),\wp'(u))}{\wp'(u)Q_n^3(\wp(u),\wp'(u)} \\ &\quad - \frac{Q_{n-2}(\wp(u),\wp'(u))Q_{n+1}^2(\wp(u),\wp'(u))}{\wp'(u)Q_n^3(\wp(u),\wp'(u))}. \end{aligned}$$

Define the polynomials R_n and S_n in the following way:

$$R_1(X) = X,$$

$$R_n(X) = XQ_n^2(X,Y) - Q_{n-1}(X,Y)Q_{n+1}(X,Y) \qquad \text{if } n > 1,$$

$$S_1(X,Y) = Y,$$

$$YS_2(X,Y) = Q_4(X,Y),$$

$$YS_n(X,Y) = Q_{n+2}(X,Y)Q_{n-1}^2(X,Y) - Q_{n-2}(X,Y)Q_{n+1}^2(X,Y) \quad \text{if } n > 2.$$

Theorem 4 *Let E be an elliptic curve over $\mathbb{C}$ given by a Weierstrass equation*

$$E : y^2 = 4x^3 - ax - b.$$

Let $n \in \mathbb{N}^*$. Let Q_n, R_n and S_n be the polynomials defined above. Let $P = (x,y) \in E(\mathbb{C})\backslash\{\mathcal{O}\}$. Then the following is true:

1. $P \in E[n] \Leftrightarrow Q_n(x,y) = 0$,
2. *if $P \notin E[n]$, then*

$$[n]P = \left(\frac{R_n(x,y)}{Q_n^2(x,y)}, \frac{S_n(x,y)}{Q_n^3(x,y)}\right)$$

Proof: See [Lan78].

□

We will now give some properties of the polynomials that have just been defined:

Property 1 *Let $E : y^2 = 4x^3 - ax - b$ be an elliptic curve defined over $\mathbb{C}$. Let $n \in \mathbb{N}^*$. Let Q_n, R_n and S_n be the polynomials defined above.*

1. *$Q_n(X,Y)$, $Y^{-1}S_n(X,Y)$ for odd n, $Y^{-1}Q_n(X,Y)$, $S_n(X,Y)$ for even n and $R_n(X,Y)$ are polynomials in $\mathbb{C}[X,Y^2]$ and can thus be seen as polynomials in $\mathbb{C}[X]$,*
2. *$Q_n(X,Y)^2$ and $R_n(X)$ are relatively prime,*
3. $$R_n(X) = X^{n^2} + \text{ lower order terms}$$
$$Q_n^2(X) = n^2X^{n^2-1} + \text{ lower order terms}$$

Proof: See [Lan78], [Sil86].

□

Later, in the chapter on elliptic curves over finite fields, we will give a definition for division polynomials for an elliptic curve defined by a "usual" Weierstrass equation (that is, without the coefficient 4), and such that the leading coefficients shall always be positive, and all the coefficient "integers". Then since it is going to be defined over $\mathbb{Z}$ and everything is described algebraically, this will be valid over any field, and in particular for finite fields.

2.3 Modular curves and modular polynomials

We don't give any precise reference in what follows. The reader can refer to [Shi71], [Ogg73], [Lan78], [Kob93].
Previously in this chapter a relation between lattices in $\mathbb{C}$ and elliptic curves over $\mathbb{C}$ was described. Going further, to any lattice can be associated a point in $\mathbb{H} = \{z \in \mathbb{C},\ \Im(z) > 0\}$ by

$$\begin{array}{ccccc} \{\text{Lattices in } \mathbb{C}\} & \longrightarrow & \mathbb{H} & & \\ \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 & \longmapsto & \tau(\Lambda) = \frac{\omega_1}{\omega_2} & \text{if } \Im(\frac{\omega_1}{\omega_2}) > 0 \\ \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 & \longmapsto & \tau(\Lambda) = \frac{\omega_2}{\omega_1} & \text{otherwise} \end{array}$$

Two lattices Λ_1 and Λ_2 are homothetic if and only if $\tau(\Lambda_1) = M.\tau(\Lambda 2)$ with $M \in SL_2(\mathbb{Z})$, the action of $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ on a point $z \in \mathbb{H}$ being

$$M.z = \frac{az+b}{cz+d}.$$

Let $\Gamma = SL_2(\mathbb{Z})$, and call it the full modular group. Thus, we have the following bijection:

$$\begin{array}{ccc} {}_\Gamma\backslash\mathbb{H} & \longrightarrow & \{\text{Isomorphism classes of elliptic curves over } \mathbb{C}\} \\ \tau & \longmapsto & E : y^2 = x^3 - g_2(\tau\mathbb{Z}+\mathbb{Z})x - g_3(\tau\mathbb{Z}+\mathbb{Z}) \end{array}$$

It can be shown that ${}_\Gamma\backslash\mathbb{H} \approx \mathbb{C}$ and in fact, the bijection is given by the j-invariant. A natural question is the following: what happens if we divide $\mathbb{H}$ by a subgroup of the full modular group? The answer is not generally known, except for a few types of subgroups.

Let $N \in \mathbb{N}^*$. Define the following subgroups of Γ by

$$\Gamma_0(N) = \left\{ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma,\ c \equiv 0\ [N] \right\}$$

$$\Gamma_1(N) = \left\{ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N),\ a \equiv d \equiv 1\ [N] \right\}$$

$$\Gamma(N) = \left\{ M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N),\ b \equiv 0\ [N] \right\}$$

Define also the following curves:

$$Y_0(N) = {}_{\Gamma_0(N)} \backslash \mathbb{H}$$

$$Y_1(N) = {}_{\Gamma_1(N)} \backslash \mathbb{H}$$

$$Y(N) = {}_{\Gamma(N)} \backslash \mathbb{H}$$

It can be shown that these curves parametrize the following different objects:

$Y_0(N)$: equivalence classes of couples (E, C) where E is an elliptic curve over $\mathbb{C}$, and $C \subset E(\mathbb{C})$ is a cyclic subgroup of order N

$Y_1(N)$: equivalence classes of couples (E, P) where E is an elliptic curve over $\mathbb{C}$, and $P \in E[N]$ is a point of exact order N

$Y(N)$: let $\zeta \in \mathbb{C}$ be a primitive N-th root of unity, and let e_N be a Weil pairing (which will be defined later). Then it parametrizes equivalence classes of triplets (E, P_1, P_2) where E is an elliptic curve over $\mathbb{C}$, $P_1, P_2 \in E[N]$ such that $e_N(P_1, P_2) = \zeta$.

In order to work with compact Riemann surfaces, $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is used instead of $\mathbb{H}$. The action of $SL_2(\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Q})$ is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \begin{bmatrix} x & y \end{bmatrix} = \begin{bmatrix} ax + by & cx + dy \end{bmatrix}.$$

We then get the Riemann surfaces $X_0(N)$, $X_1(N)$ and $X(N)$. The genus of these curves is well known.
Moreover, we can also find a modular equation for $X_0(N)$, that is an algebraic relation

$$\Phi_N(X, Y) = 0.$$

This polynomial has the following properties:

- $\Phi_N(X, j) = \prod_{i=1}^{\Psi(N)} (X - j \circ \alpha_i) \in \mathbb{Z}[X, j]$ where j is the j-invariant, $\Psi(N) = \prod_{p|N} \left(1 + \frac{1}{p}\right)$ and the α_i's are representatives of the right cosets of $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}),\ ad - bc = N \text{ and } a \wedge b \wedge c \wedge d = 1 \right\}$ in Γ,
- $\Phi_N(X, j)$ is irreducible over $\mathbb{C}(j)$ and is of degree $\Psi(N)$,
- $\Phi_N(X, j) = \Phi_N(j, X)$
- If p is prime, $\Phi_p(X, j) \equiv (X - j^p)(X^p - j)\ [p]$,
- Let E_1, E_2 be two elliptic curves over $\mathbb{C}$ with j-invariant j_1 and j_2 respectively. Then there exists an isogeny $\lambda : E_1 \longrightarrow E_2$ with cyclic kernel of order N if and only if

$$\Phi_N(j_1, j_2) = 0.$$

These polynomials are called the modular polynomials.

Later, in the chapter on elliptic curves defined over finite fields, we will work with these curves generalized to finite fields, even if the construction given here is not valid any longer. The modular polynomials can be generalized too, with the same properties, and these will be used in the SEA algorithm.

Chapter 3

Elliptic curves over finite fields

In this chapter, we discuss elliptic curves over finite fields. We assume that the characteristic of the field is different from 2 or 3, which allows us to assume that any elliptic curve E is given by a reduced Weierstrass equation

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

We begin by describing an endomorphism particular to elliptic curves over fields of non-zero charactristic, the Frobenius endomorphism, and then the cardinality of the group of rational points. We finally return to division polynomials as well as modular curves. At the end, we will mention twists, which we will (ab)use afterwards.
We introduce some notation. Let p be a prime number, $p \geqslant 5$. Let $q = p^n$ be a power of p. We denote by $\mathbb{F}_q$ a field with q elements, and by $\overline{\mathbb{F}_q}$ an algebraic closure. Let

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. We define the quantities b_2, b_4, b_6, b_8, c_4, c_6, ω, j and Δ as done in [Sil86] or [BSS00].
Let

$$E(\overline{\mathbb{F}_q}) = \left\{(x,y) \in \overline{\mathbb{F}_q}^2,\ y^2 = x^3 + a_4x + a_6\right\} \cup \{\mathcal{O}\},$$

$$E(\mathbb{F}_q) = \left\{(x,y) \in \mathbb{F}_q^2,\ (x,y) \in E(\overline{\mathbb{F}_q})\right\} \cup \{\mathcal{O}\}.$$

If $n \in \mathbb{N}$,

$$E[n] = \{P \in E(\overline{\mathbb{F}_q}), nP = \mathcal{O}\}$$

and

$$E(\mathbb{F}_q)[n] = E[n] \cap E(\mathbb{F}_q).$$

The endomorphism

$$\begin{array}{rccc} \varphi : & E(\overline{\mathbb{F}_q}) & \longrightarrow & E(\overline{\mathbb{F}_q}) \\ & (x,y) & \longmapsto & (x^q, y^q) \\ & \mathcal{O} & \longmapsto & \mathcal{O} \end{array}$$

is called the Frobenius endomorphism.

3.1 Frobenius endomorphism - supersingularity

The Frobenius endomorphism is an automorphism of elliptic curves. Moreover, $\varphi(E(\mathbb{F}_q)) = E(\mathbb{F}_q)$ and the following property is true :

$$\forall P \in E(\overline{\mathbb{F}_q}),\ P \in E(\mathbb{F}_q) \Leftrightarrow \varphi(P) = P.$$

From this last fact, we can deduceUsing this fact, we can prove the following theorem, due to Hasse :

Theorem 5

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

Proof: See [Sil86].

□

The study of the multiplication-by-m morphism, φ and its dual also give the following proposition :

Proposition 1 *Let $m \in \mathbb{Z}^*$.*

1. *If $m \wedge p = 1$, then $E[m] \approx \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,*
2. *Either*

$$\forall r \in \mathbb{N}^*,\ E[p^r] = \{\mathcal{O}\}$$

or

$$\forall r \in \mathbb{N}^*,\ E[p^r] \approx \mathbb{Z}/p^r\mathbb{Z}.$$

Proof: See [Sil86].

□

As a corollary of this fact,

Corollary 1 *$E(\mathbb{F}_q)$ is an abelian group of rank 1 or 2 and*

$$E(\mathbb{F}_q) \approx \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$$

with $d_2 \mid d_1$ and furthermore $d_2 \mid q-1$.

Proof: See [Men93].

□

Following the previous proposition, we see that there exist two types of elliptic curves over $\mathbb{F}_q$, namely those which have p-torsion, and those which don't. In fact, we have :

Theorem 6 *Let E be an elliptic curve defined over $\mathbb{F}_q$. For $r \geqslant 1$, let $E^{(p^r)}$ be the elliptic curve obtained from E by raising its coefficients to the p^r-th power. Let $\phi_r : E \longrightarrow E^{(p^r)}$ be the p^r-power Frobenius. Then the following assertions are equivalent :*

1. *$\exists r \geqslant 1,\ E[p^r] = \{\mathcal{O}\}$,*
2. *$\forall r \geqslant 1,\ E[p^r] = \{\mathcal{O}\}$,*

3. *The morphism $[p]$ is purely inseparable and $j \in \mathbb{F}_{p^2}$,*
4. *$End_{\overline{\mathbb{F}_q}}(E)$ is an order in a quaternion algebra,*
5. *The formal group $\hat{E}/_{\mathbb{F}_q}$ associated to E has height 2,*
6. *$\exists n, m \geqslant 1,\ \varphi^n = [p]^m$,*
7. *$\omega \neq 0$ is of the first type with $\omega = \sum_{0 \leqslant i} a_i t^i dt$ and $a_{p-1} = 0$,*
8. *If $P(X) = X^2 - tX + q$ is the characteristic polynomial of φ with $t, q \in \mathbb{Z}$, then $t \equiv 0\ [p]$.*

Proof: See [Sil86] and [Hus87].

□

It is then usual to define the following :

Definition 6 *Let E be an elliptic curve defined over a finite field. If E satisfies one of the equivalent conditions of theorem 6, then E is said to be supersingular. It is ordinary otherwise.*

Since the study of the p-th division polynomial will be based on the study of the behavior of the Frobenius on p-torsion points, it will be necessary to distinguish the supersingular case from the ordinary case. However, since the action of the Frobenius on m-torsion points when $m \wedge p = 1$ is not affected by the supersingularity, no distinction will be necessary, and just one case will be treated.

Note also that all supersingular curves can be defined over $\mathbb{F}_{p^2}$, so that the proportion of supersingular curves defined over $\mathbb{F}_{p^n}$ becomes negligable when $n \to \infty$. Note finally that because of Hasse's theorem, when $p \geqslant 5$, an elliptic curve over $\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) = p+1$.

Corollary 2 *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and let $P(X) = X^2 - tX + q$ be the characteristic polynomial of the Frobenius endomorphism. Then $\#E(\mathbb{F}_q) = q+1-t$. Moreover, if α and β are the two complex roots of $P(X)$, then*

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

Proof: See [Hus87]

□

3.2 The Weil pairing

In order to show the key lemma of the chapter on the possible factorisations of division polynomials, we will use a bilinear map, the Weil pairing. We will just give the property of such a pairing. The reader might look in [Men93], [BSS00] or [Sil86] for practical definitions of the pairing.

Theorem 7 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $m \in \mathbb{N}^*$ be such that $m \wedge p = 1$. Let μ_m be the set of m-th roots of unity in $\overline{\mathbb{F}_q}$. Then there exists a pairing*

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

which is

bilinear

$$\forall (S_1, S_2, T) \in E[m]^3,\ e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$

and

$$\forall (S, T_1, T_2) \in E[m]^3,\ e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2),$$

alternate

$$\forall S \in E[m],\ e_m(S, S) = 1$$

which implies that

$$\forall (S,T) \in E[m]^2,\ e_m(T, S) = e_m(S, T)^{-1},$$

non-degenerate

$$\forall S \in E[m], (\forall T \in E[m], e_m(S, T) = 1) \Rightarrow S = \mathcal{O},$$

Galois-invariant

$$\forall \sigma \in Gal(\overline{\mathbb{F}_q}, \mathbb{F}_q),\ \forall (S, T) \in E[m]^2,\ e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma),$$

compatible *If $m' \wedge p = 1$, $S \in E[mm']$ and $T \in E[m]$, then*

$$e_{mm'}(S, T) = e_m([m']S, T).$$

Proof: See [Sil86].

□

Definition 7 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then a pairing such as described in theorem 7 is called a Weil pairing.*

Note that a Weil pairing is not unique. The Weil pairing is used in an article of Howe [How93] to define a link between a certain modular curve and classes of elliptic curves. The Weil pairing can also be used to prove the following property :

Property 2 *Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $m \in \mathbb{N}^*$ be such that $m \wedge p = 1$. Then*

$$E[m] \subset E(\mathbb{F}_q) \Rightarrow m^2 \mid \#E(\mathbb{F}_q) \text{ and } m \mid q - 1.$$

Proof: See [Sil86] or [Sch87].

□

The converse is generally false. Nevertheless, Balasubramanian and Koblitz proved the following partial converse :

Property 3 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $m \in \mathbb{N}^*$ be such that $m \wedge p = 1$. Assume that $q \not\equiv 1\ [m]$. Assume also that $m \mid \#E(\mathbb{F}_q)$. Then*

$$E[m] \subset E(\mathbb{F}_{q^n}) \Leftrightarrow m \mid q^n - 1.$$

Proof: See [BK98].

□

3.3 Division polynomials

As we wrote for elliptic curves over $\mathbb{C}$, we can also define division polynomials for elliptic curves over $\mathbb{F}_q$. If

$$E : f(x, y) = y^2 - x^3 - a_4x - a_6 = 0$$

is an elliptic curve defined over $\mathbb{F}_q$, then define the following functions ψ_i, ϕ_i, $\omega_i \in \mathbb{F}_q[x,y]$ by :

$$\psi_1(x,y) = 1,$$

$$\psi_2(x,y) = 2y,$$

$$\psi_3(x,y) = 3x^4 + 6a_4x^2 + 12a_6x - a_4^2,$$

$$\psi_4(x,y) = 4y\left(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - 8a_6^2 - a_4^3\right),$$

$$\psi_{2m+1}(x,y) = \psi_{m+2}(x,y)\psi_m^3(x,y) - \psi_{m-1}(x,y)\psi_{m+1}^3(x,y),$$

$$2y\psi_{2m}(x,y) = \psi_m(x,y)\left(\psi_{m+2}(x,y)\psi_{m-1}^2(x,y) - \psi_{m-2}(x,y)\psi_{m+1}^2(x,y)\right),$$

$$\phi_m(x,y) = x\psi_m^2(x,y) - \psi_{m-1}(x,y)\psi_{m+1}(x,y),$$

$$4y\omega_m(x,y) = \psi_{m+2}(x,y)\psi_{m-1}^2(x,y) - \psi_{m-2}(x,y)\psi_{m+1}^2(x,y).$$

Proposition 2 *The ϕ_i, ψ_i and ω_i are polynomials. Moreover, if we consider them modulo $f(x,y)$, then ϕ_i, ψ_i, $y^{-1}\omega_i$ for odd i and ϕ_i, $(2y)^{-1}\psi_i$ ω_i for even i are in $\mathbb{F}_q[x]$. We have*

$$\phi_i(x) = x^{i^2} + \textit{ lower order terms},$$

$$\psi_i(x) = ix^{\frac{i^2-1}{2}} + \textit{ lower order terms if } i \textit{ is odd},$$

$$\omega_i(x,y) = yx^{\frac{3i^2}{2}} + \textit{ lower order terms if } i \textit{ is odd},$$

$$\psi_i(x,y) = iyx^{\frac{i^2-4}{2}} + \textit{ lower order terms if } i \textit{ is even}$$

and

$$\omega_i(x) = x^{\frac{3i^2}{2}} + \textit{ lower order terms if } i \textit{ is even}.$$

Finally, the polynomials ϕ_i and ψ_i^2 are relatively prime and

$$\forall P = (x_0,y_0) \in E(\overline{\mathbb{F}_q}) \backslash E[i],\ [i]P = \left(\frac{\phi_i(x_0)}{\psi_i^2(x_0,y_0)}, \frac{\omega_i(x_0,y_0)}{\psi_i^3(x_0,y_0)}\right)$$

as well as

$$\forall P = (x_0,y_0) \in E(\overline{\mathbb{F}_q}),\ [i]P = \mathcal{O} \Leftrightarrow \psi_i(x_0,y_0) = 0.$$

Definition 8 *Let E be an elliptic curve over $\mathbb{F}_q$ and $n \in \mathbb{N}^*$. The n-th division polynomial is the polynomial ψ_n.*

Property 4 *Let E be an elliptic curve defined over $\mathbb{F}_q$ by an equation*

$$E : f(x,y) = y^2 - (x^3 + a_4x + a_6) = 0.$$

Let l be an odd prime. Then

$$E[l] \approx \mathbb{F}_q[X,Y]/_{(f(X,Y),\psi_l(X))}.$$

Proof: See [CM94].

□

3.4 Modular curves

To define modular curves over $\mathbb{C}$, we use subgroups of $SL_2(\mathbb{Z})$ to divide $\mathbb{H}$. In the case of finite fields, this is no longer possible. However, using different techniques as in [DR73] or [KM85], we can define some curves having the same properties as the ones given in the complex case. We will here give some results taken from [Len87] and [How93] :

Let l be a prime different from p. Consider all couples (E,P) where E is an elliptic curve defined over $\mathbb{F}_p$ and $P \in E(\mathbb{F}_p)[l]$. Two such couples (E,P) and (E',P') are equivalent over $\mathbb{F}_p$ (resp. over $\overline{\mathbb{F}_p}$) if there exists an isomorphism $u : E \longrightarrow E'$ over $\mathbb{F}_p$ (resp. over $\overline{\mathbb{F}_p}$) such that $u(P) = P'$. Denote the set of equivalence over $\mathbb{F}_p$ (resp. over $\overline{\mathbb{F}_p}$) by $Z_1(l)(\mathbb{F}_p)$ (resp. $Y_1(l)(\mathbb{F}_p)$). The cardinality of the set $Y_1(l)(\mathbb{F}_p)$ can be estimated by using the properties of the modular curve $X_1(l)$, which can be defined over $\mathbb{F}_p$ as well.

Property 5

1. *$X_1(l)$ is a complete non-singular irreducible curve defined over $\mathbb{F}_p$,*
2. *The genus of $X_1(l)$ equals 0 for $l = 2$ or 3, and $1 + \frac{1}{24}(l-1)(l-11)$ for $l \geqslant 5$,*
3. *The set $Y_1(l)(\mathbb{F}_p)$ can in a natural way be considered as a subset of the set $X_1(l)(\mathbb{F}_p)$ of the points of $X_1(l)$ defined over $\mathbb{F}_p$,*

4. *The cardinality of the complement of* $Y_1(l)(\mathbb{F}_p)$ *in* $X_1(l)(\mathbb{F}_p)$ *is bounded from above by the number of cusps of* $X_1(l)$*, which equals* 2 *for* $l = 2$ *and* $l-1$ *for* $l > 2$.

Proof: See [Len87].

□

This will give us the number of curves up to isomorphism that have a l-torsion point. But some curves are counted too many times, namely the curves that have a non-cyclic l-torsion subgroup. Therefore we introduce the following modular curve in the same way as before, but using the Weil-pairing this time : assume that $p \equiv 1\ [l]$, and fix a primitive l-th root of unity $\zeta \in \mathbb{F}_p$ as well as a Weil pairing e_l. Consider triples (E, P, Q) consisting of one elliptic curve E over $\mathbb{F}_p$ as well as two points $P, Q \in E(\mathbb{F}_p)[l]$ satisfying $e_l(P, Q) = \zeta$. Two such triples (E, P, Q) and (E', P', Q') are equivalent over $\mathbb{F}_p$ (resp. over $\overline{\mathbb{F}_p}$) if there exists an isomorphism $u : E \longrightarrow E'$ over $\mathbb{F}_p$ (resp. over $\overline{\mathbb{F}_p}$) such that $u(P) = P'$ an $u(Q) = Q'$. The set of equivalence classes over $\mathbb{F}_p$ (resp. over $\overline{\mathbb{F}_p}$) is denoted by $Z(l)(\mathbb{F}_p)$ (resp. $Y(l)(\mathbb{F}_p)$). The cardinality of the set $Y(l)(\mathbb{F}_p)$ can be estimated by using the properties of the modular curve $X(l)$, which can be defined over $\mathbb{F}_p$ as well :

Property 6

1. $X(l)$ *is a complete non-singular irreducible curve defined over* $\mathbb{F}_p$,
2. *The genus of* $X(l)$ *equals* 0 *for* $l = 2$*, and* $1 + \frac{1}{24}(l^2-1)(l-6)$ *for* $l \geqslant 3$,
3. *The set* $Y(l)(\mathbb{F}_p)$ *can in a natural way be considered as a subset of the set* $X(l)(\mathbb{F}_p)$ *of points of* $X(l)$ *defined over* $\mathbb{F}_p$,
4. *The cardinality of the complement of* $Y(l)(\mathbb{F}_p)$ *in* $X(l)(\mathbb{F}_p)$ *is bounded from above by the number of cusps of* $X(l)$*, which equals* 3 *for* $l = 2$ *and* $\frac{l^2-1}{2}$ *for* $l > 2$.

Proof: See [Len87].

□

Finally, Lenstra proves :

Lemma 1 *If* $l > 2$ *is a prime different from* p*, then*

$$\#Z_1(l)(\mathbb{F}_p) = \#Y_1(l)(\mathbb{F}_p) + O(1),$$

and if $p \equiv 1\ [l]$,

$$\#Z(l)(\mathbb{F}_p) = \#Y(l)(\mathbb{F}_p) + O(1).$$

Proof: See [Len87].

□

3.5 Twists

The idea of the twist is the following. Let $E : y^2 = x^3 + a_4x + a_6 = f(x)$ be an elliptic curve defined over $\mathbb{F}_q$. Then, any point $x \in \mathbb{F}_q$ gives rise to 2 points if $f(x)$ is a non-zero square in $\mathbb{F}_q$, one point if $f(x) = 0$ and none if $f(x)$ is not a square in $\mathbb{F}_q$. The idea is to define a sort of complementary curve. Let γ be a non-square in $\mathbb{F}_q$. Then $\gamma f(x)$ is a non-zero square if and only $f(x)$ is a non-zero non-square. Therefore, the curve $E' : y^2 = \gamma f(x)$ is such that $\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2(q+1)$. More precisely,

Definition 9 *Let* $E : y^2 = x^3 + a_4x + a_6$ *be an elliptic curve defined over* $\mathbb{F}_q$*. Let* $D \in \mathbb{F}_q \backslash \mathbb{F}_q^2$*. Then the* D*-twist of* E *is the elliptic curve*

$$\widetilde{E}^D : y^2 = x^3 + D^2a_4x + D^3a_6.$$

Note that the D-twist of an elliptic curve is indeed an elliptic curve, which is also defined over $\mathbb{F}_q$.

Property 7 *Let* E *be an elliptic curve defined over* $\mathbb{F}_q$*. Let* D *be a non-square in* $\mathbb{F}_q$*. Then* E *and its* D*-twist have the same* j*-invariant, and therefore are isomorphic over* $\overline{\mathbb{F}_q}$*. If* $\delta \in \mathbb{F}_{q^2}$ *is such that* $\delta^2 = D$*, then an isomorphism is given by*

$$\begin{array}{rccc} \varphi_\delta : & E(\overline{\mathbb{F}_q}) & \longrightarrow & \widetilde{E}^D(\overline{\mathbb{F}_q}) \\ & (x, y) & \longmapsto & (\delta^2 x, \delta^3 y) \\ & \mathcal{O} & \longmapsto & \mathcal{O} \end{array}.$$

Property 8 *Let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$*, and let* $\widetilde{E}^D$ *be its* D *twist for* $D \in \mathbb{F}_q \backslash \mathbb{F}_q^2$*. Let* n *be odd. Then we have*

$$\#E(\mathbb{F}_{q^n}) + \#\widetilde{E}^D(\mathbb{F}_{q^n}) = 2(q^n + 1).$$

Moreover,

$$\#E(\mathbb{F}_q) \cdot \#\widetilde{E}^D(\mathbb{F}_q) = \#E(\mathbb{F}_{q^2}).$$

Proof: Straightforward.

□

We will now give and prove a relation between the division polynomials of an elliptic curve and a twist.

Lemma 2 *Let $E : y^2 = x^3 + a_4x + a_6 = f(x)$ be an elliptic curve over $\mathbb{F}_q$ and $D \in \mathbb{F}_q$ be a quadratic non-residue. Let $\widetilde{E}^D : y^2 = x^3 + D^2a_4x + D^3a_6$ be a quadratic twist of E. If ψ_n and $\widetilde{\psi}_n^D$ are the division polynomials of E and $\widetilde{E}^D$ respectively, then*

$$\widetilde{\psi}_n^D(X) = D^{\frac{n^2-1}{2}}\psi_n\left(\frac{X}{D}\right) \text{ for } n \text{ odd}$$

and

$$\widetilde{\psi}_n^D(X,Y) = D^{\frac{n^2-4}{2}}\psi_n\left(\frac{X}{D},Y\right) \text{ for } n \text{ even.}$$

Proof: This is an easy consequence of proposition 2 page 29.

□

This lemma will allow us later to say that the division polynomials of an elliptic curve and any of its twists have the same factorisation pattern.

Chapter 4

Cryptographical and algorithmic aspects

In this chapter, we will deal with two topics that motivated this dissertation. This dissertation is in a subtile form dedicated to cryptography. From the point of view of division polynomials, we wanted to study the group structure of elliptic curves defined over finite fields. This has two ramifications. First, division polynomials were used in Schoof's algorithm to find the number of rational points on such elliptic curves; this is what we are going to discuss first. Second, we can use cyclic elliptic curves to define one-way functions, as Kaliski did.

4.1 Schoof's algorithm

In 1985, in [Sch85], Schoof published the first efficient algorithm to calculate the number of points on an elliptic curve defined over a finite field. This algorithm, which runs in $O(\log^8 q)$ (while the best known algorithm at that time ran in $O(q^{1/4+\epsilon})$), was afterwards improved by numerous researchers. These algorithms are nevertheless based on the following same principles :

1. The number of rational points on an elliptic curve defined over a finite field $\mathbb{F}_q$ is directly related to the trace t of the Frobenius endomorphism,
2. By Hasse's theorem, $|t| \leqslant 2\sqrt{q}$,
3. We can find, for every prime l, t modulo l, by looking at the action of the Frobenius on l-torsion points,
4. We can get t back using the Chinese remainder theorem if we have found t modulo l for enough primes l, and the number of necessary primes l is small compared to q.

Lemma 3 *Define l_{max} as the minimum integer such that*

$$\prod_{\substack{l \text{ prime} \\ 2 \leqslant l \leqslant l_{max} \\ l \neq p}} l > 4\sqrt{q}.$$

Let E be an elliptic curve defined over $\mathbb{F}_q$. Then the trace t of the Frobenius is entirely determined by the set $\{t\ [l],\ l \in \{2, \ldots, l_{max}\},\ l \text{ prime}\}$.

Proof: See [Sch95], [BSS00].

□

Lemma 4 *Let E be an elliptic curve defined over $\mathbb{F}_q$ by*

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

Then

$$t \equiv 1 \ [2] \Leftrightarrow (X^3 + a_4X + a_6) \wedge (X^q - X) = 1.$$

Proof: See [Sch95], [BSS00].

□

Lemma 5 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $P \in E[l]\backslash\{\mathcal{O}\}$. Let $q_l \in \{0, \ldots, l-1\}$ be such that $q_l \equiv q \ [l]$. Then there exists a unique $\tau \in \{0, \ldots, l-1\}$ such that*

$$\varphi^2(P) + [q_l]P = [\tau]\varphi(P).$$

Moreover,

$$t_l = \tau \ [l].$$

Proof: See [Sch95], [BSS00].

□

The idea that makes all the computations fast is that instead of working with points that have to be found, we work with polynomials in $\mathbb{F}_q[X, Y]$ modulo the curve equation as well as the division polynomials. Here is the algorithm, some details being intentionally repressed for simplicity :

Algorithm 1: Schoof's algorithm

Input: An elliptic curve $E : f(x, y) = y^2 - x^3 - a_4x - a_6 = 0$ defined over $\mathbb{F}_q$
Output: The cardinality of $E(\mathbb{F}_q)$

(1) $M := 2$
(2) $g := (X^3 + a_4X + a_6) \wedge (X^q - X)$
(3) **if** $g == 1$ **then** $S := \{(1, 2)\}$
(4) **else** $S := \{(0, 2)\}$
(5) $l := 3$
(6) **while** $M < 4\sqrt{q}$
(7) Compute symbolically the x-coordinate $L_X(x, y)$ of $(x^{q^2}, y^{q^2}) + [q_l](x, y)$ modulo ψ_l and $f(x, y)$ to

(8) eliminate powers of y higher than 1 and get a polynomial of minimal degree in x.
$\tau := 0$
(9) Compute symbolically the x-coordinate $R_X(x, y)$ of $[\tau](x^q, y^q)$ modulo ψ_l and $f(x, y)$ to eliminate powers of y higher than 1 and get a polynomial of minimal degree in x.
(10) Equate $L_X(x, y)$ and $R_X(x, y)$, clear denominators, and, still working modulo ψ_l and $f(x, y)$, get an equation of the form $a_X(x) - b_X(x)y = 0$, with $deg(a_X), deg(b_X) < deg(\psi_l)$.
(11) $h_X(x) := a_X(x)^2 - b_X(x)^2 (x^3 + a_4x + a_6)$
(12) $g_X := h_X(x) \wedge \psi_l(x)$
(13) **if** $g_X == 1$
(14) **then**
(15) $\tau := \tau + 1$
(16) **goto** 9
(17) **else**
(18) Compute symbolically the y-coordinate $L_Y(x, y)$ of $(x^{q^2}, y^{q^2}) + [q_l](x, y)$ modulo ψ_l and $f(x, y)$ to eliminate powers of y higher than 1 and get a polynomial of minimal degree in x.
(19) Compute symbolically the y-coordinate $R_Y(x, y)$ of $[\tau](x^q, y^q)$ modulo ψ_l and $f(x, y)$ to eliminate powers of y higher than 1 and get a polynomial of minimal degree in x.
(20) Equate $L_Y(x, y)$ and $R_Y(x, y)$, clear denominators, and, still working modulo ψ_l and $f(x, y)$, get an equation of the form $a_Y(x) - b_Y(x)y = 0$, with $deg(a_Y) < deg(\psi_l)$ and $deg(b_Y) < deg(\psi_l)$.
(21) $h_Y(x) := a_Y(x)^2 - b_Y(x)^2 (x^3 + a_4x + a_6)$
(22) $g_Y := h_Y(x) \wedge \psi_l(x)$
(23) **if** $g_Y == 1$ **then** $S := S \cup \{(l - \tau, l)\}$
(24) **else** $S := S \cup \{\tau, l)\}$
(25) $M := M \times l$
(26) $l := NextPrime(l)$
(27) Using the Chinese remainder theorem, recover the trace $t \in \{-2\sqrt{q}, \ldots, 2\sqrt{q}\}$
(28) **return** $q + 1 - t$

Theorem 8 *This algorithm works and runs in* $O(\log^8 q)$.

Proof: See [Sch95].

□

4.2 The SEA algorithm

Since the publication of Schoof's algorithm in 1985, a lot of research has been done to improve the efficiency of the algorithm. The biggest improvements have been made by Elkies and Atkin. The ideas are the following :

It is sometimes possible to work modulo a factor of Ψ_l of lower degree, and in particular modulo a factor of degree $\frac{l-1}{2}$ (Elkies),

If this is not possible, we can nevertheless find a small set of possible traces modulo l (Atkin).

Definition 10 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let t be the trace of the Frobenius endomorphism. Let $l \geqslant 3$, $l \neq p$ be a prime number. Then l is an Elkies prime for E if $t^2 - 4q$ is a square in $\mathbb{F}_l$, and is an Atkin prime otherwise.*

Proposition 3 *Let E be a non-supersingular elliptic curve defined over $\mathbb{F}_q$ with j-invariant different from 0, 1728. Let $\phi_l(x, j(E)) = h_1(x)\dots h_s(x)$ be the factorisation of $\phi_l(x, j(E))$ in $\mathbb{F}_q[x]$ into a product of irreducible polynomials. Then there are the following possibilities for the degrees of $h_1, \dots, h_s$:*

i) $1, 1, \dots, 1$,

ii) 1 *and* l,

iii) $1, 1, r, \dots, r$, $r > 1$ *and* $r \mid l - 1$,

iv) $r, \dots, r$, $r > 1$ *and* $r \mid l + 1$.

Proof: See [Sch95], [BSS00].

□

Property 9 *Let E be an elliptic curve over $\mathbb{F}_q$. l is an Elkies prime for E in the cases i), ii) and iii) of the previous proposition, and an Atkin prime for E in the last case.*

Proof: See [BSS00].

□

In the case of an Elkies prime l for an elliptic curve E, $\Phi_l(x, j(E))$ is used to find an isogenous curve E_1 together with an isogeny $\mu : E \longrightarrow E_1$ of degree l. We then define

$$F_l(X) = \prod_{\pm P \in Ker\mu \setminus \{\mathcal{O}\}} (X - x(P)),$$

and this polynomial is a factor of degree $\frac{l-1}{2}$ of $\Psi_l(X)$. It is used in the computations to find $\lambda \in \{0, \dots, l-1\}$ such that

$$(x^q, y^q) = [\lambda](x, y)$$

for a point $P = (x, y)$ of l-torsion. All the computations are made in the same way as in Schoof's algorithm, except that everything is done modulo F_l instead of Ψ_l, which reduces dramatically the complexity.
In the case of an Atkin prime l for E, $\phi_l(x, j(E))$ has only irreducible factors over $\mathbb{F}_q$ of degree $r > 1$ and $r \mid l + 1$. Then Atkin shows that we can reduce the set of possible traces modulo l to a set of cardinality $\Phi_{Euler}(r)$, where Φ_{Euler} is the Euler phi function. This is worse than Elkies, but better than Schoof.
The ideal is to reconcile the two methods in order to get the least possible number of Atkin primes, but enough of them so that the biggest prime used in the algorithm isn't too large. But we won't get into this.
Here is a sketch of the SEA (Schoof- Elkies- Atkin) algorithm, which doesn't take into account the possibility of improving the speed by optimizing the number of Atkin primes, and which eludes all the particular cases :

Algorithm 2: SEA algorithm

Input: An elliptic curve $E : y^2 = x^3 + a_4x + a_6$ over $\mathbb{F}_q$
Output: The cardinality of $E(\mathbb{F}_q)$
(1) $M := 2$
(2) $l := 2$
(3) $A := \emptyset$
(4) $g := (X^3 + a_4X + a_6) \wedge (X^q - X)$
(5) **if** $g == 1$ **then** $E := \{(1, 2)\}$
(6) **else** $E := \{(0, 2)\}$
(7) $l := 3$

(8) **while** $M < 4\sqrt{q}$
(9) Compute $\phi_l(X, j(E))$ and its factorisation over $\mathbb{F}_q$
(10) **if** l is an Elkies prime
(11) **then**
(12) Compute a $F_l(X)$
(13) Find $\lambda \in \mathbb{F}_l$ eigenvalue of φ
(14) $E := E \cup \left\{ \left(\lambda + \frac{q}{\lambda}, l \right) \right\}$
(15) **else**
(16) Determine a set T such that $t\ [l] \in T$
(17) $A := A \cup \{(T, l)\}$
(18) $M := M \times l$
(19) $l := NextPrime(l)$
(20) Retrieve $t \in \{-2\sqrt{q}, \ldots, 2\sqrt{q}\}$ by using the sets A, E, the Chinese reminder theorem and Baby Step - Giant Step
(21) **return** $q + 1 - t$

Theorem 9 *This algorithm works and runs in* $O(\log^6 q)$.

Proof: See [BSS00]. A more thorough discussion of the algorithm can be found there. See also [CM94].

□

Other improvements have been made by Morain, Couveignes, Lercier and Muller... but these will not be discussed here.

4.3 One-way permutations

In cryptography, it is really important to have one-way functions, that is functions that are easy to compute, but very difficult to invert. No proof has been made for their existence or non-existence, but it is generally believed that such functions exist. An example of a candidate is exponentiation in finite fields. These functions are used to build secure pseudorandom number generators, hash functions, key generation for public key cryptosystems.
In 1991, Kaliski [Kal91] proposed a candidate for a one-way permutation involving elliptic curves over prime finite fields.
We identify $\mathbb{F}_p$ with $\{0, \ldots, p-1\}$ in a natural way, and we will use the

following notation for $x \in \mathbb{F}_p$:

$$x > 0 \Leftrightarrow 0 < x \leqslant \frac{p-1}{2},$$

and

$$x < 0 \Leftrightarrow \frac{p+1}{2} \leqslant x \leqslant p-1.$$

We also define $i : \mathbb{F}_p \longrightarrow \{0, \ldots, p-1\} \subset \mathbb{N}$.

Theorem 10 *Let* $E : y^2 = x^3 + a_4 x + a_6$ *be an elliptic curve defined over* $\mathbb{F}_p$ *and let* D *be a quadratic non-residue in* $\mathbb{F}_p$. *Define*

$$l : \begin{array}{ccccc} E(\mathbb{F}_p) & \longrightarrow & \{0, \ldots, 2p+1\} & & \\ (x,y) & \longmapsto & i(Dx) & \text{if } y \geqslant 0 & \\ (x,y) & \longmapsto & i(Dx)+p+1 & \text{if } y < 0 & \\ \mathcal{O} & \longmapsto & p & & \end{array}.$$

Define also

$$l' : \begin{array}{ccccc} \widetilde{E}^D(\mathbb{F}_p) & \longrightarrow & \{0, \ldots, 2p+1\} & & \\ (x,y) & \longmapsto & i(x) & \text{if } y > 0 & \\ (x,y) & \longmapsto & i(x)+p+1 & \text{if } y \leqslant 0 & \\ \mathcal{O} & \longmapsto & 2p+1 & & \end{array}.$$

Then l *and* l' *are both one-to-one maps, and* $Im(l) \cap Im(l') = \emptyset$. *Assume moreover that* $E(\mathbb{F}_p)$ *and* $\widetilde{E}^D(\mathbb{F}_p)$ *are both cyclic groups. Let* $G \in E(\mathbb{F}_p)$ *and* $G' \in \widetilde{E}^D(\mathbb{F}_p)$ *be two generators. Let* $n = \#E(\mathbb{F}_p)$. *Define*

$$f_E : \begin{array}{ccccc} \{0, \ldots, 2p+1\} & \longrightarrow & \{0, \ldots, 2p+1\} & & \\ m & \longmapsto & l([m]G) & \text{if } 0 \leqslant m < n & \\ m & \longmapsto & l'([m]G') & \text{if } n \leqslant m \leqslant 2p+1 & \end{array}.$$

Then f_E *is a permutation of the set* $\{0, \ldots, 2p+1\}$.

Proof: See [Kal91].

□

Conjecture 1 *The map* f_E *defined in the previous theorem is a one-way permutation.*

In [Kal91], it is proved that f_E is one-way if the elliptic curve discrete logarithm problem is hard.

In the theorem, it is assumed that both $E(\mathbb{F}_p)$ and $\widetilde{E}^D(\mathbb{F}_p)$ are cyclic groups. But the cyclicity of these groups is strongly related to their division polynomials, which are equal for both curves since they are twists of each other. This is what we are going to study now.

Chapter 5

2 and 3 torsion points

To begin with, we are going to look at the structure of the group of rational points of an elliptic curve, and more specifically at points of 2 and 3-torsion. To achieve our goal, we need to study two polynomials of degree 3, namely the polynomial defining the elliptic curve for the study of 2-torsion points, and a factor of degree 3 of the third division polynomial for the study of 3-torsion points. In the first case, we just need to know the parity of the number of irreducible factors of the polynomial under consideration, and an extension of a theorem of Pellet (theorem 11) will relate this parity to the discriminant of the polynomial. In the second case, this is not enough since the polynomial has either 1 or 3 irreducible factors; therefore we study exclusively polynomials of degree 3 over finite fields. Since it is no more difficult, we give the proofs of some of the results for a wider class of fields. After this brief study, we study the cyclicity of the group of rational points using a theorem of Schoof (theorem 13), and end up with the study of 2 and 3-torsion points.

5.1 Study of polynomials of degree 3

We will begin by giving a theorem which relates the number of irreducible factors of a separable polynomial to its discriminant. The theorem was first proved by Pellet [Pel78] for prime finite fields of characteristic different from 2, but we give here a proof for a wider class of fields.

Definition 11 *Let $\mathbb{K}$ be a field. $\mathbb{K}$ is said to be of cyclic type if the following two properties are satisfied:*

The mapping $\chi : \mathbb{K}^* \longrightarrow \pm 1$, given by $\chi(x) = 1$ if and only if $x \in \mathbb{K}^2$, is a character, i.e. a homomorphism of groups.

For any irreducible separable polynomial $f \in \mathbb{K}[X]$, the extension $(\mathbb{K}[X]/f(X))/\mathbb{K}$ is cyclic, i.e. Galois with cyclic Galois group G_f.

χ is called the quadratic character associated to $\mathbb{K}$.

Typical examples of such fields are finite fields, $\mathbb{R}$, $\mathbb{C}$, but not $\mathbb{Q}$.
We now extend Pellet's theorem as follows:

Theorem 11 *Let $\mathbb{K}$ be a field of cyclic type of characteristic different from 2, and χ its associated quadratic character. Let $P \in \mathbb{K}[X]$ be a separable polynomial of degree n with discriminant $\mathcal{D}$. Let ω be the number of irreducible factors of P in $\mathbb{K}[X]$. Then*

$$\chi(\mathcal{D}) = (-1)^{n-\omega}.$$

Proof: First of all, let $Q = \lambda P$ with $\lambda \in \mathbb{K}^*$, then the discriminant $\mathcal{D}_Q$ of Q is $\mathcal{D}_Q = \lambda^{2n-2}\mathcal{D}$ and then

$$\chi(\mathcal{D}_Q) = \chi(\lambda)^{2(n-1)}\chi(\mathcal{D}) = \chi(\mathcal{D})$$

so that we may assume that P is monic.
Assume first that P is irreducible. In the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, write

$$P(X) = \prod_{i=1}^{n}(X - x_i)$$

with $x_i \in \overline{\mathbb{K}}$. Let $\sigma \in G_P$ be a generator of the Galois group G_P. Then σ induces a permutation on the set $\{x_1, ..., x_n\}$. Decompose $\tau = \sigma|_{\{x_1,...,x_n\}}$ as a product of cycles with disjoint support

$$\tau = \sigma_1 \circ ... \circ \sigma_t.$$

We know that given two roots x_i and x_j, there exists an automorphism ρ of $\mathbb{K}[X]/P(X)$ such that $\rho(x_i) = x_j$. In particular, $\rho \in G_P$ and there exists r such that $\rho = \tau^r$. $t \geqslant 2$ would be absurd since the supports of the σ_i are disjoint. Thus τ is a cycle of length n since $degP = \#G_P = \# < \tau >$. Then, reindexing the roots, we may suppose that $\tau = (x_1, ..., x_n)$.
We know that

$$\mathcal{D} = \prod_{1 \leqslant i < j \leqslant n}(x_i - x_j)^2$$

and $\mathcal{D} \neq 0$ since P is separable. Let

$$g = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j).$$

We have $g^2 = \mathcal{D} \in \mathbb{K}$, so that $\chi(\mathcal{D}) = 1$ if and only if $g \in \mathbb{K}$. But $g \in \mathbb{K}$ if and only if $\forall \rho \in G_P,\ \rho(g) = g$, i.e. since G_P is generated by σ, if and only if $\sigma(g) = g$. But,

$$\begin{aligned}
\sigma(g) &= \prod_{1 \leqslant i < j \leqslant n} (\sigma(x_i) - \sigma(x_j)) \\
&= \prod_{1 \leqslant i < j \leqslant n-1} (\sigma(x_i) - \sigma(x_j)) \prod_{1 \leqslant i < j = n} (\sigma(x_i) - \sigma(x_j)) \\
&= \prod_{1 \leqslant i < j \leqslant n-1} (x_{i+1} - x_{j+1}) \prod_{1 \leqslant i < n} (x_{i+1} - x_1) \\
&= \prod_{2 \leqslant i < j \leqslant n} (x_i - x_j) \prod_{1 = i < j \leqslant n} (x_j - x_i) \\
&= \prod_{2 \leqslant i < j \leqslant n} (x_i - x_j) \prod_{1 = i < j \leqslant n} -(x_i - x_j) \\
&= (-1)^{n-1} \prod_{1 \leqslant i < j \leqslant n} (\sigma(x_i) - \sigma(x_j)) \\
&= (-1)^{n-1} g
\end{aligned}$$

Then, since the characteristic of $\mathbb{K}$ is different from 2,

$$g \in \mathbb{K} \Leftrightarrow \sigma(g) = g \Leftrightarrow n \equiv 1\ [2]$$

and therefore we get

$$\chi(\mathcal{D}) = (-1)^{n-1}$$

and the theorem is proved when P is irreducible.
We shall now treat the general case by induction on the number of factors ω of P. We have seen that it is true for $\omega = 1$. Suppose that we have proved the theorem for all polynomials with the number of irreducible factors strictly less than ω. Write

$$P = \prod_{i=1}^{\omega} f_i$$

with f_i monic and irreducible in $\mathbb{K}[X]$. Let $Q = \prod_{i=1}^{\omega-1} f_i$ and $R = f_\omega$. Let $\mathcal{D}_Q$ and $\mathcal{D}_R$ be their respective discriminants. Let $d = deg(R)$. By hypothesis,

we have

$$\chi(\mathcal{D}_R) = (-1)^{d-1}$$

and

$$\chi(\mathcal{D}_Q) = (-1)^{n-d-(\omega-1)}.$$

Then, if the roots of Q are $(x_1, ..., x_{n-d})$ and those of R are $(x_{n-d+1}, ..., x_n)$, we have

$$\begin{aligned}
\mathcal{D} &= \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2 \\
&= \prod_{1 \leqslant i < j \leqslant n-d} (x_i - x_j)^2 \prod_{n-d+1 \leqslant i < j \leqslant n} (x_i - x_j)^2 \prod_{i=1}^{n-d} \prod_{j=n-d+1}^{n} (x_i - x_j)^2 \\
&= \mathcal{D}_Q \mathcal{D}_R \prod_{j=n-d+1}^{n} \left(\prod_{i=1}^{n-d} (x_j - x_i)^2 \right) \\
&= \mathcal{D}_Q \mathcal{D}_R \prod_{j=n-d+1}^{n} Q(x_j)^2
\end{aligned}$$

Let $D = \prod_{j=n-d+1}^{n} Q(x_j)$. If $\sigma \in G_R$ is a generator of the Galois group, then we know that σ permutes the roots of R and is the identity on $\mathbb{K}$, so that σ permutes the terms in D. We therefore have

$$\sigma(D) = D \Rightarrow D \in \mathbb{K}.$$

Thus

$$\begin{aligned}
\chi(\mathcal{D}) &= \chi(\mathcal{D}_Q)\chi(\mathcal{D}_R)\chi(D)^2 \\
&= (-1)^{n-d-\omega+1}(-1)^{d-1} \\
&= (-1)^{n-\omega}
\end{aligned}$$

□

Corollary 3 *Let $p \neq 2$ be a prime and q a power of p. Let $P \in \mathbb{F}_q[X]$ be a separable polynomial of discriminant $\mathcal{D}$, and ω the number of irreducible factors of P over $\mathbb{F}_q$. Let $\chi(x) = x^{\frac{q-1}{2}}$, then*

$$\chi(\mathcal{D}) = (-1)^{degP-\omega}.$$

Proof: $\mathbb{F}_q$ satisfies all the conditions, and χ is the quadratic character associated to $\mathbb{F}_q$ (it is the Legendre symbol in the case $p = q$).

□

We now look more carefully at polynomials of degree 3. We know that such polynomials are of 3 possible types: $((1,3))$, $((1,1),(2,1))$ or $((3,1))$, according to whether the polynomial has 3 roots in the base field, only 1 root, or is irreducible. We will here give a criterion allowing us to differentiate the 3 cases.

Theorem 12 *Let $\mathbb{K}$ be a field of cyclic type of characteristic different from 2, 3. Let χ be its associated quadratic character, and*

$$P(X) = X^3 + aX + b$$

a polynomial of discriminant $\mathcal{D} \neq 0$. If $a \neq 0$, consider

$$Q(X) = X^2 + \frac{3b}{a}X - \frac{a}{3} \in \mathbb{K}[X].$$

Let α and β be the two roots of Q and $k = \mathbb{K}(\alpha, \beta)$. Then we have

$$P \text{ is of type } ((1,3)) \Leftrightarrow \chi(\mathcal{D}) = 1 \text{ and } \frac{\alpha}{\beta} \in k^3,$$

$$P \text{ is of type } ((1,1),(2,1)) \Leftrightarrow \chi(\mathcal{D}) = -1,$$

and

$$P \text{ is of type } ((3,1)) \Leftrightarrow \chi(\mathcal{D}) = 1 \text{ and } \frac{\alpha}{\beta} \notin k^3.$$

If $a = 0$, then

$$P \text{ is of type } ((1,3)) \Leftrightarrow \chi(\mathcal{D}) = 1 \text{ and } b \in k^3,$$

$$P \text{ is of type } ((1,1),(2,1)) \Leftrightarrow \chi(\mathcal{D}) = -1,$$

and

$$P \text{ is of type } ((3,1)) \Leftrightarrow \chi(\mathcal{D}) = 1 \text{ and } b \notin k^3.$$

Proof: The case P is of type $((1,1),(2,1))$ if and only if $\chi(\mathcal{D}) = -1$ is just a particular case of theorem 11. The case $a = 0$ is also obvious. We then assume that $a \neq 0$ and $\chi(\mathcal{D}) = 1$. Let Δ be the discriminant of Q. Then we check that

$$\Delta = \frac{-3\mathcal{D}}{(3a)^2} \neq 0,$$

and therefore, $\alpha \neq \beta$, and k is an extension which is at most quadratic over $\mathbb{K}$. We also have

$$P(X) = X^3 - 3\alpha\beta X + \alpha\beta(\alpha + \beta).$$

We check that the resultant of P and Q is

$$\begin{aligned} Res(P,Q) &= \frac{16a^6 - 216b^2a^3 - 729b^4}{27a^3} \\ &= -\frac{(4a^3 + 27b^2)^2}{27u^3} \\ &= -\frac{\mathcal{D}^2}{27u^3} \neq 0. \end{aligned}$$

In particular, if $x_0 \in \overline{\mathbb{K}}$ is a root of P, then we have both $x_0 \neq \alpha$ and $x_0 \neq \beta$. Consider $A = \frac{x_0 - \alpha}{x_0 - \beta}$. Then

$$A^3 = \frac{\alpha}{\beta}.$$

Let $\rho \in \overline{\mathbb{K}}$ be a cube root of $\frac{\alpha}{\beta}$, and let $\zeta_3 \in \overline{\mathbb{K}}$ be a primitive cube root of unity. It is then clear that the three roots of $P(X)$ are

$$x_t = \frac{\alpha - \rho\zeta_3^t\beta}{1 - \rho\zeta_3^t} \text{ for } t \in \{0,1,2\}$$

(note that $\alpha \neq \beta \Rightarrow \rho\zeta_3^t - 1 \neq 0$.) This is also true when $\chi(\mathcal{D}) = -1$. Suppose now that $\frac{\alpha}{\beta}$ is a cube in k. Then we can choose $\rho \in k$. Then $x_0 = \frac{\alpha - \rho\beta}{1 - \rho}$ is a root of P in k, which is an extension at most quadratic over $\mathbb{K}$. That P is of type $((3,1))$ would be absurd, because then x would be in a cubic extension of $\mathbb{K}$, and not in $\mathbb{K}$. Thus P is of type $((1,3))$. Conversely, let $x \in \mathbb{K}$ be a root of P. Then $A \in k$ and $A^3 = \frac{\alpha}{\beta}$, so that $\frac{\alpha}{\beta}$ is a cube in k.

□

5.2 Cyclicity of the group of rational points

In this section, we will only consider elliptic curves defined over a finite field. We begin by giving a necessary condition for the cyclicity of the group of rational points, and then we will give necessary and sufficient criteria for the cyclicity of the subgroups of 2 and 3 torsion. For the subgroup of 3 torsion points, the cyclicity will only depend on the j-invariant, as long as

$j \neq 0$. Before this, we will give some results on the twists; results we will need throughout this dissertation. We now give the necessary condition for the cyclicity we have been talking about, a result due to Schoof [Sch87]:

Theorem 13 *Let E be an elliptic curve defined over a field $\mathbb{F}_q$, q being a power of a prime p. Let t be the trace of the Frobenius endomorphism φ, and let $n \in \mathbb{N}^*$ be prime to p. Then the two following assertions are equivalent:*

i) $E[n] \subset E(\mathbb{F}_q)$

ii) $n \mid t-2,\ n^2 \mid q+1-t$ *and either* $\varphi \in \mathbb{Z}$ *or* $\mathcal{O}\left(\dfrac{t^2-4q}{n^2}\right) \subset End_{\mathbb{F}_q}(E)$,

where $\mathcal{O}(d)$ is the imaginary quadratic order of discriminant d.

Proof: See [Sch87].

□

Corollary 4 *With the previous hypothesis, if for every prime $l \neq p$ dividing $t-2$, l^2 does not divide $\#E(\mathbb{F}_q) = q+1-t$, then the group $E(\mathbb{F}_q)$ is cyclic.*

Proof: We know that a finite abelian group G is cyclic if and only if for every prime l dividing $\#G$, $G[l] \approx \mathbb{Z}/l\mathbb{Z}$. Suppose that $E(\mathbb{F}_q)$ is not cyclic. By the previous remark, there exists a prime l dividing $q+1-t$ such that $E(\mathbb{F}_q)[l] \not\approx \mathbb{Z}/l\mathbb{Z}$. But we know that for $l \neq p$,

$$\{0\} \subset E(\mathbb{F}_q)[l] \subset E[l] \approx \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}.$$

Since l divides $q+1-t$ and $E(\mathbb{F}_q)[l] \not\approx \mathbb{Z}/l\mathbb{Z}$, we must therefore have $E(\mathbb{F}_q)[l] = E[l] \approx \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, which leads to $E[l] \subset E(\mathbb{F}_q)$ and by the previous theorem, $l \mid t-2$ and $l^2 \mid q+1-t$.

□

Example 1 Consider the curve $E : y^2 = x^3 + 9x + 57$ over $\mathbb{F}_{89}$. This curve has $98 = 2 * 7^2$ rational points, and the trace of the Frobenius is $t = -8$. Since neither 2^2 nor 5^2 divide 98, the group of rational points is cyclic. More precisely, this group is generated by the point $(3, 17)$.

Corollary 5 *All elliptic curves over a finite field with trace of Frobenius equal to either 1 or 3 have a cyclic group of rational points.*

Proof: In this case, $|t-2| = 1$, so no prime divides $t-2$.

□

5.2.1 2 and 3-cyclicity

We are now going to see the previously mentioned criteria, which relate the discriminant of the elliptic curve to the cyclicity of the rational points of 2 or 3 torsion.

Definition 12 *Let G be an abelian group and $n \in \mathbb{N}^*$. G is called n-cyclic when the subgroup of n-torsion points is cyclic.*

Remark: A finite abelian group G is cyclic if and only if G is l-cyclic for every prime l.

2-cyclicity

In this section, we will suppose that the field $\mathbb{K}$ is of characteristic different from 2. In the case when the characteristic is 2, the group of rational points is necessarily 2-cyclic.

Theorem 14 *Let $\mathbb{K}$ be a finite field of characteristic different from 2 and*

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

an elliptic curve defined over $\mathbb{K}$. Let Δ be the discriminant of E. Suppose that $2 \mid \#E(\mathbb{K})$. Then we have

$$E(\mathbb{K})\ is\ 2-cyclic \Leftrightarrow \Delta \notin \mathbb{K}^2.$$

Proof: Doing the change of variables $x = x'$ and $y = y' - \frac{a_1}{2}x' - \frac{a_3}{2}$, and renaming x' and y', which leaves the discriminant Δ unchanged, we may assume that $a_1 = a_3 = 0$. Then we have

$$E[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\},$$

where the x_i's are the three different roots of $f(x) = x^3 + a_2x^2 + a_4x + a_6$ in $\overline{\mathbb{K}}$. Since 2 divides $\#E(\mathbb{K})$, we know that one of the roots is in $\mathbb{K}$. Therefore f is of type $((1,1),(2,1))$ or $((1,3))$. In the first case, $E(\mathbb{K})[2]$ is cyclic, in the latter case, it is not. According to theorem 11 page 46, we can deduce that

$$E(K)\ is\ 2-cyclic \Leftrightarrow \Delta \notin \mathbb{K}^2.$$

□

3-cyclicity

In this part, $\mathbb{K}$ will be a finite field $\mathbb{F}_q$ of characteristic $p \neq 2,3$. We are going to study the 3-cyclicity of $E(\mathbb{F}_q)$ for an elliptic curve E defined over $\mathbb{F}_q$. According to Schoof's theorem (theorem 13 page 51), if 3 doesn't divide $q-1$ or 9 doesn't divide the number of rational points on the curve, then $E(\mathbb{F}_q)$ is necessarily cyclic. We shall therefore assume that both $3 \mid q-1$ and $9 \mid \#E(\mathbb{F}_q)$. We are now going to relate the 3-cyclicity of $E(\mathbb{F}_q)$ to the discriminant Δ of E, and then to its j-invariant when the latter is non-zero. We will first have to know that any root of the third division polynomial ψ_3 in $\mathbb{F}_q$ is the x-coordinate of a point in $E(\mathbb{F}_q)[3]$.

Lemma 6 *Let q be a power of a prime $p > 3$ and let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Assume that $q \equiv 1$ [3].Assume also that $\#E(\mathbb{F}_q) \equiv 0$ [3]. Let ψ_3 be the third division polynomial of this curve,

$$\psi_3(X) = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8.$$

Then we have

$$x_0 \in \mathbb{F}_q \text{ is a root of } \psi_3 \Leftrightarrow \exists P = (x_0, y_0) \in E(\mathbb{F}_q)[3].$$

Remark: This is not a particular case of proposition 2 page 29.
Proof: By definition, we have: $x_0 \in \overline{\mathbb{F}_q}$ is a root of ψ_3 if and only if $\exists P = (x_0, y_0) \in E[3]$, and therefore, one way is straightforward. Assume now that $x_0 \in \mathbb{F}_q$ is a root of ψ_3. Thus there exists a point $P = (x_0, y_0) \in E[3]$. Assume that $y_0 \notin \mathbb{F}_q$. Since

$$y_0^2 = x_0^3 + a_4x_0 + a_6,$$

we can deduce that $y_0 \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Let $D = x_0^3 + a_4x_0 + a_6 \in \mathbb{F}_q$. We have just seen that $D \notin \mathbb{F}_q^2$. We consider then the twisted curve

$$\widetilde{E}^D : y^2 = x^3 + D^2a_4X + D^3a_6.$$

We know that

$$\begin{array}{rccc} \varphi_{y_0} : & E(\mathbb{F}_{q^2}) & \longrightarrow & \widetilde{E}^D(\mathbb{F}_{q^2}) \\ & (t,u) & \longmapsto & (Dt, y_0^3u) \end{array}$$

is an isomorphism. But $x_0 \in \mathbb{F}_q$, $D \in \mathbb{F}_q$, $y_0 \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and so $Dx_0 \in \mathbb{F}_q$ and $y_0^4 \in \mathbb{F}_q$, and we get $\varphi_{y_0}(x_0, y_0) \in \widetilde{E}^D(\mathbb{F}_q)$. Moreover, since $(x_0, y_0) \in E[3]$ and φ_{y_0} is a morphism, then $\varphi_{y_0}(x_0, y_0) \in \widetilde{E}^D[3]$. We thus have

$$\varphi_{y_0}(x_0, y_0) \in \widetilde{E}^D(\mathbb{F}_q)[3]$$

and since $\varphi_{y_0}(x_0, y_0) \neq \mathcal{O}$, we must have

$$\widetilde{N}^D \equiv 0 \ [3].$$

We then conclude that

$$2(q+1) = N + \widetilde{N}^D \equiv 0 \ [3]$$

which is absurd since $q \equiv 1$ [3].

□

We come now to our criterion:

Theorem 15 *Let q be a power of a prime $p \neq 2,3$ and let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$ of discriminant Δ. Assume that $q \equiv 1$ [3] and $\#E(\mathbb{F}_q) \equiv 0$ [9]. Then $E(\mathbb{F}_q)$ is not 3-cyclic if and only if $\Delta \in \mathbb{F}_q^3$.

Proof: By hypothesis, there exists a rational point $P = (x_0, y_0)$ of order 3, and the question is to know whether or not there exists another rational point of order 3 independent of P (in which case $E(\mathbb{F}_q)$ is not cyclic), or not. With the change of variables $x = x' - x_0$ and $y = y' - y_0$, we can assume that the point $Q = (0,0)$ is a point of order 3 on the curve E, and with the change of variables $y' = y + \dfrac{a_4}{a_3}x$ and $x' = x$, we can assume that the equation is given by

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

We then have the following quantities:

$$b_2 = a_1^2, \quad b_4 = a_1a_3, \quad b_6 = a_3^2, \quad b_8 = 0$$

$$\Delta = a_1^3a_3^3 - 27a_3^4$$

Note that $a_3 \neq 0$, otherwise the curve would be singular. The x-coordinates of the points of exact order 3 in $\overline{\mathbb{F}_q}$ are given by the roots of the third division polynomial ψ_3, which in this case is given by

$$\begin{aligned}\psi_3(X) &= 3X^4 + b_2X^3 + 3b_4X^2 + b_6X + b_8 \\ &= 3X\varphi_3(X)\end{aligned}$$

where

$$\varphi_3(X) = X^3 + \alpha_2X^2 + \alpha_4X + \alpha_6$$

with

$$\alpha_2 = \frac{a_1^2}{3}, \quad \alpha_4 = a_1a_3, \quad \alpha_6 = a_3^2.$$

This polynomial is of a certain kind: it has either 3 roots in $\mathbb{F}_q$ (corresponding to the non-zero x-coordinates of the six points of order 3 not in $\{\mathcal{O}, Q, -Q\}$), or no roots in $\mathbb{F}_q$, that is φ_3 is irreducible in $\mathbb{F}_q[X]$, which is the case if and only if $E(\mathbb{F}_q)[3]$ is cyclic. We will now put φ_3 in the form

$$\theta_3(X) = X^3 + \beta_4X + \beta_6$$

by performing the change of variables $X = X' - \dfrac{\alpha_2}{3}$. Then we have the following quantities:

$$\beta_4 = \alpha_4 - \frac{\alpha_2^2}{3} = \frac{a_1}{27a_3^3}\Delta,$$

and

$$\beta_6 = \alpha_6 - \frac{\alpha_2\alpha_4}{3} + \frac{2\alpha_2^3}{27} = \frac{1}{729}\left(2a_1^6 + 81a_1^3a_3 + 729a_3^2\right).$$

Finally, θ_3 has discriminant

$$\mathcal{D} = -4\beta_4^3 - 27\beta_6^2 = \frac{1}{27}\left(-a_1^6a_3^2 + 54a_1^3a_3^3 - 729a_3^4\right).$$

The two polynomials φ_3 and θ_3 are of the same type: either both are irreducible over $\mathbb{F}_q$, or both have 3 different roots in $\mathbb{F}_q$. We then consider 2 cases, $\beta_4 = 0$ and $\beta_4 \neq 0$:

* $\boldsymbol{\beta_4 = 0}$

  In this case, θ_3 is irreducible over $\mathbb{F}_q$ if and only if β_6 is not a cubic residue in $\mathbb{F}_q$. But $\beta_4 = 0 \Leftrightarrow a_1 = 0$, so that $\beta_6 = a_3^2$ and $\Delta = -27a_3^4 = (-3a_3)^3a_3$, and we see that β_6 is not a cubic residue if

  and only if a_3 is not a cubic residue, i.e., if and only if Δ is not a cubic residue in $\mathbb{F}_q$.

* $\boldsymbol{\beta_4 \neq 0}$

  In this case, we consider the polynomial

$$g(X) = X^2 + \frac{3\beta_6}{\beta_4}X - \frac{\beta_4}{3}$$

  whose discriminant is

$$\delta = \frac{-3\mathcal{D}}{(3\beta_4)^2} = \left(\frac{3a_3}{a_1}\right)^2,$$

  which is a square in $\mathbb{F}_q$. We then consider the quantity A defined above, and we easily find that

$$A = \frac{\alpha}{\beta} = \left(\frac{a_1^3a_3^3}{\Delta}\right)^{\pm 1}.$$

  By theorem 12 page 49, we know that θ_3 is irreducible over $\mathbb{F}_q$ if and only if A is not a cubic residue in $\mathbb{F}_q(\sqrt{\delta}) = \mathbb{F}_q$, i.e., if and only if Δ is not a cubic residue in $\mathbb{F}_q$.

Since $E(\mathbb{F}_p)[3]$ is cyclic if and only if the polynomial φ_3 (or, equivalently, the polynomial θ_3) is irreducible, we get the desired result.

□

Corollary 6 *Let q be a power of a prime $p \neq 2, 3$. Let E be an elliptic curve defined over $\mathbb{F}_q$ with a rational 3-torsion point, and non-zero j-invariant j. Then*

$$E(\mathbb{F}_q) \textit{ is } 3-\textit{cyclic} \Leftrightarrow j \notin \mathbb{F}_q^3.$$

Proof: We can describe E by a Weierstrass equation

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

Then we have

$$j = \frac{c_4^3}{\Delta}$$

and we therefore see that

$$\Delta \in \mathbb{F}_q^3 \Leftrightarrow j \in \mathbb{F}_q^3.$$

□

Chapter 6

Factorisation of the division polynomials

We have just seen that the 2 and 3-cyclicity of the group of rational points of an elliptic curve defined over $\mathbb{F}_q$ is related to the type of the second and third division polynomials $\psi_2(X,Y) = 2Y$ and $\psi_3(X) = 3X^4+6a_4X^2+12a_6X-a_4^2$. It is then natural to search for the different types of the division polynomials $\psi_l(X)$ for a prime l and see whether the discriminant $\mathcal{D}_l$ of ψ_l can be used to distinguish the l-cyclicity from the non l-cyclicity. The latter will be done in the next chapter. We answer the former here.

The degrees of different irreducible factors of the division polynomials are given by the degrees of the extensions of $\mathbb{F}_q$ in which the x-coordinates of the points of l-torsion lie, that is almost on which the points of l-torsion are defined. We thus study the possible extensions on which these points are defined, and this can be done by studying the Frobenius endomorphism. We have to distinguish two main cases. On the one hand, when l equals the characteristic p of the field, the points of l-torsion form a $\mathbb{F}_l$-vector space of dimension 0 (the curve is supersingular) or 1 (the curve is ordinary), and the study of the Frobenius endomorphism is reduced to the study of its trace (section 6.1). On the other hand, when l is different from p, then the points of l-torsion form a $\mathbb{F}_l$ vector-space of dimension 2. Then either all the l-torsion points are defined over the same extension, which renders the degrees easy to study (lemma 13), or they are defined over different extensions. In such a case, we use the Weil pairing to describe the action of the Frobenius (lemma 9), and we then find the possible degrees of the irreducible factors (lemma 11 and 12), since we can find a connection between the degrees of

the extensions where the x-coordinates of the l-torsion points lie and the way the Frobenius endomorphism acts on these points (lemma 10).

6.1 Study of ψ_p where p is the characteristic of the field

A general result on the division polynomials ψ_n of an elliptic curve

$$E : y^2 = x^3 + a_4x + a_6$$

defined over a field $\mathbb{K}$ of characteristic different from 2 and 3, is that ψ_n for odd n, considered as a polynomial in $\mathbb{Z}[a_4, a_6, X, Y]$ is a polynomial in X of degree $\frac{n^2-1}{2}$ and of leading coefficient n. Considered as a polynomial in $\mathbb{K}[X]$, this result remains true, except when the characteristic p of $\mathbb{K}$ is non-zero and $p \mid n$, in which case ψ_n is a polynomial in $\mathbb{K}[X]$ of degree strictly less than $\frac{n^2-1}{2}$. It is the case we are interested in here. Once again, we will distinguish two cases, according to whether E is supersingular or not. The first case is the easiest, and this is the one we will treat first. But before that, we will give a general result, due to Cassels [Cas49]:

Theorem 16 *Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over a field $\mathbb{K}$. Let $m \in \mathbb{N}^*$, and consider ψ_m as a polynomial in $\mathbb{Z}[a_4, a_6, X, Y]$. Then we have*

$$\frac{\partial(\psi_m^2)}{\partial X} \equiv 0 \ [m]$$

Corollary 7 *Let $p > 3$ be a prime and q a power of p. Let E be an elliptic curve defined over $\mathbb{F}_q$. Then the p^{th} division polynomial is inseparable.*

Corollary 8 *Let $p > 3$ be a prime and let $\mathbb{K}$ be a perfect field of characteristic p. Let E be an ordinary elliptic curve defined over $\mathbb{K}$. Then there exists a separable polynomial $f \in \mathbb{K}[X]$ of degree $\frac{p-1}{2}$ such that*

$$\psi_p(X) = f(X)^p.$$

Proof: See [CH96]. □

Corollary 9 *Let $p > 3$ be a prime and q a power of p. Let E be an elliptic curve defined over $\mathbb{F}_q$. Then $deg(\psi_p)$ is a multiple of p.*

6.1.1 The elliptic curve is supersingular

This is the simplest case, since the division polynomial will be a constant. In a certain case, we will see that the constant is also known.

Theorem 17 *Let $p > 3$ be a prime and $\mathbb{K}$ be a field of characteristic p. Let E be a supersingular elliptic curve defined over $\mathbb{K}$. Then,*

$$\forall n \in \mathbb{N}^*,\ \exists k_n \in \mathbb{K}^* \text{ such that } \psi_{p^n}(X) = k_n.$$

Moreover, we have

$$k_n = k_1^{\frac{p^{2n}-1}{p^2-1}}.$$

Proof: Suppose that ψ_{p^n} is not a constant. Let $x \in \overline{\mathbb{K}}$ be a root of ψ_{p^n} and let $y \in \overline{\mathbb{K}}$ be such that $(x, y) \in E(\overline{K})$. Then we know that $(x, y) \in E[p^n] \backslash \{\mathcal{O}\}$. But E is supersingular, so $E[p^n] = \{\mathcal{O}\}$, which is absurd. Thus, ψ_{p^n} has no root in $\overline{\mathbb{K}}$, i.e. ψ_{p^n} is a non-zero constant.
We also have the relation, for a point $M = \in E(\overline{\mathbb{K}})$ [CH96],

$$\psi_{mn}(M) = \psi_m^{n^2}(M)\psi_n([m]M),$$

which implies that

$$k_{n+1} = k_n^{p^2}.k_1$$

and the result follows easily.

□

In the case where $p = q$, we have a result due to Cheon and Hahn:

Theorem 18 *Let $p > 3$ be a prime and E be a supersingular elliptic curve defined over $\mathbb{F}_p$. Then*

$$\psi_p(X) = -1.$$

Proof: See [CH96].

□

6.1.2 The elliptic curve is ordinary

We know by corollary 8 that the polynomial ψ_p is of degree $p\frac{p-1}{2}$, and we are now going to look at its leading coefficient, but we just have a result for fields of the form $\mathbb{F}_p$ for $p > 3$ prime. We are going to prove that in this

case, the leading coefficient is equal to the trace of the Frobenius. Thus, we will know the number of rational points on the curve just by looking at the leading coefficient of the p-th division polynomial, but this is not really effective.

Theorem 19 *Let $p > 3$ be a prime and let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_p$. Let $\varphi \in End(E)$ be the Frobenius endomorphism, and let t be the trace of φ. Let $e_{\frac{p-1}{2}}$ be the coefficient of the term of degree $p\dfrac{p-1}{2}$ of the division polynomial ψ_p. Then

$$e_{\frac{p-1}{2}} = t$$

in $\mathbb{F}_p$.

Proof: We will use the notation of Silverman [Sil86]. We will need the following lemma:

Lemma 7 *Under the same hypothesis, consider the formal group $\mathcal{F}$ associated to E. Then, if we write*

$$[p](z) = \sum_{i=1}^{\infty} d_i z^{ip},$$

and

$$\psi_p(X) = \sum_{i=0}^{\frac{p-1}{2}} e_i X^{ip},$$

we have

$$e_{\frac{p-1}{2}} = d_1.$$

Proof: If $P = (x, y) \in E(\overline{\mathbb{F}_p})$ and $[p]P \neq \mathcal{O}$, then

$$[p](P) = \left(\frac{\phi_p(x,y)}{\psi_p^2(x,y)}, \frac{\omega_p(x,y)}{\psi_p^3(x,y)}\right) = (x_p(x,y), y_p(x,y)).$$

We also have

$$[p](z) = z_p = -\frac{x_p}{y_p} = -\frac{\phi_p(x,y)\psi_p(x,y)}{\omega_p(x,y)}.$$

Since p is odd, we have

$$\phi_p(x,y) = x^{p^2} + \sum_{i=0}^{p^2-1} g_i x^i$$

and

$$\omega_p(x,y) = y\left[x^{\frac{3}{2}(p^2-1)} + \sum_{i=0}^{\frac{3}{2}(p^2-3)} h_i x^i\right].$$

Then we get

$$z_p = -\frac{e_{\frac{p-1}{2}} x^{p\frac{p-1}{2}+p^2} + \sum_{i=0}^{p\frac{p-1}{2}+p^2-1} l_i x^i}{y\left[x^{\frac{3}{2}(p^2-1)} + \sum_{i=0}^{\frac{3}{2}(p^2-3)} h_i x^i\right]}.$$

But we also have

$$x(z) = z^{-2} + \sum_{i\geqslant 2} m_i z^i$$

and

$$y(z) = -z^{-3} + \sum_{i\geqslant 1} n_i z^i.$$

At last we get

$$\begin{aligned} z_p &= -\frac{e_{\frac{p-1}{2}} z^{-(p(p-1)+2p^2)} + \sum_{i>-(p(p-1)+2p^2)} q_i z^i}{\left(z^{-3} + \sum_{i>-3} r_i z^i\right)\left(z^{-3(p^2-1)} + \sum_{i>-3(p^2-1)} s_i z^i\right)} \\ &= \frac{e_{\frac{p-1}{2}} z^{-p(3p-1)} + \sum_{i>-p(3p-1)} u_i z^i}{z^{-3-3(p^2-1)} + \sum_{i>-3-3(p^2-1)} v_i z^i} \\ &= e_{\frac{p-1}{2}} z^p + \sum_{i>p} w_i z^i. \end{aligned}$$

Comparing the coefficients, we get the desired result.

□

Let $\mathcal{F}$ be the formal group associated to the elliptic curve. Let

$$\omega(z) = \left(1 + \sum_{i>0} f_i z^i\right) dz$$

be the invariant differential. Then, according to a theorem due to Manin [Man63] (see also [Olsa]), we have

$$f_p = t.$$

Write also

$$[p](z) = \sum_{i>1} d_i z^{ip}.$$

Then according to [Yui78],

$$d_1 = f_p.$$

The theorem then follows by the previous lemma.

□

We are now going to look at the factorisation of ψ_p in the case when E is an ordinary elliptic curve defined over a finite field of characteristic p. We have already seen that the leading coefficient can be closely related to the trace of the Frobenius endomorphism, at least in the case when the field is $\mathbb{F}_p$. But the factorisation is also intimately related to the trace of the Frobenius. We will first need the following lemma, which also holds for supersingular curves:

Lemma 8 *Let $p > 3$ be a prime, q a power of p and E an elliptic curve defined over $\mathbb{F}_q$. Let t be the trace of the Frobenius endomorphism φ. For $s \in \mathbb{N}^*$, let $N_s = \#E(\mathbb{F}_{q^s})$. Then*

$$N_s \equiv 1 - t^s \ [q].$$

Proof: Consider the characteristic polynomial of the Frobenius endomorphism

$$P(X) = X^2 - tX + q.$$

Let α, β be the 2 complex roots of P. Then we know that we have

$$\alpha\beta = q, \ t = \alpha + \beta$$

and

$$N_s = 1 + q - (\alpha^s + \beta^s).$$

The case $s=1$ is trivial. Assume $s \geqslant 2$. We have

$$\begin{aligned} t^s - (\alpha^s + \beta^s) &= (\alpha+\beta)^s - (\alpha^s+\beta^s) \\ &= \sum_{i=0}^{s} \binom{i}{s} \alpha^i \beta^{s-i} - (\alpha^s+\beta^s) \\ &= \sum_{i=1}^{s-1} \binom{i}{s} \alpha^i \beta^{s-i} \\ &= \alpha\beta \sum_{i=1}^{s-1} \binom{i}{s} \alpha^{i-1} \beta^{s-i-1} \\ &= q\gamma \end{aligned}$$

where

$$\gamma = \sum_{i=1}^{s-1} \binom{i}{s} \alpha^{i-1} \beta^{s-i-1} = \frac{t^s - (\alpha^s+\beta^s)}{q} \in \mathbb{Q}.$$

Consider now Ω the integral closure of $\mathbb{Z}$ in the extension $\mathbb{Q}(\alpha,\beta)$ of $\mathbb{Q}$ which is at most quadratic. Since $P(\alpha) = P(\beta) = 0$, we have $\alpha, \beta \in \Omega$, and therefore $\gamma \in \Omega$. Finally,

$$\gamma \in \Omega \cap \mathbb{Q} = \mathbb{Z} \Rightarrow t^s - (\alpha^s + \beta^s) \equiv 0 \ [q],$$

which means that

$$N_s \equiv 1 - t^s \ [q].$$

□

Theorem 20 *Let $p > 3$ be a prime, q a power of p and*

$$E : y^2 = x^3 + a_4 x + a_6$$

an ordinary elliptic curve defined over $\mathbb{F}_q$. Let t be the trace of the Frobenius φ. Let $\beta = ord_{\mathbb{F}_p^*} t$ and $\alpha = \beta$ if β is odd, $\alpha = \frac{\beta}{2}$ if β is even. Let $e_{\frac{p-1}{2}}$ be the leading coefficient of ψ_p. Then ψ_p is of type

$$\left(e_{\frac{p-1}{2}}, \left(\alpha, p\frac{p-1}{2\alpha} \right) \right).$$

Proof: Since E is ordinary, we know that $t \not\equiv 0 \ [p]$ and therefore α and β are well defined.
According to corollary 8 page 60, we can write

$$\psi_p(X) = f(X)^p$$

with f a separable polynomial in $\mathbb{F}_q[X]$, so that if $I(X)$ is an irreducible factor of $\psi_p(X)$ over $\mathbb{F}_q$, then it will appear with multiplicity exactly p. Let thus $I(X)$ be an irreducible factor of $\psi_p(X)$ over $\mathbb{F}_q$, $d = deg(I)$ and $x_0 \in \mathbb{F}_{q^d}$ be a root of $I(X)$. Let $y_0 \in \overline{\mathbb{F}_q}$ be a square root of $x_0^3 + a_4 x_0 + a_6$. Then $P = (x_0, y_0) \in E(\mathbb{F}_{q^d})$ or $P \in E(\mathbb{F}_{q^{2d}})$, depending on whether $x_0^3 + a_4 x_0 + a_6$ is a square in $\mathbb{F}_{q^d}$ or not. By construction, $P \in E[p] \approx \mathbb{Z}/p\mathbb{Z}$ and P thus generates $E[p]$. By the definition of β, we then must have $\beta = d$ or $\beta = 2d$ depending on whether $x_0^3 + a_4 x_0 + a_6$ is a square in $\mathbb{F}_{q^d}$ or not. If β is odd, we must have $\beta = d$. Suppose then that β is even. Let D be a quadratic non-residue in $\mathbb{F}_{q^\alpha}$ and let $\delta \in \mathbb{F}_{q^\beta}$ be a square root of D. Consider the twist

$$\widetilde{E}^D : y^2 = x^3 + a_4 D^2 x + a_6 D^3.$$

By definition of α and β, we have

$$N_\alpha \equiv 1 - t^\alpha \ [q] \Rightarrow N_\alpha \equiv 1 - t^\alpha \not\equiv 0 \ [p].$$

But we also have

$$N_\beta = N_\alpha \widetilde{N}_\alpha^D \equiv 0 \ [p].$$

We can thus deduce that

$$\widetilde{N}_\alpha^D \equiv 0 \ [p]$$

and therefore

$$\mathbb{Z}/p\mathbb{Z} \subset \widetilde{E}^D(\mathbb{F}_{q^\alpha})[p] \subset \widetilde{E}^D[p] \approx E[p] \approx \mathbb{Z}/p\mathbb{Z}$$

which implies

$$\widetilde{E}^D(\mathbb{F}_{q^\alpha})[p] = \widetilde{E}^D(\mathbb{F}_{q^\alpha})[p] = \widetilde{E}^D[p]$$

Moreover, $\varphi_\delta(P) = (Dx_0, \delta^3 y_0) \in \widetilde{E}^D(\mathbb{F}_{q^\beta})[p]$, and from the previous remarks, we get that $Dx_0 \in \mathbb{F}_{q^\alpha}$, $x_0 \in \mathbb{F}_{q^\alpha}$ and finally $d \leqslant \alpha$. But, since either $d = \beta$ or $d = \alpha$, we get that $d = \alpha$.

□

We will find an example of this in appendix A page 93.

6.2 Study of ψ_l where l is not the characteristic of the field

We have just seen the possible factorisations of the division polynomials ψ_p in the case when p is the characteristic of the finite field of definition of the elliptic curve. This factorisation is closely related to the Frobenius endomorphism. We are now going to look at the possible factorisation of the division polynomials ψ_l, in the case when $l \neq p$. To achieve this, we will use two tools, namely the Weil pairing and the twists. The Weil pairing will allow us to see how the Frobenius endomorphism acts on l-torsion points, whereas twists will allow us to see where the l-torsion points are defined, since we don't have the property

$$x \in \mathbb{F}_{q^\alpha} \textit{ is a root of } \psi_l(x) \Leftrightarrow \exists P = (x,y) \in E(\mathbb{F}_{q^\alpha})[l].$$

As just mentioned, we will begin by looking at the action of the Frobenius on l-torsion points.

Lemma 9 *Let $p > 3$ be a prime and q be a power of p. Let*

$$E : y^2 = x^3 + a_4 x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Let φ be the Frobenius endomorphism defined over $\mathbb{F}_q$. Let l be a prime different from p, and α minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Assume moreover that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Let then $P \in E(\mathbb{F}_{q^\alpha})[l] \backslash \{\mathcal{O}\}$ and $Q \in E[l] \backslash E(\mathbb{F}_{q^\alpha})[l]$. Then there exist constants θ, ρ, μ and ν in $\mathbb{Z}$ such that

- $\varphi(P) = \rho P$,
- $\theta\rho \equiv 1\ [l]$,
- $\nu(1 - q\theta^2) \equiv 1\ [l]$ *if* $1 - q\theta^2 \not\equiv 0\ [l]$,
- $\forall n \in \mathbb{N}$,

$$\varphi^n(Q) = (q\theta)^n Q + \nu\mu\rho^{n-1}\left(1 - q^n\theta^{2n}\right) P \textit{ if } 1 - q\theta^2 \not\equiv 0\ [l]$$

and

$$\varphi^n(Q) = (q\theta)^n Q + n\mu\rho^{n-1} P \textit{ if } 1 - q\theta^2 \equiv 0\ [l].$$

Moreover, the multiplicative order of ρ in $\mathbb{Z}/l\mathbb{Z}^*$ is exactly α.

Proof: φ is an endomorphism of $E(\mathbb{F}_{q^\alpha})[l]$ so that

$$\varphi(P) \in E(\mathbb{F}_{q^\alpha})[l] = < P > \approx \mathbb{Z}/l\mathbb{Z}.$$

Thus, there exists $\rho \in \mathbb{Z}$ such that $\varphi(P) = \rho P$. Obviously, $\rho \not\equiv 0\ [l]$. Let β be the multiplicative order of ρ in $\mathbb{Z}/l\mathbb{Z}^*$. We then have

$$\forall m \in \mathbb{N},\ \varphi^m(P) = \rho^m P.$$

But φ^m is also the Frobenius endomorphism over $\mathbb{F}_{q^m}$. Since $P \in E(\mathbb{F}_{q^\alpha})$, we must have

$$P = \varphi^\alpha(P) = \rho^\alpha P \Rightarrow \rho^\alpha \equiv 1\ [l].$$

The definition of β gives us then that $\alpha \geqslant \beta$. But we also have

$$P = \rho^\beta P = \varphi^\beta(P) \Rightarrow P \in E(\mathbb{F}_{q^\beta}),$$

and then, since P is a l-torsion point, $l \mid N_\beta$, and by the very definition of α, $\alpha \leqslant \beta$, which means that $\alpha = \beta$.
Let

$$e_l : E[l] \times E[l] \longrightarrow \mu_l$$

be the Weil pairing, where μ_l is the subgroup of l-th roots of unity in $\overline{\mathbb{F}_q}$, and $\zeta_l = e_l(Q,P)$. Then ζ_l is a primitive l^{th}-root of unity since (Q,P) is a basis of $E[l]$. We have

$$e_l(\varphi(Q), \rho P) = e_l(\varphi(Q), \varphi(P)) = e_l(Q,P)^\varphi = \zeta_l^q.$$

Let us write $\varphi(Q)$ in the basis (Q,P): there exists $(\lambda,\mu) \in \mathbb{Z}^2$ such that $\varphi(Q) = \lambda Q + \mu P$. Then we get

$$e_l(\varphi(Q), \rho P) = e_l(\lambda Q + \mu P, \rho P) = e_l(Q,P)^{\lambda\rho} \cdot e_l(P,P)^{\mu\rho} = \zeta_l^{\lambda\rho}.$$

Comparing the two expressions, we get that

$$\lambda\rho \equiv q\ [l]$$

which implies that

$$\varphi(Q) = q\theta Q + \mu P$$

and by recursion, we get the desired result.

□

Corollary 10 *With the same hypothesis as before, if $\alpha = 1$, we have $\forall n \in \mathbb{N}$,*

$$\varphi^n(Q) = qQ + \nu\mu(1-q^n)P \; if \; q \not\equiv 1 \; [l]$$

and

$$\varphi^n(Q) = qQ + n\mu P \; if \; q \equiv 1 \; [l].$$

We are now going to look at a relation between the degree of the irreducible polynomial of the x-coordinate of a point on an elliptic curve and the action of the Frobenius endomorphism on this point.

Lemma 10 *Let $p > 3$ be a prime and q a power of p. Let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Let φ be the Frobenius endomorphism over $\mathbb{F}_q$. Let $l \neq p$ be a prime and $x_0 \in \overline{\mathbb{F}_q}$ a root of $\psi_l(X)$. Let $I(X)$ be the minimal polymomial of x_0 over $\mathbb{F}_q$. Let $P = (x_0, y_0) \in E(\overline{\mathbb{F}_q})$ be a point with x-coordinate x_0. Then $deg(I)$ is the minimal non-zero integer n_P such that $\varphi^{n_P}P = \pm P$.

Proof: Let m be the minimal integer such that $\varphi^m P = \pm P$, and let $d = deg\ I(X)$. Since $I(X)$ is irreducible over $\mathbb{F}_q$, φ^d is the Frobenius endomorphism on $\mathbb{F}_{q^d}$, and d is minimal such that $\varphi^d(x_0) = x_0$. We then have

$$\varphi^d(x_0) = x_0 \Leftrightarrow \varphi^n P = \pm P,$$

and thus $d = m$.

□

We now come to the main theorem of this section:

Theorem 21 *Let $p > 3$ be a prime and q be a power of p. Let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Let $l \neq p$ be another prime and α minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Let $P \in E(\mathbb{F}_{q^\alpha})[l] \backslash \{\mathcal{O}\}$. Let φ be the Frobenius endomorphism. If $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$, let $\rho \in \mathbb{Z}$ such that $\varphi P = \rho P$, $\theta \in \mathbb{Z}$ such that $\rho\theta \equiv 1 \; [l]$ and $\beta = ord_{\mathbb{F}_l^*} q\theta$. Then ψ_l has one of the following types:

- $\left(l, \left(\alpha, \dfrac{l-1}{2\alpha}\right), \left(\beta, \dfrac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \dfrac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right)$,

- $\left(l, \left(\alpha, \dfrac{l-1}{2\alpha}\right), \left(\dfrac{\beta}{2}, \dfrac{l-1}{\beta}\right), \left(\alpha \vee \beta, \dfrac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right)$,
- $\left(l, \left(\dfrac{\alpha}{2}, \dfrac{l-1}{\alpha}\right), \left(\beta, \dfrac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \dfrac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right)$,
- $\left(l, \left(\dfrac{\alpha}{2}, \dfrac{l-1}{\alpha}\right), \left(\dfrac{\beta}{2}, \dfrac{l-1}{\beta}\right), \left(\dfrac{\alpha \vee \beta}{2}, \dfrac{(l-1)^2}{\alpha \vee \beta}\right)\right)$,
- $\left(l, \left(\alpha, \dfrac{l-1}{2\alpha}\right), \left(\alpha l, \dfrac{l-1}{2\alpha}\right)\right)$,
- $\left(l, \left(\dfrac{\alpha}{2}, \dfrac{l-1}{\alpha}\right), \left(\dfrac{\alpha l}{2}, \dfrac{l-1}{\alpha}\right)\right)$,
- $\left(l, \left(\alpha, \dfrac{l^2-1}{2\alpha}\right)\right)$,
- $\left(l, \left(\dfrac{\alpha}{2}, \dfrac{l^2-1}{\alpha}\right)\right)$.

Proof: The theorem will follow by the three following lemmas:

Lemma 11 *Let $p > 3$ be a prime and q a power of p. Let*

$$E : y^2 = x^3 + a_4x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Let $l \neq p$ be another prime and α minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Assume that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Let $P \in E(\mathbb{F}_{q^\alpha})[l] \backslash \{\mathcal{O}\}$. Let φ be the Frobenius endomorphism. Let $\rho \in \mathbb{Z}$ such that $\varphi P = \rho P$ and $\theta \in \mathbb{Z}$ such that $\rho\theta \equiv 1 \; [l]$. Let $\beta = ord_{\mathbb{F}_l^*} q\theta$. Assume that $q\theta^2 - 1 \not\equiv 1 \; [l]$. Then ψ_l is of type:

α and β are odd

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right),$$

α is odd and β is even

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right),$$

α is even and β is odd

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right),$$

α and β are even

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\frac{\alpha \vee \beta}{2}, \frac{(l-1)^2}{\alpha \vee \beta}\right)\right).$$

Proof: Let $Q \in E[l] \backslash < P >$. Then according to lemma 9, there exists $\mu \in \mathbb{Z}$ such that $\varphi Q = q\theta Q + \mu P$. Replacing Q by $Q + \mu\rho^{-1}(q\theta^2 - 1)^{-1}P$, we may assume that $\mu \equiv 0\ [l]$. To find the factorisation of ψ_l over $\mathbb{F}_q$, it suffices by lemma 10 to find for every point $R \in < P, Q >$, the minimal non-zero integer n_R such that $\varphi^{n_R} R = \pm R$. Write R in the basis (P,Q) as $R = XP + YQ$. Then we have

$$\varphi^n R = X\rho^n P + Y(q\theta)^n Q.$$

We then have

$$\varphi^n R = \pm R \Leftrightarrow \begin{cases} X \equiv Y \equiv 0\ [l] & or, \\ X \equiv 0\ [l],\ Y \not\equiv 0\ [l]\ and\ (q\theta)^n \equiv \pm 1\ [l] & or, \\ X \not\equiv 0\ [l],\ \rho^n \equiv \pm 1\ [l]\ and\ Y \equiv 0\ [l] & or, \\ XY \not\equiv 0\ [l]\ and\ \rho^n \equiv (q\theta)^n \equiv \pm 1\ [l]. \end{cases}$$

α and β are odd

In this case, we know that $(q\theta)^n \not\equiv -1\ [l]$ and $\rho^n \not\equiv -1\ [l]$ for every $n \in \mathbb{N}$ and thus $\varphi^n R \neq -R$ for every $n \in \mathbb{N}$ if $R \neq \mathcal{O}$. If R is of the form YQ with $Y \not\equiv 0\ [l]$, then we obviously have $n_R = \beta$. In the same way, if R is of the form XP with $X \not\equiv 0\ [l]$, then we have $n_R = \alpha$. Finally, if $R = XP + YQ$ with $XY \not\equiv 0\ [l]$, then we have $\alpha \mid n_R$ and $\beta \mid n_R$, which leads to $\alpha \vee \beta \mid n_R$, and it is easy to see that $n_R = \alpha \vee \beta$. It now suffices to count the different types of points to obtain the factorisation: there exist $l-1$ points of the form XP with $X \not\equiv 0\ [l]$, $l-1$ points of the form YQ with $Y \not\equiv 0\ [l]$ and finally $(l-1)^2$ points of the last form. Since any x-coordinate appears in two different points, we thus obtain that the division polynomial ψ_l is of type:

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right).$$

α is even and β is odd

In this case, we might have $\varphi^n R = -R$ and this when R is of type XP with $X \not\equiv 0\ [l]$. In this case, we have $n_R = \frac{\alpha}{2}$. In the two other cases cited above, we necessarily have $\varphi^n R \neq -R$ for every $n \in \mathbb{N}$, whence $n_R = \beta$ if $R = YQ$ with $Y \not\equiv 0\ [l]$ and $n_R = \alpha \vee \beta$ when $R = XP + YQ$ with $XY \not\equiv 0\ [l]$. The type of ψ_l is then:

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right).$$

α is odd and β is even

We just exchange the roles of α, β, X, Y, P and Q, and ψ_l is of type

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right).$$

α and β are even

In this case, $\varphi^n R = -R$ is always possible and we have just as before $n_R = \frac{\alpha}{2}$ if $R = XP$ with $X \not\equiv 0\ [l]$, $n_R = \frac{\beta}{2}$ when $R = YQ$ with $Y \not\equiv 0\ [l]$ and $n_R = \frac{\alpha}{2} \vee \frac{\beta}{2} = \frac{\alpha \vee \beta}{2}$ in the last case. And we finally get that ψ_l is of type

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\frac{\alpha \vee \beta}{2}, \frac{(l-1)^2}{\alpha \vee \beta}\right)\right).$$

□

Corollary 11 *With the same hypothesis, we have that $\alpha \vee \beta$ is the minimal integer such that $E[l] \subset E(\mathbb{F}_{q^{\alpha \vee \beta}})$*

Proof: This follows from the proof of the lemma above.

□

Lemma 12 *Let $p > 3$ be a prime and q a power of p. Let*

$$E : y^2 = x^3 + a_4 x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Let $l \neq p$ be another prime and α minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Assume that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Let

$P \in E(\mathbb{F}_{q^\alpha})[l] \backslash \{\mathcal{O}\}$. Let φ be the Frobenius endomorphism. Let $\rho \in \mathbb{Z}$ such that $\varphi P = \rho P$ and $\theta \in \mathbb{Z}$ such that $\rho\theta \equiv 1\ [l]$. Let $\beta = ord_{\mathbb{F}_l^*} q\theta$. Assume that $q\theta^2 \equiv 1\ [l]$. Then ψ_l is of type:

α is odd

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\alpha l, \frac{l-1}{2\alpha}\right)\right),$$

α is even

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\alpha l}{2}, \frac{l-1}{\alpha}\right)\right).$$

Proof: Since $q\theta^2 \equiv 1\ [l]$, we have $\rho \equiv q\theta\ [l]$ and necessarily $\alpha = \beta$. Let $Q \in E[l] \backslash E(\mathbb{F}_{q^\alpha})[l]$ and let μ be such that $\varphi Q = q\theta Q + \mu P$. Then $\mu \not\equiv 0\ [l]$, otherwise we would have

$$\varphi Q = q\theta Q = \rho Q \Rightarrow \varphi^\alpha Q = \rho^\alpha Q = Q \Rightarrow Q \in E(\mathbb{F}_{q^\alpha})[l]$$

which is absurd. To find the factorisation of $\psi_l(X)$ over $\mathbb{F}_q$, it suffices according to lemma 9 to find, for every point $R \in < P, Q >$, the minimal non-zero integer n_R such that $\varphi^{n_R} R = \pm R$. Let us write R in the basis (P, Q) as $R = XP + YQ$. Then we have for every $n \in \mathbb{N}$,

$$\varphi^n R = (X\rho^n + Yn\mu\rho^{n-1})P + Y(q\theta)^n Q.$$

If $R = XP$ with $X \not\equiv 0\ [l]$, then necessarily n_R equals α or $\frac{\alpha}{2}$ depending on the parity of α. If $R = XP + YQ$ with $Y \not\equiv 0\ [l]$, then we must have $(q\theta)^{n_R} \equiv \pm 1\ [l]$. But this is equivalent to $\theta^{n_R} \equiv \pm 1\ [l]$, and thus we also must have $Yn_R\mu\rho^{n_R-1} \equiv 0\ [l]$. Since nothing is congruent to 0 modulo l except maybe n_R, we must have $n_R \equiv 0\ [l]$. Thus, in that case, we must have $n_R = \beta \vee l$ or $n_R = \frac{\beta \vee l}{2}$ depending on the parity of $\beta = \alpha$. Moreover, since $\beta \mid l - 1$, we have $\beta \wedge l = 1$ and thus $\beta \vee l = \beta l$. Then $\psi_l(X)$ can be of the following two types over $\mathbb{F}_q$:

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\alpha l, \frac{l-1}{2\alpha}\right)\right) \ if\ \alpha\ is\ odd$$

and

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\alpha l}{2}, \frac{l-1}{\alpha}\right)\right) \ if\ \alpha\ is\ even.$$

□

We are now going to examine the last case, when all the l-torsion points are defined over the same extension of $\mathbb{F}_q$:

Lemma 13 *Let $p > 3$ be a prime and q be a power of p. Let*

$$E : y^2 = x^3 + a_4 x + a_6$$

be an elliptic curve defined over $\mathbb{F}_q$. Let $l \neq p$ be another prime and α minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Assume that $E[l] \subset E(\mathbb{F}_{q^\alpha})$. Then ψ_l is of the type:

α is odd

$$\left(l, \left(\alpha, \frac{l^2-1}{2\alpha}\right)\right),$$

α is even

$$\left(l, \left(\frac{\alpha}{2}, \frac{l^2-1}{\alpha}\right)\right).$$

Proof: In this case, the α-th power of the Frobenius acts trivially on the l-torsion points, and α is minimal with this property. If α is odd, we then must have for every $R \in E(\mathbb{F}_{q^\alpha})[l] \backslash \{\mathcal{O}\}$, $n_R = \alpha$, and the type of ψ_l is

$$\left(l, \left(\alpha, \frac{l^2-1}{2\alpha}\right)\right).$$

If α is even, we then have $n_R = \alpha$ or $n_R = \frac{\alpha}{2}$. Let $\beta = \frac{\alpha}{2}$, $D \in \mathbb{F}_{q^\beta}$ a quadratic non-residue and $d \in \mathbb{F}_{q^\alpha}$ a square root of D. Consider the twist

$$\widetilde{E}^D : y^2 = x^3 + D^2 a_4 x + D^3 a_6.$$

Let

$$\begin{array}{rccc} \varphi_d : & E(\mathbb{F}_{q^\alpha}) & \longrightarrow & \widetilde{E}^D(\mathbb{F}_{q^\alpha}) \\ & (x, y) & \longmapsto & (Dx, Ddy) \end{array}$$

be the morphism given in section 3.5. Let m be maximal such that $l \mid N_\alpha$. By the very definition of α, we know that $l \not| N_\beta$. Moreover, we have

$$N_\alpha = \widetilde{N}_\alpha^D = N_\beta \widetilde{N}_\beta^D,$$

whence $l \mid \widetilde{N}_\beta^D$. This implies that all the points of l-torsion of $\widetilde{E}^D$ are defined over $\mathbb{F}_{q^\beta}$. In particular, if $R = (x_0, y_0) \in E(\mathbb{F}_{q^\alpha})[l]$,

$$\varphi_d(R) \in \widetilde{E}^D(\mathbb{F}_{q^\beta}) \Rightarrow Dx_0 \in \mathbb{F}_{q^\beta} \Rightarrow x_0 \in \mathbb{F}_{q^\beta}$$

and this at last implies that

$$n_R = deg(Irr(x_0, \mathbb{F}_q, X)) \leqslant \beta.$$

But we have already seen that $n_R \geqslant \beta$, whence $n_R = \frac{\alpha}{2}$ and ψ_l is of type

$$\left(l, \left(\frac{\alpha}{2}, \frac{l^2-1}{\alpha}\right)\right).$$

□

This proves the theorem.

□

We will give some examples which illustrate the theorem in appendix A, and show that all the cases can occur.

Chapter 7

A quadratic reciprocity law

As we have seen before, when studying the group of rational 2-torsion points over a finite field of odd characteristic, the cyclicity is given by the discriminant of the second division polynomial, or more accurately, by the discriminant of the square of this polynomial. We wanted to see if the discriminant of the l-th division polynomial could give some information on the cyclicity of the group of rational l-torsion points for other primes l. It is never the case. Amazingly, the fact that the discriminant of the l-th division polynomial of an elliptic curve defined over a finite field is a square or not is independent of the curve. It is just dependent on the field of definition of the curve and on the prime l. The result will be obtained by simply counting the number of irreducible factors of the l-th division polynomial and then using Pellet's theorem (theorem 11). The main idea is that the 2-valuations of q and $l-1$ are linked to the quadraticity of q modulo l. Then once again, we divide our study in two parts. First, if all the l-torsion points are defined on the same extension of $\mathbb{F}_q$, then the 2-valuations of q and of the orders of the eigenvalues of the Frobenius endomorphism acting on the l-torsion points are closely related (lemma 15 and 17). Secondly, when the l-torsion points are defined over the same extension, then we can link the 2-valuations of the degree of this extension to the 2-valuation of l^2-1 (lemma 16 and 18).

Theorem 22 *Let $p>3$ be a prime and q a power of p. Let $l \neq p$ be an odd prime. Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $\mathcal{D}_l$ be the discriminant of the l-th division polynomial of the curve. Then*

$$\mathcal{D}_l \text{ is a square in } \mathbb{F}_q \Leftrightarrow q \text{ is a square in } \mathbb{F}_l$$

The proof of the theorem will result from a combination of the analysis of the different types of the l-th division polynomial together with Pellet's theorem (theorem 11 page 46). The theorem will be a consequence of the following lemmas:

Lemma 14 *Let $p>3$ be a prime and q be a power of p. Let $l \neq p$ be an odd prime. Let $E: y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{F}_q$. Let α be minimal such that $l \mid \#E(\mathbb{F}_{q^\alpha})$. Assume that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Let φ be the Frobenius endomorphism. Let $P \in E(\mathbb{F}_{q^\alpha})[l]\backslash\{\mathcal{O}\}$ and $\rho \in \mathbb{Z}$ such that $\varphi P = \rho P$. Let $\theta \in \mathbb{Z}$ be such that $\theta\rho \equiv 1\ [l]$. Let $\beta = ord_{\mathbb{F}_l^*} q\theta$. Assume at last that $q\theta^2 \not\equiv 1\ [l]$. Then*

$$v_2(\alpha \vee \beta) \geqslant v_2(ord_{\mathbb{F}_l^*} q).$$

Proof: We already know that $\alpha \vee \beta$ is the minimal integer such that $E(\overline{\mathbb{F}_q})[l] \subset E(\mathbb{F}_{q^{\alpha\vee\beta}})$ (corollary 11 page 72). In particular, by [Sch87], we know that

$$l \mid q^{\alpha\vee\beta} - 1 \Rightarrow ord_{\mathbb{F}_l^*} q \mid \alpha \vee \beta.$$

□

Lemma 15 *Let $p>3$ be a prime and q a power of p. Let $l \neq p$ be an odd prime. Assume that q is a not a square modulo l. Let $E: y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{F}_q$. Let α be minimal such that $l \mid \#E(\mathbb{F}_{q^\alpha})$. Let $\mathcal{D}_l$ be the discriminant of the l-th division polynomial. Assume moreover that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Then $\mathcal{D}_l$ is not a square in $\mathbb{F}_q$.*

Proof: Saying that q is not a square modulo l is the same thing as saying that $v_2(ord_{\mathbb{F}_l^*} q) = v_2(l-1)$. Let ω_l be the number of irreducible factors of ψ_l over $\mathbb{F}_q$. Our goal is to show that ω_l is odd.
Let φ be the Frobenius endomorphism acting on E. Let $P \in E(\mathbb{F}_{q^\alpha})\backslash\{\mathcal{O}\}$ and $\rho \in \mathbb{Z}$ such that $\varphi P = \rho P$. Let $\theta \in \mathbb{Z}$ be such that $\theta\rho \equiv 1\ [l]$. Let $\beta = ord_{\mathbb{F}_l^*} q\theta$. By definition, both $\alpha \mid l-1$ and $\beta \mid l-1$ and thus using the previous lemma,

$$v_2(\alpha \vee \beta) = v_2(l-1).$$

In particular, since $l-1$ is even, α and β can not both be odd. Moreover, since q is not a square modulo l, $q\theta^2 \not\equiv 1\ [l]$. Therefore there remain three cases to examinate, depending on the parity of α and β. Moreover, since $v_2(\alpha \vee \beta) = Max(v_2(\alpha), v_2(\beta))$, we must have either $v_2(\alpha) = v_2(l-1)$ or

$v_2(\beta) = v_2(l-1)$. We write $l-1 = 2^s m$ with m odd.
Assume first that α is even and β is odd. Then we know that we can write $\alpha = 2^s\alpha'$ with $\alpha' \mid m$ is odd and $\beta \mid m$. In this case we know that the type of ψ_l is

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right)$$

and ω_l is given by

$$\begin{aligned}\omega_l &= \frac{l-1}{\alpha} + \frac{l-1}{2\beta} + \frac{(l-1)^2}{2(\alpha \vee \beta)} \\ &= \frac{m}{\alpha'} + 2^{s-1}\frac{m}{\beta} + 2^{s-1}\frac{m^2}{\alpha' \vee \beta} \\ &= \frac{m}{\alpha'} + 2^{s-1}\left(\frac{m}{\beta} + \frac{m^2}{\alpha' \vee \beta}\right)\end{aligned}$$

where $\frac{m}{\alpha'}$ is odd and $\frac{m}{\beta} + \frac{m^2}{\alpha' \vee \beta}$ is even. Thus, ω_l is odd. The case α odd and β even is done the same way.
Assume next that both α and β are even. Write $\alpha = 2^a\alpha'$ og $\beta = 2^b\beta'$ with $\alpha' \mid m$ og $\beta' \mid m$ are both odd. Moreover, we know that $a = s$ or $b = s$. If $a = b$, then $v_2(ord_{\mathbb{F}_l^*}\theta) = v_2(ord_{\mathbb{F}_l^*}q\theta) = v_2(l-1)$ and therefore both θ and $q\theta$ are non-square modulo l. This in turn means that q is a square modulo l which contradicts the hypothesis. We have thus exactly one of the following cases: $s > a$ or $s > b$. Assume that $s > b$ (the other case is done in the same way). Then

$$\begin{aligned}\omega_l &= \frac{l-1}{\alpha} + \frac{l-1}{\beta} + \frac{(l-1)^2}{\alpha \vee \beta} \\ &= \frac{m}{\alpha'} + 2^{s-b}\frac{m}{\beta'} + 2^s\frac{m^2}{\alpha' \vee \beta'}\end{aligned}$$

and since $s > s-b > 0$, ω_l is odd.
In all the cases, ω_l is odd, and by Pellet's theorem (theorem 11 page 46), we know that $\mathcal{D}_l$ is not a square in $\mathbb{F}_q$.

□

Lemma 16 *Let $p > 3$ be a prime and q a power of p. Let $l \neq p$ be an odd prime. Assume that q is not a square modulo l. Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{F}_q$. Let α be minimal such that $l \mid \#E(\mathbb{F}_{q^\alpha})$.*

Assume that $E[l] \subset E(\mathbb{F}_{q^\alpha})$. Let $\mathcal{D}_l$ be the discriminant of the l-th division polynomial. Then $\mathcal{D}_l$ is not a square in $\mathbb{F}_q$.

Proof: We will first prove that $v_2(l-1)+1 \leqslant v_2(\alpha)$. This will be enough for the case $l \equiv 1$ [4], but we will have to work a little bit more for the case $l \equiv 3$ [4]. By [Sch87], since $E[l] \subset E(\mathbb{F}_{q^\alpha})$, we know that $l \mid q^\alpha - 1$ and therefore

$$1 \leqslant v_2(l-1) = v_2(ord_{\mathbb{F}_l^*}q) \leqslant v_2(\alpha).$$

In particular, α is even, and ψ_l of type

$$\left(l, \left(\frac{\alpha}{2}, \frac{l^2-1}{\alpha}\right)\right)$$

and $\alpha \mid l^2 - 1$. Let D be a quadratic non-residue in $\mathbb{F}_{q^{\frac{\alpha}{2}}}$, and let $\widetilde{E}^D$ be the D-twist of E. Then, as we did in lemma 13, we can show that

$$\widetilde{E}^D[l] \subset \widetilde{E}^D(\mathbb{F}_{q^{\frac{\alpha}{2}}}).$$

Then using the same argument, we have

$$l \mid q^{\frac{\alpha}{2}} - 1 \Rightarrow v_2(ord_{\mathbb{F}_l^*}q) \leqslant v_2(\alpha) - 1.$$

When $l \equiv 1$ [4], we have that $1 = v_2(l+1)$, and therefore

$$v_2(l^2-1) = v_2(l-1) + v_2(l+1) \leqslant v_2(\alpha).$$

We want to prove the same thing when $l \equiv 3$ [4]. Let P and Q be two linearly independent points in $E(\mathbb{F}_{q^\alpha})[l]$. Let φ be the Frobenius endomorphism acting on E. Then in the basis (P, Q) over $\mathbb{F}_l$, φ is given by a matrix of the form $M_\varphi = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{F}_l)$. Let $\chi(X)$ be the characteristic polynomial of M_φ. We know that the determinant of this matrix is $q \in \mathbb{F}_l$. If $\chi(X)$ was reducible over $\mathbb{F}_l$, then we would be able to find a point $R \in E(\mathbb{F}_{q^\alpha})$ which is an eigenvector for φ. But then $\varphi^{l-1}R = R$, which would contradict the fact that $v_2(l-1)+1 \leqslant v_2(\alpha)$. Thus $\chi(X)$ is irreducible over $\mathbb{F}_l$. Let x_1 and x_2 be the two roots of $\chi(X)$ in $\mathbb{F}_{l^2}$. Since $l \neq 2$, $\chi(X)$ is inseparable and $x_1 \neq x_2$ and therefore M_φ is diagonalizable over $\mathbb{F}_{l^2}$, $x_2 = x_1^l$ and $q = x_1x_2 = x_1^{l+1}$. Over $\mathbb{F}_{l^2}$, M_φ can be written in the form $M_\varphi = \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix}$. In particular, it is

obvious that $\alpha = ord_{\mathbb{F}_{l^2}^*} x_1$. Assume that $v_2(\alpha) < v_2(l^2-1)$. Since $\alpha \mid l^2-1$, this means that $\alpha \mid \frac{l^2-1}{2}$. But then

$$q^{\frac{l-1}{2}} = (x_1 x_2)^{\frac{l-1}{2}} = x_1^{\frac{l^2-1}{2}} = 1.$$

But this is absurd since q is by hypothesis not a square in $\mathbb{F}_l$. Therefore $v_2(\alpha) = v_2(l^2-1)$ in the case $l \equiv 3$ [4] also.
Let then ω_l be the number of irreducible factors of ψ_l over $\mathbb{F}_q$. We have $\omega_l = \frac{l^2-1}{\alpha}$ which is odd since $v_2(\alpha) = v_2(l^2-1)$. Using Pellet's theorem (theorem 11 page 46), we get that $\mathcal{D}_l$ is not a square in $\mathbb{F}_q$.

□

We have now seen that whenever q is not a square in $\mathbb{F}_l$, then the discriminant $\mathcal{D}_l$ of ψ_l is not a square in $\mathbb{F}_q$. We will now prove the converse, namely that whenever q is a square in $\mathbb{F}_l$, then $\mathcal{D}_l$ is a square in $\mathbb{F}_q$.

Lemma 17 *Let $p > 3$ be a prime and q a power of p. Let $l \neq p$ be an odd prime. Assume that q is a square modulo l. Let $E : y^2 = x^3 + a_4 x + a_6$ be an elliptic curve defined over $\mathbb{F}_q$. Let α be minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Assume that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Let $\mathcal{D}_l$ be the discriminant of the l-th division polynomial. Then $\mathcal{D}_l$ is a square in $\mathbb{F}_q$.*

Proof: Let ω_l be the number of irreducible factors of ψ_l over $\mathbb{F}_q$. Let φ be the Frobenius endomorphism acting on E. We will show that ω_l is even. Let $P \in E(\mathbb{F}_{q^\alpha})[l] \backslash \{\mathcal{O}\}$ and $\rho \in \mathbb{Z}$ such that $\varphi P = \rho P$. Let $\theta \in \mathbb{Z}$ be such that $\rho\theta \equiv 1$ [l]. Let $\beta = ord_{\mathbb{F}_l^*} q\theta$.
Assume first that $q \equiv \rho^2$ [l]. Then ψ_l is of the form

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\alpha l, \frac{l-1}{2\alpha}\right)\right) \text{ if } \alpha \text{ is odd}$$

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\alpha l}{2}, \frac{l-1}{\alpha}\right)\right) \text{ if } \alpha \text{ is even}$$

We then have $\omega_l = \frac{l-1}{\alpha}$ if α is odd and $\omega_l = 2\frac{l-1}{\alpha}$ if α is even. In any case, ω_l is even.
Assume now that $q \not\equiv \rho^2$ [l]. Write $l-1 = 2^s m$ with m odd. Write $\alpha = 2^a \alpha'$ with α' odd and $\beta = 2^b \beta'$ with β' odd. By definition of α and β, we know that $\alpha' \mid m$, $\beta' \mid m$. We have to distinguish the four usual cases:

α and β are odd
In this case, $a = b = 0$ and ψ_l is of the form

$$\left(l, \left(\alpha, \frac{l-1}{2\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right)$$

and consequently

$$\begin{aligned} \omega_l &= \frac{2^s m}{2\alpha'} + \frac{2^s m}{2\beta'} + \frac{2^{2s} m^2}{2(\alpha' \vee \beta')} \\ &= 2^{s-1}\left(\frac{m}{\alpha'} + \frac{m}{\beta'}\right) + 2^{2s-1}\frac{m^2}{\alpha' \vee \beta'}. \end{aligned}$$

But $\frac{m}{\alpha'}$ and $\frac{m}{\beta'}$ are odd and $2s - 1 \geqslant 1$, so ω_l is even.

α is even and β is odd
In this case, $b = 0$ and ψ_l is of type

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\beta, \frac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \frac{(l-1)^2}{2(\alpha \vee \beta)}\right)\right)$$

and consequently

$$\begin{aligned} \omega_l &= \frac{2^s m}{2^a \alpha'} + \frac{2^s m}{2\beta'} + \frac{2^{2s} m^2}{2^{a+1}(\alpha' \vee \beta')} \\ &= 2^{s-a}\frac{m}{\alpha'} + 2^{s-1}\frac{m}{\beta'} + 2^{2s-a-1}\frac{m^2}{\alpha' \vee \beta'} \end{aligned}$$

which is even if $s > a$ since then $s \geqslant 2$. Moreover $s = a$ is not possible: this would mean that θ is not a square since $v_2(ord_{\mathbb{F}_l^*}\theta) = v_2(l-1)$, $q\theta$ is a square since $v_2(ord_{\mathbb{F}_l^*} q\theta) < v_2(l-1)$ and thus q would not be a square in $\mathbb{F}_l$.

α is odd and β is even
This is done in the same way as previously by exchanging the roles of α and β.

α and β are even
In this case, $a \geqslant 1$ and $b \geqslant 1$. We can suppose that $a \geqslant b$ first (the converse can be done in the same way). Moreover ψ_l is of type

$$\left(l, \left(\frac{\alpha}{2}, \frac{l-1}{\alpha}\right), \left(\frac{\beta}{2}, \frac{l-1}{\beta}\right), \left(\frac{\alpha \vee \beta}{2}, \frac{(l-1)^2}{\alpha \vee \beta}\right)\right)$$

and consequently

$$\begin{aligned}\omega_l &= \frac{2^s m}{2^a\alpha'}+\frac{2^s m}{2^b\beta'}+\frac{2^{2s}m^2}{2^a(\alpha'\vee\beta')}\\ &= 2^{s-a}\frac{m}{\alpha'}+2^{s-b}\frac{m}{\beta'}+2^{2s-a}\frac{m^2}{\alpha'\vee\beta'}.\end{aligned}$$

Thus in this case, ω_l is even again if $s \neq a$. If $s = a$, then as we saw before θ is not a square in $\mathbb{F}_l$, which means that $q\theta$ is not a square in $\mathbb{F}_l$, and in turn, $b = v_2(ord_{\mathbb{F}_l^*}q\theta) = v_2(l-1) = s$ and

$$\omega_l = \frac{m}{\alpha'}+\frac{m}{\beta'}+2^s\frac{m^2}{\alpha'\vee\beta'}$$

is again even.

Finally, using Pellet's theorem (theorem 11 page 46) once more, $\mathcal{D}_l$ is a square.

□

Lemma 18 *Let $p > 3$ be a prime and q a power of p. Let $l \neq p$ be an odd prime. Assume that q is a square modulo l. Let $E : y^2 = x^3 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{F}_q$. Let α be minimal such that $l \mid N_\alpha = \#E(\mathbb{F}_{q^\alpha})$. Assume that $E[l] \subset E(\mathbb{F}_{q^\alpha})$. Then the discriminant $\mathcal{D}_l$ of ψ_l is a square in $\mathbb{F}_q$.*

Proof: Let ω_l be the number of irreducible factors of ψ_l over $\mathbb{F}_q$. We will prove that ω_l is even. Let φ be the Frobenius endomorphism acting on E over $\mathbb{F}_q$. Let χ be the characteristic polynomial of φ: $\chi(X) = X^2 - tX + q$ where t is the trace of the Frobenius. Let (P, Q) be a basis of $E(\mathbb{F}_{q^\alpha})[l]$. Then in this basis, the action of the Frobenius is given by a matrix M_φ of the form $M_\varphi = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{F}_l)$.
If χ is reducible over $\mathbb{F}_l$, then we may suppose that $c = 0$. In this case, there exists a point $R \in E[l]$ such that $\varphi R = aR$. We thus have that $\varphi^{l-1}R = R$ and therefore $\alpha \mid l-1$. But we also know that ψ_l is of type

$$\left(l, \left(\alpha, \frac{l^2-1}{2\alpha}\right)\right) \ if\ \alpha\ is\ odd$$

and

$$\left(l, \left(\frac{\alpha}{2}, \frac{l^2-1}{\alpha}\right)\right) \ if\ \alpha\ is\ even.$$

Thus $\omega_l = \frac{l^2-1}{2\alpha} = \frac{l+1}{2}\frac{l-1}{\alpha}$ if α is odd and $\omega_l = \frac{l^2-1}{\alpha} = (l+1)\frac{l-1}{\alpha}$ if α is even. In both cases, ω_l is even.
Assume now that χ is irreducible over $\mathbb{F}_l$. Then it is separable since $l \neq 2$, and M_φ is diagonalisable over $\mathbb{F}_{l^2}$ and can be written under the form $\begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix}$ with $x_1, x_2 \in \mathbb{F}_{l^2}$, $x_1 \neq x_2$ and $x_1x_2 = q$. Moreover, when looking at the action of the Frobenius of $\mathbb{F}_l$, we see that $x_1^l = x_2$ and $x_2^l = x_1$. By definition of α, we have $x_1^\alpha = 1$ and α is minimal with this property. Now, if α is odd, we have $\omega_l = \frac{l^2-1}{2\alpha}$ is even. If α is even, we have to work a little bit more. Since q is a square in $\mathbb{F}_l$, we have

$$1 = q^{\frac{l-1}{2}} = (x_1x_2)^{\frac{l-1}{2}} = x_1^{(l+1)\frac{l-1}{2}} = x_1^{\frac{l^2-1}{2}} \Rightarrow \alpha \mid \frac{l^2-1}{2}.$$

Then, $\omega_l = \frac{l^2-1}{\alpha}$ is even. Using Pellet's theorem (theorem 11 page 46) again, we get the desired result.

□

Chapter 8

Asymptotic probabilities of factorisation patterns of division polynomials

We have seen in the previous chapters which patterns can occur as factorisations of division polynomials of elliptic curves over prime finite fields. The question that naturally arises is how often a pattern occurs. In other words, given two primes p and l with $p \neq l$, what is the probability of finding an elliptic curve over $\mathbb{F}_p$ at random whose l^{th} division polynomial has a given pattern. In this chapter, we give an asymptotic answer as p approaches infinity for the probability that a randomly chosen elliptic curve over $\mathbb{F}_p$ has a linear factor in its l^{th} division polynomial. This is done by using results on modular curves over finite fields which we recall here (theorems 23 and 24), and by identifying which factorisation types correspond to these theorems (lemma 19 and thorem 25). Thereafter, we notice that when $l = 3$, the number of possible factorisation types is quite reduced, and using all the previous results, this enables us to give a complete answer for the asymptotic probabilities in p for that case. Finally, we give a conjecture for the asymptotic probabilities in p for any prime l and some evidence for it.

8.1 Number of elliptic curves defined over $\mathbb{F}_p$ with a rational l-torsion point

This section relies heavily on 3 articles of Lenstra, Howe and Vladut. We cite the two major results from these articles, after introducing some notation.

$\mathcal{E}_p$ is the set of elliptic curves defined over $\mathbb{F}_p$ up to isomorphism.

If $A \subset \mathcal{E}_p$, the the weighted cardinality $\#'A$ of A is

$$\#'A = \sum_{E \in \Omega \cap A} \frac{1}{\#Aut(E)},$$

where Ω is a set of representative of the isomorphism classes of elliptic curves.

Property 10 *We have* $\#'\mathcal{E}_p = p$

Proof: See [How93].

□

Property 11 *If* $A \subset \mathcal{E}_p$, *then* $\#A = 2\#'A + \mathcal{O}(1)$.

Proof: For any elliptic curve E with j-invariant different from 0 or 1728, $\#Aut(E) = 2$ (cf [Sil86]).

□

We then have the two following results:

Theorem 23 (Lenstra) *Let* p, l *be primes,* $p > 3$ *and* $l \neq p$. *Let* $\mathcal{E}_{p,l}$ *be the subset of* $\mathcal{E}_p$ *of elliptic curves up to isomorphism whose number of rational points is congruent to* 0 *modulo* l. *Then*

$$\#'\mathcal{E}_{p,l} = \begin{cases} \frac{p}{l-1} + \mathcal{O}(l\sqrt{p}) & if\ p \not\equiv 1\ [l] \\ \frac{lp}{l^2-1} + \mathcal{O}(l\sqrt{p}) & if\ p \equiv 1\ [l] \end{cases}.$$

Proof: See [Len87]

□

And

Theorem 24 (Howe) *Let* q *be a power of a prime and* $\{l_1, \ldots, l_r\}$ *be a set of prime divisors of* $q - 1$. *Let*

$$W(l_1, \ldots, l_r) = \{E \text{ elliptic curve over } \mathbb{F}_q,\ \#E(\mathbb{F}_q)[l_1 \ldots l_r] = l_1^2 \ldots l_r^2\}.$$

Then

$$\left| \#W(l_1,\ldots,l_r) - \frac{2q}{\prod_{i=1}^{r} l_i(l_i^2-1)} \right| \leqslant \frac{(10\sqrt{2}+1)2^r\sqrt{p}}{12}.$$

Proof: See [Vla99a], [How93].

□

8.2 Asymptotic probabilities of having a linear factor

Looking at the results of chapter 6, and keeping the same notation as in this chapter, we see that it is necessary and sufficient that $\alpha = 1$ or $\alpha = 2$ for having such a linear factor. We begin with a lemma which will allows us to treat just the case $\alpha = 1$, the case $\alpha = 2$ being a consequence of it.

Lemma 19 *Let $p \geqslant 3$ be a prime and $l \neq p$ be an odd prime. For any elliptic curve E over $\mathbb{F}_p$, let α_E be the minimal integer such that $l \mid \#E(\mathbb{F}_{p^{\alpha_E}})$. Let $D \in \mathbb{F}_p \backslash \mathbb{F}_p^2$. Then, if $p \not\equiv -1\ [l]$, we have a bijection*

$$\left\{ \begin{array}{c} E \text{ elliptic curve over } \mathbb{F}_p, \\ \alpha_E = 1 \end{array} \right\} \begin{array}{c} \longrightarrow \\ \\ \longmapsto \end{array} \left\{ \begin{array}{c} E \text{ elliptic curve over } \mathbb{F}_p, \\ \alpha_E = 2 \end{array} \right\}.$$
$$E \qquad\qquad\qquad \widetilde{E}^D$$

If $p \equiv -1\ [l]$, then $\{E \text{ elliptic curve over } \mathbb{F}_p,\ \alpha_E = 2\} = \emptyset$.

Proof: Let $p \not\equiv -1\ [l]$. Let $\delta \in \mathbb{F}_{p^2}$ be such that $\delta^2 = D$. Let E be an elliptic curve defined over $\mathbb{F}_p$ by a Weierstrass equation $y^2 = x^3 + a_4x + a_6$ with $\alpha_E = 1$. Let $F = \widetilde{E}^D$. Then $\alpha_F = 2$. Indeed, since $\alpha_E = 1$, then there exists $P_0 = (x_0, y_0) \in E(\mathbb{F}_p)[l]$. Then $(Dx_0, \delta^3 y_0) \in F(\mathbb{F}_{p^2})[l]$ and thus $\alpha_F \leqslant 2$. If $\alpha_F = 1$, then there would exist a point $(x_1, y_1) \in F(\mathbb{F}_p)[l]$ thus $P_1 = (\frac{x_1}{D}, \frac{y_1}{\delta^3}) \in E(\mathbb{F}_{p^2})[l]$. Moreover, $P_1 \notin E(\mathbb{F}_p)$ since otherwise this would mean that $y_1 = 0$ and thus $P_1 \in E[l] \cap E[2] = \{\mathcal{O}\}$. Then (P_0, P_1) forms a basis of $E[l]$ and we must have $\varphi(P_0) = P_0$ and $\varphi(P_1) = -P_1$ where φ is the Frobenius endomorphism. Thus, $Det(\varphi) \equiv -1\ [l] \equiv p\ [l]$, which is absurd.
Conversely, let F be an elliptic curve defined over $\mathbb{F}_p$ by a Weierstrass equation $y^2 = x^3 + a_4'x + a_6'$ with $\alpha_F = 2$. Let $E = \widetilde{F}^{D^{-1}}$. Since $\alpha_F = 2$, then we

know that its l^{th}-division polynomial has a linear factor. Let x_2 be a root in $\mathbb{F}_p$ of this polynomial, and $y_2 \in \mathbb{F}_{p^2}$ such that $(x_2, y_2) \in F(\mathbb{F}_{p^2})[l]$. Then $P_2 = (\frac{x_2}{D}, \frac{y_2}{\delta^3}) \in E(\mathbb{F}_p)[l]$ and thus $\alpha_E = 1$. Since $F = \widetilde{E}^D$, the first part of the lemma is proved.
If $p \equiv -1\ [l]$, let E be an elliptic curve defined by a Weierstrass equation $y^2 = x^3 + a_4x + a_6$ over $\mathbb{F}_p$ with $\alpha_E = 2$. Assume first that $E[l] \not\subset E(\mathbb{F}_{p^2})$. Then $\beta_E = ord_{\mathbb{F}_l^*}(-1)^2 p = 2$. Then using the results of chapter 6, we find that the l^{th}-division polynomial ψ_l splits, which in turn means that $E[l] \subset E(\mathbb{F}_{p^2})$. Assume therefore that $E[l] \subset E(\mathbb{F}_{p^2})$. Then once again ψ_l splits, and if we take a D-twist, then we have $\widetilde{E}^D[l] \subset E(\mathbb{F}_p)$ and this leads to $p \equiv 1\ [l]$.

□

We now come to the asymptotic probabilities we are interested in. We will use the following notation:

Let T be a pattern, l be a prime number and $m \in \{1,\ldots,l-1\}$. Let $\mathcal{P}_{l,m}$ be the set of prime numbers congruent to m modulo l. Then, if it exists,

$$P(T,l,m) = \lim_{\substack{p \in \mathcal{P}_{l,m} \\ p \to +\infty}} \frac{\#\{E \text{ elliptic curve over } \mathbb{F}_p,\ pattern(\psi_l) = T\}/_{\approx \mathbb{F}_p}}{\#\mathcal{E}_p}.$$

The theorem is:

Theorem 25 *Let l be an odd prime number and $m \in \{2,\ldots,l-2\}$. Let $\beta = ord_{\mathbb{F}_l^*} m$. Then we have*

$$P(((1, \tfrac{l^2-1}{2})), l, 1) = \frac{2}{l(l^2-1)}$$

$$P(((1, \tfrac{l-1}{2}), (l, \tfrac{l-1}{2})), l, 1) = \frac{2}{l}$$

$$P(((1, \tfrac{l-1}{2}), (\beta, \tfrac{l(l-1)}{2\beta})), l, m) = \frac{2}{l-1} \text{ if } \beta \text{ is odd}$$

$$P(((1, \tfrac{l-1}{2}), (\tfrac{\beta}{2}, \tfrac{l-1}{\beta}), (\beta, \tfrac{(l-1)^2}{2\beta})), l, m) = \frac{2}{l-1} \text{ if } \beta \text{ is even}$$

$$P(((1, l-1), (2, \tfrac{(l-1)^2}{4})), l, l-1) = \frac{1}{l-1}$$

For any other pattern having a factor of degree 1 *and any* $n \in \{1,\dots,l-1\}$, $P(T,l,n)=0$.

Proof: We treat the case $m \not\equiv \pm 1$ first, and then come back to that case. As we have just seen, it suffices to count the number of elliptic curves E defined over $\mathbb{F}_p$ up to isomorphism having the given pattern and $\alpha_E = 1$, since the result will either equal or be twice as much. Since $m \not\equiv \pm 1$ $[l]$, the pattern has to be either $T = ((1,\frac{l-1}{2}),(\beta,\frac{l(l-1)}{2\beta}))$ if β is odd or $((1,\frac{l-1}{2}),(\frac{\beta}{2},\frac{l-1}{\beta}),(\beta,\frac{(l-1)^2}{2\beta}))$ if β is even. Then Lenstra's result together with the previous lemma gives

$$P(T,l,m) = 2 \cdot \lim_{\substack{p \in \mathcal{P}_m \\ p \to +\infty}} \frac{\frac{2p}{l-1}+\mathcal{O}(l\sqrt{p})}{2p+\mathcal{O}(\sqrt{p})} = \frac{2}{l-1}.$$

Howe's result together with the previous lemma leads to that for the pattern $T = ((1,\frac{l^2-1}{2}))$,

$$P(T,l,1) = 2 \cdot \lim_{\substack{p \in \mathcal{P}_m \\ p \to +\infty}} \frac{\frac{2p}{l(l^2-1)}+\mathcal{O}(2\sqrt{p})}{2p+\mathcal{O}(\sqrt{p})} = \frac{2}{l(l^2-1)}.$$

For $S = ((1,\frac{l-1}{2}),(l,\frac{l-1}{2}))$, Lenstra's theorem, the previous result and the previous lemma give

$$P(S,l,1) + P(T,l,1) = 2 \cdot \frac{l}{l^2-1} \Rightarrow P(S,l,1) = \frac{2}{l}.$$

Finally, for $T = ((1,l-1),(2,\frac{(l-1)^2}{4}))$, Lenstra's theorem and the previous lemma give

$$P(T,l,l-1) = \frac{1}{l-1}.$$

Since the other patterns never occur, their probability is 0.

□

8.3 A complete answer when $l = 3$

When $l = 3$, we give a complete answer using the quadratic reciprocity law to exclude some cases. Indeed, if E is an elliptic curve defined over $\mathbb{F}_p$ with $p \geqslant 5$ a prime, then we easily see that the possible factorisation patterns of ψ_3 are the following:

$((1,4))$
$((1,1),(3,1))$
$((2,2))$
$((1,2),(2,1))$
$((4,1))$.

But the quadratic reciprocity law combined with Pellet's theorem gives that when $p \equiv 1$ [3], then just the first, second and third factorisations are possible, while when $p \equiv 2$ [3], just the fourth and fifth factorisations are possible. In each case, all the probabilities are known except for one, so using the previous theorem, we get

Corollary 12

$P(((1,4)),3,1) = \frac{1}{12}$
$P(((1,1),(3,1)),3,1) = \frac{2}{3}$
$P(((2,2)),3,1) = \frac{1}{4}$
$P(((1,2),(2,1)),3,2) = \frac{1}{2}$
$P(((4,1)),3,2) = \frac{1}{2}$.

8.4 Conjecture

We will now give a conjecture a la Sato-Tate but in characteristic l concerning the distribution of the Frobenius endomorphisms. We will need some notation first.
Let l be an odd prime and $m \in \{1,\dots,l-1\}$. Then

$$\mathcal{G}_{l,m} = \{M \in GL_2(\mathbb{F}_l),\ Det(M) = m\}.$$

$GL_2(\mathbb{F}_l)$ acts on this set by conjugation and we denote by $\mathcal{H}_{l,m}$ the quotient set of this action. If $M \in \mathcal{G}_{l,m}$, then $[M]$ will denote its image in $\mathcal{H}_{l,m}$, and $\omega(M)$ the cardinality of the orbit of M.
Let E be an elliptic curve over $\mathbb{F}_p$ where $p > l$ is a prime congruent with m modulo l, and let φ be the Frobenius endomorphism. Let (P,Q) be a basis of $E[l]$. Then we get a matrix M_φ of the endomorphism $\varphi \in End_{\mathbb{F}_l}(E[l])$ in this basis. M_φ is well defined up to conjugation and if E' is an elliptic curve

defined over $\mathbb{F}_p$ isomorphic to E over $\mathbb{F}_p$, then M_φ and $M_{\varphi'}$ are conjugate. So we get a well defined map

$$\begin{array}{c} \mathcal{E}_p \\ \Big\downarrow{\scriptstyle \phi} \\ \mathcal{H}_{l,m} \end{array}$$

defined by $\phi(E) = [M_\varphi]$.

Conjecture 1 *Let l be a fixed odd prime. Let $m \in \{1,\dots,l-1\}$. Let $p \in \mathcal{P}_{l,m}$. Let $M \in \mathcal{G}_{l,m}$. Then*

$$\#\phi^{-1}([M]) = 2p.\frac{\omega(M)}{l(l^2-1)} + \mathcal{O}(\sqrt{p}).$$

We have some evidence for this. First, a lot of computer computations were done, and this seems to be asymptotically true.
Moreover, using Lenstra and Howe's results, we can prove it for matrices similar to the following ones: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} l-1 & 0 \\ 0 & l-1 \end{bmatrix}$, $\begin{bmatrix} l-1 & 1 \\ 0 & l-1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix}$ and $\begin{bmatrix} l-1 & 0 \\ 0 & l-m \end{bmatrix}$, the last two ones for $m \neq 1, l-1$.
We remark that $\#\mathcal{G}_{l,m} = l(l^2-1)$. Then if we add the formula given in the conjecture over a set of representatives Ω of similar matrices, then we get

$$\begin{aligned} \sum_{M\in\Omega} \#\phi^{-1}([M]) &= \frac{2p}{l(l^2-1)} \sum_{M\in\Omega} \omega(M) + \mathcal{O}(\sqrt{p}) \\ &= \frac{2p}{l(l^2-1)} \#\mathcal{G}_{l,m} + \mathcal{O}(\sqrt{p}) \\ &= 2p + \mathcal{O}(\sqrt{p}) \end{aligned}$$

But we can also prove, using Honda's theorem, that for $p >> l$, the map ϕ is surjective, hence the left handside is equal to $\#\mathcal{E}_p$. So we find

$$\#\mathcal{E}_p \approx 2p,$$

which is known to be true.
If the conjecture is true, then we would get the following corollary. We need the following notation:

Let l be an odd prime, $m \in \{1,\dots,l-1\}$ and $n \in \mathbb{N}^*$. Then if it exists,

$$P_m(n) = \lim_{\substack{p \in \mathcal{P}_{l,m} \\ p \to +\infty}} \frac{\#\{E \text{ elliptic curve over } \mathbb{F}_p,\ [\mathbb{F}_p(E[l]) : \mathbb{F}_p] = n\}/_{\approx_{\mathbb{F}_p}}}{\#\mathcal{E}_p}.$$

Corollary 13 (conjectural) *Let l be an odd prime. Then*

$$P_1(3) = \begin{cases} \dfrac{1}{l-1} & if\ l \equiv 1\ [3] \\ \dfrac{1}{l+1} & if\ l \equiv 2\ [3] \end{cases}$$

$$P_1(4) = \begin{cases} \dfrac{1}{l-1} & if\ l \equiv 1\ [4] \\ \dfrac{1}{l+1} & if\ l \equiv 3\ [4] \end{cases}$$

$$P_1(l-1) = \frac{\varphi(l-1)}{2(l-1)}$$

$$P_1(l+1) = \frac{\varphi(l+1)}{2(l+1)}$$

Appendix A

Examples of factorisations

In this appendix, we give examples of division polynomials and their factorisation.

Factorisation of ψ_p illustrating theorem 20

Example 2 Consider the elliptic curve

$$E : y^2 = x^3 + x + 11$$

defined over $\mathbb{F}_{17}$. In this case, the 17-th division polynomial is

$$\begin{aligned}\psi_{17}(X) = &15X^{136} + 5X^{119} + 9X^{102} + 6X^{85} + 9X^{68} \\ &+ 12X^{51} + 16X^{34} + 5X^{17} + 1.\end{aligned}$$

We see that the trace of the Frobenius is $t = 15$ in $\mathbb{F}_{17}$ which is to say that $t = -2$ in $\mathbb{Z}$, because of Hasse's theorem. We also have that $ord_{\mathbb{F}_{17}^*}(15) = 8$. The factorisation of $\psi_{17}(X)$ over $\mathbb{F}_{17}$ is:

$$\psi_{17}(X) = 15(X^4+11X^3+8X+13)^{17}(X^4+12X^3+8X^2+3X+15)^{17}.$$

Factorisation of ψ_l illustrating lemma 11 when α and β are odd

Example 3 Consider the elliptic curve

$$E : y^2 = x^3 + 8x + 7$$

defined over $\mathbb{F}_{11}$. In this case, the 7-th division polynomial is

$$\begin{aligned}\psi_7(X) = &7X^{24} + 9X^{21} + X^{20} + 9X^{19} + 5X^{18} + 9X^{17} + 2X^{16} + 5X^{15} \\ &+ 8X^{14} + 6X^{13} + 5X^{12} + 6X^{11} + 3X^9 + 10X^7 + 6X^6 + 2X^5 \\ &+ 8X^3 + 4X^2 + 6X + 10.\end{aligned}$$

We have $\alpha = 1$ and $\beta = 3$. The factorisation of $\psi_7(X)$ over $\mathbb{F}_{11}$ is

$$\begin{aligned}\psi_7(X) = &7(X+2)(X+9)(X+10)(X^3+3X+9)(X^3+2X^2+X+9) \\ &(X^3+4X^2+6X+5)(X^3+5X^2+2X+7) \\ &(X^3+7X^2+4X+4)(X^3+8X^2+1)(X^3+8X^2+6X+2).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 11 when α is odd and β is even

Example 4 Consider the elliptic curve

$$E : y^2 = x^3 + x + 4$$

defined over $\mathbb{F}_{29}$. In this case, the 11-th division polynomial is

$$\begin{aligned}\psi_{11}(X) = &11X^{60} + 10X^{58} + 17X^{57} + 7X^{56} + 20X^{55} + 26X^{54} + 18X^{53} \\ &+ 9X^{52} + 26X^{51} + 12X^{50} + 20X^{49} + 25X^{48} + 28X^{47} + 12X^{46} \\ &+ 19X^{45}2X^{44} + 28X^{43} + 5X^{42} + 25X^{41} + 2X^{40} + 10X^{39} \\ &+ 18X^{38} + 9X^{37} + 25X^{36} + 17X^{35} + 16X^{34} + 28X^{33} + 5X^{32} \\ &+ 18X^{31} + 24X^{29} + 9X^{28} + 23X^{27} + 14X^{26} + 9X^{25} + 12X^{24} \\ &+ 14X^{23} + 14X^{22} + 9X^{20} + 23X^{19} + 21X^{18} + 8X^{17} + X^{16} \\ &+ 14X^{15} + 26X^{14} + 25X^{13} + 6X^{12} + 9X^{11} + 13X^{10} + 25X^9 \\ &+ 20X^8 + 27X^7 + 24X^6 + 15X^4 + 10X^3 + 9X^2 + 7X + 23.\end{aligned}$$

We have $\alpha = 1$ and $\beta = 10$. The factorisation of $\psi_{11}(X)$ over $\mathbb{F}_{29}$ is

$$\begin{aligned}\psi_{11}(X) = &11(X+2)(X+14)(X+17)(X+19)(X+26) \\ &(X^5+18X^4+14X^3+12X^2+5X+6) \\ &(X^{10}+15X^8+25X^7+9X^6+22X^5+11X^4+7X^3+X^2+7X+11) \\ &(X^{10}+7X^9+21X^8+10X^7+14X^6+24X^5+23X^4+25X^3+28X^2+25X+17) \\ &(X^{10}+7X^9+21X^8+11X^7+19X^6+6X^5+27X^4+16X^3+14X^2+8X+9) \\ &(X^{10}+7X^9+21X^8+18X^7+X^6+23X^5+28X^4+26X^3+22X^2+18X+24) \\ &(X^{10}+28X^9+X^8+13X^7+24X^6+19X^5+22X^4+13X^3+26X^2+15X+4).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 11 when α is even and β is odd

Example 5 Consider the elliptic curve

$$E : y^2 = x^3 + x + 5$$

defined over $\mathbb{F}_{17}$. In this case, the 7-th division polynomial is

$$\begin{aligned}\psi_7(X) = {} & 7X^{24} + 2X^{22} + 4X^{20} + X^{19} + 15X^{18} + 2X^{17} + 6X^{16} + 14X^{15} \\ & + 13X^{14} + X^{12} + 11X^{11} + 3X^{10} + 5X^8 + 16X^6 + 14X^5 \\ & + 10X^4 + 4X^3 + 4X^2 + 13X + 7.\end{aligned}$$

We have $\alpha = 2$ and $\beta = 3$. The factorisation of $\psi_7(X)$ over $\mathbb{F}_{17}$ is

$$\begin{aligned}\psi_7(X) = {} & (X+1)(X+8)(X+13)(X^3 + 9X^2 + 16X + 7) \\ & (X^6 + 11X^5 + 4X^4 + 9X^3 + 7X^2 + 14X + 13) \\ & (X^6 + 12X^5 + 5X^4 + 3X^3 + 12X^2 + 5X + 4) \\ & (X^6 + 14X^5 + 16X^4 + 13X^3 + 11X^2 + X + 11).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 11 when α and β are even

Example 6 Consider the elliptic curve

$$E : y^2 = x^3 + 8x + 4$$

defined over $\mathbb{F}_{11}$. In this case, the 7-th division polynomial is

$$\begin{aligned}\psi_7(X) = {} & 7X^{24} + 2X^{21} + X^{20} + 2X^{19} + 5X^{18} + 2X^{17} + 2X^{16} + 6X^{15} \\ & + 8X^{14} + 5X^{13} + 5X^{12} + 5X^{11} + 8X^9 + X^7 + 6X^6 + 9X^5 \\ & + 3X^3 + 4X^2 + 5X + 10.\end{aligned}$$

We have $\alpha = 2$ and $\beta = 6$. The factorisation of $\psi_7(X)$ over $\mathbb{F}_{11}$ is

$$\begin{aligned}\psi_7(X) = {} & (X+1)(X+2)(X+9)(X^3 + 3X + 2)(X^3 + 3X^2 + 10) \\ & (X^3 + 3X^2 + 6X + 9)(X^3 + 4X^2 + 4X + 7)(X^3 + 6X^2 + 2X + 4) \\ & (X^3 + 7X^2 + 6X + 6)(X^3 + 9X^2 + X + 2).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 12 when α is odd

Example 7 Consider the elliptic curve

$$E : y^2 = x^3 + x + 10$$

defined over $\mathbb{F}_{29}$. In this case, the 7-th division polynomial is

$$\begin{aligned}\psi_7(X) = {} & 7X^{24} + 18X^{22} + 4X^{20} + 11X^{19} + 6X^{18} + 21X^{16} + 24X^{15} \\ & + 8X^{14} + 13X^{12} + 10X^{11} + 3X^{10} + 8X^9 + 17X^8 + 24X^7 \\ & + 2X^6 + X^5 + 14X^4 + 24X^3 + 21X^2 + 23X + 9.\end{aligned}$$

We have $\alpha = 1$. The factorisation of $\psi_7(X)$ over $\mathbb{F}_{29}$ is

$$\begin{aligned}\psi_7(X) = {} & 7(X+3)(X+24)(X+27) \\ & (X^7 + 19X^5 + 12X^4 + 25X^3 + 3X^2 + 10X + 20) \\ & (X^7 + 6X^6 + 5X^4 + 14X^3 + 14X^2 + 23X + 26) \\ & (X^7 + 27X^6 + 6X^5 + 24X^4 + 19X^3 + 9X^2 + 25X + 18).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 12 when α is even

Example 8 Consider the elliptic curve

$$E : y^2 = x^3 + 3x + 20$$

defined over $\mathbb{F}_{29}$. In this case, the 7-th division polynomial is

$$\begin{aligned}\psi_7(X) = {} & 7X^{24} + 25X^{22} + 7X^{20} + 8X^{19} + 4X^{18} + 6X^{16} + 27X^{15} \\ & + 5X^{14} + 8X^{13} + 19X^{12} + 2X^{11} + 21X^{10} + 26X^9 + 22X^8 \\ & + 8X^7 + 24X^6 + 14X^5 + 14X^4 + 3X^3 + 5X^2 + 16X + 12.\end{aligned}$$

We have $\alpha = 2$. The factorisation of $\psi_7(X)$ over $\mathbb{F}_{29}$ is

$$\begin{aligned}\psi_7(X) = {} & (X+11)(X+14) \\ & (X+18)(X^7 + 18X^5 + 26X^4 + 23X^3 + 20X^2 + 26X + 13) \\ & (X^7 + 18X^6 + 10X^4 + 19X^2 + 11X + 24) \\ & (X^7 + 26X^6 + 21X^5 + 19X^4 + 22X^3 + 25X^2 + 14X + 16).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 13 when α is odd

Example 9 Consider the elliptic curve

$$E : y^2 = x^3 + x + 6$$

defined over $\mathbb{F}_{29}$. In this case, the 7-th division polynomial is

$$\begin{aligned}\psi_7(X) = 7X^{24} + 18X^{22} + 4X^{20} + 24X^{19} + 7X^{18} + 2X^{16} + 10X^{15} + 4X^{14} \\ + 16X^{13} + 20X^{12} + 25X^{11} + 6X^{10} + 14X^9 + 13X^8 + 14X^7 + 20X^6 \\ + 19X^5 + 13X^4 + 8X^3 + 27X^2 + X + 10.\end{aligned}$$

We have $\alpha = 3$. The factorisation of $\psi_7(X)$ over $\mathbb{F}_{29}$ is

$$\begin{aligned}\psi_7(X) = 7(X^3 + X + 22)(X^3 + 5X^2 + 9X + 15) \\ (X^3 + 13X^2 + 27X + 19)(X^3 + 16X^2 + 3X + 26) \\ (X^3 + 16X^2 + 7X + 12)(X^3 + 20X^2 + 18X + 2) \\ (X^3 + 22X^2 + 17X + 1)(X^3 + 24X^2 + X + 6).\end{aligned}$$

Factorisation of ψ_l illustrating lemma 13 when α is even

Example 10 Consider the elliptic curve

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

defined over $\mathbb{F}_{29}$. In this case, the 11-th division polynomial is

$$\begin{aligned}\psi_{11}(X) = 11X^{60} + 10X^{58} + 20X^{57} + 7X^{56} + 15X^{55} + 7X^{54} + 28X^{53} + 17X^{52} \\ + 20X^{51} + 19X^{50} + 6X^{49} + 11X^{48} + 18X^{47} + 5X^{46} + 28X^{45} + 7X^{44} \\ + 21X^{43} + 17X^{42} + 14X^{40} + 6X^{39} + 15X^{38} + 19X^{37} + 2X^{36} + 2X^{35} \\ + 8X^{34} + 17X^{33} + 21X^{32} + 2X^{31} + 11X^{30} + 28X^{29} + 19X^{28} + 6X^{27} \\ + 7X^{26} + 27X^{25} + 12X^{24} + 9X^{23} + 27X^{22} + X^{21} + X^{20} + 14X^{19} \\ + 14X^{18} + 16X^{17} + 20X^{16} + 6X^{15} + 25X^{14} + 23X^{13} + 7X^{12} + 4X^{11} \\ + 17X^{10} + 5X^9 + 15X^8 + 17X^7 + 5X^6 + 5X^5 + 21X^4 + 2X^3 + 3X^2 \\ + 15X + 6.\end{aligned}$$

We have $\alpha = 40$.The factorisation of $\psi_{11}(X)$ over $\mathbb{F}_{29}$ is

$$\begin{aligned}\psi_{11}(X) = (X^{20} + 12X^{19} + 23X^{18} + 27X^{17} + 23X^{16} + 23X^{15} + 9X^{14} + 5X^{13} \\ + 6X^{12} + X^{11} + 9X^{10} + 16X^9 + 6X^8 + 12X^7 + 17X^6 + 2X^5 + 5X^4 \\ + 24X^3 + 3X^2 + 24X + 16) \\ (X^{20} + 21X^{19} + 3X^{18} + 13X^{17} + 9X^{16} + X^{15} + 23X^{14} + 21X^{13} \\ + 9X^{12} + 22X^{10} + 27X^9 + 19X^8 + 28X^7 + 26X^6 + 28X^5 + 27X^4 \\ + 7X^3 + 5X^2 + 8X + 24) \\ (X^{20} + 25X^{19} + 21X^{18} + 20X^{17} + 16X^{16} + 22X^{15} + 22X^{14} + 28X^{13} \\ + 5X^{12} + 18X^{11} + 3X^{10} + 2X^9 + 9X^8 + 12X^7 + X^6 + 28X^5 + 24X^4 \\ + 26X^3 + 11X^2 + 17X + 11).\end{aligned}$$

Appendix B

Numerical examples for the conjecture

We gather here some numerical examples that illustrate the conjecture 1 page 91 and its corollary 13 page 92. All computations were done in Laboratoire d'informatique de l'École Polytechnique during the fall 2002. Magma was used for that purpose.

B.1 The conjecture

We just give two examples, namely for $l = 5$ and $l = 7$, and we gather everything in a table for each prime. We explain the significance of the rows:

representatives We find for any residue $r \in \mathbb{F}_l^*$, a list of representatives of conjugacy classes of 2×2 matrices over $\mathbb{F}_l$ of determinant r,

theoretical ratio We compute for any matrice in the above list the quotient of the cardinality of its orbit by the set of all matrices of determinant r (this is the $\frac{\omega(M)}{l(l^2-1)}$ of the conjecture).

numerical ratio For any odd prime $p < 15000$ congruent to r, and for any isomorphism class of elliptic curves defined over $\mathbb{F}_p$, we compute the conjugacy class of the action of the Frobenius on l-torsion points. We then do the total arithmetical mean.

difference This last line is just the difference between the theoretical and arithmetical ratios.

$l = 5$

$\underline{r = 1}$

representatives	$\begin{bmatrix}2&2\\0&3\end{bmatrix}$	$\begin{bmatrix}3&3\\2&4\end{bmatrix}$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}3&4\\2&3\end{bmatrix}$	$\begin{bmatrix}4&0\\0&4\end{bmatrix}$	$\begin{bmatrix}2&4\\4&1\end{bmatrix}$	$\begin{bmatrix}4&1\\4&0\end{bmatrix}$
theoretical ratio	25%	20%	0,8333%	16,6667%	0,8333%	20%	16,6667%
numerical ratio	25,0183%	19,9885%	0,8357%	16,6666%	0,8357%	19,9885%	16,6665%
difference	−0,0183%	0,0115%	−0,0024%	0,0001%	−0,0024%	0,0115%	0,0001%

$\underline{r = 2}$

representatives	$\begin{bmatrix}3&1\\3&0\end{bmatrix}$	$\begin{bmatrix}3&0\\1&4\end{bmatrix}$	$\begin{bmatrix}1&3\\2&3\end{bmatrix}$	$\begin{bmatrix}4&4\\3&1\end{bmatrix}$	$\begin{bmatrix}4&3\\2&2\end{bmatrix}$
theoretical ratio	25%	25%	16,6667%	16,6667%	16,6667%
numerical ratio	24,9894%	24,9894%	16,6667%	16,6879%	16,6667%
difference	0,0106%	0,0106%	−0,0000%	−0,0212%	−0,0001%

$\underline{r = 3}$

representatives	$\begin{bmatrix}1&1\\1&4\end{bmatrix}$	$\begin{bmatrix}3&0\\0&1\end{bmatrix}$	$\begin{bmatrix}2&2\\1&0\end{bmatrix}$	$\begin{bmatrix}4&3\\1&4\end{bmatrix}$	$\begin{bmatrix}4&0\\1&2\end{bmatrix}$
theoretical ratio	16,6667%	25%	16,6667%	16,6667%	25%
numerical ratio	16,6882%	24,9892%	16,6667%	16,6667%	24,9892%
difference	−0,0215%	0,0108%	−0,0000%	−0,0000%	0,0108%

$\underline{r = 4}$

representatives	$\begin{bmatrix}3&4\\4&0\end{bmatrix}$	$\begin{bmatrix}3&0\\0&3\end{bmatrix}$	$\begin{bmatrix}2&0\\0&2\end{bmatrix}$	$\begin{bmatrix}1&1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&1\\1&4\end{bmatrix}$	$\begin{bmatrix}2&1\\2&3\end{bmatrix}$	$\begin{bmatrix}3&1\\3&4\end{bmatrix}$
theoretical ratio	16,6667%	0,8333%	0,8333%	20%	20%	25%	16,6667%
numerical ratio	16,6665%	0,8371%	0,8371%	19,9943%	19,9943%	25,0040%	16,6665%
difference	0,0002%	−0,0038%	−0,0038%	0,0057%	0,0057%	−0,0040%	0,0002%

$l = 7$

$\underline{r = 1}$

representatives	$\begin{bmatrix}6&1\\6&0\end{bmatrix}$	$\begin{bmatrix}2&2\\6&3\end{bmatrix}$	$\begin{bmatrix}6&2\\1&4\end{bmatrix}$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}6&0\\0&6\end{bmatrix}$	$\begin{bmatrix}0&2\\3&0\end{bmatrix}$	$\begin{bmatrix}6&3\\6&2\end{bmatrix}$	$\begin{bmatrix}2&6\\4&2\end{bmatrix}$	$\begin{bmatrix}4&2\\6&5\end{bmatrix}$
theoretical ratio	16, 6667%	14, 2857%	12, 5%	0, 2976%	0, 2976%	12, 5%	16, 6667%	12, 5%	14, 2857%
numerical ratio	16, 6666%	14, 2764%	12, 4968%	0, 2997%	0, 2997%	12, 5212%	16, 6666%	12, 4968%	14, 2764%
difference	0, 0001%	0, 0093%	0, 0032%	−0, 0021%	−0, 0021%	−0, 0212%	0, 0001%	0, 0032%	0, 0093%

$\underline{r = 2}$

representatives	$\begin{bmatrix}2&0\\0&1\end{bmatrix}$	$\begin{bmatrix}5&1\\5&0\end{bmatrix}$	$\begin{bmatrix}3&0\\0&3\end{bmatrix}$	$\begin{bmatrix}5&6\\1&3\end{bmatrix}$	$\begin{bmatrix}5&0\\3&6\end{bmatrix}$	$\begin{bmatrix}4&0\\0&4\end{bmatrix}$	$\begin{bmatrix}4&1\\4&5\end{bmatrix}$	$\begin{bmatrix}1&5\\2&5\end{bmatrix}$	$\begin{bmatrix}6&6\\3&1\end{bmatrix}$
theoretical ratio	16, 6667%	12, 5%	0, 2976%	14, 2857%	16, 6667%	0, 2976%	12, 5%	14, 2857%	12, 5%
numerical ratio	16, 6595%	12, 4902%	0, 3001%	14, 2862%	16, 6595%	0, 3001%	12, 4902%	14, 2862%	12, 5281%
difference	0, 0072%	0, 0098%	−0, 0025%	−0, 0005%	0, 0072%	−0, 0025%	0, 0098%	−0, 0005%	−0, 0281%

$\underline{r = 3}$

representatives	$\begin{bmatrix}4&1\\4&0\end{bmatrix}$	$\begin{bmatrix}0&4\\1&6\end{bmatrix}$	$\begin{bmatrix}5&6\\6&5\end{bmatrix}$	$\begin{bmatrix}6&6\\5&2\end{bmatrix}$	$\begin{bmatrix}3&3\\5&6\end{bmatrix}$	$\begin{bmatrix}6&4\\3&6\end{bmatrix}$	$\begin{bmatrix}4&6\\5&3\end{bmatrix}$
theoretical ratio	16, 6667%	12, 5%	16, 6667%	12, 5%	12, 5%	12, 5%	16, 6667%
numerical ratio	16, 6595%	12, 4982%	16, 6595%	12, 4982%	12, 4982%	12, 4982%	16, 6881%
difference	0, 0072%	0, 0018%	0, 0072%	0, 0018%	0, 0018%	0, 0018%	−0, 0214%

$\underline{r = 4}$

representatives	$\begin{bmatrix}5&0\\0&5\end{bmatrix}$	$\begin{bmatrix}1&3\\6&1\end{bmatrix}$	$\begin{bmatrix}3&5\\5&5\end{bmatrix}$	$\begin{bmatrix}3&3\\1&0\end{bmatrix}$	$\begin{bmatrix}4&0\\0&1\end{bmatrix}$	$\begin{bmatrix}1&2\\3&3\end{bmatrix}$	$\begin{bmatrix}2&0\\0&2\end{bmatrix}$	$\begin{bmatrix}2&1\\6&5\end{bmatrix}$	$\begin{bmatrix}0&3\\1&6\end{bmatrix}$
theoretical ratio	0, 2976%	16, 6667%	12, 5%	14, 2857%	16, 6667%	14, 2857%	0, 2976%	12, 5%	12, 5%
numerical ratio	0, 3007%	16, 6595%	12, 4974%	14, 2821%	16, 6595%	14, 2821%	0, 3007%	12, 5207%	12, 4974%
difference	−0, 0031%	0, 0072%	0, 0026%	0, 0036%	0, 0072%	0, 0036%	−0, 0031%	−0, 0207%	0, 0026%

$\underline{r = 5}$

representatives	$\begin{bmatrix}4&5\\1&6\end{bmatrix}$	$\begin{bmatrix}5&0\\0&1\end{bmatrix}$	$\begin{bmatrix}4&0\\6&3\end{bmatrix}$	$\begin{bmatrix}3&6\\6&2\end{bmatrix}$	$\begin{bmatrix}2&2\\1&0\end{bmatrix}$	$\begin{bmatrix}6&3\\6&5\end{bmatrix}$	$\begin{bmatrix}2&1\\0&6\end{bmatrix}$
theoretical ratio	12, 5%	16, 6667%	16, 6667%	12, 5%	12, 5%	12, 5%	16, 6667%
numerical ratio	12, 4982%	16, 6594%	16, 6883%	12, 4982%	12, 4982%	12, 4982%	16, 6594%
difference	0, 0018%	0, 0073%	−0, 0216%	0, 0018%	0, 0018%	0, 0018%	0, 0073%

$\underline{r = 6}$

representatives	$\begin{bmatrix}6&0\\0&1\end{bmatrix}$	$\begin{bmatrix}5&4\\6&6\end{bmatrix}$	$\begin{bmatrix}5&1\\5&5\end{bmatrix}$	$\begin{bmatrix}5&5\\0&4\end{bmatrix}$	$\begin{bmatrix}0&1\\1&6\end{bmatrix}$	$\begin{bmatrix}2&0\\3&3\end{bmatrix}$	$\begin{bmatrix}1&1\\1&0\end{bmatrix}$
theoretical ratio	16, 6667%	12, 5%	12, 5%	16, 6667%	12, 5%	16, 6667%	12, 5%
numerical ratio	16, 6737%	12, 4982%	12, 4982%	16, 6667%	12, 4982%	16, 6667%	12, 4982%
difference	−0, 0070%	0, 0018%	0, 0018%	0, 0000%	0, 0018%	0, 0000%	0, 0018%

B.2 The corollary

We give here some examples that the corollary of the conjecture holds numerically. The results of the computations are gathered in four tables, each corresponding to a case α of the corollary. The tables are organized in the following way:

First column The prime l which is tested,

Second column It corresponds to an integer M such that for any prime $p < M$ and which is congruent to 1 modulo l, we have taken all the classes of isomorphisms of elliptic curves E defined over $\mathbb{F}_p$ and taken into account those which are such that the degree $[\mathbb{F}_p(E[l]) : \mathbb{F}_p] = \alpha$,

Third column This is the ratio of the number of curves found as we have just said divided by the total number of curves,

Fourth column This is the expected ratio we should get if the conjecture is true,

Fifth column This is the difference between the theoretical ratio and the numerical ratio.

$\alpha = 3$

l	M	numerical ratio	theoretical ratio	difference
5	50000	16,6789%	1/6	0,0122%
7	50000	16,6757%	1/6	0,0091%
11	25000	8,3231%	1/12	0,0102%
13	50000	8,3393%	1/12	0,0060%
17	50000	5,5641%	1/18	0,0085%
19	50000	5,5590%	1/18	0,0035%
23	20000	4,1571%	1/24	0,0096%
37	50000	2,7662%	1/36	0,0116%
43	15000	2,3686%	1/42	0.0124%
47	50000	2,0827%	1/48	0,0006%
59	50000	1,6639%	1/60	0,0027%
83	50000	1,1895%	1/84	0,0010%
107	25000	0,8762%	1/108	0,0497%
227	100000	0,4197%	1/228	0,0189%
347	100000	0,2656%	1/348	0,0218%
563	250000	0,1615%	1/564	0,0158%

$\alpha = 4$

l	M	numerical ratio	theoretical ratio	difference
5	50000	24,9769%	1/4	0,0231%
7	50000	12,4818%	1/8	0,0182%
11	25000	8,2921%	1/12	0,0412%
13	50000	8,3204%	1/12	0,0129%
17	50000	6,2369%	1/16	0,0131%
19	50000	5,0013%	1/20	0,0013%
23	20000	4,1847%	1/24	0,0180%
37	50000	2,7905%	1/36	0,0127%
43	15000	2,3531%	1/42	0,0278%
47	50000	2,0967%	1/46	0,0772%
59	50000	1,6437%	1/60	0,0230%
83	50000	1,2141%	1/82	0,0055%
107	25000	1,0813%	1/108	0,1553%
227	100000	0,4603%	1/228	0,0217%
347	100000	0,4046%	1/348	0,1173%
563	250000	0,2358%	1/564	0,1430%

$\alpha = l - 1$

l	M	numerical ratio	theoretical ratio	difference
5	50000	24,9769%	$1/4 = 2/8$	0,0231%
7	50000	16,6757%	$1/6 = 2/12$	0,0091%
11	25000	20,0324%	$1/5 = 4/20$	0,0324%
13	50000	16,6609%	$1/6 = 4/24$	0,0057%
17	50000	25,0105%	$1/4 = 8/32$	0,0105%
19	50000	16,6693%	$1/6 = 6/36$	0,0026%
23	20000	22,7378%	$5/22 = 10/44$	0,0105%
37	50000	16,6884%	$1/6 = 12/72$	0,0217%
43	15000	14,2784%	$1/7 = 12/84$	0,0073%
47	50000	23,9865%	$11/46 = 22/92$	0,0734%
59	50000	24,1200%	$7/29 = 28/116$	0.0179%
83	50000	24,2985%	$10/41 = 40/164$	0,0918%
107	25000	24,7755%	$13/53 = 52/212$	0,2472%
227	100000	24,7224%	$28/113 = 112/452$	0,0564%
347	100000	25,2346%	$43/173 = 172/692$	0,3791%

$$\alpha = l + 1$$

l	M	numerical ratio	theoretical ratio	difference
5	50000	$16,6789\%$	$1/6 = 2/12$	$0,0122\%$
7	50000	$25,0072\%$	$1/4 = 4/16$	$0,0072\%$
11	25000	$16,6952\%$	$1/6 = 4/24$	$0,0285\%$
13	50000	$21,4497\%$	$3/14 = 6/28$	$0,0211\%$
17	50000	$16,6679\%$	$1/6 = 6/36$	$0,0012\%$
19	50000	$20,1058\%$	$2/10 = 8/40$	$0,1058\%$
23	20000	$16,7165\%$	$1/6 = 8/48$	$0,04988\%$
37	50000	$23,7027\%$	$9/38 = 18/76$	$0,0185\%$
43	15000	$22,7077\%$	$5/22 = 20/88$	$0,0196\%$
47	50000	$16,6823\%$	$1/6 = 16/96$	$0,0156\%$
59	50000	$13,4139\%$	$2/15 = 16/120$	$0,0805\%$
83	50000	$14,4283\%$	$1/7 = 24/168$	$0,1426\%$
107	25000	$16,3816\%$	$1/6 = 36/216$	$0,2851\%$
227	100000	$15,8363\%$	$3/19 = 72/456$	$0,0468\%$
347	100000	$15,8676\%$	$14/87 = 112/696$	$0,2244\%$

Bibliography

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Perseus books, 1969.

[Bir68] B.J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *Journal of the London Mathematical Society*, 43:57–60, 1968.

[BK98] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology*, 11:141–145, 1998.

[BSS00] I. Blake, G. Seroussi, and N. Smart. *Elliptic curves in cryptography*. Cambridge University Press, 2000.

[Cai02] C. Cailler. Sur les congruences du troisième degré. *L'enseignement mathématique*, 10:474–487, 1902.

[Car67] L. Carlitz. A note on irreducible cubics. *Det kongelige norske videnskabers selskabs forhandlinger*, 40(5):25–30, 1967.

[Car70] P. Cartier. Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques. *Actes du Congrès International des Mathématiciens*, 2:291–299, 1970.

[Cas49] J.W.S. Cassels. A note on the division values of $\wp(u)$. *Proceedings of the Cambridge philosophical society*, 45:167–172, 1949.

[Cas66] J.W.S. Cassels. Diophantine equations with special reference to elliptic curves. *Journal of the London mathematical society*, 41:193–291, 1966.

[Cas72] J.W.S. Cassels. Corrigendum, a note on the division values of $\wp(u)$. In *Proceedings of the Cambridge philosophical society* [Cas49], page 431.

[Cas95] J.W.S. Cassels. *Lectures on elliptic curves*. Cambridge University Press, 1995.

[CH96] J. Cheon and S. Hahn. Division polynomials of elliptic curves over finite fields. *Proceedings of the japan academy*, 72(Serie A):226–227, 1996.

[CM94] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In *ANTS I*, volume 877 of *Lecture notes in computer science*, pages 43–58. Springer-Verlag, 1994.

[Cou96] J.-M. Couveignes. Computing l-isogenies using the p-torsion. In *ANTS II*, volume 1122 of *Lecture notes in computer science*, pages 59–65. Springer-Verlag, 1996.

[Cox89] D.A. Cox. *Primes of the form x^2+ny^2*. John Wiley & sons, inc., 1989.

[CP01] J.J. Cannon and C. Playoust. *An introduction to algebraic programming with Magma*. Springer-Verlag, 2001.

[Del69] P. Deligne. Variétés abéliennes ordinaires sur un corps fini. *Inventiones Mathematicae*, 8:238–243, 1969.

[Deu41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionkörper. *Abhandlungen Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[Dew98] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Mathematics of computation*, 67(223):1247–1252, 1998.

[Dew99] L. Dewaghe. Isogénie entre courbes elliptiques. *Utilitas Mathematica*, 55:123–127, 1999.

[DH98] S. DiPippo and E. Howe. Real polynomials with all roots on the unit circle and abelian varieties over finite fields. *Journal of number Theory*, 73:426–450, 1998.

[Die73] J. Dieudonné. *Introduction to the theory of formal groups*. Marcel Dekker, Inc., 1973.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, volume 349 of *Lecture notes in mathematics*, pages 143–316. Springer-Verlag, 1973.

[Elk95] N.D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory, proceedings of a conference in honor of A.O.L. Atkin*, volume 7 of *Studies in advanced mathematics*, pages 21–76. AMS/IP, 1995.

[Frö68] A. Fröhlich. *Formal groups*. Number Lecture notes in mathematics 74 in Lecture notes in mathematics. Springer-Verlag, 1968.

[Fri72a] R: Fricke. *Die elliptischen Funktionen une ihre Anwendungen - erster Teil*. Johnson Reprint Corporation, 1972.

[Fri72b] R: Fricke. *Die elliptischen Funktionen une ihre Anwendungen - zweiter Teil*. Johnson Reprint Corporation, 1972.

[Har77] R. Hartshorne. *Algebraic geometry*. Number 52 in Graduate texts in mathematics. Springer-Verlag, 1977.

[Haz78] M. Hazewinkel. *Formal groups and applications*. Academic Press, 1978.

[Hon68a] T. Honda. Formal groups and zeta-functions. *Osaka journal of mathematics*, 5:199–213, 1968.

[Hon68b] T. Honda. Isogeny of abelian varieties over finite fields. *Journal of the mathematical society of Japan*, 20(1–2):83–95, 1968.

[Hon70] T. Honda. On the theory of commutative formal groups. *Journal of the mathematical society of Japan*, 22:213–246, 1970.

[How93] E. Howe. On the group orders of elliptic curves over finite fields. *Composition Mathematica*, 85(2):229–247, 1993.

[Hus87] D. Husemöller. *Elliptic curves*. Number 111 in Graduate texts in mathematics. Springer-Verlag, 1987.

[HW60] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers*. Oxford at the Clarendon Press, fourth edition, 1960.

[Kal91] B.S. Kaliski. One-way permutation on elliptic curves. *Journal of cryptology*, 3(3):187–199, 1991.

[KM85] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. Number 108 in Annals of mathematical studies. Princeton University Press, 1985.

[Kob87a] N. Koblitz. *A course in number theory and cryptography*. Number 114 in Graduate texts in mathematics. Springer-Verlag, 1987.

[Kob87b] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[Kob93] N. Koblitz. *Introduction to elliptic curves and modular forms*. Number 97 in Graduate texts in mathematics. Springer-Verlag, second edition, 1993.

[Koh96] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, fall 1996.

[Kub76] D.S. Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London mathematical society*, 33(2):193–237, 1976.

[Lan73] S. Lang. *Elliptic functions*. Addison-Wesley, 1973.

[Lan78] S. Lang. *Elliptic curves diophantine analysis*. Number 231 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1978.

[Lan94a] S. Lang. *Algebra*. Addison-Wesley, second edition, 1994.

[Lan94b] S. Lang. *Algebraic number theory*. Number 110 in Graduate texts in mathematics. Springer-Verlag, second edition, 1994.

[Len87] H.W.Jr Lenstra. Factoring integers with elliptic curves. *Annals of mathematics (2)*, 126(3):649–673, 1987.

[Lid83] R. Lidl. *Finite fields*, volume 20 of *Encyclopedia of mathematics and its applications*. Addison-Wesley, 1983.

[Man63] J.I. Manin. The theory of commutative formal groups over field of finite characteristic. *Russian mathematical surveys*, 18:1–84, 1963.

[MB+93] A.J. Menezes, , I.F. Blake, X. Gao, R.C. Mullin, S.A Vanstone, and T. Yaghoobian. *Applications of finite fields*. Kluwer Academic Publishers, 1993.

[McK94] J. McKee. Computing division polynomials. *Mathematics of computation*, 63(208):767–771, 1994.

[Men93] A.J. Menezes. *Elliptic curve public key cryptosystems*. Kluwer Academic Publishers, 1993.

[Mil68] J.S. Milne. Extensions of abelian varieties defined over a finite field. *Inventiones Mathematicae*, 5:63–84, 1968.

[Mil86] V.S. Miller. *Use of elliptic curves in cryptography*, pages 417–426. Number 218 in Lecture notes in computer science. Springer-Verlag, 1986.

[Mir07] D. Mirimanoff. Sur les congruences du troisième degré. *L'enseignement mathematique*, pages 381–384, 1907.

[Mor90] F. Morain. *Solving equations of small degree modulo large primes*. PhD thesis, Université de Lyon 1, sep. 1990. part of thesis.

[Mor91] F. Morain. Building cyclic elliptic curves modulo large primes. *Lecture notes in computer science*, 547:328–336, 1991.

[Mor95] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *Journal de théorie des nombres de Bordeaux*, 7:255–282, 1995.

[MOV93] A.J. Menezes, T. Okamoto, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE transactions in information theory*, 39(5):1639–1646, 1993.

[MS76] B. Mazur and J.P. Serre. *Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg)*, pages 238–255. Number 514 in Lecture notes in mathematics. Springer-Verlag, 1976.

[Mur99] V.K. Murty. Frobenius distributions and Galois representations. In *Automorphic forms, automorphic representations, and arithmetic*, pages 193–211, 1999.

[MvOV97] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of applied cryptography*. CRC Press, 1997.

[Nak97] T. Nakamura. On characteristic polynomials of formal groups over finite fields. *Matematische Nachrichten*, 188:289–299, 1997.

[Ogg73] A.P. Ogg. *Survey of modular functions of one variable*, pages 1–35. Number 320 in Lecture notes in mathematics. Springer-Verlag, 1973. Notes by F. van Oystaeyen.

[Olsa] L. Olson. Introduction to formal groups. Introductory lectures at the University of Bergen.

[Olsb] L. Olson. Notes on elliptic curves. Notes and examples.

[Ols75] L. Olson. Torsion points on elliptic curves with given j-invariant. *Manuscripta Mathematica*, 16(2):145–150, 1975.

[Ols79] L. Olson. The trace of Frobenius for elliptic curves with complex multiplication. In *Algebraic geometry, proccedings of summer meeting, University of Copenhagen, 1978*, number 732 in Lecture notes in mathematics, pages 454–476. Springer-Verlag, 1979.

[Pel78] A.E. Pellet. Sur la décomposition d'une fonction entière en facteurs irréductibles suivant un module premier p. *Comptes Rendus de l'Académie des Sciences de Paris*, 86:1071–1072, 1878.

[Per94] D. Perrin. *Cours d'algèbre*. Ecole Normale Superieure de Jeunes Filles, 1994.

[Per95] D. Perrin. *Géométrie algébrique*. InterÉditions/CNRS Éditions, 1995.

[Rib95] K. Ribet. Galois representations and modular forms. *Bulletin of the american mathematical society*, 32(4):375–402, 1995.

[SA98] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete logarithm for anomalous elliptic curves. *Comentarii Mathematici Universitatis Sancti Pauli*, 47(1):81–92, 1998.

[SA99] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete logarithm for anomalous elliptic curves, errata. *Comentarii Mathematici Universitatis Sancti Pauli*, 48(2):211–213, 1999.

[Sat] T. Satoh. Asymptotically fast algorithm for computing the Frobenius substitution and norms over unramified extension of p-adic number fields. unpublished preprint available at http://www.rimath.saitama-u.ac.jp/lab.en/TkkzSatoh/Preprint.html.

[Sch40] S. Schwarz. Sur le nombre des racines et des facteurs irréductibles d'une congruence donnée. *Casopis pro pestovani matematiky a fysiky*, 69:128–145, 1940.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44:483–494, 1985.

[Sch87] R. Schoof. Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory*, 46(Series A):183–211, 1987.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7:219–254, 1995.

[Sem98] I.A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Mathematics of Computation*, 67(221):353–356, 1998.

[Sem00] I.A. Semaev. Discrete log algorithm for special modulus. Conference ECC2000 in Essen, Oct 2000.

[Ser70] J.P. Serre. *p-torsion des courbes elliptiques (d'après Y. Manin)*, pages 281–294. Number 180 in Lecture notes in mathematics. Springer-Verlag, 1970.

[Ser72] J-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1972.

[Ser73] J.-P. Serre. *A course in arithmetic*. Number 7 in Graduate texts in mathematics. Springer-Verlag, 1973.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Graduate texts in mathematics. Princeton University Press, 1971.

[Sil86] J.H. Silverman. *The arithmetic of elliptic curves*. Number 106 in Graduate texts in mathematics. Springer-Verlag, 1986.

[Sil94] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Number 151 in Graduate texts in mathematics. Springer-Verlag, 1994.

[Skj] B. Skjernaa. Satoh's algorithm in characteristic 2. Available at http://home.imf.au.dk/skjernaa/.

[Sko37] T. Skolem. Zwei Sätze über kubische Kongruenzen. *Det kongelige norske videnskabers selskabs forhandlinger*, 10(24):89–92, 1937.

[Sko52a] T. Skolem. The general congruence of the 4th degree modulo p, p prime. *Norsk matematiske tidskrifter*, 34:73–80, 1952.

[Sko52b] T. Skolem. On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p. *Norsk matematiske tidskrifter*, 34:81–85, 1952.

[Sma99] N. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*, 12(3):193–196, 1999.

[ST] T. Satoh and Y. Taguchi. Computing zeta functions for ordinary formal groups over finite fields. unpublished preprint available at http://www.rimath.saitama-u.ac.jp/lab.en/TkkzSatoh/Preprint.html.

[ST92] J.H. Silverman and J. Tate. *Rational points on elliptic curves*. Springer-Verlag, 1992.

[Swa62] R.G. Swan. Factorization of polynomials over finite fields. *Pacific journal of mathematics*, 12:1099–1106, 1962.

[Tat66] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 2:134–144, 1966.

[Tat74] J. Tate. The arithmetic of elliptic curves. *Inventiones Mathematicae*, 23:179–206, 1974.

[Tau49] O. Taussky. On a theorem of Latimer and MacDuffee. *Canadian Journal of Mathematics*, 1:300–302, 1949.

[Vél71] J. Vélu. Isogénies entre courbes elliptiques. *Comptes rendus de l'académie des sciences de Paris*, 273(Série A):238–241, 1971.

[Vla99a] S.G. Vladut. Cyclicity statistics for elliptic curves over finite fields. *Finite fields and their applications*, 5(1):13–25, 1999.

[Vla99b] S.G. Vladut. On the cyclicity of elliptic curves over finite field extensions. *Finite fields and their applications*, 5(1):354–363, 1999.

[Vla01] S. Vladut. Isogeny class and Frobenius root statistics for abelian varieties over finite fields. *Moscow mathematical journal*, 1(1):125–139, 2001.

[Vola] J.F. Voloch. The discrete logarithm problem on elliptic curves and descent. Available at http://www.ma.utexas.edu/users/voloch/oldpreprint.html.

[Volb] J.F. Voloch. Relating the Smart-Satoh-Araki and Semaev approaches to the discrete logarithm problem on anomalous elliptic curves. Available at http://www.ma.utexas.edu/users/voloch/oldpreprint.html.

[Wal84] D.I. Wallace. Conjugacy classes of hyperbolic matrices in SL(n,$\mathbb{Z}$) and ideal classes in an order. *Transactions of the american mathematical society*, 283(1):177–184, 1984.

[Wat69] W. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École normale supérieure*, 2:521–560, 1969.

[Web95] H. Weber. *Lehrbuch der Algebra*. Braunschweig : Vieweg und Son, 1895.

[WM69] W.C. Waterhouse and J.S. Milne. Abelian varieties over finite fields. In *Proceedings of the symposium of pure mathematics, volume XX, 1969*, pages 53–64, 1969.

[Yos73] H. Yoshida. On an analogue of the Sato conjecture. *Inventiones Mathematicae*, 19:261–277, 1973.

[Yui78] N. Yui. Elliptic curves and canonical subgroups of formal groups. *Journal für die reine und angewandte Mathematik*, 303/304:319–331, 1978.

[Yui79] N. Yui. Formal groups and some arithmetic properties of elliptic curves. In *Algebraic geometry, proccedings of summer meeting, University of Copenhagen, 1978*, number 732 in Lecture notes in mathematics, pages 630–658. Springer-Verlag, 1979.