UAM (Madrid) May 2009

Point counting on elliptic curves

By
Christophe RITZENTHALER

Contents

Chapter 1

Introduction

1.1 The discrete logarithm problem

1.1.1 General setting

Cryptography is playing a more and more important role in our society : smart-card, INTERNET payment, online banking.... All these applications needs to protect information. There exists two main strategies. The first one, historically, is called *symmetric key cryptography*. Roughly speaking, it is based on combinatoric tricks and only the owners of the secret key can cipher and decipher. In 1976, Diffie and Hellman introduced the new concept of *public key cryptography*. This protocol solves in particular the important problem (for INTERNET) of creation of secret key over a non-secure channel (which was not possible with symmetric cryptography). Here is the principle :

1. Goal : Alice and Bob wants to share a secret key (to cipher and decipher later with a traditional symmetric protocol for instance).
2. let G be a cyclic group. Let $g \in G$ be a generator.
3. Alice chooses $a \in \mathbb{Z}$ and sends g^a to Bob.
4. Bob chooses $b \in \mathbb{Z}$ and sends g^b to Alice.
5. Secret shared : g^{ab}.

One sees that the difficulty to break the code is based on the difficulty to compute $a = \log_g(g^a)$ (in fact to compute g^{ab} knowing g^a, g^b but these two problems are believed equivalent and they are if $\#G$ is not divisible by the square of a large prime (Maurer and Wolf 99)). This type of problem is called *discrete logarithm problem*. Does it exist groups for which this problem is difficult (whereas the computation of g^a remains easy of course) ? A problem is said difficult if one cannot solve it in a reasonable time with a good computer. More specifically that means that the number of operations would be greater than 2^{60}.
For a general group G, there is always an attack in $\mathcal{O}(\sqrt{|G|})$ (the ρ-Pollard method),

so $|G|$ must have at least 120 bits.

Remark 1. The complexity of the attack –or of construction, computations– (exponential, subexponential, polynomial) is measured in term of $\log_2 |G|$.

One is of course interested in groups for which the order is small (and then the protocol fast) in other words groups with no subexponential attacks. This is not the case for $\mathbb{F}_{p^n}$ for which there is an attack in $L_{p^n}(1/3, (64/9)^{1/3})$ when n is small (NFS) and $L_{p^n}(1/3, (32/9)^{1/3})$ when p is small (FFS). Recall that

$$L_q(a, C) = \exp(C(\log q)^a (\log\log q)^{1-a}).$$

Another possible group is the group of rational points of a Jacobian over a finite fields.

1.1.2 Recall on curves over finite fields

In 1949, André Weil made a series of very general conjectures concerning the number of points on varieties defined over finite fields. We restrict here to the case of curves.
Let $k = \mathbb{F}_q$ and for all $n \geq 1$, let k_n be the extension of degree n of k. Let C/k be a (projective smooth) curve of genus g over k.

Definition 1.1.1. *The* Zeta function *of C over k is the power series*

$$Z(C/k; T) = \exp\left(\sum_{n=1}^{\infty} |C(k_n)| \frac{T^n}{n}\right).$$

Theorem 1.1.1 (Weil conjectures)**.** *With the above notations, we have the following properties.*

1. *Rationality :*
$$Z(C/k; T) \in \mathbb{Q}(T).$$

2. *Functional equation :*
$$Z(C/k; 1/(qT)) = (qT^2)^{1-g} Z(C/k; T).$$

3. *Riemann hypothesis :*
there exists a polynomial $f \in \mathbb{Z}[T]$ of degree $2g$ such that
$$f(T) = \prod_{i=1}^{2g} (1 - T\alpha_i)$$
with $|\alpha_i| = \sqrt{q}$ for all i and such that
$$Z(C/k; T) = \frac{f(T)}{(1-T)(1-qT)}.$$

Corollary 1.1.1. *We have* $|C(\mathbb{F}_{q^n})| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$.

Proof. We have

$$\begin{aligned} \log(Z(C/k;T) = \sum |C(k_n)|T^n/n &= \log(f(T)) - \log(1-T) - log(1-qT) \\ &= \sum \log(1-\alpha_i T) + \sum T^n/n + \sum q^n T^n/n \\ &= \sum_n \left(-\sum_i (\alpha_i^n) + 1 + q^n \right) T^n/n \end{aligned}$$

□

If we particularize to the case of elliptic curves ($g = 1$).

Theorem 1.1.2. *Let k be a field with q elements and E/k be an elliptic curve. Then there is an $a \in \mathbb{Z}$ (called* the trace *of E/k) such that*

$$Z(E/k;T) = \frac{1 - aT + qT}{(1-T)(1-qT)}$$

Further $Z(E:k;1/qT) = Z(E/k;T)$ and

$$1 - aT + qT^2 = (1-\alpha T)(1-\beta T) \text{ with } |\alpha| = |\beta| = \sqrt{q}.$$

Corollary 1.1.2. *With the notations above, there exists a polynomial (called the* Frobenius polynomial *of E/k)*

$$\chi := T^2 - aT + q = (T-\alpha)(T-\beta)$$

such that $|E(k)| = \chi(1)$ and for every extension k_n of k of degree n, $|E(k_n)| = (1 - \alpha^n)(1-\beta^n)$.
Moreover (Hasse-Weil bound)

$$||E(k)| - q - 1| \leq 2\sqrt{q}.$$

Example 1. *Consider the elliptic curve : $E/\mathbb{F}_7 : y^2 = x^3 + 2$. It has 9 rational points, namely $(0:1:0), (0:3:1), (0:4:1), (3:1:1), (3:6:1), (5:1:1), (5:6:1), (6:1:1), (6:6:1)$. So we must have*

$$Z(E/\mathbb{F}_7;T) = \frac{7T^2 + T + 1}{(1-T)(1-7T)}.$$

In particular the number of points of $E/\mathbb{F}_{49}$ is $1 + 49 - (1^2 - 2 \cdot 7) = 63$ (which can be checked with a computer).

These conjectures were solved by Weil (in the case of curves and abelian varieties). The general case was solved by Deligne in 1973.

1.1.3 Discrete logarithm problem in the Jacobian of curves

Jacobian have a certain dimension g and their number of points over $\mathbb{F}_q$ is approximately q^g. In order to have fast operations, it is good to have q as small as possible and so g has to be big. However, attacks become more powerful for large g as the following table giving the complexity of the best index calculus attack shows

	$g=1$	$g=2$	$g=3$	$g=4$
Generic $\sqrt{q^g}$	$q^{1/2}$	q	$q^{3/2}$	q^2
Index calculus (2000)	-	-	q^2	q^2
Reduced basis (2000)	-	-	$q^{3/2}$	$q^{8/5}$
Single large prime (2003)	-	-	$q^{10/7}$	$q^{14/9}$
Double large prime (2005)	-	-	$q^{4/3}$	$q^{3/2}$
Low degree (2006)	-	-	q	

Moreover, asymptotically, Enge and Gaudry showed that if $g/\log q \to \infty$ then the complexity is $L_{q^g}(\frac{1}{2}, C)$. Recently (2009), Enge-Gaudry and Thom have announced a $L_{q^g}(\frac{1}{3}, C)$ for low degree curves.

Hence what is left today is more or less $g = 1$ and $g = 2$ curves. The former are better understood on the mathematical side and computationally easier and better handled. We will know only speak about genus 1 curves, which over finite fields are elliptic curves.

1.2 Number of points on elliptic curves

As for any group used for the DLP problem, we need that the order of the group is almost a prime (i.e contains a large prime factor). Otherwise it is easy to break the problem by working on each factor and using the Chinese Remainder Theorem. This raised the problem of finding elliptic curves over a finite field $\mathbb{F}_q$ whose number of rational points is almost a prime. This topic has been a fruitful area of elliptic cryptography for the last 25 years and we can classify methods in three subsections.

1.2.1 Elementary methods

Let us present some elementary methods and their limits.

Counting points.

if the field is $\mathbb{F}_p$ with $p > 2$ we can always write our elliptic curve $E : y^2 = f(x)$ with $\deg f = 3$. Hence the number of points on $E(\mathbb{F}_p)$ is

$$1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right).$$

Obviously the complexity is $\mathcal{O}(p)$ and the limit is $p \approx 2^{30}$.

Exercise 1. *Adapt the previous method to the case of* $\mathbb{F}_{2^n}$.

Baby steps-giant steps.

this is based on the observation that

$$|p+1-\#E(\mathbb{F}_p)| < 2\sqrt{p}.$$

This is Hasse-Weil bound refined for $q=p$ prime (the trace $\pm 2\sqrt{p}$ cannot be reached). The idea is to pick a random point $P \in E(\mathbb{F}_p)$ and to compute an integer $m \in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ such that $mP=0$. If m is the only such number in the interval, it follows that $m=\#E(\mathbb{F}_p)$. It is easy to pick a point P randomly by choosing an x and see if $f(x)$ is a square.

Baby steps : make a list of the first $s=\sqrt[4]{p}$ multiple of P. Note that we know $-iP$ as well. Next compute $Q=(2s+1)P$ and $R=(p+1)P$.

Giant steps : compute $R, R\pm Q, R\pm 2Q, \dots R\pm tQ$ where $t=\lfloor 2\sqrt{p}/(2s+1)\rfloor \approx \sqrt[4]{p}$. Now Hasse-Weil bound tells us that

$$(p+1)P - \#E(\mathbb{F}_p)P = kP, \quad k \in \{-2\sqrt{p}+1, \dots, 2\sqrt{p}-1\}.$$

This means that $R=kP$ and we can write $k=(2s+1)i+j$ with $i \in \{0, \pm 1, \dots, \pm t\}$ and $j \in \{0, \pm 1, \dots, \pm s\}$.

Putting $m=p+1+(2s+1)i-j$ we get $mP=0$ and we get an algorithm is $\mathcal{O}(\sqrt[4]{p}$.

Remark 2. To avoid problem that m is not the only such number in the interval, Mestre showed that one can work simultaneously with the curve and its quadratic twist.

However this is still an exponential method.

To work with extensions.

Let $E/\mathbb{F}_q$ be an elliptic curve over a small field where we can easily compute its number of points N. Let $t=1+q-N$ and write $P(X)=X^2-tX+q=(X-\alpha)(X-\beta)$. Then for every n $\#E(\mathbb{F}_{q^n})=(1-\alpha^n)(1-\beta^n)$.

Exercise 2. *Show how to compute this number without computing the roots (use resultant for instance).*

This is indeed a very fast method to count points. But several restrictive attacks gave an insecure feeling about it. They are base on the so called Weil descent principle. For $E/\mathbb{F}_{q^k}$, one constructs $C/\mathbb{F}_q$ of small genus and $\phi : C \to E$ sur $\mathbb{F}_{q^k}$. Then one transfers the DLP by

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q} \circ \phi^* : E(\mathbb{F}_{q^k}) \to \mathrm{Jac}(C)(\mathbb{F}_q).$$

Practically

- Menezes, Qu : does not work for all elliptic curves over $\mathbb{F}_{2^n}$ for $n \in [160, 600]$ prime.
- Menezes, Teske, Weng (resp. Hess) : for $2^{94}/2^{162}$ (resp. $2^{123}/2^{156}$) isomorphism classes of elliptic curves over $\mathbb{F}_{2^{23\cdot 7}}$ (resp. $\mathbb{F}_{2^{31\cdot 5}}$) this reduces the DLP to 2^{48} (resp. 2^{45}) steps (on hyperelliptic curves of genus 8 (resp. 31) over $\mathbb{F}_{2^{23}}$ (resp. $\mathbb{F}_{2^5}$)).
- Diem : if $(q, 6) = 1$ then there exists a transfer from $\mathbb{F}_{q^7}$ to $\mathbb{F}_q$.

1.2.2 Polynomial time methods

From the previous methods, we learned that we have to take $\mathbb{F}_q$ to be either a prime field $\mathbb{F}_p$ with p large or $\mathbb{F}_{p^n}$ with p small and n prime. Are there other restrictions ? Only few : one has to avoid $\#E(\mathbb{F}_q) = q$ (bad anyway), supersingular curves or curves with $\#E(\mathbb{F}_q) = q - 1$.

Two ways exist to obtain our curve, which have been developed more generally for any curves of genus g (at least theoretically) :

- One takes random curves of genus g over $\mathbb{F}_q$ and one has a fast way to compute the number of points. These algorithms belongs to four categories :
  1. l-adics methods : for $g = 1$ (Schoof); works in large characteristics.
  2. Cohomological methods : the most used today is Kedlaya's algorithm. It works well when the characteristic is small.
  3. p-adic methods based on the canonical lift : they were introduced by Satoh for elliptic curves in 2000.
  4. Deformation theory : this (for the moment theoretical) method was introduced by Lauder in 2002.
- On construct a curve over a number field whose Jacobian endomorphism ring has a good structure (CM). Then one reduces the curve modulo suitable large prime for which it is easy to compute the order from the structure. These CM methods have been developed for $g = 1, 2$ (and certain $g = 3$) curves.

We will focus on two methods : an l-adic method, called also SEA (Schoof-Elkies-Atkin algorithm) and a 2-adic method which is a elegant variant of Satoh's algorithm : the AGM-method for genus 1 curve. The former is originally do to Schoof and the complexity was dramatically improved by Elkies and Atkin. Nowadays, the current record is the computation of the number of points over a finite fied with $p = 10^{2099} + 6243$ elements. The latter was developed in 2000 by Mestre and implemented by Lercier-Lubicz. It is nowadays the fastest one in characteristic 2 : a record over $\mathbb{F}_{2^{100002}}$ was obtained.

Chapter 2

Zeta function in large characteristics

References : handbook of elliptic and hyperelliptic curve cryptography.

2.1 Schoof's algorithm

2.1.1 Main idea

In 1985 Schoof was the first to describe a polynomial time algorithm to count the number of points on an elliptic curve E over a large prime field $\mathbb{F}_p$. In the remainder of this section, we will assume that $p > 3$ and his means that E can be given by an equation of the form

$$E : y^2 = x^3 + a_4x + a_6 \text{ with } a_4, a_6 \in \mathbb{F}_p.$$

Recall that $|E(\mathbb{F}_p)| = p + 1 - t$ with t the trace of the Frobenius endomorphism p and by Hasse's Theorem we have $|t| \leq 2\sqrt{p}$. The main idea of Schoof?s algorithm is to compute t modulo various small primes $\ell_1, \dots \ell_r$ such that $\prod_{i=1}^{r} \ell_i > 4\sqrt{p}$. The trace t can then be determined using the Chinese Remainder Theorem and the group order follows. From the prime number theorem, it follows that r is $\mathcal{O}(\log p/ \log\log p)$ and that the largest prime ℓ_r is of order $\mathcal{O}(\log p)$. To illustrate the idea, we show how to compute $t \pmod 2$. Since p is an odd prime, we have $|E(\mathbb{F}_p)| \equiv t \pmod 2$, so $t \equiv 0 \pmod 2$ if and only if $E(\mathbb{F}_p)$ has a nontrivial $\mathbb{F}_p$-rational point of order two. The nontrivial points of order two are given by $(\xi_i, 0)$ with ξ_i a root of $X^3 + a_4X + a_6$. Therefore, if $X^3 + a_4X + a_6$ is irreducible over $\mathbb{F}_p$ we have $t \equiv 1 \pmod 2$ otherwise, $t \equiv 0 \pmod 2$. Note that the polynomial $X^3 + a_4X + a_6$ is irreducible over $\mathbb{F}_p$ if and only if $\gcd(X^3 + a_4X + a_6; X^p - X) = 1$. The computation of $t \pmod 2$ thus boils down to polynomial arithmetic modulo $X^3 + a_4X + a_6$.
More generally, we obtain the trace t modulo a prime ℓ by computing with the ℓ-torsion points. Recall that the Frobenius endomorphism ϕ_p is defined by $\phi_p : E(\mathbb{F}_p) \to E(\mathbb{F}_p) : (x, y) \mapsto (x_p, y_p)$ and that it cancels its characteristic polynomial, i.e.

$$\phi_p^2 - [t]\phi_p + [p] = 0.$$

By restricting to nontrivial ℓ-torsion points $P \in E(\overline{\mathbb{F}}_p)$ we obtain the reduced equation in the $\mathbb{F}_\ell$ vectorial space $E[\ell](\overline{\mathbb{F}}_p)$

$$\phi_p^2(P) + [p_\ell]P = [t_\ell]P$$

with $t_\ell \equiv t \pmod{l}$ and $p_l \equiv p \pmod{\ell}$ and $0 \leq t_\ell, p_\ell < l$.
$P = (x_1, y_1)$ is a nontrivial ℓ-torsion point if and only if x_1 is a root of the ℓ-th division polynomial f_ℓ. The nontrivial ℓ-torsion points can therefore be described as the solutions of the system of equations

$$Y^2 - X^3 - a_4X - a_6 = 0, \quad f_\ell(X) = 0.$$

This implies that the equation

$$(X^{p^2}, Y^{p^2}) + [p_\ell](X, Y) = [t_\ell](X^p, Y^p)$$

holds modulo the polynomial $f_\ell(X)$ and $E(X, Y) = Y^2 - X^3 - a_4X - a_6$. To compute t_ℓ one simply try all $\tau \in \{0, \ldots, \ell - 1\}$ until we find the unique value τ for which the equation is true modulo $f_\ell(X)$ and $E(X, Y)$.

2.1.2 Implementation and complexity

The computation of $[a](X, Y)$ is done using division polynomials and the classical formulae. Recall that for $\gcd(\ell, p) = 1$ we have $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and thus $\deg(f_\ell) = (\ell^2 - 1)/2$ (when $\ell \neq 2$). The computation of (X^{p^2}, Y^{p^2}) and (X^p, Y^p) modulo f_ℓ and $E(X, Y)$ clearly takes $\mathcal{O}(\log p)$ multiplications in the ring $\mathbb{F}_p[X, Y]/(E(X, Y), f_\ell(X))$. Since $\deg f_\ell$ is of order $\mathcal{O}(\ell^2)$, each of these multiplication takes $\mathcal{O}(\ell^{2\mu} \log^\mu p)$ bit-operations, so computing $t \pmod{\ell}$ requires $\mathcal{O}(\ell^{2\mu} \log^{1+\mu} p)$ bit operations. Summing over all primes ℓ_i this gives a complexity of $\mathcal{O}(\log^{2+3\mu} p)$ bit-operations.

Note that if we could replace the division polynomials f‘ by alternative polynomials of lower degree, the complexity of the algorithm would drop considerably. In the next section, we show that for ordinary elliptic curves it is possible to use alternative polynomials for about half the primes ‘ and show how to deal with the other primes.

2.2 Atkin primes

2.2.1 The action of Frobenius on the ℓ-torsion points

For every prime ℓ we introduce the so called emphmodular equation. This is a symmetric polynomial $\Phi_\ell(S, T) \in \mathbb{Z}[S, T]$ which is equal to $S^{\ell+1} - S^\ell T^\ell + T^{\ell+1}$ plus terms of the form $S^i T^j$ with $i, j \leq \ell$ and $i + j < 2\ell$. The polynomial is defined by the property that for any field F of characteristic not ℓ and for every j-invariant $j \in F$, the $\ell + 1$ roots of $\Phi_\ell(j, T) = 0$ are precisely the j-invariants of the isogenous curves E/C where $j(E) = j$ and C runs through the $\ell + 1$ cyclic subgroup of $E[\ell]$.

The polynomial $\Phi_\ell(S, T)$ describes a singular model for the modular curve $X_0(\ell) \in \mathbb{P}^1 \times \mathbb{P}^1$ over $\mathbb{Z}$.

Example 2.

$$\begin{aligned}\Phi_3(X,Y) &= X^4 - X^3Y^3 + Y^4 + 2232(X^3Y^2 + X^2Y^3) - 1069956(X^3Y + XY^3) \\ &\quad +36864000(X^3 + Y^3) + 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2) \\ &\quad +452984832000000(X^2 + Y^2) - 770845966336000000XY \\ &\quad +1855425871872000000000(X + Y).\end{aligned}$$

Proposition 2.2.1. *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ with j-invariant $j \neq 0, 1728$. Then*

1. *the polynomial $\Phi_\ell(j,T)$ has a zero $\tilde{j} \in \mathbb{F}_{p^r}$ if and only if the kernel C of the corresponding isogeny $E \to E/C$ is a one-dimensional eigenspace of $\phi_p r$ in $E[\ell]$.*
2. *the polynomial $\Phi_\ell(j,T)$ splits completely in $\mathbb{F}_{p^r}[T]$ if and only if ϕ_p acts as a scalar matrix on $E[\ell]$.*

Proof. If C is an eigenspace of ϕ_p^r, it is stable under the action of the Galois group generated by ϕ_p^r. Therefore the isogeny $E \to E/C$ is defined over $\mathbb{F}_{p^r}$ and the j-invariant of E/C is contained in $\mathbb{F}_{p^r}$.
Conversely, if $\Phi_\ell(j,\tilde{j}) = 0$ then there is a cyclic subgroup $C \in E[\ell]$ such that the j-invariant of E/C is equal to $\tilde{j} \in \mathbb{F}_{p^r}$. Let E' be an elliptic curve over $\mathbb{F}_{p^r}$ with j-invariant equal to $\tilde{j}$. Let $E/C \to E'$ be an $\overline{\mathbb{F}}_p$-isomorphism and let $f : E \to E/C \to E'$ be the compositve isogeny. It has kernel C.
The group $H := Hom_{\mathbb{F}_{p^r}}(E,E')$ of isogenies $E \to E'$ that are defined over $\mathbb{F}_{p^r}$ is a subgroup of the group of all isogenies. Since E is ordinary $Hom_{\overline{\mathbb{F}}_p}(E,E')$ is a free rank 2 $\mathbb{Z}$-module. The subgroup H is either trivial or equal to $Hom_{\overline{\mathbb{F}}_p}(E,E')$. Therefore f is defined over $\mathbb{F}_{p^r}$ as soon as there exists an isogeny $E \to E'$ which is defined over $\mathbb{F}_{p^r}$. This means that C is an eigenspace of ϕ_p^r as soon as curves E and E' are $\mathbb{F}_{p^r}$-isogenous, or equivalently, when their Frobenius endomorphisms over $\mathbb{F}_{p^r}$ satisfy the same characteristic equation.
We will show that E' can be chosen like this. Since E and E' are isogenous over $\overline{\mathbb{F}}_p$ their geometric ring of endomorphism are orders in the same imaginary quadratic field K. Let ψ and ψ' the respective Frobenius of E and E' over $\mathbb{F}_{p^r}$. In K we have up to complex conjugation that

$$\psi^s = \psi'^s$$

for some positive integer s. If $\psi = \psi'$ we are done. If $\psi = -\psi'$ we replace E' by its quadratic twist and we are done. From now on we suppose that $\psi \neq \pm\psi'$.

□

Proposition 2.2.2. *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ with j-invariant $j \neq 0, 1728$. Let $\Phi_\ell(j,T) = f_1 f_2 \cdots f_s$ be the factorization of $\Phi_\ell(j,T) \in \mathbb{F}_p[T]$ as a product of irreducible polynomials. Then there are the following possibilities for the degrees of f_i*

1. *1 and ℓ; in other words $\Phi_\ell(j,T)$ factors as a product of a linear factor and an irreducible factors of degree ℓ. In this case ℓ divides the discriminant $t^2 - 4p$. We put $r = \ell$ in this case.*

2. $1, 1, r, r, \ldots, r$; *in this case* $t^2 - 4p$ *is a square modulo* ℓ, *the degree* r *divides* $\ell - 1$ *and* ϕ_p *acts on* $E[\ell]$ *as a scalar matrix.*

3. $r, r, \ldots, r$ *for some* $r > 1$; *in this case* $t^2 - 4p$ *is not a square modulo* ℓ, *the degree* r *divides* $\ell + 1$ *and* ϕ_p *acts on* $E[\ell]$ *as a* 2×2 *matrix with an irreducible characteristic polynomial modulo* ℓ.

In all cases, r *is the order of* ϕ_p *in the group* $PGL_2(\mathbb{F}_\ell)$ *and the trace* t *of* ϕ_p *satisfies*

$$t^2 \equiv (\zeta + \zeta^{-1})^2 p \pmod{\ell}$$

for some primitive r*-th root of unity* $\zeta \in \overline{\mathbb{F}}_\ell$.

Proposition 2.2.3. *Let* E *be an ordinary elliptic curve over* $\mathbb{F}_p$ *with* j*-invariant* $j \neq 0, 1728$. *Let* ℓ *be an odd prime and let* s *denote the number of irreducible factors of* $\Phi_\ell(j, T) \in \mathbb{F}_p[T]$. *Then*

$$(-1)^s = \left(\frac{p}{l}\right).$$

2.2.2 Atkin primes

Definition 2.2.1. *A prime* ℓ *is called an* Elkies prime *(resp. an* Atkin prime*) if* $t^2 - 4p$ *is a square modulo* ℓ *(resp. not a square).*

To decide if a prime ℓ is an Atkin or Elkies prime, Proposition 2.2.2 shows that it suffices to compute $g(T) = \gcd(\Phi_\ell(j, T), T^p - T)$. Since $\Phi_\ell(j, T)$ has degree $\ell + 1$ this requires $\mathcal{O}(\ell^\mu \log p^{1+\mu})$ bit-operations.

Let us assume that ℓ is an Atkin prime ℓ, to limit the possibilities for $t \pmod{\ell}$, we need to compute the exact order r of the Frobenius endomorphism in $PGL_2(\mathbb{F}_\ell)$, by computing

$$g_i(T) = \gcd(\Phi_\ell(j, T), T^{p^i} - T)$$

for $i = 2, \ldots$ until $g_i(T) = \Phi_\ell(j, T)$. To speed up this computation, i should be limited to the divisors of $\ell + 1$ that satisfy $(-1)^{(\ell+1)/i} = \left(\frac{p}{\ell}\right)$. Once r is determined there are only $\phi(r) \leq (\ell+1)/2$ choices for the r-th root ζ. By symmetric there are $\phi(r)/2$ possible values for t_ℓ^2 and accordingly $\phi(r)$ values for t_ℓ.

Atkin repeats this computation for various small primes ℓ and then uses a baby-step/giant-step-like algorithm to determine the correct value of the trace of Frobenius. Note that only the computations with the modular polynomials are polynomial time; the baby-step giant-step algorithm on the other hand is an exponential time algorithm.

Chapter 3

Zeta function in small characteristics

3.1 The complex theory

3.1.1 Elliptic integrals

It was historically the first case handled : Lagrange [Lag67, t.II,p.253-312] and Gauss [Gau70, t.III,p.352-353,261-403] introduced the *Arithmetic geometric mean* to compute elliptic integrals.

Theorem 3.1.1. *Let a, b be two reals such that $0 < b < a$. We have*

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2\cos^2 t + b^2 \sin^2 t}} = \frac{\pi}{2\mathrm{M}(a,b)},$$

where $\mathrm{M}(a,b)$ *(*arithmetic geometric mean *of a and b) is the common limit of*

$$\begin{cases} a_0 = a & a_{n+1} = \frac{a_n + b_n}{2} \\ b_0 = b & b_{n+1} = \sqrt{a_n b_n} \end{cases}$$

Since

$$|a_{n+1} - b_{n+1}| = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} = \frac{(a_n - b_n)^2}{2(\sqrt{a_n} + \sqrt{b_n})^2} \leq \frac{(a_n - b_n)^2}{8b_1}$$

these two sequences are adjacent and the convergence is quadratic. This method is then better than traditional numeric integrations.
The proof is based on a tricky change of variables which transforms the parameters a, b in the integral into a_1, b_1. Taking the limit one has then the theorem.
To understand this change of variables we are going to algebraize our problem. Put $x = e_3 + (e_2 - e_3)\sin^2 t$ with

$$\begin{cases} a_0^2 & = e_1 - e_3 \\ b_0^2 & = e_1 - e_2 \\ 0 & = e_1 + e_2 + e_3 \end{cases}$$

We can reformulate the theorem as :

Theorem 3.1.2.
$$\int_{e_3}^{e_2} \frac{dx}{\sqrt{P(x)}} = \frac{\pi}{2\mathrm{M}(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$$
with $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$, $e_3 < e_2 < e_1$.

One recognizes the integral of a regular differential form on the elliptic curve $E : y^2 = P(x)$. What can be its value ?

3.1.2 Recall on tori and elliptic curves

Curves have not always been curves, before they were ... surfaces ! Indeed it is a deep and nice result that irreducible algebraic smooth curves over $\mathbb{C}$ and compact Riemann surfaces are actually the same notion seen under two different spotlights. Hence curves over $\mathbb{C}$ inherit a bunch of analytic properties. Moreover in the case of elliptic curves over $\mathbb{C}$, the structure is even richer : the curves are (connex, compact) Lie groups and can be represented by quotients of $\mathbb{C}$ by a lattice (i.e tori) as we will see.
Reference : Silverman (the arithmetic of elliptic curves, Chap.VI)

Let $\Lambda \subset \mathbb{C}$ be a lattice, that is Λ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis of $\mathbb{C}$. There exists two elements $\omega_i \in \mathbb{C}$ (linearly independent over $\mathbb{R}$) such that $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.
Let us consider the topological variety $X = \mathbb{C}/\Lambda$. X is called a *torus*. Indeed, topologically, X is a square where the 2 pairs of opposite borders have been identified. In particular X is of genus 1 (it is a 'donuts' with 1 hole). One shows that X is in fact an compact analytic variety. Moreover it is easy to describe the functions on it

Definition 3.1.1. *An* elliptic function *is a meromorphic function* $f(z)$ *on* $\mathbb{C}$ *which satisfies*
$$f(z + \omega) = f(z) \text{ for all } \omega \in \Lambda, z \in C.$$

Elliptic functions with no poles are constant as the surface is compact. Can we construct non constant elliptic functions ?

Definition 3.1.2. *The* Weierstrass $\mathcal{P}$-function *is defined by the series*
$$\mathcal{P}(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z + \omega)^2} - \frac{1}{\omega^2} \right).$$

The function $\mathcal{P}' = d\mathcal{P}(z, \Lambda)/dz$ is also an elliptic function. One can prove that all elliptic function is a polynomial in $\mathcal{P}$ and $\mathcal{P}'$.
Let us define also the *Eisenstein series* G_n of weight n by
$$G_n = \sum_{\omega \in \in \Lambda \setminus \{0\}} \omega^{-n}.$$

The fundamental result is

Theorem 3.1.3. *The elliptic functions $\mathcal{P}$ and $\mathcal{P}'$ satisfy the equation*

$$\mathcal{P}'^2 = 4\mathcal{P}^3 - 60G_4\mathcal{P} - 140G_6.$$

This is the affine equation for an elliptic curve E. The map

$$\begin{array}{rccll} u: & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0:1:0) & z \in \Lambda \end{array}$$

is a complex analytic isomorphism of Riemann surfaces and a group homomorphism (for the natural additive structure on $\mathbb{C}/\Lambda$.
Reciprocally if $E/\mathbb{C}$ is an elliptic curve, there exists a lattice Λ such that $\mathbb{C}/\Lambda$ is isomorphic to $E(\mathbb{C})$ (uniformization theorem).

Remark 3. Note that $u^*(dx/y) = d(\mathcal{P}(z))/\mathcal{P}'(z) = dz$.

A natural question is then the following : starting from $\mathbb{C}$ how can we compute a lattice Λ ?

Proposition 3.1.1. *Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass coordinate functions x, y. Let α, β be paths on $E(\mathbb{C})$ giving a basis for $H_1(E, \mathbb{Z})$. Then if*

$$\omega_1 = \int_\alpha dx/y \text{ and } \omega_2 = \int_\beta dx/y$$

and if Λ is the lattice generated by the ω_i one has complex analytic isomorphism

$$F : E(\mathbb{C}) \to \mathbb{C}/\Lambda, \quad F(P) = \int_O^P dx/y \pmod{\Lambda}.$$

This map is inverse of u.

3.1.3 Periods

Let us come back to our curve $E : y^2 = 4(x - e_1)(x - e_2)(-e_3)$. If one denotes by $\mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ (ω_1 real ω_2 purely imaginary) the complex torus $E(\mathbb{C})$, one has the isomorphism

$$\begin{array}{rccll} u: & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0:1:0) & z \in \Lambda \end{array}$$

and (see figure 3.1)

$$\omega_1 = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} dz = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} \frac{d\mathcal{P}(z)}{\mathcal{P}'(z)} = 2\int_{e_3}^{e_2} \frac{dx}{y} = 2\int_{e_3}^{e_2} \frac{dt}{\sqrt{P(t)}}$$

The problem is now the computation of a period of a differential of the 1st kind on a Riemann surface.

Suppose, we chose the basis of Λ such that $\tau = \omega_2/\omega_1$ has a positive imaginary part. In the theory of abelian varieties over $\mathbb{C}$, it is classical to introduce *theta functions*. They can be seen as holomorphic sections of sheaves but we want to give here a more straightforward definition for elliptic curves (see [Ros86] for the general theory).

Definition 3.1.3. *Let $\tau \in \mathbb{H}$, $\epsilon, \epsilon' \in \{0,1\}$. One defines the* theta function with characteristic (ϵ, ϵ') *by*

$$\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](z,\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi(n+\epsilon/2)^2\tau + 2i\pi(n+\epsilon/2)(z+\epsilon'/2))$$

It is an analytic function of the variable z. If $z = 0$, one denotes also $\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](0,\tau) = \vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)$. When $(\epsilon,\epsilon') \neq (1,1)$, $\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau) \neq 0$ and is called a *theta constant*.
These values have the following properties.

Proposition 3.1.2. *1. Limit :*

$$\lim_{\mathrm{Im}\,\tau\to+\infty} \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau) = \lim_{\mathrm{Im}\,\tau\to+\infty} \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau) = 1.$$

2. Thomae's formula :

$$\begin{cases} \omega_1\sqrt{e_1-e_3} = & \pi\cdot\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \\ \omega_1\sqrt{e_1-e_2} = & \pi\cdot\vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 \end{cases}$$

3. Duplication formula :

$$\begin{cases} \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2\tau)^2 = & \frac{\vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2+\vartheta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2}{2} \\ \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2\tau)^2 = & \sqrt{\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2\vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2} \end{cases}$$

Remark 4. As the theta constants are positive reals (because τ is purely imaginary), the sign of the square roots is always the positive one. When it is no more the case, the choice is a bit more subtle (see [Cox84]).

3.1.4 Proofs

We want to give two proofs of Th.3.1.2. The first one is straightforward. As the duplication formula is exactly the AGM recursion, we can write

$$\begin{cases} a_0 = \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 & a_n = \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2^n\tau)^2 \\ b_0 = \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 & b_n = \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2^n\tau)^2 \end{cases}$$

By the limit property, one has

$$\mathrm{M}\left(\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2, \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2\right) = 1.$$

The AGM recursion being homogeneous, one obtains the theorem thanks to Thomae formula :

$$M(a_0,b_0)=M(\frac{\omega_1\sqrt{e_1-e_3}}{\pi},\frac{\omega_1\sqrt{e_1-e_2}}{\pi})=\frac{\omega_1}{\pi}M(\sqrt{e_1-e_3},\sqrt{e_1-e_2})=1.$$

The second proof will reveal the true geometry behind the result. Consider again the elliptic curve $E : y^2 = P(x)$. This curve is isomorphic to the curve $E_\tau = E_{a_0,b_0}$ defined by

$$\begin{aligned} E_\tau : y_0^2 &= x_0(x_0-(e_1-e_3))(x_0-(e_1-e_2)) && (3.1)\\ &= x_0\left(x_0-\frac{\pi^2}{\omega_1^2}\cdot\vartheta\begin{bmatrix}0\\0\end{bmatrix}(\tau)^4\right)\left(x_0-\frac{\pi^2}{\omega_1^2}\cdot\vartheta\begin{bmatrix}0\\1\end{bmatrix}(\tau)^4\right) && (3.2)\\ &= x_0(x_0-a_0^2)(x_0-b_0^2), && (3.3)\end{aligned}$$

One can then construct the following diagram.

$$\begin{array}{ccc} \mathbb{C}/\mathbb{Z}\omega_1+\mathbb{Z}2\omega_2 & \xrightarrow{G:z\mapsto z} & \mathbb{C}/\mathbb{Z}\omega_1+\mathbb{Z}\omega_2 \\ {\scriptstyle u_{2\tau}}\downarrow\simeq & & \simeq\downarrow{\scriptstyle u_\tau} \\ E_{2\tau}(\mathbb{C}) & \underset{f}{\overset{g}{\rightleftarrows}} & E_\tau(\mathbb{C}) \end{array}$$

where $E_{2\tau} = E_{a_1,b_1}$ and f, g are 2-isogenies given by (see for instance [BM89]):

$$\begin{aligned} g:(x_1,y_1) &\mapsto \left(x_1(1+\frac{a_1^2-b_1^2}{x_1-a_1^2}),\frac{y_1(x_1^2-2x_1a_1^2+a_1^2b_1^2)}{(x_1-a_1^2)^2}\right) && (3.4)\\ f:(x_0,y_0) &\mapsto \left(\frac{y_0^2}{4x_0^2}+(\frac{a+b}{2})^2,-\frac{y_0(a^2b^2-x_0^2)}{8x_0^2}\right) && (3.5)\end{aligned}$$

In particular the kernel of f is $< (0,0) >$.
We can now finish the proof : since $G^*(dz) = dz$ we have $g^*(dx_0/y_0) = dx_1/y_1$. Now

$$\omega_1=2\int_{e_1}^{\infty}\frac{dx}{y}=2\int_0^{-\infty}\frac{-i}{2}\frac{dx_0}{y_0}=\int_0^{-\infty}-i\frac{dx_1}{y_1}=\ldots=\int_0^{-\infty}-i\frac{dx_n}{y_n}.$$

By iteration :

$$E_\tau\to E_{2\tau}\to\ldots\to E_{2^n\tau}\to\ldots\to E_\infty : y^2=x(x-M(a_0,b_0)^2)^2.$$

But E_∞ is a genus 0 curve which means that there exists a parametrization which gives

$$\omega_1=\int_0^{-\infty}-i\frac{dx}{\sqrt{x(x-M(a_0,b_0)^2)^2}}=\left[-2\frac{\mathrm{Arctan}(\frac{\sqrt{\mathrm{x}}}{\mathrm{M(a_0,b_0)}})}{\mathrm{M(a_0,b_0)}}\right]_0^{-\infty}=\frac{\pi}{\mathrm{M}(a_0,b_0)}.$$

3.2 2-adic method

Let $q = 2^N, k = \mathbb{F}_q$ and $\mathbb{Q}_q$ be the unramified extension of degree N of $\mathbb{Q}_2$, $\mathbb{Z}_q$ its ring of integers, ν its valuation and σ the Frobenius substitution (i.e the unique Galois automorphism of $\mathbb{Q}_q$ such that $\sigma x \equiv x^2 \pmod 2$, see Chap. **??**). The aim of this section is to give an algorithm which we can present as

$$\tilde{E}/\mathbb{F}_q \text{ ordinary e.c. } \stackrel{\text{lift}}{\longrightarrow} E/\mathbb{Z}_q \stackrel{\text{AGM}}{\underset{\text{cv}}{\longrightarrow}} \mathcal{E}/\mathbb{Z}_q \text{ canonical lift } \stackrel{\text{AGM}}{\longrightarrow} \text{Frobenius trace.}$$

Let us detail now the different parts.

3.2.1 Theory of the canonical lift

3.2.2 Lift, canonical lift

Let E be an elliptic curve over $k = \mathbb{F}_q$. Let $\mathbb{Z}_q = W(\mathbb{F}_q)$ be the ring constructed in Chap.**??** and $\mathbb{Q}_q$ its field of fractions. Let also σ be the Frobenius substitution. As E is defined by an equation with coefficients in k, we can lift the non-zero coefficients of this equation over $\mathbb{Z}_q$ and then obtain the equation of an elliptic curve $\mathcal{E}$ over $\mathbb{Q}_q$. The curve $\mathcal{E}$ is called *a lift* of E.
As we have seen in the proof of the Weil conjectures, the Frobenius endomorphism π is strongly connected to the number of points of the curve and we would like to find on $\mathcal{E}$ an isogeny that lifts π. We restrict to the case of ordinary curves. In this case, we know that $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ so we actually ask that our curve $\mathcal{E}$ has a quadratic field for its endomorphism ring. This situation is quite rare in characteristic 0 as we have seen in Chap. **??** and we cannot expect this to happen for an arbitrary lift. On this other hand, such a lift always exists :

Theorem 3.2.1 ([Mes72, V, Th.3.3, Cor. 3.4])**.** *Let E/k be an ordinary elliptic curve. There exists an unique –up to isomorphism– elliptic curve $E^\uparrow$ over $\mathbb{Z}_q$ such that $E^\uparrow \otimes k \simeq E$ and*

$$End_{\mathbb{Q}_q}(E^\uparrow) \simeq End_k(E).$$

We call $E^\uparrow$ the canonical lift *of E.*

If $f \in \mathrm{End}_k(E)$, we denote $f^\uparrow \in \mathrm{End}_{\mathbb{Q}_q}(E^\uparrow)$ its canonical lift.

Remark 5. This theorem was proved in the case of elliptic curves by Deuring [Deu41] then generalized by Lubin, Serre and Tate [LST64].

Corollary 3.2.1 ([Mes72, Appendix, Cor 1.2])**.** *$E^\uparrow$ is the canonical lift of E iff there exists $Fr^\uparrow : E^\uparrow \to {}^\sigma(A^\uparrow)$ lifting Fr.*

Remark 6. It is not always possible to lift a supersingular elliptic curve with its ring of endomorphism as this one may be an order in a quaternion algebra (Caution : it may also be $\mathbb{Z}$ if all the endomorphisms are not rational).

As an isomorphism class of elliptic curve is given by its j-invariant, we can characterized this curve by an unique element $J \in \mathbb{Z}_q$. Another useful characterization is the following.

Theorem 3.2.2 ([VPV01, §. 2]). *Let $x \in \mathbb{Z}_q$ such that $x \equiv J \pmod{2^i}$ with $i \in \mathbb{N}$. Then there exists a unique $y \in \mathbb{Z}_q$ such that $y \equiv x^2 \pmod 2$ and $\Phi_2(x, y) = 0$. Moreover $y \equiv j((\tilde{E}^{(2)})^{\uparrow}) = J^{\sigma} \pmod{2^{i+1}}$.*

Recall that Φ_p is the modular polynomial of order p.

Remark 7. It is an important result in CM theory that J is in fact an algebraic integer and the curve $E^{\uparrow}$ exists actually over $\overline{Q}$. The degree of the extension $\mathbb{Q}(J)/\mathbb{Q}$ is given by the class number of $\mathrm{End}(E) \otimes \mathbb{Q}$. As the discriminant of this extension is heuristically in $\sqrt{q}$, the degree of this extension may quickly becomes too big for explicit computations.

As we explained earlier, the general philosophy is to obtain curves in characteristic 0 in order to apply analytic results. Indeed, one has then the outstanding result linking the geometry and the arithmetic of the Frobenius.

Proposition 3.2.1 (Satoh). *Let E be an elliptic curve over k with trace of Frobenius a. Let ω be a regular differential on $E^{\uparrow}$ and let $c \in \mathbb{Q}_q$ the element defined by $(\pi^{\uparrow})^*(\omega) = c \cdot \omega$. Then $a = c + q/c$.*

3.2.3 Lift

In characteristic 0 we want to use the form $E_{a,b} : y^2 = x(x - a^2)(x - b^2)$. Of course we cannot use this model in characteristic 2. We propose two different solutions to solve this problem.

First solution

Lemma 3.2.1 ([Ver03]). *Let $a, b \in 1 + 4\mathbb{Z}_q$ with $b/a \in 1 + 8\mathbb{Z}_q$. Then*

$$\begin{aligned} E_{a,b} &\xrightarrow{\sim} E : y^2 + xy = x^3 + rx^2 + sx + t \\ (x, y) &\to \left(\frac{x - ab}{4}, \frac{y - x + ab}{8} \right) \end{aligned}$$

for some $r, s, t \in \mathbb{Z}_q$ such that

$$\tilde{E} : y^2 + xy = x^3 + \left(\frac{a - b}{8} \right).$$

We then consider $\tilde{E}$ as $y^2 + xy = x^3 + c$, let $r \in \mathbb{Z}_q$ such that $r \equiv \sqrt{c} \pmod 2$ and take

$$\begin{cases} a_0 = 1 + 4r \\ b_0 = 1 - 4r \end{cases}$$

The advantage of this model is that there is a rational 4 torsion point $(c^{1/4}, c^{1/2})$. This point enables to find the sign of $\pm \mathrm{tr}(\pi)$ that occurs at the end of the algorithm because $\mathrm{tr}(\pi) \equiv 1 \pmod 4$. The drawback is that this model does not represent all cases. Moreover it gives no clue about a possible generalization to hyperelliptic cases.

Second solution

Starting with a general ordinary elliptic curve $\tilde{E} : y^2 + xy = x^3 + a_2x^2 + a_4x + a_6$, we can always get rid of the a_6 coefficient. We lift then $\tilde{E}$ naturally and make the transformation

$$Y^2 = (y + \frac{x}{2})^2 = x(x^2 + \frac{4a_2 + 1}{4}x + 1).$$

We can factorize the left member over $\mathbb{Q}_q$ in $x(x - \alpha)(x - \beta)$ with $\nu(\alpha) = -2$ and $\nu(\beta) = 2$. Let $X = x - \alpha$ we have then a model

$$Y^2 = X(X + \alpha)(X + \alpha - \beta).$$

As $\nu(\frac{\alpha-\beta}{\alpha} - 1) = \nu(\frac{\alpha}{\beta}) = 4$, we can take

$$\begin{cases} a_0 = 1 \\ b_0 = \sqrt{\frac{\alpha-\beta}{\alpha}} \in \mathbb{Z}_q \end{cases}$$

and consider the curve

$$Y^2 = X(X - 1)(X - b_0^2).$$

Note that this curve is not isomorphic over $\mathbb{Q}_q$ to the original one but is a quadratic twist. However, as we will obtain the trace of the Frobenius only up to a sign, this is not an issue.

Remark 8. We have to get rid of the a_6 coefficient, otherwise we might have to factorize the left member in a ramified extension of $\mathbb{Q}_2$ (it is the case for instance with $y^2 + xy = x^3 + 1$).

3.2.4 Convergence

Let start with a model $E_0 = E_{a_0,b_0}$ over $\mathbb{Z}_q$ lifting $\tilde{E}$. Let denote $E_i = E_{a_i,b_i}$ the elliptic curves obtained by AGM iterations. Let denote also $\tilde{E}^{\uparrow}$ the canonical lift of $\tilde{E}$ which is completely characterized by its j-invariant J. We want to prove that the AGM sequence converges to the Galois cycle associated to the canonical lift. We give two proofs.

First proof

We are going to use Th. 3.2.2. If E and E' are two elliptic curves that are p-isogenous then $\Phi_p(j(E), j(E')) = 0$.
We have of course $\Phi_2(E_i, E_{i+1}) = 0$ by the complex computations of 3.1. An easy computation shows also the following congruence.

Lemma 3.2.2. $j(E_{i+1}) \equiv j(E_i)^2 \pmod 2$.

By iteration of the AGM we then obtain

$$j(E_n) \equiv j((\tilde{E}^{(2^n)})^{\uparrow}) \pmod{2^{n+1}}.$$

Second proof

The second proof uses a result of Carls. It avoids explicit invariants and is then useful for generalization.

Theorem 3.2.3 ([Car02, Th.3]). *Let A be an abelian variety over $\mathbb{F}_q$, $\mathcal{A}/\mathbb{Z}_q$ be an ordinary abelian scheme with special fiber A. One defines a sequence*

$$\mathcal{A} = \mathcal{A}_0 \to \mathcal{A}_1 \to \dots$$

where the kernel of the isogenies are the components $\mathcal{A}_i[2]^{loc}$ (i.e the 2-torsion points in the kernel of the reduction). We have

$$\lim_{n\to\infty} \mathcal{A}_{nN} = A^{\uparrow}$$

i.e for all n, $(\mathcal{A}_{Nn})/\mathbb{Z}_q^{(Nn+1)} \simeq (A^{\uparrow}_{Nn})/\mathbb{Z}_q^{(Nn+1)}$ where $\mathbb{Z}_q^{(i)} = \mathbb{Z}_q/2^i\mathbb{Z}_q \simeq \mathbb{Z}/2^i\mathbb{Z}$. In particular the convergence is linear.

Using 3.1 we see that if we still denote by $f : E_i \to E_{i+1}$ the 2-isogeny induced by the AGM-iteration, then $\ker f =< (0,0) >$ and $(0,0)$ reduces on $\tilde{O}$ (because the kernel corresponds to the point $(\alpha, 0)$ in the reduction, which is of negative valuation). We can then apply the previous theorem.

3.2.5 Trace of the Frobenius

To compute the Frobenius polynomial we only need the trace of the Frobenius on $V_l(\tilde{E})$ for $l \neq p$. But this trace can be already read on regular differentials as we have seen in Prop. 3.2.1. With the notations of the proposition, we have $\chi(X) = X^2 - (c+q/c)\cdot X + q$. We need also the following elementary lemma.

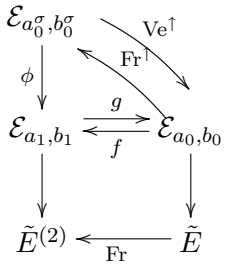
Lemma 3.2.3. *Let $E_{a,b} : y^2 = x(x-a^2)(x-b^2)$ et $E_{a',b'} : y'^2 = x'(x'-a'^2)(x'-b'^2)$ with $\frac{a^2}{b^2} \equiv \frac{a'^2}{b'^2} \equiv 1 \pmod 2$. If E and E' are isomorphic then $x = u^2x'$ and $y = u^3y'$ with $u^2 = \frac{a^2+b^2}{a'^2+b'^2}$. Furthermore $\frac{a^2}{b^2} = \frac{a'^2}{b'^2}$ or $\frac{a^2}{b^2} = \frac{b'^2}{a'^2}$.*

Proof. The two curves being isomorphic, there exists $(u, r) \in (\mathbb{Z}_q^* \times Q_q)$ such that $x = u^2x' + r$ and $y = u^3y'$. It is enough to show that $r = 0$. With the usual notations of [Sil92, chap.III,1.2], one has

$$\begin{aligned} -4u^2(a'^2 + b'^2) = b'_2 &= b_2 + 12r = -4(a^2+b^2) + 12r \\ 0 = u^6 b'_6 &= 4r(r-a^2)(r-b^2) \end{aligned}$$

The first equality shows that $r \equiv 0 \pmod 2$ and the second that $r = 0$ since neither a^2 or b^2 are congruent to 0. The first equality gives also the value of u^2. □

Let $\mathcal{E}_{a_0,b_0}$ be the canonical lift. We can then construct the following diagram



where ϕ is an isomorphism because the two maps have the same kernel $< (0,0) >$. Let $\omega = dx/y$, we then get

$$(\mathrm{Ve}^\uparrow)^*(\omega) = (g \circ \phi)^*(\omega) = \phi^*(\omega) = \frac{\omega}{u}$$

with $u^2 = \frac{a_1^2+b_1^2}{(a_0^2)^\sigma+(b_0^2)^\sigma}$ because g acts by identity as we can see on the explicit formula or with the complex interpretation of g as $z \mapsto z$.
We want to simplify a bit the expression of u^2. we have

$$u^2 = \left(\frac{a_1}{a_0^\sigma}\right)^2 \frac{1+\left(\frac{b_1}{a_1}\right)^2}{1+\left(\frac{b_0^\sigma}{a_0^\sigma}\right)^2}.$$

Let $\lambda_1 = b_1/a_1$ and $\lambda_0 = b_0/a_0$. By Lem.3.2.3, $\lambda_1^2 = (\lambda_0^2)^\sigma$ or $\lambda_1^2 = \frac{1}{(\lambda_0^2)^\sigma}$. Let us prove that it is the first case which occurs. We can write $\lambda_i = 1 + 8c_i$ with $c_i \in \mathbb{Z}_q$ so the first case occurs iff

$$c_1 \equiv c_0^\sigma \pmod 4.$$

By the AGM iteration, we have

$$1 + 8c_1 = \frac{1+4c_0}{\sqrt{1+8c_0}} \Rightarrow c_1 \equiv c_0^2 \pmod 4.$$

As after the first iteration c_0 is itself a square α_0^2 modulo 4, we have

$$c_0^\sigma \equiv (\alpha_0^2)^\sigma \equiv \alpha_0^4 \equiv c_0^2 \pmod 4.$$

So we get $c_1 \equiv c_0^\sigma \pmod 4$ which proves

$$u = \pm\frac{a_1}{a_0^\sigma}.$$

The trace of the Frobenius endomorphism is the same as the trace of the Verschiebung. One has

$$\mathrm{tr}(\pi) = \mathrm{tr}(V) = \mathrm{tr}(\mathrm{Ve}^{\sigma^{N-1}} \circ \cdots \circ \mathrm{Ve}) = \pm\left(\frac{1}{N(u)} + 2^N N(u)\right)$$

with $N(u) = \mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}(a_1/a_0)$.

3.2.6 Complexity and Conclusion

Since by the Hasse-Weil theorem $\mathrm{tr}(\pi) \leq 2\sqrt{q}$ it is enough to compute the previous norm with $\lceil N/2 \rceil + 2$ bits. Several implementations of this method have been achieved : see [Ver03] for a nice overview and running times. The best complexity obtained is quasi-quadratic in time and quadratic in space.

One of the attractive aspect of the AGM method is the simplicity of the formulas involved. Another one is the natural generalizations one can obtain for hyperelliptic curves and non hyperelliptic curves of genus 3. On the contrary it seems that generalization to other characteristics would be less efficient and less elegant due to the complexity of the new AGM formulas.

Figure 3.1: The map u

Bibliography

[BM89] J.-B. Bost & J.-F. Mestre, Moyenne Arithmético-géométrique et Périodes des courbes de genre 1 et 2, Gaz. Math., S.M.F. **38** (1989) , 36-64.

[Car02] R. Carls, Approximation of canonical lifts, in preparation, (2002) available on `http://www.math.leidenuniv.nl/~carls/`.

[Cox84] D. Cox, The arithmetic-geometric mean of Gauss, Enseign. Math. **30** (1984), 275-330.

[Deu41] M. Deuring, Die Typen der Multiplikatoringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ Hamburg **14** (1941), 197-272.

[Gau70] C.F. Gauss, *Werke*, Vol. **12**, Göttingen, (1870-1927).

[Lag67] J.L. Lagrange, *Oeuvres*, Vol. **14**, Gauthiers-Villars, Paris (1867-1892).

[LST64] J. Lubin & J.-P. Serre & J. Tate, *Elliptic Curves and formal groups*, notes disponibles sur `http://ma.utexas.edu/users/voloch/lst.html`, (1964).

[Mes72] W. Messing, *The crystals Associated to Barsotti-Tate Groups : with Applications to Abelian Schemes*, Lect. Notes in Math., **264**, Berin-Heidelberg-New-York, Springer (1972).

[Mes02] J.-F. Mestre, Algorithmes pour compter des points en petite caractéristique en genre 1 et 2, available at `www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps` (2002).

[Sil92] J.H Silverman, *The Arithmetic of Elliptic Curves*, **106**, Springer, (1992).

[Rit03] C. Ritzenthaler : *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*, PhD thesis, Université Paris 7 - Denis Diderot, June 2003 available on `http://www.math.jussieu.fr/~ritzenth`.

[Ros86] M. Rosen, Abelian varieties over $\mathbb{C}$, in *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag, (1986).

[VPV01] F. Vercauteren, B. Preneel & J. Vandewalle , A memory efficient version of Satoh's algorithm, Adv. in Cryptology, Eurocrypt (2001) (Innsbruck, Austria, Mai

2001), Lect. Notes in Comput. Sci. **2045**, 1-13, ed. Pfitzmann, Berlin, Heidelberg: Springer-Verlag (2001).

[Ver03] F. Vercauteren *computing Zeta functions of curves over finite fields*, PhD thesis, Katholicke Universiteit Leuven, 2003.