AGM for point counting

1 The complex theory

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 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 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 ?

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 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 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 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 1. 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 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.

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

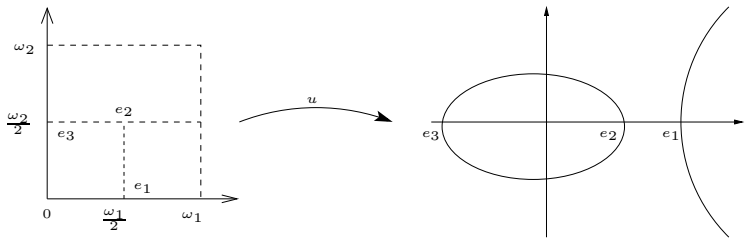
$$\begin{array}{rccll} u: & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0:1:0) & z \in \Lambda \end{array}$$

and (see figure 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

Figure 1: The map u



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 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 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 2. 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]).

1.4 Proofs

We want to give two proofs of Th.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

$$\begin{aligned} E_\tau : y_0^2 &= x_0(x_0-(e_1-e_3))(x_0-(e_1-e_2)) && (1)\\ &= x_0\left(x_0 - \frac{\pi^2}{\omega_1^2}\cdot \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^4\right)\left(x_0 - \frac{\pi^2}{\omega_1^2}\cdot \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^4\right) && (2)\\ &= x_0(x_0-a_0^2)(x_0-b_0^2), && (3) \end{aligned}$$

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]):

$$g : (x_1, y_1) \mapsto \left(x_1(1 + \frac{a_1^2 - b_1^2}{x_1 - a_1^2}), \frac{y_1(x_1^2 - 2x_1a_1^2 + a_1^2b_1^2)}{(x_1 - a_1^2)^2} \right) \quad (4)$$

$$f : (x_0, y_0) \mapsto \left(\frac{y_0^2}{4x_0^2} + (\frac{a_0 + b_0}{2})^2, -\frac{y_0(a_0^2b_0^2 - x_0^2)}{8x_0^2} \right) \quad (5)$$

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

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

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 $\sigma x \equiv x^2 \pmod 2$). The aim of this section is to give an algorithm which we can present as

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

Let us detail now the different parts.

2.1 Theory of the canonical lift

Let E be an elliptic curve over $k = \mathbb{F}_q$. 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, the Frobenius endomorphism ϕ_q is strongly connected to the number of points of the curve and we would like to find on $\mathcal{E}$ an isogeny that lifts ϕ_q. We restrict to the case of ordinary curves. In this case, we know that $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\phi_q)$ so we actually ask that our curve $\mathcal{E}$ has a quadratic field as endomorphism ring. This situation is quite rare in characteristic 0 and we cannot expect this to happen for an arbitrary lift. However a good lift always exists :

Theorem 2.1 ([Mes72, V, Th.3.3, Cor. 3.4]). *Let $\tilde{E}/k$ be an ordinary elliptic curve. There exists an unique –up to isomorphism– elliptic curve $E^\uparrow$ over $\mathbb{Z}_q$ such that $E^\uparrow \otimes k \simeq \tilde{E}$ and*

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

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

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

Remark 3. This theorem was proved in the case of elliptic curves by Deuring [Deu41] then generalized by Lubin, Serre and Tate [LST64].

Corollary 2.1 ([Mes72, Appendix, Cor 1.2]). *$E^\uparrow$ is the canonical lift of $\tilde{E}$ iff there exists $\phi_2^\uparrow : E^\uparrow \to {}^\sigma(E^\uparrow)$ lifting $\phi_2 : \tilde{E} \to \tilde{E}^{(2)}$.*

Remark 4. 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 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 5. It is an important result in CM theory that J is in fact an algebraic integer and the curve $E^\uparrow$ exists actually over $\overline{\mathbb{Q}}$. The degree of the extension $\mathbb{Q}(J)/\mathbb{Q}$ is given by the class number of $\mathrm{End}(\tilde{E}) \otimes \mathbb{Q}$. 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 2.1 (Satoh). *Let $\tilde{E}$ 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 $(\phi_q^\uparrow)^*(\omega) = c \cdot \omega$. Then $a = c + q/c$.*

2.2 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.

2.2.1 First solution

Lemma 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 $\pm\mathrm{tr}(\phi_q)$ that occurs at the end of the algorithm because $\mathrm{tr}(\phi_q) \equiv 1 \pmod 4$. The drawback is that this model does not represent all cases. Moreover it gives no clue about a possible generalization to hyperelliptic cases.

2.2.2 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

$$Y^2 = (y + \frac{x}{2})^2 = x(x^2 + \frac{4a_2 + 1}{4}x + a_4).$$

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 $\nu(\frac{\alpha-\beta}{\alpha} - 1) = \nu(\frac{\beta}{\alpha}) = 4$, 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 6. 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 $y^2 + xy = x^3 + 1$).

2.3 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.

2.3.1 First proof

We are going to use Th. 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 1. An easy computation shows also the following congruence.

Lemma 2.2. $j(E_{i+1}) \equiv j(E_i)^2 \pmod 2$.

By iteration of the AGM we then obtain

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

2.3.2 Second proof

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

Theorem 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, $(\mathcal{A}_{Nn})/\mathbb{Z}_q^{(Nn+1)} \simeq (A^{\uparrow})/\mathbb{Z}_q^{(Nn+1)}$ 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 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.

2.4 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. 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.

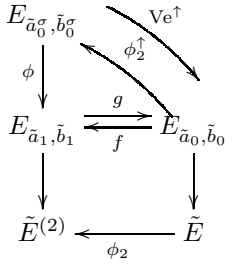
Lemma 2.3. *Let $E_{a,b} : y^2 = x(x-a^2)(x-b^2)$ et $E_{a',b'} : y'^2 = x'(x'-a'^2)(x'-b'^2)$ with $\frac{a^2}{b^2} \equiv \frac{a'^2}{b'^2} \equiv 1 \pmod 2$. If E and E' are isomorphic then $x = u^2x'$ and $y = u^3y'$ with $u^2 = \frac{a^2+b^2}{a'^2+b'^2}$. Furthermore $\frac{a^2}{b^2} = \frac{a'^2}{b'^2}$ or $\frac{a^2}{b^2} = \frac{b'^2}{a'^2}$.*

Proof. The two curves being isomorphic, there exists $(u, r) \in (\mathbb{Z}_q^* \times \mathbb{Q}_q)$ 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 $E_{\tilde{a}_0,\tilde{b}_0}$ be the canonical lift. We can then construct the following diagram



where $\tilde{a}_1, \tilde{b}_1$ are obtained after one step of the AGM from $\tilde{a}_0, \tilde{b}_0$ and 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.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

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

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

2.5 Complexity and Conclusion

Since by the Hasse-Weil theorem $\mathrm{tr}(\phi_q) \leq 2\sqrt{q}$ 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. Here is a short history of the p-adic lifting methods with their complexity and main idea.

99 :	Satoh ($p > 3$, $X(1)$)	lift all $E^{\uparrow^{\sigma^i}}$ (no computation of σ)	$\tilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
	Fouquet-Gaudry-Harley	$p = 2, 3$	”
	Skjernaa	new comp. of $\ker \phi_p^\uparrow : E^\uparrow \to E^{\uparrow^\sigma}$	”
	Vercauteren	lift only one curve	$\tilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 :	Mestre ($p = 2$, $X_0(8)$)	very simple isogeny (AGM)	” $\phi_q^\uparrow$ for free
	Satoh-Skjernaa-Takachi ($p = 2$)	quick computation of σ	$\tilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
	Kim *et al.* ($p = 2$)	normal gaussian base (BGN)	” (no precomp.)
01 :	Gaudry MSST ($p = 2$)	AGM+ SST smaller deg.	”
	Lercier-Lubicz ($p = 2$)	BGN + better Newton	$\tilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 :	Harley ($p = 2$)	general Newton + norm computation	” (for all n)
03 :	Kohel ($X_0(p)$ de genre 0)	modular AGM $p = 3, 5, 7, 13$	”
04 :	Gustavsen-Ranestad	geometric AGM $p = 3$	$\tilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
06- :	Carls-Kohel-Lubicz	geometric AGM $p > 2$	?

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.

References

[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.