COUNTING POINTS ON ELLIPTIC CURVES

OLE ANDRE BIRKEDAL

Abstract. hei hei

Contents

1. Frobnius and finite fields

Throughout this section our fields k will be finite, so let $char(k) = p$ for a prime p. This means that $k = \mathbb{F}_q$ for some $q = p^r$.

Definition 1. *The* Frobenius *endomorphism is the p^{th}-power map*

$$\phi : k \to k$$

$$x \mapsto x^p$$

which induces a map on curves as follows

$$\phi : E(k) \to E^{\phi}(k)$$

$$(x_0, \ldots, x_n) \mapsto (x_0^p, \ldots, x_n^p)$$

where E^{ϕ} is the curve E with ϕ applied to its coefficients.

$$E : y^2 = x^3 + ax + b \quad E : y^2 = x^3 + \phi(a)x + \phi(b)$$

We can apply the Frobenius endomorphism r times

$$\phi^r(x) = x^{p^r} = x^q$$

And since every finite field of q elements is the splitting field of $x^q - x$, it is in other words the fixed points of the q^{th} Frobenius endomorphism

$$\phi^r(x) = x \iff x \in \mathbb{F}_q$$

The same is true for all intermediate fields of size p^k with $0 < k \leq r$, so in general we have that the ϕ^k fixes the elements of the field $\mathbb{F}_{p^k}$.

Proposition 1. *The degree map*

$$deg : Hom(E_1, E_2) \to \mathbb{Z}$$

is a positive quadratic form.

Proof. Clearly $deg(f) = deg(-f)$. The only thing that takes a proof is the bilinearity of the pairing

$$End(E_1, E_2) \times End(E_1, E_2) \to \mathbb{Z}$$

$$(\phi, \psi) \mapsto deg(\phi + \psi) - deg(\phi) - deg(\psi)$$

For this proof we will make extentive use of the dual isogeny, but first notice that we have an injection of multiplication by n maps:

$$[\quad] : \mathbb{Z} \to End(E_1)$$

A calculation then yields

$$\begin{aligned} [\langle \phi, \psi \rangle] &= [deg(\phi + \psi)] - [deg(\phi)] - [deg(\psi)] \\ &= (\widehat{\phi + \psi})(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi \\ &= \widehat{\phi}\psi + \widehat{\psi}\phi \end{aligned}$$

The pairing is then shown to be linear in the first varible, the second variable is similar.

$$\begin{aligned} [\langle \phi_1 + \phi_2, \psi \rangle] &= \widehat{\psi}(\phi_1 + \phi_2) + (\widehat{\phi_1 + \phi_2})\psi \\ &= (\widehat{\psi}\phi_1 + \widehat{\phi_1}\psi) + (\widehat{\psi}\phi_2 + \widehat{\phi_2}\psi) \\ &= [\langle \phi_1, \psi \rangle] + [\rangle \phi_2, \psi \rangle] \end{aligned}$$

□

Theorem 1. *Let ϕ be the q^{th} frobenius map on $E/\mathbb{F}_q$. Then the map $1 - \phi$ is seperable, and $\#ker(1 - \phi) = deg(1 - \phi)$.*

Proof. Recall from chapter **??** that a map ψ is separable if and only if $\psi^*(\omega) \neq 0$, where ω is the invariant differential. Using that the Frobenius ϕ is inseparable [Silverman, 1992] we compute

$$\begin{aligned}(1-\phi)^*(\omega) &= [1]^*\omega - \phi^*(\omega) \\ &= \omega - 0 \\ &= \omega\end{aligned}$$

thus $(1-\phi)^*(\omega) = 0$ if and only if $\omega = 0$, but the invariant differential is non-zero so $(1-\phi)^*(\omega) \neq 0$ which means $1-\phi$ is separable. □

Lemma 1. ***(Cauchy-Schwartz inequality)****. Let A be an abelian group and*

$$d : A \to \mathbb{Z}$$

a positive definite quadratic form. Then for all $\psi, \phi \in A$ the following holds

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}$$

Proof. Let $\psi, \phi \in A$. From the definition of a quadratic form there is a bilinear pairing

$$L(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi)$$

Using this definition, the fact that d is positive definite and letting $m, n \in \mathbb{Z}$ where $m = -L(\psi, \phi)$ and $n = 2d(\psi)$ we calculate

$$\begin{aligned}0 \leq d(m\psi - n\phi) &= d(m\psi) + L(m\psi, n\phi) + d(n\phi) \\ &= m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi) \\ &= d(\psi)\left(4d(\psi)d(\phi) - L(\psi, \phi)^2\right)\end{aligned}$$

where on the last line we make the substitution. If $d(\psi) = 0$ the inequality is trivial, if $d(\psi) \neq 0$ then we divide it out and obtain our result

$$L(\psi, \phi)^2 \leq 4d(\psi)d(\phi)$$

□

Theorem 2. ***(Hasse's theorem)****. Let E be an elliptic curve over a finite field k with q elements, then*

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

Proof. We let $\phi_q : E \to E$ be the q^{th} Frobenius endomorphism on E given by $(x, y) \mapsto (x^q, y^q)$. Recall that ϕ_q fixes our field of q elements, thus

$$P \in E(k) \quad \iff \quad \phi_q(P) = P$$

Writing out the right hand side of the implication we see that

$$0 = P - \phi_q(P) = (1 - \phi_q)(P)$$

which enables us to count the number of points in $E(k)$ by counting the number of points in the kernel of the seperable map $1 - \phi_q$. Recall from before that the number of points in the kernel is equal to the degree of the seperable map

$$\#E(k) = \#ker(1 - \phi_q) = deg(1 - \phi_q)$$

We have shown in that the degree map on $End(E)$ is a positive definite quadratic form, so by using the inequality from the previous theorem we calculate

$$|deg(1 - \phi_q) - deg(\phi_q) - deg(1)| = |\#E(k) - q - 1| \leq 2\sqrt{deg(\phi_q)} = 2\sqrt{q}$$

□

Proposition 2. *If $\psi \in End(E)$ then $det(\psi_\ell) = deg(\psi)$, where ψ_ℓ is a 2×2 matrix acting on the Tate module $T_\ell(E)$.*

Proof. We fix a basis $v_1, v_2 \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ for $T_\ell(E)$ and denote the matrix associated to this basis by

$$\psi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

We now calculate by relying heavily on the ℓ-adic Weil pairing, $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$.

$$\begin{aligned} e(v_1, v_2)^{deg(\psi)} &= e([deg\psi]v_1, v_2) \\ &= e(\psi_\ell \widehat{\psi_\ell} v_1, v_2) \\ &= e(\psi_\ell v_1, \psi_\ell v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(av_1, dv_2)e(cv_2, bv_1) \\ &= e(av_1, dv_2)e(bv_1, cv_2)^{-1} \\ &= e(v_1, v_2)^{ad} e(v_1, v_2)^{-bc} \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{det\psi_\ell} \end{aligned}$$

Since the pairing is non-degenerate we obtain $deg(\psi) = det(\psi_\ell)$. □

Writing out the determinant of $1 - A$ for any matrix A we get

$$\begin{vmatrix} 1-a & -b \\ -c & 1-d \end{vmatrix} = 1 - (a+d) + ad - bc = 1 - tr(A) + det(A)$$

so we see that $tr(\psi_\ell) = 1 + det(\psi_\ell) - det(1 - \psi_\ell)$. Using the previous theorem we get

$$tr(\psi_\ell) = 1 + deg(\psi_\ell) - deg(1 - \psi_\ell)$$

by substituting with the q^{th} Frobenius endomorphism on $T_\ell(E)$ and setting $\tau = tr(\phi_q)$ we get

$$\#E(k) = 1 + q - \tau$$

where we know from Hasse's theorem that $|\tau| \leq 2\sqrt{q}$.

The next proposition will be used in chapter 3, it is easy to prove and gives a nice expression of the Frobenius trace in terms of the dual isogeny.

Proposition 3. *Let $\phi : E \to E$ be the q^{th} Frobenius endomorphism and $\widehat{\phi}$ its dual, then the following holds*

$$t = tr(\phi) = \phi + \widehat{\phi}$$

Proof. Recall that $1 - \phi$ is seperable, so

$$(1 - \phi)(\widehat{1 - \phi}) = deg(1 - \phi) = \#ker(1 - \phi) = \#E(k)$$

Expanding the product on the left we get

$$\begin{aligned} (1 - \phi)(\widehat{1 - \phi}) &= (1 - \phi)(1 - \widehat{\phi}) \\ &= 1 - (\phi + \widehat{\phi}) + \phi\widehat{\phi} \\ &= 1 - (\phi + \widehat{\phi}) + q \end{aligned}$$

From before we had that $\#E(k) = q + 1 - t$ and we just calculated that $\#E(k) = q + 1 - (\phi + \widehat{\phi})$ so the result follows. □

2. Schoof's algorithm and improvements

2.1. **Division polynomials.** The idea of Schoof's algorithm is to calculate the Frobenius trace modulo small primes, then assemble this information using the Chinese remainder theorem. Chosing the set of small primes such that their product $N > 4\sqrt{q}$ (with q the size of our field) gives us the trace t modulo N, which by the Hasse bound is exactly the Frobenius trace.

Recall for this section that an elliptic curve corresponds to a lattice Λ so we have an isomorphism

$$\bar{k}/\Lambda \simeq E(\bar{k})$$

$$z \mapsto (\wp(z), \wp'(z))$$

where $\wp(z)$ is the elliptic Weierstrass function

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}$$

Definition 2. *The* division polynomials *are polynomials* $\Psi_n(x, y) \in \mathbb{Z}[x, y, A, B]$ *defined by the recurrence relations*

$$\begin{aligned}
\Psi_0 &= 0 \\
\Psi_1 &= 1 \\
\Psi_2 &= 2y \\
\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\Psi_{2n+1} &= \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1} \\
\Psi_{2n} &= (2y)^{-1}\Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)
\end{aligned}$$

where $\Psi_n(x, y) = 0$ *is and only if* $(x, y) \in E[n]$.

The construction of these polynomials can be done in at least two ways and I will discuss both of them briefly.

One way of doing this is to construct a function having poles at the n-torsion points of our elliptic curve as follows

$$f_n(z) = n^2 \prod(\wp(z) - \wp(u))$$

where the product is taken over all n-torsion points of $\bar{k}/\Lambda$, denoted $\bar{k}/\Lambda[n]$. This function has roots at exactly the n-torsion points by definition, which is at least what we want. A more throrough examination of this method can be found in [Lang, 1979]. Another way which is more elementary but highly computational is to work explicitly with the addition formulas for elliptic curves.

Replacing the terms y^2 in Ψ_n by $x^3 + Ax + B$ we obtain polynomials Ψ'_n in $\mathbb{F}_q[x]$ if is n is odd or $y\mathbb{F}_q[x]$ if n is even. To avoid this distinction we define

$$f_n(x) = \begin{cases} \Psi'_n(x, y) & \text{if n is odd} \\ \Psi'_n(x, y)/y & \text{if n is even} \end{cases}$$

Proposition 4. *Let* $n \geq 2$ *and* Ψ_n *the division polynomial as defined above, then*

$$nP = (x - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4y\Psi_n^3})$$

2.2. **Schoof's algorithm.** For an elliptic curve over $\mathbb{F}_q$ given by

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

we want to compute the size of $\#E(\mathbb{F}_q)$, we know from before that

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

where t is the trace of the Frobenius as seen in chapter 1. We know that t satisfies the Hasse bound namely

$$|\#E(\mathbb{F}_q) - q - 1| = |t| < 2\sqrt{q}$$

Let $S = \{3, 5, 7, 11, \dots L\}$ be the set of odd primes $\leq L$ such that the product is bigger than the Hasse interval

$$N = \prod_{\ell \in S} \ell > 4\sqrt{q}$$

If we can then calculate $t \pmod{\ell}$ for all $\ell \in S$ we can uniquely determine $t \pmod{N}$ by invoking the Chinese remainder theorem, which then by the Hasse bound is our Frobenius trace t.

We will now look at how to calculate $t \pmod{\ell}$. Let ϕ be the Frobenius endomorphism resticted to $E[\ell]$ and let q_ℓ, τ be q and t reduced modulo ℓ respectively. The computation of τ can then be done by checking if

$$\phi^2(P) + q_\ell P = \tau\phi(P)$$

holds for $P \in E[\ell]$. To perform the addition on the left hand side of the equality we need to distinguish the cases where the points are on a vertical line or not. In other words we have to verify if for $P = (x, y) \in E[\ell]$ the following holds

$$\phi^2(P) = \pm q_\ell P$$

Noting that $-P = (x, -y)$ we write out the equality for the x-coordinates in terms of division polynomials

$$x^{q^2} = x - \frac{\Psi_{q_\ell - 1}\Psi_{q_\ell + 1}}{\Psi_{q_\ell}^2}(x, y)$$

Writing this out in terms of $f_n(x)$ and noting that for n even we have $\Psi_n(x, y) = yf_n(x)$, a calculation for q_ℓ even yields

$$\begin{aligned} x^{q^2} &= \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)}{(f_{q_\ell} y)^2} \\ &= \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)}{f_{q_\ell}^2 (x^3 + Ax + B)} \end{aligned}$$

The calculation for q_ℓ odd is similar and we get the equality

$$x^{q^2} = \begin{cases} x - \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)}{f_{q_\ell}^2 (x^3 + Ax + B)} & \text{if } q_\ell \text{ is even} \\ x - \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)(x^3 + Ax + B)}{f_{q_\ell}^2(x)} & \text{if } q_\ell \text{ is odd} \end{cases}$$

We thus get two equations and we want to verify they have any solutions $P \in E[\ell]$. For doing this we compute the following greatest common divisors

$$\gcd((x^{q^2} - x) f_{q_\ell}^2 (x^3 + Ax + B) + f_{q_\ell - 1}(x) f_{q_\ell + 1}(x), f_\ell(x)) \quad (q_\ell \text{ even})$$

$$\gcd((x^{q^2} - x) f_{q_\ell}^2 (x) + f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)(x^3 + Ax + B), f_\ell(x)) \quad (q_\ell \text{ odd})$$

We are now going to treat the rest in two cases, depending on the value from the above gcds.

Case 1: gcd $\neq 1$ meaning there exist a non-zero ℓ-torsion point P such that $\phi^2(P) = \pm q_\ell P$. If $\phi^2(P) = -q_\ell P$ we have that $\tau\phi(P) = 0$ but since $\phi(P) \neq 0$ we know that $\tau = 0$. If $\phi^2(P) = q_\ell P$ we have that

$$2q_\ell P = \tau\phi(P) \Leftrightarrow \phi(P) = \frac{2q_\ell}{\tau}$$

Substituting the last equality into $\phi^2(P) = q_\ell P$ we obtain

$$\frac{4q_\ell^2}{\tau^2} = q_\ell P \Leftrightarrow 4q_\ell P = \tau^2 P$$

We thus obtain the congruence $\tau^2 \equiv 4q_\ell \pmod{\ell}$

Case 2: gcd $= 1$ so $\phi^2(P) \neq \pm q_\ell P$ meaning the two points are not equal nor are they on the same vertical line for any ℓ-torsion point P. This enables us to do the addition $\phi^2(P) + q_\ell P$ using the appropriate addition formulas. Recall that if $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points on E with $P \neq Q$ we have that their sum is given by $P + Q = (x_3, y_3)$ where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = -x_1 - x_2 + \lambda^2$$

$$y_3 = -y_1 - \lambda(x_3 - x_1)$$

We can now write out the addition explicitly in terms of polynomials as follows

$$\lambda = \frac{\Psi_{q_\ell+2}\Psi_{q_\ell-1}^2 - \Psi_{q_\ell-2}\Psi_{q_\ell+1}^2 - 4y^{q^2+1}\Psi_{q_\ell}^3}{4\Psi_{q_\ell}y((x - x^{q^2})\Psi_{q_\ell}^2 - \Psi_{q_\ell-1}\Psi_{q_\ell+1}}$$

with the left hand side given by

$$\phi^2(P)+q_\ell P = \left(-x^{q^2} - x + \frac{\Psi_{q_\ell-1}\Psi_{q_\ell+1}}{\Psi_{q_\ell}^2} + \lambda^2, -y^{q^2} - \lambda\left(-2x^{q^2} - x + \frac{\Psi_{q_\ell-1}\Psi_{q_\ell+1}}{\Psi_{q_\ell}^2}\right)\right)$$

The right hand side is as before given by

$$\tau\phi(P) = \left(x^q - \left(\frac{\Psi_{\tau+1}\Psi_{\tau-1}}{\Psi_\tau^2}\right)^q, \left(\frac{\Psi_{\tau+2}\Psi_{\tau-1}^2 - \Psi_{\tau-2}\Psi_{\tau+1}^2}{4y\Psi_\tau^3}\right)^q\right)$$

So figuring out if

$$\phi^2(P) + q_\ell P = \tau\phi(P)$$

amounts to checking if the above equalities hold for $P \in E[\ell]$ and $0 \leq \tau < \ell$, working modulo the division polynomials $\Psi_\ell(x)$.

2.3. **Schoof-Elkies algorithm.** When doing the calculations in Schoof's algorithm we were working modulo the division polynomials $\Psi(x, y)$ of degree $\ell^2 - 1$. Instead we can exploit some special primes called *Elkies primes* that enables us to work in a cyclic subgroup C of $E[\ell]$. Here C will correspond to a 1-dimensional eigenspace.

The frobenius endomorphism restricted to $E[\ell]$ satisfies the characteristic equation

$$\phi^2 - \tau\phi + q_\ell = 0$$

where τ and q_ℓ is as before. The roots of this equations are the eigenvalues of $\phi|E[\ell]$ and they are given by

$$\lambda_{1,2} = \frac{\tau \pm \sqrt{\tau^2 - 4q_\ell}}{2}$$

If the discriminant $\tau^2 - 4q_\ell$ is a square modulo ℓ we have that $\lambda_{1,2} \in \mathbb{F}_q$.

Definition 3. *A prime ℓ such that $\tau^2 - 4q_\ell$ is a square modulo ℓ is called an* Elkies prime.

For primes of this type we obtain a factorization

$$(\phi - \lambda_1)(\phi - \lambda_2) = 0$$

so for an eigenvalue λ we have that $\phi(P) = \lambda P$ for a point P. Thus P is the generator for a cyclic eigenspace $C \subset E[\ell]$ of order ℓ corresponding to λ. Notice that we have an exact sequence of groups

$$0 \to C \to E \to E/C \to 0$$

where the map $E \to E/C$ has cyclic kernel C of order ℓ. Determining which primes are Elkies primes can be done by working with the modular polynomials. From [ref til modulrpoly-teorem] we have that $\Phi_\ell(j(E), j(E/C)) = 0$, so letting the isogeny $f : E \to E'$ have cyclic kernel C we get an exact sequence

$$0 \to C \to E \to E' \to 0$$

which by a diagram chase yields $E' \simeq E/C$. This argument gives us the following result

Proposition 5. *$\Phi_\ell(j(E), x) = 0$ for $x \in \mathbb{F}_q$ if and only if ℓ is an Elkies prime.*

Figuring out if ℓ is an Elkies prime can thus be done fast by calculating

$$\gcd(\Phi_\ell(j(E), x), x^q - x)$$

Now since we are working only with primes of this type we restrict ourself to working in the subspace C of order ℓ. There is thus a factor $G_\ell(x)$ of the division polynomial which has the x-coordinates of points in C as roots. Since similar points in C of different sign are on the same vertical line we only include unique points up to sign. In this way we get that the degree of $G_\ell(x)$ is $\frac{\ell-1}{2}$.

From the theory of eigenvalues we know that if λ_1, λ_2 are eigenvalues of ϕ then

$$tr(\phi) = \lambda_1 + \lambda_2$$

We also know using proposition 2 that

$$\lambda_1 \lambda_2 = det(\phi) = q$$

Using this we can recover the trace of ϕ by calculating one of the eigenvalues

$$\tau \equiv \lambda + \frac{q}{\lambda} \pmod{\ell}$$

To compute the eigenvalue λ we can thus check which of the relations

$$\phi(P) = (x^q, y^q) = \lambda P$$

holds on the eigenspace C, this mean we can work modulo $G_\ell(x)$. This enables us to work in the much smaller ring

$$\mathbb{F}_q[x, y]/(G(x), y^2 - x^3 - Ax - B)$$

and thus greatly improves Schoof's original approach.

The obstacle that remains is how we can possible calculate the factor

$$G_\ell(x) = \prod_{(x', y') \in C} (x - x')$$

of the division polynomialwhere the product is taken over all unique points $P = (x', y')$ up to sign. When calculating the gcd $\gcd(\Phi_\ell(j(E), x), x^q - x)$ we obtain a polynomial whos roots (at most two) are the j-invariants of the ℓ-isogenous curves $\tilde{E} = E/C$ where C is the eigenspace corresponding to λ. The next theorem enables us to calculate an explicit formula for the Weierstrass equation of $\tilde{E}$.

Theorem 3. *Let E be given by the equation*

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

with $j = j(E)$. Then the eqation for the ℓ-isogenous curve $\tilde{E}$ with $\tilde{j} = j(\tilde{E})$ is given by

$$\tilde{E} : y^2 = x^3 + \bar{A}x + \bar{B}$$

$$\bar{A} = -\frac{\tilde{j}'^2}{48\tilde{j}(\tilde{j} - 1728)} \quad \bar{B} = -\frac{\tilde{j}'^3}{864\tilde{j}^2(\tilde{j} - 1728)}$$

And letting

$$\Phi_{\ell,x} = \frac{\partial \Phi_\ell}{\partial x} \quad \Phi_{\ell,y} = \frac{\partial \Phi_\ell}{\partial y}$$

be the partial derivatives with respect to x and y respectively we have that

$$\bar{j}' = -\frac{18B\Phi_{\ell,x}(j,\bar{j})}{\ell A\Phi_{\ell,y}(j,\bar{j})}j$$

The next theorem will enable us to compute the sum of the x-coordinates of the points in our subspace C. This value will be used to calculate every coefficient of $G_\ell(x)$, notice that if we formally multiply out the product of $G_\ell(x)$ we get

$$G_\ell(x) = x^{\frac{\ell-1}{2}} - \frac{p_1}{2}x^{\frac{\ell-3}{2}} + \dots$$

Here p_1 is the sum of the x-coordinates of C, the division by two is because they appear twice as a result of the symmetry around the x-axis.

Theorem 4. *Given our two curves $E : y^2 = x^3 + Ax + B$ and $\tilde{E} : y^2 = x^3 + \bar{A}x + \bar{B}$ we let $E_4 = -48A$, $E_6 = 864B$ and similarly for our ℓ-isogenous curve $\bar{E_4} = -48\bar{A}$, $\bar{E_6} = 864\bar{B}$. Then we obtain an explicit formula for*

$$p_1 = \sum_{(x,y)\in C} x$$

$$p_1 = \frac{\ell}{2}J + \frac{\ell}{4}\left(\frac{E_4^2}{E_6} - \ell\frac{\bar{E_4^2}}{\bar{E_6}}\right)$$

where by using the usual partial derivative notation $\Psi_{\ell,xx} = \frac{\partial^2\Psi_\ell}{\partial x^2}$ etc. we write J as

$$J = -\frac{j'^2\Psi_{\ell,xx}(j,\tilde{j}) + 2\ell j'\tilde{j}'\Psi_{\ell,xy}(j,\tilde{j}) + \ell^2\tilde{j}'^2\Psi_{\ell,yy}(j,j')}{j'\Psi_{\ell,x}(j,j')}$$

Here $j' = -j\frac{E_6}{E_4}$ and similarly $\tilde{j}' = -\tilde{j}\frac{\tilde{E_6}}{\tilde{E_4}}$.

Given the value of p_1 we can calculate the rest of the coefficients using a theorem from [schoof-ref].

Theorem 5. *Let $\ell \neq char(k)$ be a prime, and $\phi : E \to \widetilde{E}$ be an isogeny with $\ker(\phi)$ cyclic of size ℓ, then the polynomial $G_\ell(x)$ which vanishes on the x-coordinates of elements of $\ker(\phi)$ satisfies*

$$z^{\ell-1}G_\ell(\wp(z)) = exp(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty}\frac{\widetilde{c}_k - \ell c_k}{(2k+1)(2k+2)}z^{2k+2})$$

Proof. The proof of Schoof uses analytic theory heavily, he introduces the Weierstrass ζ-function which is defined by

$$\zeta(z) = \frac{1}{z} - \sum_{k=1}^{\infty}\frac{c_k}{2k+1}z^{2k+1}$$

Differentiating we see that $\zeta'(z) = -\wp(z)$. Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be the lattice corresponding to E and then we have that $\widetilde{\Lambda} = \frac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}$ is the lattice corresponding to $\widetilde{E}$. Setting ζ and $\widetilde{\zeta}$ to be the Weierstrass ζ-functions for E and $\widetilde{E}$ respectively, Schoof eventually arrives at the equality

$$-\ell\zeta(z) + \widetilde{\zeta}(z) - p_1 z = \sum_{i=1}^{(\ell-1)/2} \frac{\wp'(z)}{\wp(z) - \wp(\frac{i}{\ell}\omega_1)}$$

Notice that $\frac{d}{dz}\wp(z) - \wp(\frac{i}{\ell}\omega_1) = \wp'(z)$ so we can invert the process of logaritmic differention

$$\frac{df}{dz} = \frac{f'}{f}$$

on both sides of the equality, setting

$$f(z) = \prod_{i=1}^{(\ell-1)/2} (\wp(z) - \wp(\frac{i}{\ell}\omega_1)$$

A thurough proof can be found in [schoof-ref]. □

The coefficients of $G_\ell(x)$ can thus be obtained by expanding both sides of the equality from the previous theorem and comparing the coefficients of like powers of z. Setting $w = z^2$ and letting $A(w)$ be the function on the right-hand side of the equality expanded as a power series in w. Also let $C(w) = \wp(z) - \frac{1}{w} = \sum_{k=1}^{\infty} c_k w^k$, the Weierstrass $\wp$-function with the first term removed. For notational convenience we write $[B(w)]_j$ for the coefficient of w^j in the power series $B(w)$. Letting g_i be the coefficient of x^i in $G_\ell(x) = x^d + \sum_{i=0}^{d-1} g_i x^i$ with $d = \frac{\ell-1}{2}$ we get the recursion

$$g_{d-i} = [A(w)]_i - \sum_{k=1}^{i} \left(\sum_{j=0}^{k} \binom{d-i+k}{k-j} [C(w)^{k-j}]_j \right) g_{d-i+k}$$

3. Satoh's algorithm

Forklaring og overblikk over de forskjellige subsection-ene.

This algorithm is divided into two parts, first we do what is called a *lifting*, then we recover the trace of the Frobenius from the lifted data.

3.1. **Lifting the j-invariants.** We begin by establishing some notation, so let $\mathbb{F}_q$ be our finite field with $q = p^n$ as before, $\mathbb{Z}_p$ the p-adic integers and $\mathbb{Q}_q$ the q-adic rationals as defined in section **??**. For this section we let σ be the p-th frobenius, and ϕ_q be the q-th frobenius. As for previous sections we denote the curves over our finite fields as $E/\mathbb{F}_q$, for the lifted curves we write $\mathscr{E}/\mathbb{Q}_q$.

Theorem 6. ***(Lubin-Serre-Tate)*** *Let $E/\mathbb{F}_q$ be an elliptic curve with j-invariant $j(E)$ and σ the p-th Frobenius on $\mathbb{Q}_q$ then the system of equations*

$$\Phi_p(x, \sigma(x)) = 0 \quad x \equiv j(E) \,(mod\, p)$$

where Φ_p is the p-th modular polynomial has a unique solution $J \in \mathbb{Z}_q$ which is the j-invariant of the canonical lift $\mathscr{E}$ of E.

The latter theorem gives an efficient way of calculating the j-invariants, in addition it has been shown [Deuring, 1941] that the canonical lift always exists and is unique (up to isomorphism).

Knowing $j(\mathscr{E})$ we can explicitly write out the Weierstrass equation for $\mathscr{E}$, but instead of lifting E to $\mathscr{E}$ directly we can consider all its conjugates

$$E, E^{\sigma}, E^{\sigma^2}, \ldots, E^{\sigma^{n-2}}, E^{\sigma^{n-1}}$$

Letting $E^{\sigma^i} = E^i$ we get a sequence of maps

$$E \xrightarrow{\sigma} E^1 \xrightarrow{\sigma} E^2 \xrightarrow{\sigma} \ldots \xrightarrow{\sigma} E^{n-1}$$

Where the composition is the q-th power Frobenius $\phi_q = \sigma\sigma\ldots\sigma : E \to E$. Recall that the $deg(\sigma) = p$ so from the theory of modular polynomials we have that

$$\Phi_p(j(E^i), j(E^{i+1})) = 0$$

Definition 4. *The* canonical lift *$\mathscr{E}$ of an elliptic curve E over $\mathbb{F}_q$ is an elliptic curve over $\mathbb{Q}_q$ such that $End(\mathscr{E}) \simeq End(E)$.*

Since the endomorphism rings are isomorphic we can lift every Frobenius on E to a Frobenius on $\mathscr{E}$. We thus obtain a commutative diagram

$$\begin{array}{ccccccccc}
\mathscr{E} & \xrightarrow{\sigma} & \mathscr{E}^1 & \xrightarrow{\sigma} & \cdots & \xrightarrow{\sigma} & \mathscr{E}^{n-1} & \xrightarrow{\sigma} & \mathscr{E} \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\
E & \xrightarrow{\sigma} & E^1 & \xrightarrow{\sigma} & \cdots & \xrightarrow{\sigma} & E^{n-1} & \xrightarrow{\sigma} & E
\end{array}$$

Since the lifted Frobenius also has degree p we have that

$$\Phi_p(j(\mathscr{E}^i), j(\mathscr{E}^{i+1})) = 0 \quad j(\mathscr{E}^i) \equiv j(\mathscr{E}^{i+1}) \,(mod\, p)$$

We thus define a function $\Theta : \mathbb{Z}_q^d \to \mathbb{Z}_q^d$ by

$$\Theta(x_0, x_1, \ldots, x_{n-1}) = (\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \ldots, \Phi_p(x_{n-1}, x_0))$$

Note that the roots of Θ are the j-invariants of our lifted curves

$$\Theta(j(\mathscr{E}), j(\mathscr{E}^2), \ldots, j(\mathscr{E}^{n-1})) = (0, 0, \ldots, 0)$$

so by solving $\Theta(\bar{x}) = 0$ using a multivariate Newton-Raphson iteration, we can recover the j-invariants to desired precision. Setting up the Jacobian matrix J_Θ of Θ, the iteration is given by

$$\bar{x}_{n+1} = \bar{x}_n - J_\Theta^{-1}\Theta(\bar{x}_n)$$

where the matrix $J_\Theta(x_0, x_1, \ldots, x_{n-1})$ is given as

$$\begin{pmatrix} \frac{\partial}{\partial x_0}\Psi_p(x_0,x_1) & \frac{\partial}{\partial x_1}\Psi_p(x_0,x_1) & 0 & \ldots & 0 & 0 \\ 0 & \frac{\partial}{\partial x_1}\Psi_p(x_1,x_2) & \frac{\partial}{\partial x_2}\Psi_p(x_1,x_2) & 0 & \ldots & 0 \\ 0 & & & & & \\ \vdots & & \ddots & & & \vdots \\ 0 & & & & & \\ \frac{\partial}{\partial x_0}\Psi_p(x_{n-1},x_0) & 0 & \ldots & 0 & 0 & \frac{\partial}{\partial x_{n-1}}\Psi_p(x_{n-1},x_0) \end{pmatrix}$$

3.2. **Recovering the trace.** Let ϕ be the q-th Frobenius and ϕ^* be the induced Frobenius on differentials, we have that $c = Tr(\phi) = \phi + \hat{\phi}$ so investigating the action of the Frobenius on the invariant differential ω we see that

$$\begin{aligned} [Tr(\phi)]^*(\omega) &= [Tr(\phi)](\omega) \\ &= (\phi + \hat{\phi})^*(\omega) \\ &= \phi^*(\omega) + \hat{\phi}^*(\omega) \\ &= \hat{\phi}^*(\omega) \end{aligned}$$

Where the last equality is using the fact that $\phi^* = 0$ since ϕ is inseperable, we thus get that $\hat{\phi}^*(\omega) = c\omega$. Recall from **??** that $\frac{dx}{y}$ is also holomorphic and invariant under translation, so for the rest of this section we define our invariant differential as such

$$\omega = \frac{dx}{y}$$

Instead of working with ϕ we work with its dual $\hat{\phi}$ and the dual of the p-th Frobenius $\hat{\sigma}$. Our diagrams will be turned around so we get commutative squares

$$\begin{array}{ccc} \mathscr{E}^{i+1} & \xrightarrow{\hat{\sigma}_{i+1}} & \mathscr{E}^{i} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ E^{i+1} & \xrightarrow{\hat{\sigma}_{i+1}} & E^{i} \end{array}$$

Letting $\hat{\mathscr{F}}_q$ be the lifted of the dual q-th Frobenius we have that $\hat{\mathscr{F}}_q = \hat{\sigma}\hat{\sigma}\ldots\hat{\sigma}$. So if $\omega_i = \omega^{\sigma^i}$ we have that $\hat{\sigma}_i^*(\omega_i) = c_i\omega_{i+1}$. A calculation then yields, using that $\sigma_i^* = c_i$

$$\begin{aligned} \hat{\mathscr{F}}_q(\omega) &= (\hat{\sigma}_1 \circ \hat{\sigma}_2 \circ \ldots \circ \hat{\sigma}_{n-1})(\omega) \\ &= ([c_1] \circ \ldots \circ [c_{n-1}](\omega) \\ &= [c_1 \ldots c_{n-1}](\omega) \end{aligned}$$

Since $\hat{\mathscr{F}}_q(\omega) = c\omega$ we have that

$$c = \prod_{i=1}^{n-1} c_i \pmod q$$

It then remains for us to calculate each c_i for every lifted p-th Frobenius endomorphism $\hat{\sigma}_i$.

From [Silverman, 1992] we have that there exists a commutative triangle

$$\begin{array}{ccc} \mathscr{E}_{i+1} & \xrightarrow{\widehat{\sigma}_{i+1}} & \mathscr{E}_i \\ & {\scriptstyle v_i} \searrow \quad \nearrow {\scriptstyle \lambda_i} & \\ & \mathscr{E}_{i+1}/\ker(\widehat{\sigma}_{i+1}) & \end{array}$$

From formulas due to Vlu (see [Vlu, 1971] or [Sato, 2003]) we can calculate the map v_i and the Weierstrass equation for the curve $\mathscr{E}_{i+1}/\ker(\widehat{\sigma}_{i+1})$. This means that in order to investigate the action of $\widehat{\sigma}_{i+1}$ on the invariant differential for all i amount to investigating how the composition $\lambda_i v_i$ acts. In addition, if we let v_i^* be the map induced on differentials then by the formulas of Velu it has trivial action on the invariant differential ω. It is then enough to calculate how the isomorphism λ_i acts on the invariant differential. Given the Weierstrass equations for our curves

$$\mathscr{E}_{i+1}/\ker(\sigma_{i+1}) : y^2 = x^3 + \alpha_{i+1}x + \beta_{i+1}$$
$$\mathscr{E}_i : y^2 = x^3 + a_i x + b_i$$
$$\lambda_i : \mathscr{E}_{i+1}/\ker(\sigma_{i+1}) \to \mathscr{E}_i$$

The function which preserves the coefficients of the curves is given by

$$(x, y) \mapsto (u_i^2 x, u_i^3 y)$$

Calculating how this acts on the curve we get the curve

$$y^2 = x^3 + u_i^{-4} a_i x + u_i^{-6} b_i$$

comparing coefficients we get the two equalities

$$u_i^{-4} a_i = \alpha_{i+1} \text{ and } u_i^{-6} b_i = \beta_{i+1}$$

Solving for u_i^2 we get

$$u_i^2 = \frac{\alpha_{i+1} b_i}{\beta_{i+1} a_i}$$

and we have our isomorphism. Now for calculating how λ_i acts on the holomorphic differential $\omega = \frac{dx}{y}$ we recall from **??** and calculate

$$\begin{aligned} \lambda_i^*(\frac{1}{y}dx) &= \lambda_i^*(\frac{1}{y}) d(\lambda_i^*(x)) \\ &= \frac{1}{u_i^3 y} d(u_i^2 x) \\ &= \frac{u_i^2 dx}{u_i^3 y} \\ &= u_i^{-1}\omega \end{aligned}$$

From our commutative triangle we thus have that

$$\widehat{\sigma_i}^*(\omega_i) = c_i = (\lambda_i v_i)^*(\omega_i) = \lambda_i^*(\omega_i) = u_i^{-1}\omega_{i+1}$$

so we have found c_i for all i, its square is given by

$$c_i^2 = \frac{\beta_{i+1} a_i}{\alpha_{i+1} b_i}$$

By our product formula for c we have the the square of c given as

$$c^2 = \prod_{i=1}^{n-1} c_i = \prod_{i=1}^{n-1} \frac{\beta_{i+1} a_i}{\alpha_{i+1} b_i}$$

Taking the square root we obtain the trace c up to sign.

References

[Deuring, 1941] Deuring, M. (1941). Die typen der multiplikatorenringe elliptischer funktionenkrper. *Abh. Math. Sem. der Univ. Hamburg.*, 14(1).

[Lang, 1979] Lang, S. (1979). *Elliptic Curves: Diophantine Analysis*. Springer.

[Sato, 2003] Sato, A. (2003). On the reduction of certain isogenies of elliptic curves via the formulas by vlu.

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

[Vlu, 1971] Vlu, J. (1971). Isognies entre courbes elliptiques. *C.R. Acad. Sci. Paris*.