COUNTING POINTS ON ELLIPTIC CURVES

OLE ANDRE BIRKEDAL

Abstract. hei hei

Contents

1. Schoof's algorithm and improvements

1.1. **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 1. *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 [serge lang-ref]. 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 1. *Let* $n \geq 2$ *and* Ψ_n *the division polynomial as defined above, then*

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

1.2. **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 section [referanse]. 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 $\Psi_\ell(x)$.

1.3. **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 2. *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 2. *$\Phi_\ell(j(E), x) = 0$ 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 [referanse] 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 1. *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 2. *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 3. *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*

$$z^{\ell-1} G_\ell(\wp(z)) = exp(-\frac{1}{2}p_1 z^2 - \sum_{k=1}^{\infty} \frac{\widetilde{c}_k - \ell c_k}{(2k+1)(2k+2)} z^{2k+2})$$

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

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