COUNTING POINTS ON ELLIPTIC CURVES

OLE ANDRE BIRKEDAL

Abstract. hei hei

Contents

1. 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.

1.1. **P-adic numbers.** Fixme

1.2. **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 [ref]. 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 1. ***(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-ref] 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 1. *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

$$\begin{tikzcd}
\mathscr{E} \arrow[r, "\sigma"] \arrow[d, "\pi"] & \mathscr{E}^1 \arrow[r, "\sigma"] \arrow[d, "\pi"] & \cdots \arrow[r, "\sigma"] & \mathscr{E}^{n-1} \arrow[r, "\sigma"] \arrow[d, "\pi"] & \mathscr{E} \arrow[d, "\pi"] \\
E \arrow[r, "\sigma"] & E^1 \arrow[r, "\sigma"] & \cdots \arrow[r, "\sigma"] & E^{n-1} \arrow[r, "\sigma"] & E
\end{tikzcd}$$

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

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

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

1.3. **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 $\hat{\phi}^*(\omega) = c\omega$ So instead of working with ϕ we work with its dual $\hat{\phi}$ and the dual of the p-th Frobenius $\hat{\sigma}$. Our diagrams [ref] will be turned around so we get commutative squares

$$\begin{tikzcd}
\mathscr{E}^{i+1} \arrow[r, "\hat{\sigma}_{i+1}"] \arrow[d, "\pi"] & \mathscr{E}^i \arrow[d, "\pi"] \\
E^{i+1} \arrow[r, "\hat{\sigma}_{i+1}"] & E^i
\end{tikzcd}$$

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

$$c = \prod_{i=1}^{n-1} c_i \quad (mod\, q)$$