Ideas

Simon Pohmann

May 11, 2022

Contents

1 My first idea

As usual, let p be a (big) prime and consider $q := p^2$. Consider a (small) prime l. Then every supersingular Elliptic Curve $E/\mathbb{F}_q$ satisfies $\Phi_n(j(E), j(E)^p) = 0$ with $n = l^{O(\log(p))}$, as the supersingular l-isogeny graph is an expander with mixing length $O(\log(p))$, hence there is a path from E to $E^{(p)}$ of length $O(\log(p))$.

Now we analyze when $\Phi_n(j(E), j(E)^p) = 0$ for an ordinary Elliptic Curve $E/\mathbb{F}_q$.

Using the isogeny graph

Since the connected component of E in the l-isogeny graph is a vulcano, we can find a path (of length $O(\log(p))$) to an Elliptic Curve in the crater, say E_0. Hence there are ascending l-isogenies

$$E \to ... \to E_0$$

Let $K := \mathrm{End}^0(E_0)$ and consider the maximal order $\mathcal{O}_K \subseteq K$, $\mathcal{O}_0 := \mathrm{End}(E_0)$ and $\mathcal{O} := \mathrm{End}(E)$. Then have that $\mathcal{O} \subseteq \mathcal{O}_0 \subseteq \mathcal{O}_K$ with $[\mathcal{O}_0 : \mathcal{O}] = l^{O(\log(p))}$ and $l \nmid [\mathcal{O}_K : \mathcal{O}_0]$.

Now we are in one of the following cases:

(I) - "bad" E_0 is defined over $\mathbb{F}_p$, i.e. $E_0^{(p)} = E_0$; Then $\Phi_n(j(E), j(E)^p) = 0$

(II) - "probably good" $E_0^{(p)}$ is (nontrivially) l-isogeneous to E_0, i.e. they are two distinct vertices on the crater; Then it is likely that $\Phi_n(j(E), j(E)^p) \neq 0$, but that depends on the distance in the crater

(III) - "good" $E_0^{(p)}$ is not l-isogeneous to E_0; Then $\Phi_n(j(E), j(E)^p) \neq 0$

1.1 Analyzing (III)

Now consider only E_0 and denote $\mathcal{O} := \mathcal{O}_0$ and $E := E_0$.

Let $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ such that $[\mathfrak{a}].E = E^{(p)}$. We have (III) if and only if $[\mathfrak{a}]$ contains no integral ideal of index l^r, for any $r \in \mathfrak{N}$. Assume it does, say $\mathfrak{b}$. Then $\mathfrak{b} = \alpha\mathfrak{a}$ for some $\alpha \in \mathfrak{a}^{-1}$ with

$$\mathfrak{N}(\alpha) = \frac{\mathfrak{N}(\mathfrak{b})}{\mathfrak{N}(\mathfrak{a})} = \frac{l^r}{\mathfrak{N}(\mathfrak{a})}$$

Since we do not require α to be integral, we can substitute α by α/l and so find that

$$\mathfrak{N}(\alpha) = \mathfrak{N}(\mathfrak{a})^{-1} \quad \text{or} \quad \mathfrak{N}(\alpha) = l\mathfrak{N}(\mathfrak{a})^{-1}$$

This leads us to the interesting (slightly weaker) question: When does there exist some $\alpha \in K$ with $\mathfrak{N}(\alpha) = N$ for some (square-free) N?

1.2 Preventing (I)

Consider an ordinary Elliptic Curve $E/\mathbb{F}_{p^2}$ and let π be the $q = p^2$-th power Frobenius. Then π satisfies $\pi^2 - t\pi + q = 0$ where $t = q + 1 - \#E(\mathbb{F}_q)$ is the trace of Frobenius. By the Hasse bound, we derive the standard bound

$$|t| \leq 2\sqrt{q} = 2p$$

Now consider the Endomorphism ring $\mathcal{O} = \mathrm{End}(E)$ in the number field $\mathcal{K} := \mathcal{O} \otimes \mathbb{Q}$. We have that $\mathbb{Z}[\pi] \subseteq \mathcal{O}$ and so $[\mathcal{O}_\mathcal{K} : \mathcal{O}] \leq [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi]]$. Now note that the discriminant of $\mathbb{Z}[\pi]$ is

$$D := d(\mathbb{Z}[\pi]) = t^2 - 4q$$

and so $-4q \leq D \leq 0$[1]. Now we use the standard fact on modules

$$d(\mathcal{O}_\mathcal{K})[\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi]]^2 = d(\mathbb{Z}[\pi])$$

and find that $[\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi]] \leq \sqrt{|d(\mathbb{Z}[\pi])|} = 2p$. After these preliminaries, we can consider the approach itself.

1.3 Choosing parameters

Let l be a prime $> 2p$ and $e = O(\log(p))$. Now consider a root $j \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ of $\Phi_{l^e}(X, X^p)$ and an Elliptic Curve E with j-invariant j. We claim that case I cannot occur.

Suppose E is ordinary. Then there is the standard ascending chain of l-isogenies

$$E \to ... \to E_0$$

such that E_0 lies on the crater, i.e. $l \nmid [\mathcal{O}_\mathcal{K} : \mathrm{End}(E_0)]$ where $\mathcal{K} = \mathrm{End}^0(E) = \mathrm{End}^0(E_0)$. However, since $[\mathcal{O}_\mathcal{K} : \mathrm{End}(E)] \leq [\mathcal{O}_\mathcal{K} : \mathbb{Z}[\pi]] \leq 2p$ where π is the q-th power Frobenius of E, we see that $l \nmid [\mathcal{O}_\mathcal{K} : \mathrm{End}(E)]$. Thus $E = E_0$.

However, we chose $j \notin \mathbb{F}_p$ and so $E = E_0$ is not defined over $\mathbb{F}_p$. Thus $E_0^{(p)} \neq E_0$, which excludes case I.

[1] In fact, since E is ordinary, we have $D \not\equiv 0 \mod p$, but that does not matter here.

Current idea

I still have to make (much) more experiments, but somehow, case II seems strange - possibly it does not even occur (I have not encountered it so far). If this is really the case (or if it is really rare), then we can just choose $l > 2p$ prime and $e = O(\log(p))$ and find a root $j \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ of $\Phi_{l^e}(X, X^p)$.

In other words, compute $F := \Phi_{l^e}(X, X^p) \mod X^q - X$ and then find a root of

$$\frac{F}{\gcd(F, X^p - X)}$$

Of course, $\deg(F) = \Theta(\log(p))$ is still exponential, so it will not work out easily...