Finding torsion bases on elliptic curves over Finite Fields

Márton Tot Bagi

7th January 2025

Motivation

- Isogeny-based cryptography is a promising post-quantum alternative
- Evaluation isogenies between supersingular elliptic curves is efficient if kernel is rational
- When the kernel is not rational it is tricky to implement computations efficiently
- PEARL-SCALLOP (Allombert, Biasse, Eriksen, Kutas, Leonardi, Page, Scheidler, Tot Bagi): isogeny-based group action where the unerlying class group can be computed more efficiently as in CSIDH but is faster than SCALLOP and SCALLOP-HD
- There is a precomputation step which requires the evaluation of a single isogeny with non-rational kernel, however, if implemented naively computations will not finish in reasonable time

Introduction

- We will focus on elliptic curves of the form $E : y^2 = x^3 + ax + b$ over finite fields, with characteristic $p \neq 2, 3$
- We know that for any $p \nmid m$ the m-torsion group of E, $E[m]$, has the structure: $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$
- For an elliptic curve E defined over $\mathbb{F}_q$ we will denote the Frobenius endomorphism with $\pi_q : (x, y) \mapsto (x^q, y^q)$

A basic algorithm

Problem

Let E be an elliptic curve over $\mathbb{F}_q$ and assume that $E[m]$ is $\mathbb{F}_q$-rational. Find a basis of $E[m]$.

- The general strategy here is to find P, Q m-torsion points and check whether they generate the m-torsion (using the Weil-pairing)
- If not, find a new Q
- Basically this reduces the problem of finding an element of order m (and computing the order of an element)

Finding a point of order m

- Let us denote the order of the point P by $o(P)$
- Let P be a random ($\mathbb{F}_q$-rational) point on ET
- Let $Q = (\#E(\mathbb{F}_q)/m^2) \cdot P$
- If $o(Q) = m$ or $o(Q) = m^2$ done, else repeat
- Small improvement, instead of just multiplying by $\#E(\mathbb{F}_q)/m^2$, we can do the following:
- Write $\#E(\mathbb{F}_q) = c \cdot d$, where c is the largest divisor of $\#E(\mathbb{F}_q)$ relative prime to m
- Then $R = (o(Q)/m) \cdot Q$, where $Q = c \cdot P$, with P a random point

Finding the order of a point

- Let Q be a point on E over $\mathbb{F}_q$
- We want to find it's order $o(Q)$
- We know, that $\#E(\mathbb{F}_q) \cdot Q = \mathcal{O} \implies o(Q) | \#E(\mathbb{F}_q)$
- Let $\#E(\mathbb{F}_q) = \prod_{i=1}^{s} p_i^{\alpha_i}$
- ($\#E(\mathbb{F}_q)$ can be replaced by another multiple of the order, if we know one, as we do above)
- Let $Q_i = (\#E(\mathbb{F}_q)/p_i^{\alpha_i}) \cdot Q$, we know that $o(Q_i) | p_i^{\alpha_i}$
- Finding $o(Q_i)$: we need the smallest (positive) j, such that $p_i^j \cdot Q_i = \mathcal{O}$
- $o(Q) = \prod o(Q_i)$
- Number of additions and doublings: $O(s \log(\#E(\mathbb{F}_q)))$

A faster algorithm

- Let $\#E(\mathbb{F}_q) = \prod_{i=1}^{s} p_i^{\alpha_i}$ as before
- If $s = 1$, find the order of Q the same way as before
- Else let $R = \prod_{i=1}^{\lfloor s/2 \rfloor} p_i^{\alpha_i} \cdot Q$, find the order of R recursively
- (We know that $o(R) | \prod_{i=\lfloor s/2 \rfloor + 1}^{s} p_i^{\alpha_i}$)
- Let $T = o(R) \cdot Q$, find it's order recursively
- $(o(T) | \prod_{i=1}^{\lfloor s/2 \rfloor} p_i^{\alpha_i})$
- $o(Q) = o(R) \cdot o(T)$
- Only $O(\log(s) \log(\#E(\mathbb{F}_q)))$ additions and doublings
- Needs storing $\log(s)$ points, while the first algorithm needed only 2 points

Division field I

- Now what if we don't know that the m-torsion is rational?
- More generally, the m-division field is the smallest extension of $\mathbb{F}_q$ over which the m torsion is rational.

Problem

Let E be an elliptic curve over $\mathbb{F}_q$. Find the degree of the m-division field.

Division field II

- One way to find it, is the division polynomial
- The division field is either the splitting field of the division polynomial, or a 2 degree extension of it
- However deciding between the two cases is expensive
- There exists a faster algorithm when m is an odd prime [vT97]

Division field and the Frobenius endomorphism

- The algorithm utilizes the following facts:
- $\pi_q^n = \pi_{q^n}$, that is the n-th power of the Frobenius, is the Frobenius over the n-th degree extension of $\mathbb{F}_q$
- π_{q^n} acts as the identity on the m-torsion $\iff$ $E[m] \subseteq E(\mathbb{F}_{q^n})$
- Hence, the order of $\pi_q|_{E[m]}$ = the degree of the m-division field
- With the help of the minimal polynomial of the Frobenius, it can calculate the order of the Frobenius

Division field of prime powers I

- Let $r = m^k$ an odd prime power
- Assume that the m^{k-1}-torsion is $\mathbb{F}_q$-rational
- Let P, Q be the basis of the r-torsion (not nessecarily defined over $\mathbb{F}_q$)
- We want to find $o(\pi_q|_{E[r]})$, which is the smallest j, such that $\pi_q^j(P) = P$ and $\pi_q^j(Q) = Q$

Division field of prime powers II

- Because the m^{k-1}-torsion is $\mathbb{F}_q$-rational, we know that $m \cdot \pi_q(P) = \pi_q(m \cdot P) = m \cdot P$
- This means that we can write $\pi_q(P) = P + P'$, where P' is an m-torsion point
- From this we can see, that

$$\pi_q^s(P) = \pi_q^{s-1}(P + P') = \pi_q^{s-1}(P) + P' = \cdots = P + s \cdot P'$$

- The r-division field degree is either 1 or m
- We can decide between the two cases using the division polynomial
- From this we get an algorithm for every odd composite number

Thank you for your attention!

A van Tuyl.
The field of N-torsion points of an elliptic curve over a finite field.
PhD thesis, M. Sc. Thesis, McMaster University, 1997.

Why the algorithm for primes cannot be extended to composites

- We can determine the $\pi_q|_{E[r]}$ just by the image of a basis of the m-torsion
- Hence we can view $\pi_q|_{E[m]}$ as an element of $GL_2(m)$
- If m is prime, there exists a Jordan normal form of $\pi_q|_{E[m]}$, whose order is the same as the order of the Frobenius and it's order can be determined (mostly) by the minimal polynomial of the Frobenius
- If m is not prime, there is no Jordan normal form

Random torsion points are not uniformly random

- Let us denote by $E[m^\infty]$ the points, which are contained in an m^k-torsion for some k. (Formally: $E[m^\infty] = \{P \in E : \exists k \in \mathbb{Z}_+ m^k\}$
- If the structure of $E[m^\infty] \cap E(\mathbb{F}_q)$ is not "nice" (i.e. not $(\mathbb{Z}/r\mathbb{Z})^2$ for some $m|r$), then choosing a random point with order m via the method explained will not result in a uniform distribution.
- This can cause problems: for example, if $E[m^\infty] \cap E(\mathbb{F}_q) \simeq \mathbb{Z}/m^2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, then almost all of the "random" points of order m will come from a specific subgroup, not generating the m-torsion
- This can be fixed by finding a basis for $E[m^\infty] \cap E(\mathbb{F}_q)$ instead of $E[m]$. This is a bit more complicated and involves a (in our case not too difficult) discrete logarithm, but overall not much more expensive than the previous algorithm

Random point and square root

- Choosing a random point works by choosing a random x, then checking whether $x^3 + ax + b$ has a square root in $\mathbb{F}_q$
- The current algorithm implemented for square root finding in PARI is the Tonelli-Shanks algorithm, whose complexity depends on r^2, with $q - 1 = 2^r \cdot w$, with w odd
- There exists however an algorithm with better asymptotic complexity, which also presents a big improvement in practice [?]
- It's runtime does not depend on r

Random point and square root II

- Let $a \in \mathbb{F}_q$. Find $x \in \mathbb{F}_q$, such that $x^2 = a$ (assume that such an x exists)
- Let $\beta = \sum_{i=0}^{n-1} x^{p^i}$, the trace of x. The main idea is that we can calculate β^2 efficiently using only a
- $\beta^2 \in \mathbb{F}_p$, where we can find β with an existing algorithm
- From β we can recover x