Note on Computational Elliptic Curves

Lei Bichang

March 13, 2025

These notes are based the course taught by Prof. Benjamin Wesolowski at ENS Lyon in 2025.

Basics

In $\mathbb{Z}$ and $\mathbb{F}_p$[1], addition and multiplication are "easy"[2].

Extended GCD algorithm

Algorithm 1: Extended GCD

Input: $a, b : \mathbb{Z}_{\geq 0}$
Output: $\gcd(a,b), u, v : \mathbb{Z}$ s.t. $\gcd(a,b) = ua + vb$

```
(x, u, v, y, u', v') ← (a, 1, 0, b, 0, 1)
while y > 0 do
    (x, y) ← (x mod y, ⌊x/y⌋)
    if r < y − r then
        (x, u, v, y, u', v') ← (y, u', v', r, u − qu', v − qv')
    else
        (x, u, v, y, u', v') ← (y, u', v', y − r, (q + 1)u' − u, (q + 1)v' − v)
return (x, u, v)
```

- Complexity $= O(\log(a)\log(b))$.
- It applies to $k[X]$, so it applies to general $\mathbb{F}_{p^r}$; the output is up to a factor in $\mathbb{F}_p^\times$.

Exponentiation

Let G be a group.

Algorithm 2: Square and Multiply

Input: $g : G$, $m = (m_i m_{i-1} \ldots m_0)_2 : \mathbb{Z}_{\geq 0}$
Output: $g^m : G$

```
z ← x for j = i − 1, i − 2, …, 0 do
    z ← z² if m_j = 1 then
        z ← z · x
return z
```

- Complexity $= O(\log(m))$, depending on the complexity of multiplication in G.

[1] Any $x \in \mathbb{F}_p$ can be represented by $\log(p)$ bits.
[2] $\exists$ polynomial (in length of input) time algorithm.

Elliptic Curves

1 Factoring polynomials over a finite field

Problem 1.1. Factorize $f(X) \in \mathbb{F}_q[X]$.

Let's start with a simpler question: how to find linear factors of f? This is equivalent to factorize

$$g(X) := \gcd(f(X), X^q - X) = \prod_{\substack{r \in \mathbb{F}_q \\ f(r)=0}} (X - r).$$

Note that the map $(\cdot)^{\frac{q-1}{2}}$ on $\mathbb{F}_q^7\times$ is the Legendre symbol $\left(\frac{\cdot}{q}\right)$. Hence for $u(X) \in \mathbb{F}_q[X]$, we have

$$g_u(X) := \gcd(g(X), u(X)^{\frac{q-1}{2}} - 1) = \prod_{\substack{f(r)=0 \\ u(r) \in (\mathbb{F}_q^\times)^2}} (X - r).$$

If we take a linear polynomial $u(X) = X + \delta$, then $g_u(X)$ is a nontrivial factor of $g(X)$ if and only if there are roots $\alpha \neq \beta$ of $f(X)$ such that $\alpha + \delta \in (\mathbb{F}_q^\times)^2$ and $\beta + \delta \notin (\mathbb{F}_q^\times)^2$.

Theorem 1 (Robin)**.** If $\alpha \neq \beta \in \mathbb{F}_q$, then

$$\#\{\delta \in \mathbb{F}_q \mid \alpha + \delta \neq 0, \beta + \delta \neq 0;\ \text{one is a square, the other isn't}\} = \frac{q-1}{2}.$$

Proof. Let

$$\psi : \mathbb{F}_q \setminus \{-\beta\} \to \mathbb{F}_q \setminus \{1\} \quad \delta \mapsto \frac{\alpha + \delta}{\beta + \delta}.$$

ψ is injective, hence bijective. Meanwhile, so the condition on LHS is equivalent to

$$\psi(\delta)^{\frac{q-1}{2}} = -1.$$

There are $\frac{q-1}{2}$ elements in $\mathbb{F}_q \setminus \{1\}$ has this property. □

Corollary 1.1. For a uniformly random $\delta \in \mathbb{F}_q$,

$$\Pr\left[\gcd(g(X), (X+\delta)^{\frac{q-1}{2}} - 1) \text{ is a nontrivial factor of } g(X)\right] \geq \frac{(q-1)/2}{q} \geq \frac{1}{3}.$$

Algorithm 3: Partial Factorization

Input: $g(X) : \mathbb{F}_q[X]$, $\deg(g) > 1$, only different linear factors over $\mathbb{F}_q$
Output: one nontrivial factorization of $g(X)$
repeat
  $\delta \leftarrow$ uniformly random in $\mathbb{F}_q$
  $g_1(X) \leftarrow \gcd(g(X), (X+\delta)^{\frac{q-1}{2}} - 1)$ **if** $0 < \deg g_1(X) < \deg g$ **then**
    return $\left(g_1(X), \frac{g(X)}{g_1(X)}\right)$
until;

Algorithm 4: Factorization

Input: $g(X) : \mathbb{F}_q[X]$, only different linear factors over $\mathbb{F}_q$

Output: Complete factorization of $g(X)$

if $\deg g = 1$ **then**

  return g

else

  $(g_1, g_2) \leftarrow$ PartialFactorization(g)

  return *(Factorization(g_1), Factorization(g_2))*

- # of calls to "PartialFactorization" is $\deg(g) - 1$.
- It is hard to analyze the precise complexity, as it is affected by the pattern of g.

How to get higher degree factors? We can get the multiplicity of linear factors[3] then consider

$$f_{\geq 2}(X) := \frac{f(X)}{\prod \text{linear factor}}.$$

Now

$$\gcd(f_{\geq 2}(X), X^{\frac{q^2-1}{2}} - 1)$$

is the product of all quadratic factors, because quadratic factors are linear factors over $\mathbb{F}_{q^2}$. Continuely raise the degree until we get the factorization.

2 Counting rational points of an elliptic curve over a finite field

Problem 2.1. Calculate $\#E(\mathbb{F}_q)$ for an elliptic curve E over $\mathbb{F}_q$.

[3]A naïve way: divide the factor until it is not a root.