Nov18

Wednesday, November 17, 2021 6:39 PM

Defⁿ $p \geq 3$ odd prime

An elliptic curve E over $\mathbb{F}_p$ is the set of points $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ satisfying

$$y^2 \equiv x^3 + ax + b \mod p$$

for $4a^3 + 27b^2 \not\equiv 0 \mod p$

together w/ O @ ∞.

$$E = \{(x, y) \in \mathbb{F}^2 \mid y^2 \equiv x^3 + ax + b \mod p\} \cup \{O\}$$

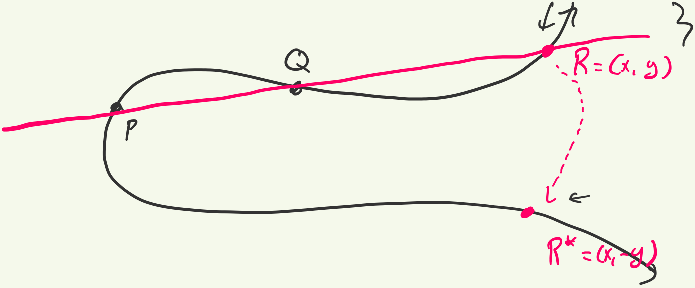
Example

$$y^2 \equiv x^3 + x + 2 \quad \text{over} \quad \mathbb{F}_p$$

$$\Rightarrow E = \{(1,1), (1,2), (2,0), O\}$$

Group Law

Over $\mathbb{R}$

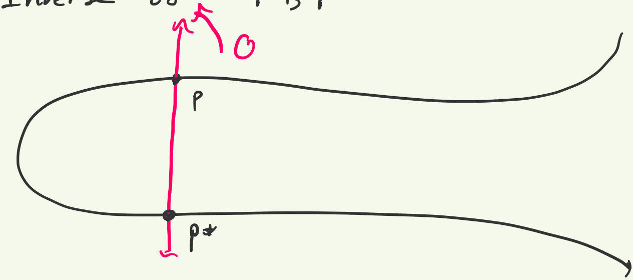


$$P \oplus Q = R^*$$

$$(P \oplus Q \oplus R = \mathcal{O})$$

$\mathcal{O}$ identity.

Inverse of P is P^*



Recall

The elliptic curve addition law can be expressed purely algebraically.

So we can do the algebra over $\mathbb{F}_p$, & get a group law for $E(\mathbb{F}_p)$

Elliptic Curve Addition Algorithm (over $\mathbb{F}_p$)

Input:
- E: elliptic curve over $\mathbb{F}_p$
  $y^2 = x^3 + ax + b$
- $P, Q \in E(\mathbb{F}_p)$

Output: $P \oplus Q$

① If $P = \mathcal{O} \Longrightarrow P \oplus Q = Q$

② If $Q = \mathcal{O} \Longrightarrow P \oplus Q = P$

Rmk

$\mathcal{O} \neq (0,0)$

$\mathcal{O} =$ pt @ ∞
$=$ identity of E

③ Set $P = (x_1, y_1)$
$Q = (x_2, y_2)$ ←

④ If $\underline{x_1 = x_2}$ & $\underline{y_1 \equiv -y_2}$ mod p ← prime

Then $P \oplus Q = \mathcal{O}$ $= \frac{y_1 - y_2}{x_1 - x_2}$

⑤ Set

$$\lambda = \left\{ \begin{array}{ll} \frac{y_2 - y_1}{x_2 - x_1} \leftarrow & \text{if } \underline{P \neq Q} \\ \frac{3x_1^2 + a}{2y_1} \leftarrow & \text{if } P = Q \\ \cancel{2} & \end{array} \right\} \begin{array}{l} \text{division} \\ \text{modulo} \\ p \\ (\text{ext. euc.} \\ \text{alg.}) \\ \uparrow \\ O(\log(p)) \end{array}$$

$$P \oplus Q = (x_3, y_3)$$

$$x_3 = \lambda^2 - x_1 - x_2 \quad \leftarrow$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad \leftarrow$$

Theorem

This algorithm runs & makes $E(\mathbb{F}_p)$ into an abelian group w/ identity $\mathcal{O}$ & invers $-(x,y) = (x,-y) = (x, p-y)$

Proof

Steps 1–4 gives id inverse.

Hard part is associativity. ∎

Example

$$y^2 = x^3 + \overset{\downarrow}{x} + 2 \quad / \mathbb{F}_3$$

$$E = \{(1,1), (1,2), (2,0), \mathcal{O}\}$$

$$(1,1)\oplus(1,2) \underset{\overset{\uparrow}{④}}{=} \mathcal{O} \qquad y_2 = 2 \equiv -1 \mod 3$$
$$= -y_1$$

$$(1,1)\oplus(2,0) \underset{\overset{\uparrow}{⑤}}{=} (1,2) \leftarrow$$

$$\lambda = \frac{0-1}{2-1} = \frac{-1}{1} = -1 \equiv 2 \mod 3$$

$$x_3 = \lambda^2 - x_1 - x_2 = 4 - 1 - 2 = 1$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$= 2(1-1) - 1 = -1 \equiv 2 \mod 3$$

$$(1,1)\oplus(1,1) = 2(1,1)$$

$$\lambda = \frac{3x_1^2 - a}{2y_1} = \frac{3-1}{2} = \frac{2}{2} = 1$$

$$x_3 = \lambda^2 - x_1 - x_2 = 1 - 1 - 1 \equiv 2 \mod 3$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = 1(1-2) - 1$$
$$= -3 \equiv 0 \mod 3$$

$$\underline{(1,1)\oplus(1,1) = (2,0)} \leftarrow$$

Exercise. Compute $\underline{(2,0)\oplus(2,0)}$.

- Prove $(x,0) \in E$

$\Longrightarrow \quad (x,0) \oplus (x,0) = \mathcal{O}$

(Say $(x,0)$ is 2-torsion or has order 2)

The Elliptic Curve Discrete Log Problem

Recall

Classical discrete log

$$\left.\begin{array}{l} g \in \mathbb{F}_p^* \quad \text{(a primitive root)} \\ h \in \mathbb{F}_p^* \end{array}\right\} \text{public}$$

$$x \quad \text{s.t.} \quad g^x \equiv h \mod p \Big\} \text{ secrete.}$$

Hard problem

Given g, h find $x := \log_g h$

This works for any group!

Let's see what this looks like for an elliptic curve.

⚠ Elliptic curves are written additively.

$$P + Q = P \oplus Q$$

So doing group law n-times

$$\underbrace{P + P + P + \cdots + P}_{n\text{-times}} = \underset{\substack{\uparrow \\ \text{integer}}}{n}\,\underset{\substack{\nwarrow \\ \text{point.}}}{P}$$

⚠ Not standard multiplication

Def$^{\underline{n}}$ E elliptic curve. $n \in \mathbb{Z}$. $P \in E$

$$nP := \begin{cases} \underbrace{P + \cdots + P}_{n\text{-times}} & n > 0 \\ \underbrace{-P + \cdots + -P}_{|n|\text{-times}} & n < 0 \\ \mathcal{O} & n = 0 \end{cases}$$

Def$^{\underline{n}}$ The elliptic curve discrete log problem (ECDLP)

is, given elliptic curve E, points $P, Q \in E$ s.t.

$$nP = Q$$

Find n.

If such an n exists it is called the elliptic discrete log base P of Q $(Q \div P)$

$$n = \log_P Q$$

Remarks

① There may be points $P, Q \in E$ s.t. there is no n w/ $nP = Q$

Ex E as above

$$2(2,0) = (2,0) \oplus (2,0) = \mathcal{O}$$

$$3(2,0) = 2(2,0) + (2,0) = \mathcal{O} + (2,0) = (2,0)$$

$$\vdots$$

$$n(2,0) = \begin{cases} (2,0) & n \text{ odd} \\ \mathcal{O} & n \text{ even.} \end{cases}$$

No $\log_{(2,0)}(1,1)$

② Also notice $3\cdot(2,0) = 1\cdot(2,0)$

⇝ is log even well defined?

(also saw this for $\mathbb{F}_p^*$ log defined mod $p-1$).

Prop If $\exists\, n$ w/ $nP = Q \Rightarrow \exists\, \infty$-ly many.

Pf/ $\exists\, s \neq 0$ s.t. $sP = 0$. ($E(\mathbb{F}_p)$ is a finite group...)

$P, 2P, 3P, \ldots$ have to repeat.

So $\exists\, i \neq j$ w/ $iP = jP$

$$\Longrightarrow (i-j)P = \mathcal{O}$$

Let $s_0 := \min\{s > 0 \text{ w/ } sP = 0\} = |P|$

$= \text{order of } P$

$\underline{n_0 P = Q} \implies$

$nP = Q \iff n = (\underline{n_0 + i \cdot \overset{\checkmark}{s_0}})$ $\quad i \in \mathbb{Z}$

Pf/ $\Leftarrow$ $(n_0 + i s_0)P = n_0 P + i(s_0 P)$

$= Q + i \cdot 0 = Q$

$\Longrightarrow$ $nP - n_0 P = Q - Q = 0$

$\quad\;\; \|$

$(n - n_0)P = 0$

$\overset{HW}{\Longrightarrow}$ $|P| \mid (n - n_0)$

so $n - n_0 = i s_0$ so $n = n_0 + i \cdot s_0$ $\emptyset$

The $\log_P Q$ is well defined modulo $s_0 = |P|$

i.e. $\log_P Q \in \mathbb{Z}/s_0\mathbb{Z} = \mathbb{Z}/|P|\mathbb{Z}$

(Analogy in $\mathbb{F}_p^*$ $\log_g h \in \mathbb{Z}/|g|\mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z}$) HW

Prop

$$\log_P : \langle \overset{\substack{E(\mathbb{F}_p) \\ \vee\!|}}{\underset{\substack{\| \\ \{P, 2P, 3P, \dots\}}}{P}} \rangle \longrightarrow \mathbb{Z}/|P|\mathbb{Z}$$

is a well defined group homomorphism

$$\log_P(Q_1+Q_2) = \log_P Q_1 + \log_P Q_2$$

⚠ Book defines $E(\mathbb{F}_p) \longrightarrow \mathbb{Z}/s\mathbb{Z}$

but this is not true in general bc $E(\mathbb{F}_p)$ may not have a single generator.

Example as above

$$E = \{\underset{P}{\underset{\shortparallel}{(1,1)}}, \underset{Q}{\underset{\shortparallel}{(1,2)}}, \underset{R}{\underset{\shortparallel}{(2,0)}}, \mathcal{O}\}$$

$$\log_P Q = 3$$

$$2P = P \oplus P = (1,1) \oplus (1,1) = (2,0) = R$$

$$3P = P + P + P = P + 2P = P + R$$

$$= (1,1) + (2,0) = (1,2) = Q$$

Lagrange $\Rightarrow$ $\underset{\underset{3}{\vee}}{|P|}$ divides $\# E(\mathbb{F}_p) = 4$

so

$$|P| = 4 \quad \& \quad \langle P \rangle = E(\mathbb{F}_p)$$

Making This Computationally Effective

Given P, Q w/ $nP = Q$, seems hard to recover n.

Idea: compute

$$P,\ 2P,\ 3P,\ 4P,\ \ldots,\ \underset{\overset{\shortparallel}{Q}}{nP} \longleftarrow$$

then it is

Recall $\#E(\mathbb{F}_p) \approx p+1 = O(p)$

Make p large $\Longrightarrow$ $E(\mathbb{F}_p)$ large which makes search alg. $O(p)$ ← Too slow!

But....

our goal (as alice) is

① Take public P

② Secret n

③ Compute $\underline{\underline{Q = nP}}$

publish ① & ③

We need a function

$$\begin{aligned} \mathbb{Z} &\longrightarrow E(\mathbb{F}_p) \\ n &\longmapsto nP \end{aligned}$$

that is fast.

doing $\underbrace{P+P+P+\cdots+P}_{n\text{-times}}$

is too slow for us as well $O(p)$

TOO slow

Recall

Same problem / $\mathbb{F}_p^*$

developed fast powering.

Have a version for elliptic curves.

Double & Add

(analogy. Fast Power was Square & multiply)

$(E, +)$ $\qquad$ $(\mathbb{F}_p^*, \times)$

Idea: To compute nP

Step 1: Write n in binary. $\boxed{r = \lfloor \log_2 n \rfloor}$

$$\underline{n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + \dots + n_r \cdot 2^r}$$

$\mathcal{O}(\log n)$

$n_i \in \{0, 1\}$ $\qquad$ $n_r = 1$

Step 2: Compute r doublings of P

↳ one EC Add step.

$$\left.\begin{aligned} Q_0 &= P \\ Q_1 &= 2Q_0 = 2P \\ Q_2 &= 2Q_1 = 4P \\ &\vdots \\ Q_r &= 2 \cdot Q_{r-1} = 2^n \cdot P \end{aligned}\right\} \quad Q_i = 2^i \cdot P$$

Step 3

$$Q = nP = n_0 Q_0 + n_1 Q + \dots + n_r Q_r \quad \} \; r \text{ additions}$$

Pf/ $n_0 Q_0 + n_1 Q_1 + \dots + n_r Q_r$

$$= n_0 \cdot P + n_1 \cdot 2P + n_2 \cdot 4P + \dots + n_r \cdot 2^r P$$

$$= (n_0 + n_1 \cdot 2 + n_2 \cdot 4 + \dots + n_r \cdot 2^r) \cdot P$$

$$= n P$$

Rmk Also a "small" version.

Time Complexity

① Time complexity of $P+Q$ (or $P+P$)

$\rightarrow$ A fixed number of basic operations $O(1)$

$\rightarrow$ At most 1 division mod p $O(\log p)$

$$O(\log(p))$$

② Double & add

Step 1: $O(\log n) \underset{\uparrow \text{Pf/}}{=} O(\log p)$

$$n \le |\langle P \rangle| \le \#E(\mathbb{F}_p) \overset{\text{last time}}{=} O(p+\sqrt{p}) = O(p)$$

Recall $$\left.\begin{aligned} &\#E(\mathbb{F}_p) = p+1+t_p \\ &-2\sqrt{p} \le t_p \le 2\sqrt{p} \end{aligned}\right\}$$

Step 2: $\underbrace{\text{Double}}_{O(\log p)}$ r-times $r = O(\log p)$

$$\Longrightarrow O((\log p)^2)$$

Step 3 $\underbrace{\text{Add}}_{O(\log(p))}$ $\underline{r}$-times

$$\longrightarrow O((\log(p))^2)$$

Total: $O(\log p) + O((\log p)^2) + O((\log p)^2) =$

$$O((\log p)^2).$$

Attacks on ECDLP

- **Babysteps Giantsteps**

Recall

We proved correctness of babyGiant for any abstract groups DLP

Goal

Given E, P, Q w/ $Q = nP$

Find n.

Algorithm

① Fix $r > \sqrt{|P|} \approx \sqrt{p}$

$\left(\text{Guarantee, } r > \underset{\uparrow}{\sqrt{p+1+2\sqrt{p}}}\right) = O(\sqrt{p})$

② Make lists

$L_1: O, P, 2P, 3P, \dots, rP$

$L_2: Q, Q - rP, Q - 2rP, \dots, Q - r^2P$

③ Find intersection

$$iP = Q - jrP$$

$$\underbrace{(i+jr)}_{}P = iP + jrP = Q$$

↑ Found n !!!

Proof:

Show lists intersect.

We did this in september (october?).

Elliptic Curve Cryptography

⟶ Diffie-Hellman ⟵

⟶ Elgamal

⟶ DSA

Diffie-Hellman

Alice & Bob agree on p & $E/\mathbb{F}_p$.

& $P \in E(\mathbb{F}_p)$

Alice

1) secret n_A
2) Computes $Q_A = n_A \cdot P$

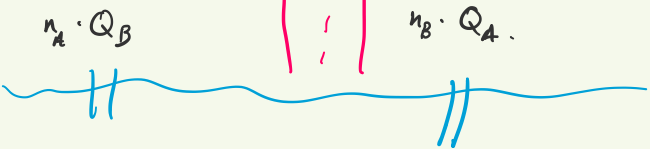
Eve

Bob

1) Secret n_B
2) computes $Q_B = n_B \cdot P$

3) Alice computes

3) Bob computes



$$n_A \cdot n_B \cdot P = n_B \cdot \underbrace{n_A \cdot P}_{}$$

Alice & Bob share a secret point of $E(\mathbb{F}_p)$.

Thanks