Elliptic curve cryptography

Elliptic curve $E: y^2 = x^3 + ax + b \mod p$

We work with "non-singular" curves

$$-16\,(4a^3 + 27b^2) \neq 0 \mod p$$

$\mathbb{Z}_p^*$ – multiplicative group mod p
will be substituted with a group defined by an elliptic curve.

Elliptic curve contains points which together with addition define a group

---

$P_1 = (x_1, y_1)$ $\qquad y_1^2 = x_1^3 + a x_1 + b$

$P_2 = (x_2, y_2)$ $\qquad y_2^2 = x_2^3 + a x_2 + b$

$P_1 + P_2 = P_3 = (x_3, y_3)$ $\qquad \boxed{E: y^2 = x^3 + ax + b}$

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

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

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P_1 \neq P_2 \\[2ex] \boxed{\dfrac{3x_1^2 + a}{2y_1}} & P_1 = P_2 \end{cases}$$

φ

if two points lie "above" each other

$P + P =$ [illegible] (O, ∞)

$P_1 + P_2 = \infty \quad (\mathcal{O})$

↳ Calligraphic $\mathcal{O}$

EXAMPLE Calculate $3P = ((P+P)+P)$ for $P = (0,1)$ (x_1, y_1)

and $E: y^2 = x^3 + 4x + 1 \mod 5$

Does P lie on E? $(P \in E)$

$$1^2 = 0^3 + 4 \cdot 0 + 1 \mod 5$$

$$1 = 1 \quad ✓$$

1.) $P + P = 2P = (x_3, y_3)$

$$X_3 = \lambda^2 - x_1 - x_1 \mod 5$$

$$\lambda = \frac{3x_1^2 + 4}{2 \cdot y_1} = \frac{3 \cdot 0^2 + 4}{2 \cdot 1} = \frac{4}{2} \mod 5$$

$$= 4 \cdot 2^{-1} \mod 5$$

$$= 2 \mod 5$$

$$x_3 = 2^2 - 0 - 0 = 4$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \mod 5$$

$$= 2(0-4) - 1 \mod 5$$

$$= 2 - 1 = 1 \mod 5$$

$2P = (4,1)$

$$1^2 = 4^3 + 4 \cdot 4 + 1 \mod 5$$

$$= -1 - 4 + 1$$

$$= -5 + 1 = 1 \quad ✓$$

$$3P = 2P + P = (4,1) + (0,1) = (x_3, y_3)$$

$x_3 = \lambda^2 - x_1 - x_2$ $\qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \bmod 5 = \frac{1-1}{4-1} = 0 \bmod p$

$= 0 - 4 - 0 = 1 \bmod 5$

$y_3 = 0(x_1 - x_3) - 1 = 4 \bmod 5$

$3P = (1,4)$ $\qquad (-1)^2 = x^3 + 4x + 1$

$1 \equiv 1^3 + 4 + 1$

$\equiv 5 + 1 \equiv 1 \bmod 5$ ✓

$K \cdot P$ - How many point additions do we need?

$\log_2 k$ $\qquad P, 2P, 4P, \ldots 2^i P$

$P = (x, 0)$

$P + P = \infty$

$P_1 = (x, y_1)$

$P_2 = (x, y_2)$ $\quad \Rightarrow \quad y_1 = -y_2$ $\qquad y^2 = \boxed{x^3 + ax + b}$

$\Rightarrow$ λ is not defined

$P_1 + P_2 = \infty$

if λ is not defined $P_1 + P_2 = \infty$ Clear geometric interpretation
(P_1 and P_2 are "above" each other
or $P_1 = P_2$ and $P = (x, 0)$)

(P_1 and P_2 are above each other or $P_1 = P_2$ and $P_1 = (x, 0)$)

$$P + \infty = P$$

$$P = (x_1, y) \in E$$

$$Q = (x_1, -y) \in E$$

$$P + Q = \infty$$

$$P = -Q$$

$$(P + Q + R) = (P + Q) + R = P + (Q + R)$$

NOW WE KNOW THAT $(E, +)$ forms a group

$$P + Q = Q + P \checkmark$$

NOW WE KNOW THAT $(E, +)$ forms a commutative group (Abelian)

Every commutative group is isomorphic to

$$\left[(\mathbb{Z}_{i_1} \times \mathbb{Z}_{i_2} \times \dots \times \mathbb{Z}_{i_n}), + \right]$$

How many elements $\prod_{j=1}^{n} i_j$

How many groups of size 4 are there?

$(\mathbb{Z}_4, +)$ $\qquad$ $(\mathbb{Z}_2 \times \mathbb{Z}_2), +$

$\{0,1,2,3\},+$

$3+3 \equiv 6 \equiv 2 \mod 4$

$2+2 = 4 \equiv 0 \mod 4$

$0+0 = 0$ ✓

$2+2 = 0$ ✓

$1+1 = 2$

$3+3 = 2$

$\{(0,0), (0,1), (1,0), (1,1)\}, +$

$(0,0)+(0,0) = (0,0)$

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

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

$(a,b)+(a,b) = (0,0)$ ✓

How many elements does $(E,+)$ have?

Hesse's theorem

E: mod p has N points

and $|N-p-1| \leq 2\sqrt{p}$

upper bound

$N-p-1 \leq 2\sqrt{p}$

$N \leq p + 2\sqrt{p} + 1$

lower bound

$-(N-p-1) \leq 2\sqrt{p}$

$-N+p+1 \leq 2\sqrt{p}$

$N \geq p - 2\sqrt{p} + 1$

$p = 5$

$N \leq 5+4+1 = 10$

$N \geq 5-4+1 = 2$

How many points $E: y^2 = x^3 + 4x + 1$ have?

is this a Quadratic Residue?

$\boxed{a^{\frac{p-1}{2}} = 1 \mod p}$

Euler's Criterion

x	$x^3+4x+1 \mod 5$	QR?	y

Euler's criterion

x	$x^3+4x+1 \bmod 5$	QR?	y	
0	1	✓	$(1,4)$	2
1	1	✓	$(1,4)$	2
2	2	×	—	
3	0	—	(0)	1
4	1	✓	$(1,4)$	2
				$+1$ (for ∞)

$y^2 = x^3+4x+1$ has 8 points.

There are 3 commutative groups of this size:

$(\mathbb{Z}_8, +)$ $\quad$ $(\mathbb{Z}_4 \times \mathbb{Z}_2), +$ $\quad$ $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2), +$

n	nP for $P=(0,1)$
1	$(0,1)$
2	$(4,1)$
3	$(1,4)$
4	$(3,0)$
5	$(1,1)$
6	$(4,4)$
7	$(0,4)$
8	∞

$\Rightarrow$ it is isomorphic to $(\mathbb{Z}_8, +)$

There is an isomorphism $f: E \to \mathbb{Z}_8$ s.t.

$$x + y = z$$
$$f(x) + f(y) = f(z)$$

$$f: nP \to n$$

$$aP + bP = (a+b)P$$

$$a+b \quad = \quad a+b$$

An example of two elliptic curves with the same number of points but a different structure:

$$y^2 = x^3 + 6x + 6 \mod 7 = \{(3,3),(3,4),(5,0),\infty\} = \mathbb{Z}_4, +$$

$$y^2 = x^3 + 6 \mod 7 = \{(1,0),(2,0),(4,0),\infty\} = (\mathbb{Z}_2 \times \mathbb{Z}_2), +$$

$$\boxed{\begin{array}{l} -16(4a^3 - 27b^2) \mod 7 \\ -16(0+27) \neq 0 \mod 7 \quad \checkmark \end{array}}$$

Discrete logarithm problem with EC

in $\mathbb{Z}_p^*$

$y = g^x \mod p$

find x given y, g, p

this is computationally hard

in $(E, +)$

$Q = x \cdot P$

finding x, s.t. holds is EC discrete logarithm equivalent

This is computationally hard

Why?

$|\mathbb{Z}_p^*| = p-1$ ✓ $\rightarrow$ this uses numbers of size $\log_2 p$

$|(E,+)| = p+1+2\sqrt{p} \rightarrow$ this uses numbers of size $\log_2 p$

We want E: mod p with a large number of points and a

We want E: mod p with a large number of points and a cyclic structure! (equivalent to $(\mathbb{Z}_n, +)$)

El Gamal encryption

$\mathbb{Z}_p^*$	$(E, +) \bmod p$
Public: p - a large prime	**Public:** $E: y^2 = x^3 + ax + b \bmod p$
q - a generator of $\mathbb{Z}_p^*$	P: generator of $(E, +)$
$y = q^x \bmod p$	$Q = x \cdot P$
Private: x	**Private:** x

Encryption of m

Choose a random $r \in \{2, \dots, p-2\}$

$$a = q^r \bmod p$$

$$b = m \cdot y^r \bmod p$$

Decrypt

$$m = b \cdot a^{-x} \bmod p$$

CORRECT

Encrypt point M

Choose a random number $r \in \{2, \dots, \mathrm{Order}(P)\}$

$$A = r \cdot P$$

$$B = M + r \cdot Q$$

$$M = B + (-x \cdot A)$$

$-x = x^{-1} \bmod \mathrm{Order}(P)$

Incorrect!

P has order K

$$B_t - x.A = M + r_0 Q - x.A$$
$$= M + r_0 x P - x.r_0 P$$
$$= M$$

Incorrect!

P has order k

$$n.P = (n \bmod k)\, P$$

$$k.P = \infty$$

$$Q + \infty = Q$$

$$\overbrace{\underbrace{P+P+P}_{\substack{k\\ \|\\ \infty}} + \underbrace{\dots}_{\substack{k\\ \|\\ \infty}} + \underbrace{P}_{n \bmod k}}^{n\text{- times}} \dots = (n \bmod k).P + \infty + \infty \dots = (n \bmod k).P$$

$$\ell.k+1$$

$$-xA = -\underbrace{x(x.P)}_{\equiv 1 \bmod k} = \overbrace{\underbrace{P+P+P}_{\substack{k\\ \|\\ \infty}} \underbrace{\dots}_{k} \underbrace{\dots}_{\substack{k\\ \|\\ \infty}} + P}^{\ell.k+1} = P$$

El Gamal Signatures

$\mathbb{Z}_p^*$ | $E \bmod p$

PUBLIC:

p - prime

q - generator of $\mathbb{Z}_p^*$

$y = q^x \bmod p$

Private: x

PUBLIC

$E \pmod p$

P - generator of $(E,+)$

$Q = x.P$

Private: x

$k = \text{Ord}(P)$

$k = Ord(P)$

Sign m:

1.) Choose r randomly from $\mathbb{Z}^*_{p-1}$

$$a = g^r \bmod p$$

$$b = r^{-1}(m - ax) \bmod (p-1)$$

Sign m:

Choose r randomly from $\mathbb{Z}^*_k$

$$A = r \cdot P = (a_1, a_2)$$

$$b = r^{-1} \cdot (m - a_1 x) \bmod k$$

Verify

$$y^a a^b \stackrel{?}{=} g^m \bmod p$$

Verify:

$$a_1 Q + b \cdot A = m P$$

$$a_1 \cdot x \cdot P + \underbrace{r^{-1}(m - a_1 \cdot x)}_{b} \cdot \underbrace{r \cdot P}_{A} =$$

$$a_1 \cdot x \cdot P + (m - a_1 \cdot x) \cdot P$$

$$a_1 \cdot x \cdot P + m \cdot P - a_1 x P$$

$$= m \cdot P$$

$\boxed{2.b}$ Pollard p-1 algorithm: TYPO IN SLIDES

$$\boxed{m = \prod_{q \mid q \text{ is a prime}} q^{\lfloor \log_q B \rfloor}}$$

← correct (slides $q^{\log n}$)

b

the smallest number divisible by all numbers $t < B$