Week 14

The DLP in $(G, \circ)$

Problem Instance: $I = (G, \alpha, \beta)$, where G is a finite group with group operation $\circ$, $\alpha \in G$ and $\beta \in H$, where $H = \{\alpha^i : i \geq 0\}$ is the subgroup of G generated by α.

Objective: find the unique integer a s.t. $0 \leq a \leq |H|-1$ & $\alpha^a = \beta$, where the notation α^a means

$$\underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{a \text{ times}}$$

We will denote this integer a by $\log_\alpha \beta$.

Generalized ElGamal Public-Key Cryptosystem

Let G be a finite group with group operation $\circ$, and let $\alpha \in G$ be an element s.t. the DLP in H is intractable where $H = \{\alpha^i : i \geq 0\}$ is the subgroup generated by α.

$\mathcal{P} = G$, $\mathcal{C} = G \times G$, & define $\mathcal{K} = \{(G, \alpha, a, \beta) : \alpha^a = \beta\}$ (secret)

- G, α, β are public
- a is secret
- for $K = (G, \alpha, a, \beta)$, & for a (secret) random number $k \in \mathbb{Z}_{|H|}$ define

$$e_K(x, k) = (y_1, y_2)$$

where $y_1 = \alpha^k$, $y_2 = x \circ \beta^k$

- for a ciphertext $y = (y_1, y_2)$, define

$$d_K(y) = y_2 \circ (y_1^a)^{-1}$$

p prime

Z_p^*, Z_{p-1}.

$(Z_p^*, \cdot)$ cyclic of order $p-1$.

isomorphic to $(Z_{p-1}, +)$

$\phi : Z_p^* \longrightarrow Z_{p-1}$.

DLP in Z_p^* $\alpha, \beta = \alpha^a \rightarrow$ find a

DLP in Z_{p-1} $\phi(\alpha), \phi(\beta) = a\,\phi(\alpha) \rightarrow$ find a is feasible.

$\phi(xy \bmod p) = (\phi(x) + \phi(y)) \bmod (p-1)$ Extended Euclidean Algm.

If we can find an efficient algm. to compute isomorphism ϕ, ⓓ we can solve DLP in $(Z_p^*, \cdot)$. → No known general method to efficiently compute the isomorphism ϕ.

Careful about the choice of your group

G

$H = \langle \alpha \rangle$ $\phi : H \rightarrow Z_{|H|}$

DLP in H can be solved efficiently

- DLP may be easy or difficult depending on the representation of the cyclic group that is used.
- Study other groups where DLP seems to be intractable.
  - $GF(p^n)$
  - Elliptic curve group.

Week 15

Elliptic Curves

- Let $p > 3$ be prime. The elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ is the set of solutions $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence

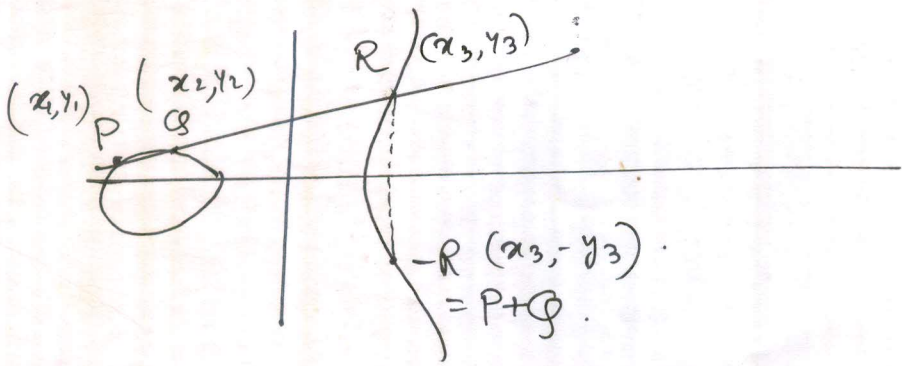
$$y^2 \equiv x^3 + ax + b \pmod{p},$$

where $a, b \in \mathbb{Z}_p$ are constants s.t. $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with a special point $\mathcal{O}$ called the point at infinity.

- Point Addition

$E/\mathbb{Z}_q : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}_p$, $4a^3 + 27b^2 \neq 0$.

We Defin: $P + \mathcal{O} = \mathcal{O} + P = P$ ($\mathcal{O}$ is the 3rd pt. of intersection of any vertical line with the curve.)



$$2y\frac{dy}{dx} = 3x^2 + a$$

$$\left.\frac{dy}{dx}\right]_{P=(x_1,y_1)} = \frac{3x_1^2 + a}{2y_1}$$

Chord & Tangent law:

PQ: $y = mx + \lambda$, $\lambda = y_1 - mx_1$, $m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q. \end{cases}$

$$(mx + \lambda)^2 = x^3 + ax + b.$$

$\Rightarrow x^3 - m^2x^2 - (2m - a)x + b - \lambda^2 = 0 \Rightarrow x_1 + x_2 + x_3 = m^2$

$P + Q\ (x_3, -y_3) \longrightarrow \therefore x_3 = m^2 - x_2 - x_1$, $y_3 = mx_3 + y_1 - mx_1$

$= \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) + y_1$

• $E/K : \quad y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0$
$a, b \in K, \; ch(K) \neq 2, 3.$

- if $P = (x_1, y_1) \neq \textcircled{H}$, then $-P = (x_1, -y_1)$.

- if $P = (x_1, y_1) \neq \textcircled{H}$, $Q = (x_2, y_2) \neq \textcircled{H}$, $P \neq -Q$,
then $P + Q = (x_3, y_3)$ with

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

where $$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ (3x_1^2 + a)/2y_1 & \text{if } P = Q, \; y_1 \neq 0. \end{cases}$$

- if $P = \textcircled{H}$, then $P + \textcircled{H} = \textcircled{H} + P = P$.

$\textcircled{H} \rightarrow$ additive identity
or
point at infinity.

$\rightarrow$ "third point of intersection" of any vertical line with the curve

Projective plane →

$$(\lambda X, \lambda Y, \lambda Z) \sim (X, Y, Z)$$

~~$(X_1, X_2, X_3) \sim X$~~

$$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$$

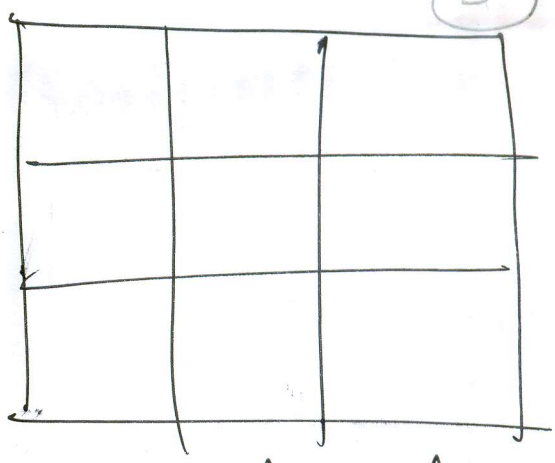
if

$X_1 = \lambda X_2$

$Y_1 = \lambda Y_2$

$Z_1 = \lambda Z_2$

for some scalar $\lambda \in k$.



equivalence classes of triples (X, Y, Z) (not all component zero)

↓

all scalar multiples of (X, Y, Z) are in the same equivalence class.

↓

this equivalence class is called projective point.

Projective point.

The equivalence class containing ~~the triple X_1~~ triple (X, Y, Z) is a projective point.

Case $Z \neq 0$ → Only one projective point

→ the class containing the triple $(x, y, 1)$.

$$(x, y, 1) \sim (X, Y, Z) \quad x = \frac{X}{Z}, \; y = \frac{Y}{Z}$$

- Thus projective plane is identified with all points (x,y) in ordinary (affine) plane

$\downarrow$ projection

the points for which $Z=0$.

↳ called line at infinity (in affine plane).

- $F(x,y)=0 \rightarrow$ a curve in affine plane.

$\downarrow$

projective equn. $\overline{F}(X,Y,Z)=0 \rightarrow$ satisfied by projective pts.

Substitute: $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$.

& multiply by power of Z to clear the denominators.

E/K: $y^2=x^3+ax+b$ in affine plane, $a,b \in K$. $4a^3+27b^2 \neq 0$. Ch. $K \neq 2,3$. ——— (1)

$Z \neq 0$

Set $x=\frac{X}{Z}$, $y=\frac{Y}{Z}$ ——— (2).

$$\frac{Y^2}{Z^2}=\frac{X^3}{Z^3}+a\frac{X}{Z}+b$$

projective eqn. $ZY^2=X^3+aXZ^2+bZ^3$ ——— (3) → is satisfied by all projective pts. (X,Y,Z) with $Z \neq 0$ for which (x,y) satisfy (1) with substitution (2).

$Z=0$ (3) $\Rightarrow 0=X^3 \Rightarrow X=0$ → (4). (0,1,0) → only equivalen class with both $X,Z=0$. cor. affine pt.

(5)

So, in projective plane

$(H) = (0,1,0)$.

↓

point of intersection of the y-axis with the line at infinity.

↓

point of infinity.

put $z=0$ in the projective eqn.

↓

intersection of all projective pts. with $z=0$ with the projective eqn

↓

intersn of the line at infinity with the projective eqn. $x=0, z=0$.

↓

intersn of the line at infinity with the y-axis.

Elliptic Curves

- K be a field & $\overline{K}$ its algebraic closure
  (if $K = F_q$, then $\overline{K} = \bigcup_{m \geq 1} F_{q^m}$)

- E/K : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$,
  $4(y + a_1x + a_3)$
  $a_1, a_2, a_3, a_4, a_6 \in K$ with no singular point.
  (Weierstrass equation).

- The set of K-rational points

$$E(K) = \{(x,y) \in K \times K\} \cup \{\mathcal{O}\}.$$

  where $\mathcal{O}$ is called the identity (also point at infinity).

- Simplified Weierstrass equation :

1. $ch(K) \neq 2, 3$:
   $y^2 = x^3 + ax + b$, $a, b \in K$, $4a^3 + 27b^2 \neq 0$.

2. $ch(K) = 2$:
   $y^2 + xy = x^3 + ax^2 + b$, $a, b \in K$, $b \neq 0$
   (non-supersingular)
   or
   $y^2 + cy = x^3 + ax + b$, $a, b, c \in K$, $c \neq 0$. (supersingular)

3. $ch(k) = 3$:

$y^2 = x^3 + ax^2 + bx + c$, $a, b, c \in k$

(cubic on the right has no multiple roots).

Group law

$E = E(\bar{k})$ given by Weierstrass eqn.

for all $P, Q \in E$

(i) $\oplus + P = P + \oplus = P$ ($\oplus$ serves as the identity)

(ii) $-\oplus = \oplus$.

(iii) if $P = (x_1, y_1) \neq \oplus$, then $-P = (x_1, -y_1 - a_1x_1 - a_3)$

$y(y + a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6$.

if (x_1, y_1) satisfy this eqn, then so does $(x_1, -y_1 - a_1x_1 - a_3)$.

(iv) (i.e. $P, -P$ are the only pts. on E with x-co-ordinate equal to x_1)

(iv) if $Q = -P$, then $P + Q = \oplus$.

(v) if $P \neq \oplus$, $Q \neq \oplus$, $Q \neq -P$, then $P + Q = -R$

where R is the third point of intersection of the line PQ (tangent PQ if $P = Q$) with the curve E.

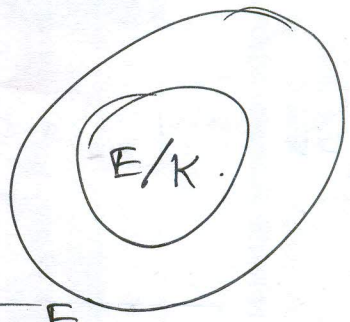
$\oplus \to$ pt. at infinity (if $Q = -P$, then $P + Q = \oplus$ $= -\oplus$)

$\to$ 3rd pt. of intersection of any vertical line with the curve E.

$E = E/\overline{K}$: Weistrass equⁿ.

Theorem

(i) $(E,+)$ is an abelian group with identity $\ominus$.



$E/\overline{K}$.

(ii) E/K is a subgroup of E.

a) (Closure) if $P, Q \in E$ then $P+Q \in E$.

b) (Associativity) if $P, Q, R \in E$ then $P+(Q+R) = (P+Q)+R$

c) (Identity) $P + \ominus = \ominus + P = P \quad \forall \; P \in E$.

d) (Inverse) for each $P \in E$, $\exists \; -P \in E$ s.t. $P+(-P) = (-P)+P = \ominus$.

e) (commutative) if $P, Q \in E$, then $P+Q = Q+P$.

Supersingular Elliptic curve

- E/F_q is supersingular if $p \mid t$ when

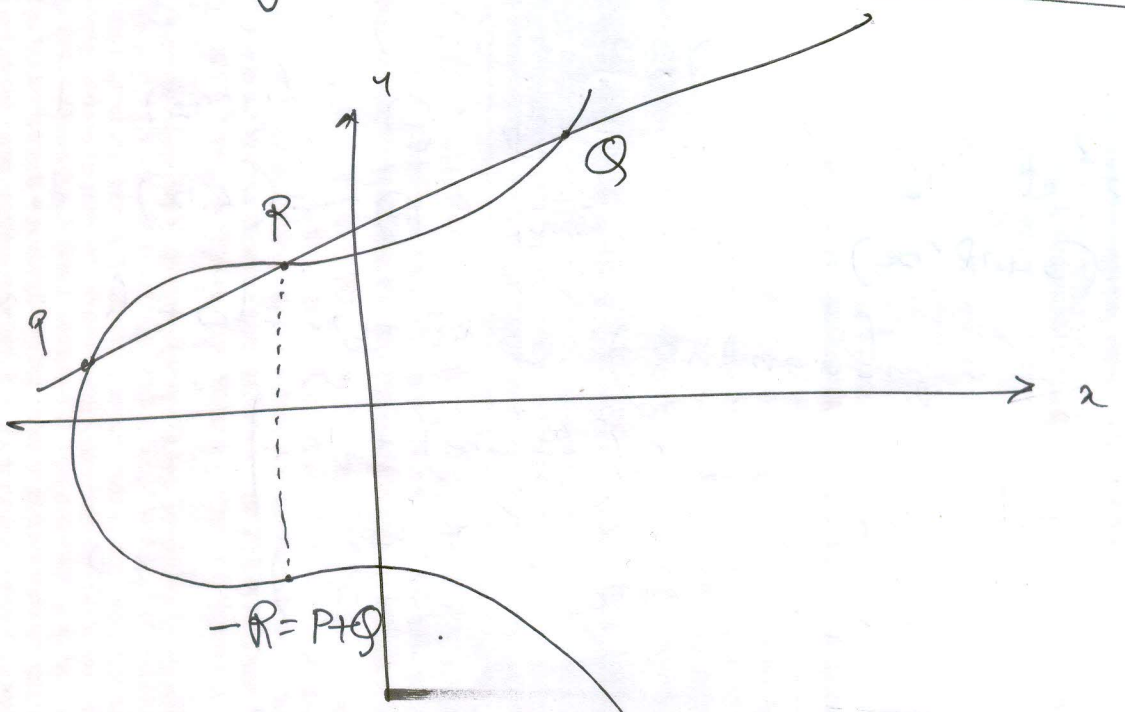
$$t = q+1 - \#E(F_q), \quad q = p^m, \quad p = ch(F_q),$$

a prime.

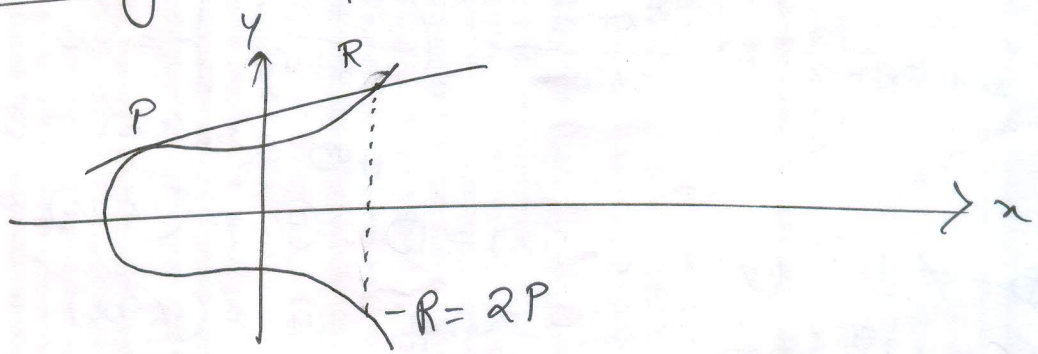
Theorem (Waterhouse) E/F_q is supersingular if

$$t^2 = 0, q, 2q, 3q \text{ or } 4q.$$

Adding two pts. P, Q on an elliptic curve



Doubling a pt. P on an elliptic curve



Addition formulae

- E/K : Weistrass eqn. $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$

if $P=(x_1,y_1)\neq \oplus$, then $-P=(x_1,-y_1-a_1x_1-a_3)$

if $P=(x_1,y_1)\neq \oplus$, $Q=(x_2,y_2)\neq \oplus$, $P\neq -Q$,

then $P+Q=(x_3,y_3)$ with

$$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2$$

$$y_3=-(\lambda+a_1)x_3-\beta-a_3$$

where

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & \text{if } P\neq Q\\[2ex] \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3} & \text{if } P=Q.\end{cases}$$

and $\beta=y_1-\lambda x_1$

- E/K : $y^2=x^3+ax+b$, $ch(K)\neq 2,3$.

if $P=(x_1,y_1)\neq \oplus$, then $-P=(x_1,-y_1)$.

if $P=(x_1,y_1)\neq \oplus$, $Q=(x_2,y_2)\neq \oplus$, $P\neq -Q$,

then $P+Q=(x_3,y_3)$ with

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

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

where $\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & \text{if } P\neq Q\\[2ex] (3x_1^2+a)/2y_1 & \text{if } P=Q.\end{cases}$ $\rightarrow$

$2P=\oplus$.
$\Rightarrow 16P=\oplus$

$y_1\neq 0$.
$P(x_1,y_1)$ with $y_1=0$
$\Rightarrow P=-P$ i.e. $2P=\oplus$.

• $E/K: \; y^2 + xy = x^3 + ax^2 + b$ (non supersingular), $ch(K) = 2$.

$y(y+x)$

if $P = (x_1, y_1) \neq \oplus$, then $-P = (x_1, y_1 + x_1)$.

if $P = (x_1, y_1) \neq \oplus$, $Q = (x_2, y_2) \neq \oplus$, $P \neq -Q$, then

then $P + Q = (x_3, y_3)$ with

$$x_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a & \text{if } P \neq Q \\ x_1^2 + \frac{b}{x_1^2} & \text{if } P = Q. \end{cases}$$

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3) + x_3 + y_1 & \text{if } P \neq Q \\ x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3 & \text{if } P = Q. \end{cases}$$

• $E/K: \; y^2 + cy = x^3 + ax + b$ (Supersingular)

if $P = (x_1, y_1) = \oplus$, then $-P = (x_1, y_1 + c)$

if $P = (x_1, y_1) \neq \oplus$, $Q = (x_2, y_2) \neq \oplus$, $P \neq -Q$,

then $P + Q = (x_3, y_3)$ with

$$x_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2 & \text{if } P \neq Q \\ \frac{x_1^4 + a^2}{c^2} & \text{if } P = Q. \end{cases}$$

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3) + y_1 + c & \text{if } P \neq Q \\ \frac{(x_1^2+a)}{c}(x_1+x_3) + y_1 + c & \text{if } P = Q \end{cases}$$

- $\#E(F_q)$ = number of pts. on E/F_q.
- $t = q+1-\#E(F_q)$.

- Z_{mn} is isomphic to $Z_m \oplus Z_n$ iff m, n are co-prime

- (Hasse's Theorem)

$$|t| \le 2\sqrt{q}.$$

$$-2\sqrt{q} \le q+1-\#E(F_q) \le 2\sqrt{q}.$$

$$-q-1-2\sqrt{q} \le -\#E(F_q) \le -q-1+2\sqrt{q}.$$

$$q+1-2\sqrt{q} \le \#E(F_q) \le q+1+2\sqrt{q}$$

- $\#E(F_q)$ can be computed in polynomial time.

- **Theorem (Weil)**

Let $t = q+1-\#E(F_q)$. Then $\#E(F_{q^k}) = q^k+1-\alpha^k-\beta^k$, where α, β are complex numbers determined from the factorization of

$$1-tT+qT^2 = (1-\alpha T)(1-\beta T).$$

Theorem $E(F_q) \cong Z_{n_1} \oplus Z_{n_2}$, where $n_2 | n_1$ and $n_2 | q-1$.

Moreover $E(F_q)$ is cyclic if $n_2 = 1$.

Example:

$Z_{15} = C_3 \oplus C_5$

$= \{0, 5, 10\} \oplus \{0, 3, 6, 9, 12\}$

$= \{0, 3, 6, 9, 12, 5, 8, 11, 14, 2, 10, 13, 1, 4, 7\}$

$\cong Z_{3+}$

(13)

Theorem

If $\gcd(n,q)=1$, then

$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$ where

$E[n] = \{ P \in E \mid nP = \Theta \}$, set of all n-torsion pts.

order 2 pts. $(a,0)$.

Theorem (Schoof) (Supersingular elliptic curve)

Let E/F_q be a supersingular elliptic curve with $t = q+1-\#E(F_q)$. Then

(i) if $t^2 = q, 2q$ or $3q$ then $E(F_q)$ is cyclic

(ii) if $t^2 = 4q$ and $t = 2\sqrt{q}$, then ~~$E(F_q)$ is~~

$$E(F_q) \cong \mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$$

(iii) if $t^2 = 4q$ and $t = -2\sqrt{q}$, then

$$E(F_q) \cong \mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$$

(iv) if $t=0$ & $q \not\equiv 3 \mod 4$, then $E(F_q)$ is cyclic

(v) if $t=0$ & $q \equiv 3 \mod 4$, then $E(F_q) \cong \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$.

$G = G_{k_1} \oplus G_{k_2} \oplus \cdots \oplus G_{k_n}$ — cyclic grs of prime-power order

Fundamental Th. of finite abelian grs.

$\cong$ → decomposition $\oplus \mathbb{Z}_{k_i}$, k_i's are pairwise co-prime.

$1^2 = 1$
$2^2 = 4$
$3^2 = 9$
$4^2 = 5$
$5^2 = 3$

$4k+3$
$11 = 4.2+3$
$13 = 4.3+1$
$5 = 4.1+1$

Example

$E/\mathbb{Z}_{11} : y^2 = x^3 + 7x + 5$.

To determine all finite pts. on E

x	$x^3+7x+5 \bmod 11$	in $QR(11)$?	y
0	5	Yes	4, 11−4 = 7
1	2	No	—
2	5	Yes	4, 7
3	9	Yes	3, 11−3 = 8
4	9	Yes	3, 8
5	0	—	—
6	10	No	—
7	1	Yes	1, 10
8	1	Yes	1, 10
9	5	Yes	4, 7
10	8	No	—

$E = \{ (0,4), (0,7), (2,4), (2,7), (3,3), (3,8), (5,0), (7,1), (7,10), (8,1), (8,10), (9,4), (9,7), \mathcal{O} \}$

(H) (I) $\#E = 16$

or order $= 2^n$ or $2p^n$ for odd prime p, $n \geq 1$

$E/\mathbb{Z}_{11}$ is not cyclic group.

Example $P = (2,4)$.

$10P$

$(10)_{10} = (1010)_2$

$10P = 2P + 8P$

$= (3,8)$.

$2^0P = P = (2,4)$.

$2^1P = 2P = (8,1)$.

$2^2P = 4P = (9,4)$

$2^3P = 8P = (5,0)$.

$$x_3 = m^2 - x_1 - x_1 \qquad m = \frac{3x_1^2 + 7}{2y_1}$$

$$y_3 = m(x_1 - x_3) - y_1.$$

$2P\,(x_3, y_3)$

$x_1 = 2, y_1 = 4.$

$$m = \frac{3(2)^2 + 7}{2(4)} = 19 \times 8^{-1} = 8 \times 7 = 56 = 1 \bmod 11$$

$7 \times \ldots = 1$

$x_3 = 1^2 - 2 - 2 = -3 = 8 \bmod 11$

$y_3 = 1(2-8) - 4 = -6 - 4 = -10 = 1 \bmod 11.$

$4P\,(x_3, y_3)$

$x_1 = 8, y_1 = 1.$

$$m = \frac{3 \times 8^2 + 7}{2 \times 1} = 199 \times 2^{-1} = 1 \times 6 = 6 \bmod 11$$

2×6

$x_3 = 6^2 - 8 - 8 = 36 - 16 = 20 = 9 \bmod 11$

$y_3 = 6(8-9) - 1 = -6 - 1 = -7 = 4 \bmod 11$

$8P\,(x_3, y_3)$

$x_1 = 9, y_1 = 4.$

$$m = \frac{3 \times 9^2 + 7}{2 \times 4} = 8 \times 8^{-1} = 8 \times 7 = 1 \bmod 11$$

$x_3 = 1 - 18 = -17 = -6 = 5 \bmod 11$

$y_3 = 1(9-5) - 4 = 4 - 4 = 0 \bmod 11$

$10P\,(x_3, y_3)$

$(x_1, y_1) = (5,1), (x_2, y_2) = (5,0)$

$$m = \frac{1-0}{8-5} = 1 \times 3^{-1} = 4 \bmod 11$$

$x_3 = 4^2 - 8 - 5 = 16 - 13 = 3$

$y_3 = 4(8-3) - 1 = 20 - 1 = 19 = 8 \bmod 11$

$64 = 3 \times 19 + 7$

$19 = 2 \times 7 + 5$

$11 = 1 \times 7 + 4$

$7 = 1 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 3 \times 1 + 0$

$81 = 3 \times 24 + 3$

$24 = 3 \times 7 + 3$

$7 = 2 \times 3 + 1$

$3 = 3 \times 1 + 0$

$250 = 22 \times 11 + 8$

$22 = 2 \times 8 + 6$

$8 = 1 \times 6 + 2$

$6 = 3 \times 2 + 0$

Example. $E/Z_{11}: y^2 = x^3 + 7x + 5$.

$P_1 = (2,4)$, $P_2 = (5,0)$.

$m = \frac{4-0}{2-5} = \frac{4}{-3}$

$= 4 \times (11-3)^{-1}$

$= 4 \times 8^{-1} \pmod{11}$

$= 4 \times 7 = 28 \pmod{11}$

$= 6$

$P_3 = P_1 + P_2 = (x_3, y_3) = ?$

$x_3 = m^2 - x_1 - x_2 = 36 - 2 - 5 = 29 = 7$

$y_3 = m(x_1 - x_3) - y_1 = 6 \times (2-7) - 4$

$= -30 - 4$

$= -34 = -1 = 10$

$P_3 = (7, 10)$.

Example $2P = ?$, $P = (44, 29)$.

$E/Z_{907}: y^2 = x^3 + 9$

$2P = (x_3, y_3)$, $(x_1, y_1) = (x_2, y_2) = (44, 29)$

$m = \frac{3x_1^2 + a}{2y_1}$

$x_3 = m^2 - x_1 - x_2 = 538^2 - 88$

$y_3 = m(x_1 - x_3) - y_1 = 538(44 - x_3) - 29$

$= \frac{3 \times (44)^2}{2 \times 29}$

$= 3 \times (44)^2 \times 58^{-1} \pmod{907}$.

$58^{-1} = 735 \pmod{907}$

$\therefore m = 3 \times (44)^2 \times 735 \pmod{907}$

$= 538$

Example. $10P$, $P = (2,4)$.

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$

$10 = (1010)_2$

$10P = 2^3 P + 2^1 P$

$= 8P + 2P$.

$P = (2,4)$

$2P = (11 - 2 - 2 = -3 = 8)$

$4P = (11(2-8) - 4 = -70 = 31)$

$8P = (8, 11)$

$4P$

$m = \frac{3 \times 4 + 7}{2 \times 4}$

$= 19 \times 8^{-1}$

$= 19 \times 7 = 56 = 1$

Example: $\text{Ord}_E(2,4)$; $\text{Ord}_E(0,4)$??

11

16.

$\#E = 16$.

$\therefore \text{Ord}_E(2,4) \mid 16$.

$\text{ord}_E(2,4) = 2, 4, 8$ or 16.

$P = (2,4)$.

$2P \neq \mathcal{O}$

$4P \neq \mathcal{O}$

$8P \neq \mathcal{O}$.

- $(2,4)$ generates as a primitive
- $(2,4)$, $(0,4)$ → analogues of primitive roots in $\mathbb{Z}_p^*$. → has max. possible order.

$16P = 8P + 8P = (x_3, y_3)$.

$8P = (5,0)$ → (A)

$8P = -8P$.

$16P = \mathcal{O}$.

$\boxed{\text{Ord}_E(2,4) = 16}$

$P = (x_3, y_3)$ with $y_3 = 0$

$\Leftrightarrow P = -P$.

$(x_3, y_3) = (x_3, -y_3)$.

$2y_3 = 0$

$y_3 = 0$.

$\therefore 2P = \mathcal{O}$.

$\therefore 16P = \mathcal{O}$.

Example. $E/F_q : y^2 = x^3 + ax + b$, $\mathrm{ch}(F_q) \neq 2, 3$.

$E[2] = ?$ $\quad P \in E[2]$ if $2P = \oplus$.

if $P = -P$.

$(x, y) = (x, -y)$

$y = 0$.

$x^3 + ax + b = 0$.

$x_1\ x_2\ x_3$.

$$E[2] = \{ \oplus, (x_1, 0), (x_2, 0), (x_3, 0) \}.$$

Example. q odd prime power, $q \equiv 2 \pmod 3$.

$E/F_q : y^2 = x^3 + b$, $b \in F_q$, $b \neq 0$.

↓ $y=0$ given

only one x as permutation

for $x \in F_q$, $x \neq 0$, $x^3 + b \in F_q$.

Check. $x \to x^3 + b$ is a permutation on F_q.

when $q \equiv 2 \pmod 3$

$q = 3k+2$

$\frac{q-1}{2}$ QR $\quad \frac{q-1}{2}$ QNR.

↓

$\to 2\frac{q-1}{2}$ pts. on Elliptic curve.

$= q - 1$.

$\left(x, \pm\sqrt{x^3 + b}\right)$.

$\to \oplus$

Total $q+1$ points.

↓

So curve is supersingular

$\to y = 0 \Rightarrow \left(\sqrt[3]{-b}, 0\right)$.

$t = q + 1 - \#E$

↙ ↙

0. $\quad q+1$

Example q be odd prime power

$$q \equiv 3 \pmod 4$$

$E/F_q : y^2 = x^3 + ax$, $a \in F_q$, $a \neq 0$.

$q = 3 \bmod 4 \Rightarrow$ -1 is QNR in F_q

$(-1)^{\frac{q-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1$.

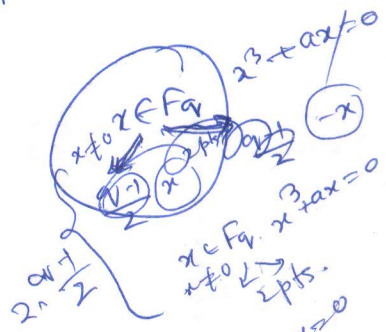
$(-x)^3 + a(-x) = -(x^3 + ax)$

~~if $x^3 + ax \neq 0$ for~~ $\rightarrow x \neq 0$.

$\therefore$ for each $x \in F_q$ for which $x^3 + ax \neq 0$, either x or $-x$ is x-coordinate of 2 pts. in E/F_q.

$\downarrow$

$\rightarrow 2 \times \frac{q-1}{2}$ pts. on E.



if $x \in F_q$, $x \neq 0$ for which $x^3 + ax = 0$, then

$x(x^2 + a) = 0$, $x = \pm\sqrt{-a}$.

$\rightarrow (0,0)$ $(\sqrt{-a}, 0)$, $(-\sqrt{-a}, 0)$ are 2 pts. on E/F_q.

$\rightarrow$ (H).

Total $q+1$ pts. $\rightarrow$ So supersingular.

$(0,1)$ order 2 pts (H)

$\downarrow$

$2 + 1 + 2 \times \frac{q-1}{2}$.

$x \in F_q$, $x \neq 0$, $x^3 + ax \neq 0$ ↓ can't be connected here

- if $x \rightarrow x^3 + ax \in$ QNR, then $-x \rightarrow -(x^3+ax) \in$ QR.
- if $x \rightarrow x^3 + ax \in$ QR, then $-x \rightarrow (-x^3 + ax) \in$ QNR.

or

Menezes-Vanstone Elliptic Curve Cryptosystem.

$E/\mathbb{Z}_p$ ($p > 3$ prime) → elliptic curve s.t. E contains a cyclic ~~subgraph~~ subgroup H in which DLP is intractable

- $\mathcal{P} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
  $\mathcal{C} = E \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
  $\mathcal{K} = \{(E, \alpha, a, \beta) : \beta = a\alpha\}$ where $\alpha \in E$.
- α, β are public
- a is secret.

Encryption

for $K = (E, \alpha, a, \beta)$, choose a secret random number $k \in \mathbb{Z}_{|H|}$, and for $x = (x_1, x_2) \in \mathbb{Z}_p^{*2}$, define

~~$e_K(x_1, x_2) =$~~

$$e_K(x, k) = (y_0, y_1, y_2)$$

where $y_0 = k\alpha$

$(c_1, c_2) = k\beta$ $\left[= ka\alpha = ay_0\right]$

$y_1 = c_1 x_1 \bmod p$

$y_2 = c_2 x_2 \bmod p$

Decryption

for ciphertext $y = (y_0, y_1, y_2)$

define $d_K(y) = (y_1 c_1^{-1} \bmod p,\ y_2 c_2^{-1} \bmod p)$

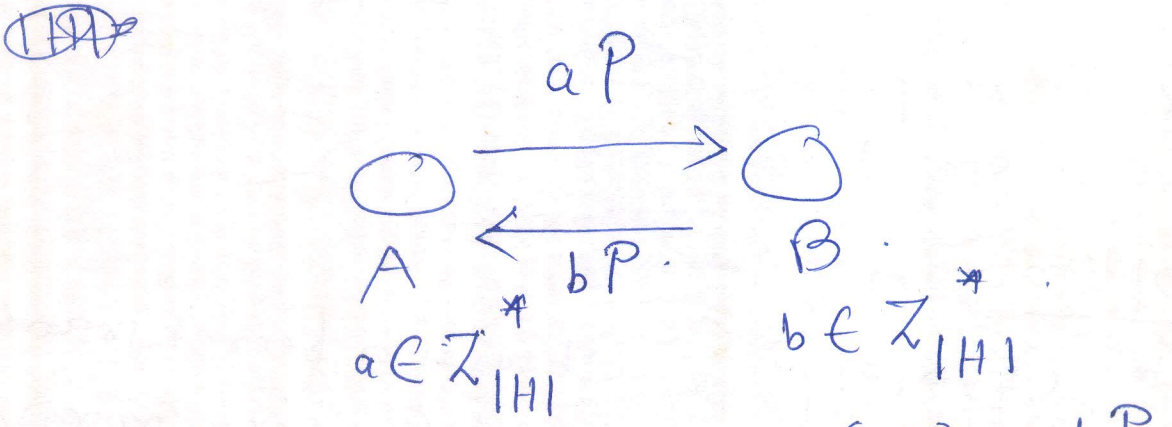
where $ay_0 = (c_1, c_2)$.

DH (Elliptic Curve Analog) Key Exchange

$G = (E/K, +)$.

Take a cyclic subgroup H of G = $\langle P \rangle$.

DLP is intractable.



DLP on H.

$H = \langle P \rangle$.

Given $\langle P, aP \rangle$ to find a?

where $a \in Z^*_{|H|}$

Security: Given $\langle P, aP, bP \rangle$ to compute abP?

hardness of CDH.

↓ Computational DH problem (CDH).

Elliptic curves over finite fields

- E/F_{p^n}, $p \neq 2, 3$.

Example: E/F_{25} : $y^2 = x^3 + x + 4$.

Soln: We can construct F_{25} as $\mathbb{Z}_5[x]/(x^2+4x+2)$

as x^2+4x+2 is an irreducible polynomial over $\mathbb{Z}_5$.

$\omega^2 + 4\omega + 2 = 0$

$\omega^2 = -4\omega - 2$

$= \omega + 3$

Then F_{25} = ~~$\{0,1,2,3,4\}$~~ the set of all polynomials of degree at most 1 with co-efficients from $\mathbb{Z}_5$

poly	vector	poly
0	00	—
1	01	ω^0
2	02	ω^5
3	03	ω^{18}
4	04	
ω	10	
$1+\omega$	11	
$2+\omega$	12	
$3+\omega$	13	
$4+\omega$	14	
2ω	20	
$1+2\omega$	21	
⋮	⋮	

$= \{0, 1, 2, 3, 4, \omega, \omega+1, \omega+2, \omega+3, \omega+4,$
$2\omega, 2\omega+1, 2\omega+2, 2\omega+3, 2\omega+4, 3\omega, 3\omega+1, 3\omega+2,$
$3\omega+3, 3\omega+4, 4\omega, 4\omega+1, 4\omega+2, 4\omega+3,$
$4\omega+4\}$

The set of quadratic residues module 25

$= \{ 1^2 = 1,\ 2^2 = 4,\ \cancel{3^2 = 4},\ \cancel{4^2 = 16 = 1},\ \omega^2 = \omega+3,\ (\omega+1)^2 = \omega+3+2\omega+1 = 3\omega+4,$

$(\omega+2)^2 = \omega+3+4\omega+4 = 2,\ (\omega+3)^2 = \omega+3+6\omega+9 = 2\omega+2$

$(\omega+4)^2 = \omega+3+8\omega+16 = 4\omega+4,\ (2\omega)^2 = 4(\omega+3) = 4\omega+2$

$(2\omega+1)^2 = 4(\omega+3)+4\omega+1 = 3\omega+3,\ (2\omega+2)^2 = 4(\omega+3)+8\omega+4 = 2\omega+1$

$(2\omega+3)^2 = 4(\omega+3)+12\omega+9 = \omega+1,\ (2\omega+4)^2 = 4(\omega+3)+16\omega+16 = 3 \}$

~~$(3\omega)^2 = 9(\omega+3) = 2\omega+1$~~ ,

$(3\omega)^2 = (-2\omega)^2$

$(3\omega+1)^2 = (-2\omega+1)^2 = (2\omega-1)^2 = (2\omega+4)^2$

$(3\omega+2)^2 = (-2\omega-3)^2 = (2\omega+3)^2$

$(3\omega+4)^2 = (-2\omega-1)^2 = (2\omega+1)^2$

$(4\omega)^2 = \omega^2,\ (4\omega+1)^2 = (-\omega+4)^2 = (\omega+4)^2,\ (4\omega+2)^2 = (-\omega-3)^2 = (\omega+3),$

$(4\omega+3)^2 = (-\omega-2)^2 = (\omega+2)$

$(4\omega+4)^2 = (-\omega-1)^2 = (\omega+1)^2$

Q $R_{25} = \{1, 4, \omega+3, 3\omega+4, 2, 2\omega+2, 4\omega+4, 4\omega+2, 3\omega+3, 2\omega+1, \omega+1, 3\}$

$27 + 3 + 1$
$= 2+7 = 9 = 4$
$64 + 8$
$= 4+8 = 12 = 2$

$\cdot \omega^2 = \omega + 3$

$\omega^3 + \omega + 4$
$\omega^2 + 3\omega + \omega + 4$
$\omega + 3 + 4\omega + 4$
$5\omega + 7$
2

$\omega^3 + 3\omega^2 + 3\omega + 1 + \omega + 4 + 1$
$\omega^2 + 3\omega + 3\omega + 4\omega + 5 + 1$
$4\omega^2 + 7\omega + 1$
$4\omega^2 + 2\omega + 1$
$4\omega + 1 + 2\omega + 1$
$6\omega + 2 + 1$
$\omega + 2 + 1$

x	x^3+x+4	quadratic residue	y
0	$4 = 2^2$	Yes	$\pm 2 \to 2, 3$
1	$1 = 1^2$	Yes	$\pm 1 \to 1, 4$
2	$4 = 2^2$	Yes	$\pm 2 \to 2, 3$
3	~~$4 = (\omega+2)^2$~~	Yes	~~$\pm(\omega+2) \to \omega+2, 4\omega+3$~~ $\pm 2 \to 2, 3$
4	$2 = (\omega+2)^2$	Yes	$\pm(\omega+2) \to \omega+2, 4\omega+3$
ω	2	Yes	$\pm(\omega+2) \to \omega+2, 4\omega+3$
$\omega+1$	$\omega+3 = \omega^2$	Yes	$\pm\omega \to \omega, 4\omega$
$\omega+2$	3ω	NO	-
$\omega+3$	$\omega+4$	NO	-
$\omega+4$	1	Yes	$\pm 1 \to 1, 4$
~~$\omega+5$~~ 2ω	$4\omega+3$	No	-
$2\omega+1$	$2\omega+1 = (3\omega+3)^2$	Yes	$\pm(3\omega+3) \to 3\omega+3, 2\omega+2$
$2\omega+2$	2ω	No	-
$2\omega+3$	$4\omega+1$	NO	
~~$2\omega+4$~~ 3ω	3ω	No	
~~$3\omega+1$~~	ω	No	
$3\omega+1$	$2\omega+3$	No	
$3\omega+2$	$\omega+2$	No	
$3\omega+3$	$3\omega+3 = (2\omega+1)^2$	~~No~~ Yes	$\pm(2\omega+1) \to 2\omega+1, 3\omega+4$
~~$3\omega+4$~~	~~$3\omega+2$~~ 1	Yes	$\pm 1 \to 1, 4$
4ω	$2 = (\omega+1)^2$	Yes	$\pm(\omega+1) \to \omega+1, 4\omega+4$
$4\omega+1$	$4\omega+4 = (\omega+4)^2$	Yes	$\pm(\omega+4) \to \omega+4, 4\omega+1$
$4\omega+2$	$2\omega+3$	No	-
$4\omega+3$	4ω	No	-

$E/F_{25} = \{(0,2), (0,3), (1,1), (1,4), \cdots, (4, \omega+2), (4, 4\omega+3), \cdots\}$ ∪ ∞

$|E/F_{25}| = 27$

~~m-torsion~~

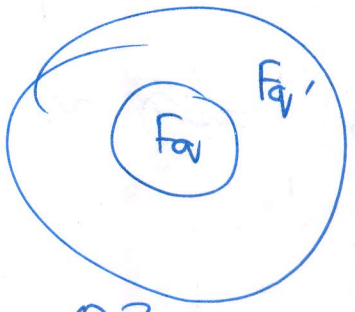
m-torsion points.

- E/F_q → Elliptic curve over F_q, $q = p^n$, p prime.
- $P \in E/F_q$ is an m-torsion point if $mP = \oplus$
  i.e. $\text{ord}(P) \mid m$.

- The set of m-torsion points of E is finite & has size atmost m^2.

- If $\gcd(m, q) = 1$, then it is always possible to find an extension field $F_{q'}$ of F_q s.t.

$E[m]$
$= \{ P \in E/F_{q'} \mid mP = \oplus \}$ |
$= m^2$



- $E[m] = \{ P \in E/F_{q'} \mid mP = \oplus \}$ $\quad \text{ord}(\oplus) = 1$
  → form a subgroup of $E/F_{q'}$
  → m-torsion subgroup of E/F_q
  $\cong Z_m \times Z_m$ with $m \mid E/F_q$,

- If m is a prime, $\gcd(m, q) = 1$ and $m \nmid q-1$, then $E[m]$ is a subgroup of E/F_{q^k} where k is the smallest +ve integer s.t. $m \mid q^k - 1$

- $k \rightarrow$ embedding degree

- $q = 5$
- $\#E/F_5 = 9$ (including θ). Take $m = 3$
  $\#E/F_{25} = 27$ (including θ). m prime, $\gcd(5,3)=1$, $3 \nmid q-1$, $m \nmid |E/F_q|$
- $E[3] \to$ set of all 3-torsion points.
  $\to$ Subgroup of E/F_{q^k}
  where k is the smallest +ve integer s.t. $3 \mid q^k - 1$ i.e. $k = 2$.

i.e. F_{25} is the smallest extension field that contains all 3-torsion pts.

$\omega^{24} = 1$

$\omega^2 = \omega + 3$
$\omega^3 = \omega^2 + 3\omega = \omega + 3 + 3\omega = 4\omega + 3$
$\omega^4 = 4\omega^2 + 3\omega = 4\omega + 12 + 3\omega = 2\omega + 2$
$\omega^5 = 2\omega^2 + 2\omega = 2\omega + 6 + 2\omega = 4\omega + 1$

- $|E[3]| = 3^2 = 9$ as $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ (as m prime)

$E[3] = \{ \mathcal{O}, (\omega+1, 4\omega), (\omega+1, \omega), (4, 4\omega+3), (4, \omega+2), (3,2), (3,3), (4\omega+2, 4\omega+1), (4\omega+2, \omega+4) \}$

- To check $3P = \mathcal{O}$ for $P = (\omega+1, 4\omega)$

$$\lambda = 2^{-1}\left((\omega+1)^2 + 1\right)\left(2 \times (4\omega)\right)^{-1}$$
$$= 3(\omega^2 + 3 + 2\omega^2 + 2)(3\omega)^{-1}$$
$$= 3(\omega + 2\omega^2)2\omega^{-1}$$

$2^{-1} = 3 \bmod 5$

$\omega^{-1} = \omega^{23} = (\omega^5)^4 \cdot \omega^3 = (4\omega+1)^4 \cdot (4\omega+3)$

To check $3P = \oplus$ for $P = (4, \omega+2)$

Calculate 2P

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

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

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

$$\lambda = \frac{(3 \times 4^2 + 1)}{2(\omega+2)}$$

$$= (3+1)\,\bar{2}^1\,(\omega+2)^{-1}$$

$$= 4 \times 3\,(\omega+2)^{-1}$$

$$= 4 \times 3\,(\omega^{15})^{-1}$$

$$= 2\,\omega^9$$

$$= 2(3\omega+1) = \omega+2$$

E/Fq : $y^2 = x^3 + ax^2 + b$

E/F25: $y^2 = x^3 + x + 4$

$a = 1, b = 4$

$\omega^{24} = 1$

$(\omega^{15})^{-1} = \omega^9$

$= 3\omega + 1$

$\omega^2 = \omega + 3.$

$\omega^3 = \omega^2 + 3\omega$

$= \omega + 3 + 3\omega$

$= 4\omega + 3.$

$\omega^4 = 4(\omega+3) + 3\omega$

$= 7\omega + 12$

$= 2\omega + 2$

$\omega^5 = 2\omega^2 + 2\omega$

$= 2(\omega+3) + 2\omega$

$= 4\omega + 6$

$= 4\omega + 1$

$\omega^6 = 4(\omega+3) + \omega$

$= 5\omega + 12$

$= 2$

$\omega^7 = 2\omega$

$\omega^8 = 2(\omega+3) = 2\omega + 1$

$\omega^9 = 2(\omega+3) + \omega = 3\omega + 1$

$\omega^{10} = 3(\omega+3) + \omega = 4\omega + 4$

$\omega^{11} = 4(\omega+3) + 4\omega = 3\omega + 2$

$\omega^{12} = 3(\omega+3) + 2\omega$

$= 4$

$\omega^{13} = 4\omega$

$\omega^{14} = 4(\omega+3) = 4\omega + 2$

$\omega^{15} = 4(\omega+3) + 2\omega = 6\omega + 12 = \omega + 2$ ✓

$\omega^{16} = (\omega+3) + 2\omega = 3\omega + 3$

$\omega^{17} = 3(\omega+3) + 3\omega = 6\omega + 9 = \omega + 4$

$\omega^{23} = \omega + 3 + \omega = 2\omega + 3$

$\omega^{24} = 2(\omega+3) + 3\omega$

$= 1$

$\omega^{24} = (\omega^{12})^2 = 16 = 1$

~~$\omega^{25} = (\omega^{12})^2\,\omega = 16\omega = \omega$~~

$\omega^{36} = (4\omega)^2 = 16\omega^2 = \omega^2$

$\omega^{18} = \omega^2 + 4\omega = \omega + 3 + 4\omega = 5\omega + 3$

$\omega^{19} = 3\omega$

$\omega^{20} = 3(\omega+3) = 3\omega + 4$

$\omega^{21} = 3(\omega+3) + 4\omega = 7\omega + 9 = 2\omega + 4$

$\omega^{22} = 2(\omega+3) + 4\omega = \omega + 1$

$x_3 = \lambda^2 - 2x_1$

$= (\omega+2)^2 - 2\times 4$

$= \omega^2 + 4\omega + 4 - 8$

$= \omega + 3 + 4\omega - 4$

$= 5\omega - 1$

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

$= (\omega+2)(4-4) - (\omega+2)$

$= -(\omega+2)$

$= 4\omega + 3$

$P = (4, \omega+2)$

$2P = (4, 4\omega+3)$, $-P = (4, -\omega-2)$

$= (4, 4\omega+3)$.

$\Rightarrow$ ~~$3P$~~ $2P = -P \Rightarrow 3P = \mathcal{O}$

$\Rightarrow P \in E[3]$.

$1^2 \equiv 1$
$2^2 \equiv 4$

$Q_5 = \{1, 4\}$

$E/F_5 : y^2 = x^3 + x + 4$

$E = \{(0, \pm 2), (1, \pm 1), (2, \pm 2), (3, \pm 2), \mathcal{O}\}$

Bilinear Pairing → Miller's algm. (PPT algm).
→ Weil pairing, Tate pairing, Eta pairing, Ate pairing.

Theorem Let $E[m]$ be the m-torsion subgroup of an elliptic curve E/F_q, where $q = p^n$ for some prime p and $m \mid \#E(F_q)$, $\gcd(m, q) = 1$ and $m \nmid (q-1)$. Let k be the smallest positive integer such that m divides $q^k - 1$, and

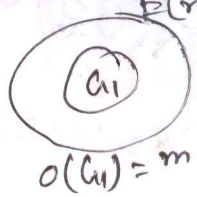
$$e_m : G_1 \times G_2 \to F_{q^k}^*$$

$k \to$ embedding degree of the curve.

be a pairing with

- $O(G_1) = m = O(G_2)$
- G_1 is a cyclic subgroup of $E[m]$.
- G_2 is a cyclic subgroup of E
- no efficiently computable isomorphism between G_1 and G_2. (Type-3 pairing — most efficient pairing generally recommended for implementation).

$|E[m]| = m^2$



Then e_m satisfies the following properties.

1. $\forall P \in G_1$ and $Q \in G_2$, the image $e_m(P, Q)$ is an m-th root of unity in $F_{q^k}^*$.
   (i.e. $e_m(P, Q)^m = 1$)
2. (Bilinear) $e_m(P_1 + Q_1, P_2) = e_m(P_1, P_2) \cdot e_m(Q_1, P_2)$
   and $e_m(P_1, P_2 + Q_2) = e_m(P_1, P_2) \cdot e_m(P_1, Q_2)$

3. If $P \in G_1$ has order m, then $\exists\ Q \in G_2$ such that $e_m(P,Q)$ is a primitive m^{th} root of unity in $F_{q^k}^*$.

i.e. $O(P) = m$

$\Rightarrow \exists\ Q \in G_2$ s.t.

$O(e_m(P,Q)) = m$ in $F_{q^k}^*$.

- The output of a pairing is an element of the cyclic subgroup μ_m of $F_{q^k}^*$ consisting of the m-th root of unity.

- Let $P \in G_1$, $O(P) = m$, $R \in \langle P \rangle$.

Let $Q \in G_2$ for which $e_m(P,Q)$ is a primitive m-th root of unity & so $\mu_m = \langle e_m(P,Q) \rangle$.

The fact that pairings are bilinear implies that the map defined by

$$\phi : \langle P \rangle \longrightarrow F_{q^k}^*$$

$$R \mapsto e_m(R,Q)$$

is an isomorphism.

- This isomorphism can be used to translate the ECDLP in $\langle P \rangle$ into DLP in μ_m.

- ~~Index~~

· Index Calculus Method can be used to solve DLP in μ_m, but cannot be applied directly to the ECDLP.

· Let $R = rP \in \langle P \rangle$. → r is the DL over the curve

Then $\beta = e_m(R, Q)$

$= e_m(rP, Q)$

$= e_m(P, Q)^r$.

$= \alpha^r$ → r is the DL over μ_m which is a cyclic subgroup of $F_{q^k}^*$.

Steps in Solving ELDLP

· E/F_q, $E[m]$ → m-torsion subgroup of $E(F_{q^k})$.

~~$m \mid q$, gcd(~~

AlgmDL(E, m, P, R) $m \mid \#E(F_{q^k})$, $\gcd(m, q) = 1$, $m \nmid q^i - 1$

the embedding degree

- find k, the smallest +ve integer for which all pts. in $E[m]$ have co-ordinates from E/F_{q^k}.

- find $Q \in E[m]$ for which $\alpha = e_m(P, Q)$

When $P \in G_1$, G_1 is a cyclic subgroup of $E[m]$, of ~~ord~~ $O(G_1) = m$.

- Compute $\beta = e_m(R, Q)$.

- Determine the DL r of β w.r.t. to the base α.

- Practically, we need to
  - find k
  - find ϕ
  - Compute pairing
  - Solve DLP in $\mathbb{F}_{q^k}^*$.

- PPT algo. due to Miller can be used to compute pairing.

- DLP Solvable or not → depends on k

  if k sufficiently small — Index Calculus Method may be used

- for randomly chosen elliptic curves over randomly chosen field, k is expected to be large in general.

- Menezes, Okamoto, Vanstone (MOV) showed
  - that — for the class of supersingular elliptic curve, the value of k is ≤ 6.
  - they provided an approach for finding a suitable pt. Q over such curves.
  - overall result is a probabilistic subexponential time algo. for solving the DLP on supersingular elliptic curves.