

Defn: $P + Q = P + Q$
any vertical line with the curve

Week 15

Elliptic Curves

(1)

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

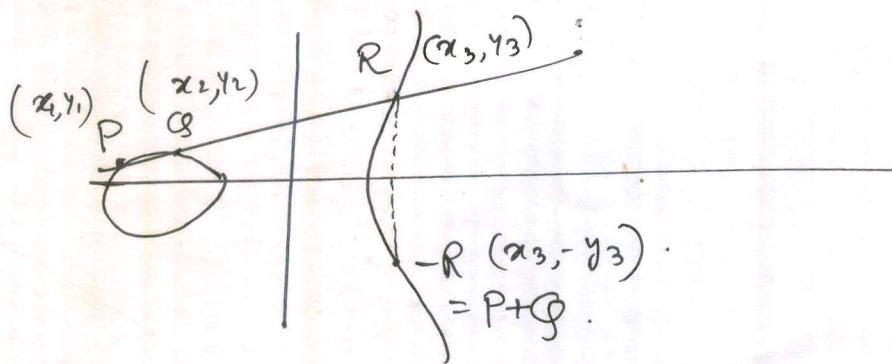
$$y^2 \equiv x^3 + ax + b \pmod{p},$$

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

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



$$\begin{aligned} 2y \frac{dy}{dx} &= 3x^2 + a \\ \left[\frac{dy}{dx} \right]_{P=(x_1, y_1)} &= \frac{3x_1^2 + a}{2y_1} \end{aligned}$$

~~PG~~ Chord & Tangent law:

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

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

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

$$\therefore x_3 = m^2 - x_1 - x_2, y_3 = \frac{m x_3 + y_1 - m x_1}{m - x_1} = \frac{y_2 - y_1}{m - x_1} (x_3 - x_1) + y_1$$

(2)

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

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

- if $P = \Theta$, then $P + \Theta = \Theta + P = P$.

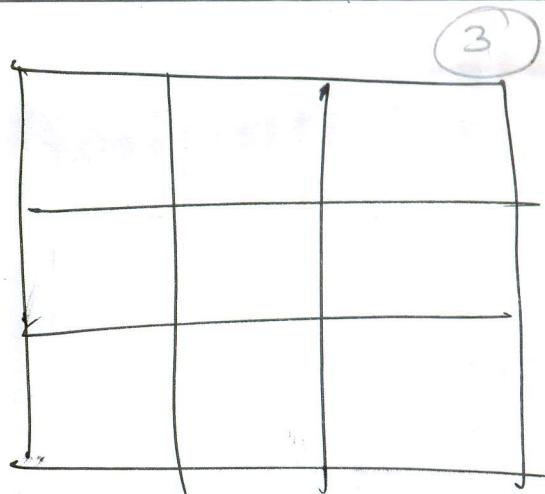
$\Theta \rightarrow$ additive identity
or

point at infinity

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

Projective plane \rightarrow

$$(\lambda x, \lambda y, \lambda z) \sim (x, y, z)$$



$$(\cancel{x_1, x_2, x_3}) \sim *$$

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$$

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 components zero)

all scalar multiples
of (x, y, z) are in the
same equivalence
class.

↓

this equivalence
class is called
projective point.

The equivalence class containing
the triple ~~*~~ triple (x, y, z)

is a projective point.

Case $z \neq 0$

Only one projective point
for triple (x, y, z) .

→ the class containing (x, y, z) .

$$\left(x, y, z \right) \sim \left(x, y, 1 \right) \quad x = \frac{x}{z}, \quad y = \frac{y}{z}$$

Thus projective plane is identified with all ④ points (x, y) in ordinary (affine) plane



the ^{projection} points for which $z = 0$.

~~points~~ called

line at infinity
in affine plane

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



^{projection} $\bar{F}(x, y, z) = 0 \rightarrow$ satisfied by projective pts.

Substitute: $x = \frac{x}{z}, y = \frac{y}{z}$.

f multiplies by power of z to clear the denominators.

$E/K: y^2 = x^3 + ax + b$ in affine plane,

$\underline{z \neq 0}$

$\underline{\quad}$ ①

$a, b \in K$
 $4a^3 + 27b^2 \neq 0$.
ch. $K \neq 2, 3$.

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.} $\underline{z^2 y^2 = x^3 + a x z^2 + b z^3} \rightarrow$ is satisfied by all projective pts. (x, y, z)

$\underline{z=0}$ ③ $\Rightarrow 0 = x^3 \Rightarrow x=0$. with $z \neq 0$ for which $(0, 1, 0) \rightarrow$ only equivalent class \rightarrow ④ cor. affin pt. (x, y) satisfy with substitution ②

~~with both $x, z = 0$~~

So, in projective plane

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

(5) put $\lambda = 0$ in the projective eqn.

↓
intersection of all projectors with pts. $\frac{z}{z} = 0$

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

with the projective eqn.

↓
point of infinity.

↓
intersection of the line at infinity with the y-axis

with the projective eqn.

$x=0, z=0$.
↓
intersection of the line at infinity with the y-axis.

Elliptic Curves

- K be a field & \bar{K} its algebraic closure
 (if $K = F_{q^n}$, then $\bar{K} = \bigcup_{m \geq 1} F_{q^{nm}}$)
- $E/K : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$,
 $a_1, a_2, a_3, a_4, a_6 \in K$ with no
 singular point.
 (Weierstrass equation).

. The set of K -rational points

$$E(K) = \{(x, y) \in K \times K\} \cup \{\Theta\}$$

when Θ is called the identity (also point at infinity).

. Simplified Weierstrass equation :

1. $\text{ch}(K) \neq 2, 3$:

$$y^2 = x^3 + ax + b, \quad a, b \in K, \quad 4a^3 + 27b^2 \neq 0.$$

2. $\text{ch}(K) = 2$:

$$y^2 + xy = x^3 + ax^2 + b, \quad a, b \in K, \quad b \neq 0$$

or (non-supersingular)

$$y^2 + cy = x^3 + ax + b, \quad a, b, c \in K, \quad c \neq 0. \quad (\text{supersingular})$$

3. $\text{ch}(K) = 3$:

(7)

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

(cubic on the right has no multiple roots).

Group Law

: $E = E(K)$ given by Weierstrass eqn.

for all $P, Q \in E$

$$(i) \quad \textcircled{H} + P = P + \textcircled{H} = P \quad \left(\begin{array}{l} \text{so } \textcircled{H} \text{ serves as the} \\ \text{identity} \end{array} \right)$$

$$(ii) \quad -\textcircled{H} = \textcircled{H}$$

(iii) if $P = (x_1, y_1) \neq \textcircled{H}$, then $-P = (x_1, -y_1 - ax_1 - a_3)$

$$y(y + ax^2 + a_3) = x^3 + a_2 x^2 + a_4 x + a_6$$

if (x_1, y_1) satisfy this eqn, then so does $(x_1, -y_1 - ax_1 - a_3)$.

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

(v) if $Q = -P$, then $P + Q = \textcircled{H}$.

(vi) if $Q = -P$, then $P + Q = -R$

(vii) if $P \neq \textcircled{H}, Q \neq \textcircled{H}, Q \neq -P$, 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 .

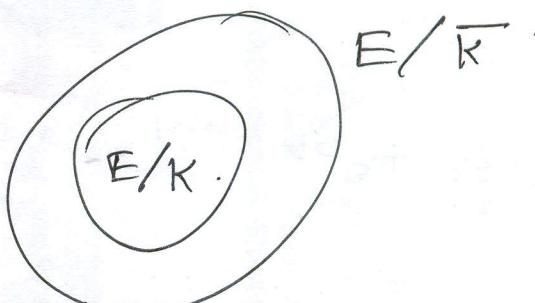
(viii) pt. at infinity $\rightarrow 3^{\text{rd}}$ pt. of intersection of a vertical line with the curve E .

$$E = E/\bar{K} : \text{Weistrass equ}^n$$

(8)

Theorem

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



(ii) E/\bar{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) $P + \Theta = \Theta + P = P \neq P \in E$.

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

e) (Commutative) ~~for all~~ if $P, Q \in E$, then $P+Q = Q+P$.

(9)

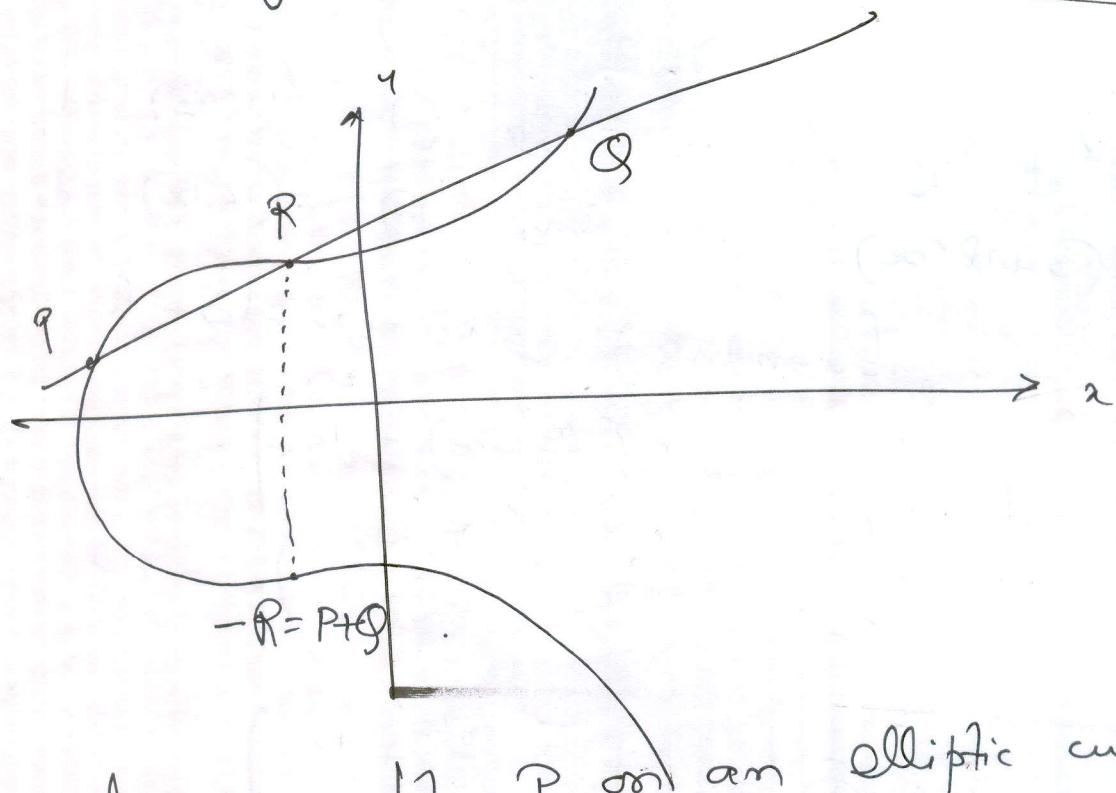
Supersingular Elliptic curve

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

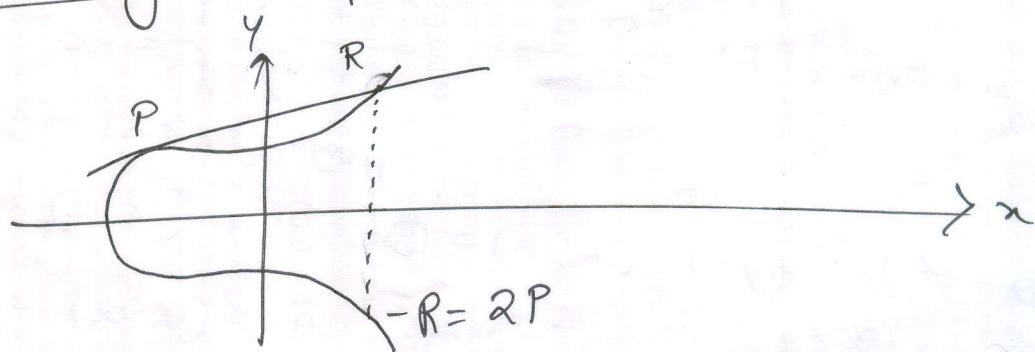
$$t = q+1 - \#E(F_q), \quad q=p^m, \quad p = \text{ch}(F_q),$$

Theorem (Waterhouse) E/F_q is supersingular ^{a priori} if
~~trace of~~ $t^2 = 0, q, 2q, 3q$ or $4q$.

~~Addit~~ Adding two pts. P, Q on an elliptic curve



Doubling a pt. P on an elliptic curve



(10)

Addition formulae

- E/K : Weierstrass equⁿ. $y^2 + a_4xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- if $P = (x_1, y_1) \neq \Theta$, then $-P = (x_1, -y_1, -a_4x_1 - a_3)$
 - if $P = (x_1, y_1) \neq \Theta$, $Q = (x_2, y_2) \neq \Theta$, $P \neq -Q$,
 - if $P = (x_1, y_1) \neq \Theta$, $Q = (x_2, y_2) \neq \Theta$, $P = -Q$,
 - then $P + Q = (x_3, y_3)$ with

$$x_3 = \lambda^2 + a_4\lambda - a_2 - x_1 - x_2$$

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

where

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

$$\text{and } \beta = y_1 - \lambda x_1$$

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

- if $P = (x_1, y_1) \neq \Theta$, then $-P = (x_1, -y_1)$.
- if $P = (x_1, y_1) \neq \Theta$, $Q = (x_2, y_2) \neq \Theta$, $P \neq -Q$,
- if $P = (x_1, y_1) \neq \Theta$, $Q = (x_2, y_2) \neq \Theta$, $P = -Q$,
- 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 $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ (3x_1^2 + a)/2y_1 & \text{if } P = Q \end{cases} \Rightarrow$

$$\begin{aligned} 2P &= \Theta \\ \Rightarrow 16P &= \Theta \\ y_1 &\neq 0 \\ \text{with } y_1 &= 0 \\ \text{with } y_1 &= 0 \\ \Rightarrow P &= P \text{ i.e. } 2P = \Theta \end{aligned}$$

$$\cdot E/\mathbb{K} : y^2 + xy = x^3 + ax^2 + b \quad (\text{non supersingular}), \quad \text{ch}(\mathbb{K}) = 2. \quad (11)$$

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

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

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

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

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

$$\cdot E/\mathbb{K} : y^2 + cy = x^3 + ax + b \quad (\text{Supersingular})$$

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

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

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

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

$$y_3 = \begin{cases} \left(\frac{y_1 + y_2}{x_1 + x_2} \right) (x_1 + x_3) + y_1 + \cancel{ac} & \text{if } P \neq Q \\ \left(\frac{x_1^4 + a}{c} \right) (x_1 + x_3) + y_1 + c & \text{if } P = Q \end{cases}$$

$\# E(F_q) = \text{number of pts. on } E/F_q$.

(12)

$t = q+1 - \# E(F_q)$.

\mathbb{Z}_{mn} isomorphic to $\mathbb{Z}_m \oplus \mathbb{Z}_n$

if

m, n are coprime

(Hasse's Theorem)

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

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

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

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

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

Theorem (Weil)

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

$$1 - 7T + qT^2 = (1 - \alpha T)(1 - \beta T).$$

Theorem $E(F_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, where $n_2 | n_1$,

and $n_2 | q-1$.

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

$$= \{0, 3, 6, 9, 12, \\ 5, 8, 11, 14, 2, \\ 10, 13, 1, 4, 16, 7\}$$

Example:

$$\begin{aligned} z_{15} &= G_3 \oplus G_5 \\ &= \{0, 5, 10\} \\ &\quad \oplus \{0, 3, 6, 9, 12\} \\ &= \mathbb{Z}_3 + \end{aligned}$$

Theorem

If $\gcd(n, q) = 1$, then (13)

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

$E[n] = \left\{ P \in E \mid nP = \Theta \right\}$, set of all
 n -torsion pts.
order 2 pts. (30).

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 $t=0$ & $q \not\equiv 3 \pmod{4}$, then $E(F_q)$ is cyclic

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

$G = G_1 \oplus G_2 \oplus \dots \oplus G_n$
 \downarrow finite groups
 prime order

Fundamental Th. of finite abelian grs.
 \Rightarrow decomposition $\oplus \mathbb{Z}_{k_i}$, k_i 's are pairwise co-prime.

Example

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

(14)

$$\begin{aligned} 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \\ 4^2 &= 5 \\ 5^2 &= 3 \end{aligned}$$

$$\begin{aligned} 4k+3 \\ 11 &= 4 \cdot 2 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 5 &= 4 \cdot 1 + 1 \end{aligned}$$

To determine all finite pts. on E

$$\begin{array}{r} 32 \\ 21 \\ \hline 53 \end{array} \quad \begin{array}{r} 69 \\ 28 \\ 97 \\ \hline 165 \\ 55 \end{array}$$

x	$x^3 + 7x + 5 \text{ mod } 11$	in QR(11)?	y
0	5	Yes	$1, 11-4=7$
1	2	No	$\bar{4}, \bar{7}$
2	5	Yes	$3, 11-3=8$
3	9	Yes	$3, 8$
4	9	Yes	-
5	0	-	-
6	10	No	-
7	1	Yes	$1, 10$
8	1	Yes	$1, 10$
9	5	Yes	$4, 7$
10	8	No	-

$$\begin{array}{r} 47 \\ 23 \\ 47 \\ \hline 11 | 263 \\ 22 \\ 3 \\ 1000 \\ 75 \\ \hline 25 \\ 25 \\ 0 \\ 10 \\ 85 \\ 85 \\ \hline 0 \\ 402 \\ 402 \\ 78 \\ 78 \\ \hline 343 \\ 343 \\ 59 \\ 59 \\ \hline 139736 \\ 33 \\ 33 \\ \hline 67 \\ 67 \\ \hline 1 \\ 1 \\ 64 \\ 502 \\ 502 \\ 61 \\ 61 \\ \hline 1323 \\ 1323 \\ 59 \\ 59 \\ \hline 81 \\ 81 \\ \hline 729 \\ 729 \\ 68 \\ 68 \\ \hline 179772 \\ 179772 \\ 77 \\ 77 \\ \hline 27 \\ 27 \\ \hline 5 \\ 5 \end{array}$$

$$E = \left\{ (0, 4), (0, 7), (\cancel{1, 4}), (\cancel{1, 7}), (2, 4), (2, 7), (3, 3), (3, 8), (\cancel{5, 0}), (\cancel{7, 1}), (7, 10), (8, 1), (8, 10), (9, 4), (9, 7), \Theta \right\}$$

$$\# E = 16$$

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

~~gr. order or 2ⁿ
order n or 2ⁿ
2, A, p or 2ⁿ
for odd p
n > 1~~

$$\begin{array}{r} 81 \\ 729 \\ 68 \\ 68 \\ \hline 179772 \\ 179772 \\ 77 \\ 77 \\ \hline 27 \\ 27 \\ \hline 5 \\ 5 \end{array}$$

Example

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

15

10 P

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

$$10P = 2P + 8P \\ = (3, 8)$$

$$\overset{0}{2}P = P = (2, 4).$$

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

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

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

$$x_3 = m^2 - x_4 - x_5$$

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

$x_1=2, y_1=4$

$$m = \frac{3x_1^2 + 7}{2x_1}$$

2 P (x_3, y_3)

$$m = \frac{3(2)^2 + 7}{2(4)} = \frac{19 \times 8}{7 \cdot \dots} = 1 \pmod{11}$$

$$x_3 = 1^2 - 2 \cdot 2 = -3 = 8 \pmod{11}$$

$$x_3 = 1^2 - 2 \cdot 2 = -3 \equiv 8 \pmod{11}$$

$$y_3 = 1(2-8)$$

Q P (x_3, y_3)

$$x_1 = 8, y_1 = 1$$

$$x_3 = 6^2 - 8 \cdot 8 = 36 - 64 = -28 \stackrel{b}{\equiv} 9 \pmod{11}$$

$$x_3 = 6^2 - 8 - 8 = 36 - 16 = 20 \quad \text{and} \\ y_3 = 6(8-9) - 1 = -6 - 1 = -7 = 4$$

$$\begin{array}{r}
 & 64 \\
 & \underline{\times} 3 \\
 = & 92 \\
 & \underline{\times} 7 \\
 \hline
 & 1199 \\
 & \underline{- 88} \\
 & 31
 \end{array}$$

8 P (x_3, y_3)

$$x=9, y_1=4$$

$$x_3 = 1 - 18 = -17 = -6 \equiv 5 \pmod{11}$$

$$x_3 = 1 - 18 = -17 = -6 \equiv 5 \pmod{11}$$

$$y_3 = 1(9 - 5) - 4 = 4 - 4 = 0 \pmod{11}$$

$$y_3 = 1(9-5) - 4 = 4 - 4 = 0 \quad \text{mod } n$$

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

(16)

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

$$\begin{aligned} m &= \frac{4-0}{2-5} = \frac{4}{-3} \\ &= 4 \times \frac{1}{8} \quad (11-3)^{-1} \\ &= 4 \times \frac{1}{8} \quad \text{mod } 11 \end{aligned}$$

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

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

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

$$= -30 - 4$$

$$= -34 = -11 = 10$$

$$= 4 \times 7 = 28 \quad \text{mod } 11$$

$$= 6$$

$$P_3 = (7, 10)$$

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

$$E/\mathbb{Z}_{907} : y^2 = x^3 + 9$$

$$2P = (x_3, y_3),$$

$$(x_1, y_1) = (x_2, y_2) = (44, 29)$$

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

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

$$\begin{aligned} m &= \frac{3x_1^2 + a}{2y_1} \\ &= \frac{3 \times (44)^2 + 9}{2 \times 29} \\ &= 3 \times (44) \times 58^{-1} \\ &= 3 \times (44) \times 58 \\ &\quad \text{mod } 907. \end{aligned}$$

Example $10P, P = (2, 1)$

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

$$2^9 = 512$$

$$2^{10} = 1024$$

$$\begin{aligned} 10 &= (1010)_2 \\ 10P &= 2^3 P + 2^1 P \\ &= 8P + 2P. \end{aligned}$$

$$\begin{aligned} m &= 3 \times (44)^2 * 735 \\ &\quad \text{mod } 907 \\ &= 538 \end{aligned}$$

$$P = (2, 4)$$

$$2P = (1 - 2, -2) = (-1, -2)$$

$$4P = (1 - 2 - 2, -2 - 2) = (1, -4)$$

$$8P = (1 - 2 - 2 - 2, -2 - 2 - 2) = (1, -10)$$

$$16P = (1 - 2 - 2 - 2 - 2, -2 - 2 - 2 - 2) = (1, 6)$$

$$\begin{aligned} m &= 3 \times 4 + 7 \\ &= 19 \times 8 \\ &= 19 \times 7 = 56 \end{aligned}$$

Example: $\text{Ord}_E(0,4) \cdot \text{Ord}_E(2,4) \cdot \frac{\text{Ord}_E(0,4)??}{\cdot 11} = 16.$

$$\text{④ } \# E = 16.$$

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

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

$$P = (0,4)$$

$$2P \neq \mathbb{H}$$

$$4P \neq \mathbb{H}$$

$$8P \neq$$

$$2P \neq \mathbb{H}$$

$$4P \neq \mathbb{H}$$

$$8P \neq \mathbb{H}$$

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

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

$$8P = (5, 0) \rightarrow \textcircled{D}$$

~~$$= 3 \times 5 + 7$$~~

$$8P = -8P.$$

$$16P = \mathbb{H}.$$

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

$$\therefore 2P = \mathbb{H}$$

$$\therefore 16P = \mathbb{H}.$$

$$\Leftrightarrow P = -P$$

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

$$2y_3 = 0$$

$$y_3 = 0.$$

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

$$E[2] = ?$$

$P \in E[2]$ if $2P = \Theta$.

if $P = -P$.
 $(x, y) = (x, -y)$

$$y = 0.$$

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

$$\begin{array}{c} \diagup \diagdown \\ x_1 x_2 x_3 \end{array}$$

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

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

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

$y=0$
given
only one x
as permutation

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

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

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

when $q \equiv 2 \pmod{3}$

$$q = 3k+2$$

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

$$= q-1.$$

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

Total $q+1$ points.

$$\rightarrow \Theta$$



$$\rightarrow y=0 \Rightarrow (\sqrt[3]{b}, 0).$$

$$t = q+1 - \#E$$

\swarrow
0.

$$q+1$$

Example q be odd prime power
 $q \equiv 3 \pmod{4}$

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

$q \equiv 3 \pmod{4} \Rightarrow -1$ is QR in F_q

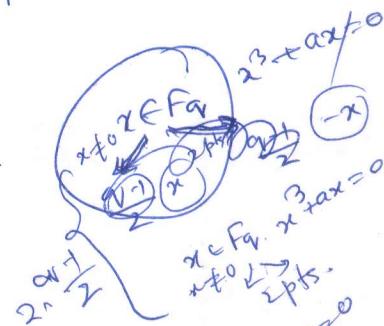
$$(-x)^3 + a(-x) = -(x^3 + ax)$$

$$\begin{aligned} (-1)^{\frac{q-1}{2}} &= (-1)^{\frac{4k+3-1}{2}} \\ &= (-1)^{\frac{4k+2}{2}} \\ &= (-1)^{\frac{2k}{2}} \\ &= (-1)^k \end{aligned}$$

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 .



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



if $x \in F_q, x \neq 0$ for which $x^3 + ax = 0$, then $x^3 + ax = 0$
 $x(x^2 + a) = 0$, $x = 0$ or $x = \pm\sqrt{-a}$.
 $\therefore x = 0$ or $x = \pm\sqrt{-a}$

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

$\rightarrow \textcircled{A}$:

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

$$\begin{aligned} &\text{order 2 pts.} \\ &(0,0) \text{ order 2 pts.} \\ &x=0 \text{ case: } x^3 + ax \neq 0 \\ &\text{then } x \rightarrow x^3 + ax \in QR. \\ &\text{if } x \rightarrow x^3 + ax \in QR \\ &\text{then } -x \rightarrow -x^3 - ax \in QR. \\ &\text{if } x \rightarrow x^3 + ax \in QR \\ &\text{then } -x \rightarrow (-x^3 - ax) \in QR. \end{aligned}$$

(20)

Menezes-Vanstone Elliptic Curve Cryptosystem

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

$$\mathcal{P} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$$

$$\mathcal{C} = E \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$$

$$\mathcal{K} = \{(E, \alpha, a, \beta) : \beta = a\alpha\}$$

- α, β are public
- a is secret

Encryption

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

define

$$e_K(x, k) =$$

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

When

$$y_0 = k\alpha$$

$$(c_1, c_2) = k\beta \cdot \begin{bmatrix} = k\alpha \\ = y_0 \end{bmatrix}$$

$$y_1 = c_1 x_1 \pmod{p}$$

$$y_2 = c_2 x_2 \pmod{p}$$

Decryption

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

define

$$d_K(y) = \begin{pmatrix} y_1^{-1} \pmod{p} \\ y_2^{-1} \pmod{p} \end{pmatrix}$$

when $a y_0 = (c_1, c_2)$.

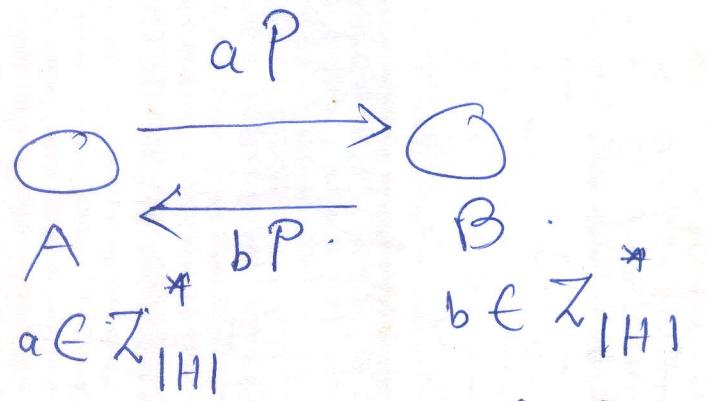
DH (Elliptic Curve Analog) (21) Key Exchange

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

Take a
Cyclic
Subgroup
H when
 $= \langle P \rangle.$

\downarrow
DLP is intractable.

(DH)



$$k = a(bP) = abP \quad k = b(aP) = abP$$

DLP over H.

$$H = \langle P \rangle.$$

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

$$\text{when } a \in \mathbb{Z}_{|H|}^*$$

Security
hardness of CDH.

Given $\langle P, aP, bP \rangle$ to compute $abP?$
 Computational DA problem (CDH).

Elliptic curves over finite fields

(22)

- 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 .

Then $F_{25} = \{0, 1, 2, 3, 4\}$

the set of all polynomials of
degree at most 1 with
coefficients from \mathbb{Z}_5

$$\begin{aligned}\omega^5 + 4\omega + 2 &= 0 \\ \omega^4 &= -4\omega - 2 \\ &= \omega + 3\end{aligned}$$

poly	vector form
0	00
1	01
2	02
3	03
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 modulo \mathbb{Z}_{25}

$$\begin{aligned}&= \{1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 1, \omega^2 = \omega + 3, (\omega+1)^2 = \omega + 3 + 2\omega + 1 \\ &\quad = 3\omega + 4, (\omega+2)^2 = \omega + 3 + 4\omega + 4 = 2, (\omega+3)^2 = \omega + 3 + 6\omega + 9 = 2\omega + 2 \\ &\quad (\omega+4)^2 = \omega + 3 + 8\omega + 16 = 4\omega + 4, (\cancel{\omega+5}) (2\omega)^2 = 4(\omega+3) = 4\omega + 2 \\ &\quad (2\omega+1)^2 = 4(\omega+3) + 4\omega + 1 = 3\omega + 3, (2\omega+2)^2 = 4(\omega+3) + 8\omega + 4 \\ &\quad = 2\omega + 1 \\ &\quad (2\omega+3)^2 = 4(\omega+3) + 12\omega + 9 = \omega + 1, (2\omega+4)^2 = 4(\omega+3) + 16\omega + 16 \\ &\quad = 3 \\ &\quad (\cancel{2\omega})^2 = 9(\omega+3) = 2\omega + 1, \end{aligned}$$

$$(3\omega)^2 = (-2\omega)^2 = \cancel{2\omega}$$

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

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

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

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

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

x	$x^3 + x + 4$	quadratic residue	y
0	$4 = 2^2$	Yes	$\pm 2 \rightarrow 2, 3$
-1	$1 = 1^2$	Yes	$\pm 1 \rightarrow 1, 4$
-2	$4 = 2^2$	Yes	$\pm 2 \rightarrow 2, 3$
-3	$4 = (\omega + 2)^2$	Yes	$\pm(\omega + 2) \rightarrow \omega + 2, 4\omega + 3$ $\pm 2 \rightarrow 2, 3$
-4	$2 = (\omega + 2)^2$	Yes	$\pm(\omega + 2) \rightarrow \omega + 2, 4\omega + 3$
ω	2	Yes	$\pm(\omega + 2) \rightarrow \omega + 2, 4\omega + 3$
$\omega + 1$	$\omega + 3 = \omega^2$	Yes	$\pm \omega \rightarrow \omega, 4\omega$
$\omega + 2$	3ω	No	-
$\omega + 3$	$\omega + 1$	No	-
$\omega + 4$	1	Yes	$\pm 1 \rightarrow 1, 4$
$\omega + 5$	$4\omega + 3$	No	-
$2\omega + 1$	$2\omega + 1 = (3\omega + 3)^2$	Yes	$\pm(3\omega + 3) \rightarrow 3\omega + 3, 2\omega + 2$
$2\omega + 2$	2ω	No	-
$2\omega + 3$	$4\omega + 1$	No	-
$2\omega + 4$	3ω	No	-
$3\omega + 5$	ω	No	-
$3\omega + 6$	$2\omega + 3$	No	-
$3\omega + 7$	$\omega + 2$	No	-
$3\omega + 8$	$3\omega + 3 = (2\omega + 1)^2$	Yes	$\pm(2\omega + 1) \rightarrow 2\omega + 1, 3\omega + 4$
$3\omega + 9$	1	Yes	$\pm 1 \rightarrow 1, 4$
$4\omega + 1$	$2 = (\omega + 1)^2$	Yes	$\pm(\omega + 1) \rightarrow \omega + 1, 4\omega + 4$
$4\omega + 2$	$4\omega + 4 = (2\omega + 1)^2$	Yes	$\pm(\omega + 4) \rightarrow \omega + 4, 4\omega + 1$
$4\omega + 3$	$2\omega + 3$	No	-
$4\omega + 4$	$4\omega + 4$	No	-
$4\omega + 5$	$4\omega + 5$	No	-

$$\begin{aligned} 2+7+3+1 \\ = 2+7=9=4 \end{aligned}$$

$$\begin{aligned} 6+8 \\ = 4+8=12=2 \end{aligned}$$

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

$$\begin{aligned} \omega^3 + \omega + 4 \\ \omega^7 + 3\omega + \omega + 4 \\ \omega + 3 + 4\omega + 4 \\ 5\omega + 7 \\ 2 \end{aligned}$$

$$\begin{aligned} \omega^3 + 3\omega^2 + 3\omega \\ + 1 + \omega + 4 \\ + 1 \\ \omega^7 + 3\omega + 3\omega \\ + 4\omega + 5\omega \\ 4\omega + 7\omega + 1 \\ 4\omega^5 + 2\omega + 1 \\ 4\omega + 1 + 2\omega \\ 6\omega + 1 + 1 \\ \omega + 2 + 1 \\ \vdots \end{aligned}$$

$$\begin{aligned} E/F_{25} \\ = \{ & (0, 1), (0, 3), \\ & (1, 1), (1, 4), \dots; \\ & (4, \omega + 2), (4, 4\omega + 3), \\ & \dots \} \cup \{0\} \end{aligned}$$

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

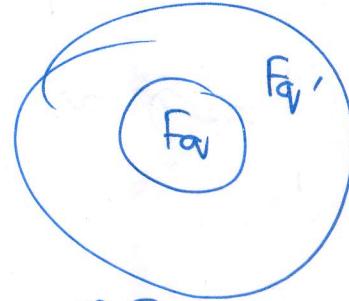
m-torsion

m-torsion points.

- $E/F_q \rightarrow$ Elliptic curve over \mathbb{F}_q , $q = p^n$, p prime.
- $P \in E/F_q$ is an m-torsion point if $mP = \Theta$
i.e. $\text{ord}(P) | m$.
- The set of m-torsion points of E is finite
& has size at most m^2 .

- If $\gcd(m, q) = 1$, then it is always possible to find an extension field F_{q^r} of F_q s.t.

$$\begin{aligned} |E[m]| \\ = & \left| \left\{ P \in E/F_{q^r} \mid mP = \Theta \right\} \right| \\ = & m^2 \end{aligned}$$



$$|E[m]| = \left| \left\{ P \in E/F_{q^r} \mid mP = \Theta \right\} \right|$$

$$\text{ord}(\Theta) = 1$$

→ form a subgroup of E/F_{q^r}

→ m-torsion subgroup of E/F_q

$$\cong \mathbb{Z}_m \times \mathbb{Z}_m$$

with $m | E/F_q$,

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

- (25)
- $q = 5$
 - $\# E/F_5 = 9$ (including Θ). Take $m = 3$
in prime, $\gcd(5, 3) = 1$,
 $\# E/F_{25} = 27$ (including Θ)
 $3 \nmid q^k - 1$, $m \nmid |E/F_{25}|$

- $E[3] \rightarrow$ set of all 3-torsion points.
 \rightarrow subgroup of E/F_{q^k}

when k is the smallest tre integer
s.t. $3|q^k - 1$ i.e. $k = 2$.

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

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

$$E[3] = \left\{ \Theta, (\omega+1, 4\omega), (\omega+1, \omega), \right.$$

$$(4, 4\omega+3), (4, \omega+2), (3, 2), (3, 3),$$

$$\left. (4\omega+2, 4\omega+1), (4\omega+2, \omega+4) \right\}$$

To check $3(\omega+1, 3P) = \Theta$ for $P = (\omega+1, 4\omega)$

$$\begin{aligned} \lambda &= 3((\omega+1)^2 + 1)(2 \times (4\omega))^{-1} \\ &= 3(\omega^2 + 3 + 2\omega^2 + 2)(3\omega)^{-1} \\ &= 3(\omega + 2\omega^2) 2\omega^{-1} \end{aligned}$$

$$3^{-1} = 9 \quad (\text{mod } 5)$$

$$2^{-1} = 3 \quad (\text{mod } 5)$$

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

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

(26)

Calculate $2P$

$$\lambda = \frac{(3x_1^2 + 1)}{2(\omega + 2)}$$

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

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

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

$$= 2 \omega^9$$

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

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

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

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

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

$$\omega^{16} = 3(\omega+3) + 2\omega = 3\omega+9$$

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

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

$$\cancel{\omega^{25}} = (\omega^{12})^3 = 16\omega = \omega$$

$$\omega^{26} \neq (4\omega)^2 = 16\omega^2 = \omega^2$$

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

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

$$\omega^{20} = 3(\omega+3) = 3\omega+9$$

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

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

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

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

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

$$E/F_{24}: \frac{y^L}{x^3 + ax^2 + b}$$

$$E/F_{25}: y^L = x^3 + x + 4$$

$$a=1, b=4$$

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

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

$$= \omega+3+3\omega \\ = 4\omega+3.$$

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

$$= 7\omega+12 \\ = 2\omega+2$$

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

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

$$= 4\omega+6$$

$$\begin{aligned} \omega^{24} &= 1 \\ (\omega+5)^{-1} &= \omega^9 \\ &= 3\omega+1 \end{aligned}$$

$$\begin{aligned} \omega^{23} &= 3\omega+3+\omega = 2\omega+3 = 4\omega+1 \\ \omega^{24} &= 2(\omega+3)+3\omega \\ &= 1 \end{aligned}$$

$$\begin{aligned} \omega^6 &= 4(\omega+3)+\omega \\ &= 5\omega+12 \end{aligned}$$

$$= 2$$

$$\omega^7 = 2\omega$$

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

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

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

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

$$x_3 = \lambda - 2x_1$$

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

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

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

$$= 5\omega - 1$$

$$P = \begin{pmatrix} 4, \omega+2 \\ 4 \end{pmatrix}$$

$$2P = \begin{pmatrix} 4, 4\omega+3 \\ 4 \end{pmatrix}, \quad -P = \begin{pmatrix} 4, -\omega-2 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} 4, 4\omega+3 \\ 4 \end{pmatrix}$$

$\Rightarrow 3P$

$$2P = -P \Rightarrow 3P = \emptyset$$

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

$$F/F_5: y \sim x^3 + x + 4$$

$$Q_5 = \{1, 4\}$$

$$\begin{matrix} 1 \\ 2 \\ 3 \\ 4 \end{matrix}$$

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

(28) \rightarrow Miller's algm. (PPT algm).
Bilinear Pairing \rightarrow 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

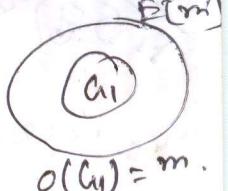
$$\epsilon_m: G_1 \times G_2 \rightarrow F_{q^k}^*$$

$| k \rightarrow \text{embedding degree of the curve.}$

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).

$| E[m] | = m$

$E[m]$


Then ϵ_m satisfies the following properties.

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

(29)

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

$$\Rightarrow \exists Q \in G_2 \text{ s.t. } \text{o}(P, Q) = m \text{ in } F_{q^k}.$$

$$\text{o}(B \epsilon_m(P, Q)) = m \text{ in } F_{q^k}^*.$$

- 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 $P \in G_1$, $\text{o}(P) = m$, $R \in \langle P \rangle$.

Let $Q \in G_2$ for which $\epsilon_m(P, Q)$ is a primitive m -th root of unity of F_{q^k} so $\mu_m = \langle \epsilon_m(P, Q) \rangle$.

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

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

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

is an isomorphism.

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

Index

30

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

- Wt. $R = \gamma P \in \langle P \rangle \rightarrow \gamma$ is the DL over the curve

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

$$= \ell_m(\gamma P, Q)$$

$$= \ell_m(P, Q)^\gamma$$

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

Steps in Solving ELDLP

- E/F_q , $E[m] \rightarrow m\text{-torsion subgroup of } E(F_q)$.

AlgMDL(E, m, P, R) $m \nmid a, \gcd(m, a) = 1, m \nmid a-1$
 $m \nmid F_q, \gcd(m, q) = 1$

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

- find $Q \in E[m]$ for which $\alpha = \ell_m(P, Q)$
 When $P \in G_1$, G_1 is a cyclic subgroup of $E[m]$, of order $\phi(G_1) = m$.

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

- Determine the DL γ of β w.r.t. the basis.

(31)

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

- PPT algos. due to Miller can be used to compute pairing.
- DLP Solvable or not \rightarrow 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.
- Menzies, Okamoto, Vanstone (MOV) showed
 - that for the class of supersingular elliptic curve, the value of k is ≤ 6 .
 - they provided an approach ~~to~~ for finding a suitable pt. ϕ over such curves.
 - overall result is a probabilistic subexponential time algos. for solving the DLP on supersingular elliptic curves.