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

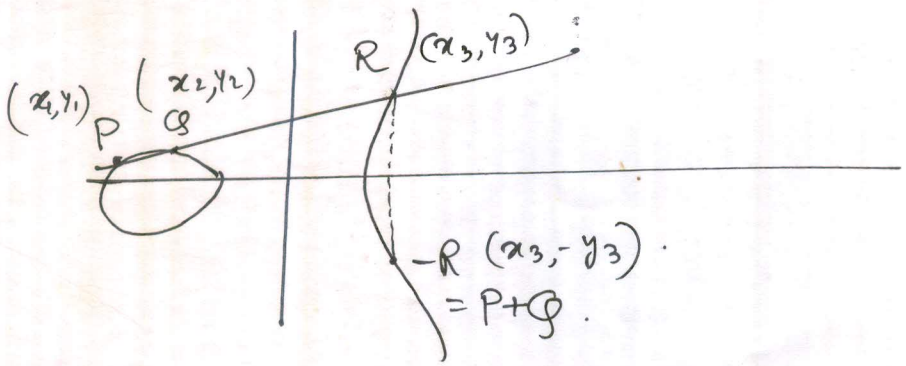
$$y^2 \equiv x^3 + ax + b \pmod{p},$$

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 →

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

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

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

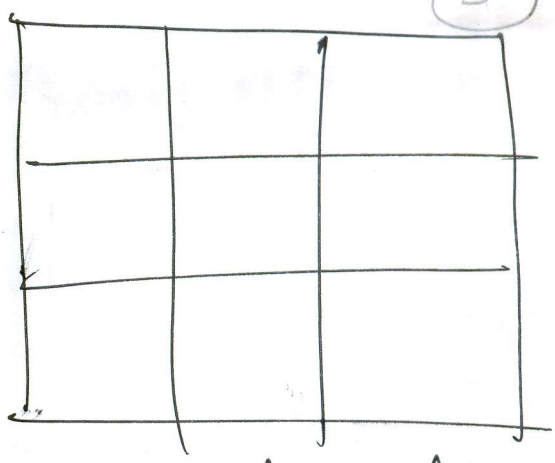
if

$X_1 = \lambda X_2$

$Y_1 = \lambda Y_2$

$Z_1 = \lambda Z_2$

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.

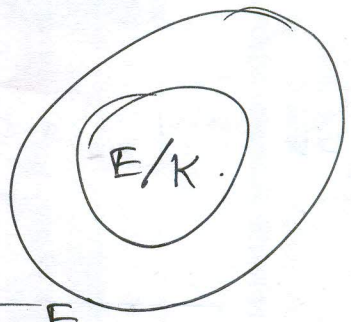
$\oplus \to$ pt. at infinity (if $Q = -P$, then $P + Q = \oplus$ $= -\oplus$)

$\to$ 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) ~~For all~~ if $P, Q \in E$, then $P+Q = Q+P$.

Supersingular Elliptic curve

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

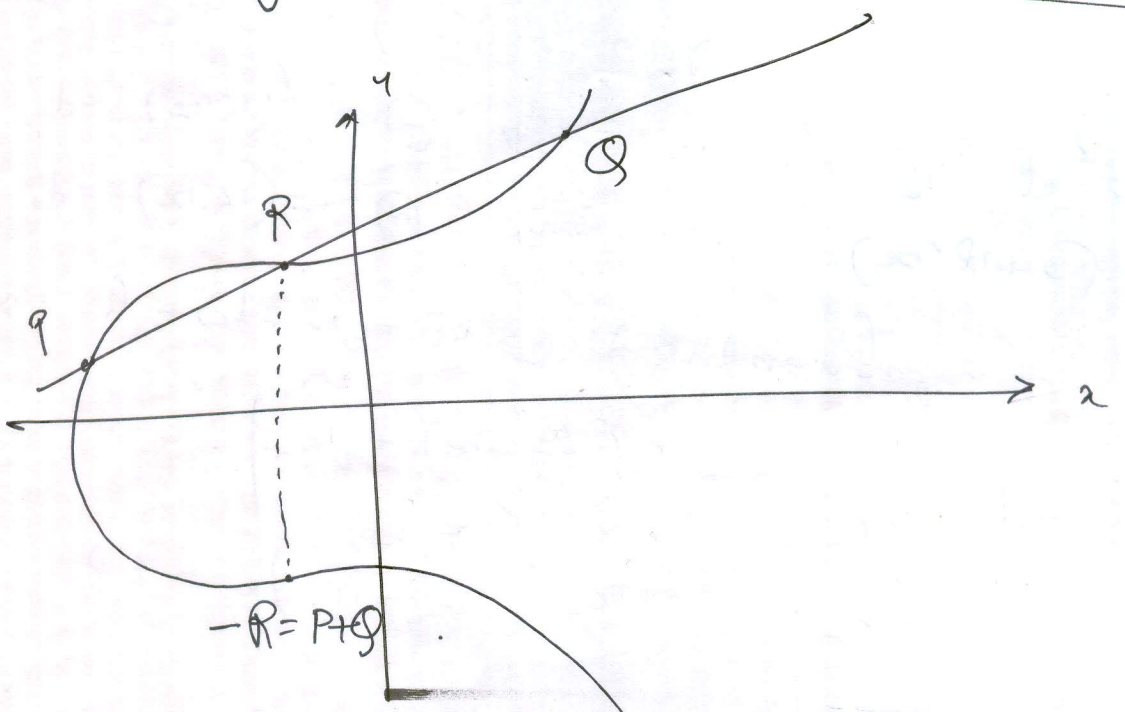
$$t = q+1 - \#E(F_q), \quad q = p^m, \quad p = ch(F_q),$$

a prime.

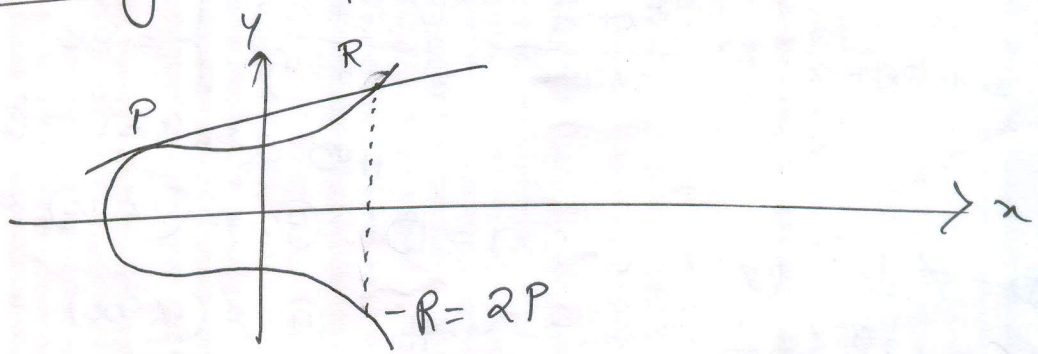
Theorem (Waterhouse) E/F_q is supersingular if

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

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

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

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

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

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

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 $y_3 = 0$

$\Leftrightarrow P = -P$.

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

$2y_3 = 0$

$y_3 = 0$.

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

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