Problem Sheet 9

9.1

$$E(\mathbb{Z}_7) = \{(x,y) \in \mathbb{Z}_7 \times \mathbb{Z}_7 \mid y^2 = x^3 + x + 2\}$$

a)

x	x^2	x^3+x+2	y	Points
0	0	2	3,4	(0,3) (0,4)
1	1	4	2,5	(1,2) (1,5)
2	4	5	–	–
3	2	4	2,5	(3,2) (3,5)
4	2	0	0	(4,0)
5	4	6	–	–
6	1	0	0	(6,0)

The set of points: $\{(0,3), (0,4), (1,2), (1,5), (3,2), (3,5), (4,0), (6,0)\}$

b) $P \in E(\mathbb{Z}_7)$

$G_P = \{nP \mid n \geq 0\}$

for point $(0,3)$

$$s = \frac{3x_p^2 + a}{2y_p} = \frac{3 \cdot 0^2 + 1}{2 \cdot 3} = \frac{1}{6} \bmod 7 = 6$$

$$x_r = s^2 - x_p - x_q = 36 \bmod 7 = 1$$

$$y_r = s(x_p - x_r) - y_p = 6(0-1) - 3 = -9 \bmod 7 = 5$$

$(1, 5)$

For point $(0, 4)$

$$s = \frac{3 \cdot 0^2 + 1}{2 \cdot 4} = \frac{1}{8} \text{ mod } 7 = 8$$

$x_r = 64 - 0 - 0 = 64 \text{ mod } 7 = 1$

$y_r = 8(0 - 1) - 4 = -12 \text{ mod } 7 = 2$

$(1, 2)$

For point $(1, 2)$

$$s = \frac{3 \cdot 1 + 1}{2 \cdot 2} = \frac{4}{4} \text{ mod } 7 = 1$$

$x_r = 1 - 1 - 1 = -1 \text{ mod } 7 = 6$

$y_r = 1(1 - 6) - 2 = -5 - 2 \text{ mod } 7$

$= -7 \text{ mod } 7$

$= 0$

$(6, 0)$

For point $(1, 5)$

$$s = \frac{3 \cdot 1 + 1}{2 \cdot 5} = \frac{4}{10} = \frac{2}{5} \text{ mod } 7 = 6$$

$x_r = 36 - 1 - 1 = 34 \text{ mod } 7 = 6$

$y_r = 6(1 - 6) - 5 = -35 \text{ mod } 7 = 0$

$(6, 0)$

for (3,2)

$$s = \frac{3 \cdot 9 + 1}{2 \cdot 2} = \frac{28}{4} = 7 \bmod 7 = 0$$

$$x_r = 0 - 3 - 3 = -6 \bmod 7 = 1$$

$$y_r = -2 \bmod 7 = 5$$

(1, 5)

For (3,5)

$$s = \frac{3 \cdot 9 + 1}{2 \cdot 5} = \frac{28}{10} = \frac{14}{5} \bmod 7 = 0$$

$$x_r = 0 - 3 - 3 = -6 \bmod 7 = 7$$

$$y_r = -5 \bmod 7 = 2$$

(1, 2)

For (4,0)

$$s = \frac{3 \cdot 16 + 7}{2 \cdot 0} = \text{undefined.}$$

No ~~group~~ other points.

Cyclic subgroups of C_P:

$$C_{P_1} = \{(0,3), (1,5), (3,2), (6,0)\}$$

$$|C_{P_1}| = 4$$

$$C_{P_2} = \{(0,4), (1,2), (3,5), (6,0)\}$$

$$|C_{P_2}| = 4$$

$$C_{P_3} = \{(4,0)\}$$

$$|C_{P_3}| = 7$$

Problem 9.2.

$$P = (30, 10), \quad E(\mathbb{Z}_{191}) = \{(x,y) \in \mathbb{Z}_{191} \times \mathbb{Z}_{191} \mid y^2 = x^3 + x + 7\}$$

a) $a = 8$, $x_a = 8$

$$E: y^2 = x^3 + x + 1 \pmod{191}$$

$$2P = P + P$$

$$s = \frac{3 \cdot x_p^2 + a}{2 y_p} = \frac{3 \cdot 900 + 1}{2 \cdot 10} = \frac{2700 + 1}{20} = \frac{2701}{20} \bmod 191$$

$$= 30$$

$$x_r = s^2 - 2x_p = 900 - 2 \cdot 30 = 840$$

$$y_r = s(x_p - x_r) - y_p = 30(30 - 840) - 10$$

$$= 30(-810) - 10$$

$$= -24310 \bmod 191$$

$$= 138$$

~~So~~ From 2P to 8 P we calculate:

$$y_A = 8 \cdot (30, 10) = (163, 69)$$

$\therefore$ Alice sends Bob $y_A = (163, 69)$

b) $b = 11$, $x_B = 11$

Compute ~~x~~ $y_B = 11P = 11 \cdot (30, 10) = (16, 22)$

$\therefore$ Bob sends $y_B = (16, 22)$ to Alice.

c) ~~A~~ Shared secret both need to calculate:

Alice : $S = x_A \cdot y_B = 8 \cdot (16, 22) = \cancel{(107, 29)}\ (107, 162)$

Bob : $S = x_B \cdot y_A = 11 \cdot (163, 69) = (107, 162)$

~~Bob~~ ~~These points are the inverse of each other.~~ The shared secret between Alice & Bob is (107, 162)

Problem 9.3

$$E(Z_{193}) = \{(x,y) \in Z_{193} \times Z_{193} \mid y^2 = x^3 + x + 1\}$$

$G = (28, 65)$, $n = 67$

a) $k = 37$, $K = ?$

$$K = k \cdot G$$
$$= 37 \cdot (28, 65)$$
$$K = (166, 154)$$

b) $e = 21$, P, $r = ?$

$$P = e \cdot G$$
$$= 21 \cdot (28, 65)$$
$$P = (35, 114)$$

$\therefore P = (35, 114)$ and $r = 35$

$\cancel{r = P \cdot x}$

$\cancel{= (35, 114)}$

c) $h = 123$

$(r, s) = ?$

$s = e^{-1} \cdot (h + r \cdot k) \pmod n$

$s = 21^{-1} \bmod 67 \ (123 + 35 \cdot 37)$

$= 16 \ (1418) \bmod 67$

$= 22688 \bmod 67$

$s = 42$

$\therefore (r, s) = (35, 42)$

d)