Math 116 HW6 Jun Ryu

1) a) $E(\mathbb{F}_5)$

$x=0 \Rightarrow y^2 = 0^3+0+2=2$

2 is not a square modulo 5

$x=1 \Rightarrow y^2 = 1^3+1+2 = 4$

$2^2 \equiv 4 \pmod 5 \Rightarrow y=2$

$3^2 \equiv 4 \pmod 5 \Rightarrow y=3$

$\Rightarrow (1,2)$ and $(1,3)$

$x=2 \Rightarrow y^2 = 2^3+2+2 = 12 \equiv 2 \pmod 5$

2 is not a square modulo 5

$x=3 \Rightarrow y^2 = 3^3+3+2 = 32 \equiv 2 \pmod 5$

2 is not a square modulo 5

$x=4 \Rightarrow y^2 = 4^3+4+2 = 70 \equiv 0 \pmod 5$

$0^2 \equiv 0 \pmod 5 \Rightarrow y=0$

$\Rightarrow (4,0)$

So, list of points is $\{\mathcal{O}, (1,2), (1,3), (4,0)\}$

b)

	$\mathcal{O}$	$(1,2)$	$(1,3)$	$(4,0)$
$\mathcal{O}$	$\mathcal{O}$	$(1,2)$	$(1,3)$	$(4,0)$
$(1,2)$	$(1,2)$	$(4,0)$	$\mathcal{O}$	$(1,3)$
$(1,3)$	$(1,3)$	$\mathcal{O}$	$(4,0)$	$(1,2)$
$(4,0)$	$(4,0)$	$(1,3)$	$(1,2)$	$\mathcal{O}$

Theorem 6.6 (Elliptic Curve Addition Algorithm). *Let*

$$E : Y^2 = X^3 + AX + B$$

be an elliptic curve and let P_1 and P_2 be points on E.

(a) *If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$.*
(b) *Otherwise, if $P_2 = \mathcal{O}$, then $P_1 + P_2 = P_1$.*
(c) *Otherwise, write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.*
(d) *If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \mathcal{O}$.*
(e) *Otherwise, define λ by*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2, \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2, \end{cases}$$

and let

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \text{and} \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

Then $P_1 + P_2 = (x_3, y_3)$.

Scratch work:

$\underline{(1,2) + (1,2):}$

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

$x_3 = 1^2 - 1 - 1 = -1 \equiv 4$

$y_3 = 1(1-4) - 2 = -5 \equiv 0$

$\Rightarrow (4,0)$

$\underline{(1,2) + (4,0):}$ $\lambda = \dfrac{0-2}{4-1} = \dfrac{-2}{3} \equiv \dfrac{3}{3} \equiv 1$

$x_3 = 1^2 - 1 - 4 = -4 \equiv 1$, $y_3 = 1(1-(-4)) - 2 = 3$

$\Rightarrow (1,3)$

$(1,3)+(4,0)$: $\lambda = \frac{0-3}{4-1} = \frac{-3}{3} = -1 \equiv 4$

$x_3 = 4^2 - 1 - 4 = 11 \equiv 1, \; y_3 = 4(1-1) - 3 = -3$
$\equiv 2$

$\Rightarrow (1,2)$

2) a)

```
In [5]: E = EllipticCurve(GF(11),[2,5])
        E.points()

Out[5]: [(0 : 1 : 0), (0 : 4 : 1), (0 : 7 : 1), (3 : 4 : 1), (3 : 7 : 1), (4 : 0 : 1), (8 : 4 : 1), (8 : 7 : 1), (9 : 2 : 1),
        (9 : 9 : 1)]
```

So, the list of points are

$\{\mathcal{O}, (0,4), (0,7), (3,4), (3,7), (4,0),$
$(8,4), (8,7), (9,2), (9,9)\}$

b)

```
In [7]: E = EllipticCurve( GF(11), [2, 5] )
        print([(P+Q) for P in E.points() for Q in E.points()])

        [(0 : 1 : 0), (0 : 4 : 1), (0 : 7 : 1), (3 : 4 : 1), (3 : 7 : 1), (4 : 0 : 1), (8 : 4 : 1), (8 : 7 : 1), (9 : 2 : 1),
        (9 : 9 : 1), (0 : 4 : 1), (9 : 2 : 1), (0 : 1 : 0), (8 : 7 : 1), (9 : 9 : 1), (8 : 4 : 1), (3 : 7 : 1), (4 : 0 : 1),
        (3 : 4 : 1), (0 : 7 : 1), (0 : 7 : 1), (0 : 1 : 0), (9 : 9 : 1), (9 : 2 : 1), (8 : 4 : 1), (8 : 7 : 1), (4 : 0 : 1),
        (3 : 4 : 1), (0 : 4 : 1), (3 : 7 : 1), (3 : 4 : 1), (8 : 7 : 1), (9 : 2 : 1), (8 : 4 : 1), (0 : 1 : 0), (9 : 9 : 1),
        (0 : 7 : 1), (3 : 7 : 1), (4 : 0 : 1), (0 : 4 : 1), (3 : 7 : 1), (9 : 9 : 1), (8 : 4 : 1), (0 : 1 : 0), (8 : 7 : 1),
        (9 : 2 : 1), (3 : 4 : 1), (0 : 4 : 1), (0 : 7 : 1), (4 : 0 : 1), (4 : 0 : 1), (8 : 4 : 1), (8 : 7 : 1), (9 : 9 : 1),
        (9 : 2 : 1), (0 : 1 : 0), (0 : 4 : 1), (0 : 7 : 1), (3 : 7 : 1), (3 : 4 : 1), (8 : 4 : 1), (3 : 7 : 1), (4 : 0 : 1),
        (0 : 7 : 1), (3 : 4 : 1), (0 : 4 : 1), (9 : 2 : 1), (0 : 1 : 0), (9 : 9 : 1), (8 : 7 : 1), (8 : 7 : 1), (4 : 0 : 1),
        (3 : 4 : 1), (3 : 7 : 1), (0 : 4 : 1), (0 : 7 : 1), (0 : 1 : 0), (9 : 9 : 1), (8 : 4 : 1), (9 : 2 : 1), (9 : 2 : 1),
        (3 : 4 : 1), (0 : 4 : 1), (4 : 0 : 1), (0 : 7 : 1), (3 : 7 : 1), (9 : 9 : 1), (8 : 4 : 1), (8 : 7 : 1), (0 : 1 : 0),
        (9 : 9 : 1), (0 : 7 : 1), (3 : 7 : 1), (0 : 4 : 1), (4 : 0 : 1), (3 : 4 : 1), (8 : 7 : 1), (9 : 2 : 1), (0 : 1 : 0),
        (8 : 4 : 1)]
```

	$\mathcal{O}$	(0,4)	(0,7)	(3,4)	(3,7)	(4,0)	(8,4)	(8,7)	(9,2)	(9,9)
$\mathcal{O}$	$\mathcal{O}$	(0,4)	(0,7)	(3,4)	(3,7)	(4,0)	(8,4)	(8,7)	(9,2)	(9,9)
(0,4)	(0,4)	(9,2)	$\mathcal{O}$	(8,7)	(9,9)	(8,4)	(3,7)	(4,0)	(3,4)	(0,7)
(0,7)	(0,7)	$\mathcal{O}$	(9,9)	(9,2)	(8,4)	(8,7)	(4,0)	(3,4)	(0,4)	(3,7)
(3,4)	(3,4)	(8,7)	(9,2)	(8,4)	$\mathcal{O}$	(9,9)	(0,7)	(3,7)	(4,0)	(0,4)
(3,7)	(3,7)	(9,9)	(8,4)	$\mathcal{O}$	(8,7)	(9,2)	(3,4)	(9,4)	(0,7)	(4,0)
(4,0)	(4,0)	(8,4)	(8,7)	(9,9)	(9,2)	$\mathcal{O}$	(0,4)	(0,7)	(3,7)	(3,4)
(8,4)	(8,4)	(3,7)	(4,0)	(0,7)	(3,4)	(9,4)	(9,2)	$\mathcal{O}$	(9,9)	(8,7)
(8,7)	(8,7)	(4,0)	(3,4)	(3,7)	(0,4)	(0,7)	$\mathcal{O}$	(9,9)	(8,4)	(9,2)
(9,2)	(9,2)	(3,4)	(0,4)	(4,0)	(0,7)	(3,7)	(9,9)	(8,4)	(8,7)	$\mathcal{O}$
(9,9)	(9,9)	(0,7)	(3,7)	(0,4)	(4,0)	(3,4)	(8,7)	(9,2)	$\mathcal{O}$	(8,4)

3)

```
In [8]: E = EllipticCurve(GF(5),[1,1])
        P = E.point([4,2])
        [(n*P) for n in list(range(1, 9))]

Out[8]: [(4 : 2 : 1),
         (3 : 4 : 1),
         (2 : 4 : 1),
         (0 : 4 : 1),
         (0 : 1 : 1),
         (2 : 1 : 1),
         (3 : 1 : 1),
         (4 : 3 : 1)]
```

From above, we notice that the 5^{th} iteration gives us $(0,1) = Q$. So,

$Q = nP$, when $\boxed{n=5}$.

4) We express n as $is+r$, for some $0 \le r < s$. Then, we have

$$Q = nP = (is+r)P = isP + rP$$
$$= i(\mathcal{O}) + rP = rP.$$

So, since n_0 is the smallest solution to $Q = nP$, $r \ge n_0$. If $r = n_0$, then r is a solution. So, we consider the case where $r > n_0$. Then, we have

$$\mathcal{O} = Q - Q = rP - n_0 P = (r - n_0)P$$

We know sP is the smallest multiple of P equaling $\mathcal{O}$, so we have

$$r - n_0 \ge s \Rightarrow r \ge s + n_0,$$

but this contradicts $r < s$, so $r \not> n_0$. Thus, $r = n_0$ and we conclude $n = is + n_0$. ✓