VE475 Homework 10

Liu Yihao 515370910207

Ex. 1 — Group structure on an elliptic curve

$$\begin{aligned}
x_3^3 + bx_3 + c &= (m^2 - x_1 - x_2)^3 + b(m^2 - x_1 - x_2) + c \\
&= m^6 - 3m^4x_1 - 3m^4x_2 + 3m^2x_1^2 + 6m^2x_1x_2 + 3m^2x_2^2 + bm^2 \\
&\quad - x_1^3 - 3x_1^2x_2 - 3x_1x_2^2 - bx_1 - x_2^3 - bx_2 + c \\
y_3^2 &= m^2(2x_1 + x_2 - m^2)^2 - 2m(2x_1 + x_2 - m^2)y_1 + y_1^2 \\
&= m^6 - 4m^4x_1 - 2m^4x_2 + 2m^3y_1 + 4m^2x_1x_2 + m^2x_2^2 - 4mx_1y_1 - 2mx_2y_1 + y_1^2 \\
x_3^3 + bx_3 + c - y_3^2 &= m^4x_1 - m^4x_2 - 2m^3y_1 - m^2x_1^2 + 2m^2x_1x_2 + 2m^2x_2^2 + bm^2 \\
&\quad + 4mx_1y_1 + 2mx_2y_1 - x_1^3 - 3x_1^2x_2 - 3x_1x_2^2 - bx_1 - x_2^3 - bx - 2 - y_1^2 + c
\end{aligned}$$

When $P_1 \neq P_2$, $m = \dfrac{y_2 - y_1}{x_2 - x_1}$

$$\begin{aligned}
x_3^3 + bx_3 + c - y_3^2 = -\frac{1}{(x_1 - x_2)^3}&(x_1^6 - 3x_1^4x_2^2 + bx_1^4 - 2bx_1^3x_2 - 2x_1^3y_1^2 + 2x_1^3y_1y_2 + x_1^3y_2^2 - cx_1^3 \\
&+ 3x_1^2x_2^4 - 3x_1^2x_2y_2^2 + 3cx_1^2x_2 + 2bx_1x_2^3 + 3x_1x_2^2y_1^2 - 3cx_1x_2^2 - bx_1y_1^2 + 2bx_1y_1y_2 \\
&- bx_1y_2^2 - x_2^6 - bx_2^4 - x_2^3y_1^2 - 2x_2^3y_1y_2 + 2x_2^3y_2^2 + cx_2^3 + bx_2y_1^2 - 2bx_2y_1y_2 + bx_2y_2^2 \\
&+ y_1^4 - 2y_1^3y_2 + 2y_1y_2^3 - y_2^4)
\end{aligned}$$

Since $y_1^2 = x_1^3 + bx + c$, $y_2^2 = x_2^3 + bx + c$, we can get

$$\begin{aligned}
x_3^3 + bx_3 + c - y_3^2 &= -\frac{1}{(x_1 - x_2)^3}[x_1^3(x_2^3 + bx_2 + c) - x_2^3(x_1^3 + bx_1 + c) - 2x_1^3(x_1^3 + bx_1 + c) \\
&\quad + 2x_2^3(x_2^3 + bx_2 + c) + 3x_1^2x_2^4 - 3x_1^4x_2^2 + (x_1^3 + bx_1 + c)^2 - (x_2^3 + bx_2 + c)^2 \\
&\quad + bx_1^4 - bx_2^4 - cx_1^3 + cx_2^3 + x_1^6 - x_2^6 - bx_1(x_1^3 + bx_1 + c) + bx_2(x_1^3 + bx_1 + c) \\
&\quad - bx_1(x_2^3 + bx_2 + c) + bx_2(x_2^3 + bx_2 + c) + 2bx_1x_2^3 - 2bx_1^3x_2 - 3cx_1x_2^2 + 3cx_1^2x_2 \\
&\quad + 2y_1y_2(x_2^3 + bx_2 + c) + 2x_1^3y_1y_2 - 2x_2^3y_1y_2 + 3x_1x_2^2(x_1^3 + bx_1 + c) \\
&\quad - 3x_1^2x_2(x_2^3 + bx_2 + c) - y_1y_2(2x_1^3 + 2bx_1 + 2c) + 2bx_1y_1y_2 - 2bx_2y_1y_2] \\
&= 0
\end{aligned}$$

So

$$y_3^2 = x_3^3 + bx_3 + c$$

When $P_1 = P_2$, $x_1 = x_2$, $y_1 = y2$, $m = \dfrac{3x_1^2 + b}{2y_1}$

$$x_3^3 + bx_3 + c - y_3^2 = x_1^3 + bx_1 - y_1^2 + c$$

Since $y_1^2 = x_1^3 + bx + c$, we can get

$$y_3^2 = x_3^3 + bx_3 + c$$

So the addition law over E is proved.

Then we need to proved the commutative law, which means for $P_1, P_2 \in E$ $P_1 + P_2 = P_2 + P_1$. Suppose $P_1 + P_2 = (x, y)$, $P_2 + P_1 = (x', y')$, first, when $P_1 = P_2$, it is obviously true. Otherwise, we know $m = m' = \dfrac{y_2 - y_1}{x_2 - x_1}$.

$$x = x' = m^2 - x_1 - x_2$$
$$y = m(x_1 - x) - y_1 = \frac{(x_1 - x)(y_2 - y_1) - (x_2 - x_1)y_1}{x_2 - x_1} = \frac{x_1y_2 - x_2y_1 - x(y_2 - y_1)}{x_2 - x_1}$$
$$y' = m(x_2 - x) - y_2 = \frac{(x_2 - x)(y_2 - y_1) - (x_2 - x_1)y_2}{x_2 - x_1} = \frac{x_1y_2 - x_2y_1 - x(y_2 - y_1)}{x_2 - x_1}$$
$$y = y'$$

So the commutative law is proved.

At last we need to prove the associative law, which means for $P_1, P_2, P_3 \in E$, $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

$$x_4' = m_{1,2}^2 - x_1 - x_2$$
$$x_4 = m_{4',3} - x_4' - x_3$$

Ex. 2 — Number of points on an elliptic curve

1.

$$m_2 \equiv \frac{3x_1^2 + 3}{2y_1} \equiv 9 \bmod 11$$
$$x_2 \equiv m_2^2 - 2x_1 \equiv 10 \bmod 11$$
$$y_2 \equiv m_2(x_1 - x_2) - y_1 \equiv 6 \bmod 11$$
$$[2]P = (10, 6)$$

$$m_4 \equiv \frac{3x_2^2 + 3}{2y_2} \equiv 6 \bmod 11$$
$$x_4 \equiv m_4^2 - 2x_2 \equiv 5 \bmod 11$$
$$y_4 \equiv m_4(x_4 - x_4) - y_2 \equiv 2 \bmod 11$$
$$[4]P = (5, 2)$$

$$m_5 \equiv \frac{y_4 - y_1}{x_4 - x_1} \equiv 6 \bmod 11$$
$$x_5 \equiv m_5^2 - x_4 - x_1 \equiv 1 \bmod 11$$
$$y_5 \equiv m_5(x_4 - x_5) - y_4 \equiv 0 \bmod 11$$
$$[5]P = (1, 0)$$

Since $y_5 = 0$,

$$[10]P = (0, 0)$$

2. There are 10 points.

3.

x mod 11	y^2 mod 11	y mod 11	Points on E
0	7	/	
1	0	/	
2	10	0	(1,0)
3	10	/	
4	6	/	
5	4	2 or 9	(5,2) or (5,9)
6	10	/	
7	8	/	
8	4	2 or 9	(8,2) or (8,9)
9	4	2 or 9	(9,2) or (9,9)
10	3	5 or 6	(10,5) or (10,6)

The elliptic curve E has 10 points: 9 calculated from the equation plus the point at the infinity $\mathcal{O}$.

Ex. 3 — ECDSA

In the Elliptic Curve Digital Signature Algorithm, we need a curve E, Point $G \in E$ and the order n of G which means $[n]G = \mathcal{O}$. We also need a cryptographic hash function h.

Alice creates a key pair, consisting of a private key integer d_A, randomly selected in the interval $[1, n-1]$, and a public key curve point $Q_A = [d_A]G$.

When Alice wants to sign a message m, the procedure is:

1. Calculate $e = h(m)$.
2. Let z be L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Generate a random integer k in $[1, n-1]$.
4. Calculate $P : (x_1, y_1) = [k]G$.
5. Calculate $r \equiv x_1 \bmod n$. If $r = 0$, retry from step 3.
6. Calculate $s \equiv k^{-1}(z + rd_A) \bmod n$. If $s = 0$, retry from step 3.

7. The signature is the pair (r, s).

When Bob wants to authenticate Alice's signature, he must have a copy of her public-key curve point Q_A. First he can verify Q_A is a valid curve point as follows:

1. Check that Q_A is not equal to the identity element $\mathcal{O}$.
2. Check that Q_A lies on the curve.
3. Check that $[n]Q_A = \mathcal{O}$.

After that, Bob follows these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = h(m)$.
3. Let z be L_n leftmost bits of e, where L_n is the bit length of the group order n.
4. Calculate $w \equiv s^{-1} \bmod n$
5. Calculate $u_1 \equiv zw \bmod n$ and $u_2 \equiv rw \bmod n$.
6. Calculate the curve point $P : (x_1, y_1) = [u_1]G + [u_2]Q_A$. If $P = \mathcal{O}$, the signature is invalid.
7. The signature is valid if $r \equiv x_1 \bmod n$, invalid otherwise.