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

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

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 $P_1, P_2, P_3 \in E$, $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Suppose we have 9 points: $\mathcal{O}, P_1, P_2, P_3, P_1 + P_2, P_2 + P_3, -(P_1 + P_2), -(P_2 + P_3), -(P_1 + P_2 + P_3)$. Connect them with 6 lines, the sum of the three values on any of them is zero. The central point $-(P_1 + P_2 + P_3)$ lies on the line through P_1 and $P_2 + P_3$, and also lies on the line through $P_1 + P_2$ and P_3. Then we can conclude that $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

So the associative law is proved.

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.

Now we should validate the correctness of the algorithm. Suppose we have $P : (x_1, y_1) = [u_1]G + [u_2]Q_A$ in step 6 of authentication.

$$\begin{aligned} P &= [u_1]G + [u_2]Q_A \\ &= [u_1 + u_2 d_A]G \\ &= [zs^{-1} + rd_A s^{-1}]G \\ &= [(z + rd_A)s^{-1}]G \\ &= [(z + rd_A)(k^{-1}(z + rd_A))^{-1}]G \\ &= [k]G \end{aligned}$$

The benefits of ECDSA is that we can get the same level of security as RSA but with smaller keys. Smaller keys have faster algorithms for generating signatures because the math involves smaller numbers. Smaller public keys mean smaller certificates and less data to pass around to establish a TLS connection. This means quicker connections and faster loading times on websites.

Ex. 4 — BB84

In the BB84 scheme, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a string of n qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$$

$$|\psi_{00}\rangle = |0\rangle$$

$$|\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Alice sends $|\psi\rangle$ over a public and authenticated quantum channel $\mathcal{E}$ to Bob. Since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits. Also, after Bob has received the qubits, we know that Eve cannot be in possession of a copy of the qubits sent to Bob, by the no-cloning theorem, unless she has made measurements. Her measurements, however, risk disturbing a particular qubit with probability 1/2 if she guesses the wrong basis.

Bob proceeds to generate a string of random bits b' of the same length as b and then measures the string he has received from Alice, a'. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in a and a' where b and b' do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

Ex. 5 — Quantum key distribution

1. Alice and Bob use the quantum channel to produce and distribute a key, and they use the classic channel to send message encrypted by that key.
2. When Eve tries to observe the information on the quantum channel, according to quantum indeterminacy, measuring an unknown quantum state changes that state in some way. When this happens, Alice and Bob can easily detect the interaction, so that they can begin with a new key which is not disturbed.

Ex. 6 — Simple questions

1.
$$U_1 \otimes V_1 = \begin{pmatrix} u_{1,1,1}V_1 & u_{1,1,2}V_1 & \cdots & u_{1,1,n}V_1 \\ u_{1,2,1}V_1 & u_{1,2,2}V_1 & \cdots & u_{1,2,n}V_1 \\ \vdots & \vdots & \ddots & \vdots \\ u_{1,n,1}V_1 & u_{1,n,2}V_1 & \cdots & u_{1,n,n}V_1 \end{pmatrix}$$
$$= \begin{pmatrix} u_{1,1,1}v_{1,1,1} & \cdots & u_{1,1,1}v_{1,1,n} & \cdots & \cdots & u_{1,1,n}v_{1,1,1} & \cdots & u_{1,1,n}v_{1,1,n} \\ \vdots & \ddots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ u_{1,1,1}v_{1,n,1} & \cdots & u_{1,1,1}v_{1,n,n} & \cdots & \cdots & u_{1,1,n}v_{1,n,1} & \cdots & u_{1,1,n}v_{1,n,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ u_{1,1,n}v_{1,1,1} & \cdots & u_{1,1,n}v_{1,1,n} & \cdots & \cdots & u_{1,n,n}v_{1,1,1} & \cdots & u_{1,n,n}v_{1,1,n} \\ \vdots & \ddots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ u_{1,1,n}v_{1,n,1} & \cdots & u_{1,1,n}v_{1,n,n} & \cdots & \cdots & u_{1,n,n}v_{1,n,1} & \cdots & u_{1,n,n}v_{1,n,n} \end{pmatrix}$$

Let $i_1 = \lceil i/n \rceil$, $j_1 = \lceil j/n \rceil$, $i_2 = (i - 1 \bmod n) + 1$, $j_2 = (j - 1 \bmod n) + 1$

$$W_1 = U_1 \otimes V_1, W_2 = U_2 \otimes V_2, X = W_1 \cdot W_2$$

$$w_{1,i,j} = u_{1,i_1,j_1} v_{1,i_2,j_2} \quad (i, j \in [1, n^2])$$

$$w_{2,i,j} = u_{2,i_1,j_1} v_{2,i_2,j_2} \quad (i, j \in [1, n^2])$$

Similarly, let $k_1 = \lceil k/n \rceil$, $k_2 = (k - 1 \bmod n) + 1$

$$x_{i,j} = \sum_{k=1}^{n^2} w_{1,k,j} w_{2,i,k} = \sum_{k=1}^{n^2} u_{1,k_1,j_1} u_{2,i_1,k_1} v_{1,k_2,j_2} v_{1,i_2,k_2} \quad (i, j \in [1, n^2])$$

$$W_3 = U_1 \cdot U_2, W_4 = V_1 \cdot V_2, Y = W_3 \otimes W_4$$

$$w_{3,i,j} \sum_{k=1}^{n} u_{1,k,j} u_{2,i,k} \quad (i, j \in [1, n])$$

$$w_{4,i,j} \sum_{k=1}^{n} v_{1,k,j} v_{2,i,k} \quad (i, j \in [1, n])$$

$$y_{i,j} = \sum_{k=1}^{n} u_{1,k,j_1} u_{2,i_1,k} \sum_{k=1}^{n} v_{1,k,j_2} v_{2,i_2,k} = \sum_{k=1}^{n^2} u_{1,k_1,j_1} u_{2,i_1,k_1} v_{1,k_2,j_2} v_{1,i_2,k_2} \quad (i, j \in [1, n^2])$$

So

$$(U_1 \otimes V_1) \cdot (U_2 \otimes V_2) = (U_1 U_2) \otimes (V_1 V_2)$$

2. If we have two vector spaces V, W, while V have a basis $e_1, e_2, \cdots, e_m$ and W have a basis $f_1, f_2, \cdots, f_n$, then $U = V \otimes W$ is a vector space with basis $e_i \otimes f_j$. For any vector $v = \sum_{i=0}^{m} v_i e_i \in V$ and $w = \sum_{j=0}^{m} w_j f_j \in V$, we can get $u = v \otimes w = \sum_{i=0}^{m} \sum_{j=0}^{n} v_i w_j (e_i \otimes f_j)$ so that $u \in U$. So the operator $\otimes$ is bilinear.