Problem 1. Group structure on an elliptic curve

Given an elliptic curve of equation $y^2 = x^3 + bx + c$, we have two point $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$. Based on the defined addition, we have $P_3 = (x_3, y_3) = P_1 + P_2$. We will first prove the proposition that states

$$x_3 = m^2 - x_1 - x_2 \quad y_3 = m(x_1 - x_3) - y_1$$

by checking whether (x_3, y_3) fits the elliptic curve function $y_3^2 = x_3^3 + bx_3 + c$.

$$\begin{aligned} y_3^2 &= m^2(2x_1 + x_2 - m^2)^2 - 2m(2x_1 + x_2 - m^2)y_1 + y_1^2 \\ &= m^6 - 4m^4x_1 - 2m^4x_2 + 2m^3y_1 + 4m^2x_1x_2 + m^2x_2^2 - 4mx_1y_1 - 2mx_2y_1 + y_1^2 \end{aligned}$$

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

We need to make sure the difference between the above two terms is 0.

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

Case 1. $P_1 \neq P_2$, $m = \dfrac{y_2 - y_1}{x_2 - x_1}$

$$\begin{aligned} x_3^3 + bx_3 + c - y_3^2 = {} & -\frac{1}{(x_1 - x_2)^3}(x_1^6 - 3x_1^4x_2^2 + bx_1^4 - 2bx_1^3x_2 - 2x_1^3y_1^2 + 2x_1^3y_1y_2 + x_1^3y_2^2 - cx_1^3 \\ & + 3x_1^2x_2^4 - 3x_1^2x_2y_2^2 + 3cx_1^2x_2 + 2bx_1x_2^3 + 3x_1x_2^2y_1^2 - 3cx_1x_2^2 - bx_1y_1^2 + 2bx_1y_1y_2 \\ & - bx_1y_2^2 - x_2^6 - bx_2^4 - x_2^3y_1^2 - 2x_2^3y_1y_2 + 2x_2^3y_2^2 + cx_2^3 + bx_2y_1^2 - 2bx_2y_1y_2 + bx_2y_2^2 \\ & + y_1^4 - 2y_1^3y_2 + 2y_1y_2^3 - y_2^4) \\ = {} & -\frac{1}{(x_1 - x_2)^3}[x_1^3(x_2^3 + bx_2 + c) - x_2^3(x_1^3 + bx_1 + c) - 2x_1^3(x_1^3 + bx_1 + c) \\ & + 2x_2^3(x_2^3 + bx_2 + c) + 3x_1^2x_2^4 - 3x_1^4x_2^2 + (x_1^3 + bx_1 + c)^2 - (x_2^3 + bx_2 + c)^2 \\ & + bx_1^4 - bx_2^4 - cx_1^3 + cx_2^3 + x_1^6 - x_2^6 - bx_1(x_1^3 + bx_1 + c) + bx_2(x_1^3 + bx_1 + c) \\ & - bx_1(x_2^3 + bx_2 + c) + bx_2(x_2^3 + bx_2 + c) + 2bx_1x_2^3 - 2bx_1^3x_2 - 3cx_1x_2^2 + 3cx_1^2x_2 \\ & + 2y_1y_2(x_2^3 + bx_2 + c) + 2x_1^3y_1y_2 - 2x_2^3y_1y_2 + 3x_1x_2^2(x_1^3 + bx_1 + c) \\ & - 3x_1^2x_2(x_2^3 + bx_2 + c) - y_1y_2(2x_1^3 + 2bx_1 + 2c) + 2bx_1y_1y_2 - 2bx_2y_1y_2] \\ = {} & 0 \end{aligned}$$

Case 2. $P_1 = P_2$, $m = \dfrac{3x_1^2 + b}{2y_1}$

$$\begin{aligned} x_3^3 + bx_3 + c - y_3^2 &= x_1^3 + bx_1 - y_1^2 + c \\ &= x_1^3 + bx_1 - (x_1^3 + bx + c) + c \\ &= 0 \end{aligned}$$

- **Commutative Law**
  Suppose $P_1 + P_2 = (x, y)$, $P_2 + P_1 = (x', y')$, we want to show $x = x', y = y'$
  1. When $P_1 = P_2$, it is obviously true.
  2. When $P_1 \neq P_2$, $m = m' = \dfrac{y_2 - y_1}{x_2 - x_1}$.

$$x = x' = m^2 - x_1 - x_2$$

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

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

- **Associative Law**
  Suppose we have points P_1, P_2, P_3 on curve E. According to the definition, we have

$$(P_1 + P_2 + P_3) = \mathcal{O}$$

  Therefore, we have

$$P_1 + P_2 = -P_3$$
$$P_2 + P_3 = -P_1$$

  Thus

$$(P_1 + P_2) + P_3 = (-P_3) + P_3 = \mathcal{O}$$
$$P_1 + (P_2 + P_3) = P_1 + (-P_1) = \mathcal{O}$$

  Hence we prove that $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

Problem 2. Number of points on an elliptic curve

1. Given $x_1 = 8, y_1 = 9, b = 3$

$$m_2 \equiv \frac{3x_1^2 + 3}{2y_1} \equiv 9 \mod 11$$

$$x_2 \equiv m_2^2 - 2x_1 \equiv 10 \mod 11$$
$$y_2 \equiv m_2(x_1 - x_2) - y_1 \equiv 6 \mod 11$$
$$[2]P = (10, 6)$$

$$m_4 \equiv \frac{3x_2^2 + 3}{2y_2} \equiv 6 \mod 11$$
$$x_4 \equiv m_4^2 - 2x_2 \equiv 5 \mod 11$$
$$y_4 \equiv m_4(x_4 - x_4) - y_2 \equiv 2 \mod 11$$
$$m_5 \equiv \frac{y_4 - y_1}{x_4 - x_1} \equiv 6 \mod 11$$

$$x_5 \equiv m_5^2 - x_4 - x_1 \equiv 1 \mod 11$$
$$y_5 \equiv m_5(x_4 - x_5) - y_4 \equiv 0 \mod 11$$
$$[5]P = (1, 0)$$

$$m_{10} \equiv \frac{3x_5^2 + 3}{2y_5} \text{ dosen't exist.}$$
$$[10]P = \mathcal{O} = (0, 0)$$

2. About 11. (10 according to (3).)

3. Given elliptic curve $y^2 = x^3 + 3x + 7 \mod 11$. The points on E are pair of elements (x, y) that satisfy the equation.

$x \mod 11$	$y^2 \mod 11$	$y \mod 11$	Points on E
0	7		
1	0	0	(1,0)
2	10		
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)

Including the infinite point $\mathcal{O}$, there are 10 points in total.

Problem 3. ECDSA

In the Elliptic Curve Digital Signature Algorithm (ECDS), we need a cryptographic hash function h, an elliptic curve E, a Point $G \in E$, the order n of G such that $[n]G = \mathcal{O}$.

Initial setup

1. Creates a key pair, consisting of a private key integer d_A
2. Randomly selected in the interval $[1, n-1]$
3. a public key curve point $Q_A = [d_A]G$

Sign procedure

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 $r \equiv x_1 \mod n$. If $r = 0$, retry from step 3.
6. Calculate $s \equiv k^{-1}(z + rd_A) \mod n$. If $s = 0$, retry from step 3.
7. The signature is the pair (r, s).

Authentication procedure

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

Validation

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

Benefits

- ECDSA is about twice the size of the security level, which saves a lot of key bits compared to other algorithms like DSA.
- ECDSA has faster algorithms for generating signatures because of the computation involves smaller numbers.
- ECDSA has a smaller size of data of certificate to establish a TLS connection which leads to faster connection.

Problem 4. BB84

BB84 is the first quantum cryptography protocol, which is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal and an authenticated public classical channel.

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:

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

where a_i and b_i are i-th bit of a and b. Together $a_i b_i$ provides the index of the following four qubits.

$$|\psi_{00}\rangle = |0\rangle$$
$$|\psi_{10}\rangle = |1\rangle$$
$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

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.

Problem 5. Quantum key distribution

1. Alice and Bob could use the quantum channel to distribute a quantum key according to some protocols like BB84, and they use the classic channel to send message encrypted by that key.

2. During the key distribution in quantum channel, Eve's measurements towards the random elements will lead to errors found when comparing keys. If Eve chooses the same base as Alice, it will not affect Bob's measurement results, and Alice and Bob will not find Eve when they compare part of the key. But there is still a 50% probability that Eve will choose a different basis from Alice to make the measurement, which will change the state of that element. At this time, Bob will has his measurement again with a 50% probability to get a different result from Alice. Therefore they can easily find out the existence of the Eve when the comparing quantum states are different, and they could immediately change another undistributed key to use on the classical channel.

Problem 6. Simple questions

1. Given $n \times n$ matrices U_1, U_2, V_1, V_2, denote

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

And U_2, V_1, V_2 shares the same notation as above.

According to the definition of **kronecker product,** we have

$$\begin{aligned}(U_1 \otimes V_1)(U_2 \otimes V_2) &= \begin{pmatrix} u_{1,1,1}V_1 & \cdots & u_{1,1,n}V_1 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_1 & \cdots & u_{1,n,n}V_1 \end{pmatrix} \cdot \begin{pmatrix} u_{2,1,1}V_2 & \cdots & u_{2,1,n}V_2 \\ \vdots & \ddots & \vdots \\ u_{2,n,1}V_2 & \cdots & u_{2,n,n}V_2 \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^n u_{1,1,i}u_{2,i,1}V_1V_2 & \cdots & \sum_{i=1}^n u_{1,1,i}u_{2,i,n}V_1V_2 \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n u_{1,n,i}u_{2,i,1}V_1V_2 & \cdots & \sum_{i=1}^n u_{1,n,i}u_{2,i,n}V_1V_2 \end{pmatrix} \\ &= U_1U_2 \otimes V_1V_2\end{aligned}$$

2. To show the operator $\otimes$ is bilinear, which means we need to show

$$\begin{aligned}U_1 \otimes (V_1 + V_2) &= U_1 \otimes V_1 + U_1 \otimes V_2 \\ (U_1 + U_2) \otimes V_1 &= U_1 \otimes V_1 + U_2 \otimes V_1\end{aligned}$$

I will only show the detailed proof for the first equation because they are very similar.

$$\begin{aligned}U_1 \otimes (V_1 + V_2) &= \begin{pmatrix} u_{1,1,1}(V_1+V_2) & \cdots & u_{1,1,n}(V_1+V_2) \\ \vdots & \ddots & \vdots \\ u_{1,n,1}(V_1+V_2) & \cdots & u_{1,n,n}(V_1+V_2) \end{pmatrix} \\ &= \begin{pmatrix} u_{1,1,1}V_1 & \cdots & u_{1,1,n}V_1 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_1 & \cdots & u_{1,n,n}V_1 \end{pmatrix} + \begin{pmatrix} u_{1,1,1}V_2 & \cdots & u_{1,1,n}V_2 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_2 & \cdots & u_{1,n,n}V_2 \end{pmatrix} \\ &= U_1 \otimes V_1 + U_1 \otimes V_2\end{aligned}$$

Hence, $\otimes$ is bilinear.