Problem set 11

Problems 6, 7 and 8 are based on stuff we’ll discuss on Monday.

(1) Write \( X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3) \). Prove that \( 4A^3 + 27B^2 = 0 \iff \{ e_i \} \) not all distinct.

(2) Let \( E \) be defined by \( y^2 = x^3 + x + 1 \). Compute the number of points in the group \( E(\mathbb{F}_p) \) for \( p = 3, 5, 7, \) and \( 11 \). In each case verify Hasse’s bound \( |a_p| < 2\sqrt{p} \), where \( a_p = |E(\mathbb{F}_p)| - p - 1 \).

(3) With \( E \) as in (2), \( P = (4, 2) \) and \( Q = (0, 1) \) belong to \( E(\mathbb{F}_5) \). Find \( n \) such that \( nP = Q \).

(4) Let \( E \) be an elliptic curve over \( \mathbb{F}_p \), and \( P, Q \in E(\mathbb{F}_p) \). Assume \( Q \in \langle P \rangle \) and let \( n_0 > 0 \) be the smallest solution to \( nP = Q \), and \( s > 0 \) be the smallest solution to \( sP = o \). Prove that every solution to \( Q = nP \) takes the form \( n_0 + is \) for some \( i \in \mathbb{Z} \). [Hint: Write \( n \) as \( is + r \) for some \( 0 \leq r < s \) and determine the value of \( r \).]

(5) Adapt the Pollard \( \rho \) algorithm for the DLP (explained in §V.A) to the ECDLP. (Write out the algorithm and briefly justify why it works.)

(6) Let \( E \) be the elliptic curve \( y^2 = x^3 - x \). Find the group structure of \( E(\mathbb{F}_5) \) and \( E(\mathbb{F}_{11}) \).

(7) Alice and Bob agree to use the elliptic Diffie-Hellman key exchange with the prime \( p = 2671 \), elliptic curve \( E: Y^2 = X^3 + 171X + 853 \), and point \( P = (1980, 431) \in E(\mathbb{F}_p) \).

(a) Alice sends to Bob the point \( Q_A = (2110, 543) \). Bob decides to use the secret multiplier \( n_B = 1943 \). What point should Bob send to Alice?

(b) What is their secret shared value?

(c) How difficult is it for Eve to figure out Alice’s secret multiplier \( n_A \)? (Try to find it using PARI.)

(d) Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the \( x \)-coordinate \( x_A = 2 \) of her point \( Q_A \). Bob decides to use the secret multiplier \( n_B = 875 \). What single number modulo \( p \) should Bob send to Alice, and what is their secret shared value?

(8) [HPS] p. 341 #5.16