IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises VIII.

1. Factor $n = 923$ using the elliptic curve $E : y^2 = x^3 + 2x + 9 \pmod{n}$ and the point $P = (0, 3)$. Show the computation steps.

2. Let P be a point on an elliptic curve $E : y^2 = x^3 + ax + b \pmod{n}$ where $n > 1$. Prove that there exist i, $j \in \mathbb{N}$, $i \neq j$, such that $iP = jP$.

3. (a) Factorize $2^{29} - 1$ using the second Pollard ρ-algorithm with $f(x) = x^2 + 1$.
   (b) Use the Pollard's $p - 1$ method to factor $n = 8549$ with $a = 50$ and $b = 17$.

4. For a modulus n, an exponent e is called a universal exponent if $x^e \equiv 1 \pmod{n}$ for all x with $\gcd(x, n) = 1$.

   Universal Exponent Factorization Method
   Let e be a universal exponent for n and set $e = 2^b m$ where $b \geq 0$ and m is odd. Execute the following steps.

   (i) Choose a random a such that $1 < a < n - 1$. If $\gcd(a, n) > 1$, then we have a factor of n, and we terminate the algorithm. Otherwise go to step (ii).

   (ii) Let $x_0 \equiv a^m \pmod{n}$. If $x_0 \equiv 1 \pmod{n}$, then go to step (i).
   Otherwise, compute $x_j \equiv x_{j-1}^2 \pmod{n}$ for all $j = 1, \ldots, b$.
   - If $x_j \equiv -1 \pmod{n}$, then go to step (i).
   - If $x_j \equiv 1 \pmod{n}$, but $x_{j-1} \not\equiv 1 \pmod{n}$, then $\gcd(x_{j-1} - 1, n)$ is a nontrivial factor of n so we can terminate the algorithm.

   (a) Use the algorithm above to factor $n = 76859539$ with the universal exponent $e = 12807000$.
   (b) Find a universal exponent for $n = 2^{a+2}$. Justify your answer.

5. Let $n > 0$ be an integer. Show that n is a prime if and only if for any $k \in \{1, 2, \ldots, n - 1\}$ $\binom{n}{k}$ is divisible by n.

6. Consider the elliptic curve $E : y^2 = x^3 + 568x + 1350 \pmod{1723}$ and the point $X = (524, 1413)$. Compute the point $144X$.

7. Consider the eliptic curve $E : y^2 = x^3 + x + 3 \pmod{11}$.
   (a) Find a group isomorphic to the eliptic curve E.
   (b) Suppose that Alice and Bob use E in the elliptic version of the ElGamal scheme.
   Alice chooses $Q = (9, 9)$ and a secret number k. Then she computes $P = k(9, 9) = (6, 7)$ and makes P public. Bob chooses a message M, a random number r and sends $Y_1 = rQ = (5, 10)$ and $Y_2 = M + rP = (1, 4)$ to Alice. Your task is to find M.