MAT2250 Exercise list
Spring 2024 - Instructor: Kris Shaw

11. Week of May 13th - Public key exchange cryptography

Warm ups.

(1) Show that 2 is a primitive root mod 5.
(2) Compute 2^{103} modulo 5 using Fermat's little theorem.
(3) Compute 3^7 modulo 11 using the sequential squaring method,
(4) Verify that $(x, y) = (3, 5) \in \mathbb{Z}_{11}^2$ is a point on the elliptic curve over $\mathbb{Z}_{11}$ defined by

$$y^2 \equiv x^3 + x + 6 \mod 11.$$

Problem 11.1. Solve the discrete logarithm problem

$$3 \equiv 7^x \mod 11$$

for $x \in \{0, 1, \ldots, 10\}$.

Problem 11.2. Let a be a primitive root mod p. Show that b is also a primitive root mod p if and only if $b \equiv a^k \mod p$ for some $k \in \{1, \ldots, p-1\}$ where $gcd(k, p-1) = 1$.

Problem 11.3. In a Diffie-Hellman key exchange Alice and Bob share the public key $p = 11$ and $a = 2$. Alice sends $A = 10$ to Bob and Bob sends $B = 6$ to Alice. What is their shared secret key K?

The *ElGamal protocol* encrypts a text T to a cipher

$$C \equiv KT \mod p.$$

Using the ElGamal protocol with their public keys and shared secret, Bob sends the number $C = 6$ to Alice. What was the original number T?

Problem 11.4. (From Final Exam Spring 2020 at home exam) Alice publishes the public key $n = 91$ and $k = 5$ hoping to receive secret messages via the RSA protocol. Use the fact that n is not very large combined with the Euclidean algorithm in reverse to crack Alice's secret key.

Decode the following message that was sent from Bob to Alice using a (modular) calculator:

$$63 \quad 71 \quad 23 \quad 0 \quad 80 \quad 71 \quad 13 \quad 13 \quad 31 \quad 44.$$

Each block represents the encryption of a single letter via space = 0, A = 1, B = 2, C = 3, D = 4.... and then encrypted using RSA with Alice's public key. Explain the computation used to decode.