Math 116 Spring 2022
Homework 3

Due Friday, April 22nd

Problem 1. (Elgamal PKC 2.8, with Sage) Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the Elgamal public key cryptosystem.

(a) Alice chooses $a = 947$ as her private key. What is the value of her public key A?

(b) Bob chooses $b = 716$ as his private key, so his public key is

$$B = 2^{716} \equiv 469 \pmod{1373}$$

Alice encrypts the message $m = 583$ using the random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

(c) Alice decides to choose a new private key $a = 299$ with assocaited public key $A = 2^{299} \equiv 34 \pmod{1373}$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.

Problem 2. (Optional, do NOT submit) Read Section 2.5 on groups and do several exercises from Section 2.5 as practice.

Problem 3. (Order, 2.16) Verify the following assertions from Example 2.16:

(a) $x^2 + \sqrt{x} = \mathcal{O}(x^2)$.

(b) $5 + 6x^2 - 37x^5 = \mathcal{O}(x^5)$.

(c) $k^{300} = \mathcal{O}(2^k)$.

(d) $\ln k = \mathcal{O}(k^{0.001})$.

(e) $k^2 2^k = \mathcal{O}(e^{2k})$.

(f) $N^{10} 2^N = \mathcal{O}(e^n)$.

Problem 4. (Shank's Babystep–Giantstep algorithm, 2.17. (a) by hand, (b) with Sage) Use Shanks's babystep–giantstep method to solve the following discrete logarithm problems

(a) $11^x = 21$ inn $\mathbb{F}_{71}$.

(b) $156^x = 116$ in $\mathbb{F}_{593}$.

Problem 5. (Chinese Remainder Theorem, 2.18(a)(b)(d), by hand) Solve each of the following simultaneous systems of congruences or explain why no solution exists.

(a) $x \equiv 3 \pmod 7$ and $x \equiv 4 \pmod 9$.

(b) $x \equiv 137 \pmod{423}$ and $x \equiv 87 \pmod{191}$.

(c) $x \equiv 5 \pmod 9$, $x \equiv 6 \pmod{10}$, and $x \equiv 7 \pmod{11}$.