CS 380/525: Intro to Cryptography
Fall 2022
Assignment 3, due 10/13, before class
Total points: 100

Note: You can either typset your assignments or write them electronically, handwritten solutions will not be accepted. Please refer to the class notes for worked out examples.

1. (20 points) Multiplicative inverses:

   (a) (5 points) Find set of multiplicative inverses in $GF(29)$.

   (b) (15 points) Use Extended Euclidean algorithm to find multiplicative inverses of ($20 \mod 79$), ($3 \mod 62$), and ($22 \mod 91$), and ($5 \mod 23$).

2. (10 points) How many integers modulo 11^3 have inverses? You may find the following theorem useful:

   Theorem 0.1 *(Modular division theorem) For any integer a, and modulus $N > 1$, a has a multiplicative inverse modulo N, if and only if a is relatively prime to N.*

3. (20 points) Find the set of polynomials in $GF(2^5)$ and $GF(5^2)$.

4. (15 points) We had worked out a few examples of Euclid's algorithm and the extended Euclidean algorithm in class. Use that as a reference to solve the following:

   (a) Find $d = gcd(423, 128)$. Are they co-prime? Find integers x, y, such that $d = x \cdot 423 + y \cdot 128$.

   (b) Find $d = gcd(588, 210)$. Are they co-prime? Find integers x, y, such that $d = x \cdot 588 + y \cdot 210$.

   (c) Find $d = gcd(899, 493)$. Are they co-prime? Find integers x, y, such that $d = x \cdot 899 + y \cdot 493$.

5. (15 points) Compute the following using Chinese remainder theorem, and/or the group-order rule. You may also use the modular arithemetic rules in "numTheoryI.pdf".

   (a) $3^{1000} \mod 100$

   (b) $101^{4,800,000,002} \mod 35$

   (c) $46^{51} \mod 55$

6. (10 points) Is $(4^{1536} - 9^{4824})$ divisible by 25?

7. (10 points) Is the difference between $5^{30,000}$ and $6^{123,456}$ a multiple of 23?

How to submit: Please upload your **pdf** file on Canvas. You can use my posted template for typesetting your assignment, but aren't required to do so.