Math 1580 – Problem Set 2. Due Friday Sep. 23, 4pm

The first two problems on this problem set give a proof of the primitive root theorem:

Primitive Root Theorem. *Let p be a prime number. Then there exists an element $g \in \mathbb{Z}/p\mathbb{Z}$ such that*

$$(\mathbb{Z}/p\mathbb{Z})^* = \left\{1, g, g^2, \dots, g^{p-2}\right\}.$$

For the first problem, you will need the following fact, a proof of which is sketched at the end of this problem set.

Fact 1. *For p prime, there are at most k solutions to the equation $x^k \equiv 1 \pmod p$.*

Problem 1. Fix a prime p and let $N(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^*$ with order d. Show that if $N(d) > 0$, then $N(d) = \phi(d)$, where ϕ is Euler's phi function.

(Recall that $\phi(d)$ is the number of $a \in 1, 2, \dots, d-1$ such that $\gcd(a, d) = 1$, and that the order of a is the smallest k such that $a^k \equiv 1 \pmod p$.) Here are some steps:

(a) If there exists an a with order d, then a solves the equation $x^d \equiv 1$ in $\mathbb{Z}/p\mathbb{Z}$. Show that any other solution to this equation must be one of $1, a, a^2, \dots, a^{d-1}$. (Use Fact 1.)

(b) Let $b = a^k$, for some $1 \leq k \leq d-1$. Show that b has order $d/\gcd(k, d)$. (Hint: think about the prime factorizations of d and k.)

(c) Conclude from (a) and (b) that, provided some element a with order d exists, then all the elements of order d are of the form a^k where $\gcd(k, d) = 1$, and that there are precisely $\phi(d)$ of these.

Problem 2. Prove the Primitive Root Theorem using the following steps.

(a) Show that the Primitive Root Theorem is equivalent to the statement that $N(p-1) > 0$.

(b) From the result you proved in Problem 1, show that $N(d) \leq \phi(d)$ for all $d|(p-1)$, and show that, since the number of elements in $(\mathbb{Z}/p\mathbb{Z})^*$ is $p-1$,

$$p - 1 = \sum_{d\,|(p-1)} N(d) \leq \sum_{d\,|(p-1)} \phi(d).$$

(c) Show that for any integer n,

$$\sum_{d\,|n} \phi(d) = n. \tag{1}$$

Hint: consider the list of unreduced fractions

$$\frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n}, \frac{n}{n} \tag{2}$$

and their reduced forms $m/n = a/d$ where $\gcd(a, d) = 1$. Argue that since $1 \leq m \leq n$, we have $1 \leq a \leq d$, and so the number of fractions in the list (2) whose reduced form has denominator d is $\phi(d)$. Use this to show (1).

(d) Combine the above two steps to conclude that

$$p - 1 = \sum_{d|(p-1)} N(d) \leq \sum_{d\,|(p-1)} \phi(d) = p - 1$$

so equality holds, and therefore $N(d) = \phi(d)$ for all d dividing $p-1$. Show that $\phi(p-1) > 0$ and conclude the theorem.

Problem 3. The *Hill cipher* is a symmetric cipher wherein the messages m and ciphertexts c are vectors of dimension n with coefficients in $\mathbb{Z}/p\mathbb{Z}$, with p prime. Encryption and decryption are given by

$$e_k(m) = k_1 m + k_2 \pmod{p}$$
$$d_k(c) = k_1^{-1}(c - k_2) \pmod{p},$$

where k_2 is a column vector of length n, and k_1 is an invertible $n \times n$ matrix, with inverse k_1^{-1}. The key consists of k_1 and k_2.

(a) Use the Hill cipher with $p = 7$ and key $k_1 = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$, $k_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$.

  (i) Encrypt the message $m = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.

  (ii) What is the matrix k_1^{-1} used for decryption?

  (iii) Decrypt the message $c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$.

(b) Explain why the Hill cipher is vulnerable to a chosen plaintext attack.

(c) The following plaintext/ciphertext pairs were generated using a Hill cipher with the prime $p = 11$. Find the key k_1, k_2.

$$m_1 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \; c_1 = \begin{pmatrix} 1 \\ 8 \end{pmatrix}, \quad m_2 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, \; c_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}, \quad m_3 = \begin{pmatrix} 7 \\ 1 \end{pmatrix}, \; c_2 = \begin{pmatrix} 8 \\ 7 \end{pmatrix}$$

(d) Explain how any simple substitution cipher that involves a permutation of the alphabet can be thought of as a special case of the Hill cipher.

Problem 4. Let g be a primitive root for $\mathbb{F}_p$. Define $\log_g(h)$ to be the number x such that $g^x \equiv h \pmod{p}$.

(a) Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h \pmod{p}$. Prove that $a \equiv b \pmod{p-1}$. Explain why this implies that the map

$$\log_g : \mathbb{F}_p^* \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}$$

is well-defined.

(b) Prove that $\log_g(h_1 h_2) = \log_g(h_1) + \log_g(h_2)$ for all $h_1, h_2 \in \mathbb{F}_p^*$.

(c) Prove that $\log_g(h^n) = n \log_g(h)$ for all $h \in \mathbb{F}_p^*$ and $n \in \mathbb{Z}$.

(d) Compute $\log_2(13)$ for the prime 23.

Problem 5. 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

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

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

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

Proof sketch of Fact 1. Solutions to $x^k \equiv 1 \pmod p$ are the same as roots of the polynomial $x^k - 1$ in $\mathbb{Z}/p\mathbb{Z}$. Specifically, we say a polynomial $p(x)$ has a root α in $\mathbb{Z}/p\mathbb{Z}$ (or any other ring) if $p(\alpha)$ evaluates to 0 in $\mathbb{Z}/p\mathbb{Z}$.

We know that when p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a *field*, meaning all nonzero elements have an inverse. You are no doubt familiar with polynomials over the fields $\mathbb{R}$ and $\mathbb{C}$, and you learned that over these fields, a polynomial of degree k has at most k roots (exactly k if the field is $\mathbb{C}$, but no matter). In fact, this holds over any field:

A polynomial of degree k over a field $\mathbb{F}$ has at most k roots in $\mathbb{F}$.

This is because, if α is a root of $p(x)$, then we can do *polynomial long division* to write

$$p(x) = (x - \alpha)q(x)$$

where the degree of q is less than the degree of p, and vice versa. Continuing this process, it is clear that p has at most $\deg(p)$ roots. $\square$

This does not work over $\mathbb{Z}/m\mathbb{Z}$ when m is not prime, because doing polynomial long division over $\mathbb{Z}/m\mathbb{Z}$ requires the division of constants in $\mathbb{Z}/m\mathbb{Z}$, and if m is not prime, then there are numbers which do not have inverses.

Observe for instance that there are 4 solutions to $x^2 \equiv 1 \pmod 8$.