Math 5405/Cryptography/Spring 2013
Some Number Theoretic Preliminaries

Prime Numbers are an essential tool in modern cryptography.

Definition. An integer $p > 1$ is *prime* if its only divisors are 1 and p. An integer $n > 1$ that is not prime is called *composite*.

Facts. (i) Each integer $n > 1$ factors uniquely as a product of primes (up to reordering the factors).

(ii) There are infinitely many primes. In any arithmetic progression:

$$a, a+d, a+2d, a+3d, \ldots \text{ with } \gcd(a,d) = 1$$

there are infinitely many primes.

Prime Issues. Given a (very large) integer n, how do we:

(a) Determine quickly whether n is prime (probably vs for sure)?

(b) If it is composite, quickly factor n? (The BIG question!)

(c) Given a prime p, compute "discrete logarithms" (mod p).

Groups and Rings are useful "algebraic" concepts.

Definition. (a) A *group* is a set G with a "multiplication":

$$\cdot : G \times G \to G \text{ with the following properties}$$

(i) Multiplication is associative.

(ii) There is a unique identity element $e \in G$ with the property that:

$$e \cdot g = g = g \cdot e \text{ for all } g \in G$$

(iii) Each $g \in G$ has a unique inverse element $g^{-1} \in G$ such that:

$$g \cdot g^{-1} = e = g^{-1} \cdot g$$

If multiplication is also communtative, then G is an *abelian* group.

(b) A *ring* is a set R with an addition and multiplication:

$$+ : R \times R \to R \;\text{ and }\; \cdot : R \times R \to R \text{ such that}$$

(i) $(R, +)$ is an abelian group. The additive identity is called 0.

(ii) $(R, \cdot)$ satisfies the first two properties of a group. It cannot satisfy the third since 0 is not invertible. We call the multiplicative identity 1. If $R^\times$ is the set of invertible elements, however, then $(R^\times, \cdot)$ is a group.

(iii) Addition and multiplication satisfy the distributive law.

If multiplication is commutative, then R is called a *commutative* ring.

A *field* is a commutative ring in which only 0 is not invertible.

Examples. (a) The integers mod n ($\mathbb{Z}/n\mathbb{Z}$) are a commutative ring.

(b) $\mathbb{Z}/p\mathbb{Z}$ is a **field** exactly when p is a prime. It is also denoted $\mathbb{F}_p$.

(c) The $n \times n$ matrices are a (non-commutative) ring, denoted:

$$M(n, R)$$

where the entries of the matrix belong to the (commutative) ring R. For example:

(i) $\mathrm{M}(n, \mathbb{R})$ are matrices with real coefficients.

(ii) $\mathrm{M}(n, \mathbb{Q})$ are matrices with rational coefficients.

(iii) $\mathrm{M}(n, \mathbb{Z})$ are matrices with integer coefficients.

(iii) $\mathrm{M}(n, \mathbb{F}_p)$ are matrices with integer mod p coefficients.

Cramer's Rule. An $n \times n$ matrix $A \in M(n, R)$ has a multiplicative inverse if and only if $\det(A)$ has a multiplicative inverse in the ring R.

Notation. The (non-abelian) group $(M(n, R)^\times, \cdot)$ of **invertible** $n \times n$ matrices is denoted by:

$$\mathrm{GL}(n, R)$$

The subgroup of matrices of determinant 1 is denoted by:

$$\mathrm{SL}(n, R)$$

Definition. A finite abelian group G is *cyclic* if there is an element $g \in G$ such that:

$$G = \{g, g^2, g^3, \ldots, g^d = e\}$$

Any such g is called a *primitive* element. Once $g \in G$ is identified as a primitive element, then the other primitive elements are exactly the powers g^e with the property that $\gcd(e, d) = 1$.

Fact. The abelian groups $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ are cyclic, though it not obvious which numbers mod p are the primitive elements.

Some Equations you will need to be able to solve include:

$$ax + by = c \text{ with integer coefficients } a, b, c$$

When $\gcd(a, b)|c$, this has infinitely many integer solutions.
When $\gcd(a, b) \not| \, c$, this has no integer solutions.

(Review how these solutions are found using Euclid's algorithm).

Note that solving:

$$ax + ny = 1$$

gives $x = a^{-1}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, so each a with $\gcd(a, n) = 1$ has an inverse.

You will also be asked to solve the

Chinese Remainder Problem. Given congruences equations:

$$x \equiv a_1 \pmod{n_1}, \cdots, x \equiv a_m \pmod{n_m}$$

with each $\gcd(n_i, n_j) = 1$, there is an $x \pmod{n_1 \cdots n_m}$ solving all the congruences simultaneously.

It will be important for applications to be able to quickly compute:

$$a^n \text{ (mod p)}$$

when n and p are large numbers. This can be done by writing n in binary and recognizing that a^{2^k} is computed via k **successive squares**.

Euler's Theorem:

$$a^{\phi(n)} \equiv 1 \text{ (mod n) for all invertible } a \in \mathbb{Z}/n\mathbb{Z}$$

where $\phi(n)$ is the Euler ϕ function (or *totient*) defined by:

$$\phi(n) = \text{ the number of invertible elements of } \mathbb{Z}/n\mathbb{Z}$$

There is a convenient formula for the phi function:

$$\phi(n) = \phi(p_1^{k_1} \cdots p_m^{k_m}) = \prod (p_i^{k_i} - p_i^{k_i - 1}) = n \cdot \prod (1 - \frac{1}{p_i})$$

so you "only" need to know the prime factors of n to compute $\phi(n)$.

Corollary (Fermat's Little Theorem):

$$a^{p-1} \equiv 1 \text{ (mod p) for all } a \in \mathbb{F}_p$$

Corollary: An equation of the form:

$$x^d \equiv 1 \text{ (mod p)}$$

has d distinct solutions ($\phi(d)$ of them primitive) if $d | p - 1$.

Corollary: An equation of the form:

$$x^d \equiv a \text{ (mod p)}$$

where $\gcd(d, p - 1) = 1$ has exactly **one** solution, given by $x = a^e$, where $e = d^{-1}$ as integers $\pmod{p - 1}$.

Quadratic Reciprocity is a very deep Number Theory result.

Definition. The *Legendre symbol* for primes p and $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ is:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ has (two) square roots} \pmod{p} \\ -1 \text{ if } a \text{ has no square roots} \pmod{p} \end{cases}$$

The Legendre symbol is *multiplicative*, i.e. if $a = bc$, then:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{c}{p}\right)$$

This follows from

Euler's Criterion. If p is an odd prime, then:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

This immediately gives:

$$(*) \quad \left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } & p \equiv 1 \pmod{4} \\ -1 \text{ if } & p \equiv 3 \pmod{4} \end{cases}$$

It is a little bit harder to prove:

$$(**) \quad \left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } & p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 \text{ if } & p \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$$

and the really deep result allows one to compute any Legendre symbol:

Theorem (QR). If p and q are (distinct) odd primes, then:

$$(***) \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless both $p \equiv 3 \pmod{4}$ **and** $q \equiv 3 \pmod{4}$, in which case:

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

It is useful to generalize this to *Jacobi symbols* defined by:

$$\left(\frac{a}{p_1^{k_1}\cdots p_m^{k_m}}\right) := \left(\frac{a}{p_1}\right)^{k_1}\cdots\left(\frac{a}{p_m}\right)^{k_m}$$

when $n = p_1^{k_1}\cdots p_m^{k_m}$ and $\gcd(a, n) = 1$.

These symbols are multiplicative, and satisfy the same statements $(*), (**)$ and $(***)$ with "odd p (and q)" replaced by "odd m (and n)".

Warning. When the base n is composite, the Jacobi symbol does not, in general, compute whether or not a is a square (mod n).

A final remark on **finite fields**. There are finite fields with any prime power number of elements. Any two such fields are isomorphic, hence it is allowed to denote *the* finite field with p^k elements as:

$$\mathbb{F}_{p^k}$$

But keep in mind that the rings $\mathbb{Z}/p^k\mathbb{Z}$ are **not** fields when $k > 1$.