CS655: Cryptography **Feb 15, 2007**

Lecture Outline for Review of Basic Number Theory[1]

Algebra Basics

1. Group: Given a non-empty set G, and a binary operation $\cdot$ over G. We say that $(G, \cdot)$ is a group if the following holds:

Closure:	For every $a, b \in G, \quad a \cdot b \in G$
Associativity:	For every $a, b, c \in G, \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
Identity:	There exists an element $\mathbf{1} \in G$ such that for every $a \in G, \quad a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$
Invertibility:	For every $a \in G$ there exists unique $b \in G$ such that $a \cdot b = b \cdot a = \mathbf{1}$. The element b is referred to as the *inverse* of the element a, and is denoted a^{-1}.

2. A group $(G, \cdot)$ is called *abelian* (or commutative) if it satisfies the following property:

   Commutative For every $a, b \in G, \quad a \cdot b = b \cdot a$.

3. Given a group $(G, \cdot)$, we say $(G', \cdot)$ is a subgroup of $(G, \cdot)$ if $G' \subseteq G$ and $(G', \cdot)$ is also group.

4. *Examples:* We use $\mathbb{Z}$ ($\mathbb{Q}$, $\mathbb{R}$, resp.) to denote the set of all integers (rational numbers, real numbers, resp.), and $\mathbb{Z}^+$ ($\mathbb{Q}^+$, $\mathbb{R}^+$, resp.) the set of all *positive* integers (rational numbers, real numbers, resp.)

   - $(\mathbb{Z}, +)$ is an abelian group;
   - $(\mathbb{Z}, \times)$ is not a group.
   - $(\mathbb{Q}, +)$ is an abelian group, so is $(\mathbb{R}, +)$;
   - $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group; so is $(\mathbb{R} \setminus \{0\}, \times)$
   - $(\mathbb{Q}^+, \times)$ is an abelian group; it is a subgroup of $(\mathbb{Q} - \{0\}, \times)$.

5. *Lagrange's theorem*: If $(G', \cdot)$ is a subgroup of $((G, \cdot)$, and both G' and G are finite, then $|G'|$ divides $|G|$.

6. Given group $\langle G, \cdot \rangle$ and an element $a \in G$, use $\langle a \rangle$ to denote the set $\{\mathbf{1}, a, a^2, a^3, \cdots\}$.

   - $\langle a \rangle \subseteq G$; hence $\langle a \rangle$ contains at most $|G|$ elements; hence there exists an integer r such that $a^r = \mathbf{1}$.
   - $(\langle a \rangle, \cdot)$ is also a group; it is a subgroup of G.

7. A group $(G, \cdot)$ is said to be a cyclic group if there exists an element $g \in G$ such that $\langle g \rangle = G$.

[1] Portions taken from Dan Boneh's number theory fact sheet.

Number Theory Basics

1. The *greatest common divisor* (gcd) of integers a, b (written $\gcd(a, b)$) is the greatest integer d such that $d|a$ and $d|b$.

   When $\gcd(a, b) = 1$, we say that a and b are relatively prime.

2. Given integers a and b, then $d = \gcd(a, b)$ is the least positive integer that can be represented as $ax + by$, where x and y are integer numbers.

   - E.g., $\gcd(100, 36) = 4$ and $4 = 4 * 100 + (-11) * 36 = 400 - 396$.

   The Extended Euclidian algorithm finds $d = \gcd(a, b)$ and x, y such that $d = ax + by$.

3. For $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, we write $a \equiv b \pmod{n}$ iff $n|(b - a)$.

   Note that $a \equiv b \pmod{n}$ iff $(a \bmod n) = (b \bmod n)$.

   The congruence relation modulo n is an equivalence relation, i.e., it is reflexive, symmetric, and transitive.

4. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then we have $a + c \equiv b + d \pmod{n}$, $a - c \equiv b + d \pmod{n}$, and $a \times c \equiv b \times d \pmod{n}$.

   From $ax \equiv bx \pmod{n}$, we can conclude $a \equiv b \pmod{n}$ if $\gcd(x, n) = 1$.

5. Fix $n \in \mathbb{Z}^+$. We use $\mathbb{Z}_n$ to denote $\{0, 1, \cdots, n - 1\}$, and $\mathbb{Z}_n^*$ to denote the set $\{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

   For a prime number p, we have $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$.

   Define addition $\oplus$ over $\mathbb{Z}_n$, $a \oplus b = (a + b) \mod n$. We often overload $+$ to use it for $\oplus$.

   Define multiplication $\otimes$ over $\mathbb{Z}_n$, $a \otimes b = a \times b \mod n$. We often overload $\times$ and use it $\otimes$. (Following common convention, we sometimes omit $\times$ and write just ab.)

6. An alternative view of modular arithmetic is to view each element $a \in \mathbb{Z}_n$ as the equivalence class $[a] = \{x \in \mathbb{Z} \mid a \equiv x \pmod{n}\}$. Addition is defined as: $[a] \oplus [b] = [a + b]$. Multiplication is defined as $[a] \otimes [b] = [a \times b]$.

7. Properties of modular arithmetic:

   - $\langle \mathbb{Z}_n, + \rangle$ is a group.
   - $\langle \mathbb{Z}_n^*, \times \rangle$ is a group. For every $a \in \mathbb{Z}_n^*$, we have $\gcd(a, n) = 1$; thus there exists x, y such that $ax + ny = 1$; let $b = x \bmod n$, we have $b \in \mathbb{Z}_n^*$ and $ab = 1$.

     Example: $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, and $1 \times 1 = 1$, $2 \times 4 = 1$, $3 \times 5 = 1$, $6 \times 6 = 1$.

8. The *Chinese Remainder Theorem*: Let $k \geq 2$. Suppose that $n_1, n_2, \cdots, n_k$ are integers that are pairwise relatively prime. Let $N = n_1 n_2 \cdots n_k$. Then for any integers $a_1, a_2, \cdots, a_k$, there exists a *unique* element in $\mathbb{Z}_N$ that solves the following system of congruences:

$$
\begin{aligned}
x &\equiv a_1 \pmod{n_1} \\
x &\equiv a_2 \pmod{n_2} \\
&\vdots \\
x &\equiv a_k \pmod{n_k}
\end{aligned}
$$

Proof: Let $m_i = N/n_i$. Then $\gcd(m_i, n_i) = 1$. Let $e_i = (m_i^{-1} \bmod n_i)$. The solution is

$$x = \sum_{i=1}^{k} a_i m_i e_i$$

$$a_1 m_1 e_1 + a_2 m_2 e_2 + \cdots + a_k m_k e_k = a_i m_i e_i = a_i m_i (m_i^{-1} \bmod n_i) = a_i \pmod{n_i}$$

9. Euler's totient function: Define $\phi(n) = |\mathbb{Z}_n^*|$.

   When n_1 and n_2 are relatively prime, then $\phi(n_1 n_2) = \phi(n_1)\phi(n_2)$.

   > Proof. Define the function $f : \mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$ as $f(x) = (x \bmod p, x \bmod q)$, then by the CRT, f is a one-to-one mapping from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$. Further, f is a one-to-one mapping from $\mathbb{Z}_n^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

   $\phi(p^e) = p^e - p^{e-1}$, and
   $\phi\left(n = p_1^{e_1} \cdots p_k^{e_k}\right) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}) = \prod_{i=1}^{k} p_i^{e_i} (1 - \frac{1}{p_i}) = n \prod_{i=1}^{k} \frac{1}{p_i}$

Arithmetic modulo primes

Basic facts

1. We are dealing with primes p on the order of 300 digits long (1024 bits).

2. *Fermat's Theorem*: For any $a \neq 0 \bmod p$, we have: $a^{p-1} = 1 \bmod p$.

   > Direct proof: The set $\{a, 2a \bmod p, 3a \bmod p, \cdots, (p-1)a \bmod p\}$ is a permutation of $\{1, 2, \cdots, (p-1)\}$.
   > Then $a \times 2a \times \cdots \times (p-1)a = (p-1)! \pmod{p}$.
   > Then $a^{p-1} \times (p-1)! = (p-1)! \pmod{p}$.
   > Because $\gcd((p-1)!, p) = 1$, we have $a^{p-1} = 1 \pmod{p}$.

3. $\mathbb{Z}_p^*$ is a cyclic group. I.e., there exist generators in $\mathbb{Z}_p^*$. Such elements are also called primitive roots

   Example: in $\mathbb{Z}_7^*$, $\quad \langle 3 \rangle = \{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_3^*$

4. Not every element of $\mathbb{Z}_p^*$ is a generator (primitive root).

   Example: $\quad$ in $\mathbb{Z}_7$ we have $\langle 2 \rangle = \{1, 2, 4\}$.

5. Testing whether an element a in $\mathbb{Z}_p^*$ is a generator (primitive root): calculate the prime factorization of $\phi(p-1)$; let $p_1, \cdots, p_k$ be $\phi(p-1)$'s prime factors. For each p_i, calculate $a^{\phi(p-1)/p_i} \bmod p$. We have a is a generator iff $a^{\phi(p-1)/p_i} \neq 1 \pmod{p}$ for each i.

6. Let g be a generator of $\mathbb{Z}_p^*$, then $x = g^j$ is a generator if and only if $\gcd(j, (p-1)) = 1$. Hence the number of generators is $\phi(p-1)$.

7. The *order* of $a \in \mathbb{Z}_p^*$ is the smallest positive integer a such that $g^a = 1 (\bmod p)$.

   The order of $a \in \mathbb{Z}_p^*$ is denoted $\mathrm{ord}_p(a)$.

   Example: $\mathrm{ord}_7(3) = 6$ and $\mathrm{ord}_7(2) = 3$.

8. Corollary of Lagrange's theorem: For all $a \in \mathbb{Z}_p^*$ we have $\mathrm{ord}_p(a) | (p-1)$.

9. If the factorization of $p-1$ is known then there is a simple and efficient algorithm to determine $\mathrm{ord}_p(a)$ for any $a \in \mathbb{Z}_p^*$.

10. Let $g \in Zps$ be a generator of $\mathbb{Z}_p^*$. Suppose that q is a prime factor of $(p-1)$ (i.e., $q|(p-1)$ and q is prime). Let $h = g^{(p-1)/q}$. Then the element h has order q.

    $\langle h \rangle = \{1, h, h^2, \cdots, h^{q-1}\}$ is called the subgroup generated by h; the subgroup has q elements.

    Each element in $\langle h \rangle$ (except for 1) is a generator of $\langle h \rangle$.

    - One commonly used setting is to use $p = 2q + 1$, where both p and q are primes. And use the subgroup $\langle h \rangle$, where h is an order-q element in $\mathbb{Z}_p^*$.
    - Another commonly used setting is to use p of 1024 bits such that $(p-1)$ has a prime factor q of 160 bits. Find an element h of order q, and use the subgroup $\langle h \rangle$.

Quadratic residues

1. The *square root* of $x \in \mathbb{Z}_p$ is a number $y \in \mathbb{Z}_p$ such that $y^2 = x \bmod p$.

   Example: $\sqrt{2} \bmod 7 = 3$ since $3^2 = 2 \bmod 7$.
   $\sqrt{3} \bmod 7$ does not exist.

2. An element $x \in \mathbb{Z}_p^*$ is called a *Quadratic Residue (QR)* if it has a square root in $\mathbb{Z}_p$.

3. How many square roots does $x \in \mathbb{Z}_p$ have?

   If $x^2 = y^2 \bmod p$ then $0 = x^2 - y^2 = (x-y)(x+y) \bmod p$.

   Since p is prime, we know that either $p|(x-y)$ or $p|(x+y)$. Therefore, either $x = y (\bmod p)$ or $x = -y (\bmod p)$.

   Hence, elements in $\mathbb{Z}_p$ has either zero square roots or two square roots.

   If a is a square root of x (modulo p), then $-a$ is also a square root of x (modulo p).

4. Easy fact: Let g be a generator of $\mathbb{Z}_p^*$, then $x = g^r$ is QR iff r is even.

   Exactly half the elements of $\mathbb{Z}_p^*$ are QRs.

5. Euler's criterion: $x \in \mathbb{Z}_p$ is a QR if and only if $x^{(p-1)/2} = 1$.

   Proof. Let $x = g^r$, where g is a generator. Then $x^{(p-1)/2} = g^{(p-1)r/2} = 1$ if and only if $(p-1) \Big| \frac{(p-1)r}{2}$, which is true iff r is even.

Example: $2^{(7-1)/2} = 1 \bmod 7$ but $3^{(7-1)/2} = -1 \bmod 7$.

6. For any $x \in \mathbb{Z}_p^*$, $\quad a = x^{(p-1)/2}$ is a square root of 1.

   Square roots of 1 modulo p is 1 and -1.

   Hence, for $x \in \mathbb{Z}_p^*$ we know that $x^{(p-1)/2}$ is 1 or -1.

7. Legendre symbol: for $x \in \mathbb{Z}_p$ define

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a QR in } \mathbb{Z}_p \\ -1 & \text{if } x \text{ is not a QR in } \mathbb{Z}_p \\ 0 & \text{if } x = 0 \bmod p \end{cases}$$

   Let $x = g^r$. The Legendre symbol reveals the parity of r.

8. By Euler's Criterion, we know that $\left(\frac{x}{p}\right) = x^{(p-1)/2} \bmod p$.

   Thus the Legendre symbol can be efficiently computed.

9. When $p = 3 \bmod 4$, computing square roots of $x \in \mathbb{Z}_p^*$ is easy.

   Simply compute $a = x^{(p+1)/4} \bmod p$.

   $a = \sqrt{x}$ because $a^2 = x^{(p+1)/2} = x \cdot x^{(p-1)/2} = x \cdot 1 = x \pmod p$.

10. When $p = 1 \bmod 4$ computing square roots in $\mathbb{Z}_p$ is possible but more complicated; a randomized algorithm is typically used.

Easy problems in $\mathbb{Z}_p$

1. Generating a random element. Adding and multiplying elements.
2. Computing $g^r \bmod p$ is easy even if r is very large. (Using the repeated squaring algorithm.)
3. Inverting an element. Solving linear systems.
4. Testing if an element in a QR and computing its square root if it is a QR.

Problems that are believed to be hard in $\mathbb{Z}_p$:

1. Let g be a generator of $\mathbb{Z}_p^*$. Given $x \in \mathbb{Z}_p^*$ find an r such that $x = g^r \bmod p$. This is known as the *discrete log problem.*

2. Let g be a generator of $\mathbb{Z}_p^*$. Given $x = g^{r_1}$ and $y = g^{r_2}$, where r_1 and r_2 are randomly chosen. Find $z = g^{r_1 r_2}$. This is known as the *Computational Diffie-Hellman problem.*

3. Let g be a generator of $\mathbb{Z}_p^*$. Given g, g^{r_1}, and g^{r_2} where r_1 and r_2 are randomly chosen. Distinguish $g^{r_1 r_2}$ from g^{r_3}. This is known as the *Computational Diffie-Hellman problem.*

   This is typically formalized as the following: One is given a tuple (g, x, y, z), which is drawn from one of the following two ensembles:

- (g, g^a, g^b, g^{ab}), where g is a random generator and a, b are randomly chosen from $\{0, 1, \cdots, p-1\}$.
- (g, g^a, g^b, g^c), where g is a random generator and a, b, c are randomly chosen from $\{0, 1, \cdots, p-1\}$.

Arithmetic modulo composites

1. We are dealing with integers N on the order of 300 digits long (1024 bits). Unless otherwise stated, N is the product of two equal size primes, e.g., each on the order of 150 digits (512 bits).

2. Euler's Theorem: Let $N \in Z^+$, $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} = 1 \pmod{N}$.

   As a consequence, if $i \equiv j \pmod{\phi(N)}$, then $a^i = a^j \pmod{N}$.

3. Let $p > q$ be two primes and $N = pq$. The percentage of elements in $\mathbb{Z}_N$ but not $\mathbb{Z}_N^*$ is

   $$\frac{pq - (p-1)(q-1)}{pq} = \frac{p+q-1}{pq} < \frac{2p}{pq} = \frac{2}{q},$$

   which is extremely small when q is large (512 bits).

4. Let p, q be integers that are relatively prime. Let $N = pq$. Given $r_1 \in \mathbb{Z}_p$ and $r_2 \in \mathbb{Z}_p$ there exists a *unique* element $s \in \mathbb{Z}_N$ such that $s = r_1 \bmod p$ and $s = r_2 \bmod p$. Furthermore, s can be computed efficiently.

5. The CRT shows that each element $s \in \mathbb{Z}_N$ can be viewed as a pair (s_1, s_2) where $s_1 = s \bmod p$ and $s_2 = s \bmod q$. The uniqueness guarantee shows that each pair $(s_1, s_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$ corresponds to one element of $\mathbb{Z}_N$.

6. Note that by the CRT, if $x = y \bmod p$ and $x = y \bmod q$, then $x = y \bmod N$.

7. An element $s \in \mathbb{Z}_N^*$ is a QR if and only if $s \bmod p$ is a QR in $\mathbb{Z}_p$ and $s \bmod q$ is a QR in $\mathbb{Z}_q$.

   - If $s = a^2 \bmod N$, then $s = a^2 \bmod p$ and $s = a^2 \bmod q$.

   Hence the number of QR in $\mathbb{Z}_N$ is $\frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{\phi(N)}{2}$.

8. Jacobi symbol: for $x \in \mathbb{Z}_N$ define $\left(\frac{x}{N}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{x}{q}\right)$.

   Half of $\mathbb{Z}_N^*$ has Jacobi symbol being 1, among which half are QR.

   There is an efficient algorithm to compute the Jacobi symbol of $x \in \mathbb{Z}_N$ without knowing the factorization of N.

9. Consider the RSA function $f(x) = x^2 \bmod N$. When e is odd we have that:

   $$\left(\frac{x^e}{N}\right) = \left(\frac{x^e}{p}\right) \cdot \left(\frac{x^e}{q}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{x}{q}\right) = \left(\frac{x}{N}\right)$$

   Hence, given an RSA ciphertext $C = x^e \bmod N$ the Jacobi symbol of C reveals the Jacobi symbol of x.

Problems that are believed to be hard if the factorization of N is unknown, but become easy if the factorization of N is known :

1. Finding prime factors of N.
2. Testing if an element in $\mathbb{Z}_N$ is QR.
3. Computing the square root of a QR in $\mathbb{Z}_N$.

   This is provably as hard as factoring N.

   When the factorization of $N = pq$ is known, one computes the square root of $x \in \mathbb{Z}_n^*$ by first computing $\sqrt{x} \bmod p$ and then $\sqrt{x} \bmod q$, and then using CRT to obtain the square roots.
4. Computing the e'th roots modulo N when $\gcd(e, \phi(N)) = 1$.