YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467b: Cryptography and Computer Security *Handout #5*
*Professor M. J. Fischer* *February 9, 2010*

# Number Theory Summary

**Integers** Let $\mathbf{Z}$ denote the integers and $\mathbf{Z}^+$ the positive integers.

**Division** For $a \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$, there exist unique integers $q, r$ such that $a = nq + r$ and $0 \le r < n$. We denote the *quotient* $q$ by $\lfloor a/n \rfloor$ and the *remainder* $r$ by $a \bmod n$. We say $n$ *divides* $a$ (written $n \,|\, a$) if $a \bmod n = 0$. If $n \,|\, a$, $n$ is called a *divisor* of $a$. If also $1 < n < |a|$, $n$ is said to be a *proper divisor* of $a$.

**Greatest common divisor** The *greatest common divisor* (gcd) of integers $a, b$ (written $\gcd(a, b)$ or simply $(a, b)$) is the greatest integer $d$ such that $d \,|\, a$ and $d \,|\, b$. If $\gcd(a, b) = 1$, then $a$ and $b$ are said to be *relatively prime*.

**Euclidean algorithm** Computes $\gcd(a, b)$. Based on two facts: $\gcd(0, b) = b$; $\gcd(a, b) = \gcd(b, a - qb)$ for any $q \in \mathbf{Z}$. For rapid convergence, take $q = \lfloor a/b \rfloor$, in which case $a - qb = a \bmod b$.

**Congruence** For $a, b \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$, we write $a \equiv b \pmod{n}$ iff $n \mid (b - a)$. Note $a \equiv b \pmod{n}$ iff $(a \bmod n) = (b \bmod n)$.

**Modular arithmetic** Fix $n \in \mathbf{Z}^+$. Let $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$ and let $\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n \mid \gcd(a, n) = 1\}$. For integers $a, b$, define $a \oplus b = (a + b) \bmod n$ and $a \otimes b = ab \bmod n$. $\oplus$ and $\otimes$ are associative and commutative, and $\otimes$ distributes over $\oplus$. Moreover, $\bmod n$ distributes over both $+$ and $\times$, so for example, $a + b \times (c + d) \bmod n = (a \bmod n) + (b \bmod n) \times ((c \bmod n) + (d \bmod n)) = a \oplus b \otimes (c \oplus d)$. $\mathbf{Z}_n$ is closed under $\oplus$ and $\otimes$, and $\mathbf{Z}_n^*$ is closed under $\otimes$.

**Primes and prime factorization** A number $p \ge 2$ is *prime* if it has no proper divisors. Any positive number $n$ can be written uniquely (up to the order of the factors) as a product of primes. Equivalently, there exist unique integers $k, p_1, \ldots, p_k, e_1, \ldots, e_k$ such that $n = \prod_{i=1}^{k} {p_i}^{e_i}$, $k \ge 0$, $p_1 < p_2 < \ldots < p_k$ are primes, and each $e_i \ge 1$. The product $\prod_{i=1}^{k} {p_i}^{e_i}$ is called the *prime factorization* of $n$. A positive number $n$ is *composite* if $(\sum_{i=1}^{k} e_i) \ge 2$ in its prime factorization. By these definitions, $n = 1$ has prime factorization with $k = 0$, so 1 is neither prime nor composite.

**Linear congruences** Let $a, b \in \mathbf{Z}$, $n \in \mathbf{Z}^+$. Let $d = \gcd(a, n)$. If $d \,|\, b$, then there are $d$ solutions $x$ in $\mathbf{Z}_n$ to the congruence equation $ax \equiv b \pmod{n}$. If $d \nmid b$, then $ax \equiv b \pmod{n}$ has no solution.

**Extended Euclidean algorithm** Finds one solution of $ax \equiv b \pmod{n}$, or announces that there are none. Call a triple $(g, u, v)$ *valid* if $g = au + nv$. Algorithm generates valid triples starting with $(n, 0, 1)$ and $(a, 1, 0)$. Goal is to find valid triple $(g, u, v)$ such that $g \mid b$. If found, then $u(b/g)$ solves $ax \equiv b \pmod{n}$. If none exists, then no solution. Given valid $(g, u, v)$, $(g', u', v')$, can generate new valid triple $(g - qg', u - qu', v - qv')$ for any $q \in Z$. For rapid convergence, choose $q = \lfloor g/g' \rfloor$, and retain always last two triples. Note: Sequence of generated $g$-values is exactly the same as the sequence of numbers generated by the Euclidean algorithm.

**Inverses** Let $n \in \mathbf{Z}^+$, $a \in \mathbf{Z}$. There exists unique $b \in \mathbf{Z}$ such that $ab \equiv 1 \pmod{n}$ iff $\gcd(a, n) = 1$. Such a $b$, when it exists, is called an *inverse* of $a$ modulo $n$. We write $a^{-1}$ for the unique inverse of $a$ modulo $n$ that is also in $\mathbf{Z}_n$. Can find $a^{-1} \bmod n$ efficiently by using Extended Euclidean algorithm to solve $ax \equiv 1 \pmod{n}$.

**Chinese remainder theorem** Let $n_1, \ldots, n_k$ be pairwise relatively prime numbers in $\mathbf{Z}^+$, let $a_1, \ldots, a_k$ be integers, and let $n = \prod_i n_i$. There exists a unique $x \in Z_n$ such that $x \equiv a_i \pmod{n_i}$ for all $1 \leq i \leq k$. To compute $x$, let $N_i = n/n_i$ and compute $M_i = N_i^{-1} \bmod n_i$, $1 <= i <= k$. Then $x = (\sum_{i=1}^{k} a_i M_i N_i) \bmod n$.

**Euler function** Let $\phi(n) = |\mathbf{Z}_n^*|$. One can show that $\phi(n) = \prod_{i=1}^{k} (p_i - 1) {p_i}^{e_i - 1}$, where $\prod_{i=1}^{k} {p_i}^{e_i}$ is the prime factorization of $n$. In particular, if $p$ is prime, then $\phi(p) = p - 1$, and if $p, q$ are distinct primes, then $\phi(pq) = (p-1)(q-1)$.

**Euler's theorem** Let $n \in \mathbf{Z}^+$, $a \in \mathbf{Z}_n^*$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$. As a consequence, if $r \equiv s \pmod{\phi(n)}$ then $a^r \equiv a^s \pmod{n}$.

**Order of an element** Let $n \in \mathbf{Z}^+$, $a \in \mathbf{Z}_n^*$. We define $\mathrm{ord}(a)$, the *order* of $a$ modulo $n$, to be the smallest number $k \geq 1$ such that $a^k \equiv 1 \pmod{n}$. Fact: $\mathrm{ord}(a) \,|\, \phi(n)$.

**Primitive roots** Let $n \in \mathbf{Z}^+$, $a \in \mathbf{Z}_n^*$. $a$ is a *primitive root* of $n$ iff $\mathrm{ord}(a) = \phi(n)$. For a primitive root $a$, it follows that $\mathbf{Z}_n^* = \{a \bmod n, a^2 \bmod n, \ldots, a^{\phi(n)} \bmod n\}$. If $n$ has a primitive root, then it has $\phi(\phi(n))$ primitive roots. Primitive roots exist for every prime $p$ (and for some other numbers as well). $a$ is a primitive root of $p$ iff $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for every prime divisor $q$ of $p - 1$.

**Discrete log** Let $p$ be a prime, $a$ a primitive root of $p$, $b \in \mathbf{Z}_p^*$ such that $b \equiv a^k \pmod{p}$ for some $k$, $0 \leq k \leq p - 2$. We say $k$ is the *discrete logarithm* of $b$ to the base $a$.

**Quadratic residues** Let $a \in \mathbf{Z}$, $n \in \mathbf{Z}^+$. $a$ is a *quadratic residue* modulo $n$ if there exists $y$ such that $a \equiv y^2 \pmod{n}$. $a$ is sometimes called a *square* and $y$ its *square root*.

**Quadratic residues modulo a prime** If $p$ is an odd prime, then every quadratic residue in $\mathbf{Z}_p^*$ has exactly two square roots in $\mathbf{Z}_p^*$, and exactly half of the elements in $\mathbf{Z}_p^*$ are quadratic residues. Let $a \in \mathbf{Z}_p^*$ be a quadratic residue. Then $a^{(p-1)/2} \equiv (y^2)^{(p-1)/2} \equiv y^{p-1} \equiv 1 \pmod{p}$, where $y$ a square root of $a$ modulo $p$. Let $g$ be a primitive root modulo $p$. If $a \equiv g^k \pmod{p}$, then $a$ is a quadratic residue modulo $p$ iff $k$ is even, in which case its two square roots are $g^{k/2} \bmod p$ and $-g^{k/2} \bmod p$. If $p \equiv 3 \pmod{4}$ and $a \in \mathbf{Z}_p^*$ is a quadratic residue modulo $p$, then $a^{(p+1)/4}$ is a square root of $a$, since $(a^{(p+1)/4})^2 \equiv aa^{(p-1)/2} \equiv a \pmod{p}$.

**Quadratic residues modulo products of two primes** If $n = pq$ for $p, q$ distinct odd primes, then every quadratic residue in $\mathbf{Z}_n^*$ has exactly four square roots in $\mathbf{Z}_n^*$, and exactly 1/4 of the elements in $\mathbf{Z}_n^*$ are quadratic residues. An element $a \in \mathbf{Z}_n^*$ is a quadratic residue modulo $n$ iff it is a quadratic residue modulo $p$ and modulo $q$. The four square roots of $a$ can be found from its two square roots modulo $p$ and its two square roots modulo $q$ using the Chinese remainder theorem.

**Legendre symbol** Let $a \geq 0$, $p$ an odd prime. $\left(\frac{a}{p}\right) = 1$ if $a$ is a quadratic residue modulo $p$, $-1$ if $a$ is a quadratic non-residue modulo $p$, and $0$ if $p \,|\, a$. Fact: $\left(\frac{a}{p}\right) = a^{(p-1)/2}$.

**Jacobi symbol** Let $a \geq 0$, $n$ an odd positive number with prime factorization $\prod_{i=1}^{k} {p_i}^{e_i}$. We define $\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$. (By convention, this product is 1 when $k = 0$, so $\left(\frac{a}{1}\right) = 1$.) The Jacobi and Legendre symbols agree when $n$ is an odd prime. If $\left(\frac{a}{n}\right) = -1$ then $a$ is definitely not a quadratic residue modulo $n$, but if $\left(\frac{a}{n}\right) = 1$, $a$ might or might not be a quadratic residue.

**Computing the Jacobi symbol** $\left(\frac{a}{n}\right)$ can be computed efficiently by a straightforward recursive algorithm, based on the following identities: $\left(\frac{0}{1}\right) = 1$; $\left(\frac{0}{n}\right) = 0$ for $n \neq 1$; $\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right)$ if $a_1 \equiv a_2 \pmod{n}$; $\left(\frac{2}{n}\right) = 1$ if $n \equiv \pm 1 \pmod{8}$; $\left(\frac{2}{n}\right) = -1$ if $n \equiv \pm 3 \pmod{8}$; $\left(\frac{2a}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{a}{n}\right)$; $\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)$ if $a \equiv 1 \pmod{4}$ or $n \equiv 1 \pmod{4}$; $\left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right)$ if $a \equiv n \equiv 3 \pmod{4}$.

**Solovay-Strassen test for compositeness** Let $n \in \mathbf{Z}^+$. If $n$ is composite, then for roughly 1/2 of the numbers $a \in \mathbf{Z}_n^*$, $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$. If $n$ is prime, then for every $a \in \mathbf{Z}_n^*$, $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$.

**Miller-Rabin test for compositeness** Let $n \in \mathbf{Z}^+$ and write $n-1 = 2^k m$, where $m$ is odd. Choose $1 \leq a \leq n-1$. Compute $b_i = a^{m2^i} \bmod n$ for $i = 0, 1, \ldots, k-1$. If $n$ is composite, then for roughly $3/4$ of the possible values for $a$, $b_0 \neq 1$ and $b_i \neq -1$ for $0 \leq i \leq k-1$. If $n$ is prime, then for every $a$, either $b_0 = 1$ or $b_i = -1$ for some $i$, $0 \leq i \leq k-1$.

*Michael J. Fischer*

*(Thanks to Miklós Csűrös, Andrei Serjantov, and Jerry Moon for pointing out errors in previous drafts.)*

*Last modified: October 26, 2000.*