COS 433: Cryptography — Princeton University
Handout: Basic Number Theory — Date: January 30, 2017

Basic Number Theory

1 Divisibility and Primality

Given two integers a, b, we say that a *divides* b if there exists an integer c such that $b = ac$. We denote this by $a|b$. In this case, a is a *divisor* of b. If a does not divide b, we write $a \nmid b$.

An integer $p > 1$ is *prime* if the only divisors of p are ± 1 and $\pm p$. That is, for every $a \notin \{\pm 1, \pm p\}$, $a \mid p$. An integer $n > 1$ is *composite* if it is not prime. In other words, there exists an integer $a \notin \{\pm 1, \pm n\}$ such that $a|n$. Primality can be tested in time polynomial in the bit-length of p.

Theorem 1 (Fundamental Theorem of Arithmetic)**.** *For any non-zero integer n, n can be expressed as*

$$n = \pm \prod_{i=1}^{k} p_i^{a_i}$$

for primes $p_1 < \cdots < p_k$ and positive integers $a_i > 0$. Moreover, the representation is unique. Here, we take the convention that the empty product ($k = 0$) evaluates to 1.

The *greatest common divisor* (GCD) of two integers a, b is the largest integer d such that $d|a$ and $d|b$. We denote d by $\mathsf{GCD}(a, b)$. The Euclidean algorithm computes $\mathsf{GCD}(a, b)$, and if a, b are n-bits, the running time is $O(n^3)$ (asymptotically faster algrithms exist, but the hidden constants make the Euclidean algorithm superior except for extremely large numbers). Two integers a, b are said to be *relatively prime* if $\mathsf{GCD}(a, b) = 1$.

2 Modular Arithmetic

Fix an integer $n > 1$. Think of n as being quite large, e.g. 1024 bits.

Two integers a, b are said to be *congruent modulo* n if $n|(a - b)$. In this case, we write $a \equiv b \mod n$. Note that congruency modulo n is transitive: if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

For any integer a, there is a unique integer r, $0 \leq r < n$, such that $a \equiv r \mod n$. Given a, we will use $a \bmod n$ to denote this r. Note that by $a \bmod n$ can be computed in quadratic time (in the bit-length of a and n).

The mod operation induces an *additive group* structure on the set $\{0, \cdots, n-1\}$. The identity is 0. To add or subtract two elements a, b, simply add or subtract over the integers, and then reduce the result mod n: $(a \pm b) \bmod n$. This process takes linear time in the bit-length of a, b, n (Note that we do not need to pay the full quadratic cost of the modular reduction since we know that $a + b$ is at most $2n$).

In fact, we can even give a *ring* structure with multiplicative identity 1. To multiply two elements, simply multiply over the integers and reduce mod$n$: $(a \times b) \bmod n$. Multiplication can be performed in quadratic time using the grade-school multiplication algorithm, though asymptotically faster algorithms exist for very large integers. We will denote the set $\{0, \cdots, n-1\}$, along with the induced ring structure, by $\mathbb{Z}_n$.

For some integers, it is also possible to compute multiplicative inverses mod$n$. Suppose $a \in \mathbb{Z}_n$ is relatively prime to n. a is called a *unit* of $\mathbb{Z}_n$. Then, there is a unique integer $b \in \mathbb{Z}_p$ such that $a \times b \equiv 1 \mod n$. We will denote this b by $a^{-1} \bmod n$. The Extended Euclidean algorithm allows for efficiently computing the inverse of a, if it exists, and the running time is cubic in the bit-length of its inputs. For an integer a that is *not* relatively prime to n, there is no multiplicative inverse.

For an integer c and a unit a, we define $c/a \bmod n$ to be $(c \times (a^{-1} \bmod n)) \bmod n$.

Denote by $\mathbb{Z}_n^*$ the set of units of $\mathbb{Z}_n$. Then $\mathbb{Z}_n^*$ is a multiplicative group with identity 1. The number of elements in $\mathbb{Z}_n^*$ is given by the Euler totient function $\phi(n)$. For $n = \prod_{i=1}^{k} p_i^{a_i}$,

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) = n \times \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Given integer b and element $a \in \mathbb{Z}_p^*$, it is possible to compute $a^b \bmod n$ efficiently (in the bit-length of a, b, n) by repeated squaring.

An element $a \in \mathbb{Z}_n$ is a *quadratic residue mod n* if there exists an element $r \in \mathbb{Z}_n$ such that $a \equiv r^2 \mod n$. In this case, r is called a *square root* of a.

2.1 The Prime Case

Let p be a prime, and consider the sets $\mathbb{Z}_p$,$\mathbb{Z}_p^*$. Since p has no divisors other than 1 and itself, the only non-unit of $\mathbb{Z}_p$ is 0, so we have that $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$, which has size $\phi(p) = p - 1$. This means $\mathbb{Z}_p$ is a *field*: all non-zero elements are invertible.

Theorem 2 (Fermat's Little Theorem)**.** *For any integer a, $a^p \equiv a \mod p$. If $a \not\equiv 0$ mod n, then $a^{p-1} \equiv 1 \mod p$.*

Theorem 3. *The multiplicative group $\mathbb{Z}_p^*$ is* cyclic. *That is, there is an element $g \in \mathbb{Z}_p^*$ such that $\mathbb{Z}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$. g is called a* generator *of $\mathbb{Z}_p^*$.*

Quadratic Residues mod p. Assume $p > 2$. Given a quadratic residue $a \equiv r^2 \mod p$ other than 0, there are exactly two square roots of a: $+r$ and $-r$. This follows from the fact that over a field, the polynomial $x^2 - a$ has at most two roots. In particular, there are only two square roots of 1 mod p, namely $+1$ and -1.

Easy problems in $\mathbb{Z}_p$.

- Addition, subtraction, multiplication, division, exponentiation
- Generating a random element
- Determine if a is a quadratic residue
- If a is a quadratic residue, determine one of its roots
- Solving low-degree polynomial equations

Problems believed to be hard in $\mathbb{Z}_p$.

- Discrete log: given a generator g for $\mathbb{Z}_p^*$ and $h = g^r \mod p$, compute r.
- Computational Diffie-Hellman: given a generator g, and elements $x = g^a \mod p$ and $y = g^b \mod p$, compute $z = g^{ab} \mod p$

2.2 The Composite Case

Let n be a composite number.

Theorem 4 (Euler's Theorem)**.** *For any integer $a \in \mathbb{Z}_n^*$, $a^{\phi(n)} \equiv 1 \mod n$.*

This follows from Lagrange's theorem and the fact that $\mathbb{Z}_n^*$ is a multiplicative group with size $\phi(n)$.

Chinese Remainder Theorem (CRT). Let $n = pq$ where p, q are relatively prime. Then given $r \in \mathbb{Z}_p$, $s \in \mathbb{Z}_q$, there exists a unique integer $t \in \mathbb{Z}_n$ such that $r = t \mod p$ and $s = t \mod q$. Moreover, s can be computed efficiently.

This means that each $t \in \mathbb{Z}_n$ can be viewed as a pair $(r, s) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Arithmetic operations in Z_n corresponds to component-wise operations on $Z_p \times Z_q$. So $t_0 + t_1$ corresponds to the pair $(r_0 + r_1, s_0 + s_1)$ and $t_0 \times t_1$ corresponds to $(r_0 \times r_1, s_0 \times s_1)$.

Therefore, an element $t \in \mathbb{Z}_n$ is invertible in $\mathbb{Z}_n$ if and only if r and s are invertible in $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively. Similarly, t is q quadratic residue if and only if r, s are quadratic residues.

We will now focus on the case where n is a product of 2 primes, say p and q. We will generally consider the case where p and q are about the same size. Then we have that $\mathbb{Z}_n^*$ has size $(p-1)(q-1)$. This can be easily seen using the Chinese Remainder Theorem and the fact that $\mathbb{Z}_p^*$ and $\mathbb{Z}_q^*$ have $(p-1)$ and $(q-1)$ elements, respectively.

Quadratic Residues. If $a = t^2 \bmod n$, there are actually now 4 square roots. Indeed, if we consider $r = t \bmod p$ and $s = t \bmod q$, the four square roots are the result of applying the CRT to the four pairs $(\pm r, \pm s)$.

Easy problems in $\mathbb{Z}_n$.

- Addition, subtraction, multiplication, division, exponentiation
- Generating a random element
- Solving linear equations

Problems believed to be hard in $\mathbb{Z}_n$.

- Discrete log, computational Diffie-Hellman
- Factoring n
- Determine if a is a quadratic residue, computing a square root.
- Solving non-linear (even degree 2) polynomial equations.