1 Number Theory and Cryptography

1.1 Divisibility and Modular Arithmetic

Definition

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$ (or equivalently, if $\frac{b}{a}$ is an integer). When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

We can express $a \mid b$ using quantifiers as $\exists c(ac = b)$.

There are some basic properties of divisibility of integers:

- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- If $a \mid b$, then $a \mid bc$ for all integers c
- If $a \mid b$ and $b \mid c$, then $a \mid c$

Corollary 1.1

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

Theorem 1.2: The Division Algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

In the equality given in the division algorithm, d is called the divisor, a is called the divided, q is called the quotient, and r is called the remainder. The notation $q = a$ **div** d is used to denote quotient, and $r = a \mod d$ is used to notate the remainder.

When a is an integer and d is a positive integer, a **div** $d = \lfloor a/d \rfloor$ and $a \mod d = a - d$.

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a congruence and that m is its modulus. If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Theorem 1.3

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mod m = b \mod m$.

Theorem 1.4

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Theorem 1.5

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

and

$$ac \equiv bd \pmod{m}$$

Corollary 1.6

Let m be a positive integer and let a and b be integers. Then:

$$(a + b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

and

$$ab \mod m = ((a \mod m)(b \mod m)) \mod m$$

We can define arithmetic operations on Z_m, the set of nonnegative integers less than m, that is, the set $0, 1, \ldots, m-1$. We definte the the addition of these integers as:

$$a +_m b = (a + b) \mod m$$

We can define the multiplication of these integers as

$$a \cdot_m b = (a \cdot b) \mod m$$

Here are some properties of these:

- Closure - If a and b belong to Z_m, then $a +_m b$ and $a \cdot_m b$ belong to z_m.
- Associativity - If a, b, and c, belong to Z_m, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m) c$.
- Commutativity - If a and b belong to Z_m, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- Identity elements - The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
- Additive Inverses - If $a \neq 0$ belongs to Z_m, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.
- Distributivity - If a, b, and c belong to Z_m, then $a \cdot_m (b +_m c) = (a \cdot_m n) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

1.2 Integer Representation and Algorithms

Theorem 1.7

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where k is a nonnegative integer, a_0, a_1,..., a_k are nonnegative integers less than b, and $a_k \neq 0$.

Choosing 2 as the base gives binary expansions of integers. In binary notation each digit is either a 0 or a 1. In other words, the binary expansion of an integer is a just a bit string.

Base 8 expansions are called octal expansions and base 16 expansions are hexadecimal expansions.

We can describe an algorithm for constructing the base b expansion of an integer n.

First divide n by b to obtain a quotient and remainder:

$$n = bq_0 + a_0$$

assuming a_0 is positive and less than b.

The remainder, a_0, is the rightmost digit in the base b expansion of n. Next, divide q_0 by b to obtain:

$$q_0 = bq_1 + a_1 \qquad 0 \leq a_1 < b$$

Continue this process, successively dividing the quotients by b, obtaining additional base b digits as the remainders.

The algorithms for performing operations with integers using their binary expansions is important.

Throughout the following, lets suppose that the binary expansions of a and b are:

$$a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2, b = (b_{n-1}b_{n-2}\cdots b_1b_0)_2$$

so that a and b each have n bits.

Let's first consider the adding two integers in binary notation. The procedure is as follows:

First add their rightmost bits:

$$a_0 + b_0 = c_0 \cdot 2 + s_0$$

where s_0 is the rightmost bit in the binary expansion of $a + b$ and c_0 is the carry, either a 0 or 1.

Continue this:

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$$

This procedure produces the binary expansion of the sum:

$$a + b = (s_n s_{n-1} s_{n-2} \ldots s_1 s_0)_2$$

Now we consider multiplication. Using the distributive law it is easy to see that

$$\begin{aligned} ab &= a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1}2^{n-1}) \\ &= a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1}2^{n-1}) \end{aligned}$$

There is an algorithm for div and mod as well. Given integers a and d, where $d > 0$, we can find $q = a\mathbf{div}d$ and $r = a \mod d$ using the algorithm below.

We can show that this algorithm uses $O(q \log a)$ bit operations when $a > d$.

Given a as an integer, and d as a positive integer, we can make q equal to 0 and $r = |a|$.

While $r \geq d$, r gets assigned to $r - d$ and q gets assigned $q + 1$.

If $a < 0$ and $r > 0$ then r gets assigned $d - r$ and q gets assigned $-(q + 1)$.

We return the quotient as q and the remainder as r.

When a is divided by b, we need $O(n^2)$ bit operations to find the quotient and remainder.

In cryptography it is important to be able to find $b^n \mod m$ efficiencly without using an excessive amount of memory.

First observe that we can avoid using a large amount of memory if we compute $b^n \mod m$ by successively computing $b^k \mod m$ for $k = 1, 2, \ldots, n$ using that fact that $b^{k+1} \mod m = b(b^k \mod m) \mod m$.

To motivate the fast modular exponentiation algorithm, we can first explain how to use the binary expansion of n.

Say that $n = (a_{k-1} \dots a_1 a_0)_2$ to compute b^n. Firstly, note that:

$$b^n = b^{a_{k+1} \cdot 2^{k-1} + \dots + a_1 \cdot 2 + a_0} = b^{a_{k=1} \cdot 2^{k-1}} \dots b^{a_1 \cdot 2} \cdot b^{a_0}$$

This shows that to compute b^n we only have to compute b, b^2, b^4, $\dots$, b^{2^k}.

Note that $(b^{2^n})^2 = b^{2^{n+1}}$ when n is a nonnegative integer.

The algorithm successively finds $b \mod m, b^2 \mod m, b^4 \mod m, dots, b^{2^{k-1}} \mod m$ and multiplies together those terms $b^{2^i} \mod m$ where $a_j = 1$, finding the remainder of the product when divided by m after each multiplication. We only need to perform $O(\log_2(n))$ multiplications.

We can also show the most efficient algorithm as seen:

Let b be an integer and $n = (a_{k-1} a_{k-2} \dots a_1 a_0)_2$ and m be positive integers.

Let x be 1 and power be $b \mod m$.

For all values 0 to $k-1$, if $a_i = 1$, then x becomes $(x \cdot \text{power}) \mod m$ and power becomes power·power $\mod m$.

The return value for this algorithm is x, which is $b^n \mod m$.

This algorithm only uses $O((\log m)^2 \log n)$ bit operations to find $b^n \mod m$.

1.3 Primes and Greatest Common Divisors

Positive integers that have exactly two different positive integer factors are called prime.

Definition

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Remember that 1 is not prime, and that an integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

Theorem 1.8: The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

Theorem 1.9

If n is a composite number, then n has a prime divisor less than or equal to $\sqrt{n}$.

From this theorem above, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. This leads to the brute-force algorithm known as trial division. To use trial division, we divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes.

Because every integer has a prime factorization, it would be useful to have a procedure for finding the prime factorization. Start with the theorem above, and find if there is a prime factor not exceeding $\sqrt{n}$. If there is none found, then continue by factoring n/p. Note that n/p will have no prime factors less than p. If n/q has a prime factor q, then continue by factoring $n/(pq)$. There are infinitely many primes.

Theorem 1.10: The Prime Number Theorem

The ratio of $\pi(x)$, the number of primes not exceeding x, and $x/\ln x$ approaches 1 as x grows without bound.

Every odd integer is in one of the two arithmetic progressions $4k+1$ or $4k+3$, where $k = 1, 2, \cdots$.

The largest integer that divides two integers is called the greatest common divisor of these integers.

Definition

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Definition

The integers a and b are relatively prime if their greatest common divisor is 1.

Definition

THe integers a_1, a_2,..., a_n are pairwise relatively prime if $\gcd(a_i, a_k) = 1$ whenever $1 \leq i < j \leq n$.

Prime factorizations can be used to find the least common multiple of the integers.

Definition

THe least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

Theorem 1.11

Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b)$$

There is a more efficient way of finding the greatest common divisor using the Euclidean algorithm.

Lemma 1.12

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Proof. If we can show that the common divisors of a and b are the same as the common divisors of b and r, we will have shown that $\gcd(a, b) = \gcd(b, r)$, because both pairs must have the same greatest common divisors.

So suppose that d divides both a and b. Then it follows that d also divides $a - bq = r$. Hence, any common divisor of a and b is also a common divisor of b and r.

Likewise, suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r is also a common divisor of a and b.

Consequently, $\gcd(a, b) = \gcd(b, r)$. □

An important result is that the greatest common divisor of two integers a and b can be expressed in the form:

$$sa + tb$$

where s and t are integers. In other words, $\gcd(a, b)$ can be expressed as a linear combination with integer coefficients of a and b.

Theorem 1.13: Bezout's Theorem

If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Lemma 1.14

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Lemma 1.15

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Theorem 1.16

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

1.4 Solving Congruences

A congruence of the form

$$ax \equiv b \pmod{m}$$

where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

Our goal is to solve th linear congruence $ax \equiv b \pmod{m}$.

One method is to use an integer $\overline{a}$ such that $\overline{a}a \equiv 1 \pmod{m}$, if such an integer exists. Such an integer $\overline{a}$ is to be an inverse of a modulo m.

Theorem 1.17

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is there is a unique positive integer $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.)

We can design a more efficient algorithm than brute force to find an inverse of a modulo m when $\gcd(a, b) = 1$ using the steps of the Euclidean algorithm.

Once we have an inverse $\overline{a}$ of a modulo m, we can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides of the linear congruence by $\overline{a}$.

The Chinese remainder theory states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo of the product of the moduli.

Theorem 1.18: The Chinese Remainder Theorem

Let m_1, m_2,..., m_n be pairwise relatively prime positive integers greater than one and a_1, a_2,...,a_n arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Suppose that m_1, m_2,..., m_n are pairwise relatively prime moduli and let m be their product. By the Chinese remainder theorem, we can show that an integer a with $0 \leq a < m$ can be uniquely represented by the n-tuple consisting of its remainders upon division by m_i, $i = 1, 2, \ldots, n$. That is, we can uniquely represent a by

$$(a \mod m_1, a \mod m_2, \ldots, a \mod m_n)$$

Theorem 1.19: Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Furthermore, for every integer a we have

$$a^p \equiv a \pmod{p}$$

Fermat's little theorem tells us that if $a \in \mathbb{Z}_p$, then $a^{p-1} = 1$ in $\mathbb{Z}_p$.

Definition

Let b be a positive integer. If n is a composite positive integer, and $b^{n-1} \equiv 1 \pmod{n}$, then n is called a pseudoprime to the base b.

Definition

A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $\gcd(b, n) = 1$ is called a Carmichael number.

In the set of positive real numbers, if $b > 1$ and $x = b^y$, we say that y is the logarithm of x to the base b. Here, we will show that we can also define the concept of logarithms modulo p of positive integers, where p is a prime.

Definition

A primitive root modulo of prime p is an integer r in $\mathbb{Z}_p$ such that every nonzero element of $\mathbb{Z}_p$ is a power of r.

An important fact in number theory is that there is a primitive root modulo p for every prime p.

Suppose that p is prime and r is a primitive root modulo p. If a is an integer between 1 and $p - 1$, that is, a nonzero element of $\mathbb{Z}_p$, we know that there is a unique exponent e such that $r^e = a$ in $\mathbb{Z}_p$, that is, $r^e \mod p = a$.

Definition

Suppose that p is a prime, r is a primitive root modulo p, and a is an integer between 1 and $p - 1$ inclusive. If $r^e \mod p = a$ and $0 \leq e \leq p - 1$, we say that e is the discrete logarithm of a modulo p to the base r and we write $log_r a = e$ (where the prime p is understood).