TD 7+: A quick remainder on Number Theory

1 Primes and divisibility

Let $\mathbf{Z}$ be the set of integers. For $a, b \in \mathbf{Z}$, we say that *a divides b*, written $a|b$ if there exists $k \in \mathbf{Z}$ such that $b = ka$. If $a \notin \{1, b\}$, a is called a *factor* of b. An integer p is *prime* if it has no factors (i.e. if it has only two divisors 1 and itself).

Theorem 1. *Every integer greater than* 1 *can be expressed uniquely as a product of primes. Let* $N > 0$,

$$N = \prod_i p_i^{e_i} \text{ with } p_i \text{ prime and } e_i \geq 1.$$

Proposition 1. *Let a be an integer and b be a positive integer, there exist unique integers* q, r *such that*

$$a = qb + r \text{ with } 0 \leq r < b$$

The *greatest common divisor* of two non-negative integers a, b, written $\gcd(a, b)$, is the largest integer c such that $c|a$ and $c|b$.

Proposition 2. *Let* a, b *be positive integers. Then there exists integers* X, Y *such that* $Xa + Yb = \gcd(a, b)$. *Futhermore,* $\gcd(a, b)$ *is the smallest positive integer that can be expressed in this way.*

Given a and b, the *Euclidean algorithm* can be used to compute $\gcd(a, b)$ in polynomial time. The *extended Euclidean algorithm* can be used to compute X and Y in polynomial time as well.

Proposition 3. *Let* a, b, c, p, q, N *be integers.*

- *If* $c|ab$ *and* $\gcd(a, c) = 1$ *then* $c|b$.
- *If* $p|N$, $q|N$ *and* $\gcd(p, q) = 1$ *then* $pq|N$.

2 Modular Arithmetic

Let $a, b, N \in \mathbf{Z}$ with $N > 1$. The notation $(a \bmod N)$ denotes the remainder of a upon division by N. We say that a and b are congruent modulo N if $a \bmod N = b \bmod N$. Note that congruence modulo N is an equivalence relation. It also obeys the standard rules of arithmetic with respect to addition, substraction and multiplication. But in general it does not respect division.
If there exists b^{-1} such that $bb^{-1} = 1 \bmod N$, we say that b^{-1} is a multiplicative inverse of b modulo N. When b is invertible modulo N, we define division by b modulo N as multiplication by b^{-1} modulo N. We stress that division by b is only defined when b is invertible modulo N.

Proposition 4. *Let* a, N *be integers with* $N > 1$. *Then a is invertible modulo N if and only if* $\gcd(a, N) = 1$.

2.1 Groups

We will always deal with finite, abelian groups. We call *order* of a group the number of elements in the group.
Let $\mathbf{G}$ be a multiplicative group, $g \in \mathbf{G}$ and $b > 0$ be an integer. Then the exponentiation g^b can be computed using a polynomial number of underlying group operations in $\mathbf{G}$.

Theorem 2. *Let* $\mathbf{G}$ *be a finite group of order m. Then for any element* $g \in \mathbf{G}$, $g^m = 1$.

Corollary 1. *Let* $\mathbf{G}$ *be a finite group of order* $m > 1$. *Then for* $g \in \mathbf{G}$ *and any integer i, we have* $g^i = g^{i \bmod m}$.

3 The group $\mathbf{Z}_N^*$

For any $N > 1$, the set $\mathbb{Z}_N = \{0, \ldots, N-1\}$ is a group under addition modulo N. We now define $\mathbf{Z}_N^*$ as:

$$\mathbb{Z}^\star = \{a \in \{1, \ldots, N-1\} \,|\, \gcd(a, N) = 1\}$$

i.e. all the integers *relatively prime* to N in $\mathbb{Z}_N$. Then under multiplication modulo N, all the elements of this set are invertible.

Theorem 3. *Let $N > 1$ be an integer. Then $\mathbb{Z}^\star$ is an abelian group under multiplication modulo N.*

Euler function

The *Euler function* φ is defined as $\varphi(N) = |\mathbb{Z}^\star|$, it is the order of the group $\mathbb{Z}^\star$. When $N = p$ prime, then all elements of $\{1, \ldots, p-1\}$ are relatively prime to p, and then $\phi(p) = p - 1$. When $N = pq$ with p and q are distinct primes, then if an integer $a \in \{1, \ldots, N-1\}$ is not relatively prime to N, then either $p|a$ or $q|a$. The elements in this set divisible by p are exactly the $(q-1)$ elements $p, 2p, \ldots, (q-1)p$, and the elements divisible by q are exactly the $(p-1)$ elements $q, 2q, \ldots, (p-1)q$. The number of elements remaining is therefore

$$N - 1 - (q-1) - (p-1) = pq - q - p + 1 = (p-1)(q-1).$$

Then if $N = pq$ with p and q are distinct primes, $\phi(N) = (p-1)(q-1)$.

Theorem 4. *Let $N = \prod_i p_i^{e_i}$, where the p_i are distinct primes and $e_i \geq 1$. Then $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$.*

Theorem 5 (Fermat)**.** *Take arbitrary $N > 1$ and $a \in \mathbb{Z}^\star$, then*

$$a^{\phi(N)} = 1 \bmod N.$$

For the specific case that $N = p$ is prime, we have $a^{p-1} = 1 \bmod p$.

4 Chinese Remainder Theorem

We use the notation $\simeq$ to say that two groups are isomorphic.

Theorem 6. *Let $N = pq$ where p and q are relatively prime. Then*

$$\mathbb{Z}_N \simeq \mathbb{Z}_p \times \mathbb{Z}_q \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*.$$

Moreover, let f be the function mapping elements $x \in \{0, \ldots, N-1\}$ to pairs (x_p, x_q) with $x_p \in \{0, \ldots, p-1\}$ and $x_q \in \{0, \ldots, q-1\}$ defined by

$$f(x) = (x \bmod p, x \bmod q).$$

Then f is an isomorphism from $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$, as well as an isomorphism from $\mathbb{Z}_N^*$ to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

This theorem does not require p or q to be prime. En extension of this Theorem says that if $p_1, \ldots, p_\ell$ are pairwise relatively prime and $N = \prod_i p_i$, then

$$\mathbb{Z}_N \simeq \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_\ell} \text{ and } \mathbb{Z}_N^* \simeq \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_\ell}^*.$$

An isomorphism in each case is obtained by a natural extension of the one used in the theorem.
For the specific case of $N = pq$ product of distinct primes. The Chinese Remainder Theorem shows that addition or multiplication modulo N can be transformed to analogous operations modulo p and q. This conversion can be carried out in polynomial time if the factorisation of N is known.

5 Cyclic groups

Let $\mathbf{G}$ be a finite group and $g \in \mathbf{G}$, then the *order* of g is the smallest i such that $g^i = 1$.

Proposition 5. *If g is an element of order i, then $g^x = g^{x \bmod i}$. Furthermore, $g^x = g^y$ if, and only if, $x = y \bmod i$.*

The identity of any group $\mathbf{G}$ has order 1. At the other extreme, if there exists an element $g \in \mathbf{G}$ of order m (the order of $\mathbf{G}$), then the set $\langle g \rangle = \{g^0, g^1, \ldots\}$ generated by g is equal to $\mathbf{G}$. In this case, we call $\mathbf{G}$ a *cyclic* group and we say that g is a generator of $\mathbf{G}$.

Theorem 7. *Lagrange Let $\mathbf{G}$ be a finite group of order m and $g \in \mathbf{G}$ an element of order i. Then $i|m$.*

Corollary 2. *If $\mathbf{G}$ is a group of prime order p, then $\mathbf{G}$ is cyclic. Furthermore, all elements of $\mathbf{G}$ except the identity are generators of $\mathbf{G}$.*

Groups of prime order form one class of cyclic groups. The additive group $\mathbb{Z}$ for $N > 1$ is another example. Another important example (which does not have prime order for $p > 3$) is the following.

Theorem 8. *If p is prime, then $\mathbb{Z}_p^*$ is cyclic.*

6 Primes, factoring

Given a composite integer N, the factoring problem is to find positive integers p, q such that $N = pq$. Factoring is a classic example of hard problem, *no polynomial-time* algorithm that solves the factoring problem has been yet developed.

Primes

The distribution of primes is given by the *prime number theorem* which gives a precise bounds on the fraction of integers of a given length that are prime. This theorem implies that the probability that a random n-bit integer is prime is at least c/n for a constant c.
The most commonly-used algorithm to test primality is the *Miller-Rabin* algorithm. This algorithm takes at input an integer N and an integer t that determine the error probability. It runs in time polynomial in $|N|$ and t and if N is prime, it always outputs "prime", otherwise it outputs "prime" with probability at most 2^{-t}.
Putting all of this together there exists a polynomial-time prime-generation algorithm that, on input n, outputs a random n-bits prime except with probability negligible in n.

7 Exercises

Exercise 1. [*Factorization*]

1. Let $N = pq$ be a product of p and q two distinct primes. Show that if $\varphi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

Exercise 2. [*Generator*]

Let $p \geq 3$ be a prime. The group $\mathbb{G} = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. The purpose of the exercise is to find a generator of that group, i.e., an element g such that $(\mathbb{Z}/p\mathbb{Z})^* = \{g^k : k \in \mathbb{Z}\}$.

1. For $g \in \mathbb{G}$, we call the order of g the smallest $k > 0$ such that $g^k = 1$, denoted by $\mathcal{O}(g)$. Show that for any $g \in \mathbb{G}$, we have $\mathcal{O}(g)|p-1$.

2. Give an element of $\mathbb{G}$ that is not a generator of $\mathbb{G}$. How many elements of $\mathbb{G}$ are generators?
3. Assume that $p - 1 = 2q$ for some q that is prime. Give an efficient algorithm that finds a generator of $\mathbb{G}$. How do we find such a prime p?

Exercise 3. [*Modulo*]

Let p, N be integers with $p|N$.

1. Prove that for any integer X,
$$(X \bmod N) \bmod p = X \bmod p.$$
2. Show that, in contrast, $(X \bmod p) \bmod N$ may not be equal to $X \bmod N$.

Exercise 4. [*Algebraic structure*]

Let $N = pq$ with p and q distinct odd primes of identical bit-size. We want to study the algebraic structure of $(\mathbb{Z}/N^2\mathbb{Z})^\star$. Show the following propositions:

1. $\gcd(N, \varphi(N)) = 1$.
2. For any $a \in \mathbb{N}$, $(1 + N)^a = (1 + aN) \bmod N^2$.
3. As a consequence, $(1 + N)$ has order $N \bmod N^2$.

Exercise 5. [*Phi function*]

1. Let p be a prime, show that $\varphi(p) = p - 1$.
2. Let p and q be distinct primes and $N = pq$, show that $\varphi(N) = (p - 1)(q - 1)$.
3. Let p be a prime and $e \geq 1$ an integer. Show that
$$\varphi(p^e) = p^{e-1}(p - 1).$$
4. Let p, q be relatively prime. Show that $\varphi(pq) = \varphi(p)\varphi(q)$.
5. Prove Theorem 4.

Exercise 6. [*RSA*]

1. Let $N = pq$ for p and q distinct primes, and e, d integers such that $ed = 1 \bmod \varphi(N)$. Show that for all $x \in \mathbb{Z}_N$, we have $(x^e)^d = x \bmod N$.

   Hint: *Use the Chinese remainder theorem.*

Exercise 7. [Quadratic residues]

$\rightarrow$ *read again* ***Exercise 5 from TD 2***