Lection 6: Theory of numbers

15.03.2019

Filipp Rukhovich

Hello Muscat International Bootcamp 2019

Work by modulo

In many problems of sport programming (combinatorial, DP etc), answer can be very big number. To make the life easier and avoid a difference of standard libraries of different languages, participants are asked to find the remainder of division of answer by some fixed natural modulo.

Definition

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then, one says that a is divided by b if there exist such a number $c \in \mathbb{Z}$ that $a = b * c$. Also in this case, one says that a is a multiple of b.

Definition

Let $a, b \in \mathbb{Z}$, $mod \in \mathbb{Z}_+$. We will say a is *equal*, or *equivalent*, by modulo mod if $a - b$ is divided by mod. Notation: $a \equiv_{mod} b$.

Work by modulo

Definition

Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+$. Then, there exist and only integers q, r, $r \in [0, b)$, such that $a = b * q + r$. These q, r are called *quotient* and *remainder* of division of a by b, correspondingly. r is also denoted as $rem_b(a)$.

For example, if we divide 13 by 3, then the quotient will be 4, and the remainder — 1, because $13 = 3 * 4 + 1$. But if we divide -13 by 3, then quotient will be -5, and remainder is 2 $(-13 = 3 * (-5) + 2)$.

The notion of remainder is connected with operator % in some programming languages. Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$. If $a \geqslant 0$, then $a\%b$ is $rem_b(a)$.

For example $(-14)\%3$ is equal to -2. It can be easily proved that if $a < 0$ then $a\%b = rem_b(a) - b$.

Work by modulo

Obviously, for any $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+$, $k \in \mathbb{Z}$:
$rem_b(a) = rem_b(a - b) = rem_b(a + b) = rem_b(a + k * b)$ (because if $a = q * b + r$ then $a - b = (q - 1) * b + r$, $a + b = (q + 1) * b + r$, $a + k * b = (q + k) * b + r$).

Lemma

Let $a, b \in \mathbb{Z}, mod \in \mathbb{Z}_+$. Then,
$rem_{mod}(a + b) = rem_{mod}(rem_{mod}(a) + rem_{mod}(b))$.

Proof

Let $a = q_a * mod + r_a$, $b = q_b * mod + r_b$, q_a, q_b, $r_a, r_b \in \mathbb{Z}$, $r_a = rem_{mod}(a)$, $r_b = rem_{mod}(b)$. Then,
$rem_{mod}(a + b) = rem_{mod}(q_a * mod + r_a + q_b * mod + r_b) = rem_{mod}(r_a + r_b)$, QED.

Work by modulo

Analogically we can prove the following lemma.

Lemma

Let $a, b \in \mathbb{Z}$, $mod \in \mathbb{Z}_+$. Then,
$rem_{mod}(a - b) = rem_{mod}(rem_{mod}(a) - rem_{mod}(b))$, and also
$rem_{mod}(a * b) = rem_{mod}(rem_{mod}(a) * rem_{mod}(b))$.

Suppose that, for example, we are to calculate number $3^{1000000} + 2^{10000} - 38^{34}$ by modulo $MOD = 10^9 + 7$. To do that, it's not necessary to calculate very long numbers and then take it by modulo — we can do it in type *long long*!

Work by modulo

```
int deg3 = 1;
for (int i = 1; i <= 1000000; ++i)
    deg3 = (deg3 * 3) % MOD;
int deg2 = 1;
for (int i = 1; i <= 10000; ++i)
    deg2 = (deg2 * 2) % MOD;
int deg38 = 1;
for (int i = 1; i <= 34; ++i)
    deg38 = (deg38 * 38) % MOD;
int ans = deg3 + deg2 - deg38;
if (ans < 0)
    ans += MOD;
```

Fast exponentation and prime numbers

Working by modulo MOD, one can calculate a^n for big n — for example, $n = 10^{18}$!

As we remember, it's impossible to calculate a^n in a straightforward way — we are to calculate it faster. But let $a2 = (a * a)\%MOD$; then if n is even then $a^n \equiv_{MOD} a2^{n/2}$; otherwise $a^n = a * a2^{(n-1)/2}$. It reduces the exponent in two times, and the complexity of the calculation of degree is $O(log\ \ n)$.

A division will be discussed later.

One of the most popular moduloes in different problems are prime moduloes, like $10^9 + 7$ or $10^9 + 9$ — they make the probability of random coincidence of calculated answer with correct one smaller in case of some mistake.

Prime numbers: checking whether it's prime

Definition

Positive integer $p \geqslant 2$ is called *prime* if it has two divisors — 1 and p.

For any number p, 1 and p are called trivial divisors of p; all other numbers are called non-trivial. So, p is prime if and only if there are no any non-trivial divisors for p.

For example, $2, 3, 5, 43, 79, 83$ are primes, while $4 = 2 * 2$, $35 = 5 * 7$, 2^{17} are not.

How to check whether given an integer p is prime or not?

Of course we can do it in $O(p)$ by just checking all numbers between 2 and $p - 1$ to be non-trivial divisors; but note that if p has a non-trivial divisor q then p has a non-trivial divisor which doesn't exceed $\sqrt{p}$ (it is for example q or p/q). It gives us a possibility to check only such a numbers q that $2 \leqslant q$, $q^2 \leqslant p$ and reduces the complexity of the algorithm to $O(\sqrt{p})$.

Prime numbers: sieve of Eratosthenes

Suppose now that we have a positive integer n and what to reveal for each number from 2 to n whether it's prime or not. One can check all the numbers independently, and the complexity will be $O(n\sqrt{n})$.

We will discuss more effective method which is called "sieve of Eratosphenes". The idea is the following:

1. Define boolean array *bool isNonPrime*$[2..n]$; initially, *isPrime*$[i]$ is false for any $i \in [2, n]$;
2. Iterate i over all the numbers from 2 to n; for each number i, do the following:
   - if *isNonPrime*$[i]$ $=$ *true* then go to the next i;
   - otherwise, assign *isNonPrime*$[j]$ to be j for $j = 2 * i, 3 * i, \dots, \lfloor \frac{n}{i} \rfloor * i$.
3. After performing that, for any i, *isNonPrime*$[i]$ is false if and only if i is prime.

Prime moduloes: division

Let's move back to work by modulo.

Suppose that we want to calculate a ratio $\frac{a}{b}$ for some very-very big integers a and b by **prime** modulo MOD; it can be guaranteed that a is divided by b, but we have only numbers $a' = rem_{MOD}(a)$, $b' = rem_{MOD}(b)$, $b' > 0$. The question is: how to find $rem_{MOD}(\frac{a}{b})$?

One can show (and we will prove it later) that there is the only integer $c' \in [0, MOD)$ such that $a' \equiv_{MOD} b' * c'$. The following famous theorem helps to find c'.

Little Fermat's theorem

Let p be a prime number, and integer $a \in [1, p)$. Then, $a^{p-1} \equiv_p 1$.

According to this theorem, c' can be equal to $rem_{MOD}(a' * b'^{MOD-2})$.

Greatest common divisor

The next important thing we will discuss is a notion of *greatest common divisor*. Let a, b be nonnegative integers, and at least one of them is nonzero.

Definition

Positive integer c is called *common divisor* of numbers a, b if a, b are both multiple of c. The greatest sucn a number is called *greatest common divisor* of numbers a and b, or $GCD(a, b)$.

How to find it effectively?

Lemma

Suppose that $a \geqslant b > 0$. Then, $GCD(a, b) = GCD(a - b, b)$.

It's true because integer c is a common divisor of numbers a and b if and only if c is a common divisor of numbers $a - b$ and b.

Greatest common divisor: Euclid's algorithm

The following lemma is a straightforward consequence of the previous one because $rem_b(a) = a - b * \lfloor \frac{a}{b} \rfloor$.

Lemma

Suppose that $a \geqslant b > 0$. Then, $GCD(a, b) = GCD(b, rem_b(a))$.

Last lemma gives us the following algorithm of finding $GCD(a, b)$ for some nonnegative integers a, b:

- if $b = 0$ then $GCD(a, b) = a$;
- otherwise, $GCD(a, b) = GCD(b, rem_b(a))$.

This algorithm is called *Euclid's algorithm*. It can be proved that the complexity of its algorithm is $O(log(a + b))$.

Greatest common divisor and diophantine equation

Definition

Let $a, b, c \in \mathbb{Z}$. Then, $ax + by = c$ is called *linear diophantine equation*. We'll call it just diophantine equation.

Is it possible to solve such a equation in integers? In other words is there at least on pair of integer (x_0, y_0) such that $a * x_0 + b * y_0 = c$?

Diophantine equation with coprime coefficients

If $GCD(a, b) = 1$ then the solution exists.

Proof.

We'll prove it by induction by b. If $b = 0$ then $a = 1$, so (1, 0) is a solution; it is a base step.
To prove the induction step, let $b > 0$, and $a = q * b + r$, $r = rem_b(a)$. $GCD(a, r) = 1$; so, according to inductive hypothesis, there are such (x_1, y_1) that $b * x_1 + r * y_1 = 1$. It means that
$1 = b * x_1 + r * y_1 = b * x_1 + (a - q * b) * y_1 = a * y_1 + b * (x_1 - q * y_1)$;
so, $(y_1, x_1 - q * y_1)$ is a solution, QED.

GCD and contractility lemma

The preceding lemma gave us a constructive $O(log\ (a+b))$— algorithm to find some solution for diophantine equation if it exists.

Definition

Nonnegative integers a, b, such that $a+b>0$, are called coprime if $GCD(a, b) = 1$.

The following lemma is a core of proof many important facts.

Contractility lemma

Suppose that a, b, m are nonnegative integers, $m > 0$, ab is multiple of m but m is coprime with a. Then, b is a multiple of m.

Proof

As we proved earlier, there exists such integer x, y that $ax + my = 1$. Then, $abx + mby = b$. Both abx and mby are multiples of m, so b is a multiple of m, QED.

GCD and diophantine equations

Consider again the equation $ax + by = 1$ for coprime nonnegative a, b. We proved that there are such a solution (x_0, y_0). But what about other solutions?

Let (x_1, y_1) be some solution. Then, we know that $a(x_1 - x_0) + b(y_1 - y_0) = 0$. It means that $a(x_1 - x_0)$ is a multiple of b; according to contractility lemma, $x_1 - x_0$ is a multiple of b, i.e. $x_1 = x_0 + bt$ for some integer t. Then, $y_1 = y_0 - at$. For any integer t, $(x_0 + bt, y_0 - at)$ is a solution; it brings us to the following

Lemma

All possible solutions of diophantine equation $ax + by = 1$ for coprime (a, b) are $\{(x_0 + bt, y_0 - at) \mid t \in \mathbb{Z}\}$, for some solution (x_0, y_0).

GCD and fundamental theorem of arithmetics

The contractility lemma brings us to the following problem:

Fundamental theorem of arithmetics

For each integer $n \geqslant 2$, there exists and only such a pair of sequences $(p_1, p_2, \ldots, p_k)$, $(a_1, a_2, \ldots, a_k)$ of equal length called k that:

- $(p_1, p_2, \ldots, p_k)$ is an increasing sequence of prime numbers;
- $(a_1, a_2, \ldots, a_k)$ is a sequence of nonnegative integers;
- $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$.

Last representation of n is called factorization of number n.

The existence of factorization can be seen using greedy approach; the uniqueness is a consequence of the contractility lemma.

Chinese theorem of arithmetics

Prove one more important theorem of theory of numbers.

Chinese remainder theorem: shorten version

Let a, b be coprime positive integers, and $r_a \in [0, a), r_b \in [0, b)$ be some remainders by modulo a and b, correspondingly. Then, there exist the only number $c \in [0, ab)$ such that $rem_a(c) = r_a$ and $rem_b(c) = r_b$.

Proof

Consider an equation $r_a + ax = r_b + by$, for x, y as variables we are to find. This equation is equivalent to diophantine, and a, b are coprime. Then, there exist a solution (x_0, y_0). Let c' be $r_a + ax_0 = r_b + by_0$. Obviously, c' satisfies all the conditions except lying in $[0, ab)$; then, $rem_{ab}(c')$ is such a c what we need. The uniqueness can be seen from the fact that there are ab number in $[0, ab)$, and for any of ab possible pairs (r_a, r_b) there are a solution in $[0, ab)$.

Chinese theorem of arithmetics

More generalized version of the theorem can be proved.

Chinese remainder theorem: full version

Let $a_1, a_2, \ldots, a_n$ be pairwise coprime positive integers, and $r_1 \in [0, a_1), r_2 \in [0, a_2), \ldots, r_n \in [0, a_n)$ be some remainders by modulo a_1, a_2, …, a_n, correspondingly. Then, there exist the only number $c \in [0, a_1 a_2 \ldots a_n)$ such that $rem_{a_i}(c) = r_i$, $i = 1, 2, \ldots, n$.

Euler's theorem

The last question for today is Euler's theorem.

Definition

Let $n \in \mathbb{Z}_+$. Then, $\phi(n)$ is the number of such positive integers which are less than n and are coprime with n.

Three following facts are correct:

Lemma about properties of ϕ

1. if p is prime that $\phi(p) = p - 1$;
2. if p is prime and a is positive integer then $\phi(p^a) = (p - 1) * p^{a-1}$;
3. if n, m are positive coprime integers then $\phi(nm) = \phi(n) * \phi(m)$

Euler's theorem

Briefly proof last lemma. First claim is obvious. The second claim is correct because any number which is not coprime with p^a should be multiple of p, and there are exactly p^{a-1} such number on the segment $[1..p^a]$.

To prove the third claim of lemma, one can note that according to chinese remainder theorem, the remainder c of some number x by modulo nm is uniquely defined by the remainders of x by modulo n and m, and vice verse; moreover both these remainders are coprime with their moduloes if and only if c is coprime with nm.

Euler's theorem

Summarizing three facts of previous lemma, we get the following fact.

Formula of ϕ

Let $n \geqslant 2$ be an integer, and $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is its factorization. Then, $\phi(n) = (p_1 - 1) * p_1^{a_1 - 1}(p_2 - 1)^{a_2 - 1} \dots (p_k - 1) * p_k^{a_k - 1}$.

$\phi(n)$ is important because of the following

Euler's theorem

If a and m are positive coprime integers then $a^{\phi(m)} \equiv_m 1$.