

Introduction to Number Theory

Basics

Let Z be the set of integers and N be the set of natural numbers. That is,

$$\begin{aligned}Z &= \{ \dots, -2, -1, 0, 1, 2, \dots \} \\N &= \{ 0, 1, 2, \dots \}\end{aligned}$$

In the following, variables take integers by default.

Theorem. For any integer a and any integer $b > 0$, there are unique q and r such that

$$a = qb + r, 0 \leq r < b$$

Here q is the quotient and r is the remainder. If $r = 0$, that is, if b divides a , we write $b \mid a$.

If $m \mid a - b$ for $m > 0$, we write $a \equiv b \pmod{m}$, and say a is congruent to b modulo m .

Lemma. For fixed m , the relation “ $\equiv \pmod{m}$ ” is an equivalence relation, that is,

- (1) reflexive, $a \equiv a \pmod{m}$
- (2) symmetric, $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
- (3) transitive, $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

By this lemma, we can partition Z by the relation “ $\equiv \pmod{m}$ ”, or simply “ $\equiv (m)$ ”, into equivalence classes. Let $[a]$ be the equivalence class including a , that is

$$[a] = \{ b \mid b = a + km, k \in Z \}.$$

Let the operation on equivalence classes be defined by

$$[a] \pm [b] = [a \pm b]$$

$$[a] * [b] = [a * b].$$

These operations are well defined thank to the following lemma. Then the quotient algebra $Z/\equiv (m)$ forms a finite ring of order m . We express $Z/\equiv (m)$ by representatives $\{0, 1, \dots, m-1\}$. We also denote $Z/\equiv (m)$ by Z_m .

Example. Z_5 .

+	0, 1, 2, 3, 4
0	0 1 2 3 4
1	1 2 3 4 0
2	2 3 4 0 1
3	3 4 0 1 2
4	4 0 1 2 3

*	0 1 2 3 4
0	0 0 0 0 0
1	0 1 2 3 4
2	0 2 4 1 3
3	0 3 1 4 2
4	0 4 3 2 1

Lemma. Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

$$a \pm c \equiv b \pm d \pmod{m}, a * c \equiv b * d \pmod{m}.$$

Let $\gcd(a, b)$ be the greatest common divisor of $a > 0$ and $b > 0$. If $\gcd(a, b) = 1$, a and b are said to be mutually prime.

Lemma. For any $a > 0$ and $b > 0$, there exist x and y such that $d = ax + by$ where $d = \gcd(a, b)$.

From this we have,

Lemma. For $a > 0$ and $m > 0$, $\gcd(a, m) = 1$ if and only if for some x , $a * x \equiv 1 \pmod{m}$.

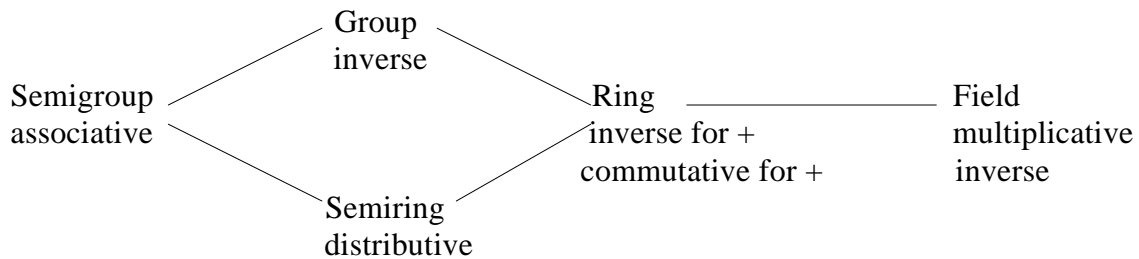
Corollary. Let $p > 0$ be a prime number. Then $Z/\equiv (p)$ or Z_p is a field.

Note. In a field F , any $a \in F$ has a multiplicative inverse a^{-1} , that is, $a * a^{-1} = 1$.

For algebraic systems, we have the following axioms.

Associative	$a(bc) = (ab)c$
Commutative	$ab = ba$
Unit element	$1a = a1 = a$
Inverse	$a a^{-1} = a^{-1} a = 1$
Distributive	$a(b+c) = ab + ac, (a+b)c = ac + bc.$

We have weaker systems to a stronger systems from left to right with additional axioms.



For $m > 0$, the number of integers between 1 and m which are mutually prime to m is called the Euler (totient) function, denoted by $\phi(m)$. That is,

$$\phi(m) = \{ a \in \mathbb{Z}_m \mid \gcd(a, m) = 1 \}.$$

$$\phi(1) = 1$$

$$\phi(2) = 1$$

$$\phi(3) = 2, \{1, 2\}$$

$$\phi(4) = 2, \{1, 3\}$$

$$\phi(5) = 4, \{1, 2, 3, 4\}$$

$$\phi(6) = 2, \{1, 5\}.$$

Let \mathbb{Z}_m^* be the set defined by

$$\mathbb{Z}_m^* = \{ a \in \mathbb{Z}_m \mid \gcd(a, m) = 1 \}.$$

Then the size of this set is $\phi(m)$. We have a few theorems.

Theorem. \mathbb{Z}_m forms a group under multiplication. The unit is 1.

Theorem. For any finite group such that the order is n , $x^n = 1$.

Proof. For $x \in G$, we generate $1, x, x^2, \dots$. Since G is finite we must have $x^a = x^b$ for some a and b such that $1 \leq a < b \leq n$. Then for $m = b - a$ such that $1 \leq m \leq n-1$, $x^m = 1$. The subset $\{1, x, \dots, x^{m-1}\}$ forms a subgroup of G . According to Lagrange's theorem, $|H|$ divides $|G|$, that is $m \mid n$. Thus $x^n = x^{km} = 1$ for some k .

Definition. Let H be a subgroup of group G . The right coset Ha of H in G specified by a is defined by

$$Ha = \{ ha \mid h \in H \}.$$

Congruence modulo H is defined by

$$a \equiv b \pmod{H} \Leftrightarrow ab^{-1} \in H.$$

Theorem. Congruence modulo H is an equivalence relation.

Lemma. $|H| = |Ha|$.

Proof. The mapping $f : H \rightarrow Ha$ defined by $f(h) = ha$ is a bijection (one-to-one and onto mapping).

Definition. The number of equivalence classes is the index denoted by $[G:H]$.

From this we see that $|G| = |H|[G:H]$. Hence,

Theorem (Lagrange). For a group and its subgroup H , $|H| \mid |G|$.

Since $|Z_m^*| = \varphi(m)$, and for any $a \in Z_m^*$, $a^{\varphi(m)} = 1$, we have the following.

Theorem (Fermat). For any $a \in Z$ and $m > 0$, if $\gcd(a, m) = 1$,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

When $m = p$ is a prime in particular, and $\gcd(a, p) = 1$,

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

Lemma. For $m > 0$, let the factoring of m be given by

$$m = (p_1^{e(1)})(p_2^{e(2)}) \dots (p_r^{e(r)}).$$

Then

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{e(1)})\varphi(p_2^{e(2)})\dots\varphi(p_r^{e(r)}) \\ &= m(1-1/p_1)(1-1/p_2)\dots(1-1/p_r). \end{aligned}$$

In particular

$$\varphi(p^e) = p^{(e-1)}(p-1), \quad \varphi(2p^e) = p^{(e-1)}(p-1).$$

Definition. For mutually prime a and $m > 0$, and $e > 0$, let $a^e \equiv 1 \pmod{m}$ and for any e' such that $0 < e' < e$, $\text{not}(a^{e'} \equiv 1 \pmod{m})$. Then e is said to be the order of a modulo m .

Lemma. Let e be the order of $a \pmod{m}$ for $m > 0$. If $a^f \equiv 1 \pmod{m}$ for $f > 0$, then $e \mid f$.

Proof. There are q and r such that

$$f = qe + r, \text{ and } 0 \leq r < e.$$

If $r \neq 0$, we have

$$a^f \equiv a^{(qe+r)} \equiv a^{qe} a^r \equiv (a^e)^q a^r \equiv a^r \pmod{m}.$$

From this we have $a^r \equiv 1 \pmod{m}$, which contradicts the way we defined e .

In general, Z_m^* is a finite commutative group. If it is a cyclic group in addition, that is, for some a ,

$$Z^* = \{1, a, \dots, a^{\phi(m)-1}\},$$

then a is said to be a primitive root of m . In other words, a is a primitive root of m if the order of a modulo m is $\phi(m)$. Further in other words, a is a primitive root of m if

- (1) $a^{\phi(m)} \equiv 1 \pmod{m}$, and
- (2) for any r such that $0 < r < \phi(m)$, $a^r \not\equiv 1$.

Example. For 7, $\phi(7) = 6$. We enumerate the powers of some integers.

- 1, 2, 4, 1. 2 is not a primitive root.
- 1, 3, 2, 6, 4, 5, 1. 3 is a primitive root.

For 8, $\phi(8) = 4$, and there is no primitive root.

Theorem. There are primitive roots only for $m = 2, 4, p^e, 2p^e$ for prime $p > 2$.

Evaluation of x^n

In stead of performing $n-1$ multiplications, we can compute x^n in $2\lfloor \log n \rfloor$ multiplications.

```
n = (b(m-1)...b(1)b(0)) : binary expression of n, e.g., 5 = (101)
y:=1;
for i:=m-1 downto 0 do begin
  y:=y*y;
  if b(i)=1 then y:=y*x
end.
```

This method is called “repeated squaring”.

Theory of Fibonacci Numbers

The Fibonacci sequence is defined by

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \dots$$

That is

$$x(0) = 0, \quad x(1) = 1,$$

$$x(n+2) = x(n+1) + x(n), \quad (n \geq 0).$$

A homogeneous difference equation is defined by

$$x(0)=b(0), \quad x(1)=b(1), \quad \dots, \quad x(k-1)=b(k-1),$$

$$x(n+k) = a(1)x(n+k-1) + \dots + a(k)x(n).$$

The general solution is given by

$$x(n) = c(1)r(1)^n + \dots + c(k)r(k)^n,$$

where $r(i)$ is the i -th root of the characteristic equation

$$r^k - a(1)r^{k-1} - \dots - a(k) = 0.$$

Here we assume that all the k roots of the characteristic equation are different. The constants $c(1), \dots, c(k)$ are determined by the k initial conditions.

For the Fibonacci sequence, the characteristic equation is

$$r^2 - r - 1 = 0,$$

the solution of which is given by

$$r(1) = (1 + \sqrt{5})/2, r(2) = (1 - \sqrt{5})/2.$$

Therefore the general solution becomes as follows.

$$x(n) = c(1)r(1)^n + c(2)r(2)^n.$$

From the initial condition, we have the following simultaneous equation.

$$\begin{aligned} c(1) + c(2) &= 0 \\ c(1)(1 + \sqrt{5})/2 + c(2)(1 - \sqrt{5})/2 &= 1. \end{aligned}$$

From this we have

$$c(1) = 1/\sqrt{5}, c(2) = -1/\sqrt{5}.$$

Thus the n -th Fibonacci number $x(n)$ is given by

$$x(n) = (1/\sqrt{5})((1 + \sqrt{5})/2)^n - (1/\sqrt{5})((1 - \sqrt{5})/2)^n$$

The growth rate of $x(n)$ is measured by the first term which is dominant, that is, an exponential function of $r(1) = 1.618..$

With a primitive approach it takes $O(n)$ time to compute $x(n)$. The following algorithm computes $x(n)$ in $O(\log n)$ time, which is based on repeated squaring. The difference equation is expressed by vectors and a matrix as

$$(x(0) \ x(1)) = (0, 1)$$

$$(x(n-1) \ x(n)) = (x(n-2) \ x(n-1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Then we have

$$(x(n-1) \ x(n)) = (x(0) \ x(1)) \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{(n-1)}$$

Hence we can use the fast algorithm to evaluate x^n based on repeated squaring as applied to a matrix.

Euclidean Algorithm for Greatest Common Divisors

We compute the greatest common divisor of a and $b > 0$, $\gcd(a, b)$. Let us divide a by b , yielding the following equation for the quotient q and remainder r .

$$a = bq + r, \quad 0 \leq r < b$$

We observe that $\gcd(a, b) = \gcd(b, r)$. The important point here is that the problem of $\gcd(a, b)$ has been reduced to that of $\gcd(b, r)$. Then we can repeat this process as shown below.

Let $a = r(0)$, $b = r(1)$, $q = q(1)$ and $r = r(2)$ in the above. We repeat division as follows:

$$\begin{aligned} a &= b \cdot q(1) + r(2), & 0 \leq r(2) < b \\ b &= r(2) \cdot q(2) + r(3), & 0 \leq r(3) < r(2) \\ &\dots \\ r(i-1) &= r(i) \cdot q(i) + r(i+1), & 0 \leq r(i+1) < r(i) \\ &\dots \\ r(n) &= r(n) \cdot q(n) + r(n+1), & r(n+1) = 0 \end{aligned}$$

That is we finish at the n -th division.

Theorem. $\gcd(a, b) = r(n)$.

Proof. Theorem follows from

$$\gcd(a, b) = \gcd(b, r(2)) = \gcd(r(2), r(3)) = \dots = \gcd(r(n), r(n+1)) = \gcd(r(n), 0) = r(n).$$

Example. $a = 91$, $b = 35$.

$$\begin{aligned} 91 &= (35)2 + 21, & q(1) &= 2, & r(2) &= 21 \\ 35 &= (21)1 + 14, & q(2) &= 1, & r(3) &= 14 \\ 21 &= (14)1 + 7, & q(3) &= 1, & r(4) &= 7 \\ 14 &= (7)2 + 0, & q(4) &= 2, & r(5) &= 0 \end{aligned}$$

$$\gcd(91, 35) = 7.$$

Sequences $\{a(i)\}$ and $\{b(i)\}$ are defined as follows:

$$\begin{aligned} a(0) &= 0, & a(1) &= 1, & a(i) &= a(i-2) - q(i-1)a(i-1) \\ b(0) &= 1, & b(1) &= 0, & b(i) &= b(i-2) - q(i-1)b(i-1). \end{aligned}$$

Theorem. For any $i > 0$, $a*b(i) + b*a(i) = r(i)$.

Proof. Induction on I .

$$\begin{aligned} i=0, & \quad a*b(0) + b*a(0) = a = r(0) \\ i=1, & \quad a*b(1) + b*a(1) = b = r(1) \end{aligned}$$

Assume theorem is true for up to i . Then

$$\begin{aligned} a*b(i+1) + b*a(i+1) &= a(b(i-1) - q(i)b(i)) + b(a(i-1) - q(i)a(i)) \\ &= a*b(i-1) + b*a(i-1) - q(i)(a*b(i) + b*a(i)) \\ &= r(i-1) - q(i)r(i) \\ &= r(i-1). \end{aligned}$$

Let $i = n$ in the theorem. Then we have

$$a*b(n) + b*a(n) = \gcd(a, b).$$

That is we can find an integer solution (x, y) that satisfies the equation

$$ax + by = \gcd(a, b).$$

Example. For the previous example of $a = 91$ and $b = 75$. We have

$$\begin{aligned} a(2) &= -2, & a(3) &= 3, & a(4) &= -5 \\ b(2) &= 1, & b(3) &= -1, & b(4) &= 2. \end{aligned}$$

From this we have the solution $(x=1, y=-5)$ for $91x + 35y = 7$.

In the case of $\gcd(a, b) = 1$, the solution for $ax + by = 1$ has the following meaning.

$$x = a^{(-1)} \bmod b, \quad y = b^{(-1)} \bmod a.$$

Example. If we divide both sides of the previous example, we have $13x + 5y = 1$. Since 13 and 5 are mutually prime, each has a multiplicative inverse modulo each other. For example, $5^{(-1)} = -5$. To get a positive multiplicative inverse, we have $-5 + 13 = 8$.

The following procedure computes the greatest common divisor of a and b together with the sequences $\{a(i)\}$ and $\{b(i)\}$.

1. $w_0 := a; w_1 := b;$
 2. $u_0 := 0; u_1 := 1;$
 3. $v_0 := 1; v_1 := 0;$
 4. while $w_1 > 0$ do begin
 5. $q := w_0 \text{ div } w_1;$
 6. $w_2 := w_0 - q * w_1; w_0 := w_1; w_1 := w_2;$
 7. $u_2 := u_0 - q * u_1; u_0 := u_1; u_1 := u_2;$
 8. $v_2 := v_0 - q * v_1; v_0 := v_1; v_1 := v_2$
 9. end
- { $w_0 = \text{gcd}(a, b), u_0 = b^{-1} \text{ mod } a, v_0 = a^{-1} \text{ mod } b$ }.

If u_0 or v_0 is negative at the end, we can add a or b respectively to get a positive inverse.

Analysis of Euclidean algorithm

Let $D(a, b)$ be the number of divisions performed in the algorithm. Let $f(n)$ be defined by

$$f(0) = 1, f(1) = 2,$$

$$f(n) = f(n-1) + f(n-2), \quad n \geq 2$$

That is, $f(n) = x(n+2)$ where $x(n)$ is the n -th Fibonacci number. Thus

$$f(n) = (1/\sqrt{5})((1+\sqrt{5})/2)^{n+2} - (1/\sqrt{5})((1-\sqrt{5})/2)^{n+2}.$$

Lemma.

$$\text{For all } n \geq 0, \quad f(n+1) \leq 2 * f(n), \quad f(n) \geq ((1+\sqrt{5})/2)^n$$

Theorem.

$$\text{For } 0 \leq b \leq a \leq f(n), \quad D(a, b) \leq n \text{ for } n \geq 0.$$

Proof. Induction on n .

Basis. $n=1$. Since $f(1) = 2$, we classify a and b such that $0 \leq b \leq a \leq 2$ into a few cases.

When $b=0$, $D(a, b)=0$. When $b=1$, $D(a, b)=1$. When $a=b=2$, $D(a, b)=1$.

Induction step. Assume theorem is true for up to n , and assume $0 \leq b \leq a \leq f(n+1)$. The we classify the situation into two cases.

(1) $b \leq f(n)$. When $b=0$, $D(a, b)=0$. Let $b > 0$. Since $0 \leq r(2) < b$, we have $D(a, r(2)) \leq n$ from the inductive hypothesis. Thus $D(a, b) = D(b, r(2)) + 1 \leq n+1$.

(2) $f(n) < b$. From lemma, we have $a < 2b$. Thus

$$r(2) = a \text{ mod } b = a - b < f(n+1) - f(n) = f(n+1).$$

When $r(2) = 0$, $D(a, b) = 1$. When $r(2) > 0$, we have $0 \leq r(3) < r(2) < f(n-1)$. From the inductive hypothesis,

$$D(a, b) = D(b, r(2)) + 1 = D(R(2), r(3)) + 2 < n-1 + 2 = n+1.$$

Now let a and b be positive integers expressed by up to k bits. Then we have $0 <= b <= a <= 2^k - 1$. Let $\phi = (1 + \sqrt{5})/2$ and $n = \lceil k \log_2 \phi \rceil = 1.44k$. Then from $\phi^k >= 2^k$ and lemma, where ϕ is the first root of the characteristic equation, we have

$$0 <= b <= a < \phi^n <= f(n).$$

From theorem, we have $D(a, b) <= n$. That is, the number of divisions is not more than $1.44k$. Let the time for division of two k -bit numbers be $O(D(k))$. Then the Euclidean algorithm runs in $O(kD(k))$ time. If we use the simple $O(k^2)$ algorithm for division, the Euclidean algorithm runs in $O(k^3)$ time.

Quadratic residues and probabilistic primality test

Let $m > 0$ and a such that $\gcd(a, m) = 1$ be given. If equation $x^2 \equiv a \pmod{m}$ has an integer solution, we say a is a quadratic residue modulo m , and otherwise a is said to be a quadratic non-residue modulo m . From this definition, we have if $a \equiv b \pmod{m}$,

$$a \text{ is a quadratic residue modulo } m \Leftrightarrow b \text{ is a quadratic residue modulo } m.$$

If c is an integer solution for $x^2 \equiv a \pmod{m}$, then any d such that $d \equiv c \pmod{m}$ is also a solution. Thus we can only consider the range $1, 2, \dots, m-1$ for residues and solutions.

Theorem A. Let $p > 2$ be a prime. Any $a >= 0$ such that $\gcd(a, p) = 1$ is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. If a such that $\gcd(a, p) = 1$ is a quadratic non-residue modulo p , then we have $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Proof. For a such that $\gcd(a, p) = 1$, suppose a is a quadratic residue modulo p . For solution c for equation $x^2 \equiv a \pmod{p}$, obviously we have $\gcd(c, p) = 1$. Thus raising both sides of $a \equiv c^2 \pmod{p}$ to the $(p-1)/2$ -th power, we have $a^{(p-1)/2} \equiv c^{p-1} \equiv 1 \pmod{p}$ from Fermat's theorem.

Conversely suppose $a^{(p-1)/2} \equiv 1 \pmod{p}$. Since $\gcd(a, p) = 1$, we have a primitive root g such that $a \equiv g^r \pmod{p}$ for some r . By raising both sides to the $(p-1)/2$ -th power, we have $g^{r(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$. Since the order of $g \pmod{p}$ is $p-1$, and from the property of the order, $p-1$ must divide $r(p-1)/2$. Thus $r/2$ must be an integer. That is, $r = 2k$ for some integer k . From this $g^{2k} \equiv a \pmod{p}$ and a is a quadratic residue modulo p .

The latter half of the theorem can be seen in the following way. From Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$. By factoring, we have

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}.$$

From the former half of the theorem, if a is not a quadratic non-residue modulo p , $a^{(p-1)/2}$ can not be divided by p . Thus we must have $a^{(p-1)/2} + 1 \equiv 0 \pmod{p}$.

Theorem B. Let $p > 2$ be a prime. Let $\gcd(a, p) = \gcd(b, p) = 1$. If both of a and b are quadratic residues or non-residues modulo p , then ab is a quadratic residue. If one is a residue and the other is a non-residue, then ab is a non-residue.

Proof. If $a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv 1 \pmod{p}$, or $a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv -1 \pmod{p}$, then $(ab)^{(p-1)/2} \equiv 1 \pmod{p}$. Hence from the previous theorem, if both are residues or non-residues, ab is a residue. If $a^{(p-1)/2} \equiv 1 \pmod{p}$ and $b^{(p-1)/2} \equiv -1 \pmod{p}$, $(ab)^{(p-1)/2} \equiv -1 \pmod{p}$, and hence ab is a non-residue.

For a prime $p > 2$, we define the Legendre symbol $L(a, p)$ by

$$L(a, p) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a non-residue.} \end{cases}$$

Theorem A says that for a prime $p > 2$ and a such that $\gcd(a, p) = 1$,

$$L(a, p) \equiv a^{(p-1)/2} \pmod{p}.$$

From previous discussions and Theorem B, we have

$$\begin{aligned} a \equiv b \pmod{p} &\Rightarrow L(a, p) = L(b, p) \\ L(ab, p) &= L(a, p)L(b, p). \end{aligned}$$

Next we define the Jacobi symbol $J(a, m)$ for an odd number $m > 2$ and a such that $\gcd(a, m) = 1$ by

$$J(a, m) = L(a, p_1)L(a, p_2)\dots L(a, p_n),$$

where $m = p_1 * p_2 * \dots * p_n$ is a factorization of m into primes p_1, p_2, \dots, p_n .

For odd m and $n > 2$ such that $\gcd(a, m) = \gcd(b, m) = \gcd(m, n) = 1$, we have:

$$(1) J(1, m) = 1$$

$$(2) \begin{aligned} a \equiv b \pmod{m} &\Rightarrow J(a, m) = J(b, m) \\ J(a, m) &= J(a \pmod{m}, m) \end{aligned}$$

$$(3) J(ab, m) = J(a, m)J(b, m)$$

$$(4) J(2, m) = (-1)^{(m^2 - 1)/8}$$

$$(5) J(m, n) = J(n, m)(-1)^{((m-1)(n-1)/4)}.$$

Since the Legendre symbol is a special case of the Jacobi symbol, the above five properties hold for the Legendre symbol as well.

If $m > 2$ is a prime, we have $J(a, m) = L(a, m)$, and hence

$$J(a, m) \equiv a^{(m-1)/2} \pmod{m}.$$

If for an odd number $m > 2$ and some a ($0 < a < m$), the above formula does not hold, we can judge that m is not a prime. This is called the Euler criterion for non-primality. If the above formula holds, however, we can not judge that m is a prime.

Let us judge that m is a prime if the formula holds for a random a such that $0 < a < m$ and $\gcd(a, m) = 1$. If m is a prime, this judgement is correct. In other words, if the formula does not hold, we can judge that m is a composite. If the number of a 's such that the formula holds for a composite m is not greater than $q(m-1)$ for $0 < q < 1$, the probability of wrong judgement is not greater than q . Let us test the formula k times for random a 's. If the formula does not hold before the end of k tests, we halt and judge that m is a composite. Then the probability of wrong judgement when we declare m is a prime after k successful tests is not greater than q^k . Solovay and Strassen (1977) showed that $q \leq 1/2$ as shown in the following theorem.

Let m be an odd composite number. Let formulas (1) and (2) be defined for $0 < a < n$ by

- (1) $\gcd(a, n) = 1$
- (2) $\gcd(a, n) = 1$ and $a^{(n-1)/2} \equiv J(a, n) \pmod{n}$.

Let $G(n)$ be the set of a such that a satisfies (1). Let $H(n)$ be the set of a such that a satisfies (2).

Theorem (Solovay and Strassen). $H(n)$ is a proper subgroup of $G(n)$. Therefore $|H(n)| \leq |G(n)|/2$

Proof. See R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," SIAM Jour. on Computing, vol. 6, no. 1 (1977), pp. 84-85 and vol. 7, no. 1 (1978) p. 118.

Thus by the Euler criterion, we have $q = 1/2$ for probabilistic primality test. Now we proceed to an algorithm for computing formula (2).

To compute $a^{(n-1)/2} \pmod{n}$, we can use repeated squaring with mod n operation inserted after each multiplication. Thus, if we use a primitive $O(k^2)$ method for multiplication and division with $k = \lceil \log_2 n \rceil$ bits, we can compute the above in $O(k^3)$ time. Now $J(a, n)$ can be computed by the following algorithm.

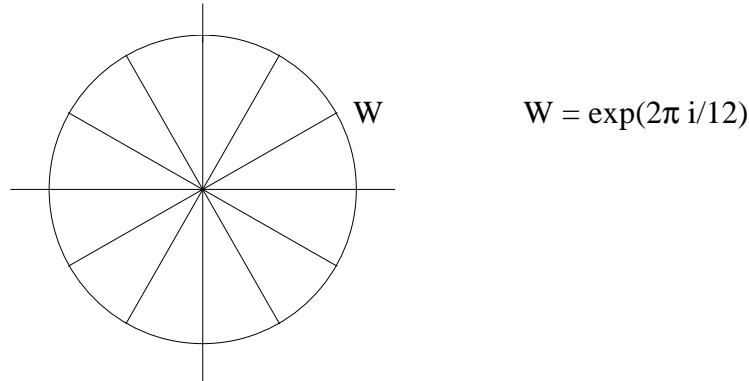
1. function $J(a, m)$
2. begin
3. if $n=0$ then report "a is composite"
4. else if $a=1$ then $J:=1$
5. else if a is even then $J := J(a/2, n) * (-1)^{((n^2-1)/8)}$
6. else $J := J(n \bmod a, a) * (-1)^{((a-1)(n-1)/4)}$
7. end

Line 6 is a part of the Euclidean algorithm, and hence the time for this algorithm is $O(k^3)$. Thus for one a , the Euler criterion takes $O(n^3)$ time.

Introduction to Fast Fourier Transform (FFT)

Basics

Let W be the principal n -th root of 1 in the complex plane, that is, $W = \exp(2\pi i/n)$, where $i = \sqrt{-1}$. See below.



Then we have

$$(1) \quad W^n = 1$$

$$(2) \quad \sum_{j=0}^{n-1} W^{kj} = 0 \quad (k = 0, \dots, n-1)$$

The discrete Fourier transform (DFT) of the sequence of complex numbers $X(j)$ ($j=0, \dots, n-1$) is defined by the sequence $y(k)$ ($k=0, \dots, n-1$) where

$$y(k) = \sum_{j=0}^{n-1} X(j)W^{kj}.$$

The inverse discrete Fourier transform (IDFT) of sequence $\{y(k)\}$ is defined by the sequence $z(l)$ where

$$z(l) = (1/n) \sum_{k=0}^{n-1} y(k)W^{-lk} \quad (l = 0, \dots, n-1)$$

Theorem. $x(j) = z(j)$ for $j = 0, \dots, n-1$. That is,

$$x(j) = (1/n) \sum_{k=0}^{n-1} y(k)W^{-kj}$$

Proof. Let $\mathbf{x} = (x(0), \dots, x(n-1))$, $\mathbf{y} = (y(0), \dots, y(n-1))$, and $\mathbf{z} = (z(0), \dots, z(n-1))$. Let matrices A and B be defined as $A = (a(i,j))$ and $B = (b(i,j))$ where

$$a(i,j) = W^{ij}, \quad b(i,j) = (1/n)W^{-ij}$$

Then we have $\mathbf{y} = \mathbf{x}\mathbf{A}$ and $\mathbf{z} = \mathbf{y}\mathbf{B}$. It suffices to show that $\mathbf{B} = \mathbf{A}^{-1}$. Let $\mathbf{C} = \mathbf{B}\mathbf{A}$. Then we have

$$c(i,j) = (1/n) \sum_{[k=0 \text{ to } n-1]} W^{(j-i)k}.$$

When $i = j$, $W^{(j-i)k} = 1$, so $c(i,i) = 1$. When $i \neq j$, let $l = j - i$. Then from (2), we have

$$\sum_{[k=0 \text{ to } n-1]} W^{lk} = 0.$$

Thus $c(i,j) = 0$ for $i \neq j$.

From this we see that IDFT is indeed an inverse transform.

The convolution of two sequences $(x(0), \dots, x(n-1))$ and $(y(0), \dots, y(n-1))$ is defined by $(z(0), \dots, z(2n-1))$ where

$$z(j) = \sum_{[k=0 \text{ to } n]} x(j-k)y(k) \quad (j = 0, \dots, 2n-1).$$

Here we assume $x(k) = 0$ for $k < 0$ and $k \geq n$. From this definition, it is clear that $z(2n-1) = 0$, which is added to the sequence to adjust to the length of $2n$.

Theorem. Let the DFTs of $(x(0), \dots, x(n-1), 0, \dots, 0)$ and $(y(0), \dots, y(n-1), 0, \dots, 0)$ of length $2n$ each be $(x'(0), \dots, x'(2n))$ and $(y'(0), \dots, y'(2n))$. The convolution $(z(0), \dots, z(2n))$ defined above is equal to the IDFT of $(x'(0)y'(0), \dots, x'(2n-1)y'(2n-1))$.

Proof. Let the DFT of $(z(0), \dots, z(2n-1))$ be $(z'(0), \dots, z'(2n-1))$. Then

$$\begin{aligned} z'(l) &= \sum_{[j=0 \text{ to } n-1]} \sum_{[k=0 \text{ to } n-1]} x(j-k)y(k)W^{lj} \\ &= \sum_{[k=0 \text{ to } n-1]} \sum_{[i=k \text{ to } 2n-1-k]} x(i)y(k)W^{l(i+k)}, \quad \text{where } i = j-k \\ &= \sum_{[k=0 \text{ to } n-1]} \sum_{[j=0 \text{ to } n-1]} x(i)y(k)W^{l(i+k)} \\ &= \sum_{[i=0 \text{ to } n-1]} x(i)W^{li} \sum_{[k=0 \text{ to } n-1]} y(k)W^{lk}. \end{aligned}$$

On the other hand, for $(x'(0), \dots, x'(2n-1))$ and $(y'(0), \dots, y'(2n-1))$ we have

$$x'(l) = \sum_{[k=0 \text{ to } 2n-1]} x(k)W^{lk} = \sum_{[k=0 \text{ to } n-1]} x(k)W^{lk} \quad (l = 0, \dots, 2n-1)$$

$$y'(l) = \sum_{[k=0 \text{ to } 2n-1]} y(k)W^{lk} = \sum_{[k=0 \text{ to } n-1]} y(k)W^{lk} \quad (l = 0, \dots, 2n-1)$$

Thus we have $z'(l) = x'(l)y'(l)$ ($l = 0, \dots, 2n-1$).

Next let us consider multiplying two polynomials

$$\begin{aligned} f(z) &= x(0) + x(1)z + \dots + x(n-1)z^{n-1} \\ g(z) &= y(0) + y(1)z + \dots + y(n-1)z^{n-1}. \end{aligned}$$

The product is given by

$$\begin{aligned} f(z)g(z) &= x(0)y(0) + (x(0)y(1) + x(1)y(0))z \\ &\quad + \dots \\ &\quad + (x(0)y(k) + x(1)y(k-1) + \dots + x(k)y(0))z^k \\ &\quad + \dots \\ &\quad + x(n-1)y(n-1)z^{2n-2} + 0z^{2n-1}. \end{aligned}$$

That is, the k -th coefficient is the convolution $z(k)$. Next consider multiplying two multi-precision binary numbers $(a(n-1)\dots a(1)a(0))$ and $(b(n-1)\dots b(1)b(0))$. As we see from the following figure, we can modify the convolution computation for multiplication. Let the binary form of the product be $(c(2n-1)\dots c(1)c(0))$.

$$\begin{array}{rcccc} & & a(n-1) & \dots & a(1) & a(0) \\ & & b(n-1) & \dots & b(1) & b(0) \\ \hline & & a(n-1)b(0) & & a(1)b(0) & a(0)b(0) \\ & a(n-1)b(1) & & & a(0)b(1) & \\ \hline a(n-1)b(n-1) & & a(0)b(n-1) & & & \\ \hline c(2n-1) & c(2n-2) & & c(n-1) & c(1) & c(0) \end{array}$$

Here $c(i)$ ($i=0, \dots, 2n-1$) can be computed in the following way. Let $d(i)$ ($i=0, \dots, 2n-1$) be the convolution of $(a(0), \dots, a(n-1))$ and $(b(0), \dots, b(n-1))$.

```

c(0) := d(0);
for i:= 0 to 2n-1 do begin
  c(i+1) := d(i+1) + c(i) div 2;
  c(i) := c(i) mod 2
end.

```

If we go through FFT, all computations described in this section can be done in $O(n \log n)$ time, whereas straightforward methods take $O(n^2)$ time.