

Number Theory

Divisibility: We use the notation

$$a|b$$

to mean “ a divides b ” exactly. So $3|6$, $15|45$ etc. while the symbol \nmid means “does not divide evenly”, so $5 \nmid 8$, and $12 \nmid 16$ etc. Note that $a|0$ holds for all a , i.e. zero is divisible by everything.

Greatest Common Divisor The greatest common divisor (GCD) of a and b is defined as:

$$\gcd(a, b) = \max\{g : g|a \text{ and } g|b\}$$

So for example, $\gcd(20,65) = 5$, $\gcd(19,38) = 19$, $\gcd(5,12) = 1$ etc.

Lowest Common Multiple The lowest common multiple (LCM) of a and b is defined as:

$$\text{lcm}(a, b) = \min\{l : a|l \text{ and } b|l\}$$

So for example, $\text{lcm}(20,30) = 60$, $\text{lcm}(19,38) = 38$, $\text{lcm}(5,12) = 60$ etc.

Lemma The GCD $g(a, b)$ and LCM $l(a, b)$ satisfy:

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

Factorization

A *prime* $p > 1$ is a number with no divisors except for p and 1.

Other numbers are called *composite*. Composite numbers have unique factorizations as powers of primes. That is, every number (primes too) n can be uniquely expressed as a product:

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

For example $84 = 2^2 \times 3 \times 7$.

Division Theorem

Given a dividend a and a divisor b , there are unique integers q and $r \in [0, \dots, b - 1]$ such that:

$$a = qb + r$$

and we write $q = a \text{ div } b$ for the quotient and $r = a \text{ mod } b$ for the remainder.

Note that $b|a$ is equivalent to $a \text{ mod } b = 0$

Euclid's Algorithm

Euclid's algorithm is a method for efficiently computing GCDs. Its based on the observation that if

$$g = \gcd(a, b)$$

then

$$r = a \bmod b = a - qb$$

is also divisible by g because both a and b are. By repeatedly taking remainders, we can reduce the size of the numbers whose gcd we are computing, until eventually we get the gcd itself.

$$\begin{aligned} r_1 &= a \\ r_2 &= b \\ r_3 &= r_1 \bmod r_2 \\ r_4 &= r_2 \bmod r_3 \\ &\vdots \\ r_k &= r_{k-2} \bmod r_{k-1} \\ 0 &= r_{k-1} \bmod r_k \end{aligned}$$

Notice first that since a remainder (r_k) is always smaller than a divisor (r_{k-1}), this sequence is decreasing, except perhaps for the first two elements. It is easy to show that the common divisors of any pair of consecutive r_i 's are the same. That is, the number g is a common divisor of r_j and r_{j-1} if and only if it is a common divisor of r_j and r_{j+1} . So the gcd g is a divisor of all the elements in the sequence. Since the sequence is strictly decreasing, we get smaller and smaller multiples of g , and must eventually get zero. The element before is a multiple of g , and it must exactly divide the element before it. Since those two elements have gcd g , the penultimate element must be g . So we return the last non-zero element $g = r_k$ from the remainder sequence as the gcd.

Euclid's algorithm is fast. The remainder sequence is bounded by a decreasing geometric series, and we have that:

Lemma Euclid's algorithm takes $O(\log a)$ steps to compute $\gcd(a, b)$.

Extended Euclid

We can get more information from Euclid's algorithm by doing some book-keeping. In particular, if $g = \gcd(a, b)$, the extended Euclid algorithm computes x, y such that

$$g = ax + by$$

This follows easily by induction. Suppose that we can express

$$r_i = x_i a + y_i b$$

Clearly this is true for $i = 1, 2$ with the (x_i, y_i) pairs $(1, 0)$ and $(0, 1)$ respectively. Suppose its true

for i and $i + 1$. We prove it holds for $i + 2$. Now

$$r_{i+2} = r_i - q_{i+2}r_{i+1} = (ax_i + by_i) + q_{i+2}(ax_{i+1} + by_{i+1}) = a(x_i + q_{i+2}x_{i+1}) + b(y_i + q_{i+2}y_{i+1})$$

Which proves the identity we were looking for and establishes the inductive formulae:

$$\begin{aligned} x_{i+2} &= (x_i + q_{i+2}x_{i+1}) \\ y_{i+2} &= (y_i + q_{i+2}y_{i+1}) \end{aligned}$$

And if r_k is the last remainder in the sequence, we see that

$$g = \gcd(a, b) = r_k = x_k a + y_k b$$

To implement extended Euclid, simply initialize (x_1, y_1) and (x_2, y_2) to $(1, 0)$ and $(0, 1)$ respectively, and use the above inductive formula as the remainders are computed.

The extended Euclid algorithm has a number of applications. One of the most important is for computing inverses mod n . Suppose we apply extended Euclid to two elements a and n whose gcd is 1. Then extended Euclid will compute x and y satisfying:

$$1 = ax + ny$$

If we reduce mod n , we get that $1 = ax \pmod{n}$, or in other words, x is the inverse of $a \pmod{n}$.

The Multiplicative Group \mathbb{Z}_n^*

Recall that a group is a set with a binary operator defined on it which satisfies closure under the operator, associativity, identity and inverse. We can define a set which is closed under multiplication mod n :

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$$

and then \mathbb{Z}_n^* will be a group under multiplication mod n . The identity is 1, and associativity follows from associativity of multiplication. You can check yourself that it satisfies closure. Inverse follows because we can use extended Euclid to compute inverses as above for any elements that satisfy $\gcd(a, n) = 1$.

Relative Primality We say “ a is relatively prime to n ” whenever $\gcd(a, n) = 1$.

Note that if n is prime, then all the elements in \mathbb{Z}_n are relatively prime to n except for 0. Thus $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$ for prime n .

Finite Fields

A *field* F is a set D which has two operators $+$, $*$ defined on it. There are two groups, an additive group $(D, +)$ and a multiplicative group $(D^*, *)$, where $D^* = D - \{0\}$.

Example: The set \mathbb{Z}_p of integers mod p is a field when p is a prime. The $+$ operator is addition mod p and the $*$ operator is multiplication mod p .

If n is not prime, \mathbb{Z}_n is not a field. The set \mathbb{Z}_n contains factors of n , and they do not have multiplicative inverses mod n . So \mathbb{Z}_n^* is not a group under multiplication mod n .

Euler's Totient Function

The Euler Totient function $\phi(n)$ counts the number of elements in the multiplicative group \mathbb{Z}_n^* ,

$$\phi(n) = |\mathbb{Z}_n^*|$$

We already know that for a prime p , $\phi(p) = p - 1$. For a general n , the totient function depends on the prime factorization of n . Suppose

$$n = p_1^{k_1} \cdots p_t^{k_t}$$

then the value of the totient function is

$$\phi(n) = \prod_{i=1}^t p_i^{k_i-1} (p_i - 1) = n \prod_{i=1}^t (1 - 1/p_i)$$

We won't give a proof here, but it is not hard to derive it using the inclusion/exclusion principle. An *intuitive* proof is that the totient function counts numbers that are not divisible by any of the p_i 's. The probability that a number is *not* divisible by p_i is $1 - 1/p_i$, and we claim that those probabilities are independent. So the number of elements that are not divisible by any of the p_i 's is

$$n \prod_{i=1}^t (1 - 1/p_i)$$

Next we state two theorems which are very important in number theory and cryptography:

Euler's Theorem For any element $a \in \mathbb{Z}_n^*$,

$$a^{\phi(n)} = 1 \pmod{n}$$

For a prime p , recall that $\phi(p) = p - 1$. Making that substitution gives us Fermat's theorem (not the famous one):

Fermat's Theorem For a prime p and any element $a \in \mathbb{Z}_p^*$,

$$a^{(p-1)} = 1 \pmod{p}$$

You should recall a fast powering algorithm from CS170. It allows you to compute

$$a^{(p-1)} \pmod{p}$$

in time which is polynomial in $\log p$.

Generators

A generator of a group G is an element whose powers comprise the entire group G . If a group has a generator, then it is said to be a **cyclic** group. One easy observation we can make is that if

the order of G is a prime $p > 1$, then G is a cyclic group. Why? In fact every element except the identity is a generator in that case.

In particular, for every prime p , the additive group $(\mathbb{Z}_p, +)$ is cyclic. Its order is p , and every element except 0 generates the whole group.

For multiplicative groups, we don't get very far with the above observation. For prime p , the order of (\mathbb{Z}_p^*, \times) is $p - 1$. If p is prime and greater than 2, it must be odd, and $p - 1$ must be even. That is, the order of (\mathbb{Z}_p^*, \times) for $p > 2$ is divisible by 2. So we can't apply the above theorem. But that doesn't mean that (\mathbb{Z}_p^*, \times) is not cyclic. In fact it always is:

Theorem The multiplicative group (\mathbb{Z}_n^*, \times) is cyclic if and only if n is either:

1, 2, 4, p^k , or $2p^k$

where p is an odd prime, and k is a positive integer.

This theorem is quite complicated to prove, and we won't do that here. It is anyway not all that interesting to know that a group is cyclic (has a generator). What is interesting is if there are *lots* of generators. In fact, that is the case for cyclic groups. Once you have a generator, many powers of that generator will also be generators.

Lemma If g is a generator of (\mathbb{Z}_n^*, \times) , then so is g^k so long as $\gcd(k, \phi(n)) = 1$.

This lemma shows that there are at least as many generators for a cyclic group (\mathbb{Z}_n^*, \times) as there are integers k which are less than and relatively prime to $\phi(n)$. Those k values are precisely the elements of $\mathbb{Z}_{\phi(n)}^*$, and there are $\phi(\phi(n))$ of them.

To recap, if the multiplicative group (\mathbb{Z}_n^*, \times) is cyclic, then at least $\phi(\phi(n))$ of its elements are generators. The multiplicative group itself has $\phi(n)$ elements, so the fraction of elements which are generators is $\phi(\phi(n))/\phi(n)$. This is a clumsy expression. If we define $N = \phi(n)$ as the order of the group, then the fraction of generators is $\phi(N)/N$. The following lemma shows that this ratio isn't too small:

Lemma For any $N > 1$,

$$\frac{\phi(N)}{N} = \Omega\left(\frac{1}{\log N}\right)$$

The reason that is so interesting is that for a cyclic group like (\mathbb{Z}_p, \times) , at least $1/\log p$ of the elements will be generators (actually at least $1/\log N$ which is at least $1/\log p$ because $N = \phi(p) < p$). So if we pick elements at random, we only need to make about $O(\log p)$ guesses before we have a good chance of getting a generator. We can do quite a few interesting things with generators. For example, we can prove that p is prime even if we didn't know in advance that it is, by showing that the generator has order $p - 1$. The above results show that we can do this, and hence discover large primes, in time polynomial in $\log p$.