Chapter 6. Discrete Logarithms

Table of Contents

Cyclic Groups and Generators

Some groups have an interesting property: all the elements in the group can be obtained by repeatedly applying the group operation to a particular group element. If a group has such a property, it is called a cyclic group and the particular group element is called a generator. A trivial example is the group Z_n, the additive group of integers modulo n. In Z_n, 1 is always a generator:

$1 \equiv 1 \bmod n$

$1+1 \equiv 2 \bmod n$

$1+1+1 \equiv 3 \bmod n$

...

$1+1+1+...+1 \equiv n \equiv 0 \bmod n$

If a group is cyclic, then there may exist multiple generators. For example, we know Z_5 is a cyclic group. The element 1 is a generator for sure. And if we take a look at 2, we can find:

$2 \equiv 2 \bmod 5$

$2+2 \equiv 4 \bmod 5$

$2+2+2 \equiv 6 \equiv 1 \bmod 5$

$2+2+2+2 \equiv 8 \equiv 3 \bmod 5$

$2+2+2+2+2 \equiv 10 \equiv 0 \bmod 5$

So all the group elements $\{0,1,2,3,4\}$ in Z_5 can also be generated by 2. That is to say, 2 is also a generator for the group Z_5.

Not every element in a group is a generator. For example, the identity element in a group will never be a generator. No matter how many times you apply the group operator to the identity element, the only element you can yield is the identity element itself. For example, in Z_n, 0 is the identity element and $0+0+...+0 \equiv 0 \bmod n$ in all cases.

Not every group is cyclic. For example, Z_n^*, the multiplicative group modulo n, is cyclic if and only if n is 1 or 2 or 4 or p^k or $2*p^k$ for an odd prime number p and $k \geq 1$. So Z_5^* must be a cyclic group because 5 is a prime number. Actually all the elements in Z_5^*, $\{1,2,3,4\}$ can be generated by 2:

$2^1 \equiv 2 \bmod 5$

$2^2 \equiv 4 \bmod 5$

$2^3 \equiv 8 \equiv 3 \bmod 5$

$2^4 \equiv 16 \equiv 1 \bmod 5$

And Z_{12}^* is not a cyclic group. The elements in Z_{12}^* are: {1,5,7,11}. Obviously the identity element 1 cannot be a generator. Let's check the other three elements:

$5^1 \equiv 5 \bmod 12$	$7^1 \equiv 7 \bmod 12$	$11^1 \equiv 11 \bmod 12$
$5^2 \equiv 25 \equiv 1 \bmod 12$	$7^2 \equiv 49 \equiv 1 \bmod 12$	$11^2 \equiv 121 \equiv 1 \bmod 12$

None of the elements can generate the whole group. Therefore, none of them is a generator. So Z_{12}^* is indeed not cyclic.

If Z_n^* is cyclic and g is a generator of Z_n^*, then g is also called a primitive root modulo n.

Prev
Euler's Totient Function and Euler's Theorem

Home

Next
Discrete Logarithm Problem