

Appendix 2. Cyclic groups, group generators

The bonus problem 2 (1p) in Moodle is based on this appendix.

Diffie Hellman key exchange and ECDHE key exchange are both based on cyclic groups. In this appendix, we review the concepts of group and cyclic group and use their properties to find a group generator of multiplicative group Z_p .

Basic concepts

Definition 1: A set G with operation $*$ defined in G is called a group, if it has the following properties.

G1) $a*b \in G$ for all $a, b \in G$

G2) $(a*b)*c = a*(b*c)$ for $a, b, c \in G$

G3) G has a neutral element e for which $a*e = e*a = a$ for all $a \in G$

G4) Every element $a \in G$ has an inverse element a^{-1} for which $a^{-1} * a = a * a^{-1} = e$

Example : The number set Z_p^* of integers $\{1, 2, \dots, p-1\}$ is a group where the group operation is multiplication $a*b \pmod{p}$.

The neutral element of Z_p^* is number 1. All elements $a \in Z_p^*$ have an inverse element $a^{-1} \in Z_p^*$. Indeed, modulus p is a prime and therefore $\gcd(a, p) = 1$ for all $a \in Z_p^*$. Inverse can be calculated using Euclid's extended GDC algorithm.

Definition 2: Let G be a finite group of n elements.

If there is such an element $g \in G$ that the set of its powers $\{g, g^2, \dots, g^n\}$ includes all elements of G , we say that group G is **cyclic** and the element g is a **generator** of group G .

If p is prime, the number set Z_p^* of integers $\{1, 2, \dots, p-1\}$ is a cyclic group. Diffie Hellman key exchange uses this group.

Example: Group Z_{13}^* is cyclic. For example number 7 is a generator of Z_{13}^* , because the set of powers $\{7^1 \pmod{13}, 7^2 \pmod{13}, \dots, 7^{12} \pmod{13}\} = \{7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1\}$ contains all the elements of Z_{13}^* .

Definition 3: If H is a group and H is a subset of group G , we say that H is a **subgroup** of group G .

Example: Set $H = \{1, 3, 9\}$ is a subgroup of Z_{13}^* .

The multiplication table, where operation is $a*b \pmod{13}$ shows that all group properties G1, ..., G4 hold.

	1	3	9
1	1	3	9
3	3	9	1
9	9	1	3

This group is cyclic, because 3 generate all its elements: $\{3, 3^2, 3^3\} \pmod{13} = \{3, 9, 1\}$

Properties of multiplicative groups Z_p^*

1. All elements a of $Z_p^* = \{1, 2, \dots, p-1\}$ generate a cyclic subgroup of Z_p^*
2. The size of the subgroup generated by element a is called **the order of element a** and denoted **Ord(a)**.
3. Lagrange's theorem: Ord(a) is a divisor of $p-1$ for all $a \in Z_p^*$.
4. If Ord(g) is $p-1$, *element g is called a generator of Z_p^* or primitive root of Z_p^**

The next property follows from properties 1 – 4.

5. Let d_1, d_2, \dots, d_n be the list of divisors of $p-1$ in ascending order (where $d_1=1$ and $d_n=p-1$)

Then, the generators are those elements g of Z_p^* , for which only the last power of g in the sequence $g^{d_1}, g^{d_2}, \dots, g^{d_n}$ equals 1 (mod p).

Example. Below is a table of powers ($a^k \bmod 11$) of elements of Z_{11}^* .

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	Subgroup size
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	10 (generator)
3	3	9	5	4	1	3	9	5	4	1	5
4	4	5	9	3	1	4	5	9	3	1	5
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	10 (generator)
7	7	5	2	3	10	4	6	9	8	1	10 (generator)
8	8	9	6	4	10	3	2	5	7	1	10 (generator)
9	9	4	3	5	1	9	4	3	5	1	5
10	10	1	10	1	10	1	10	1	10	1	2

There are 4 generators: $\{2, 6, 7, 8\}$

All the subgroup sizes 1, 2, 5, and 10 are divisors of 10 (in general $p-1$) as Lagrange's theorem predicts.

The previous theory provides a tool for finding a group generator of Z_p^*

Case1: Generator test, when p is a relatively small prime

Let d_1, d_2, \dots, d_n be the divisors of $p-1$ in ascending order.

An integer $g \in Z_p^*$ is a generator if and only if the last integer in the list of powers $g^{d_1}, g^{d_2}, \dots, g^{d_n}$ equals 1.

Example: a) Test if number 5 a generator of Z_{29}^* or not?

Divisors of $p-1 = 28$ are $\{1, 2, 4, 7, 14, 28\}$. Raising 5 to all the powers in the divisor list gives (using WolframAlpha) $5^{\{1,2,4,7,14,28\} \bmod 29} = \{5, 25, 16, 28, 1, 1\}$. Number 5 is not a generator, because the last two numbers are ones. (WolframAlpha allows to calculate all powers with only one command line)

$2^{\{1,2,4,7,14,28\} \bmod 29} = \{2, 4, 16, 12, 28, 1\}$. Number 2 is a generator of Z_{29}^*

Case2: Finding a generator, when p is very large prime

When prime p is very large, for example 1000 bit integer, it is often impossible to factor $p - 1$. Some divisors are trivial: 1, 2 and $p - 1$ (2 is a divisor, because $p - 1$ is even). However, if $p - 1$ has very large factors, some of the divisors may be not be found.

Example. If $p = 265738830135992486377941683556469254997964098756853$,
then $p - 1 = 265738830135992486377941683556469254997964098756852$
Attempts to factor $p - 1$ further fail.

Strong primes

Definition: A prime p is called a "strong prime", if also $(p-1)/2$ is a prime.

In other words: If p is a strong prime, then $p - 1$ has only four divisors: $\{1, 2, (p-1)/2, p - 1\}$

Some versions of Diffie-Hellman key exchange protocol uses strong primes as modulus p . To find these primes, one can write a Python program or utilize the help of chatGPT. Such a program generated 1033 primes, out of which 75 were strong primes within the range of 10000-20000. In some other Diffie-Hellman versions the system parameter g may be any element of Z_p^* with adequately high order instead of being a generator. In that case the use of a strong prime p is not a necessity.

Generator test is easy to do for Z_p^* , if p is a strong prime.

Example. Integer $p = 200087$ is a strong prime. Divisors of $p - 1$ are $\{1, 2, 100043, 200086\}$.
Test if number 5 is a generator of Z_{200087}^* .

Calculation of powers $5^{\{1, 2, 100043, 200086\}} \bmod 200087$ gives $\{5, 25, 200086, 1\}$,
which shows that number 5 is a generator of Z_{200087}^* .

Rule: Number of generators of $Z_p^* = \phi(p-1)$, where ϕ is Euler's totient function.

(More general rule is that for any divisor d of $p - 1$ the number of elements of order d is $\phi(d)$)

If p is a strong prime, then $p - 1 = 2 \cdot r$, where $r = (p-1)/2$ is also a prime.
Now $\phi(2 \cdot r) = (2-1)(r-1) = (p-1)/2 - 1 \approx (p-1)/2$.

Hence: If p is a large prime, nearly 50% of elements of Z_p^* are generators.
