Order of the Group

Order of the Group

Order of a finite group |G|, to be the number of elements in the group G. In $G = <Z_{21}*, \times>$, it can be proved that the order of a group is $\phi(n)$.

Example

What is the order of group $G = <Z_{21}*, \times>$? $|G| = \phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$. There are 12 elements in this group: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20. All are relatively prime with 21.

Order of an Element

Order of an Element

In a group **$G = <Z_n*, \times>$, order of an element 'a' is the smallest integer 'i' such that $a^i = 1 \pmod n$.**

Example

Find the order of all elements in $G = <Z_{10}*, \times>$.

Solution

This group has only $\phi(10) = 4$ elements: 1, 3, 7, 9. We can find the order of each element by trial and error.

a. $1^1 \equiv 1 \bmod (10) \rightarrow \mathrm{ord}(1) = 1.$

b. $3^4 \equiv 1 \bmod (10) \rightarrow \mathrm{ord}(3) = 4.$

c. $7^4 \equiv 1 \bmod (10) \rightarrow \mathrm{ord}(7) = 4.$

d. $9^2 \equiv 1 \bmod (10) \rightarrow \mathrm{ord}(9) = 2.$

Continued

Primitive Roots In the group $G = <Z_n*, \times>$, when the order of an element is the same as $\phi(n)$, **that element is called the primitive root of the group**.

Example

Table shows that there are no primitive roots in $G = <Z_8*, \times>$ because no element has the order equal to $\phi(8) = 4$. The order of elements are all smaller than 4.

Continued

Example

Table shows the result of $a^i \equiv x(\text{mod}7)$ for the group G = <Z_7*, ×>. In this group, ϕ(7) = 6.

Table 9.5 *Example 9.50*

		$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
	$a = 1$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
	$a = 2$	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
Primitive root →	$a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
	$a = 4$	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
Primitive root →	$a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
	$a = 6$	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

Continued

The group $G = \langle Z_n{*}, \times\rangle$ has primitive roots only if n is 2, 4, p^t, or $2p^t$.

Example

For which value of n, does the group $G = \langle Z_n{*}, \times\rangle$ have primitive roots: 17, 20, 38, and 50?

Solution

a. $G = \langle Z_{17}{*}, \times\rangle$ has primitive roots, 17 is a prime.

b. $G = \langle Z_{20}{*}, \times\rangle$ has no primitive roots.

c. $G = \langle Z_{38}{*}, \times\rangle$ has primitive roots, $38 = 2 \times 19$ prime.

d. $G = \langle Z_{50}{*}, \times\rangle$ has primitive roots, $50 = 2 \times 5^2$ and 5 is a prime.

Continued

If the group G = <Z_n*, ×> has any primitive root, the number of primitive roots is $\phi(\phi(n))$.

Primitive Roots mod 13

- a is a primitive root mod p if $\{a^k \mid 1 \leqq k \leqq p-1\} = \{1,2, \ldots, p-1\}$

♪ 2, 6,7,11 are primitive roots mod 13

- $3^3 \equiv 1 \pmod{13}$, $4^6 \equiv 1 \pmod{13}$, $5^4 \equiv 1 \pmod{13}$,
- $8^4 \equiv 1 \pmod{13}$, $9^3 \equiv 1 \pmod{13}$, $10^6 \equiv 1 \pmod{13}$,
- $12^2 \equiv 1 \pmod{13}$