PRIMITIVE ROOTS

Lakshmy K V

October 21, 2020

Units Modulo an Integer

Let n be a positive integer. Consider the integers modulo n. If a is coprime to n, then by Euclid's algorithm we can find integers b and c such that

$$\begin{aligned} ab + nc &= 1 \\ \implies ab &\equiv 1 \bmod n. \end{aligned}$$

In other words, any integer a which is coprime to n has a multiplicative inverse modulo n. Such an integer a is called a unit modulo n. The set of all units in $\mathbb{Z}_n$ is denoted by U_n. It is clear that if a is in U_n, so is its inverse. Moreover, if a and b are in U_n, so is their product modulo n. Thus, U_n is a group under multiplication. Recall that Euler's ϕ-function counts the number of elements in U_n.

For example:

$$\begin{aligned} U_5 &= \{1,\ 2,\ 3,\ 4\}, \\ U_7 &= \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}, \\ U_8 &= \{1,\ 3,\ 5,\ 7\}, \\ U_{15} &= \{1,\ 2,\ 4,\ 7,\ 8\ 11,\ 13,\ 14\}. \end{aligned}$$

Observe that each element in U_5 is a power of 2 modulo 5, and each element in U_7 is a power of 3 modulo 7. In other words U_5 and U_7 are cyclic groups under multiplication modulo 5 and 7 respectively, and 2 and 3 are their respective generators. On the other hand, we can not find such generating element in U_8, as square of each of its element is 1 modulo 8. We want to characterize the positive integers n such that U_n is cyclic.

DEFINITION 4.1. *Let h be the smallest positive integer such that $a^h \equiv 1$ mod n. Then h is called the order of a modulo n.*

LEMMA 4.4. *Let a be an integer coprime to n. Then the order of a^i modulo n is*

$$d = \frac{h}{gcd(i,h)},$$

where h is the order of a modulo n

Proof: Let the order of a^i modulo n be m. We will show that $d|m$ and $m|d$. Observe that

$$(a^i)^m \equiv 1 \bmod n \implies h \mid im.$$

After canceling the gcd (h,i), we must have $d \mid m$. Conversely, it is clear from the definition of d that id is divisible by $d \cdot gcd(i,h) = h$, hence

$$(a^i)^d \equiv a^{id} \equiv 1 \bmod n,$$

hence $m \mid d$. Thus, $m = d$. □

Definition 4.5. *An integer g is called a primitive root modulo n if the order of g modulo n is $\phi(n)$.*

For example, 2 is a primitive root of $n = 5$. And so is 3. Similarly, 3 is a primitive root of 7. Primitive roots may not exist for certain integers n. For example, $U_{12} = \{1, 5, 7, 11\}$, and the order of 5, 7, 11 in U_{12} is 2, and the order of 1 is 1. Hence there are no primitive roots for 12. If one primitive root exists for an integer n, it is easy to prove that there are $\phi(\phi(n))$ of them. We will give a proof later.

Proposition 4.6. *Let g be a primitive root modulo n. Then, $U_n = \{g^i \mid i = 1, 2, \cdots \phi(n)\}$.*

Proposition 4.7. *Suppose there exists a primitive root g modulo n. Then n has precisely $\phi(\phi(n))$ number of primitive roots.*

Proof: Any element of U_n is of the form g^i for some integer i. Suppose g^i is another primitive root of n. Then the order of g^i modulo n is $\phi(n)$, hence we must have $gcd(i, \phi(n)) = 1$. Conversely, if $(i, \phi(n)) = 1$ then the order of g^i is $\phi(n)$. Hence there are precisely $\phi(\phi(n))$ primitive roots for n provided it has one. $\square$

For example, $U_{10} = \{1, 3, 7, 9\}$ and 3 is a primitive root: $3^2 \equiv 9 \bmod 10$, $3^3 \equiv 7 \bmod 10$, $3^4 \equiv 1 \bmod 10$. Therefore the order of 3 in $U - 10$ is 4. Clearly, 9 is not a primitive root as its order modulo 10 is 2: $9^2 \equiv 1 \bmod 10$. One can verify that order of 7 modulo 10 is 4, so 7 is also a primitive root modulo 10. Thus, the number of primitive roots modulo 10 are $2 = \phi(\phi(10))$.

PROPOSITION 4.11. *There is no primitive root modulo 2^e if $e \geq 3$.*

THEOREM 4.12. *Let p be an odd prime and e be any positive integer. Let g be a primitive root of p. Then either g or $g+p$ is a primitive root for p^e for all $e \geq 2$.*

LEMMA 4.13. *If $n = kl$ where $k > 2$ and $l > 2$ are two co-prime integers, then n does not have a primitive root.*

Lemma: Any odd primitive root of p^e will be a primitive root of $2p^e$

THEOREM 4.14. *A natural number n has a primitive root if and only if n is one of the following: 1, 2, 4, p^e or $2p^e$ where p is an odd prime.*

4.4 Exercises

1. (A) Find a primitive root for the following primes:

$$11,\ 13,\ 17,\ 19.$$

   (B) How many primitive roots does each prime above have?

   (C) List all the primitive roots for each of the primes above.

2. Find an element of

   (A) order 5 modulo 11

   (B) order 4 modulo 13

   (C) of order 8 modulo 17

   (D) of order 6 modulo 19.

3. Can you find a element of order 12 modulo 29?

4. If a is a primitive root of an odd prime p, show that

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

5. If a and b are two primitive roots of an odd prime p, show that ab can not be a primitive root of p.

6. Show that the primitive roots of an odd prime p occur in pairs (a, a') where

$$aa' \equiv 1 \bmod p, \qquad a \not\equiv a' \bmod p.$$

10. (A) Find a primitive root for the following prime powers:

$$5^2,\ 3^3,\ 7^2,\ 11^2,\ 11^3.$$

(B) How many primitive roots does each one of them have?

(C) Find the largest possible order of an element in U_n when n is

$$\begin{array}{cccc} (i) & 25 & (ii) & 50 \\ (iii) & 75 & (iv) & 100. \end{array}$$

(D) List all the primitive roots for each one of them.

11. (A) List the composite numbers which have a primitive root in the following:

$$10,\ 12,\ 14,\ 15,\ 18,\ 21,\ 22,\ 28,\ 98.$$

(B) Find a primitive root for the composite numbers in the list found.

(C) Determine all the primitive roots in each case.