Primitive Roots And Orders

Masum Billal

In this note, we will discuss some basic theories of primitive root and some of its application in problems. We assume the following notations:

- *s.t.* is the short form of *such that*.
- *i.e.* is the short form of *in explanation*.
- *qr* is the short form of *quadratic residue*.
- $\varphi(n)$ is Euler Totient Function of n.
- $ord_n(a) = x$ is the order of $a \pmod n$.
- $\nu_p(n) = \alpha$ or $p^\alpha || n$ denotes the maximum positive integer α s.t. $p^\alpha | n$ i.e. $p^\alpha | n$ but $p^{\alpha+1} \nmid n$.
- (a, b) denotes $\gcd(a, b)$ i.e. the greatest common divisor of a and b.
- $[a, b]$ denotes $lcm(a, b)$ i.e. the least common multiple of a and b.
- $a \perp b$ denotes a is co-prime to b or relatively prime to b or $(a, b) = 1$ i.e. a and b doesn't share any common factor other than 1.
- $pr_n = g$ denotes g is a primitive root $\pmod n$.

1. Definitions

Definition (Order Modulo Integers)**.** For positive integers a and n, if x is the smallest positive integer s.t.

$$a^x \equiv 1 \pmod n$$

then x is called the *order of a modulo n*. We denote this by $ord_n(a) = x$.

Example. $ord_8(3) = 2$ i.e. 2 is the smallest positive integer s.t. $3^2 \equiv 1 \pmod 8$.

Definition (Totient Function)**.** The number of positive integers less than or equal to n which are co-prime to n is $\varphi(n)$.

Example. $\varphi(6) = 2, \varphi(7) = 6$.

Definition (Primitive Root)**.** A positive integer g is called a *primitive root* of n if $ord_n(a) = \varphi(n)$, that is if $a^x \not\equiv 1 \pmod n$ for $x < \varphi(n)$. Let's say, $pr_n = g$ means g is a primitive root $\pmod n$.

Example. $pr_7 = 3$ since $\varphi(7) = 6$ and $3^i \not\equiv 1 \pmod 7$ for $i \in \{1, 2, 3, 4, 5\}$.

Definition (Quadratic Residue)**.** a is a qr of n if

$$x^2 \equiv a \pmod{n}$$

for some x.

Definition (Legendre Symbol)**.** $\left(\frac{a}{p}\right)$ is called the *Legendre symbol* for a prime p. It is defined by:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } p|a \\ 1 \text{ if } a \text{ is a qr of } p \\ -1 \text{ otherwise} \end{cases}$$

2. Theorems & Lemmas

THEOREM 1. *If $pr_n = g$ then $g^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$ for any prime $p|\varphi(n)$.*

Remark. The converse is also true.

Proof. That's pretty straight forward. □

THEOREM 2. *If $ord_n(a) = d$ and $a^x \equiv 1 \pmod{n}$ then $d|x$.*

Proof. If $x < d$, it would contradict the fact that, d is such smallest positive integer. Therefore, $x > d$ and we assume $x = dq + r$ with $r < x$. But $a^x \equiv a^{dq}a^r \equiv 1 \pmod{n}$ which implies $a^r \equiv 1 \pmod{n}$. But this is impossible unless $r = 0$. Hence $d|x$. □

THEOREM 3. *If $m \perp n$ are positive integers s.t. $ord_m(a) = d, ord_n(a) = e$ then $ord_{mn}(a) = [d, e]$.*

Proof. Let $ord_{mn}(a) = h$, so

$$a^h \equiv 1 \pmod{mn}$$

which gives $a^h \equiv 1 \pmod{m}, a^h \equiv 1 \pmod{n}$.

$$a^d \equiv 1 \pmod{m},$$

$$a^e \equiv 1 \pmod{n}$$

so by the theorem 2, $d|h, e|h$. Therefore, for the minimum h, we have $h = [d, e]$ to satisfy the conditions. □

THEOREM 4. *The values of n for which n has a primitive root are $2, 4, p^k, 2p^k$ for an odd prime p and a positive integer k.*

Proof. First we check out the possibility of 2 and 4. Now, for an odd a we can easily prove by induction that,

$$2^k | a^{2^{k-2}} - 1$$

But $\varphi(2^k) = 2^{k-1}$, therefore, a is never a primitive root of 2^k. Next, we consider $n = ab$ with $\gcd(a, b) = 1$ and $a > b > 2$ so that $\varphi(b) > 1$, and hence even. Let g be a primitive root of n.

$$g^{\varphi(ab)} \equiv 1 \pmod n$$

$$\Rightarrow g^{\varphi(a)\varphi(b)} \equiv 1 \pmod n$$

We will show that this can't hold for there exists a $k < \varphi(n)$ s.t.

$$a^k \equiv 1 \pmod n$$

Let $ord_a(g) = d, ord_b(g) = e$. Then $d|\varphi(a), e|\varphi(b)$ from

$$g^{\varphi(a)} \equiv 1 \pmod a$$

$$g^{\varphi(b)} \equiv 1 \pmod b$$

So, by theorem 3,

$$\begin{aligned} ord_{ab}(g) &= [d, e] \\ &\leq [\varphi(a), \varphi(b)] \\ &\leq \frac{\varphi(ab)}{2} \end{aligned}$$

from the fact that $\varphi(a), \varphi(b)$ are both even. But this gives us the contradiction we are looking for,

$$a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod n$$

with $\varphi(n) > \dfrac{\varphi(n)}{2}$. Therefore, under this condition, there is no primitive root for n. We are left with the values $2p^k$ and p^k for an odd prime p.

$\square$

Theorem 5. *If $pr_n = g$ then*

$$\mathbb{G} = \{g^1, g^2, \ldots, g^{p-1}\}$$

forms a complete set of residue $\pmod n$.

Proof. Instead, we assume that there are indexes i and j s.t.

$$g^i \equiv g^j \pmod n$$

with $p - 1 \geq i > j \geq 1$. Of-course $n \perp g$. Thus, $g^{i-j} \equiv 1 \pmod n$ by the cancellation rule. But since $i - j < p - 1$ this contradicts with the minimality of $ord_n(g)$.

$\square$

THEOREM 6. *Let $\mathbb{U}$ be the set of positive integers $g_1, \ldots, g_{\varphi(n)}$ less than or equal to n and co-prime to n*

$$\mathbb{U} = \{g_1, \ldots, g_{\varphi(n)}\}$$

Then,

$$g_1 \cdots g_{\varphi(n)} \equiv a^{\frac{\varphi(n)}{2}} \pmod{n}$$

Proof. Let a be any $non - qr$ of n. For any $g \in \mathbb{U}$ there is a unique h s.t.

$$gh \equiv a \pmod{n}$$

This follows since $gi \equiv gj \pmod{n}$ isn't possible for $i < j < n$. Thus, we can pair up the $\varphi(n)$ elements of $\mathbb{U}$ into $\dfrac{\varphi(n)}{2}$ pairs, each giving a remainder a. Hence,

$$g_1 \cdots g_{\varphi(n)} \equiv a^{\frac{\varphi(n)}{2}} \pmod{n}$$

□

THEOREM 7. *If m has a primitive root, then*

$$g_1 \cdots g_{\varphi(n)} \equiv -1 \pmod{n}$$

otherwise,

$$g_1 \cdots g_{\varphi(n)} \equiv 1 \pmod{n}$$

Proof. Combining 4 and 1 along with the fact that p odd prime implies $p^k | a^2 - 1 \Rightarrow p^k | a + 1$ or $p^k | a - 1$, we get the desired proof. □

THEOREM 8. *If n has a primitive root, then it has $\varphi(\varphi(n))$ primitive roots.*

Proof. Let g be a primitive root of n. Then $g^{\varphi(n)} \equiv 1 \pmod{n}$. Consider the numbers g^i. It has order $\dfrac{\varphi(n)}{\gcd(\varphi(n), i)}$. So it has order $\varphi(n)$ if $\gcd(i, \varphi(n)) = 1$. There are such $\varphi(\varphi(n))$ numbers, hence n has $\varphi(\varphi(n))$ primitive roots. □

3. Problems

3.1. For any positive integer $a \perp n$,

$$n|\varphi(a^n - 1)$$

Solution. First note that,

$$a^n \equiv 1 \pmod{a^n - 1}$$

and since $a^k - 1 < a^n - 1$ for $k < n$, we can say $ord_{a^n-1}(a) = n$. From Fermat-Euler theorem,

$$a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}$$

since $a \perp a^n - 1$. By theorem 2, $n|\varphi(a^n - 1)$.

3.2. For every $n \in \mathbb{N}$ there are pair-wise positive integers $a_1, a_2, \ldots, a_{\varphi(n)}$ and another k each $\leq n$ s.t.

$$n|\left(\sum_{i=1}^{k} a_i\right)^2 + \left(\prod_{i=1}^{k} a_i\right)^2 - 1$$

Solution. We already know that $\varphi(n)$ is even. We choose k positive integers $g_1, \ldots, g_k$ with $k = \varphi(n)$ and $g_i \perp n, g_i \leq n$. Note that, if $\gcd(n, g_i) = \gcd(n, n - g_i) = 1$. This yields $g_i = g_{\varphi(n)-i}$. So we have $g_i + g_{k-i} = n$. Then, $\sum_{i=1}^{k} g_i = \sum_{i=1}^{\frac{k}{2}} g_i + g_{k-i} = \sum n$, which is divisible by n. Now, theorem 6 gives $(g_1 \cdots g_k)^2 \equiv 1 \pmod{a}^{\varphi(n)} \equiv 1 \pmod{n}$. This gives the desired result.

3.3. Let G be a group with $|G| = n$ and an operation $\cdot$. Find all G s.t. $\exists a \in G$ s.t. $a \cdot a \cdots a = e$ where e is the identity of G and the operation is done n times.