IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728. Volume 5, Issue 4 (Jan. - Feb. 2013), PP 08-11
www.iosrjournals.org

.

Properties of semi primitive roots

Dr.K.Vijaya lakshmi
Head, Department of Mathematics, Loyola Academy, Secunderabad.

Abstract: *We know that the smallest positive integer f such that $a^f \equiv 1$ mod m is called the exponent of 'a' modulo m and is denoted by $\exp_m a$. We say that 'a' is a semi-primitive root mod m if $\exp_m a = \frac{\phi(m)}{2}$. In this paper we discuss the properties of the semi primitive roots and examine for which prime 2 is a semi-primitive root. If S is the sum of semi-primitive roots less than p then we proved that $S \equiv \mu(\frac{p-1}{2}) \bmod p$ .Also we proved that if 'a' is a semi primitive root then 'a' is a quadratic residue, converse need not be true. It was established that whenever a is a semi-primitive root mod p where p is of the form 4n+3 then –a is a semi primitive root and if p = 4n+1 then $\exp_m(-a) = \frac{p-1}{4}$.We establish that 2 is semi-primitive root for mod p whenever 'p' is of the form 2q+1where 'q' is an odd prime of the form 4n+3 and if 4n+1,8n+3 are primes then –2 is a semi-primitive root mod 8n+3 by using Gauss Lemma [1].*

Definition: Suppose 'a' is any integer and m is a positive integer such that (a, m) = 1.

We say that a is a semi-primitive root mod m if $\exp_m a = \phi(m)/2$. From the definition

It is clear that $a, a^2, \ldots\ldots a^{\frac{\phi(m)}{2}}$ are in congruent mod m and they form a cyclic sub group of reduced residue system mod m.

Theorem 1: If m has a primitive root then there are exactly $\frac{\phi(\phi(m))}{2}$ semi primitive roots given by

$$S = \left\{ a^n : 1 \le n < \frac{\phi(m)}{2}, (n, \frac{\phi(m)}{2}) = 1 \right\}$$

Proof: If a is a semi-primitive root then

$$\exp_m a = \exp_m a^n = \frac{\phi(m)}{2} \Leftrightarrow (n, \frac{\phi(m)}{2}) = 1$$

So every member of S is a semi-primitive root mod m. Conversely, if 'g' is a semi-primitive root then

$$\exp_m a^k = \exp_m g = \frac{\phi(m)}{2} \text{ for } 1 \le k \le \frac{\phi(m)}{2}$$

$$\therefore (k, \frac{\phi(m)}{2}) = 1$$

Now we find the sum of semi-primitive roots less than 'p'.

Theorem 2 : If p is an odd prime and S is the sum of semi-primitive roots less than p then

$$S \equiv \mu(\frac{p-1}{2}) \bmod p$$

Proof: Suppose 'a' is a semi-primitive root mod p, then a^n is a semi-primitive root mod p.

$$\Leftrightarrow (n, \frac{p-1}{2}) = 1$$

$$\therefore S = \sum_{1 \le n \le \frac{p-1}{2}} a^n \bmod p$$

But $\sum_{1 \le n \le \frac{p-1}{2}} a^n = \sum_{1 \le n \le \frac{p-1}{2}} a^n \sum_{d/n \& d/\frac{p-1}{2}} \mu(d) = \sum_{d/\frac{p-1}{2}} \mu(d) a^{n\delta}$

$$= \sum_{\delta \prec \frac{p-1}{2d}} (a^d)^\delta \cdot \sum_{d/\frac{p-1}{2}} \mu(d)$$

$$= \mu(\frac{p-1}{2}) a^{\frac{p-1}{2}} + \sum_{\delta \prec \frac{p-1}{2d}} (a^d)^\delta \sum_{d/\frac{p-1}{2}} \mu(d)$$

$$= \mu(\frac{p-1}{2}) a^{\frac{p-1}{2}} + \sum_{d/\frac{p-1}{2}} \mu(d) \frac{a^d (a^{\frac{p-1}{2}} - 1)}{a^d - 1}$$

Since $d / \frac{p-1}{2}$ and $\frac{a^{\frac{p-1}{2}} - 1}{a^d - 1}$ is an integer we have $S = \mu(\frac{p-1}{2})$ mod p.

If p is a prime of the form 8n+1,then $\mu(\frac{p-1}{2}) = \mu(4n) = 0 . \therefore S = 0$

We know that 'a' is quadratic residue mod p if $x^2 \equiv$ a (mod p) has a solution.

Theorem3: If 'a' is semi-primitive root mod p then 'a' is a quadratic residue mod p. ***Proof: A is a semi primitive root mod p*** $\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$

Since p is an odd prime p has a primitive root say g.

Now (a, p) = 1 we have $a \equiv g^k \bmod p; 1 \le k \le \phi(p)$

$$1 \equiv a^{\frac{p-1}{2}} \equiv (g^k)^{\frac{p-1}{2}} \pmod p$$

$\Rightarrow$p-1 divides k. $\frac{p-1}{2}$ since g is a primitive root mod p.

$\Rightarrow \frac{k}{2}$ is an integer i.e $\frac{k}{2} = m$

$$\therefore a \equiv (g^m)^2 \pmod p$$

$\Rightarrow g^m$ is a solution of $\therefore x^2 \equiv a \pmod p$ Therefore a is a quadratic residue mod p.

However converse is not true as there are $\frac{\phi(\phi(p))}{2}$ semi-primitive roots and $\frac{p-1}{2}$ quadratic residues.

Theorem4: If ‘a’ is a primitive root mod p where p =4n+3,then –a is a semi primitive root mod p.

Proof: Let ‘a’ be a primitive root mod p.

Then $a^{p-1} \equiv 1 \bmod p \Rightarrow (-a)^{p-1} \equiv 1 \bmod p$

$a^{p-1} \equiv 1 \bmod p \Rightarrow (a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \bmod p$

$\Rightarrow a^{\frac{p-1}{2}} \equiv -1 \bmod p$ as a is a primitive root mod p.

$\Rightarrow (-a)^{\frac{p-1}{2}} \equiv 1 \bmod p$

Suppose $\exp_m$ (-a) = f

Then f $\mid \frac{p-1}{2}$, $1 \le f \le \frac{p-1}{2}$; i.e. 2f < p-1

Since $\exp_m$ (-a) = f we have $(-a)^{2f} \equiv 1 (\bmod p)$

$\Rightarrow a^{2f} \equiv 1 (\bmod p)$ which is a contradiction since ‘a’ is a primitive root mod p.

Therefore f = $\frac{p-1}{2}$

Hence –a is semi-primitive root mod p.

Similarly we can prove that if ‘p’ is of the form 4n+1 then $\exp_m$ (-a)= p-1/4 when n is odd.

Theorem5: If 8n-1 and 4n-1 are primes then 2 is a semi-primitive root mod 8n-1.
Proof; Let p = 8n-1 and q= 4n-1.Then p-1 = 2q.
From Gauss lemma we have

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} (\bmod p)$$

And

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8n-1)^2-1}{8}} = (-1)^{8n^2-2n} = 1 \; i.e. \; 2^{\frac{p-1}{2}} \equiv 1 (\bmod p)$$

$$\therefore 2^{\frac{p-1}{2}} \equiv 1 (\bmod p)$$

Suppose $\exp_p 2$ = f then $2^f \equiv 1 (\bmod p)$ and f divides p-1/2 i.e f $\mid$ q
Since q is a prime we have f = q.

Thus 2 is a semi-primitive root mod p.

Theorem 6: ‘2’ is a semi primitive root mod p, where p =2q+1, q being an odd prime of the form 4n+3.

Proof: Let p = 2q+1 then p-1/2 = q where q = 4n+3

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(2q+1)^2-1}{8}} = (-1)^{\frac{4q^2+4q}{8}} = (-1)^{\frac{4(4n+3)^2+4(4n+3)}{8}} = (-1)^{8n^2+14n+6} = 1$$

$$\therefore 2^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$$

By Gauss lemma,
Suppose $\exp_p 2 = f$ then $2^f \equiv 1(\text{mod p})$ and *f* divides p-1/2 i.e. $f \mid q$

Since q is a prime we have *f* = q.

Thus 2 is a semi-primitive root mod p.

Theorem7: If 8n+3 and 4n+1are primes then –2 is a semi-primitive root mod 8n+3.

Proof: let p = 8n+3 and q = 4n + 1 So p-1/2 = 4n+1.

By Gauss lemma

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(8n+3)^2-1}{8}} = (-1)^{8n^2+6n+1} = (-1)^{(4n+1)(2n+1)} = -1$$

$$\therefore 2^{\frac{p-1}{2}} \equiv -1(\text{mod } p) hence (-2)^{\frac{p-1}{2}} \equiv 1 \text{mod } p$$

Suppose $\exp_p(-2) = f$ then $(-2)^f \equiv 1(\text{mod p})$ and *f* divides p-1/2 i.e $f \mid q$

Since q is a prime we have *f* = q

Thus -2 is a semi-primitive root mod p.

Key Words: Universal exponent, exponent, λ - primitive root,
semi-primitive root, primitive root.

References:

[1] Apostol Tom M: Introduction to Analytic Number Theory, Springer International Student Edition.
[2] Leveque W.J.: Topics in Number Theory, Vol. 1 Reading mass (1956).
[3] Vegh E: λ- primitive roots. Portugaliae Mathematica 40(1981) 297-303.
[4] An Introduction to Theory of Numbers by Ivan Niven, Herbert S. Zuckerman – Wiley Eastern Limited.
[5] Elementary Number theory by David M .Burton.