IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 11, Issue 2 Ver. II (Mar - Apr. 2015), PP 14-17
www.iosrjournals.org

Existence of Semi Primitive Root Mod P^{α}

Dr. K.Vijayalakshmi, Loyola Academy Degree & P.G.College,
Old Alwal, Secunderabad, Telengana, India.

I. Introduction

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 $\exp_m a = \frac{\phi(m)}{2}$. We proved that there exists a semi-primitive root for mod m when m = p^{α}, 2 p^{α}(for$\alpha>2$), $2^2.p^{\alpha}$ and 2^{α}if $\alpha>3$. Also it was established that there exists a semi-primitive root for mod m when m = p_1p_2 where p_1 and p_2 are distinct odd primes and at least one prime is of the form 4n+3.In this paper we discuss the existence of semi primitive root mod p^{α}whenever it exists for mod p. we have If 'a' is a semi primitive root mod p^2 then $\frac{\phi(p^2)}{2} = \frac{p(p-1)}{2} \geq \frac{p-1}{2} \Rightarrow a^{\frac{p-1}{2}} \neq 1$ modp^2.Hence the relation $a^{\frac{p-1}{2}} \neq 1$ modp^2 is a necessary condition for a semi primitive root a mod p to be a semi primitive root mod p^2. Conversely we prove that when 'a' is a semi primitive root mod p then a is also a semi primitive root mod p^{α} for $\alpha \geq 2$ if $a^{\frac{p-1}{2}} \neq 1$ modp^2.
To prove the main result we prove the following lemma.

Lemma: Let 'a' be a semi primitive root mod p such that
$a^{\frac{p-1}{2}} \neq 1$ modp^2.Then $a^{\frac{\phi(p^{\alpha-1})}{2}} \neq 1$ mod $p^{\alpha}$for $\alpha \geq 2$.
Proof: We prove the lemma by induction on α.

If $\alpha = 2$ then $a^{\frac{p-1}{2}} \neq 1$ modp^2.i.e the result is true for $\alpha = 2$
Suppose that the result is true for α then

$$a^{\frac{\phi(p^{\alpha-1})}{2}} \neq 1 \text{ mod } p^{\alpha-1} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(1)$$

By Euler's theorem we have

$$a^{\phi(p^{\alpha-1})} \equiv 1 (\text{mod } p^{\alpha-1}) \Rightarrow \left(a^{\frac{\phi(p^{\alpha-1})}{2}} \right)^2 \equiv 1 \ (\text{mod } p^{\alpha-1})$$

$$\Rightarrow (a^{\frac{\phi(p^{\alpha-1})}{2}} + 1)(a^{\frac{\phi(p^{\alpha-1})}{2}} - 1) \equiv 0 \ (\text{mod } p^{\alpha-1})$$

$$\Rightarrow a^{\frac{\phi(p^{\alpha-1})}{2}} \equiv -1 \ (\text{mod } p^{\alpha-1}) \text{ since } a^{\frac{\phi(p^{\alpha-1})}{2}} \neq 1 \text{ mod } p^{\alpha-1}.$$

$$\Rightarrow p^{\alpha-1} | (a^{\frac{\phi(p^{\alpha-1})}{2}} + 1)$$

$$\Rightarrow a^{\frac{\phi(p^{\alpha-1})}{2}} = -1 + kp^{\alpha-1}$$

Rising to the powers of p on both sides we get

$$a^{\frac{p.\phi(p^{\alpha-1})}{2}} = (-1 + kp^{\alpha-1})^p$$

$$\Rightarrow a^{\frac{\phi(p^\alpha)}{2}} = (-1)^p + kp^\alpha + k^2 \frac{p(p-1)}{2} p^{2(\alpha-1)} + \ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\Rightarrow a^{\frac{\phi(p^\alpha)}{2}} \equiv (-1 + kp^\alpha) \text{(Mod } p^{\alpha+1})$$

If possible suppose that $a^{\frac{\phi(p^\alpha)}{2}} \equiv 1 (\text{mod } p^{\alpha+1})$

Then $-1 + kp^\alpha \equiv 1(\text{Mod } p^{\alpha+1}) \Rightarrow p^{\alpha+1}$ divides $kp^\alpha - 2 \Rightarrow$ p divides $kp^\alpha - 2$

$\Rightarrow$ p divides k.p^α and p divides $kp^\alpha - 2 \Rightarrow$ p divides 2 which is a contradiction.

Therefore $a^{\frac{\phi(p^\alpha)}{2}} \neq 1 (\text{Mod } p^{\alpha+1})$. Hence the result is true for α+1.
Thus by induction the result is true for all α≥2.
Theorem: Let p be an odd prime, then we have

(i) If a is a semi primitive root mod p , then a is also a primitive root mod p^α for every $\alpha \geq 2$if and only if $a^{\frac{p-1}{2}} \neq 1$ modp^2.

(ii) There is at least one semi primitive root mod p such that $a^{\frac{p-1}{2}} \neq 1$ modp^2.

Proof: Suppose a is a semi primitive root mod p.
If a is a semi primitive root mod p^α for every α≥2 then in particular it is semi primitive root mod p^2. And hence

$a^{\frac{p-1}{2}} \neq 1$ modp^2.

Conversely suppose $a^{\frac{p-1}{2}} \neq 1$ modp^2.
Now we show that 'a' is a semi primitive root for mod p^α.
Suppose $\exp_{p^\alpha} a = t$

We prove that $t = \frac{\phi(p^\alpha)}{2} = \frac{p^{\alpha-1}(p-1)}{2}$

Since $a^t \equiv 1$ (mod p^α) we have $a^t \equiv 1$ (mod p)

Therefore $\frac{\phi(p)}{2}$ divides t.$\Rightarrow$ t = q. $\frac{\phi(p)}{2}$

Now t divides $\frac{\phi(p^\alpha)}{2} \Rightarrow$ q. $\frac{\phi(p)}{2}$ divides $\frac{\phi(p^\alpha)}{2}$

$\Rightarrow$ q. $\frac{p-1}{2}$ divides $\frac{p^{\alpha-1}(p-1)}{2} \Rightarrow$ q divides $p^{\alpha-1} \Rightarrow$ q= $p^{\beta-1}$ where $\beta \leq \alpha$-1.
Now it is sufficient to prove β = α-1.
Suppose β < α-1. Then $\beta \leq \alpha$-2.

Now $t = \frac{p^\beta(p-1)}{2} \mid \frac{p^{\alpha-2}(p-1)}{2} \Rightarrow t = \frac{p^\beta(p-1)}{2} \mid \frac{\phi(p^{\alpha-1})}{2}$

$a^{\frac{\phi(p^{\alpha-1})}{2}} \equiv 1$mod p^α which is a contradiction by above lemma.

Therefore p = α-1. Hence $t = \frac{\phi(p^{\alpha})}{2} = \frac{p^{\alpha-1}(p-1)}{2}$

Thus a is a semi primitive root mod p^{α}.

Proof of (ii): If $a^{\frac{p-1}{2}} \neq 1$ modp^2 then by (i) a is a semi primitive root mod p^{α}.

Suppose $a^{\frac{p-1}{2}} \equiv 1$ modp^2

Let x be any other semi primitive root satisfying $x^{\frac{p-1}{2}} \neq 1$ modp^2

And x = a + p

$$x^{\frac{p-1}{2}} = (a+p)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} + \frac{p-1}{2}.a^{\frac{p-3}{2}}.p + \frac{p-1}{2}.\frac{p-3}{2}a^{\frac{p-5}{2}}.p^2 + ...$$

Therefore $x \equiv a^{\frac{p-1}{2}} - \frac{p}{2}.a^{\frac{p-3}{2}}$ mod p^2.

If $\frac{p}{2}.a^{\frac{p-3}{2}} \equiv 0$ mod p^2 then $a^{\frac{p-3}{2}} \equiv 0$ mod p^2 which is a contradiction since 'a' is a semi primitive root mod p.

Therefore $x^{\frac{p-1}{2}} \neq 1$ modp^2

Hence there exists at least one semi primitive root mod p^{α} for α≥2.

Theorem: If 'a' is a primitive root mod p ad p = 4n +3 then –a is a semi primitive root mod p.

Proof: a is a primitive root mod p $\Rightarrow a^{p-1} \equiv 1$ mod p

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

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

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

$\Rightarrow (-a)^{\frac{p-1}{2}} \equiv 1$ mod p since $\frac{p-1}{2} = 2n+1$ is odd.

Let $\exp_p(-a) = f$ Then $f \mid \frac{p-1}{2}$.

If $f < \frac{p-1}{2}$ then $2f$ < p-1

Since $\exp_p(-a) = f$ we have $(-a)^{2f} \equiv 1$ mod p.$\Rightarrow a^{2f} \equiv 1$ mod p.This is a contradiction since a is a primitive root mod p.

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

Hence -a is a semi primitive root mod p.

Also it is clear that if ‘a’ is a semi primitive root mod p then $\exp_p(-a) = \frac{p-1}{4}$ where p is a prime of the form 4n +1 and n is odd.

References

[1]. Introduction to Analytic Number Theory, Springer International Student Edition.
[2]. An Introduction to Theory of Numbers by Ivan Niven, Herbert S. Zuckerman – Wiley Eastern Limited.
[3]. Elementary Number theory by David M .Burton.