NUMBER THEORY COURSE

LESSON : PRIMITIVE ROOTS-II

1. Composite numbers having primitve roots

Once the case of prime numbers is settled, the best approach to look at the corresponding problem for composite numbers is to look at the powers of primes first and then try to see if the probelm for an arbitrary composite can be reduced to its coprime factors. We follow more or less a similar approach but in this case the only even prime 2 plays a different and important role so we start with the following.

Theorem 1.1. *For $k > 2$, 2^k has no primitive root.*

Proof. We show that any odd integer a has order strictly less than $\varphi(2^k) = 2^{k-1}$ (Note that integers that are coprime to 2^k are precisely the odd numbers). To this end, we prove by induction on k that for any odd a, $a^{2^{k-2}} \equiv 1 \mod 2^k$. For $k = 3$, we have $a^{2^{k-2}} = a^2$ and $2^k = 8$. We know that for any odd a, $a^2 \equiv 1 \mod 8$ and therefore the result is true for $k = 3$. Now assume that for some k, $a^{2^{k-2}} \equiv 1 \mod 2^k$. Now

$$\begin{aligned} a^{2^{k-2}} &\equiv 1 \mod 2^k \\ \Rightarrow a^{2^{k-2}} &= 1 + b2^k \quad \text{for some } b, \end{aligned}$$

squaring both the sides we obtain

$$\begin{aligned} a^{2^{k-1}} &= \left(1 + b2^k\right)^2 \\ &= 1 + 2(b2^k) + b^2 2^{2k} \\ &= 1 + 2^{k+1}(b + b^2 2^{k-1}) \\ &\equiv 1 \mod 2^{k+1}. \end{aligned}$$

□

Once again, instead of moving to powers of odd primes, we move to composites of special types in order to cover all the negative results first.

Theorem 1.2. *Let a be a composite number that can be written as the product mn where both m and n are greater than 2 and are coprime then a has no primitive root.*

Proof. Since gcd $(m,\ n) = 1$, we have $\varphi(mn) = \varphi(m)\varphi(n)$. As usual, we shall prove that order of any integer a relatively prime to mn is strictly less than $\varphi(m)\varphi(n)$. We prove that $a^{\varphi(m)\varphi(n)/2} \equiv 1 \mod mn$ for any a with gcd $(a,\ mn) = 1$.Since $m, n > 2$, both $\varphi(m)$ and $\varphi(n)$ are even so that we may write $\varphi(m) = 2s$ and $\varphi(n) = 2t$. Now, by Euler's theorem,

$$a^{\varphi(m)} \equiv 1 \mod m,$$

and

$$a^{\varphi(n)} \equiv 1 \mod n.$$

(Note that gcd $(a,\ mn) = 1 \Rightarrow$ gcd $(a,\ m) = 1$ and gcd $(a,\ n) = 1$). Now, $a^{2st} \equiv (a^{2s})^t \equiv 1 \mod m$ and $a^{2st} \equiv (a^{2t})^s \equiv 1 \mod n$. Combining the two congruences, we get

$$a^{2st} \equiv 1 \mod mn,$$

but $2st = \varphi(m)\varphi(n)/2$ which establishes our claim. □

The theorem in itself is powerful enough to determine non-existence of primitive roots for a fairly large class of integers. The following Corollaries supports the claim.

Corollary 1.3. *If n is divisible by two odd primes then n has no primitive roots.*

Proof. Let p and q be two distinct prime divisors of n. We take m_1 to be the highest power of p that divides n and $m_2 = n/m_1$. Then, $m_1 > 2$ and as q is an odd prime that divides m_2, m_2 too is larger than 2. Moreover, gcd $(m_1,\ m_2) = 1$ and by the theorem $n = m_1m_2$ has no primitve roots. □

Corollary 1.4. *A number n of the form $2^m p^k$ where p is an odd prime and $m \geq 2$ has no primitve roots.*

Proof. Once again, we may take $n_1 = 2^m$ and $n_2 = p^k$. The thereom is straightaway applicable to the composite n_1n_2. □

Example 1.5. We start looking at composite numbers and observe whether they may have a primitive root or not.

Number	Has Primitive Roots (Y/N)	Explanation
4	Y	3 is a primitive root
6	Y	5 is a primitive root
8	N	$8 = 2^3$ (Th. 1.3)
9	Y	2 is a primitive root
10	Y	3 is a primitive root
12	N	$12 = 2^2 \times 3$ (Cor. 1.4)
14	Y	3 is a primitive root
15	N	$15 = 3 \times 5$ (Cor.1.3)

In the above example, we could determine that the composites 8, 12 and 15 have no primitive roots based on the results known so far. But it may be noted that for the composites where hypotheses of theorems 1.1 and 1.2 were not applicable, the answer was always Y. Though the table is too small to draw a conclusion, it will turn out that the indications may indeed be proved. In what follows, we will establish that composites of the types p^k and $2p^k$ indeed have primitive roots.

Lemma 1.6. *If p is an odd prime then there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \mod p^2$.*

Proof. Since p is a prime, it has a primitive root. Let r be any primiitve root of p. If $r^{p-1} \not\equiv 1 \mod p^2$ then we are done. Otherwise, if $r^{p-1} \equiv 1 \mod p^2$, take $r' = r + p$.

Since $r' \equiv r \mod p$, r' is also a primitive root of p. Now

$$\begin{aligned} r'^{p-1} &= (r+p)^{p-1} \\ &= r^{p-1} + \binom{p-1}{1} r^{p-2} p + \binom{p-1}{2} r^{p-3} p^2 + \ldots + p^{p-1} \\ &= r^{p-1} + (p-1)pr^{p-2} + p^2 y, \quad \text{for some integer } y \\ &\equiv r^{p-1} + (p-1)pr^{p-2} \mod p^2 \\ &\equiv 1 - pr^{p-2} \mod p^2, \end{aligned}$$

where the last congruence is obtained by using our assumption that $r^{p-1} \equiv 1 \mod p^2$. Therefore we have

$$(r')^{p-1} \equiv 1 - pr^{p-2} \mod p^2. \tag{1.1}$$

Now, if $(r')^{p-1} \equiv 1 \mod p^2$ then from eq (1.1), we must have $pr^{p-2} \equiv 0 \mod p^2$ which would imply that $p \mid r^{p-2}$. But this is not possible as gcd $(p,\ r) = 1$. □

Corollary 1.7. *If p is an odd prime then p^2 has a primitive root.*

Proof. By above lemma, there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \mod p^2$. Since gcd $(r,\ p) = 1$, we have gcd $(r,\ p^2) = 1$. We will prove that r is a primitive root of p^2. Let $k = Ord_{p^2} r$. Then k divides $\varphi(p^2) = p(p-1)$. Divisors of $p(p-1)$ are of the type $p^\alpha t$ where $\alpha = 0, 1$ and $t \mid (p-1)$. If $\alpha = 0$, we have $r^t \equiv 1 \mod p^2$. As $t \mid (p-1)$, we have $r^{p-1} \equiv 1 \mod p^2$ which contradicts the choice of r. If $\alpha = 1$ then $r^{pt} \equiv 1 \mod p^2$ which implies $r^{pt} \equiv 1 \mod p$. But by Fermat's theorem, $r^p \equiv r \mod p$ so that $r^{pt} \equiv r^t \equiv 1 \mod p$ which forces $t = p-1$ as r is a primitive root of p. Thus $Ord_{p^2} r = \varphi(p^2)$. □

Remark 1.1. Let p be an odd prime. In lemma 1.6 we have seen that if r is a primitive root of p then one of r and $r+p$ satisfies $r^{p-1} \not\equiv 1 \mod p^2$. From the Corollary 1.7, we conclude that either r or $r+p$ is a primitive root of p^2.

Lemma 1.8. *Let p be an odd prime and let r be a primitive root of p such that $r^{p-1} \not\equiv 1 \mod p^2$. Then for each postitve integer $k \geq 2$*

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k \tag{1.2}$$

Proof. The proof is by induction on k. $k = 2$ case is the part of the hypothesis of the theorem. Now assume that for some $k \geq 2$, (1.2) holds. We need to prove

$$r^{p^{k-1}(p-1)} \not\equiv 1 \mod p^{k+1}$$

Since gcd $(r,\ p^{k-1}) = 1$, by Euler's theorem,

$$r^{\varphi(p^{k-1})} \equiv 1 \mod p^{k-1}.$$

Since $\varphi(p^{k-1}) = p^{k-2}(p-1)$, we have

$$r^{p^{k-2}(p-1)} \equiv 1 \mod p^{k-1},$$

so that $r^{p^{k-2}(p-1)} = 1 + bp^{k-1}$ for some integer b with $p \nmid b$. Now,

$$\begin{aligned} r^{p^{k-1}(p-1)} &= r^{p^{k-2}p(p-1)} \\ &= \left(r^{p^{k-2}(p-1)}\right)^p \\ &= \left(1 + bp^{k-1}\right)^p \\ &= 1 + bp^k + \binom{p}{2}(bp^{k-1})^2 + \ldots + (bp^{k-1})^p \\ &\equiv 1 + bp^k \mod p^{k+1}. \end{aligned}$$

Since $p \nmid b$, $p^{k+1} \nmid bp^k$ and therefore

$$r^{p^{k-1}(p-1)} \not\equiv 1 \mod p^{k+1}.$$

□

Theorem 1.9. *If p is an odd prime number and $k \geq 1$, then there exists a primitive root for p^k.*

Proof. Let r be a primitive root of p satisfying

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k.$$

We prove that this r is a primitive root of p^k. Let $Ord_{p^k} r = \ell$ then ℓ must be of the form $p^\alpha t$ where $0 \leq \alpha \leq k-1$ and $t \mid (p-1)$. $\alpha < k-1$ would contradict the choice of r. So $\ell = p^{k-1}t$. Now, $r^\ell \equiv 1 \mod p^k \Rightarrow r^\ell \equiv 1 \mod p$. But $r^{p^{k-1}} \equiv r \mod p$ therefore $r^\ell \equiv r^t \equiv 1 \mod p$. This forces $t = p - 1$. Thus $\ell = \varphi(p^k)$ and the proof is complete. □

Corollary 1.10. *There are primitive roots for $2p^k$ where p is an odd prime and $k \geq 1$.*

Proof. Let r be a primitive root of p^k. One of the two numbers r or $r + p^k$ is odd and both are primitive roots of $2p^k$ (Since $r + p^k \equiv r \mod p^k$). So we may assume r to be odd. Let ℓ be the order of r modulo $2p^k$. This order is defined as gcd $(r, 2p^k) = 1$. Since $\varphi(2p^k) = \varphi(p^k)$, ℓ must divide $\varphi(p^k)$. But $r^\ell \equiv 1 \mod 2p^k \Rightarrow r^\ell \equiv 1 \mod p^k$ and therefore $\varphi(p^k)$ divides ℓ. Hence $\ell = \varphi(p^k) = \varphi(2p^k)$. □