Unit 9: PRIMITIVE ROOTS AND INDICES

UNIT STRUCTURE

9.1 Learning Objectives
9.2 Introduction
9.3 The order of an integer modulo$n$
9.4 Primitive roots
9.5 Primitive roots for primes
9.6 Composite numbers having primitive roots
9.7 The theory of indices
9.8 Let Us Sum Up
9.9 Answers to Check Your Progress
9.10 Further Reading
9.11 Model Questions

9.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of congruences and the order of an integer modulo n
- Define and identify primitive roots.
- Recognize integers for which primitive roots exist.
- Explain the theory of indices and how it simplifies calculations in modular arithmetic.
- Apply primitive root and index techniques to solve number theoretic problems.

9.2 INTRODUCTION

In number theory, the study of congruences forms a foundation for many advanced concepts. One such important idea is that of primitive roots, which allows us to describe all non-zero residues modulo n in terms of powers of a single integer. This has deep applications in solving congruences, constructing cyclic groups, and also in modern areas like cryptography.

A closely related idea is the order of an integer modulo n, which tells us how many times we must multiply the number by itself to get 1 under modular arithmetic. When an integer has maximum possible order modulo n, it is called a primitive root modulo n.

Furthermore, indices (or discrete logarithms) provide a powerful tool for simplifying computations involving primitive roots.

9.3THE ORDER OF AN INTEGER MODULO n

If $n > 1$ is any integer and a is another integer such that $(a,n) = 1$.Then the order of a of modulo n is the smallest positive integer k such that $a^k \equiv 1(mod\ n)$.

We consider the successive powers of 2 modulo 7.

$2^1 \equiv 2(mod 7), 2^2 \equiv 4(mod 7), 2^3 \equiv 1(mod 7), 2^4 \equiv 2(mod 7), 2^5 \equiv 4(mod 7),$

$2^6 \equiv 1(mod 7), \cdots,$

From which it follows that the integer 2 has order 3 modulo 7.

Example 1: The order of 2 modulo 7 is 3.

We have $2^1 \equiv 2(mod\ 7)$

$$2^2 \equiv 4(mod\ 7)$$

$$2^3 \equiv 1(mod\ 7)$$

∴The order of 2 modulo 7 is 3.

Example 2: The order of 3 modulo 8 is 2.

We have $3^1 \equiv 3(mod\ 8)$

$$3^2 \equiv 1(mod\ 8)$$

∴The order of 3 modulo 8 is 2.

Example 3: The order of 2 modulo 8 is not defined.

We have $2^1 \equiv 2(mod\ 8)$

$$2^4 \equiv 4(mod\ 8)$$

$$2^3 \equiv 0(mod\ 8)$$

.

.

.

$$2^n \equiv 0(mod\ 8) \forall\ n \geq 3.$$

∴ The order of 2 modulo 8 is not defined.

Now, our first theorem will clarify why certain integers possess an order modulo a given integer, while others do not have any order defined modulo that integer.

Theorem 9.3.1: If a is an integer having order k modulo n i.e.,$a^k \equiv 1(mod\ n)$,then

(i) $a^h \equiv 1(mod\ n)$ for some integer h then $k|h$

(ii) $a \equiv b\ (mod\ n) \Rightarrow b$ has order k modulo n.

(iii) $a^i \equiv a^j (mod\ n) \Leftrightarrow i \equiv j (mod\ k)$

(iv) $(a, n) = 1$ i.e., a and k are coprime.

Proof: (i) If $a^h \equiv 1\ (mod\ n)$,then by definition of order $h \geq k$.

By division algorithm we have

$h = kq + r, \quad 0 \leq r < k$

Therefore, $a^h = a^{kq+r}$

$$= a^{kq}.a^r$$

$$\equiv 1^q.a^r (mod\ n)$$

Or $1(mod\ n) \equiv a^r (mod\ n)$

Or $a^r \equiv 1(mod\ n)$ (1)

But $r < k$ (the order of a),therefore (1) holds only when $r = 0$. So $h = kq$ or $\frac{h}{k} = q$.

Thus,$k|h$.

(ii) If $a \equiv b(mod\ n)$,then $a^k \equiv b^k (mod\ n)$

$\Rightarrow 1(mod\ n) \equiv b^k (mod\ n)$ [$\because k$ is the order of a]

$\Rightarrow b^k \equiv 1(mod\ n)$.

This shows that order of b is k modulo n.

(iii) We have, $a^i \equiv a^j (mod\ n)$

$$\Leftrightarrow a^{|i-j|} \equiv 1(mod\ n)$$

$$\Leftrightarrow h||i - j|$$

$\Leftrightarrow i \equiv j(mod\ h)$.

(v) Let $d > 1$ be a common divisor of a and n.Then $d|a$ and $d|n$.

Since $a^k \equiv 1(mod\ n)$

$a^k = 1 + \lambda n$ for some integer λ.

Now $d|a \Rightarrow d|a^k$,also $d|n$.

$$\therefore \quad d|a^k - \lambda n = 1$$

$\Rightarrow d = 1$.

Theorem 9.3.2: If a has order k mod n, then a^h has order $\frac{k}{d}$ where $d = (k, h)$.

Proof: Let a^h has order t modulo n.

Then $\left(a^h\right)^t \equiv 1(mod\ n)$

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

Also a has order k mod n.

Therefore $k|ht$

Now since $d = (k, h)$,we have integers k_1, h_1 such that $k = dk_1$,$h = dh_1$,$(k_1, h_1) = 1$.

So, $k|ht \Rightarrow k_1 d|h_1 dt$

$\Longrightarrow k_1|t$ $[\because (k_1, h_1) = 1]$

$\Rightarrow \frac{k}{d}|t$ (1)

Now $\left(a^h\right)^{k/d} = \left(a^h\right)^{k_1}$

$$= \left(a^{dh_1}\right)^{k_1}$$

$$= \left(a^{dk_1}\right)^{h_1}$$

$$= \left(a^k\right)^{h_1}$$

$$\equiv 1(mod\ n)$$

Therefore $t|\frac{k}{d}$ (2)

From (1) and (2), we have

$t = \frac{k}{d}$.

Corollary 1: Ifa has order h modulo n.Then a^h has order k modulo n iff $(h, k) = 1$.

Theorem 9.3.3: If the orders of $a_1$and $a_2$modulo $n$be $k_1$and $k_2$respectively and $(k_1, k_2) = 1$.Then the order of $a_1 a_2 (mod\ n)$is $k_1 k_2$.

Proof: Let the order of $a_1 a_2 (mod\ n) \equiv k$.

Then $(a_1 a_2)^k \equiv 1(mod\ n)$

$$\Rightarrow [(a_1 a_2)^k]^k \equiv 1(mod\ n)$$

$$\Rightarrow a_1^{kk_2} . a_2^{kk_2} \equiv 1(mod\ n)$$

$\Rightarrow a_1^{kk_2} \equiv 1(mod\ n)[\because a_2^{k_2} \equiv 1(mod\ n)]$

$\Rightarrow k_1|kk_2$.

But $(k_1, k_2) = 1$.Therefore, $k_1|k$. (1)

Similarly, we can show that, $k_2|k$. (2)

From (1) and (2), we have

$k_1 k_2|k$. (3)

Now $a_1^{k_1 k_2} \equiv 1(mod\ n)$ and $a_2^{k_1 k_2} \equiv 1(mod\ n)$

$$(a_1 a_2)^{k_1 k_2} \equiv 1(mod\ n)$$

$\Rightarrow k|k_1 k_2$ (4)

From (3) and (4), we have

$k = k_1 k_2$.

Example 4: Find the order of $5\ (mod\ 29)$.

Solution: We have $\phi(29) = 29 - 1 = 28 = 2^2 \times 7$.

The divisors of $\phi(29)$ are 2,4,7,14,28.

Now $5^2 \equiv -4(mod\ 29)$

$$5^4 \equiv 16(mod\ 29)$$

$$5^7 = 5^4 \times 5^2 \times 5$$

$$\equiv 16 \times (-4) \times 5(mod\ 29)$$

$$\equiv -1(mod\ 29)$$

$$5^{14} \equiv 1\ (mod\ 29)$$

∴ order of 5 modulo 29 is 14.

W CHECK YOUR PROGRESS

Q1) Show that order of 3 modulo 9 is not defined.

Q2) Show that order of 3 modulo 5 is 4.

Q3) What condition must be satisfied for an integer a to have an order modulo n?

Q4) Find the order of 5 modulo 14.

Q5) Determine the order of 3 modulo 10.

9.4 PRIMITIVE ROOTS

If an integer a has order $\phi(n)$ modulo n (a positive integer) and $(a, n) = 1$, then a is a primitive root of n.

Thus, n has a primitive root a if

$a^{\phi(n)} \equiv 1(mod\ n)$ and $a^k \equiv 1\ (mod\ n) \forall\ k < \phi(n)$.

Example 5: List the primitive roots modulo 6.

Solution: We have $\phi(6) = 2$; and any integer (mod 6) is congruent to one of 0,1,2,3,4 or 5. Therefore, the primitive roots (mod 6) will be amongst 2,3,4,5.

Now, $2^2 \equiv 4\ (mod\ 6)$

$$3^2 \equiv 3(mod\ 6)$$

$$4^2 \equiv 2(mod\ 6)$$

and $5^2 \equiv 1(mod\ 6)$.

Thus, we observe that 5 is the only primitive root (mod 6).

Example 6: Find the primitive roots of 15.

Solution: We have $\phi(15) = \phi(3.5)$

$$= \phi(3).\phi(5)$$

$= (3-1)(5-1) = 8 = 2^3$.

This means that if a primitive root exists modulo 15, its order must be 8.

Therefore 2 is the only prime divisor of $\phi(15)$.

The possible coprime to 15 are 1,2,4,7,8,11,13,14.

Therefore, Possible primitive roots must be among are 2,7,11,13. [Because 1 is trivial; 4, 8, 14 will repeat earlier powers.]

To be a primitive root mod 15, a number must have order 8.

Now$2^4 \equiv 1(mod\ 15)$

Since it becomes 1 at power 4 (not 8), 2 **is not** a primitive root.

$7^4 \equiv 1(mod\ 15)$,

So, 7 is not a primitive root.

$$13^4 \equiv 1(mod\ 15)$$

So, 7 is not a primitive root.

$$4^2 \equiv 1(mod\ 15)$$

So, 4 is not a primitive root.

$$11^2 \equiv 1(mod\ 15)$$

So, 11 is not a primitive root.

This shows that there exists no primitive root of 15.

Theorem 9.4.1: If a is a primitive root modulo n ,then $a, a^2, \cdots, a^{\phi(n)}$ is a reduced system $(mod\ n)$.

Proof: Since a is a primitive root $mod\ n$, we have $(a, n) = 1$.

$\Rightarrow (a^k, n) = 1, 1 \leq k \leq \phi(n)$

The integers $a, a^2, \cdots, a^{\phi(n)}$ are in congruent $(mod\ n)$.

Let r be an integer coprime to n.

We have to show that

$r \equiv a^n (mod\ n)$ for some h

Satisfying $1 \leq h \leq \phi(n) - 1$.Let $a_1, a_2, \cdots, a_{\phi(n)}$ be the reduced system $(mod\ n)$ having all integers less than or equal to n.Then $r \equiv a_i (mod\ n)$ for some unique i satisfying $1 \leq i \leq \phi(n)$.

For k satisfying $1 \leq k \leq \phi(n) - 1$, there exists a unique j such that

$$a^k \equiv a_j (mod\ n)$$

Therefore, if $a_j \equiv a^h (mod\ n), 1 \leq h \leq \phi(n) - 1$

Then $r \equiv a^h (mod\ n)$.

Hence, $a, a^2, \cdots, a^{\phi(n)}$ is a reduced system $(mod\ n)$.

W CHECK YOUR PROGRESS

Q6) Show that 3 is a primitive root of 7.

Q7) List the primitive roots modulo 7.

Q8) List the primitive roots modulo 8.

Q9) Find the primitive roots of 10.

9.5 PRIMITIVE ROOTS FOR PRIMES

Theorem 9.5.1: (Lagrange Theorem) : Let$p$ is a prime and let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is a polynomial of degree $n \geq 1$ with integral coefficient, where

$$a_n \not\equiv 0 (mod\ p)$$

Then the congruence $f(x) \equiv 0 (mod\ p)$ has at most$n$ incongruent solutions modulo$p$.

Proof: We proceed by induction on n,the degree of $f(x)$.

If$n = 1$, the given polynomial is of the form

$f(x) = a_1 x + a_0$ (1)

Since $(a_1, p) = 1$, Theorem (Linear congruence) state that the congruence$a_1 x \equiv -a_0 (mod\ p)$ has a unique solution modulo p.

Hence, the theorem is true for $n = 1$.

Let the theorem be true for $n = m - 1$ solutions i.e., $f(x) \equiv 0 (mod\ p)$ has $m - 1$ incongruent solutions.Let $f(x)$ be a function of degree m.Then either $f(x) \equiv 0 (mod\ p)$ has no solution and we have nothing to do or at least one solution (say a).

If $f(x)$ is divided by $x - a$,the result is

$f(x) = (x - a)q(x) + r$ (2)

where $q(x)$ is a polynomial of degree $(m - 1)$ with integral coefficients and r is an integer.

Putting $x = a$ in (2), we obtain

$$0 \equiv f(a) = (a - a)q(a) + r = r (mod\ p)$$

And therefore $f(x) \equiv (x-a)q(x)(mod\ p)$

If b is another one of the incongruent solutions of $f(x) \equiv 0(mod\ p)$,then

$$0 \equiv f(b) = (b-a)q(b)(mod\ p)$$

Because $b - a \not\equiv 0(mod\ p)$,we may cancel to conclude that $q(b) \equiv 0(mod\ p)$;in other words,any solution of f$(x) \equiv 0(mod\ p)$ that is different from a must satisfy $q(x) \equiv 0(mod\ p)$.By our induction assumption,the latter congruence can possess at most $m-1$ incongruent solutions,and therefore $f(x) \equiv 0(mod\ p)$ has no more than m incongruent solutions.

This completes the induction step.

Hence the proof.

Theorem 9.5.2: If p is a prime and $d|p-1$,then the congruence $x^d - 1 \equiv 0(mod\ p)$ has exactly d solutions.

Proof: Since $d|p-1$,we have $p-1 = dr$ for some r.

Therefore $x^{p-1} - 1 = \left(x^d - 1\right)f(x)$

Where $f(x) = x^{d(r-1)} + \cdots + x^d + 1$ has integral coefficients and is of degree

$$d(k-1) = p - 1 - d.$$

By Lagrange's theorem, the congruence $f(x) \equiv 0(mod\ p)$ has at most $p-1-d$ solutions.

We also know from Fermat's theorem that $x^{p-1} - 1 \equiv 0(mod\ p)$ has $p-1$ incongruent solutions $1,2,\cdots,p-1$.

Now any solution $x = a$ of $x^{p-1} - 1 \equiv 0(mod\ p)$ that is not a solution of $f(x) \equiv 0(mod\ p)$ should satisfy

$x^d - 1 \equiv 0(mod\ p)$.

Now,$0 \equiv a^{p-1} - 1 = \left(a^d - 1\right)f(a)(mod\ p)$

With $p \nmid f(a)$,implies that $p|a^d - 1$.

Therefore,$x^d - 1 \equiv 0(mod\ p)$ must have at least $p-1-(p-1-d) = d$ solutions.

The last congruence possesses d solutions and hence, exactly$d$ solutions.

Theorem 9.5.3: If p is a prime and $d|p-1$,then there are exactly $\phi(d)$ incongruent integers having d modulo p.

Proof: Since $d|p-1$ and $\psi(d)$denote the number of integers $k, 1 \le k \le p-1$,that have order d modulo p.

Now since each integer between 1 and $p-1$ has order d for some $d|p-1$.

$p - 1 = \sum_{d|p-1} \psi(d)$ (1)

Also by Gauss theorem, we have

$p-1=\sum_{d|p-1}\phi(d)$ (2)

From (1) and (2)

$\sum_{d|p-1}\psi(d)=\sum_{d|p-1}\phi(d)$ (3)

Given an arbitrary divisor d of $p-1$,there are two possibilities: we either $\psi(d)=0$ or $\psi(d)>0$. If $\psi(d)=0$,then certainly $\psi(d)\leq\phi(d)$.

Suppose that $\psi(d)>0$,so that there exists an integer a of order d.Then the d integers $a,a^2,\cdots,a^d$ are incongruent modulo p and each of them satisfies the polynomial congruence $x^d-1\equiv 0(mod\ p)$. (4)

By Theorem Theorem9.6, there will be no other solutions of (4).

Therefore, any integer that has order d modulo p should be congruent of $a,a^2,\cdots,a^d$.

But $\phi(d)$ of these powers has order d.Therefore $\psi(d)=\phi(d)$.

Hence, the number of integers having order d modulo p is equal to $\phi(d)$.

Theorem 9.5.4: If$(a,m)=1$,then a is a primitive root of $m$if and only if$a^{\frac{\phi(m)}{p}}\not\equiv 1(mod\ m)$ for every prime divisor$p$ of $\phi(m)$.

Proof: We assume that

$$a^{\frac{\phi(m)}{p}}\not\equiv 1(mod\ m)$$

for every prime divisor p of $\phi(m)$.

We want to prove that a is a primitive root of m.

Suppose if possible a is not a primitive root of m.Then the order of $a(mod\ m)$ is some integer r less than $\phi(m)$.This gives that r divides $\phi(m)$.

Thus, we have that $\frac{\phi(m)}{r}$ is an integer and so it is divisible by some prime divisor p of $\phi(m)$.

Therefore,$a^{\frac{\phi(m)}{p}}=(a^r)^{\frac{\phi(m)}{rp}}\equiv 1(mod\ m)$ $[\because a^r\equiv 1(mod\ m)]$

Hence, the assumption that a is not a primitive root is wrong.

Therefore, a must be a primitive root.

Conversely, let$a$ is a primitive root of m.

Then,$a^{\phi(m)}\equiv 1(mod\ m)$ and $a^k\not\equiv 1(mod\ m)$ for $0<k<\phi(m)$

Now, for any prime divisor p of $\phi(m)$:

$$\frac{\phi(m)}{p}<\phi(m)$$

Therefore, by the definition of primitive root,

$$a^{\frac{\phi(m)}{p}} \not\equiv 1(mod\ m)$$

for every prime divisor p of $\phi(m)$.

Example 7: Find a primitive root $mod 5^2$.

Solution: We have that 2 is a primitive root of 5.

Also $2^2 \equiv 4(mod\ 5), 2^3 \equiv 3(mod\ 5), 2^4 \equiv 1(mod\ 5)$

Further $2^4 \not\equiv 1(mod\ 5^2), 2^5 \equiv 7(mod\ 5^2), 2^6 \equiv 14(mod\ 5^2), 2^7 \equiv 3(mod\ 5^2), \cdots,$

$2^{20} \equiv 1(mod\ 5^2)$.

Therefore,2 is a primitive root $(mod\ 5^2)$.

Similarly, we can show that 3 is a primitive root $(mod\ 5^2)$.

Example 8: Find the primitive roots 17.

Solution: We have $\phi(17) = 17 - 1 = 16 = 2^4$.

Thus, $\phi(17)$ has only one prime factor 2. Also$\left(\frac{16}{2}\right) = 8$.

Therefore,a is a primitive root of 17if $a^8 \not\equiv 1(mod\ 17)$.

Now,$2^8 \equiv 1(mod\ 17)$.

and $3^8 \not\equiv 1(mod\ 17)$.

Thus, 3 is the smallest primitive root of 17.

Similarly, we can show that

$$5^8 \not\equiv 1(mod\ 17)$$
$$6^8 \not\equiv 1(mod\ 17)$$
$$7^8 \not\equiv 1(mod\ 17)$$
$$10^8 \not\equiv 1(mod\ 17)$$
$$11^8 \not\equiv 1(mod\ 17)$$
$$12^8 \not\equiv 1(mod\ 17)$$
$$14^8 \not\equiv 1(mod\ 17)$$

Thus, the primitive roots of 17 are 3,5,6,7,10,11,12 and 14.

Composite numbers having primitive roots

9.6 COMPOSITE NUMBERS HAVING PRIMITIVE ROOTS

In this section, we will discuss those composite numbers that possess primitive roots.

Theorem 9.6.1: For $n \geq 3$,the integer 2^n has no primitive roots.

Proof: Let a be an odd integer.

We will show that $a^{2^{n-2}} \equiv 1(mod\ 2^n)$ for $n \geq 3$

For $n = 3$,we have

$$a^2 \equiv 1(mod\ 3)$$

We have $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1(mod\ 3)$ [$\because a$ is odd]

Thus,$a^2 \equiv 1(mod\ 8)$.

Suppose the statement holds for $n = m \geq 3$ i.e.,

$$a^{2^{m-2}} \equiv 1(mod\ 2^m)$$

This is equivalent to the equation

$a^{2^{m-2}} = 1 + \lambda 2^m$ where λ is an integer.

Squaring both sides, we obtain

$$a^{2^{m-1}} = \left(a^{2^{m-2}}\right)^2 = 1 + 2(\lambda 2^m) + (b2^m)^2$$

$$= 1 + 2^{m+1}(\lambda + \lambda^2 2^{m-1})$$

$$\equiv 1(mod\ 2^{m+1})$$

This shows that the result is true for $n = m + 1$.

Hence,by mathematical induction the result is true for all values of n.

Also,the integers relatively prime to 2^m are the odd integers and $\phi(2^m) = 2^m - 1$.

Therefore $a^{\phi\left(\frac{2^m}{2}\right)} \equiv 1(mod\ 2^m)$

and hence there is no primitive root of 2^m.

Theorem 9.6.2: If $m, n > 2$ and $(m, n) = 1$,then there exists no primitive root $(mod\ mn)$.

Proof: Suppose that$a$ is a primitive root to mn i.e., order of $a = \phi(mn)$.

Then $(a, mn) = 1$ and a has order $\phi(mn) mod\ mn$.

Now $(a, mn) = 1 \Rightarrow (a, m) = 1$ and $(a, n) = 1$.

Now, by Euler's Theorem,$a^{\phi(m)} \equiv 1(mod\ m)$ and $a^{\phi(n)} \equiv 1(mod\ n)$

Let $h = \frac{\phi(m)\phi(n)}{[\phi(m)\phi(n)]}$ (1)

Since $m, n > 2$,we have

$\big(\phi(m), \phi(n)\big) \geq 2$ [$\because$ $\phi(m)\phi(n)$both are even] (2)

From (1) and (2),we have

$$h \leq \frac{\phi(m), \phi(n)}{2} = \frac{\phi(mn)}{2}$$

$$< \phi(mn)$$

Now $a^h = \big(a^{\phi(m)}\big)^{\frac{\phi(n)}{(\phi(m),\phi(n))}} \equiv 1(mod\ m)$ (3)

And $a^h = \big(a^{\phi(n)}\big)^{\frac{\phi(m)}{(\phi(m),\phi(n))}} \equiv 1(mod\ n)$ (4)

From (3) and (4), we have

$a^h \equiv 1(mod\ mn)$ [$\because$ $(m, n) = 1$]

This contradicts the assumption that order of a is $\phi(mn)$.

Theorem 9.6.3: 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 an odd prime, it has a primitive root. Let r be the primitive root of p.

If $r^{p-1} \not\equiv 1(mod\ p^2)$, then the proof is complete. If$r^{p-1} \equiv 1(mod\ p^2)$,we replace r by r_1 given by $r_1 = r + p$ which is also a primitive root of p.

Now $r_1^{p-1} \equiv (r + p)^{p-1}$

$$\equiv r^{p-1} + (p-1)pr^{p-2}(mod\ p^2)$$

$$\equiv 1 + (p-1)pr^{p-2}(mod\ p^2)[\because\ r^{p-1} \equiv 1(mod\ p^2)]$$

$$\equiv (1 - pr^{p-2})(mod\ p^2)$$

Since r be the primitive root of p, we have $(r, p) = 1$.

Therefore$p \nmid r^{p-1}$.

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

Corollary: Ifp is an odd prime, thenp^2 has a primitive root. In other words, for a primitive root r of p,either r or $r+p$ (or both) is a primitive root of p^2.

Theorem 9.6.4: If p is an odd prime and r a primitive root of p such that $r^{p-1} \not\equiv 1(mod\ p^2)$ then for each positive integer$k \geq 2$,

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

Proof: For $k=2$,the result is true by the hypothesis. Let the result be true for $k \geq 2$.

We shall show that the result is true for $k+1$.

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

$$r^{p^{k-2}(p-1)}=r^{\phi\left(p^{k-1}\right)} \equiv 1\left(mod\ p^{k-1}\right)$$

Hence, there exists an integer a such that

$$r^{p^{k-2}(p-1)}=1+ap^{k-1}, p \nmid a$$

Raise both sides of this equation to the pth power and expand to obtain

$$r^{p^{k-1}(p-1)}=\left(1+ap^{k-1}\right)^p$$

$$\equiv 1+ap^k\left(mod\ p^{k+1}\right)$$

Since $p \nmid a$,we have

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

This shows that the result is true for $k+1$.

Hence, by mathematical induction the given result will be true for all values of $k \geq 2$.

Theorem 9.6.5: There exists a primitive root for p^k when p is an odd prime and $k \geq 1$.

Proof: Let p be an odd prime. If$k=1$,there exists a primitive root $(mod\ p)$.

For $k>1$,let r be a primitive root$(mod\ p)$.

Then as shown in theorem9.12.

We have

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

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

We will show that r is a primitive root for all powers of p.

Let n be the order of $r\ mod\ p^k$.Then n must divide $\phi(p^k) = p^{k-1}(p-1)$.

Also $r^n \equiv 1(mod\ p^k)$ implies $r^n \equiv 1(mod\ p)$ and $(p-1)|n$.

Therefore,n takes the form $n = p^{n_1}(p-1), 0 \leq n_1 \leq k-1$.

Now, if $n \neq p^{k-1}(p-1)$ then $p^{k-2}(p-1)$ is divisible by n and we can write

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

This contradicts the initial assumed value of r.

Therefore,$n = p^{k-1}(p-1)$ and r is a primitive root of p^k.

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

Proof: Let r be an odd primitive root for p^k.Then $(r, 2p^k) = 1$.Then order n of r modulo $2p^k$ should divide

$$\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$$

Now,$r^n \equiv 1(mod\ 2p^k) \Rightarrow r^n \equiv 1(mod\ p^k)$.

Therefore, $\phi(p^k)|n$, so $n = \phi(2p^k)$.

Hence,r is a primitive root of$2p^k$.

Example 9: Find the primitive root of 15.

Solution: The relatively primes to 15 are 2,4,7,8,11,13,14.

Also, $\phi(15) = \phi(3.5)$

$$= (3-1)(5-1)$$

$= 2.4 = 8 = 2^3$.

This means the only prime divisor of $\phi(15)$ is 2.

$\frac{\phi(m)}{p} = \frac{\phi(15)}{2} = \frac{8}{2} = 4.$

Now a is a primitive root of 15 if$a^{\frac{\phi(15)}{2}} = a^4 \not\equiv 1(mod\ 15)$.

We have $2^4 \equiv 1(mod\ 15)$

$$4^4 \equiv 1(mod\ 15)$$

$$7^4 \equiv 1(mod\ 15)$$

$$8^4 \equiv 1(mod\ 15)$$

$$11^4 \equiv 1\ (mod\ 15)$$

$$13^4 \equiv 1(mod\ 15)$$

$$14^4 \equiv 1(mod\ 15)$$

Since every number relatively prime to 15 satisfies$a^4 \equiv 1(mod\ 15)$.

no number has order 8 modulo 15.

Therefore, there exists no primitive root of 15.

9.7 THE THEORY OF INDICES

If r is a primitive root of n and$(a, n) = 1$,then the smallest positive integer h such that $a \equiv r^h(mod\ n)$ is called the index of a relative to r.

Customarily, we denote the index of a relative to r by $ind_r a$.

Clearly,$1 \leq ind_r a \leq \phi(n)$ and

$$r^{ind_r a} \equiv a(mod\ n)$$

For example, the integer 2 is a primitive root of 5 and

$2^1 \equiv 2\ ,2^2 \equiv 4\ ,2^3 \equiv 3,2^4 \equiv 1(mod\ 5)$

It follows that

$ind_2 1 = 4,ind_2 2 = 1,ind_2 2 = 1,ind_2 4 = 2.$

Example 10: Find the index of 3 $(mod\ 5)$.

Solution: A primitive root modulo 5 is 2 (the smallest one).

Now, we compute powers of 2 modulo 5

$2^1 = 2\ ,2^2 = 4\ ,2^3 = 8 \equiv 3(mod\ 5).$

We observe that $2^3 \equiv 3(mod\ 5)$

The index of 3 relative to the primitive root 2 is:

$ind_2(3) = 3.$

Example 11: Find the index of 9 (mod 19)

Solution: The smallest primitive root of 19 is 2.

This means all numbers that are coprime to 19 can be written as some power of 2 (mod 19).

Now, we check powers of 2:

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,2^4 = 16,2^5 = 32 \equiv 13,2^6 = 64 \equiv 7\ ,2^7 = 128 \equiv 14,$

$2^8 = 256 \equiv 9\ .$

So,$2^8 \equiv 9(mod\ 19).$

Therefore, $ind_2 9 = 8.$

or simply $ind.\ 9 = 8.$

Example 12: Find the index of 5 $(mod\ 13).$

Solution: The smallest primitive root of 13 is 2.

This means every number coprime to 13 can be written as some power of 2 (mod 13).

Now,we check powers of 2 modulo 13:

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8\ ,2^4 = 16 \equiv 3,2^5 = 32 \equiv 6,2^6 \equiv 12,2^7 \equiv 11,2^8 \equiv 9,$

and $2^9 = 512 \equiv 5\ (mod\ 13).$

Therefore, $ind._2\ 5 = 9.$

The other primitive roots of 13 are:6,7,11.

Also,$6^9 \equiv 5(mod\ 13)$

$$\therefore ind._6 5 \equiv 9$$

and, $7^3 \equiv 5(mod\ 13)$

$$\therefore ind._7 5 \equiv 3$$

and, $11^3 \equiv 5(mod\ 13)$

$\therefore ind._{11} 5 \equiv 3.$

Note: Indices follow rules similar to those of logarithms, with the primitive root acting like the base of a logarithm.

Theorem 9..6.6: Let a be a primitive root modulo n and b,c and k are any integers, then

(i) $b \equiv c(mod\ n) \Rightarrow ind.b \equiv ind.c\big(mod\ \phi(n)\big)$

(ii) $ind.(bc) \equiv ind.b + ind.c\big(mod\ \phi(n)\big)$

(iii) $ind.b^k \equiv k\ ind.b\big(mod\ \phi(n)\big)$ for $k > 0$.

(iv) $ind.1 \equiv 0\big(mod\ \phi(n)\big)$

Proof: Let $ind.b = r_1$ and $ind.c = r_2$.

Then $b \equiv a^{r_1}(mod\ n)$ and $c \equiv a^{r_1}(mod\ n)$

(i) Suppose, $b \equiv c(mod\ n)$

$$\Rightarrow a^{r_1} \equiv a^{r_2}(mod\ n)$$

$$\Rightarrow a^{r_1 - r_2} \equiv 1(mod\ n)$$

By definition, $\phi(n) | r_1 - r_2$

$$\therefore r_1 \equiv r_2[mod\ \phi(n)]$$

$$i.e. ind.b \equiv ind.c\big(mod\ \phi(n)\big)$$

(ii) We have

$$bc \equiv a^{r_1}.a^{r_2}(mod\ n)$$

$$\equiv a^{r_1 + r_2}(mod\ n)$$

Now,if$r = ind.bc$ then $bc \equiv a^r (mod\ n)$

$$\therefore \qquad r_1 + r_2 \equiv r\big(mod.\phi(n)\big)$$

i.e., $ind.(bc) = ind.b + 1\ ind.c\big(mod\ \phi(n)\big)$

(iii) We have

$$ind.b^k = ind.(b.b\ \cdots k\ times)$$

$= ind.b + ind.b + \cdots upto\ k\ times\ \big(mod\ \phi(n)\big)$.[using (ii)]

$= k\ ind.b\big(mod\ \phi(n)\big)$.

(iv)Putting $k = 0$ in (iii) ,we have

$ind.1 = 0\big(mod\ \phi(n)\big)$.

Theorem 9.6.7: If r is the smallest primitive root of n and $r^h \equiv a(mod\ n)$,then $h \equiv ind.a(mod\ n)$.

Proof: We have

$$r^h \equiv a(mod\ n)$$

$$\equiv r^{ind.a}(mod\ n)$$

Now the order of $r(mod\ n)$ is $\phi(n)$.

Therefore, $h = ind.a[mod\ \phi(n)]$.

Theorem 9.6.8: If $a_1, a_2, \cdots, a_k$ are all primes to $n[mod\ \phi(n)]$.

Then,$ind.a_1 + ind.a_2 + \cdots + ind.a_k = ind.a_1 a_2 \cdots a_k$.

Proof:If r is the smallestprimitive root of n,then we have

$$r^{ind.a_1} \equiv a_1(mod\ n)$$

$$r^{ind.a_1} \equiv a_1 (mod\ n)$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$r^{ind.a_k} \equiv a_k (mod\ n)$$

Therefore,

$r^{ind.a_1+ind.a_1+\cdots+ind.a_k} \equiv a_1 a_2 \cdots a_k (mod\ n)$.

Hence,

$ind.a_1 + ind.a_2 + \cdots + ind.a_k \equiv a_1 a_2 \cdots a_k \big(mod\ \phi(n)\big)$.

Note: The theory of indices can be applied to solve congruences.

Example 13: Solve the linear congruence:$7x \equiv 2(mod\ 9)$

Solution: We know that 2 is a primitive root modulo 9.

Now, $2^1 = 2$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 \equiv 7(mod\ 9)$$

$$2^5 \equiv 5(mod\ 9)$$

$$2^6 \equiv 1(mod\ 9)$$

This gives that index of 2 is 1 and 7 is 4.

The given congruence $7x \equiv 2(mod\ 9)$ is equivalent to

$$ind.7 + ind.x \equiv ind.2\big(mod\ \phi(9)\big)$$

$$\Rightarrow 4 + ind.x \equiv 1(mod\ 6)[\because\ \phi(9) = 6]$$

$$\Rightarrow ind.x \equiv -3(mod\ 6)$$

$$\equiv 3(mod\ 6)$$

$$\Rightarrow x \equiv 2^3(mod\ 9)$$

$$\equiv 8(mod\ 9)$$

This gives that the solution of the given congruence are of the form $9t + 8$ where $t = 0, \pm 1, \cdots$.

Example 14: Solve the congruence $17x^{20} \equiv 19(mod\ 37)$.

Solution: The given congruence is equivalent

$$ind.17 + 20\ ind.x = ind.19\big(mod\ \phi(37)\big)$$

$$\Rightarrow 7 + 20\ ind.x = 35(mod\ 36)[\because\ \phi(37) = 36]$$

$$\Rightarrow 20\ ind.x \equiv 28(mod\ 36)$$

$\Rightarrow ind.x = 5,14,23,32\ (mod\ 36)$.

The integers corresponding to these indices are 32,30,5,7.

Therefore, the solution of the given congruence is given by

$x = 5,7,30,32(mod\ 37)$.

W CHECK YOUR PROGRESS

Q10) Obtain the index of $17(mod\ 18)$.

Q11) Solve the linear congruence:$7x \equiv 2(mod\ 9)$

Q12) Solve the linear congruence:$x^3 \equiv 5(mod\ 13)$

2 9.8 LET US SUM UP

- If $n > 1$ is any integer and a is another integer such that $(a, n) = 1$.Then the order of a of modulo n is the smallest positive integer k such that $a^k \equiv 1(mod\ n)$.
- If a is an integer having order k modulo n i.e., $a^k \equiv 1(mod\ n)$, then
  (i) $a^h \equiv 1(mod\ n)$ for some integer h then $k|h$
  (ii) $a \equiv b\ (mod\ n) \Rightarrow b$ has order k modulo n.
  (iii) $a^i \equiv a^j(mod\ n) \Leftrightarrow i \equiv j(mod\ k)$
  (iv) $(a, n) = 1$ i.e., a and k are coprime.

- If a has order k mod n, then a^h has order $\frac{k}{d}$ where $d = (k, h)$.
- If the orders of a_1 and a_2 modulo n be k_1 and k_2 respectively and $(k_1, k_2) = 1$. Then the order of $a_1a_2(mod\ n)$ is k_1k_2 .
- If an integer a has order $\phi(n)$ modulo n (a positive integer) and $(a, n) = 1$, then a is a primitive root of n.Thus, n has a primitive root a if $a^{\phi(n)} \equiv 1(mod\ n)$ and $a^k \equiv 1\ (mod\ n) \forall\ k < \phi(n)$.
- If a is a primitive root modulo n ,then $a, a^2, \cdots, a^{\phi(n)}$ is a reduced system $(mod\ n)$.
- (Lagrange Theorem) : Let$p$ is a prime and let
  $$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$
  is a polynomial of degree $n \geq 1$ with integral coefficient, where
  $$a_n \not\equiv 0(mod\ p)$$
  Then the congruence $f(x) \equiv 0(mod\ p)$ has at most$n$ incongruent solutions modulo$p$.
- If p is a prime and $d|p - 1$,then the congruence $x^d - 1 \equiv 0(mod\ p)$ has exactly d solutions.
- If p is a prime and $d|p - 1$,then there are exactly $\phi(d)$ incongruent integers having d modulo p.
- If$(a, m) = 1$,then a is a primitive root of $m$if and only if$a^{\frac{\phi(m)}{p}} \not\equiv 1(mod\ m)$ for every prime divisor$p$ of $\phi(m)$.

- For $n \geq 3$,the integer 2^n has no primitive roots.
- If $m, n > 2$ and $(m, n) = 1$,then there exists no primitive root $(mod\ mn)$.
- If p is an odd prime and r a primitive root of p such that $r^{p-1} \not\equiv 1(mod\ p^2)$ then for each positive integer$k \geq 2$,

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

- There exists a primitive root for p^k when p is an odd prime and $k \geq 1$.
- If r is a primitive root of n and$(a, n) = 1$,then the smallest positive integer h such that $a \equiv r^h(mod\ n)$ is called the index of a relative to r.

  Customarily, we denote the index of a relative to r by $ind_r a$.

- Let a be a primitive root modulo n and b,c and k are any integers, then

  (i) $b \equiv c(mod\ n) \Rightarrow ind.\, b \equiv ind.\, c\big(mod\ \phi(n)\big)$

  (ii) $ind.\,(bc) \equiv ind.\, b + ind.\, c\big(mod\ \phi(n)\big)$

  (iii) $ind.\, b^k \equiv k\ ind.\, b\big(mod\ \phi(n)\big)$ for $k > 0$.

  (iv) $ind.\, 1 \equiv 0\big(mod\ \phi(n)\big)$

- If $a_1, a_2, \cdots, a_k$ are all primes to $n[mod\ \phi(n)]$.

  Then, $ind.\, a_1 + ind.\, a_2 + \cdots + ind.\, a_k = ind.\, a_1 a_2 \cdots a_k$.

K 1.8 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q1:

We have $3^1 \equiv 3(mod\ 9)$

$$3^2 \equiv 0(mod\ 9)$$

$$3^3 \equiv 0(mod\ 9)$$

..
.
.

$$3^n \equiv 0(mod\ 9) \forall n \geq 2$$

This shows that order of 3 modulo 9 is not defined.

Answer to Q2: We have $3^1 \equiv 3(mod\ 5)$

$$3^2 \equiv 4(mod\ 5)$$

$$3^3 \equiv 2(mod\ 5)$$

$$3^4 \equiv 1(mod\ 5)$$

This shows that order of 3 modulo 5 is 4.

Answer to Q3: The integer a must be coprime to n, i.e.,$g.c.d\ (a,n) = 1$.If this condition is not satisfied, then a does not have an order modulo n.

Answer to Q4: First we check: g. c. d (5,14) =1, so order exists.

Now, we compute $5^1 \equiv 5(mod\ 14)$

$$5^2 \equiv 11(mod\ 14)$$

$$5^3 \equiv 13(mod\ 14)$$

$$5^4 \equiv 9(mod\ 14)$$

$$5^5 \equiv 3(mod\ 14)$$

$$5^6 \equiv 1(mod\ 14)$$

The smallest exponent giving 1 is 6.

So, the order of 5 modulo 14 is 6.

Answer to Q5: We check gcd(3,10)=1.

Now, we compute $3^1 \equiv 3(mod\ 10)$

$$3^2 \equiv 9(mod\ 10)$$

$$3^3 \equiv 7(mod\ 10)$$

$$3^4 \equiv 1(mod\ 10)$$

The smallest exponent giving 1 is 4.

So, the order of 3 modulo 10 is 4.

Answer to Q6: We have $\phi(7) = 6$

$$3^1 \equiv 3(mod\ 7)$$

$$3^2 \equiv 2(mod\ 7)$$

$$3^3 \equiv 6(mod\ 7)$$

$$3^4 \equiv 2(mod\ 7)$$

$$3^5 \equiv 5(mod\ 7)$$

$$3^6 \equiv 1(mod\ 7)$$

Thus, $3^{\phi(7)} \equiv 1(mod\ 7)$

Hence,3 is a primitive root of 7.

Answer to Q7: Here 2,3,4,5,6 are all coprime to 7. Hence, we must find the primitive roots (mod 7) amongst these integers. Also,$\phi(7) = 6$.

Now, $2^2 \equiv 4(mod\ 7)$

and $2^3 \equiv 1(mod\ 7)$

∴ 2 is not a primitive root $(mod\ 7)$

$$3^2 \equiv 2(mod\ 7)$$

$$3^3 \equiv 6(mod\ 7)$$

$$3^4 \equiv 4(mod\ 7)$$

$3^5 \equiv 5(mod\ 7)$ and

$$3^6 \equiv 1(mod\ 7)$$

∴ 3 is a primitive root $(mod\ 7)$.

$$4^2 \equiv 2(mod\ 7)$$

$$4^3 \equiv 1(mod\ 7)$$

∴ 4 is not a primitive root $(mod\ 7)$.

Also, $5^2 \equiv 4(mod\ 7)$

$$5^3 \equiv 6(mod\ 7)$$

$$5^4 \equiv 2(mod\ 7)$$

$$5^5 \equiv 3(mod\ 7)$$

$$5^6 \equiv 1(mod\ 7)$$

Hence, 5 is not a primitive root $(mod\ 7)$.

Now,$6^2 \equiv 1(mod\ 7)$,6 cannot be a primitive root $(mod\ 7)$.Hence,3 and 5 are only primitive roots $(mod\ 7)$.

Answer to Q8: Since $\phi(8) = 4$ and 1,3,5,7 are coprime to 8;hence possible primitive roots can be 3,5 or 7.

Now, $3^2 \equiv 1(mod\ 8)$,$5^2 \equiv 1(mod\ 8)$,$7^2 \equiv 1(mod\ 8)$.

None of 3,5,7 is primitive root (mod 8). Hence, there exists no primitive roots(mod8).

Answer to Q9: Do yourself

Answer to Q10: It can be shown that the smallest primitive root of 18 is 5. This means every number that is coprime with 18 can be written as a power of 5 (mod 18).
Now, we compute powers of 5 modulo 18:
$5^1 = 5,5^2 = 25 \equiv 7(mod\ 18),5^3 = 35 \equiv 17(mod\ 18)$
Hence,$5^3 \equiv 17(mod\ 18)$
Thus, the index of 17 with respect to the primitive root 5 is:$ind._5\ 17 = 3$.
Answer to Q11:
We know that 5 is a primitive root modulo 23.
Also,$5^1 \equiv 5(mod\ 23)$

$$5^2 \equiv 2(mod\ 23)$$
$$5^3 \equiv 10(mod\ 23)$$
$$5^4 \equiv 4(mod\ 23)$$
$$5^5 \equiv 20(mod\ 23)$$
$$5^6 \equiv 8(mod\ 23)$$
$$5^7 \equiv 17(mod\ 23)$$
$$5^8 \equiv 16(mod\ 23)$$
$$5^9 \equiv 11(mod\ 23)$$

$5^{10} \equiv 9(mod\ 23)$, and

$11x^3 \equiv 2(mod\ 23)$ is equivalent to

$$ind.11 + 3ind.x \equiv ind.2(mod\ 22)$$
$$\Rightarrow 9 + 3ind.x \equiv 2(mod\ 22)$$
$$\Rightarrow 3ind.x \equiv -7(mod\ 22)$$
$$\Rightarrow 2ind.x \equiv 15(mod\ 22)$$
$$\Rightarrow indx \equiv 5(mod\ 23)$$

Hence, $x \equiv 5^5(mod\ 23)$

$$\Rightarrow x \equiv 20(mod\ 23)$$

Thus, $x = 23t + 20, t = 0, \pm1, \pm2, \cdots$ are all solutions of the given congruence.

Answer to Q12:

We know that 2 is a primitive root modulo 13.

Now, we have

$$2^1 \equiv 2(mod\ 13)$$
$$2^2 \equiv 4(mod\ 13)$$
$$2^3 \equiv 8(mod\ 13)$$
$$2^4 \equiv 3(mod\ 13)$$
$$2^5 \equiv 6(mod\ 13)$$
$$2^6 \equiv 12(mod\ 13)$$
$$2^7 \equiv 11(mod\ 13)$$
$$2^8 \equiv 9(mod\ 13)$$
$$2^9 \equiv 5(mod\ 13)$$

From this, we conclude that the index of 2 is 1, while the index of 5 is 9.

The given congruence $x^3 \equiv 5(mod\ 13)$ is equivalent to

$$\equiv ind.5\big(mod\ \phi(13)\big)$$
$$3ind._2\ x \equiv 9\big(mod\ \phi(13)\big) \qquad [\because\ \phi(13) = 12]$$
$$\equiv 9(mod\ 12)$$
$$\Rightarrow ind._2\ x \equiv 3(mod\ 4)$$
$$\equiv 3,7,11.$$

The integers corresponding to these will be 8,11 and 7.

Therefore, the required solution are

$x \equiv 7,8$ and $11(mod\ 13)$.

O1.9 FURTHER READING

1. David M. Burton, Elementary Number Theory (7^{th} Edn.), McGraw Hill Education (India) Private Limited, Chennai-600116, 2018.

2. S. B. Malik, Basic Number Theory (2^{nd} revised Edn.), Vikash Publishing House Private Limited, Noida-201301, 2017.

3. George E. Andrews, Number Theory, Hindustan Publishing Corporation, New Delhi.

4. S. G. Telang, Number Theory, Tata McGraw-Hill Publishing Company Limited.

5. Hardy, G. H. And Wright, E. M., Theory of Numbers, Oxford Science Publications, 2003.

M 9.10 MODEL QUESTIONS

Q1. Find the order of the integers 2,3 and 5:

(a) modulo 17.

(b) modulo 19.

(c) modulo 23.

Q2. Given that a has order 3 modulo p,where p is an odd prime, show that $a+1$ must have order 6 modulo p.

Q3. Verify that 2 is a primitive root of 19, but not of 17.

Q4. Let r be a primitive root of the integer n.Prove that r^k is a primitive root of n if and only if $gcd(k, \phi(n)) = 1$.

Q5. Find two primitive roots of 10.

Q6. List all primitive roots modulo 5; modulo10, modulo12, and modulo 16.

Q7. How many primitive roots modulo 15 exist?

Q8. Find the order of 3 modulo 19.

Q9. Show that 2 is not a primitive root of 17.

Q10. Find the order of 5 $(mod\ 7^2)$.

Q11. Find two primitive roots of 10.

Q12. Find primitive roots of 3^3.

Q13. Find all primitive roots of 82.

Q14. Determine all primitive roots of 3^2,3^3 and 3^4.

Q15. Obtain all the primitive roots of 41 and 82.

Q16: Solve the following congruences:

(i) $7x^3 \equiv 3(mod\ 11)$

(ii) $4x \equiv 19(mod\ 23)$

(iii) $57^x \equiv 2(mod\ 23)$

*** *** ***