NUMBER THEORY COURSE

LESSON : PRIMITIVE ROOTS

1. Introduction

The additive group of the ring $(\mathbb{Z}_n, +, \cdot)$ of integers modulo n is known to be cyclic but the multiplicative group of units in $\mathbb{Z}_n$ namely $U(n)$ may or may not be cyclic. The Lesson on primitive roots is aimed to determine the values of n for which $U(n)$ is cyclic. Moreover, for a given $n > 1$, the problem of finding generators of $U(n)$, whenever it is cyclic will also be settled.

We start with a simple result before giving the first definition.

Proposition 1.1. *Let $a, n \in \mathbb{Z}$, $n > 1$. Then $a^k \equiv 1 \mod n$ for some $k > 0$ iff gcd $(a,\ n) = 1$.*

Proof. If gcd $(a,\ n) = 1$ then by Euler's theorem, $a^{\varphi n} \equiv 1 \mod n$. Conversely, if there is some $k > 0$ such that $a^k \equiv 1 \mod n$, we claim that $ax \equiv 1 \mod n$ has a solution. If $k = 1$, $x = 1$ is a solution. If $k > 1$, $x = a^{k-1}$ is a solution. But we know that solvability of $ax \equiv 1 \mod n$ is equivalent to gcd $(a,\ n) = 1$. □

Definitions 1.1. Let $n > 1$ and a be an integer such that gcd $(a,\ n) = 1$. k is called the order of a modulo n if k is the least postitve integer such that

$$a^k \equiv 1 \mod n.$$

We write $Ord_n a = k$.

In view of the above proposition, the assumption gcd $(a,\ n) = 1$ is necessary as well as sufficient for the definition of order of a modulo n make sense.

By reducing down a modulo n, one may obtain an element of the group $U(n)$. Definition 1.1 simply defines order of this element in the group $U(n)$.

Definitions 1.2 (Primitive root)**.** An integer a, if exists, such that $Ord_n a = \phi(n)$ is called a primitive root of n.

2. Primitive roots for primes

In most of the probes related to modular arithmatic, starting with primes happens to be a nice idea. In this section we try to find whether there exists a primitive root for a prime or not, and if it does, what are the possible integers that may be primitive roots for the prime.

The first tool we need is a result due to Lagrange. The fundamental theorem of algebra tells that any polynomial with complex coefficients uses to have as many zeros as its degree. If a polynomial of degree n with rational coefficients is viewed as a polynomial with complex coefficients, one knows that it has n many (not necessarily distinct) complex zeross. Out of those complex zeross, some may be rational numbers and therefore the maximum number of rational zeros is n. A similar result can be stated for polynomials with coefficients from the field $\mathbb{Z}_p$.

However, over an arbitrary ring, there are no bounds for number of zeros of a polynomial.

Example 2.1. Consider the ring $\mathbb{Z}_8$. The elements $1, 3, 5$ and 7 are all zeros of $x^2 + 7$.

We now prove the result for the fields $\mathbb{Z}_p$.

Theorem 2.2. *Let p be a prime and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be a polynomial with integral coefficients of degree $n \geq 1$ and $a_n \not\equiv 0 \mod p$. Then the congruence*

$$f(x) \equiv 0 \mod p$$

has at most n incongruent solutions modulo p.

Proof. The proof is by induction on degree of f. If degree f is 1, then $f(x) = a_1 x + a_0$. Let x_0 be the solution of $a_x \equiv 1 \mod p$ then $y = -x_0 a_0$ is the unique solution to $f(x) \equiv 0 \mod p$. Now assume that the result is true for all polynomials with degree less than or equal to n and let deg $f = n + 1$. If $f(x) \equiv 0 \mod p$ does not have a solution then we are done. If it has a solution α then by division algorithm we may write

$$f(x) = (x - \alpha)g(x) + r(x)$$

with deg $r < 1$ (Since deg $(x - \alpha)$=1) *i.e.* r is an integer. Putting $x = \alpha$, we get $r \equiv 0 \mod p$ and $f(x) \equiv (x - \alpha)g(x) \mod p$. Now suppose β be a solution of $f(x) \equiv 0 \mod p$ that is incongruent to α modulo p.Then

$$0 \equiv f(\beta) \equiv (\beta - \alpha)g(\beta) \mod p$$

Since $\beta - \alpha \not\equiv 0 \mod p$, we have $g(\beta) \equiv 0 \mod p$. Since deg g=n, by our induction hypothesis, there are atmost n such β that are incongruent modulo p. Hence $f(x) \equiv 0 \mod p$ has at most $n + 1$ many solutions incongruent modulo p. □

Remark 2.1. Above theorem can be restated as "A polynomial of degree n in $\mathbb{Z}_p[x]$ can have at most n zeros in the base field $\mathbb{Z}_p$." A close look at the proof indicates that the key part is availability of the division algorithm. Using the long division algorithm, one may conclude that division algorithm holds in $\mathbb{F}[x]$ for any field $\mathbb{F}$. Therefore it may be concluded that any polynomial of degree n in $\mathbb{F}[x]$ can have at most n zeros.

Proposition 2.3. *If p is a prime then the equation $x^{p-1} \equiv 1 \mod p$ has precisely $p - 1$ roots that are incongruent modulo p.*

Proof. Let $a \in \{1, 2, \ldots, p - 1\}$ then by Fermat's theorem, $a^{p-1} \equiv 1 \mod p$.e So thte equation $x^{p-1} \equiv 1 \mod p$ has at least $p - 1$ incongruent solutions. The result now follows by Lagrange's theorem. □

Proposition 2.4. *If p is a prime and $d \big| p - 1$ then $x^d - 1 \equiv 0 \mod p$ has precisely d roots incongrunet modulo p.*

Proof. When $d \big| p - 1$, $(x^d - 1) \big| (x^{p-1} - 1)$ so that we may write

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

for some polynomial $g(x)$ of degree $p - 1 - d$. By Lagrange's theorem, g can have at most $p - 1 - d$ incongruent zeros. Any zero of x^{p-1} is a zero of $x^d - 1$ or of $g(x)$. $x^{p-1} - 1$ has $p - 1$ incongruent zeros which is the maximum possible number of zeros. Therefore both the polynomials $x^d - 1$ and $g(x)$ must have resp. d and $p - 1 - d$ incongruent zeros. □

Remark 2.2 (A new proof of Wilson's theorem)**.** Define the polynomial

$$f(x) = (x-1)(x-2)\dots(x-p+1) - \left(x^{p-1}-1\right).$$

This polynomial is of degree less than $p-1$ as x^{p-1} term gets cancelled out. We write

$$f(x) = a_{p-2}x^{p-2} + \ldots + a_1 x + a_0.$$

Let $a \in \{1, 2, \ldots, p-1\}$. Then $(a-1)(a-2)\ldots(a-p+1) = 0$ and by Fermat's theorem, $x^{p-1} - 1 \equiv 0 \mod p$. Therefore the equation $f(x) \equiv 0 \mod p$ has $p-1$ incongrunt solutions. This is possible only when f is the zero polynomial *i.e.* $a_{p-2} = a_{p-3} = \ldots = a_0 \equiv 0 \mod p$. Therefore, for any integer a,

$$\begin{aligned} (a-1)(a-2)\dots(a-p+1) - \left(a^{p-1}-1\right) &\equiv 0 \mod p \\ \textit{i.e. } (a-1)(a-2)\dots(a-p+1) &\equiv \left(a^{p-1}-1\right) \mod p \end{aligned}$$

Putting $a = p-1$ above, we get

$$(p-1)! \equiv -1 \mod p$$

The next objective is to prove the existence of primitive roots for prime numbers. If that is assumed, for a prime p, the group $U(p)$ would become cyclic of order $p-1$. In that case, our knowledge of group theory tells that for every divisor d of $p-1$, there is exactly one subgroup of $U(p)$ or order d which would contain $\varphi(d)$ many elements of order d. The following theorem establishes all these facts about $U(p)$ in one go.

Theorem 2.5. *Let p be a prime and $d \Big| (p-1)$ then there are exactly $\varphi(d)$ many incongruent integers having order d modulo p.*

Proof. The proof relies on the Lagrange's theorem and the identity

$$p - 1 = \sum_{d \big| (p-1)} \varphi(d). \tag{2.1}$$

Since every element of the set $A = \{1, 2, \ldots, p-1\}$ is coprime to p, it has a finite order that divides $\varphi(p) = p-1$. Therefore, if $\psi(d)$ denotes the number of elements of A having order d then we have

$$p - 1 = \sum_{d | (p-1)} \psi(d). \tag{2.2}$$

Comparing equations (2.1) and (2.2), we get

$$\sum_{d \big| (p-1)} \varphi(d) = \sum_{d \big| (p-1)} \psi(d). \tag{2.3}$$

We first prove that if for some d, $\psi(d)$ is non-zero then $\psi(d)$ must be equal to $\varphi(d)$. Let a be of order d in A. Then, for any $1 \le k \le p-1$, $Ord_p a^k = \dfrac{d}{\text{gcd}\,(d,\ k)}$ so that $Ord_p a^k = d$ iff gcd $(d,\ k) = 1$. So there are exactly $\phi(d)$ many integers in A whose order is d. Finally, all the elements of A satisfy $x^d - 1 \equiv 0 \mod p$ so by Lagrange's theorem, any integer whose order is d must be congruent to some integer in A. Thus the total number of incongruent integers having order d modulo p must be $\varphi(d)$. Finally, it is easy to see that $\psi(d) \neq 0$ for any divisor d of $p-1$. For if $\psi(d_0) = 0$

for some divisor d_0 of $p-1$ then the equation (2.3) can not hold, as $vp(d_0) > 0$. This completes the proof. □

Corollary 2.6. *If p is a prime, then there are exactly $\varphi(p-1)$ incongruent primitive roots of p.*

Proof. Take $d = p-1$ in the above theorem. □

Example 2.1. If p is a prime of type $4k+1$ then the congruence $x^2 \equiv -1 \mod p$ admits a solution.

Since $p = 4k+1$, 4 is a divisor of $p-1$. Thus there exists an integer of order 4 modulo p. Let a be one such integer. Then

$$\begin{aligned} a^4 &\equiv 1 \mod p \\ \implies a^4 - 1 &\equiv 0 \mod p \\ \implies (a^2-1)(a^2+1) &\equiv 0 \mod p. \end{aligned}$$

Therefore, $a^2 - 1 \equiv 0 \mod p$ or $a^2+1 \equiv 0 \mod p$. But $a^2-1 \equiv 0 \mod p$ contradicts to the assumption that order of a modulo p was 4. Hence $a^2+1 \equiv 0 \mod p$ holds whereby, a becomes a solution to the congruence $x^2 \equiv -1 \mod p$.

3. Exercises

Exercise 1. If p is an odd prime, prove that

(a) the only incongruent solutions of $x^2 \equiv 1 \mod p$ are 1 and $p-1$.

(b) The congruence $x^{p-2} + \ldots + x^2 + x + 1 \equiv 0 \mod p$ has exactly $p-2$ incongruent solutions and they are $2, 3, \ldots, p-1$.

Hint : (a) $x^2 \equiv 1 \mod p \implies (x-1)(x+1) \equiv 0 \mod p$ whereby, $x \equiv \pm 1 \mod p$. (b) Clearly, 1 does not sarisfy the congruence. If $a \not\equiv 1 \mod p$ satisfies the congruence $a^{p-2} + \ldots + a^2 + a + 1 \equiv 0 \mod p$ if and only if

$$\begin{aligned} (a-1)(a^{p-2} + \ldots + a^2 + a + 1) &\equiv 0 \mod p \\ \iff a^{p-1} - 1 &\equiv 0 \mod p. \end{aligned}$$

Exercise 2. Determine all the primitive roots of 17.

Hint : By hit and trial, it turns out that 2 is not a primitive root of 17 but 3 is. Now, $\varphi(17) = 16$. There must be $\varphi(16) = 8$ primitive roots of 7. These primitive roots are of type 3^k where gcd $(k,\ 16) = 1$.

Exercise 3. Given that 3 is a primitive root of 43, find all positive integers less than 43 whose order is 6 modulo 43.

Hint : Order of an element of type 3^k is $\frac{42}{\text{gcd }(k,\ 42)}$. Possible values of k are 7, 35 (there can be 2 elements only of order 6 as $\varphi(6) = 2$).

Exercise 4. Assume that r and r' are primitive roots of an odd prime p. Show that rr' can not be a primitive root of p.

Hint : First, observe that any primitve s of p satisfies $s^{(p-1)/2} \equiv -1 \mod p$. For $s^{(p-1)/2}$ is a root of $x^2 \equiv 1 \mod p$ and $s^{(p-1)/2} \not\equiv 1 \mod p$. Now, $(rr')^{(p-1)/2} \equiv r^{(p-1)/2} r'^{(p-1)/2} \equiv 1 \mod p$ and thus rr' can not be a primitive root of p.

Exercise 5. For a prime $p > 3$, prove that primitive roots of p occur in pairs $r,\ r'$ where $rr' \equiv 1 \mod p$.

Hint : Let r be a primitive root for p. Since gcd $(r,\ n) = 1$, the congruence $rr' \equiv 1 \mod p$ has a unique solution. It is easy to see that r' can be taken to be r^{p-2}. Since $p > 3$, $r \not\equiv r' \mod p$.

Exercise 6. Let r be a primitive root of the odd prime p. Prove that
(a) if $p \equiv 1 \mod 4$, then $-r$ is also a primitive root of p.
(b) if $p \equiv 3 \mod 4$, then $-r$ has order $(p-1)/2$ modulo p.

Hint : (a) If $p \equiv 1 \mod 4$ then $(p-1)/2$ is even. Suppose, if possible, $(-r)^k \equiv 1 \mod p$. If $k < p-1$ then k must be an odd divisor of $p-1$. Therefore $k \mid \frac{p-1}{2}$ so that $(-r)^{(p-1)/2} \equiv 1 \mod p$. But $(-r)^{(p-1)/2} \equiv r^{(p-1)/2} \mod p$, as $(p-1)/2$ is even. This contradicts to the assumption that r was a primitive root of p. (b) As in part (a), $(-r)^k \equiv 1 \mod p$ is possible only for odd divisors of $p-1$. If $k < \frac{p-1}{2}$, then $2k < p-1$ and $r^{2k} \equiv 1 \mod p$ which is a contradiction.

4. 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 4.1. *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 4.2. *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 4.3. *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 $n = m_1 m_2$ has no primitve roots. □

Corollary 4.4. *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 $n_1 n_2$. □

Example 4.5. 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. 4.3)
9	Y	2 is a primitive root
10	Y	3 is a primitive root
12	N	$12 = 2^2 \times 3$ (Cor. 4.4)
14	Y	3 is a primitive root
15	N	$15 = 3 \times 5$ (Cor.4.3)

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 4.1 and 4.2 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 4.6. *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

$$(r')^{p-1} \equiv 1 - pr^{p-2} \mod p^2. \tag{4.1}$$

Now, if $(r')^{p-1} \equiv 1 \mod p^2$ then from eq (4.1), 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 4.7. *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 4.1. Let p be an odd prime. In lemma 4.6 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 4.7, we conclude that either r or $r + p$ is a primitive root of p^2.

Lemma 4.8. *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 $k \geq 2$*

$$r^{p^{k-2}(p-1)} \not\equiv 1 \mod p^k \tag{4.2}$$

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 $k \geq 2$, (4.2) 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 4.9. *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 4.10. *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 p^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 $\ell = \varphi(p^k) = \varphi(2p^k)$. □

Remark 4.2. The facts proved in this lesson about primitive roots are stated in terms of $U(n)$ groups in the Chapter on External Direct Products (Page 160 in seventh Edition). It would be an interesting exercise for the reader to compare the two versions of the same fact.

5. Exercises

Exercise 7. Find the four primitive roots of 26.

Hint : First note that $26 = 2 \times 13$, and 13 is a prime so 26 has primitive roots. Number of primitive roots is $\varphi(\varphi(26)) = \varphi(12) = 4$. That is why the exercise is asking for 'the four' primitive roots of 26.

The strategy is based on Corollary 4.10. We just need to find an odd primitive root of 13 and that would be one primitive root of 26. It is easy to see by inspection that 2 is a primitive root of 13. But we need an odd number so we consider 13+2=15. Then 15 is a primitve root of 26. Finding other primitive roots is now a routine.

In the following exercises, p is an odd prime.

Exercise 8. Show that there are as many primitive roots of $2p^n$ as of p^n.

Hint : Number of primitive roots of p^n is $\varphi(\varphi(p^n))$ and that of $2p^n$ is $\varphi(\varphi(2p^n))$. When p is odd,

$$\varphi(2p^n) = \varphi(2)\varphi(p^n) = \varphi(p^n).$$

Exercise 9. A primitive root of p^2 is also a primitive root of $p^n,\ n \geq 2$.

Hint : Use induction on n. We have $Ord_{p^2} r = p(p-1)$ so that

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

Assume that $Ord_{p^k} r = p^{k-1}(p-1)$ and try to show that $Ord_{p^{k+1}} r = p^k(p-1)$.

Exercise 10. r is a primitive root of p^2. Show that the solution of the congruence $x^{p-1} \equiv 1 \mod p^2$ are precisely the integers $r^p, r^{2p}, \ldots, r^{p(p-1)}$.

Hint : First note that for any integer $m = kp,\ 1 \leq k \leq p-1$, $(r^m)^{p-1} = r^{kp(p-1)} = (r^{\varphi(p^2)})^k \equiv 1 \mod p^2$. Moreover, no two numbers $r^{k_1 p}$ and $r^{k_2}p$ are congruent modulo p^2 for $k_1 \neq k_2$, $1 \leq k_1, k_2, \leq p-1$ (How?). Therefore we have $p-1$ many integers that satisfy the congrunece $x^{p-1} \equiv 1 \mod p^2$ and are inccongruent modulo p^2. By Lagrange theorem, these integers are all the incongruent solutions as the degree of congruence equation is $p-1$.