NUMBER THEORY COURSE

LESSON : PRIMITIVE ROOTS-I

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

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

Let $a \in \{1,2,\dots,p-1\}$. Then $(a-1)(a-2)\dots(a-p+1) = 0$ 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.* $a_{p-2} = a_{p-3} = \dots = a_0 \equiv 0 \mod p$. 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 $A = \{1,2,\dots,p-1\}$ 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 $1 \le k \le p-1$, $Ord_p a^k = \dfrac{d}{\gcd(d,\ k)}$ 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 $\frac{42}{\gcd(k, 42)}$. 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.