# Notes of Feb 28, 2018

Pushkar R. Tiwari

Definition : a is a primitive root modulo is prime $p$ is the powers $a^1$ ,$a^2$,$a^3$,$a^{n-1}$ produce all of the non zero residues modulo $p$.

Theorem: Every prime number has primitive roots. It has $\varphi(p-1)$ many of them.
For what values of b does $X^2 \equiv b \pmod{11}$ have a solution?
1,3,4,5,9
Why does $X^2 \equiv 6 \pmod{11}$ not have a solution ?
Try all values of X, nothing works

| a | $a^2$ |
|---|---|
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 5 |
| 5 | 3 |
| 6 | 3 |
| 7 | 5 |
| 8 | 9 |
| 9 | 4 |
| 10 | 1 |

$\rightarrow$ Definition : We say that a (mod n) is a quadratic residue modulo n if $X^2 \equiv a(\text{mod n})$ has at least one solution.

Def: if $X^2 \equiv a(\text{mod n})$ does not have a solution then is called a quadratic non-residue.

How can we tell if a is a quadratic residue modulo a prime number P(without trying all possible values of X)?

Define the Legendre Symbol ("a on P") as follows:

$$\left(\frac{a}{P}\right) \begin{cases} 1 & \text{if } X^2 \equiv a(\text{mod P}) \text{ has a solution} \\ -1 & \text{if } X^2 \equiv a \text{ (mod P) does not have a solution} \\ 0 & \text{if } a \equiv 0(\text{mod P}) \text{ does not have a solution} \end{cases}$$

Legendre symbol is only defined when the number on bottom is prime.

Rules for Legendre Symbols

1. If a ≡b(mod P) then (a/P)=(b/P)

2. (1/p)=1(1 is always a quadratic residue.)

3.(ab/P)=(a/P)(b/P)

4. Quadratic Reciprocity: If p and q are both odd primes then,

$$(q/p)=\begin{cases} -(p/q) & \text{if } p\equiv 3(mod 4) \text{ and } q\equiv 3(\text{mod } 4) \\ (p/q) & \text{otherwise} \end{cases}$$

$$5.(2/p) = \begin{cases} 1 & \text{if p is 1 or 7(mod 8)} \\ -1 & \text{if p is 3 or 5(mod 8)} \end{cases}$$

Biggest problem with Legendre symbols is the need to factor the number on top.
Once we get to really large numbers this won't always be possible.

## Jacobi symbol:

Like the Legendre Symbol in that $(p/q)=\begin{cases} 1 & \text{if p is quadratic residue (mod q)} \\ -1 & \text{if p is not quadratic residue (mod q)} \end{cases}$

But it doesn't mean anything if the number on bottom is composite.
(n/m)={ +1/-1
but $(n/m)$=1 does not necessarily mean that $X^2$≡n(mod m) has a solution.

## Rules for Jacobi Symbol

1.If a ≡b(mod n) then (a/n)=(b/n)

2.(1/n)=1

3.(2n/m)=(2/m)(n/m)

4. If n and m are both odd and gcd(m,n)=1 then,

$$(n/m)=\begin{cases} -(m/n) & \text{if } m\equiv 3(mod 4) \text{ and n}\equiv 3(mod\ 4) \\ (m/n) & \text{otherwise} \end{cases}$$

$$5.(2/n) = \begin{cases} 1 & \text{if n is 1 or 7(mod 8)} \\ -1 & \text{if n is 3 or 5(mod 8)} \end{cases}$$