Lecture-3: In the previous lecture we proved Wilson's Theorem. This states that if p is a prime then $(p-1)! \equiv -1 \pmod{p}$. We begin with some Corollaries of this Theorem.

Proposition: Let p be an odd prime. The equation $x^2 \equiv -1 \bmod p$ has a solution $\Leftrightarrow$ $p \equiv 1 \bmod 4$

Proof: Assume $x^2 \equiv -1 \bmod p$ has a solution. Further assume $p \equiv 3 \bmod 4$. Raising both sides to the power $\frac{p-1}{2}$ we get

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \bmod p$$

By Fermat's theorem $x^{p-1} \equiv 1 \bmod p$. As $\frac{p-1}{2}$ is odd $\Rightarrow$ $(-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$. Thus, we get

$$1 \equiv (x^2)^{\frac{p-1}{2}} \equiv -1 \bmod p.$$ This is a contradiction.

Next assume that $p \equiv 1 \bmod 4$. By Wilson's theorem we can write

$$1 \cdot 2 \cdots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{p+3}{2} \cdots p-1 \equiv -1 \bmod p$$

$$\frac{p+1}{2} \equiv p - \frac{p-1}{2} \equiv -\frac{p-1}{2} \bmod p$$

$$\frac{p+3}{2} \equiv p - \frac{p-3}{2} \equiv -\frac{p-3}{2} \bmod p$$

$$\vdots$$

$$\Rightarrow (p-1)! \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv -1 \bmod p$$

As $\frac{p-1}{2}$ is even $\Rightarrow$ $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \bmod p$.

Thus, $x^2 \equiv -1 \bmod p$ has a solution. This completes the proof of the Proposition.

Lemma: Let $n>1$. Then n is prime $\iff (n-1)! \equiv -1 \bmod n$.

Proof: If n is prime then the above is precisely Wilson's theorem. If n is not prime then we can write $n=ab$, where $a>1$ and $b>1$.

If $(n-1)! \equiv -1 \bmod n$, then going further mod a, we get $(n-1)! \equiv -1 \bmod a$. But as $a < n-1$, we get $a \mid (n-1)!$, that is,

$$0 \equiv -1 \bmod a,$$

which is a contradiction. Thus, $(n-1)! \not\equiv -1 \bmod a$.
This completes the proof.

Let R be a ring and let $f(x) \in R[x]$ be a polynomial. Let $a \in R$ and assume $f(a)=0$. Using the binomial expansion, we can write

$$f(x) = f(x-a+a) = (x-a)g(x) + f(a)$$

$$\Rightarrow f(x) = (x-a)g(x)$$

We will use the above in the following Proposition.

Proposition: Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial of degree n. Then $f(x)$ has almost n distinct roots.

Proof: Suppose $f(x)$ has $n+1$ distinct roots $a_1, a_2, \dots, a_n, a_{n+1}$.
Applying the previous discussion to a_1, we get

$$f(x) = (x-a_1)f_1(x) \qquad \deg(f_1(x)) = n-1.$$

Substituting $x = a_2$, we get

$$0 = f(a_2) = (a_2-a_1)f_1(a_2) \Rightarrow f_1(a_2)=0 \text{ as } a_2-a_1 \neq 0$$

and $\mathbb{Z}_p$ is a field.

$$\Rightarrow f_1(x) = (x-a_2)f_2(x) \qquad \deg(f_2(x)) = n-2.$$

Proceeding in this manner we get

$$f(x) = (x-a_1)(x-a_2)\dots(x-a_n)c \qquad c \neq 0,\ c \in \mathbb{Z}_p.$$

When we put $X = a_{n+1}$ in the above we get

$0 = f(a_{n+1}) = (a_{n+1} - a_1) \cdots (a_{n+1} - a_n)c$ which is a contradiction as the RHS $\neq 0$.

This proves the proposition.

In the previous lecture we introduced the groups $(\mathbb{Z}/n\mathbb{Z})^\times$. Now we shall try to understand the structure of these groups.

Proposition: Let p be a prime. Then the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proof: The structure theorem for finite abelian groups says the following: Let G be a finite abelian group.

$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, where $n_1 > 1$ and

$$n_1 | n_2 | \cdots | n_r.$$

Note that this implies that the order of every element divides n_r. Moreover, the above says that

$$|G| = n_1 n_2 \cdots n_r.$$

We apply the above to $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

This shows that if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, then order of a divides n_r. Thus,

$x^{n_r} \equiv 1 \mod p$ has at least $p-1$ distinct solutions. By the previous proposition we get $n_r \geq p-1$. But we also have

$$p-1 = n_1 n_2 \cdots n_r$$

This forces that $r = 1$ and $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. This completes the proof.