Lecture 2: In the previous lecture we saw that there are infinitely many primes. We can ask several questions related to infinitude of primes of certain types:

① Fix integers a and b such that $(a,b)=1$. Consider the arithmetic progression $\{a+kb \mid k\in\mathbb{Z}\}$. Does this contain infinitely many primes? Yes! This is a theorem of Dirichlet.

② Are there infinitely many twin prime pairs? The answer to this is not known. However, we have the following very interesting result by Yitang Zhang: Let $p_1, p_2, \ldots$ be the set of primes arranged in increasing order. There is an integer N such that $p_{n+1}-p_n \le N$ for infinitely many n.

Chinese Remainder Theorem: Let $m>1$, $n>1$ be integers which are coprime. Then the natural map

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$a \bmod mn \longmapsto (a \bmod m,\ a \bmod n)$$

is an isomorphism.

Proof: It is obvious that this map is a group homomorphism. As the cardinality of the domain and codomain are the same, the map is an isomorphism $\iff$ it is injective.

Suppose $a \bmod mn \longmapsto (0,0)$. Then $m \mid a$ and $n \mid a$. As m and n are coprime $\Rightarrow mn \mid a$. Thus, $a \equiv 0 \bmod mn$. This proves injectivity and hence the proof is complete.

Remark: The Chinese Remainder Theorem can be rephrased as follows: Let $(m,n)=1$. Then the equation

$$x \equiv a \bmod m$$
$$x \equiv b \bmod n$$

has a unique solution modulo mn.

Lemma: $\mathbb{Z}/p\mathbb{Z}$ is a field for p prime

Proof: As $\mathbb{Z}/p\mathbb{Z}$ is a ring, to show it is a field, it suffices to show that if $a \neq 0$ then there is b such that $ab = 1$. If $a \neq 0$ then $p \nmid a$. Thus, $(p, a) = 1$. There are integers x, y such that $px + ay = 1$. $\Rightarrow ay \equiv 1 \bmod p$. This completes the proof.

Let p be a prime

Fermat's little Theorem: Let $a \in \mathbb{Z}/p\mathbb{Z}$ and $a \neq 0$. Then $a^{p-1} \equiv 1 \bmod p$.

Proof: We can use Lagrange's Theorem, which says that in a group G, $a^{|G|} = e$ $\forall\, a \in G$.

An elementary proof can be given as follows.

Consider the map $m_a : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$, $m_a(x) = ax$.

This is a group homomorphism. If $ax = 0 \Rightarrow x = 0$. Thus, this is injective and so is bijective. As $m_a(0) = 0$, it takes the set $S = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ to itself. Thus, $m_a(S) = S$.

Thus, $\{1, 2, \dots, p-1\} = \{a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)\}$.

$$\Rightarrow \quad \prod_{s \in S} s = \prod_{s \in S} a \cdot s = a^{p-1} \prod_{s \in S} s$$

Since $\prod_{s \in S} s = (p-1)! \bmod p \neq 0 \Rightarrow a^{p-1} \equiv 1 \bmod p$.

This completes the proof.

A generalization of the above to $\mathbb{Z}/n\mathbb{Z}$ is Euler's Theorem. Let $n > 1$. Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the group of units in $\mathbb{Z}/n\mathbb{Z}$, that is,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{u \in \mathbb{Z}/n\mathbb{Z} \mid \exists\, v \in \mathbb{Z}/n\mathbb{Z} \text{ such that } uv \equiv 1\}$$

Let $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Then $v^{\varphi(n)} \equiv 1$.

Proof: Again, we can use Lagrange's Theorem to prove the above. Alternatively, we can prove this as before. Consider the map $m_v : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$. This is an isomorphism (Check!).

Claim: $m_v(S) = S$. Let $a \in S$, then $\exists\, b$ such that $ab = 1$. Then $(va)(bv) = (vv)\cdot(ab) = 1$. $\Rightarrow vv \in S$.

Thus, $$\overline{\prod_{s\in S}} s = \overline{\prod_{s\in S}} v\cdot s = v^{\varphi(n)} \overline{\prod_{s\in S}} s.$$

As $\overline{\prod_{s\in S}} s$ is a finite product of units and so is a unit.

Multiplying by its inverse we get that $v^{\varphi(n)} \equiv 1 \bmod n$.

Wilson's Theorem: Let p be a prime. Then $(p-1)! \equiv -1 \bmod p$.

Proof: Let $a \in S = \{1, 2, \ldots p-1\}$. For each a, there is an $a' \in S$ such that $aa' = 1$. If $a' = a$, then we get $a^2 = 1$ $\Rightarrow$ $a^2 - 1 = (a-1)(a+1) \equiv 0 \bmod p$. As $\mathbb{Z}/p\mathbb{Z}$ is a field, the product of two nonzero elements can never be 0. Thus, $a^2 = 1$ holds $(\Leftrightarrow)$ $a = \pm 1$.

Thus, consider the set $T = \{2, 3, \ldots p-2\}$. We can divide T into $\frac{p-3}{2}$ pairs of the type $\{a, a'\}$ with $aa' = 1$. Note $a \neq a'$.

Thus, $$(p-1)! = \overline{\prod_{s\in S}} s = \left(\overline{\prod_{t\in T}} t\right)(p-1)$$
$$= \left(\overline{\prod_{\{a,a'\}}} aa'\right)(p-1) = 1\cdot(p-1)$$
$$= -1 \bmod p.$$

This completes the proof.