Lecture 5 : In the previous lecture we proved that if $p$ is an odd prime then the group of units in $\mathbb{Z}/p^n\mathbb{Z}$, which we denoted $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is a cyclic group of order $(p-1)p^{n-1}$.

What can we say when $p=2$?

$(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\} \cong \mathbb{Z}/2\mathbb{Z}$

$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. This is a group of order 4 with no element of order 4. Thus, it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In the previous lecture we proved that when $n \geq 3$, we have $(1+2^2)^{2^{n-3}} \equiv 1 + 2^{n-1} \bmod 2^n$. —— (A)
We also saw that

$$(\mathbb{Z}/2^n\mathbb{Z})^\times = \{1 + 2j \mid 0 \leq j < 2^{n-2}\}.$$

Proposition : Let $n \geq 3$. Then $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$.

Proof : The proof is similar to the case when $p$ is odd. Consider two subgroups of $(\mathbb{Z}/2^n\mathbb{Z})^\times$. $H = \{\pm 1\}$ and $K =$ subgroup generated by the element 5. As $\#(\mathbb{Z}/2^n\mathbb{Z})^\times = 2^{n-1}$ it follows that order of any element is a power of 2. By statement (A) it follows that order of $5 \geq 2^{n-2}$.
If the order of 5 were $2^{n-1}$, then that would mean that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is cyclic. But note that

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/8\mathbb{Z})^\times$$

$$\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \longmapsto \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

and so clearly this map is surjective. If $(\mathbb{Z}/2^n\mathbb{Z})^\times$ were cyclic, then the image of the generator would generate $(\mathbb{Z}/8\mathbb{Z})^\times$. But we know $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. This shows $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic. Thus, 5 has order $2^{n-2}$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

This shows $K = \langle 5 \rangle$ and has order $2^{n-2}$.

We claim that $H \cap K = \{1\}$. If not, then we would get that $-1 \in K$. $-1$ has order 2. As $K \cong \mathbb{Z}/2^{n-2}\mathbb{Z}$, the unique element of order 2 is $5^{2^{n-3}}$ ($5 \mapsto 1$ as the unique element of order 2 in $\mathbb{Z}/2^{n-2}\mathbb{Z}$ is $2^{n-3}$.

But by (A) we have $5^{2^{n-3}} = 1 + 2^{n-1}$. This forces that
$$1 + 2^{n-1} \equiv -1 \mod 2^n.$$
But this is a contradiction as $n \geq 3$. This shows that $H \cap K = \{e\}$.

Consider the group homomorphism

$$H \times K \longrightarrow (\mathbb{Z}/2^n\mathbb{Z})^\times \qquad (h,k) \mapsto hk$$

This is a group homomorphism as $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is abelian. The kernel is precisely $H \cap K = \{e\}$. As $H \times K$ and $(\mathbb{Z}/2^n\mathbb{Z})^\times$ have the same cardinality, it follows that this map is an isomorphism. Thus, $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2^{n-2} \times \mathbb{Z}/2$.

This complete the proof.

Combining these two with the Chinese Remainder Theorem we get the following. Let $n = p_1^{r_1} \cdots p_l^{r_l}$ be a prime factorization

Then $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_l^{r_l}\mathbb{Z})^\times$

This is because $\mathbb{Z}/n\mathbb{Z} \xrightarrow[\text{Rings}]{\sim} \mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_l^{r_l}$ and

so the groups of units are also isomorphic. Thus, we understand the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ for all $n$.

Proposition: $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic $\iff$ $n = p^l$ or $n = 2p^l$ for some odd prime $p$.

Proof: If $n = p^l$ or $n = 2p^l$ for an odd prime $p$, then it is clear using the above structure theorem that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic.

For the converse we use the following. A subgroup of a cyclic group is cyclic. If $H$ and $K$ are two groups of even order, then let $h \in H$ and $k \in K$ be elements of order 2. Then we have inclusions

$$\mathbb{Z}/2\mathbb{Z} \longrightarrow H \qquad \text{and} \qquad \mathbb{Z}/2\mathbb{Z} \longrightarrow K$$

$$\bar{1} \longmapsto h \qquad\qquad \bar{1} \longmapsto k$$

Taking their product we get a group homomorphism

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow H \times K \quad \text{which is an inclusion.}$$

But clearly, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not cyclic and so $H \times K$ is not cyclic.

Again use the structure theorem for $(\mathbb{Z}/n\mathbb{Z})^\times$ to conclude the converse.