Lecture 4: In the previous lecture we proved that the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. In this lecture let us analyze the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

We will use the following Lemma.

Lemma: (a) Let $n \geq 2$ and let p be an odd prime. Then
$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \mod p^n$$
(b) $(1+2^2)^{2^{n-3}} \equiv 1 + 2^{n-1} \mod 2^n$.

Proof: (a) We shall prove both assertions by induction on n. When $n = 2$, it is obvious that
$$(1+p)^{p^0} \equiv 1 + p \mod p^2.$$
Let us assume the assertion has been proved for all $k \leq n$ and consider $k = n+1$. By the induction hypothesis, we have
$$(1+p)^{p^{n-2}} = 1 + p^{n-1} + ap^n \quad \text{for some } a \in \mathbb{Z}$$
$$= 1 + p^{n-1}(1+ap)$$
Raising both sides to power p we get
$$(1+p)^{p^{n-1}} = (1 + p^{n-1}(1+ap))^p$$
$$= 1 + p^n(1+ap) + \sum_{i \geq 2} \binom{p}{i} \left[p^{(n-1)}(1+ap)\right]^i$$

When $i \geq 2$, we have $i(n-1) \geq 2(n-1) \geq n+1$ when $n \geq 3$.

Thus, $(1+p)^{p^{n-1}} = 1 + p^n + ap^{n+1} + p^{n+1}b$. Going mod p^{n+1} completes the proof of (a).

(b) The base case is $n = 3$, where the statement is obvious as $(1+2^2)^{2^0} \equiv 1 + 2^2 \mod 2^3$.

Let us assume the assertion has been proved for all $k \le n$ and consider $k = n+1$. By the induction hypothesis, we have

$$(1+2^2)^{2^{n-3}} = 1 + 2^{n-1} + a\,2^n \qquad \text{for some } a \in \mathbb{Z}$$
$$= 1 + 2^{n-1}(1+2a)$$

Squaring both sides we get

$$(1+2^2)^{2^{n-2}} = 1 + 2^n(1+2a) + 2^{2(n-1)}(1+2a)^2$$

$2(n-1) \ge n+1$ as $n \ge 3$.

$$\Rightarrow (1+2^2)^{2^{n-2}} = 1 + 2^n + 2^{n+1}a + 2^{n+1}b.$$

Going modulo 2^{n+1} proves (b).

We will need the following results from group theory, which we leave as exercises.

(G1) Let G be a group and let a be an element of order $l = l_1 l_2$. Then order of a^{l_1} is l_2.

(G2) Let G be a finite abelian group. Let $h \in G$ be an element of order l and let $k \in G$ be an element of order m. Then

(a) There is an element in G whose order is $\operatorname{lcm}(l,m)$.

(b) If $\gcd(l,m) = 1$, then order of $hk = lm$.

Lemma: Let $n > 1$ be an integer. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of residue classes $\bar{a}$ where $(a,n) = 1$.

Proof: Suppose $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \Rightarrow$ there is $\bar{b}$ such that $\bar{a}\bar{b} = 1$.

$\Rightarrow ab - 1 = yn \Rightarrow ab - yn = 1$.

Thus, 1 is in the ideal generated by a and n, and so $(a,n) = 1$.

Conversely, if $(a,n) = 1$, then there are integers b and y such that $ab - ny = 1$. Going mod n we see $\bar{a}\bar{b} = 1$, that is, $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

This completes the proof of the lemma. ◁

Proposition: Let p be an odd prime. Let $n \geq 1$. Then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is a cyclic group of order $p^{n-1}(p-1)$.

Proof: Let us first compute the cardinality of this group. The integers i, where $0 \leq i \leq p^n - 1$, give unique representatives for residue classes modulo p^n. In view of the previous lemma, $\bar{i} \in (\mathbb{Z}/p^n\mathbb{Z})^*$ $\iff$ $(i, p^n) = 1$. Note that $(i,p^n) = 1$ $\iff$ $(i,p) = 1$ $\iff$ $p \nmid i$.

Thus, we conclude $\#(\mathbb{Z}/p^n\mathbb{Z})^\times = \#\left\{ i \;\middle|\; \begin{matrix} 0 \leq i < p^n - 1 \\ p \nmid i \end{matrix} \right\}$

The multiples of p in the set $\{0, \dots, p^n - 1\}$ are precisely $\{ lp \mid 0 \leq l < p^{n-1} - 1 \}$.

Thus, $\#(\mathbb{Z}/p^n\mathbb{Z})^\times = \#(\mathbb{Z}/p^n\mathbb{Z}) - \#\{ lp \mid 0 \leq l < p^{n-1} - 1 \}$

$$= p^n - p^{n-1} = p^{n-1}(p-1).$$

To show that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic, we will produce two elements in this group, one which has order $p-1$ and the other which has order p^{n-1}. Then we will use (G2) above, which shows that there is an element of order $p^{n-1}(p-1)$.

Consider the ring homomorphism $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. This is clearly surjective.

We have inclusions

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \cup & & \cup \\ (\mathbb{Z}/p^n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \end{array}$$

Let $a \in \mathbb{Z}$ be such that $\bar{a}$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. As $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is surjective, there is b such that $\bar{b} \mapsto \bar{a}$. We claim that the integer b is coprime to p^n. To check this it suffices to check b is coprime to p. But $b \equiv a \bmod p$, which shows $p \nmid b$. Thus, b is coprime to p^n, and so $\bar{b}$ is in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Let l be the order of $\bar{b}$. Then $\bar{b}^l = 1 \bmod p^n$. Going mod p we get $\bar{a}^l \equiv 1 \bmod p$. As $\bar{a}$ has order $p-1 \Rightarrow p-1 \mid l$. Thus, $l = (p-1)m$.

Using (G1) we get that order of $\bar{b}^m$ is exactly $p-1$.

Among the elements $0 \le i < p^n - 1$, the elements which coprime to p are exactly $\left\{ a + pj \;\middle|\; \begin{array}{l} 1 \le a \le p-1 \text{ and} \\ 0 \le j < p^{n-1} - 1 \end{array} \right\}$.

Residue classes of these uniquely represent elements of $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus, from this description, it is clear that the map $(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ is given by $a + pj \mapsto a \bmod p$.
Clearly, the kernel of this map is residue classes

$K = \{ 1 + pj \mid 0 \le j < p^{n-1} - 1 \}$.

Notice that $\#K = p^{n-1}$. Thus, if $x \in K$ is any element, then order of x has to be of the form $p^{n'}$. It follows that if we find $x \in K$ such that $x^{p^{n-2}} \neq 1$, then the order of x is forced to be p^{n-1}. We will show precisely this.

By our earlier lemma it follows that

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \mod p^n.$$

As $1+p^{n-1} \not\equiv 1 \mod p^n$, it follows that order of $1+p$ is p^{n-1}.

Now using (6.2) it follows that there is an element of order $p^{n-1}(p-1)$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, that is, it is cyclic.