Primitive Roots

Let $p$ denote a prime number. As mentioned before, the group of invertible elements in $\mathbb{Z}/p\mathbb{Z}$ (which we'll denote by $(\mathbb{Z}/p\mathbb{Z})^\times$) is an abelian group of order $p - 1$. In other words, $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots, [p - 1]_p\}$ is an abelian group via multiplication in $\mathbb{Z}/p\mathbb{Z}$. We want to show that this is a cyclic group. In other words, we want to show that there is an $[a]_p$ of order $p - 1$.

**Lemma 1:** Suppose $G$ is an abelian group and suppose that $a$ and $b$ are elements of $G$ of finite order. If the greatest common divisor of $o(a)$ and $o(b)$ is 1, then $o(ab) = o(a)o(b)$.

**Proof:** For notational convenience, let's write $m = o(a)$ and $n = o(b)$. Consider the two cyclic subgroups $\langle a \rangle$ and $\langle b \rangle$ of $G$. The intersection of these two subgroups, call it $H$, is a subgroup of both $\langle a \rangle$ and $\langle b \rangle$. By Lagrange's Theorem, the order of $H$ must divide both $m$ and $n$. Since $m$ and $n$ are relatively prime, we conclude that the order of $H$ is 1. In other words, if $a^j = b^k$ for some $j, k \in \mathbb{Z}$, then $a^j = b^k = e$ since $a^j, b^k \in H = \{e\}$.

Since $G$ is abelian, $(ab)^j = a^j b^j$ for any integer $j$. Suppose $(ab)^j = e$. Then $a^j b^j = e$, so that $a^j = (b^j)^{-1} = b^{-j}$. Thus, $a^j = b^{-j} = e$. But this implies that $j$ is a multiple of $m$ and $n$, and since $m$ and $n$ are relatively prime, this means that $j$ must be a multiple of $mn$. Thus, the order of $ab$ is a multiple of $mn$. On the other hand, $(ab)^{mn} = (a^n)^m(b^m)^n = e^m e^n = e$, so the order of $ab$ is exactly $mn$.

**Lemma 2:** Suppose $G$ is a finite abelian group and choose an element $a \in G$ of largest order. Then $b^{o(a)} = e$ for all elements $b \in G$.

**Proof:** For notational convenience, write $n = o(a)$. Suppose to the contrary that there is an element $b$ where $b^n \neq e$. Write $m = o(b)$. Then $m \nmid n$. Via the Fundamental Theorem of Arithmetic, there must be a prime power $p^i$ which divides $m$ but doesn’t divide $n$. Write $n = p^i k$ and $m = p^i l$, where $p$ doesn’t divide $k$ or $l$. Since we said $p^i$ doesn’t divide $n$, $i$ must be less that $j$.

Now $a^{p^i}$ has order $k$ and $b^j$ has order $p^j$. Since $p \nmid k$, by Lemma 1 the element $a^{p^i}b^j$ has order $p^j k$. But $j > i$, which implies that $p^j k$ is greater than $p^i k$, which was supposedly the largest order of any element of $G$. This contradiction shows that there was no element $b$ with $b^n \neq e$. 


Theorem: For any prime number \( p \), the finite abelian group \( (\mathbb{Z}/p\mathbb{Z})^\times \) is cyclic.

Proof: Denote the largest order of the elements of \( (\mathbb{Z}/p\mathbb{Z})^\times \) by \( n \). Since \([a]_p^{p-1} = [1]_p\) by Fermat’s little Theorem (Lagrange’s Theorem, if you prefer) for all \([a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times\), we must have \( n \leq p - 1 \). We want to show that \( n = p - 1 \).

By Lemma 2, \([a]^n = [1]_p\) for all \([a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times\). In other words, every element of \( (\mathbb{Z}/p\mathbb{Z})^\times \) is a root of the polynomial \( X^n - [1]_p \), a polynomial with coefficients in \( \mathbb{Z}/p\mathbb{Z} \). This is a polynomial of degree \( n \) with \( p - 1 \) roots in \( \mathbb{Z}/p\mathbb{Z} \), so \( n \geq p - 1 \).

This shows that \( n = p - 1 \). In particular, there is an element of order \( p - 1 \), so that \( (\mathbb{Z}/p\mathbb{Z})^\times \) is cyclic.

An element of \( (\mathbb{Z}/p\mathbb{Z})^\times \) of order \( p - 1 \), i.e., a generator of the cyclic group, is called a primitive root mod \( p \).