Recall that our goal is to show that $\mathbb{Z}_p^\times$ is cyclic when $p$ is a prime number. Here’s what we have so far:

• $\mathbb{Z}_p^\times$ is a finite abelian group of order $p - 1$.

• By Lagrange’s theorem $[a]_p^{p-1} = 1$ for all $[a]_p \in \mathbb{Z}_p^\times$.

• There is a smallest number $n$ such that $[a]_p^n = 1$ for all $[a]_p \in \mathbb{Z}_p^\times$. This number $n$ is called the exponent of the group $\mathbb{Z}_p^\times$.

• This number $n$ is no greater than $p - 1$.

• There is an element of $\mathbb{Z}_p^\times$ whose order is this number $n$.

The goal, then, is to show that this number $n$ is equal to $p - 1$.

Now this is all just from the theory of groups. Since not all groups of order $p - 1$ are cyclic, there must be something special about $\mathbb{Z}_p^\times$. Notice that we’ve only used multiplication; we can also add elements of $\mathbb{Z}_p^\times$ together. In other words, we haven’t used the fact that $\mathbb{Z}_p$ is a field.

Definition: Suppose $F$ is a field. An element $a \in F^\times$ is called a root of unity if $a^n = 1$ for some positive integer $n$. In other words, the roots of unity of $F$ are the elements of the group $F^\times$ of finite order.

Note that the set of roots of unity of a field is a subgroup of the group of non-zero elements of the field.

Examples:

1) $\mathbb{R}$

2) $\mathbb{Z}_p$

3) $\mathbb{C}$
**Theorem 2**: Suppose $F$ is a field with finitely many roots of unity. Then the group of roots of unity is cyclic. In particular, the group $\mathbb{Z}_p^\times$ is cyclic for any prime number $p$.

**Proof**: Let $U$ denote the group of roots of unity and let $m$ denote its order. Since $U$ is a finite abelian group, it has a finite exponent; call it $n$. Then $a^n = 1$ for all $a \in U$ and $n \leq m$. Moreover, there is an element of $U$ of order $n$.

Now each $a \in U$ is a root of the polynomial $X^n - 1$. This is a polynomial with coefficients in $F$. For any $a \in U$ we can use the division algorithm for polynomials with coefficients in $F$ and write

$$X^n - 1 = Q(X)(X - a) + R(X),$$

where the degree of $R(X)$ is no greater than zero. Since $a$ is a root of both $X^n - 1$ and $X - a$, it must also be a root of $R(X)$. But since the degree of $R(X)$ is no greater than zero, $R(X)$ must be 0. In this way we see that the monic degree one polynomial $X - a$ divides the polynomial $X^n - 1$ for all roots of unity $a$.

There are $m$ roots of unity, and corresponding to each of these roots of unity is a distinct monic polynomial of degree one that divides $X^n - 1$. Denote the product of these $m$ monic polynomials of degree one by $P(X)$; the degree of $P(X)$ is $m$. Since polynomials of degree 1 are irreducible, we have $m$ distinct monic irreducible factors of the polynomial $X^n - 1$. According to the Fundamental Theorem of Arithmetic for polynomials, the product $P(X)$ of these distinct monic irreducible polynomials must divide $X^n - 1$.

We have constructed a polynomial $P(X)$ of degree $m$ that divides the polynomial $X^n - 1$ of degree $n$. This implies that $m \leq n$, and since we already knew $n \leq m$, we must have $n = m$. Since $U$ has an element of order $n = m$, which is the order of $U$, the group $U$ must be cyclic.