Proof that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic

Uthsav Chitra

March 14, 2017

1 Preliminary Results

We present here a more group-theoretic proof that the unit group of $\mathbb{Z}/p\mathbb{Z}$ is cyclic.

Definition 1.1

Let G be a finite, abelian group, and let $g \in G$. We define **the order of** g, or $\text{ord}(g)$, as the least positive integer n such that $g^n = 1$. Alternatively, we can define $\text{ord}(g)$ as the greatest common factor of $\{x \in \mathbb{Z} : g^x = 1\}$. (Why are these equal?)

We first prove some lemmas. In what follows, assume G is a finite, abelian group.

Lemma 1.2

Let $a \in G$, with $\text{ord}(a) = n$. Then, for any $k \mid n$, there exists a $c \in G$ with $\text{ord}(c) = k$.

Proof. Take $c = a^{n/k}$. □

Lemma 1.3

Let $a, b \in G$, with $\text{ord}(a) = n$, $\text{ord}(b) = m$, with $(n, m) = 1$. Then, there exists $c \in G$ with $\text{ord}(c) = nm$.

Proof. I claim ab has order nm. Since $(ab)^{nm} = (a^n)^m(b^m)^n = 1^m 1^n = 1$, we can write $\text{ord}(ab) = k$, for some $k \mid nm$. Now,

$$(ab)^k = 1 \implies a^k = b^{-k}. \tag{1}$$

Raising both sides to the mth power yields $a^{mk} = 1$. Thus, $n \mid mk$. But since $(n, m) = 1$, this implies $n \mid k$. Switching the role of a and b, we also see that $m \mid k$. Thus, $nm \mid k$, so we have $k = nm$. □

Lemma 1.4

Let $a, b \in G$, with $\text{ord}(a) = n$ and $\text{ord}(b) = m$. Then, there exists $c \in G$ such that $\text{ord}(c) = [n, m]$.

Proof. By the first lemma, there exists $c_1, c_2, c_3 \in G$ with

$$\text{ord}(c_1) = (n, m) \tag{2}$$

$$\text{ord}(c_2) = \frac{n}{(n, m)} \tag{3}$$

$$\text{ord}(c_3) = \frac{m}{(n, m)}. \tag{4}$$

Since each of the above orders are pairwise relatively prime, by the second lemma, there exists $c \in G$ such that

$$\operatorname{ord}(c) = (n, m) \cdot \frac{n}{(n, m)} \cdot \frac{m}{(n, m)} = \frac{nm}{(n, m)} = [n, m], \tag{5}$$

as desired. □

We include the following lemma for completeness. Its proof can be found in Chapter 4 of the textbook (Ireland-Rosen).

Lemma 1.5

For $d \mid p - 1$, $x^d - 1$ has exactly d roots in $(\mathbb{Z}/p\mathbb{Z})^\times$.

2 Proof

Theorem 2.1

$(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proof. Assume not. Let $\operatorname{ord}(i) = m_i$, let $G = (\mathbb{Z}/p\mathbb{Z})^\times$, and let $d = [m_1, \ldots, m_{p-1}]$. By Lemma 1.4, there exists $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $\operatorname{ord}(c) = d$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is not cyclic, d must be a strict divisor of $p - 1$, since otherwise c would be a generator.

Now, for every $i \in (\mathbb{Z}/p\mathbb{Z})^\times$, since $m_i \mid d$, we have

$$i^d - 1 = (i^{m_i})^{d/m_i} - 1 = 1^{d/m_i} - 1 = 0. \tag{6}$$

Thus, every $i \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a root of $x^d - 1$, so $x^d - 1$ has $p - 1$ roots. However, by Lemma 1.5, $x^d - 1$ has exactly d roots. Since $d < p - 1$, we have a contradiction. □