Structure of $(\mathbb{Z}/p^n\mathbb{Z})^\times$

Seewoo Lee

February 15, 2022

We are going to prove the following well-known result:

Theorem 1. *Let p be a prime and $n \geq 1$ be an integer. Then*

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \begin{cases} \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z} & p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & p = 2,\ n \geq 2 \\ 1 & p = 2,\ n = 1 \end{cases}$$

In other words, unit group of a ring $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic for odd prime p and product of two cyclic groups for $p = 2$. There are some elementary proofs of this, but they are all complicated. Here we introduce p-adic proof of this.

First, we'll deal with odd prime p, since $p = 2$ case needs more concern.

Proposition 1. *For an odd prime p, we have*

$$\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

Proof. Consider the following exact sequence of abelian groups

$$1 \to 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \xrightarrow{\bmod p} (\mathbb{Z}/p\mathbb{Z})^\times \to 1.$$

Surprisingly, there exists a section $\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ of mod p map, which is called the Teichmüller character. This map is defined as

$$\omega(x) := \lim_{n\to\infty} x^{p^n},$$

which converges. (This can be regarded as a unique solution of $\omega(x)^p = \omega(x)$ that is congruent to x mod p.) Hence the sequence splits and we have

$$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times (1 + p\mathbb{Z}_p)$$

since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. To prove $(1 + p\mathbb{Z}_p, \times) \simeq (\mathbb{Z}_p, +)$, we use the logarithm map, defined as a power series. For $x \in p\mathbb{Z}_p$, the series

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$$

converges and satisfies $\log((1+x)(1+y)) = \log(1+x) + \log(1+y)$. One can show that this gives an isomorphism between $1 + p\mathbb{Z}_p$ and $p\mathbb{Z}_p$, and the inverse map corresponds to an exponential map

$$\exp : p\mathbb{Z}_p \to 1 + p\mathbb{Z}_p, \quad z \mapsto 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} \cdots .$$

Hence we have an isomorphism

$$(1 + p\mathbb{Z}_p, \times) \to (\mathbb{Z}_p, +), \quad 1 + x \mapsto \frac{1}{p} \log(1 + x) = \frac{1}{p}\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots\right).$$

Note that by unfolding all of these, the resulting isomorphism $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \to \mathbb{Z}_p^\times$ can be written as

$$(m, z) \mapsto \omega(g_p^m) \exp(pz) = \omega(g_p)^m \exp(pz)$$

where g_p is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$. $\square$

Now we can prove our theorem for the odd prime case. Consider the following diagram:

$$\begin{tikzcd}
1 \arrow[r] & 1 + p\mathbb{Z}_p \arrow[r] \arrow[d, "\text{mod } p^n"'] & \mathbb{Z}_p^\times \arrow[r, "\text{mod } p"] \arrow[d, "\text{mod } p^n"'] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] \arrow[d, equal] \arrow[l, dotted, bend left, "\omega"] & 1 \\
1 \arrow[r] & U \arrow[r] & (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r, "\text{mod } p"] & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] \arrow[l, dotted, bend left, "\omega \text{ mod } p^n"] & 1
\end{tikzcd}$$

where

$$U = \{a \equiv 1 \pmod{p}\} \subset (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

This is a commutative diagram and the first row is exact, and it is easy to check that second row is also exact. Hence $(\mathbb{Z}/p^n)^\times \simeq U \times (\mathbb{Z}/p\mathbb{Z})^\times$. Since U and $(\mathbb{Z}/p\mathbb{Z})^\times$ have coprime orders, we only need to check that U is a cyclic group.

We've already showed that $(\mathbb{Z}_p, +) \simeq (1 + p\mathbb{Z}_p, \times)$, and $\mathbb{Z}$ is a cyclic dense subgroup of $\mathbb{Z}_p$. Now we have a following diagram

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \simeq 1 + p\mathbb{Z}_p \to U$$

where the last map is a mod p^n reduction map. All of these maps are continuous when we endow U with a discrete topology. Hence the image of $\mathbb{Z}$ under this map is a dense subgroup of U, so is U itself. In other words, the image of 1, $\exp(p)$, is a generator of U.

By combining all of these maps, we can compute a generator of the cyclic group $(\mathbb{Z}/p^n\mathbb{Z})^\times$:

$$g_{p,n} = \omega(g_p) \exp(p) \text{ mod } p^n$$

is a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

For example, let $p = 5$ and $n = 4$. Then $(\mathbb{Z}/5\mathbb{Z})^\times = \langle 2 \rangle$. We have

$$\begin{aligned}\omega(2) &= \lim_{n\to\infty} 2^{5^n} \\ &\equiv 2^{5^4} \pmod{5^4} \\ &\equiv 182 \pmod{5^4}\end{aligned}$$

and

$$\begin{aligned}\exp(5) &= 1 + 5 + \frac{5^2}{2} + \frac{5^3}{6} + \cdots \\ &\equiv 1 + 5 - 2\cdot 5^2 \cdot (1 + 5 + 5^2 + \cdots) + 5^3 \cdot (1 - 5 + 5^2 - \cdots) \pmod{5^4} \\ &\equiv 1 + 5 - 2\cdot 5^2 + 3\cdot 5^3 \pmod{5^4} \\ &\equiv 71 \pmod{5^4}\end{aligned}$$

Hence

$$182 \cdot 71 \equiv 422 \pmod{5^4}$$

is a generator of $(\mathbb{Z}/5^4\mathbb{Z})^\times$.

In case of $p = 2$, exponential function doesn't converges on $2\mathbb{Z}_2 \subset \mathbb{Z}_2$, so we have to study more carefully. We have the following:

Proposition 2.

$$\mathbb{Z}_2^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$$

Proof. Consider the following exact sequence of abelian groups

$$1 \to 1 + 4\mathbb{Z}_2 \to \mathbb{Z}_2^\times \xrightarrow{\text{mod } 4} (\mathbb{Z}/4\mathbb{Z})^\times \to 1.$$

This exact sequence splits since there exists a section $(\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{Z}_2^\times$ defined as $3 \mapsto -1$. Hence we have

$$\mathbb{Z}_2^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times (1 + 4\mathbb{Z}_2).$$

Now, as before, logarithm and exponential maps give isomorphism between $(1 + 4\mathbb{Z}_2, \times)$ and $(\mathbb{Z}_2, +)$. We have

$$(1 + 4\mathbb{Z}_2, \times) \simeq (\mathbb{Z}_2, +), \quad 1 + x \mapsto \frac{1}{4}\log(1+x) = \frac{1}{4}\left(x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots\right)$$

with an inverse

$$(\mathbb{Z}_2, +) \simeq (1 + 4\mathbb{Z}_2, \times), \quad z \mapsto \exp(4z) = 1 + 4z + \frac{(4z)^2}{2!} + \frac{(4z)^3}{3!} + \cdots$$

$\square$

Now we can prove our theorem for $p = 2$. Assume that $n > 1$. Consider the following diagram:

$$
\begin{tikzcd}
1 \arrow[r] & 1+4\mathbb{Z}_2 \arrow[r] \arrow[d, "\bmod 2^n"'] & \mathbb{Z}_2^\times \arrow[r, "\bmod 4"] \arrow[d, "\bmod 2^n"'] & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[r] \arrow[l, dotted, bend left, "\omega"] \arrow[d, equal] & 1 \\
1 \arrow[r] & U \arrow[r] & (\mathbb{Z}/2^n\mathbb{Z})^\times \arrow[r, "\bmod 4"] & (\mathbb{Z}/4\mathbb{Z})^\times \arrow[r] \arrow[l, dotted, bend left, "\omega \bmod 2^n"] & 1
\end{tikzcd}
$$

where

$$U = \{a \equiv 1 \pmod 4\} \subset (\mathbb{Z}/2^n\mathbb{Z})^\times.$$

As before, the diagram commutes and both rows are split exact. By the same argument as $p > 2$, U is a cyclic group and we have

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times U \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

Hence $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has index 2 cyclic subgroup, which is generated by $\exp(4)$.

For example, if $n = 6$, then

$$
\begin{aligned}
\exp(4) &= 1 + 4 + \frac{4^2}{2} + \frac{4^3}{6} + \frac{4^4}{24} + \frac{4^5}{120} + \cdots \\
&\equiv 1 + 2^2 + 2^3 + 2^5 \cdot (1 - 2 + 2^2 - \cdots) + 2^5 \cdot (1 - 2 + 2^2 - \cdots) \pmod{2^6} \\
&\equiv 1 + 2^2 + 2^3 + 2 \cdot 2^5 \pmod{2^6} \\
&\equiv 13 \pmod{2^6}
\end{aligned}
$$

so 13 is an element of $(\mathbb{Z}/2^6\mathbb{Z})^\times$ of order $16 = 2^4$, and $(\mathbb{Z}/2^6\mathbb{Z})^\times$ is generated by 13 and -1.