Structure of $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$

Ryan Taylor

October 2021

1 Introduction

This is basically for my own reference. I always return to proving this all over again once and once again, simply because I do not remember how I proved it last time. I think every time the prove goes a little different. Therefore, this is to set the record for the proof I came up with this time, 10 Oct. 2021. It bases on some problem sets I did 3 years ago at Ross Mathematics Program.

2 $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ Cyclic

Theorem 2.1. *Let p be a prime number. The group $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ is Cyclic.*

There are a lot of proofs for this. Some use the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field and a polynomial has roots no more than its degree, some others use properties of abelian groups. Either way, I will not prove it here. I might do later when I have more free time. But now I have notes to write up, example sheets to look at (Algebraic Topology is hard) and we are here to day to only quickly remark upon the structure of $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$.

3 Order of $1+p$ in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$

As the title suggests, we investigate the order of $1+p+p^k\mathbb{Z}$ in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$.

Lemma 3.1. *Let p be a prime number, $k \geq 1$ positive integer. Then*

- *If $p \neq 2$, $a \equiv 1 \pmod{p^k} \iff a^p \equiv 1 \pmod{p^{k+1}}$;*
- *If $p = 2$, $a \equiv \pm 1 \pmod{2^k} \iff a^2 \equiv 1 \pmod{2^{k+1}}$.*

Proof. **Case 1**: $p \neq 2$.
($\Longrightarrow$) Suppose $a \equiv 1 \pmod{p^k}$. Then $a \equiv 1(p)$, and hence

$$1 + a + \cdots + a^{p-1} \equiv 1 + 1 + \cdots + 1 \equiv 0 \pmod{p}$$

Hence $p \cdot p^k \mid (a-1)\left(1 + a + \cdots + a^{p-1}\right) = (a^p - 1)$, equivalently $a^p \equiv 1(p^{k+1})$.

($\Longleftarrow$) Suppose $a^p \equiv 1(p^{k+1})$. Then $a^p \equiv 1(p)$ and hence $a \equiv 1(p)$ by Fermat's Little Theorem. Again, $p \mid (1 + a + \cdots + a^{p-1})$.

Suppose $a \equiv 1 + np(p^2)$ for some $n \in \{0, 1, \ldots, p-1\}$. We have

$$\begin{aligned} 1 + a + \cdots + a^{p-1} \pmod{p^2} &\equiv 1 + (1+np) + (1+np)^2 + \cdots + (1+np)^{p-1} \pmod{p^2} \\ &\equiv 1 + (1+np) + (1+2np) + \ldots (1+(p-1)np) \pmod{p^2} \\ &\equiv p + np(1 + 2 + \cdots + p - 1) \pmod{p^2} \\ &\equiv p + np^2 \frac{p-1}{2} \pmod{p^2} \\ &\equiv p \pmod{p^2} \end{aligned}$$

Hence $p^2 \nmid (1 + a + \cdots + a^{p-1})$. Hence the power of p in $(1 + a + \cdots + a^{p-1})$ is exactly 1. As $p^{k+1} \mid (a^p - 1) = (a-1)(1 + a + \cdots + a^{p-1})$, $p^k \mid (a-1)$ and hence $a \equiv 1(p^k)$.

Case 2: $p = 2$. Even though $(a \pm 1)$ are both even, they cannot be both multiple of 2^2. Hence

$$\begin{aligned} a^2 \equiv 1 \pmod{2^{k+1}} &\iff 2^{k+1} \mid (a-1)(a+1) \\ &\iff a \equiv 1, 2^k - 1, 2^k + 1, -1 \pmod{2^{k+1}} \\ &\iff a \equiv \pm 1 \pmod{2^k} \end{aligned}$$

□

Due to this special disobedience of $p = 2$, we have to do case work in a the remaining parts of the paper.

Lemma 3.2. *Let $p \neq 2$ be a prime number, and $k \geq 1$ positive integer. Then*

- $(1+p)^{p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$;
- $(1+p)^{p^k} \equiv 1 \pmod{p^{k+1}}$.

In other words, $(1+p)$ has order p^k in $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$.

We prove this by induction.

When $k = 1$, $(1+p)^{p^0} = 1 + p \not\equiv 1(p^2)$ clearly. On the other hand,

$$(1+p)^{p^1} \equiv 1 + \binom{p}{1} p \equiv 1 \pmod{p^2},$$

When $k \geq 2$, by Lemma 3.1 and induction hypothesis we have

- $(1+p)^{p^{k-2}} \not\equiv 1 \pmod{p^k} \iff (1+p)^{p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$;
- $(1+p)^{p^{k-1}} \equiv 1 \pmod{p^k} \iff (1+p)^{p^k} \equiv 1 \pmod{p^{k+1}}$.

This lemma in the case $p = 2$ is quite different and much more difficult to prove:

Lemma 3.3. *Let $k \geq 1$ positive integer. Then $3^{2^k} \equiv 1 \pmod{2^{k+2}}$.*

Proof. We also prove this statement by induction. When $k = 1$, $3^{2^1} = 9 \equiv 1 \pmod{2^3}$. When $k \geq 2$, by Lemma 3.1 and induction hypothesis,

$$3^{2^{k-1}} \equiv 1 \pmod{2^{k+1}} \implies 3^{2^k} \equiv 1 \pmod{2^{k+2}}.$$

□

Lemma 3.4. *Let $k \geq 2$, $1 \leq n \leq k$ both be positive integers. Suppose $n = 2^{m_0}q$ for some q odd and m_0 nonnegative integer. The power of 2 in the factorisation of $\binom{2^k}{n}$ is $k - m_0$.*

Proof. We know the formula for the power of 2 in a factorial. Hence

$$\begin{aligned}
\text{Power of 2 in } \binom{2^k}{n} &= \sum_{m=1}^{\infty} \left(\lfloor \frac{2^k}{2^m} \rfloor - \lfloor \frac{2^k - n}{2^m} \rfloor - \lfloor \frac{n}{2^m} \rfloor \right) \\
&= \sum_{m=1}^{k} \left(2^{k-m} - \lfloor 2^{k-m} - \frac{n}{2^m} \rfloor - \lfloor \frac{n}{2^m} \rfloor \right) \\
&= \sum_{m=1}^{k} \left(\lceil \frac{n}{2^m} \rceil - \lfloor \frac{n}{2^m} \rfloor \right) \\
&= \#\{m \mid 1 \leq m \leq k, 2^m \nmid n\} \\
&= \#\{m \mid m_0 < m \leq k\} \\
&= k - m_0
\end{aligned}$$

□

Lemma 3.5. *When $k \geq 2$, $3^{2^{k-1}} \equiv 2^{k+1} + 1 \not\equiv 1 \pmod{2^{k+2}}$.*

Proof. We attempt to expand $3^{2^{k-1}} \pmod{2^{k+2}}$ by regarding $3 = 1 + 2$ and use the binomial theorem. We have the terms $\binom{2^{k-1}}{n}2^n$ for $n = 0, \ldots, 2^{k-1}$ in the binomial expansion. We analyse first, which terms do not vanish $\pmod{2^{k+2}}$ by examining the power of 2 in that term.

By Lemma 3.5, when $0 \neq n = 2^{m_0}q$, the power of 2 in $\binom{2^{k-1}}{n}2^n$ is $n + k - 1 - m_0$. When is this power less than $k + 2$? Equivalently, when does $2^{m_0}q - m_0 \leq 2$? By doing careful (and easy) casework, and noticing q must be odd, we receive $(m_0, q) = (0, 1), (1, 1)$, or $(2, 1)$, which corresponds to $n = 1, 2, 4$. Adding the case $n = 0$, we realise that all other terms $\binom{2^{k-1}}{n}2^n$ vanish $\pmod{2^{k+2}}$ except when $n = 0, 1, 2, 4$. Hence

$$\begin{aligned}
3^{2^{k-1}} &\equiv (1+2)^{2^{k-1}} \pmod{2^{k+2}} \\
&\equiv \sum_{n=0,1,2,4} \binom{2^{k-1}}{n} 2^n \pmod{2^{k+2}} \\
&\equiv 1 + 2^k + 2^k(2^{k-1} - 1) + \frac{1}{3}\left[(2^{k-1} - 1)(2^{k-2} - 1)(2^{k-1} - 3)\right] 2^{k+1} \pmod{2^{k+2}} \\
&\equiv 1 + 2^{2k-1} + 2^{k+1}(2^{k-2} - 1) \pmod{2^{k+2}}
\end{aligned}$$

- When $k = 2$, this reduces to $1 + 2^{2k-1} \equiv 1 + 2^3 \pmod{2^4}$;
- when $k \geq 3$, $2k - 1 \geq k + 2$ and $2^{k-2} - 1$ is odd. Hence this reduces to $1 + 2^{k+1} \pmod{2^{k+2}}$.

Either way, we receive $3^{2^{k-1}} \equiv 2^{k+1} + 1 \not\equiv 1 \pmod{2^{k+2}}$. □

Remark. When $k = 1$, $3^{2^0} \equiv 3 \equiv 2^2 - 1 \pmod{2^3}$. It is not $2^2 + 1$, but at least it is not 1. So 3 has order 2 in $(\mathbb{Z}/2^3\mathbb{Z})^*$

Combining this Remark, Lemma 3.3 and 3.5,

Corollary 3.5.1. *When $k \geq 1$, 3 has order 2^k in $(\mathbb{Z}/2^{k+2}\mathbb{Z})^*$.*

4 Structure of $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$

Again, we need to separate the case $p = 2$. We do $p \neq 2$ first.

Lemma 4.1. *Let G be an abelian group, and g, $h \in G$ has order m and n respectively. Furthermore assume $(m, n) = 1$. Then gh has order mn.*

Proof. Suppose gh has order r. Clearly $(gh)^{mn} = e$, so $r \mid mn$. We show $mn \mid r$.

As $(gh)^r = 1$, $g^r = (h^{-1})^r$. Left hand side is an element with order dividing m, right hand side is an element with order dividing n. But they are the same element! Therefore, this element must have order 1 as $(m, n) = 1$, and hence $g^r = (h^{-1})^r = 1$. We conclude $m|r$ and $n|r$. □

Theorem 4.2. *Suppose $p \neq 2$, and $k \geq 1$. Then $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ is a cyclic group of order $(p-1)p^{k-1}$.*

Proof. The part about the group's order is obvious (Euler Totient Function). The case where $k = 1$ is exactly Theorem 2.1. Now we assume $k \geq 2$.

By Lemma 3.2, $(1 + p)$ has order p^{k-1} in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$. By Theorem 2.1, there is an element $a \in \{0, \ldots, p-1\}$ with order $p - 1$ in $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$. Then the order of a must be divisible by $p - 1$ in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$, as $a^r \equiv 1(p^k) \implies a^r \equiv 1(p) \implies (p-1)|r$. Hence there is some power of a, say a', with order $p - 1$ in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$.

We found element of order p^{k-1} and $p - 1$ in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$. By Lemma 4.1, their product has order $(p-1)p^{k-1}$, which is the size of the group. Hence it is a cyclic group. □

Theorem 4.3. *Suppose $k \geq 2$. Then $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^* \cong C_2 \times C_{2^{k-2}}$.*

Proof. There are two proofs for this. One constructive, and the other less so. We begin with the non-constructive proof first.

We first realize that all of the results in Section 3 with modulo 2^k definitely applies to cases when $k \geq 4$. Therefore, one could check the cases $k = 2$ and $k = 3$ manually, or perform a similar argument but be careful. Checking is insanely easy, because there are groups of order 2 and 4. We assume $k \geq 4$. Now we proceed with the first proof.

First Proof starts here

Easily, $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ is an abelian group of order 2^{k-1}. Using the theory of finite abelian groups, it must be the direct product of some cyclic groups, each of order a power of 2. We know that it cannot be $C_{2^{k-1}}$: take any element $a \in \{1, 3, \ldots, 2^k - 1\}$, then $a^2 \equiv 1 \pmod{2^3}$, and by Lemma 3.1, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$, so it cannot have order 2^{k-2}. [Another way to realize that the group cannot be cyclic is because it has $3 \neq \varphi(2)$ elements of order 2: $\pm 1, 2^k \pm 1$ by Lemma 3.1]

On the other hand, 3 is an element of order 2^{k-2} exactly by Corollary 3.5.1. Upon contemplation, the only possible structure for this group is $C_2 \times C_{2^{k-2}}$.

First Proof ends here

I know. This proof is not so satisfying. So here is a proof that tells you how to construct an isomorphism between $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ and $C_2 \times C_{2^{k-2}}$.

Second Proof starts here

Again, 3 is an element of order 2^{k-2} by Corollary 3.5.1. We consider $\langle 3\rangle \leq \left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$. This cyclic group of order 2^{k-2} has exactly $\varphi(2) = 1$ element of order 2. By its uniqueness, it must be $3^{2^{k-3}}$. What is it? This is why we explicitly calculated it in Lemma 3.5: it is $2^{k-1}+1$ [and, when $k = 3$, $2^{k-1} - 1$]. Hence, we see that -1, another element of order 2, is not in the group!

Hence $\langle 3\rangle$ and $\langle -1\rangle$ are two normal subgroups of $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ that only intersect at the identity. Their sizes, 2^{k-2} and 2, multiply to the size of the group. Hence, by the Direct Product Theorem, $\langle 3\rangle \times \langle -1\rangle \cong \left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$. The isomorphism is also given by the Direct Product Theorem: $(3^m, (-1)^n) \mapsto 3^m(-1)^n$.

Second Proof ends here □

5 Structure of $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$

Chinese Remainder Theorem!