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

R. C. Daileda

April 6, 2018

The group-theoretic structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ is well-known. We have seen that if $N = p_1^{n_1} \cdots p_r^{n_r}$ with p_i distinct primes and $n_i \in \mathbb{N}$, then the ring isomorphism ρ of the Chinese remainder theorem provides a multiplication preserving bijection

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/p_1^{n_1}\mathbb{Z})^\times \times \cdots (\mathbb{Z}/p_r^{n_r}\mathbb{Z})^\times$$

(below we will define such a function to be a *group ismorphism*). This reduces the study of the general unit group $(\mathbb{Z}/n\mathbb{Z})^\times$ to understanding the unit group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ with prime power modulus. It turns out that the structure of these groups depends on whether or not $p = 2$. Moreover, when p is odd, the proof of the main structure theorem on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ will be broken down into the cases $n = 1$, $n = 2$ and $n \geq 3$ separately. Before we can get into any of this, however, we need some preliminary results.

1 Gauss' Result on $\varphi(n)$

Given $n \in \mathbb{N}$ and a positive $d|n$ let

$$S_d = \{1 \leq a \leq n \,|\, (a,n) = d\}$$

and

$$T_d = \left\{ k\frac{n}{d} \,|\, 1 \leq k \leq d, (k,d) = 1 \right\}.$$

The sets S_d partition the integers from 1 to n according to their GCD with n.

We claim that

$$S_{n/d} = T_d. \tag{1}$$

First note that any element $k\frac{n}{d} \in T_d$ satisfies

$$\left(k\frac{n}{d}, n\right) = \left(k\frac{n}{d}, d\frac{n}{d}\right) = \frac{n}{d}\,(k,d) = \frac{n}{d}$$

and hence belongs to $S_{n/d}$. Conversely, for $a \in S_{n/d}$ we have

$$\frac{n}{d} = (a,n) = \left(\frac{a}{n/d}\frac{n}{d}, d\frac{n}{d}\right) = \frac{n}{d}\left(\frac{a}{n/d}, d\right) \;\Rightarrow\; \left(\frac{a}{n/d}, d\right) = 1,$$

and hence $a = \frac{a}{n/d}\frac{n}{d} \in T_d$.

We apply (1) to prove the following essential result on Euler's φ function.

Corollary 1 (Gauss)**.** *For any* $n \in \mathbb{N}$*,*

$$\sum_{d|n} \varphi(d) = n,$$

the sum running over the positive divisors of n*.*

Proof. As d runs through the (positive) divisors of n, so does n/d. Hence,

$$\{1 \leq a \leq n\} = \bigcup_{d|n} S_d = \bigcup_{d|n} S_{n/d}$$

since (a, n) takes on the value of each divisor of n at least once. Since the sets S_d are pairwise disjoint (no integer has more than one GCD with n), taking the size of each of the sets above, and using equation (1), yields

$$n = \sum_{d|n} |S_{n/d}| = \sum_{d|n} |T_d| = \sum_{d|n} \varphi(d).$$

□

Example 1. The (positive) divisors of 20 are 1, 2, 4, 5, 10 and 20. We see that

$$\sum_{d|20} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) = 1 + 1 + 2 + 4 + 4 + 8 = 20,$$

as claimed. ♦

2 Cyclic Groups and Primitive Roots

Definition 1. Let G be a group and $g \in G$. The set

$$\langle g \rangle = \{g^n \,|\, n \in \mathbb{Z}\}$$

is called the *cyclic subgroup (of* G*) generated by* g*.* If $G = \langle g \rangle$ for some $g \in G$ we say that G is *cyclic.* ▲

Remark 1. The set $\langle g \rangle$ is itself a group under the binary operation on G. Hence the use of the term *subgroup.* ▼

Definition 2. If $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic with generator $a + n\mathbb{Z}$, we say that a is a *primitive root modulo* n*.* ▲

Remark 2. Although entirely standard, we find the term *primitive root* to be somewhat archaic. We have introduced it in the interest of cultural literacy, but will rarely use it, preferring the term *generator* instead. ▼

Example 2.

- $(\mathbb{Z}, +)$ is cyclic since it is generated by ± 1, e.g. $n = n \cdot 1$ for and $n \in \mathbb{Z}$.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic since it is generated by $1 + n\mathbb{Z}$, i.e. $a + n\mathbb{Z} = a(1 + n\mathbb{Z})$ for any $a \in \mathbb{Z}$.
- $(\mathbb{Z}/8\mathbb{Z})^\times$ is *not* cyclic since for any $x + 8\mathbb{Z} \in (\mathbb{Z}/8\mathbb{Z})^\times$,
$$\langle x + 8\mathbb{Z}\rangle = \{1 + 8\mathbb{Z}, x + 8\mathbb{Z}\} \neq (\mathbb{Z}/8\mathbb{Z})^\times$$
since $x^2 \equiv 1 \pmod 8$ for all odd x. Therefore there does not exist a primitive root modulo 8.
- Every cyclic group is abelian since $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$ for all $m, n \in \mathbb{Z}$.

♦

Given an element $g \in G$, the size of $\langle g\rangle$ is intimately related to $\mathrm{ord}(g)$.

Lemma 1. *Let G be a group and $g \in G$. Then $|\langle g\rangle| = \mathrm{ord}(g)$.*

Proof. First assume $\mathrm{ord}(g) = \infty$. Then no two powers of g are equal, for otherwise we'd have $g^i = g^j$ with $i < j$ and hence $g^{j-i} = e$ with $j - i > 0$, implying $\mathrm{ord}(g) < \infty$. Thus $\langle g\rangle$ is infinite (it can be bijected with $\mathbb{Z}$), and the result follows.[1]

Now suppose $\mathrm{ord}(g) = n \in \mathbb{N}$. The group elements $e, g, g^2, \ldots, g^{n-1}$ must be distinct since otherwise, as above, we end up with $g^k = e$ for some $1 \leq k \leq n-1$, contradicting the minimality of $n = \mathrm{ord}(g)$. Moreover, given any $m \in \mathbb{Z}$ we can write $m = qn + r$ with $0 \leq r \leq n - 1$ so that
$$g^m = (g^n)^q g^r = e^q g^r = g^r \in \{e, g, g^2, \ldots, g^{n-1}\}.$$
It follows that $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$, and since these elements are distinct, $|\langle g\rangle| = n = \mathrm{ord}(g)$.

□

Remark 3.

If G is a finite group and $g \in G$, then G is cyclic and generated by g if and only if $\mathrm{ord}(g) = |G|$. We will tacitly assume this fact from now on.

▼

Lemma 2 (Generators of a Cyclic Group)**.** *Let $G = \langle g\rangle$ be a finite cyclic group of order n. Then $G = \langle h\rangle$ if and only if*
$$h \in \{g^a \mid (a, n) = 1\}.$$

Proof. Suppose that $h = g^a$ with $(a, n) = 1$. Then clearly $\langle h\rangle \subseteq \langle g\rangle$ as every power of h is a power of g. For the reverse containment, use Bézout's lemma to write $ra + sn = 1$. Then $h^r = g^{ar} = g^{1-sn} = g \cdot (g^n)^{-s} = g \cdot e = g$. Hence every power of g is a power of h and so $\langle g\rangle \subseteq \langle h\rangle$ as well.

Now suppose that $\langle g\rangle = \langle h\rangle$. Then $h = g^a$ for some $a \in \mathbb{Z}$. Since $g \in \langle h\rangle$, $g = h^r = g^{ra}$ for some $r \in \mathbb{Z}$. Hence $g^{1-ra} = e$ so that $n = \mathrm{ord}(g)$ (by the previous lemma) divides $1 - ra$. This means that $ra \equiv 1 \pmod n$ so that a in a unit modulo n and hence $(a, n) = 1$.

□

[1] This is the reason we say that an element that doesn't have an order has infinite order: so that this lemma will hold in this case as well.

Corollary 2. *Let G be a finite cyclic group of order n. Then G has exactly $\varphi(n)$ generators.*

Proof. Write $G = \langle g \rangle$ so that the distinct elements of G are $e, g, g^2, \ldots, g^{n-1}$. Then according to Lemma 2 the number of generators of G is

$$\#\{1 \leq a \leq n-1 \,|\, (a,n) = 1\} = \varphi(n).$$

□

Example 3.

- The only generators of $(\mathbb{Z}/n\mathbb{Z}, +)$ are $a(1 + n\mathbb{Z}) = a + n\mathbb{Z}$ where $(a,n) = 1$, i.e. the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$.
- One can easily show that $2 + 11\mathbb{Z}$ generates $(\mathbb{Z}/11\mathbb{Z})^\times$. Since this group has order 10, the only other generators are $(2 + 11\mathbb{Z})^3 = 8 + 11/\mathbb{Z}$, $(2 + 11/\mathbb{Z})^7 = 7 + 11\mathbb{Z}$ and $(2 + 11/\mathbb{Z})^9 = 6 + 11/\mathbb{Z}$.

♦

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

The structure of prime power modulus unit groups begins simply with the case of prime modulus. Recall that when p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field, i.e. a commutative ring in which every nonzero element is a unit. We will be interested in counting the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ of each allowable order $d|p-1$. Because we can't determine these elements directly, we will instead interpret them as solutions of the polynomial equation $x^d - 1 = 0$, which turns the problem into counting the roots of special polynomials. Since we are working in a field, there is a natural limit to the number of roots a polynomial can have. To deduce this limit we first prove the following lemma.

Lemma 3. *Let F be a field and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \;\; a_i \in F, \;\; a_n \neq 0$$

be a polynomial over F of degree n. *If $r \in F$ and $f(r) = 0$, then*

$$f(x) = (x - r)g(x)$$

where $g(x)$ is a polynomial over F of degree $n - 1$.

Proof. Replace x by $(x - r) + r$ in $f(x)$, apply the binomial theorem to each summand and collect terms with common powers of $x - r$. Since $f(r) = 0$ this yields

$$\begin{aligned}
f(x) &= a_n(x - r + r)^n + a_{n-1}(x - r + r)^{n-1} + \cdots + a_1(x - r + r) + a_0 \\
&= a_n(x - r)^n + b_{n-1}(x - r)^{n-1} + \cdots + b_1(x - r) + f(r) \\
&= (x - r)\left(a_n(x - r)^{n-1} + b_{n-1}(x - r)^{n-2} + \cdots + b_1\right) + 0 \;\; (b_i \in F) \\
&= (x - r)\left(a_n(x - r)^{n-1} + b_{n-1}(x - r)^{n-2} + \cdots + b_1\right) \\
&= (x - r)\underbrace{\left(a_n x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0\right)}_{g(x)} \;\; (c_i \in F),
\end{aligned}$$

where in the final line we have again used the binomial theorem to expand each power of $x - r$. □

Theorem 1 (Lagrange). *Let F be a field and let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \;\; a_i \in F, \;\; a_n \neq 0$$

be a polynomial over F of degree n. Then the equation $f(x) = 0$ has at most n solutions in F.

Proof. We induct on n. When $n = 1$ we have the equation

$$a_1 x + a_0 = 0, \;\; a_0, a_1 \in F, \;\; a_1 \neq 0,$$

which has the unique solution $x = -a_1^{-1}a_0 \in F$, since F is a field.

Now assume the result holds for all polynomials over F of some degree $n \geq 1$. Consider

$$f(x) = a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0, \;\; a_i \in F, \;\; a_{n+1} \neq 0.$$

If $f(x) = 0$ has no solutions in F there is nothing to prove, so assume that $f(r) = 0$ for some $r \in F$. According to the lemma, $f(x) = (x - r)g(x)$ for some polynomial $g(x)$ over F of degree n. Since F is a field, we find that if $f(s) = 0$ for some $s \in F$, $s \neq r$, then $g(s) = 0$. Since $g(x)$ has degree n, by our inductive hypothesis there are at most n possible values for s. Hence $f(x) = 0$ has at most $n + 1$ solutions, and we have established the next case. Induction gives us the result. $\square$

Lemma 4. *Let p be a prime. For each $d|p-1$, the equation $x^d - 1 = 0$ has exactly d solutions in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. By Fermat's little theorem the equation $x^{p-1} - 1 = 0$ has *exactly* $p - 1$ solutions in $\mathbb{Z}/p\mathbb{Z}$, namely the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ ($0 + p\mathbb{Z}$ is certainly not a solution). Write $p - 1 = kd$ so that

$$x^{p-1} - 1 = x^{dk} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1).$$

Then $x^{p-1} - 1 = 0$ if and only if $x^d - 1 = 0$ or $x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 = 0$, since $\mathbb{Z}/p\mathbb{Z}$ is a field. Lagrange's theorem tells us that the number N_1 of solutions to $x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$ satisfies $N_1 \leq dk - d = p - 1 - d$. Likewise, N_2, the number of solutions to $x^d - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$, must satisfy $N_2 \leq p - 1 - (p - 1 - d) = d$. As $x^{p-1} - 1 = 0$ has exactly $p - 1$ solutions we therefore have[2]

$$p - 1 \leq N_1 + N_2 = (p - 1 - d) + d = p - 1$$

and hence we must actually have $N_1 = p - 1 - d$ and $N_2 = d$. The latter equality gives the statement of the lemma. $\square$

Remark 4.

- Note that if $a + p\mathbb{Z}$ solves $x^d - 1 = 0$, then we actually have $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Indeed, in this case $(a + p\mathbb{Z})^{-1} = (a + p\mathbb{Z})^{d-1}$.
- In view of the remark above, we see that for $d|p-1$, the solutions of $x^d - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$ are the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ with order dividing d.

[2] We do not know *a priori* that the two factors of $x^{p-1} - 1$ don't share roots.

- The proof of the preceding lemma allows us to conclude that $x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 = 0$ (where k is the divisor of $p-1$ complementary to d) has exactly $p-1-d$ solutions in $\mathbb{Z}/p\mathbb{Z}$ and that these must be distinct from the solutions to $x^d - 1 = 0$.

▼

Lemma 5. *Let p be a prime, $d|p-1$. The number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d is either 0 or $\varphi(d)$.*[3]

Proof. Suppose there exists an $a + p\mathbb{Z}$ of order d in $(\mathbb{Z}/p\mathbb{Z})^\times$. Let H denote the subgroup it generates. Then H contains d elements, each of which is a solution to $x^d - 1 = 0$. Given that any other element of order d would generate a subgroup with the same property, and that $x^d - 1 = 0$ has only d solutions, it must be that H contains every element of order d. Now $b + p\mathbb{Z} \in H$ has order d if and only if $H = \langle b + p\mathbb{Z}\rangle$ and according to the corollary to Lemma 2, H has exactly $\varphi(d)$ generators. This is what we needed to show. □

We are finally ready to determine the structure of $(\mathbb{Z}/p\mathbb{Z})^\times$.

Theorem 2. *Let p be a prime. For every $d|p-1$, there are exactly $\varphi(d)$ elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d. In particular, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. For each $d|p-1$ let $\gamma(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d. According to Lemma 5, $\gamma(d) \leq \varphi(d)$ for all d. Moreover, since every element has some order dividing $p-1$, and by Gauss' result,

$$p - 1 = \sum_{d|p-1} \gamma(d) = \sum_{d|p-1} \varphi(d).$$

This equality implies that, in fact, $\gamma(d) = \varphi(d)$ for all d, as claimed. In particular, $\gamma(p-1) = \varphi(p-1) \geq 1$ so that elements of order $p - 1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$ exist, i.e. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. □

Example 4.

p	Generators of $(\mathbb{Z}/p\mathbb{Z})^\times$
3	$2 + 3\mathbb{Z}$
5	$2 + 5\mathbb{Z}$, $3 + 5\mathbb{Z}$
7	$3 + 7\mathbb{Z}$, $5 + 7\mathbb{Z}$
11	$2 + 11\mathbb{Z}$, $6 + 11\mathbb{Z}$, $7 + 11\mathbb{Z}$, $8 + 11\mathbb{Z}$
13	$2 + 13\mathbb{Z}$, $6 + 13\mathbb{Z}$, $7 + 13\mathbb{Z}$, $11 + 13\mathbb{Z}$
17	$3 + 17\mathbb{Z}$, $5 + 17\mathbb{Z}$, $6 + 17\mathbb{Z}$, $7 + 17\mathbb{Z}$, $10 + 17\mathbb{Z}$, $11 + 17\mathbb{Z}$, $12 + 17\mathbb{Z}$, $14 + 17\mathbb{Z}$
19	$2 + 19\mathbb{Z}$, $3 + 19\mathbb{Z}$, $10 + 19\mathbb{Z}$, $13 + 19\mathbb{Z}$, $14 + 19\mathbb{Z}$, $15 + 19\mathbb{Z}$

♦

Remark 5.

- We've given an indirect (nonconstructive) proof of the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic because we have to: there's no (known) way to actually *find* a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ without actually knowing p. Once we have one generator it is easy to produce them all via Lemma 2, but it's nailing down the existence of that first generator that's so tricky.

[3] We will soon see that 0 never occurs, but we need this intermediate result in order to establish that stronger fact.

- *Artin's (primitive root) conjecture* states that if $a \neq \pm 1, \square$, then the set of primes p for which $a + p\mathbb{Z}$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$ has positive asymptotic density in the set of all primes. In particular, there are infinitely many such primes. However, there is not a single value of a for which this result has been established. Hooley proved that Artin's conjecture is a consequence of the Generalized Riemann Hypothesis for zeta functions of number fields, another conjectural result. There are partial results, however, along the lines of Artin's conjecture that *have* been proven. It is a consequence of a result of Heath-Brown, for example, that at least one of 2, 3 or 5 is a primitive root for infinitely many primes.
- The argument we've used to establish Theorem 2 is easily generalized to any finite subgroup of the multiplicative group $F^\times$ of an arbitrary field F. That is, if F is a field and G is a finite subgroup of $F^\times$, then G is cyclic. Again, the proof is nonconstructive: it does not provide a generator, but merely establishes that one must exist.

▼

4 The Structure of $(\mathbb{Z}/p^2\mathbb{Z})^\times$

We will deduce the structure of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ from that of $(\mathbb{Z}/p\mathbb{Z})^\times$. The two groups are naturally connected by a *homomorphism*, a group-theoretic tool we will take advantage of to simplify our presentation.

Definition 3. Let G, H be groups. A function $f : G \to H$ is called a *homomorphism* provided $f(ab) = f(a)f(b)$ for all a, $b \in G$. A bijective homomorphism is called an *isomorphism.*
▲

Example 5.

- It is not difficult to show that if f is a homomorphism then $f(e_G) = e_H$ and $f(a^n) = f(a)^n$ for all $n \in \mathbb{Z}$.
- If $m, n \in \mathbb{N}$ and $m|n$, we have seen that the *reduction map*

$$\begin{aligned} r :& (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \\ & a + n\mathbb{Z} \mapsto a + m\mathbb{Z} \end{aligned}$$

  preserves multiplication of congruence classes, hence is a homomorphism of groups.
- If $n_1, n_2, \ldots, n_r \in \mathbb{N}$ are pairwise relatively prime and $N = n_1 n_2 \cdots n_r$, we have seen that

$$\begin{aligned} \rho :& (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times \\ & a + N\mathbb{Z} \mapsto (a + n_1\mathbb{Z}, a + n_2\mathbb{Z}, \ldots, a + n_r\mathbb{Z}) \end{aligned}$$

  is a multiplication preserving bijection, hence is an isomorphism of groups.
- If $G = \langle g \rangle$ is a cyclic group of order n, it is not difficult to show that the map $c : \mathbb{Z}/n\mathbb{Z} \to G$ given by $a + n\mathbb{Z} \mapsto g^a$ is a well-defined (additive to multiplicative) group

homomorphism. Since a can take on any value in $\mathbb{Z}$, c is clearly surjective, so by Lemma 6 and the pigeon-hole principle it is an isomorphism.

Similarly, if $\mathrm{ord}(g) = \infty$, then the map $\widehat{c} : \mathbb{Z} \to G$ defined by $a \mapsto g^a$ is a surjective homomorphism. The proof of Lemma 6 shows that $\widehat{c}$ is also injective and is therefore an isomorphism.

The moral is that every cyclic group is isomorphic to one of $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$, i.e. up to relabelling these are the *only* cyclic groups!

♦

Our primary application of group homomorphisms will be through the following result.

Lemma 6. *Let $f : G \to H$ be a homomorphism of groups. If $a \in G$ has finite order, then $\mathrm{ord}(f(a)) | \mathrm{ord}(a)$.*

Proof. Let $n = \mathrm{ord}(a)$. Then $a^n = e_G$ so that

$$e_H = f(e_G) = f(a^n) = f(a)^n \;\; \Rightarrow \;\; \mathrm{ord}(f(a))|n.$$

□

We are now ready for the main result of this section.

Theorem 3. *Let p be a prime, $n \in \mathbb{N}$. Then $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is cyclic.*

Proof. Let $g + p\mathbb{Z}$ be a generator for $(\mathbb{Z}/p\mathbb{Z})^\times$. We claim that either $g + p^2\mathbb{Z}$ or $g + p + p^2\mathbb{Z}$ generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Let $r : (\mathbb{Z}/p^2\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ denote the reduction map. Since r is a homomorphism and $r(g + p^2\mathbb{Z}) = r(g + p + p^2\mathbb{Z}) = g + p\mathbb{Z}$, according to Lemma 6 the orders of $g + p^2\mathbb{Z}$ and $g + p + p^2\mathbb{Z}$ are both divisible by $p - 1$. Since$|(\mathbb{Z}/p^2\mathbb{Z})^\times| = p(p - 1)$, their orders are therefore either $p - 1$ or $p(p - 1)$.

Assume that $g + p^2\mathbb{Z}$ does *not* generate $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Then according to the preceding paragraph it must have order $p - 1$, and to show that $g + p + p^2\mathbb{Z}$ *is* a generator it suffices to show that $(g + p + p^2\mathbb{Z})^{p-1} \neq 1 + p^2\mathbb{Z}$, i.e. that $(g + p)^{p-1} \not\equiv 1 \,(\mathrm{mod}\ p^2)$. If we apply the binomial theorem we obtain

$$\begin{aligned} (g + p)^{p-1} &= g^{p-1} + (p - 1)g^{p-2}p + kp^2 \\ &\equiv 1 + (p - 1)g^{p-2}p \ (\mathrm{mod}\ p^2), \end{aligned}$$

since $g+p^2\mathbb{Z}$ has order $p-1$. This final quantity is $\equiv 1 \,(\mathrm{mod}\ p^2)$ if and only if $p^2|(p-1)g^{p-2}p$ or $p|(p - 1)g^{p-2}$. But $(p, p - 1) = (p, g) = 1$, so this cannot occur. The proof is complete.

□

Example 6. The first example of a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ that *does not* generate $(\mathbb{Z}/p^2\mathbb{Z})^\times$ occurs when $p = 29$ and $g = 14 + 29\mathbb{Z}$: g has order 28 in *both* groups. According to the proof, this means that $14 + 29 + 29^2\mathbb{Z} = 43 + 29^2\mathbb{Z}$ generates $(\mathbb{Z}/29^2\mathbb{Z})^\times$ instead. ♦

5 The Structure of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for Odd p

The passage from $(\mathbb{Z}/p^2\mathbb{Z})^\times$ to $(\mathbb{Z}/p^n\mathbb{Z})^\times$ will be achieved via the following result.

Lemma 7. *Let p be an odd prime, $n \in \mathbb{N}$. If $(x,p)=1$, then $x^p \equiv 1 \pmod{p^{n+1}}$ if and only if $x \equiv 1 \pmod{p^n}$.*

Proof. Suppose that $x \equiv 1 \pmod{p^n}$. Then $p^n | x-1$. Furthermore, $p|x-1$ implies $x \equiv 1 \pmod{p}$ so that

$$x^{p-1} + x^{p-2} + \cdots + x + 1 \equiv 1 + 1 + \cdots + 1 \equiv p \equiv 0 \pmod{p}$$

so that $p | x^{p-1} + x^{p-2} + \cdots + x + 1$. Therefore

$$p^{n+1} | (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) = x^p - 1 \quad \Rightarrow \quad x^p \equiv 1 \pmod{p^{n+1}}.$$

We prove the converse by induction on n. When $n=1$ suppose we have $x^p \equiv 1 \pmod{p^2}$. By Fermat's theorem we have

$$x^p = x \cdot x^{p-1} = x(1+kp) = 1 + \ell p^2 \quad \Rightarrow \quad x \equiv 1 \pmod{p}$$

as claimed. Now suppose we have proven the result for some $n \in \mathbb{N}$ and assume $x^p \equiv 1 \pmod{p^{n+2}}$. Then $x^p \equiv 1 \pmod{p^{n+1}}$ so that $x \equiv 1 \pmod{p^n}$ by the inductive hypothesis. Write $x = 1 + kp^n$ so that

$$x^p = (1+kp^n)^p = 1 + pkp^n + \sum_{j=2}^{p} \binom{p}{j} k^j p^{nj} = 1 + pkp^n + \ell p^{2n+1} + k^p p^{np},$$

since all the middle binomial coefficients $\binom{p}{j}$ are divisible by p. Since $2n+1 \geq n+2$ and $np \geq n+2$ (as $p \geq 3$), we find that

$$1 \equiv x^p \equiv 1 + kp^{n+1} \pmod{p^{n+2}}$$

so that

$$p^{n+2} | (1 + kp^{n+1}) - 1 = kp^{n+1} \quad \Rightarrow \quad p|k.$$

Since $x = 1 + kp^n$, it follows that $x \equiv 1 \pmod{p^{n+1}}$. Induction completes the proof. □

Remark 6. This result is *false* if $p=2$, and this is what prevents $(\mathbb{Z}/2^n\mathbb{Z})^\times$ from being cyclic for $n \geq 3$. For example, $x^2 \equiv 1 \pmod{8}$ for all odd x, but it is certainly not true that $x \equiv 1 \pmod{4}$ for all odd x. ▼

Theorem 4. *Let p be an odd prime, $n \in \mathbb{N}$. Then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.*

Proof. We induct on $n \geq 2$, the base case having been established in the preceding section. Now suppose we have proven that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for some $n \geq 2$ with generator $g + p^n\mathbb{Z}$. We claim that $g + p^{n+1}\mathbb{Z}$ generates $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. Letting $r : (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ denote the reduction map, we know from Lemma 6 that $p^{n-1}(p-1)$ divides the order of $g + p^{n+1}\mathbb{Z}$. So to show it is a generator of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ it suffices to show that $(g + pn + 1\mathbb{Z})^{p^{n-1}(p-1)} \neq 1 + p^{n+1}\mathbb{Z}$, i.e. that $g^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$.

Assume that this is not the case. Then according to Lemma 7, $g^{p^{n-2}(p-1)} \equiv 1 \pmod{p^n}$. But this contradicts the fact that $g + p^n\mathbb{Z}$ has order $p^{n-1}(p-1)$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Therefore $g + pn + 1\mathbb{Z}$ generates $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ as claimed, and the theorem is established by induction. □

Example 7.

- We have seen that $14+29\mathbb{Z}$ generates $(\mathbb{Z}/29\mathbb{Z})^\times$ and that $43+29^2\mathbb{Z}$ generates $(\mathbb{Z}/29^2\mathbb{Z})^\times$. According to the proof of the preceding theorem, $43+29^n\mathbb{Z}$ generates $43+29^n\mathbb{Z}$ for all $n \geq 3$.
- $2+5\mathbb{Z}$ generates $(\mathbb{Z}/5\mathbb{Z})^\times$. According to the proof of Theorem 3, $2+25\mathbb{Z}$ either has order $5-1=4$ or order $5(5-1)=20$ in $(\mathbb{Z}/25\mathbb{Z})^\times$. Since $2^4 = 16 \not\equiv 1 \pmod{25}$, we must be in the latter situation. Hence $2+5^n\mathbb{Z}$ generates $(\mathbb{Z}/5^n\mathbb{Z})^\times$ for all $n \geq 1$.

♦

6 The Structure of $(\mathbb{Z}/2^n\mathbb{Z})^\times$

When $n = 1, 2$, the structure of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is easy to determine. When $n = 1$ we simply get the trivial group $\{1+2\mathbb{Z}\}$, and when $n = 2$ we get the cyclic group with two elements $\langle 3+4\mathbb{Z}\rangle$. When $n \geq 3$ matters are decidedly more subtle. For example, we have the next elementary result, which immediately shows that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is *never* cyclic for $n \geq 3$.

Lemma 8. *For odd $x \in \mathbb{Z}$ and $n \geq 3$, $x^{2^{n-2}} \equiv 1 \pmod{2^n}$.*

Proof. By induction on $n \geq 3$. When $n = 3$ every odd number satisfies $x \equiv 1, 3, 5, 7 \pmod 8$. Squaring each of these we find that $x^2 \equiv 1 \pmod 8$ in every case, as claimed.

Now assume the result holds for some $n \geq 3$. If x is odd we have

$$x^{2^{n-2}} = 1 + k2^n \quad \Rightarrow \quad x^{2^{n-1}} = (x^{2^{n-2}})^2 = (1+k2^n)^2 = 1 + k2^{n+1} + k^2 2^{2n} \equiv 1 \pmod{2^{n+1}}.$$

The proof is finished by induction.

□

Lemma 8 shows that for $n \geq 3$ every element of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has order at most 2^{n-2}, while $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has order $\varphi(2^n) = 2^{n-1}$, which justifies the claim made just prior to the statement of the lemma. It turns out that the bound 2^{n-2} on the order of elements of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is *sharp*: there are, indeed, elements whose orders achieve this size. To prove this we require the next fact.

Lemma 9. *For $n \in \mathbb{N}$ the exact power of 2 dividing $5^{2^n} - 1$ is 2^{n+2}.*

Proof. We induct on n. When $n = 1$, $5^{2^n} - 1 = 24$ which is exactly divisible by $8 = 2^3$, so the result holds. Now assume the result for some $n \geq 1$ and consider

$$5^{2^{n+1}} - 1 = (5^{2^n})^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1). \tag{2}$$

By hypothesis, 2^{n+2} exactly divides $5^{2^n} - 1$. Since $5^{2^n} + 1$ is even, it's certainly divisible by 2. But it isn't divisible by 4 since

$$5^{2^n} + 1 \equiv 1 + 1 \equiv 2 \not\equiv 0 \pmod 4.$$

So $5^{2^n} + 1$ is exactly divisible by 2. Hence the product (2) is exactly divisible by 2^{n+3}, and the proof is completed by induction. □

Lemma 10. *Let $n \geq 3$. Then $5+2^n\mathbb{Z}$ has order 2^{n-2} in $(\mathbb{Z}/2^n\mathbb{Z})^\times$.*

Proof. According to Lemma 8, the order of $5 + 2^n\mathbb{Z}$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ divides 2^{n-2}. So it suffices to show $(5 + 2^n\mathbb{Z})^{2^{n-3}} \neq 1 + 2^n\mathbb{Z}$, that is $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. If this were not the case, we'd have $2^n | 5^{2^{n-3}} - 1$. But according to Lemma 9 this is impossible, which proves what we need. □

Lemma 10 shows that, for $n \geq 3$, the subgroup $\langle 5 + 2^n\mathbb{Z}\rangle$ of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has order 2^{n-2} and therefore accounts for exactly half of the larger group's elements. To get the other half we need one additional lemma.

Lemma 11. *If $n \geq 2$, then $5^m \not\equiv -1 \pmod{2^n}$ for any $m \in \mathbb{N}$.*

Proof. Suppose otherwise. Then $2^n | 5^m + 1$ for some $m \in \mathbb{N}$. Since $n \geq 2$, this implies $4 | 5^m + 1$ or

$$0 \equiv 5^m + 1 \equiv 1 + 1 \equiv 2 \pmod 4,$$

which is impossible. □

Theorem 5. *Let $n \geq 3$. Then $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is isomorphic to $\langle -1 + 2^n\mathbb{Z}\rangle \times \langle 5 + 2^n\mathbb{Z}\rangle$. The first factor has order 2 and the second has order 2^{n-2}.*

Proof. Define $f : \langle -1 + 2^n\mathbb{Z}\rangle \times \langle 5 + 2^n\mathbb{Z}\rangle \to (\mathbb{Z}/2^n\mathbb{Z})^\times$ by $(\epsilon + 2^n\mathbb{Z}, 5^k + 2^n\mathbb{Z}) \mapsto \epsilon 5^k + 2^n\mathbb{Z}$. It is easy to see that this is a homomorphism. Since both the domain and codomain of f have size 2^{n-1}, to check that f is a bijection it suffices to show that it is injective.

So suppose that $\epsilon 5^k + 2^n\mathbb{Z} = \delta 5^\ell + 2^n\mathbb{Z}$ for some $\epsilon, \delta \in \{\pm 1\}$ and $k \leq \ell$. Then $\epsilon 5^k \equiv \delta 5^\ell \pmod{2^n}$ so that $5^{\ell-k} \equiv \epsilon\delta \pmod{2^n}$. By the preceding lemma, $\epsilon = \delta$ and hence $5^\ell \equiv 5^k \pmod{2^n}$. Thus $(\epsilon + 2^n\mathbb{Z}, 5^k + 2^n\mathbb{Z}) = (\delta + 2^n\mathbb{Z}, 5^\ell + 2^n\mathbb{Z})$, proving that f is an injection. □

Remark 7. According to *Lagrange's theorem* from algebra, the size of a subgroup of a finite group G must divide $|G|$. It follows that no proper subgroup of a finite group G can have size larger than $|G|/2$. Hence no proper subgroup of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ can have size larger than 2^{n-2} (when $n \geq 3$). Since $5 + 2^n\mathbb{Z}$ generates a cyclic subgroup of this maximal size, one often says that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is *almost cyclic*. ▼

7 When is $(\mathbb{Z}/n\mathbb{Z})^\times$ Cyclic?

Let $n \in \mathbb{N}$, $n \geq 2$. Write $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ for distinct primes p_i, and $n_i \in \mathbb{N}$. Then, as noted above, the map ρ of the CRT provides an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ with the group

$$(\mathbb{Z}/p_1^{n_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{n_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{n_r}\mathbb{Z})^\times, \tag{3}$$

and according to what we have proven each factor is either cyclic or almost cyclic (if $p_i = 2$ and $n_i \geq 3$).

We will determine when $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic by analyzing its 2-torsion subgroup. Recall that if G is an abelian group, its 2-torsion subgroup is

$$G(2) = \{g \in G \mid g^2 = e\},$$

which consists of the elements of G that are their own inverses. Of fundamental importance are the following result and its corollary.

Lemma 12. *Let G be a finite cyclic group of even order. Then $|G(2)| = 2$.*

Proof. Let $G = \langle g \rangle$ and $n = |G| = \text{ord}(g)$. Note that $\{e, g^{n/2}\} \subseteq G(2)$. We claim the sets are actually equal. Let $a \in G(2)$. We know $a = g^k$ for some k and $e = a^2 = g^{2k}$ so that $n|2k$ and hence $(n/2)|k$. Write $k = m(n/2)$ and apply the division algorithm to further write $m = 2q + r$ with $r = 0, 1$. Then

$$a = g^k = (g^{n/2})^{2q+r} = g^{nq}(g^{n/2})^r = (g^{n/2})^r \in \{e, g^{n/2}\}$$

which proves that $G(2) \subseteq \{e, g^{n/2}\}$, as claimed.

Since $g^{n/2} \neq e$ this proves that $|G(2)| = |\{e, g^{n/2}\}| = 2$.

$\square$

Corollary 3. *Let G be a finite abelian group of even order. If $|G(2)| \neq 2$, then G is* not *cyclic.*

Proof. This is just the contrapositive of the lemma. $\square$

Notice that $\varphi(n)$ is even if $n \geq 3$ so that we can attempt to apply Corollary 3 to $(\mathbb{Z}/n\mathbb{Z})^\times$. Before we do, we state one more result, whose proof we leave as a straightforward exercise.

Lemma 13. *Let $G_1, G_2, \ldots, G_n$ be abelian groups and $G = G_1 \times G_2 \times \cdots \times G_n$. Then $G(2) = G_1(2) \times G_2(2) \times \cdots \times G_n(2)$.*

Theorem 6. *If n is divisible by two odd primes, of the form $4m$ where m is odd, or is divisible by 8, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is* not *cyclic.*

Proof. If n is divisible by distinct odd primes, say p and q, then we know $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to

$$(\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/q^b\mathbb{Z})^\times \times \cdots .$$

Since both $(\mathbb{Z}/p^a\mathbb{Z})^\times$ and $(\mathbb{Z}/q^b\mathbb{Z})^\times$ are cyclic groups of even order, Lemma 12 implies their 2-torsion subgroups both have size two. By Lemma 13, this means $(\mathbb{Z}/n\mathbb{Z})^\times$ has 2-torsion subgroup of size at least 4. By Corollary 3, we conclude that $(\mathbb{Z}/n\mathbb{Z})^\times$ is not cyclic.

The same argument applies when $n = 4m$ with m odd, since then m is divisible by an odd prime p, $(\mathbb{Z}/4\mathbb{Z})^\times$ has order 2 and $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to

$$(\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/p^a\mathbb{Z})^\times \times \cdots .$$

Finally, if $8|n$, then $n = 2^k m$ with $k \geq 3$ and m odd so that $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \times (\mathbb{Z}/m\mathbb{Z})^\times$$

and again the first two factors provide at least four 2-torsion elements, preventing $(\mathbb{Z}/n\mathbb{Z})^\times$ from being cyclic. $\square$

Corollary 4. *Let $n \in \mathbb{N}$. The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if:*

1. *$n = 2, 4$;*
2. *$n = p^a$ for some odd prime p and $n \in \mathbb{N}$;*
3. *$n = 2p^a$ for some odd prime p and $n \in \mathbb{N}$.*

Proof. The preceding theorem shows that these are the only possibilities for cyclic $(\mathbb{Z}/n\mathbb{Z})^\times$. We need only check that they actually work. Based on what we know so far, the only question is case 3. But in this case the reduction map $r : (\mathbb{Z}/2p^a\mathbb{Z})^\times \to (\mathbb{Z}/p^a\mathbb{Z})^\times$ is actually an isomorphism since it is surjective and both groups have size $\varphi(p^a)$. Consequently, since $(\mathbb{Z}/p^a\mathbb{Z})^\times$ is cyclic so is $(\mathbb{Z}/2p^a\mathbb{Z})^\times$. □

We are finally in a position to answer a question posed in the context of Wilson's theorem. Namely, what is the result when all of the elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ are multiplied together? Equivalently, what is the congruence class of

$$\prod_{\substack{1\leq a\leq n-1\\(a,n)=1}} a$$

modulo n? Wilson's theorem asserts that when $n = p$ is prime, we always get -1 modulo p. To determine what happens in general, we first remind the reader of the main abstract ingredient in the proof of Wilson's theorem. Given a finite abelian group G, by pairing elements with their inverses we proved that

$$\prod_{g\in G} g = \prod_{g\in G(2)} g.$$

It turns out that when $G = (\mathbb{Z}/n\mathbb{Z})^\times$, $n > 2$, there is another natural pairing among the elements of $G(2)$. Specifically, note that if $a + n\mathbb{Z} \in G(2)$, then $-a + n\mathbb{Z} \in G(2)$ since $(-a + n\mathbb{Z})^2 = (-a)^2 + n\mathbb{Z} = a^2 + n\mathbb{Z} = (a + n\mathbb{Z})^2 = 1 + n\mathbb{Z}$. Moreover, $a + n\mathbb{Z} \neq -a + n\mathbb{Z}$, since otherwise $n|2a$, which would imply $n|2$ as $(n, a) = 1$, an impossibility. Finally, note that if we pair $a + n\mathbb{Z}$ and $-a + n\mathbb{Z}$ in the product over $G(2)$, we get

$$(a + n\mathbb{Z})(-a + n\mathbb{Z}) = -a^2 + n\mathbb{Z} = -(a + n\mathbb{Z})^2 = -1 + n\mathbb{Z}.$$

Since there are half as many pairs of elements of $G(2)$ as there are individual elements, we have therefore proven the following result.

Lemma 14. *Let $n > 2$ and $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Then*

$$\prod_{g\in G} g = \prod_{g\in G(2)} g = (-1)^{|G(2)|/2} + n\mathbb{Z}.$$

Equivalently,

$$\prod_{\substack{1\leq a\leq n-1\\(a,n)=1}} a \equiv (-1)^{|G(2)|/2} \pmod{n}.$$

Note that we could have proven this result some time ago, as it uses none of the structural facts about $(\mathbb{Z}/n\mathbb{Z})^\times$ that we have deduced so far. But at that point we would have been unable to determine $|G(2)|$ and actually evaluate the product. However, we can do so now.

We need to count $G(2)$ when $G = (\mathbb{Z}/n\mathbb{Z})^\times$. According to the decomposition (3) of $(\mathbb{Z}/n\mathbb{Z})^\times$ and the structure theorems for $(\mathbb{Z}/p^m\mathbb{Z})^\times$, we find that $(\mathbb{Z}/n\mathbb{Z})^\times$ is always the product of (at least one) cyclic groups of even order. Each has 2-torsion of size two by Lemma 12, which means that $|G(2)| = 2^N$,[4] where N is the number of cyclic factors, by

[4]It is true in general for an arbitrary abelian group G that, if $G(2)$ is finite, then $|G(2)|$ is a power of 2. This is a consequence of a result in group theory known as Cauchy's Theorem.

Lemma 13. If $N > 1$ then G is not cyclic by Corollary 3, whereas if $N = 1$, G is definitely cyclic since it is isomorphic to a "product" with a single cyclic factor. Applying this in the preceding Lemma we obtain our final result.

Theorem 7. *For $n > 2$*

$$\prod_{\substack{1 \le a \le n-1 \\ (a,n)=1}} a \equiv \begin{cases} -1 \pmod{n} & \text{if } (\mathbb{Z}/n\mathbb{Z})^\times \text{ is cyclic,} \\ 1 \pmod{n} & \text{otherwise.} \end{cases}$$

Example 8. If $n = 20$ we have

$$\begin{aligned} \prod_{\substack{1 \le a \le 19 \\ (a,20)=1}} a &= 1 \cdot 3 \cdot 7 \cdot 9 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \\ &\equiv 1 \cdot 3 \cdot 7 \cdot 9 \cdot (-9) \cdot (-7) \cdot (-3) \cdot (-1) \pmod{20} \\ &\equiv (-1)^4 \cdot 1^2 \cdot 3^2 \cdot 7^2 \cdot 9^2 \pmod{20} \\ &\equiv 9 \cdot 9 \pmod{20} \\ &\equiv 1 \pmod{20} \end{aligned}$$

as expected, since

$$(\mathbb{Z}/20\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

is not a cyclic group. ♦