Cyclic groups and elementary number theory II

1 Subgroups of $\mathbb{Z}/n\mathbb{Z}$

From now on, we shall generally drop the brackets $[\cdot]_n$ enclosing elements of $\mathbb{Z}/n\mathbb{Z}$, unless we want to compare an integer a with its equivalence class $[a]_n$ in $\mathbb{Z}/n\mathbb{Z}$, or we want to view a as an element of $\mathbb{Z}/n\mathbb{Z}$ for possibly different n, in which case we will write $[a]_n$ for emphasis. We start by giving a criterion for when the equation $ax = b$ has a solution in $\mathbb{Z}/n\mathbb{Z}$, or equivalently when the congruence equation $ax \equiv b \bmod n$ has a solution in integers. First, there is the following observation whose proof is left as homework:

Lemma 1.1. *Let $n \in \mathbb{N}$and let $a, a' \in \mathbb{Z}$ with $a \equiv a' \bmod n$.*

(i) *Suppose that $d|n$. Then $d|a \iff d|a' \iff [a]_n \in \langle [d]_n \rangle$.*

(ii) *We have $\gcd(a, n) = \gcd(a', n)$. Hence the function $[a]_n \mapsto \gcd(a, n)$ is a well-defined function from $\mathbb{Z}/n\mathbb{Z}$ to $\{1, \ldots, n\}$. In particular, a and n are relatively prime $\iff$ a' and n are relatively prime, and hence the statement that $[a]_n$ and n are relatively prime is well-defined.* □

Proposition 1.2. *Given $a, c \in \mathbb{Z}/n\mathbb{Z}$, there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ such that $ax = c \iff c \in \langle d \rangle$, where $d = \gcd(a, n)$.*

Proof. The equation $ax = c$ has a solution in $\mathbb{Z}/n\mathbb{Z} \iff$ the equation $ax \equiv c \bmod n$ has a solution $x \in \mathbb{Z}$ (where we somewhat carelessly use the same letters a, c to denote elements of $\mathbb{Z}/n\mathbb{Z}$ and integer representatives of the corresponding equivalence classes). But $ax \equiv c \bmod n$ has a solution $x \in \mathbb{Z} \iff$ there exists an integer y such that $ax + ny = \iff$ there exist integers x, y such that $ax + ny = c$. We have seen that this last condition is equivalent to: $d|c$. By using the previous lemma, we see that this condition is equivalent to: $c \in \langle d \rangle$. □

Corollary 1.3. *Given $a, \in \mathbb{Z}/n\mathbb{Z}$, there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ such that $ax = 1$, i.e. a is an invertible element of $(\mathbb{Z}/n\mathbb{Z}, \cdot) \iff \gcd(a, n) = 1$, i.e. a and n are relatively prime.* □

Definition 1.4. Let $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$. Equivalently, $(\mathbb{Z}/n\mathbb{Z})^*$ is the set of all $a \in \mathbb{Z}/n\mathbb{Z}$ such that there exists an $x \in \mathbb{Z}/n\mathbb{Z}$ with $ax = 1$, i.e. a is an invertible element in the binary structure $(\mathbb{Z}/n\mathbb{Z}, \cdot)$.

Proposition 1.5. *$((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ is an abelian group.*

Proof. The product of two invertible elements is invertible, so that multiplication is a well-defined operation on $(\mathbb{Z}/n\mathbb{Z})^*$. It is associative and commutative, since these properties hold for multiplication on $\mathbb{Z}/n\mathbb{Z}$. Clearly 1 is an identity for $\cdot$, and by definition, every $a \in (\mathbb{Z}/n\mathbb{Z})^*$ has a multiplicative inverse $a^{-1} \in \mathbb{Z}/n\mathbb{Z}$, which is invertible and hence in $(\mathbb{Z}/n\mathbb{Z})^*$ as well. Thus $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ is an abelian group. □

Whenever we write $(\mathbb{Z}/n\mathbb{Z})^*$, the group operation is understood to be multiplication. Note that $(\mathbb{Z}/n\mathbb{Z})^*$ is **not** a subgroup of $\mathbb{Z}/n\mathbb{Z}$ (where the operation is necessarily $+$). The definition of the group $(\mathbb{Z}/n\mathbb{Z})^*$ follows a familiar pattern: begin with an associate binary structure $(X, *)$ with an identity e, for example, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, $(\mathbb{M}_n(\mathbb{R}), \cdot)$, or $(X^X, \circ)$. None of the above binary structures is a group, because there are always elements which are not invertible. But the subset of invertible elements does give a group. In the examples, we obtain the groups $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(GL_n(\mathbb{R}), \cdot)$, and $(S_X, \circ)$.

Example 1.6. (i) $(\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\}$. Necessarily $(\mathbb{Z}/6\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ and 5 has order 2, i.e. $5^2 = 1$ in $\mathbb{Z}/6\mathbb{Z}$.

(ii) $(\mathbb{Z}/5\mathbb{Z})^* = \{1, 2, 3, 4\}$ and hence $\#((\mathbb{Z}/5\mathbb{Z})^*) = 4$. It is easy to see that $(\mathbb{Z}/5\mathbb{Z})^*$ is cyclic. In fact, $2^2 = 4$, $2^3 = 3$, and $2^4 = 1$, so that $(\mathbb{Z}/5\mathbb{Z})^* = \langle 2 \rangle$.

(iii) On the other hand, $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ and hence $\#((\mathbb{Z}/8\mathbb{Z}))^* = 4$ as well. But $(\mathbb{Z}/8\mathbb{Z})^*$ is not cyclic, as $3^2 = 5^2 = 7^2 = 1$. Hence every element of $(\mathbb{Z}/8\mathbb{Z})^*$ has order 1 or 2. In particular, there is no element of $(\mathbb{Z}/8\mathbb{Z})^*$ of order 4, so that $(\mathbb{Z}/8\mathbb{Z})^*$ is not cyclic.

Definition 1.7. Define the *Euler ϕ-function* $\phi \colon \mathbb{N} \to \mathbb{N}$ via:

$$\phi(n) = \#((\mathbb{Z}/n\mathbb{Z})^*).$$

Thus $\phi(n)$ is the number of $a \in \mathbb{Z}$, $0 \leq a \leq n - 1$, such that $\gcd(a, n) = 1$.

For example, if p is a prime, $\phi(p) = p - 1$. If $n = p^k$ is a prime power, so that p is a prime and $k \in \mathbb{N}$, then an integer a is **not** relatively prime to $p^k \iff$ it has a factor in common with $p \iff p|k \iff k$ is a multiple

of p. Now there are $p^k/p = p^{k-1}$ multiples of p between 0 and $p^k - 1$. Thus the number of integers a, $0 \leq a \leq p^k - 1$ which are relatively prime to p^k is

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

In general, for $n > 1$, $1 \leq \phi(n) \leq n-1$, and it is easy to see that $\phi(n) = n-1 \iff n$ is prime. A table of the first few values of ϕ is given below:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

We will describe more properties of the function $\phi(n)$ shortly.

We return to the problem of describing all subgroups of $\mathbb{Z}/n\mathbb{Z}$. The following theorem gives a complete description.

Theorem 1.8. *Let $n \in \mathbb{N}$.*

(i) *Every subgroup of $\mathbb{Z}/n\mathbb{Z}$ is cyclic.*

(ii) *If $a \in \mathbb{Z}/n\mathbb{Z}$ and $d = \gcd(a, n)$, then $\langle a \rangle = \langle d \rangle$.*

(iii) *If $a \in \mathbb{Z}/n\mathbb{Z}$ and $d = \gcd(a, n)$, the order of a is n/d.*

(iv) *The order of every subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides n.*

(v) *For each divisor d of n, there is exactly one subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d, namely $\langle n/d \rangle$.*

Proof. (i) We have already seen this.

(ii) Since $d|a$, $a \in \langle d \rangle$, and hence $\langle a \rangle \subseteq \langle d \rangle$. Conversely, by Proposition 1.2, there exists an x such that $ax = d$, hence $x \cdot a = d$, and therefore $d \in \langle a \rangle$. Thus $\langle d \rangle \subseteq \langle a \rangle$. It follows that $\langle a \rangle = \langle d \rangle$.

(iii) By (ii), $\langle a \rangle = \langle d \rangle$ and hence the order of a, which we know to be $\#(\langle a \rangle)$ is equal to $\#(\langle d \rangle)$, in other words the order of d. Clearly $(n/d) \cdot d = n = 0$ in $\mathbb{Z}/n\mathbb{Z}$, and hence the order of d is at most n/d. On the other hand, if $0 < k < n/d$, then $0 < k \cdot d < n$, so $k \cdot d \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. Hence n/d is the smallest positive integer k such that $k \cdot d = 0$. So the order of d and hence of a is n/d.

(iv) If $H \leq \mathbb{Z}/n\mathbb{Z}$, then $H = \langle a \rangle$ for some a, and the order of H is then the order of a, namely n/d for some divisor d of n. But clearly n/d divides n.

(v) By (i) and (ii), every subgroup H of $\mathbb{Z}/n\mathbb{Z}$ is of the form $\langle e \rangle$ for some divisor e of n. By (iii), the order of H is n/e. Thus the unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d is $\langle e \rangle$ with $n/e = d$, i.e. $e = n/d$. □

Remark 1.9. We can carry over the results above to **every** cyclic group $G = \langle g \rangle$ of order n. Thus, for example, $\langle g^a \rangle = \langle g^d \rangle$ where $d = \gcd(a, n)$, every subgroup is of this form, and, for every divisor d of n, the order of $\langle g^d \rangle$ is n/d, or equivalently the order of $\langle g^{n/d} \rangle$ is d.

Corollary 1.10. *$\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$, i.e. a is a generator of $\mathbb{Z}/n\mathbb{Z}$, $\iff$ $\gcd(a, n) = 1$ $\iff$ $a \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Proof. $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$ $\iff$ the order of a is n $\iff$ for $d = \gcd(a, n)$, $n/d = n$ $\iff$ $d = 1$. □

Given $a \in (\mathbb{Z}/n\mathbb{Z})^*$, be careful not to confuse the order of a as an element of $\mathbb{Z}/n\mathbb{Z}$ with the order of a as an element of $(\mathbb{Z}/n\mathbb{Z})^*$. As an element of $\mathbb{Z}/n\mathbb{Z}$, a **always** has order n by the above corollary. But as an element of element of $(\mathbb{Z}/n\mathbb{Z})^*$, the order of a could be 1 (if $a = 1$) and in general it is at most $\phi(n)$.

Corollary 1.11. *If G is a cyclic group of order n, the number of generators of G is $\phi(n)$.*

Proof. It is enough to check this for $G = \mathbb{Z}/n\mathbb{Z}$, where it follows from the previous corollary and the definition of $\phi(n)$. □

More precisely, if $G = \langle g \rangle$ is a cyclic group of order n, then the generators of G are all of the form g^a, for $0 \leq a \leq n-1$ and $\gcd(a, n) = 1$. For example, the generators of μ_n are exactly the n^{th} roots of unity of the form $e^{2\pi ai/n}$ with $\gcd(a, n) = 1$. These are called the *primitive n^{th} roots of unity*.

Corollary 1.12. *For each $d|n$, there are exactly $\phi(d)$ elements of $\mathbb{Z}/n\mathbb{Z}$ of order d.*

Proof. Given $a \in \mathbb{Z}/n\mathbb{Z}$, the order of a is d $\iff$ $\#(\langle a \rangle) = d$ $\iff$ $\langle a \rangle = \langle n/d \rangle$ $\iff$ $a \in \langle n/d \rangle$ and a is a generator of $\langle n/d \rangle$. Since $\langle n/d \rangle$ is a cyclic group of order d, it has exactly $\phi(d)$ generators, by the preceding corollary. Hence there are exactly $\phi(d)$ elements a of $\mathbb{Z}/n\mathbb{Z}$ of order d. □

This leads to the following identity for the Euler ϕ-function:

Corollary 1.13. *For each natural number n,*

$$\sum_{d|n} \phi(d) = n.$$

Proof. Every element of $\mathbb{Z}/n\mathbb{Z}$ has order d dividing n, by (iii) of the theorem. By the previous corollary, there are exactly $\phi(d)$ elements of $\mathbb{Z}/n\mathbb{Z}$ of order d. Hence the sum $\sum_{d|n} \phi(d)$ counts the number of elements of $\mathbb{Z}/n\mathbb{Z}$, namely n. □

For example, the divisors of 20 are 1, 2, 4, 5, 10, and 20. We have

$$\begin{aligned}\phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(10) + \phi(20) \\ = 1 + 1 + 2 + 4 + 4 + 8 = 20.\end{aligned}$$

Remark 1.14. By (iv) of the theorem, the order of every subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides the order of $\mathbb{Z}/n\mathbb{Z}$. In fact, as we shall see, this holds true for every finite group and is called *Lagrange's theorem*: if G is a finite group and $H \leq G$, then $\#(H)|\#(G)$. However, the fact that $\mathbb{Z}/n\mathbb{Z}$ has exactly one subgroup of order d for each divisor d of $n = \#(\mathbb{Z}/n\mathbb{Z})$ is a **very special** property of $\mathbb{Z}/n\mathbb{Z}$. For a general finite group G and a divisor d of $\#(G)$, there may be no subgroups of G of order d, or several (as in the case of D_3 or Q).

2 The Chinese remainder theorem

Theorem 2.1 (Chinese remainder theorem)**.** *Let $n, m \in \mathbb{Z}$ with $\gcd(n, m) = 1$. Then*

$$(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/nm\mathbb{Z}.$$

Equivalently, $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ is cyclic.

An equivalent formulation is the following:

Theorem 2.2 (Chinese remainder theorem version 2)**.** *Let $n, m \in \mathbb{Z}$ with $\gcd(n, m) = 1$. Then, for all $r, s \in \mathbb{Z}$, there exists an $x \in \mathbb{Z}$ such that*

$$\begin{aligned}x &\equiv r \bmod n; \\ x &\equiv s \bmod m.\end{aligned}$$

Moreover, if x and x' satisfy the above congruences, then $x \equiv x' \bmod nm$.

In this form, the result was known (both in China and later in India and the West) circa 300–500 AD.

To prove the Chinese remainder theorem, we begin with the following general lemma about groups (whose statement was suggested in a homework problem):

Lemma 2.3. *Let G_1 and G_2 be groups, let $g_1 \in G_1$ and $g_2 \in G_2$. Suppose that g_1 has finite order d_1 and that g_2 has finite order d_2. Then the order of (g_1, g_2) in the group $G_1 \times G_2$ is the least common multiple of d_1 and d_2.*

Proof. Let N be a positive integer. Then $(g_1, g_2)^N = (g_1^N, g_2^N)$. Hence $(g_1, g_2)^N = (1, 1) \iff g_1^N = 1$ and $g_2^N = 1 \iff$ the order d_1 of g_1 divides N and that the order d_2 of g_2 divides N, i.e. N is a common multiple of d_1 and d_2. In particular, the order of (g_1, g_2) is the smallest positive integer which is a multiple both of d_1 and of d_2, i.e. the least common multiple of d_1 and d_2. □

Proof of the Chinese remainder theorem. Applying the lemma to the element $(1, 1) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, we see that the order of $(1, 1)$ is the least common multiple of n and m. A general formula (homework) shows that the least common multiple of n and m is equal to $nm/\gcd(n, m)$, and thus is nm if $\gcd(n, m) = 1$. (In fact, it is easy to verify this directly in case $\gcd(n, m) = 1$.) Thus, under the assumption that $\gcd(n, m) = 1$, $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ has an element of order nm, which is the order of $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$. Hence $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ is cyclic, and in fact it is generated by $(1, 1)$. □

Remark 2.4. If $\gcd(n, m) > 1$, then arguments similar to the proof above show that the order of every element of $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ divides the least common multiple of n and m, which is $nm/\gcd(n, m)$ and hence is strictly smaller than nm. Thus no element of $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ has order nm, so that $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ is not cyclic. For example, we have seen that every element in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has order 1 or 2.

To see the link between the version of the Chinese remainder theorem that we proved and version 2, still under the assumption that $\gcd(n, m) = 1$, recall that since the element $(1, 1) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ has order nm, there is an explicit isomorphism $f\colon \mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ given by $f(a) = (a, a)$. More precisely, to keep track of which groups we are working in, we could write this as

$$f([a]_{nm}) = ([a]_n, [a]_m).$$

(Recall by a homework that the function $g_1\colon \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $g_1([a]_{nm}) = [a]_n$ is well-defined since $n|nm$, and similarly for the function $g_2\colon \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $g_2([a]_{nm}) = [a]_m$.) Since f is an isomorphism, it is also a bijection. Hence, for every $[r]_n \in \mathbb{Z}/n\mathbb{Z}$ and $[s]_m \in \mathbb{Z}/m\mathbb{Z}$, there is a unique $[x]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$ such that $f([x]_{nm}) = ([r]_n, [s]_m)$. This is essentially version 2 of the Chinese remainder theorem.

Remark 2.5. (1) There is also a proof of version 2 of the Chinese remainder theorem which gives an explicit recipe for x.

(2) In case n and m are not necessarily relatively prime, it is easy to give necessary and sufficient conditions for the congruence

$$x \equiv r \bmod n;$$
$$x \equiv s \bmod m$$

to have a solution.

We turn now to a multiplicative form of the Chinese remainder theorem.

Proposition 2.6. *Suppose that* $\gcd(n, m) = 1$*, and let* g *denote the restriction of the isomorphism* $f\colon \mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ *given above to* $(\mathbb{Z}/nm\mathbb{Z})^*$*.*

(i) *The image of* g *is* $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$*.*

(ii) *If we denote by* f^* *the resulting bijection* $(\mathbb{Z}/nm\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$*, then* f^* *is an isomorphism. Thus in particular*

$$(\mathbb{Z}/nm\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*.$$

Proof. (i) This follows from the fact that, given $a \in \mathbb{Z}$, $\gcd(a, nm) = 1 \iff \gcd(a, n) = \gcd(a, m) = 1$, which is a homework problem. Thus, if $[a]_{nm} \in (\mathbb{Z}/nm\mathbb{Z})^*$, $g([a]_{nm}) = f([a]_{nm}) = ([a]_n, [a]_m) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$. Thus the image of g is contained in $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$, and g is injective since f is injective. To see that the image of g is exactly $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$, let $([r]_n, [s]_m) \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$. Then, since f is surjective, there is an $[a]_{nm} \in \mathbb{Z}/nm\mathbb{Z}$ such that $f([a]_{nm}) = ([a]_n, [a]_m) = ([r]_n, [s]_m)$. Then $\gcd(a, n) = \gcd(r, n) = 1$ and similarly $\gcd(a, m) = \gcd(s, m) = 1$. It follows from the homework problem that $a \in (\mathbb{Z}/nm\mathbb{Z})^*$. Thus the image of g is $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$, and g defines a bijection

$$f^*\colon (\mathbb{Z}/nm\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*.$$

To see that f^* is an isomorphism, we compute:

$$f^*([a]_{nm}[b]_{nm}) = f^*([ab]_{nm}) = ([ab]_n, [ab]_m);$$
$$f^*([a]_{nm})f^*([b]_{nm}) = ([a]_n, [a]_m)([b]_n, [b]_m) = ([ab]_n, [ab]_m).$$

Thus $f^*([a]_{nm}[b]_{nm}) = f^*([a]_{nm})f^*([b]_{nm})$ and so f^* is an isomorphism. $\square$

We obtain as a corollary:

Corollary 2.7. *If* $\gcd(n, m) = 1$*, then* $\phi(nm) = \phi(n)\phi(m)$. □

This leads to the following explicit formula for $\phi(n)$:

Corollary 2.8. *Suppose that* $n = p_1^{a_1} \cdots p_r^{a_r}$ *is the prime factorization of* n*, so that* $p_1, \ldots, p_r$ *are* ***distinct*** *primes and* $a_i \geq 1$*. Then*

$$\phi(n) = p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1). \quad \square$$

(Sometimes this is written as $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, where the product is taken over all of the primes dividing n.)

Later we shall discuss (but not fully prove):

Theorem 2.9 (Existence of a primitive root)**.** *If* p *is a prime, then* $(\mathbb{Z}/p\mathbb{Z})^*$ *is cyclic.* □

Here, a generator for the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ is called a *primitive root*.

Using this, one can show:

Theorem 2.10. *The group* $(\mathbb{Z}/n\mathbb{Z})^*$ *is cyclic* $\iff$ n *satisfies one of the following:*

1. $n = p^k$ *is a prime power, where* p *is an odd prime.*
2. $n = 2p^k$*, where* p *is an odd prime.*
3. $n = 2$ *or* 4. □

We see that $(\mathbb{Z}/n\mathbb{Z})^*$ is rarely a cyclic group. However, Proposition 2.6 and induction imply that, if the prime factorization of n is $p_1^{a_1} \cdots p_r^{a_r}$ as above, then

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{a_r}\mathbb{Z})^*.$$

This is still a **product** of cyclic groups. Here special attention has to be given to possible factors of the form $(\mathbb{Z}/2^a\mathbb{Z})^*$; one can show that $(\mathbb{Z}/2^a\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^{a-2}$, which is not cyclic if $a > 2$ but is still a product of cyclic groups. More generally:

Theorem 2.11 (Fundamental theorem of finite abelian groups)**.** *Every finite abelian group is isomorphic to a product of cyclic groups.* □

There is also a uniqueness statement which is part of the theorem, which is a little complicated to state, but which roughly says that the failure of uniqueness in the expression of an abelian group as a product of cyclic groups is due to the Chinese remainder theorem, which implies that, for $\gcd(n, m) = 1$, we can replace a pair of factors $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ by $\mathbb{Z}/nm\mathbb{Z}$.