Cyclic groups and elementary number theory

1 Long division with remainder

The story of cyclic groups is very much connected with elementary number theory (factorization, prime numbers, congruences). We prove some basic facts from “first principles,” using a few results about addition, multiplication, and order in \( \mathbb{N} \). One of the most basic facts is the following:

**Theorem 1.1** (Long division with remainder). Let \( n \in \mathbb{N} \). Then for all \( a \in \mathbb{Z} \), there exist unique integers \( q \) and \( r \) with \( 0 \leq r \leq n - 1 \) such that

\[
a = nq + r.
\]

Here \( q \) stands for quotient and \( r \) for remainder.

**Proof.** Existence: Define the subset \( X \) of \( \mathbb{Z} \) by

\[
X = \{a - nq : q \in \mathbb{Z}, a - nq \geq 0\}.
\]

First we claim that \( X \neq \emptyset \). If \( a \geq 0 \), take \( q = 0 \), so that \( a - nq = a \geq 0 \) is an element of \( X \). If \( a < 0 \), take \( q = a \). Then \( a - nq = a - na = a(1 - n) \geq 0 \) since \( a < 0 \) and \( 1 - n \leq 0 \). Again, \( X \) has the element \( a - na \) and so is non-empty.

Next we claim that \( X \) has a smallest element. If \( 0 \in X \), then \( 0 \) is clearly the smallest element of \( X \). If \( 0 \notin X \), then \( X \subseteq \mathbb{N} \) and hence, since \( X \neq \emptyset \), \( X \) has a smallest element by the well-ordering principle. In either case, let \( r \) be the smallest element of \( X \). Then by definition, \( r = a - nq \) and \( r \geq 0 \). Note that \( a = nq + r \). To prove the existence part of the theorem, it suffices to show that \( r \leq n-1 \). We argue by contradiction: if \( r \geq n \), then \( 0 \leq r - n < r \). But

\[
r - n = a - nq - n = a - n(q + 1).
\]

Since \( r - n \geq 0, r - n \in X \) by the definition of \( X \). But \( r - n < r \) contradicting the choice of \( r \) as the smallest element of \( X \). Hence \( r \leq n-1 \) and \( a = nq + r \).

Uniqueness: suppose that \( a = nq_1 + r_1 = nq_2 + r_2 \), where \( q_i, r_i \in \mathbb{Z} \) and \( 0 \leq r_i \leq n - 1 \) for \( i = 1, 2 \). We must show that \( q_1 = q_2 \) and that \( r_1 = r_2 \).
Now either \( r_1 \leq r_2 \) or \( r_2 \leq r_1 \). By symmetry, we can assume that \( r_1 \leq r_2 \). Then
\[
  r_2 - r_1 = nq_1 - nq_2 = n(q_1 - q_2).
\]
Moreover,
\[
  0 \leq r_2 - r_1 \leq r_2 \leq n - 1 < n.
\]
If \( r_2 - r_1 \neq 0 \), then \( r_2 - r_1 \) is a positive integer divisible by \( n \), and hence
\( r_2 - r_1 \geq n \). This contradicts \( r_2 - r_1 \leq n - 1 \). Thus \( r_2 - r_1 = 0 \), i.e. \( r_2 = r_1 \).

Then \( n(q_1 - q_2) = 0 \). Since \( n \in \mathbb{N} \), \( n \neq 0 \). Thus \( q_1 - q_2 = 0 \), so that
\( q_1 = q_2 \). \( \square \)

**Corollary 1.2.** Let \( n \in \mathbb{N} \). Every equivalence class \([a]_n \in \mathbb{Z}/n\mathbb{Z}\) has a unique representative \( r \) with \( 0 \leq r \leq n - 1 \). Hence \( \#(\mathbb{Z}/n\mathbb{Z}) = n \) and, as a set,
\[
\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.
\]

**Proof.** Given \([a]_n \in \mathbb{Z}/n\mathbb{Z}\), write \( a = nq + r \), with \( 0 \leq r \leq n - 1 \). Then \( a \equiv r \mod n \), so that \([a]_n = [r]_n\). To see that \( r \) is the unique representative of \([a]_n\), such that \( 0 \leq r \leq n - 1 \), suppose that \([r_1]_n = [r_2]_n\) with \( 0 \leq r_1, r_2 \leq n - 1 \). Then \( a = nq_1 + r_1 = nq_2 + r_2 \) for some integers \( q_1, q_2 \), and so \( r_1 = r_2 \) by the uniqueness statement of Theorem 1.1. \( \square \)

**Corollary 1.3.** Let \( G \) be a group and let \( g \in G \) be an element of (finite) order \( n \).

(i) Every element of \( \langle g \rangle \) can be uniquely written as \( g^r \), \( 0 \leq r \leq n - 1 \).
Hence \( \#(\langle g \rangle) = n \).

(ii) For all \( N \in \mathbb{Z} \), \( g^N = 1 \iff n | N \).

(iii) \( \langle g \rangle \cong \mathbb{Z}/n\mathbb{Z} \). In fact, there is a unique isomorphism \( f: \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle \) such that \( f([1]_n) = g \).

**Proof.** (i) Every element of \( \langle g \rangle \) is of the form \( g^a \) for some \( a \in \mathbb{Z} \). Write \( a = nq + r \) with \( 0 \leq r \leq n - 1 \). Then
\[
  g^a = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r = 1^q g^r = g^r.
\]
Hence every element of \( \langle g \rangle \) is equal to \( g^r \) for some \( r \) with \( 0 \leq r \leq n - 1 \).
To see the uniqueness, suppose that \( g^{r_1} = g^{r_2} \) with \( 0 \leq r_1, r_2 \leq n - 1 \). By symmetry we can assume that \( r_1 \leq r_2 \). Then
\[
  1 = g^{r_1} g^{-r_1} = g^{r_2} g^{-r_1} = g^{r_2-r_1}.
\]
As before, $0 \leq r_2 - r_1 \leq r_2 \leq n - 1 < n$. Since $n$ is the order of $g$, and hence the smallest positive power $k$ of $g$ such that $g^k = 1$, we must have $r_2 - r_1 = 0$, i.e. $r_1 = r_2$. This proves the uniqueness part of (i).

(ii) Let $n \in \mathbb{Z}$ be arbitrary. Then $N = nq + r$, where $0 \leq r \leq n - 1$, and $n|N \iff r = 0$. Then, as in the proof of (i),

$$g^N = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r = 1^q g^r = g^r.$$  

Moreover, by (i) or directly from the definition of order, $g^r = 1 \iff r = 0$. Thus $g^N = 1 \iff n|N$.

(iii) Define $f : \mathbb{Z}/n\mathbb{Z} \to \langle g \rangle$ via: $f([a]_n) = g^a$. Then $f$ is well-defined since $a' \in [a]_n \iff a' \equiv a \bmod n \iff a' = a + nk$, and in this case

$$g^a = g^{a+nk} = g^a g^{nk} = g^a.$$  

$f$ is surjective, since every element of $\langle g \rangle$ is of the form $g^a$ for some $a \in \mathbb{Z}$. $f$ is injective by (i) and the previous corollary: if $f([a_1]_n) = f([a_2]_n)$, write $a_1 = nq_1 + r_1$ and $a_2 = nq_2 + r_2$, where $0 \leq r_1, r_2 \leq n - 1$. Then, since $f$ is well-defined, $f([a_1]_n) = f([a_2]_n) = g^{r_1}$, and similarly $f([a_2]_n) = g^{r_2}$. Thus, if $f([a_1]_n) = f([a_2]_n)$, then $g^{r_1} = g^{r_2}$ and hence $r_1 = r_2$. It follows that $[a_1]_n = [r_1]_n = [r_2]_n = [a_2]_n$, and thus $f$ is injective, hence a bijection. (Another proof uses the pigeonhole principle and the fact that $f$ is a surjection from $\mathbb{Z}/n\mathbb{Z}$ to $\langle g \rangle$, both of which have $n$ elements.) To show that $f$ is an isomorphism, we must check that, for all $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$, $f([a]_n + [b]_n) = f([a]_n)f([b]_n)$. But, by definition of addition in $\mathbb{Z}/n\mathbb{Z}$,

$$f([a]_n + [b]_n) = f([a + b]_n) = g^{a+b} = g^a g^b = g^{[a]_n} g^{[b]_n} = f([a]_n) f([b]_n).$$  

Thus $f$ is an isomorphism. Finally, $f$ is uniquely specified by the requirement that $f([1]_n) = g$, for then $f([a]_n) = f(a \cdot [1]_n) = (f([1]_n)^a) = g^a$.  

**Corollary 1.4.** Every cyclic group is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$.  

*Proof.* Every cyclic group $G$ is of the form $\langle g \rangle$ for some $g \in G$. The proof then follows from the previous handout in case $g$ has infinite order and from (iii) above in case $g$ has finite order.  

From now on, we shall focus on the groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. The previous corollary tells us that any algebraic result (e.g. concerning the nature of subgroups or orders of elements) which is proved for $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ will have a natural analogue for an arbitrary cyclic group.
Proposition 1.5. Every subgroup of \( \mathbb{Z} \) is cyclic.

Proof. Let \( H \leq \mathbb{Z} \). If \( H = \{0\} \), then \( H = \langle 0 \rangle \) and hence \( H \) is cyclic. Thus we may assume that there exists an \( a \in H \), \( a \neq 0 \). Then \( -a \in H \) as well, and either \( a > 0 \) or \( -a > 0 \). In particular, the set \( H \cap \mathbb{N} \) is nonempty. Let \( d \) be the smallest element of \( H \cap \mathbb{N} \), which exists by the well-ordering principle. To prove the proposition, we shall show that \( H = \langle d \rangle \). We shall do so by showing that \( \langle d \rangle \subseteq H \) and that \( H \subseteq \langle d \rangle \).

Since \( d \in H \cap \mathbb{N} \), \( d \in H \), and hence \( \langle d \rangle \subseteq H \). So we must show that \( H \subseteq \langle d \rangle \). Let \( a \in H \); we must show that \( a \in \langle d \rangle \). Applying long division with remainder to \( a \), we can write \( a = dq + r \) with \( 0 \leq r \leq d - 1 \). As we have seen, \( \langle d \rangle \subseteq H \), and hence \( dq \in H \). Since \( H \) is a subgroup, \( -dq \in H \), and, since \( a \in H \), \( a - dq = r \in H \). If \( r > 0 \), then \( r \in \mathbb{N} \), \( r \in H \), and \( r \leq d - 1 < d \). This contradicts the choice of \( d \) as the smallest positive element of \( H \). Hence \( r = 0 \), i.e. \( a - dq = 0 \) and thus \( a = dq \in \langle d \rangle \). It follows that \( H \subseteq \langle d \rangle \) and hence that \( H = \langle d \rangle \). Thus \( H \) is cyclic. \( \square \)

A very similar argument shows:

Proposition 1.6. Let \( n \in \mathbb{N} \). Then every subgroup \( H \) of \( \mathbb{Z}/n\mathbb{Z} \) is cyclic.

Proof. In this case, we let

\[ X = \{ r \in \mathbb{Z} : 0 \leq r \leq n - 1 \text{ and } [r]_n \in H \} . \]

Then \( X \) is a finite set, and as before there is a smallest element \( d \in X \) and hence \([d]_n \in H \). We claim that \( H = \langle [d]_n \rangle \). Clearly \( \langle [d]_n \rangle \subseteq H \). Conversely, if \([k]_n \in H \), we can write \( k = dq + s \), where \( 0 \leq s \leq d - 1 \). Then \([k]_n = [dq + s]_n = q \cdot [d]_n + [s]_n \). It follows that \([s]_n = q \cdot [d]_n - [k]_n \in H \). Since \( 0 \leq s \leq d - 1 < d \leq n - 1 \), we must have, by the definition of \( d \), \( s = 0 \). Thus \([k]_n \in \langle [d]_n \rangle \). It follows that \( H \subseteq \langle [d]_n \rangle \) and hence that \( H = \langle [d]_n \rangle \). \( \square \)

Corollary 1.7. Every subgroup of a cyclic group is cyclic.

Here, we use the result that every cyclic group is isomorphic to \( \mathbb{Z} \) or \( \mathbb{Z}/n\mathbb{Z} \) as well as the facts, previously discussed, that if \( f : G_1 \rightarrow G_2 \) is an isomorphism, then a subset \( H \) of \( G_1 \) is a subgroup of \( G_1 \iff f(H) \) is a subgroup of \( G_2 \), and that, if \( H = \langle g \rangle \) is a cyclic subgroup of \( G_1 \), then \( f(\langle g \rangle) \) is a cyclic subgroup of \( G_2 \), in fact it is \( \langle f(g) \rangle \).

Every subgroup of \( \mathbb{Z} \) can be uniquely described as \( \langle 0 \rangle \) or as \( \langle d \rangle \), where \( d > 0 \). We shall give a similar precise description of the subgroups of \( \mathbb{Z}/n\mathbb{Z} \) later.
2 Factorization

Recall that, if \(a, b \in \mathbb{Z}\), then \(a \mid b \iff\) there exists a \(k \in \mathbb{Z}\) such that \(b = ak\) \(\iff\) \(b\) is a multiple of \(a\) \(\iff\) \(b \in \langle a \rangle \iff \langle b \rangle \subseteq \langle a \rangle\). Note also that divisibility is transitive (if \(a \mid b\) and \(b \mid c\), then \(a \mid c\)), and that, if \(a \mid b\) and \(a \mid c\), then, for all \(r, s \in \mathbb{Z}\), \(a \mid (rb + sc)\).

**Definition 2.1.** Let \(a, b \in \mathbb{Z}\), not both 0. A greatest common divisor of \(a\) and \(b\) (written \(\gcd(a, b)\)) is an element \(d \in \mathbb{N}\) such that \(d \mid a\), \(d \mid b\), and, for all \(e \in \mathbb{Z}\), if \(e \mid a\) and \(e \mid b\), then \(e \mid d\).

**Remark 2.2.** (i) If a gcd of \(a\) and \(b\) exists, then it is unique. For, if \(d_1\) and \(d_2\) are two such, then \(d_1 \mid d_2\), say \(d_2 = kd_1\), and \(d_2 \mid d_1\), say \(d_1 = \ell d_2\). It follows that \(d_1 = k\ell d_1\), hence that \(k\ell = 1\). Thus \(k = 1\) and \(d_1 = d_2\).

(ii) If \(d\) is a gcd of \(a\) and \(b\), it follows from the definition that \(d\) is the largest natural number dividing both \(a\) and \(b\). However, \(d\) has the stronger property of the definition.

(iii) From grade school, a familiar recipe for computing \(\gcd(a, b) = d\) is to factor \(a\) and \(b\) into products of prime powers. Then the prime factors of \(d\) are the primes which divide both \(a\) and \(b\), and the power to which a prime \(p\) occurs in the factorization of \(d\) is given as follows: if \(p^{n_1}\) is the largest power of \(p\) dividing \(a\), and \(p^{n_2}\) is the largest power of \(p\) dividing \(b\), then the largest power of \(p\) dividing \(d\) is \(p^{\min(n_1, n_2)}\). However, there are much more computationally efficient ways to find \(\gcd(a, b)\) which do not involve factoring \(a\) and \(b\) into primes (a computationally very hard problem).

The following result tells us that gcds always exist:

**Theorem 2.3.** Let \(a, b \in \mathbb{Z}\), not both 0. Then a gcd of \(a\) and \(b\) exists, and it is necessarily unique by (i) of the preceding remark. Moreover, there exist \(x_0, y_0 \in \mathbb{Z}\) such that \(d = \gcd(a, b) = ax_0 + by_0\).

**Proof.** Consider the set

\[ H = \{ax + by : x, y \in \mathbb{Z}\}. \]

We claim that \(H\) is a subgroup of \(\mathbb{Z}\) containing \(a\) and \(b\); in fact, it is the subgroup \(\langle a, b \rangle\) generated by \(a\) and \(b\) as previously defined (since \(ax + by = x \cdot a + y \cdot b\)). We will show this directly: first, \(H\) is closed under + since, given two elements \(ax_1 + by_1, ax_2 + by_2\) of \(H\),

\[(ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2) \in H.\]

5
Clearly, \(0 = a \cdot 0 + b \cdot 0 \in H\), and if \(ax + by \in H\), then \(- (ax + by) = a(-x) + b(-y) \in H\). Thus \(H\) is a subgroup. Moreover, note that \(a = a \cdot 1 + b \cdot 0 \in H\) and \(b = a \cdot 0 + b \cdot 1 \in H\).

Since every subgroup of \(\mathbb{Z}\) is cyclic, there exists a \(d \in \mathbb{Z}\) such that \(H = \langle d \rangle\). Also, \(H \neq \{0\}\) since \(a, b \in H\) and by assumption at least one of them is nonzero. Thus we may assume that \(d > 0\), i.e. that \(d \in \mathbb{N}\). To complete the proof of the theorem, it suffices to prove that \(d\) is a gcd of \(a\) and \(b\), since necessarily \(d = ax_0 + by_0\) for some \(x_0, y_0 \in \mathbb{Z}\). Since \(a \in H = \langle d \rangle\), \(d \mid a\). Similarly, \(d \mid b\). Hence, \(d\) is a common divisor of \(a\) and \(b\). Finally, if \(e \mid a\) and \(e \mid b\), then \(e \mid ax_0 + by_0 = d\). Thus \(d = \gcd(a, b)\). □

For future reference, we note the following corollary of the proof:

**Corollary 2.4.** Let \(a, b \in \mathbb{Z}\), not both 0, and let \(d = \gcd(a, b)\). Then, for all \(c \in \mathbb{Z}\), there exist \(x, y \in \mathbb{Z}\) such that \(ax + by = c \iff d \mid c\).

**Proof.** The set of all integers \(c\) of the form \(ax + by\) is by definition the subgroup \(H\) of the proof of the theorem, and we have seen that \(H = \langle d \rangle\) is the set of all multiples of \(d\). □

**Definition 2.5.** Let \(a, b \in \mathbb{Z}\), not both 0. Then \(a\) and \(b\) are relatively prime if \(\gcd(a, b) = 1\). In other words, if an integer \(e\) divides both \(a\) and \(b\), then \(e = \pm 1\).

**Lemma 2.6.** Given integers \(a\) and \(b\), not both 0, \(a\) and \(b\) are relatively prime \(\iff\) there exist \(x, y \in \mathbb{Z}\) such that \(ax + by = 1\).

**Proof.** By the previous corollary, there exist \(x, y \in \mathbb{Z}\) such that \(ax + by = 1\) \(\iff\) \(d = \gcd(a, b)\) divides 1 \(\iff\) \(d = 1\). □

We then have the following basic result:

**Proposition 2.7.** Let \(a, b \in \mathbb{Z}\) be relatively prime. If \(a \mid bc\), then \(a \mid c\).

**Proof.** By the previous corollary, there exist \(x, y \in \mathbb{Z}\) such that \(ax + by = 1\). Then \(c = c(ax) + c(by) = a(cx) + (bc)y\). By assumption, \(a \mid bc\) and clearly \(a \mid a\). Thus \(a \mid (a(cx) + (bc)y) = c\). □

The corollary is most often applied to primes:

**Definition 2.8.** Let \(p \in \mathbb{N}\). Then \(p\) is a prime or prime number if \(p > 1\), and for all \(n \in \mathbb{N}\), if \(n \mid p\) then either \(n = 1\) or \(n = p\).

We then have the following property of prime numbers:
Lemma 2.9. Let $p$ be a prime and let $n \in \mathbb{Z}$. Then either $p$ and $n$ are relatively prime or $p|n$.

Proof. Let $d = \gcd(p, n)$. Then $d \in \mathbb{N}$ and $d|p$. Thus, either $d = 1$ or $d = p$. If $d = 1$, then $p$ and $n$ are relatively prime by definition. If $d = p$, then $p|n$. \qed

Corollary 2.10. Let $p$ be a prime and let $a, b \in \mathbb{Z}$. If $p|ab$, then either $p|a$ or $p|b$. In other words, if a prime divides a product, then it divides one of the factors.

Proof. Suppose that $p$ does not divide $a$. Then, by Lemma 2.9, $p$ and $a$ are relatively prime. Then, by Proposition 2.7, $p$ divides $b$. \qed

Corollary 2.11. Let $p$ be a prime and let $a_1, \ldots, a_k \in \mathbb{Z}$. If $p|a_1 \cdots a_k$, then there exists an $i$ such that $p|a_i$.

Proof. This follows from the above and a straightforward induction argument. \qed

The previous corollary is one of the key steps in the following:

Theorem 2.12 (Fundamental theorem of arithmetic). Let $n \in \mathbb{N}$, $n > 1$. Then $n$ can be uniquely factored into primes. More precisely, there exist primes $p_1, \ldots, p_r$ such that $n = p_1 \cdots p_r$, and this product is unique in the sense that, if

$$p_1 \cdots p_r = q_1 \cdots q_s,$$

where the $p_i$ and $q_j$ are primes, then $r = s$, and, after possibly reordering, $q_i = p_i$ for every $i$.

Proof. Existence: this is done via complete induction on $n$, starting with $n = 2$. Clearly $2$ is a product of primes in the sense of the theorem ($r = 1$, $p_1 = 2$). Given $n \in \mathbb{N}$, $n > 2$, suppose that we have shown that, for every $k \leq n$, $k$ is a product of primes. For the inductive step, we must show that $n + 1$ is a product of primes. If $n + 1$ is itself a prime, we are done as in the case $n = 2$: take $r = 1$ and $p_1 = n + 1$. Otherwise, $n + 1 = k_1 k_2$, with $1 < k_i \leq n$. Then by the inductive hypothesis, both $k_1$ and $k_2$ are products of primes. Hence, so is $n + 1$.

Uniqueness: Suppose that $p_1 \cdots p_r = q_1 \cdots q_s$, where the $p_i$ and $q_j$ are primes. We argue by induction on $r$. If $r = 1$, then $p_1 = q_1 \cdots q_s$, where the $q_j$ are primes. Hence $s = 1$ as well, for otherwise $p_1$ would have a nontrivial factorization, and then $p_1 = q_1$. For the inductive step, suppose
that $p_1 \cdots p_{r+1} = q_1 \cdots q_s$, then the left hand side is a multiple of $p_{r+1}$, so that $p_{r+1}$ divides $q_1 \cdots q_s$. Hence, there exists an $i$ such that $p_{r+1} \mid q_i$. Since $q_i$ is a prime, $p_{r+1} = q_i$. After relabeling the $q_i$, we can assume that $i = s$. Then

$$p_1 \cdots p_{r+1} = q_1 \cdots q_{s-1} p_{r+1},$$

so that after canceling the last factor we have $p_1 \cdots p_r = q_1 \cdots q_{s-1}$. By the inductive hypothesis, $s - 1 = r$, i.e. $s = r + 1$, and after relabeling $q_i = p_i$, $1 \leq i \leq r$. This completes the inductive step and hence the proof of the theorem.

\[ \square \]

3 \hspace{1em} 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 $ax \equiv b \pmod{n}$ has a solution in integers. First, there is the following observation whose proof is left as homework:

**Lemma 3.1.** (i) Let $n \in \mathbb{N}$. If $a, a' \in \mathbb{Z}$ and $a \equiv a' \pmod{n}$, then $\gcd(a, n) = \gcd(a', n)$. 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 the statement that $[a]_n$ and $n$ are relatively prime is well-defined.

(ii) If $d \mid n$ and $c, c'$ are integers such that $c \equiv c' \pmod{n}$, then $d \mid c \iff d \mid c'$ $\iff [c]_n \in \langle [d]_n \rangle$.

**Proposition 3.2.** 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 $ax \equiv c \pmod{n}$ 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 $ax \equiv c \pmod{n}$ has a solution $x \in \mathbb{Z}$ $\iff$ there exists an integer $k$ such that $ax = c + nk$, $\iff$ there exist integers $x, k$ such that $ax + by = c$, $\iff$ there exist integers $x, y$ such that $ax + by = c$. (Here, given $k$, we set $y = -k$ and conversely.) We have seen that this last condition is equivalent to: $d \mid c$. By using the previous lemma, we see that this condition is equivalent to: $c \in \langle d \rangle$. \[ \square \]
Corollary 3.3. 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 \((\mathbb{Z}/n\mathbb{Z}, \cdot)\) ⇐⇒ \( \gcd(a, n) = 1 \), i.e. \( a \) and \( n \) are relatively prime. \( \square \)

Definition 3.4. 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 3.5. \((\mathbb{Z}/n\mathbb{Z})^*, \cdot\) is an abelian group.

Proof. As we have seen in the homework, 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. \( \square \)

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 \((X, \ast)\) with an identity \(e\), for example, \((\mathbb{Q}, \cdot)\), \((\mathbb{R}, \cdot)\), \((\mathbb{C}, \cdot)\), \((\mathbb{M}_n(\mathbb{R}), \cdot)\), or \((\mathbb{X}^\times, \circ)\). 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 \((\mathbb{Q}^\times, \cdot)\), \((\mathbb{R}^\times, \cdot)\), \((\mathbb{C}^\times, \cdot)\), \((GL_n(\mathbb{R}), \cdot)\), and \((S_X, \circ)\).

Example 3.6. (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 3.7. Define the Euler \(\phi\)-function \(\phi: \mathbb{N} \rightarrow \mathbb{N}\) 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 \(\phi\) is given below:

<table>
<thead>
<tr>
<th>(n)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\phi(n))</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>10</td>
<td>4</td>
</tr>
</tbody>
</table>

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 3.8.** 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 3.2, 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 \(n\).
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. $e = n/d$.

\textbf{Corollary 3.9.} $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$, i.e. $a$ is a generator of $\mathbb{Z}/n\mathbb{Z}$, $\iff$ $\gcd(a, n) = 1$ $\iff$ $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

\textit{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 $\mathbb{Z}/n\mathbb{Z}$, $a$ \textbf{always} has order $n$ by the above corollary. But as an element of $(\mathbb{Z}/n\mathbb{Z})^*$, the order of $a$ could be 1 (if $a = 1$) and in general it is at most $\phi(n)$.

\textbf{Corollary 3.10.} If $G$ is a cyclic group of order $n$, the number of generators of $G$ is $\phi(n)$.

\textit{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 $\phi(n)$.

\textbf{Corollary 3.11.} For each $d | n$, there are exactly $\phi(d)$ elements of $\mathbb{Z}/n\mathbb{Z}$ of order $d$.

\textit{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 $\phi$-function:

\textbf{Corollary 3.12.} For each natural number $n$,

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

\textit{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 $n$. 

\[\Box\]
For example, the divisors of 20 are 1, 2, 4, 5, 10, and 20. We have
\[
\phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(10) + \phi(20) = 1 + 1 + 2 + 4 + 4 + 8 = 20.
\]

**Remark 3.13.** 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 \(Q\)).

### 4 The Chinese remainder theorem

**Theorem 4.1** (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 4.2** (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
\[
x \equiv r \mod n;
\]
\[
x \equiv s \mod m.
\]
Moreover, if \(x\) and \(x'\) satisfy the above congruences, then \(x \equiv x' \mod nm\).

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 4.3.** 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 $(g_1, g_2)^N = (1, 1) \iff g_1 = 1$ and $g_2 = 1 \iff$ 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 $d_2$. \qed

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 $(1, 1)$. \qed

Remark 4.4. 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 $f: \mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ 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 $g_1: \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $g_1([a]_{nm}) = [a]_n$ is well-defined since $n|nm$, and similarly for the function $g_2: \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ 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 4.5. (1) There is also a proof of version 2 of the Chinese remainder theorem which gives an explicit recipe for $x$. 

13
(2) In case \( n \) and \( m \) are not necessarily relatively prime, it is easy to give necessary and sufficient conditions for the congruence

\[
x \equiv r \mod n;
\]
\[
x \equiv s \mod m
\]
to have a solution.

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

**Proposition 4.6.** Suppose that \( \gcd(n, m) = 1 \), and let \( g \) denote the restriction of the isomorphism \( f: \mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \) 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

\[
f^*: (\mathbb{Z}/nm\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*.
\]

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

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

**Corollary 4.8.** 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

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

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

Using this, one can show:

**Theorem 4.10.** 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 4.6 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 4.11 (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 $\mathbb{Z}/nm\mathbb{Z}$. 

15