

§12 Group of Units Modulo n

Let n be a natural number and consider \mathbb{Z}_n . We defined two operations on this set, namely addition and multiplication (Lemma 6.3). With respect to addition, \mathbb{Z}_n forms a group. What about multiplication? With respect to multiplication, \mathbb{Z}_n is not a group unless $n = 1$. This can be easily seen from the fact that $\bar{0}$ has no multiplicative inverse in \mathbb{Z}_n (Lemma 6.4(12); note that $\bar{0} \neq \bar{1}$ when $n \neq 1$). However, as in Example 9.4(h), a suitable subset of \mathbb{Z}_n is a group under multiplication.

12.1 Lemma: Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $\bar{a} = \bar{b}$ in \mathbb{Z}_n , then $(a, n) = (b, n)$.

Proof: If $\bar{a} = \bar{b}$ in \mathbb{Z}_n , then $a \equiv b \pmod{n}$, so $n|b - a$, so $nk = b - a$ for some $k \in \mathbb{Z}$. We put $d_1 = (a, n)$ and $d_2 = (b, n)$. We have $d_1|n$ and $d_1|a$, thus $d_1|nk + a$, thus $d_1|b$. From $d_1|n$ and $d_1|b$, we get $d_1|(b, n)$, so $d_1|d_2$. Likewise we obtain $d_2|d_1$. So $|d_1| = |d_2|$ by Lemma 5.2(12) and, since d_1, d_2 are positive, we have $d_1 = d_2$. \square

The preceding lemma tells that the mapping $\mathbb{Z}_n \rightarrow \mathbb{N}$ is well defined. The

$$\bar{a} \rightarrow (a, n)$$

claim of the lemma is not self-evident and requires proof. Compare it to the apparently similar but *wrong* assertion that $\bar{a} = \bar{b}$ implies $(a, n^2) = (b, n^2)$. By Lemma 12.1, the following definition is meaningful.

12.2 Definition: Let $n \in \mathbb{N}$ and $\bar{a} \in \mathbb{Z}_n$, where $a \in \mathbb{Z}$. If $(a, n) = 1$, then \bar{a} is called a *unit* in \mathbb{Z}_n . The set of all units in \mathbb{Z}_n will be denoted by \mathbb{Z}_n^\times .

The reader will observe that U in Example 9.4(h) is exactly \mathbb{Z}_8^\times . We see $\mathbb{Z}_7^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. More generally, $\mathbb{Z}_p^\times = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$ for any prime number p . So $|\mathbb{Z}_p^\times| = p - 1$. When $n > 1$, \mathbb{Z}_n^\times consists of the residue classes of the numbers among $1, 2, 3, \dots, n - 1, n$ that are relatively prime to n .

By the definition of Euler's phi function, we conclude $|\mathbb{Z}_n^\times| = \varphi(n)$. So $\varphi(12) = 4$ and in fact $\mathbb{Z}_{12}^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$. Also, $\varphi(15) = 8$ and $\mathbb{Z}_{15}^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$.

12.3 Lemma: *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $(a, n) = (b, n) = 1$, then $(ab, n) = 1$.*

Proof: This follows from the fundamental theorem of arithmetic (Theorem 5.17), but we give another proof. We put $d = (ab, n)$ and assume, by way of contradiction, that $d > 1$. Then $p|d$ for some prime number p (Theorem 5.13). So

$$\begin{array}{lll}
 p|ab & \text{and} & p|n \\
 p|a \text{ or } p|b & \text{and} & p|n \quad (\text{Euclid's} \\
 \text{lemma}) & & \\
 p|a \text{ and } p|n & \text{or} & p|b \text{ and } p|n \\
 p|(a, n) & \text{or} & p|(b, n),
 \end{array}$$

contrary to the hypothesis $(a, n) = 1 = (b, n)$. So $(ab, n) = d = 1$. □

12.4 Theorem: *For any $n \in \mathbb{N}$, \mathbb{Z}_n^\times is a group under multiplication.*

Proof: (cf. Example 9.4(h).) We check the group axioms.

(i) Is \mathbb{Z}_n^\times closed under multiplication? Let $\bar{a}, \bar{b} \in \mathbb{Z}_n^\times$, so that a, b are integers with $(a, n) = 1 = (b, n)$. We ask whether $\overline{ab} \in \mathbb{Z}_n^\times$, i.e., which is equivalent to asking whether $(ab, n) = 1$. By Lemma 12.3, ab is indeed relatively prime to n and so \mathbb{Z}_n^\times is closed under multiplication.

(ii) Multiplication in \mathbb{Z}_n^\times is associative since it is in fact associative in \mathbb{Z}_n (Lemma 6.4(7)).

(iii) $\bar{1} \in \mathbb{Z}_n^\times$ as $(1, n) = 1$ and $\bar{a} \bar{1} = \overline{a1} = \bar{a}$ for all $\bar{a} \in \mathbb{Z}_n^\times$. Hence $\bar{1}$ is an identity element of \mathbb{Z}_n^\times .

(iv) Each element in \mathbb{Z}_n^\times has an inverse in \mathbb{Z}_n^\times . This follows from Lemma 6.4(9). Let us recall its proof. If $\bar{a} \in \mathbb{Z}_n^\times$, with $a \in \mathbb{Z}$ and $(a, n) = 1$, then there are integers x, y such that $ax + ny = 1$. From this we

get $\bar{a} \bar{x} = \bar{1}$, so \bar{x} is an inverse of \bar{a} . Yes, but this is not enough. We must further show that $\bar{x} \in \mathbb{Z}_n^\times$, or equivalently that $(x, n) = 1$. This follows from the equation $ax + ny = 1$, since $d = (x, n)$ implies $d|x$, $d|n$, so $d|ax + ny$, so $d|1$, so $d = 1$.

Hence \mathbb{Z}_n^\times is a group under multiplication. □

\mathbb{Z}_n^\times is a finite group of order $\varphi(n)$. Using Lemma 11.7, we obtain $\bar{a}^{\varphi(n)} = \bar{1}$ for all $\bar{a} \in \mathbb{Z}_n^\times$. Writing this in congruence notation, we get an important theorem of number theory due to L. Euler.

12.5 Theorem (Euler's theorem): *Let $n \in \mathbb{N}$. For all integers that are relatively prime to n , we have*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \quad \square$$

The case when n is a prime number had already been observed by Pierre de Fermat (1601-1665). The result is known as Fermat's theorem or as Fermat's little theorem.

12.6 Theorem (Fermat's theorem): *If p is a positive prime number then*

$$a^{p-1} \equiv 1 \pmod{p}$$

for all integers a that are relatively prime to p (i.e., for all integers a such that $p \nmid a$). □

Multiplying both sides of the congruence $a^{p-1} \equiv 1 \pmod{p}$ by a , we get $a^p \equiv a \pmod{p}$. The latter congruence is true also without the hypothesis $(a, p) = 1$, since both a^p and a are congruent to $0 \pmod{p}$ when $(a, p) \neq 1$. This is also known as Fermat's (little) theorem.

12.7 Theorem (Fermat's theorem): *If p is a prime number, then*

$$a^p \equiv a \pmod{p}$$

for all integers a .

□

Exercises

1. Prove that \mathbb{Z}_n^\times is an abelian group under multiplication.
2. Construct the multiplication tables of \mathbb{Z}_n^\times for $n = 2, 4, 6, 10, 12$.
3. What are the orders of $\bar{2}$ in \mathbb{Z}_3^\times , $\bar{2}$ in \mathbb{Z}_5^\times , $\bar{3}$ in \mathbb{Z}_7^\times , $\bar{2}$ in \mathbb{Z}_{11}^\times , $\bar{2}$ in \mathbb{Z}_{13}^\times , $\bar{3}$ in \mathbb{Z}_{17}^\times , $\bar{2}$ in \mathbb{Z}_{19}^\times , $\bar{5}$ in \mathbb{Z}_{23}^\times ? What do you guess?
4. Show that \mathbb{Z}_3^\times , $\mathbb{Z}_{3^2}^\times$, $\mathbb{Z}_{3^3}^\times$, $\mathbb{Z}_{3^4}^\times$ are cyclic.
5. Assume p is prime, \mathbb{Z}_p^\times is cyclic, and $m \in \mathbb{N}$, $m \geq 2$. Prove that $\mathbb{Z}_{p^m}^\times$ is cyclic by establishing that, if \bar{a} in \mathbb{Z}_p^\times is a generator of \mathbb{Z}_p^\times , then either \bar{a} or $\overline{a+p}$ in $\mathbb{Z}_{p^m}^\times$ is a generator of $\mathbb{Z}_{p^m}^\times$.
6. Find the order of $\bar{5}$ in \mathbb{Z}_8^\times , in \mathbb{Z}_{16}^\times , in \mathbb{Z}_{32}^\times , in \mathbb{Z}_{64}^\times .
7. Prove or disprove: if $a \in \mathbb{Z}$ and $a \equiv 5 \pmod{8}$, then the order of \bar{a} in $\mathbb{Z}_{2^m}^\times$ is 2^{m-2} for all $m \geq 3$.
8. Show that \mathbb{Z}_{pq}^\times is not cyclic if p and q are positive odd prime numbers. (Hint: What is $\varphi(pq)$ and what is $a^{(p-1)(q-1)/2}$ congruent to \pmod{pq} if a is an integer relatively prime to pq ?)