4. The Groups $(\mathbb{Z}_m, +)$ and $(\mathbb{Z}_p^*, \cdot)$

For $m \in \mathbb{Z}$, let $m\mathbb{Z} = \{mx : x \in Z\}$, then, by Hw2.Q6.(d), $m\mathbb{Z} \leqslant (\mathbb{Z}, +)$. In the sequel we investigate the sets $\mathbb{Z}/m\mathbb{Z}$ for positive integers m.

The set $\mathbb{Z}/m\mathbb{Z}$ contains m pairwise disjoint "copies" of $m\mathbb{Z}$ and every set in $\mathbb{Z}/m\mathbb{Z}$ is of the form $x+m\mathbb{Z}$, for some $x \in \mathbb{Z}$. If $x+m\mathbb{Z} = y+m\mathbb{Z}$, then, by Lemma 3.6 (d), $x-y \in m\mathbb{Z}$, so, $x-y = km$ for some $k \in \mathbb{Z}$. Hence,

$$x + m\mathbb{Z} = y + m\mathbb{Z} \iff x = km + y \iff x \equiv y \pmod{m}.$$

Instead of $x \equiv y \pmod{m}$ we write just $x \equiv_m y$.
It is easy to see that $\mathbb{Z}/m\mathbb{Z} = \{0+m\mathbb{Z}, 1+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}\}$, and hence,

$$\mathbb{Z}_m := \{0, 1, \dots, m-1\}$$

is a transversal for $m\mathbb{Z}$ in $\mathbb{Z}$. In particular, for every $x+m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ there is exactly one $a \in \mathbb{Z}_m$ such that $x+m\mathbb{Z} = a+m\mathbb{Z}$, namely the unique $a \in \mathbb{Z}_m$ such that $x \equiv_m a$.
Let us define an operation "$+$" on $\mathbb{Z}/m\mathbb{Z}$ as follows:

$$\begin{array}{rccc} + : & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ & (x+m\mathbb{Z}\,,\, y+m\mathbb{Z}) & \mapsto & (x+y)+m\mathbb{Z} \end{array}$$

It remains to show that "$+$" is an operation on $\mathbb{Z}/m\mathbb{Z}$, or in other words, that "$+$" is well defined:

Fact 4.1. If $x+m\mathbb{Z} = x'+m\mathbb{Z}$ and $y+m\mathbb{Z} = y'+m\mathbb{Z}$, then $(x+m\mathbb{Z})+(y+m\mathbb{Z}) = (x'+m\mathbb{Z})+(y'+m\mathbb{Z})$.

Proof. If $x+m\mathbb{Z} = x'+m\mathbb{Z}$ and $y+m\mathbb{Z} = y'+m\mathbb{Z}$, then, by Lemma 3.6 (d), $x'-x \in m\mathbb{Z}$ and $y'-y \in m\mathbb{Z}$. Now, $(x+m\mathbb{Z})+(y+m\mathbb{Z}) = (x+y)+m\mathbb{Z}$, and therefore, by Lemma 3.6 (c), $(x+y)+m\mathbb{Z} = (x+y)+\big((x'-x)+(y'-y)+m\mathbb{Z}\big) = (x'+y')+m\mathbb{Z} = (x'+m\mathbb{Z})+(y'+m\mathbb{Z})$. Thus, $(x+m\mathbb{Z})+(y+m\mathbb{Z}) = (x'+m\mathbb{Z})+(y'+m\mathbb{Z})$, which shows that the operation "$+$" on $\mathbb{Z}/m\mathbb{Z}$ is well defined. ⊣

The following fact is straightforward:

Fact 4.2. $\big(\mathbb{Z}/m\mathbb{Z}, +\big)$ is an abelian group.

Since every element of $\mathbb{Z}/m\mathbb{Z}$ is of the form $a+m\mathbb{Z}$ for some $a \in \mathbb{Z}_m$, let us identify the set $\mathbb{Z}/m\mathbb{Z}$ with the set $\mathbb{Z}_m$. This identification induces an operation "$+$" on $\mathbb{Z}_m$:

$$\begin{array}{rccc} + : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & (a\,,\, b) & \mapsto & a+b =: c \end{array}$$

where $c \in \mathbb{Z}_m$ is such that $a+b \equiv_m c$. So, by Fact 4.2, $(\mathbb{Z}_m, +)$ is an abelian group.

Since every integer $x \in \mathbb{Z}$ belongs to exactly one coset of $\mathbb{Z}/m\mathbb{Z}$, each $x \in \mathbb{Z}$ corresponds to exactly one element of $\mathbb{Z}_m$, say to $(x)_m \in \mathbb{Z}_m$. Now, by Fact 4.1, if $(x)_m = (x')_m$ and $(y)_m = (y')_m$, which is the same as $x \equiv_m x'$ and $y \equiv_m y'$, then $(x+y)_m = (x'+y')_m$. Moreover, we get

$$(x)_m = (x')_m \text{ and } (y)_m = (y')_m \implies (x \cdot y)_m = (x' \cdot y')_m\,,$$

or in other words,

$$x \equiv_m x' \text{ and } y \equiv_m y' \implies x \cdot y \equiv_m x' \cdot y'\,.$$

PROPOSITION 4.3. The group $(\mathbb{Z}_m, +)$ is a cyclic group of order m.

Proof. By definition, $|\mathbb{Z}_m| = m$. Now, since the order of 1 is m, we have $\langle 1 \rangle = \mathbb{Z}_m$ which implies that $\mathbb{Z}_m$ is cyclic. ⊣

Multiplication is also an operation on $\mathbb{Z}_m$ and for all $a, b, c \in \mathbb{Z}_m$ we have $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, which is called the **distributive law**.

In the following, let $m \geq 2$ and let $\mathbb{Z}_m^* := \mathbb{Z}_m \setminus \{0\} = \{1, \ldots, m-1\}$. Is $(\mathbb{Z}_m^*, \cdot)$ a group?

LEMMA 4.4. $(\mathbb{Z}_m^*, \cdot)$ is a group if and only if multiplication is an operation on $\mathbb{Z}_m^*$.

Proof. $(\Leftarrow)$ If multiplication is an operation on $\mathbb{Z}_m^*$, then it is obviously associative and even commutative. Let us assume that multiplication is an operation on $\mathbb{Z}_m^*$. Suppose $a \cdot b \equiv_m a \cdot c$ (for some $a, b, c \in \mathbb{Z}_m^*$), then $(a \cdot b) - (a \cdot c) \equiv_m 0$, and thus, by the distributive law, $a \cdot (b - c) \equiv_m 0$. Now, $0 \notin \mathbb{Z}_m^*$, and since we assumed that multiplication is an operation on $\mathbb{Z}_m^*$, we must have $(b - c) \equiv_m 0$, which implies $b \equiv_m c$, and since $b, c \in \mathbb{Z}_m$, we get $b = c$. Because multiplication is commutative, this shows that $(\mathbb{Z}_m^*, \cdot)$ is cancellative. So, by Proposition 1.5 (since $\mathbb{Z}_m^*$ is finite), $(\mathbb{Z}_m^*, \cdot)$ is a group.
$(\Rightarrow)$ This is obvious. ⊣

THEOREM 4.5. $(\mathbb{Z}_p^*, \cdot)$ is a group if and only if p is a prime number.

Proof. $(\Rightarrow)$ If p is not a prime number, then there are $n, m \in \mathbb{Z}_p^*$ such that $p = n \cdot m$. Thus, $n \cdot m = p \equiv_p 0 \notin \mathbb{Z}_p^*$, which implies that multiplication is not an operation on $\mathbb{Z}_p^*$. Hence, by Lemma 4.4, $(\mathbb{Z}_p^*, \cdot)$ is not a group.
$(\Leftarrow)$ Suppose p is prime and let $n, m \in \mathbb{Z}_p^*$. So, $1 \leq n, m < p$, which implies that p neither divides n nor m. Now, since p is prime, $p \nmid n \cdot m$, which is the same as saying $n \cdot m \not\equiv_m 0$. Hence, multiplication is an operation on $\mathbb{Z}_p^*$ and by Lemma 4.4, $(\mathbb{Z}_p^*, \cdot)$ is a group. ⊣

In fact, for every prime number p, $(\mathbb{Z}_p^*, \cdot)$ is even a cyclic group, or in other words, there is always an element in $(\mathbb{Z}_p^*, \cdot)$ of order $p - 1$ (we omit the proof).

LEMMA 4.6. If p is prime, then for each $k \in \mathbb{Z}_p^*$ we have $k^{p-1} \equiv_p 1$.

Proof. We work in $(\mathbb{Z}_p^*, \cdot)$. Let $k \in \mathbb{Z}_p^*$, then $\langle k \rangle$ is a cyclic subgroup of $(\mathbb{Z}_p^*, \cdot)$, and since $|(\mathbb{Z}_p^*, \cdot)| = p - 1$, by Theorem 3.11 we get that $\operatorname{ord}(k) = |\langle k \rangle|$ divides $p - 1$. So, there is some positive integer ℓ such that $\ell \cdot \operatorname{ord}(k) = p - 1$. Now, in $\mathbb{Z}_p^*$ we have

$$k^{p-1} = k^{\ell \cdot \operatorname{ord}(k)} = \left(k^{\operatorname{ord}(k)}\right)^{\ell} = 1^{\ell} = 1\,,$$

which implies $k^{p-1} \equiv_p 1$. ⊣

Let us conclude this section with Fermat's little theorem:

THEOREM 4.7. If p is prime and n is a positive integer such that $p \nmid n$, then

$$p \mid n^{p-1} - 1\,.$$

Proof. We work in $(\mathbb{Z}_p^*, \cdot)$. $|(\mathbb{Z}_p^*, \cdot)| = p - 1$ and by Lemma 4.6, for every $k \in \mathbb{Z}_p^*$ we have $k^{p-1} \equiv_p 1$. Now, if $k \equiv_p n$, then $k^{p-1} \equiv_p n^{p-1}$. In particular, if $n \not\equiv_p 0$ (or equivalently, if $p \nmid n$), then $n^{p-1} \equiv_p 1$. Hence, $n^{p-1} - 1 \equiv_p 0$, or in other words, $p \mid n^{p-1} - 1$. ⊣