2 The Structure of + and × on $\mathbb{Z}$

2.1 Basic Observations

We may naturally express + and × in the following set theoretic way:

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto a + b \end{aligned}$$

$$\begin{aligned} \times : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (a, b) &\mapsto a \times b \end{aligned}$$

Here are 4 elementary properties that + satisfies:

- (Associativity): $a + (b + c) = (a + b) + c \ \forall a, b, c \in \mathbb{Z}$
- (Existence of additive identity) $a + 0 = 0 + a = a \ \forall a \in \mathbb{Z}$.
- (Existence of additive inverses) $a + (-a) = (-a) + a = 0 \ \forall a \in \mathbb{Z}$
- (Commutativity) $a + b = b + a \ \forall a, b \in \mathbb{Z}$.

Here are 3 elementary properties that × satisfy:

- (Associativity): $a \times (b \times c) = (a \times b) \times c \ \forall a, b, c \in \mathbb{Z}$
- (Existence of multiplicative identity) $a \times 1 = 1 \times a = a \ \forall a \in \mathbb{Z}$.
- (Commutativity) $a \times b = b \times a \ \forall a, b \in \mathbb{Z}$.

The operations of + and × interact by the following law:

- (Distributivity) $a \times (b + c) = (a \times b) + (a \times c) \ \forall a, b, c \in \mathbb{Z}$.

From now on we'll simplify the notation for multiplication to $a \times b = ab$.

Remarks

1. Each of these properties is totally obvious but will form the foundations of future definitions: groups and rings.
2. All of the above hold for + and × on $\mathbb{Q}$. In this case there is an extra property that non-zero elements have multiplicative inverses:

   $$\text{Given } a \in \mathbb{Q} \backslash \{0\}, \ \exists b \in \mathbb{Q} \text{ such that } ab = ba = 1.$$

   This extra property will motivate the definition of a field.

3. The significance of the Associativity laws is that summing and multiplying a finite collection of integers makes sense, i.e. is independent of how we do it.

It is an important property of $\mathbb{Z}$ (and $\mathbb{Q}$) that the product of two non-zero elements is again non-zero. More precisiely: $a, b \in \mathbb{Z}$ such that $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$. Later this property will mean that $\mathbb{Z}$ is something called an *integral domain*. This has the following useful consequence:

Cancellation Law: For $a, b, c \in \mathbb{Z}$, $ca = cb$ and $c \neq 0 \Rightarrow a = b$.

This is proven using the distributive law together with the fact that $\mathbb{Z}$ is an integral domain. I leave it an exercise to the reader.

2.2 Factorization and the Fundamental Theorem of Arithmetic

Definition. *Let $a, b \in \mathbb{Z}$. Then a divides $b \iff \exists c \in \mathbb{Z}$ such that $b = ca$. We denote this by $a|b$ and say that a is a divisor (or factor) of b.*

Observe that 0 is divisible by every integer. The only integers which divide 1 are 1 and -1. Any way of expressing an integer as the product of a finite collection of integers is called a *factorization*.

Definition. *A prime number p is an integer greater than 1 whose only positive divisors are p and 1. A positive integer which is not prime is called composite.*

Remark. *$\mathbb{Z}$ is generated by 1 under addition. By this I mean that every integer can be attained by successively adding 1 (or -1) to itself. Under multiplication the situation is much more complicated. There is clearly no single generator of $\mathbb{Z}$ under multiplication in the above sense.*

Definition. *Let $a, b \in \mathbb{Z}$. The highest common factor of a and b, denoted $HCF(a, b)$, is the largest positive integer which is a common factor of a and b. Two non-zero integers $a, b \in \mathbb{Z}$ are said to be coprime if $HCF(a, b) = 1$.*

Here are some important elementary properties of divisibility dating back to Euclid (300BC), which I'll state without proof. We'll actually prove them later in far more generality.

Remainder Theorem. *Given $a, b \in \mathbb{Z}$, if $b > 0$ then $\exists!\ q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$.*

Theorem. *Given $a, b \in \mathbb{Z}$, $\exists u, v \in \mathbb{Z}$ such that $au + bv = HCF(a, b)$. In particular, a and b are coprime if an only if there exist $u, v \in \mathbb{Z}$ such that $au + bv = 1$.*

Euclid's Lemma. *Let p be a prime number and $a, b \in \mathbb{Z}$. Then*

$$p|ab \Rightarrow p|a \text{ or } p|b$$

The Fundamental Theorem of Arithmetic. *Every positive integer, a, greater than* 1 *can be written as a product of primes:*

$$a = p_1 p_2 ... p_r.$$

Such a factorization is unique up to ordering.

Proof. If there is a positive integer not expressible as a product of primes, let $c \in \mathbb{N}$ be the least such element. The integer c is not 1 or a prime, hence $c = c_1 c_2$ where $c_1, c_c \in \mathbb{N}$, $c_1 < c$ and $c_2 < c$. By our choice of c we know that both c_1 and c_2 are the product of primes. Hence c much be expressible as the product of primes. This is a contradiction. Hence all positive integers can be written as the product of primes.

We must prove the uniqueness (up to ordering) of any such decomposition. Let

$$a = p_1 p_2 ... p_r = q_1 q_2 ... q_s$$

be two factorizations of a into a product of primes. Then $p_1 | q_1 q_2 ... q_s$. By Euclid's Lemma we know that $p_1 | q_i$ for some i. After renumbering we may assume $i = 1$. However q_1 is a prime, so $p_1 = q_1$. Applying the cancellation law we obtain

$$p_2 ... p_r = q_2 ... q_s.$$

Assume that $r < s$. We can continue this process until we have:

$$1 = q_{r+1} .. q_s.$$

This is a contradiction as 1 is not divisible by any prime. Hence $r = s$ and after renumbering $p_i = q_i \ \forall i$. □

Using this we can prove the following beautiful fact:

Theorem. *There are infinitely many distinct prime numbers.*

Proof. Suppose that there are finitely many distinct primes $p_1, p_2 .... p_r$. Consider $c = p_1 p_2 ... p_r + 1$. Clearly $c > 1$. By the Fundamental Theorem of Arithmetic, c is divisible by at least one prime, say p_1. Then $c = p_1 d$ for some $d \in \mathbb{Z}$. Hence we have

$$p_1(d - p_2 ... p_r) = c - p_1 p_2 .. p_r = 1.$$

This is a contradiction as no prime divides 1. Hence there are infinitely many distinct primes. □

The Fundamental Theorem of Arithmetic also tells us that every positive element $a \in \mathbb{Q}$ can be written uniquely (up to reordering) in the form:

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}; \ p_i \text{ prime and } \alpha_i \in \mathbb{Z}$$

The Fundamental Theorem also tells us that two positive integers are coprime if and only if they have no common prime divisor. This immediately shows that every positive element $a \in \mathbb{Q}$ can be written uniquely in the form:

$$a = \frac{\alpha}{\beta}, \alpha, \beta \in \mathbb{N} \text{ and coprime.}$$

We have seen that both $\mathbb{Z}$ and $\mathbb{Q}$ are examples of sets with two concepts of composition ($+$ and $\times$) which satisfy a collection of abstract conditions. We have also seen that the structure of $\mathbb{Z}$ together with $\times$ is very rich. Can we think of other examples of sets with a concept of $+$ and $\times$ which satisfy the same elementary properties?

2.3 Congruences

Fix $m \in \mathbb{N}$. By the remainder theorem, if $a \in \mathbb{Z}, \exists\, !\; q, r \in \mathbb{Z}$ such that $a = qm + r$ and $0 \leq r < m$. We call r the *remainder* of a modulo m. This gives the natural equivalence relation on $\mathbb{Z}$:

$$a \sim b \iff a \text{ and } b \text{ have the same remainder modulo } m \iff m|(a-b)$$

Important Exercise. *Check this really is an equivalence relation!*

Definition. *$a, b \in \mathbb{Z}$ are* ***congruent modulo m*** $\iff m|(a-b)$. *This can also be written:*

$$a \equiv b \mod m.$$

Remarks. 1. *The equivalence classes of $\mathbb{Z}$ under this relation are indexed by the possible remainder modulo m. Hence, there are m distinct equivalence classes which we call* ***residue classes****. We denote the set of all residue classes $\mathbb{Z}/m\mathbb{Z}$.*

2. *There is a natural surjective map*

$$\begin{aligned} [\,] \;\; : \;\; & \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \\ & a \mapsto [a] \end{aligned} \tag{1}$$

Note that this is clearly not injective as many integers have the same remainder modulo m. Also observe that $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], ...[m-1]\}$.

The following result allows us to define $+$ and $\times$ on $\mathbb{Z}/m\mathbb{Z}$.

Propostion. *Let $m \in \mathbb{N}$. Then,$\forall a, b, a', b' \in \mathbb{Z}$:*

$$[a] = [a'] \text{ and } [b] = [b'] \Rightarrow [a+b] = [a'+b'] \text{ and } [ab] = [a'b'].$$

Proof. This is a very good exercise. □

Definition. *We **define** addition and multiplication on $\mathbb{Z}/m\mathbb{Z}$ by*

$$[a] \times [b] = [a \times b] \ \forall a, b \in \mathbb{Z} \qquad [a] + [b] = [a + b] \ \forall a, b \in \mathbb{Z}$$

Remark. *Note that there is ambiguity in the definition, because it seems to depend on making a choice of representative of each residue class. The proposition shows us that the resulting residue classes are independent of this choice, hence $+$ and $\times$ are well defined on $\mathbb{Z}/m\mathbb{Z}$.*

Our construction of $+$ and $\times$ on $\mathbb{Z}/m\mathbb{Z}$ is lifted from $\mathbb{Z}$, hence they satisfy the eight elementary properites that $+$ and $\times$ satisfied on $\mathbb{Z}$. In particular $[0] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $0 \in \mathbb{Z}$:

$$[0] + [a] = [a] + [0] = [a], \ \forall [a] \in \mathbb{Z}/m\mathbb{Z};$$

and $[1] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $1 \in \mathbb{Z}$:

$$[1] \times [a] = [a] \times [1] = [a], \ \forall [a] \in \mathbb{Z}/m\mathbb{Z}.$$

We say that $[a] \in \mathbb{Z}/m\mathbb{Z}$ is non-zero if $[a] \neq [0]$. Even though $+$ and $\times$ on $\mathbb{Z}/m\mathbb{Z}$ share the same elementary properties with $+$ and $\times$ on $\mathbb{Z}$, they behave quite differently in this case. As an example, notice that

$$[1] + [1] + [1] + \cdots + [1](m \text{ times}) = [m] = [0]$$

Hence we can add 1 (in $\mathbb{Z}/m\mathbb{Z}$) to itself and eventually get 0 (in $\mathbb{Z}/m\mathbb{Z}$).

Also observe that if m is composite with $m = rs$, where $r < m$ and $s < m$ then $[r]$ and $[s]$ are both non-zero ($\neq [0]$) in $\mathbb{Z}/m\mathbb{Z}$, but $[r] \times [s] = [rs] = [m] = [0] \in \mathbb{Z}/m\mathbb{Z}$. Hence we can have two non-zero elements *multiplying* together to give *zero*.

Proposition. *For every $m \in \mathbb{N}, a \in \mathbb{Z}$ the congruence*

$$ax \equiv 1 \mod m$$

has a solution (in $\mathbb{Z}$) iff a and m are coprime.

Proof. This is just a restatement of the fact that a and m coprime $\iff \exists u, v \in \mathbb{Z}$ such that $au + mv = 1$. $\square$

Observe that the congruence above can be rewritten as $[a] \times [x] = [1]$ in $\mathbb{Z}/m\mathbb{Z}$. We say that $[a] \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse if $\exists [x] \in \mathbb{Z}/m\mathbb{Z}$ such that $[a] \times [x] = [1]$. Hence we deduce that the only elements of $\mathbb{Z}/m\mathbb{Z}$ with muliplicative inverse are those given by $[a]$, where a is coprime to m.

Recall that $\times$ on $\mathbb{Q}$ had the extra property that all non-zero elements had *multiplicative inverses*. When does this happen in $\mathbb{Z}/m\mathbb{Z}$?. By the above we see that this can happen $\iff \{1, 2, \cdots, m-1\}$ are all coprime to m. This can only happen if m is prime. We have thus proven the following:

Corollary. *All non-zero elements of $\mathbb{Z}/m\mathbb{Z}$ have a multiplicative inverse $\iff$ m is prime.*

Later this will be restated as $\mathbb{Z}/m\mathbb{Z}$ is a *field* $\iff$ m is a prime. These are examples of things called *finite fields*.

Important Exercise. *Show that if m is prime then the product of two non-zero elements of $\mathbb{Z}/m\mathbb{Z}$ is again non-zero.*

Key Observation: There are naturally occuring sets (other than $\mathbb{Z}$ and $\mathbb{Q}$) which come equipped with a concept of $+$ and $\times$, whose most basic properties are the same as those of the usual addition and multiplication on $\mathbb{Z}$ or $\mathbb{Q}$. **Don't be fooled into thinking all other examples will come from numbers. As we'll see, there are many examples which are much more exotic**.