2. Divisibility in the integers

We begin with a definition:

**Definition:** Let \(a, b\) be integers, with \(a \neq 0\). We say \(a\) divides \(b\) if \(b = ac\) for some \(c \in \mathbb{Z}\). Equivalently, \(a\) divides \(b\) if \(\frac{b}{a} \in \mathbb{Z}\). We write this as \(a \mid b\). We sometimes also say that \(a\) is a factor or a divisor of \(b\).

So, for example, \(3 \mid 6\) but \(3\) doesn’t divide \(5\). Zero doesn’t divide anything (even itself). On the other hand, \(1 \mid a\) for all \(a \in \mathbb{Z}\). Notice that if \(a \mid b\) and \(b \neq 0\) then \(|a| \leq |b|\). Thus, there are only finitely many divisors of a nonzero integer. The set of all divisors of \(10\) for instance is \(\{-10, -5, -2, -1, 1, 2, 5, 10\}\).

Here is a basic result we will use frequently:

**Proposition 1.** Let \(a, b, c, x, y\) be integers and suppose \(a \mid b\) and \(a \mid c\). Then \(a \mid (bx + cy)\).

**Proof.** Since \(a \mid b\) and \(a \mid c\), we have \(b = ar\) and \(c = as\) for some \(r, s \in \mathbb{Z}\). Then \(bx + cy = (ar)x + (as)y = a(rx + sy) = at\), where \(t = rx + sy \in \mathbb{Z}\). By definition of divides, \(a \mid (bx + cy)\). \(\square\)

**Exercises:**

1. Let \(a, b, c\) be integers such that \(a \mid b\) and \(a \mid (b + c)\). Prove \(a \mid c\).

2. Let \(a, b, c\) be integers and suppose \(a \mid bc\). Is it necessarily the case that \(a \mid b\) or \(a \mid c\)?

An important fact about the integers is that we can divide any two (nonzero) integers and get a unique quotient and remainder.

**Theorem 2.** (The Division Theorem) Let \(a\) and \(b\) be integers, with \(b \neq 0\). Then there exists unique integers \(q\) and \(r\), with \(0 \leq r < b\), such that \(a = bq + r\).

**Proof.** Let \(S = \{a - bx \mid x \in \mathbb{Z}, a - bx \geq 0\}\). Clearly, \(S\) is a set of non-negative integers. Also, \(S\) is not empty: If \(a \geq 0\) then \(a = a - b(0) \in S\) (here \(x = 0\)). If \(a < 0\), then \(a(1 - b) \geq 0\) since \(b \geq 1\). Then \(a(1 - b) = a - ba \in S\) (here \(x = a\)). Now, it is an axiom of the integers that every set of nonnegative integers has a least element. (This is called the Well Ordering Axiom.) So let \(r\) be the least element of \(S\). Then, as \(r \in S\), \(r = a - bq\) for some \(q \in \mathbb{Z}\). Therefore, we have \(a = bq + r\). Since \(r \in S\), we have \(r \geq 0\). We need to show that \(r < b\). Suppose not. Then \(r \geq b\). Then \(r - b \geq 0\) and \(r - b = (a - bq) - b = a - b(q + 1) \in S\) (here \(x = q + 1\)). But \(r - b < r\) and \(r\) was chosen as the least element in \(S\). This is a contradiction. Hence, the assumption that \(r \geq b\) must be false. Therefore, \(r < b\).

This establishes the existence of the integers \(q\) and \(r\). The uniqueness is left as a homework exercise. \(\square\)

**Exercises:**

1. Find \(q\) and \(r\) such that \(a = bq + r\) and \(0 \leq r < b\) for the following:
   
   (a) \(a = 87, b = 13\).
   
   (b) \(a = 57, b = 79\).
   
   (c) \(a = -100, b = 30\).
2. Suppose the remainder upon dividing $a$ by $b$ is $r$ and $r \neq 0$. Prove that the remainder upon dividing $-a$ by $b$ is $b - r$.

**Homework:**

1. Prove that 2 divides $n^2 - n$ for every integer $n$.

2. Prove that 3 divides $n^3 - n$ for every integer $n$.

3. Is it true that 4 divides $n^4 - n$ for every integer $n$?

4. Prove the uniqueness part of the Division Theorem. (Hint: Suppose $a = bq + r$ and $a = bt + s$ where $a, b, q, t, r, s$ are integers, $b > 0$, and $0 \leq r < b$ and $0 \leq s < b$. Show that $q = t$ and $r = s$.)