1.3: Divisibility and the Division Algorithm

We now discuss the concept of divisibility and its properties.

**Integer Divisibility**

If \(a\) and \(b\) are integers such that \(a \neq 0\), then we say "\(a\) divides \(b\)" if there exists an integer \(k\) such that \(b = ka\).

If \(a\) divides \(b\), we also say "\(a\) is a factor of \(b\)" or "\(b\) is a multiple of \(a\)" and we write \(a \mid b\). If \(a\) doesn’t divide \(b\), we write \(a \nmid b\). For example \(2 \mid 4\) and \(7 \mid 63\), while \(5 \nmid 26\).

a. Note that any even integer has the form \(2k\) for some integer \(k\), while any odd integer has the form \(2k+1\) for some integer \(k\). Thus \(2 \mid n\) if \(n\) is even, while \(2 \nmid n\) if \(n\) is odd.

b. \(\forall a \in \mathbb{Z}\) one has that \(a \mid 0\).

c. If \(b \in \mathbb{Z}\) is such that \(|b| < a\), and \(b \neq 0\), then \(a \nmid b\).

If \(a\) and \(b\) are integers such that \(a \mid b\) and \(b \mid c\), then \(a \mid c\).

Since \(a \mid b\) and \(b \mid c\), then there exist integers \(k_1\) and \(k_2\) such that \(b = k_1a\) and \(c = k_2b\). As a result, we have \(c = k_1k_2a\) and hence \(a \mid c\).

Since \(6 \mid 18\) and \(18 \mid 36\), then \(6 \mid 36\).

The following theorem states that if an integer divides two other integers then it divides any linear combination of these integers.
If \(a, b, c, m\) and \(n\) are integers, and if \(c \mid a\) and \(c \mid b\), then \(c \mid (ma + nb)\).

Since \(c \mid a\) and \(c \mid b\), then by definition there exists \(k_1\) and \(k_2\) such that \(a = k_1c\) and \(b = k_2c\). Thus \([ma + nb = mk_1c + nk_2c = c(mk_1 + nk_2),\) and hence \(c \mid (ma + nb)\).

Theorem [thm4] can be generalized to any finite linear combination as follows. If \([a \mid b_1, a \mid b_2, \ldots, a \mid b_n]\) then \([a \mid \sum_{j=1}^{n} k_j b_j]\) for any set of integers \((k_1, \ldots, k_n) \in \mathbb{Z}\). It would be a nice exercise to prove the generalization by induction.

The following theorem states somewhat an elementary but very useful result.

Theorem [thm5] The Division Algorithm If \((a)\) and \((b)\) are integers such that \((b > 0)\), then there exist unique integers \((q)\) and \((r)\) such that \((a = bq + r)\) where \((0 \leq r < b)\).

Consider the set \((A = \{a - bk \mid k \in \mathbb{Z} \})\). Note that \((A)\) is nonempty since for \((k < \frac{a}{b})\), \((a - bk < 0)\). By the well ordering principle, \((A)\) has a least element \((r = a - bq)\) for some \((q)\). Notice that \((r \geq 0)\) by construction. Now if \((r < b)\) then (since \((b > 0)\)) \([r < b = a - bq < a - b(q + 1) = a - bq + b < a - bq + b = r < b]\). This leads to a contradiction since \((r)\) is assumed to be the least positive integer of the form \((r = a - bq)\). As a result we have \((0 \leq r < b)\).

We will show that \((q)\) and \((r)\) are unique. Suppose that \((a = bq_1 + r_1)\) and \((a = bq_2 + r_2)\) with \((0 \leq r_1 < b)\) and \((0 \leq r_2 < b)\). Then we have \([b(q_1 - q_2) + (r_1 - r_2) = 0]\). As a result we have \([b(q_1 - q_2) = r_2 - r_1]\). Thus we get that \(b \mid (r_2 - r_1)\). And since \((\max(r_1, r_2) \leq r_2 = r_1,\) \(\max(r_1, r_2) = \max(r_1, r_2),\) and \(b > \max(r_1, r_2)\), then \((r_2 - r_1)\) must be \((0)\), i.e. \((r_2 = r_1)\). And since \((bq_1 + r_1 = bq_2 + r_2)\), we also get that \((q_1 = q_2)\). This proves uniqueness.

If \((a = 71)\) and \((b = 6)\), then \((71 = 6 \cdot 11 + 5)\). Here \((q = 11)\) and \((r = 5)\).

**Exercises**

1. Show that \((5 \mid 25, 19 \mid 38)\) and \((2 \mid 98)\).
2. Use the division algorithm to find the quotient and the remainder when 76 is divided by 13.
3. Use the division algorithm to find the quotient and the remainder when -100 is divided by 13.
4. Show that if \((a, b, c)\) and \((d)\) are integers with \((a)\) and \((c)\) nonzero, such that \((a \mid b)\) and \((c \mid d)\), then \((ac \mid bd)\).
5. Show that if \((a)\) and \((b)\) are positive integers and \((a \mid b)\), then \((a \mid leq b)\).
6. Prove that the sum of two even integers is even, the sum of two odd integers is even and the sum of an even integer and an odd integer is odd.
7. Show that the product of two even integers is even, the product of two odd integers is odd and the product of an even integer and an odd integer is even.
8. Show that if \((m)\) is an integer then \((3)\) divides \((m^3 - m)\).
9. Show that the square of every odd integer is of the form \((8m + 1)\).
10. Show that the square of any integer is of the form \((3m)\) or \((3m + 1)\) but not of the form \((3m + 2)\).
11. Show that if \((ac \mid bd)\), then \((a \mid bd)\).
12. Show that if $a \mid b$ and $b \mid a$ then $a = \pm b$.

Contributors and Attributions

- Dr. Wissam Raji, Ph.D., of the American University in Beirut. His work was selected by the Saylor Foundation’s Open Textbook Challenge for public release under a Creative Commons Attribution (CC BY) license.