Elementary Number Theory: Divisibility Theory in the Integers

Arjun Vardhan

†

Created: 5th April 2022
Last updated: 5th April 2022

1 Division Algorithm

- **Division Algorithm: Let $a, b \in \mathbb{Z}$, $b > 0$. Then there exist unique integers r, q such that $a = qb + r$, $0 \leq r < b$.** *Proof:* Let $S = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}$. Since $b \geq 1$, $|a|b \geq |a|$, and so $a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$. Thus S is nonempty. By the well ordering principle, S must have a least element r. By the definition of S, there exists $q \in \mathbb{Z}$ such that $r = a - qb$, $r \geq 0$. Suppose $r \geq b$. Then $a - (q+1)b = (a - qb) - b = r - b \geq 0$. Thus $a - (q+1)b \in S$, but since r is the least element of S, this is a contradiction. So $r < b$. Now, suppose that $a = qb + r = q'b + r'$, where $0 \leq r < b$, $0 \leq r' < b$. Then $r' - r = b(q - q')$ and so $|r - r'| = b|q - q'|$. On adding the inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we get $-b < r' - r < b$, or $|r' - r| < b$. Thus $b|q - q'| < b$, implying that $0 \leq |q - q'| < 1$. So $q - q' = 0$ and thus $r - r' = 0$. Thus q and r are unique. ■

- **Corollary: Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then there exist unique integers r, q such that $a = qb + r$, $0 \leq r < |b|$.** *Proof:* Let $b < 0$. Then $|b| > 0$, and by the division algorithm there exist unique integers q' and r such that $a = q'|b| + r$. Since $|b| = -b$, let $q = -q'$ to get $a = qb + r$, with $0 \leq r < |b|$. ■

2 Greatest Common Divisor

- Let $a, b \in \mathbb{Z}$, $a \neq 0$. b is said to be divisible by a, denoted $a \mid b$ if there exists $c \in \mathbb{Z}$ such that $b = ac$.

- **Let $a, b, c \in \mathbb{Z}$. Then:**

  1. $a \mid 0$, $1 \mid a$, and $a \mid a$. *Proof:* $0 = 0 \times a$, $1 = 1 \times a$ and $a = 1 \times a$. ■
  2. $a \mid 1$ if and only if $a = \pm 1$. *Proof:* Suppose $a \mid 1$. Then $1 = na$ for some $n \in \mathbb{Z}$. Let $|a| > 1$. Since $n \neq 0$, $|na| > 1$, which is a contradiction. So $|a| = 1$, and thus $a = \pm 1$. Conversely, suppose $a = +1$. Then $1 = 1 \times 1 = (-1) \times (-1)$. ■
  3. If $a \mid b$ and $c \mid d$, then $ac \mid bd$. *Proof:* There exist integers m, n such that $b = am$ and $d = cn$. Then $ac(mn) = bd$. ■
  4. If $a \mid b$ and $b \mid c$, then $a \mid c$. *Proof:* There exist integers m, n such that $b = am$ and $c = bn$. Then $c = a(mn)$. ■
  5. $a \mid b$ and $b \mid a$ if and only if $a = \pm b$. *Proof:* Suppose $a \mid b$ and $b \mid a$.
  6. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$. *Proof:*
  7. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$. *Proof:*

- Let $a, b \in \mathbb{Z}$, $|a| + |b| \neq 0$. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the positive integer d satisfying: $d \mid a$, $d \mid b$, and if $c \mid a$ and $c \mid b$, then $c \leq d$.

-

3 Euclidean Algorithm

4 The Diophantine Equation $ax + by = c$