Elementary Number Theory: Divisibility Theory in the Integers

Arjun Vardhan

†

Created: 5th April 2022
Last updated: 16th May 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 $b \mid a$. There exist integers m, n such that $a = bm$ and $b = an$. Thus $a = amn$, implying $mn = 1$. So $m = n = \pm 1$ and thus $a = \pm b$. The converse is obvious. ■
  6. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$. *Proof:* There exists an integer c such that $b = ac$. Since $b \neq 0$, $c \neq 0$. So $|b| = |a||c|$. Since $c \neq 0$, $|c| \geq 1$ and thus $|b| = |a||c| \geq |a|$. ■
  7. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$. *Proof:* There exist integers r, s such that $b = ar$ and $c = as$. Given integers x, y, $bx + cy = arx + asy = a(rx + zy)$. So $a \mid (bx + xy)$ for all $x, y \in \mathbb{Z}$. ■

- 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 $c \leq d$.

- **Given** $a, b \in \mathbb{Z}$**,** $|a| + |b| \neq 0$**, there exist** $x, y \in \mathbb{Z}$ **such that** $\gcd(a, b) = ax + by$**.** *Proof:* Consider the set $S = \{au + bv : u, v \in \mathbb{Z}, au + bv > 0\}$. S is nonempty as $|a| = (au + b \times 0) \in S$, where $u = \pm 1$. By the well ordering principle, S must contain a least element d. By the definition of S, there exist integers x, y such that $d = ax + by$. Using the division algorithm, we obtain $q, r \in \mathbb{Z}$ such that $a = qd + r$, $0 \leq r < d$. Then $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$. If $r > 0$, then $r \in S$, but this contradicts d being the least element of S. Thus $r = 0$, and $d \mid a$. By the same reasoning, $d \mid b$. Let c be a positive common divisor of a and b. Then $c \mid (ax + by) = d$, and so $c = |c| \leq |d| = d$. Thus $d = \gcd(a, b)$. ■

- **If** $a, b \in \mathbb{Z}$**, then the set** $T = \{ax + by : x, y \in \mathbb{Z}\}$ **is the set of all multiples of** $d = \gcd(a, b)$**.** *Proof:* Since $d \mid a$ and $d \mid b$, $d \mid (ax + by)$ for all $x, y \in \mathbb{Z}$. Conversely, there exist $x_0, y_0 \in \mathbb{Z}$ such that $d = ax_0 + by_0$. Given $n \in Z$, $nd = anx_0 + bny_0 \in T$. Thus T is the set of all multiples of d. ■

- Let $a, b \in \mathbb{Z}$, $|a| + |b| \neq 0$. a and b are said to be relatively prime or coprime if $\gcd(a, b) = 1$.

- a **and** b **are relatively prime if and only if there exist** $x, y \in \mathbb{Z}$ **such that** $1 = ax + by$**.** *Proof:* If $\gcd(a, b) = 1$, then there exist x, y such that $1 = ax + by$. Conversely, suppose $1 = ax + by$ and $d = \gcd(a, b)$. Then $d \mid (ax + by) = 1$ and so $d = 1$. ■

- **If** $\gcd(a, b) = d$**, then** $\gcd(a/d, b/d) = 1$**.** *Proof:* There exist x, y such that $d = ax + by$. Then $1 = \frac{a}{d}x + \frac{b}{d}y$. Thus $\gcd(a/d, b/d) = 1$. ■

- **If** $a \mid c$ **and** $b \mid c$**, with** $\gcd(a, b) = 1$**, then** $ab \mid c$**.** *Proof:* There exist r, s such that $c = ar = bs$. There exist x, y such that $1 = ax + by$. Then, $c = c \times 1 = c(ax + by) = acx + bcy \implies c = a(bs)x + b(ar)y = ab(sx + ry)$. So $ab \mid c$. ■

- **Euclid's Lemma: If** $a \mid bc$**, with** $\gcd(a, b) = 1$**, then** $a \mid c$**.** *Proof:* There exist $x, y \in \mathbb{Z}$ such that $1 = ax + by$. Then $c = c \times 1 = c(ax + by) = acx + bcy$. Since $a \mid ac$ and $a \mid bc$, $a \mid (acx + bcy) = c$. ■

- **Let** $a, b \in \mathbb{Z}, |a| + |b| \neq 0$**,** $d \in \mathbb{Z}^+$**. Then,** $d = \gcd(a, b)$ **if and only if** d **is a common divisor of** a **and** b **and for all** $c \in \mathbb{Z}$ **such that** c **is a common divisor,** $c \mid d$**.** *Proof:* Suppose $d = \gcd(a, b)$. Then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. Since $c \mid a$ and $c \mid b$, $c \mid (ax + by) = d$. Conversely, suppose d is an integer satisfying the conditions. Since $c \mid d$, $c \leq d$ and so $d = \gcd(a, b)$. ■

3 Euclidean Algorithm

- **Euclidean Algorithm:** Let $a, b \in \mathbb{Z}$. Since $\gcd(|a|, |b|) = \gcd(a, b)$, we can assume that $a \geq b > 0$. Applying the division algorithm, we get $a = q_1 b + r_1$, $0 \leq r_1 < b$. If $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. Otherwise, apply the division algorithm again on b and r_1 to get $b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$. If $r_2 = 0$, we are done. Otherwise divide r_1 by r_2 and so on. The last nonzero remainder obtained in this way is $\gcd(a, b)$.

- **If** $a = qb + r$**, then** $\gcd(a, b) = \gcd(b, r)$**.** *Proof:* If $d = \gcd(a, b)$, then $d \mid (a - qb)$ or $d \mid r$. Thus d is a common divisor of b and r. Suppose c is also a common divisor of b and r. Then $c \mid qb + r = a$, so $c \mid a$ and thus $c \leq d$. Therefore, $gcd(b, r) = d$. This provides the justification for the Euclidean Algorithm. ■

- **If** $k > 0$**, then** $\gcd(ka, kb) = k \gcd(a, b)$**.** *Proof:* Multiplying the equations for the euclidean algorithm on a and b by k, we see that the last nonzero remainder is $k \cdot \gcd(a, b)$. So $\gcd(ka, kb) = k \gcd(a, b)$. ■

- **Corollary: If** $k \neq 0$**, then** $\gcd(ka, kb) = |k| \gcd(a, b)$**.** *Proof:* Let $k < 0$. Then $-k = |k| > 0$, and so $\gcd(ka, kb) = \gcd(-ka, -kb) = \gcd(a|k|, b|k|) = |k| \gcd(a, b)$. ■

- The least common multiple of $a, b \in \mathbb{Z} \backslash \{0\}$, denoted by $\operatorname{lcm}(a, b)$, is the positive integer m satisfying the following: $a \mid m$, $b \mid m$, and if $a \mid c$ and $b \mid c$, with $c > 0$, then $m \leq c$.

- **Let** $a, b \in \mathbb{Z}^+$**. Then,** $\gcd(a, b) \cdot \mathbf{lcm}(a, b) = ab$**.** *Proof:* Let $d = \gcd(a, b)$ with $a = dr$, $b = ds$ for some integers r and s. Let $m = \frac{ab}{d}$. Then $m = as = rb$, and thus m is a common multiple of a and b. Let c be any positive integer that is a common multiple of a and b, say $c = au = bv$. There exist integers x, y such that $d = ax + by$. Then, $\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{c}{b}x + \frac{c}{a}y = vx + uy$. So $m \leq c$, and thus $m = \operatorname{lcm}(a, b)$. Therefore $\operatorname{lcm}(a, b) \gcd(a, b) = ab$. ■

- **Corollary: Let $a, b \in \mathbb{Z}^+$. Then, $\textbf{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.**

4 The Diophantine Equation $ax + by = c$

- Any equation in one or more unknowns that has to be solved in the integers is called a Diophantine equation.

- The simplest type is the linear diophantine equation $ax + by = c$, where a, b, c are integers and a and b are not both zero.

- **The linear diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$.** *Proof:* There exist integers r, s such that $a = dr$ and $b = ds$. Suppose a solution exists, i.e., $ax_0 + by_0 = c$ for some x_0, y_0, then $c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$. Conversely, suppose $c = dt$. There exist x_0, y_0 such that $d = ax_0 + by_0$. Then $c = dt = a(tx_0) + b(ty_0)$. ■

- **If x_0, y_0 is any particular solution for $ax + by = c$, then all other solutions are given by $x = x_0 + (\frac{b}{d})t$, $y = y_0 - (\frac{a}{d})t$, where t is an arbitrary integer and $d = \gcd(a, b)$.** *Proof:* Let x', y' be any other solution of the equation. Then, $ax_0 + by_0 = c = ax' + by' \implies a(x' - x_0) = b(y_0 - y')$. There exist relatively prime integers r, s such that $a = dr$ and $b = ds$. Thus $r(x' - x_0) = s(y_0 - y')$. By Euclid's lemma, $y_o - y' = rt$ for some integer t. Thus $x' - x_0 = st$. From this we obtain $x' = x_0 + st = x_0 + (\frac{b}{d})t$ and $y' = y_0 - rt = y_0 - (\frac{a}{d})t$. It can also be shown that these values satisfy the diophantine equation for any integer t: $ax' + by' = a[x_0 + (\frac{b}{d})t] + b[y_0 - (\frac{a}{d})t] = ax_0 + by_0 + (\frac{ab}{d} - \frac{ab}{d})t = c + 0 = c$. Thus there an infinite number of solutions. ■