Number Theory

Number theory is concerned with divisibility, prime numbers, congruences, and pattern in whole numbers and integers. It is known as the "Queen of Mathematics" (Gauss). Number theory plays a central role in modern applications such as cryptography, coding theory, computer security, music, authenticators, error codes, and more.

Divisibility

We will say that a divides b, denoted $a \mid b$, if and only if there exists an integer d such that $a \cdot d = b$. If a does not divide b, then we will write $a \nmid b$.

$$2 \mid 6, \quad -5 \mid 50, \quad 4 \nmid 2$$

- If $a \mid b$ and $b \mid c$, then $a \mid c$.

  Proof. Suppose $a \mid b$ and $b \mid c$. By definition, $b = m \cdot a$ and $c = n \cdot b$.

  $$\begin{aligned} c &= n \cdot b \\ c &= n \cdot (m \cdot a) \\ c &= (n \cdot m) \cdot a \quad \text{let } x = n \cdot m,\ n \in \mathbb{Z} \\ c &= x \cdot a \end{aligned}$$

  By definition, $a \mid c$. □

- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- If $a \mid b$ and $a \mid c$, then $a \mid (m \cdot b + n \cdot c)$ for any integers m and n
- If $d \mid a$, then $d \mid (c \cdot a)$ for any integer c

Example

Is it possible to have 100 coins, made up of p pennies, d dimes, and q quarters, be worth exactly, \$5.00?

First, assume there is a solution. Then we have:

$$p + d + q = 100$$

$$p + 10 \cdot d + 25 \cdot q = 500$$

Subtracting these equations gives us:

$$(p + 10 \cdot d + 25 \cdot q) - (p + d + q) = 500 - 100$$

$$9 \cdot d + 24 \cdot q = 400$$

Since $3 \mid 9$ and $3 \mid 24$, we have that:

$$3 \mid (9 \cdot d + 24 \cdot q)$$

That is, $3 \mid 400$, but $3 \nmid 400$. This is a contradiction. Having \$5.00 with 100 pennies, dimes and quarters is impossible.

Greatest Common Divisor (GCD)

We say that d is the greatest common divisor of a and b, $d = (a, b) = \gcd(a, b)$ if and only if $d \mid a$ and $d \mid b$, and if $c \mid a$ and $c \mid b$, then $c \leq d$.

$$(2, 6) = 2, \quad (3, 4) = 1, \quad (7, 0) = 7$$

If $(a, b) = 1$, then we will say that a and b are relatively prime.

Theorem : (1.1)

If $(a, b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. Suppose that $d = (a, b)$ and that $c = \left(\frac{a}{d}, \frac{b}{d}\right)$. Then, there exists integers q and r such that:

$$c \cdot q = \frac{a}{d} \quad \text{and} \quad c \cdot r = \frac{b}{d}$$

By rearranging these equations, we have that:

$$(c \cdot d) \cdot q = a \quad \text{and} \quad (c \cdot d) \cdot r = b$$

This shows that cd is a common divisor of a and b, so

$$1 \leq cd \leq (a, b) = d$$

Since d is positive, this gives $c = 1$ as desired. □

Theorem : Division Algorithm (1.2)

Given positive integers a and b, $b \neq 0$, there exists unique integers q and r, with $0 \leq r < b$, such that:

$$a = b \cdot q + r$$

Proof. Consider the set of integers:

$$\{a, a - b, a - 2b, a - 3b, \dots\}$$

From this set, let $r = a - qb$ be the smallest non-negative integer. It remains to show that q and r and unique. Suppose that there are integers q_1 and r_1 such that:

$$a = bq + r = bq_1 + r_1$$

By subtracting the two equations, we have that:

$$b(q - q_1) + (r - r_1) = 0$$

Since $b \mid 0$ and $b \mid (b(q - q_1))$, we have that $b \mid (r - r_1)$. However, $-b < r - r_1 < b$, therefore, we have that $r = r_1$. Substituting this into $0 = b(q - q_1) + (r - r_1)$ gives us that $q = q_1$. Therefore, q and r are unique. □