Integers

Paolo Bettelini

Contents

1 Divides operator

1.1 Definition

Given two integers a and b, we say that $a \mid b$ if a divides b, meaning that

$$\exists x \mid ax = b$$

.

1.2 Properties

Given the integers a, b and c

$$\begin{aligned} a \mid b \iff -a \mid b \iff a \mid -b \\ |a| \leq |b|, \quad b \neq 0 \\ a \mid b \implies a \mid bc \\ a \mid b \wedge b \mid c \implies a \mid c \end{aligned}$$

2 Division with remainder

Given two integers a and b with $b > 0$,

$$\exists_{=1} q, r \mid a = bq + r, \quad 0 \leq r < b$$

Let q and r be the quotient and remainder of the division of b by a. The common divisors of a and b are equivalent to the common divisors of r and q.

3 Euclidean algorithm

Euclid's algorithm, is an efficient method for computing the greatest common divisor of two integers a and b where $b > 0$.

Consider

$$a = bq + r$$

The process is iterative. For each iteration take the coefficient of the quotient (b) and divide it by the remainder.

$$\begin{aligned} & a = bq + r, & 0 \leq r < b \\ & b = rq_1 + r_1, & 0 \leq r_1 < r \\ & r = r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\ & \quad \vdots & \\ & r_n = r_{n+1} q_{n+2} + r_{n+1}, & 0 \leq r_{n+2} < r_{n+1} \\ & r_{n+1} = r_{n+2} q_{n+3} + 0 & \end{aligned}$$

This sequence is stricly decreasing and will terminate with a null remainder. The last remainder r_{n+2} is then the greatest common divisor between a and b.

4 Bézout's identity

Let a and b be integers with greatest common divisor d. Then, there exist integers x and y such that

$$ax + by = d$$

Furthermore, the integers $az + bt$ are multiples of d.

5 Greatest common divisor of multiple integers

The greatest common divisors of $a_0, a_1, \cdots, a_n$, denoted $\gcd(a_0, a_1, \cdots, a_n)$, is the greatest integer n such that $n \mid a_k$.

There exists integers u_k such that

$$a_0 u_0 + \cdots a_n u_n = \gcd(a_0, a_1, \cdots, a_n)$$

For $n \geq 2$, $\gcd(\gcd(a_0, \cdots, a_{n-1}), a_n) = \gcd(a_0, \cdots, a_n)$.

Given an integer c, $\gcd(ca_0, ca_1, \cdots, ca_n) = c \cdot \gcd(a_0, a_1, \cdots, a_n)$.

5.1 Coprime numbers

Two integers a and b are said to be **coprime** if they have no common divisor other than 1, meaning that $\gcd(a, b) = 1$.

Let $d = \gcd(a, b) \neq 0$. Then, the integers a' and b' where $a = da'$ and $b = db'$ are coprime because $d = \gcd(da', db') = d \cdot \gcd(a', b') \implies \gcd(a', b') = 1$.

6 Linear diophantine equations

6.1 Definition

A linear diophantine equations is an equation with 2 or more integer unknowns of the following form.

$$a_1x_1 + a_2 + x_2 + \cdots + a_nx_n = b$$

where $a_i, x_i, b \in \mathbb{Z}$ and x_i are unknowns.

The equation is solvable iff $\gcd(a_1, a_2, \cdots, a_n) \mid b$. This is because the left-hand side will always be a value that is a multiple of $\gcd(a_1, a_2, \cdots, a_n)$.

In fact, if $\gcd(a_1, a_2, \cdots, a_n) \mid b$, then $b = \gcd(a_1, a_2, \cdots, a_n)e$ for some e.
By the Bezout identity, which can be find using Euclid's algorithm, we have

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = \gcd(a_1, a_2, \cdots, a_n)$$

meaning that an integer solution is given by $x_n = ev_n$.

6.2 Two unkowns

Let

$$ax + by = c$$

be a solvable diophantine equation and let $d = \gcd(a, b)$. If $d = 0$, this means that $a = b = 0$ and $c = 0$ since $d \mid c$ (identity). Otherwise, let $a = da'$, $b = db'$ and $c = dc'$, then the equation is equivalent to

$$a'x + b'y = c'$$

Consider any solution to the equation $x = \overline{x}$ and $y = \overline{y}$, then the equation has infinitely many other solutions given by

$$x = \overline{x} + b'hy \qquad\qquad = \overline{y} + a'h$$

for any $h \in \mathbb{Z}$.

7 Modular arithmetic

7.1 Congruence

Let $a, b, n \in \mathbb{Z}$. We say that a and b are said to be congruent modulo n, denoted as $a \equiv b \pmod{n}$, if $a - b$ is a multiple of n.

Note that $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{1}$.

7.2 Congruence relation

The congruence relation modulo n is an equivalence relation.

- **Reflexive**: $\forall a, a - a = 0$, which is always a multiple of n.
- **Symmetric**: $a \equiv b \pmod{n} \implies \exists k \,|\, a - b = kn \implies b - a = -kn$. Since $-kn$ is a multiple of n, then $b \equiv a \pmod{n}$.
- **Transitive**: $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n}$ implies that both $a - b$ and $b - c$ are multiples of n. $\exists h, k \,|\, nh = a - b \wedge nk = b - c \implies a - b + b - c = nh + nk \implies a - c = n(h + k)$ which means that $a - c$ is also a multiple of n, so $a \equiv c \pmod{n}$.

7.3 Congruence class

The equivalence class of an integer a with respect to modulo n is said to be a **congruence class**, denoted $[a]_n$.

$$[a]_n \{a + kn \,|\, k \in \mathbb{Z}\}$$

Note that

$$[a]_n = [a + kn]_n, \quad k \in \mathbb{Z}$$

7.4 Quotient set

The set of all congruence classes modulo n is denoted $\mathbb{Z}/n$.

Note that $\mathbb{Z}/n$ has n elements:

$$[0]_n, [1]_n, \cdots, [n-1]_n,$$