

Integers

Paolo Bettelini

Contents

1	Divides operator	2
1.1	Definition	2
1.2	Properties	2
2	Division with remainder	2
3	Euclidean algorithm	2
4	Bézout's identity	3
5	Greatest common divisor of multiple integers	3
5.1	Coprime numbers	3
6	Linear diophantine equations	4
6.1	Definition	4
6.2	Two unknowns	4

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.

$$\begin{array}{ll} a = bq + r, & 0 \leq r < b \\ b = rq_1 + r_1, & 0 \leq r_1 < r \\ r = r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ \vdots & \\ r_n = r_{n+1}q_{n+2} + r_{n+1}, & 0 \leq r_{n+2} < r_{n+1} \\ r_{n+1} = r_{n+2}q_{n+3} + 0 & \end{array}$$

This sequence is strictly 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, \dots, a_n , denoted $\gcd(a_0, a_1, \dots, a_n)$, is the greatest integer n such that $n \mid a_k$.

There exists integers u_k such that

$$a_0u_0 + \dots + a_nu_n = \gcd(a_0, a_1, \dots, a_n)$$

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

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

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.

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

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

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

In fact, if $\gcd(a_1, a_2, \dots, a_n) \mid b$, then $b = \gcd(a_1, a_2, \dots, a_n)e$ for some e .

By the Bezout identity, which can be find using Euclid's algorithm, we have

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

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

6.2 Two unknowns

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 $x = \bar{x}$ and $y = \bar{y}$, then the equation has infinitely many other solutions given by

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

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