Integers

Paolo Bettelini

Contents

1 Divide 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

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

1.3 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.

1.4 Euclidean algorithm

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

1.5 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.