

Modular Arithmetic Definitions and Propositions

- (1) The “floor” function is defined by the formula

$$\lfloor x \rfloor := (\text{the greatest integer less than or equal to } x).$$

This is also known as “the greatest integer function,” and in old texts is denoted by (whole) brackets. Examples: $\lfloor 3.789 \rfloor = 3$; $\lfloor -3.789 \rfloor = -4$.

- (2) The “mod” **operator** is defined as follows:

$$x \bmod y := x - y \cdot \lfloor x/y \rfloor$$

if $y \neq 0$. For positive integers x and y , $x \bmod y =$ the remainder in integer division of x by y . Examples: $110 \bmod 26 = 6$; $-52 \bmod 26 = 0$.

- (3) The “mod” **relation** is defined as follows:

$$a \equiv b \pmod{m} \text{ if and only if } a \bmod m = b \bmod m.$$

The above definitions make sense even for real numbers. When a, b, m are integers and $m > 0$,

$$a \equiv b \pmod{m} \text{ if and only if } a - b \text{ is a multiple of } m.$$

Examples: $110 \equiv 6 \pmod{26}$; $-80 \equiv 24 \pmod{26}$.

- (4) Let a, b be integers. Then $a|b$, read “ a divides b ,” if and only if b is a multiple, i.e., an integer multiple, of a : $b = ka$ for some integer k . Examples: $7|98$; $-5|100$; but $8 \nmid 26$ (8 does not divide 26).

- (5) Graham, Knuth, and Patashnik’s divisibility definition (assume that a and b are integers):

$$a \setminus b \text{ if and only if } a > 0 \text{ and } a|b.$$

- (6) The “greatest common divisor,” abbreviated gcd, of a set of integers is, of course, the largest positive integer that divides every integer in the set. Examples: $\gcd(24, 52) = 4$; $\gcd(54, 42) = 6$.

- (7) Let a, x, m be integers with $m > 0$. Let $g = \gcd(a, m)$. The number of solutions of $ax \equiv b \pmod{m}$ in the set $\{1, 2, \dots, m\}$ is 0 if $g \nmid b$ and is g if $g|b$.