Divides

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Informally: "a fits into b" or "a is a factor of b"

"The small number goes first*" *when both are positive integers

Examples: $5 \mid 15$ $\quad -3 \mid 9$ $\quad 5 \nmid 21$

Division Theorem

Division Theorem:

For any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

q is referred to as the quotient

r is referred to as the remainder

Congruence

We need a formal definition of $a \equiv b \pmod{m}$.

We can't just say "a and b are on the same place in the m clock ☺"

Definition:

For integers a, b and positive integer m, we say $a \equiv b \pmod{m}$ iff $m \mid (a - b)$.

Note: $a \equiv b \pmod{m}$ is equivalent to $a \% m = b \% m$.

We will actually prove that the two notions are the same. But, the formal definition is much easier to use in proofs.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \quad b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.