Modular Arithmetic

Division

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that

$$b = ac$$

We write $a \mid b$

When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a.

Division Algorithm

Let a be an integer and d a positive integer.

Then there are unique integers q and r, with $0 \le r < d$, such that

$$a = dq + r$$

d = divisor

a = dividend

q = quotient

r = remainder

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

Congruence

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if $m \mid a - b$.

$$a \equiv b \pmod{m}$$

Is $7 \equiv 5 \pmod{6}$?

Is $18 \equiv 9 \pmod{3}$?

Congruence

Let a and b be integers, and let m be a positive integer.
Then $a \equiv b \pmod{m}$ if and only if a **mod** m = b **mod** m.

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Congruence

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that

$$a = b + km.$$

Congruence

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

Congruence

Let m be a positive integer and let a and b be integers. Then

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m.$$

Congruence

Find $(-133 \ \mathbf{mod}\ 23 + 261 \ \mathbf{mod}\ 23) \ \mathbf{mod}\ 23 = ?$