
Definition 1 : Given integers a and m, with $m > 0$,
a ***mod*** m is defined to be the remainder when a is divided by m.

Definition 2 : If two integers x and y have the same remainder when $n \mid x$ and $n \mid y$ for a positive integer n,
then x and y are **equivalent modulo** n (or x equals y *mod* n).
− We write either "x *mod* $n \equiv y$ *mod* n" or "$x \equiv y$ *mod* n".
− $x \equiv y$ (*mod* n)
: we also read "x is congruent to y modulo (or *mod*) n.

Example

(1) 12 *mod* 5

(2) 139 *mod* 3

(3) $1142 \equiv x$ *mod* 5. Find x for $x \in \{x \in \mathbb{Z} | 10 \leq x \leq 15\}$.

Theorem 1 . Given integers a, b, and m,

1. $a \equiv b$ *mod* m if and only if $a - b = k \cdot m$ for some integer k.

2. If $a \equiv b \; mod \; m$ and $c \equiv d \; mod \; m$, then

(1) $a + c \equiv b + d \; mod \; m$.

(2) $a \cdot c \equiv b \cdot d \; mod \; m$.

Theorem 2. If n is a square number, then $n \; mod \; 4$ is 0 or 1.

Theorem 3. Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$. Then the equation

$$ax \equiv b \ mod \ c$$

has a solution x if and only if $gcd(a, c) \mid b$.

Exercise If a function $f : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$f(a) = a \ mod \ m$$

then is a function f one–to–one? onto? What is its range?

Fermat's Little Theorem. Let p be a prime number, then $x^p \equiv x \quad mod\, p$ for all $x \in \mathbb{Z}$.

Read the proof in the textbook and be prepared to discuss the proof in class.

Using Fermat's Little Theorem, prove the following.

Corollary. Let p be a prime number and $p \nmid x$. Then $x^{p-1} \equiv 1 \quad mod\, p$.