CH 13 Congruence of Integers

mrevanishere

November 16, 2020

1 Congruence

DEFINITION: Let m be a pos int. For $a, b \in \mathbb{Z}$ if m divides $b - a$ we write $a \equiv b \bmod m$ and say a is congruent to b modulo m
Prop 13.1: Every int is congruent to exactly one of the numbers 0 to m-1 modulo m
Prop 13.2: Let m be a pos int. The following are true, for all $a, b, c, \in \mathbb{Z}$:
(1) $a \equiv a \mod m$
(2) if $a \equiv b \mod m$ then $b \equiv a \mod m$
(3) if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$

2 Arithmetic with Congruences

Prop 13.3: Suppose $a \equiv b \mod m$ and $c \equiv d \mod m$. Then:
$a + c \equiv b + d \mod m$ and $ac \equiv bd \mod m$.
Prop 13.4: If $a \equiv b \mod m$, and n is a pos int, then
$a^n \equiv b^n \mod m$
Prop 13.5:
(1) Let a and m be coprime integers. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \mod m$, then $x \equiv y \mod m$
(2) Let p be a prime, and let a be an int that is not divisible by p. If $x, y \in \mathbb{Z}$ are such that $xa \equiv ya \mod p$, then $x \equiv y \mod p$

3 Congruence Equations

$ax \equiv b \mod m, x \in \mathbb{Z}$ is a linear congruence equation
Prop 13.6: The congruence equation $ax \equiv b \bmod m$ has a solution $x \in \mathbb{Z}$ iff

$hcf(a, m)$ divides b

4 The System $\mathbb{Z}_m$

"the integers modulo m".
Examples