Math 2710

Oct 2-4

Congruence

Let m be a positive integer. Given two integers a and b, we say that "a is congruent to b modulo m" if m divides $a - b$. We write this:

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

For example, $11 \equiv 39 \pmod 7$ because $39 - 11 = 28$ and 28 is divisible by 7.

Properties of Congruence

For a fixed m, the congruence relation has properties similar to "$=$":

Proposition 3.11. Let m be a fixed positive integer, and let a, b, and c be other integers. Then

- $a \equiv a \pmod{m}$.
- if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

Proposition 3.12. The congruence relation behaves well with respect to arithmetic. Suppose $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Then:

- $ax + by \equiv a'x + b'y \pmod{m}$ for all integers x and y.
- $ab \equiv a'b' \pmod{m}$.

Examples

We saw that $11 \equiv 39 \pmod 7$. Therefore

- $11^2 \equiv 39^2 \pmod 7$
- $(5)(11) \equiv (5)(39) \pmod 7$
- $(5)(11) \equiv (-2)(39) \pmod 7$ because $5 \equiv -2 \pmod 7$.

Proposition: Every integer a is congruent mod m to exactly one integer in the set $\{0, 1, \ldots, m-1\}$. Two integers a and b are congruent modulo m if and only if a and b have the same remainder when divided by m.

Also every integer a is congruent mod m to exactly one integer in the set $\{1-m, 2-m, \ldots, -1, 0\}$.

Dividing both sides of a congruence

It is NOT true in general that if $b \not\equiv 0 \pmod{m}$ and $ab \equiv cb \pmod{m}$ then $a \equiv c \pmod{m}$.

For example $6 \equiv -12 \pmod{18}$ but $1 \not\equiv -2 \pmod{18}$.

What is true is the following.

Proposition. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$.

Proof: If $ac \equiv bc \pmod{m}$ then $m|(ac - bc) = (a - b)c$. If $\gcd(c, m) = 1$ then by Proposition 2.28 we have $m|(a - b)$ and therefore $a \equiv b \pmod{m}$.