Math 2710

Oct 2-11

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

Congruence equations in general

One can go further and understand exactly what happens with the equation $ax \equiv b \pmod{m}$ using the main theorem on linear diophantine equations.

Finding a solution to $ax \equiv b \pmod{m}$ means finding an integer x so that m divides $ax - b$. In other words, finding y and x so that $ax - b = my$. But this is the diophantine equation $ax - my = b$ and we know that this as a solution if and only if $\gcd(a, m)|b$ and, in that case, there are infinitely many solutions given by $x_0 + nmd$ where $d = \gcd(a, m)$. In other words, the solutions are $x \equiv x_0 \pmod{(m/d)}$.

This means there are d solutions mod m, given by $x_0 + n(m/d)$ with $n = 0, 1, \ldots, d - 1$. See Theorem 3.54 on page 69.

Equivalence Relations

A relation R between two elements of a set S is called an equivalence relation if it is symmetric, reflexive, and transitive.

Examples: on the integers, equality and congruence modulo m are equivalence relations. On objects, having the same color is an equivalence relation. One people, having the same last name is an equivalence relation.

An equivalence relation partitions the set into equivalence classes. The class of an element $a \in S$, written $[a]$, is the subset of S consisting of elements b such that bRa.

- $a \in [a]$.
- Two equivalence classes are either disjoint or identical.

Congruence classes

Suppose S is a set and $\sim$ is an equivalence relation. Then we know that S is divided up into classes $[x]$ where $[x] = \{y \in S : y \sim x\}$.

The element x is called a representative of the class.

In the case of congruence modulo a fixed integer m, there are m classes $[0], \ldots, [m-1]$.

Each class is an *arithmetic progression*:

$$[x] = \ldots, x-5m, x-4m, x-3m, x-2m, x-m, x, x+m, x+2m, \ldots$$

Arithmetic on congruence classes

One can do arithmetic on equivalence classes by defining $[a]+[b] = [a+b]$ and $[a][b] = [ab]$.

Proposition: This definition makes sense. In other words, if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $[a]+[b] = [a+b] = [a'+b'] = [a']+[b']$ and similarly for products.

The set of congruence classes modulo m is written $\mathbb{Z}_m$ in the book.

Inverses

If m is prime, then the equation $ax \equiv 1 \pmod{m}$ has a solution x provided $a \neq 0 \bmod m$.

This follows from Euclid's algorithm.

Theorem: If p is prime and n is any integer then $n^p \equiv n \pmod{p}$. If $p \not| n$, then $n^{p-1} \equiv 1 \pmod{p}$.

Proof: First, show that $a, 2a, 3a, \ldots, (p-1)a$ are all different modulo p. So they are a rearrangment of $1, 2, \ldots, p-1$. Then all of them together to get

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}.$$

Since $p \not| (p-1)!$, cancel it from both sides and get $a^{p-1} \equiv 1$.