

Math 300 Spring 2008 - Note 4

Zhigang Han, Umass at Amherst

1 Congruences

1.1 Congruence

Def 1: Let m be a fixed positive integer, $a, b \in \mathbb{Z}$. If $m|a - b$, we say “ a is congruent to b modulo m ”, and write

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

If $m \nmid a - b$, we say “ a is not congruent to b modulo m ”, and write

$$a \not\equiv b \pmod{m}.$$

Rmk : $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some $k \in \mathbb{Z}$.

Eg 1: $77 \equiv 37 \pmod{10}$, and $77 = 37 + 4 \cdot 10$.

Prop 1: Let $a, b, c \in \mathbb{Z}$. Then

- (i) $a \equiv a \pmod{m}$.
- (ii) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- (iii) If $a \equiv b \pmod{m}$, and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Prop 2: Let $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Then

- (i) $a + b \equiv a' + b' \pmod{m}$.
- (ii) $a - b \equiv a' - b' \pmod{m}$.
- (iii) $a \cdot b \equiv a' \cdot b' \pmod{m}$.

Rmk: Using (iii), one can easily show that if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all $n \in \mathbb{N}$.

Eg 3: Show that $3^{2n} \equiv 2^n \pmod{7}$ for all $n \in \mathbb{N}$.

Rmk: Another corollary is that if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$. The converse, however, does not hold in general. For instance, $9 \cdot 5 \equiv 5 \cdot 5 \pmod{10}$, but $9 \not\equiv 5 \pmod{10}$.

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

Eg 2: $9 \cdot 5 \equiv 5 \cdot 5 \pmod{4}$ and $\gcd(5, 4) = 1$, so $9 \equiv 5 \pmod{4}$.

Prop 3: $a \equiv b \pmod{m}$ if and only if a and b have the same remainders when divided by m .

Rmk: This implies that every integer must be congruent precisely to one of $0, 1, 2, \dots, m - 1$ modulo m .

Eg 4: What day is 2^{2008} days from today?

Tests for Divisibility:

(i) A number is divisible by 9 if and only if the sum of its digits is divisible by 9.

(ii) A number is divisible by 3 if and only if the sum of its digits is divisible by 3.

(iii) A number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

1.2 Equivalence Relations

Def 1: A **relation** on a set A is a subset S of $A \times A$. We say a is related to b , and write aRb , if $(a, b) \in S$. We say a is not related to b , and write $a \not R b$, if $(a, b) \notin S$.

Eg 1 (Examples of Relations):

(i) **Greater Than:** Let $A = \mathbb{R}$ and $S = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a > b\}$. Then aRb means $a > b$.

(ii) **Divisibility:** Let $A = \mathbb{Z}$ and $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \text{ divides } b\}$. Then aRb means $a \mid b$.

(iii) **Equality:** Let A be any set, and $S = \{(a, a) \mid a \in A\} \subset A \times A$. Then aRb means $a = b$.

(iv) **Congruence modulo m :** For $a, b \in \mathbb{Z}$, aRb when $a \equiv b \pmod{m}$.

Def 2: Let R be a relation on a set A .

(i) R is **symmetric** if aRb implies bRa .

(ii) R is **transitive** if aRb and bRc implies aRc .

(iii) R is **reflexive** if aRa for all $a \in A$.

Def 3: An **equivalence relation** on a set A is a relation R which is symmetric, transitive and reflexive.

Rmk: When R is an equivalence relation, we also say a is equivalent to b if aRb .

Eg 2: (iii) and (iv) in Eg 1 are equivalence relations, while (i) and (ii) are not.

Eg 3: Let R be a relation on \mathbb{R} such that aRb if and only if $a - b \in \mathbb{Q}$. Show that R is an equivalence relation.

Def 4: Let R be an equivalence relation on a set A . The **equivalence class** of a , denoted by $[a]$, is the subset of A consisting of all elements in A that are equivalent to a . That is,

$$[a] := \{x \in A \mid xRa\}.$$

The element a is called a **representative** of the equivalence class $[a]$.

Eg 4: Let R be the relation of congruence modulo 2. Then

$$\begin{aligned}[0] &= \{x \mid x \equiv 0 \pmod{2}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} \\ [1] &= \{x \mid x \equiv 1 \pmod{2}\} = \{\dots, -3, -1, 1, 3, 5, \dots\} \\ [2] &= \{x \mid x \equiv 2 \pmod{2}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} = [0].\end{aligned}$$

In fact, there are only two distinct equivalence classes, even integers and odd integers. Any even number is a representative of $[0]$, and any odd number is a representative of $[1]$. And every integer lies in exactly one congruence class.

Prop 4: Let R be an equivalence relation on a set A . If $a, b \in A$, then

- (i) $a \in [a]$.
- (ii) $[a] = [b]$ if and only if aRb ,
- (iii) $[a] \cap [b] = \emptyset$ if and only if $a \not R b$.

Rmk: This proposition says that two equivalence classes under any equivalence relation R are either identical or disjoint, and the set of equivalence classes gives a disjoint decomposition of A as $A = A_1 \cup A_2 \cup \dots \cup A_k$, which is called a **partition** of A .

Eg 5: Let R be a relation on $A = \{1, 2, 3, 4\}$ such that aRb if and only if $a \equiv b \pmod{2}$ (**Show that R is an equivalence relation!**). Then there are two distinct equivalence classes $[1] = \{1, 3\}$ and $[2] = \{2, 4\}$, which gives a partition of A as $A = \{1, 3\} \cup \{2, 4\}$.

1.3 Modulo Arithmetic and Groups

Def 5: The **congruence class modulo** m of the integer a is the set of integers

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}.$$

The set of congruence classes of integers, under the congruence relation modulo m , is called the set of **integers modulo** m and is denoted by \mathbb{Z}_m . That is,

$$\mathbb{Z}_m = \{[0], [1], [2], \dots, [m-1]\}.$$

Def 6 (Modular Arithmetic): Let $[a], [b] \in \mathbb{Z}_m$. We define addition $+$ and multiplication \cdot on \mathbb{Z}_m by $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$.

Rmk: Since these operations are defined in terms of representatives, we need to show that these operations are **well defined**. That is, the definition is independent of the choice of representatives. **Show it!**

Eg 6: Write the addition and multiplication table for \mathbb{Z}_4 and \mathbb{Z}_5 .

Fermat's little Theorem: Let p be a prime which does not divide $a \in \mathbb{Z}$. Then

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

Cor 1: Let p be a prime. Then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$.

Cor 2: Let p be a prime. Then every nonzero element $[a] \in \mathbb{Z}_p$ has a **(multiplicative) inverse**, that is, there exists an element $b \in \mathbb{Z}_p$ such that $[a] \cdot [b] = [1]$.

Rmk: To find the inverse of a in \mathbb{Z}_p , one needs to solve $[a][x] = [1]$. This means $ax \equiv 1 \pmod{p}$, which is equivalent to $ax + py = 1$. The last equation can be solved by extended Euclidean algorithm.

Eg 7: Find the inverse of $[4]$ in \mathbb{Z}_{13} .