

Chapter 2 Congruences

2.1 Congruences

Definition Let $m > 0, m \in \mathbb{Z}$. Let $a, b \in \mathbb{Z}$.

We say a is congruent to b modulo m and write ----- if -----

Examples

- (1) $18 \equiv \text{-----} \pmod{5}$ size -----
 (2) $-25 \equiv \text{-----} \pmod{6}$ size -----

Proposition Let $m > 0, m \in \mathbb{Z}$, Let $a, b, c \in \mathbb{Z}$. Then

- (1) [REFLEXIVE]
- (2) [SYMMETRIC]
- (3) [TRANSITIVE]

PROOF:

(7)

Corollary Let $m > 0, m \in \mathbb{Z}$.

Then \mathbb{Z} can be partitioned into m equivalence classes under \sim_m .

Example Let $m=3$. There are 3 equivalence classes:

Definition Let $m \in \mathbb{Z}$, $m > 1$.

A complete residue system modulo m is a

Example

(a) $\{0, 1\}$ is a complete residue system mod 3.
Every integer is

(b) $\{1, 2\}$ is also complete residue system mod 3.

Proposition Let $m > 1$, $m \in \mathbb{Z}$.

The set $\{0, 1, \dots, m-1\}$ is a complete residue system mod m .

Proof.

Proposition Let $m \in \mathbb{Z}$, $m > 1$. Let $a, b, c, d \in \mathbb{Z}$.

Suppose $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$. Then

(a) $a + c \equiv \quad \pmod{m}$,

(b) $ac \equiv \quad \pmod{m}$.

Proof.

Proposition (#15). Let $a, b \in \mathbb{Z}$ & suppose $a \equiv b \pmod{m}$

Then $a^n \equiv \quad \pmod{m}$ if $n \quad \dots$

PROOF:

Ex #17 A positive integer is divisible by 3
iff the sum of digits -----.

PROOF:

Cancellation Property

- ① If $a, b, c \in \mathbb{R}$, ----- and $ab = ac$
then -----.
- ② Let $m > 1$. Suppose $a, b, c \in \mathbb{Z}$ & $a \neq 0 \pmod{m}$ &
 $ab \equiv ac \pmod{m}$.
Does this imply that $b \equiv c \pmod{m}$?

Proposition Let $m \geq 1, a, b, c \in \mathbb{Z}$.

Then $ab \equiv ac \pmod{m}$

iff $b \equiv c \pmod{m}$).

PROOF:

(\Rightarrow)

(\Leftarrow)

(7)

Example $2 \cdot 1 \equiv 2 \cdot 5 \pmod{8}$ since $2 \cdot 1 = 2$ and $2 \cdot 5 = 10$ and $10 - 2 = 8$.

This implies

2.2 Linear Congruences in One Variable

A linear congruence in one variable has
the form _____.

Example! Find all solutions $x \in \mathbb{Z}$: $3x \equiv 2 \pmod{7}$.

(2) Find all solutions $x \in \mathbb{Z}$: $3x \equiv 2 \pmod{9}$.

Let $x \in \mathbb{Z}$.

$x \pmod{9}$

$3x \pmod{9}$

NOTE

Suppose $x \in \mathbb{Z}$
all $3x \equiv 2 \pmod{9}$.

Then

0

1

2

3

4

5

6

7

8

(3) Solve $3x \equiv 3 \pmod{9}$.

Theorem: Let $m, a, b \in \mathbb{Z}$ with $m > 1$, and suppose $d = (\underline{\quad}, \underline{\quad})$.

(1) If $\underline{\quad}$ then the linear congruence
 $ax \equiv b \pmod{m}$

has $\underline{\quad}$.

(2) If $\underline{\quad}$ then the linear congruence
 (*) $ax \equiv b \pmod{m}$

has $\underline{\quad}$ incongruent solutions $\pmod{\underline{\quad}}$ given
 by

$$x \equiv$$

where $\underline{\quad}$.

PROOF: Let $m, a, b \in \mathbb{Z}$, $m > 1$ & $d = (\underline{\quad}, \underline{\quad})$.

(1) Suppose $x \in \mathbb{Z}$ and $ax \equiv b \pmod{m}$.
 Then

(2) Suppose $\underline{\quad}$. Since $d = (\underline{\quad}, \underline{\quad})$ there

(10)

Therefore $x_0 = \text{---}$ is a solution to (*)
We show

$x_0 + \text{---}$ are also solutions to (*)
if $x_0 \text{---}$.

Let x_0 be a particular solution of (*) & let x_1 be any solution of (*). We show that

(11)

Let x_0 be a particular solution of (*) & let x be any solution of (*). We show that

$$x \equiv$$

all these solutions are $\text{---} \text{---} \text{---} \pmod{\text{---}}$.

Finally we show that the --- solutions

are $\text{---} \text{---} \text{---} \pmod{\text{---}}$.

Hence (*) has incongruent solutions (mod)⁽¹²⁾
given by $x \equiv$

Example (#28(d))

Find all least nonnegative incongruent solutions

$$(*) \quad 12x \equiv 16 \pmod{32}.$$

.D

Multiplicative Inverse mod m

Definition Let $m \in \mathbb{Z}$, $m > 1$ & $a \in \mathbb{Z}$.

The integer a has a multiplicative inverse mod m if _____;

a has a mult. inverse mod m iff

The linear congruence _____ has

Corollary Let $m, a \in \mathbb{Z}$ with $m > 1$.

a has a multiplicative inverse

if and only if _____.

PROOF:

Example(a) Find a mult. inverse of 3 (mod 7).

Note: _____.

We want x : _____.

$x \pmod{7}$	$3x \pmod{7}$
0	
1	
2	
3	
4	
5	
6	

_____ is a
multiplicative inverse
of 3 (mod 7).

(b) Hence solve $3x \equiv 2 \pmod{7}$.

Proposition Let $a, c, m \in \mathbb{Z}$, $m > 1$ & $(a, m) = 1$.
Let b be the multiplicative inverse of $a \pmod{m}$.

The congruence

$$ax \equiv c \pmod{m}$$

has the solution given by

$$x \equiv \frac{cb}{a} \pmod{m}.$$

Example

- (a) Find multi. inverse of 30 mod 77.
(b) Hence solve $30x \equiv 71 \pmod{77}$.

NOTE: $(30, 77) = \dots$

(15)

We use the Euclidean Alg:

$$77 = (\quad) \cdot 30 +$$

$$17 =$$

Hence

and $_ _$ is mult. inverse of 30 mod 77.

(b) $30x \equiv 71 \pmod{77}.$

2.3 The Chinese Remainder Theorem

This method is thought to be originally due to



孫子算經卷上
 唐觀美行卷上 輕重都尉 李漢等奉勅注釋

度之所起起於忽欲知其忽蠶吐絲為忽十忽
 為一絲十絲為一毫十毫為一釐十釐為一分
 十分為一寸十寸為一尺十尺為一丈十丈為
 一引五十尺為一端四十尺為一疋六尺為一
 步二百四十步為一畝三百步為一里
 稱之所起起於黍十黍為一粟十粟為一銖二
 十四銖為一兩十六兩為一斤三十斤為一鈞

(-----)

Chinese Remainder Theorem

Let m_1, m_2, \dots, m_n

be -----

(ie $(m_i, m_j) =$

f).

Let $b_1, b_2, \dots, b_n \in \mathbb{Z}$.

The system of linear congruences

$$(*) \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv \quad \quad \quad \pmod{m_2} \\ \vdots \\ x \equiv \quad \quad \quad \pmod{m_n} \end{cases}$$

has a ----- solution mod M

where $M = \dots$. The solution is given by $x \equiv$

where f_j for $1 \leq j \leq n$,

----- and -----

Example Solve

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 4 \pmod{6} \\ x \equiv 3 \pmod{5} \end{cases}$$

$$(\quad, \quad) = (\quad, \quad) = (\quad, \quad) = \quad .$$

$$M =$$

$$b_1 =$$

$$b_2 =$$

$$b_3 =$$

$$m_1 =$$

$$m_2 =$$

$$m_3 =$$

$$M_1 =$$

$$M_2 =$$

$$M_3 =$$

We solve

$$\text{Take } x_1 =$$

We solve

$$\text{Take } x_2 =$$

We solve

$$\text{Take } x_3 =$$

Let $x =$

Answer:

Check:

To prove the CRT we need

Proposition

(a) [Ex 42(b) p. 22 ch1].

Let $a, b_1, b_2, \dots, b_n \in \mathbb{Z}$ with

$$(a, b_1) = (a, b_2) = \dots = (a, b_n) = 1.$$

Then

$$(a, b_1 b_2 \dots b_n) = 1.$$

(b) [Ex 43(1), p. 22, ch1]

Let $a_1, a_2, \dots, a_n, c \in \mathbb{Z}$ with

a_1, a_2, \dots, a_n -----

$$\left(\begin{array}{c} \text{ie} \\ \text{If} \end{array} \begin{array}{c} (a_i, a_j) = 1 \\ a_i | c \text{ for each } 1 \leq i \leq n \end{array} \right) \text{ for } \dots$$

Then

Proof of CRT

Let $m_1, m_2, \dots, m_n, b_1, b_2, \dots, b_n \in \mathbb{Z}$

with m_1, m_2, \dots, m_n _____.

Let $M =$ _____,

$$M_i =$$

for $1 \leq i \leq n$. Let $1 \leq i \leq n$

Then $(m_j, m_i) = 1$ for _____.

So

$$\prod_{j \neq i} m_j = M_i \quad \& \quad (M_i, m_i) = \text{_____}$$

Hence M_i has a mult. inverse mod _____,

ie

$$M_i x_i \equiv \text{_____} \pmod{\text{_____}}$$

for _____.

Now

let

$$x =$$

Now let $1 \leq i \leq n$ be fixed.

If $j \neq i$, $m_i \mid$ _____ $\equiv 0 \pmod{m_i}$.

So

$$x \equiv$$

$$\text{as required. Hence } x \text{ is } \text{_____}$$

_____.

It remains to show uniqueness.

Suppose x' is a soln to (1). Then

(20)

2.4 Wilson's Theorem

Lemma Let p be prime & $a \in \mathbb{Z}$. Then a is its own multiplicative inverse mod p if and only if _____.

PROOF Let p be prime & $a \in \mathbb{Z}$

(\Rightarrow) Suppose a is its own mult. inverse mod p .
Then

(\Leftarrow) Suppose

Wilson's Theorem Let p be -----
Then $(p-1)! \equiv -1 \pmod{p}$.

Idea of Proof $p=13$.

$$(p-1)! =$$

$$(2)(3) \dots =$$

$$(3)(4) \dots =$$

$$(4)(5) \dots =$$

$$(5)(6) \dots =$$

$$(6)(7) \dots =$$

$$\begin{aligned} \text{So } (p-1)! &= \\ &= \\ &\equiv \\ &\equiv \\ &\equiv \end{aligned}$$

Proof of Wilson's Theorem

The Theorem is true for $p=2$ since -----

The Theorem is true for $p=3$ since

Let $p > 3$ be prime. Let $1 \leq a \leq p-1$ with $a \in \mathbb{Z}$.

Proposition Let $n \in \mathbb{Z}$ with $n > 1$.

If $(n-1)! \equiv \quad \pmod{n}$ then n is _____.

PROOF:

Suppose $n \in \mathbb{Z}$, $n > 1$ & $(n-1)! \equiv \quad \pmod{n}$.

Suppose $n = ab$ where $a, b \in \mathbb{Z}$ and
 $1 \leq a < n$.

Corollary Let $n \in \mathbb{Z}$ & $n > 1$. Then n
 is prime if and only if _____.

2.5 Fermat's Little Theorem & Pseudo primes

Fermat's Little Theorem

Let p be prime and suppose _____.

Then

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

PROOF: Let p be prime & suppose _____.

Consider the integers

(*) $a, 2a, 3a, \dots, (p-1)a.$

Example Use Fermat's Little Theorem to find the least nonnegative residue of $2^{2015} \pmod{17}$.

Corollary to F.L.T Let p be prime, $a \in \mathbb{Z}$ with $p \nmid a$.
Then $a^{p-1} \pmod{p}$ is the multiplicative inverse of $a \pmod{p}$.

Proof:

Corollary Let $a \in \mathbb{Z}$, & suppose p is prime.
Then

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

Proof: Let $a \in \mathbb{Z}$, & suppose p is prime.

Case 1 $a \equiv 0 \pmod{p}$.

Case 2 $a \not\equiv 0 \pmod{p}$.

Corollary If p is prime then $2^p \equiv 2 \pmod{p}$

Question: Is the converse true?

Definition n is a pseudoprime if

Example 341 is pseudoprime.

2.6 Euler's Theorem

The Euler phi-Function Let n be a positive integer.

We define

$$\phi(n) := \left\{ \begin{array}{l} \text{---} \\ \text{---} \end{array} \right\}$$

= # of

Examples

$\phi(1)$	=	1
$\phi(2)$	=	1, 2
$\phi(3)$	=	1, 2, 3
$\phi(4)$	=	1, 2, 3, 4
$\phi(5)$	=	1, 2, 3, 4, 5
$\phi(6)$	=	1, 2, 3, 4, 5, 6

Note Let p be prime then $(p, p) = \text{---}$,
and $(x, p) = \text{---}$ for $\text{---} \leq x \leq \text{---}$.

$$\phi(p) = \text{---}, \text{ if } p \text{ is prime.}$$

Lemma Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$.

If $(a, m) = 1$, then --- .

Proof.

Lemma 2 Let $m \in \mathbb{Z}$, $m \neq 0$.

(a) Let $a, b \in \mathbb{Z}$ with $(a, m) = (b, m) = 1$.

Then $(ab, m) =$.

(b) If $a_1, a_2, \dots, a_n \in \mathbb{Z}$, &

$(a_1, m) = (a_2, m) = \dots = (a_n, m) =$,

then

$($, $m) =$.

Proof: see Ex 4.2 pp 21-22 Chapt 1.

Euler's Theorem Let $a, m \in \mathbb{Z}$ with $m > 1$,

and suppose a and m are relatively prime. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof: Let $a, m \in \mathbb{Z}$, with $m > 1$ & a and m relatively prime.

The result is clearly true for $n=1$.

Assume $m > 1$, and let

(*) $r_1, r_2, \dots, r_{\phi(m)}$

be the elements of the set

$$\{ \quad : \quad \}$$

NOTE (m, m)

Example (Ex 67)

$m=16$. The set of integers x , $1 \leq x \leq 16$ with $(x, 16) = 1$ is

{ , , , , , , , }

So $\phi(16) = \dots$ Show $9^{-1} \equiv 1 \pmod{16}$
by following the proof of Euler's Thm.

(32)

Proposition Let $m \in \mathbb{Z}$ with $m > 1$.

Let $S = \{x \in \mathbb{Z} : 1 \leq x \leq m \text{ \& } (x, m) = 1\}$.

Let $T = \{x \in \mathbb{Z} : (x, m) = 1\}$.

Every

PROOF (EX.)

NOTE: $|S| =$

Example $m = 12$.

$S = \{x \in \mathbb{Z} : 1 \leq x \leq 12 \text{ \& } (x, 12) = 1\}$

$= \{1, 5, 7, 11\}$.

So

$\phi(12) = |S| =$

Let $y = 29$.

Then

Definition: Let $m \in \mathbb{Z}$, with $m > 1$. Any set
of ----- integers such that -----

is called a reduced residue system mod m .

Example

$\{1, 5, 7, 11\}$ is a reduced residue system mod 12.

$\{1, 5, 7, 11\}$ is also a reduced residue system mod 12 since