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) $18 \equiv$ (mod 5) since _____.
(2) $-25 \equiv$ (mod 6) since _____.

Proposition Let $m > 0$, $m \in \mathbb{Z}$, Let $a, b, c \in \mathbb{Z}$. Then
(1) [REFLEXIVE]
(2) [SYMMETRIC]
(3) [TRANSITIVE]

PROOF:

<u>Corollary</u> Let $m>0$, $m\in\mathbb{Z}$.
Then ___ can be partitioned into ______
________ under __________.

<u>Example</u> Let $m=3$. There are ___ equivalence classes:

Definition Let $m \in \mathbb{Z}$, $m \geq 1$.
A **complete residue system modulo m** is a

Example

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

(b) $\{\ ,\ ,\ \}$ is also complete residue syst. mod 3.

Proposition Let $m \geq 1$, $m \in \mathbb{Z}$.
The set $\{\ ,\ ,\ , \ldots,\ \}$ 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) $a + c \equiv$ _____ $\pmod{m}$,

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

Proof.

Proposition (#15). Let $a, b \in \mathbb{Z}$ & suppose $a \equiv b \pmod{m}$
Then $a^n \equiv$ ___ $\pmod{m}$ if/ n _____.

PROOF:

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

PROOF:

Cancellation Property

(1) If $a, b, c \in R$, --- then ----. ab = ac

(2) Let $m \geq 1$. Suppose $a, b, c \in \mathbb{Z}$ & $a \not\equiv 0 \pmod{m}$ & $ab \equiv ac \pmod{m}$.
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 $b \equiv c \pmod{\quad}$.

PROOF:

($\Rightarrow$)

($\Leftarrow$)

Example $2 \cdot 1 = 2.5 \pmod 8$ since _____

This implies

2.2 Linear Congruence in One Variable

A linear congruence in one variable has the form _____.

Example (1) 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 $x \in \mathbb{Z}$.

$x \pmod 9$	$3x \pmod 9$
0	
1	
2	
3	
4	
5	
6	
7	
8	

NOTE
Suppose $x \in \mathbb{Z}$ and $3x \equiv 2 \pmod 9$.
Then

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

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

(1) If _____ then the linear congruence

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

has _____.

(2) If _____ then the linear congruence

(*) $ax \equiv b \pmod{m}$

has ___ incongruent solutions (mod ___) given by

$x \equiv$

where _____.

Proof: Let $m, a, b \in \mathbb{Z}$, $m \geq 1$ & $d = (\_\_, \_\_)$.

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

Then

(2) Suppose ____. Since $d = (\_\_, \_\_)$ then

(a)

Therefore $x_0 =$ ___ is a solution to (*)
We show
$x_0 +$ ___ are also solutions to (*)
if x_0 ___.

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

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

$$x \equiv$$

and these solutions are _____ (mod __).

Finally we show that the __ solutions are _____ (mod __).

Hence (*) has ___ incongruent solutions (mod ___) given by

$x \equiv$

□

Example (#28(d))

Find all least nonnegative incongruent solutions to

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

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 $m, a \in \mathbb{Z}$ w.t. $m > 1$.
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 mod m.
The congruence

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

has the ____ solution given by

$$x \equiv \quad \pmod{\quad}.$$

Example

(a) Find mult. inverse of 30 mod 77.

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

NOTE: $(30, 77) =$ ___.

We use the Euclidean Alg:

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

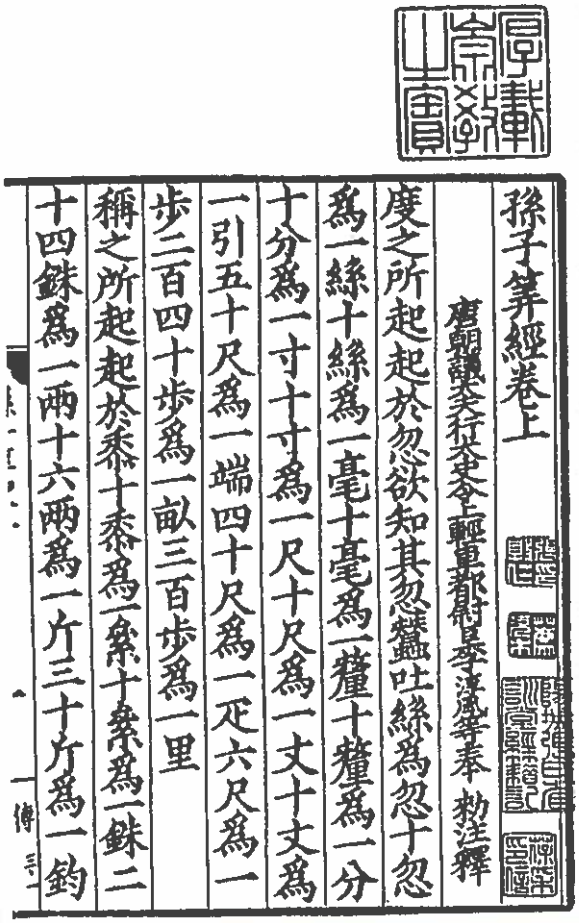
$17 =$

Hence

and __ is mult. inverse of 30 mod 77.

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

2.3 The Chinese Remainder Theorem



孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠛蠓吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一累十累爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

This method is thought to be originally due to

_____ _____

(_____ = _____).

Chinese Remainde Theorem

Let $m_1, m_2, \ldots, m_n$ be _____

(ie $(m_i, m_j) =$ _____).

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

The system of linear congruences

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

has a _____ solution mod M

where $M =$ _____. The solution is given by

$x \equiv$

where for $1 \le j \le n$,

_ _ _ _ _ _ _ and _ _ _ _ _ _ _ .

Example Solve

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

(,) = (,) = (,) = .

$M =$

$b_1 =$ $b_2 =$ $b_3 =$

$m_1 =$ $m_2 =$ $m_3 =$

$M_1 =$ $M_2 =$ $M_3 =$

We solve

Take $x_1 =$

We solve

Take $x_2 =$

We solve

Take $x_3 =$

Let $x =$

Answer :

Check:

To prove the CRT we need

Proposition

(a) [Ex 42(b) p. 22 Ch1].

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

(,) = (,) = ... = (,) =

Then

(a ,) = 1.

(b) [Ex 43(c), p. 22, Ch1]

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

$a_1, a_2, \ldots, a_n$ ---------

(ic (a_i ,) = for).

If $a_i \mid c$ for each $1 \le i \le n$

Then ---------.

Proof of CRT

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

with $m_1, m_2, \ldots, m_n$ _____.

Let $M =$,

$M_i =$

If $1 \le i \le n$. Let $1 \le i \le n$

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

So

$\prod$ $= M_i$ & $(M_i, m_i) =$ ___.

Hence M_i has a mult inverse mod ___,

ie

$M_i x_i \equiv$ ___ (mod ___)

for _____.

Now let

$x =$.

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

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

So

$x \equiv$,

and $x \equiv$,

as required. Hence x is _____.

It remains to show uniqueness.

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

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 $(\quad)! \equiv \quad \pmod{p}$.

Idea of Proof $p = 13$.

$(p-1)! =$

$(2)(\quad) =$
$(3)(\quad) =$
$(4)(\quad) =$
$(5)(\quad) =$
$(6)(\quad) =$

So $(p-1)! =$
$=$
$\equiv$
$\equiv$
$\equiv$

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 $(n-1)! \equiv$ _____ $(\text{mod } n)$ then n is _____.

Proof:

Suppose $n \in \mathbb{Z}$, $n > 1$ & $(n-1)! \equiv$ _____ $(\text{mod } n)$.

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

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

2.5 Fermat's Little Theorem & Pseudoprimes

Fermat's Little Theorem

Let p be prime and suppose ____.

Then

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

PROOF: Let p be prime & suppose ____.

Consider the integers

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

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

Corollary to FLT Let p be prime, $a \in \mathbb{Z}$ with $p \nmid a$. Then $\overline{a^{p-2}}$ is the multiplicative inverse of $a \bmod p$.

Proof:

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

$$a^p \equiv \quad (\text{mod } p).$$

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

Case1 $a \equiv 0 \pmod{p}$.

Case2 $a \not\equiv 0 \pmod{p}$.

Corollary If p is prime then $2^p \equiv \quad (\text{mod } \quad)$

Question: Is the converse true?

Definition n is a pseudoprime if _____
_____.

Example ___ is pseudoprime.

2.6 Euler's Theorem

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

$$\phi(n) := \{ \quad : \quad \}$$

$$= \#\text{ of}$$

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 $(p,p) =$ ___,

and $(x,p) =$ ___ for $\_\_ \leq x \leq \_\_$.

$\therefore$

$\phi(p) =$ ___, if p is prime.

Lemma 1 Let $a, b \in \mathbb{Z}$ s.t. $a \equiv b \pmod{m}$.

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 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, &
$(a_1, m) = (a_2, m) = \cdots = (a_n, m) =$,
then
(, m) = .

Proof: See Ex 42 pp 21-22 Chabb 1.

Euler's Theorem Let $a, m \in \mathbb{Z}$ w.r. $m \geq$;
and suppose — — — — — . Then

$$a^{\cdots} \equiv 1 \pmod{m}.$$

Proof: Let $a, m \in \mathbb{Z}$, with $m \geq 1$ & — — — — — .
The result is clearly true for $n = 1$.
Assume $m > 1$, and let

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

be the elements of the set

{ : }

NOTE (m, m)

Example (Ex 67)

$m = 16$. The set of integers x, $1 \le x \le 16$ s.t. $(x, 16) = 1$ is

$\{\ ,\ ,\ ,\ ,\ ,\ ,\ ,\ \}$.

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

Proposition Let $m \in \mathbb{Z}$ with $m \geq 1$.
Let $S = \{ x \in \mathbb{Z} : 1 \leq x \leq m \ \& \ (x, m) = 1 \}$.
Let $T = \{ x \in \mathbb{Z} : (x, m) = 1 \}$.
Every

PROOF (EX.)
NOTE: $|S| =$

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

$= \{ 1, \ , \ , \ \}$.

So
$\phi(12) = |S| =$
Let $q = 29$.
Then

Definition: Let $m \in \mathbb{Z}$, with $m \geq 1$. Any ~~set~~
of ___ integers such that _____
_____
is called a reduced residue system mod m.

Example

$\{\ ,\ ,\ ,\ \}$ is a reduced residue system mod 12.

$\{\ ,\ ,\ ,\ \}$ is also a reduced residue system mod 12 since