Lec 6, 7, 8

Complete Residue Systems (contd...)

Solution of linear congruences

Reduced residue system

Euler - Phi function

] Topics covered in these notes.

Eg 1) Note that in

$$12 \equiv 2 \pmod 5 \quad \text{— (1)}$$

we can cancel the factor 2 from both sides as

$$6 \equiv 1 \pmod 5$$

is true.

Eg 2) However, in

$$15 \equiv 45 \pmod{10}, \quad \text{— (2)}$$

we cannot cancel 15 from both sides of the congruence as

$$1 \equiv 3 \pmod{10}$$

is an incorrect statement. So, when is cancellation allowed in modular arithmetic?

Theorem 3.5

Let a & m be integers with $m > 0$.

$$ax \equiv ay \pmod m \iff x \equiv y \pmod{\frac{m}{(a,m)}}.$$

The idea from the above theorem is that one can do cancellation of 15 on either sides of (2) however with respect to a new modulus $m' = \frac{10}{(15,10)} = 2$.

ie, $1 \equiv 3 \pmod{10}$ is false however cancellation of 15 with respect to $m' = 2$ is valid.

Proof of theorem 3.5

"$\Rightarrow$" Given $ax \equiv ay \pmod{m}$. We show that $x \equiv y \pmod{\frac{m}{(a,m)}}$ is true.

Clearly, $m \mid a(x-y)$. If we let $m = m_1 d$ & $a = a_1 d$, then $m_1 d \mid a_1 d(x-y) \Rightarrow m_1 \mid a_1(x-y)$. Note that $(m_1, a_1) = 1$ & hence, $m_1 \mid x-y$.

ie, $x \equiv y \pmod{\frac{m}{(a,m)}}$.

"$\Leftarrow$" Given $m_1 \mid (x-y) \Rightarrow m_1 d \mid d(x-y)$

But $d(x-y) \mid a(x-y)$ as $d \mid a$.

By transitivity,

$m_1 d \mid a(x-y)$

ie, $m \mid a(x-y)$ or in other words

$ax \equiv ay \pmod{m}$.

Corollary 3.6

Let $(a,m) = 1$. Then,

a) $ax \equiv ay \pmod{m} \iff x \equiv y \pmod{m}$.

b) If $\{x_1, x_2, \ldots, x_m\}$ is a CRS modulo m, then

$\{ax_1, ax_2, \ldots, ax_m\}$ is also a CRS modulo m.

Proof :- a) is easily seen from Thm 3.5.

b) To show that $\{ax_1, \ldots, ax_m\}$ is a CRS modulo m, it suffices to show that any pair ax_i & ax_j are incongruent to each other modulo m.

Suppose there exist some $i \neq j$ such that

$ax_i \equiv ax_j \pmod{m}$,

by part a),

$$x_i \equiv x_j \pmod{m}$$

That is two distinct elements $x_i \& x_j$ in $\{x_1, x_2, .., x_m\}$ are congruent to each other which is impossible as it is a CRS.

Hence, no two elements ax_i & ax_j are congruent to each other & hence, the set $\{ax_1, .., ax_m\}$ is a CRS as well.

Note that since both $\{x_1, x_2, .., x_m\}$ & $\{ax_1, .., ax_m\}$ are complete residue classes modulo m, any x_i in the first CRS is congruent to exactly one ax_j modulo m.

Thus, one can reinterpret this fact in the following way. Let b be any integer in $\mathbb{Z}_m$ & $(a,m) = 1$. Then the linear congruence

$$ax \equiv b \pmod{m} \quad -(3)$$

has a unique solution modulo m.

Eg 3) The equation $5x \equiv 6 \pmod{8}$ has a unique solution $x \in \{0,1,2..,7\}$. By inspection, one can see $x = 6$ is a solution.

However, if $x = 6$ is a solution, so is $x = 6+8$ as $5(14) - 6$ is a multiple of 8. In fact, any element in the residue class of 6

ie, $\overline{6} = \{ \ldots, -2, 6, 14, 22, \ldots \}$
is also a solution.

Hence, from now onwards, when we speak of no. of solutions of a congruence equation, we shall mean the no. of incongruent solutions modulo m, ie, the no. of solutions contained in the set

$\{1, 2, 3, .., m\}$ or

any other complete residue system modulo m.

Notice that in (3), existence and uniqueness of the soln depended on a & m being co-prime.
Once the assumption $(a,m)=1$ is removed, it is not necessary that (3) has a unique soln. In fact, (3) may not have a solution at all.

In general, any linear congruence of the form

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

may have

(i) NO solutions

Eg. $2x \equiv 3 \pmod{4}$.

(ii) Unique soln.

Eg. $5x \equiv 6 \pmod{8}$

(iii) More than one (incongruent) solutions

Eg. $6x \equiv 4 \pmod{8}$.

The following theorem helps to identify the nature of solutions.

Theorem 3.7) Let $m \geq 1$, a & b be integers.

Consider the linear congruence $ax \equiv b \pmod{m}$. — (4)

i) Assume $(a,m)=d$. Then, the linear congruence in (4) has solutions iff $d \mid b$.

(ii) Assume $(a,m)=1$. Then, the linear congruence in (4) has a unique solution modulo m.

(iii) Assume $(a,m)=d$ & suppose that $d \mid b$. Then, (4) has exactly d incongruent solutions mod m.

These are given by

$$t,\ t+\frac{m}{d},\ t+2\left(\frac{m}{d}\right),\ \ldots,\ t+(d-1)\frac{m}{d}$$

where

t is the unique solution for $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Theorem 3.8)

If $(a,m)=1$, then $\exists\ x \in \mathbb{Z}$ such that

$$ax \equiv 1 \pmod{m}.$$

Proof :- By Euclidean algorithm, $\exists\ x, y \in \mathbb{Z}$ s.t

$$ax + my = 1 \Rightarrow m \mid ax-1$$

$$\Rightarrow ax \equiv 1 \pmod{m}$$

Remark :- In Theorem 3.8, x could be thought of as that element which when multiplied by a gives $1 \pmod{m}$. In this sense, x could be thought of as the inverse of a modulo m.

Defn :- If $(a,m) = 1$, then the unique soln. of the linear congruence

$$ax \equiv 1 \pmod{m}$$

is called the inverse of a modulo m.

Uniqueness is in the following sense : Any 2 integers say x_1 & x_2 which satisfy

$$ax_1 \equiv 1 \pmod{m} \quad \&$$

$$ax_2 \equiv 1 \pmod{m}$$

are congruent to each other, i.e, $x_1 \equiv x_2 \pmod{m}$.

Q1) Solve $2x \equiv 1 \pmod{5}$

$(2,5) = 1 \Rightarrow$ By Theorem 3.7 (ii), there is only one

soln modulo 5. By trial & error or inspection, we see immediately that $x=3$ is that solution.

Q2) Solve $2x \equiv 4 \pmod 5$

$\because$ $2x \equiv 1 \pmod 5$ has soln $x_0 = 3$, clearly $2(4x_0) \equiv 4 \pmod 5$. Hence, 12 is a soln modulo 5.

ie, $x = 2 \pmod 5$ is the unique soln.

Q3) Solve $4x \equiv 6 \pmod 8$

$d = (a,m) = (4,8) = 4 \quad \not| \; b = 6$

Since $d \nmid b$, there are no solutions.

Q4) Solve $4x \equiv 8 \pmod{10}$.

$d = (a,m) = (4,10) = 2$
$b = 8 \Rightarrow$ There are d solutions modulo 10.

However, by Thm 3.5, one notices that

$4x \equiv 8 \pmod{10}$ has solutions iff

$$x \equiv 2 \left(\text{mod } \frac{10}{(4,10)}\right)$$

ie, $x \equiv 2 \pmod 5$.

Hence, solutions mod 10 are exactly 2 & 7.

One can also use Thm 3.7 to solve Q4) to find the exact solutions. Notice that $d = (4,10) = 2$ & hence, the unique solution of $2x \equiv 4 \pmod 5$ is needed to be found out which is already done in Q2).
Hence, $t = 2$.

The other solution for $4x \equiv 8 \pmod{10}$ is

$$t + \frac{m}{d} = 2 + \frac{10}{2} = 7$$

I Find all solutions of the congruence

a) $20x \equiv 4 \pmod{30}$.

b) $20x \equiv 30 \pmod{4}$

c) $353x \equiv 254 \pmod{400}$

(Already done in class ! Use Euclidean algorithm to find y such that

$353y \equiv 1 \pmod{400}$. Then,

$x = 254y$ is the desired solution.).

II Solve, if there exists a solution

d) $15x \equiv 25 \pmod{35}$.

e) $15x \equiv 24 \pmod{35}$

f) $57x \equiv 87 \pmod{105}$

Reduced residue system modulo m.

(RRS mod m)

It is a set of integers r_i such that

1) $(r_i, m) = 1$

2) $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$

3) Any x co-prime to m is congruent modulo m to some member r_i of the set.

Eg. 4) $m = 12$

All the below sets are examples of RRS mod m.

$S_1 = (\mathbb{Z}_{12})^* = \{1, 5, 7, 11\}$.

$S_2 = \{13, -7, 19, -13\}$

$S_3 = \{1, 5, -5, -1\}$.

$\mathbb{Z}_m^*$ is the set of numbers $n \in \mathbb{N}$ such that

1) $1 \leq n \leq m$

2) $(n, m) = 1$.

Eg 5) Let p be a prime. Then,

$\mathbb{Z}_p^* = \{1, 2, 3, 4, 5, \ldots, p-1\}$.

Let $|\mathbb{Z}_p^*|$ or $\#(\mathbb{Z}_p^*)$ denote the cardinality of $\mathbb{Z}_p^*$

a) Then, $|\mathbb{Z}_p^*| = p-1$, as the only element n between 1 & p which is not coprime to p is $n = p$ itself.

b) $|\mathbb{Z}_{p^2}^*| = p^2 - p$.

c) More generally,

Theorem 3.9) Let p be a prime & $n \in \mathbb{N}$.

Then, $|(\mathbb{Z}_{p^n})^*| = p^n - p^{n-1}$.

Proof :-

To see this, notice that if we remove those numbers m between 1 & p^n which are not coprime to p^n, then what is left is the set $(\mathbb{Z}_{p^n})^*$.

How to count the no.s m such $1 \leq m \leq p^n$ & $(m, p^n) > 1$?

Clearly, if $(m, p^n) > 1$, then $p \mid m$ as p is the only prime factor of p^n. Hence, m can be written as

$$m = lp. \quad \text{for some } l \in \mathbb{N}$$

But,

$1 \leq lp \leq p^n$. However, it is true that

$$p \leq lp \leq p^n$$

as any non-zero positive multiple of p is atleast p. Hence,

$$1 \leq l \leq p^{n-1}.$$

Hence, there are p^{n-1} elements that are not coprime to p^n between 1 & p^n.

Hence, $|(\mathbb{Z}_{p^n})^*| = p^n - p^{n-1}$.

Euler-Phi function

Euler-Phi : $\phi(m)$ is defined as the cardinality of any reduced residue system modulo m.

$$\phi(m) = |(\mathbb{Z}_m)^*|$$

$$= \sum_{\substack{k=1 \\ (k,m)=1}}^{m} 1 .$$

m	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(m)$	1	1	2	2	4	2	6	4	6	4	10	4

Properties of Euler-Phi function

Theorem 3.10) ϕ is a multiplicative function.

That is, if $m_1, m_2 \in \mathbb{N}$ such that $(m_1, m_2) = 1$, then

$$\phi(m_1 m_2) = \phi(m_1)\,\phi(m_2).$$

Notice that if m_3 is such that $(m_1, m_2, m_3) = 1$, then,

$$\phi(m_1 m_2 m_3) = \phi(m_1)\,\phi(m_2)\,\phi(m_3).$$

Theorem 3.11) For $n \geq 1$, we have

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Here, $\prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ means:

If $p_1, \ldots, p_r$ are all distinct prime divisors of n, then

$$\prod_{p \mid n} \left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Exercise: Show that for each $n \geq 1$,

$$\phi(10^n) = 4 \cdot 10^{n-1}.$$

Euler-Fermats Theorem