Lec 8, 9, 10

These notes cover

1) reduced residue system (contd...)
2) Fermat's thm & Euler's generalisation
3) Related problems.
4) Chinese remainder theorem & problems

Ex 1) Let $m \in \mathbb{N}$ & $a, b \in \mathbb{Z}$.
If $(a,m) = (b,m) = 1$, show that $(ab, m) = 1$.

Recall Corollary 3.6 b) One could ask a similar question in the case of reduced residue systems too.

Theorem 3.5

Given a reduced residue system modulo m $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ & an integer a coprime to m (ie $(a,m) = 1$), the set (obtained after multiplication of a)

$$\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$$

is also a reduced residue system.

Proof :-

Note that if $(r_i, m) = 1$, then $(ar_i, m) = 1$ by above exercise. Further in the latter set, there are $\phi(m)$ elements. Hence, to show that

$$S = \{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$$

is a reduced residue class mod m, it suffices to show that ar_i & ar_j are incongruent mod m.
On the contrary, if for some pair (i,j) such that $1 \le i \neq j \le \phi(m)$, $ar_i \equiv ar_j \pmod m$, then clearly, $r_i \equiv r_j \pmod m$ by Theorem 3.3. However, r_i & r_j are 2 distinct elements in the former set $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ & hence are incongruent by definition. Thus, all elements of S are incongruent to each other.

Fermat Theorem & Euler's generalisation

Theorem 3.6 (Fermat's Little Theorem)

Let p denote a prime. Let a be an integer.

(i) If $p \nmid a$, then
$$a^{p-1} \equiv 1 \pmod{p}$$

(ii) Further
$$a^p \equiv a \pmod{p}$$
holds (irrespective of whether $p \mid a$ or not) for any $a \in \mathbb{Z}$.

Remark:-

Proof of part (i) will not be discussed. It comes as a consequence of Euler's generalisation which will come next.

However, to see (ii), it is very easy. Let $p \mid a$. Thus, it follows that $p \mid a(a^{p-1}-1)$. Now, notice the following equivalences.

$$p \mid a(a^{p-1}-1)$$
$$\Leftrightarrow \quad a(a^{p-1}-1) \equiv 0 \pmod{p}$$
$$\Leftrightarrow \quad a^p \equiv a \pmod{p}.$$

If $p \nmid a$, then by assuming part (i), we see that

$$p \mid a^{p-1}-1 \Rightarrow p \mid a(a^{p-1}-1)$$
$$\Updownarrow$$
$$a^p \equiv a \pmod{p}.$$

Euler's generalisation of Fermat's Little Theorem

Thm 3.7) If $(a,m)=1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof: Not part of exam. Refer Thm 2.8 Pg 51 of Niven Zuckerman.

Consider the standard reduced residue system modulo 8 namely, $(\mathbb{Z}_8)^* = \{1, 3, 5, 7\}$. Multiplying each element by 3 (or any residue of 3 mod 8 for that matter), we get a set $\{3, 9, 15, 21\}$. Further,

Elements of $(\mathbb{Z}_8)^*$: 1, 3, 5, 7

$1 \equiv 9 \pmod 8$
$3 \equiv 3 \pmod 8$
$5 \equiv 21 \pmod 8$
$7 \equiv 15 \pmod 8$

Elements of second set: 9, 3, 21, 15

Multiplying all these congruences, we get

$$1 \cdot 3 \cdot 5 \cdot 7 \equiv 9 \cdot 3 \cdot 21 \cdot 15 \pmod 8$$

$$\text{i.e., } (1 \cdot 3 \cdot 5 \cdot 7) \cdot 1 \equiv (3 \cdot 1 \cdot 7 \cdot 5) \times 3^4 \pmod 8$$

Cancelling $1 \cdot 3 \cdot 5 \cdot 7$ from both sides (use Thm 3.3 ii), we get

$$3^4 \equiv 1 \pmod 8$$

Here, $\phi(8) = 4 = |\mathbb{Z}_8^*|$.

More generally, if $(a, m) = 1$, we can do the same thing to get

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

Exercises

1) Show that $7 \mid 3^{2n+1} + 2^{n+2}$ for all $n \geq 0$.

2) Prove that a) $7 \mid n^6 - 1$ if $(n, 7) = 1$. b) Let k be any natural no. Show that $7 \mid n^{6k-1}$ if $(n, 7) = 1$

c) Show that $n^7 - n$ is divisible by 42 for any $n \in \mathbb{Z}$.

Use: $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$.

Next, we will see how Euler's thm can be used to solve diophantine equations of the form

$$ax \equiv 1 \pmod m \quad \text{where } (a, m) = 1.$$

Recall that we had already seen how to solve such equations using Euclidean algorithm. Euler's theorem gives you another way.

Theorem 3.8) If $(a,m)=1$, then the unique solution modulo m of the linear congruence

$$ax \equiv b \pmod{m} \quad — (\star)$$

is given by

$$x_0 \equiv b\, a^{\phi(m)-1} \pmod{m}.$$

Proof :-

Since $a^{\phi(m)} \equiv a \cdot a^{\phi(m)-1} \equiv 1 \pmod{m}$

if $(a,m)=1$, we see that

$x_1 = a^{\phi(m)-1}$ is the unique (why ?) solution for

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

Then, $a(x_1 b) \equiv a(b\, a^{\phi(m)-1}) \equiv b \pmod{m}$ by multiplying throughout by b. Then,

$x_0 = b\, a^{\phi(m)-1}$ is the unique soln for $(\star)$

Remark

Due to uniqueness, the solution obtained using Euclidean algorithm & Euler's thm have to be congruent mod m to each other.

Problems

① Solve $5x \equiv 3 \pmod{24}$ using
a) Euclidean algorithm b) Euler's thm.

Ans: By Euclidean algorithm or otherwise (trial & error), we see that $5 \times (5) + 24(-1) = 1$

ie, $5(5) \equiv 1 \pmod{24}$

ie, 5 is the inverse of 5 mod 24.

Then, $5 \cdot 5 \cdot 3 \equiv 3 \pmod{24}$

ie, $x_0 = 15 \pmod{24}$ is a solution for

$$5x \equiv 3 \pmod{24}.$$

Pr 2) Solve $25x \equiv 15 \pmod{120}$.

Soln :- $\gcd(25, 120) = 5$ & $5 \mid 15$

$\Rightarrow$ There are 5 incongruent soln. modulo 120.

Now, by cancellation of common factor from 25 & 15, we get by Theorem 3.5 that

$$5x \equiv 3 \pmod{\frac{120}{(5, 120)}}$$

i.e, $5x \equiv 3 \pmod{24}$ — (†)

By problem 1, soln for eqn (†) is $x_0 = 15 \pmod{24}$.

However, choices for x_0 between 1 & 120 are

$$15,\ 15+24,\ 15+2\times24,\ 15+3\times24,\ 15+4\times24$$

These are the 5 incongruent solutions modulo 120.

Pr 3) What is the

a) last digit in the decimal representation of 3^{400}?

b) last digit in the decimal representation of 2^{400}?

c) last two digits (—— " ——) of 3^{400}?

Ans:- a) Let n be any natural no. & its decimal expn is

$$n = 10^m a_m + 10^{m-1} a_{m-1} + \cdots + 10 a_1 + a_0$$
$$= 10q + r \quad \text{where } 0 \le r = a_0 < 10.$$

Thus, in question a), we have to find r.

Similarly, in b) & c), we have to find $r' = 10a_1 + a_0$

as $n = 100q' + r'$, where $0 \le r' = 10a_1 + a_0 < 100$.

By Eulers Thm, $3^{\phi(10)} \equiv 1 \pmod{10}$ & $\phi(10) = 4$

$$\Rightarrow 3^{400} \equiv 1^{100} \equiv 1 \pmod{10}$$

$\Rightarrow$ last digit of 3^{400} is 1.

c) Ill^by, last two digits of 3^{400} can be found. (Exercise).

b) Here, $(2,10) \neq 1 \Rightarrow$ Consider $n = 5$ which is a factor of 10, coprime to 2.

$$\Rightarrow 2^{\phi(10)} \equiv 1 \pmod 5$$

$$\Rightarrow 2^{400} \equiv 1^{100} \equiv 1 \pmod 5$$

$$\Rightarrow 2^{400} \equiv 1 \text{ or } 6 \pmod{10}$$

Since 2^{400} & 10 are even, $2^{400} \equiv 1 \pmod{10}$ cannot happen as $10 \mid 2^{400} - 1 \Rightarrow 1$ is even.

So, $2^{400} \equiv 6 \pmod{10}$.

Exercises from 2.1 (Niven Zuckerman)

1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 14, 15, 19, 20, 21, 22, 28
29, 30, 32, 33.

Exercises from 2.2 (Niven)

5, 6, 8

8 is a challenge question & will not be asked for mid sem exam.

Challenge questions (Not part of mid-term exam syllabus)

d) Last two digits in the decimal expansion of 2^{400}?

e) Sec 2.2 (98) Niven.

Lec 9 :- CHINESE REMAINDER THEOREM

We now consider the important problem of solving simultaneous congruences.

Sunzi (~ 3-5 CE) posed the following problem in his mathematical treatise "Sunzi Suanjing"
— meaning The mathematical classic of Master Sun (Sunzi)

"There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over & by sevens, two are left over. How many things are there ?"

His work never contained any proof or algorithm. A partial algorithm was supplied by Aryabhatta (6 CE). Further, Brahmagupta, Fibonacci & Gauss worked on these.

Chinese Remainder Theorem is a systematic algorithm to solve simultaneous linear congruences.

Theorem 4.1 Assume $m_1, m_2, \ldots, m_r$ be positive integers relative prime in pairs, ie $(m_i, m_j) = 1$ if $i \neq j$. Let $a_1, a_2, \ldots, a_r$ be arbitrary integers. Then, the system of congruences

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}\right\} \quad (\star)$$

has exactly one solution modulo $m = m_1 m_2 \ldots m_r = \prod_{i=1}^{r} m_i$.

Further, if x_0 is one such solution, then an integer x satisfies all the congruences in $(\star)$ iff $x \equiv x_0 \pmod{m}$.

Remark: If $M_i = \frac{m}{m_i}$ for each $1 \leq i \leq r$, and b_i is the (unique) inverse of M_i modulo m_i, then a solution is given by $x_0 = M_1 b_1 a_1 + M_2 b_2 a_2 + \ldots + M_r b_r a_r$.

Example 1) Find the least positive integer x such that

$$x \equiv 5 \pmod 7$$
$$x \equiv 7 \pmod{11}$$
$$x \equiv 3 \pmod{13}$$

Soln :- Following earlier notations, we have

$m_1 = 7$ $\quad a_1 = 5$

$m_2 = 11$ $\quad a_2 = 7$

$m_3 = 13$ $\quad a_3 = 3$.

$$m = m_1 m_2 m_3 = 7 \cdot 11 \cdot 13.$$

$$M_1 = \frac{m}{m_1} = 11 \cdot 13; \quad M_2 = \frac{m}{m_2} = 7 \cdot 13; \quad M_3 = \frac{m}{m_3} = 7 \cdot 11$$

b_1 : Inverse of M_1 mod m_1

To find b_1, we have to solve $M_1 x \equiv 1 \pmod{m_1}$, ie

$$11 \cdot 13 \cdot x \equiv 1 \pmod 7$$

$\because 11 \equiv 4 \pmod 7$ & $13 \equiv -1 \pmod 7$, we can rewrite the above eqn as $-4x \equiv 1 \pmod 7$ which is further same as solving $3x \equiv 1 \pmod 7$

$\Rightarrow$ Soln is $5 \pmod 7$

$$\Rightarrow b_1 \equiv 5 \pmod 7.$$

III^{ly}, by solving $7 \cdot 13 x \equiv 1 \pmod{11}$, we get $7 \cdot 13 \equiv 7 \cdot 2 \equiv 3 \pmod{11} \Rightarrow 3x \equiv 1 \pmod{11}$ has soln. $b_2 \equiv 4 \pmod{11}$.

III^{ly}, $b_3 = -1 \,(13)$. Thus, a soln $x_0 = \sum_{i=1}^{3} M_i b_i a_i$

$$= 11 \cdot 13 \cdot 5 \cdot 5 + 7 \cdot 13 \cdot 4 \cdot 7 + 7 \cdot 11 \cdot (-1) \cdot 3 = 5892$$

is found. To get the least, take $5892 \pmod{7 \cdot 11 \cdot 13}$ to get

$$x_0 \equiv 887 \pmod{7 \times 11 \times 13}$$

Note that if we remove the hypothesis that modulus m_i-s are relatively prime (pairwise), then the existence of a soln of the simultaneous system (A) is no longer guaranteed. For example:

Eg. Show that there is no x for which both

$$x \equiv 29 \pmod{52} \quad \text{and}$$
$$x \equiv 19 \pmod{72}. \quad \text{holds.}$$

Facts :- 1) If x_0 is a solution for both the following congruences

$$x \equiv a \pmod{m_1} \quad \&$$
$$x \equiv a \pmod{m_2},$$

where $(m_1, m_2) = 1$, then, x_0 is a soln. for

$$x \equiv a \pmod{m_1 m_2}.$$

2) If x_0 is a solution for the congruence $x \equiv a \pmod{m_1 m_2}$, then, x_0 is a solution for the simultaneous congruences

$$x \equiv a \pmod{m_1}$$
$$x \equiv a \pmod{m_2}$$

Here, we don't need $(m_1, m_2) = 1$.

Soln. for above example

Let x_0 be a soln for $x \equiv 29 \pmod{52}$, then it is also a soln. for $x \equiv 29 \equiv 3 \pmod{13}$ & $x \equiv 29 \equiv 1 \pmod{4}$

ie, $x_0 \equiv 1 \pmod{4}$ & $x_0 \equiv 3 \pmod{13}$. — (1)

Further if x_0 is a soln for $x \equiv 19 \pmod{72}$, then

$$x_0 \equiv 19 \equiv 1 \pmod{18} \quad \& \quad x_0 \equiv 19 \equiv 3 \pmod{4} \quad — (2)$$

To arrive at (1) & (2), we used Fact 2) above.

Thus, $x_0 \equiv 1 \pmod 4$ as well as $x_0 \equiv 3 \pmod 4$.
Thus, such an x_0 cannot exist.

Remark :-
One could also work with $72 = 9 \times 8$ & arrive at a contradiction.

Exercise Determine whether the system

$$x \equiv 3 \pmod{10}$$
$$x \equiv 8 \pmod{15}$$
$$x \equiv 5 \pmod{84}$$

has a solution & if so, how many modulo 420.

Simultaneous systems of congruence (linear) that have no soln. are sometimes called inconsistent.

Exercises

1) Solve $x \equiv 6 \pmod{11}$
$x \equiv 13 \pmod{16}$
$x \equiv 9 \pmod{21}$
$x \equiv 19 \pmod{25}$, $1 \le x \le 11 \cdot 16 \cdot 21, 25$

2) Section 2.3 Problems
1, 2, 3, 4,