Math 312, Lecture 8, 25/5/2018

Last time: linear equations:

(1) $a + (-a) \equiv 0 \ (m)$

(specifically, $a + (m-a) \equiv 0 \ (m)$)

(2) If $(a, m) = 1$, have $\bar{a}$ s.t. $a \cdot \bar{a} \equiv 1 \ (m)$

("modular inverse") - divide by a using $\bar{a}$.

(If $(a,m) = d > 1$, then $a \cdot \frac{m}{d} \equiv 0 \ (m)$ so a can't be invertible)

Eg. $2 \cdot 4 = 8 \equiv 1 \ (7)$ so $2, 4$ are inverse to each other mod 7.

(3) let $d = \gcd(a, m)$. Consider equation $ax \equiv b \ (m)$.

If $d = 1$, a is invertible always have a unique solution mod m ($x \equiv \bar{a}b$ (mod m))

unique class

If $d > 1$, $d \nmid b$, no solutions at all

If $d > 1$, $d \mid b$, $ax \equiv b \ (m) \iff \frac{a}{d} \cdot x \equiv \frac{b}{d} \ \left(\frac{m}{d}\right)$

now $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ (PS2) so unique solution mod $\frac{m}{d}$, splits into $\underline{d}$ solutions mod m.

Today

(1) Several variables

(2) ~~Multiple~~ ~~a~~ Simultaneous congruence & the Chinese Remainder Theorem

---

Example: Solve

$$\begin{cases} 5x + 2y \equiv 3 \\ 2x + 7y \equiv 5 \end{cases} \quad (12)$$

certainly, $5x+2y \equiv 3 \ (12) \iff 2y \equiv 3-5x \ (12)$

but "$y = \frac{3-5x}{2}$" doesn't make sense: 2 not invertible mod 12 ($\gcd(2,12) = 2 > 1$)..

Instead, $5 \cdot 5 = 25 = 24+1 \equiv 1 \ (12)$ so let's multiply 1st eqn. by 5: if (x,y) is a solution get:

$$5 \cdot 5x + 5 \cdot 2y \equiv 3 \cdot 5$$

$3 \cdot 5 = 15 \equiv 3 \ (12)$

$$x + 10y \equiv 3 \quad (12)$$

add

$$2x + 7y \equiv 5 \quad (12)$$

subtracting twice 1st eqn from 2nd get

$$(7-20)y \equiv 5-6 \quad (12)$$

$7-20 = -13 \equiv -1 \ (12)$

i.e. $-y \equiv -1 \ (12)$ so $y \equiv 1 \ (12)$

then $x \equiv 3 - 10y \equiv 3 - 10 \equiv -7 \equiv 5 \quad (12)$

Conversely, $5\cdot 5+2\cdot 1=25+2\equiv 1+2\equiv 3\ (12)$ ✓

$2\cdot 5+7\cdot 1=17=12+5\equiv 5\ (12)$ ✓.

<u>Aside:</u> $\det\begin{pmatrix}5 & 2\\ 2 & 7\end{pmatrix}=31\equiv 7\ (12)$ is invertible, mod 12

so our matrix is invertible must have a unique solution

<u>Observe:</u> If p is prime, any $1\le a<p$ is prime to p.

So <u>mod p</u>, a is invertible <u>iff</u> $a\not\equiv 0\ (p)$

(say: integers mod p form a "field")

(If m is composite, $m=a\cdot b$, $1<a,b<m$, then $ab\equiv 0\ (m)$

so ~~neithe~~ ~~niether~~ neither is invertible)

Different pf: Let $a\in\mathbb{Z}$. If $p\nmid a$ then $(a,p)=1$

(gcd (a,p) must divide p, so it's either 1 or p)

So a is invertible mod p

Pf above: Let $a\in\mathbb{Z}$ suppose $a\not\equiv 0\ (p)$. Then $a\equiv r\ (p)$

with $0\le r<p$ (division thm). But $r\not\equiv 0$ $(p\nmid a)$

so $1\le r<p$. So ~~p~~ r is prime to p and hence invertible

Consider solving $x^2 \equiv 1 \ (35)$ from pov of solving

$$35 \mid x^2-1 \iff 5\cdot 7 \mid (x-1)(x+1)$$

Now either, $5\cdot 7 \mid x-1$ then $x \equiv 1 \ (35)$

or $5\cdot 7 \mid x+1$ then $x \equiv -1 \ (35)$

or $5 \mid x-1,\ 7 \mid x+1$ then $x \equiv 6 \ (35)$

or $7 \mid x-1,\ 5 \mid x+1$ then $x \equiv -6 \ (35)$

One view: solving $x^2-1 \equiv 0 \ (35)$ same as separately solving $x_5^2-1 \equiv 0 \ (5)$

$x_7^2-1 \equiv 0 \ (7)$

then for any solution (x_5, x_7) we get a solution x_{35}. mod 35

Another view: Can find x s.t. at the same time:

$$x \equiv 1 \ (5) \text{ and } x \equiv -1 \ (7)$$

then $x^2 \equiv 1 \ (5)$ and $x^2 \equiv 1 \ (7)$ so x^2-1 is divisible by 5, and by 7 hence by 35.

Note: Equation $x \equiv 1 \ (5)$ has 7 solutions mod 35:

1, 6, 11, 16, 21, 26, 31

Equation $x \equiv -1 \ (7)$ has 5 solutions mod 35

$-1, -8, -15, -22, -29$

34, 27, 20, 13, 6

The Chinese Remainder Thm

(putting together information from different moduli).

~~Solve~~ Motivation

Solve $x^2 \equiv 1 \ (7)$:

7 is prime

(1) note $7 \mid x^2-1$ iff $7 \mid (x-1)(x+1)$ iff $7 \mid x-1$ or $7 \mid x+1$

iff $x \equiv 1$ or $x \equiv -1 \ (7)$

(2) Different view: have $(x-1)(x+1) \equiv 0 \ (7)$

either $x \equiv 1 \ (7)$ or $x-1 \not\equiv 0 \ (7)$. In the second case, $x-1$ is invertible, so can divide by it

get $x+1 \equiv 0 \ (7)$, i.e. $x \equiv -1 \ (7)$

works for any prime p, shows: polynomial of degree d has at most d roots mod p, <u>if p is prime</u>

What about non-prime moduli?

<u>Examples</u>: (1) If x is odd, $x^2 \equiv 1 \ (4)$ even $x^2 \equiv 1 \ (8)$

(squaring is finicky mod powers of 2)

(2) $6^2 = 36 \equiv 1 \ (35)$, i.e. $x \equiv 6 \ (35)$ solves $x^2 \equiv 1 \ (35)$

but $6 \not\equiv \pm 1 \ (35)$

In fact, the solutions are $\pm 1, \pm 6$ mod 35.

Two interpretations:

(1) The set of integers $\{x \mid x \in \mathbb{Z} \mid x \equiv 1 \ (5)\}$

$$= \{1, 6, 11, 16, \ldots, -4, -9, \ldots\} = \{1+5k\}_{k\in\mathbb{Z}}$$

breaks up as the union of the sets:

$$\{1+35k\}_{k\in\mathbb{Z}} \cup \{6+35k\}_{k\in\mathbb{Z}} \cup \ \ldots \ \cup \{31+35k\}_{k\in\mathbb{Z}}$$

(2) Among the residue classes mod 35, the classes of $1, 6, 11, \ldots, 31$ are $\equiv 1 \ (5)$

warning for 2nd pov: if $m' \mid m$ makes sense to take a mod m ask about class of a mod m'.

If $m' \nmid m$ it doesn't make sense.

Theorem: Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime. Let $M = \prod_i m_i$. Let $\{a_i\}_{i=1}^{r} \subset \mathbb{Z}$ (really, a_i are classes mod m_i)

Then: (1) there is $a \in \mathbb{Z}$ s.t. $a \equiv a_i \pmod{m_i}$ for each i.

(2) a is unique mod M.

(3) (Cor) this respects arithmetic

Proof for $m_1 = 5$, $m_2 = 7$, $M = 5 \cdot 7 = 35$.

<u>Informally</u>: $\left\{ \begin{matrix} \text{classes} \\ \text{mod } 35 \end{matrix} \right\} \cong \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} : \begin{matrix} a_1 \text{ mod } 5 \\ a_2 \text{ mod } 7 \end{matrix} \right\}$

① Look for "basis": find class b_1 s.t. $\begin{cases} b_1 \equiv 1 \ (5) \\ b_1 \equiv 0 \ (7) \end{cases}$

class b_2: $\begin{cases} b_2 \equiv 0 \ (5) \\ b_2 \equiv 1 \ (7) \end{cases}$

implicit unknown

<u>How to find b_1</u>: Say $b_1 = 7x$ want $7x + 5y = 1$

$\gcd(5,7) = 1$ so x, y exist, e.g. $2 = 7 - 5$

$1 = 5 - 2 \cdot 2 = 3 \cdot 5 - 2 \cdot 7$

so $x = -2$ works, i.e. $7x = -14 \equiv 21 \ (35)$

i.e. take $b_1 = 21$

From $3 \cdot 5 + (-2) \cdot 7 = 1$ also get $b_2 = 15$ then

$$\begin{cases} b_2 \equiv 0 \ (5) \\ b_2 \equiv 1 \ (7) \end{cases}$$

In general "$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$".

So given a_1, a_2 consider $a = a_1 b_1 + a_2 b_2$.

$= 21 a_1 + 15 a_2$

Then $a \equiv 1 \cdot a_1 + 0 \cdot a_2 \equiv a_1 \ (5)$

$a \equiv 0 \cdot a_1 + 1 \cdot a_2 \equiv a_2 \ (7)$ ✓

E.g. If we want $x \equiv 1 \ (5)$
$x \equiv -1 \ (7)$

take $x = 21 \cdot 1 + 15 \cdot (-1) = 6$

Pf for $r = 2$

Given m_1, m_2, choose x_1, x_2 s.t. $m_1 x_1 + m_2 x_2 = 1$

gcd $(m_1, m_2) = 1$, so can do this.

Set $b_1 = m_2 x_2$, $b_2 = m_1 x_1$

~~Then $b_1 \equiv 1$~~

Given a_1, a_2 set $a = a_1 b_1 + a_2 b_2$

Then mod m_1, $b_1 \equiv 1$ $b_2 \equiv 0$, $a \equiv a_1$

mod m_2, $b_1 \equiv 0$, $b_1 \equiv 1$, $a \equiv a_2$ ✓

a is unique mod $M = m_1 m_2$: If a' also works, then $a - a' \equiv 0 \ (m_1)$
$a - a' \equiv 0 \ (m_2)$

so $a - a'$ is divisible by m_1 & by m_2.

But $(m_1, m_2) = 1$ so $\operatorname{lcm}(m_1, m_2) = \dfrac{m_1 m_2}{(m_1, m_2)} = m_1 m_2$

so $M \mid a - a'$, ie $a \equiv a' \ (M)$