4.2 - Linear Congruences I

Equations mod m

Any integer eqn. can become an eqn. mod m

Ex: $6x+3=7 \longrightarrow$ $6x+3 \equiv 7 \mod 4$
$6x+3 \equiv 7 \mod 5$
$6x+3 \equiv 7 \mod 6$

Ex: $x^2+2x+1=0 \rightarrow x^2+2x+1 \equiv 0 \mod 2$

Non ex: $e^x = e^3 \not\longrightarrow e^x \equiv e^3 \mod m$

Lesson: Having int. solns. $\not\Longleftrightarrow$ an eqn. can become modular

Q. Relationship between solutions in $\mathbb{Z}$ and solns. mod m?

Note: $6x+3=7$ has no soln. in $\mathbb{Z}$

$6x+3 \equiv 7 \mod 4 \leftrightarrow 6x \equiv 4 \mod 4$
$(4 \equiv 0 \mod 4) \leftrightarrow 6x \equiv 0 \mod 4$

$\leftarrow \quad x = 2$

also

$x = 0$

$\frac{6x}{2} \equiv \frac{0}{2}$

Observe $2 \not\equiv 0 \mod 4$ $\quad \mod \frac{4}{2}$

Lesson: eqns. can have no solns. in $\mathbb{Z}$, yet multiple solns. mod m $\quad 3x \equiv 0 \mod 2$

Lesson: linear eqns. can have multiple noncongruent solns. mod m.

Ex: $x^2 + 2x + 1 = 0$ has a soln. in $\mathbb{Z}$

$x = -1$

Notice this gives a soln. mod m for every m

$x^2 + 2x + 1 \equiv 0 \mod m$

and we try $x = -1$, we get

$0 \equiv 0 \mod m$ ✓

Lesson: if an eqn. has a soln. in $\mathbb{Z}$, then it has a soln. mod m.

Goal: Solve linear eqns. mod m

$$ax + b \equiv c \mod m$$

$$\updownarrow$$

$$ax \equiv c - b \mod m$$

all we're going to focus on $ax \equiv r \mod m$

Ex: $6x \equiv 9 \mod 15$

Goal: "divide by 6"

Recall: if $ac \equiv bc \mod m$, then

$$a \equiv b \mod \frac{m}{(m,c)}$$

Note: we can't use this thm to divide by 6 b/c 9 is not div. by 6

$6x \equiv 9 \mod 15 \iff \exists k \in \mathbb{Z} : 6x - 9 = 15k$

$6x - 15k = 9$

Observe: $6x - 15k = 9$ is a lin. Diophantine equ. in two vars.

(1) Find a particular soln
- use Euclidean alg.
- inspection: $6 \cdot 4 - 15 \cdot 1 = 9$

$x_0 = 4 \quad k_0 = 1$

(2) generalize: $x = 4 + \frac{15}{(6,15)} n = 4 + 5n$

$k = 1 + \frac{6}{(6,15)} n = 1 + 2n$

$6x \equiv 9 \mod 15 \quad | \quad x = 4 + 5n$

$n = 0 \to x = 4 \to 6 \cdot 4 = 24 \equiv 9 \mod 15$ ✓

$n = 1 \to x = 9 \to 6 \cdot 9 = 54 \equiv 9 \mod 15$ ✓

$n = 2 \to x = 14$ - — — — — ✓

$n = 3 \to x = 19$ - — — — — ✓

Q: Why do we know that $x = 19$ is soln w/o needing to compute $6 \cdot 19$?

Note $19 \equiv 4 \mod 15$

So $6 \cdot 19 \equiv 6 \cdot 4 \mod 15$ (bc 4 is a soln.)

$\equiv 9 \mod 15$

Fact: If x_0 is a soln to $ax \equiv b \mod m$,
then so is $x_0 + mk$ for any k

Pf: Note $a(x_0 + mk) = ax_0 + amk$

$\equiv 0 \mod m$

$\equiv ax_0 \mod m$

$\equiv b \mod m$

But not every soln. looks like $x_0 + mk$

For $6x \equiv 9 \mod 15$

$x = 4$ and $x = 9$ worked.

Q: How many solns. are there to
$ax \equiv b \mod m$ and how can
we classify them?

Since if x_0 is a soln. $x_0 + mk$ is a soln.

we count $\ldots, x_0 - m, x_0, x_0 + m, x_0 + 2m, \ldots$
as the same soln.

Thm: Let $a, b, m \in \mathbb{Z}$ with $m > 0$. If $(a, b) \nmid m$, then $ax \equiv b \bmod m$ has no solns. If $(a, b) \mid m$, then $ax \equiv b \bmod m$ has (a, m) incongruent solns. $(\bmod m)$.

↳ i.e. (a, m) distinct classes of solns. mod m

Recall $6x \equiv 9 \bmod 15$
$a \quad b \quad m$

Note: $(a, b) = (6, 9) = 3 \mid 15 = m$ ✓

$(6, 15) = 3$ solns. mod 15

$x \equiv 4, 9, 14 \bmod 15$

Pf: $ax \equiv b \bmod m$

$\leftrightarrow \exists y \in \mathbb{Z}: \quad ax - b = my$

$ax - my = b$

If $(a,m) \nmid b$, no solns.

If $(a,m) \mid b$, then $\exists\, x_0, y_0 \in \mathbb{Z}$

s.t. $ax_0 - my_0 = b$

Moreover, every soln. looks like

$$x = x_0 + \frac{m}{(a,m)} k$$

for some

$$y = y_0 + \frac{a}{(a,m)} k \qquad k \in \mathbb{Z}$$

$$\{a_1 m : x_0,\ x_0 + \frac{m}{(a,m)},\ x_0 + 2\frac{m}{(a,m)},$$

$$\ldots,\ x_0 + \left\{(a,m) - 1\right\} \frac{m}{(a,m)}$$

are all distinct mod m

i.e. $x_0 + k \cdot \frac{m}{(a,m)}$ are distinct mod m

when $0 \le k < (a,m)$

Suppose $x_0 + k \cdot \frac{a}{(a,n)} \equiv x_0 + j \frac{a}{(a,n)} \pmod{n}$

for $0 \le k, j < (a, n)$

Goal: show $k = j$

$\rightarrow$ $k \frac{a}{(a,n)} \equiv j \cdot \frac{a}{(a,n)} \pmod{n}$

Note. $\frac{n}{(a,n)} \mid n$

$3x \equiv 6 \pmod{9}$

$x \equiv 2 \pmod{3}$

div thm. $k \equiv j \pmod{\frac{n}{\left(\frac{n}{(a,n)}\right)}}$

$\rightarrow$ $k \equiv j \pmod{(a,n)}$

Recall $0 \le k, j < (a, n)$

So $k = j$

By contra positive. if $k \neq j$,

then $x_0 + k \cdot \frac{m}{(a,m)} \not\equiv x_0 + j\frac{m}{(a,m)}$

mod m

Since $0 \leq k < (a,m)$. There

are (a,m) such numbers

of the form $x_0 + k \cdot \frac{m}{(a,m)}$

and hence, (a,m) distinct

solns. mod m

Special Case: Inverses

By prev. thm, $ax \equiv 1 \mod m$ has a unique soln. iff $(a, m) = 1$

Morally, this soln is "$\frac{1}{a}$" or "a^{-1}"

Ex: $7 \cdot 5 \equiv 1 \mod 34$

5 is the inverse of 7 mod 34 and vice versa

Ex: $7x \equiv 12 \mod 34$ has ! soln. b/c $(7, 34) = 1$

unique

Eg. $\exists!$ x s.t. ....

We can use the inverse of 7 to solve.

$7x \equiv 12 \mod 34$

$$\rightarrow \quad 5 \cdot 7 \cdot x \equiv 5 \cdot 12 \mod 34$$

$$1 \cdot x \equiv 26$$

* Every number which is rel. prime to m has an inverse mod m *

Suppose m is prime.

Then every $a \in \mathbb{Z}$ with $0 < a < m$

is rel. prime to m

* Every $a \neq 0$ has an inverse mod m *

Cor. $\mathbb{Z}/p\mathbb{Z}$ is a field