Solving Congruences

Suppose we wanted to solve

① $3x \equiv 7 \pmod{10}$

② $6x \equiv 7 \pmod{10}$

③ $6x \equiv 8 \pmod{10}$

① $3x \equiv 7 \pmod{10}$

morally, want to "divide" by 3 $\pmod{10}$

i.e. we want some s such that $3s \equiv 1 \pmod{10}$

notice that $3 \cdot 7 = 21 \equiv 1 \pmod{10}$

mult. by 7 to get

$21x \equiv 7 \cdot 9 \pmod{10}$

$1 \cdot x \equiv 9 \pmod{10}$

check: $3 \cdot 9 = 27 \equiv 7 \pmod{10}$ ✓

$7, 17, \underline{27}, 37$

$\downarrow$

9

(2) $6x \equiv 7 \pmod{10}$

never going to work:
$6x - 7$ is not a multiple of 10,
because it's not even a multiple of 2!

(3) $6x \equiv 8 \pmod{10}$

$6x - 8$ is a mult. of 10
if and only if $3x - 4$ is a mult. of 5

so this is the same as solving

$3x \equiv 4 \pmod{5}$ ⟩ mult. by 2
$6x \equiv 8 \pmod{5}$
$1x \equiv 3 \pmod{5}$

if you want to go back to mod 10:

$x \equiv 3$ or $8 \pmod{10}$

check: $6 \cdot 3 = 18 \equiv 8 \pmod{10}$
$6 \cdot 8 = 48 \equiv 8 \pmod{10}$

Theorem: (1) If $\gcd(c, m) = 1$ then we can solve

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

for any b.
The sol. is unique mod m.

$3x \equiv 7 \pmod{10}$

(2) If $\gcd(c, m) = d > 1$ then we can solve

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

iff $d \mid b$.

$6x \equiv 7 \pmod{10}$
$6x \equiv 8$

Then it's equiv. to solving

$$\frac{c}{d} x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d} \right)$$

Proof (1) Since $\gcd(c, m) = 1$,
we can write $cs + mt = 1$
for some $s, t \in \mathbb{Z}$.

Multiply by b to get

$$csb + mtb = b$$

Then if we take $x = sb$,

$$cx + mtb = b$$

so $cx \equiv b \pmod{m}$

Suppose we have two solutions

$cx \equiv 6 \pmod m$

and $cy \equiv 6 \pmod m$

then $cx - cy \equiv 0 \pmod m$

i.e. $m \mid cx - cy = c(x-y)$

because $\gcd(m, c) = 1$,
we must have $m \mid x-y$ { WHY?

i.e $x \equiv y \pmod m$

example
if $10 \mid 3z$
then $10 \mid z$

let $z = x - y$
if $\gcd(m, c) = 1$
and $m \mid cz$ then $m \mid z$

again write $1 = cs + mt$

so $z = csz + mtz$

m divides cz

m divides this too

so m divides z.

(2) if $\gcd(c, m) = d$
then write $c = dc'$
and $m = dm'$
where now $\gcd(c', m') = 1$

$6 = 2 \cdot 3$
$10 = 2 \cdot 5$

Solving $cx \equiv b \pmod{m}$

or $c'dx \equiv b \pmod{m'd}$

or $c'dx - b = m'd \cdot k$ for some k.

then $b = c'dx - m'dk$

had better be a mult. of d

if it is, divide by d

$$c'x - \frac{b}{d} = m'k$$

which is the same as

$$c'x \equiv \frac{b}{d} \pmod{m'}$$

(could have defined $b' = b/d$ ...)

Chinese Remainder Theorem

Example: Nick was going to put his class into breakout rooms of 4 but there was one student left over. So then he did rooms of 3, and there were 2 left over, which was better. What can we say?

want to solve $x \equiv 1 \pmod{4}$

and $x \equiv 2 \pmod{3}$

answer can only be up to mults. of 12...

x:	0	1	2	3	4	5	6	7	8	9	10	11
mod 4:	0	1	2	3	0	1	2	3	0	1	2	3
mod 3:	0	1	2	0	1	2	0	1	2	0	1	2

we must have $x \equiv 5 \pmod{12}$

So $x = 5, 17, 29, 41, \ldots$

(most reasonable...)

for bigger numbers:

$x \equiv 41 \pmod 5$

$x \equiv 2 \pmod 9$

don't want to list $0, 1, \ldots, 45$ and solve by brute force.

How can we be more systematic?

next time.