Last time: solving $cx \equiv b \pmod{m}$

need to find s such that $cs \equiv 1 \pmod{m}$
then multiply through

$419x \equiv 4000 \pmod{999}$ from worksheet

$49x \equiv 4 \pmod{999}$

could solve $7y \equiv 2 \pmod{999}$
and then take $x \equiv y^2 \ldots$

Bézout

in fact $571 \cdot 7 \equiv 1 \pmod{999}$

where did this come from?

$y \equiv 571 \cdot 2 \equiv 1142 \equiv 143 \pmod{99}$

$x \equiv y^2 \equiv 20449 \equiv 469 \pmod{999}$

Run Euclidean algorithm on 7 and 999

142
$7 \overline{)999}$
7
29
28
19
14
5

$5 = 999 - 142 \cdot 7$

1
$5 \overline{)7}$
5
2

$2 = 7 - 5$
$= 7 - 999 + 142 \cdot 7$
$= 143 \cdot 7 - 999$

$$\begin{array}{r} 2 \\ 2\overline{)5} \\ \underline{4} \\ 1 \end{array}$$

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

$$= 999 - 142\cdot 7 - 286\cdot 7 + 2\cdot 999$$

$$= 3\cdot 999 - 428\cdot 7$$

So $-428\cdot 7 \equiv 1 \pmod{999}$

or $571\cdot 7 \equiv 1 \pmod{999}$

Chinese Remainder Theorem.

Example: 5 kids split a big bag of M+Ms.

divide evenly w/ 4 left over.

4 more kids join them.
re-divide the bag w/ 2 left over.

What can we say?
let x = # of M+Ms.

$x \equiv 4 \pmod{5}$ and $x \equiv 2 \pmod{9}$

know that $\gcd(5, 9) = 1$

$1 = 2\cdot 5 - 9$ what if we wrote $1 = 4\cdot 9 - 7\cdot 5$

multiply by 2:

$$2 = 4\cdot 5 - 2\cdot 9$$

so $4\cdot 5 = 20 \equiv 2 \mod 9$

and $\equiv 0 \mod 5$

multiply by 4:

$$4 = 8\cdot 5 - 4\cdot 9$$

so $-4\cdot 9 = -36 \equiv 4 \mod 5$

and $\equiv 0 \mod 9$

add them up: $20 - 36 = -16 \equiv 29 \mod 45$

get $74 \equiv 29 \pmod{45}$

$29 \equiv 4 \pmod 5$ $\quad$ $29 \equiv 2 \pmod 9$

Theorem:

the equations $x \equiv a \pmod m$

$x \equiv b \pmod n$

have a common sol. if $\gcd(m,n) = 1$

sol. is unique $\pmod{mn}$

Pf. because $\gcd(m,n) = 1$, we can write

$ms + nt = 1$ some $s, t \in \mathbb{Z}$.

then $x = bms + ant$ does the job?

$x \equiv ant \equiv a \cdot 1 \pmod m$

$x \equiv bms \equiv b \cdot 1 \pmod n$

uniqueness: if $y \equiv a \pmod m$
and $y \equiv b \pmod n$
is another sol.

then $x \equiv y \mod m$ and $\mod n$

$m \mid y - x$ and $n \mid y - x$

So $mn \mid y - x$ because $\gcd(m,n) = 1$
like on Wednesday.

So $y \equiv x \pmod{mn}$.