Last time: solving \( cx \equiv 6 \pmod{m} \)

need to find \( s \) such that \( cs \equiv 1 \pmod{m} \)

then multiply through

\[ 49x \equiv 4000 \pmod{999} \] from worksheet

\[ 49x \equiv 41 \pmod{999} \]

could solve \( 7y \equiv 2 \pmod{999} \)

and then take \( x = y^2 \ldots \)

\[ \text{[Bézout]} \]

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

where did this come from?

\[ y \equiv 571 \cdot 2 \equiv 1142 \equiv 143 \pmod{999} \]

\[ x \equiv y^2 \equiv 20449 \equiv 4169 \pmod{999} \]

Run Euclidean algorithm on 7 and 999

\[
\begin{array}{c|cc}
7 & 142 & 5 \\
\hline
999 & 999 & 0 \\
7 & 7 & 1 \\
27 & 27 & 0 \\
19 & 19 & 5 \\
14 & 14 & 2 \\
5 & 5 & 2 \\
2 & 2 & 0 \\
\end{array}
\]

5 = 999 - 142 \cdot 7

2 = 7 - 5

5 = 7 - 999 + 142 \cdot 7

2 = 143 \cdot 7 - 999
\[
\sqrt{\frac{5}{4}} = \frac{1}{2} = 2.2
\]

\[
\frac{1}{2} = 997 - 142.7 - 286.7 + 2.999 = 3.999 - 428.7
\]

so 

\[
-428.7 \equiv 1 \pmod{999}
\]

or 

\[
571.3 \equiv 1 \pmod{999}
\]

Chinese Remainder Theorem.

Example: 5 kids split a big bag of M+Ms. divide evenly w/ 1 left over. 4 more kids join them. re-divide the bag w/ 2 left over.

What can we say?

Let \( x \equiv \# \) of M+Ms.

\[
x \equiv 1 \pmod{5} \quad \text{and} \quad x \equiv 2 \pmod{9}
\]

Know that \( \gcd(5, 9) = 1 \)

\[1 = 2 \cdot 5 - 9 \quad \text{what if we wrote} \quad 1 = 4 \cdot 9 - 7 \cdot 5\]
multiply by 2:

\[ 2 = 4.5 - 2.9 \]
so \[ 4.5 = 20 \equiv 2 \mod 9 \]
and \[ 20 \equiv 0 \mod 5 \]

multiply by 4:

\[ 4 = 6.5 - 4.9 \]
so \[ -4.9 = 36 \equiv 0 \mod 5 \]
and \[ 36 \equiv 0 \mod 9 \]

add them up: \[ 20 - 3k = -16 \equiv 29 \mod 45 \]
get \[ 74 = 29 \pmod{45} \]
\[ 29 \equiv 4 \pmod{1} \]
\[ 29 \equiv 2 \pmod{9} \]

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 \( x = bms +antt \) does the job?

\[ x \equiv bms \equiv a \cdot 1 \pmod{m} \]
\[ x \equiv bms \equiv b \cdot 1 \pmod{n} \]
Uniqueness: if \( y \equiv a \pmod{mn} \) and \( y \equiv b \pmod{n} \)

is another sol.

Then \( x \equiv y \pmod{m} \) and \( x \equiv y \pmod{n} \)

\( m \mid y - x \) and \( n \mid y - x \)

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

So \( y \equiv x \pmod{mn} \).