we can still solve equations

e.g. \( x^2 + 3x + 2 \equiv 0 \pmod{5} \)

<table>
<thead>
<tr>
<th>x</th>
<th>get</th>
<th>solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2 \equiv 2 \pmod{5}</td>
<td>NO</td>
</tr>
<tr>
<td>1</td>
<td>6 \equiv 1 \pmod{5}</td>
<td>NO</td>
</tr>
<tr>
<td>2</td>
<td>12 \equiv 2 \pmod{5}</td>
<td>NO</td>
</tr>
<tr>
<td>3</td>
<td>20 \equiv 0 \pmod{5}</td>
<td>YES</td>
</tr>
<tr>
<td>4</td>
<td>30 \equiv 0 \pmod{5}</td>
<td>YES</td>
</tr>
</tbody>
</table>
mostly what we want are sots
to
\[ a \times x \equiv c \mod m \]

sometimes lots of solutions

eq.
\[ 4x \equiv 8 \mod 16 \]
sol. \[ 2, 6, 10, 14 \]

\[ a = 4, \ c = 8 \]
\[ m = 16 \]
\[ g = gcd(4, 16) = 4 \]

so 4 solutions
Some time exactly one solution.

\[ a = 3, \ c = 1, \ m = 7 \]
\[ g = \gcd (3, 7) = 1 \]
So 1 solution

\[ 3x = 1 \mod 7 \]

\[ x = 5 \text{ is the solution (only)} \]

because
\[ 3 \cdot 5 = 15 = 1 \mod 7 \]

since
\[ 15 = 2 \cdot 7 + 1 \]
Theorem:
\[a, c, m \in \mathbb{Z}, \ m \geq 1,\]
\[g = \gcd(a, m)\]

if \( g \nmid c \) then \( \text{no solutions to } ax = c \mod m \)

if \( g \mid c \) then \( g \) solutions to \( ax = c \mod m \)
Proof:
\[ ax \equiv c \mod m \quad g = g \left( d \left( \frac{a}{m} \right) \right) \]

Case 1, suppose \( g \nmid C \)

and \( \text{BWOC} \), suppose \( \exists \) a solution \( S \), so that \( a \cdot S \equiv C \mod m \)

\[ \Rightarrow m \mid aS - C \Rightarrow aS - C = km \quad \text{for some } K. \]

\[ \Rightarrow aS - km = C \]

but \( g \mid aS - km \) since \( g \mid a \) and \( g \mid m \)

\[ \Rightarrow g \mid C \quad \Rightarrow \text{since } g \nmid C \]

\[ \therefore \text{NO solutions.} \]
\[ 3x = 4 \mod 12 \]

\[ a = 3, \quad c = 4, \quad m = 12 \]

\[ g = \gcd(3, 12) = 3 \]

\[ 3 \times 4, \text{ so no solutions.} \]
Case 2: suppose \( g|C \).

If \( g|C \), so \( C = kg \) for some \( k \).

Also since \( g = g_l(g, m) \), \( \frac{u_0}{v_0} \) is the

\[ au_0 + mv_0 = g \]

so \( ak u_0 + m k v_0 = kg = C \)

\[ \Rightarrow ak u_0 - C = m \cdot k v_0 \]

i.e. \( m|ak u_0 - C \)

so \( ak u_0 = C \mod m \)

\[ \Rightarrow k u_0 \text{ is a solution.} \]
other solutions? let $x_0 = k x_0$,

say: $a \; x_1 \equiv c \pmod{m}$, so

$$m \mid a_1 - c,$$

but $a x_1 \equiv c = a x_0 \pmod{m}$, so

$$m \mid a x_1 - a x_0,$$

$$m \mid a (x_1 - x_0),$$

$$w \mid a (x_1 - x_0),$$

$$w \mid s (x_1 - x_0),$$

since $r \mid s$, so $r \mid x_1 - x_0$.

ie $\exists l$ so that

$$x_1 - x_0 = l r,$$

$$x_1 = l r + x_0,$$

where $r = \gcd(a, m)$.

Thus any solution has the form

$$x_i = l \frac{m}{\gcd(a, m)} x_0 \mbox{ for some } l \leq \frac{m}{\gcd(a, m)},$$

and we get a solution for $l = 0, 1, 2 \ldots \frac{m}{\gcd(a, m)} - 1$. So $\frac{m}{\gcd(a, m)}$ solutions.