

Thm. Let $a, b, m \in \mathbb{N}$.

$$ax \equiv b \pmod{m} \\ \text{has a solution}$$

if and
only if

$$\gcd(a, m) \mid b.$$

The equivalence $\uparrow$ is equivalent to Bezout's

$$ax + my = b. \xrightarrow{\text{mod } m} ax \equiv b \pmod{m}$$

Ex: $10x \equiv 3 \pmod{12}.$

$\underset{a}{10} \quad \underset{b}{3} \quad \underset{m}{12}$

There exists a sol. iff $\gcd(10, 12) \mid 3.$

There is no solution!

Ex: $10x \equiv 6 \pmod{12}$.

We know there is a solution. How to find?

Work with $10x + 12y = 6$.

$$10x + 12y = 2 = \gcd(10, 12)$$

→

$$10(-1) + 12(1) = 2$$

Now reduce modulo 12:

$$10 \cdot 11 \equiv 10 \cdot (-1) \equiv 2 \pmod{12}$$

$$10z \equiv 2 \pmod{12} \\ z = 11$$

Multiply our sol. by 3:

$$10(-3) + 12(3) = 6$$

Reduce mod. 12: $(55) \quad 10(-3) \equiv 6 \pmod{12} \quad x \equiv 9 \pmod{12}$

Solve for x : $ax \equiv b \pmod{m}$.

$$d = \gcd(a, m)$$

1. Check $d \mid b$.

2. Solve $ax + my = d$ (Euclid)

3. Multiply by b/d :

$$\frac{ab}{d}x + \frac{mb}{d}y = b$$

4. Reduce modulo m .

5. Get $x \in \mathbb{Z}_m$.

Let's think about the number of solutions to
 $ax \equiv b \pmod{m}$

(Just talking about $x \in \mathbb{Z}_m$.) Let $d = \gcd(a, m)$.

If $d \nmid b \Rightarrow$ No solutions.

If $d \mid b$, there are exactly d distinct solutions. Let's see why.

In this case, $d \mid a$, $d \mid m$, $d \mid b$, so we factor

$$a'x \equiv b' \pmod{m'}$$

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Then

$$\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1.$$

(57)

Therefore, there is a solution to

$$a'y \equiv 1 \pmod{m'}$$

$$\text{so } y = (a')^{-1}.$$

$$a'x \equiv b' \pmod{m'}$$

Multiply by $(a')^{-1}$:

$$1 \cdot x \equiv \frac{b'}{a'} \stackrel{x_0}{=} \pmod{m'}$$

There is a solution! (In $\mathbb{Z}_{m'}$). Therefore,

$$\boxed{x = x_0 + k \frac{m}{d} \quad \text{for } k \in \{0, 1, 2, \dots, d-1\}}$$

all in $\mathbb{Z}_m$

(58)

But wait, there's more!

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 3 & (\text{mod } 5) \\ x \equiv 2 & (\text{mod } 7) \end{cases}$$

If there is a solution x_0 , then there are infinitely many:

$$x = x_0 + \underline{3 \cdot 5 \cdot 7 \cdot t}$$

$$\text{for } t \in \mathbb{Z}$$

(If a problem is too difficult, solve an easier version instead.)

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

$$x \equiv 3 \pmod{5}$$

Let's look at the first:

Consider $x=2$. Works for first but not 2nd.

[What is 5^{-1} in $\mathbb{Z}_3$. $5^{-1} \equiv 2 \pmod{3}$] ignore.

$$2x \equiv \underline{5x \equiv 1 \pmod{3}} \quad \text{~~2x \equiv 1 \pmod{3}}~~$$

$$2x \equiv 6 \equiv 1 \pmod{5}.$$

Now:

$$2x \equiv 1 \pmod{3}$$

$$2x \equiv 1 \pmod{5}.$$

$$\boxed{x=8}$$

(60)