

Why does this theorem hold?

$$a \cdot x \equiv 1 \pmod{m}$$

This means, there is some $k \in \mathbb{Z}$

$$ax - 1 = km.$$

Rearranging...

$$ax - km = 1$$

$\Downarrow$

$$ax + m(-k) = 1$$

(can always find a sol. $\rightarrow$) $ax + by = \gcd(a, b)$

(47)

Bézout

If we have an x such that

$$ax \equiv 1 \pmod{m},$$

then we have a solution ~~to~~ $(x, -k)$ to the Diophantine equation:

$$ax + my = 1$$

By one of our theorems, we know

$$\boxed{ax + by = c \text{ has a sol.}} \text{ --- if and only if --- } \boxed{\gcd(a, b) \mid c}.$$

Thus,

$$\gcd(a, m) = 1.$$

Try other direction yourself! (48)



$ax \equiv 1 \pmod{m}$ if and only if a, m coprime.

How to find inverses (multiplicative inverses)!

Goal: Find $a^{-1} \pmod{m}$

Step 0: Compute $\gcd(a, m)$

If $\gcd(a, m) \neq 1$, abandon ship!

Now assume coprime.

Use Euclid's alg. to solve

$$ax + my = 1.$$

Reduce x modulo m .

The result is a^{-1} .

(49)

so that
 x is between
0 and $m-1$

Still an involved
computation - but
beats trying
in its

Ex:

$$7x \equiv 1 \pmod{15}$$

Mental arithmetic:

$$7 \cdot 2 = 14 \equiv -1 \quad . \quad 7 \cdot \underline{-2} = -14 \equiv -(-1) \equiv 1$$

13 ←

Now using the ~~a~~ alg.

$$7x + 15y = 1$$

$$7(-2) + 15(1) = 1$$

So $x \equiv 13$ in $\mathbb{Z}_{15}$ is our sol.

$7^{-1} \equiv 13$ in $\mathbb{Z}_{15}$. $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$.

(50)

Note:

$$\frac{b}{a} = ba^{-1}$$

This might make sense in $\mathbb{Z}_m$
(if a, m are coprime.)

Ex: Find an integer in $\{0, 1, \dots, 8\}$
& that is equivalent to $7^{-1} \pmod{9}$.

Sol. One needs to solve $7x \equiv 1 \pmod{9}$

$$7^{-1} \equiv x \pmod{9}$$

$$7x + 9y = 1$$

$$7 \cdot 4 \equiv 28 \equiv 1 \pmod{9}$$

(51)

$$\gcd(7, 9)$$

$$9 = 1 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + \underline{1}$$

$$2 = 2 \cdot 1 + 0$$

$$1 = \overset{x}{1} \cdot \underline{7} + \overset{y}{(-3)} \cdot \underline{2}$$

$$= 1 \cdot 7 + (-3) \cdot (9 - 1 \cdot 7)$$

$$= \overset{x}{4} \cdot \underline{7} - \overset{y}{3} \cdot \underline{9}$$

~~compute~~ $\frac{3}{5} \equiv x \pmod{12}$
Find $x \in \mathbb{Z}_{12}$

$$3 \cdot 5^{-1} \equiv x \pmod{12}$$

Find 5^{-1} . We need solve

$$5y \equiv 1 \pmod{12}$$

$$\boxed{y=5}$$

$$5 \cdot 5 = 25 = 1 + 24 \equiv 1 \pmod{12}.$$

$$\text{So } 5^{-1} \equiv 5 \pmod{12}$$

$$3 \cdot 5^{-1} \equiv 3 \cdot 5 = 15 \equiv 3 \pmod{12}$$

Thus,

$$x \equiv 3 \pmod{12}.$$

(53)