3336

Office Hour

11:07

unmute to ask questions!

Use the Euclidean Algorithm to find a solution to the congruence equation $-33x \equiv 1 \bmod 45$ (if a solution exists).

a) ○ There are no solutions because $\gcd(-33, 45) \neq 1$.

b) ○ $x = -1/33$ is a solution.

c) ○ $x = -45/33$ is a solution.

d) ○ $x = 15$ is a solution.

e) ○ $x = -11$ is a solution.

$ax \equiv b \bmod n$

$\gcd(a, n) \mid b$?

yes, there are solutions

no, there are no solutions

$\gcd(-33, 45) = 3$

$b = 1$ 3 does not divide 1

Using the Euclidean Algorithm (repeat the Division Algorithm)

$45 = (-1)(-33) + \underline{12}$ $0 \leq r < |-33|$

$-33 = (-3)(12) + \underline{3}$ $0 \leq \quad < 12$

$12 = 4 \cdot 3 + \underline{0}$

stop.

gcd is the remainder above

$\boxed{\gcd(-33, 45) = 3}$ ✓

Find a solution to the congruence equation $-13x \equiv 12 \bmod 18$.

a) $x = 0$ is a solution.

b) $x = 42$ is a solution.

c) $x = 41$ is a solution.

d) $x = 132$ is a solution.

e) There are no solutions.

Euc Alg.

$-13x \equiv 12 \bmod 18$

$+18$

$5 \equiv -13 \bmod 18$

$5x \equiv 12 \bmod 18$

$\gcd(5,18) = 1$ $\quad 1 \mid 12$ ✓

$18 = 3\cdot 5 + 3 \longrightarrow 3 = 18 - 3(5)$

$5 = 1\cdot 3 + 2 \longrightarrow 2 = 5 - 1(3)$

$3 = 1\cdot 2 + 1 \longrightarrow 1 = 3 - 1(2)$

$2 = 2\cdot 1 + 0 \quad \to 1 = 3 - 1(5 - 1\cdot 3) =$

Reversing / Back-sub Euc. Alg to get Bezout

$1 = 3 - 1(5 - 1\cdot 3) = 3 - 5 + 1\cdot 3 = 3(2) - 5(1)$

$= 3(5 - 1\cdot 3) - 5\cdot 1 = 3\cdot 5 - 3\cdot 3 - 5\cdot 1$

$= 2(3) - 1(5) = 2(18 - 3\cdot 5) - 1(5)$

$= 2(18) - 6(5) - 1(5) = 2(18) - 7(5)$ inv

$$\underbrace{1 = 2\cdot 18 + (-7)\cdot 5}$$

the inverse of 5 (mod 18) is -7

check $\quad 5x \equiv 12 \bmod 18$

multiply both sides by the inverse of 5, i.e. by -7

$x \equiv (-7)(12) \bmod 18$

$\boxed{x \equiv -84}$

$5\cdot(-84) = -420 = \underbrace{(-24)\cdot 18}_{-432} + 12$ ✓

$x = -84$ is a solution

$x = -66$ " "

$x = -48$ $\quad x = -30 \ldots$ $\quad x = 6,$ $\quad x = 24,$ $\boxed{x = 42}$

Wait!!! $\gcd(5, 18) = 1 \longrightarrow$ one solution

How are there so many?

$\boxed{\text{One solution}}$ in our "standard remainder set"

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots, 15, 16, 17\}$

$ax \equiv b \mod n$

$\gcd(a, n) \mid b \quad \wedge \quad \gcd(a, n) > 1 \implies$ multi solutions in $\{0, 1, 2, \ldots, n-1\}$

What do we do here?

1) divide the whole equation by $\gcd(a, n)$

$$\frac{a}{\gcd(a,n)} x \equiv \frac{b}{\gcd(a,n)} \mod \frac{n}{\gcd(a,n)}$$

$$Ax \equiv B \mod N$$

$\gcd(A, N) = 1$

solve this one as before!

2) you'll get one solution, x_0 to $Ax \equiv B \mod N$

x_0 will also be a solution to $ax \equiv b \mod n$

rewrite $x_0 \in \{0, 1, 2, \ldots, n-1\}$

3) $x_0 + \frac{n}{\gcd(a,n)}$ will create more solutions in here

ex) $6x \equiv 3 \mod 9$

$a = 6, \; b = 3, \; n = 9$

$\gcd(6,9) = 3 \quad 3 \mid 3 \Rightarrow$ solutions ✓ $\quad 3 > 1$ mult. solutions in $\mathbb{Z}_9$

divide by $\gcd(6,9) = 3$

$$6x \equiv 3 \mod 9$$

$$2x \equiv 1 \mod 3$$

gcd(2,3)

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

$2 = \underline{2} \cdot 1 + \underline{0}$

$\gcd(2,3) = 1$

Bezout's Id.

$1 = 3 + (-1)(2)$

inverse of 2 is -1 (in $\mathbb{Z}_3$)

look at this mod 3

$(-1)(2) = 1 + \underbrace{\text{a mult. of } 3}_{\equiv 0 \mod 3}$

$(-1)(2) \equiv 1 \mod 3$

$$2x \equiv 1 \mod 3$$

$$(-1) \cdot 2x \equiv (-1)(1) \mod 3$$

$$x \equiv -1 \mod 3$$

$$\boxed{x = -1}$$

Recall: original equation was $6x \equiv 3 \mod 9$

<u>Check</u> $6 \cdot (-1) = -6 \overset{?}{\equiv} 3 \mod 9$

$-6 - 3 = -9$ is a mult. of 9 ✓

rewrite $\boxed{x = -1}$ as a solution in $\{0, 1, 2, 3, 4, 5, 6, 7, \boxed{8}\}$??

$-1 \equiv \underline{8} \mod 9$

add $\frac{n}{\gcd(a,n)} = \frac{9}{3} = 3$ to our solution to create new ones

$8 + 3 = 11 \equiv 2 \mod 9$

$2 + 3 = 5 \equiv 5 \mod 9$

$5 + 3 = 8 \equiv 8 \mod 9$ ✓