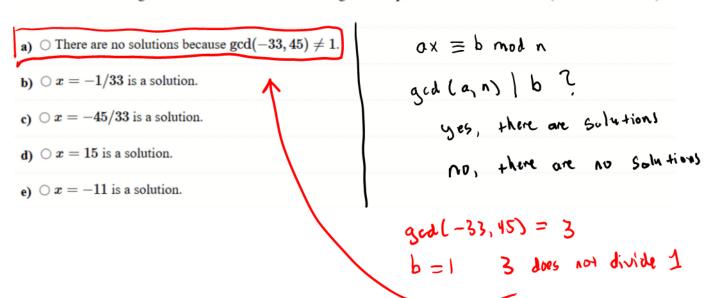
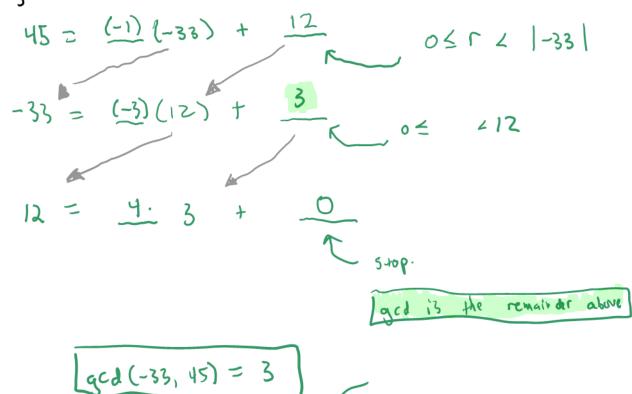


Unmute to ask questions!

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



Using the Euclidean Algorithm (repent the Division Algorithm)



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

Eva Alg.

- a) x = 0 is a solution.
- x=42 is a solution.
- c)

 x = 41 is a solution.
- d)

 x = 132 is a solution.
- e) There are no solutions.

$$1=3-1(5-1\cdot3)=3-5+1\cdot3=3(2)-5(1)$$

$$=3(5-1\cdot3)-5\cdot1=3\cdot5-3\cdot3-5\cdot1$$

$$=2(3)-1(5)=2(18-3\cdot5)-1(5)$$

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

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

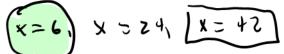
the inverse of 5 (mod 18) is -7

cheel 5x = 12 mod 18

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

X = (-7)(12) mod 18 -

$$5.(-84) = -420 = (-24).18 + 12$$



wait!!! gcd (5,18) =1 -> one solution How one three so many?

One solution in our "standard renainder bez" € 0,1, 2, 3, 4, 5, 6) 7, 8, ..., 15, 16, 17 }

 $ax \equiv b \mod n$ gcd (a_1n) | b \wedge gcd $(a_1n) > 1 \Rightarrow$ muth solutions in & 0, 1, 2, . ~, 1~13

What do we do here?

1) divide the whole equation by gedla, n)

$$\frac{a}{\gcd(a_1n)} \times = \frac{b}{\gcd(a_2n)} \mod \frac{n}{\gcd(a_2n)}$$

Ax = B mod N

gul
$$(A, N) = 1$$

solve this one as before!

2) you'll get one solution, xo to Ax = B mod N Xo will also be a solution to ax = b mod n

3) $x_0 + \frac{n}{ard(a_{in})}$ will create more solutions in here

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

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

$$gcd(c_19) = 3 \quad 3|3 \Rightarrow solutions \checkmark \quad 371 \text{ mult. solutions in } \mathbb{Z}_q$$

$$divide by all 6,91 = 3$$

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

$$gcd(2,3)$$

$$Be \neq out's Id$$

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

$$3 = 1 \cdot 2 + 1$$

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

$$3 = 1 \cdot 2 + 0$$

$$4 \cdot 10 \cdot 10 \cdot 10 \cdot 10$$

$$(-1)(2) = 1 \cdot 10 \cdot 10 \cdot 10$$

$$(-1)(2) = 1 \cdot 10 \cdot 10 \cdot 10$$

$$(-1)(2) = 1 \cdot 10 \cdot 10 \cdot 10$$

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

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

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

$$x = -1$$

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

Check 6. (-1) = -6 = 3 mod 9

-6-3 = -9 is a mult of 9 V

rewrite x = -1 as a solution in $\{20,1,2,3,4\}$ $\{5,7\}$ $\{6,7\}$ $\{8\}$

add $\frac{n}{\gcd(a_i n)} = \frac{9}{3} = 3$ to our solution to create new onis