3336

Office Hour

9:05 pm

unmute to ask!

start time (meeting closes at 9:15 pm)

Find a solution to the congruence equation $23x \equiv 19 \bmod 8$.

a) $x = 29$ is a solution.

$29 \equiv 5 \bmod 8$

b) $x = 19/23$ is a solution. ← not a solution

c) $x = 11$ is a solution.

d) $x = 8/23$ is a solution. ← not a solution

e) $x = 8$ is a solution.

Solutions should be integers $x \in \mathbb{Z}$

$ax \equiv b \bmod n$

$\gcd(23, 8) = 1$

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

yes, there are solutions

no, no solutions

$\gcd(a, n) = 1$

there is one solution

in $\{0, 1, 2, \dots, n-1\}$

$\{0, 1, 2, \dots, 7\}$

2) compute $\gcd(23, 8)$ using Euclid's algorithm

3) "reverse the steps" in Euclid's Algorithm to get Bezout's Identity

4) you can find a^{-1}

$a^{-1}ax \equiv a^{-1}b \mod n$

$x = a^{-1}b \mod n$

if we run these steps we will find $x \equiv -19 \mod 8 \equiv 5 \mod 8$

Check

$23x \equiv 19 \mod 8$

$x = 29$

$23 \cdot 29 = 667$

$667 = 81 \cdot 8 + 19$ < $19 \equiv 3 \mod 8$

$667 = 83 \cdot 8 + 3$

Find a solution to the congruence equation $23x \equiv 19 \bmod 8$.

$23x \equiv 19 \bmod 8$

$19 \equiv 3 \bmod 8$

$23x \equiv 3 \bmod 8$

$23 \equiv 7 \bmod 8$

$7x \equiv 3 \bmod 8$

Quiz 10 #10

Recall Bezout's Identity:

$$\forall a, b \in \mathbb{Z},\ \exists x, y \in \mathbb{Z},\ ax + by = \gcd(a, b)$$

If we apply this identity to the pair of integers $a = 14$ and $b = 17$ we produce the statement

$$\exists x, y \in \mathbb{Z},\ 14x + 17y = \gcd(14, 17).$$

Of the options provided, which values can we use for x and y to show this statement is true? Are there *other or additional values* one can use for x and y?

a) $x = 28$ and $y = -23$, and this pair is the only *unique* solution!
b) $x = 17$ and $y = 0$, and this pair is the only *unique* solution!
c) There are no solutions to this equation. Bezout's Identity does not apply because the integers a and b are too big..
d) $x = 17$ and $y = 0$, and *yes* there are other solutions!
e) $x = 28$ and $y = -23$, and *yes* there are other solutions!

Euclid's Algorithm

$\gcd(17, 14) = 1$

$17 = \underline{1} \cdot 14 + \underline{3}$

$14 = \underline{4} \cdot 3 + \underline{2}$

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

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

Bezout's Id

$1 = 3 - 1 \cdot 2$

$2 = 14 - 4 \cdot 3$

$3 = 17 - 1 \cdot 14$

$1 = 3 - 1 \cdot (14 - 4 \cdot 3)$

$1 = 3 - 1 \cdot 14 + 4 \cdot 3$

$1 = 5 \cdot 3 - 1 \cdot 14$

$1 = 5 \cdot (17 - 14) - 14$

$\boxed{1 = 5 \cdot 17 - 6 \cdot 14}$

$$(-6)\cdot 14 + 5\cdot 17 = \gcd(14,17)$$

we found coefficients

$x = -6, \quad y = 5$

<u>but</u> other solutions will exist!

we can check $x = 28$ & $y = -23$ also work