PRINTABLE VERSION

Quiz 11

You scored 100 out of 100

Question 1

Your answer is CORRECT.

The congruence equation "$80 \equiv -105 \bmod 37$ " means

use the first definition of modular arithematic

integer *x* is "*congruent mod n*" to integer *y* means:

- **First Definition:** $x - y$ is a multiple of *n*
  - in notation: $\exists m \in \mathbb{Z},\ x - y = m * n$

a) When $37 - (-105)$ is divided by 80 the remainder is 0.

b) When 37 is divided by $80 - (-105)$ the remainder is 0.

c) When $37 - (-105)$ is divided by 80 the remainder is 0.

d) When $80 - (-105)$ is divided by 37 the remainder is 0.

Question 2

Your answer is CORRECT.

The integers 92 and -28 are congruent mod n for which value of n?

$92 \equiv -28 \bmod n$

remainder of $\frac{92}{n}$ = remainder of $\frac{-28}{n}$

a) $\mathrm{n} = 92$

b) $\mathrm{n} = -28$

c) $\mathrm{n} = 16$

d) There are no values of n for which these two integers are congruent (except $\mathrm{n} = 1$).

e) $\mathrm{n} = 15$

Question 3

Your answer is CORRECT.

Consider the following proposition:

Proposition. If $\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{n}$, then $\mathrm{a}^4 \equiv \mathrm{b}^4 \bmod \mathrm{n}$.

If you were writing a direct proof of this proposition, which of the following statements could be used as your first line?

use the first definition of modular arithematic

integer *x* is "*congruent mod n*" to integer *y* means:

- **First Definition:** $x - y$ is a multiple of *n*
  - in notation: $\exists m \in \mathbb{Z},\ x - y = m * n$

a) Suppose a is a multiple of b and n.

b) Suppose b is a multiple of a and n.

c) Suppose $(a - b)$ is a multiple of n.

d) Suppose n is a multiple of $(a - b)$.

e) Suppose $a \cdot b = n$.

Question 4

Your answer is CORRECT.

Is the following statement true or false?

$$\exists\, x, y, z \in Z,\ n \in N^*,\ (x \equiv y \bmod n\ \wedge\ y \equiv z \bmod n)\ \wedge\ (x \not\equiv z \bmod n)$$

(Note: for this problem N^* refers to the positive natural numbers $N^* = N - \{0\} = \{1, 2, 3, \ldots\}$.)

if x is congruent to y, and y is congruent to z, then x should also be congruent to z

a) This statement is true.

b) This statement is false.

Question 5

Your answer is CORRECT.

A (direct) proof for a Proposition is presented below. Read through the proof and then determine which Proposition was proven.

Undefined control sequence \square

you'd think by quiz 11 they'd know how to make a quiz lmao

a) $\forall\, m \in Z,\ (m \equiv 1 \bmod 2)\ \Rightarrow\ (m^2 \equiv 1 \bmod 8)$

b) $\forall\, m \in Z,\ (m \equiv 1 \bmod 2)\ \Rightarrow\ (m^2 \equiv 0 \bmod 8)$.

c) $\forall\, m \in Z,\ (m^2 \equiv 1 \bmod 2)\ \Rightarrow\ (m \equiv 1 \bmod 8)$.

d) Technically no proposition was proven true since there is a mistake in Line 4; neither k nor $k + 1$ have to be even.

Question 6

Your answer is CORRECT.

Use the Euclidean Algorithm to find the inverse of $-13 \bmod 28$ (if it exists).

a) 28 is an inverse.

b) 15 is an inverse.

c) $-1/13$ is an inverse.

d) $-28/13$ is an inverse.

$-13 \bmod 28$
$+28$
$15 \bmod 28$
$\gcd(15,28)$
$28 = \underline{1} \cdot 15 + \underline{13} \rightarrow 13 = 28 - 1 \cdot 15$
$15 = \underline{1} \cdot 13 + \underline{2} \rightarrow 2 = 15 - 1(13)$
$13 = \underline{6} \cdot 2 + \underline{1} \rightarrow 1 = 13 - 6(2)$
$2 = \underline{2} \cdot 1 + \underline{0}$

$1 = 13 - 6(15 - 1 \cdot 13)$
$= 13 - 6(15) + 6(13)$
$= 28 - 1 \cdot 15 - 6(15) + 6(28 - 1 \cdot 15)$
$= 28 - 7(15) + 6(28) - 6(15)$
$= 7(28) - 13(15) = 1$
$0 \quad -13(15) \equiv 1 \pmod{28}$
inverse

e) -13 does not have an inverse mod 28 because $\gcd(-13, 28) \neq 1$.

Question 7

Your answer is CORRECT.

Of the options provided below, determine the one that best completes this sentence: "The modular equation $-10x \equiv 17 \bmod 4$ ________________ "

only has solutions if gcd(a,n)|b

a) has exactly one solution.

b) has multiple solutions.

c) has no solutions.

$\gcd(-10, 4) = 2$

$2 \nmid 17$ no solutions!

Question 8

Your answer is CORRECT.

Which steps should one take when solving a congruence equation $ax \equiv b \bmod n$? A helpful summary is presented below, only one step is missing:

Steps for solving $ax \equiv b \bmod n$.

Step 1. Use the Euclidean Algorithm to compute $\gcd(a, n)$.

Step 2. If $\gcd(a, n) \mid b$, then proceed to step 3, otherwise there are no solutions.

Step 3. Use work from Step 1 to calculate one solution $x_0 \in \mathbb{Z}$.

Step 4.

Of the following options, which could be used for the missing Step 3?

a) Step 4. Add $\frac{a}{\gcd(a, n)}$ to x_0 to create other solutions.

b) Step 4. Add $\frac{b}{\gcd(a, n)}$ to x_0 to create other solutions.

c) Step 4. Add b to x_0 to create other solutions.

d) Step 4. Add $\frac{\gcd(a, n)}{b}$ to x_0 to create other solutions.

Look at lecture 33 notes, last example

also lecture 34, example with 3x congruent 24 mod 9

e) Step 4. Add $\dfrac{n}{\gcd(a, n)}$ to x_0 to create other solutions.

Question 9

Your answer is CORRECT.

Find a solution to the congruence equation $7x \equiv -3 \bmod 3$.

a) $x = 3/7$ is a solution.

b) $x = 4$ is a soltuion.

c) $x = 3/7$ is a solution.

d) $x = 9$ is a solution.

e) $x = 10$ is a solution.

$7x \equiv -3 \pmod 3$

$\gcd(7,3) = 1$

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

$3 = \underline{3}\cdot 1 + \underline{0}$

$1 = \underset{\text{inv}}{1}(7) - \underset{0}{2}(3)$

$x \equiv -3 \pmod 3$

$-3+3=0+3=3+3=6+3=9$

Question 10

Your answer is CORRECT.

Find a solution to the congruence equation $-18x \equiv 4 \bmod 13$.

a) $x = 0$ is a solution.

b) $x = 21$ is a solution.

c) $x = 19$ is a solution.

d) There are no solutions.

e) $x = 20$ is a solution.

$-18x \equiv 4 \pmod{13}$

$+13 \downarrow$

$-5x \equiv 4 \pmod{13}$

$+13 \downarrow$

$8x \equiv 4 \pmod{13}$

$\downarrow$

$(5)8x \equiv (5)4 \bmod 13$

$x \equiv \underline{20} \pmod{13}$

$\gcd(8,13) = 1$

$13 = \underline{1}\cdot 8 + \underline{5} \rightarrow 5 = 13 - 1(8)$

$8 = \underline{1}\cdot 5 + \underline{3} \rightarrow 3 = 8 - 1(5)$

$5 = \underline{1}\cdot 3 + \underline{2} \rightarrow 2 = 5 - 1(3)$

$3 = \underline{1}\cdot 2 + \underline{1} \rightarrow 1 = 3 - 1(2)$

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

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

$= 1(8 - 1\cdot 5) - 5 + 1(8 - 1\cdot 5)$

$= 8 - 1\cdot 5 - 1\cdot 5 + 8 - 1\cdot 5$

$= 2(8) - 3(5)$

$= 2(8) - 3(13 - 1\cdot 8)$

$= 2(8) - 3(13) + 3(8)$

$= \underset{\text{inv}}{5}(8) - \underset{0}{3}(13) = 1$