

Modular Arithmetic



Easy
Congruence
Relations

Harder
Congruence
Relations

Properties of
Modular
Arithmetic

Theorems
Associated with
Modular
Arithmetic

Miscellaneous

Abstract Algebra
Modular Arithmetic

GameBoard

Full Screen

Quit

Easy Congruence Relations for 100.



$$\text{If } 62 \equiv x \pmod{5}$$

$$x = 0$$

$$x = 1$$

$$x = 2$$

$$x = 3$$

$$x = 4$$

Easy Congruence Relations for 200.



$$38 \equiv x \pmod{12}$$

$$x = 0$$

$$x = 2$$

$$x = 4$$

$$x = 8$$

$$x = 10$$

Easy Congruence Relations for 300.

$$125 \equiv 1 \pmod{x}$$

$$x = 31$$

$$x = 11$$

$$x = 9$$

$$x = 26$$

$$x = 14$$



Easy Congruence Relations for 400.

$$x \equiv 7 \pmod{13}$$

$$x = 31$$

$$x = 45$$

$$x = 56$$

$$x = 72$$

$$x = 86$$



Harder Congruence Relations for 100.



$$-7 \equiv x \pmod{17}$$

4

6

10

12

16

Harder Congruence Relations for 200.



Solve $x + x + x \equiv 0 \pmod{3}$

0

1

2

None of the above

All of the above

Harder Congruence Relations for 300.



How would you express: "the sum of two even numbers is even" in $\pmod{2}$?

$$1 + 0 \equiv 0 \pmod{2}$$

$$1 + 0 \equiv 1 \pmod{2}$$

$$0 + 0 \equiv 0 \pmod{2}$$

$$0 + 0 \equiv 1 \pmod{2}$$

$$1 + 1 \equiv 0 \pmod{2}$$

Harder Congruence Relations for 400.



What number would fit within this class of integers?

$\dots, -14, -8, -2, 0, 6, 12, 18, \dots$

26

34

48

52

68

Properties of Modular Arithmetic for 100.



We say that two integers a and b are congruent modulo m if there is an integer k such that

$$a - b = m/k$$

$$a - kb = m$$

$$ka - b = m$$

$$a - b = km$$

$$a + b = km$$

Properties of Modular Arithmetic for 200.



What is the name of this property in modular arithmetic?

$$a \equiv a \pmod{m}.$$

closed under addition

symmetry

transitivity

reflexivity

closed under multiplication

Properties of Modular Arithmetic for 300.



What is the name of this property in modular arithmetic?

If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

closed under addition

symmetry

transitivity

reflexivity

closed under multiplication

Properties of Modular Arithmetic for 400.



What is the name of this property in modular arithmetic?

If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

closed under addition

symmetry

transitivity

reflexivity

closed under multiplication

Theorems Associated with Modular Arithmetic for 100.

What is the name of the following theorem?

$$|G| = |G : H||H|$$

- Euler's Theorem
- Lagrange's Theorem
- Chinese Remainder Theorem
- Fermat's Little Theorem
- None of the above

Theorems Associated with Modular Arithmetic for 200.



What is the name of the following theorem?

$$a^p(n) \equiv 1 \pmod{n}$$

Euler's Theorem

Lagrange's Theorem

Chinese Remainder Theorem

Fermat's Little Theorem

None of the above

Theorems Associated with Modular Arithmetic for 300.

What is the name of the following theorem? For p prime, $a^p \equiv a \pmod{p}$

Euler's Theorem

Lagrange's Theorem

Chinese Remainder Theorem

Fermat's Little Theorem

None of the above

Theorems Associated with Modular Arithmetic for 400.

What is the name of the following theorem? Suppose n_1, n_2, n_k are positive integers which are pairwise co-prime. Then, for any given set of integers a_1, a_2, a_k , there exists an integer x solving the system of simultaneous congruences $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}, \dots, x \equiv a_k \pmod{n_k}$.

Euler's Theorem

Lagrange's Theorem

Chinese Remainder Theorem

Fermat's Little Theorem



None of the above



Abstract Algebra
Modular Arithmetic

- GameBoard
- Full Screen
- Quit

Miscellaneous for 100.



Who played a major role in the discovery of Modular Arithmetic?

Laplace

Lagrange

Bernoulli

Leibnitz

Pascal

Gauss

Abstract Algebra

Modular Arithmetic

GameBoard

Full Screen

Quit

Miscellaneous for 200.



In what year was Modular Arithmetic first discovered?

Around 2500 BC

1651

1724

1801

2001

Abstract Algebra
Modular Arithmetic

GameBoard

Full Screen

Quit

Miscellaneous for 300.

If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$ then $(a + c) \equiv (b + d) \pmod{N}$. Why is this so?

Modular arithmetic is reflexive

Modular arithmetic is symmetric

Modular arithmetic is closed under addition

Modular arithmetic is closed under multiplication

None of the above



Miscellaneous for 400.



What is the name of the following theorem? $nx + my = 1$

Euler's Theorem

Lagrange's Theorem

Chinese Remainder Theorem

Fermat's Little Theorem

Bezout's Theorem