Discrete Mathematics

(Relations)

Pramod Ganapathi
Department of Computer Science
State University of New York at Stony Brook

January 24, 2021

Are these functions?

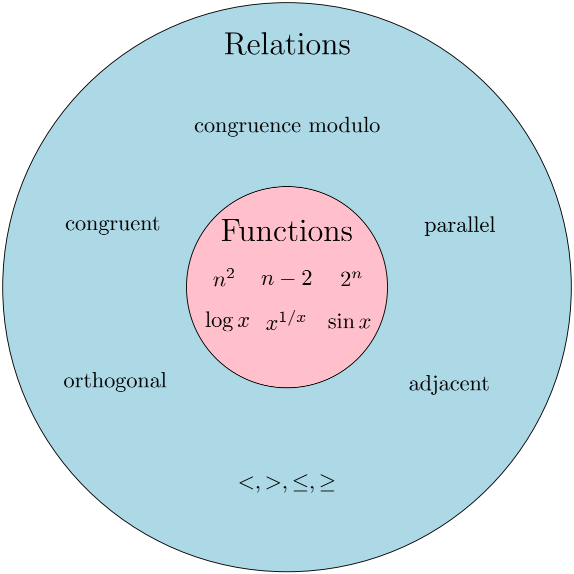
Problem

- Are these functions?
  - rational $p =$ rational q
  - $m < n$
  - d does not divide n
  - n leaves a remainder of 5 when divided by d
  - line ℓ_1 is parallel to line ℓ_2
  - person a is a parent of person b
  - triangle t_1 is congruent to triangle t_2
  - edge e_1 is adjacent to edge e_2
  - matrix A is orthogonal to matrix B

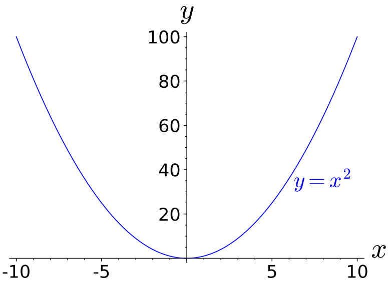
  No! (Because an input is mapped to more than one output.)
- What are these mappings called?

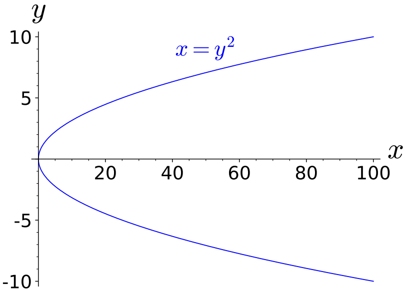
  Relations!

Functions vs. relations



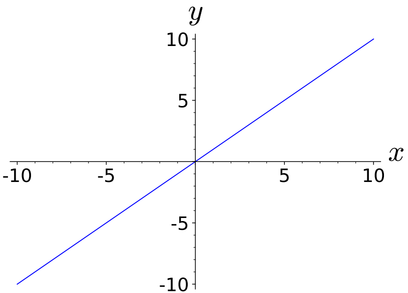
Functions vs. relations

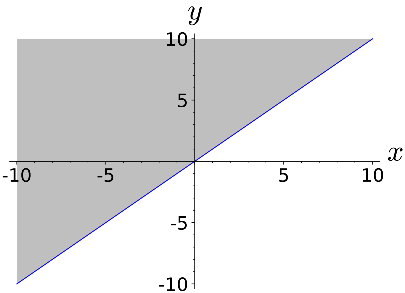




	$y = x^2$	$y = \pm\sqrt{x}$
Function?	✓	✗
Relation?	✓	✓

Functions vs. relations





	$y = x$	$y \geq x$
Function?	✓	✗
Relation?	✓	✓

What is a binary relation?

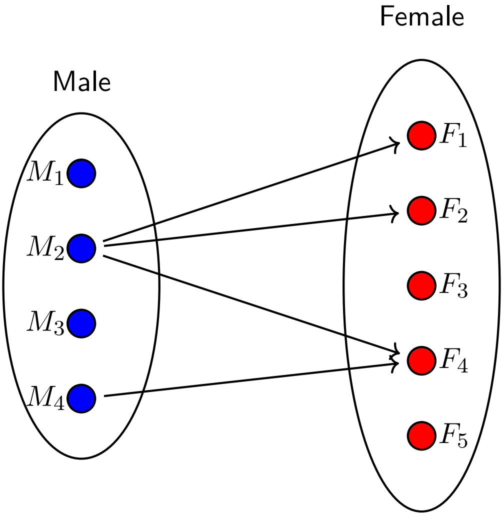
Definition

- If A and B are sets, then a binary relation from A to B is a subset of $A \times B$.
- We say that x is related to y by R, written $x\ R\ y$, if, and only if, $(x, y) \in R$. Denoted as $\boxed{x\ R\ y \Leftrightarrow (x, y) \in R}$.

Relationship

- Set of all functions is a proper subset of the set of all relations.

Example: Marriage relation



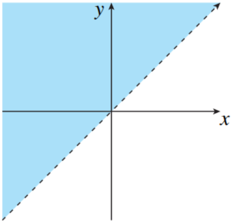
Example: Less than

Problem

- A relation $L : \mathbb{R} \to \mathbb{R}$ as follows.
  For all real numbers x and y, $(x, y) \in L \Leftrightarrow x\ L\ y \Leftrightarrow x < y$.
  Draw the graph of L as a subset of the Cartesian plane $\mathbb{R} \times \mathbb{R}$.

Solution

- $L = \{(-10.678, 30.23), (17.13, 45.98), (100/9, 200), \ldots\}$
- Graph:



Example: Congruence modulo 2

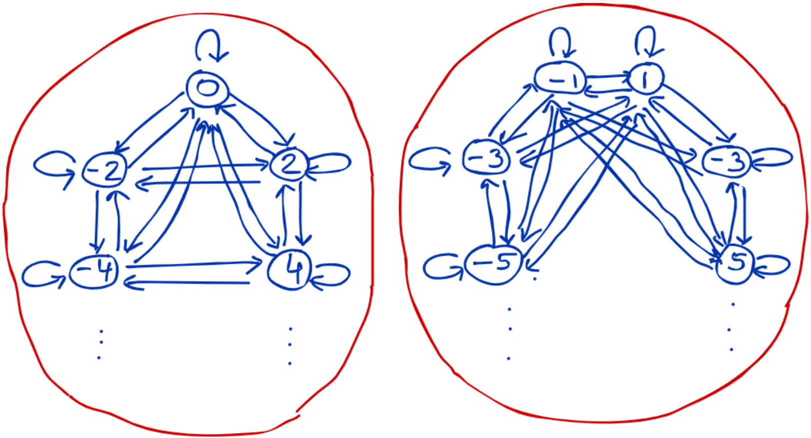
Problem

- Define a relation $C : \mathbb{Z} \to \mathbb{Z}$ as follows.
  For all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, $m\ C\ n \Leftrightarrow m - n$ is even.
- Prove that if n is any odd integer, then $n\ C\ 1$.

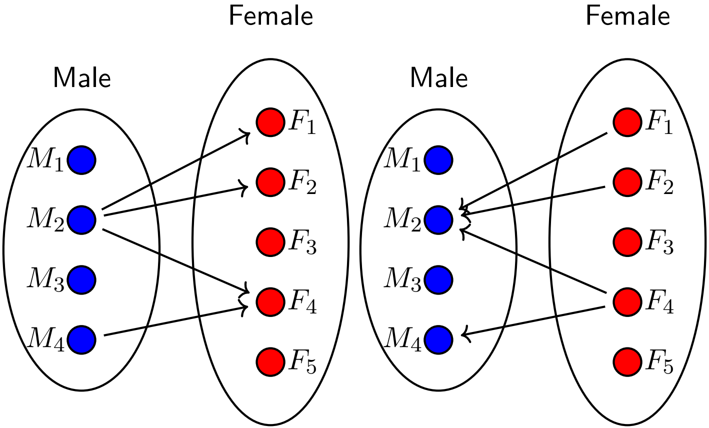
Solution

- $A = \{(2, 4), (56, 10), (-88, -64), \ldots\}$
  $B = \{(7, 7), (57, 11), (-87, -63), \ldots\}$
  $C = A \cup B$
- Proof. $(n, 1) \in C \Leftrightarrow n\ C\ 1 \Leftrightarrow n - 1$ is even
  Suppose n is odd i.e., $n = 2k + 1$ for some integer k.
  This implies that $n - 1 = 2k$ is even.

Example: Congruence modulo 2



Inverse of a relation



Inverse of a relation

Definition

- Let R be a relation from A to B.
  Then inverse relation R^{-1} from B to A is:
  $\boxed{R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}}$.
- For all $x \in A$ and $y \in B$,
  $\boxed{(x, y) \in R \Leftrightarrow (y, x) \in R^{-1}}$.

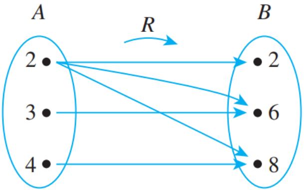
Example: Inverse of a finite relation

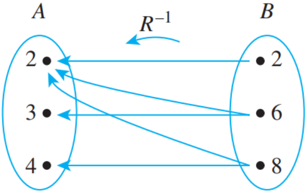
Problem

- Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$.
  Let $R : A$ to B. For all $(a, b) \in A \times B$, $a\ R\ b \Leftrightarrow a \mid b$
- Determine R and R^{-1}. Draw arrow diagrams for both.
  Describe R^{-1} in words.

Solution

- $R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$
  $R^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}$
- For all $(b, a) \in B \times A$,
  $(b, a) \in R^{-1} \Leftrightarrow b$ is a multiple of a





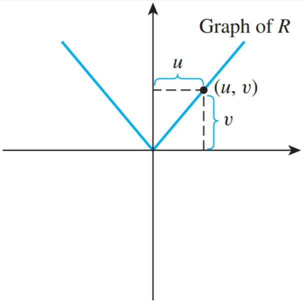
Example: Inverse of an infinite relation

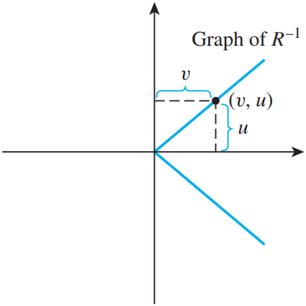
Problem

- Define a relation R from $\mathbb{R}$ to $\mathbb{R}$ as follows:
  For all $(u, v) \in \mathbb{R} \times \mathbb{R}$, $u \; R \; v \Leftrightarrow v = 2|u|$.
- Draw the graphs of R and R^{-1} in the Cartesian plane.
  Is R^{-1} a function?

Solution

- R^{-1} is not a function. Why?





Relation on a set

Definition

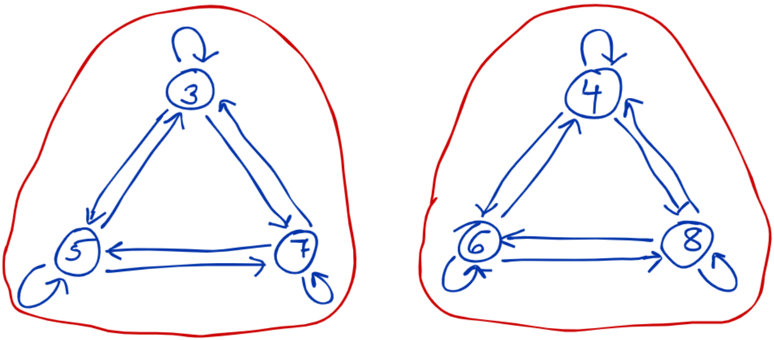
- A relation on a set A is a relation from A to A.
- The resulting arrow diagram is a directed graph possibly containing loops

Example: Relation on a set

Problem

- Let $A = \{3, 4, 5, 6, 7, 8\}$. Define relation R on A as follows. For all $x, y \in A$, $x\ R\ y \Leftrightarrow 2|(x-y)$. Draw the graph of R.

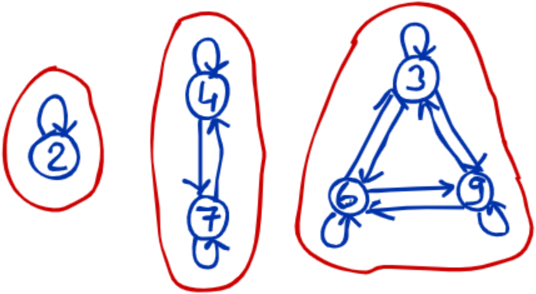
Solution



Reflexivity, symmetry, and transitivity

Properties

- Set $A = \{2, 3, 4, 6, 7, 9\}$
  Relation R on set A is: $\forall x, y \in A,\ x\ R\ y \Leftrightarrow 3 \mid (x - y)$



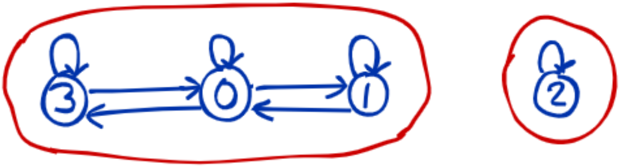
- Reflexivity. $\forall x \in A, (x, x) \in R$.
- Symmetry. $\forall x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
- Transitivity.
  $\forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Example

Problem

- $A = \{0, 1, 2, 3\}$.
  $R = \{(0,0), (0,1), (0,3), (1,0), (1,1), (2,2), (3,0), (3,3)\}$.
  Is R reflexive, symmetric, and transitive?

Solution



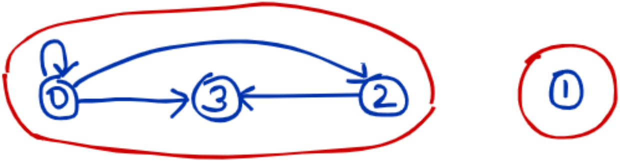
- Reflexive. $\forall x \in A, (x, x) \in R$.
- Symmetric. $\forall x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
- Not transitive. e.g.: $(1, 0), (0, 3) \in R$ but $(1, 3) \notin R$.
  $\exists x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \notin R$.

Example

Problem

- $A = \{0, 1, 2, 3\}$. $R = \{(0, 0), (0, 2), (0, 3), (2, 3)\}$.
  Is R reflexive, symmetric, and transitive?

Solution



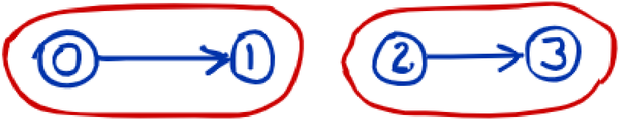
- Not reflexive. e.g.: $(1, 1) \notin R$. $\exists x \in A, (x, x) \notin R$.
- Not symmetric. e.g.: $(0, 3) \in R$ but $(3, 0) \notin R$.
  $\exists x, y \in A$, if $(x, y) \in R$, then $(y, x) \notin R$.
- Transitive.
  $\forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Example

Problem

- $A = \{0, 1, 2, 3\}$. $R = \{(0, 1), (2, 3)\}$.
  Is R reflexive, symmetric, and transitive?

Solution



- Not reflexive. e.g.: $(0, 0) \notin R$. $\exists x \in A, (x, x) \notin R$.
- Not symmetric. e.g.: $(0, 1) \in R$ but $(1, 0) \notin R$.
  $\exists x, y \in A$, if $(x, y) \in R$, then $(y, x) \notin R$.
- Transitive. Why?
  $\forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Equivalence relation and equivalence class

Definition

- Relation R on set A is an equivalence relation iff $\boxed{R \text{ is reflexive, symmetric, and transitive.}}$
- Equivalence class of element a, denoted by $[a]$, for an equivalence relation is defined as: $\boxed{[a] = \{x \in A \mid (x, a) \in R\}.}$

Example: Less than

Problem

- Suppose R is a relation on $\mathbb{R}$ such that $x \; R \; y \Leftrightarrow x < y$.
  Is R an equivalence relation?

Solution

- Not reflexive. e.g.: $0 \not< 0$. $\exists x \in \mathbb{R}, x \not< x$.
- Not symmetric. e.g.: $0 < 1$ but $1 \not< 0$.
  $\exists x, y \in \mathbb{R}$, if $x < y$, then $y \not< x$.
- Transitive. $\forall x, y, z \in \mathbb{R}$, if $x < y$ and $y < z$, then $x < z$.

So, R is not an equivalence relation.

Example: Equality (or Identity relation)

Problem

- Suppose R is a relation on $\mathbb{R}$ such that $x\;R\;y \Leftrightarrow x = y$.
  Is R an equivalence relation?

Solution

- Reflexive. $\forall x \in \mathbb{R}, x = x$.
- Symmetric. $\forall x, y \in \mathbb{R}$, if $x = y$, then $y = x$.
- Transitive. $\forall x, y, z \in \mathbb{R}$, if $x = y$ and $y = z$, then $x = z$.

So, R is an equivalence relation.

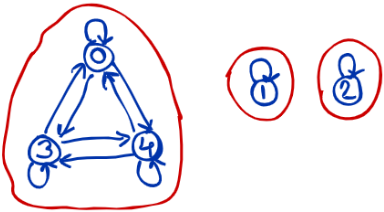
Equivalence classes: $[a] = \{a\}$.

Example: Partition

Problem

- Suppose R is a partition relation on A such that $\forall x, y \in A$, $x \; R \; y \Leftrightarrow x, y \in A_i$ for some subset A_i.
- $A = \{0, 1, 2, 3, 4\}$. Partition of A is $\{\{0, 3, 4\}, \{1\}, \{2\}\}$. Is R an equivalence relation?

Solution



- R is reflexive, symmetric, and transitive.
- So, R is an equivalence relation.
- Equivalence classes: $[0] = \{0, 3, 4\}, [1] = \{1\}$, and $[2] = \{2\}$.

Example: Partition

Problem

- Suppose R is a partition relation on A such that $\forall x, y \in A$, $x \; R \; y \Leftrightarrow x, y \in A_i$ for some subset A_i.
  Is R an equivalence relation?

Solution

- Reflexive. $\forall m \in A$, $(m, m) \in R$.
- Symmetric. $\forall m, n \in A$, if $(m, n) \in R$, then $(n, m) \in R$.
- Transitive.
  $\forall m, n, p \in A$, if $(m, n) \in R$ and $(n, p) \in R$, then $(m, p) \in R$.

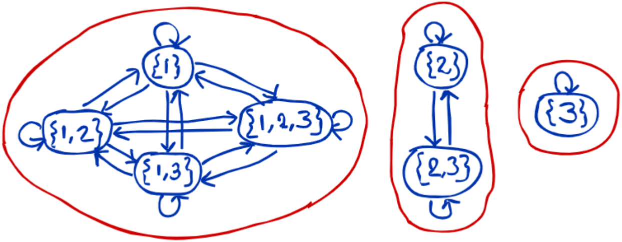
So, R is an equivalence relation.

Example: Least element

Problem

- Let X denote the power set of $\{1, 2, 3\}$.
  Suppose R is a relation on X such that $\forall A, B \in X$
  $A \; R \; B \Leftrightarrow$ Least element of A is same as that of B.
  Is R an equivalence relation?

Solution



- R is reflexive, symmetric, and transitive.
- So, R is an equivalence relation.
- Equivalence classes: $[\{1\}]$, $[\{2\}]$, and $[\{3\}]$.

Example: Congruence modulo 3

Problem

- Suppose R is a relation on $\mathbb{Z}$ such that $m\ R\ n \Leftrightarrow 3 \mid (m-n)$. Is R an equivalence relation?

Solution

- Reflexive. $\forall m \in A, 3 \mid (m-m)$.
- Symmetric. $\forall m, n \in A$, if $3 \mid (m-n)$, then $3 \mid (n-m)$.
- Transitive.
  $\forall m, n, p \in A$, if $3 \mid (m-n)$ and $3 \mid (n-p)$, then $3 \mid (m-p)$.

So, R is an equivalence relation.

Example: Congruence modulo 3

Solution

- Equivalence classes.

  Three distinct equivalence classes are $[0]$, $[1]$, and $[2]$.

  $[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{3}\} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

  $[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{3}\} = \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \ldots\}$

  $[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod{3}\} = \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \ldots\}$

  Intuition.

  $[0]$ = Set of integers when divided by 3 leave a remainder of 0.

  $[1]$ = Set of integers when divided by 3 leave a remainder of 1.

  $[2]$ = Set of integers when divided by 3 leave a remainder of 2.

Congruence modulo n

Definition

Let a and b be integers and n be a positive integer.
The following statements are equivalent:

- a and b leave the same remainder when divided by n.
  $\boxed{a \bmod n = b \bmod n.}$
- $\boxed{n \mid (a - b).}$
- a is congruent to b modulo n.
  $\boxed{a \equiv b \pmod{n}}$
- $\boxed{a = b + kn}$ for some integer k.

Examples

- $12 \equiv 7 \pmod{5}$
- $6 \equiv -6 \pmod{4}$
- $3 \equiv 3 \pmod{7}$

Example: Congruence modulo n

Problem

- Suppose R is a relation on $\mathbb{Z}$ such that
  $a \; R \; b \Leftrightarrow a \equiv b \pmod{n}$.
  Is R an equivalence relation?

Solution

- Reflexive. $\forall a \in \mathbb{Z}, a \equiv a \pmod{n}$.
- Symmetric.
  $\forall a, b \in \mathbb{Z}$, if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
- Transitive.
  $\forall a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

So, R is an equivalence relation.

Equivalence classes: $[0], [1], \ldots, [n-1]$.

Example: Congruence modulo n

Solution

- R is Reflexive. Show that $\forall a \in \mathbb{Z}, n \mid (a - a)$. We know that $a - a = 0$ and $n \mid 0$. Hence, $n \mid (a - a)$.
- R is Symmetric. Show that $\forall a, b \in \mathbb{Z}$, if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$. We see that $a \equiv b \pmod{n}$ means $n \mid (a - b)$.

  Let $(a - b) = nk$, for some integer k.

  $\implies -(a - b) = -nk$ (multiply both sides by -1)

  $\implies (b - a) = n(-k)$ (simplify)

  $\implies n \mid (b - a)$ ($-k$ is an integer; use defn. of divisibility)

  In other words, $b \equiv a \pmod{n}$.

Example: Congruence modulo n

Solution

- R is transitive. Show that $\forall a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
  We see that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply that $n \mid (a - b)$ and $n \mid (b - c)$, respectively.
  Let $(a - b) = nk$ and $(b - c) = n\ell$, for some integers k and ℓ.
  Adding the two equations, we get
  $(a - c) = (k + \ell)n$, where $k + \ell$ is an integer because addition is closed on integers.
  By definition of divisibility, $n \mid (a - c)$ or $a \equiv c \pmod{n}$.

Modular arithmetic

Modular arithmetic

Let a, b, c, d, n be integers with $n > 1$.
Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then

1. $\boxed{(a + b) \equiv (c + d) \pmod{n}}$
2. $\boxed{(a - b) \equiv (c - d) \pmod{n}}$
3. $\boxed{(ab) \equiv (cd) \pmod{n}}$
4. $\boxed{(a^m) \equiv (c^m) \pmod{n}}$ for all positive integers m

Units digit

Problem

- What is the units digit of 1483^{8650}?

Solution

- Units digit of 1483^{8650} is the units digit of 3^{8650}.
- Units digit of $3^0, 3^1, 3^2, 3^3$, and 3^4 are $1, 3, 9, 7$, and 1, respectively.
- Periodicity is 4. Therefore,
- Units digit of 3^{4k+0} is 1.
  Units digit of 3^{4k+1} is 3.
  Units digit of 3^{4k+2} is 9.
  Units digit of 3^{4k+3} is 7.
- Units digit of $3^{8650} = 3^{4\times 2162+2}$ is 9.
- Hence, the answer is 9.

Equation solving

Problem

- Use modular arithmetic to solve the equations.
  $16x + 12y = 32$ and $40x - 9y = 7$.

Solution

- Apply $\bmod 3$ on both sides of the first equation.
  $(16x + 12y) \bmod 3 \equiv 32 \bmod 3$
  $\implies x \equiv 2 \bmod 3$
  Similarly, apply $\bmod 3$ on both sides of the second equation.
  $(40x - 9y) \bmod 3 \equiv 7 \bmod 3$
  $\implies x \equiv 1 \bmod 3$
- These two congruences are contradictory.
  Hence, the system of equations does not have a solution.

Universal product code (UPC)

- Check digits are used to reduce errors universal product codes, tracking operations for shipping operations, book identification numbers (ISBNs), vehicle numbers, ID for the healthcare industry, etc.
- UPC is a 12-digit number, where the last digit is the check digit.
- Suppose the first 11 digits of the UPC are $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}$. Then the check digit can be computed using the following formula $\boxed{a_{12} = (210 - k) \bmod 10}$, where $\boxed{k = 3(a_1 + a_3 + \cdots + a_{11}) + (a_2 + a_4 + \cdots + a_{10})}$

Universal product code (UPC)

Problem

- The first eleven digits of the UPC for a package of ink cartridges are 88442334010. What is the check digit?

Solution

- $k = 3(8+4+2+3+0+0) + (8+4+3+4+1) = 71$
  check digit $= (210 - 71) \bmod 10 = 9$