

30.01.2023 matematyka dyskretna

część 1

5. Sprawdź, czy następujące relacje R w zbiorze X są zwrotne, symetryczne, antysymetryczne, przechodnie i spójne:

- a) $X = \mathbb{Z}, xRy \Leftrightarrow 3 \mid x - y$,
- b) $X = \mathbb{N}, xRy \Leftrightarrow 2 \mid x + y$,
- c) $X = \mathbb{N}, xRy \Leftrightarrow 3 \mid x + y$,
- d) $X = \mathbb{Z}, xRy \Leftrightarrow 5 \mid x^3 - y^3$,
- e) $X = \mathbb{R}, xRy \Leftrightarrow x^2 = y^2$,
- f) $X = \mathbb{R}, xRy \Leftrightarrow x^2 \neq y^2$,
- g) $X = \mathbb{R}, xRy \Leftrightarrow x^3 = y^3$,
- h) $X = \mathbb{R}, xRy \Leftrightarrow |x| < |y|$,
- i) $X = \mathbb{R}, xRy \Leftrightarrow |x| + |y| = 3$,
- j) $X = \mathbb{N}, xRy \Leftrightarrow x > y \vee y > x$,
- k) $X = \mathbb{R}, xRy \Leftrightarrow x - y \in \mathbb{Q}$,
- l) $X = 2^{\mathbb{N}}, xRy \Leftrightarrow |x \Delta y| < +\infty$.

$$778899$$

$$288$$

$$67788$$

$$127788$$

$$27999999$$

$$\begin{array}{r} 11 \\ 20 \\ 30 \\ \hline 51 \end{array}$$

$$99 = 3 \cdot 3 \cdot 11$$

$$88 = 2 \cdot 2 \cdot 11$$

$$77 = 7 \cdot 11$$

$$7788 = 2 \cdot 2 \cdot 3 \cdot 11 \cdot 59$$

$$9977 = 11 \cdot 907$$

$$778899$$

$$887799$$

$$999999$$

wszystka podzielne przez 11

$$990000$$

$$8800$$

$$77$$

n - ilość segmentów

$$998877$$

$$11(7|222|3 \cdot 3) \cdot 100^n + 11(7|2 \cdot 2 \cdot 2|3 \cdot 3) \cdot 100^{n-1} + 11(7|2 \cdot 2 \cdot 2|3 \cdot 3) 100^{n-2} + \dots + 11(7|2 \cdot 2 \cdot 2|3 \cdot 3) \cdot 100^0$$

liczba jest podzielna przez 11, kombinacje 2, 8, 7 i inne liczby pierwsze

$$y = \{2, 4, 5, 6, 7\}$$

10. Niech

Wyznacz elementy wyróżnione oraz kresy zbioru A jako podzbioru \mathbb{N} uporządkowanego przez relację podzielności.

∞
 16
 8
 4
 6 25
 125
 element maksymalne: 6, 10, 7
 5 10 25
 2 5 7
 elementy minimalne
 największy: brak

elementy minnabe: 2, 5, 7

największy: brak

najmniejszy: 6 rok

kres gorny:

nie istnieje (nie ma być ograniczony przez nic)

Kres datowy: 1

kręsy znajdowanie elementów

$$X = N^2$$

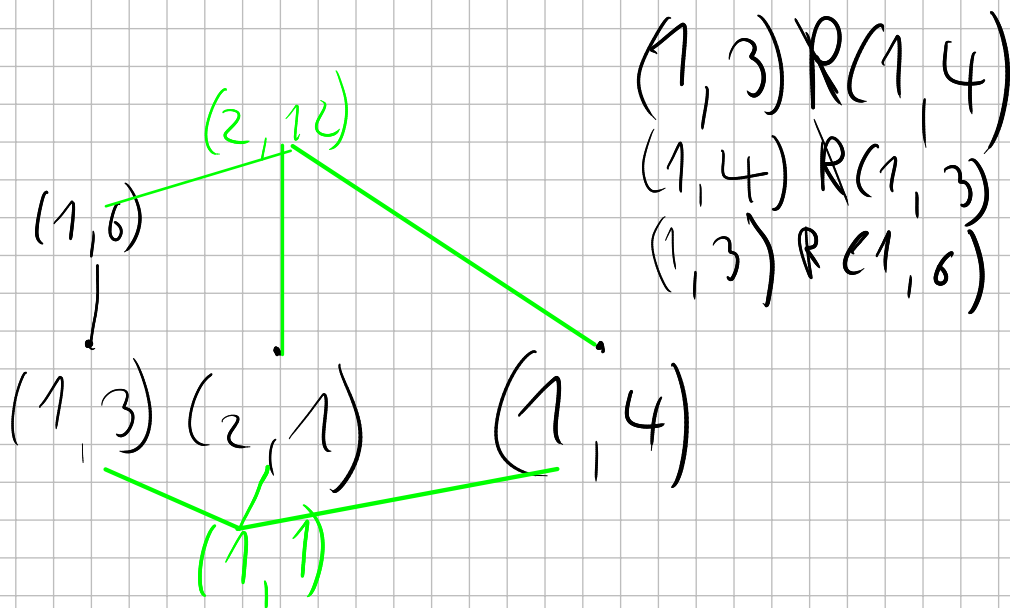
$$(x, y) \in R(t) \Leftrightarrow x \leq c \wedge y \mid t$$

$$(1, 21) R (2, 7)$$

$$3 \times 2 \wedge 21 \mid 7$$

$$x \leq y \wedge y \mid x$$

$$A = \{(2, 1), (1, 3), (1, 4), (1, 6)\}$$



elementy minnowe: $(1, 3), (2, 1), (1, 4)$

elementy max: $(1, 6), (2, 1), (1, 4)$

element najmniejszy: brak

element największy: brak

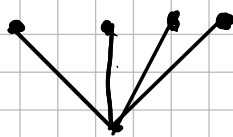
król: $(1, 1)$ $\inf A = (1, 1)$

król: $(2, 12)$ $\sup A = (2, 12)$

12)

 $k \in \mathbb{N}$ - liczba ustalona

$$A = ? \quad |A| = k+1$$

1 minimalny
reszta max

$$x R y \Leftrightarrow x | y$$

17. Które z następujących relacji R w zbiorze X są relacjami równoważności?

1. zwrotna
2. symetryczna
3. przechodnia

a) $X = \mathbb{Z}, x R y \Leftrightarrow 3 \mid x - y$.

b) $X = \mathbb{N}, x R y \Leftrightarrow xy$ jest liczbą nieparzystą.

c) $X = \mathbb{N}, x R y \Leftrightarrow \forall t \in \mathbb{N} xy = t^2$.

d) $X = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}, (x, y) R (s, t) \Leftrightarrow x, s \neq 0 \wedge xs > 0$.

e) $X = 2^Y$ dla pewnego zbioru $Y, x R y \Leftrightarrow x \subset y \vee y \subset x$.

f) $X = \mathbb{N}_0^2 = \mathbb{N}_0 \times \mathbb{N}_0, (m, n) R (a, b) \Leftrightarrow m + b = n + a$.

g) $X = \mathbb{Z} \times \mathbb{N}, (m, n) R (a, b) \Leftrightarrow mb = na$.

Dla relacji równoważności opisz klasy abstrakcji względem tej relacji.

1 $x R x$

2 $x R y \Rightarrow y R x$

3 $x R y \wedge y R z \Rightarrow x R z$

w)

$$X = \mathbb{N}, x R y \Leftrightarrow 2 \nmid x$$

 $2 \nmid x$ nie jest zwrotna więc nie jest równoważność

g)

$$X = 2^Y \text{ dla } Y$$

$$x R y \Leftrightarrow x \subset y \vee y \subset x$$

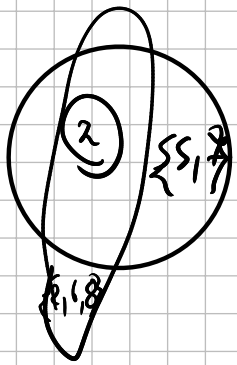
$$x R x \Leftrightarrow x \subset x \text{ tak}$$

$$x R y \Rightarrow y R x$$

$$x \subset y \vee y \subset x \Rightarrow y \subset x \vee x \subset y - \text{tak}$$

$$x R y \wedge y R z \Rightarrow x R z$$

$$(x < y \vee y < x) \wedge (z < y \vee y < z) \Rightarrow (x < z \vee z < y)$$



$$X = \{5, 7\}$$

$$Y = \{2\}$$

$$Z = \{2, 6, 8\}$$

Relacja przystawania
przystość

$$a \equiv b \pmod{n}$$

oznaczenie relacji

oznaczenie

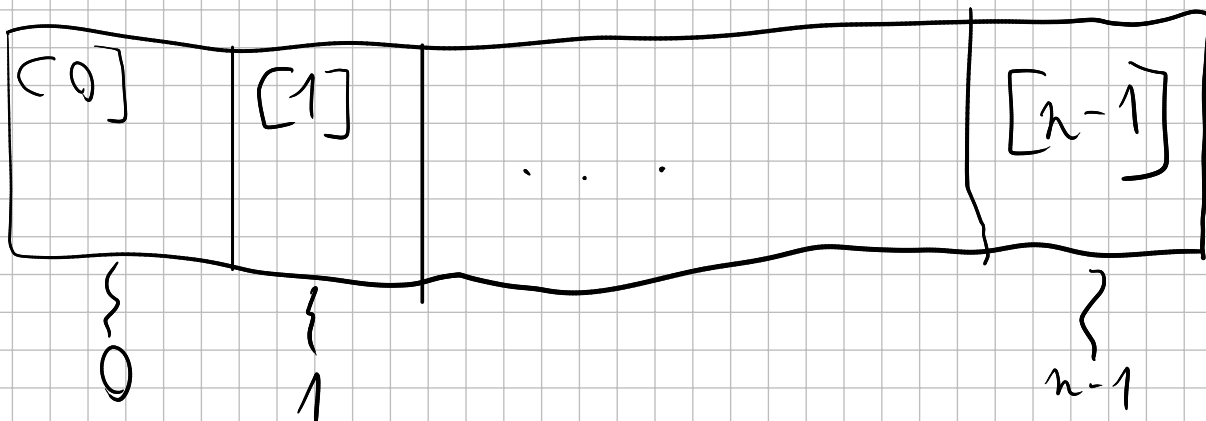
$$\mathbb{Z}, n \mid a - b$$

$$a \% n \rightsquigarrow$$

$$a \bmod n$$

działanie

$$\mathbb{Z}, n$$



$$\{0, 1, \dots, n-1\} \stackrel{\text{ozn}}{=} \mathbb{Z}_n$$

$$20x \equiv 6 \pmod{74}$$

$$20x = 6 + 74k$$

$$10x = 3 + 37k \Leftrightarrow 10x \equiv 3 \pmod{37}$$

Def

k - reszta z dzielenia

$k \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ jeżeli istnieje liczba
 m dla której

$km \equiv 1 \pmod{n}$ to nazywamy ją elementem
odwrotnym do k .

$$\boxed{x \cdot a \cdot r = \frac{1}{x} \text{ podobnie}}_S$$

$$k^{-1} = m \in \mathbb{Z}_n$$

$$10^{-1} \equiv 11 \pmod{37} \Leftrightarrow$$

$$10^{-1} \equiv 26 \pmod{37} \Leftrightarrow$$

$$10^{-1} \equiv 53 \pmod{37}$$

$k \in \mathbb{Z}_n$ ma element odwrotny wtedy i tylko wtedy
gdy:

$$\text{NWD}(k, n) = 1$$

RAE

$$\text{NWD}(k, n) = 1 \Rightarrow \exists_{r, t} \in \mathbb{Z} \quad rk + tn = 1 \Rightarrow rk = 1 \pmod{n}$$

przebieg
bo dla $rk = 1 + m \cdot n$
dla 1

$$\text{NWD}(k, n) > 1 \Rightarrow rk \equiv 1 \pmod{n}, rk = 1 + m \cdot n$$
$$1 = rk - mn$$

Iw

Jedyności elementu odwrotnego

$$k^{-1} = m \wedge k^{-1} = l \Leftrightarrow m = l$$

Dow.

$$\textcircled{m} = m \cdot 1 = m (k \cdot l) = m \cdot k \cdot l = 1 \textcircled{l}$$

Vklady kongruenci

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{15} \end{cases}$$

$$x = 1 + 13k, k \in \mathbb{Z}$$

$$1 + 13k \equiv 4 \pmod{15}$$

$$13k \equiv 3 \pmod{15}$$

$$13k \equiv 3 \pmod{15}$$

d	q	s	t
15		1	0
		0	1
13	1	1	1
2	6	1	-1
1	2	-6	7
0			

$$1 = -6 \cdot 15 + 7 \cdot 13$$

$$1 \equiv 7 \cdot 13 \pmod{15}$$

$$7 \cdot 13 k \equiv 7 \cdot 3 \pmod{15}$$

$$k \equiv 6 \pmod{15}$$

$$k = 6 + 15l$$

$$x = 1 + 13(6 + 15l)$$

$$x = 79 + \underbrace{13 \cdot 15l}_{195l}$$

rozwiązanie równania

kongruencji: $x = 79 + 195l$

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \quad \begin{array}{l} \text{CHIŃSKIETWIERDZENIE} \\ \text{O RESZTACH} \end{array}$$

$$a, b \in \mathbb{Z}$$

$$\wedge m, n \in \mathbb{N}; m, n \geq 2$$

$$\wedge \text{NWD}(m, n) = 1 \text{ (względnie pierwsze)}$$

$$\Rightarrow \text{w zbiorze } \{0, 1, \dots, m \cdot n - 1\}$$

istnieje tylko jedno rozwiązanie x

spełniające (*)

Każde inne rozwiązanie różni się od x_0 o wielokrotność $m \cdot n$

$$\left\{ \begin{array}{l} 0 \leq x_0 \leq m \cdot n - 1 \\ x = x_0 + k \cdot m \cdot n \end{array} \right\}$$

Tw

$$a_1, \dots, a_k \in \mathbb{Z}, n_1, \dots, n_k \geq 2$$

$$\wedge \text{NWD}(n_i, n_j) = 1$$

$$\Rightarrow x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

...

$$x \equiv a_k \pmod{n_k}$$

ma jedno rozwiązanie w zbiorze $\{0, 1, \dots, n_1 n_2 \dots n_k\}$

$$x = x_0 + n_1 \cdot n_2 \cdot \dots \cdot n_k \cdot m, \quad m \in \mathbb{Z}$$

listy zstata

.....

5 3

4 2

7 5

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{4} \\ x \equiv 5 \pmod{7} \end{cases}$$

SYSTEMY RESZTOWE

RNS

$$m, n - \text{mialynly} \quad \text{NWD}(m, n) = 1$$

$$\{0, 1, \dots, m \cdot n - 1\} \xleftrightarrow{\text{CTR}} \{a, b\} \quad a \in \mathbb{Z}_m, b \in \mathbb{Z}_n$$

$$m = 13, n = 15$$

$$\{0, 1, \dots, 195\} \ni 79 \Leftrightarrow (1, 4) \in \mathbb{Z}_{13} \times \mathbb{Z}_{15}$$

$$\mathbb{Z}_{195} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{15}$$

$$m = 3, n = 4 \quad \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$$

\mathbb{Z}_{12}
 0
 1

$(x \bmod 3, x \bmod 4)$
 $\mathbb{Z}_3 \times \mathbb{Z}_4$
 (0, 0)
 (1, 1)

2

3

4

5

6

7

8

9

10

11

(2, 2)

(0, 3)

(1, 0)

(2, 1)

(0, 2)

(1, 3)

(2, 0)

(0, 1)

(1, 2)

(2, 3)

pozycjonare jest wrednie

1 A 3 ter

X 11 ter

10 11 ter

$$u^{32} + u^{32} \\ 2^{32} \quad 2^{32} - 1$$

$$\mathbb{Z}_{2^{64}} \cong \mathbb{Z}_{32} \times \mathbb{Z}_{32}$$

Bigint is kinda fast RN

1
2
4
8
16

$$\begin{array}{r} 110 \\ 111 \\ \hline 1001 \end{array}$$

ONE clock cycle

$$2 + 7 = 9$$

$$(2, 2) + (1, 3) = (0, 1)$$

$$(2^0 \bmod 3, 2^0 \bmod 4) + (7^0 \bmod 3, 7^0 \bmod 4)$$

$$\begin{array}{c} \downarrow \\ \text{mem: } (2, 2); (1, 3) \\ \downarrow \\ (0, 1) \end{array}$$

KRYPTOGRAFIA:

