30.01.2023 matematyka dyskretna

Część B

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) $X = 2^{\mathbb{N}}$, $xRy \Leftrightarrow |x \triangle y| < +\infty$.

7788 99

2 88
6 7788
12 7788
27 999999

11
20
30
11
51

$99 = 3 \cdot 3 \cdot 11$
$88 = 2 \cdot 2 \cdot 11$
$77 = 7 \cdot 11$

$7788 = 2 \cdot 2 \cdot 3 \cdot 11 \cdot 59$
$9977 = 11 \cdot 907$

7788 99
88779 9
99 99 99

wszystko podzielne przez 11

990000
8800
77

n - ilość segmentów
99 8877

$11(7|22.2|3\cdot3)\cdot100^n + 11(7|2\cdot2\cdot2|3\cdot3)\cdot100^{n-1}$
$+ 11(7|2\cdot2\cdot2|3\cdot3)100^{n-2} + \ldots + 11(7|2\cdot2\cdot2|3\cdot3)\cdot100^0$

liczba jest podzielna przez 11, kombinacje 2, 3, 7 i inne liczby pierwsze

$X = \{1, 3, 5, 7, \ldots\}$

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

$X \cap Y = \{1, 2, 3, 4, 6, 9, 11 \ldots\}$

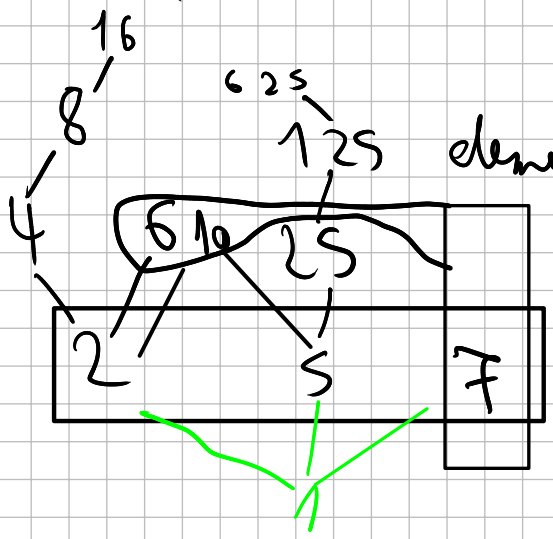
10. Niech

$$A = \{2^n : n \in \mathbb{N}\} \cup \{5^n : n \in \mathbb{N}\} \cup \{6, 7, 10\}.$$

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

$A = \{2^n : n \in N\} \cup \{5^n : n \in N\} \cup \{6, 7, 10\}$

∞



elementy maksymalne: 6, 10, 7

elementy minimalne: 2, 5, 7

największy: brak

najmniejszy: brak

kres górny:

nie istnieje (nie mają być ograniczony przez nic)

kres dolny: 1

kresy znajdowanie elementów

$X = N^2$

$(x, y) R (t, t) \iff x \mid z \wedge y \mid t$

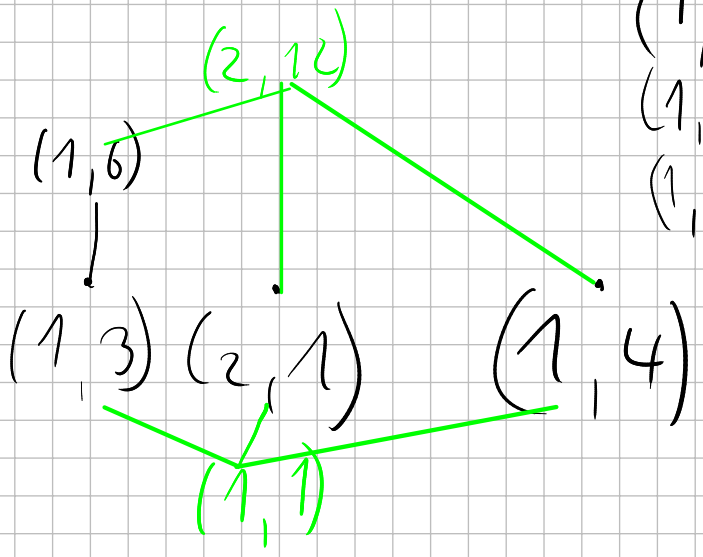
$(2,1) R (2,7)$

$3 \leq 2 \wedge 2 \mid 7$

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

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

$(1,3) R (1,4)$
$(1,4) R (1,3)$
$(1,3) R (1,6)$



elementy minimalne: $(1,3)$; $(2,1)$; $(1,4)$

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

element najmniejszy: brak

element największy: brak

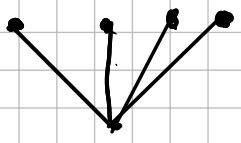
kres dolny: $(1,1)$ $\quad \inf A = (1,1)$

kres górny: $(2,12)$ $\quad \sup A = (2,12)$

12)

$k \in \mathbb{N}$ – liczba ustalona

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



1 minimalny

reszta max

$$x R y \Leftrightarrow x \mid y$$

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

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

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

c) $X = \mathbb{N}$, $xRy \Leftrightarrow \bigvee_{t \in \mathbb{N}} xy = t^2$.

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, $xRy \Leftrightarrow x \subset y \vee y \subset x$.

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. zwrotna
2. symetryczna
3. przechodnia

1 $x R x$

2 $x R y \Rightarrow y R x$

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

v)

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

$2 R z$ nie jest zwrotna więc nie jest równoważnością

g)

$X = 2^Y$ dla Y

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

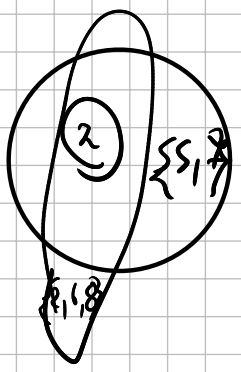
$$x R x \Leftrightarrow x \subset x \quad \text{tak}$$

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

$$x \subset y \vee y \subset x \Rightarrow y \subset x \cup x \subset y \quad \text{– tak}$$

$$xRy \wedge yRz \Rightarrow xRz$$

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



$X = \{5, 7\}$

$y = \{2\}$

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

Relacja przystawania

przystaje

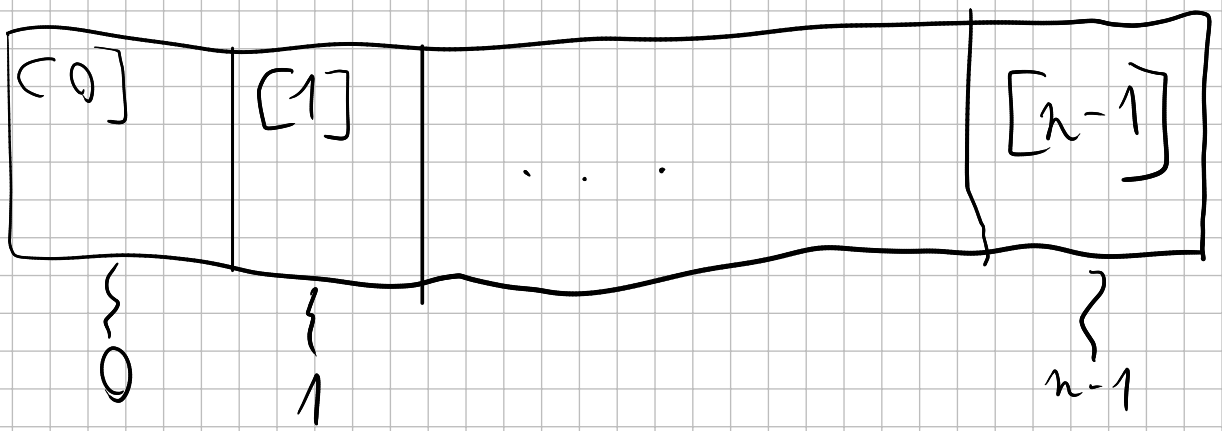
$\mathbb{Z}$, $n \mid a - b$ $\quad a \equiv b \pmod{n}$

oznaczenie relacji → oznaczenie

$a \,\%\, n \Leftrightarrow a \bmod n$

$\bmod$ ← działanie

$\mathbb{Z}, n$



$$\{0, 1, \ldots, n-1\} \overset{\text{wzn}}{=} \mathbb{Z}_n$$

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

$20x = 6 + 74k$

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

Def

k - reszta z dzielenia

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

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

$\frac{5}{x}$ odw $= \frac{1}{x}$ podobnie $\frac{5}{x}$

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

$10^{-1} \equiv (-11) \pmod{37} \Leftrightarrow$
$10^{-1} \equiv 26 \pmod{37} \Leftrightarrow$
$10^{-1} = 63 \pmod{37}$

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

$NWD(k, n) = 1$

RAE

$NWD(k, n) = 1 \Rightarrow \bigvee_{n,t \in \mathbb{Z}} nk + tn = 1 \Rightarrow nk = 1 \pmod{n}$

$NWD(k, n) > 1 \Rightarrow nk \equiv 1 \pmod{n}, nk = 1 + m \cdot n$

$1 = nk - mn$

sprzeczność bo $d \mid nk - mn$ a $d \nmid 1$

Tw Jedyność elementu odwrotnego

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

Dow.

$m = m \cdot 1 = m(k \cdot l) = m \cdot k \cdot l = 1 \cdot l$

Układy kongruencji

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

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

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

$13k = 3 \pmod{15}$

$-2k = 3 \pmod{15}$

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

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

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

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

$k = 6 \pmod{15}$

$k = 6 + 15l$

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

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

rozwiązanie równania kongruencji: $x = 79 + 195l$

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

CHIŃSKIE TWIERDZENIE O RESZTACH

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

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

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

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

istnieje <u>tylko jedno</u> rozwiązanie x

spełniające (*)

Każde inne rozwiązanie różni się od x_0

o wielokrotność $m \cdot n$

$$\begin{cases} 0 \leq x_0 \leq n \cdot n - 1 \\ x = x_0 + k \cdot m \cdot n \end{cases}$$

Ind

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

$\wedge$ NWD$(n_1, n_j) = 1$

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

$x = a_2 \pmod{n_2}$

$\ldots$

$x = a_k \pmod{n_k}$

ma jedno rozwiązanie w zbiorze $\{0, 1, \ldots, n_1 \cdot \ldots \cdot n_k - 1\}$

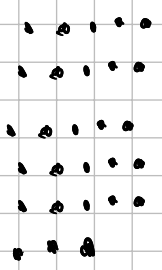
$x = x_0 + n_1 \cdot n_2 \cdot \ldots \cdot n_k \cdot m, \quad m \in \mathbb{Z}$

ustawi zostało

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 – moduły $\quad NWD(m,n) = 1$

$\{0, 1, \ldots, m \cdot n - 1\} \overset{CTR}{\longleftrightarrow} \{(a,b)\}$ $\quad a \in \mathbb{Z}_m, b \in \mathbb{Z}_n$

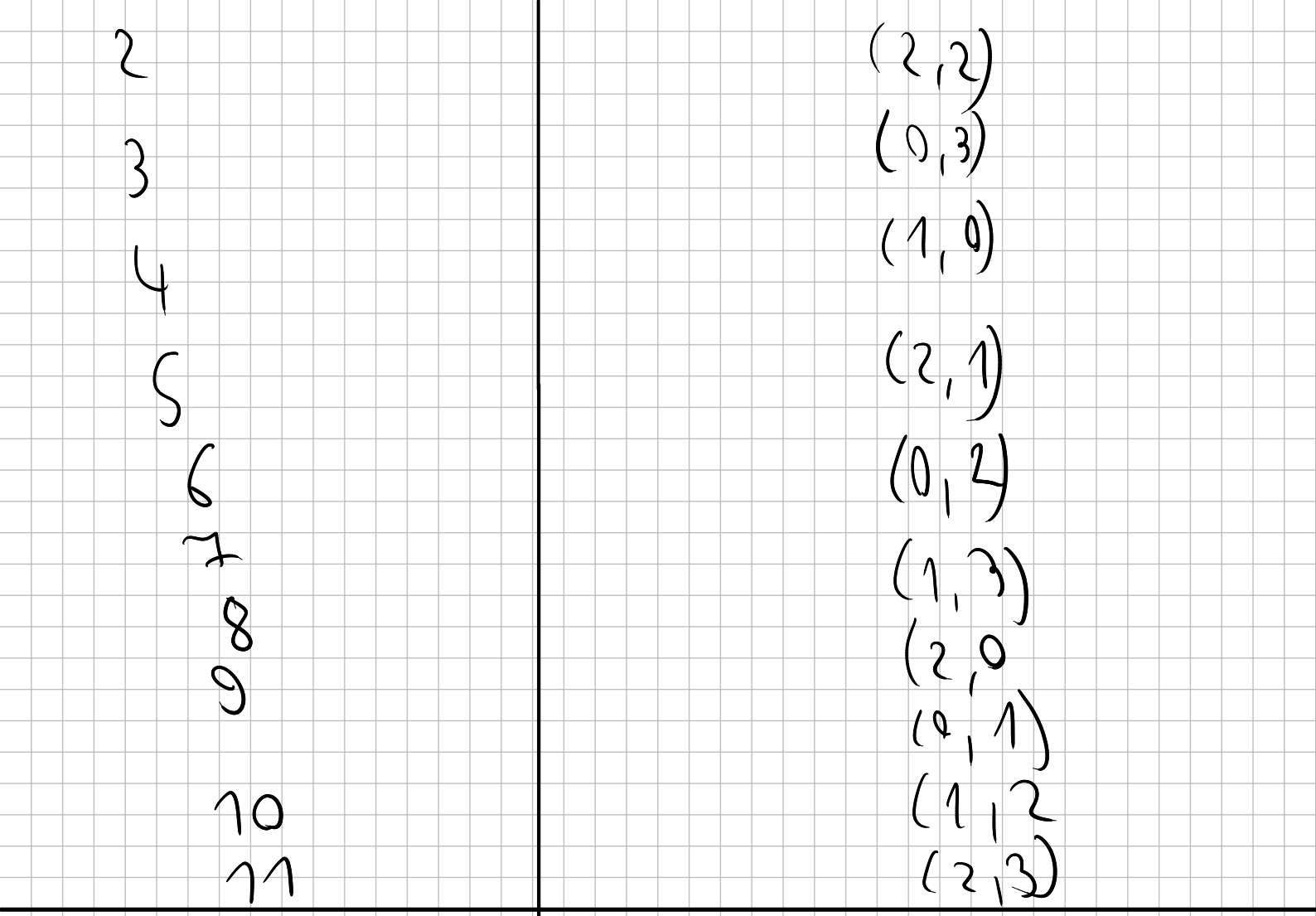
$m = 13, \quad n = 15$

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

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

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

x	$(x \bmod 3, x \bmod 4)$
$\mathbb{Z}_{12}$	$\mathbb{Z}_3 \times \mathbb{Z}_4$
0	(0, 0)
1	(1, 1)



pozycyjność jest wredna

1A3 ten

X11 ten

1011 ten

$u32 + u32$

2^{32} $2^{32}-1$

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

Bigint is kinda fast RN

1
2
4
8
16

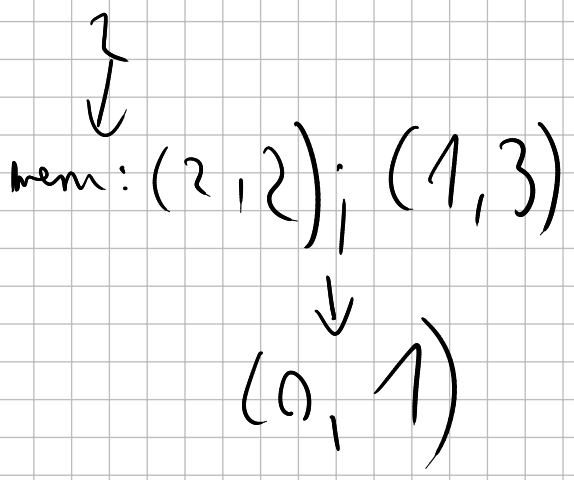
$$\begin{array}{r} 110 \\ 111 \\ \hline 1001 \end{array}$$

ONE clock cycle

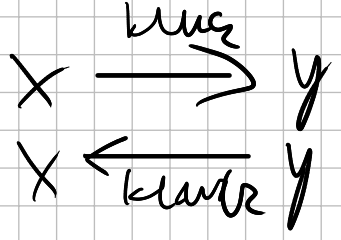
$2+7=9$

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

$(2\%3, 2\%4)+(7\%3, 7\%4)$

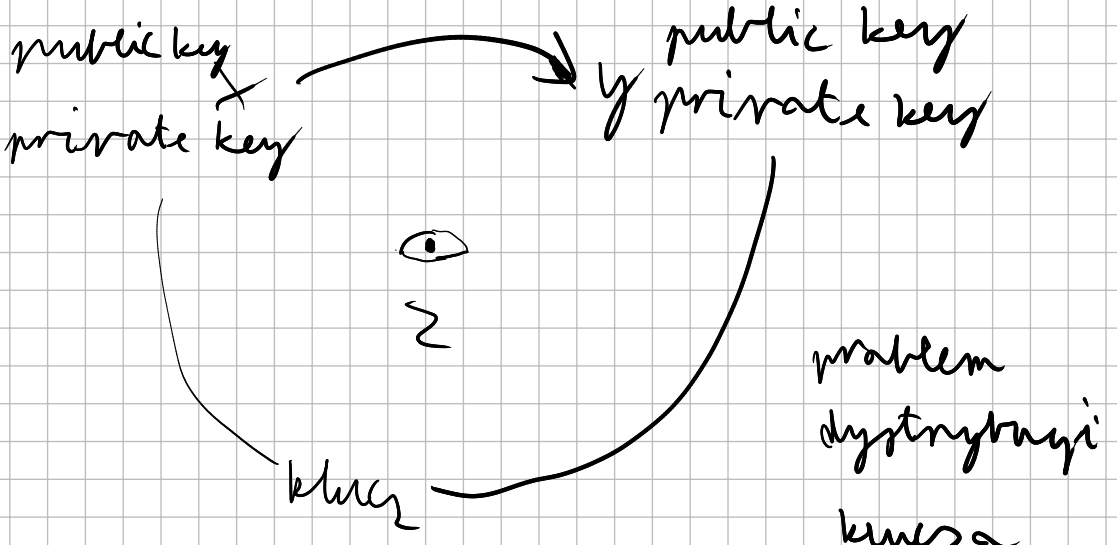


KRYPTOGRAFIA:



szyfrowanie 1 klucz publiczny

AES



problem dystrybucji kluczy