

Stefan Sokołowski

MATEMATYKA DYSKRETNA

wykład 5

Inst. Informatyki Stosowanej, ANS
Elbląg, 2024/2025

Wykład 5, str. 1

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$			
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$			
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$			
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$			
F	$q \mid a^n \iff q \mid a$			
G	$q \mid a^2 \iff q \mid a \bmod q$			

A: z zał.: $r = q \cdot k \wedge a = r \cdot \ell$
więc: $a = (q \cdot k) \cdot \ell = q \cdot (k \cdot \ell)$
stąd: $q \mid a$

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$			
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$			
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$			
F	$q \mid a^n \iff q \mid a$			
G	$q \mid a^2 \iff q \mid a \bmod q$			

B: z zał.: $a = q \cdot k \wedge b = q \cdot \ell$
 więc: $ab = (q \cdot k) \cdot (q \cdot \ell) = q^2 \cdot (k \cdot \ell)$
 stąd: $q^2 \mid ab$

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie		
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$			
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$			
F	$q \mid a^n \iff q \mid a$			
G	$q \mid a^2 \iff q \mid a \bmod q$			

C: kontrprzykład: $2 \mid 4 \wedge 4 \mid 4$
 ale: $2 \cdot 4 \nmid 4$

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie	tak	
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$			
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$			
F	$q \mid a^n \iff q \mid a$			
G	$q \mid a^2 \iff q \mid a \bmod q$			

C: z tw. o jednozn. rozkł.:

$$a = \underbrace{p_1 \dots p_a}_{q} \cdot \underbrace{p'_1 \dots p'_b}_r \cdot \underbrace{p''_1 \dots p''_c}$$

żadnych wspólnych

p_i, p'_i, p''_i — liczby pierwsze

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie	tak	
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$	tak		
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$			
F	$q \mid a^n \iff q \mid a$			
G	$q \mid a^2 \iff q \mid a \bmod q$			

D: z zał.: $a = q \cdot k \wedge b = r \cdot \ell$

więc: $ab = (q \cdot k) \cdot (r \cdot \ell) = (q \cdot r) \cdot (k \cdot \ell)$

stąd: $qr \mid ab$

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie	tak	
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$	tak		
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$	tak		
F	$q \mid a^n \iff q \mid a$			
G	$q \mid a^2 \iff q \mid a \bmod q$			

E: z zał.: $a = q \cdot k \wedge k = (a/q) = r \cdot \ell$
 więc: $a = q \cdot (r \cdot \ell) = r \cdot (q \cdot \ell) \wedge (a/r) = q \cdot \ell$
 stąd: $r \mid a \wedge q \mid (a/r)$

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie	tak	
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$	tak		
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$	tak		
F	$q \mid a^n \iff q \mid a$	nie	—	
G	$q \mid a^2 \iff q \mid a \bmod q$			

F: kontrprzykład: $4 \mid 2^2$
 ale: $4 \nmid 2$

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie	tak	
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$	tak		
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$	tak		
F	$q \mid a^n \iff q \mid a$	nie	—	tak
G	$q \mid a^2 \iff q \mid a \bmod q$			

Podzielność

Własności podzielności przez liczby pierwsze, względnie pierwsze i wcale nie pierwsze

Zakładamy, że q, r, a, b, n są całkowite dodatnie.

	własność	dla wszystkich dodatnich	jeśli q i r względnie pierwsze	jeśli q pierwsze
A	$q \mid r \wedge r \mid a \Rightarrow q \mid a$	tak		
B	$q \mid a \wedge q \mid b \Rightarrow q^2 \mid ab$	tak		
C	$q \mid a \wedge r \mid a \Rightarrow qr \mid a$	nie	tak	
D	$q \mid a \wedge r \mid b \Rightarrow qr \mid ab$	tak		
E	$q \mid a \wedge r \mid (a/q) \Rightarrow r \mid a \wedge q \mid (a/r)$	tak		
F	$q \mid a^n \iff q \mid a$	nie	—	tak
G	$q \mid a^2 \iff q \mid a \bmod q$	nie	—	tak

Polityka zaokrągleń do liczb całkowitych



Art. 96.

1. Sejm składa się z 460 posłów.
2. Wybory do Sejmu są powszechne, równe, bezpośrednie i **proporcjonalne** oraz odbywają się w głosowaniu tajnym.

Co to znaczy?
Jaki współczynnik proporcjonalności??

Czy to w ogóle da się zrobić?

Polityka zaokrągleń do liczb całkowitych

Głosowało: 21 596 674 wyborców

Miejsc w Sejmie: 460

„Cena” 1 miejsca: $\frac{21\,596\,674}{460} \approx 46\,949.291\,30$

partia	uzyskane głosy	mandaty	
		proporcjonalne	faktyczne
PiS	7 640 854	162.746 950 8	194
KO	6 629 402	141.203 452 0	157
3. Droga	3 110 670	66.255 952 19	65
Nowa Lewica	1 859 018	39.596 295 24	26
Konfederacja	1 547 364	32.958 197 17	18

... więc wybory **nie są** proporcjonalne.

Liczby pochodzą z
<https://sejmsenat2023.pkw.gov.pl/sejmsenat2023/pl/sejm/wynik/pl>

Polityka zaokrągleń do liczb całkowitych

Wybory **nie są** proporcjonalne. To wynika

- trochę z metody d'Hondta zaokrąglania,
- z progu 5-procentowego,
- głównie z samej konieczności zaokrąglania **w okręgach**.

Partia pechowa może stracić na zaokrąglaniu do 41 mandatów (po 1 w okręgu).

Ordynacja wyborcza „proporcjonalna zaokrąglana” sprowadza się

- przy okręgach 1-mandatowych $\longrightarrow$ do czysto większościowej
- przy okręgu 460-mandatowym $\longrightarrow$ do prawie proporcjonalnej

U nas okręgi są ok. 11-mandatowe...

nwd jako kombinacja liniowa

Wiemy, że dla dowolnych $a, b \in \mathbb{Z}$ (t.ż. przynajmniej jedna jest niezerowa) istnieją współczynniki $x, y \in \mathbb{Z}$ spełniające

$$x \cdot a + y \cdot b = \text{nwd}(a, b)$$

Ale takich współczynników jest dużo...

Twierdzenie: *Jeżeli*

$$x \cdot a + y \cdot b = \text{nwd}(a, b)$$

to dla każdego $t \in \mathbb{Z}$ zachodzi

$$\left(x + \frac{b \cdot t}{\text{nwd}(a, b)}\right) \cdot a + \left(y - \frac{a \cdot t}{\text{nwd}(a, b)}\right) \cdot b = \text{nwd}(a, b)$$

Dowód:

$$\begin{aligned} &\left(x + \frac{b \cdot t}{\text{nwd}(a, b)}\right) \cdot a + \left(y - \frac{a \cdot t}{\text{nwd}(a, b)}\right) \cdot b \\ &= x \cdot a + \frac{b \cdot t \cdot a}{\text{nwd}(a, b)} + y \cdot b - \frac{a \cdot t \cdot b}{\text{nwd}(a, b)} = x \cdot a + y \cdot b = \text{nwd}(a, b) \end{aligned}$$

□

Gdzie szukać liczb pierwszych?

Twierdzenie:

Dla każdej liczby naturalnej $n \geq 1$ istnieje liczba pierwsza p taka, że

$$n < p \leq n! + 1$$

Dowód:

Jeśli $n! + 1$ jest pierwsza, to $p = n! + 1$.

Jeśli $n! + 1$ jest złożona, to niech $p \geq 2$ — pierwsza t.ż.

$$p \mid n! + 1$$

Oczywiście $p \leq n! + 1$; ale czy $n < p$?

Gdyby $p \leq n$, to $p \mid n!$; jednocześnie $p \mid n! + 1$; więc

$$p \mid (n! + 1) - n! = 1$$

— sprzeczne z tym

□

nwd i nww

Definicja: (nwd)

Największy wspólny **dzielnik** liczb $a, b \in \mathbb{Z} \setminus \{0\}$ to **największa** taka $d \in \mathbb{N}$, że

$$d \mid a \quad \text{ i } \quad d \mid b$$

Oznaczenie: $d = \text{nwd}(a, b)$

Twierdzenie:

$$\text{nwd}(a, b) \cdot \text{nww}(a, b) = |a| \cdot |b|$$

Dowód: (bardzo nieformalny...)

Rozpiszmy obie liczby na iloczynny czynników pierwszych:

$$a = p_1 \cdot \dots \cdot p_n$$

$$b = p'_1 \cdot \dots \cdot p'_m$$

Oczywiście $|ab| = p_1 \cdot \dots \cdot p_n \cdot p'_1 \cdot \dots \cdot p'_m$.

Iloczyn tych czynników, które występują zarówno w rozkładzie a jak w rozkładzie b to $\text{nwd}(a, b)$. Jeśli wykreślimy z tego iloczynu **jedną ich kopię**, czyli podzielimy iloczyn ab przez $\text{nwd}(a, b)$, to pozostanie jedna kopia wspólnych, oraz te, które występują w rozkładzie tylko jednej z liczb. Czyli pozostanie minimum tego, co jest potrzebne, żeby dzielić się zarówno przez a jak przez b . Czyli $\text{nww}(a, b)$.

□

Definicja: (nww)

Najmniejsza wspólna **wielokrotność** liczb $a, b \in \mathbb{Z} \setminus \{0\}$ to **najmniejsza** taka $k \in \mathbb{N}$, że

$$a \mid k \quad \text{ i } \quad b \mid k$$

Oznaczenie: $d = \text{nww}(a, b)$

nwd i nww

Prosty wniosek:

$$a \text{ i } b \text{ są względnie pierwsze} \iff \text{nww}(a, b) = |a \cdot b|$$

Przykład:

$$24 = 4 \cdot 6 = 2 \cdot 12 = \text{nwd}(4, 6) \cdot \text{nww}(4, 6)$$

$$24 = \underbrace{2 \cdot 2}_4 \cdot \overbrace{2 \cdot 3}^6 = \underbrace{2}_2 \cdot \overbrace{2 \cdot 2 \cdot 3}^{12}$$

Przykład:

$$810 = 18 \cdot 45 = 9 \cdot 90 = \text{nwd}(18, 45) \cdot \text{nww}(18, 45)$$

$$810 = \underbrace{2 \cdot 3 \cdot 3}_{18} \cdot \overbrace{3 \cdot 3 \cdot 5}^{45} = \underbrace{3 \cdot 3}_9 \cdot \overbrace{2 \cdot 3 \cdot 3 \cdot 5}^{90}$$

Kongruencje

równoważne sformułowania

Definicja: (kongruencja)

Niech $n \in \mathbb{N} \setminus \{0, 1\}$ i $a, b \in \mathbb{Z}$. Wtedy

$$\left. \begin{array}{l} a \text{ przystaje do } b \text{ modulo } n \\ a \text{ jest równe } b \text{ modulo } n \\ a \text{ jest kongruentne do } b \text{ modulo } n \\ a \equiv b \pmod{n} \\ a \equiv_n b \end{array} \right\} \stackrel{\text{def}}{\iff} \left\{ \begin{array}{l} a \bmod n = b \bmod n \\ n \mid a - b \end{array} \right.$$

równoważne warunki

Twierdzenie:

Niech $n \in \mathbb{N} \setminus \{0, 1\}$ i $a, b, c \in \mathbb{Z}$. Wtedy

1. $a \equiv_n a$
2. jeśli $a \equiv_n b$ to $b \equiv_n a$
3. jeśli $a \equiv_n b$ i $b \equiv_n c$ to $a \equiv_n c$

Wniosek:

$\equiv_n$ jest relacją równoważności w $\mathbb{Z}$

Oznaczenie: $[a]_n$ — klasa abstrakcji relacji $\equiv_n$

Kongruencje

Przykłady:

$$[0]_7 = [-7]_7 = [7]_7 = [14]_7 = \{\dots, -14, -7, 0, 7, 14, 21, \dots\}$$

$$[5]_7 = [-2]_7 = [12]_7 = [19]_7 = \{\dots, -9, -2, 5, 12, 19, 26, \dots\}$$

$$[-11]_{12} = [-23]_{12} = [1]_{12} = [13]_{12} = \{\dots, -35, -23, 1, 13, 25, \dots\}$$

Zadanie:

Wyznaczyć zbiór $[16]_5 \cap [11]_4$.

$[16]_5$ — zbiór liczb, których reszta z dzielenia przez 5 jest taka sama jak dla 16, czyli 1

$[11]_4$ — zbiór liczb, których reszta z dzielenia przez 4 jest taka sama jak dla 11, czyli 3

Część wspólna — liczby postaci $5a + 1$ i jednocześnie $4b + 3$.

$$5a + 1 = 4b + 3$$

$$5a - 4b = 2 \quad \text{— równanie diofantyczne; rozwiązanie: } a = 4t + 2 \quad b = 5t + 2$$

$$5 \cdot (4t + 2) + 1 = 20t + 11$$

Odpowiedź:

$$[16]_5 \cap [11]_4 = [11]_{20}$$

Własności relacji $\equiv_n$

Twierdzenie:

$$\text{Jeżeli } \left\{ \begin{array}{l} a \equiv_n b \\ c \equiv_n d \end{array} \text{ oraz} \right\}, \text{ to } \left\{ \begin{array}{l} a + c \equiv_n b + d \\ a - c \equiv_n b - d \\ a \cdot c \equiv_n b \cdot d \end{array} \right. \begin{array}{l} i \\ i \\ i \end{array}$$

Dowód:

Z założenia istnieją k i ℓ t.ż. $a - b = kn$ i $c - d = \ell n$. Więc

$$(a + c) - (b + d) = (a - b) + (c - d) = kn + \ell n = (k + \ell)n \quad \text{więc} \quad a + c \equiv_n b + d$$

$$(a - c) - (b - d) = (a - b) - (c - d) = kn - \ell n = (k - \ell)n \quad \text{więc} \quad a - c \equiv_n b - d$$

$$ac - bd = a(c - d) + d(a - b) = a\ell n + dkn = (a\ell + dk)n \quad \text{więc} \quad ac \equiv_n bd$$

□

W zasadzie **kongruencją** nazywa się ogólnie równoważność „zgodną” z działaniami. To twierdzenie wykazuje, że $\equiv_n$ jest kongruencją.

Wniosek:

Jeżeli $a \equiv_n b$, to $a^k \equiv_n b^k$.

To ułatwia szybkie rachunki reszt. Np.: jaka jest reszta z dzielenia 723^{32} przez 20?

$$723^{32} \equiv_{20} 3^{32} = 81^8 \equiv_{20} 1^8 = 1$$

kongruencja

równość

Własności relacji $\equiv_n$

A jak jest z dzieleniem?

$$\text{Czy } \left\{ \begin{array}{l} a \equiv_n b \\ c \equiv_n d \end{array} \right\} \text{ oraz } \Rightarrow a/c \equiv_n b/d ?$$

$$\text{Mamy } \left\{ \begin{array}{l} 10 \equiv_6 4 \\ 2 \equiv_6 2 \end{array} \right\} \text{ — } \left\{ \begin{array}{l} \text{czy } 10/2 \equiv_6 4/2 \text{ ?} \\ \text{czyli czy } 5 \equiv_6 2 \text{ ?} \end{array} \right\}$$

Ale $6 \nmid 5-2$, więc tak nie jest.

Wniosek:

Relacja $\equiv_n$ jest kongruencją za względu na dodawanie, odejmowanie i mnożenie. Ale nie jest kongruencją ze względu na dzielenie.

Własności relacji $\equiv_n$

Ale jednak (z pewnymi zastrzeżeniami — patrz niżej) kongruencje można skracać przez wspólny czynnik...

Twierdzenie: (o skracaniu)

$$\text{Z } ax \equiv_n ay \text{ wynika } x \equiv_{(n/\text{nwd}(a,n))} y.$$

Wniosek:

Jeśli a i n są względnie pierwsze, to z $ax \equiv_n ay$ wynika $x \equiv_n y$ (można skracać przez czynnik względnie pierwszy z modułem).

Dowód: (tw. o skracaniu)

Z założenia wynika $a(x - y) = n \cdot k$ dla pewnego $k \in \mathbb{Z}$. Wobec tego

$$\frac{a}{\text{nwd}(a,n)} \cdot (x - y) = \frac{n}{\text{nwd}(a,n)} \cdot k$$

$\frac{a}{\text{nwd}(a,n)}$ i $\frac{n}{\text{nwd}(a,n)}$ są względnie pierwsze. Więc pierwsza z nich nie może dzielić się przez żaden czynnik drugiej; wobec tego $\frac{n}{\text{nwd}(a,n)}$ dzieli $x - y$. Stąd teza.

□

Własności relacji $\equiv_n$

Przykład: (skracania)

$$2 \cdot 9 = 18 = 4 \cdot 4 + 2$$

$$2 \cdot 7 = 14 = 4 \cdot 3 + 2$$

więc

$$\cancel{2} \cdot 9 \equiv_4 \cancel{2} \cdot 7$$

czyli

$$\cancel{9} \equiv_4 \cancel{7} \quad \text{--- NIE!}$$

ale $\frac{4}{\text{nwd}(2,4)} = \frac{4}{2} = 2$, więc

$$9 \equiv_2 7$$

Przykład: (skracania)

$$25 \cdot 1 = 25 = 15 \cdot 1 + 10$$

$$25 \cdot 4 = 100 = 15 \cdot 6 + 10$$

więc

$$\cancel{25} \cdot 1 \equiv_{15} \cancel{25} \cdot 4$$

czyli

$$\cancel{1} \equiv_{15} \cancel{4} \quad \text{--- NIE!}$$

ale $\frac{15}{\text{nwd}(25,15)} = \frac{15}{5} = 3$, więc

$$1 \equiv_3 4$$

Liniowe równania „modulo”

Przykład:

Znaleźć wszystkie rozwiązania kongruencji

$$3x \equiv_8 5$$

Przejrzenie wszystkich reszt:

$[x]_8$	$[3x]_8$
$[0]_8$	$[0]_8$
$[1]_8$	$[3]_8$
$[2]_8$	$[6]_8$
$[3]_8$	$[1]_8$
$[4]_8$	$[4]_8$
$[5]_8$	$[7]_8$
$[6]_8$	$[2]_8$
$[7]_8$	$[5]_8$

$$3 \cdot 7 \equiv_8 5$$

Rozwiązanie systematyczne:

$$3x + 8t = 5$$

Znaleźć nwd współczynników:

$$8 = 8 \cdot 1 + 3 \cdot 0$$

$$3 = 8 \cdot 0 + 3 \cdot 1$$

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

$$1 = 8 \cdot (-1) + 3 \cdot 3$$

$$8 \cdot (-1) + 3 \cdot 3 = 1 \quad || \text{ mod } 8$$

$$3 \cdot 3 \equiv_8 1 \quad || \cdot 5$$

$$3 \cdot 15 \equiv_8 5 \quad 15 \equiv_8 7$$

$$3 \cdot 7 \equiv_8 5$$

Liniowe równania „modulo”

Twierdzenie: (o rozwiązywaniu równań „modulo”)

Jeśli a i n są względnie pierwsze, to kongruencja

$$a \cdot x \equiv_n b$$

ma w zbiorze $\{0, 1, 2, \dots, n-1\}$ **dokładnie jedno rozwiązanie**.

Dowód:

Względnie pierwsze — więc istnieją $s, t \in \mathbb{Z}$ t.ż.

$$as + nt = 1 \quad || \cdot b$$

$$asb + ntb = b \quad || \bmod n$$

$$a(sb) \equiv_n b$$

więc $x = sb \bmod n$ jest rozwiązaniem.

Gdyby były dwa rozwiązania

$$a \cdot x_0 \equiv_n b \quad \text{oraz} \quad a \cdot x_1 \equiv_n b$$

to

$$a \cdot x_0 \equiv_n a \cdot x_1$$

co można skrócić do

$$x_0 \equiv_n x_1$$

ponieważ a i n są względnie pierwsze.

□

Liniowe równania „modulo”

Twierdzenie: (o rozwiązywaniu równań „modulo”)

Rozwiązania równania „modulo” $a \cdot x \equiv_n b$ są jak niżej:

(a) jeśli $d = \text{nwd}(a, n) \nmid b$ to rozwiązań nie ma;

(b) jeśli $d = \text{nwd}(a, n) \mid b$ to wszystkie rozwiązania w zbiorze $\{0, 1, \dots, n-1\}$ są postaci

$$x_0 + k \cdot \frac{n}{d} \quad \text{dla } 0 \leq k < d$$

gdzie x_0 jest rozwiązaniem równania uproszczonego

$$\frac{a}{d} \cdot x \equiv_{\frac{n}{d}} \frac{b}{d}$$

Dowód: — punkt (a)

$$a \cdot x \equiv_n b \iff \exists_{\ell \in \mathbb{Z}} ax + \ell n = b$$

$$\iff \exists_{\ell \in \mathbb{Z}} d \cdot \left(\frac{a}{d} \cdot x + \frac{n}{d} \cdot \ell \right) = b$$

więc b musi dzielić się przez d , żeby zachodziła równość.

□

Liniowe równania „modulo”

Twierdzenie: (o rozwiązywaniu równań „modulo”)

Rozwiązania równania „modulo” $a \cdot x \equiv_n b$ są jak niżej:

- (a) jeśli $d = \text{nwd}(a, n) \nmid b$ to rozwiązań nie ma;
 (b) jeśli $d = \text{nwd}(a, n) \mid b$ to wszystkie rozwiązania w zbiorze $\{0, 1, \dots, n-1\}$ są postaci

$$x_0 + k \cdot \frac{n}{d} \quad \text{dla } 0 \leq k < d$$

gdzie x_0 jest rozwiązaniem równania uproszczonego

$$\frac{a}{d} \cdot x \equiv_{\frac{n}{d}} \frac{b}{d}$$

Dowód: — punkt (b)

$$\begin{aligned} a \cdot x \equiv_n b &\iff \exists \ell \in \mathbb{Z} \ a \cdot x - b = n \cdot \ell \\ &\iff \exists \ell \in \mathbb{Z} \ \frac{a}{d} \cdot x - \frac{b}{d} = \frac{n}{d} \cdot \ell \end{aligned}$$

więc x musi być rozwiązaniem równania

$$\frac{a}{d} \cdot x \equiv_{\frac{n}{d}} \frac{b}{d}$$

a takie rozwiązanie x_0 jest tylko jedno w zbiorze $\{1, 2, \dots, \frac{n}{d} - 1\}$.

$$\begin{aligned} a \cdot (x_0 + k \cdot \frac{n}{d}) &= d \cdot \frac{a}{d} \cdot x_0 + k \cdot \frac{a}{d} \cdot n = d \cdot (\frac{n}{d} \cdot \ell + \frac{b}{d}) + k \cdot \frac{a}{d} \cdot n \\ &= b + n \cdot (\ell + k \cdot \frac{a}{d}) \equiv_n b \end{aligned}$$

□

Liniowe równania „modulo”

Zadanie:

Wyznaczyć wszystkie rozwiązania kongruencji

$$8 \cdot x \equiv_{20} 12$$

w zbiorze $\{0, 1, \dots, 19\}$.

Rozwiązanie:

$$\text{nwd}(8, 20) = 4$$

Ponieważ $4 \mid 12$, rozwiązania istnieją.

Zacznijmy od równania uproszczonego

$$\frac{8}{4} \cdot x \equiv_{\frac{20}{4}} \frac{12}{4} \quad \text{czyli} \quad 2 \cdot x \equiv_5 3$$

Jego rozwiązaniem jest oczywiście $x = 4$; więc wszystkie rozwiązania równania oryginalnego to

$$4 + 0 \cdot \frac{20}{4}, 4 + 1 \cdot \frac{20}{4}, 4 + 2 \cdot \frac{20}{4}, 4 + 3 \cdot \frac{20}{4}$$

czyli

$$4, 9, 14, 19$$

Liniowe równania „modulo”

Zadanie:

Wyznaczyć wszystkie rozwiązania kongruencji

$$2912 \cdot x \equiv_{3060} 284$$

w zbiorze $\{0, 1, \dots, 3059\}$.

Rozwiązanie:

Z algorytmu Euklidesa wyznaczamy $\text{nwd}(2912, 3060) = 4$

Ponieważ $4 \mid 284$, rozwiązania istnieją.

Zacznijmy od równania uproszczonego

$$\frac{2912}{4} \cdot x \equiv_{\frac{3060}{4}} \frac{284}{4} \quad \text{czyli} \quad 728 \cdot x \equiv_{765} 71 \quad \text{czyli} \quad 728 \cdot x + 765 \cdot k = 71$$

Z algorytmu Euklidesa mamy $728 \cdot 62 \equiv_{765} 1$, więc $728 \cdot 62 \cdot 71 \equiv_{765} 71$, więc $728 \cdot 440 \equiv_{765} 71$, więc $728 \cdot 577 \equiv_{765} 71$

Wszystkie rozwiązania równania oryginalnego to

$$577 + 0 \cdot \frac{3060}{4}, 577 + 1 \cdot \frac{3060}{4}, 577 + 2 \cdot \frac{3060}{4}, 577 + 3 \cdot \frac{3060}{4}$$

czyli

$$577, 1342, 2107, 2872$$