

Stefan Sokołowski

MATEMATYKA DYSKRETNA

wykład 6

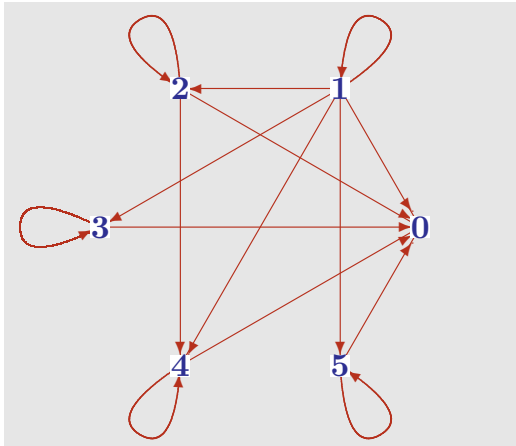
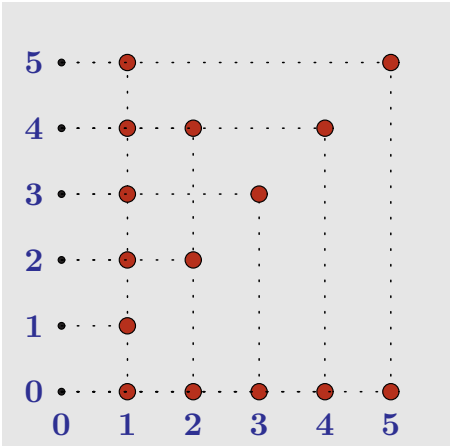
Inst. Informatyki Stosowanej, ANS
Elbląg, 2024/2025

Wykład 6, str. 1

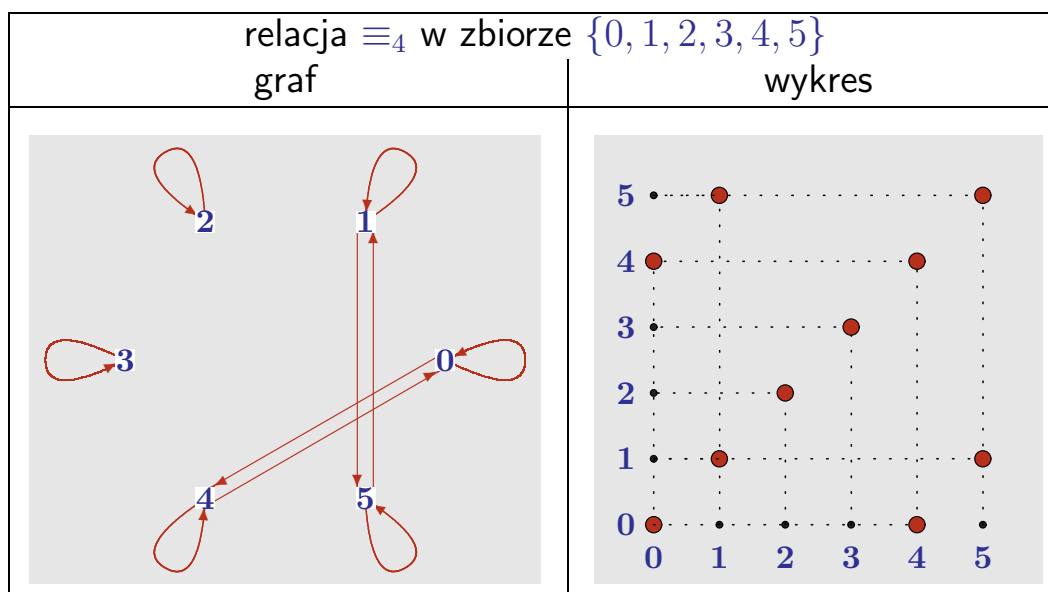
Powtórka z relacji

Bedziemy rozważać relacje między elementami jakiegoś zbioru X oraz **tego samego** zbioru X

Oznaczenia: a jest w relacji R z b $\begin{cases} aRb \\ (a, b) \in R \end{cases}$

relacja (podzielność) w zbiorze $\{0, 1, 2, 3, 4, 5\}$ graf	wykres
	

Powtórka z relacji



Powtórka z relacji

Definicja: (własności relacji)

Relacja R w zbiorze X jest

- *zwrotna*, jeżeli $\forall_{x \in X} xRx$
- *symetryczna*, jeżeli $\forall_{x,y \in X} xRy \implies yRx$
- *przechodnia*, jeżeli $\forall_{x,y,z \in X} xRy \wedge yRz \implies xRz$

Definicja: (równoważność)

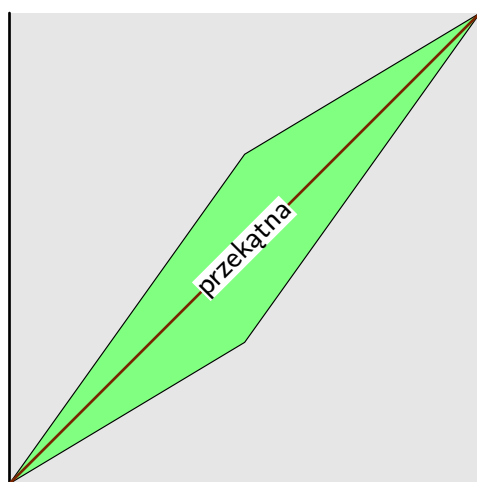
Relacja R w zbiorze X jest relacją *równoważności*, jeżeli jest zwrotna, symetryczna i przechodnia.

Powtórka z relacji

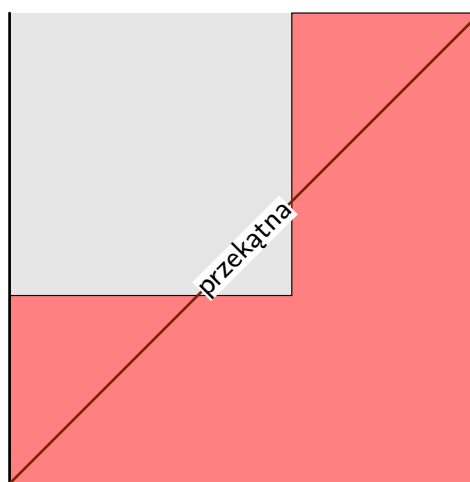
Przykłady:

- **różność w $\mathbb{Z}$:** $pRq \stackrel{\text{def}}{\iff} p \neq q$
symetryczna, ale
nie zwrotna (np. $\neg 0 \neq 0$)
nie przechodnia (np. $0 \neq 1 \wedge 1 \neq 0$ ale $\neg 0 \neq 0$)
- **ostra mniejszość w $\mathbb{Z}$:** $pRq \stackrel{\text{def}}{\iff} p < q$
przechodnia, ale
nie zwrotna (np. $\neg 0 < 0$)
nie symetryczna (np. $0 < 1$ ale $\neg 1 < 0$)
- **nieostra mniejszość w $\mathbb{Z}$:** $pRq \stackrel{\text{def}}{\iff} p \leq q$
przechodnia, zwrotna, ale
nie symetryczna (np. $0 \leq 1$ ale $\neg 1 \leq 0$)
- **względna pierwszość w $\mathbb{Z} \setminus \{0\}$:** $pRq \stackrel{\text{def}}{\iff} \text{nwd}(p, q) = 1$
symetryczna, ale
nie zwrotna (np. $\neg \text{nwd}(5, 5) = 1$)
nie przechodnia (np. $\text{nwd}(2, 3) = 1 \wedge \text{nwd}(3, 4) = 1$ ale $\neg \text{nwd}(2, 4) = 1$)

Własności relacji a postacie ich wykresów



zwrotna

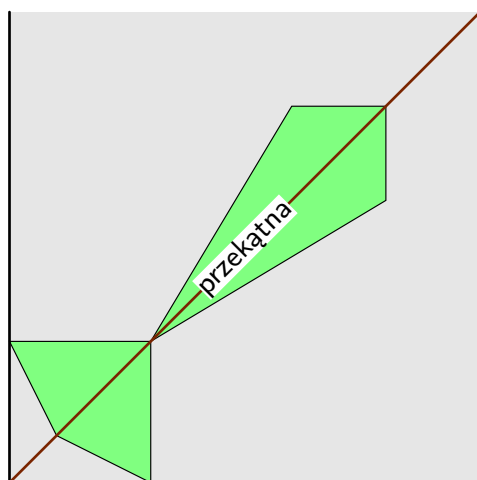


niezwrotna

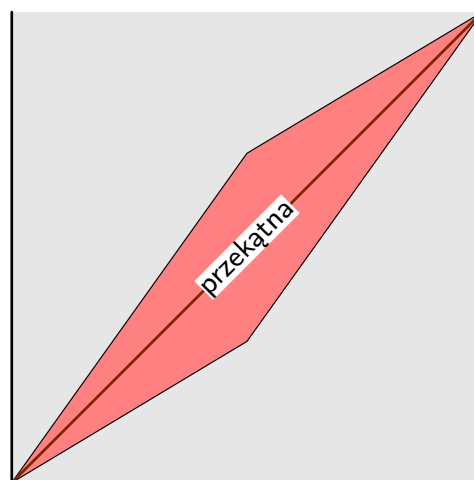
Nieformalnie:

Relacja jest **zwrotna** jeśli jej wykres zawiera przekątną.

Własności relacji a postacie ich wykresów



symetryczna



niesymetryczna

Nieformalnie:

Relacja jest **symetryczna** jeśli jej wykres jest symetryczny względem przekątnej.

Relacje równoważności

(zwrotne, symetryczne, przechodnie)

Przykłady:

- (a) równość w dowolnym X : $xRy \stackrel{\text{def}}{\iff} x = y$
- (b) równość wartości funkcji $f : X \rightarrow Y$:
 $x_1Rx_2 \stackrel{\text{def}}{\iff} f(x_1) = f(x_2)$
- (c) równoważność „modulo” n w $\mathbb{Z}$:
 $pRq \stackrel{\text{def}}{\iff} p \equiv_n q$
 $\iff$ reszty z dzielenia p i q przez n są równe

Powyższe przykłady (a) i (c) to szczególne przypadki przykładu (b).

Relacje równoważności

Definicja: (klasy abstrakcji)

Niech R będzie relacją równoważności w zbiorze X i niech $x \in X$. Przez klasę abstrakcji (inaczej: klasę równoważności) elementu x względem relacji R rozumiemy zbiór

$$[x]_R \stackrel{\text{def}}{=} \{x' \in X \mid x'Rx\}$$

czyli zbiór tych elementów zbioru X , które są w relacji R z x .

Wniosek ze zwrotności:

Przy założeniach jak wyżej: $x \in [x]_R$.

Twierdzenie: (o klasach abstrakcji)

Jeśli R jest relacją równoważności w zbiorze X , to dla każdych elementów $x_1 \in X$ oraz $x_2 \in X$

- jeśli x_1Rx_2 , to oba wyznaczają tę samą klasę abstrakcji: $[x_1]_R = [x_2]_R$
- jeśli $\neg x_1Rx_2$, to ich klasy abstrakcji są rozłączne: $[x_1]_R \cap [x_2]_R = \emptyset$

(To wynika z symetryczności i przechodniości R)

Relacje równoważności

Definicja: (zbiór ilorazowy)

Niech R będzie relacją równoważności w zbiorze X . Zbiór klas abstrakcji wszystkich elementów zbioru X względem relacji R oznaczamy przez X/R i nazywamy zbiorem ilorazowym X przez R :

$$X/R \stackrel{\text{def}}{=} \{[x]_R \mid x \in X\}$$

(X/R jest więc zbiorem zbiorów)

Definicja: (przekształcenie ilorazowe)

Niech R będzie relacją równoważności w zbiorze X . Przez przekształcenie ilorazowe rozumiemy funkcję

$$\begin{aligned} \varphi_R : X &\rightarrow X/R \\ \varphi_R(x) &\stackrel{\text{def}}{=} [x]_R \end{aligned}$$

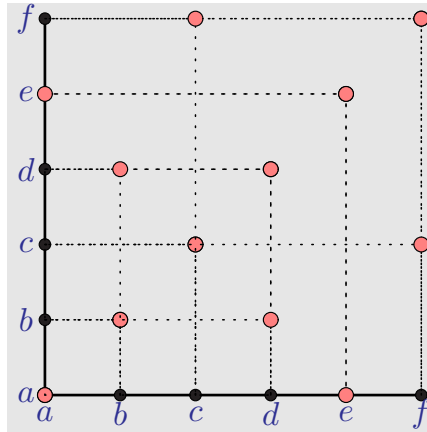
czyli przyporządkowującą każdemu elementowi jego klasę abstrakcji.

Relacje równoważności

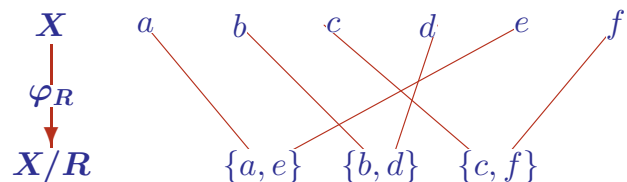
Przykład:

$$X = \{a, b, c, d, e, f\}$$

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, e), (e, a), (b, d), (d, b), (c, f), (f, c)\}$$



$$X/R = \{\{a, e\}, \{b, d\}, \{c, f\}\}$$



Równoważność zachowująca działanie

A jeśli w zbiorze X jest określona jakaś operacja (działanie)...

$$\odot : X \times X \rightarrow X$$

Definicja:

Relacja R w zbiorze X nazywa się kongruencją ze względu na działanie

$$\odot : X \times X \rightarrow X \text{ jeśli}$$

- R jest relacją równoważności w X , oraz
- dla każdych $x, x', y, y' \in X$

$$xRx' \wedge yRy' \implies (x \odot y) R (x' \odot y')$$

Jeśli R jest kongruencją ze względu na $\odot$, to istnieje naturalne przeniesienie działania $\odot$ na zbiór ilorazowy:

$$\odot : X/R \times X/R \rightarrow X/R$$

$$[x]_R \odot [y]_R \stackrel{\text{def}}{=} [x \odot y]_R$$

Czy to jest dobra definicja?

Równoważność zachowująca działanie

$$\odot : X/R \times X/R \rightarrow X/R$$

$$[x]_R \odot [y]_R \stackrel{\text{def}}{=} [x \odot y]_R$$

Czy to jest dobra definicja?

Operacja na klasach abstrakcji została zdefiniowana tak, że

- (a) najpierw wybieramy pojedyncze elementy x i y z ich klas abstrakcji
- (b) potem stosujemy do nich $\odot$ określony na X , żeby uzyskać $x \odot y$
- (c) w końcu przechodzimy do jego klasy abstrakcji $[x \odot y]_R$

Czy otrzymamy ten sam wynik, jeśli w punkcie (a) wybierzemy **inne** elementy z tych samych klas abstrakcji?

$$[x]_R \odot [y]_R \stackrel{\text{def}}{=} [x \odot y]_R$$

Założmy, że $x' \in [x]_R$ i $y' \in [y]_R$, więc $[x']_R = [x]_R$ i $[y']_R = [y]_R$.

Czy $[x' \odot y']_R = [x \odot y]_R$?

Z definicji kongruencji $(x' \odot y') R (x \odot y)$, więc OK.

Kongruencje $\equiv_n$ w $\mathbb{Z}$

Fakty już poznane:

Dla każdego $n \in \mathbb{N}$ t.ż. $n \geq 2$ relacja $\equiv_n$ dana przez

$$\begin{aligned} a \equiv_n b &\iff a \bmod n = b \bmod n \\ &\iff n \mid a - b \end{aligned}$$

jest kongruencją w $\mathbb{Z}$ ze względu na dodawanie, odejmowanie i mnożenie.

Oznaczenia:

Zbiór ilorazowy $\mathbb{Z}/\equiv_n$ oznaczamy zwykle przez $\mathbb{Z}_n$,
a jego element $[a]_{\equiv_n}$ przez $[a]_n$.

Najczęściej jako reprezentanta klasy $[a]_n$ wybieramy taki a , który spełnia $0 \leq a < n$ i często (dla uproszczenia) piszemy samo a zamiast $[a]_n$.

Kongruencje $\equiv_n$ w $\mathbb{Z}$

Przykład: tabelki działań w $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Przykład: tabelki działań w $\mathbb{Z}_{10}$:

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

•	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Kongruencje $\equiv_n$ w $\mathbb{Z}$

Twierdzenie: (własności działań w $\mathbb{Z}_n$)

- *łączność:* $a + (b + c) \equiv_n (a + b) + c$
 $a \cdot (b \cdot c) \equiv_n (a \cdot b) \cdot c$
- *przemienność:* $a + b \equiv_n b + a$
 $a \cdot b \equiv_n b \cdot a$
- *rozdzielność:* $(a + b) \cdot c \equiv_n (a \cdot c) + (b \cdot c)$
- *elementy neutralne:* $a + 0 \equiv_n a$
 $a \cdot 1 \equiv_n a$
- *element przeciwny:* $a + (-a) \equiv_n 0$

Kongruencje $\equiv_n$ w $\mathbb{Z}$

Do każdego $a \in \mathbb{Z}_n$ istnieje $-a \in \mathbb{Z}_n$ t.ż.

$$a + (-a) \equiv_n 0$$

Więc istnieje działanie *przeciwnie* do dodawania.

A dla mnożenia?

Czy dla każdego $a \in \mathbb{Z}_n$ t.ż. $a \neq 0$ istnieje b *odwrotny* do a : taki, że

$$a \cdot b \equiv_n 1 \quad ?$$

NIE. Np. w $\mathbb{Z}_{10}$: $5 \cdot b = 0$ lub $5 \cdot b = 5$, a nigdy 1.

Twierdzenie: (odwracanie w $\mathbb{Z}_n$)

Element $a \in \mathbb{Z}_n \setminus \{[0]_n\}$ posiada odwrotny wtedy i tylko wtedy, gdy $\text{nwd}(a, n) = 1$.

Dowód:

$$\begin{aligned} \text{nwd}(a, n) = 1 &\iff a \cdot x + n \cdot y = 1 \quad \text{dla pewnych } x, y \in \mathbb{Z} \\ &\iff a \cdot x + 0 \cdot y \equiv_n 1 \\ &\iff a \cdot x = 1 \end{aligned}$$

□

Kongruencje $\equiv_n$ w $\mathbb{Z}$

Wniosek:

W $\mathbb{Z}_n \setminus \{[0]_n\}$ **każdy** element $a \neq 0$ posiada **dokładnie jeden** odwrotny wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

Wobec tego, jeśli n jest liczbą pierwszą, to w $\mathbb{Z}_n$ określone jest działanie dzielenia

$$\begin{aligned} / : \mathbb{Z}_n \times \mathbb{Z}_n \setminus \{[0]_n\} &\rightarrow \mathbb{Z}_n \setminus \{[0]_n\} \\ a / b &\stackrel{\text{def}}{=} a \cdot (\text{el. odwrotny do } b \text{ w } \mathbb{Z}_n) \end{aligned}$$

Czy $\equiv_n$ jest kongruencją ze względu na dzielenie?

NIE CAŁKIEM... : dzielenie **nie jest** działaniem w $\mathbb{Z}$, bo nie każde dwie liczby dają się podzielić. Ale:

Prosty fakt:

Jeśli n jest liczbą pierwszą, $a, b, c \in \mathbb{Z}$ i $a / b = c$ to

$$(a \bmod n) / (b \bmod n) \equiv_n c$$

Dowód:

Z założenia: $a = b \cdot c$. Stąd

$$a \bmod n = (b \cdot c) \bmod n \equiv_n (b \bmod n) \cdot (c \bmod n)$$

□

Podzielność przez 3

Twierdzenie:

Reszta z dzielenia liczby $a \geq 0$ przez 3 jest taka sama jak reszta z dzielenia jej sumy cyfr dziesiętnych przez 3.

Dowód:

Niech $c_0, c_1, c_2, \dots, c_k$ będą cyframi liczby a od najmłodszej do najstarszej:

$$a = c_0 + c_1 \cdot 10 + c_2 \cdot 10^2 + \dots + c_k \cdot 10^k = \sum_{i=0}^k c_i \cdot 10^i$$

i $0 \leq c_i < 10$ dla $i \in \{0, 1, 2, \dots, k\}$. Wtedy

$$a \bmod 3 = \left(\sum_{i=0}^k c_i \cdot 10^i \right) \bmod 3 = \sum_{i=0}^k (c_i \bmod 3) \cdot (10 \bmod 3)^i$$

ponieważ $10 \bmod 3 = 1$

$$= \sum_{i=0}^k (c_i \bmod 3) = \left(\sum_{i=0}^k c_i \right) \bmod 3$$

□

Podzielność przez 9

Twierdzenie:

Reszta z dzielenia liczby $a \geq 0$ przez 9 jest taka sama jak reszta z dzielenia jej sumy cyfr dziesiętnych przez 9.

Dowód:

Tak samo jak dla 3:

$$a \bmod 9 = \left(\sum_{i=0}^k c_i \cdot 10^i \right) \bmod 9 = \sum_{i=0}^k (c_i \bmod 9) \cdot (10 \bmod 9)^i$$

$$= \sum_{i=0}^k (c_i \bmod 9) = \left(\sum_{i=0}^k c_i \right) \bmod 9$$

— bo $10 \bmod 9 = 1$ (analogicznie do poprzedniego $10 \bmod 3 = 1$).

□

Podzielność przez 11

Twierdzenie:

Reszta z dzielenia liczby $a \geq 0$ przez 11 jest taka sama jak reszta z dzielenia jej **naprzemiennej** sumy cyfr dziesiętnych

$c_0 - c_1 + c_2 - \dots + (-1)^k \cdot c_k$
przez 11.

Dowód:

Tak samo jak dla 3 i dla 9:

$$\begin{aligned} a \bmod 11 &= \left(\sum_{i=0}^k c_i \cdot 10^i \right) \bmod 11 = \sum_{i=0}^k (c_i \bmod 11) \cdot (10 \bmod 11)^i \\ &= \sum_{i=0}^k (c_i \bmod 11) \cdot (-1)^i = \left(\sum_{i=0}^k (-1)^i \cdot c_i \right) \bmod 11 \end{aligned}$$

□

Przykład:

$$\begin{aligned} 546372819 \bmod 11 &= (9 - 1 + 8 - 2 + 7 - 3 + 6 - 4 + 5) \bmod 11 \\ &= 25 \bmod 11 = (5 - 2) \bmod 11 = 3 \bmod 11 = 3 \end{aligned}$$

Obliczenia i równania „modulo”

Przykład:

$$(4005 + 2 \cdot 175)^2 \equiv_{85} ?$$

$$\begin{aligned} (4005 + 2 \cdot 175)^2 &\quad \text{(ponieważ: } 4005 \bmod 85 = 10 \\ &\quad 175 \bmod 85 = 5) \\ &\equiv_{85} (10 + 2 \cdot 5)^2 \equiv_{85} 400 \\ &\equiv_{85} 60 \end{aligned}$$

Przykład:

$$2^{2024} \cdot 3^{2025} \equiv_{100} ?$$

$$\begin{aligned} 2^{2024} \cdot 3^{2025} &\equiv_{100} 2^{7 \cdot 289 + 1} \cdot 3^{5 \cdot 405} \equiv_{100} (2^7)^{289} \cdot 2 \cdot (3^5)^{405} \equiv_{100} 28^{289} \cdot 2 \cdot 43^{405} \\ &\equiv_{100} 28^{2 \cdot 144 + 1} \cdot 2 \cdot 43^{2 \cdot 202 + 1} \equiv_{100} (84^{144} \cdot 28) \cdot 2 \cdot (49^{202} \cdot 43) \\ &\equiv_{100} 84^{144} \cdot 49^{202} \cdot (28 \cdot 2 \cdot 43) \equiv_{100} 56^{72} \cdot \cancel{1^{101}} \cdot 8 \equiv_{100} 36^{36} \cdot 8 \\ &\equiv_{100} 96^{18} \cdot 8 \equiv_{100} 16^9 \cdot 8 \equiv_{100} 56^4 \cdot 16 \cdot 8 \equiv_{100} 36^2 \cdot 28 \\ &\equiv_{100} 96 \cdot 28 \equiv_{100} 88 \end{aligned}$$

Obliczenia i równania „modulo”

Przykład:

$$377 \cdot ? \equiv_{464} 58$$

$$\begin{array}{rcl} 464 & = & 464 \cdot 1 + 377 \cdot 0 \\ 377 & = & 464 \cdot 0 + 377 \cdot 1 \\ 87 & = & 464 \cdot 1 + 377 \cdot (-1) \\ 29 & = & 464 \cdot (-4) + 377 \cdot 5 \\ 0 & = & 464 \cdot \dots \end{array}$$

Stąd:

$$\begin{array}{l} 377 \cdot 5 \equiv_{464} 29 \quad || \cdot 2 \\ 377 \cdot 10 \equiv_{464} 58 \end{array}$$

Przykład:

$$20 \cdot ? \equiv_{637} 102$$

$$\begin{array}{rcl} 637 & = & 637 \cdot 1 + 20 \cdot 0 \\ 20 & = & 637 \cdot 0 + 20 \cdot 1 \\ 17 & = & 637 \cdot 1 + 20 \cdot (-31) \\ 3 & = & 637 \cdot (-1) + 20 \cdot 32 \\ 2 & = & 637 \cdot 6 + 20 \cdot (-191) \\ 1 & = & 637 \cdot (-7) + 20 \cdot 223 \\ 0 & = & 637 \cdot \dots \end{array}$$

Stąd:

$$\begin{array}{l} 20 \cdot 223 \equiv_{637} 1 \quad || \cdot 102 \\ 20 \cdot (223 \cdot 102) \equiv_{637} 102 \\ 20 \cdot 451 \equiv_{637} 102 \end{array}$$

Obliczenia i równania „modulo”

Przykład:

Rozwiązać w $\mathbb{Z}_{11}$ układ z 2 niewiadomymi:

$$\begin{cases} 2x + 3y \equiv_{11} 1 \\ 6x + 5y \equiv_{11} 5 \end{cases}$$

$$2x + 3y \equiv_{11} 1 \quad || \cdot 6 \quad (\text{bo } 2 \cdot 6 \equiv_{11} 1)$$

$$x + 7y \equiv_{11} 6$$

$$x \equiv_{11} 6 - 7y$$

$$6 \cdot (6 - 7y) + 5y \equiv_{11} 5$$

$$36 - 42y + 5y \equiv_{11} 5$$

$$37y \equiv_{11} 31$$

$$4y \equiv_{11} -2$$

$$2y \equiv_{11} -1$$

$$2y \equiv_{11} 10$$

$$y \equiv_{11} 5$$

$$x \equiv_{11} 6 - 7 \cdot 5$$

$$x \equiv_{11} -29$$

$$x \equiv_{11} 4$$

Obliczenia i równania „modulo”

Zadanie:

Udowodnić, że dla każdego $n \in \mathbb{N}$ zachodzi $45 \mid 47^{2n} - 7^{2n}$.

$$47^{2n} - 7^{2n} \equiv_{45} 2^{2n} - 49^n \equiv_{45} 4^n - 4^n = 0$$

Zadanie:

Udowodnić, że dla każdego $n \in \mathbb{N}$ zachodzi $13 \mid 3^{n+2} + 4^{2n+1}$.

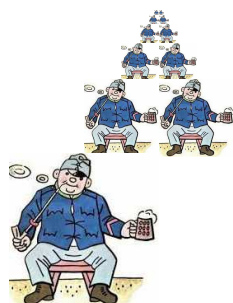
$$\begin{aligned} 3^{n+2} + 4^{2n+1} &= 3^n \cdot 9 + 4^{2n} \cdot 4 = 3^n \cdot 9 + 16^n \cdot 4 \\ &\equiv_{13} 3^n \cdot 9 + 3^n \cdot 4 = 3^n \cdot (9 + 4) = 3^n \cdot 13 \equiv_{13} 0 \end{aligned}$$

Chińskie twierdzenie o resztach

Legenda:

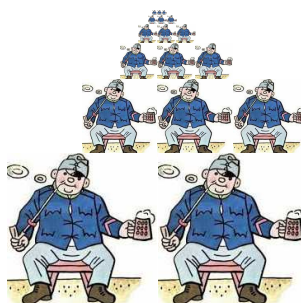
W starodawnej chińskiej armii zamiast „kolejno odlicz” kazano wojsku ustawiać się w rozmaite szyki i wnioskowano o liczebności oddziału wg liczb żołnierzy, którzy do szyku **nie** pasowali.

Parami...



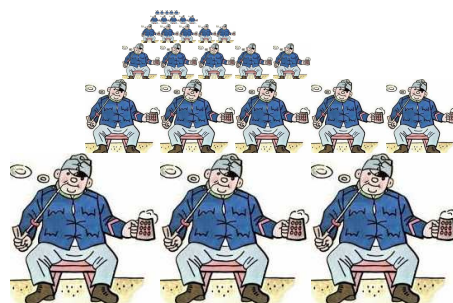
...jeden bez pary.

Trójkami...



...dwaj bez trójki.

Piątkami...



...trzej bez piątki.

W tym przypadku liczba żołnierzy n musi spełniać:

$$\left. \begin{aligned} n \bmod 2 &= 1 \\ n \bmod 3 &= 2 \\ n \bmod 5 &= 3 \end{aligned} \right\}$$

Jedno z możliwych rozwiązań: $n = 23$.
Czy istnieją inne?

Chińskie twierdzenie o resztach

Po raz pierwszy:

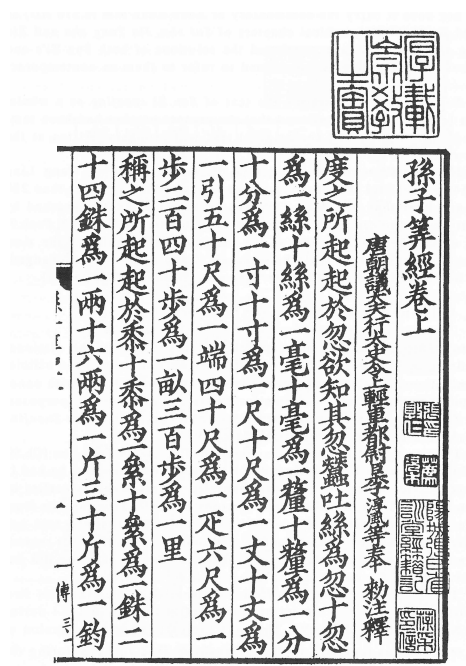
Sun Zi, Chiny wiek III-V

Porządne sformułowanie:

Aryabhata, Indie wiek VI

Pełna ogólność:

Qin Jiushao, Chiny wiek XIII



Chińskie twierdzenie o resztach

Twierdzenie:

Założenia:

- $m_1, m_2, \dots, m_k \in \mathbb{N}$ niezerowe; $M \stackrel{\text{def}}{=} m_1 \cdot m_2 \cdot \dots \cdot m_k$;
- $\text{nwd}(m_i, m_j) = 1$ dla $i \neq j$, $i, j \in \{1, 2, \dots, k\}$;
- $a_1, a_2, \dots, a_k \in \mathbb{N}$ niezerowe.

Wtedy układ kongruencji:

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \\ \dots\dots\dots \\ x \equiv_{m_k} a_k \end{cases}$$

Niech $s_1, s_2, \dots, s_k$ t.ż. $\begin{cases} \frac{M}{m_1} \cdot s_1 \equiv_{m_1} 1 \\ \frac{M}{m_2} \cdot s_2 \equiv_{m_2} 1 \\ \dots\dots\dots \\ \frac{M}{m_k} \cdot s_k \equiv_{m_k} 1 \end{cases}$

ma dokładnie jedno rozwiązanie modulo M , dane przez

$$x_0 = \left(\frac{M}{m_1} \cdot s_1 \cdot a_1 + \frac{M}{m_2} \cdot s_2 \cdot a_2 + \dots + \frac{M}{m_k} \cdot s_k \cdot a_k \right) \bmod M$$

Chińskie twierdzenie o resztach

Przykład-bajka:

7 złodziei dzieli się łupem — sakiewką ze zrabowanymi talarami. Okazuje się, że jeśli podzielią się po równo, to pozostanie 5 talarów, których nie ma jak podzielić. Ale jeśli pominą Roztargnionego Antka (który i tak się nie połapie) to pozostaną im tylko 2 niepodzielne talary.



Ile talarów jest w sakiewce?

$$\begin{cases} x \equiv_6 2 \\ x \equiv_7 5 \end{cases} \quad \text{Obliczenie } s_1, s_2: \quad \begin{array}{ll} 7 \cdot s_1 \equiv_6 1 & \longrightarrow s_1 = 1 \\ 6 \cdot s_2 \equiv_7 1 & \longrightarrow s_2 = 6 \end{array}$$

Rozwiązanie:

$$\begin{aligned} x_0 &= (7 \cdot 1 \cdot 2 + 6 \cdot 6 \cdot 5) \bmod (7 \cdot 6) = (14 + 180) \bmod 42 \\ &= (14 + 12) \bmod 42 = \mathbf{26} \end{aligned}$$

Odpowiedź: talarów w sakiewce jest 26,

$$\text{albo } 26 + 42 = 68,$$

$$\text{albo } 26 + 2 \cdot 42 = 110,$$

$$\text{albo } 26 + 3 \cdot 42 = 152,$$

$$\text{albo } \dots$$

Chińskie twierdzenie o resztach

Przykład:

$$\begin{cases} x \equiv_3 2 \\ x \equiv_7 4 \\ x \equiv_{10} 6 \end{cases} \quad \begin{array}{l} \text{nwd}(3, 7) = 1, \text{ nwd}(3, 10) = 1, \text{ nwd}(7, 10) = 1 \\ \text{— więc rozwiązanie istnieje.} \end{array}$$

Obliczenie s_1, s_2, s_3 :

$$7 \cdot 10 \cdot s_1 \equiv_3 1 \quad \longrightarrow \quad s_1 = 1$$

$$3 \cdot 10 \cdot s_2 \equiv_7 1 \quad \longrightarrow \quad s_2 = 4$$

$$3 \cdot 7 \cdot s_3 \equiv_{10} 1 \quad \longrightarrow \quad s_3 = 1$$

Rozwiązanie:

$$\begin{aligned} x_0 &= (70 \cdot 1 \cdot 2 + 30 \cdot 4 \cdot 4 + 21 \cdot 1 \cdot 6) \bmod (3 \cdot 7 \cdot 10) \\ &= (140 + 480 + 126) \bmod 210 = 746 \bmod 210 = \mathbf{116} \end{aligned}$$