# Elementy teorii liczb i algebry abstrakcyjnej

Aleksandra Gorzkowska

Elektronika i Telekomunikacja
Wydział Informatyki, Elektroniki i Telekomunikacji

# Arytmetyka modularna

## Twierdzenie (Dzielenie z resztą)

*Niech* $a, b \in \mathbb{Z}$, $b > 0$, *wtedy* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *gdzie* $0 \leq r < b$.

# Arytmetyka modularna

## Twierdzenie (Dzielenie z resztą)

*Niech* $a, b \in \mathbb{Z}$, $b > 0$, *wtedy* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *gdzie* $0 \leq r < b$.

## Przykład

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$

# Arytmetyka modularna

## Twierdzenie (Dzielenie z resztą)

*Niech* $a, b \in \mathbb{Z}$, $b > 0$, *wtedy* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *gdzie* $0 \leq r < b$.

## Przykład

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$
2. $a = -11, b = 3$: $-11 = -4 \cdot 3 + 1$

# Arytmetyka modularna

## Twierdzenie (Dzielenie z resztą)

*Niech* $a, b \in \mathbb{Z}$, $b > 0$, *wtedy* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *gdzie* $0 \leq r < b$.

## Przykład

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$
2. $a = -11, b = 3$: $-11 = -4 \cdot 3 + 1$
3. $a = -27, b = 4$: $-27 = -7 \cdot 4 + 1$

# Arytmetyka modularna

## Twierdzenie (Dzielenie z resztą)

*Niech* $a, b \in \mathbb{Z}$, $b > 0$, *wtedy* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *gdzie* $0 \leq r < b$.

## Przykład

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$
2. $a = -11, b = 3$: $-11 = -4 \cdot 3 + 1$
3. $a = -27, b = 4$: $-27 = -7 \cdot 4 + 1$
4. $a = 18, b = 7$, $a = -103, b = 20$

## Definicja (Relacja podzielności)

Niech $a, b \in \mathbb{Z}$, $b > 0$. Zapisujemy

$$b|a \Leftrightarrow \exists k \in \mathbb{Z}\colon\ a = k \cdot b$$

Czytamy: "$b$ dzieli $a$"

## Definicja (Relacja podzielności)

Niech $a, b \in \mathbb{Z}$, $b > 0$. Zapisujemy

$$b|a \Leftrightarrow \exists k \in \mathbb{Z}\colon\ a = k \cdot b$$

Czytamy: "$b$ dzieli $a$"

## Definicja (Przystawanie liczb modulo)

Niech $a, b \in \mathbb{Z}$ oraz $m \in \mathbb{N}_+$. Mówimy, że $a$ przystaje do $b$ modulo $m$, gdy

$$m|b - a$$

Zapis: $m|b - a \Leftrightarrow a \equiv_m b \Leftrightarrow a = b(\mathrm{mod}\ m)$

## Definicja (Relacja podzielności)

Niech $a, b \in \mathbb{Z}$, $b > 0$. Zapisujemy

$$b|a \Leftrightarrow \exists k \in \mathbb{Z}\colon\ a = k \cdot b$$

Czytamy: "$b$ dzieli $a$"

## Definicja (Przystawanie liczb modulo)

Niech $a, b \in \mathbb{Z}$ oraz $m \in \mathbb{N}_+$. Mówimy, że $a$ przystaje do $b$ modulo $m$, gdy

$$m|b - a$$

Zapis: $m|b - a \Leftrightarrow a \equiv_m b \Leftrightarrow a = b(\mathrm{mod}\ m)$

**Obserwacja**: $a = b(\mathrm{mod}\ m) \Leftrightarrow a$ oraz $b$ maja tę samą resztę z dzielenia przez $m$

## Twierdzenie

*Niech* $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}_+$, $n \in \mathbb{N}$
*Jeśli* $a = b \pmod m$ *oraz* $c = d \pmod m$, *to*

1. $a + c = b + d \pmod m$,
2. $a \cdot c = b \cdot d \pmod m$,
3. $a^n = b^n \pmod m$.

## Twierdzenie

*Niech* $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}_+$, $n \in \mathbb{N}$
*Jeśli* $a = b \pmod m$ *oraz* $c = d \pmod m$, *to*

1. $a + c = b + d \pmod m$,
2. $a \cdot c = b \cdot d \pmod m$,
3. $a^n = b^n \pmod m$.

## Przykład

$13 = 5 \pmod 8$, $2 = 18 \pmod 8$
$13 + 2 = 5 + 18 \pmod 8 = 7 \pmod 8$,
$13 \cdot 2 = 5 \cdot 18 \pmod 8 = 2 \pmod 8$

## Definicja

Niech $a, b \in \mathbb{N}$. Liczbę $d \in \mathbb{N}$ nazywamy największym wspólnym dzielnikiem liczb $a$ oraz $b$, jeśli:

1. $d|a$ oraz $d|b$,
2. $\forall c \in \mathbb{N}\colon\ [(c|a \wedge c|b) \Rightarrow c|d]$.

Oznaczenie: $\mathrm{NWD}(a, b)$

## Definicja

Niech $a, b \in \mathbb{N}$. Liczbę $d \in \mathbb{N}$ nazywamy największym wspólnym dzielnikiem liczb $a$ oraz $b$, jeśli:

1. $d|a$ oraz $d|b$,
2. $\forall c \in \mathbb{N}\colon\ [(c|a \wedge c|b) \Rightarrow c|d]$.

Oznaczenie: $\mathrm{NWD}(a, b)$

## Definicja

Mówimy, że liczby $a$ i $b$ są względnie pierwsze, jeśli $\mathrm{NWD}(a, b) = 1$.
Oznaczenie: $a \perp b$

# Algorytm Euklidesa

$a, b \in \mathbb{N}_+$, $a > b$

Tworzymy rekurencyjnie ciąg reszt $(r_k)$:

$r_0 = a$, $r_1 = b$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$.

# Algorytm Euklidesa

$a, b \in \mathbb{N}_+$, $a > b$

Tworzymy rekurencyjnie ciąg reszt $(r_k)$:

$r_0 = a$, $r_1 = b$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$.

Ostatnia niezerowa reszta jest równa $\mathrm{NWD}(a, b)$.

# Algorytm Euklidesa

$a, b \in \mathbb{N}_+$, $a > b$
Tworzymy rekurencyjnie ciąg reszt $(r_k)$:
$r_0 = a$, $r_1 = b$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$.

Ostatnia niezerowa reszta jest równa $\mathrm{NWD}(a, b)$.

## Przykład

$\mathrm{NWD}(121, 114)$:

## Twierdzenie

*Niech* $a, b \in \mathbb{N}$, $a^2 + b^2 > 0$, *wtedy*

$$\mathrm{NWD}(a, b) = \min\{c > 0 \colon c = \alpha \cdot a + \beta \cdot b, \alpha, \beta \in \mathbb{Z}\}$$

## Twierdzenie

*Niech* $a, b \in \mathbb{N}$, $a^2 + b^2 > 0$, *wtedy*

$$\mathrm{NWD}(a, b) = \min\{c > 0 \colon c = \alpha \cdot a + \beta \cdot b, \alpha, \beta \in \mathbb{Z}\}$$

## Przykład

Znajdź $\alpha, \beta$, takie że $\mathrm{NWD}(121, 114) = \alpha \cdot 121 + \beta \cdot 114$:

## Definicja

Strukturę algebraiczną $(X, \circ)$ nazywamy grupą, jeśli spełnione są warunki:

0. działanie $\circ$ jest wewnętrzne, tj. $\forall x, y \in X \; x \circ y \in X$,

## Definicja

Strukturę algebraiczną $(X, \circ)$ nazywamy grupą, jeśli spełnione są warunki:

0. działanie $\circ$ jest wewnętrzne, tj. $\forall x, y \in X \; x \circ y \in X$,
1. działanie $\circ$ jest łączne, tj. $\forall x, y, z \in X \; (x \circ y) \circ z = x \circ (y \circ z)$,

## Definicja

Strukturę algebraiczną $(X, \circ)$ nazywamy grupą, jeśli spełnione są warunki:

0. działanie $\circ$ jest wewnętrzne, tj. $\forall x, y \in X \; x \circ y \in X$,
1. działanie $\circ$ jest łączne, tj. $\forall x, y, z \in X \; (x \circ y) \circ z = x \circ (y \circ z)$,
2. działanie $\circ$ ma element neutralny $e \in X$, tj. $\exists e \in X \; \forall x \in X \; x \circ e = e \circ x = x$,

## Definicja

Strukturę algebraiczną $(X, \circ)$ nazywamy grupą, jeśli spełnione są warunki:

0. działanie $\circ$ jest wewnętrzne, tj. $\forall x, y \in X \; x \circ y \in X$,
1. działanie $\circ$ jest łączne, tj. $\forall x, y, z \in X \; (x \circ y) \circ z = x \circ (y \circ z)$,
2. działanie $\circ$ ma element neutralny $e \in X$, tj. $\exists e \in X \; \forall x \in X \; x \circ e = e \circ x = x$,
3. dla każdego elementu $x \in X$ istnieje element symetryczny, tj. $\forall x \in X \; \exists y \in X : x \circ y = y \circ x = e$.

## Definicja

Strukturę algebraiczną $(X, \circ)$ nazywamy grupą, jeśli spełnione są warunki:

0. działanie $\circ$ jest wewnętrzne, tj. $\forall x, y \in X \; x \circ y \in X$,
1. działanie $\circ$ jest łączne, tj. $\forall x, y, z \in X \; (x \circ y) \circ z = x \circ (y \circ z)$,
2. działanie $\circ$ ma element neutralny $e \in X$, tj. $\exists e \in X \; \forall x \in X \; x \circ e = e \circ x = x$,
3. dla każdego elementu $x \in X$ istnieje element symetryczny, tj. $\forall x \in X \; \exists y \in X : x \circ y = y \circ x = e$.

Jeśli dodatkowo działanie $\circ$ jest przemienne, tj. $\forall x, y \in X \; x \circ y = y \circ x$, to grupę nazywamy przemienną lub abelową.

Stosuje się dwa rodzaje notacji:

- addytywną; $\circ \to +$
  el. symetryczny nazywamy przeciwnym i oznaczamy $-x$,
- multiplikatywną: $\circ \to \cdot$
  el. symetryczny nazywamy odwrotnym i oznaczamy $x^{-1}$.

## Przykład

$(\mathbb{N}, +)$ - zb. liczb naturalnych z dodawaniem, czy spełnia warunki?

0. suma dwóch liczb naturalnych jest liczbą naturalną; $+$ wewnętrzne ✓,

## Przykład

$(\mathbb{N}, +)$ - zb. liczb naturalnych z dodawaniem, czy spełnia warunki?

0. suma dwóch liczb naturalnych jest liczbą naturalną; $+$ wewnętrzne ✓,
1. kolejność dodawania liczb $x + y + z$ nie ma znaczenia; $+$ łączne ✓,

## Przykład

$(\mathbb{N}, +)$ - zb. liczb naturalnych z dodawaniem, czy spełnia warunki?

0. suma dwóch liczb naturalnych jest liczbą naturalną; $+$ wewnętrzne ✓,
1. kolejność dodawania liczb $x + y + z$ nie ma znaczenia; $+$ łączne ✓,
2. dla dowolnej liczby naturalnej $n$ mamy $n + 0 = 0 + n = n$; istnieje el. neutralny $e = 0$ ✓,

## Przykład

$(\mathbb{N}, +)$ - zb. liczb naturalnych z dodawaniem, czy spełnia warunki?

0. suma dwóch liczb naturalnych jest liczbą naturalną; $+$ wewnętrzne ✓,
1. kolejność dodawania liczb $x + y + z$ nie ma znaczenia; $+$ łączne ✓,
2. dla dowolnej liczby naturalnej $n$ mamy $n + 0 = 0 + n = n$; istnieje el. neutralny $e = 0$ ✓,
3. dla dowolnej liczny naturalnej $n$, jej elementem symetrycznym (przeciwnym) jest $-n$ ALE! $-n$ nie jest liczbą naturalną; el. symetryczny ✗.

$(\mathbb{N}, +)$ nie jest grupą

## Przykład

- $(\mathbb{Z}, +)$ - zb. liczb całkowitych z dodawaniem jest grupą, bo:
  1. suma dwóch liczb całkowitych jest liczbą całkowitą; $+$ wewnętrzne ✓,
  2. kolejność dodawania liczb $x + y + z$ nie ma znaczenia; $+$ łączne ✓,
  3. $e = 0$; istnieje el. neutralny ✓,
  4. dla dowolnej liczny całkowitej $n$, jej elementem symetrycznym (przeciwnym) jest $-n$. Licba $-n$ jest liczbą całkowitą ✓.

  Dodatkowo dodawanie jest przemienne, więc $(\mathbb{Z}, +)$ - grupa abelowa.

## Przykład

- $(\mathbb{Z}, +)$ - zb. liczb całkowitych z dodawaniem jest grupą, bo:
  1. suma dwóch liczb całkowitych jest liczbą całkowitą; $+$ wewnętrzne ✓,
  2. kolejność dodawania liczb $x + y + z$ nie ma znaczenia; $+$ łączne ✓,
  3. $e = 0$; istnieje el. neutralny ✓,
  4. dla dowolnej liczny całkowitej $n$, jej elementem symetrycznym (przeciwnym) jest $-n$. Licba $-n$ jest liczbą całkowitą ✓.

  Dodatkowo dodawanie jest przemienne, więc $(\mathbb{Z}, +)$ - grupa abelowa.
- $(\mathbb{Z}, -)$ - nie jest grupą; $-$ nie jest łączne.
  Np. $(3 - (-1)) - 2 = 4 - 2 = 2; 3 - (-1 - 2) = 3 - (-3) = 6$

## Przykład

- $(\mathbb{Z}, +)$ - zb. liczb całkowitych z dodawaniem jest grupą, bo:
  1. suma dwóch liczb całkowitych jest liczbą całkowitą; $+$ wewnętrzne ✓,
  2. kolejność dodawania liczb $x + y + z$ nie ma znaczenia; $+$ łączne ✓,
  3. $e = 0$; istnieje el. neutralny ✓,
  4. dla dowolnej liczny całkowitej $n$, jej elementem symetrycznym (przeciwnym) jest $-n$. Licba $-n$ jest liczbą całkowitą ✓.

  Dodatkowo dodawanie jest przemienne, więc $(\mathbb{Z}, +)$ - grupa abelowa.
- $(\mathbb{Z}, -)$ - nie jest grupą; $-$ nie jest łączne.
  Np. $(3 - (-1)) - 2 = 4 - 2 = 2; 3 - (-1 - 2) = 3 - (-3) = 6$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ - grupa abelowa

Zbiór wszystkich możliwych reszt z dzielenia przez $n$ oznaczamy $\mathbb{Z}_n$, czyli

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

Określamy działanie "dodawanie modulo $n$" $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ nastepująco:

$$\forall a, b \in \mathbb{Z}_n \quad a +_n b = k \iff a + b \equiv_n k \wedge k \in \mathbb{Z}_n$$

Czytaj: Wynikiem działania dodawanie modulo $n$ jest reszta z dzielenia przez $n$ sumy liczb $a + b$.

Struktura $(\mathbb{Z}_n, +_n)$ jest grupą abelową.

0. $+_n$ wewnętrzne ✓,
1. $+_n$ łączne ✓, bo możemy dodać trzy liczby w dowolnej kolejności i na końcu wziąć resztę z dzielenia przez $n$,
2. el. neutralny: $e = 0 \in \mathbb{Z}_n$ ✓,
3. el. przeciwny: dla $k \in \mathbb{Z}_n$ el. przeciwnym jest $n - k \in \mathbb{Z}_n$ ✓,
4. $+_n$ przemienne, bo dodawanie jest przemienne.

Definiujemy też działanie "mnożenie modulo $n$" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ następująco:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

Definiujemy też działanie "mnożenie modulo $n$" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ następująco:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

Czy struktura $(\mathbb{Z}_n, \cdot_n)$ jest grupą?
Nie jest! El. neutralnym mnożenia jest $e = 1$. Ale nie każdy element ma el. odwrotny! Element 0 nie ma el. odwrotnego.

Definiujemy też działanie "mnożenie modulo $n$" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ następująco:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

Czy struktura $(\mathbb{Z}_n, \cdot_n)$ jest grupą?
Nie jest! El. neutralnym mnożenia jest $e = 1$. Ale nie każdy element ma el. odwrotny! Element 0 nie ma el. odwrotnego.

Czy zatem $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ jest grupą?
Nadal nie! Np. $(\mathbb{Z}_8, \cdot_8)$ nie jest grupą, bo $2 \cdot_8 4 = 0 \notin \mathbb{Z}_8 \setminus \{0\}$, czyli działanie $\cdot_8$ nie jest wewnętrzne w $\mathbb{Z}_8 \setminus \{0\}$.

Definiujemy też działanie "mnożenie modulo $n$" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ następująco:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

Czy struktura $(\mathbb{Z}_n, \cdot_n)$ jest grupą?
Nie jest! El. neutralnym mnożenia jest $e = 1$. Ale nie każdy element ma el. odwrotny! Element 0 nie ma el. odwrotnego.

Czy zatem $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ jest grupą?
Nadal nie! Np. $(\mathbb{Z}_8, \cdot_8)$ nie jest grupą, bo $2 \cdot_8 4 = 0 \notin \mathbb{Z}_8 \setminus \{0\}$, czyli działanie $\cdot_8$ nie jest wewnętrzne w $\mathbb{Z}_8 \setminus \{0\}$.

Jak więc zdefiniować grupę z działaniem $\cdot_n$?

## Twierdzenie

*Element* $a \in \mathbb{Z}_n$ *posiada w strukturze* $(\mathbb{Z}_n, \cdot_n)$ *element odwrotny wtedy i tylko wtedy, gdy* $a \perp n$.

## Twierdzenie

*Element $a \in \mathbb{Z}_n$ posiada w strukturze $(\mathbb{Z}_n, \cdot_n)$ element odwrotny wtedy i tylko wtedy, gdy $a \perp n$.*

Niech $\mathbb{Z}_n^*$ oznacza zbiór wszystkich elementów zbioru $\mathbb{Z}_n$ względnie pierwszych z $n$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \perp n\}$$

Wtedy $(\mathbb{Z}_n^*, \cdot_n)$ jest grupą abelową.

## Twierdzenie

*Element $a \in \mathbb{Z}_n$ posiada w strukturze $(\mathbb{Z}_n, \cdot_n)$ element odwrotny wtedy i tylko wtedy, gdy $a \perp n$.*

Niech $\mathbb{Z}_n^*$ oznacza zbiór wszystkich elementów zbioru $\mathbb{Z}_n$ względnie pierwszych z $n$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \perp n\}$$

Wtedy $(\mathbb{Z}_n^*, \cdot_n)$ jest grupą abelową.

Dla uproszczenia zapisu piszemy $+$ zamiast $+_n$ oraz $\cdot$ zamiast $\cdot_n$.
Liczba $n$ jest znana z kontekstu.

Dzięki algorytmowi Euklidesa możemy znaleźć element odwrotny do elementu $x$ grupy $(\mathbb{Z}_n^*, \cdot_n)$. Przyjmujemy $a = n, b = x$.

Dzięki algorytmowi Euklidesa możemy znaleźć element odwrotny do elementu $x$ grupy $(\mathbb{Z}_n^*, \cdot_n)$. Przyjmujemy $a = n, b = x$.

## Przykład

Znajdź $114^{-1}$ w $\mathbb{Z}_{121}^*$.

Z algorytmu Euklidesa wiemy, że $\mathrm{NWD}(121, 114) = 1$, więc 114 i 121 są względnie pierwsze i $114^{-1}$ istnieje.
Ponadto, $1 = 49 \cdot 121 - 52 \cdot 114$.
Obustronnie stosujemy modulo 121:

$$1 \equiv_{121} -52 \cdot 114 \Rightarrow 114^{-1} = -52 (\mathrm{mod}\ 121)$$

Ale $-52$ nie należy do zbioru $\mathbb{Z}_{121}^*$. Aby uzyskać odpowiedź należy do wyniku dodać (czasami odjąć) 121 tyle razy, aby otrzymać liczbę pomiędzy 0 i 120. W tym przypadku $-52 \equiv_{121} 69$, więc $114^{-1} = 69$ w $\mathbb{Z}_{121}^*$.

Po co nam szukanie elementów odwrotnych w grupie $\mathbb{Z}_n^*$?
Otóż mają one zastosowanie w rozwiązywaniu tzw. kongruencji (równań modulo), o których za chwilę.

Po co nam szukanie elementów odwrotnych w grupie $\mathbb{Z}_n^*$?
Otóż mają one zastosowanie w rozwiązywaniu tzw. kongruencji (równań modulo), o których za chwilę.

## Uwaga

*Prawo skracania:*

$$\forall a, b, c \in \mathbb{Z}\ \forall m \in \mathbb{N}_+((ac \equiv_m bc \wedge c \perp m) \Rightarrow a \equiv_m b).$$

W prawie skracania chodzi o to, że jeśli dwie liczby przystają modulo $m$, to możemy takie równanie podzielić stronami przez $c$, o ile $c$ jest względnie pierwsze z $m$. Dzielenie w tym przypadku zastępujemy mnożeniem przez el. odwrotny do $c$, czyli mnożymy przez $c^{-1}$.

## Twierdzenie (Chińskie twierdzenie o resztach)

*Niech* $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ *oraz* $m_1, m_2, \ldots, m_n \in \mathbb{N}_+$, $m_i$ *są parami względnie pierwsze.*
*Wtedy układ kongruencji*

$$\begin{cases} x &= a_1 (\mathrm{mod}\ m_1) \\ x &= a_2 (\mathrm{mod}\ m_2) \\ &\vdots \\ x &= a_n (\mathrm{mod}\ m_n) \end{cases}$$

*ma dokładnie jedno rozwiązanie modulo* $\prod_{i=1}^{n} m_i$ *i wszystkie pozostałe rozwiązania całkowite przystają do niego modulo* $\prod_{i=1}^{n} m_i$.

## Przykład

Rozwiąż podany układ kongruencji.

$$\begin{cases} x &= 3(\mathrm{mod}\ 7) \\ x &= 0(\mathrm{mod}\ 4) \\ x &= 8(\mathrm{mod}\ 25) \end{cases}$$

Aby mieć pewność, że rozwiązanie istnieje, musimy sprawdzić czy liczby $7, 4, 25$ są parami względnie pierwsze.
$\mathrm{NWD}(7,4) = 1, \mathrm{NWD}(7,25) = 1, \mathrm{NWD}(4,25) = 1.$
Zgadza się, są parami względnie pierwsze.

Równanie $x = 3(\mathrm{mod}\ 7)$ można zapisać jako $x = 7a + 3$ (reszta z dzielenia $x$ przez 7 wynosi 3)

## Przykład

Rozwiązując taki układ będziemy sukcesywnie zmniejszać liczbę równań o jeden, aż otrzymamy jedno równanie - to będzie wynik. W tym celu wybieramy dwa dowolne równania i rozwiązujemy układ tych dwóch kongruencji. Przyrównujemy do siebie prawe strony:

$$3 + 7a = 0 + 4b$$

Dążymy do obliczenia $a$ lub $b$. Takie równanie obustronnie skracamy modulo mniejsza z liczb $m_1 = 7$ i $m_2 = 4$.

$$3 + 3a = 0 (\mathrm{mod}\ 4)\ /-3$$

$$3a = -3 = 1 (\mathrm{mod}\ 4)$$

## Przykład

Teraz wykorzystamy prawo skracania. Chcemy obustronnie podzielić przez 3, czyli pomnożyć przez $3^{-1}$. Ponieważ $3 \perp 4$, więc $3^{-1}$ w $\mathbb{Z}_4^*$ istnieje. Wyznaczamy je z algorytmu Euklidesa.
$3^{-1}$ w $\mathbb{Z}_4^*$:

$$4 = 1 \cdot 3 + 1$$
$$1 = 4 - 1 \cdot 3$$
$$1 = -1 \cdot 3 (\mathrm{mod}\ 4)$$
$$3^{-1} = -1 = 3 (\mathrm{mod}\ 4)$$

## Przykład

Wracamy do naszego równania:

$$3a = 1(\mathrm{mod}\ 4)\ /\cdot 3^{-1}$$
$$a = 3^{-1} = 3(\mathrm{mod}\ 4)$$

Czyli wynik to $a = 3 + 4k$. Podstawiamy:

$$x = 3 + 7a = 3 + 7(3 + 4k) = 24 + 28k$$

Układ kongruencji, który mamy rozwiązać wygląda teraz tak:

$$\begin{cases} x &= 24(\mathrm{mod}\ 28) \\ x &= 8(\mathrm{mod}\ 25) \end{cases}$$

Rozwiązujemy go analogicznie.

## Przykład

$$x = 24 + 28k = 8 + 25c \ /(\mathrm{mod}\ 25)$$
$$24 + 3k = 8(\mathrm{mod}\ 25)$$
$$3k = -16 = 9(\mathrm{mod}\ 25)\ / \cdot 3^{-1}$$

$3^{-1}$ w $\mathbb{Z}_{25}^*$:

$$25 = 8 \cdot 3 + 1$$
$$1 = 25 - 8 \cdot 3$$
$$1 = -8 \cdot 3(\mathrm{mod}\ 25)$$
$$3^{-1} = -8 = 17(\mathrm{mod}\ 25)$$

## Przykład

Powrót do równania:

$$k = 9 \cdot 17 = 153 = 3 (\mathrm{mod}\ 25)$$

$$k = 3 + 25l$$

Podstawiamy:
$x = 24 + 28(3 + 25l) = 24 + 84 + 4 \cdot 7 \cdot 25l = 108 (\mathrm{mod}\ 4 \cdot 7 \cdot 25)$.

Odpowiedź: $x = 108$.

# Rząd grupy

## Definicja

Rzędem grupy $(X, \circ)$ nazywamy liczbę elementów tej grupy, czyli liczbę elementów zbioru $X$.
Oznaczenie: $|X|$

# Rząd grupy

## Definicja

Rzędem grupy $(X, \circ)$ nazywamy liczbę elementów tej grupy, czyli liczbę elementów zbioru $X$.
Oznaczenie: $|X|$

## Przykład

$(\mathbb{Z}_n, +_n)$: $|\mathbb{Z}_n| = n$, bo $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

# Rząd grupy

## Definicja

Rzędem grupy $(X, \circ)$ nazywamy liczbę elementów tej grupy, czyli liczbę elementów zbioru $X$.
Oznaczenie: $|X|$

## Przykład

$(\mathbb{Z}_n, +_n)$: $|\mathbb{Z}_n| = n$, bo $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

A jaki jest rząd grupy $(\mathbb{Z}_n^*, \cdot_n)$?

## Definicja

Funkcja Eulera to funkcja, która liczbie naturalnej $n$ przypisuje ile jest liczb mniejszych od $n$ i względnie pierwszych z $n$.

$$\varphi\colon \mathbb{N} \ni n \mapsto \varphi(n) = |\{m \in \mathbb{N}\colon m < n \wedge m \perp n\}|$$

Zatem $|\mathbb{Z}_n^*| = \varphi(n)$.

## Definicja

Funkcja Eulera to funkcja, która liczbie naturalnej $n$ przypisuje ile jest liczb mniejszych od $n$ i względnie pierwszych z $n$.

$$\varphi\colon \mathbb{N} \ni n \mapsto \varphi(n) = |\{m \in \mathbb{N}\colon m < n \wedge m \perp n\}|$$

Zatem $|\mathbb{Z}_n^*| = \varphi(n)$.

## Przykład

$\varphi(0) = 0, \varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2$
$\varphi(p) = p - 1, p \in \mathbb{P}$ (oznaczenie zbioru liczb pierwszych)

A co jeśli $n$ nie jest liczbą pierwszą? Jak policzyć $\varphi(n)$?

## Twierdzenie

*Jeśli dany jest rozkład liczby n na czynniki pierwsze*
$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \forall i \ \alpha_i \neq 0, \forall i \ p_i \in \mathbb{P}, p_i \neq p_j$ *dla* $i \neq j$, *to*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

A co jeśli $n$ nie jest liczbą pierwszą? Jak policzyć $\varphi(n)$?

## Twierdzenie

*Jeśli dany jest rozkład liczby n na czynniki pierwsze* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \forall i\ \alpha_i \neq 0, \forall i\ p_i \in \mathbb{P}, p_i \neq p_j$ *dla* $i \neq j$, *to*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Wnioski:

- Jeśli $n = p \in \mathbb{P}$, to $\varphi(n) = n\left(1 - \frac{1}{p}\right) = n - 1$,
- Jeśli $n = p_1 p_2$, to
  $\varphi(n) = p_1 p_2\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) = (p_1 - 1)(p_2 - 1)$.

## Przykład

$|\mathbb{Z}_{450}^*| = ?$, czyli $\varphi(450) = ?$

$450 = 2 \cdot 3^2 \cdot 5^2$

$$\varphi(450) = 450 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 2 \cdot 3^2 \cdot 5^2 \cdot \frac{1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5} =$$

$$= 2 \cdot 3 \cdot 4 \cdot 5 = 120$$

# Potęga elementu w grupie

Niech $(X, \circ)$ (notacja multiplikatywna), $e$- element neutralny, $x \in X$
Wówczas definiujemy całkowite potęgi elementu $x$

1. $x^0 := e$,
2. $\forall n \in \mathbb{N}\ x^{n+1} := x^n \circ x$,
3. $\forall n \in \mathbb{Z}, n < 0\ x^n := (x^{-1})^{-n}$

Czyli $x^2 = x \circ x$, $x^3 = x \circ x \circ x$, $x^{-2} = x^{-1} \circ x^{-1}$.

W notacji addytywnej mówimy o krotności elementu w grupie.
Zamiast pisać $x^k$ zapisujemy wtedy $k \cdot x$.

# Rząd elementu w grupie

## Definicja

Rzędem elementu w grupie $(X, \circ)$ nazywamy najmniejszy wykładnik potęgi tego elementu, która jest równa elementowi neutralnemu. Czyli takie $k$, że

$$k = \min\{m \in \mathbb{N}_+ : x^m = e\}$$

Oznaczenie: $|x|$

**Uwaga**: $|e| = 1$

**Twierdzenie**

*W grupie skończonej (mającej skończoną liczbę elementów) każdy element ma rząd skończony.*

**Twierdzenie**

*W grupie skończonej (mającej skończoną liczbę elementów) każdy element ma rząd skończony.*

**Twierdzenie**

*Rząd każdego elementu grupy skończonej dzieli rząd grupy.*

## Przykład

- W grupie $(\mathbb{Z}_8^*, \cdot)$ mamy:
  $|1| = 1$ - jest to el. neutralny;
  $|3| = 2$, bo $3^2 = 3 \cdot 3 = 9 = 1 (\mathrm{mod}\ 8)$,
  $|5| = 2$, bo $5^2 = 25 = 1 (\mathrm{mod}\ 8)$.

  Zadanie: Oblicz rząd 7 w tej grupie. Czy w tej grupią są jeszcze jakieś elementy?

## Przykład

- W grupie $(\mathbb{Z}_8^*, \cdot)$ mamy:
  $|1| = 1$ - jest to el. neutralny;
  $|3| = 2$, bo $3^2 = 3 \cdot 3 = 9 = 1 (\mathrm{mod}\ 8)$,
  $|5| = 2$, bo $5^2 = 25 = 1 (\mathrm{mod}\ 8)$.

  Zadanie: Oblicz rząd 7 w tej grupie. Czy w tej grupią są jeszcze jakieś elementy?
- W grupie $(\mathbb{Z}_8, +)$ szukamy najmniejszej krotności elementu, która będzie równa $0 = e$. Mamy więc:
  $|1| = 8$, bo $1 + 1 = 2 \neq 0$, $1 + 1 + 1 = 3$, itd. aż dojdziemy do $8 \cdot 1 = 0 (\mathrm{mod}\ 8)$,
  $|2| = 4$, $|3| = 8$ (sprawdź!), $|4| = 2$.

  Zadanie: Znajdź rząd pozostałych elementów tej grupy. Zauważ, że rząd elementu musi być dzielnikiem liczby 8 (rzędu grupy), czyli wynosi $1, 2, 4$ lub $8$.

Poniższe dwa twierdzenia są ważne z punktu widzenia zastosowań. Dzięki nim metody kodowania Rabina i RSA działają!

## Twierdzenie (Euler)

*Jeżeli* $a, n \in \mathbb{N}_+$, $a \perp n$, *to* $a^{\varphi(n)} = 1 (\mathrm{mod}\ n)$.

## Twierdzenie (małe twierdzenie Fermata)

*Jeżeli* $a \in \mathbb{Z}$, $p \in \mathbb{P}$, *to* $a^p = a (\mathrm{mod}\ p)$.