## ZASADA INDUKCJI MATEMATYCZNEJ

Predykat, inaczej zdanie wyrażające bądź to cechę zawartego w nim podmiotu, bądź też związki występujące pomiędzy jego podmiotami. Umożliwia w skrótowy, symboliczny sposób zapisywać zdania wyrażające właściwości i/lub relacje o prawdziwości, których chcemy wykazać.

**Dowód indukcyjny:**

Należy wykazać, że właściwość predykatu $P(n)$ jest spełniona dla wszystkich liczb naturalnych począwszy od pewnego $k$, czyli $n \geqslant k, \quad n, k \in N$.

### Zasada indukcji matematycznej

Jeżeli istnieje taka liczba naturalna $n_0$, że:

$1^o$ $P(n_0)$ jest zdaniem prawdziwym

$2^o$ dla dowolnej liczby naturalnej $n \geqslant n_0$ jest prawdziwa implikacja

$$P(n) \Rightarrow P(n+1),$$

to $P(n)$ jest zdaniem prawdziwym $\forall n \geqslant n_0$.

### PRZYKŁADY

1. Wykazać, że $1 + 2 + 3 \cdot + n = \dfrac{n(n+1)}{2}$

   Dowód indukcyjny:

   (1) (Baza indukcyjna) Dla $n = 1$, mamy: $1 = \dfrac{1(1+1)}{2} \Leftrightarrow 1 = 1$;

   (2) (Założenie indukcyjne) Dla $n = k$ zachodzi $1 + 2 + 3 \cdot + k = \dfrac{k(k+1)}{2}$.

   (3) (Teza indukcyjna)

   Dla $n = k+1$, pokazać, że zachodzi równość $1 + 2 + 3 \cdot + k + (k+1) = \dfrac{(k+1)(k+2)}{2}$.

   Dowód:

   $1 + 2 + 3 \cdot + k + (k+1) = \dfrac{k(k+1)}{2} + (k+1) = \dfrac{(k+1)(k+2)}{2}$ cnd.

2. Udowodnić, że $2n + 1 < 2^n$ dla $n \geqslant 3$.

   1) $n = 3, \quad 2 \cdot 3 + 1 = 7 < 8 = 2^3$

   2) Założenie: $2n + 1 < 2^n$

   3) Teza: $2(n+1) + 1 < 2^{n+1}$

   Dowód.

   $2(n+1) + 1 = 2n + 3 < 2^n + 4 = 2^n + 2^2 \leqslant 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.

### ZADANIA

1. Pokazać, że $n^2 < 2^n$, dla $n \geqslant 5$.

2. Udowodnić, że iloczyn dwóch liczb nieparzystych jest liczba nieparzystą.

3. Udowodnić, że liczba $\sqrt{3}$ jest niewymierna.

4. Korzystając z indukcji matematycznej udowodnić, że dla każdej liczby naturalnej $n$ liczba $4^n$–1 podzielna jest przez 3.

## FUNKCJE CAŁKOWITOLICZBOWE

Liczby całkowite są podstawą matematyki dyskretnej. Często jesteśmy zmuszeni przekształcać liczby wymierne lub rzeczywiste na całkowite. Jednymi z takich przekształceń są funkcje całkowitoliczbowe: *podłoga* i *sufit* (*powała*).

$$\text{Niech } f : R \to Z$$

1. Funkcja *podłoga* $\lfloor\ \rfloor$ (dolne zaokrąglenie całkowitoliczbowe)

$$x \in R, \quad \lfloor x \rfloor = \max\{k \in Z : k \leqslant x\}$$

$\lfloor x \rfloor = k \Leftrightarrow k \leqslant x < k+1$

$\lfloor x \rfloor = k \Leftrightarrow x-1 < k \leqslant x$

np. $\lfloor e \rfloor = 2, \quad \lfloor -e \rfloor = -3, \quad \lfloor 2 \rfloor = 2, \quad \lfloor -3,5 \rfloor = -4$

Różnicę $\{x\} = x - \lfloor x \rfloor$ nazywamy *częścią ułamkową* $x$.

2. Funkcja powała $\lceil\ \rceil$ (górne zaokrąglenie całkowitoliczbowe)

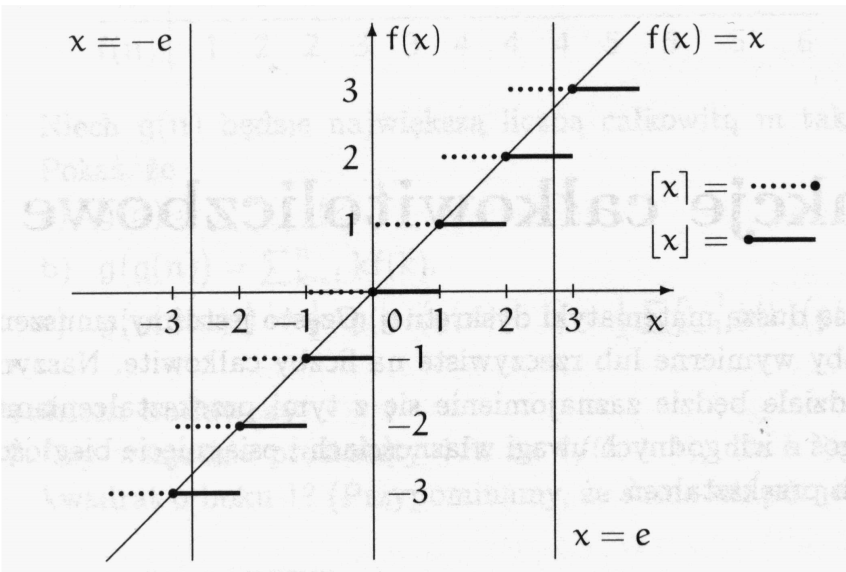
$$x \in R, \quad \lceil x \rceil = \min\{k \in Z : k \geqslant x\}$$

$\lceil x \rceil = k \Leftrightarrow k-1 < x \leqslant k$

$\lceil x \rceil = k \Leftrightarrow x \leqslant k < x+1$

np. $\lceil -e \rceil = -2, \quad \lfloor 5 \rfloor = 5, \quad \lfloor 1,7 \rfloor = 2$

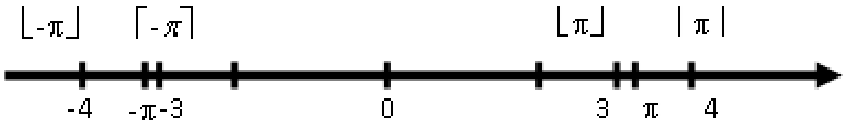
$$\lfloor x \rfloor = \max\{k \in Z : k \leqslant x\}, \qquad \lceil x \rceil = \min\{k \in Z : k \geqslant x\}$$




Rys.3.1 Wykres funkcji podłoga i sufit

## Własności funkcji podłoga i powała

1. $\lfloor -x \rfloor = -\lceil x \rceil$
2. $\lceil -x \rceil = -\lfloor x \rfloor$
3. $\lfloor x+n \rfloor = \lfloor x \rfloor + n;\quad n \in Z$
4. $\lfloor nx \rfloor \neq n \lfloor x \rfloor;\quad n \in Z$
5. $\lfloor x \rfloor = x \Leftrightarrow x \in Z \Leftrightarrow \lceil x \rceil = x$




Rys. Ilustracja funkcji $\lfloor\ \rfloor$ i $\lceil\ \rceil$

**Twierdzenie**
Jeżeli funkcja $f(x)$ jest ciągła, to

$$\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor \text{ oraz } \lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil .$$

Z tego twierdzenia wynika, że np. $\lfloor \sqrt{x} \rfloor = \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$.

## Zastosowanie funkcji podłoga i sufit

### PRZYKŁAD 4.

Ile bitów zajmuje napisanie liczby naturalnej $\alpha$ w postaci binarnej?

Odwróćmy pytanie. Jaką największa liczbę można zapisać na $n$ bitach?

Liczba taka ma wszystkie bity równe 1 w swoim rozwinięciu binarnym (111...1), więc jej wartość jest równa:

$$2^{n-1} + 2^{n-2} + ... + 2^1 + 2^0 = 2^n - 1.$$

Tę równość można uzasadnić obliczając sumę ciągu geometrycznego o ilorazie $q = 2$ i $a_1 = 1$ ($S = \dfrac{2^n - 1}{2 - 1}$).

Stąd $2^n - 1 \geqslant \alpha$ czyli $2^n \geqslant \alpha + 1$ *(logarytmując otrzymujemy)*

$$n \geqslant \log_2(\alpha + 1).$$

Aby była to najmniejsza liczba bitów korzystamy z funkcji sufit, czyli

$$n = \lceil \log_2(\alpha + 1) \rceil .$$

Inaczej, liczba zapisana na n bitach spełnia nierówność

$2^{n-1} \leqslant \alpha < 2^n$ *(logarytmując otrzymujemy)* $n - 1 \leqslant \log_2 \alpha < n$

Korzystając z funkcji podłoga

$$n - 1 = \lfloor \log_2 \alpha \rfloor \text{ więc } n = \lfloor \log_2 \alpha \rfloor + 1.$$

Na przykład:

$\alpha = 19,\quad 2^4 \leqslant 19 < 2^5,\quad n = \lfloor \log_2 19 \rfloor + 1,\ 19 = (10011)_2$

## ASYMPTOTYKA

**PRZYKŁAD 5.**

Silnię liczby naturalnej można trywialnie oszacować przez

$$n! = 1 \cdot 2 \cdot \dots \cdot n \leqslant n^n.$$

Istnieją także dokładniejsze oszacowania:

$$n^{\frac{n}{2}} \leqslant n! \leqslant \left(\frac{n+1}{2}\right)^n.$$

Nierówności w oszacowaniach bywają skomplikowane. Często wystarczają nam przybliżone, asymptotyczne oszacowania ciągów lub ogólniej funkcji. Opisują one zachowanie funkcji wraz ze wzrostem argumentu.

W oszacowaniach asymptotycznych posługujemy się ogólnie przyjętymi symbolami opisującymi asymptotyczne zachowanie jednej funkcji wobec drugiej. Najpowszechniej używany jest symbol $O$ przydatny w analizie górnej granicy asymptotycznej.

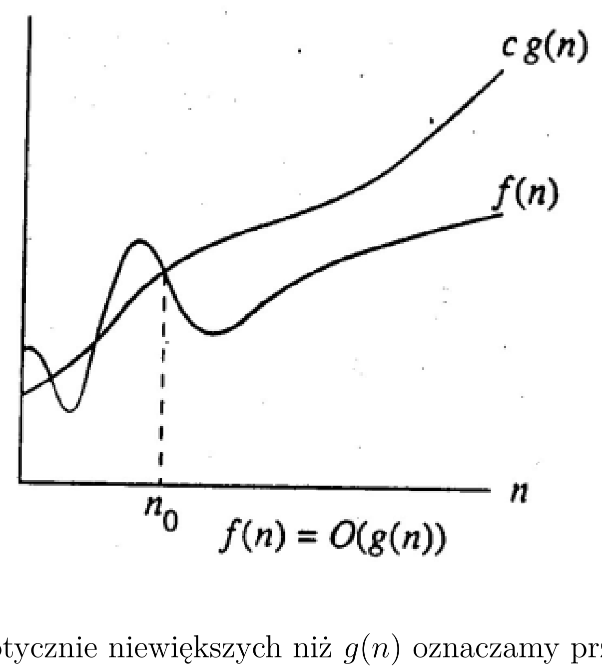
### Notacja asymptotyczna

***Funkcja asymptotycznie niewiększa*** od funkcji $g(n)$ to taka funkcja $f : N \to R$, dla której istnieją $c > 0$ i $n_0 \in N$ takie, że

$$|f(n)| \leqslant c \cdot |g(n)|$$

dla wszystkich $n \geqslant n_0$.

Mówimy, że $|f(n)| \leqslant c \cdot |g(n)|$ zachodzi dla prawie wszystkich liczb naturalnych $n$.




Zbiór funkcji asymptotycznie niewiększych niż $g(n)$ oznaczamy przez $O(g(n))$.

Ponieważ $O(g(n))$ jest zbiorem funkcji, poprawnie powinniśmy zapisywać $f(n) \in O(g(n))$, gdy $f$ spełnia warunek podany w definicji. Jednak przyjęło się zapisywać $f(n) = O(g(n))$. Jest to pewne nadużycie symbolu równości.

W związku z tym napis $f(n) = O(g(n))$ czytamy $f(n)$ jest $O$-duże od $g(n)$".

$$f(n) = O(g(n)) \;\Leftrightarrow\; \exists (c > 0, n_0 \in N) : |f(n)| \leqslant c \cdot |g(n)| \quad \forall n \geqslant n_0$$

## PRZYKŁADY

1. $O(1)$ to zbiór funkcji ograniczonych.

   Istotnie warunek $|f(n)| \leqslant c$ zachodzący dla prawie wszystkich $n$ łatwo jest, poprzez zamianę stałej $c$ na inną $c'$, sprowadzić do warunku $|f(n)| \leqslant c'$ zachodzącego już dla wszystkich $n \in N$, jako że skończenie wiele wartości $|f(n)|$ dla początkowych $n$ daje się ograniczyć przez stałą.

   - każda funkcja stała jest $O(1)$, np. $f(n) = 1000$ jest $O(1)$,
     bo $|f(n)| = 1000 \leqslant 1000$, dla dowolnego $n$,
   - $(-1)^n = O(1)$, bo $|(-1)^n| \leqslant 1$ dla dowolnego $n$,
   - $\frac{1}{n} = O(1)$, bo $\frac{1}{n} \leqslant 1$,dla dowolnego $n \geqslant 1$,
   - $\frac{\log n}{n} = O(1)$, bo $\log n < n$ dla $n \geqslant 1$, zatem $\frac{\log n}{n} \leqslant 1$, dla $n \geqslant 1$.

2. $O(n)$ to zbiór funkcji ograniczonych przez funkcję liniową:

   - wszystkie funkcje $O(1)$ są też $O(n)$,
   - $10n + 25 = O(n)$, bo $|10n + 25| \leqslant 11n$, dla $n \geqslant 25$,
   - $2n + 3\log n - 100 = O(n)$, bo $|2n + 3\log n - 100| \leqslant 3n$, dla dowolnego $n$.

3. $O(n^2)$

   - $3n^2 + 10n - 1 = O(n^2)$,
   - $\frac{n(n+1)}{2} = O(n^2)$.

4. $O(2^n)$

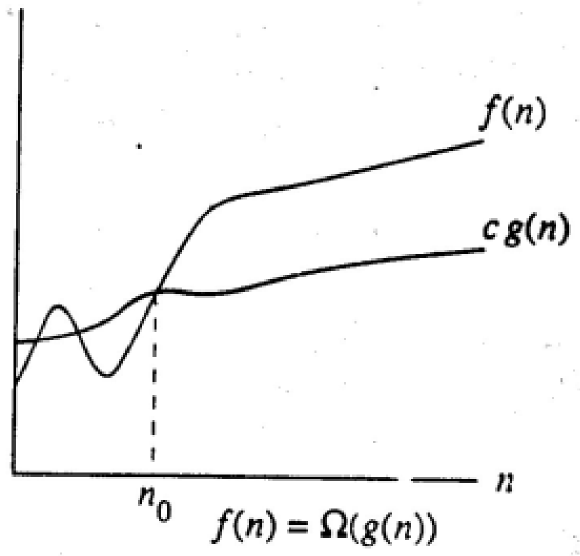
   - $3 \cdot 2^n + n = O(2^n)$, bo $n \leqslant 2^n$, a zatem $3 \cdot 2^n + n \leqslant 4 \cdot 2^n$, dla dowolnego $n$.

**Funkcja asymptotycznie nie mniejsza** od funkcji $g(n)$ to taka funkcja $f : N \to R$, dla której istnieją $c > 0,\ n_0 \in N$, że

$$c \cdot |g(n)| \leqslant |f(n)|\,,$$

dla wszystkich $n \geqslant n_0$.

Zbiór funkcji asymptotycznie nie mniejszych niż $g(n)$ oznaczamy przez $\Omega(g(n))$.

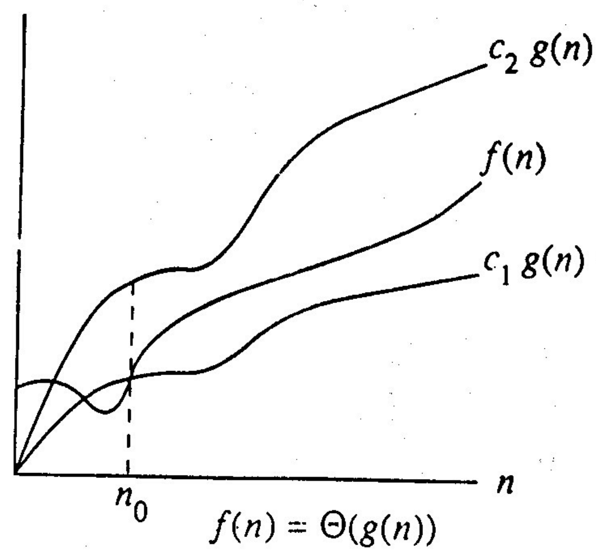



**Funkcja asymptotycznie podobna** do funkcji $g(n)$ to taka funkcja $f : N \to R$, dla której istnieją $c_0, c_1 > 0, n_0 \in N$, że

$$c_0 \cdot |g(n)| \leqslant |f(n)| \leqslant c_1 |g(n)|,$$

dla wszystkich $n \geqslant n_0$.

Zbiór funkcji asymptotycznie podobnych do $g(n)$ oznaczamy przez $\Theta(g(n))$. A zatem $\Theta(g(n)) = O(g(n)) \cap \Omega(g(n))$.




**Funkcja asymptotycznie mniejsza** od funkcji $g(n)$, to taka funkcja $f : N \to R$, że $\exists c > 0,\ n_0 \in N$, takie że

$$|f(n)| < c \cdot |g(n)|,$$

dla wszystkich $n \geqslant n_0$.

Zbiór funkcji asymptotycznie mniejszych niż $g(n)$ oznaczamy przez $o(g(n))$.

Zatem $f(n) = o(g(n))$ wtedy i tylko wtedy, gdy

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

**Własności wiążące funkcje asymptotyczne.**
Dla funkcji $f, g : N \to R$ mamy:

- jeśli $f(n) = O(g(n)),\ g(n) = O(h(n))$,to $f(n) = O(h(n))$,
- $f(n) = O(f(n))$,
- $f(n) = O\left(O(g(n))\right) \Leftrightarrow f(n) = O(g(n))$,
- $f(n) = O(|g(n)|) \Leftrightarrow f(n) = O(g(n))$,
- $f(n) = c \cdot O(g(n)) \Leftrightarrow f(n) = O(g(n))$.

**PRZYKŁAD 6.**
Dla wielomianów $f(n), g(n)$ rząd ich wielkości wyznaczony jest przez najwyższy stopień:

$$f = O(g) \text{ wtedy i tylko wtedy, gdy def } (f) \leqslant \deg g.$$

Ustala to następującą hierarchię rzędów funkcji:

$$n, n^2, n^3, n^4, \cdots, n^d, n^{d+1}, \cdots.$$

## ALGORYTM DZIELENIA

Niech $m|n$ oznacza „$m$ dzieli $n$”.

$$m|n \Leftrightarrow m \neq 0 \wedge n = mk, \quad \text{gdzie } m, n, k \in Z.$$

Kiedy dzielimy 6 przez 3 to „nie ma problemu”, bo $6 : 3 = 2$.
Natomiast jeśli dzielimy 7 przez 3 to „nie podzieli się równo”, bo $7 : 3 = 2,333...$

Załóżmy, że $n, m \in Z$, $n \geqslant m$. Gdy podzielimy $n$ przez $m$ otrzymamy następującą równość $n = mq + r$, gdzie $0 \leqslant r < m$. Interesuje nas w jaki sposób obliczamy $q$ i $r$:
$n = mq + r / : m$, stąd $\frac{n}{m} = q + \frac{1}{m}$, czyli $q = \left\lfloor \frac{n}{m} \right\rfloor$, $q$ jest częścią całkowitą liczby $\frac{n}{m}$.

Rozważmy oznaczenia operatorów $MOD$ i $DIV$:
$n\ MOD\ m$- reszta z dzielenia $n$ przez $m$
$n\ DIV\ m$ - iloraz całkowity z dzielenia $n$ przez $m$

Niektóre kalkulatory i większość języków programowania wykonują tę czynność następująco:

$$q = nDIVm = \left\lfloor \frac{n}{m} \right\rfloor \qquad r = nMODm = \left( \frac{n}{m} - nDIVm \right) m$$

a więc $n = (nDIVm)\, m + nMODm$ i ostatecznie $0 \leqslant nMODm < m$.

**PRZYKŁAD 7.**
$7MOD3 = 1; \quad 1MOD7 = 1; \quad 7MOD7 = 0$
$7DIV3 = 2; \quad 1DIV7 = 0; \quad 7DIV7 = 1$
$31MOD7 = 3; \quad (-31)MOD7 = 4; \quad 31DIV7 = 4; \quad (-31)DIV7 = -5$

## NAJWIĘKSZY WSPÓLNY DZIELNIK DWÓCH LICZB

$$\mathrm{NWD}(m, n) = \max \{k : k > 0, k|m \wedge k|n\}$$

Największy wspólny dzielnik dwóch liczb $m$ i $n$ jest to największa liczba całkowita, która dzieli $m$ i $n$.

Obliczanie NWD dwóch liczb ma zastosowanie w obliczeniach, w których posługujemy się ułamkami zwykłymi postaci $\frac{p}{q}$, ($p, q$ - liczby względnie pierwsze).

Np. liczby 13 i 15 są względnie pierwsze ponieważ $\mathrm{NWD}(13, 15) = 1$.

Jeśli ułamek nie jest zwykły np. $\frac{8}{16}$, to sprowadzamy go do postaci zwykłej dzieląc licznik i mianownik przez ich największy wspólny dzielnik (skracanie ułamków). Dzięki temu w obliczeniach nie pojawiają się niepotrzebnie zbyt duże liczby.

$$\mathrm{NWD}(8, 16) = 8, \ \ \text{stąd } \frac{8}{16} = \frac{1}{2}.$$

Przyjmijmy, że $n \geqslant m$. Dzieląc $n$ przez $m$ otrzymamy następującą równość

$$n = mq + r, \quad \text{gdzie } 0 \leqslant m < r.$$

Wynikają stąd następujące wnioski:

1. jeśli $r = 0$, to $\mathrm{NWD}(m, n) = m$, czyli mniejsza z tych liczb jest ich największym wspólnym dzielnikiem;

2. jeśli $r \neq 0$, to $r = n - mq$, stąd wynika, że każda liczba dzieląca $n$ i $m$ dzieli również $r$, zatem, największy wspólny dzielnik $n$ i $m$ dzieli również resztę.

Z tych wniosków wynika równość:

$$\mathrm{NWD}(m, n) = \mathrm{NWD}(r, m), \text{gdzie przyjęliśmy, że } \mathrm{NWD}(0, n) = n.$$

Zależność $n = mq + r, \quad 0 \leqslant m < r$ zapewnia, że możemy generować pary liczb o tym samym największym wspólnym dzielniku. Elementy tych par tworzą malejący ciąg liczb naturalnych, a więc ten ciąg jest skończony i na jego końcu otrzymujemy szukany dzielnik.

Np. $48 = 1 \cdot 46 + 2$

$46 = 23 \cdot 2 + 0$

czyli NWD$(46, 48)$ =NWD$(2, 46) = 2$.

## ALGORYTM EUKLIDESA

Algorytm ten dla danych naturalnych $m$ i $n$, jednocześnie oblicza NWD$(m, n)$ i znajduje rozwiązanie równania:

$$mx + ny = k, \text{w którym } k = \text{NWD}(m, n).$$

Zapisujemy w postaci iteracji kolejne kroki algorytmu Euklidesa:

$$a_0 = q_1 a_1 + a_2;$$

$$a_1 = q_2 a_2 + a_3;$$

$$\cdots\cdots$$

$$\cdots\cdots$$

$$a_{l-1} = q_1 a_1 + a_{l+1},$$

gdzie $a_0 = n, a_1 =$, oraz $a_{l+1} = 0$, czyli $a_l =$ NWD$(m, n)$.

**PRZYKŁAD 8.**

Dla liczb $m = 12, n = 21$, stosując algorytm Euklidesa, wyznaczyć NWD$(12, 21)$.

$$\begin{array}{ccc} 21 = 1 \cdot 12 + 9 & \text{czyli} & 21 - 1 \cdot 12 = 9 \\ 12 = 1 \cdot 9 + 3 & \text{czyli} & 12 - 1 \cdot 9 = 3 \\ 9 = 3 \cdot 3 + 0 & \text{czyli} & 9 - 3 \cdot 3 = 0 \end{array}$$

Zatem NWD$(12, 21) = 3$.

### Zastosowanie algorytmu Euklidesa

**ZADANIE**

Dane są czerpaki o pojemności 4 i 6 litra. Czy można za pomocą tych czerpaków napełnić wodą naczynie o pojemności 15 litrów? Jeśli tak, to jak to zrobić?

Należy rozwiązać równanie

$$4x + 6y = 15, \quad \text{gdzie } x \text{ i } y \text{ są liczbami całkowitymi.}$$

Czy istnieje rozwiązanie tego równania?

Równie diofantyczne: $mx + ny = k$, gdzie $m, n,\ k \in N$ są współczynnikami równania, a $x, y \in Z$ są niewiadomymi.

**Równanie to ma rozwiązanie** wtedy i tylko wtedy, gdy $k$ jest wielokrotnością NWD$(m, n)$.

Oznacza to, że równanie z powyższego zadania nie ma rozwiązania, ponieważ $\text{NWD}(4,6) = 2$.

**PRZYKŁAD 10.**

Stosując algorytm Euklidesa wyznacz liczby całkowite $x$ i $y$ spełniające równość $333x + 1234y = 1$.

Wykonujemy algorytm Euklidesa dla liczb 333 i 1234.

$$
\begin{aligned}
&1234 = 3 \cdot 333 + 235 \quad \Rightarrow \quad 1234 - 3 \cdot 333 = 235 \\
&333 = 1 \cdot 235 + 98 \quad \Rightarrow \quad 333 - 1 \cdot 235 = 98 \\
&235 = 2 \cdot 98 + 39 \quad \Rightarrow \quad 235 - 2 \cdot 98 = 39 \\
&98 = 2 \cdot 39 + 20 \quad \Rightarrow \quad 98 - 2 \cdot 39 = 20 \\
&39 = 1 \cdot 20 + 19 \quad \Rightarrow \quad 39 - 1 \cdot 20 = 19 \\
&20 = 1 \cdot 19 + 1 \quad \Rightarrow \quad 20 - 1 \cdot 19 = 1 \\
&19 = 1 \cdot 19 + 0 \quad \Rightarrow \quad 19 - 1 \cdot 19 = 0
\end{aligned}
$$

A następnie „cofamy się”:

$$
\begin{aligned}
&20 - 1 \cdot (39 - 1 \cdot 20) = 1 \quad \Rightarrow \quad -1 \cdot 39 + 2 \cdot 20 = 1 \\
&-1 \cdot 39 + 2 \cdot (98 - 2 \cdot 39) = 1 \quad \Rightarrow \quad -5 \cdot 39 + 2 \cdot 98 = 1 \\
&-5 \cdot (235 - 2 \cdot 98) + 2 \cdot 98 = 1 \quad \Rightarrow \quad -5 \cdot 235 + 12 \cdot 98 = 1 \\
&-5 \cdot 235 + 12 \cdot (333 - 1 \cdot 235) = 1 \quad \Rightarrow \quad -17 \cdot 235 + 12 \cdot 333 = 1 \\
&-17 \cdot (1234 - 3 \cdot 333) + 12 \cdot 333 = 1 \quad \Rightarrow \quad 63 \cdot 333 - 17 \cdot 1234 = 1
\end{aligned}
$$

Ostatecznie otrzymujemy $333 \cdot 63 - 1234 \cdot 17 = 1$, stąd $x = 63,\ y = -17$.

## NAJMNIEJSZA WSPÓLNA WIELOKROTNOŚĆ

Najmniejszą wspólną wielokrotnością liczb naturalnych jest najmniejsza liczba naturalna która dzieli się przez $m$ i $n$.

$$\text{NWW}(m,n) = \min\{k : k \in Z_+,\ m|k \wedge n|k\}$$

Własności:

$$\text{NWW}(m,n) = \frac{mn}{\text{NWD}(m,n)}$$

$$\text{NWW}(m,n) = m\frac{n}{\text{NWD}(m,n)}$$

$$\text{NWW}(m,n) = m\,(nDIV\,\text{NWD(m,n)})$$

## Rozkład liczb naturalnych na czynniki pierwsze

Liczbę naturalną $n$ nazywamy **liczbą pierwszą** wtedy i tylko wtedy, gdy ma dokładnie dwa dzielniki: 1 oraz $n$.

**Liczba złożona** to taka liczba naturalna, która ma co najmniej trzy różne dzielniki. Oznacza to, że liczba 1 nie jest ani liczbą pierwszą, ani złożoną.

Najmniejszą liczbą pierwszą jest 2, a najmniejszą liczbą złożoną 4. Liczby pierwsze możemy ustawić w ciąg rosnący, którego fragment początkowy ma postać:

$$2, 3, 5, 7, 11, 13, 17, 19, \cdot$$

Wykażemy, że ciąg ten jest nieskończony, inaczej mówiąc:

**Twierdzenie**

Istnieje nieskończenie wiele liczb pierwszych.

Istnieje bardzo wiele (choć skończenie wiele) dowodów tego faktu. Oto najstarszy z nich, przypisywany Euklidesowi.

Dowód.

Załóżmy, że zbiór liczb pierwszych jest skończony i składa się z liczb $p_1, p_2, \cdots, p_k$. Rozważmy liczbę $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$. Liczba ta nie dzieli się przez żadną z liczb $p_i$, a zatem musi mieć pewien dzielnik pierwszy $p$ różny od każdego z $p_i$, dla $i = 1, 2, \cdots, n$, co przeczy założeniu.

Dowód powyższego twierdzenia pozornie sugeruje algorytm generowania kolejnych liczb pierwszych. Rozważmy ciąg liczbowy zdefiniowany przez rekurencję:

$$\begin{cases} e_1 = 1, \\ e_n = e_1 \cdot e_2 \cdot \cdots \cdot e_{n-1} + 1 \end{cases} .$$

Elementy tego ciągu nazywamy *liczbami Euklidesa.* Początkowe wyrazy tego ciągu

$$2, 3, 7, 43$$

są liczbami pierwszymi, jednak już $e_5 = 1807$ jest liczbą złożoną.

Niemniej, liczby Euklidesa są parami **względnie pierwsze** czyli

$$\mathrm{NWD}(E_m, E_n) = 1, \quad \text{gdy } n \neq m.$$

## Liczby pierwsze Mersena (Mersenn'a, XVII w.)

Najczęściej stosowanym wzorem na liczby pierwsze jest

$$2^p - 1, \quad \text{gdzie } p - \text{ liczba pierwsza}$$

Czy liczba $2^p - 1$ jest liczbą pierwszą dla każdego $p$?

Łatwo zauważyć, że liczba $2^p - 1$ nie zawsze jest pierwsza, np. dla $p = 11$ mamy: $2^{11} - 1 = 2047 = 23 \cdot 89$, ale dla $p = 2, 3, 5, 7, 19, 31, 61, 89$ liczby tej postaci są pierwsze.

Największa liczba pierwsza Mersena dla $p = 1398269$ została odkryta w 1996 roku.

**Liczby pierwsze Fermat'a**

$$L_k = 2^{2^k} + 1,$$

dla $k = 1, 2, 3, 4$ - liczba $L_k$ jest liczbą pierwszą,a dla $k = 5$ nie jest liczbą pierwszą.

Liczby pierwsze są obecnie wykorzystywane w **kryptografii** do kodowania informacji przesyłanych w sieciach komputerowych. W tym celu są potrzebne bardzo duże takie liczby.

**Problem znalezienia jakiegokolwiek algorytmu generującego wszystkie liczby pierwsze jest ciągle problemem otwartym.**

Do wyznaczania liczb pierwszych można wykorzystać tak zwane *sito Eratostenesa*, trudno jednak uznać tę metodę za efektywną. Pokażemy ją na następującym przykładzie.

**PRZYKŁAD 11.**

Wyznaczymy, wykorzystując sito Eratostenesa, wszystkie liczby pierwsze nie większe niż 15.

W tym celu wypisujemy wszystkie liczby naturalne z przedziału $[2, 15]$

$$\mathbf{2,3,4,5,6,7,8,9,10,11,12,13,14,15,}$$

wybieramy liczbę 2 jako najmniejszą liczbę pierwszą i wykreślamy co drugą liczbę spośród pozostałych

$$\mathbf{2,3,}\cancel{4}, \mathbf{5}, \cancel{6}, \mathbf{7}, \cancel{8}, \mathbf{9}, \cancel{10}, \mathbf{11}, \cancel{12}, \mathbf{13}, \cancel{14}, \mathbf{15},$$

Wśród liczb nieskreślonych wybieramy najmniejszą jest to 3, i skreślamy w ciągu zaczynającym się od 4 co trzecią liczbę:

$$\mathbf{2,3,}\cancel{4}, \mathbf{5}, \cancel{6}, \mathbf{7}, \cancel{8}, \cancel{9}, \cancel{10}, \mathbf{11}, \cancel{12}, \mathbf{13}, \cancel{14}, \cancel{15},$$

i tak dalej.

Ostatecznie otrzymujemy

$$\mathbf{2,3,}\cancel{4}, \mathbf{5}, \cancel{6}, \mathbf{7}, \cancel{8}, \cancel{9}, \cancel{10}, \mathbf{11}, \cancel{12}, \mathbf{13}, \cancel{14}, \cancel{15},$$

Liczby wytłuszczone są szukanymi liczbami pierwszymi.

Jeżeli $n \geqslant 1$, to $\pi(n)$ oznacza liczbę liczb pierwszych nie większych od $n$.

**PRZYKŁAD 12.**

$$\pi(1) = 0 \ \text{ i } \ \pi(1) = 1$$

Korzystając z przykładu 11 otrzymujemy $\pi(15) = 6$.

Można wykazać, aczkolwiek dowód tego faktu jest trudny, że dla dużych liczb naturalnych $n$

$$\pi(n) \sim \frac{n}{\ln n}.$$

W dowodzie powyższego twierdzenia korzysta się z dość oczywistej obserwacji, iż każda liczba naturalna $n > 1$ musi mieć co najmniej jeden dzielnik będący liczbą pierwszą.

Oznacza to, że każda liczba naturalna większa od 1 może być przedstawiona w postaci iloczynu liczb pierwszych. Co więcej, iloczyn ten ma jednoznacznie ustalone czynniki.

**Twierdzenie** (Zasadnicze twierdzenie arytmetyki)
Każda liczba naturalna $n > 1$ może być przedstawiona jednoznacznie (z dokładnością do kolejności czynników) jako iloczyn potęg liczb pierwszych.

Z powyższego twierdzenia wynika że każda liczba naturalna $n \geqslant 1$ może być jednoznacznie przedstawiona w postaci:

$$\prod_{i \geqslant 1} p_i^{n_i},$$

gdzie $n_i \geqslant 0$, dla każdego $i \geqslant 1$.

Istotnie, jeżeli $n = 1$, to $n_i = 0$ dla wszystkich $i \in N$. W pozostałych przypadkach, zgodnie z powyższym twierdzeniem, taka reprezentacja jest również możliwa, przy czym, rzecz jasna, prawie wszystkie (poza skończoną liczbą) wykładniki będą zerami, a zatem jedynie skończenie wiele czynników iloczynu będzie różnych od 1.

$$Re\ p(n) = (n_i)_{i \geqslant 1} \Leftrightarrow n = \prod_{i \geqslant 1} p_i^{n_i}.$$

Oznacza to, że każda liczba naturalna może być reprezentowana jako nieskończony ciąg $(n_1, n_2, \cdots)$, w którym jest tylko skończenie wiele elementów różnych od zera.

**PRZYKŁAD 13.**
$12 = 2^2 \cdot 3_1$, zatem $Rep(12) = (2, 1, 0, 0, \cdots)$. Z drugiej strony $(1, 2, 0, 0, \cdots) = Rep(2^1 \cdot 3^2) = Rep(18)$.
Zauważmy, że funkcja $Rep$ ma kilka pożytecznych własności. Przyjmijmy, że

$$Re\ p(n) = (n_i)_{i \geqslant 1}, \quad Re\ p(m) = (m_i)_{i \geqslant 1}, \quad Re\ p(k) = (k_i)_{i \geqslant 1}.$$

Wtedy

$$n = \prod_{i \geqslant 1} p_i^{n_i}, \quad m = \prod_{i \geqslant 1} p_i^{m_i},$$
$$n \cdot m = \prod_{i \geqslant 1} p_i^{n_i + m_i},$$

co oznacza, że

$$k = n \cdot m \Leftrightarrow \forall i \geqslant 1, k_i = n_i + m_i$$

a tym samym

$$n | m \Leftrightarrow \forall i \geqslant 1, n_i \leqslant m_i.$$

Możemy zatem wnioskować, że

$$k = \mathrm{NWD}(n, m) \Leftrightarrow \forall i \geqslant 1, k_i = \min\{n_i, m_i\},$$

$$k = \mathrm{NWW}(n, m) \Leftrightarrow \forall i \geqslant 1, k_i = \max\{n_i, m_i\}.$$

**PRZYKŁAD 14.**

Ponieważ

$$Rep(16) = (4, 0, 0, \cdots) \quad \text{oraz} \quad Rep(24) = (3, 1, 0, \cdots), \text{więc}$$

$$Rep(\mathrm{NWD}(24, 16)) = (3, 0, 0, \cdots),$$

czyli

$$\mathrm{NWD}(24, 16) = 23 = 8.$$

Analogicznie

$$Rep(\mathrm{NWW}(24, 16)) = (4, 1, 0, \cdots),$$

zatem

$$\mathrm{NWW}(24, 16) = 24 \cdot 31 = 48.$$

Liczby naturalne $m, n$ nazywamy *względnie pierwszymi*, co będziemy oznaczać $m \perp n$, wtedy i tylko wtedy, gdy $\mathrm{NWD}(m, n) = 1$.

Zauważmy, że dla dowolnych $n, m$, o ile $n^2 + m^2 \neq 0$, to

$$\frac{m}{\mathrm{NWD}(m, n)} \perp \frac{n}{\mathrm{NWD}(m, n)}.$$

Ponadto, jeżeli $Re\ p(m) = (m_i)_{i \geqslant 1}$, $Re\ p(n) = (n_i)_{i \geqslant 1}$, to

$$m \perp n \quad \Leftrightarrow \quad Re\ p(\mathrm{NWD}(m, n)) = (0, 0 \cdots),$$

a więc zgodnie z tym, co było wyżej

$$m \perp n \quad \Leftrightarrow \quad \forall i \geqslant 1, \min\{m_i, n_i\} = 0 \quad \Leftrightarrow \quad \forall i \geqslant 1, m_i \cdot n_i = 0.$$

Korzystając z funkcji Rep łatwo udowodnić następujące twierdzenie:

**Twierdzenie**

Dla dowolnych dodatnich liczb naturalnych $k, m, n$:

## Ćwiczenia

1. Zastosować sito Eratostenesa dla $x = 26$.
2. Znaleźć Rep(192), Rep(336) i na tej podstawie wskazać $\mathrm{NWD}(192, 336)$ oraz $\mathrm{NWW}(192, 336)$.

## ZBIORY

Pojęcie zbioru zaliczamy do pojęć pierwotnych. Zamiast zbiór mówimy też w pewnych przypadkach *klasa, przestrzeń* lub *rodzina.* Dawniej zamiast zbiór mówiono *mnogość.* Twórcą teorii zbiorów był Georg Cantor (1845 – 1918).

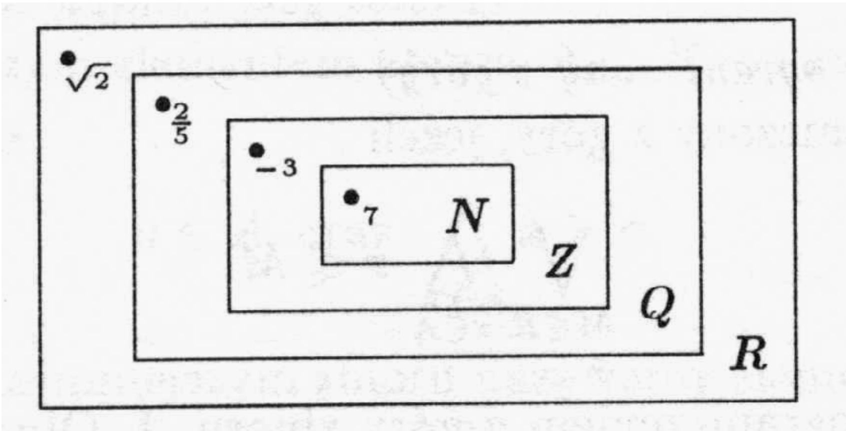
Symbolem $\{a_1, a_2, \cdots a_n\}$ , $a_i \neq a_j$, dla $i \neq j$, oznaczamy zbiór o $n$ elementach: $a_1, a_2, \cdots a_n$. Jest to zbiór skończony $n$ elementowy.

Zbiory liczbowe: $N$ – zbiór liczb naturalnych $N = \{1, 2, 3, \cdots\}$

$Z$ – zbiór liczb całkowitych $Z = \{0, \pm1, \pm2, \pm3, \pm4, \cdots\}$

$Q$ – zbiór liczb wymiernych $Q = \left\{\frac{m}{n} : m \in Z,\ n \in Z, n \neq 0\right\}$

$R$ – zbiór liczb rzeczywistych




Rys. 1.1 Relacje między zbiorami $N, Z, Q, R$

$N \subset Z \subset Q \subset R$

Moc zbioru $S$ (liczba elementów zbioru $S$) oznaczymy symbolem $|S|$

$|N| = |Z| = |Q| = \aleph_0$ (alef zero – litera hebrajska),

$|R| = c$ (continuum),

$2^S$- zbiór (rodzina) wszystkich podzbiorów zbioru $S$.

$$\left|2^S\right| = 2^{|S|}$$

## METODY DOWODZENIA

$p, q$ – zdania logiczne.

Implikacja $p \Rightarrow q$ jest *prawdziwa* iff, gdy $p$ i $q$ są prawdziwe lub $p$ jest fałszywe.

Każde twierdzenie zawiera założenia i tezę (którą należy udowodnić).
Jeżeli zdanie $p$ jest założeniem, a $q$ tezą, to dowód sprowadza się wykazania prawdziwości implikacji: $p \Rightarrow q$.

### PRZYKŁAD 15.

Tw. Jeżeli $n \in N$ jest liczbą parzystą, to $n^2$ jest liczbą parzystą.
W tym przypadku $p \equiv (n \in N$jest liczbą parzystą$)$, $q \equiv (n^2$ jest liczbą parzystą$)$. Należy udowodnić, że $p \Rightarrow q$.

$\otimes$(koniec przykładu)

Należy udowodnić, że

$$p \Rightarrow q$$

1. Dowód wprost:

Zakładając, że $p$ jest prawdą, należy wykazać prawdę $q$.

2. Dowód nie wprost - *przez kontrapozycję (zaprzeczenie)*:

Przyjmując za prawdę $\neg q$, wykazać prawdę $\neg p$ (tj. przyjmując, że $\neg q$ jest prawdziwe udowodnić: że $\neg q \Rightarrow \neg p$).
Zachodzi bowiem równoważność:

$$(\neg q \Rightarrow \neg p) \Leftrightarrow (p \Rightarrow q)$$

### PRZYKŁAD 16.

Udowodnić, że jeśli liczba $n_2$ jest parzysta, to $n$ jest też liczbą parzystą

$$p \equiv \left[n^2 \text{ jest liczbą parzystą}\right], \quad q \equiv [n \text{ jest liczbą parzystą }]$$
$$\left(\left[n^2 \text{ jest liczbą parzystą}\right] \Rightarrow [n \text{ jest liczbą parzystą}]\right) \quad \Leftrightarrow$$
$$\left(\neg\,[n \text{ jest liczbą parzystą}] \Rightarrow \neg \left[n^2 \text{ jest liczbą parzystą}\right]\right)$$

Ponadto

$(\neg\,[n \text{ jest liczbą parzystą}]) \Rightarrow n = 2k+1 \Rightarrow n^2 = 4k^2+4k+1 \Rightarrow \neg \left[n^2 \text{ jest liczbą parzystą}\right]$

$\otimes$

3. Dowód indukcyjny

Wykazać, że właściwość predykatu $P(n)$ (w tym przypadku - zdanie logiczne wiążące pewną własność z liczbami naturalnymi) jest spełniona dla wszystkich liczb naturalnych począwszy od pewnego $k$, czyli
$n \geqslant k, \quad k, n \in N$ (np. $2^n > 2n$, $\forall n \geqslant 3$ w tym przyp. $k = 3$).