

Stefan Sokołowski

MATEMATYKA DYSKRETNA

wykład 4

**Inst. Informatyki Stosowanej, ANS
Elbląg, 2024/2025**

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

(A) $n = k \cdot q + r$ oraz

(B) $0 \leq r < k$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka
$7/3 = 2$ $7 \bmod 3 = 1$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka
$7/3 = 2$ $7 \bmod 3 = 1$
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka
$7/3 = 2$ $7 \bmod 3 = 1$
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka
$7/3 = 2$ $7 \bmod 3 = 1$
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$	
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$	

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$		
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$		
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$		

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$			
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$			
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$			

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	$(-7)/3 = -2$ $(-7)\%3 = -1$		
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$			
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$			

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	$(-7)/3 = -2$ $(-7)\%3 = -1$	tak	nie
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$			
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$			

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	$(-7)/3 = -2$ $(-7)\%3 = -1$	tak	nie
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$	$7/(-3) = -2$ $7\%(-3) = 1$		
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$			

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	$(-7)/3 = -2$ $(-7)\%3 = -1$	tak	nie
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$	$7/(-3) = -2$ $7\%(-3) = 1$	tak	nie
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$			

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	$(-7)/3 = -2$ $(-7)\%3 = -1$	tak	nie
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$	$7/(-3) = -2$ $7\%(-3) = 1$	tak	nie
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$	$(-7)/(-3) == 2$ $(-7)\%(-3) == -1$		

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$(A) \quad n = k \cdot q + r \quad \text{oraz}$$

$$(B) \quad 0 \leq r < k$$

„sprawdzanie dzielenia przez mnożenie”
(3. klasa szk. podst.)

oznaczenia:

$$q = n / k \quad \text{— iloraz całkowity}$$

$$r = n \bmod k \quad \text{— reszta}$$

$$n = k \cdot (n/k) + n \bmod k$$

Uwaga: komputery liczą inaczej...

matematyka	program w C	(A) spełnione	(B) spełnione
$7/3 = 2$ $7 \bmod 3 = 1$	$7/3 = 2$ $7\%3 = 1$	tak	tak
$(-7)/3 = -3$ $(-7) \bmod 3 = 2$	$(-7)/3 = -2$ $(-7)\%3 = -1$	tak	nie
$7/(-3) = \text{błąd}$ $7 \bmod (-3) = \text{błąd}$	$7/(-3) = -2$ $7\%(-3) = 1$	tak	nie
$(-7)/(-3) = \text{błąd}$ $(-7) \bmod (-3) = \text{błąd}$	$(-7)/(-3) == 2$ $(-7)\%(-3) == -1$	tak	nie

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$, czyli k nie jest dzielnikiem n

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$, czyli k nie jest dzielnikiem n

Proste własności:

- każda liczba dodatnia k jest dzielnikiem zera

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$, czyli k nie jest dzielnikiem n

Proste własności:

- każda liczba dodatnia k jest dzielnikiem zera
- jeśli $k \mid n$, to $k \mid np$ dla każdego $p \in \mathbb{Z}$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$, czyli k nie jest dzielnikiem n

Proste własności:

- każda liczba dodatnia k jest dzielnikiem zera
- jeśli $k \mid n$, to $k \mid np$ dla każdego $p \in \mathbb{Z}$
- jeśli $k \mid n$ i $k \mid m$, to $k \mid n + m$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$, czyli k nie jest dzielnikiem n

Proste własności:

- każda liczba dodatnia k jest dzielnikiem zera
- jeśli $k \mid n$, to $k \mid np$ dla każdego $p \in \mathbb{Z}$
- jeśli $k \mid n$ i $k \mid m$, to $k \mid n + m$
- jeśli $k \mid n$, $n > 0$ i $n \mid m$, to $k \mid m$

Podzielność

Twierdzenie: (o jednoznaczności dzielenia)

Niech $n, k \in \mathbb{Z}$ i $k > 0$. Wtedy istnieje dokładnie jedna para liczb $q, r \in \mathbb{Z}$, taka że

$$n = k \cdot q + r \quad \text{oraz} \quad 0 \leq r < k$$

Na tym wykładzie:

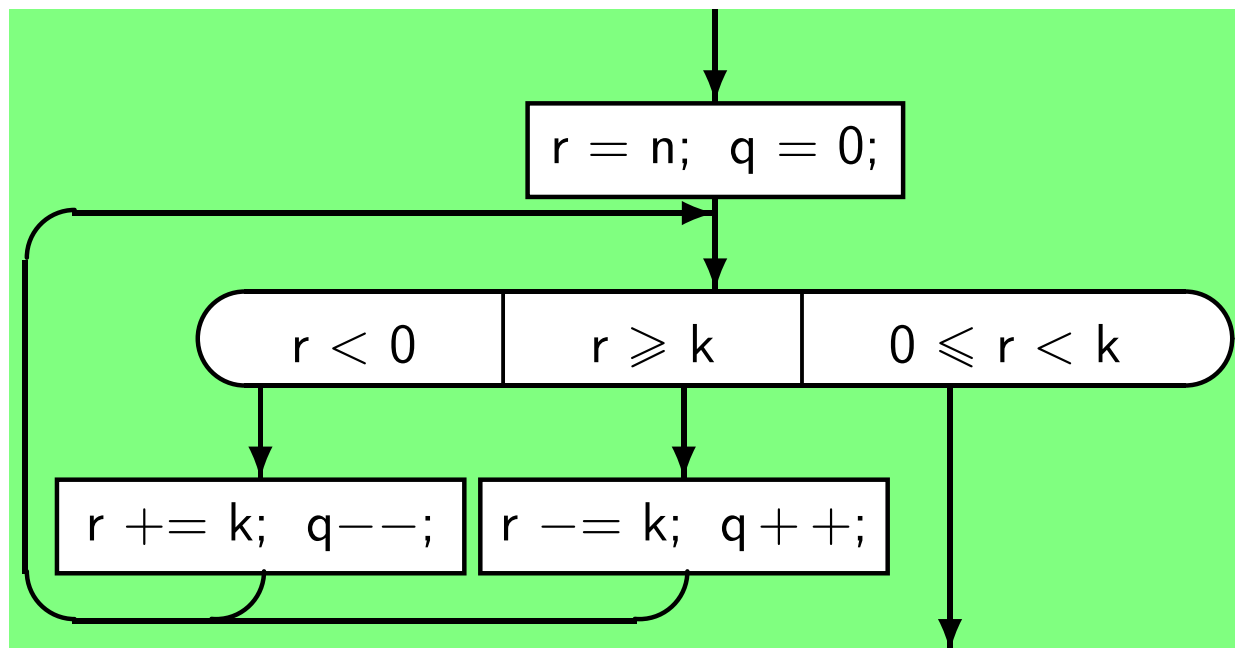
- dzielnik k jest **zawsze** ostro dodatni;
- $k \mid n$ oznacza:
 - $n \bmod k = 0$, czyli
 - $\exists_{q \in \mathbb{Z}} k \cdot q = n$, czyli
 - n dzieli się przez k , czyli
 - k jest dzielnikiem n
- $k \nmid n$ oznacza $\neg k \mid n$, czyli k nie jest dzielnikiem n

Proste własności:

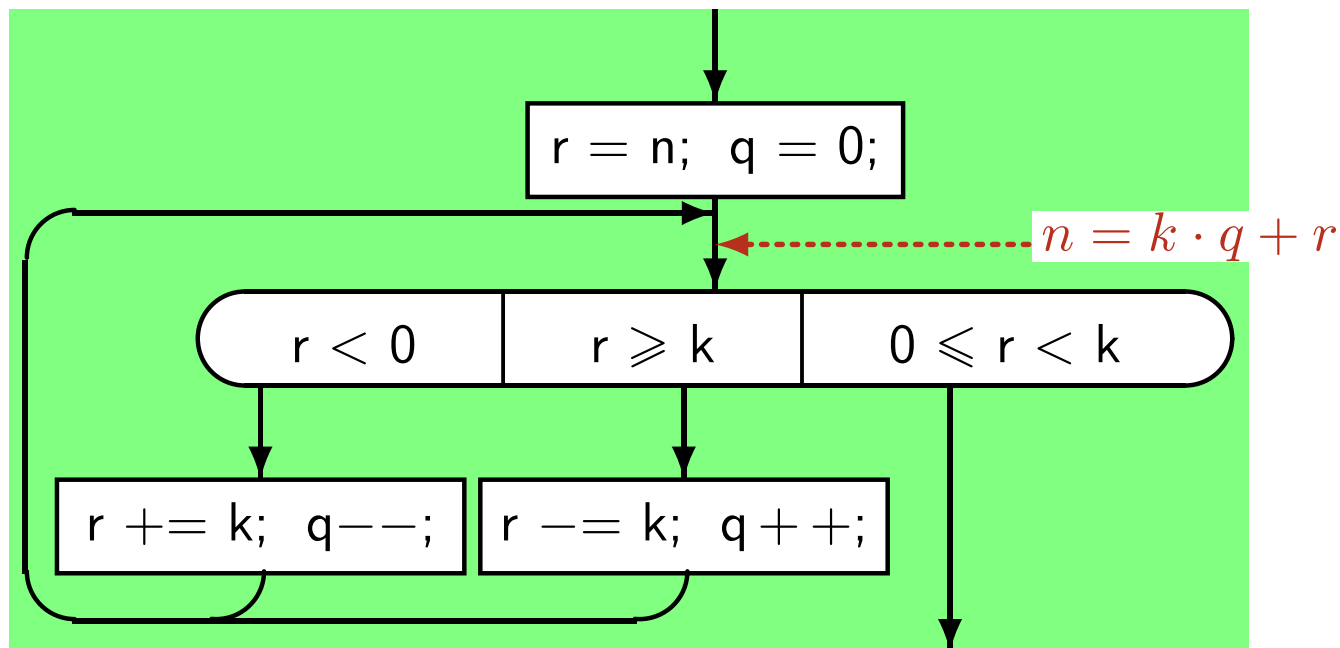
- każda liczba dodatnia k jest dzielnikiem zera
- jeśli $k \mid n$, to $k \mid np$ dla każdego $p \in \mathbb{Z}$
- jeśli $k \mid n$ i $k \mid m$, to $k \mid n + m$
- jeśli $k \mid n$, $n > 0$ i $n \mid m$, to $k \mid m$
- jeśli $n \bmod k = m \bmod k$, to $k \mid n - m$

Dzielenie przez wielokrotne odejmowanie

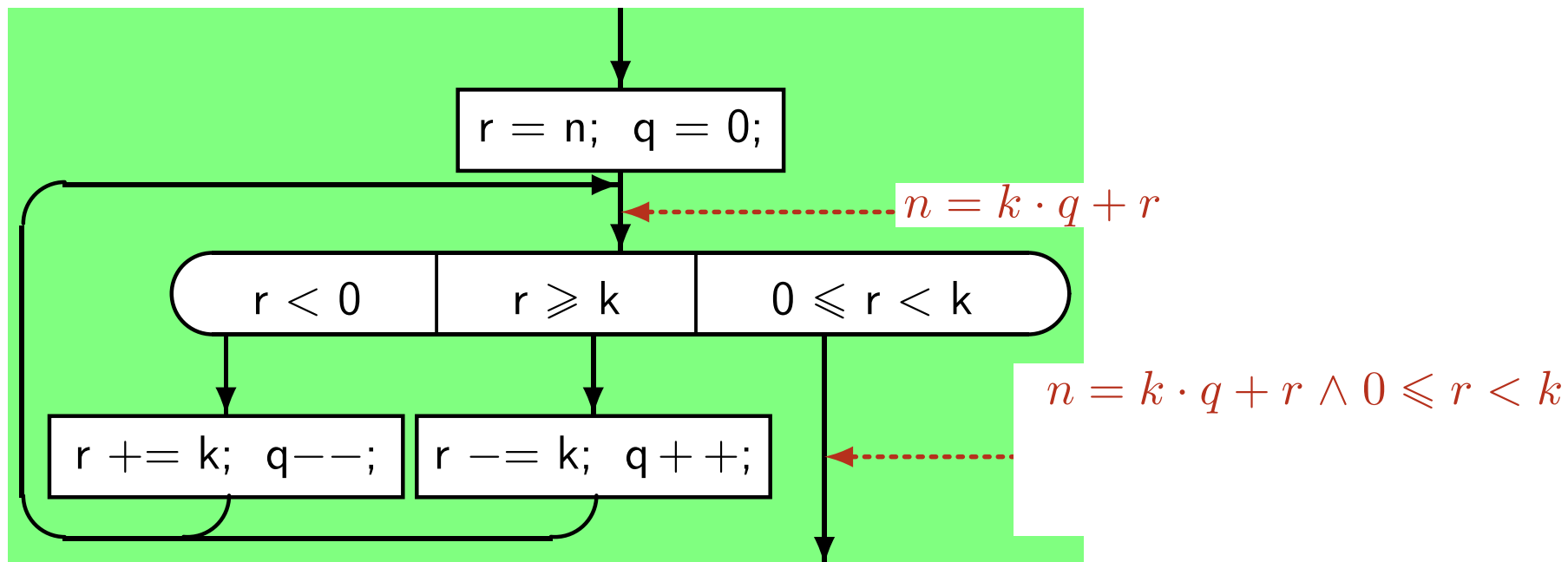
Dzielenie przez wielokrotne odejmowanie



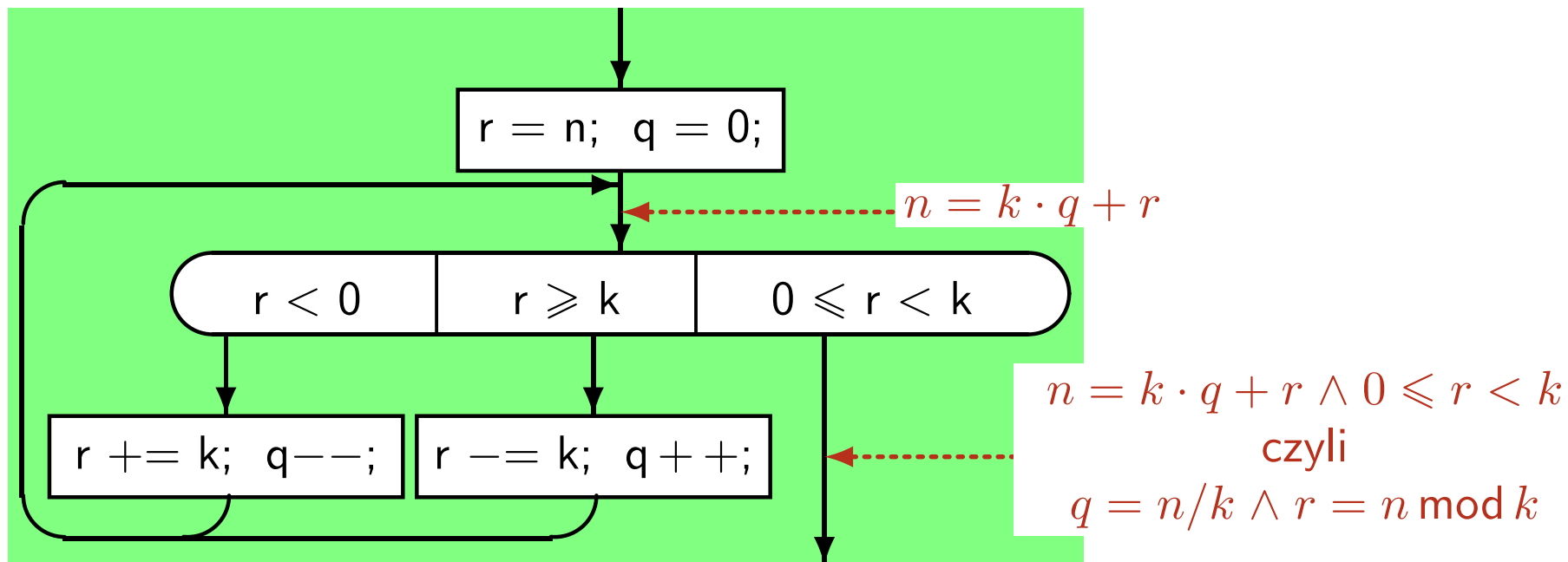
Dzielenie przez wielokrotne odejmowanie



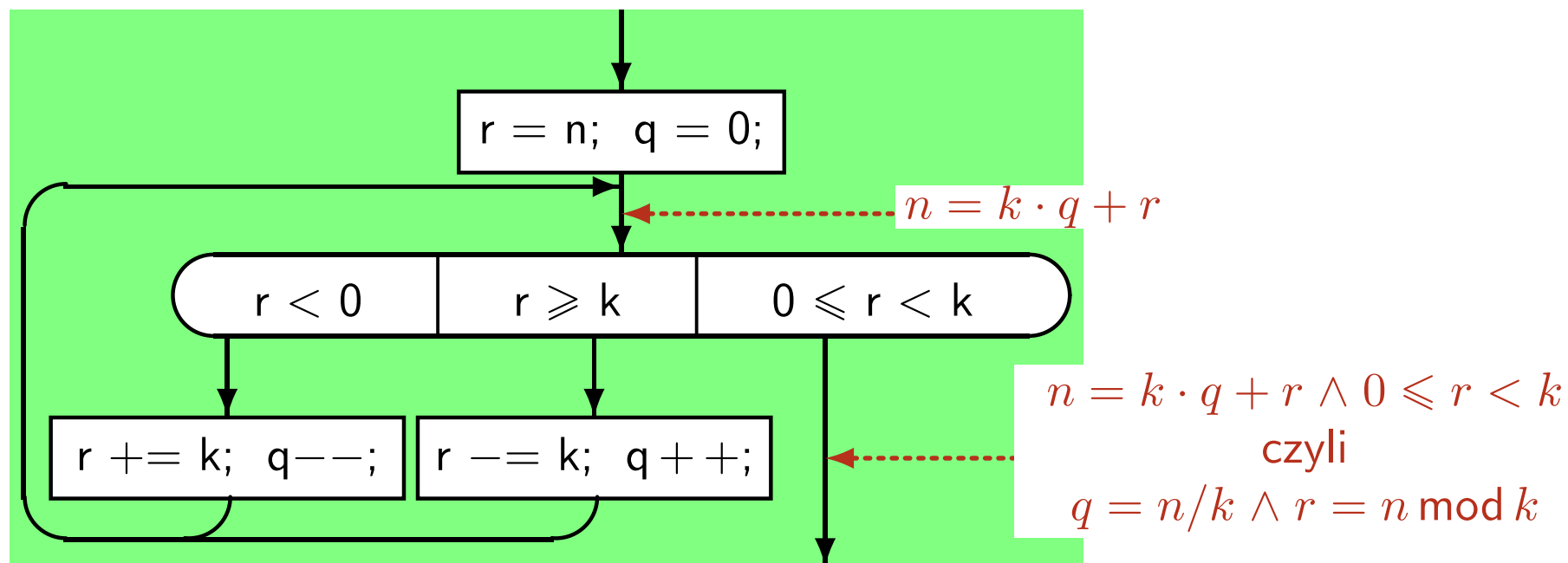
Dzielenie przez wielokrotne odejmowanie



Dzielenie przez wielokrotne odejmowanie



Dzielenie przez wielokrotne odejmowanie



```

r = n;  q = 0;
while (r < 0 || r >= k)
    if (r < 0) { r += k;  q--; }
    else { r -= k;  q++; }

```

Dzielenie „pisemne”

... w systemie dwójkowym

Dzielenie „pisemne”

... w systemie dwójkowym:

1 0 0 1 1 0 : 1 0 1

Dzielenie „pisemne”

... w systemie dwójkowym:



Dzielenie „pisemne”

... w systemie dwójkowym:

$$100110 : 101$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r} 1 \\ 100110 : 101 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r} 1 \\ 100110 : 101 \\ \underline{101} \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

Diagram illustrating binary long division:

$$\begin{array}{r}
 100110 : 101 = 101 \\
 \underline{100} \\
 00110 \\
 \underline{00101} \\
 00011 \\
 \underline{00010} \\
 00010 \\
 \underline{00010} \\
 00000
 \end{array}$$

Annotations:

- dzielnik** (divisor) points to the divisor 101 .
- dzielną koniecznie nieujemną** (dividend must be non-negative) points to the dividend 100110 .

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r}
 1 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001
 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

			1	1					
1	0	0	1	1	0	:	1	0	1
		1	0	1					
		1	0	0	1				

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r}
 11 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 101 \\
 \hline
 0
 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r}
 11 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 101 \\
 \hline
 100
 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r}
 11 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 101 \\
 \hline
 1000
 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r}
 111 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 101 \\
 \hline
 1000
 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

The image shows a handwritten binary division problem on a light gray background. The division is set up as follows:

$$\begin{array}{r}
 111 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 101 \\
 \hline
 1000 \\
 101 \\
 \hline

 \end{array}$$

Annotations with red arrows:

- An arrow points from the text **dzielnik** to the divisor 101 .
- An arrow points from a text box to the dividend 100110 .

The text box contains the following text:

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

$$\begin{array}{r}
 111 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 101 \\
 \hline
 1000 \\
 101 \\
 \hline
 11
 \end{array}$$

dzielnik

dzielna
koniecznie
nieujemna

Dzielenie „pisemne”

... w systemie dwójkowym:

The diagram illustrates the binary long division process. The dividend is 100110 and the divisor is 101. The quotient is 111 and the remainder is 11.

				1	1	1			
1	0	0	1	1	0	:	1	0	1
		1	0	1					
	1	0	0	1					
			1	0	1				
		1	0	0	0				
				1	0	1			
					1	1			

Annotations:

- iloraz** (quotient) points to the result 111.
- dzielnik** (divisor) points to the divisor 101.
- dzielna** (dividend) points to the dividend 100110.
- koniecznie** (necessarily) and **nieujemna** (non-negative) are part of a note indicating that the remainder must be non-negative.
- reszta** (remainder) points to the final remainder 11.

Dzielenie „pisemne”

... w systemie dwójkowym:

Diagram illustrating binary long division (Dzielenie „pisemne” w systemie dwójkowym):

$$\begin{array}{r}
 111 \\
 100110 : 101 \\
 \underline{100} \\
 101 \\
 \underline{101} \\
 000 \\
 101 \\
 \underline{101} \\
 000 \\
 101 \\
 \underline{101} \\
 11
 \end{array}$$

Annotations:

- iloraz** (quotient) points to the result 111 .
- dzielnik** (divisor) points to the divisor 101 .
- reszta** (remainder) points to the final remainder 11 .
- A note states: **dzielna koniecznie nieujemna** (dividend must be non-negative).

- tak liczą komputery

Dzielenie „pisemne”

... w systemie dwójkowym:

The diagram illustrates the binary long division process. It shows the dividend 100110, the divisor 101, and the quotient 111. The process involves subtracting the divisor from the dividend in steps, with the final remainder being 11. Annotations include 'iloraz' (quotient) pointing to the result, 'dzielnik' (divisor) pointing to 101, and 'reszta' (remainder) pointing to 11. A note states 'dzielna koniecznie nieujemna' (dividend must be non-negative).

$$\begin{array}{r}
 111 \\
 \hline
 100110 : 101 \\
 101 \\
 \hline
 1001 \\
 011 \\
 \hline
 0000 \\
 011 \\
 \hline
 11
 \end{array}$$

iloraz

dzielnik

dzielna
koniecznie
nieujemna

reszta

- tak liczą komputery
- znacznie szybsze niż wielokrotne odejmowanie

Dzielenie „pisemne”

... w systemie dwójkowym:

The diagram illustrates the binary long division process. It shows the dividend 100110, the divisor 101, and the resulting quotient 111. The remainder is 11. The process involves subtracting the divisor from the dividend in a series of steps, with the quotient being built up as the process continues. The remainder is the final result of the division.

				1	1	1			
1	0	0	1	1	0	:	1	0	1
		1	0	1					
	1	0	0	1					
			1	0	1				
		1	0	0	0				
				1	0	1			
					1	1			

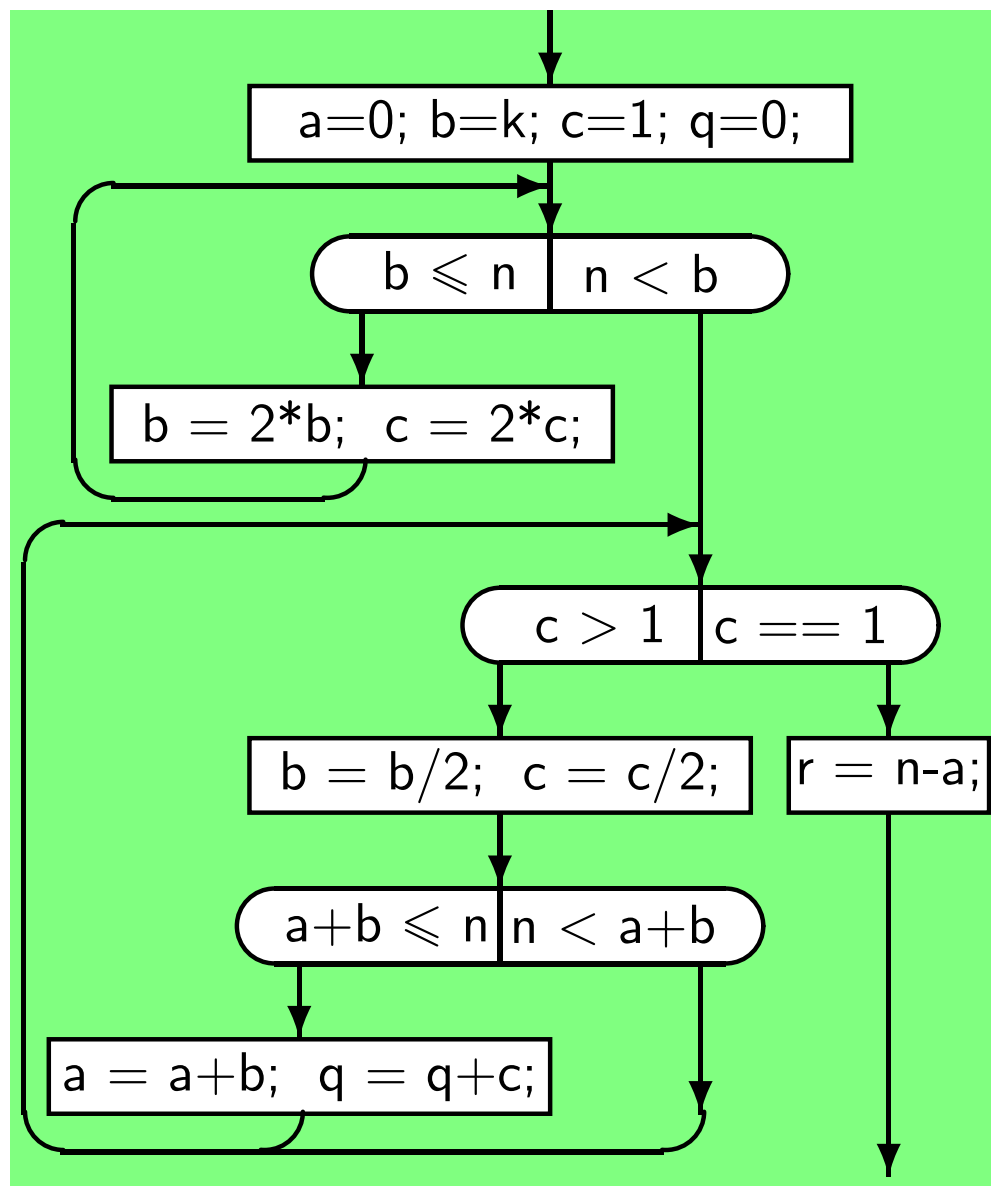
Labels and arrows:

- iloraz** (quotient) points to the top row of the quotient (1 1 1).
- dzielnik** (divisor) points to the divisor (1 0 1).
- reszta** (remainder) points to the final remainder (1 1).
- dzielna koniecznie nieujemna** (dividend must be non-negative) points to the dividend (1 0 0 1 1 0).

- tak liczą komputery
- znacznie szybsze niż wielokrotne odejmowanie
- trudniejsze do zaprogramowania i przekonania się o poprawności

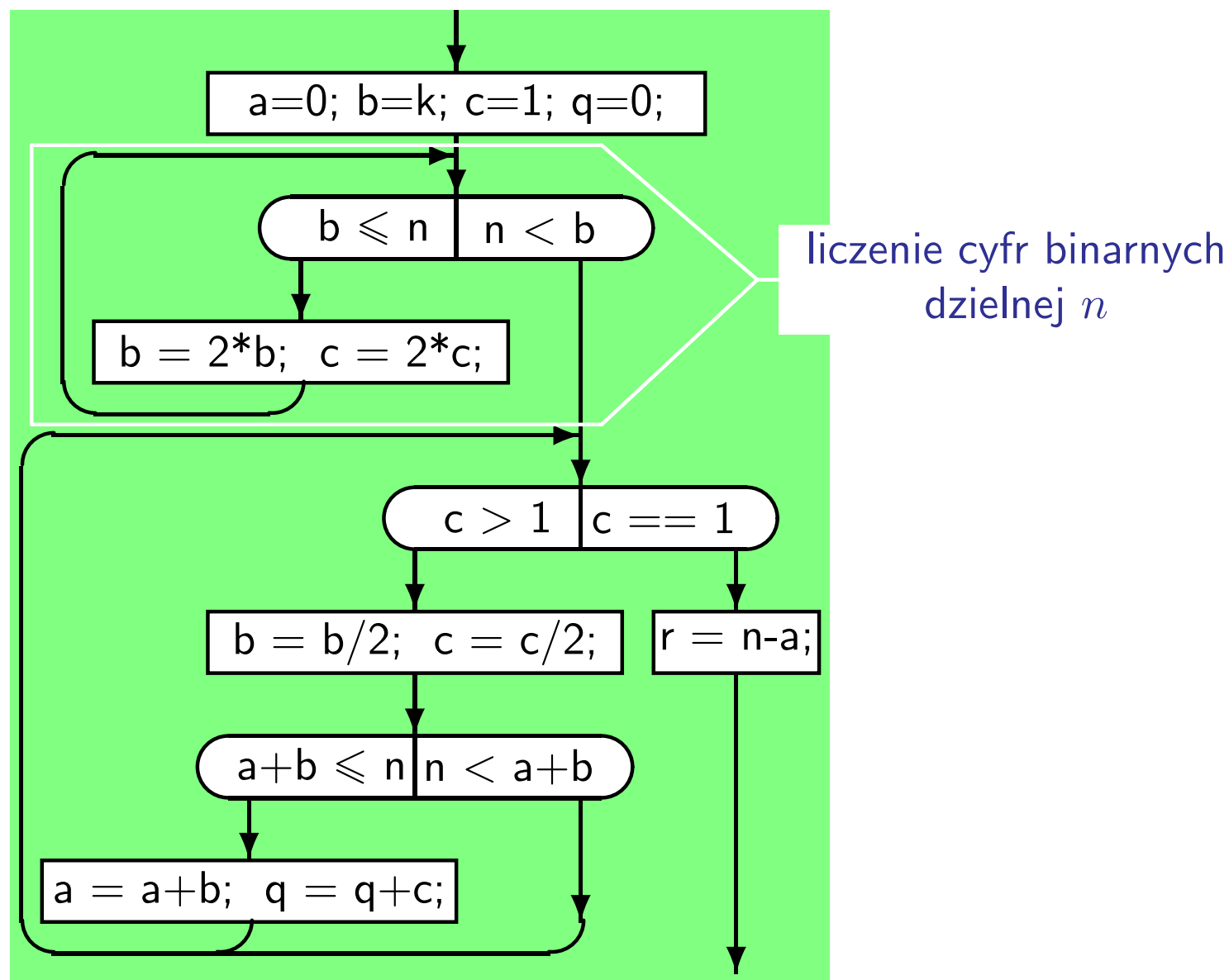
Dzielenie „pisemne”

... w systemie dwójkowym:



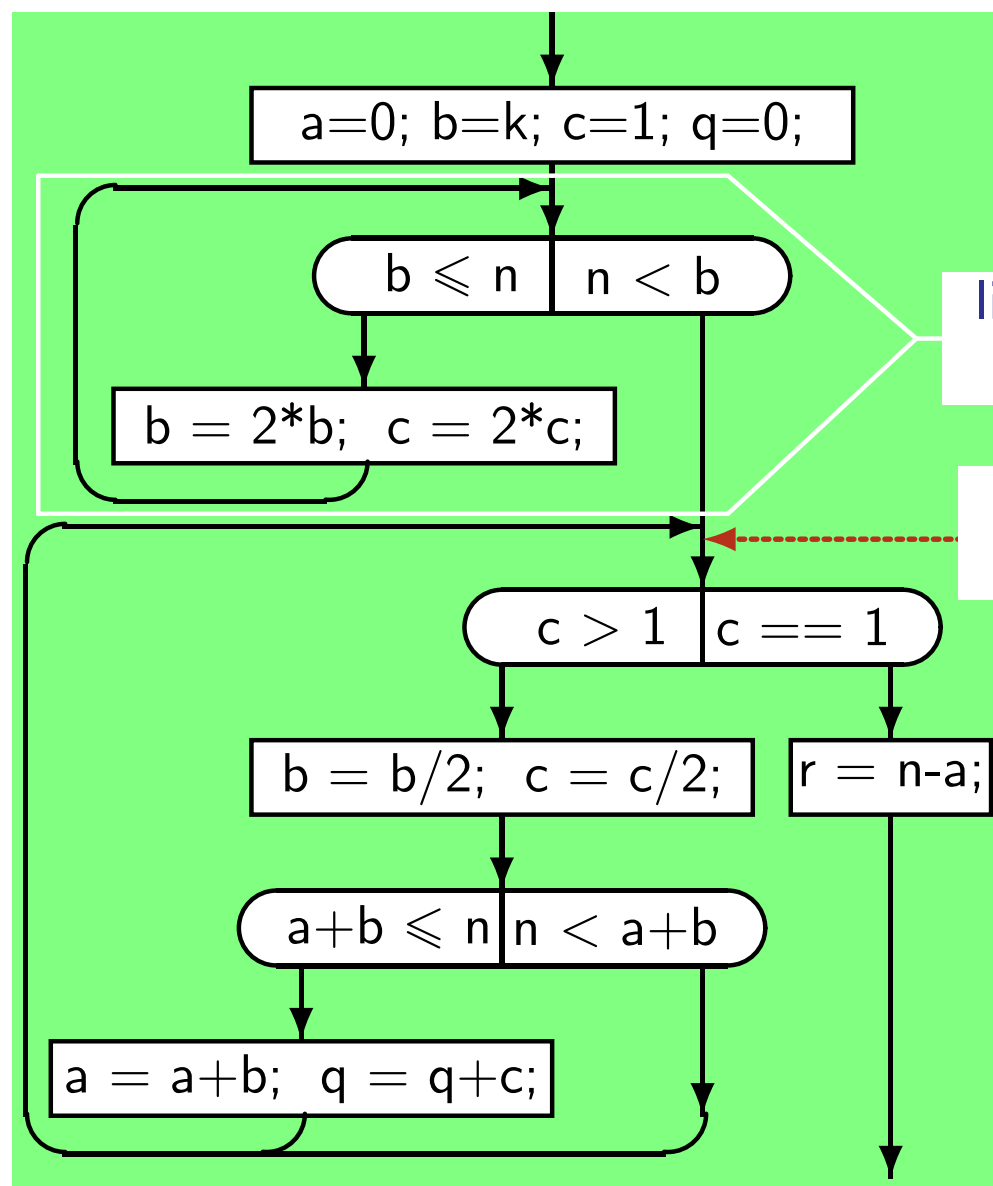
Dzielenie „pisemne”

... w systemie dwójkowym:



Dzielenie „pisemne”

... w systemie dwójkowym:

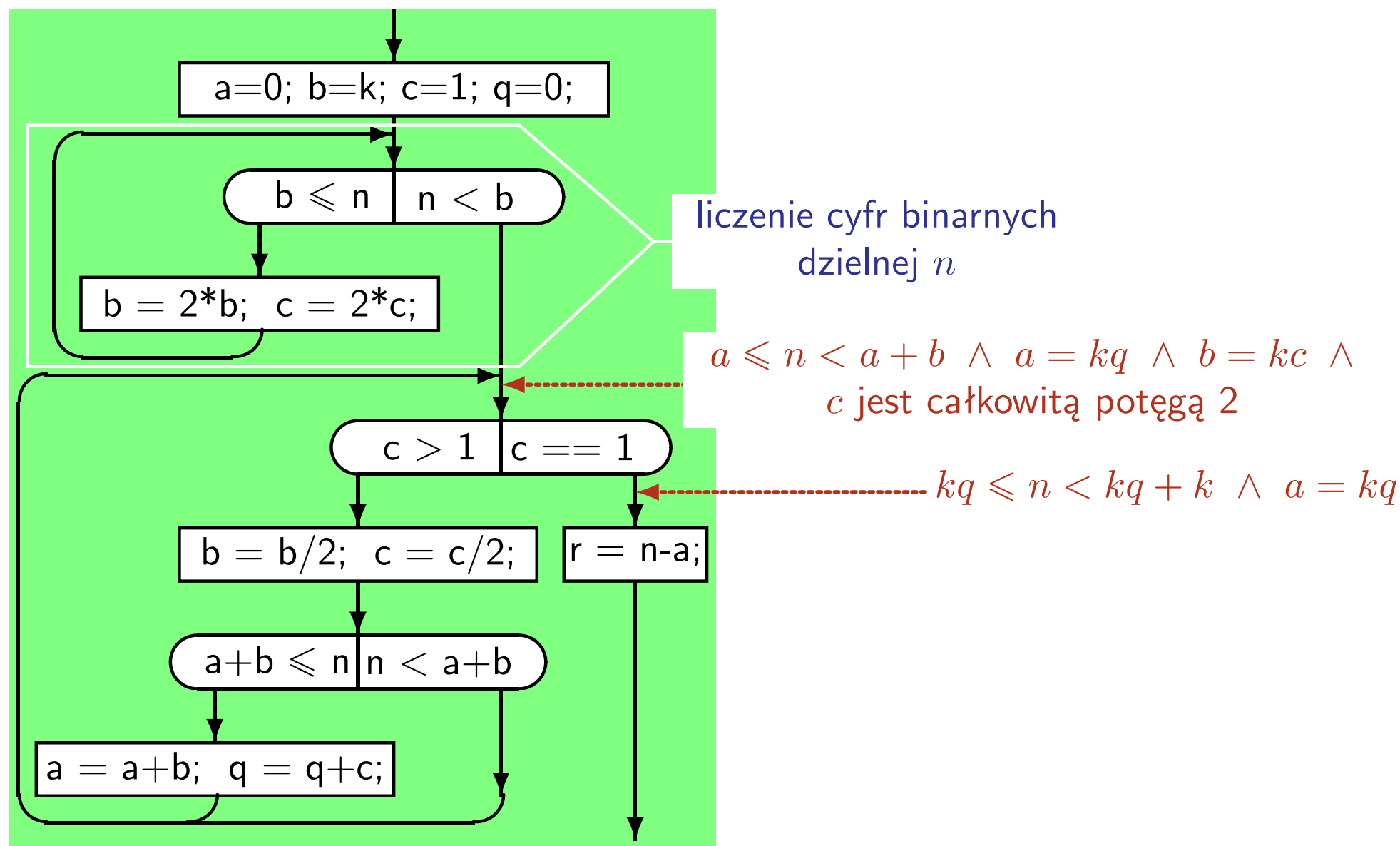


liczenie cyfr binarnych
dzielnej n

$a \leq n < a + b \wedge a = kq \wedge b = kc \wedge$
 c jest całkowitą potęgą 2

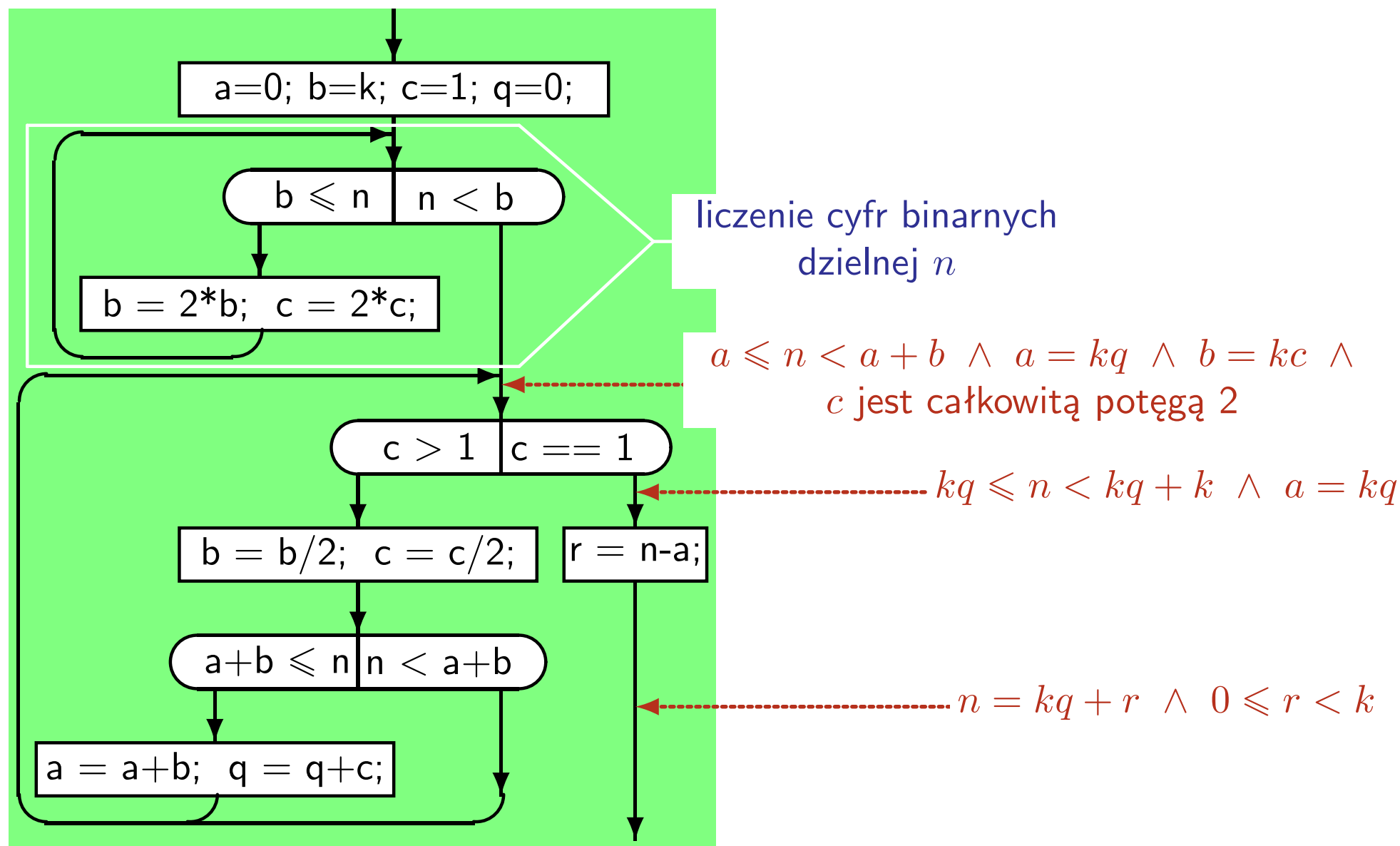
Dzielenie „pisemne”

... w systemie dwójkowym:



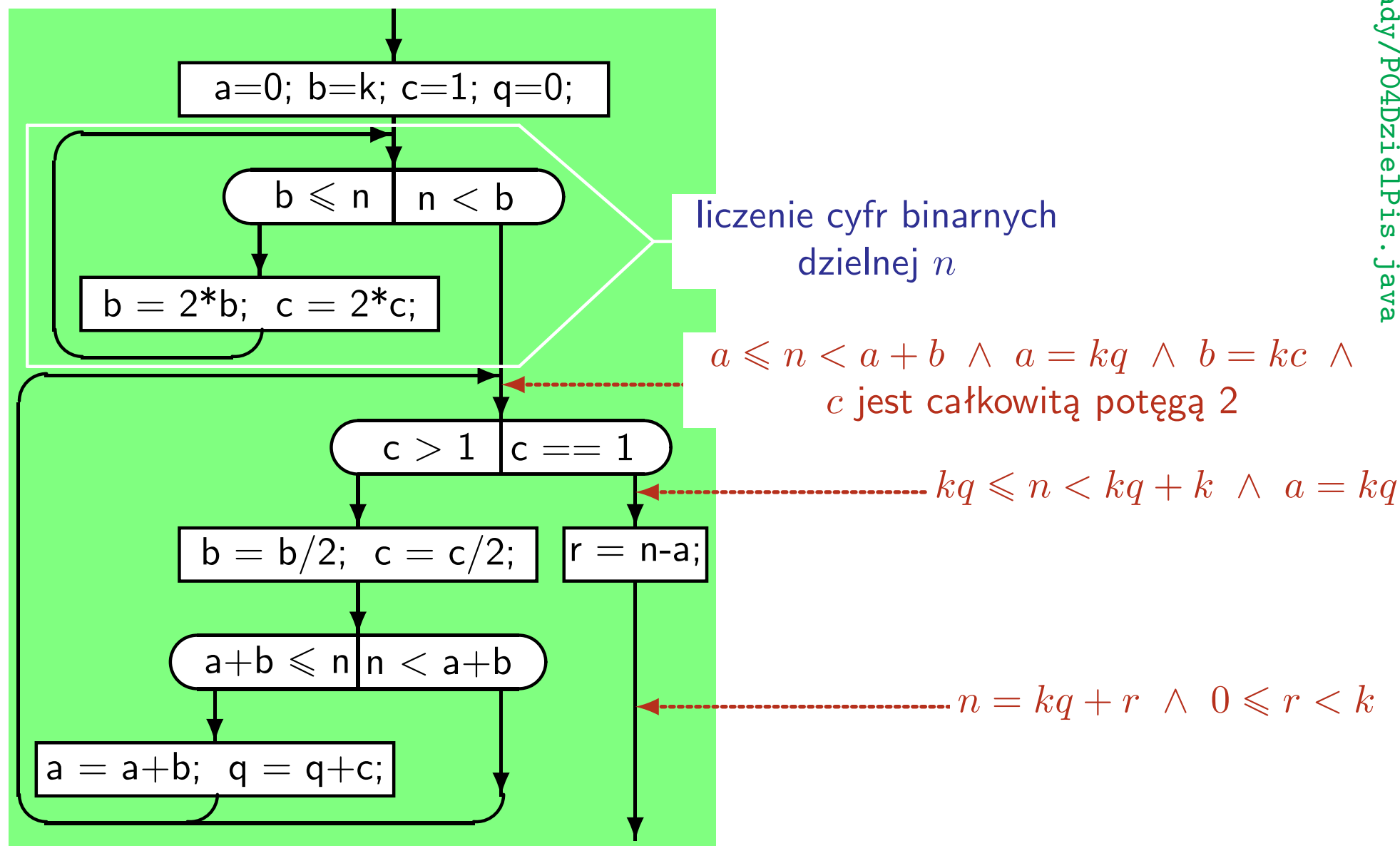
Dzielenie „pisemne”

... w systemie dwójkowym:



Dzielenie „pisemne”

... w systemie dwójkowym:



Podzielność

A co z dzieleniem liczb ujemnych?

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa.

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Więc ilorazem jest $-(q + 1)$, a reszta wynosi $k - r$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Więc ilorazem jest $-(q + 1)$, a reszta wynosi $k - r$, przy tym (tak jak potrzebujemy) $0 < k - r < k$.

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Więc ilorazem jest $-(q + 1)$, a reszta wynosi $k - r$, przy tym (tak jak potrzebujemy) $0 < k - r < k$.

Przykład:

$$n = -13$$

$$k = 5$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Więc ilorazem jest $-(q + 1)$, a reszta wynosi $k - r$, przy tym (tak jak potrzebujemy) $0 < k - r < k$.

Przykład:

$$n = -13$$

$$k = 5$$

wtedy

$$13/5 = 2$$

$$13 \bmod 5 = 3$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Więc ilorazem jest $-(q + 1)$, a reszta wynosi $k - r$, przy tym (tak jak potrzebujemy) $0 < k - r < k$.

Przykład:

$$\begin{aligned} n &= -13 \\ k &= 5 \end{aligned}$$

wtedy

$$\begin{aligned} 13/5 &= 2 \\ 13 \bmod 5 &= 3 \end{aligned}$$

więc

$$\begin{aligned} (-13)/5 &= -(13/5 + 1) = -3 \\ (-13) \bmod 5 &= 5 - 3 = 2 \end{aligned}$$

Podzielność

A co z dzieleniem liczb ujemnych?

Niech $n < 0$ i $k > 0$. Wtedy $-n > 0$ i potrafimy policzyć iloraz i resztę:

$$-n = k \cdot q + r \wedge 0 \leq r < k$$

więc

$$n = k \cdot (-q) - r$$

Jeśli $r = 0$, to $n = k \cdot (-q)$ i ilorazem jest $-q$, a reszta jest zerowa. Jeśli $0 < r < k$, to

$$n = k \cdot (-q) - r = k \cdot (-(q + 1)) + (k - r)$$

Więc ilorazem jest $-(q + 1)$, a reszta wynosi $k - r$, przy tym (tak jak potrzebujemy) $0 < k - r < k$.

Przykład:

$$\begin{array}{llll} n = -13 & & 13/5 = 2 & \\ k = 5 & \text{wtedy} & 13 \bmod 5 = 3 & \text{więc} \end{array} \quad \begin{array}{l} (-13)/5 = -(13/5 + 1) = -3 \\ (-13) \bmod 5 = 5 - 3 = 2 \end{array}$$

— podzielić przeciwną liczbę dodatnią i wynik poprawić j.w.

Liczenie reszty w życiu codziennym

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Kalkulator: $173521 / 2025 = 85.689\,382\,72\dots$

iloraz
rzeczywisty

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Kalkulator: $173521 / 2025 = 85.689\,382\,72\dots$

iloraz
rzeczywisty

Zaokrąglenie: $173521 / 2025 = 85$

iloraz
całkowity

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Kalkulator: $173521 / 2025 = 85.689\,382\,72\dots$

iloraz
rzeczywisty

Zaokrąglenie: $173521 / 2025 = 85$

iloraz
całkowity

Obliczenie reszty: ponieważ $n = (n/k) \cdot k + n \bmod k$, więc
$$n \bmod k = n - (n/k) \cdot k$$

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Kalkulator: $173521 / 2025 = 85.689\,382\,72\dots$

iloraz
rzeczywisty

Zaokrąglenie: $173521 / 2025 = 85$

iloraz
całkowity

Obliczenie reszty: ponieważ $n = (n/k) \cdot k + n \bmod k$, więc

$$\begin{aligned} n \bmod k &= n - (n/k) \cdot k \\ &= 173521 - 85 \cdot 2025 \end{aligned}$$

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Kalkulator: $173521 / 2025 = 85.689\,382\,72\dots$

iloraz
rzeczywisty

Zaokrąglenie: $173521 / 2025 = 85$

iloraz
całkowity

Obliczenie reszty: ponieważ $n = (n/k) \cdot k + n \bmod k$, więc

$$\begin{aligned} n \bmod k &= n - (n/k) \cdot k \\ &= 173521 - 85 \cdot 2025 \\ &= 173521 - 172125 \end{aligned}$$

Liczenie reszty w życiu codziennym

Przykład:

Jak policzyć resztę z dzielenia liczby 173521 przez liczbę 2025, jeśli **nie ma** na kalkulatorze działania `mod` ?

Kalkulator: $173521 / 2025 = 85.689\,382\,72\dots$

iloraz
rzeczywisty

Zaokrąglenie: $173521 / 2025 = 85$

iloraz
całkowity

Obliczenie reszty: ponieważ $n = (n/k) \cdot k + n \bmod k$, więc

$$\begin{aligned} n \bmod k &= n - (n/k) \cdot k \\ &= 173521 - 85 \cdot 2025 \\ &= 173521 - 172125 \\ &= 1396 \end{aligned}$$

Największy wspólny dzielnik

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16)$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16) = \text{nwd}(12, -16)$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16) = \text{nwd}(12, -16) = \text{nwd}(-12, -16)$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16) = \text{nwd}(12, -16) = \text{nwd}(-12, -16) = 4$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16) = \text{nwd}(12, -16) = \text{nwd}(-12, -16) = 4$
- jeśli $a \neq 0$, to $\text{nwd}(a, 0) = |a|$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16) = \text{nwd}(12, -16) = \text{nwd}(-12, -16) = 4$
- jeśli $a \neq 0$, to $\text{nwd}(a, 0) = |a|$
- jeśli $a \neq 0$, to $\text{nwd}(ba, a) = |a|$

Największy wspólny dzielnik

Definicja:

Niech $a, b \in \mathbb{Z}$, przynajmniej jedna z nich różna od zera. Wtedy

- **wspólny dzielnik** liczb a i b to każda taka liczba $d \in \mathbb{N}$, że $d \mid a \wedge d \mid b$
- **największy wspólny dzielnik** liczb a i b to największa liczba wśród ich wspólnych dzielników.

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

Przykłady:

- $\text{nwd}(12, 16) = \text{nwd}(-12, 16) = \text{nwd}(12, -16) = \text{nwd}(-12, -16) = 4$
- jeśli $a \neq 0$, to $\text{nwd}(a, 0) = |a|$
- jeśli $a \neq 0$, to $\text{nwd}(ba, a) = |a|$
- $\text{nwd}(0, 0)$ nie istnieje

Algorytm Euklidesa (do liczenia *nwd*)

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$\text{nwd}(315, 270)$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\text{nwd}(315, 270) = \text{nwd}(270, 315 \bmod 270)$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\text{nwd}(315, 270) = \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45)$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\text{nwd}(1365, 1122) = \text{nwd}(1122, 1365 \bmod 1122)$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
 więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned} \text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45 \end{aligned}$$

$$\begin{aligned} \text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36) = \text{nwd}(36, 21) \\ &= \text{nwd}(21, 36 \bmod 21) \end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36) = \text{nwd}(36, 21) \\ &= \text{nwd}(21, 36 \bmod 21) = \text{nwd}(21, 15) \\ &= \text{nwd}(15, 21 \bmod 15)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
 więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned} \text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45 \end{aligned}$$

$$\begin{aligned} \text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36) = \text{nwd}(36, 21) \\ &= \text{nwd}(21, 36 \bmod 21) = \text{nwd}(21, 15) \\ &= \text{nwd}(15, 21 \bmod 15) = \text{nwd}(15, 6) \\ &= \text{nwd}(6, 15 \bmod 6) \end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
 więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned} \text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45 \end{aligned}$$

$$\begin{aligned} \text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36) = \text{nwd}(36, 21) \\ &= \text{nwd}(21, 36 \bmod 21) = \text{nwd}(21, 15) \\ &= \text{nwd}(15, 21 \bmod 15) = \text{nwd}(15, 6) \\ &= \text{nwd}(6, 15 \bmod 6) = \text{nwd}(6, 3) \end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned}\text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45\end{aligned}$$

$$\begin{aligned}\text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36) = \text{nwd}(36, 21) \\ &= \text{nwd}(21, 36 \bmod 21) = \text{nwd}(21, 15) \\ &= \text{nwd}(15, 21 \bmod 15) = \text{nwd}(15, 6) \\ &= \text{nwd}(6, 15 \bmod 6) = \text{nwd}(6, 3) = \text{nwd}(3, 0)\end{aligned}$$

Algorytm Euklidesa (do liczenia nwd)

Założmy, że $n = kq + r$:

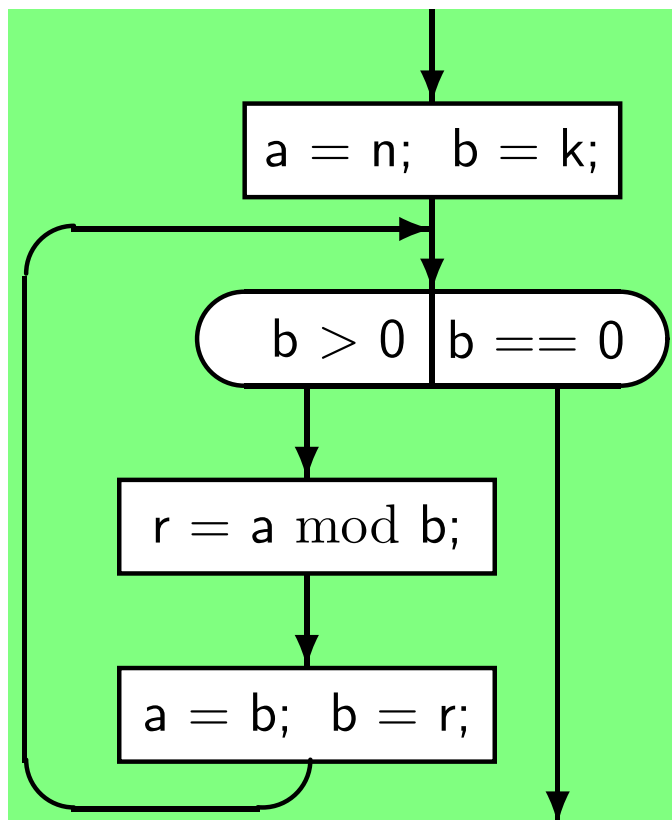
- jeśli $d \mid n$ i $d \mid k$, to $d \mid r$
- jeśli $d \mid r$ i $d \mid k$, to $d \mid n$

Więc zbiór wspólnych dzielników n i k = zbiór wspólnych dzielników r i k
 więc $\text{nwd}(n, k) = \text{nwd}(n \bmod k, k)$

$$\begin{aligned} \text{nwd}(315, 270) &= \text{nwd}(270, 315 \bmod 270) = \text{nwd}(270, 45) \\ &= \text{nwd}(45, 270 \bmod 45) = \text{nwd}(45, 0) \\ &= 45 \end{aligned}$$

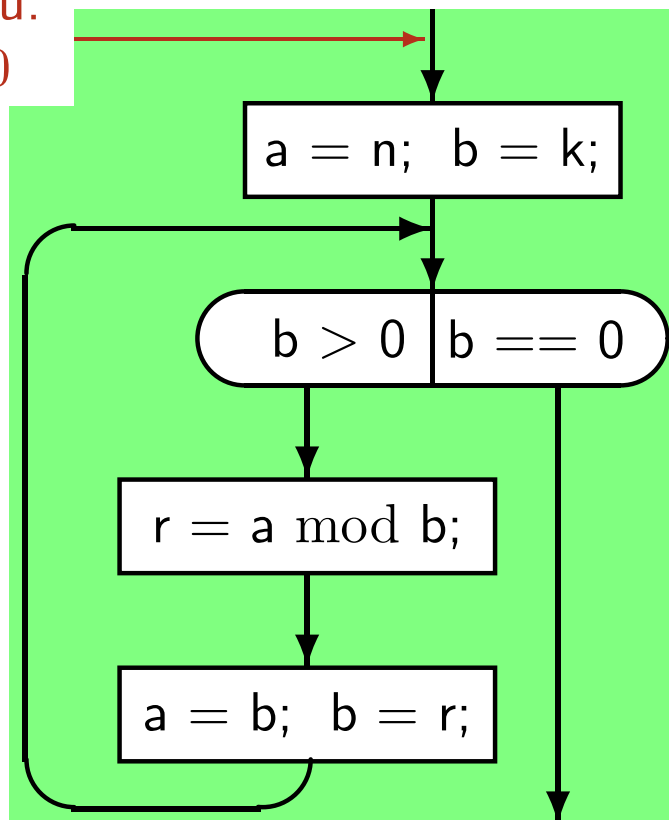
$$\begin{aligned} \text{nwd}(1365, 1122) &= \text{nwd}(1122, 1365 \bmod 1122) = \text{nwd}(1122, 243) \\ &= \text{nwd}(243, 1122 \bmod 243) = \text{nwd}(243, 150) \\ &= \text{nwd}(150, 243 \bmod 150) = \text{nwd}(150, 93) \\ &= \text{nwd}(93, 150 \bmod 93) = \text{nwd}(93, 57) \\ &= \text{nwd}(57, 93 \bmod 57) = \text{nwd}(57, 36) \\ &= \text{nwd}(36, 57 \bmod 36) = \text{nwd}(36, 21) \\ &= \text{nwd}(21, 36 \bmod 21) = \text{nwd}(21, 15) \\ &= \text{nwd}(15, 21 \bmod 15) = \text{nwd}(15, 6) \\ &= \text{nwd}(6, 15 \bmod 6) = \text{nwd}(6, 3) = \text{nwd}(3, 0) \\ &= 3 \end{aligned}$$

Algorytm Euklidesa (do liczenia *nwd*)



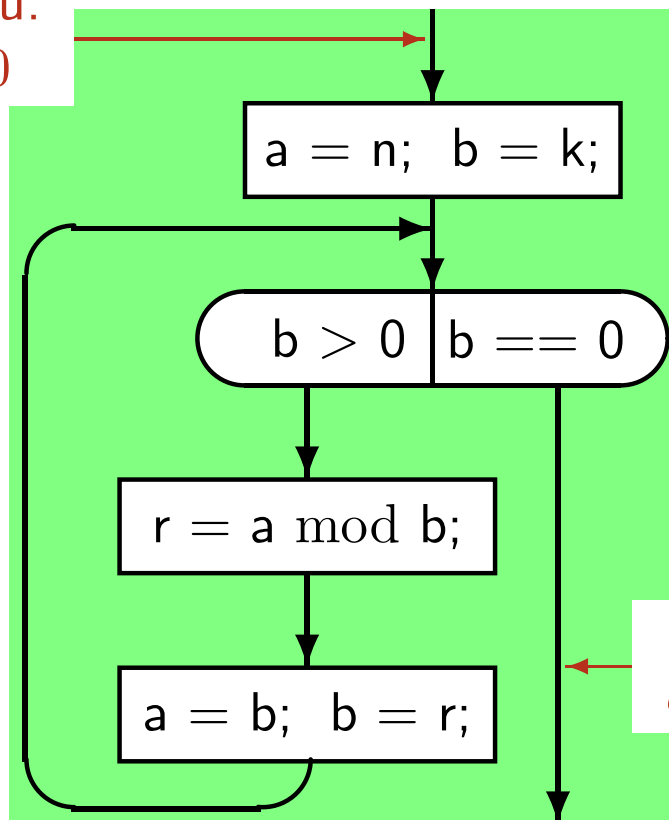
Algorytm Euklidesa (do liczenia *nwd*)

na początku:
 $n \geq k > 0$



Algorytm Euklidesa (do liczenia nwd)

na początku:
 $n \geq k > 0$



teraz:
 $a = \text{nwd}(n, k)$

nwd(a, b) jako kombinacja liniowa a i b

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

Jeśli ta liczba kroków jest zerem, to $\text{nwd}(a, 0) = a = 1 \cdot a + 0 \cdot b$



nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

Jeśli ta liczba kroków jest zerem, to $\text{nwd}(a, 0) = a = 1 \cdot a + 0 \cdot b$

Jeśli żaden z argumentów jeszcze nie jest zerem, to

$$\text{nwd}(a, b) = \text{nwd}(a \bmod b, b)$$

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

Jeśli ta liczba kroków jest zerem, to $\text{nwd}(a, 0) = a = 1 \cdot a + 0 \cdot b$

Jeśli żaden z argumentów jeszcze nie jest zerem, to

$$\text{nwd}(a, b) = \text{nwd}(a \bmod b, b) = \text{nwd}(a - (a/b) \cdot b, b)$$

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

Jeśli ta liczba kroków jest zerem, to $\text{nwd}(a, 0) = a = 1 \cdot a + 0 \cdot b$

Jeśli żaden z argumentów jeszcze nie jest zerem, to

$$\begin{aligned} \text{nwd}(a, b) &= \text{nwd}(a \bmod b, b) = \text{nwd}(a - (a/b) \cdot b, b) \\ &= x' \cdot (a - (a/b) \cdot b) + y' \cdot b \end{aligned}$$

z zał. ind.

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

Jeśli ta liczba kroków jest zerem, to $\text{nwd}(a, 0) = a = 1 \cdot a + 0 \cdot b$

Jeśli żaden z argumentów jeszcze nie jest zerem, to

$$\begin{aligned} \text{nwd}(a, b) &= \text{nwd}(a \bmod b, b) = \text{nwd}(a - (a/b) \cdot b, b) \\ &= x' \cdot (a - (a/b) \cdot b) + y' \cdot b \\ \text{z zał. ind.} \quad &= x' \cdot a + \underbrace{(-x' \cdot (a/b) + y')} \cdot b \end{aligned}$$

nwd(a, b) jako kombinacja liniowa a i b

Twierdzenie:

Jeśli $a, b \in \mathbb{Z}$ i co najmniej jedna z liczb a i b jest różna od zera, to istnieją takie współczynniki $x, y \in \mathbb{Z}$, że

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

Dowód:

Indukcja ze względu na liczbę kroków wykonywanych przez algorytm Euklidesa do momentu, kiedy jeden z argumentów stanie się zerem.

Jeśli ta liczba kroków jest zerem, to $\text{nwd}(a, 0) = a = 1 \cdot a + 0 \cdot b$

Jeśli żaden z argumentów jeszcze nie jest zerem, to

$$\begin{aligned}
 \text{nwd}(a, b) &= \text{nwd}(a \bmod b, b) = \text{nwd}(a - (a/b) \cdot b, b) \\
 &= x' \cdot (a - (a/b) \cdot b) + y' \cdot b \\
 &= \underbrace{x' \cdot a}_{x} + \underbrace{(-x' \cdot (a/b) + y') \cdot b}_y
 \end{aligned}$$

z zał. ind. $\nearrow$



$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$$1200 = 1 \cdot 1200 + 0 \cdot 372 \quad |$$

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$$\begin{array}{rcl} 1200 & = & 1 \cdot 1200 + 0 \cdot 372 \\ 372 & = & 0 \cdot 1200 + 1 \cdot 372 \end{array} \quad \left| \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

$$\begin{array}{rclcl} 1200 & = & 1 \cdot 1200 & + & 0 \cdot 372 \\ 372 & = & 0 \cdot 1200 & + & 1 \cdot 372 \end{array} \quad \left| \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$$\begin{array}{rcll} 1200 & = & 1 \cdot 1200 + 0 \cdot 372 & \\ 372 & = & 0 \cdot 1200 + 1 \cdot 372 & \\ 84 & & & \left| \begin{array}{l} 1200 - 3 \cdot 372 = 84 \end{array} \right. \end{array}$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$$\begin{array}{rcl} 1200 & = & 1 \cdot 1200 + 0 \cdot 372 \\ 372 & = & 0 \cdot 1200 + 1 \cdot 372 \\ 84 & = & 1 \cdot 1200 - 3 \cdot 372 \end{array} \quad \left| \quad 1200 - 3 \cdot 372 = 84 \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$$\begin{array}{rclcl}
 1200 & = & 1 \cdot 1200 + & 0 \cdot 372 & \\
 372 & = & 0 \cdot 1200 + & 1 \cdot 372 & \\
 84 & = & 1 \cdot 1200 - & 3 \cdot 372 & \\
 36 & & & &
 \end{array}
 \left| \begin{array}{l} \\ 1200 - 3 \cdot 372 = 84 \\ 372 - 4 \cdot 84 = 36 \end{array} \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$$\begin{array}{rcl}
 1200 & = & 1 \cdot 1200 + 0 \cdot 372 \\
 372 & = & 0 \cdot 1200 + 1 \cdot 372 \\
 84 & = & 1 \cdot 1200 - 3 \cdot 372 \\
 36 & = & -4 \cdot 1200 + 13 \cdot 372
 \end{array}
 \left| \begin{array}{l} \\ \\ 1200 - 3 \cdot 372 = 84 \\ 372 - 4 \cdot 84 = 36 \end{array} \right.$$

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

$1200 =$	$1 \cdot 1200 +$	$0 \cdot 372$	
$372 =$	$0 \cdot 1200 +$	$1 \cdot 372$	
$84 =$	$1 \cdot 1200 -$	$3 \cdot 372$	$1200 - 3 \cdot 372 = 84$
$36 =$	$-4 \cdot 1200 +$	$13 \cdot 372$	$372 - 4 \cdot 84 = 36$
$12 =$	$9 \cdot 1200 -$	$29 \cdot 372$	$84 - 2 \cdot 36 = 12$

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

1200	$=$	$1 \cdot 1200 + 0 \cdot 372$	
372	$=$	$0 \cdot 1200 + 1 \cdot 372$	
84	$=$	$1 \cdot 1200 - 3 \cdot 372$	$1200 - 3 \cdot 372 = 84$
36	$=$	$-4 \cdot 1200 + 13 \cdot 372$	$372 - 4 \cdot 84 = 36$
12	$=$	$9 \cdot 1200 - 29 \cdot 372$	$84 - 2 \cdot 36 = 12$
0			$36 - 3 \cdot 12 = 0$

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

1200	$=$	$1 \cdot 1200 + 0 \cdot 372$	
372	$=$	$0 \cdot 1200 + 1 \cdot 372$	$1200 - 3 \cdot 372 = 84$
84	$=$	$1 \cdot 1200 - 3 \cdot 372$	$372 - 4 \cdot 84 = 36$
36	$=$	$-4 \cdot 1200 + 13 \cdot 372$	$84 - 2 \cdot 36 = 12$
$\text{nwd}(1200, 372) =$	12	$= 9 \cdot 1200 - 29 \cdot 372$	$36 - 3 \cdot 12 = 0$
	0		

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

Dla danych $a, b \in \mathbb{Z}$ (przynajmniej jedna z nich różna od zera) chcemy wyznaczyć takie $x, y \in \mathbb{Z}$, że

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

Działamy na kombinacjach liniowych liczb a i b .

Przykład: $\text{nwd}(1200, 372) = ? \cdot 1200 + ? \cdot 372$

1200	$=$	$1 \cdot 1200 + 0 \cdot 372$	
372	$=$	$0 \cdot 1200 + 1 \cdot 372$	$1200 - 3 \cdot 372 = 84$
84	$=$	$1 \cdot 1200 - 3 \cdot 372$	$372 - 4 \cdot 84 = 36$
36	$=$	$-4 \cdot 1200 + 13 \cdot 372$	$84 - 2 \cdot 36 = 12$
$\text{nwd}(1200, 372) = 12$	$=$	$9 \cdot 1200 - 29 \cdot 372$	$36 - 3 \cdot 12 = 0$
0			

szukana
kombinacja
liniowa

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

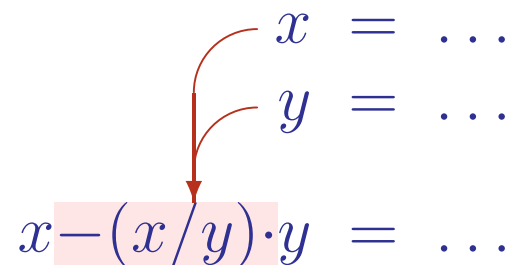
Jak znaleźć współczynniki takiej kombinacji liniowej?

$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

W każdym kroku:

- po lewej stronie równości stosujemy algorytm Euklidesa; t.zn.

$$\begin{array}{l} x = \dots \\ y = \dots \\ x - (x/y) \cdot y = \dots \end{array}$$


$\text{nwd}(a, b)$ jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

W każdym kroku:

- po lewej stronie równości stosujemy algorytm Euklidesa; t.zn.

$$\begin{aligned} x &= \dots \\ y &= \dots \\ x - (x/y) \cdot y &= \dots \end{aligned}$$

- po prawej stronie równości stosujemy **te same** działania na współczynnikach kombinacji liniowej:

$$\begin{aligned} \dots &= v \cdot a \dots \\ \dots &= z \cdot a \dots \\ \dots &= v - (x/y) \cdot z \cdot a \dots \end{aligned}$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

$$x = v \cdot a + w \cdot b$$

$$y = z \cdot a + t \cdot b$$

$$? = ? \cdot a + ? \cdot b$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

$$x = v \cdot a + w \cdot b$$

$$y = z \cdot a + t \cdot b$$

TUTAJ:
reszta z dzielenia

x przez y :

$$x - (x/y) \cdot y$$



$$? = ? \cdot a + ? \cdot b$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

$$x = v \cdot a + w \cdot b$$

$$y = z \cdot a + t \cdot b$$

$$? = ? \cdot a + ? \cdot b$$

TUTAJ:

reszta z dzielenia

x przez y :

$$x - (x/y) \cdot y$$



TUTAJ:

odejmowanie wierszy

z tym samym mnożnikiem:

$$v - (x/y) \cdot z$$

nwd(a, b) jako kombinacja liniowa a i b

Jak znaleźć współczynniki takiej kombinacji liniowej?

TUTAJ:
reszta z dzielenia
 x przez y :
 $x - (x/y) \cdot y$

$$x = v \cdot a + w \cdot b$$

$$y = z \cdot a + t \cdot b$$

$$? = ? \cdot a + ? \cdot b$$

TUTAJ:
odejmowanie wierszy
z tym samym mnożnikiem:
 $v - (x/y) \cdot z$

TUTAJ:
odejmowanie wierszy
z tym samym mnożnikiem:
 $w - (x/y) \cdot t$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\begin{array}{lcl} \textcircled{1} & 1543 & = & 1 \cdot 1543 + & 0 \cdot 188 \\ \textcircled{2} & 188 & = & 0 \cdot 1543 + & 1 \cdot 188 \end{array} \quad \left| \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\begin{array}{lcl} \textcircled{1} & 1543 & = 1 \cdot 1543 + 0 \cdot 188 \\ \textcircled{2} & 188 & = 0 \cdot 1543 + 1 \cdot 188 \end{array} \quad \left| \quad 1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8 \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\begin{array}{lcl}
 \textcircled{1} & 1543 & = 1 \cdot 1543 + 0 \cdot 188 \\
 \textcircled{2} & 188 & = 0 \cdot 1543 + 1 \cdot 188 \\
 \textcircled{3} & 39 & = 1 \cdot 1543 - 8 \cdot 188
 \end{array} \quad \left| \quad 1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8 \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\begin{array}{lcl}
 \textcircled{1} & 1543 = & 1 \cdot 1543 + 0 \cdot 188 \\
 \textcircled{2} & 188 = & 0 \cdot 1543 + 1 \cdot 188 \\
 \textcircled{3} & 39 = & 1 \cdot 1543 - 8 \cdot 188
 \end{array}
 \quad \left| \begin{array}{l}
 1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8 \\
 188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4
 \end{array} \right.$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

①	$1543 =$	$1 \cdot 1543 +$	$0 \cdot 188$	
②	$188 =$	$0 \cdot 1543 +$	$1 \cdot 188$	$1543/188 = 8, \text{ ①} - \text{ ②} \cdot 8$
③	$39 =$	$1 \cdot 1543 -$	$8 \cdot 188$	$188/39 = 4, \text{ ②} - \text{ ③} \cdot 4$
④	$32 =$	$-4 \cdot 1543 +$	$33 \cdot 188$	$39/32 = 1, \text{ ③} - \text{ ④} \cdot 1$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

①	$1543 =$	$1 \cdot 1543 +$	$0 \cdot 188$	
②	$188 =$	$0 \cdot 1543 +$	$1 \cdot 188$	$1543/188 = 8, \text{ ①} - \text{ ②} \cdot 8$
③	$39 =$	$1 \cdot 1543 -$	$8 \cdot 188$	$188/39 = 4, \text{ ②} - \text{ ③} \cdot 4$
④	$32 =$	$-4 \cdot 1543 +$	$33 \cdot 188$	$39/32 = 1, \text{ ③} - \text{ ④} \cdot 1$
⑤	$7 =$	$5 \cdot 1543 -$	$41 \cdot 188$	$32/7 = 4, \text{ ④} - \text{ ⑤} \cdot 4$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$\textcircled{7} \quad 3 = 29 \cdot 1543 - 238 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$\textcircled{7} \quad 3 = 29 \cdot 1543 - 238 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

$$4/3 = 1, \textcircled{6} - \textcircled{7} \cdot 1$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$\textcircled{7} \quad 3 = 29 \cdot 1543 - 238 \cdot 188$$

$$\textcircled{8} \quad 1 = -53 \cdot 1543 + 435 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

$$4/3 = 1, \textcircled{6} - \textcircled{7} \cdot 1$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$\textcircled{7} \quad 3 = 29 \cdot 1543 - 238 \cdot 188$$

$$\textcircled{8} \quad 1 = -53 \cdot 1543 + 435 \cdot 188$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

$$4/3 = 1, \textcircled{6} - \textcircled{7} \cdot 1$$

$$3/1 = 3, \textcircled{7} - \textcircled{8} \cdot 3$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$\textcircled{7} \quad 3 = 29 \cdot 1543 - 238 \cdot 188$$

$$\textcircled{8} \quad 1 = -53 \cdot 1543 + 435 \cdot 188$$

$$\textcircled{9} \quad 0 = \dots\dots\dots$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

$$4/3 = 1, \textcircled{6} - \textcircled{7} \cdot 1$$

$$3/1 = 3, \textcircled{7} - \textcircled{8} \cdot 3$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

$$\textcircled{1} \quad 1543 = 1 \cdot 1543 + 0 \cdot 188$$

$$\textcircled{2} \quad 188 = 0 \cdot 1543 + 1 \cdot 188$$

$$\textcircled{3} \quad 39 = 1 \cdot 1543 - 8 \cdot 188$$

$$\textcircled{4} \quad 32 = -4 \cdot 1543 + 33 \cdot 188$$

$$\textcircled{5} \quad 7 = 5 \cdot 1543 - 41 \cdot 188$$

$$\textcircled{6} \quad 4 = -24 \cdot 1543 + 197 \cdot 188$$

$$\textcircled{7} \quad 3 = 29 \cdot 1543 - 238 \cdot 188$$

$$\textcircled{8} \quad 1 = -53 \cdot 1543 + 435 \cdot 188$$

$$\textcircled{9} \quad 0 = \dots\dots\dots$$

$$1543/188 = 8, \textcircled{1} - \textcircled{2} \cdot 8$$

$$188/39 = 4, \textcircled{2} - \textcircled{3} \cdot 4$$

$$39/32 = 1, \textcircled{3} - \textcircled{4} \cdot 1$$

$$32/7 = 4, \textcircled{4} - \textcircled{5} \cdot 4$$

$$7/4 = 1, \textcircled{5} - \textcircled{6} \cdot 1$$

$$4/3 = 1, \textcircled{6} - \textcircled{7} \cdot 1$$

$$3/1 = 3, \textcircled{7} - \textcircled{8} \cdot 3$$

nwd(a, b) jako kombinacja liniowa a i b

Przykład: $\text{nwd}(1543, 188) = ? \cdot 1543 + ? \cdot 188$

①	$1543 = 1 \cdot 1543 + 0 \cdot 188$	
②	$188 = 0 \cdot 1543 + 1 \cdot 188$	$1543/188 = 8, \text{ ①} - \text{ ②} \cdot 8$
③	$39 = 1 \cdot 1543 - 8 \cdot 188$	$188/39 = 4, \text{ ②} - \text{ ③} \cdot 4$
④	$32 = -4 \cdot 1543 + 33 \cdot 188$	$39/32 = 1, \text{ ③} - \text{ ④} \cdot 1$
⑤	$7 = 5 \cdot 1543 - 41 \cdot 188$	$32/7 = 4, \text{ ④} - \text{ ⑤} \cdot 4$
⑥	$4 = -24 \cdot 1543 + 197 \cdot 188$	$7/4 = 1, \text{ ⑤} - \text{ ⑥} \cdot 1$
⑦	$3 = 29 \cdot 1543 - 238 \cdot 188$	$4/3 = 1, \text{ ⑥} - \text{ ⑦} \cdot 1$
⑧	$1 = -53 \cdot 1543 + 435 \cdot 188$	$3/1 = 3, \text{ ⑦} - \text{ ⑧} \cdot 3$
⑨	$0 = \dots\dots\dots$	

więc $\text{nwd}(1543, 188) = -53 \cdot 1543 + 435 \cdot 188$

Waga szalkowa



Jak odważyć 100 g towaru, kiedy dysponujemy tylko odważnikami 500 g i 200 g?

Waga szalkowa



Jak odważyć 100 g towaru, kiedy dysponujemy tylko odważnikami 500 g i 200 g?

$$\text{nwd}(500, 200) = 100 = 1 \cdot 500 - 2 \cdot 200$$

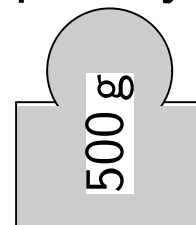
Waga szalkowa



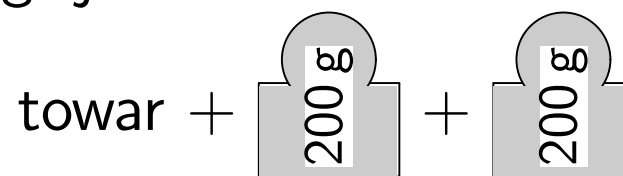
Jak odważyć 100 g towaru, kiedy dysponujemy tylko odważnikami 500 g i 200 g?

$$\text{nwd}(500, 200) = 100 = 1 \cdot 500 - 2 \cdot 200$$

Na jednej szalce położyć



a na drugiej



towar +

+

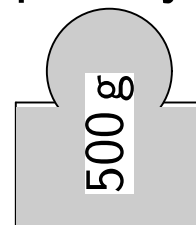
Waga szalkowa



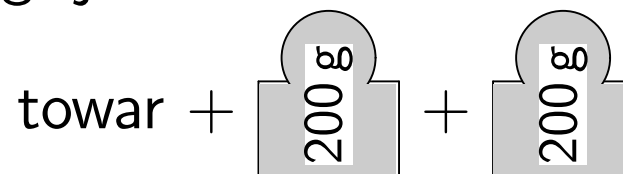
Jak odważyć 100 g towaru, kiedy dysponujemy tylko odważnikami 500 g i 200 g?

$$\text{nwd}(500, 200) = 100 = 1 \cdot 500 - 2 \cdot 200$$

Na jednej szalce położyć



a na drugiej



Odważnikami a -gramowymi i b -gramowymi można odważyć c gramów towaru $\iff \text{nwd}(a, b) \mid c$, czyli c jest wielokrotnością $\text{nwd}(a, b)$

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

— czyli wtedy, gdy nie mają wspólnych dzielników większych od 1

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

- czyli wtedy, gdy nie mają wspólnych dzielników większych od 1
- czyli wtedy, gdy $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

- czyli wtedy, gdy nie mają wspólnych dzielników większych od 1
- czyli wtedy, gdy $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$

Przykłady:

Liczby 65 i 77 są względnie pierwsze, bo $32 \cdot 65 - 27 \cdot 77 = 1$.

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

— czyli wtedy, gdy nie mają wspólnych dzielników większych od 1

— czyli wtedy, gdy $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$

Przykłady:

Liczby 65 i 77 są względnie pierwsze, bo $32 \cdot 65 - 27 \cdot 77 = 1$.

Liczby 66 i 78 nie są względnie pierwsze, bo $\text{nwd}(66, 78) = 6$.

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

— czyli wtedy, gdy nie mają wspólnych dzielników większych od 1

— czyli wtedy, gdy $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$

Przykłady:

Liczby 65 i 77 są względnie pierwsze, bo $32 \cdot 65 - 27 \cdot 77 = 1$.

Liczby 66 i 78 nie są względnie pierwsze, bo $\text{nwd}(66, 78) = 6$.

Fakt:

Każde dwie różne liczby pierwsze są względnie pierwsze.

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

— czyli wtedy, gdy nie mają wspólnych dzielników większych od 1

— czyli wtedy, gdy $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$

Przykłady:

Liczby 65 i 77 są względnie pierwsze, bo $32 \cdot 65 - 27 \cdot 77 = 1$.

Liczby 66 i 78 nie są względnie pierwsze, bo $\text{nwd}(66, 78) = 6$.

Fakt:

Każde dwie różne liczby pierwsze są względnie pierwsze.

Wniosek:

Samymi monetami po 7 zł i 11 zł można zapłacić dowolną całkowitą kwotę — o ile obie strony transakcji mają ich wystarczająco dużo.

Liczby względnie pierwsze

Definicja:

Dwie liczby całkowite a i b są względnie pierwsze $\iff \text{nwd}(a, b) = 1$.

— czyli wtedy, gdy nie mają wspólnych dzielników większych od 1

— czyli wtedy, gdy $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$

Przykłady:

Liczby 65 i 77 są względnie pierwsze, bo $32 \cdot 65 - 27 \cdot 77 = 1$.

Liczby 66 i 78 nie są względnie pierwsze, bo $\text{nwd}(66, 78) = 6$.

Fakt:

Każde dwie różne liczby pierwsze są względnie pierwsze.

Wniosek:

Samymi monetami po 7 zł i 11 zł można zapłacić dowolną całkowitą kwotę — o ile obie strony transakcji mają ich wystarczająco dużo.

— ponieważ $2 \cdot 11 - 3 \cdot 7 = 1$, więc jeśli trzeba zapłacić n zł, to:

$$2n \cdot 11 - 3n \cdot 7 = n$$

należy dać $2n$ monet po 11 zł i dostać reszty $3n$ monet po 7 zł.

Równania diofantyczne

Równania diofantyczne

Diofantos z Aleksandrii (III w. n.e.)



Równania diofantyczne

Diofantos z Aleksandrii (III w. n.e.)

Epitafium na jego grobie w tłumaczeniu na łacinę:

Hunc Diophantus habet tumulum, qui tempora vitae illius, mira denotat arte tibi. Egit sextantem juvenis; lanugine malas vestire hinc coepit parte duodecima. Septante uxori post haec sociatur; et anno formosus quinto nascitur inde puer. Semissem aetatis postquam attigit ille paternae, infelix subita morte peremptus obit. Quattuor aestates genitor lugere superstes cogitur. Hinc annos illius assequere.



Równania diofantyczne

Diofantos z Aleksandrii (III w. n.e.)

Epitafium na jego grobie w tłumaczeniu na łacinę:

Hunc Diophantus habet tumulum, qui tempora vitae illius, mira denotat arte tibi. Egit sextantem juvenis; lanugine malas vestire hinc coepit parte duodecima. Septante uxori post haec sociatur; et anno formosus quinto nascitur inde puer. Semissem aetatis postquam attigit ille paternae, infelix subita morte peremptus obit. Quattuor aestates genitor lugere superstes cogitur. Hinc annos illius assequere.



Żeby dowiedzieć się, ile lat przeżył Diofantos, trzeba

- znać łacinę

Równania diofantyczne

Diofantos z Aleksandrii (III w. n.e.)

Epitafium na jego grobie w tłumaczeniu na łacinę:

Hunc Diophantus habet tumulum, qui tempora vitae illius, mira denotat arte tibi. Egit sextantem juvenis; lanugine malas vestire hinc coepit parte duodecima. Septante uxori post haec sociatur; et anno formosus quinto nascitur inde puer. Semissem aetatis postquam attigit ille paternae, infelix subita morte peremptus obit. Quattuor aestates genitor lugere superstes cogitur. Hinc annos illius assequere.



Żeby dowiedzieć się, ile lat przeżył Diofantos, trzeba

- znać łacinę, oraz
- rozwiązać proste równanie diofantyczne.

Równania diofantyczne

- równania wielu zmiennych, postaci $f(x_1, \dots, x_n) = 0$

Równania diofantyczne

- równania wielu zmiennych, postaci $f(x_1, \dots, x_n) = 0$
- występują w nich tylko liczby całkowite

Równania diofantyczne

- równania wielu zmiennych, postaci $f(x_1, \dots, x_n) = 0$
- występują w nich tylko liczby całkowite
- interesują nas tylko rozwiązania całkowite

Równania diofantyczne

- równania wielu zmiennych, postaci $f(x_1, \dots, x_n) = 0$
- występują w nich tylko liczby całkowite
- interesują nas tylko rozwiązania całkowite

Przykład: (bez rozwiązań)

$$2x - 5 = 0$$

$$x^2 + 1 = 0$$

Równania diofantyczne

- równania wielu zmiennych, postaci $f(x_1, \dots, x_n) = 0$
- występują w nich tylko liczby całkowite
- interesują nas tylko rozwiązania całkowite

Przykład: (bez rozwiązań)

$$2x - 5 = 0$$

$$x^2 + 1 = 0$$

Przykład: (z jednym rozwiązaniem)

$$x - 1 = 0$$

Równania diofantyczne

- równania wielu zmiennych, postaci $f(x_1, \dots, x_n) = 0$
- występują w nich tylko liczby całkowite
- interesują nas tylko rozwiązania całkowite

Przykład: (bez rozwiązań)

$$2x - 5 = 0$$

$$x^2 + 1 = 0$$

Przykład: (z jednym rozwiązaniem)

$$x - 1 = 0$$

Przykład: (z wieloma rozwiązaniami)

$$x + y = 0$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$(2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (2n^2 + 2n + 2n^2 + 2n + 1) \cdot (2n^2 + 2n - 2n^2 - 2n - 1) \end{aligned}$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (2n^2 + 2n - 2n^2 - 2n - 1) \end{aligned}$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \end{aligned}$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \\ &= (2n + 1)^2 + (4n^2 + 4n + 1) \cdot (-1) \end{aligned}$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \\ &= (2n + 1)^2 + (4n^2 + 4n + 1) \cdot (-1) = (2n + 1)^2 - (2n + 1)^2 \end{aligned}$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \\ &= (2n + 1)^2 + (4n^2 + 4n + 1) \cdot (-1) = (2n + 1)^2 - (2n + 1)^2 \\ &= 0 \end{aligned}$$

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \\ &= (2n + 1)^2 + (4n^2 + 4n + 1) \cdot (-1) = (2n + 1)^2 - (2n + 1)^2 \\ &= 0 \end{aligned}$$

Przykład: (równanie Fermata)

Równanie $x^n + y^n - z^n = 0$ nie ma rozwiązania dla żadnego $n \geq 3$.

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \\ &= (2n + 1)^2 + (4n^2 + 4n + 1) \cdot (-1) = (2n + 1)^2 - (2n + 1)^2 \\ &= 0 \end{aligned}$$

Przykład: (równanie Fermata)

Równanie $x^n + y^n - z^n = 0$ nie ma rozwiązania dla żadnego $n \geq 3$.

Tak napisał Pierre de Fermat w 1673, ale nie podał dowodu

Równania diofantyczne

Przykład: (równanie Pitagorasa)

$$x^2 + y^2 - z^2 = 0$$

Dla każdego $n \in \mathbb{N}$, trójka $\left\{ \begin{array}{l} x = 2n + 1 \\ y = 2n^2 + 2n \\ z = 2n^2 + 2n + 1 \end{array} \right\}$ stanowi rozwiązanie, bo:

$$\begin{aligned} & (2n + 1)^2 + (2n^2 + 2n)^2 - (2n^2 + 2n + 1)^2 \\ &= (2n + 1)^2 + (\underline{2n^2} + \underline{2n} + \underline{2n^2} + \underline{2n} + 1) \cdot (\underline{2n^2} + \underline{2n} - \underline{2n^2} - \underline{2n} - 1) \\ &= (2n + 1)^2 + (4n^2 + 4n + 1) \cdot (-1) = (2n + 1)^2 - (2n + 1)^2 \\ &= 0 \end{aligned}$$

Przykład: (równanie Fermata)

Równanie $x^n + y^n - z^n = 0$ nie ma rozwiązania dla żadnego $n \geq 3$.

Tak napisał Pierre de Fermat w 1673, ale nie podał dowodu; dowód podał Andrew Wiles w 1995.

Liniowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Liniowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Liniowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$d = \text{nwd}(n, m) = n \cdot x' + m \cdot y'$$

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot x' \cdot s + m \cdot y' \cdot s \end{aligned}$$

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Inne rozwiązania: dla dowolnego $t \in \mathbb{Z}$

$$\begin{cases} x = x' \cdot s + \frac{m}{d} \cdot t \\ y = y' \cdot s - \frac{n}{d} \cdot t \end{cases}$$

jest rozwiązaniem

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Inne rozwiązania: dla dowolnego $t \in \mathbb{Z}$

$$\begin{cases} x = x' \cdot s + \frac{m}{d} \cdot t \\ y = y' \cdot s - \frac{n}{d} \cdot t \end{cases}$$

jest rozwiązaniem:

$$n \cdot \left(x' \cdot s + \frac{m}{d} \cdot t \right) + m \cdot \left(y' \cdot s - \frac{n}{d} \cdot t \right)$$

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Inne rozwiązania: dla dowolnego $t \in \mathbb{Z}$

$$\begin{cases} x = x' \cdot s + \frac{m}{d} \cdot t \\ y = y' \cdot s - \frac{n}{d} \cdot t \end{cases}$$

jest rozwiązaniem:

$$\begin{aligned} &n \cdot \left(x' \cdot s + \frac{m}{d} \cdot t \right) + m \cdot \left(y' \cdot s - \frac{n}{d} \cdot t \right) \\ &= n \cdot x' \cdot s + m \cdot y' \cdot s + \frac{nm}{d} \cdot t - \frac{mn}{d} \cdot t \end{aligned}$$

Liniowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Inne rozwiązania: dla dowolnego $t \in \mathbb{Z}$

$$\begin{cases} x = x' \cdot s + \frac{m}{d} \cdot t \\ y = y' \cdot s - \frac{n}{d} \cdot t \end{cases}$$

jest rozwiązaniem:

$$\begin{aligned} &n \cdot \left(x' \cdot s + \frac{m}{d} \cdot t \right) + m \cdot \left(y' \cdot s - \frac{n}{d} \cdot t \right) \\ &= n \cdot x' \cdot s + m \cdot y' \cdot s + \frac{nm}{d} \cdot t - \frac{mn}{d} \cdot t \\ &= (n \cdot x' + m \cdot y') \cdot s \end{aligned}$$

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Inne rozwiązania: dla dowolnego $t \in \mathbb{Z}$

$$\begin{cases} x = x' \cdot s + \frac{m}{d} \cdot t \\ y = y' \cdot s - \frac{n}{d} \cdot t \end{cases}$$

jest rozwiązaniem:

$$\begin{aligned} &n \cdot \left(x' \cdot s + \frac{m}{d} \cdot t \right) + m \cdot \left(y' \cdot s - \frac{n}{d} \cdot t \right) \\ &= n \cdot x' \cdot s + m \cdot y' \cdot s + \frac{nm}{d} \cdot t - \frac{mn}{d} \cdot t \\ &= (n \cdot x' + m \cdot y') \cdot s = \text{nwd}(n, m) \cdot s \end{aligned}$$

Linowe równania diofantyczne

z 2 niewiadomymi:

$$nx + my = k$$

Rozwiązanie może nie istnieć, np. dla $2x + 2y = 1$

Jeśli $d = \text{nwd}(n, m) \mid k$, to rozwiązanie istnieje i można je wyznaczyć tak:
dla pewnych $x', y', s \in \mathbb{Z}$ zachodzi:

$$\begin{aligned} d &= \text{nwd}(n, m) = n \cdot x' + m \cdot y' & \text{i} \\ k &= \text{nwd}(n, m) \cdot s = n \cdot \underbrace{x' \cdot s}_x + m \cdot \underbrace{y' \cdot s}_y \end{aligned}$$

Inne rozwiązania: dla dowolnego $t \in \mathbb{Z}$

$$\begin{cases} x = x' \cdot s + \frac{m}{d} \cdot t \\ y = y' \cdot s - \frac{n}{d} \cdot t \end{cases}$$

jest rozwiązaniem:

$$\begin{aligned} &n \cdot \left(x' \cdot s + \frac{m}{d} \cdot t \right) + m \cdot \left(y' \cdot s - \frac{n}{d} \cdot t \right) \\ &= n \cdot x' \cdot s + m \cdot y' \cdot s + \frac{nm}{d} \cdot t - \frac{mn}{d} \cdot t \\ &= (n \cdot x' + m \cdot y') \cdot s = \text{nwd}(n, m) \cdot s = k \end{aligned}$$

Liniowe równania diofantyczne

Przykład: $6x - 8y = 4$

Liniowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

Liniowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

$$4 = \text{nwd}(6, -8) \cdot 2$$

Liniowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

$$4 = \text{nwd}(6, -8) \cdot 2, \text{ więc } \begin{cases} x = -1 \cdot 2 \\ y = -1 \cdot 2 \end{cases} = \begin{cases} x = -2 \\ y = -2 \end{cases}$$

jest rozwiązaniem.

Linowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

$$4 = \text{nwd}(6, -8) \cdot 2, \text{ więc } \begin{cases} x = -1 \cdot 2 \\ y = -1 \cdot 2 \end{cases} = \begin{cases} x = -2 \\ y = -2 \end{cases}$$

jest rozwiązaniem. Wszystkie rozwiązania:

$$\begin{cases} x = -2 + \frac{-8}{2} \cdot t \\ y = -2 - \frac{6}{2} \cdot t \end{cases}$$

dla $t \in \mathbb{Z}$.

Linowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

$$4 = \text{nwd}(6, -8) \cdot 2, \text{ więc } \begin{cases} x = -1 \cdot 2 \\ y = -1 \cdot 2 \end{cases} = \begin{cases} x = -2 \\ y = -2 \end{cases}$$

jest rozwiązaniem. Wszystkie rozwiązania:

$$\begin{cases} x = -2 + \frac{-8}{2} \cdot t \\ y = -2 - \frac{6}{2} \cdot t \end{cases}$$

dla $t \in \mathbb{Z}$.

Przykład: $6x - 8y = 7$

Linowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

$$4 = \text{nwd}(6, -8) \cdot 2, \text{ więc } \begin{cases} x = -1 \cdot 2 \\ y = -1 \cdot 2 \end{cases} = \begin{cases} x = -2 \\ y = -2 \end{cases}$$

jest rozwiązaniem. Wszystkie rozwiązania:

$$\begin{cases} x = -2 + \frac{-8}{2} \cdot t \\ y = -2 - \frac{6}{2} \cdot t \end{cases}$$

dla $t \in \mathbb{Z}$.

Przykład: $6x - 8y = 7$

$$\text{nwd}(6, -8) = 2 \nmid 7$$

Linowe równania diofantyczne

Przykład: $6x - 8y = 4$

$$\text{nwd}(6, -8) = 2 = 6 \cdot (-1) + (-8) \cdot (-1)$$

$$4 = \text{nwd}(6, -8) \cdot 2, \text{ więc } \begin{cases} x = -1 \cdot 2 \\ y = -1 \cdot 2 \end{cases} = \begin{cases} x = -2 \\ y = -2 \end{cases}$$

jest rozwiązaniem. Wszystkie rozwiązania:

$$\begin{cases} x = -2 + \frac{-8}{2} \cdot t \\ y = -2 - \frac{6}{2} \cdot t \end{cases}$$

dla $t \in \mathbb{Z}$.

Przykład: $6x - 8y = 7$

$$\text{nwd}(6, -8) = 2 \nmid 7, \text{ więc rozwiązanie nie istnieje}$$

Liniowe równania diofantyczne

Przykład: $12x + 28y = 8$

Liniowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją.

Liniowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Liniowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$

Linowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$:

$$7 = 1 \cdot 7 + 0 \cdot 3$$

Linowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$:

$$7 = 1 \cdot 7 + 0 \cdot 3$$

$$3 = 0 \cdot 7 + 1 \cdot 3$$

Liniowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$:

$$7 = 1 \cdot 7 + 0 \cdot 3$$

$$3 = 0 \cdot 7 + 1 \cdot 3$$

$$1 = 1 \cdot 7 - 2 \cdot 3$$

Liniowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$:

$$7 = 1 \cdot 7 + 0 \cdot 3$$

$$3 = 0 \cdot 7 + 1 \cdot 3$$

$$1 = 1 \cdot 7 - 2 \cdot 3$$

więc $(-2) \cdot 3 + 1 \cdot 7 = 1$

Linowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$:

$$7 = 1 \cdot 7 + 0 \cdot 3$$

$$3 = 0 \cdot 7 + 1 \cdot 3$$

$$1 = 1 \cdot 7 - 2 \cdot 3$$

więc $(-2) \cdot 3 + 1 \cdot 7 = 1$, więc $\begin{Bmatrix} x = -2 \cdot 2 \\ y = 1 \cdot 2 \end{Bmatrix} = \begin{Bmatrix} x = -4 \\ y = 2 \end{Bmatrix}$ jest jednym z rozwiązań

Linowe równania diofantyczne

Przykład: $12x + 28y = 8$

NWD współczynników wynosi 4, wyraz wolny dzieli się przez 4, więc rozwiązania istnieją. Żeby je znaleźć najlepiej jest zacząć od podzielenia obu stron równania przez 4 i otrzymać prostsze równoważne

$$3x + 7y = 2$$

Algorytm Euklidesa, żeby wyznaczyć takie $m, n \in \mathbb{Z}$, że $\text{nwd}(3, 7) = 3m + 7n$:

$$7 = 1 \cdot 7 + 0 \cdot 3$$

$$3 = 0 \cdot 7 + 1 \cdot 3$$

$$1 = 1 \cdot 7 - 2 \cdot 3$$

więc $(-2) \cdot 3 + 1 \cdot 7 = 1$, więc $\begin{Bmatrix} x = -2 \cdot 2 \\ y = 1 \cdot 2 \end{Bmatrix} = \begin{Bmatrix} x = -4 \\ y = 2 \end{Bmatrix}$ jest jednym z rozwiązań

Wszystkie rozwiązania:

$$\begin{Bmatrix} x = -4 + 7t \\ y = 2 - 3t \end{Bmatrix}$$

Liczby pierwsze

Definicja:

Liczba $n \in \mathbb{N}$ jest pierwsza, jeśli dzieli się **tylko** przez 1 i n .

Liczby pierwsze

Definicja:

Liczba $n \in \mathbb{N}$ jest pierwsza, jeśli dzieli się *tylko* przez 1 i n .

Twierdzenie: (Euklidesa)

Zbiór $\mathcal{P}$ liczb pierwszych jest nieskończony.

Liczby pierwsze

Definicja:

Liczba $n \in \mathbb{N}$ jest pierwsza, jeśli dzieli się **tylko** przez 1 i n .

Twierdzenie: (Euklidesa)

Zbiór $\mathcal{P}$ liczb pierwszych jest nieskończony.

Dowód:

Gdyby był skończony, $\mathcal{P} = \{p_1, \dots, p_n\}$, to niech ℓ będzie iloczynem wszystkich tych liczb:

$$\ell = p_1 \cdot \dots \cdot p_n$$

Liczby pierwsze

Definicja:

Liczba $n \in \mathbb{N}$ jest pierwsza, jeśli dzieli się **tylko** przez 1 i n .

Twierdzenie: (Euklidesa)

Zbiór $\mathcal{P}$ liczb pierwszych jest nieskończony.

Dowód:

Gdyby był skończony, $\mathcal{P} = \{p_1, \dots, p_n\}$, to niech ℓ będzie iloczynem wszystkich tych liczb:

$$\ell = p_1 \cdot \dots \cdot p_n$$

Liczba $\ell + 1$ nie dzieli się przez żadną liczbę ze zbioru $\mathcal{P}$ (zawsze daje resztę 1), więc jest pierwsza

Liczby pierwsze

Definicja:

Liczba $n \in \mathbb{N}$ jest pierwsza, jeśli dzieli się *tylko* przez 1 i n .

Twierdzenie: (Euklidesa)

Zbiór $\mathcal{P}$ liczb pierwszych jest nieskończony.

Dowód:

Gdyby był skończony, $\mathcal{P} = \{p_1, \dots, p_n\}$, to niech ℓ będzie iloczynem wszystkich tych liczb:

$$\ell = p_1 \cdot \dots \cdot p_n$$

Liczba $\ell + 1$ nie dzieli się przez żadną liczbę ze zbioru $\mathcal{P}$ (zawsze daje resztę 1), więc jest pierwsza; ale jest większa od wszystkich w $\mathcal{P}$ — sprzeczność.



Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na biało.

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na biało. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalowujemy p na zielono

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na biało. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalowujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalowujemy na czerwono

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na biało. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )  
  if ( $p$  jest biała) {  
    przemaluj  $p$  na zielono;  
    for ( $i=2*p$ ;  $i \leq n$ ;  $i=i+p$ )  
      przemaluj  $i$  na czerwono;  
  }
```

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )  
  if ( $p$  jest biała) {  
    przemaluj  $p$  na zielono;  
    for ( $i=2*p$ ;  $i \leq n$ ;  $i=i+p$ )  
      przemaluj  $i$  na czerwono;  
  }
```

Liczby zielone są pierwsze.

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

p

Tabliczka wszystkich liczb od 2 do n pomalowanych na biało. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalowujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalowujemy na czerwono

```

for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
    if ( $p$  jest biała) {
        przemaluj  $p$  na zielono;
        for ( $i=2^*p$ ;  $i \leq n$ ;  $i=i+p$ )
            przemaluj  $i$  na czerwono;
    }

```

Liczby zielone są pierwsze.

[illegible]

Tabliczka wszystkich liczb od 2 do n pomalowanych na biało. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalowujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalowujemy na czerwono

```

for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
    if ( $p$  jest biała) {
        przemaluj  $p$  na zielono;
        for ( $i=2^*p$ ;  $i \leq n$ ;  $i=i+p$ )
            przemaluj  $i$  na czerwono;
    }

```

Liczby zielone są pierwsze.

[illegible]

Liczby pierwsze

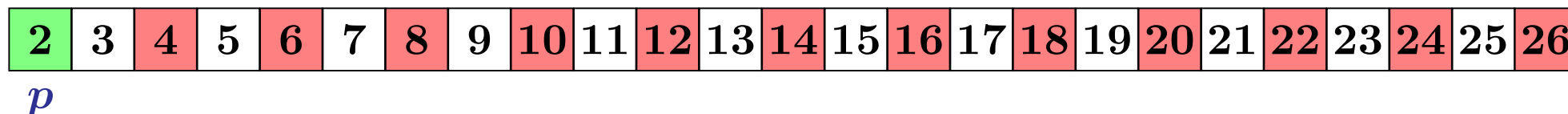
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

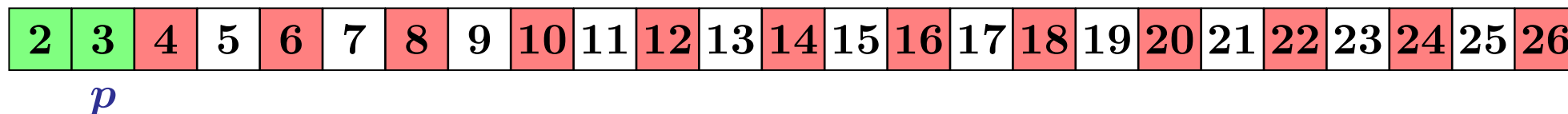
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.

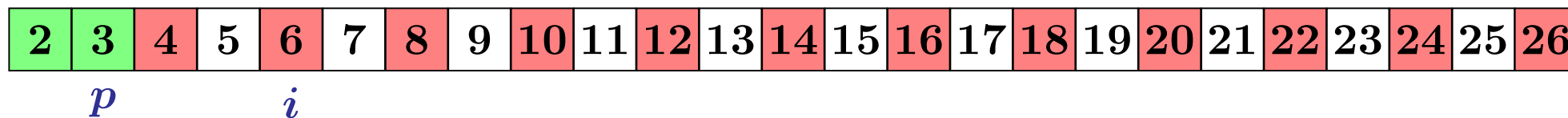


Tabliczka wszystkich liczb od 2 do n pomalowanych na biało. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalowujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalowujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
    if ( $p$  jest biała) {
        przemaluj  $p$  na zielono;
        for ( $i=2^*p$ ;  $i \leq n$ ;  $i=i+p$ )
            przemaluj  $i$  na czerwono;
    }
```

Liczby zielone są pierwsze.



Liczby pierwsze

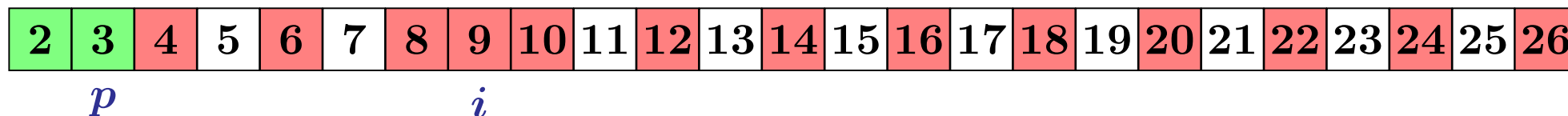
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalowujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalowujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

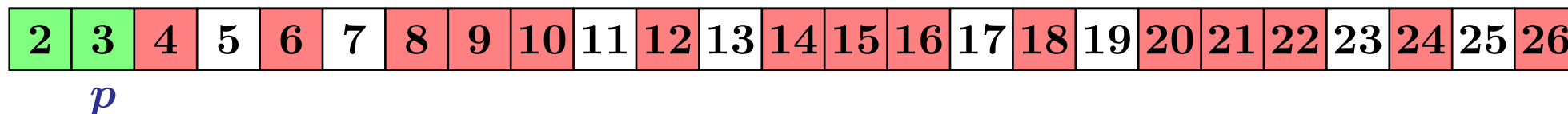
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

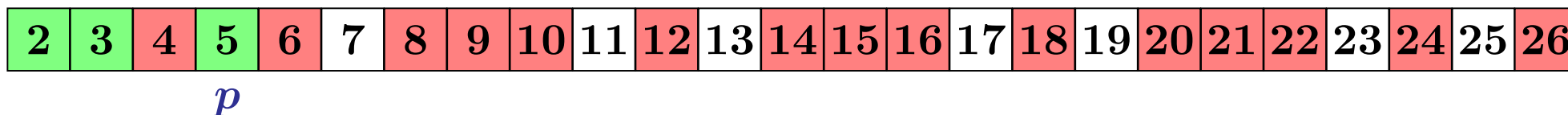
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

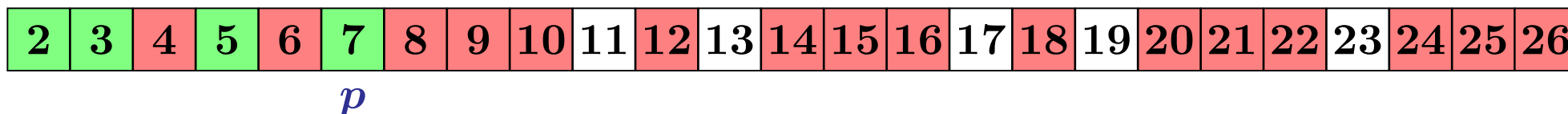
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

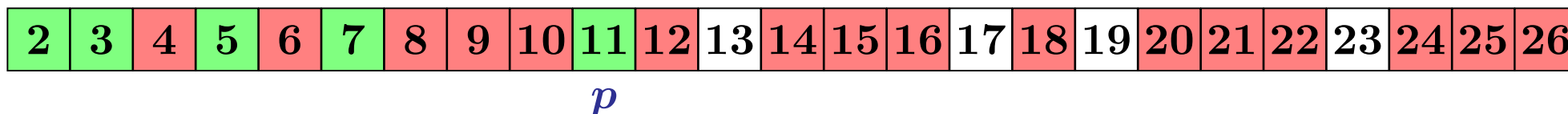
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

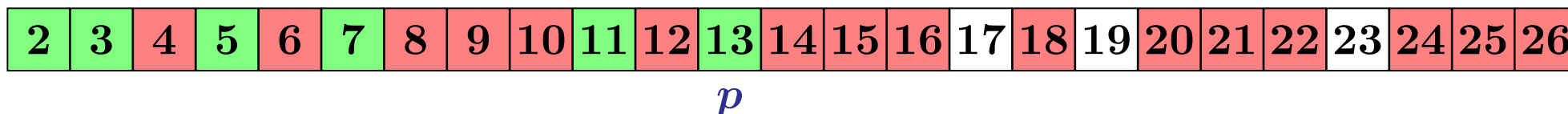
Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białe. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.



Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

p

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

p

Liczby pierwsze

Sito Eratosthenesa — do znajdowania wszystkich liczb pierwszych nie większych od danego $n \in \mathbb{N}$.

Tabliczka wszystkich liczb od 2 do n pomalowanych na białą. Przeglądamy te liczby od najmniejszej w górę; dla każdej **białej** p :

- przemalujemy p na zielono
- począwszy od $2p$ co p -tą liczbę przemalujemy na czerwono

```
for ( $p=2$ ;  $p \leq n$ ;  $p++$ )
  if ( $p$  jest biała) {
    przemaluj  $p$  na zielono;
    for ( $i=2 \cdot p$ ;  $i \leq n$ ;  $i=i+p$ )
      przemaluj  $i$  na czerwono;
  }
```

Liczby zielone są pierwsze.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

p

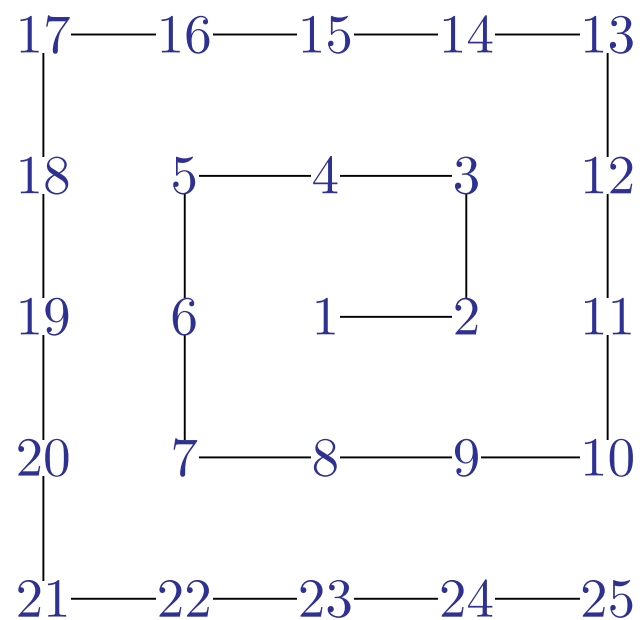
Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

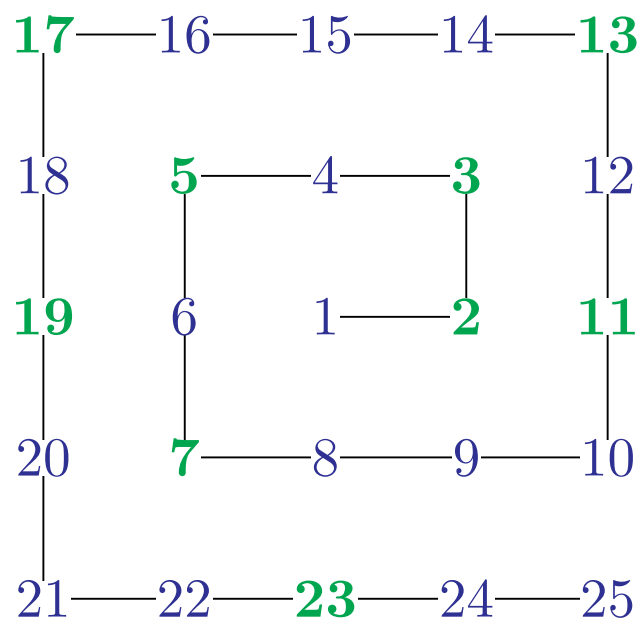
Spirala Ulama



Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

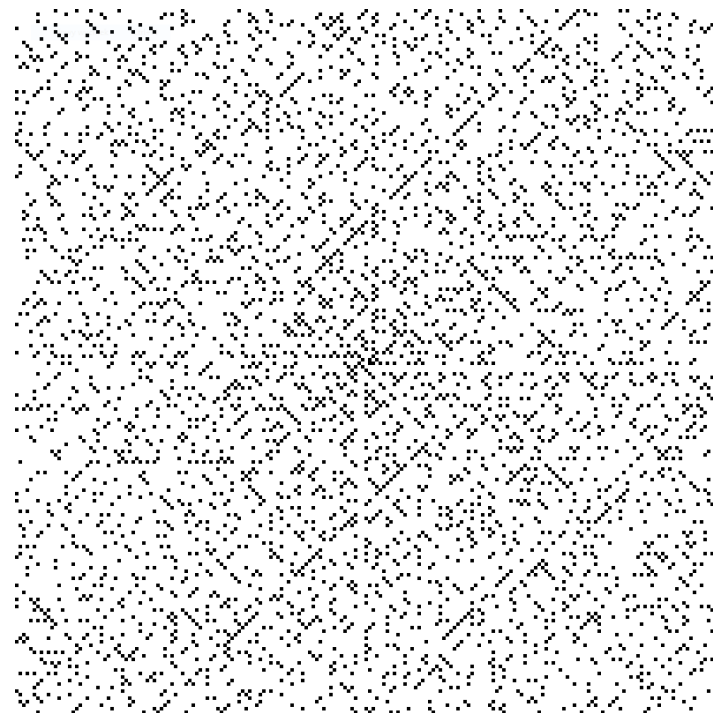
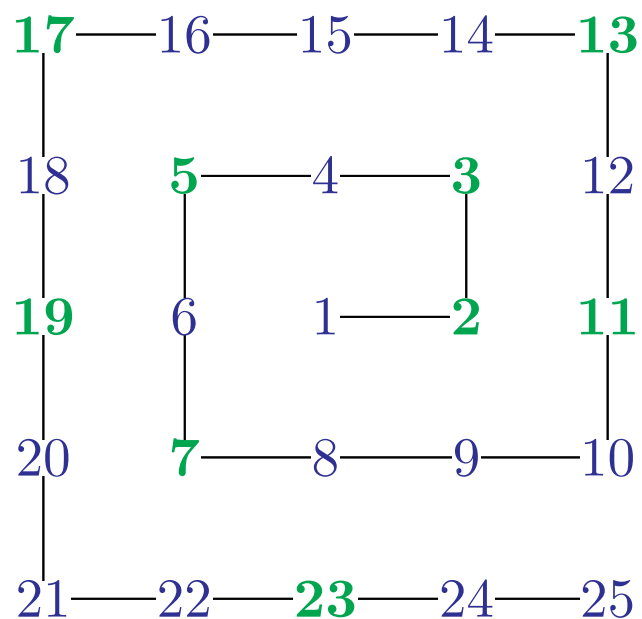
Spirala Ulama



Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

Spirala Ulama

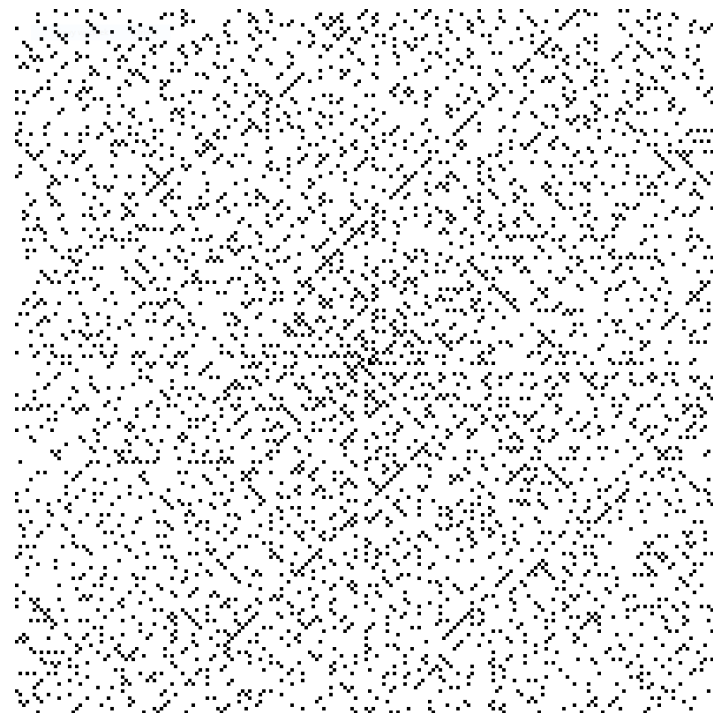
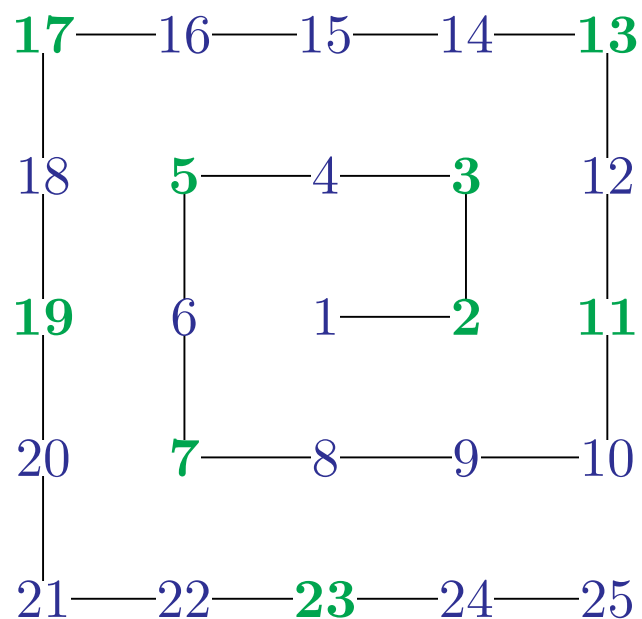


200 × 200

Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

Spirala Ulama



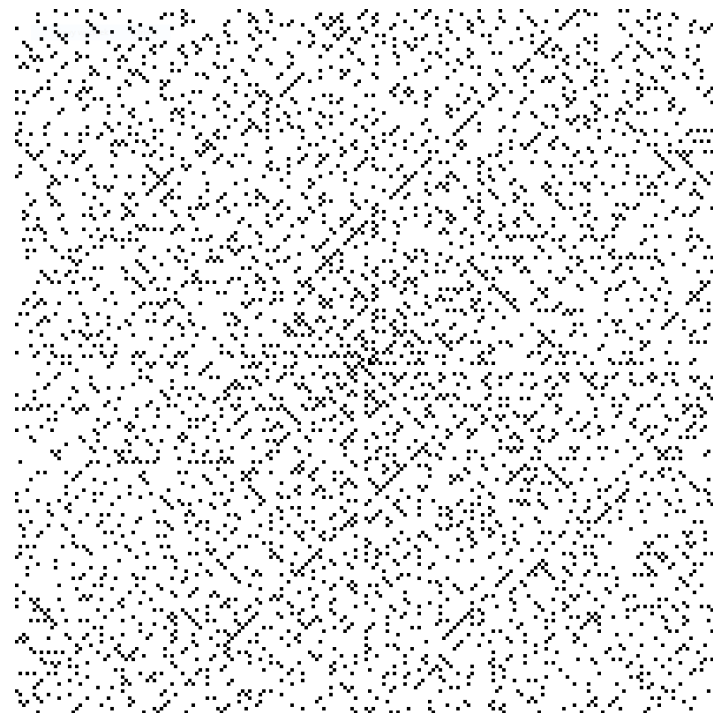
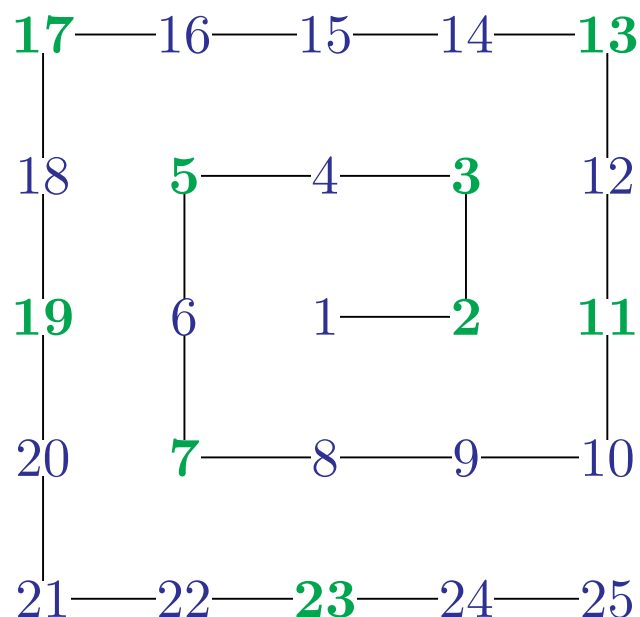
200 × 200

Trwa „wyścig” o znalezienie największej liczby **na pewno** pierwszej.

Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

Spirala Ulama



200 × 200

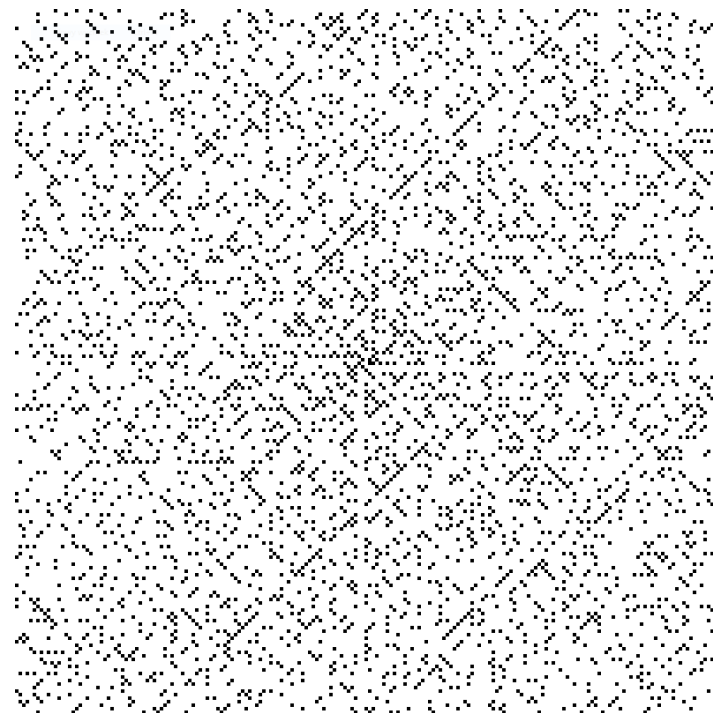
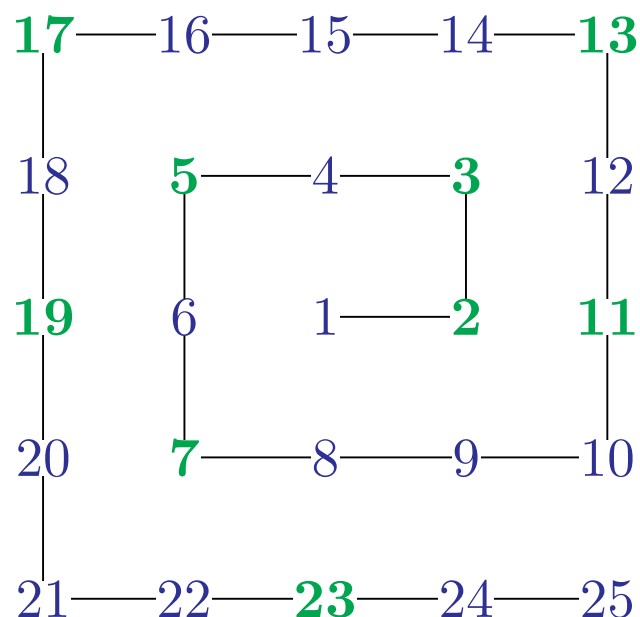
Trwa „wyścig” o znalezienie największej liczby **na pewno** pierwszej. Na razie (październik 2024) rekordzistką jest

$$2^{136\,279\,841} - 1$$

Liczby pierwsze

Nie ma prostego wzoru na liczby pierwsze.

Spirala Ulama



200 × 200

Trwa „wyścig” o znalezienie największej liczby **na pewno** pierwszej. Na razie (październik 2024) rekordzistką jest

$$2^{136\,279\,841} - 1$$

(ponad 41 mln cyfr dziesiętnych)

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n - 1$$

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n - 1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n - 1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n - 1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n - 1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Dowód:

Założmy, że n jest złożona, więc $n = p \cdot q$ dla jakichś $p, q \in \mathbb{N}$, $p \geq 2$ i $q \geq 2$.

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n - 1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Dowód:

Założmy, że n jest złożona, więc $n = p \cdot q$ dla jakichś $p, q \in \mathbb{N}$, $p \geq 2$ i $q \geq 2$. Zgodnie z założeniem mamy $p > \sqrt{n}$ i $q > \sqrt{n}$.

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n-1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Dowód:

Założmy, że n jest złożona, więc $n = p \cdot q$ dla jakichś $p, q \in \mathbb{N}$, $p \geq 2$ i $q \geq 2$. Zgodnie z założeniem mamy $p > \sqrt{n}$ i $q > \sqrt{n}$. Więc

$$n = p \cdot q$$

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n-1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Dowód:

Założmy, że n jest złożona, więc $n = p \cdot q$ dla jakichś $p, q \in \mathbb{N}$, $p \geq 2$ i $q \geq 2$. Zgodnie z założeniem mamy $p > \sqrt{n}$ i $q > \sqrt{n}$. Więc

$$n = p \cdot q > \sqrt{n} \cdot \sqrt{n}$$

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n-1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Dowód:

Założmy, że n jest złożona, więc $n = p \cdot q$ dla jakichś $p, q \in \mathbb{N}$, $p \geq 2$ i $q \geq 2$. Zgodnie z założeniem mamy $p > \sqrt{n}$ i $q > \sqrt{n}$. Więc

$$n = p \cdot q > \sqrt{n} \cdot \sqrt{n} = n$$

Czy dana liczba jest pierwsza?

Dla sprawdzenia pierwszości liczby $n \in \mathbb{N}$ możemy sprawdzać jej podzielność przez kolejne liczby naturalne

$$2, 3, 4, 5, \dots, n-1$$

Jeśli po drodze któraś z reszt dzielenia wyniesie 0, to wiemy, że jest złożona; w przeciwnym przypadku jest pierwsza.

Czy trzeba sprawdzać aż tyle?

Twierdzenie:

Jeśli liczba n nie dzieli się przez żadną k taką że $2 \leq k \leq \sqrt{n}$, to jest pierwsza.

Dowód:

Założmy, że n jest złożona, więc $n = p \cdot q$ dla jakichś $p, q \in \mathbb{N}$, $p \geq 2$ i $q \geq 2$. Zgodnie z założeniem mamy $p > \sqrt{n}$ i $q > \sqrt{n}$. Więc

$$n = p \cdot q > \sqrt{n} \cdot \sqrt{n} = n$$

— sprzeczność.



Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;    r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)    n jest złożona;  
else    n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;    r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)    n jest złożona;  
else    n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

$8 \cdot 8 = 64 > 53$ więc pierwsza.

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

$8 \cdot 8 = 64 > 53$ więc pierwsza.

Wystarczy sprawdzać podzielność przez liczby pierwsze.

Czy dana liczba jest pierwsza?

```
p=1;  
do {  
    p++;  r = n%p;  
}  
while (r != 0 && p*p < n);  
if (r == 0)  n jest złożona;  
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

$8 \cdot 8 = 64 > 53$ więc pierwsza.

Wystarczy sprawdzać podzielność przez liczby pierwsze.

Czy dana liczba jest pierwsza?

```
p=1;
do {
    p++;  r = n%p;
}
while (r != 0 && p*p < n);
if (r == 0)  n jest złożona;
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

$8 \cdot 8 = 64 > 53$ więc pierwsza.

Wystarczy sprawdzać podzielność przez liczby pierwsze.

Czy 173 jest liczbą pierwszą?

Czy dana liczba jest pierwsza?

```
p=1;
do {
    p++;  r = n%p;
}
while (r != 0 && p*p < n);
if (r == 0)  n jest złożona;
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

$8 \cdot 8 = 64 > 53$ więc pierwsza.

Wystarczy sprawdzać podzielność przez liczby pierwsze.

Czy 173 jest liczbą pierwszą?

$$173 \bmod 2 = 1 \quad 173 \bmod 7 = 5$$

$$173 \bmod 3 = 2 \quad 173 \bmod 11 = 8$$

$$173 \bmod 5 = 3 \quad 173 \bmod 13 = 4$$

Czy dana liczba jest pierwsza?

```
p=1;
do {
    p++;  r = n%p;
}
while (r != 0 && p*p < n);
if (r == 0)  n jest złożona;
else  n jest pierwsza;
```

Czy 53 jest pierwsza?

$$53 \bmod 2 = 1$$

$$53 \bmod 3 = 2$$

$$53 \bmod 4 = 1$$

$$53 \bmod 5 = 3$$

$$53 \bmod 6 = 5$$

$$53 \bmod 7 = 4$$

$8 \cdot 8 = 64 > 53$ więc pierwsza.

Wystarczy sprawdzać podzielność przez liczby pierwsze.

Czy 173 jest liczbą pierwszą?

$$173 \bmod 2 = 1 \quad 173 \bmod 7 = 5$$

$$173 \bmod 3 = 2 \quad 173 \bmod 11 = 8$$

$$173 \bmod 5 = 3 \quad 173 \bmod 13 = 4$$

$17 \cdot 17 = 289 > 173$, więc 173 jest pierwsza.

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Przykłady:

- $12 = 2^2 \cdot 3^1$

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Przykłady:

- $12 = 2^2 \cdot 3^1$
- $13 = 13^1$

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Przykłady:

- $12 = 2^2 \cdot 3^1$
- $13 = 13^1$
- $360 = 2^3 \cdot 3^2 \cdot 5^1$

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Przykłady:

- $12 = 2^2 \cdot 3^1$
- $13 = 13^1$
- $360 = 2^3 \cdot 3^2 \cdot 5^1$

... ale...

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Przykłady:

- $12 = 2^2 \cdot 3^1$
- $13 = 13^1$
- $360 = 2^3 \cdot 3^2 \cdot 5^1$

... ale ...

znajdowanie rozkładów dużych liczb na czynniki jest trudne, wymaga wielkich mocy obliczeniowej

Jednoznaczność rozkładu na iloczyn pierwszych

Twierdzenie: (zasadnicze twierdzenie arytmetyki)

Każda liczba $n \in \mathbb{N}$, $n > 1$, ma jednoznaczne przedstawienie w postaci iloczynu liczb pierwszych:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$

gdzie $p_1, p_2, \dots, p_r$ są liczbami pierwszymi uporządkowanymi rosnąco, a wykładniki $k_1, k_2, \dots, k_r$ są wszystkie większe od zera.

Przykłady:

- $12 = 2^2 \cdot 3^1$
- $13 = 13^1$
- $360 = 2^3 \cdot 3^2 \cdot 5^1$

... ale...

znajdowanie rozkładów dużych liczb na czynniki jest trudne, wymaga wielkich mocy obliczeniowej — i na tym opiera się bezpieczeństwo metod szyfrowania.