Liczby całkowite

Wojciech Gajda

Klasa IE, uniwersytecka
Liceum Marii Magdaleny
Poznań, wrzesień 2012

Plan wykładu

Teoria liczb bada zbiór liczb całkowitych dodatnich:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, ...

oraz relacje pomiędzy jego podzbiorami.

Przykłady zbiorów liczb:

nieparzyste: 1, 3, 5, 9, 11, 13, . . .
parzyste: 2, 4, 6, 8, 10, 12, . . .
kwadraty: 1, 4, 16, 25, 36, 49, . . .
pierwsze: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, , . . .

1 (modulo 4): 1, 5, 9, 13, 17, 21, . . .
3 (modulo 4): 3, 7, 11, 15, 19, 23, . . .
trójkątne: 1, 3, 6, 10, 15, 21, . . .
doskonałe: 6, 28, 496, 8128, 3350336, 8589869056, . . .
Fibonacciego: 1, 1, 2, 3, 5, 8, 13, 21 . . .

Teoria liczb bada zbiór liczb całkowitych dodatnich:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots \ldots$$

oraz relacje pomiędzy jego podzbiorami.

Przykłady zbiorów liczb:

nieparzyste: $1, 3, 5, 9, 11, 13, \ldots$
parzyste: $2, 4, 6, 8, 10, 12, \ldots$
kwadraty: $1, 4, 16, 25, 36, 49, \ldots$
pierwsze: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, , \ldots$

1 (modulo 4): $1, 5, 9, 13, 17, 21, \ldots$
3 (modulo 4): $3, 7, 11, 15, 19, 23, \ldots$
trójkątne: $1, 3, 6, 10, 15, 21, \ldots$
doskonałe: $6, 28, 496, 8128, 3350336, 8589869056, \ldots$
Fibonacciego: $1, 1, 2, 3, 5, 8, 13, 21 \ldots$

Teoria liczb bada zbiór liczb całkowitych dodatnich:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots \ldots$$

oraz relacje pomiędzy jego podzbiorami.

Przykłady zbiorów liczb:

nieparzyste: $1, 3, 5, 9, 11, 13, \ldots$
parzyste: $2, 4, 6, 8, 10, 12, \ldots$
kwadraty: $1, 4, 16, 25, 36, 49, \ldots$
pierwsze: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, , \ldots$

1 (modulo 4): $1, 5, 9, 13, 17, 21, \ldots$
3 (modulo 4): $3, 7, 11, 15, 19, 23, \ldots$
trójkątne: $1, 3, 6, 10, 15, 21, \ldots$
doskonałe: $6, 28, 496, 8128, 3350336, 8589869056, \ldots$
Fibonacciego: $1, 1, 2, 3, 5, 8, 13, 21 \ldots$

Cztery pytania

- **Pytanie 1:** Czy suma dwóch kwadratów może być kwadratem ?

Odpowiedź: **TAK:** $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, $8^2 + 15^2 = 17^2$, $9^2 + 40^2 = 41^2$, $12^2 + 35^2 = 37^2$, ...
Rozwiązaniem są tzw. *trójki Piragorejskie*, których jest nieskończenie wiele. Odpowiedź znali już Babilończycy około 1500 lat przed Chrystusem.

- **Pytanie 2:** Czy suma sześcianów może być sześcianem ?| Czy suma czwartych potęg może być czwartą potęgą ? Czy, w końcu suma n-tych potęg może być n-tą potęgą ?

Odpowiedź: **NIE:** Dowód (dopiero 350 lat po postawieniu tego pytania przez Pierre de Fermata), podał w 1994 roku Andrew Wiles.

Cztery pytania

• **Pytanie 1:** Czy suma dwóch kwadratów może być kwadratem ?
Odpowiedź: **TAK:** $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, $8^2 + 15^2 = 17^2$, $9^2 + 40^2 = 41^2$, $12^2 + 35^2 = 37^2$, ...
Rozwiązaniem są tzw. *trójki Piragorejskie*, których jest nieskończenie wiele. Odpowiedź znali już Babilończycy około 1500 lat przed Chrystusem.

• **Pytanie 2:** Czy suma sześcianów może być sześcianem ?| Czy suma czwartych potęg może być czwartą potęgą ? Czy, w końcu suma n-tych potęg może być n-tą potęgą ?

Odpowiedź: **NIE:** Dowód (dopiero 350 lat po postawieniu tego pytania przez Pierre de Fermata), podał w 1994 roku Andrew Wiles.

Cztery pytania

• **Pytanie 1:** Czy suma dwóch kwadratów może być kwadratem ?
Odpowiedź: **TAK:** $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, $8^2 + 15^2 = 17^2$, $9^2 + 40^2 = 41^2$, $12^2 + 35^2 = 37^2$, ...
Rozwiązaniem są tzw. *trójki Piragorejskie*, których jest nieskończenie wiele. Odpowiedź znali już Babilończycy około 1500 lat przed Chrystusem.

• **Pytanie 2:** Czy suma sześcianów może być sześcianem ?| Czy suma czwartych potęg może być czwartą potęgą ? Czy, w końcu suma n-tych potęg może być n-tą potęgą ?

Odpowiedź: **NIE:** Dowód (dopiero 350 lat po postawieniu tego pytania przez Pierre de Fermata), podał w 1994 roku Andrew Wiles.

Cztery pytania

• **Pytanie 1:** Czy suma dwóch kwadratów może być kwadratem ?
Odpowiedź: **TAK:** $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, $8^2 + 15^2 = 17^2$, $9^2 + 40^2 = 41^2$, $12^2 + 35^2 = 37^2$, ...
Rozwiązaniem są tzw. *trójki Piragorejskie*, których jest nieskończenie wiele. Odpowiedź znali już Babilończycy około 1500 lat przed Chrystusem.

• **Pytanie 2:** Czy suma sześcianów może być sześcianem ?| Czy suma czwartych potęg może być czwartą potęgą ? Czy, w końcu suma n-tych potęg może być n-tą potęgą ?

Odpowiedź: **NIE:** Dowód (dopiero 350 lat po postawieniu tego pytania przez Pierre de Fermata), podał w 1994 roku Andrew Wiles.

Cztery pytania

• **Pytanie 1:** Czy suma dwóch kwadratów może być kwadratem ?
Odpowiedź: **TAK:** $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, $8^2 + 15^2 = 17^2$, $9^2 + 40^2 = 41^2$, $12^2 + 35^2 = 37^2$, ...
Rozwiązaniem są tzw. *trójki Piragorejskie*, których jest nieskończenie wiele. Odpowiedź znali już Babilończycy około 1500 lat przed Chrystusem.

• **Pytanie 2:** Czy suma sześcianów może być sześcianem ?| Czy suma czwartych potęg może być czwartą potęgą ? Czy, w końcu suma n-tych potęg może być n-tą potęgą ?

Odpowiedź: **NIE:** Dowód (dopiero 350 lat po postawieniu tego pytania przez Pierre de Fermata), podał w 1994 roku Andrew Wiles.

- **Pytanie 3:** Które nieparzyste liczby pierwsze są sumami dwóch kwadratów ?

Na przykład:
$3 = NIE,\ 5 = 1^2 + 2^2,\ 7 = NIE,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,$
$19 = NIE,\ 23 = NIE,\ 29 = 2^2 + 5^2,\ 31 = NIE,\ 37 = 1^2 + 6^2, \ldots.$

Odpowiedź: **NIE**, jeśli $p \equiv 3 \bmod 4$ oraz **TAK**, jeśli $p \equiv 1 \bmod 4$.

Liczby pierwsze bliźniacze:

$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (59,61),\ (71,73) \ldots$ **(?)**

- **Pytanie 4:** Czy istnieje nieskończenie wiele liczb całkowitych p takich, że p i $p+2$ są liczbami pierwszymi ?

Odpowiedź na to pytanie nie jest znana. Pytanie pochodzi z księgi Euklidesa "Elementy".

• **Pytanie 3:** Które nieparzyste liczby pierwsze są sumami dwóch kwadratów ?

Na przykład:
$3 = NIE,\ 5 = 1^2 + 2^2,\ 7 = NIE,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,$
$19 = NIE,\ 23 = NIE,\ 29 = 2^2 + 5^2,\ 31 = NIE,\ 37 = 1^2 + 6^2, \ldots.$

Odpowiedź: **NIE**, jeśli $p \equiv 3 \bmod 4$ oraz **TAK**, jeśli $p \equiv 1 \bmod 4$.

Liczby pierwsze bliźniacze:

$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (59,61),\ (71,73) \ldots$ **(?)**

• **Pytanie 4:** Czy istnieje nieskończenie wiele liczb całkowitych p takich, że p i $p+2$ są liczbami pierwszymi ?

Odpowiedź na to pytanie nie jest znana. Pytanie pochodzi z księgi Euklidesa "Elementy".

• **Pytanie 3:** Które nieparzyste liczby pierwsze są sumami dwóch kwadratów ?

Na przykład:
$3 = NIE,\ 5 = 1^2 + 2^2,\ 7 = NIE,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,$
$19 = NIE,\ 23 = NIE,\ 29 = 2^2 + 5^2,\ 31 = NIE,\ 37 = 1^2 + 6^2, \ldots.$

Odpowiedź: **NIE**, jeśli $p \equiv 3 \bmod 4$ oraz **TAK**, jeśli $p \equiv 1 \bmod 4$.

Liczby pierwsze bliźniacze:

$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (59,61),\ (71,73)\ \ldots$ **(?)**

• **Pytanie 4:** Czy istnieje nieskończenie wiele liczb całkowitych p takich, że p i $p+2$ są liczbami pierwszymi ?

Odpowiedź na to pytanie nie jest znana. Pytanie pochodzi z księgi Euklidesa "Elementy".

• **Pytanie 3:** Które nieparzyste liczby pierwsze są sumami dwóch kwadratów ?

Na przykład:
$3 = NIE,\ 5 = 1^2 + 2^2,\ 7 = NIE,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,$
$19 = NIE,\ 23 = NIE,\ 29 = 2^2 + 5^2,\ 31 = NIE,\ 37 = 1^2 + 6^2, \ldots.$

Odpowiedź: **NIE**, jeśli $p \equiv 3 \bmod 4$ oraz **TAK**, jeśli $p \equiv 1 \bmod 4$.

Liczby pierwsze bliźniacze:

$(3,5),\ (5,7),\ (11,13),\ (17,19),\ (29,31),\ (59,61),\ (71,73)\ \ldots$ **(?)**

• **Pytanie 4:** Czy istnieje nieskończenie wiele liczb całkowitych p takich, że p i $p+2$ są liczbami pierwszymi ?

Odpowiedź na to pytanie nie jest znana. Pytanie pochodzi z księgi Euklidesa "Elementy".

Plan wykładu

Podzielność liczb

Oznaczenie. Symbolem $\mathbb{Z}$ oznaczamy w teorii liczb zbiór liczb całkowitych $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Mówimy, że liczba całkowita $b \neq 0$ **dzieli liczbę całkowitą** a, jeżeli istnieje $c \in \mathbb{Z}$ takie, że $a = bc$. Fakt, że b dzieli a zapisujemy za pomocą symbolu $b|a$.

Przykład

$3|6$, $12|132$ ponieważ $6 = 2x3$ oraz $132 = 12x11$. Wypiszmy dodatnie dzielniki liczby 6, którymi są: $1, 2, 3, 6$.

Zachodzą podzielności: $4|20$ oraz $4|36$, to znaczy 4 jest wspólnym dzielnikiem liczb 20 i 36.

Więcej jest prawdą. Liczba 4 jest **największym wspólnym dzielnikiem** liczb 20 i 36.

Podzielność liczb

Oznaczenie. Symbolem $\mathbb{Z}$ oznaczamy w teorii liczb zbiór liczb całkowitych $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Mówimy, że liczba całkowita $b \neq 0$ **dzieli liczbę całkowitą** a, jeżeli istnieje $c \in \mathbb{Z}$ takie, że $a = bc$. Fakt, że b dzieli a zapisujemy za pomocą symbolu $b|a$.

Przykład
$3|6$, $12|132$ ponieważ $6 = 2x3$ oraz $132 = 12x11$. Wypiszmy dodatnie dzielniki liczby 6, którymi są: $1, 2, 3, 6$.

Zachodzą podzielności: $4|20$ oraz $4|36$, to znaczy 4 jest wspólnym dzielnikiem liczb 20 i 36.

Więcej jest prawdą. Liczba 4 jest **największym wspólnym dzielnikiem** liczb 20 i 36.

Podzielność liczb

Oznaczenie. Symbolem $\mathbb{Z}$ oznaczamy w teorii liczb zbiór liczb całkowitych $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Mówimy, że liczba całkowita $b \neq 0$ **dzieli liczbę całkowitą** a, jeżeli istnieje $c \in \mathbb{Z}$ takie, że $a = bc$. Fakt, że b dzieli a zapisujemy za pomocą symbolu $b|a$.

Przykład
$3|6$, $12|132$ ponieważ $6 = 2x3$ oraz $132 = 12x11$. Wypiszmy dodatnie dzielniki liczby 6, którymi są: $1, 2, 3, 6$.

Zachodzą podzielności: $4|20$ oraz $4|36$, to znaczy 4 jest wspólnym dzielnikiem liczb 20 i 36.

Więcej jest prawdą. Liczba 4 jest **największym wspólnym dzielnikiem** liczb 20 i 36.

Podzielność liczb

Oznaczenie. Symbolem $\mathbb{Z}$ oznaczamy w teorii liczb zbiór liczb całkowitych $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Mówimy, że liczba całkowita $b \neq 0$ **dzieli liczbę całkowitą** a, jeżeli istnieje $c \in \mathbb{Z}$ takie, że $a = bc$. Fakt, że b dzieli a zapisujemy za pomocą symbolu $b|a$.

Przykład
$3|6$, $12|132$ ponieważ $6 = 2x3$ oraz $132 = 12x11$. Wypiszmy dodatnie dzielniki liczby 6, którymi są: $1, 2, 3, 6$.

Zachodzą podzielności: $4|20$ oraz $4|36$, to znaczy 4 jest wspólnym dzielnikiem liczb 20 i 36.

Więcej jest prawdą. Liczba 4 jest **największym wspólnym dzielnikiem** liczb 20 i 36.

Algorytm Euklidesa

Największy wspólny dzielnik liczb a i b to największa liczba całkowita dodatnia, która dzieli a i b. Zapis: $NWD(a, b)$ lub z angielskiego $gcd(a, b)$.

Przykład

Łatwo sprawdzić, że $NWD(120, 225) = 15$ ponieważ $120 = 2^3 x 3 x 5$ oraz $225 = 3^2 5^2$.

Algorytm Euklidesa znajdowania NWD

Przykład $NWD(132, 36) = ?$ Wykonujemy dzielenia z resztą:

$$132 = 36x3 + 24$$

$$36 = 24x1 + \mathbf{12}$$

$$24 = 12x2 + 0$$

Ostatnia niezerowa reszta z dzielenia, to znaczy liczba 12 jest NWD(132, 36). Dlaczego ?

Algorytm Euklidesa

Największy wspólny dzielnik liczb a i b to największa liczba całkowita dodatnia, która dzieli a i b. Zapis: $NWD(a, b)$ lub z angielskiego $gcd(a, b)$.

Przykład

Łatwo sprawdzić, że $NWD(120, 225) = 15$ ponieważ $120 = 2^3 x 3 x 5$ oraz $225 = 3^2 5^2$.

Algorytm Euklidesa znajdowania NWD

Przykład $NWD(132, 36) =?$ Wykonujemy dzielenia z resztą:

$$132 = 36x3 + 24$$

$$36 = 24x1 + \mathbf{12}$$

$$24 = 12x2 + 0$$

Ostatnia niezerowa reszta z dzielenia, to znaczy liczba 12 jest NWD(132, 36). Dlaczego ?

Algorytm Euklidesa

Największy wspólny dzielnik liczb a i b to największa liczba całkowita dodatnia, która dzieli a i b. Zapis: $NWD(a, b)$ lub z angielskiego $gcd(a, b)$.

Przykład

Łatwo sprawdzić, że $NWD(120, 225) = 15$ ponieważ $120 = 2^3 x 3 x 5$ oraz $225 = 3^2 5^2$.

Algorytm Euklidesa znajdowania NWD

Przykład $NWD(132, 36) = ?$ Wykonujemy dzielenia z resztą:

$$132 = 36x3 + 24$$

$$36 = 24x1 + \mathbf{12}$$

$$24 = 12x2 + 0$$

Ostatnia niezerowa reszta z dzielenia, to znaczy liczba 12 jest $NWD(132, 36)$. Dlaczego ?

Przykład NWD(1160718174, 316258250) = ?

$$1160718174 = 3x316258250 + 211943424$$
$$316258250 = 1x211943424 + 104314826$$
$$211943424 = 2x104314826 + 3313772$$
$$104314826 = 31x3313772 + 1587894$$
$$3313772 = 2x1587894 + 137984$$
$$1587894 = 11x137984 + 70070$$
$$137984 = 1x70070 + 67914$$
$$70070 = 1x67914 + 2156$$
$$67914 = 31x2156 + \mathbf{1078}$$
$$2156 = 2x1078 + 0$$

Przykład NWD(1160718174, 316258250) = ?

$$1160718174 = 3x316258250 + 211943424$$
$$316258250 = 1x211943424 + 104314826$$
$$211943424 = 2x104314826 + 3313772$$
$$104314826 = 31x3313772 + 1587894$$
$$3313772 = 2x1587894 + 137984$$
$$1587894 = 11x137984 + 70070$$
$$137984 = 1x70070 + 67914$$
$$70070 = 1x67914 + 2156$$
$$67914 = 31x2156 + \mathbf{1078}$$
$$2156 = 2x1078 + 0$$

Przykład NWD(1160718174, 316258250) = ?

$$1160718174 = 3x316258250 + 211943424$$
$$316258250 = 1x211943424 + 104314826$$
$$211943424 = 2x104314826 + 3313772$$
$$104314826 = 31x3313772 + 1587894$$
$$3313772 = 2x1587894 + 137984$$
$$1587894 = 11x137984 + 70070$$
$$137984 = 1x70070 + 67914$$
$$70070 = 1x67914 + 2156$$
$$67914 = 31x2156 + \mathbf{1078}$$
$$2156 = 2x1078 + 0$$

Dzielenie z resztą

Niech a i b będą liczbami całkowitymi oraz niech $b \neq 0$. Istnieje wtedy dokładnie jedna para takich liczb całkowitych q oraz r, że $a = qb + r$ oraz $0 \leq r < b$. Liczbę r nazywamy **resztą z dzielenia** a przez b.

Analiza algorytmu Euklidesa

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$r_2 = q_4 r_3 + r_4$$
$$\vdots$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_n r_{n-1} + \mathbf{r_n}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

Dzielenie z resztą

Niech a i b będą liczbami całkowitymi oraz niech $b \neq 0$. Istnieje wtedy dokładnie jedna para takich liczb całkowitych q oraz r, że $a = qb + r$ oraz $0 \leq r < b$. Liczbę r nazywamy **resztą z dzielenia** a przez b.

Analiza algorytmu Euklidesa

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$r_2 = q_4 r_3 + r_4$$
$$\vdots$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_n r_{n-1} + \mathbf{r_n}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

Dzielenie z resztą

Niech a i b będą liczbami całkowitymi oraz niech $b \neq 0$. Istnieje wtedy dokładnie jedna para takich liczb całkowitych q oraz r, że $a = qb + r$ oraz $0 \leq r < b$. Liczbę r nazywamy **resztą z dzielenia** a przez b.

Analiza algorytmu Euklidesa

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$r_2 = q_4 r_3 + r_4$$
$$\vdots$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_n r_{n-1} + \mathbf{r_n}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

gdzie $b > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$.
Dla ujednolicenia notacji przyjmiemy $r_{-1} = a$ oraz $r_0 = b$. Z równań, które uzyskaliśmy wykonując dzielenia z resztą wynikają dwie własności liczby r_n (Przekonaj się o tym !):

(1) $r_n | a$ oraz $r_n | b$

(2) jeśli $d | a$ oraz $d | b$, to $d | r_1$, $d | r_2$, $\ldots$, $d | r_n$.

Zatem $r_n = NWD(a, b)$.

Dwoiedli/smy **Twierdzenie** (Euklides, 300 BC)
Dla obliczenia $NWD(a, b)$ wystarczy wykonywać dzielenia z resztą $r_{i-1} = q_{i+1} r_i + r_{i+1}$, gdzie $i = 0, 1, 2, \ldots$ tak długo, aż dla pewnego n uzyskamy $r_{n+1} = 0$. Ostatnia niezerowa reszta z dzielenia $r_n = NWD(a, b)$. Przypomnijmy, że przyjęliśmy oznaczenia $r_{-1} = a$ oraz $r_0 = b$.

gdzie $b > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$.
Dla ujednolicenia notacji przyjmiemy $r_{-1} = a$ oraz $r_0 = b$. Z równań, które uzyskaliśmy wykonując dzielenia z resztą wynikają dwie własności liczby r_n (Przekonaj się o tym !):

(1) $r_n | a$ oraz $r_n | b$

(2) jeśli $d | a$ oraz $d | b$, to $d | r_1$, $d | r_2$, $\ldots$, $d | r_n$.

Zatem $r_n = NWD(a, b)$.

Dwoiedli/smy **Twierdzenie** (Euklides, 300 BC)
Dla obliczenia $NWD(a, b)$ wystarczy wykonywać dzielenia z resztą $r_{i-1} = q_{i+1} r_i + r_{i+1}$, gdzie $i = 0, 1, 2, \ldots$ tak długo, aż dla pewnego n uzyskamy $r_{n+1} = 0$. Ostatnia niezerowa reszta z dzielenia $r_n = NWD(a, b)$. Przypomnijmy, że przyjęliśmy oznaczenia $r_{-1} = a$ oraz $r_0 = b$.

gdzie $b > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$.
Dla ujednolicenia notacji przyjmiemy $r_{-1} = a$ oraz $r_0 = b$. Z równań, które uzyskaliśmy wykonując dzielenia z resztą wynikają dwie własności liczby r_n (Przekonaj się o tym !):

(1) $r_n | a$ oraz $r_n | b$

(2) jeśli $d | a$ oraz $d | b$, to $d | r_1$, $d | r_2$, $\ldots$, $d | r_n$.

Zatem $r_n = NWD(a, b)$.

Dwoiedli/smy **Twierdzenie** (Euklides, 300 BC)
Dla obliczenia $NWD(a, b)$ wystarczy wykonywać dzielenia z resztą $r_{i-1} = q_{i+1} r_i + r_{i+1}$, gdzie $i = 0, 1, 2, \ldots$ tak długo, aż dla pewnego n uzyskamy $r_{n+1} = 0$. Ostatnia niezerowa reszta z dzielenia $r_n = NWD(a, b)$. Przypomnijmy, że przyjęliśmy oznaczenia $r_{-1} = a$ oraz $r_0 = b$.

gdzie $b > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$.
Dla ujednolicenia notacji przyjmiemy $r_{-1} = a$ oraz $r_0 = b$. Z równań, które uzyskaliśmy wykonując dzielenia z resztą wynikają dwie własności liczby r_n (Przekonaj się o tym !):

(1) $r_n | a$ oraz $r_n | b$

(2) jeśli $d | a$ oraz $d | b$, to $d | r_1$, $d | r_2$, $\ldots$, $d | r_n$.

Zatem $r_n = NWD(a, b)$.

Dwoiedli/smy **Twierdzenie** (Euklides, 300 BC)
Dla obliczenia $NWD(a, b)$ wystarczy wykonywać dzielenia z resztą $r_{i-1} = q_{i+1} r_i + r_{i+1}$, gdzie $i = 0, 1, 2, \ldots$ tak długo, aż dla pewnego n uzyskamy $r_{n+1} = 0$. Ostatnia niezerowa reszta z dzielenia $r_n = NWD(a, b)$. Przypomnijmy, że przyjęliśmy oznaczenia $r_{-1} = a$ oraz $r_0 = b$.

Ważny wniosek z AE

Przykład

Obliczyliśmy wcześniej, że $NWD(132, 36) = 12$. Z równań, które pozwoliły nam wyznaczyć ten największy wspólny dzielnik (poczynając od przedostatniego) wyliczamy teraz po kolei:

$$12 = 36 - 24x1$$
$$12 = 36 - (132 - 36x3)x1$$
$$12 = 132x(-1) + 36x4.$$

Liczby $x_1 = -1$ i $y_1 = 4$ są rozwiązaniami równania

$$132\mathbf{x} + 36\mathbf{y} = NWD(132, 36),$$

które znaleźliśmy posługując się algorytmem Euklidesa na NWD.

Ważny wniosek z AE

Przykład

Obliczyliśmy wcześniej, że $NWD(132, 36) = 12$. Z równań, które pozwoliły nam wyznaczyć ten największy wspólny dzielnik (poczynając od przedostatniego) wyliczamy teraz po kolei:

$$12 = 36 - 24x1$$
$$12 = 36 - (132 - 36x3)x1$$
$$12 = 132x(-1) + 36x4.$$

Liczby $x_1 = -1$ i $y_1 = 4$ są rozwiązaniami równania

$$132\mathbf{x} + 36\mathbf{y} = NWD(132, 36),$$

które znaleźliśmy posługując się algorytmem Euklidesa na NWD.

Wniosek

(1) Równanie $a\mathbf{x} + b\mathbf{y} = NWD(a, b)$ ma rozwiązanie (x_1, y_1), które można znaleźć za pomocą algorytmu Euklidesa na obliczenie $NWD(a, b)$.

(2) Równanie (1) ma nieskończenie wiele rozwiązań w zbiorze liczb całkowitych $\mathbb{Z}$. Każde rozwiązanie równania (1) ma postać:

$$(x_1 + k\frac{b}{d}, y_1 - k\frac{a}{d})$$

gdzie $d = NWD(a, b)$, $ax_1 + by_1 = d$ oraz $k \in \mathbb{Z}$.

Zadanie* Przeprowadzić dowód części (2) Wniosku.

Wniosek

(1) Równanie $a\mathbf{x} + b\mathbf{y} = NWD(a, b)$ ma rozwiązanie (x_1, y_1), które można znaleźć za pomocą algorytmu Euklidesa na obliczenie $NWD(a, b)$.

(2) Równanie (1) ma nieskończenie wiele rozwiązań w zbiorze liczb całkowitych $\mathbb{Z}$. Każde rozwiązanie równania (1) ma postać:

$$(x_1 + k\frac{b}{d},\ y_1 - k\frac{a}{d})$$

gdzie $d = NWD(a, b)$, $ax_1 + by_1 = d$ oraz $k \in \mathbb{Z}$.

Zadanie* Przeprowadzić dowód części (2) Wniosku.

Wniosek

(1) Równanie $a\mathbf{x} + b\mathbf{y} = NWD(a, b)$ ma rozwiązanie (x_1, y_1), które można znaleźć za pomocą algorytmu Euklidesa na obliczenie $NWD(a, b)$.

(2) Równanie (1) ma nieskończenie wiele rozwiązań w zbiorze liczb całkowitych $\mathbb{Z}$. Każde rozwiązanie równania (1) ma postać:

$$(x_1 + k\frac{b}{d},\ y_1 - k\frac{a}{d})$$

gdzie $d = NWD(a, b)$, $ax_1 + by_1 = d$ oraz $k \in \mathbb{Z}$.

Zadanie* Przeprowadzić dowód części (2) Wniosku.

Rozkład na czynniki pierwsze

Liczby pierwsze:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...
Liczby złożone:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, ...

Przypomnijmy: *Liczba $p > 1$ jest pierwsza, jeśli nie ma innych dzielników poza 1 i p.*

Fakt 1

Jeśli p jest liczbą pierwszą oraz $p|ab$, gdzie a oraz b są liczbami całkowitymi, to $p|a$ lub $p|b$.

Dowód Załóżmy, że $p|ab$, ale p nie dzieli b. Wystarczy dowieść, że wtedy $p|a$. Ponieważ p nie dzieli b, to $NWD(p, b) = 1$. Z Wniosku z Twierdzenia Euklidesa wynika zatem, że istnieją liczby całkowite x oraz y takie, że $bx + py = 1$. Mnożąc ostatnie równanie obustronnie przez a otrzymujemy $abx + apy = a$. Z tego równania i z tego, że $p|ab$ wynika już teraz bardzo łatwo, że $p|a$. □

Rozkład na czynniki pierwsze

Liczby pierwsze:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...
Liczby złożone:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, ...

Przypomnijmy: *Liczba $p > 1$ jest pierwsza, jeśli nie ma innych dzielników poza 1 i p.*

Fakt 1

Jeśli p jest liczbą pierwszą oraz $p|ab$, gdzie a oraz b są liczbami całkowitymi, to $p|a$ lub $p|b$.

Dowód Załóżmy, że $p|ab$, ale p nie dzieli b. Wystarczy dowieść, że wtedy $p|a$. Ponieważ p nie dzieli b, to $NWD(p, b) = 1$. Z Wniosku z Twierdzenia Euklidesa wynika zatem, że istnieją liczby całkowite x oraz y takie, że $bx + py = 1$. Mnożąc ostatnie równanie obustronnie przez a otrzymujemy $abx + apy = a$. Z tego równania i z tego, że $p|ab$ wynika już teraz bardzo łatwo, że $p|a$. □

Rozkład na czynniki pierwsze

Liczby pierwsze:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...
Liczby złożone:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, ...

Przypomnijmy: *Liczba $p > 1$ jest pierwsza, jeśli nie ma innych dzielników poza 1 i p.*

Fakt 1

Jeśli p jest liczbą pierwszą oraz $p|ab$, gdzie a oraz b są liczbami całkowitymi, to $p|a$ lub $p|b$.

Dowód Załóżmy, że $p|ab$, ale p nie dzieli b. Wystarczy dowieść, że wtedy $p|a$. Ponieważ p nie dzieli b, to $NWD(p, b) = 1$. Z Wniosku z Twierdzenia Euklidesa wynika zatem, że istnieją liczby całkowite x oraz y takie, że $bx + py = 1$. Mnożąc ostatnie równanie obustronnie przez a otrzymujemy $abx + apy = a$. Z tego równania i z tego, że $p|ab$ wynika już teraz bardzo łatwo, że $p|a$. □

Rozkład na czynniki pierwsze

Liczby pierwsze:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...
Liczby złożone:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, ...

Przypomnijmy: *Liczba $p > 1$ jest pierwsza, jeśli nie ma innych dzielników poza 1 i p.*

Fakt 1

Jeśli p jest liczbą pierwszą oraz $p|ab$, gdzie a oraz b są liczbami całkowitymi, to $p|a$ lub $p|b$.

Dowód Załóżmy, że $p|ab$, ale p nie dzieli b. Wystarczy dowieść, że wtedy $p|a$. Ponieważ p nie dzieli b, to $NWD(p, b) = 1$. Z Wniosku z Twierdzenia Euklidesa wynika zatem, że istnieją liczby całkowite x oraz y takie, że $bx + py = 1$. Mnożąc ostatnie równanie obustronnie przez a otrzymujemy $abx + apy = a$. Z tego równania i z tego, że $p|ab$ wynika już teraz bardzo łatwo, że $p|a$. □

Rozkład na czynniki pierwsze

Liczby pierwsze:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...
Liczby złożone:
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, ...

Przypomnijmy: *Liczba $p > 1$ jest pierwsza, jeśli nie ma innych dzielników poza 1 i p.*

Fakt 1

Jeśli p jest liczbą pierwszą oraz $p|ab$, gdzie a oraz b są liczbami całkowitymi, to $p|a$ lub $p|b$.

Dowód Załóżmy, że $p|ab$, ale p nie dzieli b. Wystarczy dowieść, że wtedy $p|a$. Ponieważ p nie dzieli b, to $NWD(p, b) = 1$. Z Wniosku z Twierdzenia Euklidesa wynika zatem, że istnieją liczby całkowite x oraz y takie, że $bx + py = 1$. Mnożąc ostatnie równanie obustronnie przez a otrzymujemy $abx + apy = a$. Z tego równania i z tego, że $p|ab$ wynika już teraz bardzo łatwo, że $p|a$. □

Fakt 2

Jeżeli liczba pierwsza p dzieli iloczyn liczb całkowitych $a_1 a_2 \ldots a_k$, to $p|a_1$, $p|a_2$, $\ldots$ lub $p|a_k$.

Zadanie* Przeprowadzić dowód Faktu 2.

Podstawowe Twierdzenie Arytmetyki (= **PTA**, Euklides, 300 BC)

Każdą liczbę całkowitą $n \geq 2$ można przedstawić w jeden sposób jako iloczyn liczb pierwszych $n = p_1 p_2 \ldots p_k$.

Uwaga

Liczby pierwsze w tym iloczynie mogą się powtarzać. Utożsamiamy dwa przedstawienia liczby w postaci iloczynu liczb pierwszych, jeżeli te iloczyny różnią się tylko kolejnością czynników. Iloczyn z twierdzenia będziemy nazywali **rozkładem liczby n na czynniki pierwsze**.

Fakt 2

Jeżeli liczba pierwsza p dzieli iloczyn liczb całkowitych $a_1 a_2 \ldots a_k$, to $p|a_1$, $p|a_2$, $\ldots$ lub $p|a_k$.

Zadanie* Przeprowadzić dowód Faktu 2.

Podstawowe Twierdzenie Arytmetyki (= **PTA**, Euklides, 300 BC)

Każdą liczbę całkowitą $n \geq 2$ można przedstawić w jeden sposób jako iloczyn liczb pierwszych $n = p_1 p_2 \ldots p_k$.

Uwaga

Liczby pierwsze w tym iloczynie mogą się powtarzać. Utożsamiamy dwa przedstawienia liczby w postaci iloczynu liczb pierwszych, jeżeli te iloczyny różnią się tylko kolejnością czynników. Iloczyn z twierdzenia będziemy nazywali **rozkładem liczby n na czynniki pierwsze**.

Fakt 2

Jeżeli liczba pierwsza p dzieli iloczyn liczb całkowitych $a_1 a_2 \ldots a_k$, to $p|a_1$, $p|a_2$, $\ldots$ lub $p|a_k$.

Zadanie* Przeprowadzić dowód Faktu 2.

Podstawowe Twierdzenie Arytmetyki (= **PTA**, Euklides, 300 BC)

Każdą liczbę całkowitą $n \geq 2$ można przedstawić w jeden sposób jako iloczyn liczb pierwszych $n = p_1 p_2 \ldots p_k$.

Uwaga

Liczby pierwsze w tym iloczynie mogą się powtarzać. Utożsamiamy dwa przedstawienia liczby w postaci iloczynu liczb pierwszych, jeżeli te iloczyny różnią się tylko kolejnością czynników. Iloczyn z twierdzenia będziemy nazywali **rozkładem liczby n na czynniki pierwsze**.

Fakt 2

Jeżeli liczba pierwsza p dzieli iloczyn liczb całkowitych $a_1 a_2 \ldots a_k$, to $p|a_1$, $p|a_2$, $\ldots$ lub $p|a_k$.

Zadanie* Przeprowadzić dowód Faktu 2.

Podstawowe Twierdzenie Arytmetyki (= **PTA**, Euklides, 300 BC)

Każdą liczbę całkowitą $n \geq 2$ można przedstawić w jeden sposób jako iloczyn liczb pierwszych $n = p_1 p_2 \ldots p_k$.

Uwaga

Liczby pierwsze w tym iloczynie mogą się powtarzać. Utożsamiamy dwa przedstawienia liczby w postaci iloczynu liczb pierwszych, jeżeli te iloczyny różnią się tylko kolejnością czynników. Iloczyn z twierdzenia będziemy nazywali **rozkładem liczby n na czynniki pierwsze**.

Dowód PTA

Dowód Uzasadnimy dwa stwierdzenia, z których wynika **PTA**.

(1) Każdą liczbę całkowitą $n \geq 2$ można zapisać w postaci iloczynu $n = p_1 p_2 \dots p_k$, dla pewnych liczb pierwszych $p_1, p_2, \dots, p_k$.

(2) Dla liczby całkowitej $n \geq 2$ istnieje co najwyżej jeden (*rozkład na czynniki pierwsze*) jak w (1).

Dowodzimy stwierdzenia (1). Dla pierwszych trzech liczb naturalnych stwierdzenie jest prawdziwe ponieważ: $n = 2 = p_1$, $n = 3 = p_2$ oraz $n = 4 = p_1 p_1$.

Niech $N \geq 2$ będzie liczbą całkowitą. Załóżmy, że rozkład (1) istnieje dla wszystkich liczb całkowitych $n \leq N$. Udowodnimy, że wówczas rozkład na czynniki z (1) istnieje także dla liczby $N+1$.

Dowód PTA

Dowód Uzasadnimy dwa stwierdzenia, z których wynika **PTA**.

(1) Każdą liczbę całkowitą $n \geq 2$ można zapisać w postaci iloczynu $n = p_1 p_2 \dots p_k$, dla pewnych liczb pierwszych $p_1, p_2, \dots, p_k$.

(2) Dla liczby całkowitej $n \geq 2$ istnieje co najwyżej jeden (*rozkład na czynniki pierwsze*) jak w (1).

Dowodzimy stwierdzenia (1). Dla pierwszych trzech liczb naturalnych stwierdzenie jest prawdziwe ponieważ: $n = 2 = p_1$, $n = 3 = p_2$ oraz $n = 4 = p_1 p_1$.

Niech $N \geq 2$ będzie liczbą całkowitą. Załóżmy, że rozkład (1) istnieje dla wszystkich liczb całkowitych $n \leq N$. Udowodnimy, że wówczas rozkład na czynniki z (1) istnieje także dla liczby $N+1$.

Dowód PTA

Dowód Uzasadnimy dwa stwierdzenia, z których wynika **PTA**.

(1) Każdą liczbę całkowitą $n \geq 2$ można zapisać w postaci iloczynu $n = p_1 p_2 \dots p_k$, dla pewnych liczb pierwszych $p_1, p_2, \dots, p_k$.

(2) Dla liczby całkowitej $n \geq 2$ istnieje co najwyżej jeden (*rozkład na czynniki pierwsze*) jak w (1).

Dowodzimy stwierdzenia (1). Dla pierwszych trzech liczb naturalnych stwierdzenie jest prawdziwe ponieważ: $n = 2 = p_1$, $n = 3 = p_2$ oraz $n = 4 = p_1 p_1$.

Niech $N \geq 2$ będzie liczbą całkowitą. Załóżmy, że rozkład (1) istnieje dla wszystkich liczb całkowitych $n \leq N$. Udowodnimy, że wówczas rozkład na czynniki z (1) istnieje także dla liczby $N+1$.

Musi zajść jeden z dwóch przypadków.

(a) Liczba $N+1$ jest pierwsza. W tym przypadku dowód (1) dla $N+1$ jest zakończony.

(b) Liczba $N+1$ jest złożona. Wtedy $N+1 = n_1 n_2$, gdzie liczby $n_1 > 1$ oraz $n_2 > 1$, czyli $n_1 \leq N$, $n_2 \leq N$. Zatem z założenia o liczbie N wynika, że $n_1 = p_1 p_2 \dots p_k$ oraz $n_2 = q_1 q_2 \dots q_\ell$ dla pewnych liczb pierwszych $p_1, p_2, \dots p_k, q_1, q_2, \dots, q_\ell$. Z tego otrzymujemy rozkład na czynniki pierwsze liczby
$N+1 = n_1 n_2 = p_1 p_2 \dots p_k q_1 q_2 \dots q_\ell$.

Wiemy już, że stwierdzenie (1) zachodzi dla liczby $N = 4$.
Z powyższego wynika, że to stwierdzenie jest prawdziwe dla $N+1 = 4+1 = 5$, zatem także dla $5+1 = 6$, $6+1 = 7$ i tak dalej. W konsekwencji widzimy, że rozkład na czynniki pierwsze (1) zachodzi dla wszystkich liczb całkowitych ≥ 2. Ten argument oparty został na metodzie *indukcji matematycznej*, którą w dowodach stosujemy bardzo często.

Musi zajść jeden z dwóch przypadków.

(a) Liczba $N+1$ jest pierwsza. W tym przypadku dowód (1) dla $N+1$ jest zakończony.

(b) Liczba $N+1$ jest złożona. Wtedy $N+1 = n_1 n_2$, gdzie liczby $n_1 > 1$ oraz $n_2 > 1$, czyli $n_1 \leq N$, $n_2 \leq N$. Zatem z założenia o liczbie N wynika, że $n_1 = p_1 p_2 \dots p_k$ oraz $n_2 = q_1 q_2 \dots q_\ell$ dla pewnych liczb pierwszych $p_1, p_2, \dots p_k, q_1, q_2, \dots, q_\ell$. Z tego otrzymujemy rozkład na czynniki pierwsze liczby $N+1 = n_1 n_2 = p_1 p_2 \dots p_k q_1 q_2 \dots q_\ell$.

Wiemy już, że stwierdzenie (1) zachodzi dla liczby $N = 4$.
Z powyższego wynika, że to stwierdzenie jest prawdziwe dla $N+1 = 4+1 = 5$, zatem także dla $5+1 = 6$, $6+1 = 7$ i tak dalej. W konsekwencji widzimy, że rozkład na czynniki pierwsze (1) zachodzi dla wszystkich liczb całkowitych ≥ 2. Ten argument oparty został na metodzie *indukcji matematycznej*, którą w dowodach stosujemy bardzo często.

Musi zajść jeden z dwóch przypadków.

(a) Liczba $N+1$ jest pierwsza. W tym przypadku dowód (1) dla $N+1$ jest zakończony.

(b) Liczba $N+1$ jest złożona. Wtedy $N+1 = n_1 n_2$, gdzie liczby $n_1 > 1$ oraz $n_2 > 1$, czyli $n_1 \leq N$, $n_2 \leq N$. Zatem z założenia o liczbie N wynika, że $n_1 = p_1 p_2 \dots p_k$ oraz $n_2 = q_1 q_2 \dots q_\ell$ dla pewnych liczb pierwszych $p_1, p_2, \dots p_k, q_1, q_2, \dots, q_\ell$. Z tego otrzymujemy rozkład na czynniki pierwsze liczby $N+1 = n_1 n_2 = p_1 p_2 \dots p_k q_1 q_2 \dots q_\ell$.

Wiemy już, że stwierdzenie (1) zachodzi dla liczby $N = 4$.
Z powyższego wynika, że to stwierdzenie jest prawdziwe dla $N+1 = 4+1 = 5$, zatem także dla $5+1 = 6$, $6+1 = 7$ i tak dalej. W konsekwencji widzimy, że rozkład na czynniki pierwsze (1) zachodzi dla wszystkich liczb całkowitych ≥ 2. Ten argument oparty został na metodzie *indukcji matematycznej*, którą w dowodach stosujemy bardzo często.

Dowodzimy stwierdzenia (2). Niech $n = p_1 p_2 \dots p_k$ i $n = q_1 q_2 \dots q_\ell$ będę dwoma rozkładami liczby n na czynniki pierwsze. Możemy przyjąć, że $k \leq \ell$.

Z **Faktu 2** i z tego, że q_j są liczbami pierwszymi wynika, że $p_1 = q_1$, $p_1 = q_2, \dots,$ lub $p_1 = q_\ell$. Zamienimy kolejność czynników tak, aby $p_1 = q_1$. Po skróceniu równości

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

przez p_1 otrzymujemy $p_2 \dots p_k = q_2 \dots q_\ell$.

Powtarzając to postępowanie k razy otrzymujemy równości $p_i = q_i$ dla $1 \leq i \leq k$ oraz $1 = q_{k+1} q_{k+2} \dots q_\ell$. Zauważmy, że ta ostatnia równość może zachodzić tylko wtedy, gdy $k = \ell$, bo liczby $q_j > 1$. $\square$

Dowodzimy stwierdzenia (2). Niech $n = p_1 p_2 \dots p_k$ i $n = q_1 q_2 \dots q_\ell$ będę dwoma rozkładami liczby n na czynniki pierwsze. Możemy przyjąć, że $k \leq \ell$.

Z **Faktu 2** i z tego, że q_j są liczbami pierwszymi wynika, że $p_1 = q_1$, $p_1 = q_2, \dots,$ lub $p_1 = q_\ell$. Zamienimy kolejność czynników tak, aby $p_1 = q_1$. Po skróceniu równości

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

przez p_1 otrzymujemy $p_2 \dots p_k = q_2 \dots q_\ell$.

Powtarzając to postępowanie k razy otrzymujemy równości $p_i = q_i$ dla $1 \leq i \leq k$ oraz $1 = q_{k+1} q_{k+2} \dots q_\ell$. Zauważmy, że ta ostatnia równość może zachodzić tylko wtedy, gdy $k = \ell$, bo liczby $q_j > 1$. $\square$

Dowodzimy stwierdzenia (2). Niech $n = p_1 p_2 \dots p_k$ i $n = q_1 q_2 \dots q_\ell$ będę dwoma rozkładami liczby n na czynniki pierwsze. Możemy przyjąć, że $k \leq \ell$.

Z **Faktu 2** i z tego, że q_j są liczbami pierwszymi wynika, że $p_1 = q_1$, $p_1 = q_2, \dots,$ lub $p_1 = q_\ell$. Zamienimy kolejność czynników tak, aby $p_1 = q_1$. Po skróceniu równości

$$p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

przez p_1 otrzymujemy $p_2 \dots p_k = q_2 \dots q_\ell$.

Powtarzając to postępowanie k razy otrzymujemy równości $p_i = q_i$ dla $1 \leq i \leq k$ oraz $1 = q_{k+1} q_{k+2} \dots q_\ell$. Zauważmy, że ta ostatnia równość może zachodzić tylko wtedy, gdy $k = \ell$, bo liczby $q_j > 1$. $\square$

Przykład

$180 = 2x90 = 2x2x3x15 = 2x2x3x3x5$

$905293 = 37x246089 = 37x43x5723 = 37x43x59x97$

Zauważmy, że jeżeli p jest najmniejszym czynnikiem pierwszym liczby złożonej n, to $n = pm \geq pp = p^2$. Wynika z tego, że $p \leq \sqrt{n}$.

Reguła

Jeżeli chcesz rozłożyć liczbę całkowitą n ma czynniki pierwsze, to wykonuj dzielenia tej liczby przez kolejne liczby pierwsze $p \leq \sqrt{n}$.

Jeśli uzyskasz $n = pm$ dla pewnego pierwszego p, to powtórz tą samą procedurę dla liczby m, i tak dalej, aż do uzyskania rozkładu n na czynniki pierwsze. Jeżeli nie znajdziesz $p \leq \sqrt{n}$ takiego, że $p|n$ to znaczy, że n jest liczbą pierwszą.

Przykład

$180 = 2x90 = 2x2x3x15 = 2x2x3x3x5$

$905293 = 37x246089 = 37x43x5723 = 37x43x59x97$

Zauważmy, że jeżeli p jest najmniejszym czynnikiem pierwszym liczby złożonej n, to $n = pm \geq pp = p^2$. Wynika z tego, że $p \leq \sqrt{n}$.

Reguła

Jeżeli chcesz rozłożyć liczbę całkowitą n ma czynniki pierwsze, to wykonuj dzielenia tej liczby przez kolejne liczby pierwsze $p \leq \sqrt{n}$.

Jeśli uzyskasz $n = pm$ dla pewnego pierwszego p, to powtórz tą samą procedurę dla liczby m, i tak dalej, aż do uzyskania rozkładu n na czynniki pierwsze. Jeżeli nie znajdziesz $p \leq \sqrt{n}$ takiego, że $p|n$ to znaczy, że n jest liczbą pierwszą.

Przykład

$180 = 2x90 = 2x2x3x15 = 2x2x3x3x5$

$905293 = 37x246089 = 37x43x5723 = 37x43x59x97$

Zauważmy, że jeżeli p jest najmniejszym czynnikiem pierwszym liczby złożonej n, to $n = pm \geq pp = p^2$. Wynika z tego, że $p \leq \sqrt{n}$.

Reguła

Jeżeli chcesz rozłożyć liczbę całkowitą n ma czynniki pierwsze, to wykonuj dzielenia tej liczby przez kolejne liczby pierwsze $p \leq \sqrt{n}$.

Jeśli uzyskasz $n = pm$ dla pewnego pierwszego p, to powtórz tą samą procedurę dla liczby m, i tak dalej, aż do uzyskania rozkładu n na czynniki pierwsze. Jeżeli nie znajdziesz $p \leq \sqrt{n}$ takiego, że $p|n$ to znaczy, że n jest liczbą pierwszą.

Przykład

$180 = 2x90 = 2x2x3x15 = 2x2x3x3x5$

$905293 = 37x246089 = 37x43x5723 = 37x43x59x97$

Zauważmy, że jeżeli p jest najmniejszym czynnikiem pierwszym liczby złożonej n, to $n = pm \geq pp = p^2$. Wynika z tego, że $p \leq \sqrt{n}$.

Reguła

Jeżeli chcesz rozłożyć liczbę całkowitą n ma czynniki pierwsze, to wykonuj dzielenia tej liczby przez kolejne liczby pierwsze $p \leq \sqrt{n}$.

Jeśli uzyskasz $n = pm$ dla pewnego pierwszego p, to powtórz tą samą procedurę dla liczby m, i tak dalej, aż do uzyskania rozkładu n na czynniki pierwsze. Jeżeli nie znajdziesz $p \leq \sqrt{n}$ takiego, że $p|n$ to znaczy, że n jest liczbą pierwszą.

Uwaga

Nasza reguła rozkładu liczby na czynniki pierwsze działa dobrze tylko dla małych liczb całkowitych (do dziesięciu cyfr znaczących). Jest bardzo nie skuteczna dla dużych liczb. Na przykład, jeśli $n = 10^{128} + 1$, to $\sqrt{n} \approx 10^{64}$ i tyle powinniśmy sprawdzić ewentualnych podzielników przed stwierdzeniem, że n jest liczbą pierwszą.

Zabierze to bardzo dużo czasu. Jeśli nasz komputer wykonuje miliard dzieleń na sekundę, to do sprawdzenia pierwszości n tą metodą potrzebowalibyśmy w przybliżeniu $3x10^{48}$ lat. Pzypomnijmy, że zgodnie z powszechnie przyjętym *modelem standardowym* wiek Wrzechświata szacuje się obecnie na około czterna/scie miliardów ($=14x10^9$) lat.

Pozostają dwa pytania, które są bardzo ważne dla zastosowań praktycznych np. w kryptografii.

(1) Jak sprawdzić czy liczba całkowita n jest pierwsza czy złożona ?
(2) Jeśli n jest liczbą złożoną, to jak skutecznie znaleźć jej czynniki pierwsze ?

Uwaga

Nasza reguła rozkładu liczby na czynniki pierwsze działa dobrze tylko dla małych liczb całkowitych (do dziesięciu cyfr znaczących). Jest bardzo nie skuteczna dla dużych liczb. Na przykład, jeśli $n = 10^{128} + 1$, to $\sqrt{n} \approx 10^{64}$ i tyle powinniśmy sprawdzić ewentualnych podzielników przed stwierdzeniem, że n jest liczbą pierwszą.

Zabierze to bardzo dużo czasu. Jeśli nasz komputer wykonuje miliard dzieleń na sekundę, to do sprawdzenia pierwszości n tą metodą potrzebowalibyśmy w przybliżeniu $3x10^{48}$ lat. Pzypomnijmy, że zgodnie z powszechnie przyjętym *modelem standardowym* wiek Wrzechświata szacuje się obecnie na około czterna/scie miliardów (=$14x10^9$) lat.

Pozostają dwa pytania, które są bardzo ważne dla zastosowań praktycznych np. w kryptografii.

(1) Jak sprawdzić czy liczba całkowita n jest pierwsza czy złożona ?
(2) Jeśli n jest liczbą złożoną, to jak skutecznie znaleźć jej czynniki pierwsze ?

Uwaga

Nasza reguła rozkładu liczby na czynniki pierwsze działa dobrze tylko dla małych liczb całkowitych (do dziesięciu cyfr znaczących). Jest bardzo nie skuteczna dla dużych liczb. Na przykład, jeśli $n = 10^{128} + 1$, to $\sqrt{n} \approx 10^{64}$ i tyle powinniśmy sprawdzić ewentualnych podzielników przed stwierdzeniem, że n jest liczbą pierwszą.

Zabierze to bardzo dużo czasu. Jeśli nasz komputer wykonuje miliard dzieleń na sekundę, to do sprawdzenia pierwszości n tą metodą potrzebowalibyśmy w przybliżeniu $3x10^{48}$ lat. Pzypomnijmy, że zgodnie z powszechnie przyjętym *modelem standardowym* wiek Wrzechświata szacuje się obecnie na około czterna/scie miliardów (=$14x10^9$) lat.

Pozostają dwa pytania, które są bardzo ważne dla zastosowań praktycznych np. w kryptografii.

(1) Jak sprawdzić czy liczba całkowita n jest pierwsza czy złożona ?
(2) Jeśli n jest liczbą złożoną, to jak skutecznie znaleźć jej czynniki pierwsze ?

Uwaga

Nasza reguła rozkładu liczby na czynniki pierwsze działa dobrze tylko dla małych liczb całkowitych (do dziesięciu cyfr znaczących). Jest bardzo nie skuteczna dla dużych liczb. Na przykład, jeśli $n = 10^{128} + 1$, to $\sqrt{n} \approx 10^{64}$ i tyle powinniśmy sprawdzić ewentualnych podzielników przed stwierdzeniem, że n jest liczbą pierwszą.

Zabierze to bardzo dużo czasu. Jeśli nasz komputer wykonuje miliard dzieleń na sekundę, to do sprawdzenia pierwszości n tą metodą potrzebowalibyśmy w przybliżeniu $3x10^{48}$ lat. Pzypomnijmy, że zgodnie z powszechnie przyjętym *modelem standardowym* wiek Wrzechświata szacuje się obecnie na około czterna/scie miliardów (=$14x10^9$) lat.

Pozostają dwa pytania, które są bardzo ważne dla zastosowań praktycznych np. w kryptografii.

(1) Jak sprawdzić czy liczba całkowita n jest pierwsza czy złożona ?
(2) Jeśli n jest liczbą złożoną, to jak skutecznie znaleźć jej czynniki pierwsze ?

Uwaga

Nasza reguła rozkładu liczby na czynniki pierwsze działa dobrze tylko dla małych liczb całkowitych (do dziesięciu cyfr znaczących). Jest bardzo nie skuteczna dla dużych liczb. Na przykład, jeśli $n = 10^{128} + 1$, to $\sqrt{n} \approx 10^{64}$ i tyle powinniśmy sprawdzić ewentualnych podzielników przed stwierdzeniem, że n jest liczbą pierwszą.

Zabierze to bardzo dużo czasu. Jeśli nasz komputer wykonuje miliard dzieleń na sekundę, to do sprawdzenia pierwszości n tą metodą potrzebowalibyśmy w przybliżeniu $3x10^{48}$ lat. Pzypomnijmy, że zgodnie z powszechnie przyjętym *modelem standardowym* wiek Wrzechświata szacuje się obecnie na około czterna/scie miliardów (=$14x10^9$) lat.

Pozostają dwa pytania, które są bardzo ważne dla zastosowań praktycznych np. w kryptografii.

(1) Jak sprawdzić czy liczba całkowita n jest pierwsza czy złożona ?
(2) Jeśli n jest liczbą złożoną, to jak skutecznie znaleźć jej czynniki pierwsze ?

Uwaga

Niech p i q będą dużymi liczbami pierwszymi (np. ≥ 1000 cyfr znaczących). Wysyłając przez Internet liczbę $n = pq$ możemy być pewni, że obserwujący naszą korespondencję w sieci nie będą w stanie wyznaczyć za pomocą swoich komputerów użytych pzez nas liczb pierwszych p i q.

Ten problem z rozkładaniem liczby na czynniki (tzw. *problem faktoryzacji*) leży u podstaw konstrukcji bezpiecznych protokółów kryptograficznych używanych do kodowania wiadomości w Internecie, a w szczególności do tzw. protokółu RSA (RSA stosuje się dzisiaj przy kodowaniu około 70% transakcji wykonywanych w sieci).

Uwaga

Niech p i q będą dużymi liczbami pierwszymi (np. ≥ 1000 cyfr znaczących). Wysyłając przez Internet liczbę $n = pq$ możemy być pewni, że obserwujący naszą korespondencję w sieci nie będą w stanie wyznaczyć za pomocą swoich komputerów użytych pzez nas liczb pierwszych p i q.

Ten problem z rozkładaniem liczby na czynniki (tzw. *problem faktoryzacji*) leży u podstaw konstrukcji bezpiecznych protokółów kryptograficznych używanych do kodowania wiadomości w Internecie, a w szczególności do tzw. protokółu RSA (RSA stosuje się dzisiaj przy kodowaniu około 70% transakcji wykonywanych w sieci).

Plan wykładu

Definicja

Niech m będzie ustaloną liczbą całkowitą dodatnią. Mówimy, że liczba a **przystaje** do liczby b **modulo** m, jeśli $m|(b-a)$. Przystawanie a do b modulo m zapisujemy w postaci tak zwanej **kongruencji** $a \equiv b \bmod m$. Liczbę m nazywamy **modułem kongruencji**.

Przykład

$7 \equiv 15 \bmod 2$, bo $2|(15-7) = 8$
$38 \equiv 55 \bmod 17$, bo $17|(55-38) = 17$, ale
$38 \not\equiv 15 \bmod 2$, ponieważ 2 nie dzieli $(15-38) = -23$.

Uwaga

Jeśli $a \equiv b \bmod m$, to b jest jedną z nieskończenie wielu liczb: $a, a \pm m, a \pm 2m, a \pm 3m, \ldots$, lub w pisząc w skrócie: b jest jedną z nieskończenie wielu liczb $b = a + km$, gdzie k przebiega zbiór liczb całkowitych.

Definicja

Niech m będzie ustaloną liczbą całkowitą dodatnią. Mówimy, że liczba a **przystaje** do liczby b **modulo** m, jeśli $m|(b-a)$. Przystawanie a do b modulo m zapisujemy w postaci tak zwanej **kongruencji** $a \equiv b \bmod m$. Liczbę m nazywamy **modułem kongruencji**.

Przykład

$7 \equiv 15 \bmod 2$, bo $2|(15-7) = 8$
$38 \equiv 55 \bmod 17$, bo $17|(55-38) = 17$, ale
$38 \not\equiv 15 \bmod 2$, ponieważ 2 nie dzieli $(15-38) = -23$.

Uwaga

Jeśli $a \equiv b \bmod m$, to b jest jedną z nieskończenie wielu liczb: $a,\ a \pm m, a \pm 2m,\ a \pm 3m, \ldots$, lub w pisząc w skrócie: b jest jedną z nieskończenie wielu liczb $b = a + km$, gdzie k przebiega zbiór liczb całkowitych.

Wszystkie liczby nieparzyste przystają do 1 modulo 2.
Wszystkie liczby parzyste przystają do 0 modulo 2.
Każdą liczbę całkowitą przystającą do 1 modulo 4 można zapisać w postaci $1 + 4k$ dla pewnego $k \in \mathbb{Z}$.
Liczby całkowite $a \equiv 3 \bmod 4$, tworzą nieskończony podzbiór w $\mathbb{Z}$ złożony z liczb postaci $3 + 4k$, gdzie k przebiega zbiór liczb całkowitych.

Fakt 3
Jeśli $a_1 \equiv b_1 \bmod m$ oraz $a_2 \equiv b_2 \bmod m$, to
$a_1 \pm a_2 \equiv b_1 \pm b_2 \bmod m$, oraz $a_1 a_2 \equiv b_1 b_2 \bmod m$,.

Zadanie*
Posługując się definicją kongruencji przeprowadzić dowód **Faktu 3**.

Wszystkie liczby nieparzyste przystają do 1 modulo 2.
Wszystkie liczby parzyste przystają do 0 modulo 2.
Każdą liczbę całkowitą przystającą do 1 modulo 4 można zapisać w postaci $1 + 4k$ dla pewnego $k \in \mathbb{Z}$.
Liczby całkowite $a \equiv 3 \mod 4$, tworzą nieskończony podzbiór w $\mathbb{Z}$ złożony z liczb postaci $3 + 4k$, gdzie k przebiega zbiór liczb całkowitych.

Fakt 3

Jeśli $a_1 \equiv b_1 \mod m$ oraz $a_2 \equiv b_2 \mod m$, to
$a_1 \pm a_2 \equiv b_1 \pm b_2 \mod m$, oraz $a_1 a_2 \equiv b_1 b_2 \mod m$,.

Zadanie*

Posługując się definicją kongruencji przeprowadzić dowód **Faktu 3**.

Wszystkie liczby nieparzyste przystają do 1 modulo 2.
Wszystkie liczby parzyste przystają do 0 modulo 2.
Każdą liczbę całkowitą przystającą do 1 modulo 4 można zapisać w postaci $1 + 4k$ dla pewnego $k \in \mathbb{Z}$.
Liczby całkowite $a \equiv 3 \mod 4$, tworzą nieskończony podzbiór w $\mathbb{Z}$ złożony z liczb postaci $3 + 4k$, gdzie k przebiega zbiór liczb całkowitych.

Fakt 3

Jeśli $a_1 \equiv b_1 \mod m$ oraz $a_2 \equiv b_2 \mod m$, to
$a_1 \pm a_2 \equiv b_1 \pm b_2 \mod m$, oraz $a_1 a_2 \equiv b_1 b_2 \mod m$,.

Zadanie*

Posługując się definicją kongruencji przeprowadzić dowód **Faktu 3**.

Wszystkie liczby nieparzyste przystają do 1 modulo 2.
Wszystkie liczby parzyste przystają do 0 modulo 2.
Każdą liczbę całkowitą przystającą do 1 modulo 4 można zapisać w postaci $1 + 4k$ dla pewnego $k \in \mathbb{Z}$.
Liczby całkowite $a \equiv 3 \mod 4$, tworzą nieskończony podzbiór w $\mathbb{Z}$ złożony z liczb postaci $3 + 4k$, gdzie k przebiega zbiór liczb całkowitych.

Fakt 3
Jeśli $a_1 \equiv b_1 \mod m$ oraz $a_2 \equiv b_2 \mod m$, to
$a_1 \pm a_2 \equiv b_1 \pm b_2 \mod m$, oraz $a_1 a_2 \equiv b_1 b_2 \mod m$,.

Zadanie*
Posługując się definicją kongruencji przeprowadzić dowód **Faktu 3**.

Uwaga Nie wolno dzielić kongruencji stronami.
Na przykład $6 \equiv 2 \bmod 4$, ale $3 \not\equiv 1 \bmod 4$.

Rozwiążemy teraz kilka prostych kongruencji.

Przykład
Znajdziemy wszystkie liczby całkowite x, które spełniają kongruencję liniową $4\mathbf{x} \equiv 3 \bmod 23$. Po pomnożeniu stronami przez 6 (porównaj **Fakt 3**) dostajemy kongruencję $24\mathbf{x} \equiv 18 \bmod 23$,, ale $24 \equiv 1 \bmod 23$, co daje rozwiązanie $\mathbf{x} \equiv 18 \bmod 23$.

Odpowiedź: Rozwiązanie stanowi zbiór wszystkich liczb całkowitych postaci $x = 18 + 23k$, gdzie $k \in \mathbb{Z}$.

Przykład
Rozwiązać kongruencję liniową $6\mathbf{x} \equiv 5 \bmod 15$. Z definicji wynika, że nasza kongruencja jest równoważna równaniu $6\mathbf{x} - 5 = 15k$, gdzie $k \in \mathbb{Z}$ lub $6\mathbf{x} - 15\mathbf{k} = 5$.

Uwaga Nie wolno dzielić kongruencji stronami.
Na przykład $6 \equiv 2 \mod 4$, ale $3 \not\equiv 1 \mod 4$.

Rozwiążemy teraz kilka prostych kongruencji.

Przykład
Znajdziemy wszystkie liczby całkowite x, które spełniają kongruencję liniową $4\mathbf{x} \equiv 3 \mod 23$. Po pomnożeniu stronami przez 6 (porównaj **Fakt 3**) dostajemy kongruencję $24\mathbf{x} \equiv 18 \mod 23$,, ale $24 \equiv 1 \mod 23$, co daje rozwiązanie $\mathbf{x} \equiv 18 \mod 23$.

Odpowiedź: Rozwiązanie stanowi zbiór wszystkich liczb całkowitych postaci $x = 18 + 23k$, gdzie $k \in \mathbb{Z}$.

Przykład
Rozwiązać kongruencję liniową $6\mathbf{x} \equiv 5 \mod 15$. Z definicji wynika, że nasza kongruencja jest równoważna równaniu $6\mathbf{x} - 5 = 15k$, gdzie $k \in \mathbb{Z}$ lub $6\mathbf{x} - 15\mathbf{k} = 5$.

Uwaga Nie wolno dzielić kongruencji stronami.
Na przykład $6 \equiv 2 \mod 4$, ale $3 \not\equiv 1 \mod 4$.

Rozwiążemy teraz kilka prostych kongruencji.

Przykład
Znajdziemy wszystkie liczby całkowite x, które spełniają kongruencję liniową $4\mathbf{x} \equiv 3 \mod 23$. Po pomnożeniu stronami przez 6 (porównaj **Fakt 3**) dostajemy kongruencję $24\mathbf{x} \equiv 18 \mod 23$,, ale $24 \equiv 1 \mod 23$, co daje rozwiązanie $\mathbf{x} \equiv 18 \mod 23$.

Odpowiedź: Rozwiązanie stanowi zbiór wszystkich liczb całkowitych postaci $x = 18 + 23k$, gdzie $k \in \mathbb{Z}$.

Przykład
Rozwiązać kongruencję liniową $6\mathbf{x} \equiv 5 \mod 15$. Z definicji wynika, że nasza kongruencja jest równoważna równaniu $6\mathbf{x} - 5 = 15k$, gdzie $k \in \mathbb{Z}$ lub $6\mathbf{x} - 15\mathbf{k} = 5$.

Uwaga Nie wolno dzielić kongruencji stronami.
Na przykład $6 \equiv 2 \mod 4$, ale $3 \not\equiv 1 \mod 4$.

Rozwiążemy teraz kilka prostych kongruencji.

Przykład
Znajdziemy wszystkie liczby całkowite x, które spełniają kongruencję liniową $4\mathbf{x} \equiv 3 \mod 23$. Po pomnożeniu stronami przez 6 (porównaj **Fakt 3**) dostajemy kongruencję $24\mathbf{x} \equiv 18 \mod 23$,, ale $24 \equiv 1 \mod 23$, co daje rozwiązanie $\mathbf{x} \equiv 18 \mod 23$.

Odpowiedź: Rozwiązanie stanowi zbiór wszystkich liczb całkowitych postaci $x = 18 + 23k$, gdzie $k \in \mathbb{Z}$.

Przykład
Rozwiązać kongruencję liniową $6\mathbf{x} \equiv 5 \mod 15$. Z definicji wynika, że nasza kongruencja jest równoważna równaniu $6\mathbf{x} - 5 = 15k$, gdzie $k \in \mathbb{Z}$ lub $6\mathbf{x} - 15\mathbf{k} = 5$.

Takie równania (niewiadomymi są **x** i **k**) potrafimy rozwiązywać za pomocą algorytmu Euklidesa. Ponieważ $NWD(6, 15) = 3$ i liczba 3 nie dzieli 5, zatem na mocy Wniosku z Twierdzenia Euklidesa o **NWD** wynika, że nasze równanie (i kongruencja !) nie ma rozwiązań w liczbach całkowitych.

Odpowiedź: Brak rozwiązań w liczbach całkowitych.

Przykład

Rozwiązać kongruencję kwadratową: $\mathbf{x}^2 \equiv 1 \mod 8$.
Wystarczy wyznaczyć te reszty z dzielenia przez 8, których kwadraty przystają do 1 modulo 8. Podstawiając za **x** w naszej kongruencji kolejno: 0, 1, 2, 3, 4, 5, 6, 7 otrzymujemy odpowiednio następujące reszty: 0, 1, 4, 1, 0, 1, 4, 1.

Odpowiedź $\mathbf{x} \equiv 1, 3, 7 \mod 8$

Kongruencje liniowe $a\mathbf{x} \equiv b \mod m$, gdzie $a, b, m \in \mathbb{Z}$ rozwiązuje się za pomocą Wniosku z Twierdzenia Euklidesa o **NWD** w taki sam sposób jak w naszym przedostatnim przykładzie.

Sformułujemy stwierdzenie, które daje pełne rozwiązanie kongruencji liniowej. Pokażemy na przykładzie jak je zastosować. Uzupełnienie szczegółów dowodu stwierdzenia pozostawiam Wam jako proste ćwiczenie do samodzielnego wykonania. Niech $d := NWD(a, m)$.

Przykład

Rozwiązać kongruencję kwadratową: $\mathbf{x}^2 \equiv 1 \mod 8$.
Wystarczy wyznaczyć te reszty z dzielenia przez 8, których kwadraty przystają do 1 modulo 8. Podstawiając za $\mathbf{x}$ w naszej kongruencji kolejno: 0, 1, 2, 3, 4, 5, 6, 7 otrzymujemy odpowiednio następujące reszty: 0, 1, 4, 1, 0, 1, 4, 1.

Odpowiedź $\mathbf{x} \equiv 1, 3, 7 \mod 8$

Kongruencje liniowe $a\mathbf{x} \equiv b \mod m$, gdzie $a, b, m \in \mathbb{Z}$ rozwiązuje się za pomocą Wniosku z Twierdzenia Euklidesa o **NWD** w taki sam sposób jak w naszym przedostatnim przykładzie.

Sformułujemy stwierdzenie, które daje pełne rozwiązanie kongruencji liniowej. Pokażemy na przykładzie jak je zastosować. Uzupełnienie szczegółów dowodu stwierdzenia pozostawiam Wam jako proste ćwiczenie do samodzielnego wykonania. Niech $d := NWD(a, m)$.

Przykład

Rozwiązać kongruencję kwadratową: $\mathbf{x}^2 \equiv 1 \mod 8$.
Wystarczy wyznaczyć te reszty z dzielenia przez 8, których kwadraty przystają do 1 modulo 8. Podstawiając za **x** w naszej kongruencji kolejno: 0, 1, 2, 3, 4, 5, 6, 7 otrzymujemy odpowiednio następujące reszty: 0, 1, 4, 1, 0, 1, 4, 1.

Odpowiedź $\mathbf{x} \equiv 1, 3, 7 \mod 8$

Kongruencje liniowe $a\mathbf{x} \equiv b \mod m$, gdzie $a, b, m \in \mathbb{Z}$ rozwiązuje się za pomocą Wniosku z Twierdzenia Euklidesa o **NWD** w taki sam sposób jak w naszym przedostatnim przykładzie.

Sformułujemy stwierdzenie, które daje pełne rozwiązanie kongruencji liniowej. Pokażemy na przykładzie jak je zastosować. Uzupełnienie szczegółów dowodu stwierdzenia pozostawiam Wam jako proste ćwiczenie do samodzielnego wykonania. Niech $d := NWD(a, m)$.

Przykład

Rozwiązać kongruencję kwadratową: $\mathbf{x}^2 \equiv 1 \mod 8$.
Wystarczy wyznaczyć te reszty z dzielenia przez 8, których kwadraty przystają do 1 modulo 8. Podstawiając za $\mathbf{x}$ w naszej kongruencji kolejno: 0, 1, 2, 3, 4, 5, 6, 7 otrzymujemy odpowiednio następujące reszty: 0, 1, 4, 1, 0, 1, 4, 1.

Odpowiedź $\mathbf{x} \equiv 1, 3, 7 \mod 8$

Kongruencje liniowe $a\mathbf{x} \equiv b \mod m$, gdzie $a, b, m \in \mathbb{Z}$ rozwiązuje się za pomocą Wniosku z Twierdzenia Euklidesa o **NWD** w taki sam sposób jak w naszym przedostatnim przykładzie.

Sformułujemy stwierdzenie, które daje pełne rozwiązanie kongruencji liniowej. Pokażemy na przykładzie jak je zastosować. Uzupełnienie szczegółów dowodu stwierdzenia pozostawiam Wam jako proste ćwiczenie do samodzielnego wykonania. Niech $d := NWD(a, m)$.

Fakt 4

(1) Jeśli d nie dzieli b, to kongruencja $a\mathbf{x} \equiv b \bmod m$ nie ma rozwiązania.

(2) Jeśli d dzieli b, to kongruencja $a\mathbf{x} \equiv b \bmod m$ ma dokładnie d rozwiązań

$$\mathbf{x} \equiv \frac{au_0 + mk}{d} \bmod m.$$

gdzie u_0 jest rozwiązaniem równania $a\mathbf{u} + b\mathbf{v} = d$ oraz $k = 0, 1, \ldots, d-1$.

Przykład Rozwiązać kongruencję liniową $943\mathbf{x} \equiv 381 \mod 2576$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(943, 2576) = 23$.
Liczba 23 nie dzieli 381. Z **Faktu 4** (1) wynika

Odpowiedź Kongruencja nie ma rozwiązań.

Przykład Rozwiązać kongruencję liniową $893\mathbf{x} \equiv 266 \mod 2432$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(893, 2432) = 19$.
Liczba 19 dzieli 266. Z **Faktu 4** (2) wynika, że kongruencja ma 19 rozwiązań modulo 2432.

Znajdziemy te rozwiązania. Za pomocą algorytmu Euklidesa znajdujemy jedno z rozwiązań równania $893\mathbf{u} - 2432\mathbf{v} = 19$, którym jest para liczb $(u, v) = (79, -29)$. Mnożąc obydwie liczby przez $\frac{266}{19} = 14$ otrzymujemy parę liczb $(x, y) = (1106, -406)$, która jest rozwiązaniem kongruencji liniowej $893\mathbf{x} - 2432\mathbf{y} = 266$.

Przykład Rozwiązać kongruencję liniową $943\mathbf{x} \equiv 381 \mod 2576$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(943, 2576) = 23$.
Liczba 23 nie dzieli 381. Z **Faktu 4** (1) wynika

Odpowiedź Kongruencja nie ma rozwiązań.

Przykład Rozwiązać kongruencję liniową $893\mathbf{x} \equiv 266 \mod 2432$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(893, 2432) = 19$.
Liczba 19 dzieli 266. Z **Faktu 4** (2) wynika, że kongruencja ma 19 rozwiązań modulo 2432.

Znajdziemy te rozwiązania. Za pomocą algorytmu Euklidesa znajdujemy jedno z rozwiązań równania $893\mathbf{u} - 2432\mathbf{v} = 19$, którym jest para liczb $(u, v) = (79, -29)$. Mnożąc obydwie liczby przez $\frac{266}{19} = 14$ otrzymujemy parę liczb $(x, y) = (1106, -406)$, która jest rozwiązaniem kongruencji liniowej $893\mathbf{x} - 2432\mathbf{y} = 266$.

Przykład Rozwiązać kongruencję liniową $943\mathbf{x} \equiv 381 \mod 2576$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(943, 2576) = 23$.
Liczba 23 nie dzieli 381. Z **Faktu 4** (1) wynika

Odpowiedź Kongruencja nie ma rozwiązań.

Przykład Rozwiązać kongruencję liniową $893\mathbf{x} \equiv 266 \mod 2432$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(893, 2432) = 19$.
Liczba 19 dzieli 266. Z **Faktu 4** (2) wynika, że kongruencja ma 19 rozwiązań modulo 2432.

Znajdziemy te rozwiązania. Za pomocą algorytmu Euklidesa znajdujemy jedno z rozwiązań równania $893\mathbf{u} - 2432\mathbf{v} = 19$, którym jest para liczb $(u, v) = (79, -29)$. Mnożąc obydwie liczby przez $\frac{266}{19} = 14$ otrzymujemy parę liczb $(x, y) = (1106, -406)$, która jest rozwiązaniem kongruencji liniowej $893\mathbf{x} - 2432\mathbf{y} = 266$.

Przykład Rozwiązać kongruencję liniową $943\mathbf{x} \equiv 381 \mod 2576$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(943, 2576) = 23$.
Liczba 23 nie dzieli 381. Z **Faktu 4** (1) wynika

Odpowiedź Kongruencja nie ma rozwiązań.

Przykład Rozwiązać kongruencję liniową $893\mathbf{x} \equiv 266 \mod 2432$.
Za pomocą algorytmu Euklidesa obliczamy $NWD(893, 2432) = 19$.
Liczba 19 dzieli 266. Z **Faktu 4** (2) wynika, że kongruencja ma 19 rozwiązań modulo 2432.

Znajdziemy te rozwiązania. Za pomocą algorytmu Euklidesa znajdujemy jedno z rozwiązań równania $893\mathbf{u} - 2432\mathbf{v} = 19$, którym jest para liczb $(u, v) = (79, -29)$. Mnożąc obydwie liczby przez $\frac{266}{19} = 14$ otrzymujemy parę liczb $(x, y) = (1106, -406)$, która jest rozwiązaniem kongruencji liniowej $893\mathbf{x} - 2432\mathbf{y} = 266$.

Rozwiązania kongruencji $893\mathbf{x} \equiv 266 \mod 2432$ otrzymujemy z $x = 1106$ dodając 19 wielokrotności liczby $\frac{2432}{19} = 128$.

Odpowiedź

1106, 1243, 1362, 1490, 1618, 1746, 1874, 2002, 2130, 2258, 2386, 82, 210, 338, 466, 594, 722, 850, 978.

Rozwiązania kongruencji $893\mathbf{x} \equiv 266 \mod 2432$ otrzymujemy z $x = 1106$ dodając 19 wielokrotności liczby $\frac{2432}{19} = 128$.

Odpowiedź

$\overline{1106}, 1243, 1362, 1490, 1618, 1746, 1874, 2002, 2130, 2258, 2386, 82, 210, 338, 466, 594, 722, 850, 978$.

Plan wykładu

Przykład

Dla $p = 11$ wyliczymy potęgi liczby 2 i liczby 3 modulo 11.

$2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 5 \bmod 11,\ 2^5 = 32 \equiv 10 \bmod 11,$
$2^6 = (2^3)^2 = 8^2 = 64 \equiv 9 \bmod 11,\ 2^7 = 2^5 2^2 = 4x10 \equiv 7 \bmod 11,$
$2^8 = (2^4)^2 = 5^2 \equiv 3 \bmod 11,\ 2^9 = 2^8 2 \equiv 6 \bmod 11,$
$2^{10} = 2^9 2 = 12 \equiv 1 \bmod 11.$

$3^2 = 9,\ 3^4 = (3^2)^2 = 81 \equiv 4 \bmod 11,$
$3^8 = (3^4)^2 = 4^2 = 16 \equiv 5 \bmod 11,$
$3^{10} = 3^8 3^2 = 5x9 = 45 \equiv 1 \bmod 11.$

Zachodzi następujący bardzo ważny wzór, który pokazuje, że wyniki rachunku z ostatniego przykładu nie są przypadkowe.

Przykład

Dla $p = 11$ wyliczymy potęgi liczby 2 i liczby 3 modulo 11.

$2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 5 \bmod 11,\ 2^5 = 32 \equiv 10 \bmod 11,$
$2^6 = (2^3)^2 = 8^2 = 64 \equiv 9 \bmod 11,\ 2^7 = 2^5 2^2 = 4x10 \equiv 7 \bmod 11,$
$2^8 = (2^4)^2 = 5^2 \equiv 3 \bmod 11,\ 2^9 = 2^8 2 \equiv 6 \bmod 11,$
$2^{10} = 2^9 2 = 12 \equiv 1 \bmod 11.$

$3^2 = 9,\ 3^4 = (3^2)^2 = 81 \equiv 4 \bmod 11,$
$3^8 = (3^4)^2 = 4^2 = 16 \equiv 5 \bmod 11,$
$3^{10} = 3^8 3^2 = 5x9 = 45 \equiv 1 \bmod 11.$

Zachodzi następujący bardzo ważny wzór, który pokazuje, że wyniki rachunku z ostatniego przykładu nie są przypadkowe.

Przykład

Dla $p = 11$ wyliczymy potęgi liczby 2 i liczby 3 modulo 11.

$2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 5 \bmod 11,\ 2^5 = 32 \equiv 10 \bmod 11,$
$2^6 = (2^3)^2 = 8^2 = 64 \equiv 9 \bmod 11,\ 2^7 = 2^5 2^2 = 4x10 \equiv 7 \bmod 11,$
$2^8 = (2^4)^2 = 5^2 \equiv 3 \bmod 11,\ 2^9 = 2^8 2 \equiv 6 \bmod 11,$
$2^{10} = 2^9 2 = 12 \equiv 1 \bmod 11.$

$3^2 = 9,\ 3^4 = (3^2)^2 = 81 \equiv 4 \bmod 11,$
$3^8 = (3^4)^2 = 4^2 = 16 \equiv 5 \bmod 11,$
$3^{10} = 3^8 3^2 = 5x9 = 45 \equiv 1 \bmod 11.$

Zachodzi następujący bardzo ważny wzór, który pokazuje, że wyniki rachunku z ostatniego przykładu nie są przypadkowe.

Przykład

Dla $p = 11$ wyliczymy potęgi liczby 2 i liczby 3 modulo 11.

$2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 5 \mod 11,\ 2^5 = 32 \equiv 10 \mod 11,$
$2^6 = (2^3)^2 = 8^2 = 64 \equiv 9 \mod 11,\ 2^7 = 2^5 2^2 = 4x10 \equiv 7 \mod 11,$
$2^8 = (2^4)^2 = 5^2 \equiv 3 \mod 11,\ 2^9 = 2^8 2 \equiv 6 \mod 11,$
$2^{10} = 2^9 2 = 12 \equiv 1 \mod 11.$

$3^2 = 9,\ 3^4 = (3^2)^2 = 81 \equiv 4 \mod 11,$
$3^8 = (3^4)^2 = 4^2 = 16 \equiv 5 \mod 11,$
$3^{10} = 3^8 3^2 = 5x9 = 45 \equiv 1 \mod 11.$

Zachodzi następujący bardzo ważny wzór, który pokazuje, że wyniki rachunku z ostatniego przykładu nie są przypadkowe.

Małe Twierdzenie Fermata(=MTF)

Niech p będzie liczbą pierwszą rożną od 2. Dla każdej liczby całkowitej a, która nie dzieli się przez p zachodzi kongruencja $a^{p-1} \equiv 1 \mod p$.

Z **MTF** wynika, że $6^{22} \equiv 1 \mod 23$, ale można sprawdzić, że $6^{22} - 1 = 23x572268277x5750745$.

Z **MTF** wynika, że $73^{100} \equiv 1 \mod 101$, ale jak można sprawdzić, $73^{100} - 1$ jest liczbą, która ma aż 186 cyfr znaczących.

Przykład

Za pomocą twierdzenia Fermata obliczymy resztę z dzielenia liczby 9^{794} przy dzieleniu przez 73.

Łatwo sprawdzić, że $794 = 72x11 + 2$ dlatego $9^{794} = 9^{72x11+2} = (9^{72})^{11}9^2$.

Z **MTF** wiemy, że $9^{72} \equiv 1 \mod 73$,

czyli $(9^{72})^{11}9^2 \equiv (1)^{11}x81 = 81 \equiv 8 \mod 73$.

Małe Twierdzenie Fermata(=MTF)

Niech p będzie liczbą pierwszą rożną od 2. Dla każdej liczby całkowitej a, która nie dzieli się przez p zachodzi kongruencja $a^{p-1} \equiv 1 \mod p$.

Z **MTF** wynika, że $6^{22} \equiv 1 \mod 23$, ale można sprawdzić, że $6^{22} - 1 = 23x572268277x5750745$.

Z **MTF** wynika, że $73^{100} \equiv 1 \mod 101$, ale jak można sprawdzić, $73^{100} - 1$ jest liczbą, która ma aż 186 cyfr znaczących.

Przykład

Za pomocą twierdzenia Fermata obliczymy resztę z dzielenia liczby 9^{794} przy dzieleniu przez 73.

Łatwo sprawdzić, że $794 = 72x11 + 2$ dlatego $9^{794} = 9^{72x11+2} = (9^{72})^{11}9^2$.
Z **MTF** wiemy, że $9^{72} \equiv 1 \mod 73$,
czyli $(9^{72})^{11}9^2 \equiv (1)^{11}x81 = 81 \equiv 8 \mod 73$.

Małe Twierdzenie Fermata(=MTF)

Niech p będzie liczbą pierwszą rożną od 2. Dla każdej liczby całkowitej a, która nie dzieli się przez p zachodzi kongruencja $a^{p-1} \equiv 1 \mod p$.

Z **MTF** wynika, że $6^{22} \equiv 1 \mod 23$, ale można sprawdzić, że $6^{22} - 1 = 23x572268277x5750745$.

Z **MTF** wynika, że $73^{100} \equiv 1 \mod 101$, ale jak można sprawdzić, $73^{100} - 1$ jest liczbą, która ma aż 186 cyfr znaczących.

Przykład

Za pomocą twierdzenia Fermata obliczymy resztę z dzielenia liczby 9^{794} przy dzieleniu przez 73.

Łatwo sprawdzić, że $794 = 72x11 + 2$ dlatego $9^{794} = 9^{72x11+2} = (9^{72})^{11}9^2$.

Z **MTF** wiemy, że $9^{72} \equiv 1 \mod 73$,

czyli $(9^{72})^{11}9^2 \equiv (1)^{11}x81 = 81 \equiv 8 \mod 73$.

Małe Twierdzenie Fermata(=MTF)

Niech p będzie liczbą pierwszą rożną od 2. Dla każdej liczby całkowitej a, która nie dzieli się przez p zachodzi kongruencja $a^{p-1} \equiv 1 \mod p$.

Z **MTF** wynika, że $6^{22} \equiv 1 \mod 23$, ale można sprawdzić, że $6^{22} - 1 = 23x572268277x5750745$.

Z **MTF** wynika, że $73^{100} \equiv 1 \mod 101$, ale jak można sprawdzić, $73^{100} - 1$ jest liczbą, która ma aż 186 cyfr znaczących.

Przykład

Za pomocą twierdzenia Fermata obliczymy resztę z dzielenia liczby 9^{794} przy dzieleniu przez 73.

Łatwo sprawdzić, że $794 = 72x11 + 2$ dlatego $9^{794} = 9^{72x11+2} = (9^{72})^{11}9^2$.

Z **MTF** wiemy, że $9^{72} \equiv 1 \mod 73$,

czyli $(9^{72})^{11}9^2 \equiv (1)^{11}x81 = 81 \equiv 8 \mod 73$.

Małe Twierdzenie Fermata(=MTF)

Niech p będzie liczbą pierwszą rożną od 2. Dla każdej liczby całkowitej a, która nie dzieli się przez p zachodzi kongruencja $a^{p-1} \equiv 1 \mod p$.

Z **MTF** wynika, że $6^{22} \equiv 1 \mod 23$, ale można sprawdzić, że $6^{22} - 1 = 23x572268277x5750745$.

Z **MTF** wynika, że $73^{100} \equiv 1 \mod 101$, ale jak można sprawdzić, $73^{100} - 1$ jest liczbą, która ma aż 186 cyfr znaczących.

Przykład

Za pomocą twierdzenia Fermata obliczymy resztę z dzielenia liczby 9^{794} przy dzieleniu przez 73.

Łatwo sprawdzić, że $794 = 72x11 + 2$ dlatego $9^{794} = 9^{72x11+2} = (9^{72})^{11}9^2$.
Z **MTF** wiemy, że $9^{72} \equiv 1 \mod 73$,
czyli $(9^{72})^{11}9^2 \equiv (1)^{11}x81 = 81 \equiv 8 \mod 73$.

Fakt 5

Jeśli a i p są takie jak w **MTF**, to zbiór reszt modulo p liczb: $a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$ jest równy zbiorowi reszt: $1,\ 2,\ 3,\ \ldots,\ (p-1)$ modulo p.

Dowód **Faktu 5**

Mamy następujace zawieranie zbiorów reszt modulo p

$$\{a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\} \quad \subset \quad \{1,\ 2,\ 3,\ \ldots,\ (p-1)\}.$$

Pokażemy, że zbiór po lewej stronie ostatniej inkluzji składa się z $(p-1)$ elementów, co pociągą natychmiast równość tych dwóch zbiórów.

Jeśli $ja \equiv ka \bmod p$, gdzie $1 < j,\ k < p$, to na mocy definicji kongruencji $p|a(j-k)$, ale p nie dzieli a z założenia.

Zatem $p|(j-k)$, a to dla takich liczb jak j i k może zachodzić tylko wtedy, gdy $j = k$. $\square$

Fakt 5

Jeśli a i p są takie jak w **MTF**, to zbiór reszt modulo p liczb: $a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$ jest równy zbiorowi reszt: $1,\ 2,\ 3,\ \ldots,\ (p-1)$ modulo p.

Dowód **Faktu 5**

Mamy następujace zawieranie zbiorów reszt modulo p

$$\{a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\} \quad \subset \quad \{1,\ 2,\ 3,\ \ldots,\ (p-1)\}.$$

Pokażemy, że zbiór po lewej stronie ostatniej inkluzji składa się z $(p-1)$ elementów, co pociągą natychmiast równość tych dwóch zbiórów.

Jeśli $ja \equiv ka \bmod p$, gdzie $1 < j,\ k < p$, to na mocy definicji kongruencji $p|a(j-k)$, ale p nie dzieli a z założenia.

Zatem $p|(j-k)$, a to dla takich liczb jak j i k może zachodzić tylko wtedy, gdy $j = k$. $\square$

Fakt 5

Jeśli a i p są takie jak w **MTF**, to zbiór reszt modulo p liczb: $a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$ jest równy zbiorowi reszt: $1,\ 2,\ 3,\ \ldots,\ (p-1)$ modulo p.

Dowód **Faktu 5**

Mamy następujace zawieranie zbiorów reszt modulo p

$$\{a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\} \quad \subset \quad \{1,\ 2,\ 3,\ \ldots,\ (p-1)\}.$$

Pokażemy, że zbiór po lewej stronie ostatniej inkluzji składa się z $(p-1)$ elementów, co pociągą natychmiast równość tych dwóch zbiórów.

Jeśli $ja \equiv ka \bmod p$, gdzie $1 < j,\ k < p$, to na mocy definicji kongruencji $p|a(j-k)$, ale p nie dzieli a z założenia.

Zatem $p|(j-k)$, a to dla takich liczb jak j i k może zachodzić tylko wtedy, gdy $j = k$. $\square$

Fakt 5

Jeśli a i p są takie jak w **MTF**, to zbiór reszt modulo p liczb: $a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$ jest równy zbiorowi reszt: $1,\ 2,\ 3,\ \ldots,\ (p-1)$ modulo p.

Dowód **Faktu 5**

Mamy następujace zawieranie zbiorów reszt modulo p

$$\{a,\ 2a,\ 3a,\ \ldots,\ (p-1)a\} \quad \subset \quad \{1,\ 2,\ 3,\ \ldots,\ (p-1)\}.$$

Pokażemy, że zbiór po lewej stronie ostatniej inkluzji składa się z $(p-1)$ elementów, co pociągą natychmiast równość tych dwóch zbiórów.

Jeśli $ja \equiv ka \bmod p$, gdzie $1 < j,\ k < p$, to na mocy definicji kongruencji $p|a(j-k)$, ale p nie dzieli a z założenia.

Zatem $p|(j-k)$, a to dla takich liczb jak j i k może zachodzić tylko wtedy, gdy $j = k$. $\square$

Dowód MTF

Utworzymy iloczyn wzystkich reszt
$W = 1\,x\,2\,x\,3\,x\,\ldots\,x\,(p-1)$ modulo p.

Na mocy **Faktu 5** zachodzi kongruencja
$W = 1\,x\,2\,x\,3\,x\,\ldots\,x\,(p-1) \equiv a\,x\,2a\,x\,3a\,\ldots\,(p-1) = a^{p-1}W \mod p$,

a po przekształceniu otrzymujemy $W(a^{p-1}-1) \equiv 0 \mod p$.

Reszta $W \not\equiv 0 \mod p$. Razem z ostatnią kongruencją implikuje to, że liczba p dzieli $a^{p-1}-1$ czyli $a^{p-1} \equiv 1 \mod p$. $\square$

Dowód MTF

Utworzymy iloczyn wzystkich reszt
$W = 1\,x\,2\,x\,3\,x\,\ldots\,x\,(p-1)$ modulo p.

Na mocy **Faktu 5** zachodzi kongruencja
$W = 1\,x\,2\,x\,3\,x\,\ldots\,x\,(p-1) \equiv a\,x\,2a\,x\,3a\,\ldots\,(p-1) = a^{p-1}W \bmod p$,

a po przekształceniu otrzymujemy $W(a^{p-1}-1) \equiv 0 \bmod p$.

Reszta $W \not\equiv 0 \bmod p$. Razem z ostatnią kongruencją implikuje to, że liczba p dzieli $a^{p-1}-1$ czyli $a^{p-1} \equiv 1 \bmod p$. $\square$

Dowód MTF

Utworzymy iloczyn wzystkich reszt
$W = 1\,x\,2\,x\,3\,x\,\ldots\,x\,(p-1)$ modulo p.

Na mocy **Faktu 5** zachodzi kongruencja
$W = 1\,x\,2\,x\,3\,x\,\ldots\,x\,(p-1) \equiv a\,x\,2a\,x\,3a\,\ldots\,(p-1) = a^{p-1}W \mod p$,

a po przekształceniu otrzymujemy $W(a^{p-1}-1) \equiv 0 \mod p$.

Reszta $W \not\equiv 0 \mod$ p. Razem z ostatnią kongruencją implikuje to, że liczba p dzieli $a^{p-1}-1$ czyli $a^{p-1} \equiv 1 \mod p$. $\square$

Plan wykładu

Trzy pytania

Pytanie 1

Ile jest liczb pierwszych ?

Pytanie 2

Czy znany jest wzór na n-tą liczbę pierwszą ?

Pytanie 3

Jakie zastosowania praktyczne mają liczby pierwsze ?

Trzy pytania

Pytanie 1

Ile jest liczb pierwszych ?

Pytanie 2

Czy znany jest wzór na n-tą liczbę pierwszą ?

Pytanie 3

Jakie zastosowania praktyczne mają liczby pierwsze ?

Trzy pytania

Pytanie 1

Ile jest liczb pierwszych ?

Pytanie 2

Czy znany jest wzór na n-tą liczbę pierwszą ?

Pytanie 3

Jakie zastosowania praktyczne mają liczby pierwsze ?

Odpowiedź na **Pytanie 1**

Twierdzenie (Euklides, VII księga *Elementów*)
Istnieje nieskończenie wiele liczb pierwszych.

Dowód Ten dowód przypisuje się Euklidesowi. Bez wątpienia jest jednym z ładniejszych dowodów, które poznajemy na wykładach z teorii liczb. Wspomnijmy w tym miejscu, że znanych jest około 80 różnych dowodów tego twierdzenia.

Załóżmy, że istnieje tylko skończenie wiele liczb pierwszych: p_1, p_2, $\ldots$, p_n. Pomysł Euklidesa sprowadza się do rozważenia własności liczby $N = p_1 p_2 \ldots p_n + 1$.

Liczba N nie jest liczbą pierwszą, ponieważ $N > p_1, p_2, \ldots, p_n$.

Odpowiedź na **Pytanie 1**

Twierdzenie (Euklides, VII księga *Elementów*)
Istnieje nieskończenie wiele liczb pierwszych.

Dowód Ten dowód przypisuje się Euklidesowi. Bez wątpienia jest jednym z ładniejszych dowodów, które poznajemy na wykładach z teorii liczb. Wspomnijmy w tym miejscu, że znanych jest około 80 różnych dowodów tego twierdzenia.

Załóżmy, że istnieje tylko skończenie wiele liczb pierwszych: p_1, p_2, $\ldots$, p_n. Pomysł Euklidesa sprowadza się do rozważenia własności liczby $N = p_1 p_2 \ldots p_n + 1$.

Liczba N nie jest liczbą pierwszą, ponieważ $N > p_1, p_2, \ldots, p_n$.

Odpowiedź na **Pytanie 1**

Twierdzenie (Euklides, VII księga *Elementów*)
Istnieje nieskończenie wiele liczb pierwszych.

Dowód Ten dowód przypisuje się Euklidesowi. Bez wątpienia jest jednym z ładniejszych dowodów, które poznajemy na wykładach z teorii liczb. Wspomnijmy w tym miejscu, że znanych jest około 80 różnych dowodów tego twierdzenia.

Załóżmy, że istnieje tylko skończenie wiele liczb pierwszych: p_1, p_2, $\ldots$, p_n. Pomysł Euklidesa sprowadza się do rozważenia własności liczby $N = p_1 p_2 \ldots p_n + 1$.

Liczba N nie jest liczbą pierwszą, ponieważ $N > p_1, p_2, \ldots, p_n$.

Odpowiedź na **Pytanie 1**

Twierdzenie (Euklides, VII księga *Elementów*)
Istnieje nieskończenie wiele liczb pierwszych.

Dowód Ten dowód przypisuje się Euklidesowi. Bez wątpienia jest jednym z ładniejszych dowodów, które poznajemy na wykładach z teorii liczb. Wspomnijmy w tym miejscu, że znanych jest około 80 różnych dowodów tego twierdzenia.

Załóżmy, że istnieje tylko skończenie wiele liczb pierwszych: p_1, p_2, $\ldots$, p_n. Pomysł Euklidesa sprowadza się do rozważenia własności liczby $N = p_1 p_2 \ldots p_n + 1$.

Liczba N nie jest liczbą pierwszą, ponieważ $N > p_1, p_2, \ldots, p_n$.

Na mocy Podstawowego Twierdzenia Arytmetyki wiemy, że N dzieli się przez liczbę pierwszą. Zatem co najmniej jedna z liczb $p_1, p_2, \ldots, p_n$ dzieli liczbę N. To jest jednak wykluczone, ponieważ jeśli $p_i|N$, to $p_i|1$, a $p_i > 2$ jako liczba pierwsza. Wynika z tego, że

Liczba N nie jest liczbą złożoną.

Podsumujmy. Założenie, że jest tylko skończenie wiele liczb pierwszych doprowadziło nas do konkluzji, że liczba N, nie jest ani liczbą pierwszą, ani liczbą złożoną. Istnienie liczby o takiej własności przeczy **PTA**. Zatem

Istnieje nieskończenie wiele liczb pierwszych. □

W dowodzie Euklidesa zastosowaliśmy *metodę dowodu niewprost*, która jest jedną z najważniejszych metod dowodowych w całej matematyce. Jej wprowadzenie przypisuje się Arystotelesowi.

Na mocy Podstawowego Twierdzenia Arytmetyki wiemy, że N dzieli się przez liczbę pierwszą. Zatem co najmniej jedna z liczb $p_1, p_2, \ldots, p_n$ dzieli liczbę N. To jest jednak wykluczone, ponieważ jeśli $p_i|N$, to $p_i|1$, a $p_i > 2$ jako liczba pierwsza. Wynika z tego, że

Liczba N nie jest liczbą złożoną.

Podsumujmy. Założenie, że jest tylko skończenie wiele liczb pierwszych doprowadziło nas do konkluzji, że liczba N, nie jest ani liczbą pierwszą, ani liczbą złożoną. Istnienie liczby o takiej własności przeczy **PTA**. Zatem

Istnieje nieskończenie wiele liczb pierwszych. □

W dowodzie Euklidesa zastosowaliśmy *metodę dowodu niewprost*, która jest jedną z najważniejszych metod dowodowych w całej matematyce. Jej wprowadzenie przypisuje się Arystotelesowi.

Na mocy Podstawowego Twierdzenia Arytmetyki wiemy, że N dzieli się przez liczbę pierwszą. Zatem co najmniej jedna z liczb $p_1, p_2, \ldots, p_n$ dzieli liczbę N. To jest jednak wykluczone, ponieważ jeśli $p_i|N$, to $p_i|1$, a $p_i > 2$ jako liczba pierwsza. Wynika z tego, że

Liczba N nie jest liczbą złożoną.

Podsumujmy. Założenie, że jest tylko skończenie wiele liczb pierwszych doprowadziło nas do konkluzji, że liczba N, nie jest ani liczbą pierwszą, ani liczbą złożoną. Istnienie liczby o takiej własności przeczy **PTA**. Zatem

Istnieje nieskończenie wiele liczb pierwszych. □

W dowodzie Euklidesa zastosowaliśmy *metodę dowodu niewprost*, która jest jedną z najważniejszych metod dowodowych w całej matematyce. Jej wprowadzenie przypisuje się Arystotelesowi.

Na mocy Podstawowego Twierdzenia Arytmetyki wiemy, że N dzieli się przez liczbę pierwszą. Zatem co najmniej jedna z liczb $p_1, p_2, \ldots, p_n$ dzieli liczbę N. To jest jednak wykluczone, ponieważ jeśli $p_i|N$, to $p_i|1$, a $p_i > 2$ jako liczba pierwsza. Wynika z tego, że

Liczba N nie jest liczbą złożoną.

Podsumujmy. Założenie, że jest tylko skończenie wiele liczb pierwszych doprowadziło nas do konkluzji, że liczba N, nie jest ani liczbą pierwszą, ani liczbą złożoną. Istnienie liczby o takiej własności przeczy **PTA**. Zatem

Istnieje nieskończenie wiele liczb pierwszych. □

W dowodzie Euklidesa zastosowaliśmy *metodę dowodu niewprost*, która jest jedną z najważniejszych metod dowodowych w całej matematyce. Jej wprowadzenie przypisuje się Arystotelesowi.

Na mocy Podstawowego Twierdzenia Arytmetyki wiemy, że N dzieli się przez liczbę pierwszą. Zatem co najmniej jedna z liczb $p_1, p_2, \ldots, p_n$ dzieli liczbę N. To jest jednak wykluczone, ponieważ jeśli $p_i|N$, to $p_i|1$, a $p_i > 2$ jako liczba pierwsza. Wynika z tego, że

Liczba N nie jest liczbą złożoną.

Podsumujmy. Założenie, że jest tylko skończenie wiele liczb pierwszych doprowadziło nas do konkluzji, że liczba N, nie jest ani liczbą pierwszą, ani liczbą złożoną. Istnienie liczby o takiej własności przeczy **PTA**. Zatem

Istnieje nieskończenie wiele liczb pierwszych. □

W dowodzie Euklidesa zastosowaliśmy *metodę dowodu niewprost*, która jest jedną z najważniejszych metod dowodowych w całej matematyce. Jej wprowadzenie przypisuje się Arystotelesowi.

Odpowiedź na **Pytanie 2**

NIE, nie znamy takiego wzoru, który pozwalałby skutecznie wyliczać kolejne liczby pierwsze p_n w zależności od n.

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots,\ p_{1000} = 7919, \ldots,$
$p_{10^6} = 15485863,\ \ldots,\ p_{10^{12}} = 29996224275833,\ \ldots$.

Liczby pierwsze rozłożone są wśród liczb całkowitych dodatnich w sposób bardzo przypadkowy. Na przykład, po liczbie 370261 kolejne 111 liczb są to liczby złożone. W jednym z zadań, które rozwiążemy wspólnie, dla każdej liczby całkowitej dodatniej k wyznaczymy znacznie większą liczbę n_k taką, że po n_k następuje kolejnych k liczb złożonych.

Relację pomiędzy liczbami n oraz p_n bada się od około 200 lat w analitycznej teorii liczb, która wykorzystuje bardzo złożony technicznie aparat matematyczny. Na zakończenie wymienimy tylko dwa fakty z tej pięknej dziedziny matematyki, które mówią coś na temat p_n

Odpowiedź na **Pytanie 2**

NIE, nie znamy takiego wzoru, który pozwalałby skutecznie wyliczać kolejne liczby pierwsze p_n w zależności od n.

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots,\ p_{1000} = 7919, \ldots,$
$p_{10^6} = 15485863,\ \ldots,\ p_{10^{12}} = 29996224275833,\ \ldots\ .$

Liczby pierwsze rozłożone są wśród liczb całkowitych dodatnich w sposób bardzo przypadkowy. Na przykład, po liczbie 370261 kolejne 111 liczb są to liczby złożone. W jednym z zadań, które rozwiążemy wspólnie, dla każdej liczby całkowitej dodatniej k wyznaczymy znacznie większą liczbę n_k taką, że po n_k następuje kolejnych k liczb złożonych.

Relację pomiędzy liczbami n oraz p_n bada się od około 200 lat w analitycznej teorii liczb, która wykorzystuje bardzo złożony technicznie aparat matematyczny. Na zakończenie wymienimy tylko dwa fakty z tej pięknej dziedziny matematyki, które mówią coś na temat p_n

Odpowiedź na **Pytanie 2**

NIE, nie znamy takiego wzoru, który pozwalałby skutecznie wyliczać kolejne liczby pierwsze p_n w zależności od n.

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots,\ p_{1000} = 7919, \ldots,$
$p_{10^6} = 15485863,\ \ldots,\ p_{10^{12}} = 29996224275833,\ \ldots$.

Liczby pierwsze rozłożone są wśród liczb całkowitych dodatnich w sposób bardzo przypadkowy. Na przykład, po liczbie 370261 kolejne 111 liczb są to liczby złożone. W jednym z zadań, które rozwiążemy wspólnie, dla każdej liczby całkowitej dodatniej k wyznaczymy znacznie większą liczbę n_k taką, że po n_k następuje kolejnych k liczb złożonych.

Relację pomiędzy liczbami n oraz p_n bada się od około 200 lat w analitycznej teorii liczb, która wykorzystuje bardzo złożony technicznie aparat matematyczny. Na zakończenie wymienimy tylko dwa fakty z tej pięknej dziedziny matematyki, które mówią coś na temat p_n

Odpowiedź na **Pytanie 2**

NIE, nie znamy takiego wzoru, który pozwalałby skutecznie wyliczać kolejne liczby pierwsze p_n w zależności od n.

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots,\ p_{1000} = 7919, \ldots,$
$p_{10^6} = 15485863,\ \ldots,\ p_{10^{12}} = 29996224275833,\ \ldots$.

Liczby pierwsze rozłożone są wśród liczb całkowitych dodatnich w sposób bardzo przypadkowy. Na przykład, po liczbie 370261 kolejne 111 liczb są to liczby złożone. W jednym z zadań, które rozwiążemy wspólnie, dla każdej liczby całkowitej dodatniej k wyznaczymy znacznie większą liczbę n_k taką, że po n_k następuje kolejnych k liczb złożonych.

Relację pomiędzy liczbami n oraz p_n bada się od około 200 lat w analitycznej teorii liczb, która wykorzystuje bardzo złożony technicznie aparat matematyczny. Na zakończenie wymienimy tylko dwa fakty z tej pięknej dziedziny matematyki, które mówią coś na temat p_n

Twierdzenie o liczbach pierwszych z 1896 roku pozwala przybliżać $p_n \approx n \ln n$, gdzie $\ln n$ oznacza *logarytm naturalny z liczby* n, którego wartość w przybliżeniu równa jest liczbie cyfr znaczących w zapisie dziesiętnym liczby n.

Posługując się tym przybliżeniem obliczamy
$p_{1000} \approx 6907 \quad (-13\%)$
$p_{10^6} \approx 13815510 \quad (-10\%)$
$p_{10^{12}} \approx 27631021115928 \quad (-8\%)$
(w nawiasach podałem błąd przybliżenia).

Nierozwiązana do dnia dzisiejszego hipoteza Riemanna z 1859 roku implikuje istnienie formuł dokładnych za pomocą, których możnaby dokładniej obliczać p_n, na przykład
$p_{1000} \approx 7773 \quad (-1,8\%)$
$p_{10^6} \approx 15479084 \quad (-0,4\%)$
$p_{10^{12}} \approx 299462470277 \quad (-0,0002\%)$.

Twierdzenie o liczbach pierwszych z 1896 roku pozwala przybliżać $p_n \approx n \ln n$, gdzie $\ln n$ oznacza *logarytm naturalny z liczby* n, którego wartość w przybliżeniu równa jest liczbie cyfr znaczących w zapisie dziesiętnym liczby n.

Posługując się tym przybliżeniem obliczamy
$p_{1000} \approx 6907 \qquad (-13\%)$
$p_{10^6} \approx 13815510 \qquad (-10\%)$
$p_{10^{12}} \approx 27631021115928 \qquad (-8\%)$
(w nawiasach podałem błąd przybliżenia).

Nierozwiązana do dnia dzisiejszego hipoteza Riemanna z 1859 roku implikuje istnienie formuł dokładnych za pomocą, których możnaby dokładniej obliczać p_n, na przykład
$p_{1000} \approx 7773 \qquad (-1,8\%)$
$p_{10^6} \approx 15479084 \qquad (-0,4\%)$
$p_{10^{12}} \approx 29946247027 \qquad (-0,0002\%).$

Twierdzenie o liczbach pierwszych z 1896 roku pozwala przybliżać $p_n \approx n \ln n$, gdzie $\ln n$ oznacza *logarytm naturalny z liczby* n, którego wartość w przybliżeniu równa jest liczbie cyfr znaczących w zapisie dziesiętnym liczby n.

Posługując się tym przybliżeniem obliczamy
$p_{1000} \approx 6907 \qquad (-13\%)$
$p_{10^6} \approx 13815510 \qquad (-10\%)$
$p_{10^{12}} \approx 27631021115928 \qquad (-8\%)$
(w nawiasach podałem błąd przybliżenia).

Nierozwiązana do dnia dzisiejszego hipoteza Riemanna z 1859 roku implikuje istnienie formuł dokładnych za pomocą, których możnaby dokładniej obliczać p_n, na przykład
$p_{1000} \approx 7773 \qquad (-1,8\%)$
$p_{10^6} \approx 15479084 \qquad (-0,4\%)$
$p_{10^{12}} \approx 299462470277 \qquad (-0,0002\%).$

Odpowiedź na **Pytanie 3**

Istnieją istotne zastosowania liczb pierwszych w naszym życiu codziennnym, chociażby wspomniane już protokóły kryptograficzne pozwalające bezpiecznie poruszać się w Internecie.

Duże liczby pierwsze znajdują także zastosowanie przy budowie dużych sieci telekomunikacyjnych (np. w telefonii komórkowej), które posiadają możliwość automatycznej korekty błędów transmisji oraz wyboru wielu nie kolidujących kanałów komunikacji.

Z drugiej strony, warto pamiętać o tym, że to nie zastosowania praktyczne stanowią główną przyczynę zainteresowania liczbami pierwszymi, i liczbami w ogóle. Ludzie od wielu lat badają własności liczb całkowitych, po prostu dlatego, że kieruje nimi *naturalna ludzka ciekawość*, która stanowi podstawę każdej dziedziny naszej wiedzy, w tym także matematyki.

Odpowiedź na **Pytanie 3**

Istnieją istotne zastosowania liczb pierwszych w naszym życiu codziennnym, chociażby wspomniane już protokóły kryptograficzne pozwalające bezpiecznie poruszać się w Internecie.

Duże liczby pierwsze znajdują także zastosowanie przy budowie dużych sieci telekomunikacyjnych (np. w telefonii komórkowej), które posiadają możliwość automatycznej korekty błędów transmisji oraz wyboru wielu nie kolidujących kanałów komunikacji.

Z drugiej strony, warto pamiętać o tym, że to nie zastosowania praktyczne stanowią główną przyczynę zainteresowania liczbami pierwszymi, i liczbami w ogóle. Ludzie od wielu lat badają własności liczb całkowitych, po prostu dlatego, że kieruje nimi *naturalna ludzka ciekawość*, która stanowi podstawę każdej dziedziny naszej wiedzy, w tym także matematyki.

Odpowiedź na **Pytanie 3**

Istnieją istotne zastosowania liczb pierwszych w naszym życiu codziennnym, chociażby wspomniane już protokóły kryptograficzne pozwalające bezpiecznie poruszać się w Internecie.

Duże liczby pierwsze znajdują także zastosowanie przy budowie dużych sieci telekomunikacyjnych (np. w telefonii komórkowej), które posiadają możliwość automatycznej korekty błędów transmisji oraz wyboru wielu nie kolidujących kanałów komunikacji.

Z drugiej strony, warto pamiętać o tym, że to nie zastosowania praktyczne stanowią główną przyczynę zainteresowania liczbami pierwszymi, i liczbami w ogóle. Ludzie od wielu lat badają własności liczb całkowitych, po prostu dlatego, że kieruje nimi *naturalna ludzka ciekawość*, która stanowi podstawę każdej dziedziny naszej wiedzy, w tym także matematyki.