Rozszerz swoje horyzonty

Tomasz Zamek-Gliszczyński

MATEMATYKA

dla dociekliwych licealistów

Zadania i nie tylko

Część I

LICZBY
FUNKCJE
CIĄGI
KOMBINATORYKA
GEOMETRIA PŁASKA
TRYGONOMETRIA
GEOMETRIA ANALITYCZNA

Spis treści

Część I

Wstęp 4
1. LICZBY 5
2. FUNKCJE 23
3. CIĄGI 37
4. KOMBINATORYKA 54
5. GEOMETRIA PŁASKA 59
6. TRYGONOMETRIA 69
7. GEOMETRIA ANALITYCZNA 81
Rozwiązania zadań 126

Część II

8. STEREOMETRIA
9. PRAWDOPODOBIEŃSTWO I STATYSTYKA
10. RACHUNEK RÓŻNICZKOWY I CAŁKOWY
Rozwiązania zadań

Wstęp

Wszystko, co zawiera niniejsza książka, zdarzyło się w szkole. Z niektórymi tematami uczniowie zgłaszali się sami, bo ich interesowały, niektóre tematy ja rozwijałem na lekcjach, nie tyle rozszerzając nasz polski program, co wkładając go w nieco inny kontekst matematyczny. Uczniowie sycili tymi tematami swoją ciekawość, a ja będę długo pamiętał te momenty, kiedy widziałem ich radość poznania i zrozumienia różnych, nowych konstrukcji matematycznych.

Nad niektórymi tematami pracuję z uczniami od wielu lat. W każdej kolejnej grupie uczniów, niezależnie od etykietek, jakie im przyznawano, zainteresowanie jest podstawą dobrej nauki. Oczywiście, każdy temat można zrobić dowolnie trudnym. Staram się przedstawiać kolejne tematy w przystępny sposób, ale ciągle dostrzegam fragmenty, które planuję za rok zrobić lepiej, zręczniej, żeby ich nauka była ciekawsza, łatwiejsza, skuteczniejsza.

Ta książka jest podsumowaniem takich właśnie wysiłków.

Tematy są uporządkowane w kolejności podobnej do kolejności działów podstawy programowej. Każdy rozdział jednak różni się i pod względem stylu, i pod względem stopniowania trudności. W części I znalazło się 7 rozdziałów, a w części II – pozostałe 3 rozdziały.

Trudno nie znać algorytmu Euklidesa i paru jego zastosowań, w geometrii – twierdzenia Menelaosa czy twierdzenia Cevy. Nie można nie znać indukcji matematycznej. Geometria trójwymiarowa nie powinna ograniczać się do graniastosłupów i ostrosłupów oraz kul i walców. Nie można nie znać podstaw rachunku różniczkowego i całkowego, w szczególności rachunku całkowego. To nie jest w porządku, że Polska jest dość wyjątkowym krajem w Europie, w którym uczniowie mają programowo nie znać całek.

W moim nauczaniu jest ukryty pewien program. Chciałbym, żeby nauka matematyki polegała w większym stopniu na nauczaniu właśnie matematyki, a nie żeby polegała tylko na przygotowaniu do egzaminu.

Gdy bardziej znasz matematykę, gdy rozumiesz więcej niż wymagają arkusze egzaminacyjne, lepiej dostosujesz się do wymagań egzaminacyjnych. Będziesz dużo skuteczniejszy. Gdy jesteś w klasie maturalnej, czyż nie patrzysz „z góry" na matematykę ze szkoły podstawowej? Jakie to było łatwe...

Życzę Wam, żebyście na każdy egzamin z matematyki mogli spojrzeć z góry jeszcze przed nim. Wymagajcie od siebie dużo, nawet gdyby inni tego od Was nie wymagali.

Autor

Podziękowania

Chciałbym bardzo serdecznie podziękować redaktorowi Jankowi Baranowskiemu za wsparcie i mobilizację.

Chciałbym też podziękować moim uczniom, którzy swoimi zainteresowaniami w dużym stopniu kierowali mnie w stronę tematów tej książki.

1. LICZBY

Liczby naturalne $N = \{0, 1, 2, 3, \ldots\}$
Liczby całkowite $Z = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$
Liczby wymierne $Q = \left\{ \frac{p}{q} : p \in Z, q \in Z \text{ i } q \neq 0 \right\}$

Liczby niewymierne to te liczby, które nie dadzą się przedstawić w postaci ułamka mającego i w liczniku, i w mianowniku liczbę całkowitą.
Liczby wymierne i niewymierne razem tworzą zbiór liczb **rzeczywistych** R.

Uwaga. W podręcznikach szkolnych liczby całkowite oznaczane są przez C, wymierne przez W, ale w książkach akademickich wymierne są Q, a całkowite Z, tak jak w całej światowej literaturze.

Liczby całkowite. Dzielenie z resztą

Twierdzenie 1.1 (o dzieleniu z resztą)
Dla dowolnych dwóch liczb całkowitych a i b, $b \neq 0$, istnieje dokładnie jedna liczba całkowita q i dokładnie jedna liczba całkowita r, $0 \leq r < |b|$, że $a = q \cdot b + r$.

Liczba q jest **ilorazem dzielenia** a przez b, a liczbę r nazywamy **resztą** z tego dzielenia.
Jeśli $r = 0$, to mówimy, że a dzieli się przez b bez reszty.

Oznaczenie. Fakt, że liczba całkowita a dzieli liczbę całkowitą b bez reszty, zapisujemy $a \mid b$.

Przykład 1.1

a) Oblicz resztę z dzielenia 14 przez –3.
b) Oblicz resztę z dzielenia 14 przez 3.
c) Oblicz resztę z dzielenia –14 przez 3.
d) Oblicz resztę z dzielenia –14 przez –3.

Rozwiązanie

a) $14 = -4 \cdot (-3) + 2$. Ilorazem jest –4, resztą 2.
b) $14 = 4 \cdot 3 + 2$. Ilorazem jest 4, a resztą 2.
c) $-14 = -5 \cdot 3 + 1$. Ilorazem jest –5, a resztą 1.
d) $-14 = 5 \cdot (-3) + 1$. Ilorazem jest 5, a resztą 1.

Własności dzielenia z resztą
$\mathbf{W_1}$ Reszta nie jest liczbą ujemną.
$\mathbf{W_2}$ Reszta z dzielenia a przez b jest taka sama jak reszta z dzielenia a przez $-b$.
$\mathbf{W_3}$ Jeśli ilorazem dzielenia a przez b jest q, to ilorazem dzielenia a przez $-b$ jest $-q$.
$\mathbf{W_4}$ Reszta z dzielenia a przez b się nie zmieni, jeśli do a dodamy dowolną wielokrotność liczby b.
$\mathbf{W_5}$ Jeśli resztą z dzielenia a przez c jest r_1, a resztą z dzielenia b przez c jest r_2, to przy dzieleniu przez c
(i) $a+b$ i r_1+r_2 mają te same reszty
(ii) $a-b$ i r_1-r_2 mają te same reszty
(iii) ab i r_1r_2 mają te same reszty.

Dowód
$\mathbf{W_1}$. W określeniu reszty r z dzielenia a przez b jest nierówność $0 \le r < |b|$.
$\mathbf{W_2}$ i $\mathbf{W_3}$. Skoro $a = qb + r$, to $a = -q(-b) + r$.
$\mathbf{W_4}$. Niech k będzie dowolną liczbą całkowitą. Jeśli $a = qb + r$,
to $a - kb = (q-k)\,b + r$.
$\mathbf{W_5}$. Oznaczmy $a = q_1c + r_1$, $b = q_2c + r_2$.

$$a+b = q_1c + q_2c + r_1 + r_2 = (q_1+q_2)c + r_1 + r_2$$
$$a-b = q_1c - q_2c + r_1 - r_2 = (q_1-q_2)c + r_1 - r_2$$
$$a \cdot b = (q_1c + r_1)(q_2c + r_2) = q_1q_2c^2 + q_1r_2c + q_2r_1c + r_1r_2 =$$
$$= (q_1q_2c + q_1r_2 + q_2r_1)c + r_1r_2$$

Prawa strona różni się od lewej o pewną wielokrotność c. ■

Przykład 1.2

Oblicz resztę z dzielenia $2^{100} + 3^{100}$ przez 5.

Rozwiązanie

Chodzi o resztę z dzielenia przez 5 liczby $2^{100} + 3^{100} = 16^{25} + 81^{25}$. Stosując $\mathbf{W_3}$ do 25 czynników, możemy 16 zastąpić przez 1 i podobnie 81 przez 1. Stosując $\mathbf{W_1}$, otrzymujemy resztę 2.
Analogicznie można pokazać, że $3^{100} - 2^{100}$ dzieli się przez 5.

Definicja 1.1

Jeśli a i b mają te same reszty z dzielenia przez c, to piszemy $a \equiv^c b$.

1.1. Oblicz resztę z dzielenia przez 5 liczby
a) $3^{101} - 2^{101}$
b) $3^{102} - 2^{102}$
c) $3^{103} - 2^{103}$
d) $3^{104} - 2^{104}$
e) $3^{105} - 2^{105}$

Dzielniki i wielokrotności. Indukcja matematyczna

Definicja 1.2

Liczbę naturalną dodatnią nazywamy **liczbą złożoną**, jeśli można ją przedstawić jako iloczyn dwóch dodatnich liczb naturalnych większych od 1.
Liczbę naturalną dodatnią nazywamy **liczbą pierwszą**, jeśli jest większa od 1 i nie można jej przedstawić jako iloczyn dwóch dodatnich liczb naturalnych większych od 1.

Najmniejszą liczbą złożoną jest 4, a najmniejszą liczbą pierwszą jest 2. Liczba 1 nie jest liczbą złożoną, ale też nie jest liczbą pierwszą.
Uwaga. Liczbę naturalną złożoną można też zdefiniować równoważnie, że jest to taka liczba naturalna, która da się przedstawić jako iloczyn dwóch liczb naturalnych mniejszych od niej.

Zasada dobrego uporządkowania liczb naturalnych
Każdy niepusty podzbiór zbioru liczb naturalnych ma element najmniejszy.

Tę własność zbioru liczb naturalnych przyjmuje się za oczywistą.
Nieujemne liczby wymierne i nieujemne liczby rzeczywiste nie są dobrze uporządkowane, bo zbiór $\left\{1, \frac{1}{2}, \frac{1}{3}, \ldots\right\}$ nie ma elementu najmniejszego.

Twierdzenie 1.2 (o rozkładzie na czynniki pierwsze)
Każda liczba naturalna większa od 1 albo jest liczbą pierwszą, albo da się przedstawić jako iloczyn liczb pierwszych.
Dowód
Zastosujemy zasadę dobrego uporządkowania.
Oznaczmy przez A zbiór tych liczb naturalnych większych lub równych 2, dla których twierdzenie jest nieprawdziwe. Nie ma w nim ani jednej liczby pierwszej, bo dla liczb pierwszych twierdzenie jest spełnione. Ale jeśli ten zbiór jest niepusty, to istnieje w nim element najmniejszy. Nazwijmy tę najmniejszą liczbę m. Jest to liczba złożona, która nie ma rozkładu na czynniki pierwsze. Można ją jednak rozłożyć na iloczyn dwóch mniejszych od niej liczb i jednocześnie większych od jeden. Nazwijmy je a i b. Tak więc $m = ab$. Liczby a i b albo obie są pierwsze, albo tylko jedna z tych liczb jest pierwsza, albo obie są złożone. Jeśli obie są pierwsze, to wtedy jest sprzeczność, bo m zostałoby rozłożone na czynniki pierwsze. Jeśli jedna jest pierwsza, a druga złożona, to ta złożona jako mniejsza od m ma rozkład na czynniki pierwsze. Znowu sprzeczność, bo m dało się rozłożyć na czynniki pierwsze. W ostatnim przypadku i a, i b są złożone i mniejsze od m, więc obie mają rozkład

na czynniki pierwsze, skąd m ma rozkład na czynniki pierwsze. Też sprzeczność. Zbiór A jest więc pusty. Wszystkie liczby naturalne spełniają twierdzenie: albo są pierwsze, albo rozkładają się na czynniki pierwsze. ■

Twierdzenie 1.3 (indukcja matematyczna)
Przypuśćmy, że pewien zbiór A liczb naturalnych $\boldsymbol{N}$ ma następujące dwie własności:

1. 0 jest elementem zbioru A ($0 \in A$)
2. Dla każdej liczby k należącej do A liczba $k + 1$ należy do A

wtedy $A = N$.

Dowód

Dowód opiera się na zasadzie dobrego uporządkowania.
Oznaczmy przez B zbiór tych liczb naturalnych, które nie są w A. Jeśli zbiór B jest niepusty, to zawiera element najmniejszy, który nie jest zerem. Nazwijmy go m. Wobec tego $m - 1$ jest elementem A. Jeśli $m - 1$ jest elementem A, to i m jest elementem A. Wobec tego m jest i elementem A i B. Niemożliwe. Przypuszczenie, że zbiór B jest niepusty prowadzi do sprzeczności. W A są wszystkie liczby naturalne. ■

Uwaga. Zdarza się, że chcemy coś udowodnić dla na przykład $n = 3, 4, 5, \ldots$ Wtedy zastępujemy 0 przez 3 i zbiorem A jest $\{3, 4, 5, \ldots\}$.

Przykład 1.3

Udowodnij, że $41^{2n} + 13^{2n} - 2$ jest podzielne przez 168 dla dowolnego $n = 0, 1, 2, 3, \ldots$

Dowód (przez indukcję)
Oznaczmy przez A zbiór tych liczb naturalnych n, dla których $41^{2n} + 13^{2n} - 2$ jest podzielne przez 168.

1. $n = 0$
   $41^{2 \cdot 0} + 13^{2 \cdot 0} - 2 = 1 + 1 - 2 = 0$ jest podzielne przez 168. $0 \in A$.
2. Załóżmy, że $k \in A$. Wtedy
   $41^{2(k+1)} + 13^{2(k+1)} - 2 = 41^2 \cdot 41^{2k} + 13^2 \cdot 13^{2k} - 2 =$
   $= 13^2 \cdot 41^{2k} + 13^2 \cdot 13^{2k} - 13^2 \cdot 2 + 13^2 \cdot 2 + (41^2 - 13^2) \cdot 41^{2k} - 2 =$
   $= 13^2(41^{2k} + 13^{2k} - 2) + 13^2 \cdot 2 + (41^2 - 13^2) \cdot 41^{2k} - 2 =$
   $= 13^2(41^{2k} + 13^{2k} - 2) + 2 \cdot (13^2 - 1) + (41 - 13)(41 + 13) \cdot 41^{2k} =$
   $= 13^2(41^{2k} + 13^{2k} - 2) + 2 \cdot 12 \cdot 14 + 28 \cdot (41 + 13) \cdot 41^{2k} =$
   $= 13^2(41^{2k} + 13^{2k} - 2) + 28 \cdot (12 + 54 \cdot 41^{2k}) =$
   $= 13^2(41^{2k} + 13^{2k} - 2) + 28 \cdot 6 \cdot (2 + 9 \cdot 41^{2k}) =$
   $= 13^2(41^{2k} + 13^{2k} - 2) + 168 \cdot (2 + 9 \cdot 41^{2k})$
   $41^{2k} + 13^{2k} - 2$ jest podzielne przez 168, bo $k \in A$. $168 \cdot (2 + 9 \cdot 41^{2k})$ jest oczywiście podzielne przez 168, a więc $41^{2(k+1)} + 13^{2(k+1)} - 2$ jest podzielne przez 168. $k + 1 \in A$.

3. Na mocy indukcji $A = N$. Inaczej mówiąc: dla każdego $n = 0, 1, 2, \ldots$ wyrażenie $41^{2n} + 13^{2n} - 2$ jest podzielne przez 168. ■

Czasami potrzebna jest tak zwana zasada indukcji zupełnej.

Twierdzenie 1.4 (zupełna indukcja matematyczna)
Przypuśćmy, że pewien zbiór A liczb naturalnych N ma następujące dwie własności:

1. 0 jest elementem zbioru A ($0 \in A$)
2. dla każdej liczby naturalnej k jeśli liczby $0, 1, 2, \ldots, k-1$ są elementami A, to k jest elementem A

wtedy $A = N$.

Dowód

Dowód opiera się na zasadzie dobrego uporządkowania.
Oznaczmy przez B zbiór tych liczb naturalnych, które nie są w A. Jeśli zbiór B jest niepusty, to zawiera element najmniejszy, który nie jest zerem. Nazwijmy go m. Wobec tego $0, 1, 2, \ldots, m-2, m-1$ są elementami A. Ale jeśli tak, to na mocy (2) m jest elementem A. Wobec tego m jest i elementem A i B. Niemożliwe. Przypuszczenie, że zbiór B jest niepusty, prowadzi do sprzeczności. W A są wszystkie liczby naturalne. ■

Uwaga. Zdarza się, że warto indukcję zacząć nie od 0, ale na przykład od 3 – z oczywistymi modyfikacjami.

Przykład 1.4

Ciąg a_n, $n = 1, 2, 3, \ldots$, jest zdefiniowany następująco:
$a_1 = 1$, $a_2 = 3$, $a_3 = 5$ i dla $n > 3$ zachodzi równość $a_n = a_{n-1} + a_{n-2} + a_{n-3}$. Udowodnij, że wszystkie wyrazy tego ciągu są nieparzyste.

Dowód (przez indukcję zupełną)
Oznaczmy przez A zbiór tych liczb naturalnych n, $n > 3$, dla których a_n jest liczbą nieparzystą.

1. a_1, a_2, a_3 są nieparzyste, więc 1, 2 i 3 są w A.
2. Weźmy teraz dowolną liczbę $k > 3$ i załóżmy, że $a_1, a_2, \ldots, a_{k-1}$ są elementami A. Wtedy
   $a_k = a_{k-1} + a_{k-2} + a_{k-3}$ jest sumą trzech liczb nieparzystych, wobec tego jest liczbą nieparzystą. Tak, więc k jest elementem A.
3. Na mocy indukcji zupełnej $A = \{1, 2, 3, \ldots\}$, czyli wszystkie wyrazy ciągu a_n, $n = 1, 2, 3, \ldots$ są nieparzyste. ■

Zbiór dzielników liczby naturalnej

Na przykład zbiorem dzielników liczby 12 jest {1, 2, 3, 4, 6, 12}. Zbiór dzielników liczby pierwszej p składa się z dwóch liczb – z jedynki i samej siebie, czyli jest to zbiór $\{1, p\}$.

Liczba 0 jest wyjątkowa. Zbiorem dzielników 0 jest zbiór nieskończony {1, 2, 3, ...}.
Wyjątkowa jest też liczba 1. Jej zbiorem dzielników jest {1}.

Definicja 1.3

Niech a i b będą dowolnymi liczbami naturalnymi, z których przynajmniej jedna jest dodatnia. Każda z nich ma swój zbiór dzielników. Część wspólna tych dwóch zbiorów, czyli zbiór wspólnych dzielników jest niepusty, bo liczba 1 jest w obu zbiorach dzielników. Największa liczba w zbiorze wspólnych dzielników jest właśnie **największym wspólnym dzielnikiem** liczb a i b.
Oznaczamy go $NWD(a, b)$.

Przykład 1.5

Niech $a > 0$.

$NWD(0, 0)$ nie istnieje.
$NWD(a, b) = NWD(b, a)$
$NWD(a, 0) = a$
$NWD(a, a) = a$
Udowodnij:
Jeśli $a \mid b$, to $NWD(a, b) = a$.

Rozwiązanie

Największym dzielnikiem liczby a jest liczba a. Największy wspólny dzielnik a i b nie może być większy niż a, ale właśnie a dzieli również b, więc jest największym wspólnym dzielnikiem liczb a i b.

Definicja 1.4

Jeśli jedynym wspólnym dzielnikiem dodatnich liczb a i b jest liczba 1, to liczby a i b nazywamy **względnie pierwszymi**. Inaczej mówiąc, dodatnie liczby a i b są względnie pierwsze, gdy $NWD(a, b) = 1$.

Twierdzenie 1.5 (lemat[1] Euklidesa)
Niech $a, b \in \boldsymbol{Z}_+$ i niech $a \geq b$. Wtedy
$NWD(a, b) = NWD(a - b, b)$.

Ten lemat można słowami wyrazić tak. Jeśli mamy znaleźć największy wspólny dzielnik dodatnich liczb całkowitych, to możemy je zastąpić mniejszą z nich i różnicą większej i mniejszej, a największy wspólny ich dzielnik będzie taki sam. Powtarzając taki krok, być może więcej razy, możemy znalezienie największego wspólnego dzielnika dwóch dodatnich liczb całkowitych zastąpić znalezieniem

[1] Lemat to zwykle twierdzenie pomocnicze, formułowane jako etap dowodu innego (ważniejszego) twierdzenia.

największego wspólnego dzielnika liczby mniejszej i reszty z dzielenia liczby większej przez mniejszą:

$$NWD(a, b) = NWD(a - kb, b),$$

gdzie k jest ilorazem dzielenia a przez b.
Lemat Euklidesa można więc wzmocnić.

Twierdzenie 1.6 (lemat Euklidesa mocniejszy)
Niech $a, b \in \mathbb{Z}_+$ oraz $a \geq b$. Wtedy dla dowolnej liczby naturalnej k
$NWD(a, b) = NWD(a - k \cdot b, b)$.
Dowód
Wystarczy pokazać, że zbiór wspólnych dzielników liczb a i b jest taki sam jak zbiór wspólnych dzielników liczb $a - kb$ i b.
Pokażemy najpierw, że zbiór wspólnych dzielników liczb a i b jest zawarty w zbiorze wspólnych dzielników liczb $a - kb$ i b. Załóżmy, że liczba c dzieli i a, i b. Wtedy dzieli również $a - kb$. Jest więc wspólnym dzielnikiem liczb a, b i $a - kb$ i b. W szczególności jest więc wspólnym dzielnikiem liczb $a - kb$ i b.
Teraz pokażemy, że zbiór wspólnych dzielników liczb $a - kb$ i b jest zawarty w zbiorze wspólnych dzielników liczb a i b. Załóżmy, że liczba c dzieli liczby $a - kb$ i b. Wtedy dzieli również liczbę $(a - kb) + kb = a$, dzieli więc i a, i b, i $a - kb$. W szczególności dzieli a i b. Jest więc wspólnym dzielnikiem liczb a i b.
Pokazaliśmy, że zbiór dzielników liczb a i b i zbiór dzielników liczb b i $a - kb$ są równe. Największy ich element jest tą samą liczbą, która jest jednocześnie $NWD(a, b)$ i $NWD(a - kb, b)$. ■

Algorytm Euklidesa
Dane są dwie nieujemne liczby całkowite a i b, nie obie zerowe, przy czym $a \geq b$. Chcemy znaleźć $d = NWD(a, b)$.

1. Jeśli $b = 0$, to $d = a$. Koniec. Jeśli $b > 0$ idź do kroku 2.
2. Dzielimy większą liczbę przez mniejszą w liczbach całkowitych. Dzielnik i reszta tworzą nową parę, którą nazywamy a i b. Idź do kroku 1.

Przykład 1.6

$$NWD(437, 323) = NWD(323, 437 - 323) = NWD(323, 114) =$$
$$= NWD(114, 323 - 2 \cdot 114) = NWD(114, 323 - 228) = NWD(114, 95) =$$
$$= NWD(95, 114 - 95) = NWD(95, 19) =$$
$$= NWD(19, 95 - 5 \cdot 19) = NWD(19, 0) = 19$$

W następnym przykładzie zobaczymy, jak algorytm Euklidesa poradzi sobie z liczbami $a = 5775$ i $b = 2015$. Od razu widać, że 5 jest wspólnym dzielnikiem obu liczb. Ale czy jest największym?
W lewej i prawej kolumnie używamy symboli a i b.

Przykład 1.7

Używając algorytmu Euklidesa, znajdź $NWD(5775, 2015)$.

Rozwiązanie

Oznaczmy $a = 5775$, $b = 2015$.

a	5775	2015	b
$a - \mathbf{2}b$	$2015 - \mathbf{2} \cdot 2015 = 1745$	2015	b
$a - \mathbf{2}b$	1745	$2015 - 1745 = 270$	$b - \mathbf{1} \cdot (a - 2b) = -a + 3b$
$a - 2b - \mathbf{6}(-a + 3b) = 7a - 20b$	$1745 - \mathbf{6} \cdot 270 = 125$	270	$-a + 3b$
$7a - 20b$	125	$270 - \mathbf{2} \cdot 125 = 20$	$-a + 3b - \mathbf{2}(7a - 20b) = -15a + 43b$
$7a - 20b - \mathbf{6} \cdot (-15a + 43b) = 97a - 278b$	$125 - \mathbf{6} \cdot 20 = 5$	20	$-15a + 43b$
$\mathbf{97}a - \mathbf{278}b$	5	$20 - \mathbf{4} \cdot 5 = 0$	$-15a + 43b - \mathbf{4} \cdot (97a - 278b) = -403a + 1155b$

$NWD(5775, 2015) = 5$. W lewej dolnej komórce tabeli widać, że $NWD(5775, 2015) = \mathbf{97} \cdot 5775 - \mathbf{278} \cdot 2015$.

Definicja 1.5

Liniową kombinacją liczb a i b o współczynnikach całkowitych nazywamy każde wyrażenie postaci $xa + yb$, w którym x i y są liczbami całkowitymi.

Powyższy przykład pokazuje, że $NWD(5775, 2015)$ jest liniową kombinacją o współczynnikach całkowitych liczb 5775 i 2015.

Spróbujmy jeszcze raz znaleźć $NWD(a, b)$ metodą Euklidesa i zobaczyć, jaką kombinacją liniową liczb a i b jest $NWD(a, b)$.

Przykład 1.8

Znajdź $NWD(5776, 2016)$ i pokaż, jaką kombinacją liniową liczb 5776 i 2016 jest $NWD(5776, 2016)$.

Rozwiązanie

a	5776	2016	b
$a - \mathbf{2}b$	$5776 - \mathbf{2} \cdot 2016 = 1744$	2016	b
$a - \mathbf{2}b$	1744	$2016 - \mathbf{1} \cdot 1744 = 272$	$b - (a - 2b) = -a + 3b$
$a - 2b - \mathbf{6}(-a + 3b) = 7a - 20b$	$1744 - \mathbf{6} \cdot 272 = 112$	272	$-a + 3b$

$7a - 20b$	112	$272 - \mathbf{2} \cdot 112 = 48$	$-a + 3b - \mathbf{2}(7a - 20b) = -15a + 43b$
$7a - 20b - \mathbf{2} \cdot (-15a + 43b) = 37a - 106b$	$112 - \mathbf{2} \cdot 48 = 16$	48	$-15a + 43b$
$37a - 106b$	16	$48 - \mathbf{3} \cdot 16 = 0$	$-15a + 43b - \mathbf{3} \cdot (37a - 106b) = -126a + 361b$

$NWD(5776, 2016) = 16$ i $NWD(5776, 2016) = 37 \cdot 5776 - 106 \cdot 2016$.

Twierdzenie 1.7
Dla dowolnych dwóch nieujemnych liczb a i b, z których przynajmniej jedna jest dodatnia, istnieją takie liczby całkowite x i y, że $NWD(a, b) = xa + yb$.
Dowód
Kolejny krok algorytmu Euklidesa zastępuje wyjściową parę liczb a i b przez „mniejszą" parę liczb a' i b', gdzie $a' \leq a$ i $b' \leq b$ i przynajmniej jedna z tych nierówności jest ostra, przy czym i a', i b' są kombinacjami liniowymi a i b. Następny krok zastępuje parę a' i b' „mniejszą" parą a'' i b'', przy czym i a'', i b'' są kombinacjami liniowymi a' i b'. Kombinacja liniowa kombinacji liniowych liczb a i b jest kombinacją liniową liczb a i b, więc i a'', i b'' są kombinacjami liniowymi a i b. Ostatecznie $NWD(a, b)$ jest kombinacją liniową liczb a i b. ■

Wniosek 1. Niech liczby a i b będą nieujemne i przynajmniej jedna nich niech będzie dodatnia.
Każdy wspólny dzielnik liczb a i b dzieli również $NWD(a, b)$.
Dowód
Wspólny dzielnik liczb a i b dzieli również dowolną kombinację liniową liczb a i b, a więc także liczbę $NWD(a, b)$, która jest pewną kombinacją liniową liczb a i b. ■

Wniosek 2. Zbiór wszystkich dzielników liczby $NWD(a, b)$ jest tym samym zbiorem, co zbiór wspólnych dzielników liczb a i b.
Dowód
Wniosek 1 mówi, że wspólny dzielnik a i b dzieli $NWD(a, b)$.
Natomiast $NWD(a, b)$ dzieli i a i b i jeśli jakaś liczba dzieli $NWD(a, b)$, to dzieli i a, i b, czyli jest wspólnym dzielnikiem a i b. ■

Twierdzenie 1.8 (twierdzenie Bézouta)
Niech a i b będą dwiema nieujemnymi liczbami całkowitymi, z których przynajmniej jedna jest dodatnia. Najmniejsza dodatnia kombinacja liniowa o całkowitych współczynnikach liczb a i b jest równa $NWD(a, b)$.

Dowód
Istnieje przynajmniej jedna kombinacja liniowa liczb a i b, która jest dodatnia, a jest nią na przykład $1 \cdot a + 1 \cdot b = a + b$. Jeśli istnieje przynajmniej jedna dodatnia kombinacja liniowa liczb a i b, to wśród wszystkich dodatnich kombinacji liniowych liczb a i b istnieje najmniejsza dodatnia kombinacja liniowa liczb a i b; oznaczmy taką kombinację przez $xa + yb$. Pokażemy, że $xa + yb$ dzieli a. Jeśli $a = 0$, to $xa + yb$ dzieli a. Przypuśćmy, że $a > 0$. Gdyby $xa + yb$ nie dzieliło liczby a, to z dzielenia a przez $xa + yb$ pozostałaby reszta r, $0 < r < xa + yb$, czyli istniałaby taka liczba całkowita k, że $a = k(xa + yb) + r$. Z tej równości r dałoby się przedstawić następująco $r = (1 - kx) \cdot a - ky \cdot b$, a więc r byłoby dodatnią kombinacją liniową liczb a i b mniejszą od najmniejszej takiej kombinacji. Niemożliwe. A więc $xa + yb$ dzieli a. Powtarzając to samo rozumowanie, dowodzimy, że $xa + by$ dzieli b. Wobec tego $xa + yb$ dzieli i a, i b. Jest więc wspólnym dzielnikiem a i b, czyli $xa + yb \leq NWD(a, b)$, ale $NWD(a, b)$ dzieli i a i b, więc dzieli $xa + yb$, zatem $NWD(a, b) \leq xa + yb$. Tak więc $xa + yb = NWD(a, b)$. ■

Twierdzenie 1.9 (następny lemat Euklidesa)
Jeśli $a \mid bc$ i $NWD(a, b) = 1$, to $a \mid c$.
Dowód
Ponieważ $NWD(a, b) = 1$, więc na mocy twierdzenia 1.7 istnieje taka kombinacja liniowa liczb a i b o współczynnikach całkowitych x i y, że $NWD(a, b) = 1 = xa + yb$. A więc $c = c \cdot 1 = c \cdot (xa + yb) = cx \cdot a + y \cdot bc$. Wobec tego $a \mid c$. ■

Jednoznaczność rozkładu liczby na czynniki pierwsze
Liczba naturalna większa od jeden jest albo pierwsza, albo złożona. Złożona ma rozkład na czynniki pierwsze. To było pokazane wcześniej (twierdzenie 1.2). Jednoznaczność nie była udowodniona.

Twierdzenie 1.10
Rozkład na czynniki pierwsze jest jednoznaczny.
Dowód
Przypuśćmy, że istnieje liczba, która ma dwa różne rozkłady na czynniki pierwsze. Jeśli tak, to istnieje najmniejsza taka liczba (z zasady dobrego uporządkowania). Nazwijmy ją a. A więc $a = p_1p_2...p_n$ i $a = q_1q_2...q_m$, gdzie wszystkie p_i i q_j są liczbami pierwszymi. Żadne p_i nie może się równać jakiemuś q_j, bo wtedy moglibyśmy podzielić liczbę a przez p_i i otrzymalibyśmy liczbę mniejszą od a, która miałaby niejednoznaczny rozkład na czynniki pierwsze. Wobec tego $\{p_1, p_2, ..., p_n\} \cap \{q_1, q_2, ..., q_m\} = \varnothing$. Liczba a dzieli się przez p_1, więc $p_1 \mid q_1q_2... q_{m-1}q_m$. Ponieważ p_1 i q_m są względnie pierwsze (dwie różne pierwsze liczby są względnie pierwsze), więc z lematu Euklidesa (twierdzenie 1.9) $p_1 \mid q_1q_2...q_{m-1}$. Kiedy postępujemy tak dalej, okazuje się, że $p_1 \mid q_1$. I znowu sprzeczność. Rozkład na czynniki pierwsze jest jednoznaczny. ■

Definicja 1.6

Najmniejsza wspólna wielokrotność dodatnich całkowitych liczb a i b to najmniejsza dodatnia liczba całkowita podzielna i przez a i przez b. Oznacza się ją $NWW(a, b)$.

Twierdzenie 1.11 (lemat)
Jeśli $a \mid c$ i $b \mid c$, to $NWW(a, b) \mid c$.
Dowód
Gdyby było nieprawdą, że $NWW(a, b) \mid c$, to istniałyby liczby q i r, $0 < r < NWW(a, b)$, że $c = k \cdot NWW(a, b) + r$. Ponieważ jednak $a \mid c$ i $b \mid c$, to i $a \mid r$, i $b \mid r$, więc $NWW(a, b)$ nie jest najmniejszą wspólną wielokrotnością liczb a i b. Sprzeczność z tym, że $NWW(a, b)$ nie dzieli c. ■

Twierdzenie 1.12 (lemat)
Niech a, b i c będą dowolnymi dodatnimi całkowitymi liczbami. Wtedy
$NWD(ac, bc) = c \cdot NWD(a, b)$
$NWW(ac, bc) = c \cdot NWW(a, b)$
Dowód
$NWD(ac, bc) = xac + ybc$, gdzie wyrażenie po prawej stronie jest najmniejszą dodatnią kombinacją liniową liczb ac i ab. Ale $xac + ybc = c(xa + yb)$, gdzie $xa + bc$ musi być najmniejszą dodatnią kombinacją liniową liczb a i b. To kończy dowód pierwszej równości.
$NWW(ac, bc)$ dzieli się przez ac i przez bc, więc dzieli się przez c.
Zatem $\dfrac{NWW(ab, ac)}{ac} = \dfrac{\dfrac{NWW(ac, bc)}{c}}{a}$ jest liczbą całkowitą
i $\dfrac{NWW(ab, ac)}{bc} = \dfrac{\dfrac{NWW(ac, bc)}{c}}{b}$ jest liczbą całkowitą.
Tak więc $\dfrac{NWW(ac, bc)}{c} \geq NWW(a, b)$, czyli $NWW(ac, bc) \geq c \cdot NWW(a, b)$.
Z drugiej strony $c \cdot NWW(a, b)$ dzieli się przez ac i dzieli się przez bc, więc $c \cdot NWW(a, b) \geq NWW(ca, cb)$. ■

Twierdzenie 1.13 (lemat)
Dla dowolnych liczb naturalnych a i b jeśli $NWD(a, b) = 1$, to $NWW(a, b) = ab$.

1.2. Znajdź największy wspólny dzielnik (NWD), stosując algorytm Euklidesa.
a) $NWD(882, 735)$
b) $NWD(1000001, 1000000)$

c) $NWD(2(1+2+3+\ldots+n), n+1)$
d) $NWD(2(1+2+3+\ldots+n)+1, n+1)$
e) $NWD(2n^2+3n+1, n+1)$

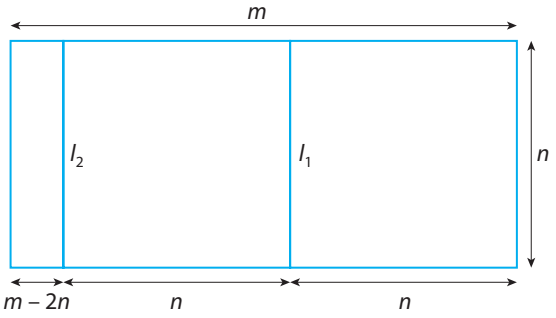
1.3. Oblicz
a) $NWW(12, 28)$
b) $NWW(47, 3)$
c) $NWW(7 \cdot 13, 13)$
d) $NWW(n, n+1)$
e) $NWW(2n^2+3n+1, n+1)$

1.4. a) Zdefiniuj $NWD(a, b, c)$
b) Czy $NWD(a, b, c) = NWD(NWD(a, b), c)$?
c) Spróbuj uogólnić algorytm Euklidesa z dwóch liczb do znajdywania *NWD* trzech liczb.
d) Znajdź $NWD(234, 567, 890)$.

1.5. Udowodnij, że jeśli $a \mid bcd$ i $NWD(a, c) = 1$ i $NWD(a, d) = 1$, to $a \mid b$.

Algorytm Euklidesa i „odcinanie" kwadratów

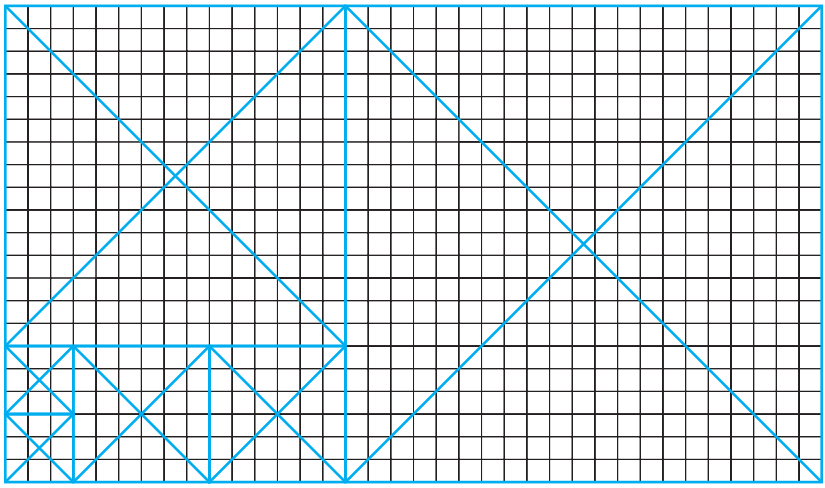
Mamy prostokąt o wymiarach m na n, gdzie $m > n$. Chcemy go pokryć jak największymi identycznymi kafelkami kwadratowymi. Wiemy, że można go pokryć kafelkami kwadratowymi o wymiarach 1 na 1. Ale może można go pokryć większymi kwadratami? Zobacz na rysunku.



Przypuśćmy, że prostokąt został pokryty identycznymi największymi z możliwych kwadratami. Na pewno odcięcie kwadratu n na n wzdłuż linii l_1 nie przetnie żadnego kwadratu, bo pewna liczba kwadratów ułożonych obok siebie osiąga łączną długość równą n. Podobnie rozumując, można od prostokąta na rysunku odciąć za jednym razem dwa kwadraty n na n wzdłuż linii l_2. Szukanie największego kwadratu, którym można „pokafelkować" prostokąt m na n, spro-

wadziliśmy więc do znalezienia największych kwadratowych kafelków pokrywających prostokąt n na $m - 2n$. A to właśnie algorytm Euklidesa. I nic w tym dziwnego, bo szukany kwadrat ma bok o długości $NWD(m, n)$.

Poniższy rysunek prostokąta 36 na 21 opisuje algorytm „odcinania" kwadratów, który prowadzi do znalezienia $NWD(36, 21)$.



Obcięcie kwadratu 21 na 21: $NWD(36, 21) = NWD(15, 21)$,
obcięcie kwadratu 15 na 15: $NWD(15, 21) = NWD(15, 6)$,
obcięcie dwóch kwadratów 6 na 6: $NWD(15, 6) = NWD(6, 3)$

„Kafelkarz" dostrzegłby, że zostały mu dwa kwadratowe kafelki 3 na 3, rozmiaru których szukał. Algorytm Euklidesa zaś powiedziałby w tym momencie: $NWD(6, 3) = NWD(0, 3) = 3$.

Odcinanie kwadratów od prostokąta 36 na 21 prowadziło do odcięcia jednego kwadratu, potem jeszcze jednego kwadratu, potem dwóch kwadratów i to doprowadziło do trzech równych kwadratów obok siebie. Każdy inny prostokąt, w którym proporcja boków byłaby jak 36 do 21, czyli jak 12 do 7 zachowałby się tak samo: 1, 1, 2 i 3 kwadraty. Różnica pomiędzy większym (36 na 21) a mniejszym (12 na 7) byłaby w wielkości ostatniego kwadratu. Ostatnim odcinanym kwadratem większego prostokąta jest kwadrat 3 na 3, a mniejszego – kwadrat 1 na 1.

Odcinanie kwadratów ma pewną przewagę nad algorytmem Euklidesa, który bada dwie liczby całkowite, bo przy odcinaniu kwadratów mogą się pojawić i w dodatku mają sens prostokąty o bokach wymiernych, a nawet niewymiernych.

Rozwiązania zadań

1. Liczby

1.1. a) $3^{4\cdot 25+1} - 2^{4\cdot 25+1} \equiv^5 3\cdot(3^4)^{25} - 2\cdot(2^4)^{25} \equiv^5 3\cdot 81^{25} - 2\cdot 16^{25} \equiv^5$
$\equiv^5 3\cdot(1^4)^{25} - 2\cdot(1^4)^{25} \equiv^5 1$; resztą jest 1
b) $3^{102} - 2^{102} \equiv^5 3^2\cdot(3^4)^{25} - 2^2\cdot(2^4)^{25} \equiv^5 9\cdot 81^{25} - 4\cdot 16^{25} \equiv^5 4\cdot 1^{25} - 4\cdot 1^{25} \equiv^5 0$
c) $3^{103} - 2^{103} \equiv^5 3^3\cdot(3^4)^{25} - 2^3\cdot(2^4)^{25} \equiv^5 27\cdot 1^{25} - 8\cdot 1^{25} \equiv^5 2 - 3 \equiv^5 -1 \equiv^5 4$
d) $3^{104} - 2^{104} \equiv^5 3^4\cdot(3^4)^{25} - 2^4\cdot(2^4)^{25} \equiv^5 81\cdot 1^{25} - 16\cdot 1^{25} \equiv^5 1 - 1 \equiv^5 0$
e) $3^{105} - 2^{105} \equiv^5 3^5 - 2^5 \equiv^5 81\cdot 3 - 32 \equiv^5 3 - 2 \equiv^5 1$

1.2. a) $NWD(882, 735) = NWD(735, 147) = NWD(147, 0) = 147$
b) $NWD(1000001, 1000000) = NWD(1000000, 1) = NWD(1, 0) = 1$
c) $NWD(n(n+1), n+1) = NWD(n+1, 0) = n+1$
d) $NWD(2(1+2+3+\ldots+n)+1, n+1) = NWD(n(n+1)+1, n+1) =$
$= NWD(1, n+1) = NWD(1, 0) = 1$
e) $NWD((2n+1)(n+1), n+1) = NWD(n+1, 0) = n+1$

1.3. a) $NWW(12, 28) = 4\cdot NWW(3, 7) = 4\cdot 3\cdot 7 = 84$
b) $NWW(47, 3) = 47\cdot 3$
c) $NWW(7\cdot 13, 13) = 13\cdot NWW(7, 1) = 13\cdot 7 = 91$
d) $NWW(n, n+1) = n(n+1)$
e) $NWW((2n+1)(n+1), n+1) = (n+1)\cdot NWW(2n+1, 1) = (n+1)(2n+1)]$

1.4. Niech $D(a)$ oznacza zbiór dzielników liczby a, $D(b)$ zbiór dzielników liczby b i $D(c)$ zbiór dzielników liczby c.
a) $NWD(a, b, c)$ jest największym elementem zbioru $D(a) \cap D(b) \cap D(c)$.
b) Tak, bo po lewej stronie jest największy element zbioru $D(a) \cap D(b) \cap D(c)$. Po prawej mamy największy element części wspólnej zbioru $D(c)$ i zbioru wszystkich dzielników $NWD(a, b)$. Pokazaliśmy (wniosek 2, twierdzenie 1.7), że zbiór wszystkich dzielników $NWD(a, b)$ i zbiór wspólnych dzielników a i b, czyli $D(a) \cap D(b)$, jest tym samym. Tak więc z równości $(D(a) \cap D(b)) \cap D(c) = D(a) \cap D(b) \cap D(c)$ wynika, że największy element obu zbiorów jest ten sam.
c) Trzeba pokazać, że jeśli $a \le b$, to $NWD(a, b, c) = NWD(a, b-a, c)$. Wiemy z dowodu lematu Euklidesa (twierdzenie 1.5), że $D(a) \cap D(b) = D(a) \cap D(b-a)$. Wobec tego $D(a) \cap D(b)) \cap D(c) = D(a) \cap D(b-a)) \cap D(c)$. Zatem i największy element obu zbiorów jest ten sam. Idźmy krok dalej: w wyrażeniu $NWD(a, b, c)$ możemy zastąpić a i b przez mniejszą z nich i resztę z dzielenia większej przez mniejszą i, oczywiście, to samo można zrobić z dowolną parą spośród liczb a, b, c.
d) $NWD(234, 567, 890) = NWD(234, 567 - 2\cdot 234, 890 - 3\cdot 234) =$
$= NWD(234, 99, 188) = NWD(99, 234 - 2\cdot 99, 188 - 99) = NWD(99, 36, 89) =$
$= NWD(36, 99 - 2\cdot 36, 89 - 2\cdot 36) = NWD(36, 27, 17) = NWD(17, 10, 2) =$
$= NWD(2, 0, 1) = NWD(1, 0, 0) = 1$