

MATEMATYCZNA DETEKTYWISTYKA

JAK SZUKAMY CAŁKOWITYCH
ROZWIĄZAŃ RÓWNAŃ

WOJCIECH KRYSZEWSKI



Radża i jego córki

Pewien radża w testamencie pozostawił swoim kilku córkom pewną liczbę pereł wraz z instrukcją, aby zostały podzielone w następujący sposób: jego najstarsza córka miała otrzymać jedną perłę i jedną siódmą pozostałych. Druga córka miała otrzymać dwie perły i jedną siódmą pozostałych. Podobnie trzecia córka miała otrzymać trzy perły i również jedną siódmą pozostałych. I tak dalej z każdą z pozostałych córek.



Najmłodsze córki poszły sądu, narzekając, że ten skomplikowany system jest bardzo niesprawiedliwy. Sędzia, który był biegły w rozwiązywaniu problemów, odpowiedział natychmiast, że skarżące się córki mylą się i że proponowany **podział jest sprawiedliwy**, bo każda z córek otrzyma tę samą liczbę pereł.

Zadanie

Ile było pereł ? Ile córek miał radża?

Rozwiązanie jest dość proste!

- x – liczba pereł, które miał radża;
- y – liczba pereł, które otrzymała każda z córek.
- $n = \frac{x}{y}$ – liczba córek.

Ile pereł otrzymała pierwsza córka?

$$y = 1 + \frac{1}{7}(x-1).$$

Przekształcając:

$$7(y-1) = x-1 \iff 7y-x=6.$$

Rozwiązanie (zgadujemy): $x=36, y=6$ i $n=6$.

Pereł było 36, każda córka dostała 6 pereł, a córek było też 6.

Czy to dobre rozwiązanie? Czy trzeba zgadywać?

Równanie

$$7y - x = 6$$

ma też rozwiązanie $x = 8, y = 2, n = 4$ lub $x = 15, y = 3, n = 5$.

ALE:

Ile pereł otrzymała druga córka?

$$y = 2 + \frac{1}{7}(x - y - 2).$$

przekształcając $8y - 12 = x$.

Mamy układ
$$\begin{cases} 7y - 6 = x \\ 8y - 12 = x. \end{cases}$$
 Ostatecznie $y = 6, x = 36$ i $n = 6$.

Mamy do czynienia z równaniem postaci

$$ax + by = c,$$

w którym współczynniki a, b są całkowite, a x, y są niewiadomymi. Szukamy rozwiązań x, y , w zbiorze liczb naturalnych ⁽¹⁾.

Równanie algebraiczne o współczynnikach całkowitych zawierające jedną, dwie lub więcej niewiadomych i którego rozwiązań poszukuje się wśród liczb całkowitych (lub wymiernych) nazywa się równaniem diofantycznym.

¹Dane są też dodatkowe warunki: np. szukamy takich $x, y \in \mathbb{N}$, aby $n = \frac{x}{y} \in \mathbb{N}$.

- Równanie $x^n + y^n = z^n$, gdzie $n \in \mathbb{N}$. Dla $n = 2$ rozwiązaniem jest tzw. **trójka pitagorejska**: długości boków w trójkącie prostokątnym, np $x = 3$, $y = 4$ i $z = 5$. O problemie **dla $n \geq 3$ jeszcze porozmawiamy**.
- Równania diofantyczne **liniowe** $ax + by = c$: o nich **wiemy wszystko**.
- Równanie $x^y = y^x$ ma dwa (różne) rozwiązania $x = 2$, $y = 4$ oraz $x = 4$, $y = 2$.
- Równanie Pella: $x^2 - ny^2 = 1$ ($n \in \mathbb{N}$).
- Równanie cyklu Collatza: $3^x y - 1 = 2^z (2^x y - 1)$; jest to obecnie jeden z najtrudniejszych problemów jakie w ogóle stawia matematyka. **Jeszcze o tym porozmawiamy**.

Zadanie (nietypowe): Oblicz sumę $x + y + z$ ($x, y, z \in \mathbb{N}$) pod warunkiem, że

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1.$$

Rozwiązania:

$x = y = z = 3$, czyli $x + y + z = 9$. A można mniej?

$x = 2, y = 3, z = 6$, $x + y + z = 11$. A można więcej?

O co chodzi z tymi równaniami diofantycznymi?

- Czy mają rozwiązania?
- Jeśli tak, to ile ich jest (skończenie, czy nieskończenie wiele)?
Co z rozwiązaniami nieujemnymi?
- Czy istnieje algorytm na wyznaczanie rozwiązań?
- Czy rozwiązania mają jakieś inne, ciekawe własności?

Skąd nazwa: „równanie diofantyczne”

Diofantos z Aleksandrii jako pierwszy systematycznie zajął się algebrą, czyli teorią rozwiązywania równań. Diofantos narzucał na rozpatrywane równania takie warunki, aby rozwiązania mieściły się w zbiorze liczb całkowitych lub, co najwyżej, w zbiorze liczb wymiernych.

Rozważał wprawdzie zadania sprowadzające się do równań typu $4x + 20 = 0$, ale twierdził, że takie równanie ma absurdalne rozwiązanie. Liczby ujemne uważał za niedopuszczalne i je odrzucał. Rozwiązywał także równanie kwadratowe, potęgowe i inne. Wprowadził wiele pojęć i rozpoczął systematyczne badania w teorii liczb.



Diofantos z Aleksandrii
214-298

W XIV wieku grecki mnich Maximus Planudes umieścił w swojej antologii następujący wiersz. Jego treść jest jednocześnie zadaniem tekstowym (i równaniem diofantycznym):

Epitafium Diofantosa

Pod tym nagrobkiem spoczywa Diofantos – a dzięki przedziwnej sztuce zmarłego jego wiek zdradzi ci ten głaz: Chłopcem przez szóstą część życia pozostać Bóg mu pozwolił, lica pokwitły mu zaś, kiedy dwunasta znów część życia minęła; gdy żywota przebył część siódmą, młodą małżonkę w dom dobry wprowadził mu Bóg, która, gdy pięć lat minęło, małego powiła mu synka. Ale okrutny chciał los, że kiedy syn ledwie wiek ojca w połowie osiągnął, ponury zabrał go los. Kojąc ogromny swój ból, szukał Diofantos wśród liczb jeszcze przez cztery lata pociechy, aż rozstał się z życiem.

Ile lat żył Diofantos?



Paryż, rok wyd. 1621, tłumacz Claude-Gaspar Bachet de Méziriac

Czy łatwo było tłumaczyć Diofantosa?



C.-G. Bachet (1581-1638)

(a) $\Delta^Y \bar{\xi} \overset{\circ}{M} \overline{\beta \phi \kappa}$ Zapis Diofantesa

(b) $\Delta^Y \Delta \bar{\alpha} \overset{\circ}{M} \overline{\lambda \varsigma} \wedge \Delta^Y \overline{\iota \beta}$

(c) $\Delta K^Y \overline{\gamma} \Delta^Y \overline{\iota \gamma} \varsigma \overline{\mu \epsilon} \wedge \Delta^Y \Delta \bar{\delta} \overset{\circ}{M} \overline{\sigma \kappa \eta}$

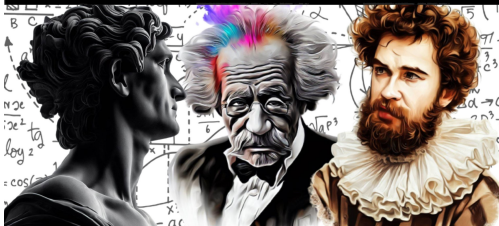
(a) $32x + 9$ Zapis nowoczesny

(b) $41x^2 - 3$

(c) $2x^3 - 3x^2 + 48$

Do Bacheta i jego dokonań jeszcze **wrócimy**.

Kto wprowadził symbole liter do matematyki ?



Paciolus	1 <i>cu. m.</i> 6 <i>ce.</i> p. 11 <i>co.</i> eguale 6
Stifelius	1 ∞ - 6 $\exists$ + 11 $\exists$ equantur 6
Bombelli	1 $\smile$. <i>m.</i> 6 $\smile$. <i>p.</i> $\smile$ eguale 6
Stevinus	1 $\textcircled{3}$ - 6 $\textcircled{2}$ + 11 $\textcircled{1}$ egale 6
Vieta	1C - 6Q + 11N egal 6
Harriot	1. <i>aaa</i> - 6. <i>aa</i> + 11. <i>a</i> = 6
Modern	$x^3 - 6x^2 + 11x = 6$

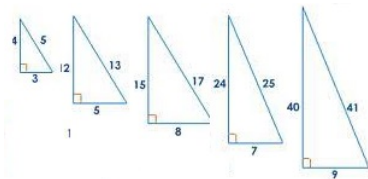
Diofantos: „Podziel kwadrat na sumę kwadratów”

Należy znaleźć liczby naturalne takie x, y, z , że

$$x^2 + y^2 = z^2.$$

Taka trójka (x, y, z) nazywa się **trójką pitagorejską**.

Nazwa pochodzi od twierdzenia Pitagorasa, gdyż każda trójka pitagorejska (x, y, z) odpowiada długościom boków trójkąta prostokątnego.



- metoda elementarna Diofantosa (i jej warianty)
- metoda Gaussa (liczby zespolone)
- metoda geometryczna

Rozważamy trójkę pitagorejską (x, y, z) , tzn. $x, y, z \in \mathbb{N}$ oraz

$$x^2 + y^2 = z^2.$$

Obserwacje:

- Kwadrat dowolnej liczby $n \in \mathbb{N}$ przy dzieleniu przez 8 daje resztę 0, 1 lub 4 (dlaczego?);
- kwadrat dowolnego nieparzystego $n \in \mathbb{N}$ przy dzieleniu przez 8 daje resztę 1; stąd suma kwadratów liczb nieparzystych daje resztę 2 podczas dzielenia przez 8.
- Zatem w parze x, y przynajmniej jedna liczba jest parzysta.

- Można założyć, że liczby x, y są względnie pierwsze (tj. nie mają wspólnych dzielników) – czemu to można zrobić?
- Przypuśćmy, że y jest parzysta, tzn. $y = 2c$, gdzie $c \in \mathbb{N}$.
- Wtedy x jest nieparzysta (dlaczego?)
- Stąd liczba z jest też nieparzysta i względnie pierwsza względem x i względem y .
- Liczby $x - z$ i $x + z$ są parzyste, a liczby $a = \frac{z-x}{2}$ i $b = \frac{z+x}{2}$ są względnie pierwsze. Ponadto $z = a + b$, $x = b - a$ oraz

$$c^2 = \left(\frac{y}{2}\right)^2 = \frac{y^2}{4} = \frac{z^2 - x^2}{4} = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right) = ab.$$

- Ponieważ a, b są względnie pierwsze, a ich iloczyn jest kwadratem, to a i b są kwadratami, tzn. istnieje liczby $m, n \in \mathbb{N}$ takie, że

$$a = m^2, b = n^2 \Rightarrow x = n^2 - m^2, y = 2mn, z = m^2 + n^2.$$

Kluczowy jest ostatni punkt rozumowania: wynika on z zasadniczego twierdzenia arytmetyki (o rozkładzie każdej liczby na iloczyn liczb pierwszych). Spróbuj to uzasadnić!

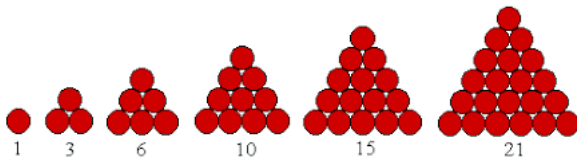
W naszym wykładzie specjalne miejsce zarezerwowane jest dla pewnego francuskiego prawnika i matematyka z zamiłowaniem [Pierre'a de Fermat](#). Jego rola w matematyce jest nie do przecenienia ... z kilku powodów.

Podczas lektury Diofantosa napisał (w 1663 roku): ...[odkryłem, że każda liczba naturalna jest sumą trzech liczb trójkątnych, jest też sumą czterech liczb kwadratowych, pięciu liczb pięciokątnych, itp., itd....](#)

Co to są liczby wielokątne? Otóż [liczba \$n\$ jest \$m\$ -kątna](#) (trójkątna $m=3$, kwadratowa $m=4$) jeśli z n kropek lub kamyków można ułożyć kształt m -kąta foremnego.



Pierre Fermat
(1601-1665)



- Na przykład: liczba n jest trójkątna wtedy i tylko wtedy, gdy

$$n = 1 + 2 + 3 + \dots + m = \frac{m(m+1)}{2},$$

dla pewnego $m \in \mathbb{N}$ – [oczywiste - znany wzór na sumę wyrazów ciągu arytmetycznego]

- Liczba $n \in \mathbb{N}$ jest trójkątna wtedy i tylko wtedy, gdy liczba $8n+1$ jest kwadratowa – [udowodnij - NAGRODA].

Dowód „wielokątnego” twierdzenia Fermata nigdy nie ujrzał światła dziennego. Czy w ogóle istniał?



Badania liczb wielokątnych prowadzili:

- J. Lagrange (1770) dla liczb kwadratowych;
- C. F. Gauss (1796) dla liczb trójkątnych;
- A. Cauchy (1813) ogólne twierdzenie wielokątne;
- M. Nathanson (1987) podał prosty i elementarny dowód.

Trzeba było 150 lat, aby uporać się z czyjąś notatką na marginesie księgi Diofantosa!

Twierdzenie wielokątne Fermata

(Nathanson 1987) Każdą liczbę $n \in \mathbb{N}$ można przedstawić jako sumę $(m+2)$ liczb $(m+2)$ -kątnych, gdzie $m = 0, 1, 2, \dots$

A SHORT PROOF OF CAUCHY'S POLYGONAL NUMBER THEOREM

MELVYN B. NATHANSON

ABSTRACT. This paper presents a simple proof that every nonnegative integer is the sum of $m + 2$ polygonal numbers of order $m + 2$.

Let $m \geq 1$. The polygonal numbers of order $m + 2$ are the integers

$$p_m(k) = \frac{m}{2}(k^2 - k) + k$$

for $k = 0, 1, 2, \dots$. Fermat [3] asserted that every nonnegative integer is the sum of $m + 2$ polygonal numbers of order $m + 2$. For $m = 2$, Lagrange [5] proved that every nonnegative integer is the sum of four squares $p_2(k) = k^2$. For $m = 1$, Gauss [4] proved that every nonnegative integer is the sum of three triangular numbers $p_1(k) = (k^2 + k)/2$, or, equivalently, that every positive integer $n \equiv 3 \pmod{8}$ is the sum of three odd squares. Cauchy [1] proved Fermat's statement for all $m \geq 3$, and Legendre [6] refined and extended this result. For $m \geq 3$ and $n \leq 120m$, Pepin [8] published tables of explicit representations of n as a sum of $m + 2$ polygonal numbers of order $m + 2$, at most four of which are different from 0 or 1. Dickson [2] prepared similar tables. Pall [7] obtained important related results on sums of values of a quadratic polynomial.

To nie koniec zagadek Fermata!

Zadanie 8 z 6 księgi "Arytmetyki" Diofantosa ma następującą treść:

Dany kwadrat rozłożyć na [sumę] dwa kwadraty.

Po śmierci Fermata na marginesie jego egzemplarza książki w tym właśnie miejscu znaleziono dopisek z roku 1637 roku o treści:

Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Przeciwnie, nie można rozłożyć ani sześcianu na sumę dwóch sześcianów, ani bikwadratu na dwa bikwadraty, i w ogóle żadnej potęgi większej niż druga na dwie potęgi z takim samym wykładnikiem. Odkryłem naprawdę zadziwiający dowód tego faktu. Margines jest na to za mały.

Wielkie Twierdzenie Fermata (1657) opubl. (1670)

Dla liczby naturalnej $n > 2$ nie istnieją takie liczby naturalne dodatnie x, y, z , dla których

$$x^n + y^n = z^n.$$

Zachował się dowód autorstwa Fermata dla $n = 3$, Gaussa dla $n = 3$ i wiele innych przypadków szczególnych.

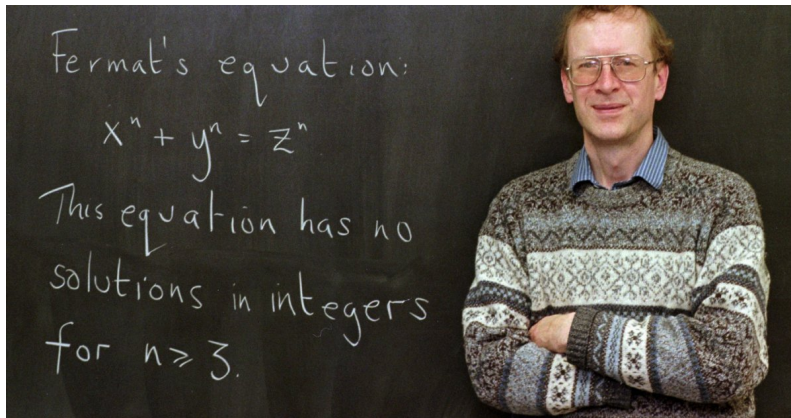


Dowód dla dowolnego $n > 2$ ostatecznie podał w 1995 roku angielski matematyk **Andrew Wiles** (po **358 latach!**). Dowód zajmował ponad 120 stron i wyrażony był w języku w języku geometrii algebraicznej i krzywych eliptycznych.

Tak na prawdę Wiles udowodnił **hipotezę Shimury-Taniyamy-Weila**:

Semistabilne krzywe eliptyczne są modularne.

To przeczy faktowi (Faltings), który mówi, że gdyby istniały takie liczby $a, b, c \in \mathbb{N}$, że $a^n + b^n = c^n$, to (pewna) krzywa $E_n(a, b, c)$ nie byłaby modularna, choć jest semistabilna. Tym samym Wiles udowodnił WTF.



- Dla $n = 3$ dowód WTF jest umiarkowanie trudny: w zasadzie każdy student matematyki go zrozumie.
- Dla $n = 4$ dowód WTF jest łatwy: stanowi nietrudne zastosowanie argumentacji prowadzącej do postaci trójek pitagorejskich [spróbuj].
- dla dowolnego n dowód jest skrajnie trudny.
- dla pewnych konkretnych wartości n istnieją niezależne dowody na ogół oparte o techniki pochodzące z teorii liczb..

Profesor **Andrew Booker** z University of Bristol rozwiązał zagadkę matematyczną sprzed 64 lat. Zagadka brzmi: **jak wyrazić liczbę $k = 33$ za pomocą sumy trzech liczb podniesionych do potęgi trzeciej**, tzn. znaleźć x, y i z tak, aby

$$x^3 + y^3 + z^3 = 33.$$

Przykład: jeśli $k = 8$, to równanie wygląda następująco

$$2^3 + 1^3 + (-1)^3 = 8.$$

Wiadomo, że dla liczby k , która po dzieleniu przez 9 daje resztę 4 lub 5, nie ma rozwiązań. To wyklucza 22 liczby z przedziału od 1 do 100. Jednak 78 pozostałych liczb powinno mieć rozwiązania. Problem był rozwiązany dla wszystkich liczb poza 33 i 42.

$$(8866128975287528)^3 + (-8778405442862239)^3 \\ + (-2736111468807040)^3 = 33.$$

Dotychczas nie udało się znaleźć rozwiązania dla $k = 42$.

Umiesz to zrobić? Będziesz sławny.

10 problem Hilberta



Dziesiąty problem Hilberta jest jednym z 23 matematycznych problemów przedstawionych przez **David Hilbert** w 1900 roku. Treść problemu można wyrazić w następujący sposób.

Czy istnieje efektywna i skończona procedura algorytmiczna, która przyjmując jako dane wejściowe współczynniki równania diofantycznego, zwraca odpowiedź „tak” lub „nie” na pytanie, czy istnieje rozwiązanie tego równania w dziedzinie liczb całkowitych.

Negatywną odpowiedź na to pytanie podał rosyjski matematyk **Jurij Matijasevich**. Sam problem miał kolosalne znaczenie dla rozwoju informatyki teoretycznej i tzw. teorii obliczalności.

Linowe równania diofantyczne z dwiema niewiadomymi

Zadanie

Ile kopert po 3zł i 7zł można kupić za 1000zł, jeśli można wydać wszystkie możliwe pieniądze?

Oznaczmy:

- x – liczba biletów po 3 zł; suma wydana za te bilety $3x$
- y – liczba biletów po 7 zł; suma wydana na te bilety $7y$.

Zatem

$$3x + 7y = 1000 \quad (\text{zgadujemy rozwiązanie: } x = 247, y = 37)$$

Prowadzi nas to do rozważania równań postaci

$$ax + by = c,$$

gdzie a, b, c są liczbami całkowitymi, $a^2 + b^2 > 0$ (tzn. $a \neq 0$ lub $b \neq 0$), a rozwiązania poszukuje się także wśród liczb całkowitych (lub naturalnych).

Takimi równaniami zajmowały się rzesze matematyków, już w starożytności. My pójdziemy w ślad twierdzenia Bacheta-Bézouta. Będziemy rozważać o istnienie rozwiązań, ich liczbę i postać.

Twierdzenie: warunek konieczny

Jeśli równanie $ax + by = c$ ma rozwiązanie (w liczbach całkowitych), to każdy wspólny dzielnik liczb a i b jest też dzielnikiem liczby c .

Dowód: Weźmy dowolny dzielnik d liczb a i b . Niech $\bar{x}, \bar{y}$ będą rozwiązaniami. Wtedy $a = nd$ i $b = md$ dla pewnych liczb całkowitych n, m oraz

$$c = a\bar{x} + b\bar{y} = nd\bar{x} + md\bar{y} = d(n\bar{x} + m\bar{y}).$$

Stąd widać, że d dzieli c .

Czy podany warunek jest również wystarczający? **TAK!**

Twierdzenie: warunek dostateczny

Jeśli $d = \text{NWD}(a, b)$ jest największym wspólnym dzielnikiem liczb a i b oraz d jest dzielnikiem liczby c , to równanie

$$ax + by = c$$

ma rozwiązania całkowite.

Dowód: Dowodzi się najpierw, że $d = \text{NWD}(a, b)$ jest **najmniejszą** liczbą naturalną w zbiorze

$$D = \{ax + by \mid x, y \text{ są liczbami całkowitymi}\}.$$

Zatem $d \in D$, czyli muszą się znaleźć liczby całkowite x_0, y_0 takie, że

$$d = ax_0 + by_0.$$

Ponieważ d dzieli c , to $c = dn$ dla pewnego całkowitego n . Stąd

$$c = dn = (ax_0 + by_0)n = a(x_0n) + b(y_0n),$$

czyli $\bar{x} = x_0n$ i $\bar{y} = y_0n$ są rozwiązaniami wyjściowego równania.

Biorąc pod uwagę oba warunki: konieczny i dostateczny otrzymujemy:

Twierdzenie Bacheta

Równanie $ax + by = c$ ma rozwiązania całkowite wtedy i tylko wtedy, gdy $d = \text{NWD}(a, b)$ jest dzielnikiem c .

Przykłady

- Równanie $16x + 28y = 36$ **ma** rozwiązanie, bo $\text{NWD}(16, 28) = 4$ i $36 = 4 \cdot 9$.
- Równanie $27x + 18y = 21$ **nie ma** rozwiązań, bo $\text{NWD}(27, 18) = 9$ i 9 nie jest dzielnikiem 21.

Aby rozwiązać równanie

$$ax + by = c$$

należy:

- 1 Obliczyć $d = \text{NWD}(a, b)$ przy pomocy **algorytmu Euklidesa** i sprawdzić, czy d jest dzielnikiem wyraży wolnego c . Jeśli tak, czyli $c = nd$ dla pewnego całkowitego n , to:
- 2 Przy pomocy **rozszerzonego algorytmu Euklidesa** znajdujemy liczby całkowite x_0, y_0 takie, że $ax_0 + by_0 = d$.
- 3 **Ogół** rozwiązań w zakresie liczb całkowitych dany jest wzorami

$$(*) \quad x = nx_0 + \frac{b}{d}t, \quad y = ny_0 - \frac{a}{d}t, \text{ gdzie } t \text{ jest całkowitym parametrem.}$$

Rozwiązań całkowitych jest **nieskończenie wiele**. Są one zadane wzorami (*).

Jaka jest geometryczna interpretacja tego faktu?

Rozszerzony algorytm Euklidesa - przykład

Znajdź x_0, y_0 takie, że $623x_0 + 42y_0 = \text{NWD}(623, 42)$.

- Szukamy $\text{NWD}(623, 42)$. UWAGA: Oznaczenie $a \pmod b$ = reszta z dzielenia a przez b .

1 $a_0 = 623, b_0 = 42$

2 $a_1 = b_0 = 42, b_1 = a_0 \pmod{b_0} = 623 \pmod{42} = 35$ bowiem $623 = 14 \cdot 42 + 35$,
czyli $35 = 623 - 14 \cdot 42$;

3 $a_2 = b_1 = 35, b_2 = a_1 \pmod{b_1} = 42 \pmod{35} = 7$ bowiem $42 = 1 \cdot 35 + 7$,
czyli $7 = 42 - 1 \cdot 35$;

4 $a_3 = b_2 = 7, b_3 = a_2 \pmod{b_2} = 35 \pmod{7} = 0$.

Stąd $\text{NWD}(623, 42) = 7$.

- Postępujemy odwrotnie:

$$7 = 42 - 1 \cdot 35 = 42 - (623 - 14 \cdot 42) = 15 \cdot 42 + (-1) \cdot 623.$$

stąd $x_0 = -1, y_0 = 15$.

Kalkulator algorytmu Euklidesa

A co z rozwiązaniami naturalnymi?

Często szukamy rozwiązań w zakresie liczb naturalnych (całkowitych nieujemnych lub dodatnich), bo to wynika z warunków zadania.

Twierdzenie Catalana (1867)

Niech $a, b, c \in \mathbb{N}$. Załóżmy, że $d = \text{NWD}(a, b)$ dzieli c . Wtedy równanie

$$ax + by = c$$

ma k rozwiązań całkowitych nieujemnych, gdzie

$$k = \left\lfloor \frac{c}{\text{NWW}(a, b)} \right\rfloor \text{ lub } k = \left\lceil \frac{c}{\text{NWW}(a, b)} \right\rceil + 1.$$

Aby zdecydować ile konkretnie: obliczamy $p = c \pmod{\text{NWW}(a, b)}$.

- jeśli równanie $ax + by = p$ ma całkowite nieujemne rozwiązania to ta liczba jest równa $\left\lfloor \frac{c}{\text{NWW}(a, b)} \right\rfloor + 1$;
- W przeciwnym przypadku ta liczba jest równa $\left\lfloor \frac{c}{\text{NWW}(a, b)} \right\rfloor$.

Wracamy do zadania o kopertach.

Zadanie

Ile kopert po 3zł i 7zł można kupić za 1000zł, jeśli można wydać wszystkie możliwe pieniądze? Na ile sposobów można to uczynić?

Czyli wracamy do równania

$$3x + 7y = 1000$$

i szukamy rozwiązań całkowitych nieujemnych.

Zgodnie z twierdzeniem Catalana liczba rozwiązań w zakresie liczb całkowitych nieujemnych wynosi $\left\lfloor \frac{1000}{21} \right\rfloor = 47$ lub 48 (tutaj $NWW(3, 5) = 21$).

Obliczamy $p = 1000 \pmod{21} = 13$.

• Badamy równanie $3x + 7y = 13$. Ma ono rozwiązanie $x = 2, y = 1$. Zatem rozwiązań jest więc 48.

Metoda Eulera rozwiązywania równań diofantycznych

Oprócz naszkicowanej metody opartej na zastosowaniu rozszerzonego algorytmu Euklidesa, można posłużyć **metodą zaproponowaną przez L. Eulera**.



Leonhard Euler (1707 - 1783)

Ponownie rozważamy równanie;

$$ax + by = c,$$

w którym $\text{NWD}(a, b) = d$ i d dzieli c . Równanie ma więc rozwiązania x_0, y_0 .



- Wyjściowe równanie jest równoważne z równaniem zredukowanym

$$Ax_0 + By_0 = C,$$

gdzie $A = \frac{a}{d}$, $B = \frac{b}{d}$ i $C = \frac{c}{d}$.

- Widzimy, że $Ax_0 - C = -By$, czyli, że liczba B dzieli różnicę $(Ax_0 - C)$, tzn.

$$Ax_0 \pmod{B} = C \pmod{B}.$$

- Ponieważ $\text{NWD}(A, B) = 1$, to istnieje tzw. **odwrotność modularna** liczby A względem B . Jest to taka liczba całkowita A' , że

$$A'A \pmod{B} = 1.$$

- Zatem

$$x_0 = A'Ax_0 \pmod{B} = A'C \pmod{B} \text{ tzn. } x_0 \text{ jest resztą z dzielenia } A'C \text{ przez } B.$$

- Obliczamy

$$y_0 = \frac{1}{B}(C - Ax_0).$$

W grę wchodzi tzw. **rachunek modularny**, który tu sprowadza się do reguły

$$a \pmod{c} b \pmod{c} = ab \pmod{c} :$$

iloczyn reszt z dzielenia a i b przez c równa się reszcie z dzielenia iloczynu ab przez c .

Ma miejsce następujące uogólnienie twierdzenia Bacheta.

Twierdzenie

Rozważamy problem:

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b,$$

gdzie współczynniki $a_1, \dots, a_n$ są liczbami całkowitymi i co najmniej jeden z nich jest różny od zera. **Równanie to ma rozwiązanie $x_1, \dots, x_n$ w zakresie liczb całkowitych wtedy i tylko wtedy, gdy $d = \text{NWD}(a_1, a_2, \dots, a_n)$ dzieli b .**



Zadanie

Smok ma 2000 głów. Rycerz może ściąć jednym cięciem 33 głowy lub 21 głów lub 17 głów lub 1 głowę. Smokowi odrasta natychmiast odpowiednio 48 głów, 0 głów, 14 głów lub 349 głów. Smok zostanie zabity, gdy wszystkie głowy będą ścięte. Czy istnieje taka strategia walki rycerza ze smokiem, aby smok zginął (tj. postradał wszystkie głowy)?

Hipoteza Collatza

Weźmy dowolną dodatnią liczbę naturalną c_0 . Jeśli jest parzysta, to niech

$$c_1 = \frac{c_0}{2}$$

w przeciwnym wypadku

$$c_1 = 3c_0 + 1.$$

Następnie z liczbą c_1 postępujemy podobnie analogicznie jak z c_0 i kontynuujemy ten proces. Otrzymamy w ten sposób ciąg liczb naturalnych.

Hipoteza: niezależnie od jakiej liczby c_0 wystartujemy, w końcu dojdziemy do liczb 4,2,1,4,2,1,....

Przykład: Zaczynając od $c_0 = 11$, mamy:

11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1.

Kalkulator hipotezy Collatza

Zadania

1. Rozwiązać równania:

(a) $3x + 6y = 9$; (b) $4x + 6y = 96$.

2. Stosując algorytm Euklidesa rozwiązać równanie:

$$65x + 39y = 26.$$

3. Rozwiąż równanie z 3 niewiadomymi:

$$12x + 15y + 7z = 11.$$

Zadania

4. Rozwiązać metodą Eulera równanie

$$18x + 24y = 60.$$

Wskazówka: Odwrotnością modularną 3 względem 4 jest 3.

5. Jak odmierzyć 15 litrów wody mając do dyspozycji dwa dzbany pojemności 4 i 9 litrów.

6. Mamy dwie klepsydry. W jednej piasek przesypuje się w ciągu 7 minut, a w drugiej – w ciągu 11 minut. Jak za ich pomocą odmierzyć 15 minut?

Zadania przykładowe do rozwiązania

1. Do przewozu zboża są do dyspozycji worki 60-kg i 80-kg. Ile potrzeba poszczególnych worków do przewozu 440 kg zboża (zakładamy, że worki muszą być pełne)? Na ile sposobów można to uczynić?

2. Fabryka wysłała towar w paczkach po 3 kg i po 5 kg. Wykazać, że można w ten sposób wysłać każdą całkowitą ilość kilogramów większą niż 7.

3. W czasie pierwszej wojny światowej toczyła się bitwa w pobliżu pewnego zamku. Jeden z pocisków rozbił stojący tam pomnik rycerza rycerza z piką w ręku. Stało się to ostatniego dnia miesiąca. Iloczyn daty dnia, numeru miesiąca, wyrażonej w stopach długości piki, połowy wyrażonego w latach wieku dowódcy baterii strzelającej do zamku oraz połowy wyrażonego w latach czasu, jaki stał pomnik, równa się 451066. W którym roku postawiono pomnik?

4. Jak badać istnienie i znajdować rozwiązania całkowite układu równań diofantycznych

$$\begin{cases} a_1x + a_2y = c_1 \\ a_2x + b_2y = c_2, \end{cases}$$

gdzie współczynniki są całkowite?



Dziękuję za uwagę

- Ustawiamy $x \leq y \leq z$. Najmniejsza liczba x nie może być 1. Czy może być $x \geq 4$? Wtedy odwrotności y, z sumują się do liczby $\geq (x-1)/x$: to nie możliwe bo $1/y + 1/z \leq 2/y \leq 2/x < (x-1)/x$.

- Wiek Diofantosa $\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x$. Stąd $x = 84$

- Smok: Zabicie smoka jest możliwe przy pomocy x cięć 33 głów, y cięć 21 głów, z cięć 17 głów oraz t cięć 1 głowy. Wtedy

$$(33-48)x + 21y + (17-14)z + (1-248)t = -15x + 21y + 3z + 348t = 2000.$$

Jednak takie równanie nie ma rozwiązań, bo $NWD(-15, 21, 3, 348) = 3$ nie dzieli 2000.

- $451066 = 29 \cdot 2 \cdot 7 \cdot 11 \cdot 101$. Zatem wiek pomnika 202 lata, a rok zburzenia był rokiem przestępnym. Mógł to być tylko 1916. Zatem pomnik postawiono w 1714 roku.