RÓWNANIA DIOFANTYCZNE

Spis treści:

1. Wprowadzenie

- Równanie diofantyczne to równanie, którego rozwiązania szuka się w zbiorze liczb całkowitych. Zwykle rozważa się równania diofantyczne o dwóch lub więcej niewiadomych – równania z jedną dają się rozwiązać metodami algebraicznymi.
- Nazwa równań pochodzi od ich twórcy greckiego matematyka *Diofantosa*.

Był on matematykiem greckim, żyjącym w III wieku n.e. w Aleksandrii. Jest autorem dzieła Arytmetyka, składającego się z 13 ksiąg, z których zachowało się 6 w języku greckim i 4. przetłumaczone na arabski. Diofantos nie znał liczb ujemnych, jednak odróżniał liczby „dodawane" od „odejmowanych poprzez stosowanie odpowiednich znaków. Diofantos miał uważać się za pierwszego matematyka, który zastosował znak równania (=) oraz znak odejmowania (-).

2. Algorytm Euklidesa

Jest to algorytm do obliczania największego wspólnego dzielnika dwóch liczb całkowitych. Opiera się na spostrzeżeniu, że jeśli od liczby większej odejmiemy mniejszą, to mniejsza liczba i otrzymana różnica będą miały taki sam wspólny dzielnik jak pierwotne liczby. Jeśli w wyniku odejmowania otrzymamy parę równych liczb, oznacza to, że znaleźliśmy NWD. Można również zamiast odejmowania przypisać liczbie a liczbę b, a liczbie b resztę z dzielenia liczby większej przez mniejszą - gdy reszta dojdzie do zera, na tym kończymy, a NWD jest równe ostatniej dodatniej reszcie. (przykł.)

Przykład:

Wyznaczmy NWD liczb 365 i 94, korzystając z algorytmu Euklidesa mamy:

$365 = 94 \cdot 3 + 83$ Otrzymaliśmy resztę różną od zera, zatem teraz podzielimy liczbę 94 przez resztę 83.

$94 = 83 \cdot 1 + 11$

$83 = 11 \cdot 7 + 6$

$11 = 6 \cdot 1 + 5$

$6 = 5 \cdot 1 + 1$

$5 = 1 \cdot 5 + 0$

NWD(365, 94) = 1

Konstrukcja:

Załóżmy, że: $a, b \in \mathbf{N}$, $a > b$ oraz $a, b \neq 0$

1. Dzieląc z resztą a przez b otrzymujemy:

$$\mathbf{a = bc_1 + r_1,} \qquad \mathbf{0 < r_1 < b,}$$

$$\mathbf{b = r_1c_2 + r_2,} \qquad \mathbf{0 < r_2 < r_1,}$$

$$\mathbf{r1 = r_2c_3 + r_3,} \qquad \mathbf{0 < r_3 < r_2,}$$

$$\mathbf{. \quad . \quad .}$$

$$\mathbf{r_{n-2} = r_{n-1}c_n + r_n,} \qquad \mathbf{0 < r_n < r_{n-1}} \qquad \mathbf{r_n \text{ - ostatnia dodatnia reszta}}$$

$$\mathbf{r_{n-1} = r_nc_{n+1} + 0}$$

Ostatecznie otrzymujemy:

$$NWD(a, b) = NWD(b, r_1) = NWD(r_1, r_2) = NWD(r_2, r_3) = \cdots = NWD(r_{n2}, r_{n-1}) = NWD(r_{n-1}, r_n) = r_n.$$

Metoda wyznaczania x, y ∈ **Z** wynika z algorytmu Euklidesa. Istotnie, dla a, b ∈ **N**, a > b mamy:

$$
\begin{aligned}
a &= bc_1 + r_1,\\
b &= r_1c_2 + r_2,\\
r_1 &= r_2c_3 + r_3,\\
&\dots\\
r_{n-2} &= r_{n-1}q_n + r_n,\\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}
\quad\Rightarrow\quad
\begin{aligned}
r_1 &= a - bc_1,\\
r2 &= b - r_1c_2,\\
r3 &= r_1 - r_2c_3,\\
&\dots\\
r_n &= r_{n-2} - r_{n-1}c_n,\\
r_{n-1} &= r_nq_{n+1}
\end{aligned}
$$

$$r_1 = a - bc_1 = a + b(-c_1)$$

$$r_2 = b - r_1c_2 = b - (a + b(-c_1))c_2 = a(-c_2) + b(1 + c_1c_2)$$

$$r3 = r_1 - r_2c_3 = a + b(-c_1) - (a(-c_2) + b(1 + c_1c_2))c3 = a(1 + c_2c_3) + b(-c_1 - c_3 - c_1c_2c_3).$$

Twierdzenie:
Niech a, b ∈ **Z** oraz a i b ≠ 0. Wtedy istnieją takie liczby całkowite x, y, że NWD(a, b) = ax + by

Przykład:

1.Wyznaczymy liczby X i Y dla a = 314 i b =161

Znajdujemy NWD(314,161)

314 = 161 · 1 + 153
161 = 153 · 1 + 8
153 = 8 · 19 + 1
8 = 1 · 8 + 0

2. „Odwracamy" algorytm Euklidesa:

1 = 153 – 8 · 19 = 314 + 161 · (-1) – (314 · (-1) + 161 (1 + 1 · 1))19 = 314(1 + 1 · 19) + 161 (-1 – 19- 1 · 1 · 19)=
= 314 · 20 + 161 · (-39)

X = 20, Y = - 39

3. Równania diofantyczne stopnia pierwszego – równanie liniowe

Równaniem diofantycznym stopnia pierwszego nazywamy równanie liniowe postaci:

$a_1X_1 + a_2X_2 + \cdots + a_nX_n = b$, gdzie $a_1, \ldots, a_n$, $b \in \mathbf{Z}$, a szukane rozwiązania (X, Y) są liczbami całkowitymi.

Zauważmy, że dla n = 1 dostajemy równanie: $\mathbf{a_1X_1 = b}$

Takie równanie ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy $a_1 \mid b$ i wówczas $X = \frac{b}{a}$

Dla n = 2 otrzymujemy równanie postaci: $\mathbf{a_1X_1 + a_2X_2 = b}$

Kiedy takie równanie ma rozwiązanie?

Jeśli zastosować rozumowanie powyżej, to można przyjąć, że takie równanie ma rozwiązanie, gdy $a_1 \mid b$ i $a_2 \mid b$.

Zauważmy jednak, że np. równanie 4X + 6Y = 10 ma rozwiązanie X = 10 i Y = −5, pomimo iż 10 nie dzieli 4 ani 6 .

Jaki zatem warunek muszą spełniać współczynniki takiego równania, aby miało ono rozwiązanie?

Mówi nam o tym następujące twierdzenie:

Równanie diofantyczne aX + bY = c ma rozwiązanie wtedy i tylko wtedy, gdy $d \mid c$, gdzie d = NWD(a, b).

Ponadto jeśli (X_0, Y_0) jest pewnym rozwiązaniem tego równania, to wszystkie inne rozwiązania mają postać:

$$\begin{cases} X = X_0 + \frac{b}{d}t \\ Y = Y_0 - \frac{a}{d}t \end{cases}$$

Przykład:

a) $4X + 6Y = 9$, NWD(6,4) = 2 i $2 \mid 9$ zatem równanie nie ma rozwiązania.
b) $5X + 9Y = 2$, NWD (9,5) = 1 i $1 \mid 2$, czyli równanie ma rozwiązanie.

Obliczanie NWD(9,5) algorytmem Euklidesa i jego „odwracanie" w celu wyznaczenia X_0 i Y_0 :

$9 = 5 \cdot 1 + 4$
$5 = 4 \cdot 1 + 1$
$4 = 1 \cdot 4 + 0$ Zatem NWD(9,5) = 1

$1 = 5 - 4 \cdot 1 = 5 - (9 + 5(-1))1 = 9(-1) + 5(1 + 1 \cdot 1) = 9 \cdot (-1) + 5 \cdot 2 \quad | \cdot 2$
$2 = 9 \cdot (-2) + 5 \cdot 4$

Więc, $X_0 = 4$, a $Y_0 = -2$

$$\begin{cases} X = 4 + 9t \\ Y = -2 - 5t \end{cases}, \text{ gdy } t \in \mathbf{Z}$$

Ćw.1 Rozwiąż podany układ równań dla x, y ∈ **N** :

$$\begin{cases} XY = 720 \\ NWD(X, Y) = 4 \end{cases}$$

Rozwiązanie:
Zauważmy, że skoro NWD(x, y) = 4, to X = 4k i Y = 4l, gdzie NWD(k, l) = 1.
Podstawiając do pierwszego równania dostajemy:
$4k \cdot 4l = 720$
$16 \cdot k \cdot l = 720$
$k \cdot l = 45$
Ponieważ liczby k i l są względnie pierwsze, to

k	l
45	1
15	3
9	5

zatem

X	Y
180	4
60	12
36	20

Musimy wykluczyć pary (60, 12), (12,60), ponieważ ich NWD wynosi 12.
Odp. Szukane pary liczb to: (4,180), (180,4), (20,36), (36,20).

Ćw.2 Wyznacz wszystkie pary (x, y) liczb całkowitych spełniające równanie:

xy = 3x + 5y + 7

Przenieśmy 3x i 5y na lewą stroną równania:

xy - 3x – 5y = 7

Aby zapisać lewą stronę równania jako iloczyn dwóch wyrażeń algebraicznych dodajmy do obu stron 15:

xy – 3x – 5y + 15 = 7 + 15
xy – 3x – 5y + 15 = 22

teraz zapiszmy to w prostszej formie:

(x – 5)(y – 3) = 22

Iloczyn dwóch liczb całkowitych wynosi 22 wtedy i tylko wtedy, gdy:

22 = 1 · 22 = 22 · 1 = 11 · 2 = 2 · 11 = -1 · -22 = -22 · -1 = -2 · -11 = -11 · -2

a) $\begin{cases} x-5 = 1 \\ y-3 = 22 \end{cases}$ b) $\begin{cases} x-5 = 22 \\ y-3 = 1 \end{cases}$ c) $\begin{cases} x-5 = 11 \\ y-3 = 2 \end{cases}$ d) $\begin{cases} x-5 = 2 \\ y-3 = 11 \end{cases}$ e) $\begin{cases} x-5 = -1 \\ y-3 = -22 \end{cases}$ f) $\begin{cases} x-5 = -22 \\ y-3 = -1 \end{cases}$ g) $\begin{cases} x-5 = -11 \\ y-3 = -2 \end{cases}$ h) $\begin{cases} x-5 = -2 \\ y-3 = -11 \end{cases}$

a) $\begin{cases} x = 6 \\ y = 27 \end{cases}$ b) $\begin{cases} x = 27 \\ y = 4 \end{cases}$ c) $\begin{cases} x = 16 \\ y = 5 \end{cases}$ d) $\begin{cases} x = 7 \\ y = 14 \end{cases}$ e) $\begin{cases} x = 4 \\ y = -19 \end{cases}$ f) $\begin{cases} x = -17 \\ y = 2 \end{cases}$ g) $\begin{cases} x = 16 \\ y = 5 \end{cases}$ h) $\begin{cases} x = 3 \\ y = 8 \end{cases}$

Odpowiedź: Równanie spełniają następujące pary liczb: (6,25), (27,4), (16,5), (7,14), (4,-19), (-17,2), (-6,1), (3,-8) .

4. Równania diofantyczne stopnia drugiego – równanie Pitagorasa

- Trójki liczb, które spełniają twierdzenie Pitagorasa nazywamy trójkami pitagorejskimi.
- Jeśli NWD(a, b, c) = 1, liczby te tworzą trójkę pierwotną
- Najsławniejszą trójkę pitagorejską tworzą liczby 3, 4, 5 – nazywamy ją także trójką egipską.

Twierdzenie:
Wszystkie trójki pitagorejskie są postaci: $t(m^2 - n^2)$, $2tmn$, $t(m^2 + n^2)$, gdzie $m, n, t \in \mathbf{Z}$, $NWD(m, n) = 1$, $2 \nmid m - n$

Ostatni zapis oznacza, że liczby m oraz n dają różne reszty z dzielenia przez 2.

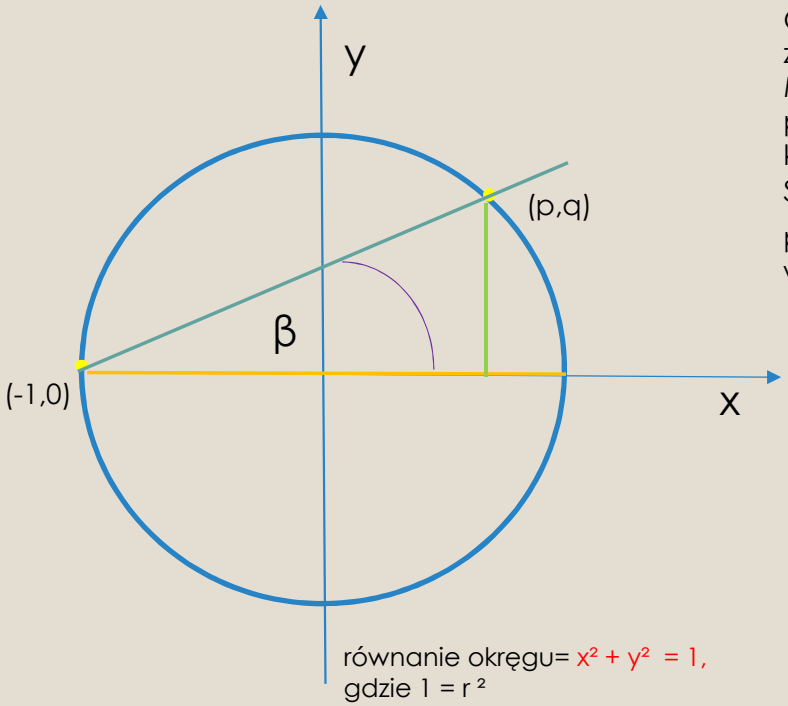
Dowód twierdzenia:

W wykrywaniu wszystkich trójek pitagorejskich pomoże nam kilka uproszczeń, które zawężą zakres poszukiwań, otóż:
1. Możemy ograniczyć zbiór wyników do liczb dodatnich, gdyż kwadrat nie zależy od znaku liczby do niego podnoszonej.
2. Jeżeli trójkę pitagorejską stanowią liczby: $\mathbf{(tx)^2 + (ty)^2 = (tz)^2 \Leftrightarrow t^2(x^2+y^2)=t^2(y^2)}$, to są nią także liczby x, y, z, więc możemy się ograniczyć do trójek zbudowanych z liczb względnie pierwszych.
3. Stw. Jedna z liczb a, b jest podzielna przez 2.
Zał. $2 \nmid a$ i $2 \nmid b$
Dow. 1, 2 dają resztę 1 z dzielenia przez 2. ($1 \equiv 1 (mod 2)$, $2 \equiv 1 (mod 2)$), czyli $a^2 + b^2$ powinny przypadku dzielenia przez 4 dawać resztę 0 lub 1, w zależności od wyniku (czy jest nim liczba parzysta, czy nieparzysta),
a otrzymujemy: dla $a = 2k + 1$, $b = 2l + 1$
$(2k + 1)^2 + (2l + 1)^2 = 4k^2 + 1 + 4k + 4l^2 + 1 + 4l = 4(k^2 + k + l^2 + l) + 2$, ($a^2 + b^2 \equiv 2 (mod 4)$) co jest nieprawdą.
Więc jedna z liczb a, b jest liczbą parzystą.

Przy wszystkich poprzednich uproszczeniach :

$a^2+b^2=c^2$ | : c ²

$(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$, gdzie $\frac{a}{c} = p$, $\frac{b}{c} = q$, (p,q) są parą pewnych punktów wymiernych, leżących na okręgu jednostkowym



Okazuje się, że potrafimy znaleźć pewną parę takich punktów, są nimi, np. (-1, 0), bo 1² + 0 = 1, zaznaczmy je na okręgu. Zaznaczmy także na okręgu punkty (p, q), które chcemy wyznaczyć. Możemy połączyć obie współrzędne pewną prostą przez nie przechodzącą. Równanie owej prostej wynosi załóżmy: y = a(x + b), gdzie współczynnik nachylenia prostej(a) wynosi tangens kąta jej nachylenia względem osi X.
Skoro a = tg β, to a = q / (p + 1), to y = $\frac{q}{p+1}$(x + b), gdzie b to taki punkt dla którego prosta przechodzi przez punkt (-1,0). W tym przypadku b = 1, bo 0 = a(-1 + 1), niezależnie od współczynnika.

Kiedy x ² + y² = 1, a = m i m ∈ **Q** mamy:
y = m(x + 1)
x² + (m(x+1)) ² = 1, po przegrupowaniu:

x²(m² + 1) + 2m²x + (m² - 1) = 0

Za x możemy podstawić zarówno -1, jak i p, więc pierwiastkami tego równania są -1 i p.

Korzystając ze wzorów Viete'a dla równania kwadratowego postaci: ax² + bx + c = 0 mamy, że:

$x_1 + x_2 = -b/a$, $x_1 \cdot x_2 = c/a$

Co w naszym przypadku daje:
- p = (m² - 1)/(m² + 1) | · (-1)
p = (1-m²)/ (1+ m²),
Wyznaczamy q ze wzoru m = q / p + 1 i po przekształceniu otrzymujemy:
q = m(p+1) = (2m) / (1+ m²)

Dla $m = k / l$ i $NWD(k, l) = 1$

$\frac{a}{c} = (k^2 - l^2) / (k^2 + l^2)$

$\frac{b}{c} = (2kl) / (k^2 + l^2)$

Skoro zakładamy, że NWD (k, l) = możemy stwierdzić, że (pewne) $a = k^2 - l^2$, $b = 2kl$, $c = k^2 + l^2$, wykryliśmy w ten sposób wszystkie trójki pierwotne.
Posługując się 2 uproszczeniem, mówiącym, że jeżeli trójkę pitagorejską stanowią liczby:
$(tx)^2 + (ty)^2 = (tz)^2 \Leftrightarrow t^2(x^2+y^2)=t^2(y^2)$, to są nią także liczby x, y, z, więc udowodniliśmy stwierdzenie.

5. Równania wyższych rzędów – równanie Fermata

Wielkie twierdzenie Fermata mówi, że dla wykładników $n \geq 3$ równanie $x_n + y_n = z_n$ nie ma rozwiązań w liczbach całkowitych dodatnich x, y, z.

Pierre de Fermat zanotował je na marginesie łacińskiego tłumaczenia książki „Arithmetica" Diofantosa i opatrzył następującą uwagą:

„Znalazłem zaiste zadziwiający dowód tego twierdzenia. Niestety, margines jest zbyt mały, by go pomieścić".

Twierdzenie zostało sformułowane przez Fermata w roku 1637. Opublikowano je dopiero w roku 1670, po odnalezieniu go w pozostałych po śmierci pismach Fermata i z miejsca stało się wyzwaniem dla kolejnych pokoleń matematyków – wiadomo bowiem było, że wiele twierdzeń formułowanych przez Fermata okazało się prawdziwymi, a ich dowody zostały znalezione przez innych. To jedno przez ponad 300 lat opierało się próbom dowodu w ogólności, znane były dowody szczególnych przypadków. Dlatego też nazwane zostało ostatnim twierdzeniem Fermata.

Dowód ostatecznie został przeprowadzony przez angielskiego matematyka **Andrew Johna Wilesa** dopiero w roku 1994, co było jedną z największych sensacji naukowych XX wieku. Zajmował ok. 100 stron A4 i wyrażony był w języku topologii i krzywych eliptycznych.

6. Zastosowania powyższych równań w zadaniach

Zad.1
Rozwiąż równania diofantyczne:
a) $45x + 60y = 5$
b) $314 + 161y = 9$
c) $966x-686y = 70$
d) $69x + 87y + 93z = 7$

Zad.2
Rozwiąż układy równań diofantycznych:

a) $\begin{cases} NWD(x, y) = 20 \\ y/x = 13/3 \end{cases}$

b) $\begin{cases} NWD(x,y) = 4 \\ NWW(x,y) = 56 \end{cases}$

c) $\begin{cases} x + y = 677 \\ NWW(x,y)/\ NWD(x,y) = 120 \end{cases}$

d) $\begin{cases} x + y = 210 \\ NWD(x,y) = 70 \end{cases}$

Zad.3
Rozwiąż w zbiorze liczb całkowitych:
$\frac{1}{x} + \frac{2}{xy} + \frac{3}{xy^2} = 1$

Zad.4
Udowodnij, że na okręgu $x^2 + y^2 = 3$ nie ma punktów wymiernych.

Opracowane na podstawie:

https://towarzystwo.edu.pl/assets/prace_matematyczne/2016_GimnNowyTarg_JJarzabek.pdf

https://pl.wikipedia.org/wiki/Twierdzenie_Fermata

http://knm.katowice.pl/licea/kolko/21.11.2011_beata_lojan/pliki/rownania_diofantyczne.pdf

https://youtu.be/RcomgYKqGE8