Równania diofantyczne

Beata Łojan

b.lojan@knm.katowice.pl

Koło Naukowe Matematyków
Uniwersytetu Śląskiego w Katowicach

www.knm.katowice.pl

III Liceum Ogólnokształcące im. Lucjana Szenwalda
w Dąbrowie Górniczej

Spis treści

Dąbrowa Górnicza, 21 listopada 2011

1. Algorytm Euklidesa

Definicja 1.1. Niech $a, b \in \mathbb{Z}$ i $b \neq 0$. Mówimy, że a jest *podzielne z resztą* przez b jeśli istnieją takie liczby $q \in \mathbb{Z}$ i $r \in \mathbb{N} \cup \{0\}$, że $a = bq + r$ oraz $0 \leqslant r < |b|$. Mówimy, że a jest *podzielne* przez b jeśli istnieje taka liczba całkowita a, że $a = bq$ (czyli reszta z dzielenia $r = 0$). Wtedy b nazywamy *dzielnikiem* liczby a.

Największym wspólnym dzielnikiem liczb całkowitych a i b nazywamy liczbę naturalną d, która jest wspólnym dzielnikiem liczb a i b oraz każdy inny wspólny dzielnik liczb a i b dzieli d.

Definicja 1.2. Niech $a, b \in \mathbb{Z}$ oraz $a \neq 0$ lub $b \neq 0$. Liczby a i b nazywamy *względnie pierwszymi* jeśli $\mathrm{NWD}(a, b) = 1$.

Twierdzenie 1.1. *Niech* $a, b \in \mathbb{N}$. *Wtedy* $ab = \mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b)$.

Twierdzenie 1.2. *Niech* $a, b \in \mathbb{Z}$ *oraz* $a \neq 0$ *i* $b \neq 0$. *Wówczas:*

$$a = bq + r \Rightarrow \mathrm{NWD}(a, b) = \mathrm{NWD}(b, r).$$

Konstrukcja 1.1 (Algorytm Euklidesa)**.** Załóżmy, że $a, b \in \mathbb{N}$ oraz $a \geqslant b$. Dzieląc z resztą a przez b otrzymujemy

Najmniejszą wspólną wielokrotnością liczb całkowitych a i b nazywamy najmniejszą liczbę naturalną w, której dzielnikami są liczby a i b, przy czym jeśli istnieje jakaś inna liczba w' o tych własnościach, to liczba w jest jej dzielnikiem.

$$a = bq_1 + r_1, \text{ gdzie } 0 \leqslant r_1 < |b| = b.$$

Jeśli $r_1 = 0$, to $\mathrm{NWD}(a, b) = b$, natomiast jeśli $r_1 > 0$, to dzielimy z resztą b przez r_1. Wtedy

$$b = r_1 q_2 + r_2, \text{ gdzie } 0 \leqslant r_2 < r_2.$$

Wówczas jeśli $r_2 = 0$, to $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, r_1) = r_1$, a jeśli $r_2 > 0$, to postępujemy jak poprzednio, czyli dzielimy z resztą r_1 przez r_2. Dostajemy

$$r_1 = r_2 q_3 + r_3, \text{ gdzie } 0 \leqslant r_3 < r_2.$$

Jeśli $r_3 = 0$, to $\mathrm{NWD}(a, b) = \mathrm{NWD}(b, r_1) = \mathrm{NWD}(r_1, r_2) = r_2$. Jeśli $r_3 > 0$, to postępujemy jak poprzednio.

Algorytm Euklidesa — algorytm obliczania największego wspólnego dzielnika dwóch liczb całkowitych. Jest to jeden z najstarszych algorytmów — został opisany przez Euklidesa ok. roku 300 p.n.e. Opiera się on na spostrzeżeniu, że jeśli od większej liczby odejmiesz mniejszą, to mniejsza liczba i otrzymana różnica będą miały taki sam największy wspólny dzielnik jak pierwotne liczby. Jeśli w wyniku kolejnego odejmowania otrzymasz parę równych liczb, oznacza to, że znalazłeś NWD. Można również zamiast odejmować brać reszty z dzielenia większej liczby przez mniejszą — gdy reszta dojdzie do zera, to kończymy, a NWD jest równe przedostatniej reszcie.

To postępowanie musi się skończyć, bo $0 \leqslant r_n < \cdots < r_3 < r_2 < r_1$, czyli istnieje takie $n \in \mathbb{N}$, że

$$\begin{aligned}
a &= bq_1 + r_1, && 0 \leqslant r_1 < b \\
b &= r_1 q_2 + r_2, && 0 \leqslant r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, && 0 \leqslant r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, && 0 \leqslant r_n < r_{n-1} \\
r_{n-1} &= r_n + q_{n+1} + 0
\end{aligned}$$

Ostatecznie dostajemy, że

$$\begin{aligned}
\mathrm{NWD}(a, b) = \mathrm{NWD}(b, r_1) = \mathrm{NWD}(r_1, r_2) = \mathrm{NWD}(r_2, r_3) = \cdots = \\
= \mathrm{NWD}(r_{n_2}, r_{n-1}) = \mathrm{NWD}(r_{n-1}, r_n) = r_n.
\end{aligned}$$

Przykład 1.1. Wyznaczymy $\mathrm{NWD}(26, 10)$.

$$\begin{aligned}
26 &= 10 \cdot 2 + 6 \\
10 &= 6 \cdot 1 + 4 \\
6 &= 4 \cdot 1 + \underbrace{2} \\
4 &= 2 \cdot 2 + 0
\end{aligned}$$

Zatem $\mathrm{NWD}(26, 10) = 2$.

Twierdzenie 1.3. *Niech* $a, b \in \mathbb{Z}$ *oraz* $a \neq 0$ *i* $b \neq 0$. *Wtedy istnieją takie liczby całkowite* x, y*, że*

$$\mathrm{NWD}(a, b) = ax + by.$$

Uwaga 1.1. Z algorytmu Euklidesa wynika metoda wyznaczania $x, y \in \mathbb{Z}$. Istotnie, dla $a, b \in \mathbb{N}$, $a \geqslant b$ mamy:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \\ r_{n-1} &= r_n + q_{n+1} + 0 \end{aligned}$$

Mamy:

$$\begin{aligned} r_1 &= a - bq_1 = a + b(-q_1) \\ r_2 &= b - r_1q_2 = b - (a + b - q_1)q_2 = a(-q_2) + b(1 + q_1q_2) \\ r_3 &= r_1 - r_2q_3 = abq_1 - (aq_2 - b(1 + q_1q_2))q_3 = \\ &= a(1 - q_2q_3) + b(-q_1 - q_3 - q_1q_2q_3). \end{aligned}$$

Postępując tak dalej mamy $r_n = 0$ oraz

$$a(\text{coś zależenego od } q_1, \ldots, q_n) + b(\text{coś zależnego od } q_1, \ldots, q_n) = ax + by$$

Przykład 1.2. Pokażemy na przykładzie jak wyznaczyć liczby X i Y. Niech $a = 234$ i $b = 164$. Korzystając z algorytmu Euklidesa wyznaczymy NWD(234, 164):

$$\begin{aligned} 234 &= 164 \cdot 1 + 70 \\ 164 &= 70 \cdot 2 + 24 \\ 70 &= 24 \cdot 2 + 22 \\ 24 &= 22 \cdot 1 + \underbrace{2}_{} \\ 22 &= 2 \cdot 11 + 0 \end{aligned}$$

Mamy zatem, że $\text{NWD}(234, 164) = 2$, a „odwracając" algorytm Euklides dostajemy:

$$\begin{aligned} 2 &= 24 - 22 \cdot 1 = 24 - (70 - 24 \cdot 2) = 24 - 70 \cdot 1 + 24 \cdot 2 = \\ &= 24 \cdot 3 - 70 \cdot 1 = 3(164 \cdot 1 - 70 \cdot 2) - 70 \cdot 1 = 3 \cdot 164 - 6 \cdot 70 - 1 \cdot 70 = \\ &= 3 \cdot 164 - 7 \cdot 234 + 7 \cdot 164 = (-7) \cdot 234 + 10 \cdot 164 \end{aligned}$$

Zatem $2 = (-7) \cdot 234 + 10 \cdot 164$, czyli $X = -7$, $Y = 10$.

2. Równania diofantyczne

Równaniem diofantycznym nazywamy każde równanie, którego rozwiązań szukamy w zbiorze liczb całkowitych lub naturalnych. Zajmiemy się najprostszymi z nich, czyli równaniami liniowymi. Nazwa tego typu równań pochodzi od greckiego matematyka Diofantosa (III w.n.e.).

Ile lat żył Diofantos?

W XIV wieku grecki mnich Maksymus Planudes umieścił w swojej antologii wiersz „Epitafium Diofanta". Jego treść jest jednocześnie zadaniem tekstowym:

Pod tym nagrobkiem spoczywa Diofant – a dzięki przedziwnej
Sztuce zmarłego i wiek zdradzi ci ten głaz:
Chłopcem przez szóstą część życia pozostać bóg mu pozwolił,
Lica pokwitły mu zaś, kiedy dwunasta znów część
Życia minęła; a znowu żywota gdy 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 Hades.
Kojąc ogromny swój ból, szukał Diofant wśród liczb
Jeszcze przez cztery lata pociechy, aż rozstał się z życiem.

2.1. Równania diofantyczne stopnia pierwszego

Definicja 2.1. *Równaniem diofantycznym stopnia pierwszego* nazywamy równanie liniowe postaci

$$a_1X_1 + a_2X_2 + \cdots + a_nX_n = b,$$

$$\left(\text{Inaczej: } \sum_{i=1}^{n} a_iX_i = b\right)$$

gdzie $a_1, \ldots, a_n, b \in \mathbb{Z}$, a szukane rozwiązania (X, Y) są liczbami całkowitymi.

Zauważmy, że dla $n = 1$ dostajemy równanie: $a_1X_1 = b$. Takie równanie ma rozwiązanie w liczbach całkowitych wtedy i tylko wtedy, gdy $a_1|b$ i wówczas $X = \frac{b}{a}$. Rozważmy równanie $6X = 12$; Oczywiście $6|12$ oraz $X = \frac{12}{6} = 2$.

Dla $n = 2$ dostajemy równanie postaci $a_1X_1 + a_2X_2 = b$. Kiedy takie równanie ma rozwiązanie? Jeśli zastosować rozumowanie powyżej, to można przyjąć, że takie równanie ma rozwiązanie, gdy $a_1|b$ i $a_2|b$. Zauważmy jednak, że np. równanie $4X + 6Y = 10$ ma rozwiązanie $X = 10$ i $Y = -5$, pomimo iż $4 \nmid 10$ i $6 \nmid 10$.

Jaki zatem warunek muszą spełniać współczynniki takiego równania, aby miało ono rozwiązanie? Mówi nam o tym następujące twierdzenie:

Twierdzenie 2.1. *Równanie diofantyczne* $aX + bY = c$ *ma rozwiązanie wtedy i tylko wtedy, gdy* $d|c$, *gdzie* $d = \text{NWD}(a, b)$. *Ponadto jeśli* (X_0, Y_0) *jest pewnym rozwiązaniem tego równania, to wszystkie inne rozwiązania mają postać:*

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

Uwaga 2.1. Ogólnie: Równanie diofantyczne $a_1X_1 + a_2X_2 + \cdots + a_nX_n = b$ ma rozwiązanie wtedy i tylko wtedy, gdy $\text{NWD}(a_1, \ldots, a_n) \mid b$.

Przykład 2.1.

(a) $2X + 6Y = 3$, $\text{NWD}(2, 6) = 2$ i $2 \nmid 3$ zatem równanie nie ma rozwiązania,

(b) $3X + 5Y = 11$, $\text{NWD}(3, 5) = 1$ i $1|11$, czyli równanie ma rozwiązanie.
Wiemy, że istnieją liczby całkowite X, Y, że $\text{NWD}(3, 5) = 3X + 5Y = 1$. Korzystając z algorytmu Euklidesa mamy:

$$\begin{aligned} 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + \underbrace{1} \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) = 3 \cdot 2 + 5 \cdot (-1) | \cdot 11 \\ 11 &= 3 \cdot 22 + 5 \cdot (-11) \end{aligned}$$

Zatem $X_0 = 22$ i $Y_0 = -11$. Ostatecznie:

$$\begin{cases} X = 22 + 5t, & t \in \mathbb{Z} \\ Y = -11 - 3t, & t \in \mathbb{Z} \end{cases}$$

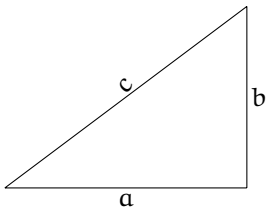
Przykład 2.2. Wiemy już, że $\text{NWD}(234, 164) = 2 = (-7) \cdot 234 + 10 \cdot 164$. Zauważmy, że poszukiwanie liczb X i Y sprowadza się do rozwiązania równania diofantycznego $234X + 164Y = 2$. Zatem rozwiązaniem tego równania jest

$$\begin{cases} X &= -7 + \frac{164}{2} \cdot t = -7 + 82 \cdot t \\ Y &= 10 - \frac{234}{2} \cdot t = 10 - 117 \cdot t \end{cases}$$

2.2. Równania drugiego stopnia — Równanie Pitagorasa

Z twierdzenia Pitagorasa wiemy, że boki trójkąta prostokątnego spełniają zależność

$$a^2 + b^2 = c^2.$$



Takie trójki liczb nazywamy *trójkami pitagorejskimi*; jeśli liczby a, b, c nie mają wspólnego dzielnika, to mówimy wtedy o trójce *pierwotnej*.

Najbardziej chyba znaną trójką jest (3,4,5). Rozwiązując równanie:

$$X^2 + Y^2 = Z^2$$

otrzymamy odpowiedź na pytanie: jakie inne trójkąty, których boki są liczbami naturalnymi, możemy jeszcze skonstruować.

Każde rozwiązanie (X_0, Y_0, Z_0) tego równania możemy zapisać w postaci:

$$\begin{aligned} X_0 &= m^2 - n^2 \\ Y_0 &= 2mn \\ Z_0 &= m^2 + n^2, \end{aligned}$$

gdzie $m, n \in \mathbb{N}$ są liczbami względnie pierwszymi (tzn.: $\mathrm{NWD}(m, n) = 1$) oraz jedna z nich jest liczbą parzystą.

m	2	3	4	5	5
n	1	2	1	2	3
X	3	5	15	21	9
Y	4	12	8	20	40
Z	5	13	17	29	41

2.3. Równania wyższych rzędów — Równanie Fermata

Historia zmagań ze znalezieniem dowodu WTF jest długa i obfitowała w wiele pomyłek znanych matematyków. W roku 1993 amerykański matematyk Andrew Wiles na wykładzie w Instytucie Newtona Uniwersytetu w Cambridge ogłosił, że udowodnił WTF. Jednak dopiero po dwóch latach, w roku 1995, po usunięciu luk w dowodzie, ukazały się dwie prace naukowe Wilesa, zawierające pełny dowód.

Najbardziej znanym równaniem diofantycznym jest *równanie Fermata*

$$X^n + Y^n = Z^n$$

Fermat w swoim egzamplarzu *Arytmetyki Diofantosa* na marginesie strony z rozwiązaniem równania Pitagorasa napisał:

„Nie można podzielić sześcianu na dwa sześciany ani czwartej potęgi na dwie czwarte potęgi, ani ogólnie żadnej potęgi wyższej niż druga na dwie takie same potęgi; znalazłem zaprawdę zadziwiający dowód tego, lecz ten margines jest zbyt wąski, by go zmieścić."

Twierdzenie 2.2 (Wielkie twierdzenie Fermata)**.** *Dla $n \geqslant 3$ równanie*

$$X^n + Y^n = Z^n$$

nie ma rozwiązania w liczbach naturalnych.

3. Zastosowania

Zadanie 3.1. Ile biletów po 3zł i 5zł można kupić za 149zł, jeśli należy wydać wszystkie możliwe pieniądze?

Rozwiązanie. Niech X będzie liczbą biletów po 3zł, a Y liczbą biletów po 5zł. Wówczas treść naszego zadania możemy opisać równaniem:

$$3X + 5Y = 149$$

Zauważmy, że $\mathrm{NWD}(5, 3) = 1$ oraz $1 \mid 149$, zatem równanie to ma rozwiązanie. Korzystając z algorytmu Euklidesa dostajemy:

$$\begin{aligned} 5 &= 3\cdot 1+2 & & 1 = 3-2\cdot 1\\ 3 &= 2\cdot 1+\underbrace{1} & \Rightarrow \quad & 1 = 3-(5-3\cdot 1)\\ 2 &= 2\cdot 1+0 & & 1 = (-1)\cdot 5+2\cdot 3 \end{aligned}$$

Przemnóżmy ostatnią równość przez 149, wówczas:

$$149 = (-149)\cdot 5+298\cdot 3$$

Zatem rozwiązaniem wyjściowego równania jest para $X_0 = -149$ i $Y_0 = 298$. Wszystkie rozwiązania są więc postaci:

$$\begin{cases} X &= 298+5\cdot t\\ Y &= -149-3\cdot t \end{cases}$$

Musimy odrzucić rozwiązania ujemne, czyli dobrać takie t, aby $X > 0$ i $Y > 0$. Mamy:

$$-59 \leqslant t \leqslant -50.$$

Zatem bilety można kupić na 10 różnych sposobów:

t	-59	-58	-57	-56	-55	-54	-53	-52	-51	-50
X	3	8	13	18	23	28	33	38	43	48
Y	28	25	22	19	16	13	10	7	4	1

Zadanie 3.2. Ile lat żył Diofantos?

Rozwiązanie. Treść zagadki możem zapisać:

$\frac{1}{6}$ życia zajęła mu młodość
potem po $\frac{1}{12}$ życia wyrosła mu broda
następnie po $\frac{1}{7}$ życia ożenił się,
po 5 latach urodził mu się syn,
syn żył połowę krócej od ojca,
ojciec zmarł 4 lata po synu.

Oznaczmy wiek Diofantosa przez X. Wystarczy zatem rozwiązać równanie:

$$\frac{1}{6}X+\frac{1}{12}X+\frac{1}{7}X+5+\frac{1}{2}X+4 = X$$

Po przekształceniach dostejemy $X = 84$. Zatem Diofantos żył 84 lata.

Zadanie 3.3. Rozwiązać układ równań:

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

Rozwiązanie. Zauważmy, że skoro $\mathrm{NWD}(X,Y) = 4$, to $X = 4k$ i $Y = 4l$, gdzie $\mathrm{NWD}(k,l) = 1$. Podstawiając do pierwszego równania dostejmy:

$$\begin{aligned} 4k\cdot 4l &= 720\\ 16\cdot k\cdot l &= 720\\ k\cdot l &= 45 \end{aligned}$$

Ponieważ liczby k i l są względnie pierwsze, to

k	l		X	Y
1	45		4	180
3	15	a zatem	20	36
5	9		36	20
9	5		180	4

Odpowiedź: Szukane pary liczb to $(4,180)$, $(20,36)$, $(36,20)$.

4. Zadania

Zadanie 4.1. Rozwiąż równania diofantyczne:

(i) $112X + 129Y = 2$;

(ii) $13X + 29Y = 31$;

(iii) $2X + 8Y + 112Z = 9$;

(iv) $10X + 119Y + 161Z = 83$;

Zadanie 4.2. Rozwiąż układy równań:

(i)
$$\begin{cases} \text{NWD}(X,Y) &= 15 \\ \text{NWW}(X,Y) &= 420 \end{cases}$$

(ii)
$$\begin{cases} \frac{X}{Y} &= \frac{11}{7} \\ \text{NWD}(X,Y) &= 45 \end{cases}$$

(iii)
$$\begin{cases} X+Y &= 180 \\ \text{NWD}(X,Y) &= 30 \end{cases}$$

(iv)
$$\begin{cases} X+Y &= 667 \\ \frac{\text{NWW}(X,Y)}{\text{NWD}(X,Y)} &= 120 \end{cases}$$

Zadanie 4.3. Do przewozu zboża są do dyspozycji worki sześćdziesięciokilogramowe i osiemdziesięciokilogramowe. Ile potrzeba poszczególnych worków do przewozu 440 kg zboża (zakładamy, że worki muszą być pełne)?

Zadanie 4.4 (Olimpiada matematyczna)**.** Fabryka wysyła towar w paczkach po 3 kg i po 5 kg. Wykazać, że można w ten sposób wysłać każdą całkowitą ilość kilogramów większą niż 7.

Zadanie 4.5 (Olimpiada matematyczna)**.** W czasie pierwszej wojny światowej toczyła się bitwa w pobliżu pewnego zamku. Jeden z pocisków rozbił stojącą u wejścia do zamku statuę 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 stała statua, równa się 451066. W którym roku postawiono statue?

Zadanie 4.6. 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 lub 0 głów, lub 14 głów lub 349 głów. Smok zostanie zabity, gdy wszystkie głowy będą ścięte. Czy istnieje taka strategia walki rycerza ze smokiem, aby smok zginął?

Literatura

[1] N.Koblitz, *Wykład z teorii liczb i kryptografii*, WNT, Warszawa, 1995

[2] W.Narkiewicz, *Teoria liczb*, Wydawnictwa Naukowe PWN, Warszawa 2003;

[3] W.Sierpiński, *250 zadań z elementarnej teorii liczb*, Biblioteczka Matematyczna 17, PZWS, Warszawa 1987

[4] W.Sierpiński, *Wstep do teorii liczb*, Biblioteczka Matematyczna 25, PZWS, Warszawa 1965.