Programowanie
po 3 wykładzie

Andrzej Giniewicz

15.03.2024

W obecnym bloku materiału po wykładzie zajmiemy się podzielnością, algorytmem Euklidesa, rozszerzonym algorytmem Euklidesa oraz równaniem diofantycznym liniowym. Dowiemy się też, jak wydać 500 zł na herbatę.

1 Największy wspólny dzielnik: algorytm naiwny

Do sprawdzenia największego wspólnego dzielnika może posłużyć sprawdzanie reszty z dzielenia. Największy wspólny dzielnik liczb a i b będziemy oznaczać przez $\gcd\{a, b\}$ od angielskiego *greatest common divisor*. Można zobaczyć, że

$$1 \leqslant \gcd\{a, b\} \leqslant \min\{a, b\}.$$

Lewa strona nierówności wynika z tego, że dla liczb naturalnych a i b, jedynka zawsze jest ich wspólnym dzielnikiem. Prawa strona nierówności może być wytłumaczona w ten sposób, że aby coś było dzielnikiem liczby, nie może być od niej większe. Oznacza to, że wspólny dzielnik dwóch liczb, musi być dzielnikiem każdej z nich, czyli musi być mniejszy bądź równy od ich minimum.

Poszukać największego wspólnego dzielnika możemy zatem za pomocą pętli idącej od $\min\{a, b\}$ do 1.

```
def gcd_loop(a, b):
    for n in range(min(a, b), 1, -1):
        if a%n==0 and b%n==0:
            return n
    return 1
```

W przypadku pesymistycznym, gdy liczby a i b są względnie pierwsze, czyli $\gcd\{a, b\} = 1$, pętla sprawdzi wszystkie wartości od $\min\{a, b\}$ do 2, po czym zwróci 1. Oznacza to, że w najgorszym wypadku algorytm wykona w przybliżeniu $\min\{a, b\}$ kroków.

2 Największy wspólny dzielnik: algorytm Euklidesa

Algorytm Euklidesa jest innym algorytmem służącym do wyznaczania największego wspólnego dzielnika dwóch liczb naturalnych, znanym od ponad 2300 lat[1]. Algorytm określony jest rekurencyjnie w następujący sposób,

$$\begin{aligned} &\gcd\{a, 0\} = a, \\ &\gcd\{a, b\} = \gcd\{b, a \bmod b\}, \qquad \text{gdy } b > 0, \end{aligned}$$

gdzie $a \bmod b$ to reszta z dzielenia a przez b.

Dowód. Przedstawimy teraz dowód algorytmu Euklidesa. Wykorzystamy indukcję ze względu na drugą zmienną funkcji gcd.

Warunek początkowy. Warunek $\gcd\{a, 0\} = a$ jest spełniony, ponieważ każda liczba dzieli zero, czyli wszystkie dzielniki liczby a są też dzielnikami 0. Wobec tego największy dzielnik liczby a jest największym wspólnym dzielnikiem a i 0, stąd a jest największym wspólnym dzielnikiem a i 0.

Założenie indukcyjne. Załóżmy teraz, że algorytm Euklidesa działa dla $\gcd\{x, y\}$, gdzie $0 \leqslant y < b$.

Krok indukcyjny. Pokażemy, że algorytm Euklidesa działa dla $\gcd\{a, b\}$. Pokażemy, że $\gcd\{a, b\} = \gcd\{b, a \bmod b\}$, co ponieważ $a \bmod b < b$ z założenia indukcyjnego zagwarantuje nam tezę.

Zauważmy, że $b \neq 0$, zatem istnieje $q \in \mathbb{Z}$ takie, że

$$a = qb + a \bmod b.$$

Wartość q jest w powyższym równaniu wynikiem dzielenia całkowitego a przez b.

Ponieważ $\gcd\{a, b\}$ dzieli a i dzieli b (jest wspólnym dzielnikiem), $\gcd\{a, b\}$ dzieli również $a \bmod b$, ponieważ

$$a \bmod b = a - qb$$

i q jest całkowite. Oznacza to, że $\gcd\{a, b\}$ dzieli b (ponieważ jest wspólnym dzielnikiem a i b) oraz dzieli $a \bmod b$ (co pokazaliśmy powyżej), czyli jest wspólnym dzielnikiem liczb b i $a \bmod b$, choć niekoniecznie ich największym wspólnym dzielnikiem. Wobec tego

$$\gcd\{a, b\} \leqslant \gcd\{b, a \bmod b\}.$$

Spójrzmy teraz na $\gcd\{b, a \bmod b\}$. Liczba ta dzieli b i dzieli $a \bmod b$, zatem dzieli również $a = qb + a \bmod b$. Ponieważ $\gcd\{b, a \bmod b\}$ dzieli b i dzieli a, jest wspólnym dzielnikiem a i b, choć niekoniecznie ich największym wspólnym dzielnikiem. Wobec tego

$$\gcd\{b, a \bmod b\} \leqslant \gcd\{a, b\}.$$

[1] Euklides opisał ten algorytm w księdze VII (stwierdzenie 3) i księdze X (stwierdzenie 4) swoich „Elementów". „Elementy" Euklidesa można przeczytać online na stronie `http://aleph0.clarku.edu/~djoyce/elements/elements.html`. Jest to jeden z najstarszych podręczników do matematyki.

Pokazaliśmy, że

$$\gcd\{a, b\} \leqslant \gcd\{b, a \bmod b\} \leqslant \gcd\{a, b\},$$

zatem musi zachodzić

$$\gcd\{a, b\} = \gcd\{b, a \bmod b\}.$$

Pokazaliśmy, że

$$\gcd\{a, b\} = \gcd\{b, a \bmod b\}.$$

Wiemy również, że $a \bmod b < b$, zatem z założenia indukcyjnego, prawa strona powyższej równości jest prawidłowym sposobem wyznaczania największego wspólnego dzielnika. W połączeniu z warunkiem początkowym $\gcd\{a, 0\} = a$, kończy to dowód. □

Postaramy się teraz przeanalizować liczbę kroków algorytmu, aby wiedzieć, czy opłaca się stosować algorytm Euklidesa w porównaniu z naiwnym algorytmem z poprzedniego podrozdziału, który trwał mniej niż $\min\{a, b\}$ kroków.

Zauważmy, że po jednym kroku algorytmu, mamy zagwarantowane to, że pierwszy argument funkcji jest ostro większy od drugiego, ponieważ mamy $\gcd\{b, a \bmod b\}$ oraz z definicji reszty z dzielenia $0 \leqslant a \bmod b < b$. Oznacza to, że jeśli uruchomimy funkcję gcd z pierwszym argumentem poniżej drugiego, funkcja „skoryguje to" już w jednym kroku, w szczególności, jeśli $a < b$, to

$$\gcd\{a, b\} = \gcd\{b, a \bmod b\} = \gcd\{b, a\}.$$

Wobec tego w obliczeniach liczby kroków będziemy zakładać, że $a > b$, ponieważ gdy to równanie nie jest spełnione, to dodajemy co najwyżej jeden krok.

Twierdzenie 1 (twierdzenie Lamyégo). *Niech n będzie liczbą kroków wykonaną przez algorytm Euklidesa obliczający* $\gcd\{a, b\}$ *dla $a > b$. Wtedy $b \geqslant F_{n+1}$, gdzie F_{n+1} jest $n + 1$ liczbą Fibonacciego.*

Dowód. Zauważmy, że algorytm Euklidesa wykonujący n kroków wylicza pary (a_k, b_k) zaczynając od (a_n, b_n) i schodząc do (a_0, b_0). O ciągach a_k i b_k wiemy, że $a_n = a$, $b_n = b$, $a_{k-1} = b_k$ oraz $b_{k-1} = a_k \bmod b_k$. Ponieważ algorytm wykonał n kroków, czyli krok 0 jest ostatnim krokiem, to $b_0 = 0$ oraz $a_0 = \gcd\{a, b\}$. Z założenia $a > b$ mamy, że dla każdego $k = 0, \ldots, n$, zachodzi $a_k > b_k$.

Udowodnimy najpierw nierówność

$$b_{k+1} \geqslant b_k + b_{k-1}.$$

Z definicji ewolucji wyrazów ciągu, mamy $a_k = b_{k+1}$ oraz $b_{k-1} = a_k \bmod b_k$. Łącząc te dwa fakty uzyskujemy $b_{k-1} = b_{k+1} \bmod b_k$. Wobec tego, skoro b_{k-1} jest resztą z dzielenia b_{k+1} przez b_k, to rozpisując b_{k+1} dla pewnego $p \geqslant 1$ (będącego wynikiem dzielenia całkowitego b_{k+1} przez b_k) zachodzi

$$b_{k+1} = pb_k + b_{k-1}.$$

Stąd, ponieważ $p \geqslant 1$,

$$b_{k+1} \geqslant b_k + b_{k-1}.$$

Wykonajmy teraz indukcję ze względu na liczbę kroków algorytmu, czyli n.

Warunek początkowy. Jeśli algorytm kończy się w jednym kroku, oznacza to, że $b > 0$, zatem najmniejsza liczba b spełniająca tę nierówność to $F_2 = 1$. Wobec tego, dla $n = 1$ mamy $b_n \geqslant F_{n+1}$, co jest zgodne z twierdzeniem.

Założenie indukcyjne. Załóżmy, że $b_k \geqslant F_k$ dla $k < n$.

Krok indukcyjny. Z udowodnionej nierówności

$$b_n \geqslant b_{n-1} + b_{n-2}.$$

Z założenia indukcyjnego $b_{n-1} \geqslant F_n$ oraz $b_{n-2} \geqslant F_{n-1}$. W połączeniu z definicją liczb Fibonacciego,

$$b = b_n \geqslant b_{n-1} + b_{n-2} \geqslant F_n + F_{n-1} = F_{n+1},$$

co kończy dowód. □

Korzystając z postaci nierekurencyjnej liczb Fibonacciego, mamy

$$a > b \geqslant F_{n+1} = \left\lfloor \frac{\varphi^{n+1}}{\sqrt{5}} + \frac{1}{2} \right\rfloor,$$

co przekłada się na

$$\min\{a, b\} \geqslant \left\lfloor \frac{\varphi^{n+1}}{\sqrt{5}} + \frac{1}{2} \right\rfloor \approx \frac{\varphi^{n+1}}{\sqrt{5}},$$

gdzie

$$\varphi = \frac{1 + \sqrt{5}}{2}.$$

Aby oszacować liczbę kroków, musimy odnaleźć najmniejsze n spełniające powyższą nierówność. Oszacowaniem tej liczby będzie n spełniające

$$\min\{a, b\} \approx \frac{\varphi^{n+1}}{\sqrt{5}},$$

czyli

$$n \approx \log_\varphi \left(\sqrt{5} \min\{a, b\} \right) - 1.$$

Załóżmy teraz, że a i b są dowolne. Ponieważ wtedy gdy $a < b$ musimy wykonać jeden dodatkowy krok, aby zachodziło $a > b$, to dobrym oszacowaniem wydaje się wartość

$$n \approx \log_\varphi \left(\sqrt{5} \min\{a, b\} \right).$$

Oznacza to, że algorytm Euklidesa jest bardzo szybkim algorytmem, wykonującym jedynie logarytmiczną liczbę kroków i w dodatku logarytmiczną liczbę od mniejszej z dwóch wartości a i b.

Prosty algorytm iteracyjny w przypadku pesymistycznym do obliczenia

$$\gcd\{1024, 57390571\},$$

wykona 1024 kroki, podczas gdy algorytm Euklidesa wykona około

$$n \approx \log_\varphi \left(\sqrt{5} \cdot 1024 \right) \approx 16$$

kroków, czyli będzie około 64 razy szybszy.

3 Równanie diofantyczne liniowe

Równanie diofantyczne liniowe to równanie

$$ax + by = c$$

dla ustalonych liczb całkowitych a, b, c, dla których a i b nie są jednocześnie zerem. Równanie to rozwiązujemy w liczbach całkowitych, czyli szukamy liczb całkowitych x, y spełniających powyższe równanie (równanie to nie stanowi problemu w liczbach rzeczywistych).

3.1 Istnienie rozwiązania

W liczbach całkowitych równanie to nie zawsze ma rozwiązanie. Okazuje się, że równanie diofantyczne liniowe $ax + by = c$ ma rozwiązanie wtedy i tylko wtedy, gdy $\gcd\{a, b\}$ dzieli c. Udowodnimy to w twierdzeniu poprzedzonym dwoma lematami.

Lemat 1. *Liczby całkowite a i b są względnie pierwsze wtedy i tylko wtedy, gdy*

$$\exists\, x,y \in \mathbb{Z}: \quad ax + by = 1.$$

Dowód. Udowodnimy dwie implikacje.

Zacznijmy od $\Longrightarrow$. Załóżmy, że liczby całkowite a i b są względnie pierwsze. Wtedy z definicji tego, że liczby te są względnie pierwsze, ich największy wspólny dzielnik to 1. Co więcej, aby w ogóle mówić o liczbach względnie pierwszych, choć jedna z nich musi być niezerowa.

Niech $S = \{ax+by : x, y \in \mathbb{Z}\}$. Chcemy pokazać, że 1 należy do S, co zagwarantuje nam tezę. W tym celu pokażemy najpierw, że w zbiorze S istnieje choć jedna liczba dodatnia. Jest tak, ponieważ $a^2+b^2 \in S$ i choć jedna z liczb a oraz b jest dodatnia, więc $aa+bb = a^2+b^2 > 0$. Ponieważ w zbiorze S istnieje choć jedna liczba dodatnia, istnieje w nim najmniejsza liczba dodatnia. Nazwijmy ją d. Wystarczy sprawdzić, że $d = 1$. Ponieważ $d \in S$, istnieją x i y takie, że $d = ax + by$.

Pokażemy teraz, że d jest wspólnym dzielnikiem a i b. Podzielmy najpierw a przez d z resztą. Mamy

$$a : d = q \text{ reszty } r,$$

dla pewnego r spełniającego $0 \leqslant r < d$. Innymi słowy, możemy zapisać

$$a = dq + r.$$

Wtedy

$$r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq) \in S.$$

Skoro $r \in S$ ale d wybraliśmy tak, aby było najmniejszym elementem dodatnim zbioru S, to z nierówności $0 \leqslant r < d$ mamy $r = 0$. Wobec tego $a = dq$, czyli d dzieli a.

Podzielmy teraz b przez d z resztą. Mamy

$$b : d = p \text{ reszty } s,$$

dla pewnego s spełniającego $0 \leqslant s < d$. Innymi słowy, możemy zapisać

$$b = dp + s.$$

Wtedy

$$s = b - dp = b - (ax + by)p = a(-xp) + b(1 - yp) \in S.$$

Skoro $s \in S$ ale d wybraliśmy tak, aby było najmniejszym elementem dodatnim zbioru S, to z nierówności $0 \leqslant s < d$ mamy $s = 0$. Wobec tego $b = dp$, czyli d dzieli b.

Pokazaliśmy, że d jest dzielnikiem liczb a oraz b, jest więc ich wspólnym dzielnikiem. Z założenia, że a i b są względnie pierwsze, wiemy, że największym wspólnym dzielnikiem tych liczb jest 1, więc $d = 1$. Pokazaliśmy więc, że $ax + by = d = 1$, czyli istnieją takie x i y, że $ax + by = 1$. Tym samym pokazaliśmy pierwsze wynikanie.

Przejdźmy teraz do dowodu w drugą stronę $\Longleftarrow$. Załóżmy, że istnieją liczby x i y całkowite takie, że $ax + by = 1$. Niech d będzie dzielnikiem a i b. Wobec tego, d dzieli $ax + by$, czyli d dzieli 1. Skoro tak, to $d = \pm 1$. Skoro dowolny dzielnik liczb a i b wynosi ± 1, to największy wspólny dzielnik liczb a i b jest równy 1. Oznacza to, że liczby a i b są względnie pierwsze, co mieliśmy pokazać. □

Lemat 2 (Tożsamość Bézouta). *Dla każdych całkowitych liczb a i b, które nie są jednocześnie zerem, istnieją liczby całkowite x i y takie, że*

$$ax + by = \gcd\{a, b\}.$$

Dowód. Ponieważ $\gcd\{a, b\}$ jest największym wspólnym dzielnikiem liczb a i b, dzieli każdą z nich bez reszty. Oznacza to, że liczby

$$p = \frac{a}{\gcd\{a, b\}}, \qquad q = \frac{b}{\gcd\{a, b\}}$$

są liczbami całkowitymi. Dodatkowo, p i q są względnie pierwsze. Gdyby nie były względnie pierwsze, $\gcd\{p, q\} > 1$, więc liczba $\gcd\{p, q\} \cdot \gcd\{a, b\} > \gcd\{a, b\}$ byłaby wspólnym dzielnikiem liczb a i b, co przeczyłoby temu, że $\gcd\{a, b\}$ jest największym wspólnym dzielnikiem liczb a i b.

Zastosujmy lemat 1 do względnie pierwszych liczb p i q. Na jego podstawie wiemy, że istnieją liczby całkowite x i y takie, że $px + qy = 1$. Wstawmy teraz definicję liczb p i q

$$\frac{a}{\gcd\{a, b\}} \cdot x + \frac{b}{\gcd\{a, b\}} \cdot y = 1.$$

Mnożąc stronami przez $\gcd\{a, b\}$ otrzymujemy

$$ax + by = \gcd\{a, b\},$$

co kończy dowód. □

Twierdzenie 2. *Dla dwóch liczb całkowitych a i b, które nie są jednocześnie równe zero, i liczby całkowitej c, równanie diofantyczne liniowe $ax + by = c$ ma rozwiązanie wtedy i tylko wtedy, gdy $\gcd\{a, b\}$ dzieli c. Innymi słowy*

$$\gcd\{a, b\} \textit{ dzieli } c \iff \exists x, y \in \mathbb{Z}: \quad ax + by = c.$$

Dowód. Udowodnimy dwie implikacje.

Zacznijmy od $\Longrightarrow$. Niech $d = \gcd\{a, b\}$. Wtedy fakt, że d dzieli c oznacza, że istnieje liczba $m \in \mathbb{Z}$ taka, że $c = md$.

Z tożsamości Bézouta (lemat 2) wiemy, że istnieją liczby całkowite x i y takie, że $ax + by = d$. Mamy zatem

$$c = md = m(ax + by) = (mx)a + (my)b.$$

Stąd istnieją liczby całkowite $p = mx$ oraz $q = my$ takie, że $c = pa + qb$, co jest naszą tezą.

Przejdźmy teraz do dowodu w drugą stronę $\Longleftarrow$. Załóżmy, że istnieją takie liczby całkowite x i y, że $ax + by = c$. Oczywiście, ponieważ $\gcd\{a, b\}$ dzieli a i dzieli b, to $\gcd\{a, b\}$ dzieli $ax + by$. Ale ponieważ $ax + by = c$, to również $\gcd\{a, b\}$ dzieli c, co kończy dowód. □

3.2 Metoda rozwiązywania

Aby rozwiązać równanie $ax + by = c$, w pierwszej kolejności sprawdzamy, czy równanie ma rozwiązanie, czyli czy $\gcd\{a, b\}$ dzieli c. Jeśli tak, dzielimy stronami przez $\gcd\{a, b\}$ otrzymując

$$\frac{a}{\gcd\{a, b\}} \cdot x + \frac{b}{\gcd\{a, b\}} \cdot y = \frac{c}{\gcd\{a, b\}}.$$

Wprowadźmy oznaczenia

$$p = \frac{a}{\gcd\{a, b\}}, \quad q = \frac{b}{\gcd\{a, b\}}.$$

Oczywiście p i q są względnie pierwsze i nasze równanie przyjmuje postać

$$px + qy = \frac{c}{\gcd\{a, b\}}.$$

Aby rozwiązać to równanie, rozwiązujemy równanie

$$px' + qy' = 1$$

uzyskując liczby całkowite x' oraz y' spełniające to równanie (liczby takie zawsze istnieją z lematu 1). Mając już x' oraz y', mnożymy poprzednie równanie stronami przez $\frac{c}{\gcd\{a,b\}}$ otrzymując

$$p \cdot \frac{x'c}{\gcd\{a, b\}} + q \cdot \frac{y'c}{\gcd\{a, b\}} = \frac{c}{\gcd\{a, b\}}.$$

Przypomnijmy, że rozwiązanie równania $ax + by = c$ spełniało też równanie

$$px + qy = \frac{c}{\gcd\{a, b\}}.$$

Oznacza to, że

$$x = \frac{x'c}{\gcd\{a, b\}}, \quad y = \frac{y'c}{\gcd\{a, b\}}$$

są rozwiązaniem wyjściowego równania diofantycznego.

Zwróćmy uwagę, że równanie

$$px' + qy' = 1,$$

możemy pomnożyć stronami przez $\gcd\{a, b\}$ uzyskując równoważne równanie

$$ax' + by' = \gcd\{a, b\},$$

co nazywamy tożsamością Bézouta (patrz lemat 2). Wobec tego najważniejszym typem równań diofantycznych liniowych, jakie musimy się nauczyć rozwiązywać, są te w postaci tożsamości Bézouta.

Równania takie rozwiązujemy za pomocą rozszerzonego algorytmu Euklidesa.

4 Rozszerzony algorytm Euklidesa

Rozszerzony algorytm Euklidesa jest algorytmem rekurencyjnym, który wylicza największy wspólny dzielnik $\gcd\{a, b\}$ oraz przy okazji znajduje jedno z możliwych rozwiązań tożsamości Bézouta $ax + by = \gcd\{a, b\}$. Przebiega on następująco:

1. dla $b = 0$ równanie $ax + by = \gcd\{a, b\}$ ma rozwiązanie $x = 1$, $y = 0$ i dodatkowo $\gcd\{a, b\} = a$,
2. dla $b \neq 0$ rozwiązujemy równanie $bx' + (a \bmod b)y' = \gcd\{b, a \bmod b\}$. Wtedy $x = y'$ i $y = x' - \left\lfloor \frac{a}{b} \right\rfloor y'$ i dodatkowo $\gcd\{a, b\} = \gcd\{b, a \bmod b\}$.

Dowód. Poprawność algorytmu udowodnimy indukcyjnie ze względu na b.

Warunek początkowy. Dla $b = 0$, równanie

$$ax + by = \gcd\{a, b\},$$

przyjmuje postać

$$ax = a,$$

ponieważ $\gcd\{a, 0\} = a$ (patrz dowód zwykłego algorytmu Euklidesa). Oznacza to, że $x = 1$ a y może być dowolny. Ponieważ algorytm szuka jednego z możliwych rozwiązań, możemy przyjąć $y = 0$.

Założenie indukcyjne. Załóżmy, że algorytm działa dla równań $ax + ty = \gcd\{a, t\}$ przy $t < b$.

Krok indukcyjny. Z założenia indukcyjnego potrafimy rozwiązać równanie

$$\gcd\{b, a \bmod b\} = bx' + (a \bmod b)y'$$

Zauważmy, że z algorytmu Euklidesa (patrz dowód zwykłego algorytmu Euklidesa) mamy

$$\gcd\{a, b\} = \gcd\{b, a \bmod b\},$$

stąd

$$ax + by = \gcd\{a, b\} = \gcd\{b, a \bmod b\} = bx' + (a \bmod b)y',$$

przy czym x' i y' wyznaczyliśmy z założenia indukcyjnego. Pozbywając się największego wspólnego dzielnika ze środka równań, uzyskujemy

$$ax + by = bx' + (a \bmod b)y'.$$

Zauważmy, że $a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b$, czyli

$$ax + by = bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right) y'.$$

Wymnóżmy nawias po prawej stronie i pogrupujmy tak, aby a i b występowały w jednym miejscu

$$bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right) y' = bx' + ay' - b\left\lfloor \frac{a}{b} \right\rfloor y' = ay' + b\left(x' - \left\lfloor \frac{a}{b} \right\rfloor y'\right).$$

Podsumowując

$$ax + by = ay' + b\left(x' - \left\lfloor \frac{a}{b} \right\rfloor y'\right),$$

co aby uzyskać równanie prawdziwe dla wszystkich a i b, oznacza

$$x = y', \quad y = x' - \left\lfloor \frac{a}{b} \right\rfloor y',$$

co należało pokazać. □

Zaimplementujmy rozszerzony algorytm Euklidesa. Będzie on zwracał trójkę liczb — $\gcd\{a, b\}$, x, y — spełniających $ax + by = \gcd\{a, b\}$.

```
def xgcd(a, b):
    if b==0:
        return (a, 1, 0)
    else:
        (gcd, x_prim, y_prim) = xgcd(b, a%b)
        return (gcd, y_prim, x_prim-a//b*y_prim)
```

Jeśli program ten uruchomimy dla argumentów `xgcd(8, 12)` otrzymamy odpowiedź $(4, -1, 1)$ co oznacza, że $\gcd\{8, 12\} = 4$, $x = -1$, $y = 1$. Podstawiając do równania $ax + by = \gcd\{a, b\}$ otrzymujemy równanie

$$8 \cdot (-1) + 12 \cdot (1) = 4,$$

które łatwo pokazać, że jest prawdziwe.

5 Przykład równania diofantycznego

Rozwiążmy w liczbach całkowitych równanie

$$18x + 16y = 500.$$

$\gcd\{18, 16\} = 2$ dzieli 500, więc równanie ma rozwiązanie. Rozwiążmy najpierw tożsamość Bézouta dla $a = 18$ i $b = 16$

$$18x' + 16y' = 2.$$

Stosujemy rozszerzony algorytm Euklidesa. $a \bmod b = 18 \bmod 16 = 2$, więc szukamy rozwiązania równania

$$16x'' + 2y'' = 2.$$

Aby rozwiązać to równanie, znów stosujemy krok algorytmu Euklidesa. Ponieważ zachodzi $16 \bmod 2 = 0$, musimy rozwiązać równanie

$$2x''' + 0y''' = 2.$$

Stąd $x''' = 1$, $y''' = 0$. Mamy też

$$x'' = y''' = 0, \quad y'' = x''' - \left\lfloor \frac{16}{2} \right\rfloor y''' = 1 - 8 \cdot 0 = 1.$$

Stąd

$$x' = y'' = 1, \quad y' = x'' - \left\lfloor \frac{18}{16} \right\rfloor y'' = 0 - 1 \cdot 1 = -1.$$

Sprawdźmy równanie

$$18x' + 16y' = 2.$$

Podstawiamy $x' = 1$, $y' = -1$ i otrzymujemy

$$18 - 16 = 2,$$

czyli równanie prawdziwe. Teraz mnożymy równanie stronami przez $\frac{500}{2} = 250$ otrzymując

$$18 \cdot (250x') + 16 \cdot (250y') = 500.$$

Podstawiając $x = 250x' = 250$ i $y = 250y' = -250$ otrzymujemy rozwiązanie wyjściowego równania

$$18x + 16y = 500.$$

6 Rozwiązanie ogólne równania diofantycznego

Twierdzenie 3. *Jeśli diofantyczne równanie liniowe ma jedno rozwiązanie, ma nieskończenie wiele rozwiązań. Jeśli x i y rozwiązują równanie $ax + by = c$, to*

$$x_k = x + \frac{b}{\gcd\{a,b\}} \cdot k, \quad y_k = y - \frac{a}{\gcd\{a,b\}} \cdot k, \qquad \text{dla } k \in \mathbb{Z}$$

również są rozwiązaniem tego równania.

Dowód. Załóżmy, że x i y są takie, że $ax + by = c$. Sprawdźmy, czy równanie to jest prawdziwe dla $ax_k + by_k = c$. Podstawmy

$$\begin{aligned} ax_k + by_k &= a\left(x + \frac{b}{\gcd\{a,b\}} \cdot k\right) + b\left(y - \frac{a}{\gcd\{a,b\}} \cdot k\right) = \\ &= ax + \frac{ab}{\gcd\{a,b\}} \cdot k + by - \frac{ba}{\gcd\{a,b\}} \cdot k = \\ &= ax + by + \frac{ab - ba}{\gcd\{a,b\}} \cdot k = ax + by + 0 \cdot k = \\ &= ax + by = c. \end{aligned}$$

Dodatkowo, ponieważ $\frac{a}{\gcd\{a,b\}}$ i $\frac{b}{\gcd\{a,b\}}$ są liczbami całkowitymi, również x_k i y_k są liczbami całkowitymi. Pokazaliśmy zatem, że są całkowitymi rozwiązaniami wyjściowego równania, są zatem rozwiązaniami równania diofantycznego liniowego $ax + by = c$. □

Wróćmy do równania z poprzedniego przykładu

$$18x + 16y = 500.$$

Jedno z rozwiązań to $x = 250$, $y = -250$, zatem rozwiązanie ogólne jest postaci

$$x_k = 250 + \frac{16}{2} \cdot k, \quad y_k = -250 - \frac{18}{2} \cdot k, \qquad \text{dla } k \in \mathbb{Z},$$

czyli

$$x_k = 250 + 8k, \quad y_k = -250 - 9k, \qquad \text{dla } k \in \mathbb{Z}.$$

Spróbujmy teraz odpowiedzieć na pytanie, ile rozwiązań ma równanie $18x + 16y = 500$ w liczbach naturalnych, czyli dla $x, y \geqslant 0$.

Musi zachodzić jednocześnie $250 + 8k \geqslant 0$ oraz $-250 - 9k \geqslant 0$. Przekształćmy te nierówności do nierówności dla k:

$$k \geqslant \frac{-250}{8}, \quad k \leqslant \frac{-250}{9}.$$

Oznacza to, że

$$\frac{-250}{8} \leqslant k \leqslant \frac{-250}{9},$$

czyli

$$-31{,}25 \leqslant k \leqslant -27{,}(7).$$

Ponieważ k musi być liczbą całkowitą, to

$$-31 \leqslant k \leqslant -28.$$

Oznacza to, że istnieją jedynie 4 rozwiązania naturalne, dla $k = -28, -29, -30, -31$. Wszystkie znajdują się w tabeli poniżej.

k	x	y
-28	$250 + 8 \cdot (-28) = 26$	$-250 - 9 \cdot (-28) = 2$
-29	$250 + 8 \cdot (-29) = 18$	$-250 - 9 \cdot (-29) = 11$
-30	$250 + 8 \cdot (-30) = 10$	$-250 - 9 \cdot (-30) = 20$
-31	$250 + 8 \cdot (-31) = 2$	$-250 - 9 \cdot (-31) = 29$

7 Zastosowanie wyników

Załóżmy, że w jednym ze sklepów trwa noworoczna promocja na herbaty. Mamy bon o wartości 500 zł, który chcemy wykorzystać w całości. Herbata Darjeeling kosztuje 18 zł za opakowanie, natomiast Yunnan 16 zł. Ile paczek herbaty i jakiej możemy zakupić tak, aby wykorzystać bon co do złotówki? Rozważmy dwa scenariusze: w pierwszym, chcemy kupić jak najwięcej herbaty, w drugim, chcemy kupić jak najbardziej różnorodny zestaw herbaty (czyli możliwie bliską liczbę paczek jednej i drugiej odmiany).

Zauważmy, że problem da się zapisać jako równanie diofantyczne liniowe w liczbach naturalnych. Załóżmy, że kupujemy x paczek herbaty Darjeeling oraz y paczek herbaty Yunnan. Oczywiście nie da się kupić pół paczki ani ujemnej wartości paczki (sprzedać sklepowi?), więc x i y są liczbami naturalnymi. Za całość zapłacimy $18x + 16y$, przy czym chcemy wydać dokładnie 500 zł, aby nie zmarnować ani złotówki z bonu. Wobec tego, nasze równanie to

$$18x + 16y = 500,$$

gdzie x i y to liczby naturalne. Jest to dokładnie to samo równanie, które rozważaliśmy w poprzednim podrozdziale, zatem mamy cztery możliwe scenariusze zakupów. Wybór opcji zależy od scenariusza.

Darjeeling	Yunnan	liczba paczek	różnica
26	2	$26 + 2 = 28$	$\|26 - 2\| = 24$
18	11	$18 + 11 = 29$	$\|18 - 11\| = 7$
10	20	$10 + 20 = 30$	$\|10 - 20\| = 10$
2	29	$2 + 29 = 31$	$\|2 - 29\| = 27$

Oznacza to, że jeśli zależy nam na jak największej liczbie paczek herbaty należy kupić 2 paczki herbaty Darjeeling oraz 29 paczek herbaty Yunnan (łącznie 31 paczek herbaty). Aby uzyskać najbardziej różnorodny zestaw herbaty, należy natomiast wybrać 18 paczek herbaty Darjeeling oraz 11 paczek herbaty Yunnan (tylko 7 paczek różnicy).

8 Co dalej?

Równanie diofantyczne liniowe w liczbach naturalnych jest jednym z najprostszych przykładów zagadnienia optymalizacyjnego nazywanego programowaniem całkowitoliczbowym. Programowanie całkowitoliczbowe znajduje bardzo wiele zastosowań w biznesie — w optymalizacji zysków przy ograniczonej liczbie zasobów. Poszczególne zmienne mogą być liczbą wyprodukowanych urządzeń, liczbą potrzebnych składników, liczbą paczek zapakowanych na samochód oraz wieloma innymi zastosowaniami. Programowanie całkowitoliczbowe, programowanie wypukłe (w tym liniowe) oraz programowanie nieliniowe są dziedzinami optymalizacji matematycznej — działki matematyki, którą warto się zainteresować, jeśli zamierzamy mieć coś wspólnego z biznesem i badaniami operacyjnymi. Zachęcam, aby wyszukać w Internecie terminy występujące w niniejszym akapicie i mieć oko na odpowiednie kursy wybieralne, jeśli kogoś ten temat zainteresuje.