



# Algorytm Euklidesa

Bartłomiej BZDEGA

*Uwaga.* W całym artykule zakładamy, że liczby  $a, b, c, d, k, m, n$  są całkowite.

Zacznijmy od prostej obserwacji: jeśli  $d$  jest wspólnym dzielnikiem liczb  $a$  i  $b$ , to dla dowolnych liczb całkowitych  $x$  i  $y$  zachodzi podzielność  $d \mid ax + by$ . Wynika to wprost z definicji podzielności. W szczególności, jeśli  $d \mid a, b$ , to  $d \mid a + b$  i  $d \mid a - b$ . Ta ostatnia podzielność w wersji: jeśli  $d \mid n$ , to  $d \mid n - d$ , jest często stosowanym trikiem w zadaniach o podzielności. Zazwyczaj działa w połączeniu z szacowaniem: jeżeli  $d \mid m$  i  $m > 0$ , to  $d \leq m$ , przy czym  $d, m$  i  $n$  zazwyczaj są pewnymi wyrażeniami algebraicznymi.

Założmy, że  $a > b \geq 0$ . Na mocy wyżej opisanych własności, jeśli  $d$  jest dzielnikiem pewnych dwóch liczb spośród:  $a, b, a - b$ , to również dzieli trzecią. Z tego wynika, że  $\text{NWD}(a, b) = \text{NWD}(a - b, b)$ . Zapiszmy dzielenie z resztą  $a = qb + r$ . Po  $q$ -krotnym zastosowaniu powyższej równości otrzymamy

$$\text{NWD}(a, b) = \text{NWD}(r, b).$$

Jest to krok *algorytmu Euklidesa* – licząc NWD dwóch liczb, większą z nich zastępujemy resztą z jej dzielenia przez mniejszą. Ostatnia niezerowa reszta jest poszukiwanym NWD.

Niech  $r_0 = a > b = r_1$ . Dla  $k \geq 0$  oznaczmy przez  $r_{k+2}$  resztę z dzielenia  $r_k$  przez  $r_{k+1}$ . Wykażemy, że  $r_k = ax_k + by_k$  dla pewnych liczb całkowitych  $x_k$  i  $y_k$ . Dla  $k = 0$  i  $k = 1$  jest to oczywiście prawdą. Indukcyjnie, dla pewnego naturalnego  $q$  mamy

$$\begin{aligned} r_{k+2} &= r_k - qr_{k+1} = (ax_k + by_k) - q(ax_{k+1} + by_{k+1}) = \\ &= a(x_k - qx_{k+1}) + b(y_k - qy_{k+1}). \end{aligned}$$

Z tego wyniku bardzo ważny wniosek: istnieją liczby całkowite  $x$  i  $y$ , dla których  $ax + by = \text{NWD}(a, b)$ . W szczególności liczby  $a$  i  $b$  są względnie pierwsze wtedy i tylko wtedy, gdy  $ax + by = 1$  dla pewnych całkowitych  $x$  i  $y$ .

Wymienię tu dwie konsekwencje tego faktu. Niech  $\text{NWD}(a, b) = 1$ . Wówczas:

- (1) jeśli  $a \mid bc$ , to  $a \mid c$ ;      (2) jeśli  $a, b \mid c$ , to  $ab \mid c$ .

*Dowód.* Niech  $ax + by = 1$ , przy czym  $x$  i  $y$  to liczby całkowite. Wtedy:

- (1) jeśli  $a \mid bc$ , to liczba  $c/a = c(ax + by)/a = cx + y(bc/a)$  jest całkowita;  
 (2) jeśli  $a, b \mid c$ , to liczba  $c/(ab) = c(ax + by)/(ab) = x(c/b) + y(c/a)$  jest całkowita.

## Zadania

- Wyznaczyć wszystkie liczby całkowite  $a$ , dla których liczba  $a^2 + 2a + 3$  jest dzielnikiem liczby  $5a^2 + 4a + 3$ .
- Niech  $d, m, n > 0$  będą liczbami naturalnymi. Udowodnić, że jeśli  $d \mid m^2n - 1$  oraz  $d \mid mn^2 - 1$ , to  $d \mid n^3 - 1$ .
- Liczby  $a$  i  $b$  są całkowite dodatnie. Wykazać, że jeśli  $a + b + 1$  jest liczbą pierwszą dzielącą  $4ab - 1$ , to  $a = b$ .
- Niech  $(F)$  będzie ciągiem Fibonacciego, tj.  $F_1 = F_2 = 1$  oraz  $F_{n+2} = F_n + F_{n+1}$  dla  $n \geq 1$ . Udowodnić, że jeśli  $0 \leq b < a \leq F_m$  dla pewnego  $m \geq 2$ , to algorytm Euklidesa obliczy  $\text{NWD}(a, b)$  w co najwyżej  $m - 2$  krokach (za krok uznajemy wykonanie dzielenia z resztą).
- Liczby całkowite dodatnie  $m$  i  $n$  spełniają podzielność  $mn \mid m^2 + n^2 + m$ . Wykazać, że  $m$  jest kwadratem liczby całkowitej.
- Liczby naturalne  $a > b > 1$  spełniają podzielności  $a + b \mid ab + 1$  i  $a - b \mid ab - 1$ . Dowiedzieć, że  $a < b\sqrt{3}$ .
- Niech  $k, m$  i  $n$  będą ustalonymi liczbami całkowitymi dodatnimi, spełniającymi warunek  $\text{NWD}(km, n) = 1$ . Dowiedzieć, że równanie  $a^k + b^m = c^n$  ma rozwiązanie w liczbach całkowitych dodatnich  $a, b, c$ .

**Wskazówki do zadań**  
 1. Zaczodź podzielnosc  $a^2 + 2a + 3 \mid 5a^2 + 4a + 3$ . Prawa strona jest równa zero albo nie mniejsza, co do bezwzględnej wartości, od lewej.  
 2. Mamy  $d \mid n(m^2n - 1) - m(mn^2 - 1)$ .  
 3. Rozłożyć na iloczyn dwóch czynników  $d \mid 4ab - 1$  i  $d \mid a + b + 1$ . Co najmniej jeden z nich musi się dzielić przez  $a + b + 1$ .  
 4. Uzasadnić i zastosować nierówność  $r_k \geq r_{k+1} + 1$  dla odpowiednich  $k$ .  
 5. Niech  $d = \text{NWD}(m, n)$ . Udowodnić, że  $d^2 \mid m$  oraz  $m \mid n^2$ . Wywnioskować z tego, że  $d^2 \mid m$  i  $d \mid n$ . Wygodnie będzie zapisać  $n = ad$  i  $m = bd$  – wtedy  $\text{NWD}(a, b) = 1$ .  
 6. Wykazać, że liczby  $a - b$  i  $a + b$  są dzielnikami  $b^2 - 1$ . Oszacować  $\text{NWD}(a - b, a + b) \geq 2$  i wywnioskować, że  $a - b \leq 2$  i czego wynika teza.  
 7. Niech  $a = 2^k x$ ,  $b = 2^k x$  i  $c = 2^k x$ . Wówczas  $a + b + m = 2^k(x + x + m)$  i  $c = 2^k x$ . Wystarczy zatem wykazać istnienie liczb całkowitych dodatnich  $x$  i  $y$ , które spełniają równość  $km = x + y$ .