Algorytm Euklidesa

Bartłomiej BZDĘGA

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 $d \leqslant m$, przy czym d, m i n zazwyczaj są pewnymi wyrażeniami algebraicznymi.

Załóżmy, że $a > b \geqslant 0$. 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 $\mathtt{NWD}(a, b) = \mathtt{NWD}(a - b, b)$. Zapiszmy dzielenie z resztą $a = qb + r$. Po q-krotnym zastosowaniu powyższej równości otrzymamy

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

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 $k \geqslant 0$ 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 wynika bardzo ważny wniosek: istnieją liczby całkowite x i y, dla których $ax + by = \mathtt{NWD}(a, b)$. 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 $\mathtt{NWD}(a, b) = 1$. Wówczas:

$$\text{(1) jeśli } a \mid bc, \text{ to } a \mid c; \qquad \text{(2) jeśli } a, b \mid c, \text{ to } ab \mid c.$$

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

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

Wskazówki do zadań

1. Zachodzi podzielność $a^2 + 2a + 3 \mid 5a^2 + 4a + 3 - 5(a^2 + 2a + 3)$. Prawa strona jest równa zeru 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 liczbę $4ab - 1 + 2(a + b + 1)$. Co najmniej jeden z nich musi się dzielić przez $a + b + 1$.
4. Uzasadnić i zastosować nierówność $r_k \geqslant r_{k+1} + r_{k+2}$ dla odpowiednich k.
5. Niech $d = \mathtt{NWD}(m, n)$. Udowodnić, że $d^2 \mid m$ oraz $m \mid n^2$. Wywnioskować z tego, że $m = d^2$. (Wygodnie będzie zapisać $n = ad$ i $m = bd$ – wtedy $\mathtt{NWD}(a, b) = 1$.)
6. Wykazać, że liczby $a - b$ i $a + b$ są dzielnikami $b^2 - 1$. Oszacować $\mathtt{NWD}(a + b, a - b) \leqslant 2$ i wywnioskować, że $a^2 - b^2 \leqslant 2(b^2 - 1)$, z czego wynika teza.
7. Niech $a = 2^{mx}$, $b = 2^{kx}$ i $c = 2^y$. Wówczas $a^k + b^m = 2^{kmx+1}$ i $c^n = 2^{ny}$, wystarczy zatem wykazać istnienie liczb całkowitych dodatnich x i y, które spełniają równość $(km)x + 1 = ny$.