44. NWD i NWW. Algorytm Euklidesa.

Teoria

Definicja. Niech $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ i nie wszystkie z tych liczb są zerami. *Największy wspólny dzielnik* liczb a_k jest to liczba

$$\mathrm{NWD}(a_1, a_2, \ldots, a_n) = \max\{d \in \mathbb{N} : d|a_k \text{ dla } k = 1, 2, \ldots, n\}.$$

Najmniejsza wspólna wielokrotność liczb a_k jest to liczba

$$\mathrm{NWW}(a_1, a_2, \ldots, a_n) = \min\{m \in \mathbb{N} : a_k|m \text{ dla } k = 1, 2, \ldots, n\}.$$

Istnienie NWD i NWW wynika z zasady ekstremum (minimum i maksimum).

Twierdzenie 1. Załóżmy, że $p_1, p_2, \ldots, p_s \in \mathbb{P}$ i dla $k = 1, 2, \ldots, n$:

$$a_k = p_1^{\alpha_{k,1}} \cdot p_2^{\alpha_{k,2}} \cdot \ldots \cdot p_s^{\alpha_{k,s}},$$

gdzie $a_{k,i} \in \mathbb{Z}_+$. Niech $\beta_i = \min(\alpha_{1,i}, \alpha_{2,i}, \ldots, \alpha_{k,i})$, $\gamma_i = \max(\alpha_{1,i}, \alpha_{2,i}, \ldots, \alpha_{k,i})$ dla $i = 1, 2, \ldots, s$. Wówczas

$$\mathrm{NWD}(a_1, a_2, \ldots, a_n) = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_s^{\beta_s}$$
$$\mathrm{NWW}(a_1, a_2, \ldots, a_n) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_s^{\gamma_s}$$

Dowód: Jest on czysto techniczny, więc przedstawię tylko intuicję. Zadajmy pytanie: w jakiej potędze liczba p_1 występuje w rozkładzie $NWD(a_1, \ldots, a_k)$ na czynniki? $\mathrm{NWD}(a_1, \ldots, a_k)$ dzieli wszystkie liczby $a_1, \ldots, a_k$. Zatem wykładnik potęgi liczby p_1 może być co najwyżej taki, jak najmniejszy wykładnik spośród potęg p_1 w rozkładach $a_1, \ldots, a_k$, aby zachodziła podzielność. To samo robimy dla pozostałych liczb pierwszych i otrzymujemy tezę. Analogicznie dowodzimy faktu dla NWW.

Stw. Jeżeli $d|a_k$ dla $k = 1, 2, \ldots, n$, to $d|\mathrm{NWD}(a_1, a_2, \ldots, a_n)$.
Jeżeli $a_k|m$, dla $k = 1, 2, \ldots, n$, to $\mathrm{NWW}(a_1, a_2, \ldots, a_n)|m$.

Dowód: Podzielności te wynikają bezpośrednio z definicji NWD i NWW.

Stw. Jeżeli $a, b \in \mathbb{Z}$ i r to reszta z dzielenia a przez b, to $\mathrm{NWD}(a, b) = \mathrm{NWD}(a - b, b) = \mathrm{NWD}(b, r)$.

Algorytm Euklidesa. Niech $a, b \in \mathbb{N}$. Aby obliczyć $NWD(a, b)$ wykonujemy kolejne dzielenia z resztą: $a = q_0 b + r_1$, $b = q_1 r_1 + r_2$, $r_1 = q_2 r_2 + r_3$, itd. Wówczas $NWD(a, b)$ jest równe ostatniej niezerowej reszcie r_k.

Twierdzenie 2. Jeżeli $a, b \in \mathbb{Z}$, to istnieją $x, y \in \mathbb{Z}$ takie, że $\mathrm{NWD}(a, b) = ax + by$. Pondato, $NWD(a, b)|ax + by$ dla dowolnych $x, y \in \mathbb{Z}$.

Dowód: Wystarczy zastosować algorytm Euklidesa i począwszy od ostatniego kroku wyznaczać NWD z równań jako kombinacje liniowe. Dla uproszczenia zobaczmy to na przykładzie: $\mathrm{NWD}(120, 32)$. Mamy: $120 = 3 \cdot 32 + 24$, $32 = 1 \cdot 24 + 8$, $24 = 3 \cdot 8$. Zatem $\mathrm{NWD}(120, 32) = 8$. Z przedostateniego równania mamy: $8 = 32 - 24$, a teraz z poprzedniego mamy: $8 = 32 - (120 - 3 \cdot 32) = 4 \cdot 32 - 1 \cdot 120$.

Zadania

1. Udowodnij stwierdzenia:

   (a) Jeżeli $a, b \in \mathbb{N}$, to $\mathrm{NWD}(a,b) \cdot \mathrm{NWW}(a,b) = ab$.

   (b) Jeżeli $a, b, c \in \mathbb{N}$, to $\mathrm{NWD}(a,b,c) = \mathrm{NWD}(\mathrm{NWD}(a,b),c)$.

   (c) Jeżeli $a, b, c \in \mathbb{N}$, $c|ab$ oraz $\mathrm{NWD}(b,c) = 1$, to $c|a$.

   (d) Jeżeli $a, b, c \in \mathbb{N}$, $a|c$, $b|c$ i $\mathrm{NWD}(a,b) = 1$, to $ab|c$.

   (e) Jeżeli $a, b_1, b_2, \ldots, b_n \in \mathbb{N}$ oraz $NWD(a, b_k) = 1$ dla $k = 1, 2, \ldots, n$, to $\mathrm{NWD}(a, b_1 b_2 \ldots b_n) = 1$.

   (f) Jeżeli $a, b, n \in \mathbb{N}$ i $\mathrm{NWD}(a,b) = 1$, to $\mathrm{NWD}(a^n, b^n) = 1$.

   (g) Jeżeli $a, b, n \in \mathbb{N}$ i $a^n|b^n$, to $a|b$.

   (h) Jeżeli $a, b, d \in \mathbb{N}$, $\mathrm{NWD}(a,b) = 1$ i $d|a+b$, to $\mathrm{NWD}(a,d) = \mathrm{NWD}(b,d) = 1$.

2. Stosując algorytm Euklidesa wyznacz $NWD(a,b)$, gdy a) $a = 329$, $b = 182$; b)$a = 543312$, $b = 65340$. Zapisz $\mathrm{NWD}(a,b)$ w postaci $ax + by$, gdzie $x, y \in \mathbb{Z}$.

3. Niech $n \in \mathbb{N}$. Pokaż, ze liczby $21n + 4$ i $14n + 3$ są względnie pierwsze.

4. Niech $n \in \mathbb{N}$. Udowodnij, że $\mathrm{NWD}(n! + 1, (n+1)! + 1) = 1$.

5. Niech $m, n \in \mathbb{N}$ i m jest liczbą nieparzystą. Udowodnij, że liczby $2^m - 1$ i $2^n + 1$ są względnie pierwsze.

   Wskazówka. Niech $d > 2$ będzie największym wspólnym dzielnikiem tych liczb. Przedstaw liczbę 2^{mn} na dwa sposoby i rozpatrz resztę modulo d.

6. Załóżmy, że $a, b \in \mathbb{Z}$. Pokaż, że $NWD(5a + 3b, 13a + 8b) = \mathrm{NWD}(a,b)$.

7. Niech a_1, $a_2, \ldots, a_k \in \mathbb{Z}$. Udowodnij, że istnieją liczby całkowite x_1, $x_2, \ldots, x_k$ takie, że $\mathrm{NWD}(a_1, a_2, \ldots, a_k) = a_1x_1 + a_2x_2 + \ldots + a_kx_k$.

8. Wykaż, że dla dowolnych liczb naturalnych a, b liczba $\mathrm{NWD}(a+b, ab) - \mathrm{NWD}(a,b)$ jest parzysta.

9. Niech $n \in \mathbb{N}$. Pokaż, że $\mathrm{NWW}(1, 2, 3, \ldots, 2n) = \mathrm{NWW}(n+1, n+2, \ldots, 2n)$.

10. Niech a, b, $c \in \mathbb{N}$. Udowodnij tożsamość

$$\mathrm{NWW}(a,b,c)^2 \cdot \mathrm{NWD}(a,b) \cdot \mathrm{NWD}(b,c) \cdot \mathrm{NWD}(c,a) = \\ = \mathrm{NWD}(a,b,c)^2 \cdot \mathrm{NWW}(a,b) \cdot \mathrm{NWW}(b,c) \cdot \mathrm{NWW}(c,a)$$

11. Udowodnij, że każda liczba naturalna $n > 6$ jest sumą dwóch liczb naturalnych > 1 względnie pierwszych.

12. ★ Ciąg a_1, $a_2, \ldots$ liczb naturalnych spełnia

$$\mathrm{NWD}(a_i, a_j) = \mathrm{NWD}(i,j) \quad \text{dla} \quad i \neq j.$$

    Wykaż, że $a_j = j$ dla każdego $j \in \mathbb{N}$.

    Wskazówka. Rozważ $j = 2i$. Wykaż, że $j|a_j$, następnie pokaż, że $k|a_j \Rightarrow k|j$.

13. ★ Niech $a, b, n \in \mathbb{N}$, $n > 1$. Pokaż, że $\mathrm{NWD}(n^a - 1, n^b - 1) = n^{\mathrm{NWD}(a,b)} - 1$.

    Wskazówka. Niech $f(x) = n^x - 1$. Niech $a > b$. Pokaż, że $\mathrm{NWD}(f(a), f(b)) = \mathrm{NWD}(f(a - b), f(b))$. Popatrz na związek z algorytmem Euklidesa.

14. ★ Niech a, b będą dodatnimi liczbami całkowitymi. Udowodnij, że

$$\mathrm{NWD}(2^a + 1, 2^b + 1) | 2^{\mathrm{NWD}(a,b)} + 1$$

    Wskazówka. Wykorzystaj poprzednie zadanie. Udowodnij i wykorzystaj wzór: $\mathrm{NWD}(xy, z) = \mathrm{NWD}(x, z) \cdot \mathrm{NWD}(y, z)$, o ile $\mathrm{NWD}(x, y) = 1$.

15. ★ Dane są liczby naturalne a, b takie, że liczba $\frac{a+1}{b} + \frac{b+1}{a}$ jest całkowita. Udowodnij, że $\mathrm{NWD}(a, b) \leqslant \sqrt{a + b}$.

16. ★ Dane są różne liczby całkowite na tablicy. Ruch polega na wytarciu pewnych dwóch różnych liczb i napisaniu ich NWD i NWW. Udowodnij, że po pewnych czasie, ruch nie będzie powodował zmiany liczb.

    Wskazówka. Pokaż, że po zmianie dwóch liczb iloczyn się nie zmienia, zaś ich suma wzrasta (nie maleje), a ciągle rosnąć nie może.

Domowe

17. Niech $a, n \in \mathbb{N}$ i $a > 1$. Udowodnij, że $\mathrm{NWD}\left(\frac{a^n-1}{a-1}, a - 1\right) = \mathrm{NWD}(a - 1, n)$.

18. Niech n będzie parzystą dodatnią liczbą całkowitą i niech a, b będą względnie pierwszymi liczbami. Znajdź a, b wiedząc, że $a + b | a^n + b^n$.