0.1 Lekcja 2. Największy wspólny dzielnik $NWN(a, b)$. Algorytm Euklidesa

Największy wspólny dzielnik dwóch liczb naturalnych a i b oznaczamy symbolem $NWD(a, b)$. Jednym ze sposobów obliczania największego wsólnego dzielnika danych liczb naturalnych a i b jest rozkład tych liczb na czynniki liczb pierwszych.

Rozpatrzmy kilka przykładów obliczania $NWD(a, b)$ przez rozkład liczb a i Rb na czynniki pierwsze

Przykład 0.1 *Niech liczba* $a = 21$ *i liczba* $b = 57$*. Rozkład tych liczb jest oczywisty*

$$21 = 3 * 7 \ \ i \ \ 57 = 3 * 19$$

Wspólnym dzielnikiem liczb 21 *i* 57 *jest liczba* 3*, ponieważ liczba* 3 *dzieli liczbę* 21 *i dzieli liczbę* 57*. Poza tym te liczba nie mają innych wspólnych dzielników.*
Skąd mamy wartość największego wspólnego dzielnika

$$NWD(21, 57) = 3$$

obliczzanie nai większego wspólnego dzielnika

Przykład 0.2 *Znajdź największy wspólny dzielnik liczb* 42 *i* 78*.*

Rozkładamy obie liczby na czynniki pierwsze według schematu

$$\begin{array}{rcl} 42 & | & 2, \\ 21 & | & 3, \\ 7 & | & 7, \\ 1 & | & \end{array} \qquad \begin{array}{rcr} 78 & | & 2 \\ 39 & | & 3 \\ 13 & | & 13 \\ 1 & | & \end{array}$$

Skąd mamy rozkład liczb

$$42 = 2 * 3 * 7 \quad i \quad 78 = 2 * 3 * 13$$

Wspólnymi czynnikami tych liczb są 2 i 3. Dlatego największym wspólnym dzielnikiem liczb 42 i 78 jest liczba $NWD(42, 78) = 2 * 3 = 6$.

Rozpatrzy jeszcze jeden przykład wyznaczania największego wspólnego dzielnika przez rozkład liczb na czynniki pierwsze

Przykład 0.3 *Znajdź największy wspólny dzielnik liczby* 210 *i liczby* 231

$$\begin{array}{rcl} 210 & | & 2, \\ 105 & | & 3, \\ 35 & | & 7, \\ 5 & | & 5 \\ 1 & | & \end{array} \qquad \begin{array}{rcr} 231 & | & 3 \\ 77 & | & 7 \\ 11 & | & 11 \\ 1 & | & \end{array}$$

Skąd mamy rozkład liczb 210 i 231 na czynniki pierwsze

$$210 = 2 * 3 * 7 * 5 \quad i \quad 231 = 3 * 7 * 11$$

Wspólnymi dzielnikami tyczh liczb są 3 i 7. Dlatego największym wspólnym dzielnikiem liczb 210 i 231 jest $NWD(210, 231) = 3 * 7 = 21$.
Sprawdzamy, że liczba $NWD(210, 231) = 21$ dzieli liczby 210 i 231

$$210 : 21 = 10 \quad oraz \quad 231 : 21 = 11.$$

0.2 Algorytm Euklidesa (325-265 B.C.)

Najbardziej efektywnym sposobem wyznaczania największego wspólnego dzielnika jest algorytm Euklidesa. Już w starożytnych czasach w Egipcie, Euklides grecki nauczyciel i dziekan wydzialu nauk przyrodniczych na Uniwersytecie w Aleksandrii podał algorytm na znajdowanie największego wspólnego dzielnika dwóch liczb naturalnych.

Algorytm Euklidesa. Obliczamy kolejne wyrazy ciągy malejącego reszt

$$r_0 > r_1 > r_2 > r_4 > ... > r_{n-1} > r_n$$

z dzielenia liczb $r_0, r_1, ..., r_n$, startując z danych liczb r_0 i r_1

$$\begin{array}{lcll}
\frac{r_0}{r_1} & = & k_2 + \frac{r_2}{r_1}, & r_2 = r_0 - k_2 * r_1 \\
\frac{r_1}{r_2} & = & k_3 + \frac{r_3}{r_2}, & r_3 = r_1 - k * 3 * r_2 \\
\frac{r_2}{r_3} & = & k_4 + \frac{r_4}{r_3}, & r_4 = r_2 - k_4 * r_3 \\
. & . & .... & ... \\
\frac{r_{n-1}}{r_n} & = & k_{n+1} + \frac{r_{n+1}}{r_n}, & r_n = r_{n-2} - k_n * r_{n-1}
\end{array}$$

Zauważmy, że powyższe wzory na reszty r_i, $i = 0, 1, 2, ..., n$, możemy zapisać jednym wzorem rekurencyjnym

$$r_i = r_{i-2} - k_i * r_{i-1}, \quad dla \;\; i = 2, 3, ..., n, \tag{1}$$

Tutaj współczynnik całkowity $k_i = E[\frac{r_i}{r_{i+1}}]$.[1]
Ostatni wyraz ciągu $r_n \neq 0$ różny od zera jest największym wspólnym dzielnikiem dwóch pierwszych wyrazów r_0, r_1, piszemy

$$r_n = NWD(r_0, r_1).$$

To wynika ze wzoru rekurencyjnego (1). Mianowicie, jeżeli liczba $d = NWD(r_0, r_1)$ jest dzielnikiem liczb r_0 i r_1 to d jest również dzielnikiem każdej następnej reszty

$$r_2 = r_0 - k_2 * r_1$$

$$r_i = r_{i-2} - k_i * r_{i-1}, \quad dla \;\; i = 2, 3, ..., n,$$

Konstrukcje ciągu rekurencyjnego (1) wijaśnimy na przykładach.

[1] E[x] entire of x oznacza całość z liczby x

Przykład 0.4 *Znajdź największy wspólny dzielnik liczb* $r_0 = 78$ *i* $r_1 = 42$ *stosując algorytm Euklidesa (1)*

1. Dzielimy liczbę większą $r_0 = 78$ przez liczbę mniejszą $r_1 = 48$, według schematu

$$\frac{r_0}{r_1} = k_2 + \frac{r_2}{r_1}, \qquad\qquad r_0 = k_2 * r_1 + r_2$$
$$\frac{78}{42} = 1 + \frac{36}{42}, \quad k_2 = 1, \quad 78 = 1 * 42 + 36.$$

i obliczamy resztę r_2 z dzielenia liczb $r_0 = 78$ przez $r_1 = 42$

$$r_2 = r_0 - k_2 * r_1,$$

$$r_2 = 78 - 1 * 42 = 36.$$

gdzie $k_2 = E[\frac{r_0}{r_1}]$ oznacza całość z dzielenia r_0 przez r_1.
[2]

2. Podstawiamy $r_1 = 42$, $r_2 = 36$ i dzielimy liczbę większą $r_1 = 42$ przez liczbę mniejszą $r_2 = 36$, według schematu

$$\frac{r_1}{r_2} = k_3 + \frac{r_3}{r_2}, \qquad\qquad r_1 = k_3 * r_2 + r_3$$
$$\frac{42}{36} = 1 + \frac{6}{36}, \quad k_3 = 1, \quad 42 = 1 * 36 + 6.$$

i obliczamy resztę z dzielenia liczb $r_1 = 42$ i $r_2 = 36$

$$r_3 = r_1 - k_3 * r_2,$$

$$r = 42 - 36 = 6.$$

3. Podstawiamy $r_2 = 36$, $r_3 = 6$ i dzielimy liczbę większą $r_2 = 36$ przez liczbę mniejszą $r_3 = 6$, według schematu

$$\frac{r_2}{r_3} = k_4 + \frac{r_4}{r_3}, \qquad\qquad r_2 = k_4 * r_3 + r_4$$
$$\frac{36}{6} = 6, \qquad k_4 = 6, \quad 36 = 6 * 6 + 0.$$

i obliczamy resztę z dzielenia liczb $r_2 = 42$ i $r_3 = 36$

$$r_4 = 36 - k_4 * 6,$$

$$r_4 = 36 - 36 = 0.$$

Największym wspólnym dzielnikiem liczb 78 i 42 jest ostatnia reszta $r_3 = 6$ różna od zera, piszemy $NWD(78, 36) = 6$

Rozpatrzymy następny przykład zastosowania algorytmu Euklidesa (1).

---

[2] E[x] entire of x oznacza całość z liczby x

Przykład 0.5 *Znajdź największy wspólny dzielnik liczb* $r_0 = 1995$ *i* $r_1 = 1190$

Podobnie jak w poprzednim przykładzie znajdujemmy największy wspólny dzielnik liczb 1995 *i* 1190 stosując wzór (1)

$$\begin{array}{cc}
r_0 = 1995, \quad r_1 == 1190 & | \quad reszta\ r \\
- - - - - - - & - - - \\
\dfrac{1995}{1190} = 1 + \dfrac{805}{1190} & | \quad r_2 = 805 \\
\dfrac{1190}{805} = 1 + \dfrac{6}{385} & | \quad r_3 = 385 \\
\dfrac{805}{385} = 2 + \dfrac{35}{385} & | \quad r_4 = 35 \\
\dfrac{385}{35} = 11 & | \quad r_5 = 0
\end{array}$$

Największym wspólnym dzielnikiem liczb 1995 i 1190 jest ostatnia reszta $r_4 = 35$ różna od zera, piszemy $NWD(1995, 1190) = 35$

Przykład 0.6 *Znajdź największy wspólny dzielnik liczb* 975 *i* 690

Rozwiązanie.
Stosujemy wyżej opisany algorytm Euklidesa obliczajmy kolejne reszty

$$\begin{array}{cc}
a = r_0 = 975, \quad b = r_1 = 690 & | \quad reszta \\
- - - - - - - - - -- & - - - - - - - - - - \\
\dfrac{975}{690} = 1 + \dfrac{285}{690} & | \quad r_2 = 975 - 1 * 690 = 285 \\
\dfrac{690}{285} = 2 + \dfrac{120}{285} & | \quad r_3 = 690 - 2 * 285 = 120 \\
\dfrac{285}{120} = 2 + \dfrac{45}{120} & | \quad r_4 = 285 - 2 * 120 = 45 \\
\dfrac{120}{45} = 2 + \dfrac{30}{45} & | \quad r_5 = 120 - 2 * 45 = 30 \\
\dfrac{45}{30} = 1 + \dfrac{15}{30} & | \quad r_6 = 45 - 1 * 30 = 15 \\
\dfrac{30}{15} = 2 & | \quad r_7 = 0
\end{array}$$

Ciąg reszt

$$975 > 690 > 285 > 120 > 45 > 30 > 15$$

jest malejący.
Ostatnia reszta z dzielenia $r_6 = 15$ różna od zera jest największym wspólnym dzielnikiem liczb naturalnych $r_0 = 975$ i $_1 = 690$, piszemy

$$NWD(975, 690) = 15.$$

Zauważmy, że największy wspólny dzielnik $r_6 = 15$ liczb $r_0 = 975$ i $r_1 = 690$ jest również największym wspólnym dzielnikiem wszystkich poprzednich reszt

$$r_2 = 285, \; r_3 = 120, \; r_4 = 45, \; r_5 = 30, \; r_6 = 15$$

3

[3] Prosty algorytm Euklidesa z powodzeniem stosuje się w systemach obliczeniowych. Jest łatwy w pisaniu kodu w językach programowania.

Zadanie 0.1 *Znajdź największy wspólny dzielnik liczb* 425 *i* 125

(i) przez rozkład tych liczb na czynniki pierwsze.

(ii) stosując algorytm Euklidesa

Zadanie 0.2 *Znajdź największy wspólny dzielnik liczb stosując algorytm Euklidesa*

$$2672 \;\; i \;\; 848$$