

Rozszerzony Algorytm Euklidesa i Liniowe równanie diofantyczne

1. Obliczyć „ręcznie” $\text{NWD}(1001, 101)$ a następnie wyznaczyć $x, y \in \mathbb{Z}$ takie, że $1001x+101y = \text{NWD}(1001, 101)$.
2. Rozwiązać „ręcznie” równanie diofantyczne $63x+69y=33$.
3. Napisać program, który dla podanych z klawiatury liczb naturalnych różnych od zera a, b (zadbać o poprawność wpisywanych danych!) wyznacza $\text{NWD}(a, b)$ oraz $x, y \in \mathbb{Z}$ takie, że $ax+by = \text{NWD}(a, b)$. Wykorzystać następujący opis:

Zadanie rozwiązujemy pracując z parą równań:

$$\begin{aligned} (1) \quad & a \cdot u + b \cdot v = w \\ (2) \quad & a \cdot x + b \cdot y = z \end{aligned}$$

I. Startujemy od równań postaci:

$$\begin{aligned} (1) \quad & a \cdot 1 + b \cdot 0 = a \\ (2) \quad & a \cdot 0 + b \cdot 1 = b, \end{aligned}$$

czyli

$$u = 1, v = 0, w = a, x = 0, y = 1, z = b$$

Pętla:

- II. Zamieniamy miejscami równania (1) z (2).
- III. Wyznaczamy całkowity iloraz q liczby w przez z
- IV. Równanie (1) zastępujemy różnicą: $(1) - (2)q$, czyli

$$\begin{aligned} u &\leftarrow u - q \cdot x \\ v &\leftarrow v - q \cdot y \\ w &\leftarrow w - q \cdot z \end{aligned}$$

- V. Wykonujemy pętlę aż $w = 0$.
- VI. Na wyjściu $z = \text{NWD}(a, b)$ oraz x, y są szukanymi współczynnikami kombinacji.

4. Napisać algorytm rozwiązujący liniowe równanie diofantyczne postaci $ax+by=c$, gdzie a, b, c są liczbami całkowitymi różnymi od zera. Wykorzystać schemat:

We: a, b, c (zadbać o to by podane liczby były różne od zera), t – dowolna liczba całkowita

Wy: xt, yt

Jeżeli $d = \text{NWD}(a, b)$ nie dzieli c to nie ma rozwiązań.

w p.p.

x', y' są takie, że $d = ax' + by'$ (wykorzystać Rozszerzony Algorytm Euklidesa z Zadania 3)

$$a' = a/d, \quad b' = b/d, \quad c' = c/d$$

$$x_0 = c'x', \quad y_0 = c'y'$$

$$xt = x_0 + b't$$

$$yt = y_0 - a't$$

5. Tak samo jak zadanie 4. przy założeniu, że
We: a, b, c (zadbać o to by podane liczby były różne od zera), $t_1 \leq t_2$ – dowolne liczby całkowite
Wy: wszystkie rozwiązania xt, yt dla t należącego do przedziału $[t_1, t_2]$.