Algorytm Euklidesa

kółko I LO Białystok
26 lutego 2013

Zadanie 1
Jeżeli a jest iloczynem potęg liczb pierwszych $p_1^{a_1}, \ldots, p_k^{a_k}$, zaś b jest iloczynem potęg tych samych liczb pierwszych $p_1^{b_1}, \ldots, p_k^{b_k}$ to ile wynosi $NWD(a, b)$?

Zadanie 2
Dla jakich liczb naturalnych n ułamek

$$\frac{3n+4}{2n+5}$$

jest liczbą całkowitą?

Rozszerzony algorytm Euklidesa Dla danych a, b całkowitych dodatnich chcemy użyć algorytmu Euklidesa do znalezienia liczb x, y całkowitych takich, że

$$x \cdot a + y \cdot b = NWD(a, b).$$

Przeanalizujmy ciąg równości:

$$1 = NWD(0,1) = NWD(2 - 2 \cdot 1, 1) = NWD(2,1) = NWD(1,2) = NWD(7 - 3 \cdot 2, 2) = NWD(7,2),$$

$$1 = 1 \cdot \boxed{0} + 1 \cdot \boxed{1} = 1 \cdot \Big(\boxed{2} - 2 \cdot \boxed{1}\Big) + 1 \cdot \boxed{1} = 1 \cdot \boxed{2} - 1 \cdot \boxed{1} = -1 \cdot \boxed{1} + 1 \cdot \boxed{2} =$$

$$-1 \cdot \Big(\boxed{7} - 3 \cdot \boxed{2}\Big) + 1 \cdot \boxed{2} = -1 \cdot \boxed{7} + 4 \cdot \boxed{2}.$$

Poniżej podajemy pseudokod uogólnionego algorytmu:

1. Załóżmy $a \neq 0$.
   Niech x', y' będą wartościami zwróconymi przez $NWD(b, a \mod b)$. Znaczy to, że
   $$x' \cdot b + y' \cdot (a \mod b) = NWD(a, b).$$
   Podstawiamy $a \mod b = a - k \cdot b$, czyli
   $$y' \cdot a + (x' - y'k) \cdot b = x' \cdot b + y' \cdot (a - k \cdot b) = NWD(a, b),$$
   więc zwracamy $y', x' - y'k$. Możemy przy tym zauważyć, że $k = \lfloor a/b \rfloor$.
2. Załóżmy $a = 0$. Wtedy zwracamy $1, 1$, bo $1 \cdot 0 + 1 \cdot b = b = NWD(a, b)$.

Zadanie 3
Niech a, b, d będą całkowite. Równanie $x \cdot a + y \cdot b = d$ ma rozwiązanie w liczbach całkowitych x, y wtedy i tylko wtedy, gdy $NWD(a, b) \big| d$.

Zadanie 4 Chińskie twierdzenie o resztach
Załóżmy, że liczby całkowite dodatnie a, b są względnie pierwsze.

Dla dowolnych reszt $r_1 \mod a$, $r_2 \mod b$ istnieje liczba całkowita M taka, że

$$M \equiv r_1 \mod a \quad \text{oraz} \quad M \equiv r_2 \mod b.$$

Wskazówka: rozważ najpierw reszty $(1, 0)$ *i* $(0, 1)$.

Zadanie 5 Konstruowanie odwrotności $\mod n$
Dana są liczby względnie pierwsze a, n. Pokaż, jak przy pomocy algorytmu Euklidesa znaleźć liczbę b taką, że $a \cdot b \equiv 1 \mod n$.

Zastosuj opisaną procedurę do znalezienia liczby b takiej, że $8b \equiv 1 \mod 61$. Spróbuj również znaleźć liczbę b taką, że $8b \equiv 1 \mod 41$.

Zadanie 6
Dla których x całkowitych liczba $x^3 + 3 \cdot x^2 + 3 \cdot x$ jest podzielna przez $x^2 + 2x + 1$?

Zadanie 7
Wyznaczyć wszystkie liczby $a \in \mathbb{R}$, dla których wielomiany $f(x) = x^5 + ax^3 + x^2 + 1$ i $g(x) = x^4 + ax^2 + x + 1$ mają wspólny pierwiastek.