

1 - Rozszerzony algorytm Euklidesa

Tuesday, 18 June 2024

16:14

Mamy liczby $a, b > 0$.

Chcemy znaleźć s, t : $s \cdot a + t \cdot b = \gcd(a, b)$

$\text{GCD}(a, b)$:

if $b == 0$:

return $(1, 0)$

if $a < b$:

swap(a, b)

$(s', t') = \text{GCD}(b, a \% b)$ $s' \cdot b + r \cdot t' = d$

return $(t', s' - t' \cdot \lfloor \frac{a}{b} \rfloor)$

Wykonamy co najwyżej $\log_2 \max(a, b)$ operacji:
„rzędy Fibonacciego”.

Złożoność: $\tilde{O}(\log^2 \max(a, b))$