Euklidov algoritam

Ulaz

Dati su prirodni brojevi a i b.

Izlaz

NZD(a, b)

Algoritam

```
nzd(m, n) {
    a = max(m, n);
    b = min(m, n);
    r = 1;

    while (r != 0) {
        r = a % b;
        a = b;
        b = r;
    }

    return a;
}

nzd(m, n) {
    while (n != 0) {
        m = m % n;
        zameni(m, n);
    }
    return m;
}
```

Složenost

O(log(m+n))

Zadaci

Zadatak 1

Konstruisati algoritam za traženje NZD-a k datih brojeva.

Rešenje: Uzmemo najmanji broj - na primer a1. Ostale a2, ..., ak zamenimo ostacima koje daju pri deljenju sa a1, posle čega se uklanjaju sve nule iz skupa. Ovim operacijama se smanjuje velicina najveceg broja u skupu!

Posle konacnog broja koraka dolazimo do sistema od samo jednog broja i to je NZD brojeva a1,a2,...,ak.Broj koji ostane na kraju je traženi rezultat.

Zadatak 2

Konstruisati algoritam za traženje NZS-a k datih brojeva.

Rešenje:

Ind. baza: Za dva broja:

```
NZS(a, b) = a · b / NZD(a, b)
```

Ind. korak: Za k + 1 brojeva kad je NZS(a_1, ..., a_k) poznat:

```
A□□ = NZS(a_1, ..., a_{k+1})
     = NZS(A_k, a_{k+1})
     = A_k · a_{k+1} / NZD(A_k, a_{k+1})
```

Zadatak 3

Napisati algoritam koji pronalazi bar jedno celobrojno rešenje jednačine ax + by = NZD(a, b)

Rešenje:

Pretp. da je a ≥ b. Tada imamo:

$$a = q_0 b + r_1, 0 \leq r_1 < b$$

$$b = q_1 r_1 + r_2, 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3, 0 \leq r_3 < r_2$$

$$\vdots$$

$$r_{n-1} = q_n r_n + r_{n+1}, 0 \leq r_{n+1} < r_n$$

$$r_n = q_{n+1} r_{n+1}$$

$$r_{n+1} = NZD(a, b)$$

Ove jednakosti je moguće zapisati i ovako:

$$r_1 = a - q_0 b$$

$$r_2 = b - q_1 r_1 = b - q_1(a - q_0 b) = -q_1 a + (1 + q_0 q_1) b$$

$$r_3 = r_1 - q_2 r_2 = \dots$$

$$\vdots$$

$$r_{i+1} = r_{i-1} - q_i r_i = \dots = x_{i+1} a + y_{i+1} b$$

$$\vdots$$

$$r_{n+1} = x_{n+1} a + y_{n+1} b$$

za neke $x_i, y_i \in \mathcal{Z}$

U n+1 koraka dobijamo x_{n+1} i y_{n+1} takvo da je r_{n+1} =NZD(a, b) = $x_{n+1} \cdot a + y_{n+1} \cdot b$

Ako je u i-tom koraku dobijeno:

$$r_i = x_i a + y_i b$$

$$r_{i-1} = x_{i-1} a + y_{i-1} b$$

$$r_{i+1} = r_{i-1} - q_i r_i = x_{i-1} a + y_{i-1} b - q_i (x_i a + y_i b)$$

$$= (x_{i-1} - q_i x_i) a + (y_{i-1} - q_i y_i) b = x_{i+1} a + y_{i+1} b$$

DAKLE,

$$x_{i+1} = x_{i-1} - q_i x_i$$

$$y_{i+1} = y_{i-1} - q_i y_i$$

Početne vrednosti su: $x_{-1} = 1$, $x_0 = 0$, $y_{-1} = 0$ i $y_0 = 1$.

Zaključujemo da je za računanje tekućeg koeficijenta potrebno znati vrednosti prethodna dva odgovarajuća koeficijenta.

```
resenje(a, b) {
    uz_a_pred = 1;
    uz_b_pred = 0;

    uz_a = 1;
    uz_b = 1;

    while (b != 0) {
        q = a / b;
        r = a % b;
        a = b;
        b = r;

        if (b != 0) {
            uz_a_temp = uz_a;
            uz_b_temp = uz_b;
            uz_a = uz_a_pred - q * uz_a;
            uz_b = uz_b_pred - q * uz_b;
            uz_a_pred = uz_a_temp;
            uz_b_pred = uz_b_temp;
        }

        x = uz_a;
        y = uz_b;
    }

    return (x, y);
}
```