UVOD U TEORIJU BROJEVA – FORMULE

Euklidov algoritam. Neka su b i $c > 0$ cijeli brojevi i neka je

$$\begin{array}{rcll} b &=& cq_1 + r_1, & 0 < r_1 < c, \\ c &=& r_1 q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 &=& r_2 q_3 + r_3, & 0 < r_3 < r_2, \\ &\vdots& & \\ r_{n-2} &=& r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &=& r_n q_{n+1}. & \end{array}$$

Tada je $r_n = (b, c)$.

* Rješenja jednadžbe $bx + cy = (b, c)$ mogu se dobiti na sljedeći način:

$$\begin{array}{llll} x_{-1} = 1, & x_0 = 0, & x_i = x_{i-2} - q_i x_{i-1}; & \\ y_{-1} = 0, & y_0 = 1, & y_i = y_{i-2} - q_i y_{i-1}; & i = 1, 2, \dots, n, \end{array}$$

$$bx_n + cy_n = (b, c).$$

* $\varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1)$

* $\tau(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \prod_{i=1}^k (\alpha_i + 1)$

* $\sigma(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \prod_{i=1}^k \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$

* Sve primitivne Pitagorine trojke (x, y, z) u kojima je y paran, dane su formulama $x = m^2 - n^2$, $y = 2mn, z = m^2 + n^2$, gdje je $m > n$ i m, n su relativno prosti brojevi različite parnosti.

Sve Pitagorine trojke dane su identitetom $[d(m^2 - n^2)]^2 + (2dmn)^2 = [d(m^2 + n^2)]^2$, $d \in \mathbb{N}$.

* Razvoj broja $\alpha \in \mathbb{R}$ u verižni razlomak (uz $\alpha_0 = \alpha$): $a_i = \lfloor \alpha_i \rfloor$, $a_i \neq \alpha_i \Rightarrow \alpha_{i+1} = \frac{1}{\alpha_i - a_i}$, $i \in \mathbb{N}_0$. Ako je $\alpha \in \mathbb{Q}$, onda postoji $n \in \mathbb{N}$ takav da je $a_n = \alpha_n$ pa je $\alpha = [a_0, a_1, \dots, a_n]$. U suprotnom je $\alpha = [a_0, a_1, a_2, \dots]$.

* Brojevi p_n i q_n (pri čemu je $\frac{p_n}{q_n}$ n-ta konvergenta u razvoju) zadovoljavaju rekurzije $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$ uz $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$.

* Ako je $\alpha = \frac{b}{c}$, $b > c > 0$, onda se razvoj broja α u verižni razlomak može dobiti iz Euklidovog algoritma: $\alpha = \frac{b}{c} = q_1 + \frac{1}{\frac{c}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = \dots = [q_1, q_2, ..., q_{n+1}]$.

* Razvoj broja $\alpha_0 = \frac{s_0 + \sqrt{d}}{t_0}$, $d \in \mathbb{N}, d \neq \square$, u verižni razlomak može se dobiti sljedećim algoritmom:

$$a_i = \left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor,\ s_{i+1} = a_i t_i - s_i,\ t_{i+1} = \frac{d - s_{i+1}^2}{t_i},\ i \in \mathbb{N}_0.$$

* Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, onda su sva rješenja ove jednadžbe dana sa (x_n, y_n) za $n \in \mathbb{N}$, gdje su x_n, y_n prirodni brojevi definirani sa $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.

* Neka je r duljina perioda u razvoju u verižni razlomak broja $\sqrt{d}$ i $\frac{p_i}{q_i}$ i-ta konvergenta u razvoju od $\sqrt{d}$.

(1) Ako je r paran, onda jednadžba oblika $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana s $x = p_{nr-1}, y = q_{nr-1}$, $n \in \mathbb{N}$.

(2) Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana sa $x = p_{nr-1}, y = q_{nr-1}$, n neparan, dok su sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana s $x = p_{nr-1}, y = q_{nr-1}$, n paran.