Fracţii continue. Atacul lui Wiener

Fie a şi b numere naturale, $b \neq 0$.

$$\begin{array}{lcll} a & = & q_1 \cdot b + r_1, & 0 < r_1 < b \\ b & = & q_2 \cdot r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 & = & q_3 \cdot r_2 + r_3, & 0 < r_3 < r_2 \\ & \vdots & & \\ r_{k-2} & = & q_k \cdot r_{k-1} + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} & = & q_{k+1} \cdot r_k & \end{array} \tag{1}$$

Fracţia $\frac{a}{b}$ poate fi scrisă după cum urmează:

$$\begin{array}{lcl} \frac{a}{b} & = & \frac{q_1 b + r_1}{b} \\ & = & q_1 + \frac{1}{\frac{b}{r_1}} \\ & = & q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} \\ & \vdots & \\ & = & q_1 + \frac{1}{q_2 + \frac{1}{\frac{\vdots}{q_k + \frac{1}{q_{k+1}}}}} \end{array}$$

Ultimul termen va fi referit ca *fracţia continuă asociată fracţiei* $\frac{a}{b}$ şi va fi notat prin $[q_1, q_2, \ldots, q_{k+1}]$. Expresiile $[q_1, q_2, \ldots, q_i]$, $1 \leq i \leq k+1$, vor fi numite *convergentele fracţiei continue* $[q_1, q_2, \ldots, q_{k+1}]$.

Considerăm numerele naturale α_i şi β_i date prin

$$\begin{array}{ll} \alpha_1 = q_1, & \beta_1 = 1 \\ \alpha_2 = q_1 \cdot q_2 + 1, & \beta_2 = q_2 \\ \alpha_i = q_i \cdot \alpha_{i-1} + \alpha_{i-2}, & \beta_i = q_i \cdot \beta_{i-1} + \beta_{i-2}, \\ & \text{pentru orice } 3 \leq i \leq k+1 \end{array} \tag{2}$$

Atunci are loc relaţia

$$[q_1, q_2, \ldots, q_i] = \frac{\alpha_i}{\beta_i},$$

$$(\alpha_i, \beta_i) = 1,$$

pentru orice $1 \leq i \leq k+1$.

Exemplul 1 Să considerăm $a = 4$, $b = 11$. Vom obţine

$$\begin{array}{rcl} 4 & = & 0 \cdot 11 + 4 \\ 11 & = & 2 \cdot 4 + 3 \\ 4 & = & 1 \cdot 3 + 1 \\ 3 & = & 3 \cdot 1 \end{array}$$

şi $[0, 2, 1, 3] = 0 + \frac{1}{2+\frac{1}{1+\frac{1}{3}}}$, $[0] = \frac{0}{1}$, $[0, 2] = \frac{1}{2}$ şi $[0, 2, 1] = \frac{1}{3}$.

Atacul lui Wiener

Fie p şi q numere prime astfel încât $q < p < 2q$, şi $n = p \cdot q$. Se aleg[1] $e, d \in \mathbf{Z}^*_{\phi(n)}$ astfel încât

$$e \cdot d \equiv 1 \; mod \; \phi(n),$$

unde $\phi(n) = (p-1)(q-1)$, şi $d < \frac{\sqrt[4]{n}}{3}$.

Există $l \in \mathbf{N}$ astfel încât

$$e \cdot d - 1 = l \cdot \phi(n).$$

Fie $[q_1, q_2, \ldots, q_{k+1}]$ fracţia contină asociată fracţiei $\frac{e}{n}$. Atunci există $1 \leq i \leq k+1$ astfel încât $[q_1, q_2, \ldots, q_i] = \frac{l}{d}$.

Având e şi n, se pot determina l şi d în felul următor:

i:=0;
`repetă`
  i:=$i + 1$;
  `determină` α_i, β_i folosind relaţiile (1) (pentru $a = e$ şi $b = n$) şi (2);
  $l := \alpha_i$; $d := \beta_i$;
`până când` $criteriu(l, d) = 1$

unde

$$criteriu(l, d) = \begin{cases} \mathtt{1}, & \text{dacă sistemul } \left\{ \begin{array}{l} x \cdot y = n \\ (x-1) \cdot (y-1) = \frac{ed-1}{l} \end{array} \right. \text{ are soluţii întregi} \\ \mathtt{0}, & \text{altfel} \end{cases}$$

[1] În loc de $\phi(n)$ se poate pune $\lambda(n)$, unde $\lambda(n) = [p-1, q-1]$.