Anexa 1

Algoritmul lui Euclid extins

După cum se ştie, algoritmul lui Euclid constituie o modalitate eficace de determinare a celui mai mare divizor comun a două numere întregi pozitive. El poate fi extins pentru a determina şi inversele elementelor dintr-un corp finit Z_n.

Să reamintim întâi algoritmul lui Euclid (forma clasică):

Fie $r_0, r_1 \in N^*$.
Se efectuează secvenţa de împărţiri succesive:

$$\begin{array}{ll} r_0 = q_1 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_2 r_2 + r_3 & 0 < r_3 < r_2 \\ \quad\vdots & \\ r_{m-2} = q_{m-1} r_{m-1} + r_m & 0 < r_m < r_{m-1} \\ r_{m-1} = q_m r_m. & \end{array} \tag{1}$$

Deoarece $cmmdc(r_0, r_1) = cmmdc(r_1, r_2) = \ldots = cmmdc(r_{m-1}, r_m) = r_m$, rezultă că cel mai mare divizor comun dintre r_0 şi r_1 este r_m.

Să definim acum şirul $t_0, t_1, \ldots, t_m$ astfel:

$$\begin{array}{l} t_0 = 0, \quad t_1 = 1 \\ t_j = t_{j-2} - q_{j-1} t_{j-1} \ (mod\ r_0), \ j \geq 2 \end{array} \tag{2}$$

Teorema 1.1. *Pentru* $0 \leq j \leq m$ *avem* $r_j \equiv t_j r_1 \ (mod\ r_0)$ *unde* r_j *şi* t_j *sunt definite de* (1) *respectiv* (2).

Demonstraţie. Se foloseşte o inducţie după j.

Pentru $j = 0$ şi $j = 1$ afirmaţia este banală.

Presupunem afirmaţia adevărată pentru $j = i - 1$ şi $j = i - 2$ ($i \geq 2$) şi să o arătăm pentru $j = i$. Toate calculele se fac modulo r_0.

Conform ipotezei de inducţie, $r_{i-2} = t_{i-2} r_1, \ r_{i-1} = t_{i-1} t_1$.

Acum:

$r_i = r_{i-2} - q_{i-1} r_{i-1} = t_{i-2} r_1 - q_{i-1} t_{i-1} r_1 = (t_{i-2} - q_{i-1} r_{i-1}) r_1 = t_i r_1.$ $\square$

Corolarul 1.1. *Dacă* $(r_0, r_1) = 1$ *atunci* $t_m = r_1^{-1}$ $(mod\ r_0)$.

Se poate da acum algoritmul extins al lui Euclid, care pentru $n > 1$ şi $b \in Z_n^*$ va determina b^{-1} *mod n* (dacă există).

Algoritmul lui Euclid extins:

1. $n_0 \longleftarrow n,\ b_0 \longleftarrow b,\ t_0 \longleftarrow 0,\ t \longleftarrow 1;$
2. $q \longleftarrow \left[\frac{n_0}{b_0}\right], \quad r \longleftarrow n_0 - q \cdot b_0;$
3. **while** $r > 0$ **do**
   - 3.1. $temp \longleftarrow t_0 - q \cdot t$
   - 3.2. **if** $temp \geq 0$ **then** $temp \longleftarrow temp \quad (mod\ n)$
     else $temp \longleftarrow n - ((-temp) \quad (mod\ n))$
   - 3.3. $n_0 \longleftarrow b_0,\ b_0 \longleftarrow r,\ t_0 \longleftarrow t,\ t \longleftarrow temp;$
   - 3.4. $q \longleftarrow \left[\frac{n_0}{b_0}\right],\ r \longleftarrow n_0 - q \cdot b_0;$
4. **if** $b_0 \neq 1$ **then** b nu are inversă *mod n*.
   else $b^{-1}\ (mod\ n) = t$.

Exemplul 1.1. *Să calculăm* 28^{-1} *mod* 75, *folosind algoritmului lui Euclid extins. Vom avea pe rând:*

n_0	b_0	q	r	t_0	t	$temp$
75	28	2	19	0	1	73
28	19	1	9	1	73	3
19	9	2	1	73	3	67
9	$\underline{1}$	9	0	3	$\underline{67}$	

Deci 28^{-1} *mod* 75 $= 67$.

Anexa 2

Teorema chineză a resturilor

Teorema 2.1. *Se dau numerele* $p_1, p_2, \ldots, p_r$ *prime între ele şi fie* $n = p_1 p_2 \ldots p_r$. *Atunci sistemul de ecuaţii*

$$x \equiv a_i \quad (mod\ p_i), \qquad 1 \leq i \leq r$$

are soluţie comună în intervalul $[0, n-1]$.

Demonstraţie. Pentru fiecare i, $cmmdc(p_i, n/p_i) = 1$; deci există numerele y_i astfel încât

$$\frac{n}{p_i} \cdot y_i \equiv 1\ (mod\ p_i).$$

De asemenea, pentru $j \neq i$, deoarece $p_j | cmmdc(n/p_i)$, avem $\frac{n}{p_i} \cdot y_i \equiv 0\ (mod\ p_j)$.

Alegem

$$x = \sum_{i=1}^{r} \frac{n}{p_i} \cdot y_i \cdot a_i\ (mod\ n).$$

Pentru orice i, x este o soluţie a ecuaţiei $x \equiv a_i\ (mod\ p_i)$ deoarece în Z_{p_i} avem $x = \frac{n}{p_i} \cdot y_i \cdot a_i = a_i$. □

Exemplul 2.1. *Fie* $r = 3$, $p_1 = 7$, $p_2 = 11$, $p_3 = 13$, *deci* $n = 1001$. *Notând* $m_i = \frac{n}{p_i}$, *avem* $m_1 = 143$, $m_2 = 91$ *şi* $m_3 = 77$.

Folosind algoritmul lui Euclid, se obţine $y_1 = 5$, $y_2 = 4$, $y_3 = 12$.

Soluţia generală este atunci

$$x = 715a_1 + 364a_2 + 924a_3\ (mod\ 1001).$$

De exemplu, pentru sistemul

$$x \equiv 5\ (mod\ 7), \quad x \equiv 3\ (mod\ 11), \quad x \equiv 10\ (mod\ 13)$$

formula de sus dă

$x = 715 \cdot 5 + 364 \cdot 3 + 924 \cdot 10\ (mod\ 1001) = 13907\ (mod\ 1001) = 894.$

Verificarea se realizează reducând x *modulo* 7, 11 *şi* 13.

2.1 Exerciţii

2.1. *Folosiţi algoritmul lui Euclid extins pentru a calcula inversele*

$$17^{-1}\ (mod\ 101), \qquad 357^{-1}\ (mod\ 1234), \qquad 3125^{-1}\ (mod\ 9987)$$

2.2. *Calculaţi* $cmmdc(57, 93)$ *şi aflaţi numerele întregi* s, t *astfel ca*

$$57s + 93t = cmmdc(57, 93).$$

2.3. *Fie funcţia* $g : Z_{105} \longrightarrow Z_3 \times Z_5 \times Z_7$ *definită*

$$g(x) = (x\ mod\ 3,\ x\ mod\ 5,\ x\ mod\ 7).$$

Găsiţi o formulă pentru g^{-1} *şi utilizaţi-o pentru a calcula* $g^{-1}(2, 2, 3)$.

2.4. *Rezolvaţi sistemul de congruenţe*

$$\begin{array}{ll} x \equiv 12 & (mod\ 25), \\ x \equiv 9 & (mod\ 26), \\ x \equiv 23 & (mod\ 27) \end{array}$$

2.5. *Rezolvaţi sistemul de congruenţe*

$$\begin{array}{ll} 13x \equiv 4 & (mod\ 99), \\ 15x \equiv 56 & (mod\ 101) \end{array}$$