Algoritmul lui Euclid extins

Se întâlnesc multe probleme care – în ultima instanţă se reduc la următorul enunţ:

> Fiind date două numere naturale a şi n prime între ele, să se afle un număr natural x astfel încât
>
> $$a \cdot x = 1 \pmod{n}$$

Numărul x este *inversul lui a modulo n*. Existenţa lui rezultă imediat din teorema

Teorema 1 *Fiind date două numere naturale a, n, există două numere întregi x, y unic determinate, astfel încât*

$$a \cdot x + n \cdot y = d$$

unde $d = (a, n)$.

Demonstraţia este cunoscută şi se bazează pe Algoritmul lui Euclid. □

Dacă se ia $d = 1$ şi se consideră calculele modulo n, se ajunge la afirmaţia cerută. În multe situaţii n este prim, ceea conduce la concluzia că în aceste cazuri, orice număr din $Z_n \setminus \{0\} = \{1, 2, \ldots, n-1\}$ admite invers.

Problema este de a construi un algoritm de complexitate cât mai mică, care să determine inversul unui număr (dacă acesta există).

Un astfel de algoritm poate fi generat tot pe baza algoritmului lui Euclid.

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 $(r_0, r_1) = (r_1, r_2) = \ldots = (r_{m-1}, r_m) = r_m$, 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:

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

Teorema 2 *Pentru $0 \leq j \leq m$ avem $r_j \equiv t_j r_1 \pmod{r_0}$ 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.

O presupunem adevărată pentru $j = i - 1$ şi $j = i - 2$ $(i \geq 2)$ si 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:

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

Corolar 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 $b \in Z_n \setminus \{0\}$ va determina $x = b^{-1}\ mod\ n$ (dacă există).

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

Exemplul 1 *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	<u>1</u>	9	0	3	<u>67</u>	

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

Un studiu al complexităţii arată că avem de-a face cu un algoritm de complexitate logaritmică.

Teorema chineză a resturilor

Apar multe probleme de genul: *Să se găsească un număr care împărţit la x să dea restul a, împărţit la y să dea restul b etc.*

Modalitatea matematică de rezolvare se bazează pe **Teorema chineză a resturilor**:

Teorema 3 *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*

$$x = a_i \pmod{p_i}, \qquad 1 \leq i \leq r$$

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

Demonstraţie: Pentru fiecare i, $(p_i, n/p_i) = 1$; deci există numerele $y_1, y_2, \ldots, y_n$ astfel încât

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

Ele pot fi aflate folosind algoritmul lui Euclid extins.

De asemenea, pentru $j \neq i$, deoarece $p_j | (n/p_i)$, avem

$$\frac{n}{p_i} \cdot y_i = 0 \ (mod\ p_j).$$

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 $x = a_i \ (mod\ p_i)$ deoarece în Z_{p_i} avem $x = \dfrac{n}{p_i} \cdot y_i \cdot a_i = a_i$. □

Exemplul 2 *Fie $r = 3$, $p_1 = 7$, $p_2 = 11$, $p_3 = 13$, deci $n = 1001$. Notând $m_i = \dfrac{n}{p_i}$, avem $m_1 = 143$, $m_2 = 91$ şi $m_3 = 77$. Folosind algoritmul lui Euclid extins, se obţine $y_1 = 5$, $y_2 = 4$, $y_3 = 12$.*

Soluţia generală este atunci

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

De exemplu, pentru sistemul

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

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 13.

Probleme:

1. Fiind dat un număr $n \in (1, 10^{10}),\ (n, 2) = 1, (n, 5) = 1$, să se afle inversul lui modulo 10^{10}.

2. Fiind dat un număr $n \in [2, 10^9]$, să se determine două numere naturale a, b astfel încât
$$a \cdot b = 1 \pmod{n}$$
iar $|a - b|$ să fie minim.

3. Fie numerele $a_1, a_2, a_3, b_1, b_2, b_3, n_1, n_2, n_3$ din intervalul $[2, 10^9]$. Ştiind că sistemul de ecuaţii
$$\left\{ \begin{array}{rcrcll} a_1x & + & b_1 & = & 0 & (mod\ n_1) \\ a_2x & + & b_2 & = & 0 & (mod\ n_2) \\ a_3x & + & b_3 & = & 0 & (mod\ n_3) \end{array} \right\}$$
are soluţie în $[1, 10^9]$, să se găsească această soluţie.

Prof. Dr. Adrian Atanasiu

8 iunie 2005