ASUPRA APLICĂRII ALGORITMULUI LUI EUCLID PENTRU AFLAREA c. m. m. d. c. A DOUA NUMERE

DE

TIBERIU POPOVICIU
Membru corespondent al Academiei R.P.R.

Comunicare prezentată în şedinţa din 24 Septemvrie 1952 a Filialei Cluj a Academiei R.P.R.

1. — Fie a, b, două numere naturale. Pentru aflarea *c. m. m. d. c.* al lor se aplică algoritmul lui Euclid, care constă în efectuarea împărţirilor succesive

$$
\begin{aligned}
b &= qa + r, \\
a &= q_1 r + r_1, \\
r &= q_2 r_1 + r_2, \\
&\ldots\ldots\ldots\ldots \\
r_{n-2} &= q_n r_{n-1} + r_n, \\
r_{n-1} &= q_{n+1} r_n .
\end{aligned}
\tag{1}
$$

Putem presupune $b > a$. Căturile $q, q_1, \ldots\ldots, q_{n+1}$ sunt numere întregi pozitive, iar resturile $r, r_1, \ldots\ldots, r_n$ deasemenea sunt numere întregi şi pozitive şi verifică inegalităţile

$$a > r > r_1 > \cdots > r_n > 0 .$$

Pentru a găsi *c. m. m. d. c.* r_n al numerelor a, b, trebuesc, conform tabloului (1), efectuate $n + 2$ împărţiri[1]). Numărul împărţirilor poate fi delimitat în mod interesant în funcţie de cel mai mic dintre numerele a şi b (adică a). Avem în această privinţă următorul rezultat bine cunoscut: [1].

TEOREMA 1. — *Numărul împărţirilor ce trebuesc efectuate pentru aflarea c. m. m. d. c. a două numere întregi şi pozitive este cel mult egal cu de 5 ori numărul cifrelor celui mai mic dintre aceste numere.*

---

[1]) Impărţirea lui r_{n-1} prin r_n poate fi evitată în cazul când divizibilitatea lui r_{n-1} prin r_n este recunoscută imediat pe o altă cale. Acest lucru se întâmplă totdeauna când $= 1$.

O demonstrație simplă a acestei teoreme a fost dată de P. L. Cebâșev [2]. In cele ce urmează vom arăta că metoda lui Cebâșev permite să precizăm puțin teorema 1.

2. — Avem $q_i \geqq 1, i = 1, 2, \ldots, n+1$ și, ținând seamă de $r_{n-1} > r_n$ deducem chiar $q_{n+1} \geqq 2$. Formulele (1) ne dau atunci

$$
(2) \qquad
\begin{aligned}
a &\geqq r + r_1, \\
r &\geqq r_1 + r_2, \\
r_1 &\geqq r_2 + r_3, \\
&\ldots\ldots\ldots\ldots \\
r_{n-2} &\geqq r_{n-1} + r_n, \\
r_{n-1} &\geqq 2r_n.
\end{aligned}
$$

Să considerăm acum șirul de numere

$$
(3) \qquad 1, 1, 2, 3, 5, 8, 13, 21, \ldots\ldots
$$

unde fiecare termen este egal cu suma celor doi termeni precedenți. Șirul (3) este deci definit de relația de recurență

$$
(4) \qquad u_0 = u_1 = 1, \quad u_m = u_{m-1} + u_{m-2}, \quad m = 2, 3, \ldots
$$

Ținând seamă de (4) și eliminând pe $r, r_1, \ldots, r_{n-1}$ din inegalitățile (2), deducem $a \geqq u_{n+2}\, r_n$ deci

$$
(5) \qquad a \geqq u_{n+2}.
$$

Această inegalitate delimitează pe n în funcție de a.

Avem acum următoarea

LEMA 1. — *Dacă* α *este rădăcina pozitivă a ecuației* $\left(\alpha = \frac{1+\sqrt{5}}{2}\right)$

$$
(6) \qquad x^2 - x - 1 = 0
$$

avem

$$
(7) \qquad u_m \geqq \alpha^{m-1}, \quad m = 0, 1, \ldots
$$

Demonstrația se face ușor prin inducție completă, ținând seamă de (4).

Se verifică ușor că avem

$$
(8) \qquad \alpha > \frac{8}{5}.
$$

Ținând seamă de ecuația (6) deducem

$$
\alpha^5 = \alpha^4 + \alpha^3 = \alpha^3(\alpha + 1) = \alpha(\alpha + 1)^2 = \alpha(3\alpha + 2) = 5\alpha + 3
$$

și din (8) rezultă că

$$
\alpha^5 > 5 \cdot \frac{8}{5} + 3 = 11.
$$

Ținând seamă de (5) și (7) deducem prin urmare

$$
a > 11^{\frac{n+1}{5}}
$$

Dacă k este numărul cifrelor lui a scris în sistemul de numerație cu baza 11, avem $a < 11^k$, deci $n + 1 < 5k$, adică $n + 2 \leqq 5k$. Putem dar enunța următoarea proprietate:

TEOREMA 2. — *Numărul împărțirilor ce trebuesc efectuate pentru aflarea c. m. m. d. c. a două numere întregi și pozitive este cel mult egal cu de 5 ori numărul cifrelor celui mai mic dintre aceste numere, scris în sistemul de numerație cu baza 11.*

3. — Rezultatul precedent se poate generaliza încă puțin.

Fie l un număr natural și să calculăm pe $[\alpha^l]$, adică partea întreagă a lui α^l, α fiind rădăcina pozitivă a ecuației (6). Se demonstrează ușor, prin inducție completă, că

$$
\alpha^l = u_{l-1}\,\alpha + u_{l-2}
$$

de unde

$$
(9) \qquad [\alpha^l] = [u_{l-1}\,\alpha] + u_{l-2}.
$$

Avem acum

LEMA 2. — *Dacă* α *este rădăcina pozitivă a ecuației* (6) *și* u_n *termenii șirului* (3), *avem*

$$
(10) \qquad [u_n \alpha] = u_{n+1} - \frac{1-(-1)^n}{2}, \quad n = 0, 1, \ldots
$$

Pentru aceasta se demonstrează întâi prin inducție completă că

$$
u_{n+1} - \alpha u_n = \frac{(-1)^{n+1}}{\alpha^{n+1}}.
$$

De aici rezultă că

$$
\begin{aligned}
u_{n+1} &< u_n \alpha < u_{n+1} + 1, \text{ pentru } n \text{ par}, \\
u_{n+1} - 1 &< u_n \alpha < u_{n+1}, \text{ pentru } n \text{ impar}
\end{aligned}
$$

ceea ce demonstrează lema 2.

Ținând acum seamă de (9) și (10) deducem

$$
(11) \qquad [\alpha^l] = u_l + u_{l-2} - \frac{1-(-1)^{l-1}}{2} = g
$$

și atunci inegalitatea (5) ne dă[2]) $a \geqq \alpha^{n+1} > [\alpha^l]^{\frac{n+1}{l}} = g^{\frac{n+1}{l}}$ sau

$$
a > g^{\frac{n+1}{l}}.
$$

Deducem prin urmare, ca mai sus, proprietatea:

2) $u_{l-1}\,\alpha$ nu poate fi întreg deci $[\alpha^l] < \alpha^l$.

TEOREMA 3. — *Numărul împărţirilor ce trebuesc efectuate pentru aflarea c. m. m. d. c. a două numere întregi şi pozitive este cel mult egal cu de l ori numărul cifrelor celui mai mic dintre aceste numere scris într'un sistem de numeraţie cu baza cel mult egală cu numărul g, dat de formula* (11).

In acest enunţ am ţinut seamă şi de faptul că numărul cifrelor unui număr descreşte când baza în care se scrie acest număr creşte.

Pentru un l dat baza de numeraţie care ne dă limitaţia cea mai bună, după metoda precedentă, este tocmai g. Pentru $l = 5$ se găseşte $g = 11$. Pentru primele 15 valori ale lui l ($\geqq 2$), baza g cea mai avantajoasă este dată în tabloul

l	g	l	g	l	g
2	2	7	29	12	321
3	4	8	46	13	521
4	6	9	76	14	842
5	11	10	122	15	1364
6	17	11	199	16	2205

Facultatea de Matimatică şi Fizică
a Universităţii „V. Babeş" din Cluj

BIBLIOGRAFIE

1. I. M. Vinogradov, *Osnovî teorii čisel*, Moskva—Leningrad, 1949, pag. 22.
2. D. Seliwanoff, *Lehrbuch der Differenzenrechnung*, 1904, pag. 91—92.

КРАТКОЕ СОДЕРЖАНИЕ

О применении алгорифма Эвклида для нахождения наибольшего общего делителя двух чисел

ТИБЕРИУ ПОПОВИЧ

Дополняя немного метод П. Л. Чебашева нахождения числа делений необходимых для определения наибольшего общего делителя двух натуральных чисел a, b ($a < b$), замечаем, что в классическом выражении по отношению к краткому a, которй должен быть взят, база 10 численной системы может быть заменена 11. Рассматривая немного более общую задачу, находим, что база 11 в некотором смысле является наилучшей.

RÉSUMÉ.

Sur la détermination par l'algorithme d'Euclid du p. g. c. d. de deux noembers.

par

TIBERIU POPOVICIU

En complétant un peu la méthode de P. L. Cebâşev pour la détermination du nombre des divisions nécessaires à faire pour obtenir le *p. g. c. d.* de deux nombres naturels a, b ($a < b$), on remarque que dans l'énoncé bien connu, relatif au multiple de a qu'on doit predre, la base 10 du système de numération peut être remplacée par 11. En examinant un problème un peu plus général, on trouve que la base 11, dans un certain sens, est la meilleure.