Lucrările Seminarului de
CREATIVITATE MATEMATICĂ
vol.2(1992-1993), 77-92

ASUPRA DETERMINĂRII CELUI MAI MARE DIVIZOR COMUN A DOUĂ ELEMENTE ÎN UNELE INELE INTEGRE

Lăcrimioara IANCU
Dana BOTORCE

În inelul Z al numerelor întregi spunem că a este un divizor al lui b, $a|b$, dacă $\exists c \in Z$ a.î. $b=a\cdot c$. Elementul d este un cel mai mare divizor comun al numerelor a şi b (cmmdc) dacă

1) $d|a$, $d|b$ şi

2) $d'|a$, $d'|b \Rightarrow d'|d$.

O metodă de calcul a cmmdc a două numere întregi este algoritmul lui Euclid, a cărui aplicabilitate este esenţial determinată de valabilitatea teoremei împărţirii cu rest.

Noţiunile de divizibilitate şi cel mai mare divizor comun a două numere întregi se extind prin analogie în inele integre, adică în inele comutative, cu unitate şi fără divizori ai lui zero.

Spre exemplu, în inelul $Z[i]=\{m+ni|m,n\in Z\}$ - inelul întregilor lui Gauss, spunem că z_1 este un divizor al lui z_2, $z_1|z_2$, dacă $\exists z\in Z[i]$ a.î. $z_2=z\cdot z_1$.

Elementul d este un cel mai mare divizor comun al elementelor $z_1, z_2 \in Z[i]$ dacă:

1) $d|z_1$, $d|z_2$

2) $d'|z_1$, $d'|z_2 \Rightarrow d'|d$

Poate fi folosit în acest caz algoritmul lui Euclid pentru a determina cmmdc a două elemente? Răspunsul afirmativ este condiţionat de valabilitatea teoremei împărţirii cu rest; ea permite elaborarea algoritmului lui Euclid pentru determinarea celui mai mare divizor comun a două elemente. Această teoremă a

introdus în algebră o clasă de inele în care are loc o relaţie de acelasi tip si anume, cele euclidiene.

Definiţie *Numim inel euclidian un inel integru A în care se defineşte o funcţie f:A\{0}->N astfel încât sunt îndeplinite urmatoarele două condiţii:*

1) oricare ar fi elementele nenule a,b∈A astfel că a divide b, rezultă că f(a)≤f(b);

2) pentru orice a,b∈A, b≠0, există q,r∈A astfel încât

$$a = bq+r, \text{ unde } r=0 \text{ sau } f(r)<f(b) \qquad (1)$$

Egalitatea din (1) se numeşte formula împărţirii cu rest în inelul euclidian A; elementele q si r se numesc câtul, respectiv restul împărţirii.

Spre exemplu, inelul numerelor întregi Z împreună cu funcţia valoare absolută f:Z->N, f(n)=|n|, este un inel euclidian.

O *proprietate* importantă a inelelor euclidiene este următoarea:

Într-un inel euclidian oricare două elemente au un cel mai mare divizor comun (şi, evident, un cel mai mic multiplu comun).

Demonstratia se bazeaza pe algoritmul lui Euclid conform căruia cel mai mare divizor comun al elementelor a si b este ultimul rest nenul din şirul de egalităţi succesive definite de împărţirea lui a la b; a lui b la restul împărţirii anterioare s.a.m.d. cu verificarea de fiecare dată a inegalităţii de tipul (1).

Lucrarea de faţă îsi propune să dea câteva exemple de inele euclidiene şi să elaboreze algoritmi recursivi de determinare a celui mai mare divizor comun a doua elemente aparţinând unor inele euclidiene diferite de inelul numerelor întregi unde acest algoritm este bine cunoscut.

Al. În Z[i] fie funcţia ce asociază fiecărui număr complex pătratul modulului său:

$$N: Z[i] \to \mathbb{N} \; ; \quad N(z) = N(m+ni) = m^2+n^2 \; .$$

Această funcţie are două proprietăţi speciale:

a) este multiplicativă $N(z_1 \cdot z_2)=N(z_1)\cdot N(z_2)$, pentru $\forall z_1, z_2 \in Z[i]$,

b) $N(z)=0$ dacă şi numai dacă $z=0$.

Inelul $Z[i]$ este conţinut ca subinel în $Q[i]=\{z\in\mathbb{C} \mid z=m+ni,\ m,n\in Q\}$ şi orice element $z=m+ni\in Z[i]$, $z\neq 0$, are un invers în $Q[i]$:

$$z^{-1} = \frac{m}{m^2+n^2} + \frac{-n}{m^2+n^2}\cdot i \ .$$

În plus funcţia N se extinde la o funcţie multiplicativă $N:Q[i]\to Q$. Fie acum $z_1=m_1+n_1 i$, $z_2=m_2+n_2 i$ elemente nenule din $Z[i]$. Atunci, în inelul $Q[i]$ are loc $z_1\cdot z_2^{-1}=\sigma+\tau i$, cu $\sigma,\tau\in Q$. Fie s şi t întregii cei mai apropiaţi de σ, respectiv τ, adică $|\sigma-s|\le\frac{1}{2}$, $|\tau-t|\le\frac{1}{2}$.

Fie $q=s+ti\in Z[i]$; atunci elementul $z_1 z_2^{-1}-q=(\sigma-s)+(\tau-t)i \in Q[i]$ are norma $N(z_1 z_2^{-1}-q)=(\tau-s)^2+(\tau-t)^2\le\frac{1}{4}+\frac{1}{4}<1$. Fie acum $r=z_1-z_2 q \in Z[i]$. Avem $N(r)=N(z_2(z_1 z_2^{-1}-q)) = N(z_2)\cdot N(z_1 z_2^{-1}-q)<N(z_2)$. Prin urmare, în $Z[i]$ are loc relaţia $z_1=z_2 q+r$, unde $N(r)<N(z_2)$. Deci cu ajutorul funcţiei N se poate efectua, în inelul $Z[i]$, o autentică împărţire cu rest.

Aplicaţie. Să se găsească în $Z[i]$ cmmdc al numerelor $z_1=4+5i$, $z_2=3+2i$. Vom căuta elementele $q_1, r_1 \in Z[i]$ care satisfac relaţia

$$z_1 = z_2 q_1 + r_1 \ , \quad N(r_1)<N(z_2) \ .$$

$$z_1\cdot z_2^{-1} = \frac{z_1}{z_2} = \frac{4+5i}{3+2i} = \frac{(4+5i(3-2i)}{13} = \frac{22}{13}+\frac{7}{13}\cdot i \ .$$

Întregii cei mai apropiaţi de $\frac{22}{13}$ şi $\frac{7}{3}$ sunt, respectiv, 2 şi 1.

Deci $q_1=2+i$, de unde $r_1 = z_1-z_2 q_1 = 4+5i-(3+2i)(2+i) = -2i$.

$N(r_1) = 4<N(z_2) = 13$.

Căutăm acum elementele $q_2, r_2 \in Z[i]$ care satisfac relaţia:

$z_2 = r_1q_2+r_2$, $N(r_2)<N(r_1)$

$z_2 \cdot r_1^{-1} = \frac{z_2}{r_1} = \frac{3+2i}{-2i} = -1+\frac{3}{2}i$. Deci q_2=-1+i (sau -1+2i),

de unde $r_2 = z_2-r_1q_2 = 3+2i-(-2i)\cdot(-1+i) = 1$; $N(r_2) = 1<N(r_1) = 4$.

În sfârșit $r_1 = r_2q_3+r_3 \Leftrightarrow -2i = 1(-2i)+0$.

Ultimul rest diferit de zero obținut prin algoritmul lui Euclid este r_2=1, care este cmmdc al numerelor 4+5i și 3+2i.

2. Vom încerca să determinăm și alte inele în care funcționează algoritmul lui Euclid pentru găsirea cmmdc a două elemente.

Fie a,b$\in$Z și fie θ o rădăcină a ecuației (1) $x^2+ax+b=0$.

Notăm $Z[\theta]=\{m+n\theta \mid m,n\in Z\}$.

În $Z[\theta]$ spunem că z_1 este un divizor al lui z_2, $z_1 \mid z_2$, dacă $\exists z\in Z[\theta]$ a.î. $z_2=z_1\cdot z$. Spunem că d este un cmmdc al elementelor z_1, z_2 dacă:

1) $d \mid z_1$, $d \mid z_2$

2) $d' \mid z_1$, $d' \mid z_2 \rightarrow d' \mid d$.

$Z[\theta]$ are următoarele proprietăți:

a) $Z[\theta]$ este subinel al lui $\mathbf{C}$ și $Z\subseteq Z[\theta]$.

Într-adevăr dacă m$\in$Z atunci putem scrie $m=m+0\cdot\theta$ și deci $m\in Z[\theta]$.

Dacă $z_1, z_2\in Z[\theta]$, $z_1=m_1+n_1\theta$, $z_2=m_2+n_2\theta$, $m_1, m_2, n_1, n_2\in Z$,

atunci $z_1+z_2=m_1+m_2+(n_1+n_2)\theta \in Z[\theta]$ și $z_1\cdot z_2 = m_1m_2+(m_1n_2+m_2n_1)\theta+n_1n_2\theta^2 \overset{(1)}{=}$

$\overset{(1)}{=} m_1m_2+(m_1n_2+m_2m)\theta+n_1n_2(-a\theta-b) = m_1m_3-n_1n_2b+(m_1n_2+m_2n_1-an_1n_2)\theta \in Z[\theta]$.

Deci $Z[\theta]$ este subinel al lui $\mathbf{C}$.

b) Dacă θ' este cealaltă rădăcină a ecuației (1), avem $Z[\theta]=Z[\theta']$.

Într-adevăr, cum $\theta+\theta'=-a \rightarrow \theta'=-a-\theta \in Z[\theta]$, deci $Z[\theta']\subseteq Z[\theta]$.

Analog obținem și incluziunea inversă $Z[\theta]\subseteq Z[\theta']$, deci $Z[\theta]=Z[\theta']$.

c) Notăm $d=a^2-4b$; deci $\theta = \frac{-a\pm\sqrt{d}}{2}$. Dacă $d\geq 0$ și d este un pătrat perfect atunci $\theta\in Z$ și deci $Z[\theta]=Z$. Prin urmare prezintă interes cazurile $d<0$ sau $d>0$ și d nu este pătrat perfect. Vom studia în

continuare aceste cazuri, utilizând drept funcţie normă aplicaţia $N: Z[\theta] \to \mathbb{N}$, $N(m+n\theta) = |(m+n\theta)(m+n\theta')| = |m^2+mn(\theta+\theta')+n^2\theta\theta'| =$

$= |m^2-amn+bn^2|$. Se verifică uşor că această aplicaţie este multiplicativă şi N(z)=0 dacă şi numai dacă z=0.

Să remarcăm că aplicaţia φ: $Z[\Theta] \to Z[\omega]$, $\varphi(m+n\Theta)=m^*+n^*\omega$ unde $m^*=m+cn$, $n^*=n$, $\omega=\theta-c$, cu $c\in Z$, este un izomorfism de inele. Prin acest izomorfism ecuaţia (1) se transformă în

(2) $(x^*+c)^2+a(x^*+c)+b = 0$, adică

(3) $x^2+x(a+2c)+c^2+ac+b = 0$, ecuaţie care are acelaşi discriminant d ca şi ecuaţia (1).

Dacă I) $a\equiv 0 \pmod 2$, punând $c=-\frac{a}{2}\in Z$ ecuaţia devine

$x^2-\frac{a^2}{4}+b=0$,adică $x^2-D=0$, unde $D=b-\frac{a^2}{4}=\frac{d}{4}\in Z$ întrucât $d\equiv 0 \pmod 4$.

II) $a\equiv 1 \pmod 2$, punând $c=-\frac{1+a}{2}\in Z$, ecuaţia devine

$x^2-x-\frac{d-1}{4}=0$. Cum în acest caz $d\equiv 1 \pmod 4$, putem nota $D=\frac{d-1}{4}\in Z$

şi ecuaţia se scrie: $x^2-x-D=0$.

Este deci suficient să studiem inelele $Z[\omega]$ astfel obţinute.

Normele în aceste inele vor fi $N(m+n\omega)=|m^2-Dn^2|$ şi respectiv

$N(m+n\omega) = |m^2+mn-Dn^2|$.

În care dintre aceste inele funcţionează teorema împărţirii cu rest (folosind normele mai sus indicate)?

În cazul I) există două posibilităţi: $D<0$ sau $D>0$.

a) $D<0$, $N(m+n\omega) = m^2-Dn^2$

Fie $z_1, z_2\in Z[\omega]$; $\frac{z_1}{z_2} = \frac{m_1+n_1\omega}{m_2+n_2\omega} = \frac{(m_1+n_1\omega)(m_2-n_2\omega)}{m_2^2-n_2^2} = \frac{m_1m_2-n_1n_2D}{m_2^2-Dn_2^2} +$

$+ \frac{m_2n_1-m_1n_2}{m_2^2-Dn_2^2}\cdot\omega = \sigma+\tau\cdot\omega$, unde $\sigma,\tau\in Q$.

Cum $\sigma,\tau\in\mathbb{Q}$ rezultă că $\exists s,t\in\mathbb{Z}$ a.î. $|\sigma-s|\leq\frac{1}{2}$, $|\tau-t|\leq\frac{1}{2}$.

Notăm $q=s+t\omega$. Atunci din $z_1=z_2q+r \Rightarrow r\in\mathbb{Z}[\omega]$, iar

$$\frac{N(r)}{N(z_2)} = N(\frac{r}{z_2}) = N(\frac{z_1}{z_2}-q) = (\sigma-s)^2-D(\tau-t)^2 \leq \frac{1}{4}-D\cdot\frac{1}{4} = \frac{1}{4}(1-D) ,$$

semnul egal intervenind doar dacă $\sigma-s=\frac{1}{2}$, $\tau-t=\frac{1}{2}$ simultan.

Căutăm valorile lui D încât $N(r)<N(z_2)$, adică $\frac{1}{4}(1-D)<1$.

Obţinem astfel D=-1, D=-2, care furnizează următoarele inele euclidiene: $\mathbb{Z}[\sqrt{-1}]=\mathbb{Z}[i]$ şi $\mathbb{Z}[\sqrt{-2}]=\mathbb{Z}[i\sqrt{2}]=\{m+ni\sqrt{2} \mid m,n\in\mathbb{Z}\}$.

b) $D>0$, $N(m+n\omega) = |m^2-Dn^2|$

Cu aceleaşi notaţii ca şi la punctul a), avem:

$$N(\frac{r}{z_2}) = \frac{N(r)}{N(z_2)} = N(\frac{z_1}{z_2}-q) = |(\sigma-s)^2-D(\tau-t)^2| \leq (\sigma-s)^2+D(\tau-t)^2 ,$$

semnul egal intervenind doar dacă $\tau-t=0$.

În continuare $\frac{N(r)}{N(z_2)} \leq (\sigma-s)^2+D(\tau-t)^2 \leq \frac{1}{4}+D\cdot\frac{1}{4} = \frac{D+1}{4}$, semnul egal intervenind în ultima inegalitate doar dacă $\sigma-s=\frac{1}{2}$, $\tau-t=\frac{1}{2}$.

Prin urmare, cel puţin una din inegalităţi este strictă, deci pentru ca $N(r)<N(z_2)$ este suficient ca $\frac{D+1}{4}\leq 1$, de unde obţinem D=1,2,3. Cum D nu trebuie să fie pătrat perfect, rămân D=2, D=3 care furnizează următoarele inele euclidiene: $\mathbb{Z}[\sqrt{2}]=\{m+n\sqrt{2}\,|\,m,n\in\mathbb{Z}\}$,

$\mathbb{Z}[\sqrt{3}] = \{m+n\sqrt{3}\,|\,m,n\in\mathbb{Z}\}$.

În cazul II) în care $N(m+n\omega) = |m^2+mn-\frac{d-1}{4}n^2|$, cu $d\equiv 1 \pmod 4$ există de asemeni două posibilităţi: $d<0$ sau $d>0$.

a) $d<0$, $N(m+n\omega) = m^2+mn-\frac{d-1}{4}n^2$

Folosind notaţii analoage celor de la punctul precedent, pentru

$z_1, z_2 \in Z[\omega]$ avem $\frac{z_1}{z_2} = \sigma+\tau\omega$, unde $\sigma,\tau\in Q$. Există deci $t\in Z$ a.î.

$|\tau-t|\le\frac{1}{2}$. Pentru t astfel determinat există $s\in Z$ a.î.

$|\sigma-s+\frac{1}{2}(\tau-t)|\le\frac{1}{2}$. Notând $q=s+t\omega$, putem scrie $z_1=z_2q+r$, de unde rezultă că $r\in Z[\omega]$. Să cercetăm în ce situaţie $N(r)<N(z_2)$.

$$\frac{N(r)}{N(z_2)} = N(\frac{r}{z_2}) = N(\frac{z_1}{z_2}-q) = (\sigma-s)^2+(\sigma-s)(\tau-t)-\frac{d-1}{4}(\tau-t)^2 =$$

$$= \left[(\sigma-s)+\frac{1}{2}(\tau-t)\right]^2-\frac{d}{4}(\tau-t)^2 \le \frac{1}{4}-\frac{d}{16} .$$

Prin urmare $N(r)<N(z_2)$ dacă $\frac{1}{4}-\frac{d}{16}<1$, adică $d>-12$.

Cum $d<0$ şi $d\equiv 1 \pmod 4$ rezultă $d=-3$, $d=-7$, $d=-11$, valori care furnizează următoarele inele euclidiene

$$Z\left[\frac{1+i\sqrt{3}}{2}\right] = \{ m+n\frac{1+i\sqrt{3}}{2} \mid m,n\in Z \} , \quad Z\left[\frac{1+i\sqrt{7}}{2}\right] = \{ m+n\frac{1+i\sqrt{7}}{2} \mid m,n\in Z \} ,$$

$$Z\left[\frac{1+i\sqrt{11}}{2}\right] = \{ m+n\frac{1+i\sqrt{11}}{2} \mid m,n\in Z \} .$$

b) $d>0$, $N(m+n\omega) = |m^2+mn-\frac{d-1}{4}n^2|$

Cu notaţii şi condiţii analoage celor de la punctul precedent obţinem,

$$\frac{N(r)}{N(z_2)} = N(\frac{r}{z_2}) = N(\frac{z_1}{z_2}-q) = |[(\sigma-s)+\frac{1}{2}(\tau-t)]^2-\frac{d}{4}(\tau-t)^2| \le$$

$\le [(\sigma-s)+\frac{1}{2}(\tau-t)]^2+\frac{d}{4}(\tau-t)^2$, egalitatea survenind doar pentru

$\tau-t=0$ şi în continuare $\frac{N(r)}{N(z_2)} \le \frac{1}{4}+\frac{d}{16}$, egalitatea survenind doar

dacă $\tau-t=\frac{1}{2}$ şi $(\sigma-s)=\frac{1}{4}$.

Prin urmare cel puţin una din cele două inegalităţi este strictă, deci condiţia ca $N(r)<N(z_2)$ este echivalentă cu $\frac{1}{4}+\frac{d}{16}\le 1$, adică

$d \le 12$.
Cum $d>0$, d nu este pătrat perfect şi $d \equiv 1 \pmod 4$ rezultă $d=5$, valoare care furnizează inelul euclidian $Z\left[\frac{1+\sqrt{5}}{2}\right] = \{ m+n\frac{1+\sqrt{5}}{2} \mid m,n \in Z \}$.

3. **Aplicaţii.** Să se găsească, folosind algoritmul lui Euclid, cmmdc al numerelor $3+4i\sqrt{2}$ şi $-2+5i\sqrt{2}$ în $Z[i\sqrt{2}]$; $1+6\frac{1+\sqrt{5}}{2}$ şi $3-7\frac{1+\sqrt{5}}{2}$ în $Z\left[\frac{1+\sqrt{5}}{2}\right]$.

a) În $Z[i\sqrt{2}]$ norma unui element $z=m+ni\sqrt{2}$ este definită ca $N(z)=m^2+2n^2$, , deci $N(3+4i\sqrt{2})=9+2\cdot 16=41$, iar $N(-2+5i\sqrt{2})=$ $=4+2\cdot 25=54$.

$$\frac{-2+5i\sqrt{2}}{3+4i\sqrt{2}} = \frac{(-2+5i\sqrt{2})(3-4i\sqrt{2})}{41} = \frac{34}{41}+\frac{23}{41}i\sqrt{2} .$$

Întregii cei mai apropiaţi de $\frac{34}{41}$ şi $\frac{23}{41}$ sunt 1 şi respectiv 1.

Deci $q_1=1+i\sqrt{2}$.

Avem $z_1=z_2q_1+r_1$, unde $z_1=-2+5i\sqrt{2}$, $z_2=3+4i\sqrt{2}$, $q_1=1+i\sqrt{2}$.

Deci $r_1=z_1-z_2q_1=-2+5i\sqrt{2}-(3+4i\sqrt{2})(1+i\sqrt{2})=3-2i\sqrt{2}$, $N(r_1)=17 <$ $< N(z_2)=41$.

Căutăm acum elementele $q_2, r_2 \in Z[i\sqrt{2}]$ care satisfac relaţia

$$z_2 = r_1q_2+r_2 , \quad N(r_2) < N(r_1)$$

$$z_2 \cdot r_1^{-1} = \frac{z_2}{r_1} = \frac{3+4i\sqrt{2}}{3-2i\sqrt{2}} = \frac{(3+4i\sqrt{2})(3+2i\sqrt{2})}{17} = \frac{-7}{17}+\frac{18}{17}i\sqrt{2} .$$

Deci $q_2=i\sqrt{2}$, de unde $r_2=z_2-r_1q_2=3+4i\sqrt{2}-(3-2i\sqrt{2})\,i\sqrt{2}=-1+i\sqrt{2}$,

$N(r_2)=3<N(r_1)=17$.

În continuare căutăm elementele $q_3, r_3\in Z[i\sqrt{2}]$ care satisfac relaţia:

$$r_1 = r_2q_3+r_3 \ , \quad N(r_3)< N(r_2)$$

$$r_1r_2^{-1} = \frac{r_1}{r_2} = \frac{3-2i\sqrt{2}}{-1+i\sqrt{2}} = \frac{(3-2i\sqrt{2})\,(-1-i\sqrt{2})}{3} = -\frac{7}{3}-\frac{1}{3}i\sqrt{2} \ .$$

Deci $q_3=-2$ iar $r_3=r_1-r_2q_3=3-2i\sqrt{3}-(-1+i\sqrt{2})\,(-2)=1$, $N(r_3)=1< N(r_2)=3$.

În sfârşit $r_2=r_3q_4+r_4 \Leftrightarrow -1+i\sqrt{2}=1\,(-1+i\sqrt{2})+0$.
Ultimul rest diferit de zero prin algoritmul lui Euclid este $r_3=1$, care este cmmdc al numerelor $3+4i\sqrt{2}$ şi $-2+5i\sqrt{2}$.

b) În $Z\left[\frac{1+\sqrt{5}}{2}\right]$ norma unui element $z=m+n\frac{1+\sqrt{5}}{2}$ este dată de

$N(z) = |m^2+mn-n^2|$. Deci $N(3-7\frac{1+\sqrt{5}}{2}) = |9-21-49|= 61$, iar

$N(1+6\frac{1+\sqrt{5}}{2})=|1+6-36|=29$.

Vom căuta elementele $q_1, r_1\in Z\left[\frac{1+\sqrt{5}}{2}\right]$ care satisfac relaţia

$$z_1 = z_2q_1+r_1 \ , \quad N(r_1)< N(z_2) \ ,$$

unde $z_1=3-7\frac{1+\sqrt{5}}{2}$ şi $z_2=1+6\frac{1+\sqrt{5}}{2}$.

$$z_1 \cdot z_2^{-1} = \frac{3-7\cdot\frac{1+\sqrt{5}}{2}}{1+6\cdot\frac{1+\sqrt{5}}{2}} = \frac{(3-7\cdot\frac{1+\sqrt{5}}{2})(1+6\cdot\frac{1-\sqrt{5}}{2})}{-29} = -\frac{63}{29}+\frac{25}{29}\cdot\frac{1+\sqrt{5}}{2}$$

Cel mai apropiat întreg de $\frac{25}{29}$ este 1, iar numărul întreg s care satisface relaţia $|-\frac{63}{29}-s+\frac{1}{2}(\frac{25}{29}-1)|\leq\frac{1}{2}$ este s=-2. Deci $q_1=-2+\frac{1+\sqrt{5}}{2}$, de unde

$$r_1=z_1-z_2q_1=3-7\cdot\frac{1+\sqrt{5}}{2}-(1+6\frac{1+\sqrt{5}}{2})(-2+\frac{1+\sqrt{5}}{2}) = -1-2\cdot\frac{1+\sqrt{5}}{2};$$

$N(r_1)=|1+2-4|=1$.

Căutăm acum elementele $q_2, r_2 \in Z\left[\frac{1+\sqrt{5}}{2}\right]$ care satisfac relaţia:

$$z_2 = r_1q_2+r_2 , \quad N(r_2) < N(r_1)$$

$$z_2 \cdot r_1^{-1} = \frac{z_2}{r_1} = \frac{1+6\cdot\frac{1+\sqrt{5}}{2}}{-1-2\cdot\frac{1+\sqrt{5}}{2}} = \frac{(1+6\cdot\frac{1+\sqrt{5}}{2})(-1-2\cdot\frac{1-\sqrt{5})}{2}}{-1} = -9+4\cdot\frac{1+\sqrt{5}}{2} = q_2$$

iar $r_2=0$.

Ultimul rest diferit de zero obţinut prin algoritmul lui Euclid este $r_1=-1-2\cdot\frac{1+\sqrt{5}}{2}$, care este cmmdc al elementelor z_1 şi z_2 în $Z\left[\frac{1+\sqrt{5}}{2}\right]$.

Observaţie Toate inelele care s-au dovedit a fi euclidiene (adică cmmdc a două elemente poate fi determinat cu ajutorul lui Euclid) sunt inele integre (comutative, cu unitate şi fără divizori ai lui zero).

Evident există inele integre în care nu numai că nu

funcţionează algoritmul lui Euclid, dar, pentru unele elemente, nici nu există un cmmmdc.

Aplicaţie Să se arate că în inelul $Z[i\sqrt{5}]$ elementele $2(1+i\sqrt{5})$ şi 6 nu au un cmmdc.

Fie $N:Z[i\sqrt{5}] \to N$, $N(z)=N(m+ni\sqrt{5})=m^2+5n^2$, aplicaţia care asociază fiecărui număr complex din $Z[i\sqrt{5}]$ pătratul modulului său. Evident ea este multiplicativă şi N(z)=0 dacă şi numai dacă z=0. Să remarcăm că dacă $z_1 | z_2$ atunci $\exists z \in Z[i\sqrt{5}]$ a.î. $z_2=z_1 \cdot z$, deci $N(z_2)=N(z_1)\cdot N(z)$, adică $N(z_1) | N(z_2)$.

Să presupunem că elementele $2(1+i\sqrt{5})$ şi 6 au, în $Z[i\sqrt{5}]$ un cmmdc notat cu d. Atunci, conform celor de mai sus, $N(d) | N(2+2i\sqrt{5})$ şi $N(d) | N(6)$, adică N(d) este un divizor comun al numerelor 24 şi 36.

Pe de altă parte să observăm că $2 | 2(1+i\sqrt{5})$ şi $2 | 6$, adică 2 este un divizor comun al elementelor considerate; aceasta implică $2 | d$ şi de aici $N(2) | N(d)$, adică $4 | N(d)$. De asemeni $1+i\sqrt{5} | 2(1+i\sqrt{5})$ şi $1+i\sqrt{5} | 6=(1+i\sqrt{5})(1-i\sqrt{5})$, adică şi $1+i\sqrt{5}$ este un divizor comun al elementelor considerate; aceasta implică $1+i\sqrt{5} | d$ şi de aici $N(1+i\sqrt{5}) | N(d)$, adică $6 | N(d)$.

Deci $N(d) | 24$, $N(d) | 36$, $4 | N(d)$, $6 | N(d)$. Toate acestea implică $N(d)=12$.

Cum $d \in Z[i\sqrt{5}]$, $d=m+ni\sqrt{5}$, $m,n \in Z$, relaţia $N(d)=12$ este echivalentă cu $m^2+5n^2=12$, ecuaţie care nu are soluţii în mulţimea numerelor întregi.

Deci elementele $2(1+i\sqrt{5})$ şi 6 nu au, în inelul $Z[i\sqrt{5}]$, un cmmdc.

B1. Determinarea celui mai mare divizor comun a două elemente în inelul întregilor lui Gauss.

```
program eucl_rec;
  { programul calculează recursiv cel mai mare divizor
    comun a două elemente nenule ale inelului lui Gauss }
  uses crt;
  type igauss=record
                  re:integer;
                  im:integer;
               end;
  var a,b,d:igauss;
  function n(a:igauss):integer;
  begin
     n:=a.im*a.im+a.re*a.re
  end;

  procedure euclid(a,b:igauss;var d:igauss);
     var c,r:igauss;
  begin
     if n(b)=0 then d:=a
               else
            begin
                  c.re:=round((a.re*b.re+a.im*b.im)    /
(b.re*b.re+b.im*b.im));
                  c.im:=round((a.im*b.re-a.re*b.im)    /
(b.re*b.re+b.im*b.im));
               r.re:=a.re-b.re*c.re+b.im*c.im;
               r.im:=a.im-b.im*c.re-b.re*c.im;
               {writeln(r.re,'+',r.im,'i');}  {pentru  urmarirea
resturilor obtinute succesiv}
               if n(r)<n(b) then euclid(b,r,d);
            end;
  end;{euclid}
begin
```

```
  clrscr;
  write('dați partea reală a numarului a ');readln(a.re);
  write('dați partea imaginară a numarului a ');readln(a.im);
  write('dați partea reală a numarului b ');readln(b.re);
  write('dați partea imaginară a numarului b ');readln(b.im);
  euclid(a,b,d);
  write('c.m.M.d.c=',d.re,' + ',d.im,'*i');
  repeat until keypressed;
end.
```

2. Determinarea celui mai mare divizor comun a două elemente în inelul $Z[t]=\{m+nt;\ m,n\in Z\}$ unde t este o rădăcină a ecuației $x^2+cx+d=0$, $c,d\in Z$.

Menționăm că inelul Z[t] împreună cu funcția $f: Z[t]\to\mathbf{N}$; $f(m+nt)=|(m+nt_1)(m+nt_2)|$, t_1 și t_2 fiind rădăcinile ecuației de mai sus, adică $f(m+nt)=|m^2-cmn+dn^2|$ este euclidian numai pentru anumiți întregi c și d. O condiție suficientă dar nu și necesară pentru aceasta este $|c|+|d|<3$ (vezi [4]). Ea conduce la inelele

$$Z;\ Z[i];\ Z[\sqrt{2}];\ Z[i\sqrt{2}];\ Z[(1+i\sqrt{3})/2];\ Z[(1+\sqrt{5})/2]\ .$$

```
program eucl_rec;
  { programul calculează recursiv cel mai mare divizor
    comun a două elemente nenule ale inelului Z[t],(iZt)
    unde t este o rădăcină a ecuației x*x + c*x + d = 0,
    unde c,d sunt intregi dați }
  uses crt;
  type iZt=record
                  fara_t:integer;
                  coef_t:integer;
             end;
  var a,b,cmmdc:iZt;
      c,d:integer;
  function n(a:iZt):integer;
  begin
```

```
      n:=a.fara_t*a.fara_t    -    c*a.fara_t*a.coef_t    +
d*a.coef_t*a.coef_t
   end;
   function f(a:iZt):integer;
   begin
      f:=abs(n(a))
   end;
   procedure euclid(a,b:iZt;var cmmdc:iZt);
      var q,r:iZt;
   begin
      if f(b)=0 then cmmdc:=a
                else
             begin
q.fara_t:=round((a.fara_t*b.fara_t-b.coef_t*a.fara_t*c+a.coef_t*b
.coef_t*d) / n(b));
       q.coef_t:=round((a.coef_t*b.fara_t-a.fara_t*b.coef_t)    /
n(b));
        r.fara_t:=a.fara_t    -    b.fara_t*q.fara_t    +
d*b.coef_t*q.coef_t;
r.coef_t:=a.coef_t+c*q.coef_t*b.coef_t-b.coef_t*q.fara_t-b.fara_t
*q.coef_t;
       writeln(r.fara_t,'+',r.coef_t,'i');    {pentru    urmărirea
resturilor obţinute succesiv}
       if f(r)<f(b) then euclid(b,r,cmmdc)
                    else writeln('INAPLICABIL');
             end;
  end;{euclid}
begin
  clrscr;
  writeln('daţi  coeficienţii  întregi  c  si  d  ai  ecuaţiei  :
x*x+c*x+d=0');
  readln(c,d);
  write('dati partea fără t a numărului a ');readln(a.fara_t);
  write('daţi coeficientul lui t a numărului a ');readln(a.coef_t);
  write('daţi partea fără t a numărului b ');readln(b.fara_t);
```

```
  write('daţi coeficientul lui t a numarului b ');readln(b.coef_t);
  euclid(a,b,cmmdc);
  write('c.m.M.d.c=',cmmdc.fara_t,' + ',cmmdc.coef_t,'*t');
  repeat until keypressed;
end.
```

B I B L I O G R A F I E

1.BARBILIAN,D.: Algebră axiomatică, vol.I, Editura Didactică şi Pedagogică, Bucureşti, 1988

2.ION,D.I., RADU,N.: Algebra, Ed. Didactică şi Pedagogică, Bucureşti, 1981

3.ION,D.I., RADU,N., NIŢĂ,C., POPESCU,D.: Probleme de algebră, Editura Didactică şi Pedagogică, Bucureşti, 1981

4.NĂSTĂSESCU,C., NIŢĂ,C., VRACIU,C.: Bazele algebrei, vol.I, Editura Academiei RSR, Bucureşti, 1986.

THE GREATEST COMMON DIVISOR OF TWO ELEMENTS IN SOME INTEGRAL DOMAINS

ABSTRACT. In this paper some computations of the greatest common divisor, in some usual integral domains, by the Euclidean algorithm are given. Two Pascal programmes for these situations are given.

UNIVERSITATEA DIN BAIA MARE
Facultatea de Litere şi Ştiinţe
str.Victoriei 76, 4800 BAIA MARE
ROMÂNIA

LICEUL "VASILE LUCACIU"
Catedra de Informatică
str.Culturii, 4800 BAIA MARE
ROMÂNIA