CURS 9

Domenii euclidiene

Definiţia 1. Spunem că un domeniu de integritate R este **domeniu euclidian** dacă există o funcţie $\delta : R^* \to \mathbb{N}$ care verifică condiţia: pentru orice $a, b \in R$ cu $b \neq 0$, există $q, r \in R$ astfel încât

$$a = bq + r, \text{ unde } r = 0 \text{ sau } \delta(r) < \delta(b). \tag{$*$}$$

Exemplul 2. Din teorema împărţirii cu rest în $\mathbb{Z}$ rezultă că domeniul $\mathbb{Z}$ împreună cu funcţia modul $\delta : \mathbb{Z} \to \mathbb{N}$, $\delta(n) = |n|$ este un domeniu euclidian.

Observaţia 3. În definiţia domeniului euclidian, existenţa elementelor $q, r \in R$ care verifică $(*)$ nu implică, în general, unicitatea lor. De exemplu, pentru $\mathbb{Z}$ şi funcţia modul, avem

$$-4 = 3(-1) + (-1), \text{ cu } 1 = |-1| < |3| = 3,$$
$$-4 = 3(-2) + 2, \text{ cu } 2 = |2| < |3| = 3.$$

Evident, doar a doua egalitate dă câtul şi restul împărţirii lui -4 la 3 în $\mathbb{Z}$.

Teorema 4. Dacă R (împreună cu δ) este un domeniu euclidian, atunci R este un domeniu cu ideale principale.

Demonstraţie. Fie I un ideal al lui R. Dacă $I = \{0\}$, atunci $I = (0)$, adică I este principal. Dacă $I \neq \{0\}$, atunci mulţimea $\{\delta(x) \mid x \in I \setminus \{0\}\} \subseteq \mathbb{N}$ este nevidă, prin urmare are un minim. Fie $a \neq 0$ unul din elementele lui I pentru care se obţine acest minim. Evident, avem

$$\delta(a) \leq \delta(x), \ \forall x \in I^*. \tag{1}$$

Pentru orice $x \in I \subseteq R$ există $q, r \in R$ astfel încât

$$x = aq + r, \text{ cu } r = 0 \text{ sau } \delta(r) < \delta(a). \tag{2}$$

De aici şi din $a, x \in I$, cum I este ideal, rezultă $r = x - aq \in I$, ceea ce (conform lui (1) şi (2)) implică $r = 0$. Acum din (2) deducem $x = aq \in aR = (a)$. Deci $I \subseteq (a)$, iar cum $a \in I$ implică $(a) \subseteq I$, am arătat că $I = (a)$, adică I este idealul principal generat de a. □

Corolarul 5. Dacă R (împreună cu δ) este un domeniu euclidian, atunci R este un domeniu factorial.

Observaţia 6. Similar cu exemplul 3 d) din cursul 4, se poate arăta că operaţiile uzuale de adunare şi înmulţire îi conferă lui $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{a + b \cdot \frac{1+i\sqrt{19}}{2} \,\middle|\, a, b \in \mathbb{Z}\right\}$ o structură de domeniu de integritate. În secţiunea ,,Apendice" este prezentată o demonstraţie accesibilă a faptului că $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ este un exemplu de domeniu cu ideale principale care nu este euclidian.

Din corolarul 5 rezultă că dacă (R, δ) este un domeniu euclidian, atunci pentru orice $a, b \in R$ există c.m.m.d.c. La fel ca în cazul numerelor întregi, şi aici putem folosi **algoritmul lui Euclid**

pentru a determina c.m.m.d.c. a două elemente. Dacă unul dintre elementele $a, b \in R$ este nul, atunci celălalt este c.m.m.d.c. al lor. Dacă $a \neq 0$ şi $b \neq 0$, atunci există $q_1, r_1 \in R$ astfel încât $a = bq_1 + r_1$, unde $r_1 = 0$ sau $\delta(r_1) < \delta(b)$. Dacă $r_1 \neq 0$, atunci există $q_2, r_2 \in R$ astfel încât $b = r_1q_2 + r_2$ unde $r_2 = 0$ sau $\delta(r_1) > \delta(r_2)$. Dacă $r_2 \neq 0$, continuând acest procedeu se obţine şirul descrescător de numere naturale $\delta(r_1) > \delta(r_2) > \cdots$. Cum acest şir este finit, după un număr finit de paşi, să zicem $n+1$, se obţine $r_{n+1} = 0$, adică avem un şir de relaţii de forma:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n-1} \end{aligned} \tag{3}$$

unde $r_i \neq 0$, $i = 1, \ldots, n$.

Teorema 7. Dacă (R, δ) este un domeniu euclidian şi $a, b \in R^*$, atunci elementul r_n din relaţiile (3) este c.m.m.d.c. al elementelor a şi b.

Demonstraţie. Din ultima relaţie din (3) rezultă că r_n divide pe r_{n-1}, apoi din penultima relaţie urmează că r_n divide pe r_{n-2}. Continuând raţionamentul rezultă că r_n divide pe a şi b. Dacă c este un alt divizor comun al lui a şi b, atunci din prima relaţie din (3) urmează că c divide pe r_1, apoi din a doua relaţie rezultă că c divide pe r_2. Continând raţionamentul urmează că c divide pe r_n. Deci r_n este c.m.m.d.c. al lui a şi b. □

Observaţia 8. Dacă R este un domeniu euclidian şi d este cm.m.d.c. al lui a şi b, atunci cu algoritmul lui Euclid se pot determina elementele $u, v \in R$ pentru care are loc relaţia din corolarul 21 din cursul 5, adică $d = au + bv$.

Pentru aceasta se procedează ca la numere întregi, când am căutat o reprezentare Bézout a c.m.m.d.c. folosind algoritmul lui Euclid: scoatem pe r_1 din prima relaţie din (3) şi îl înlocuim în a doua relaţie din (3), apoi scoatem pe r_2 din relaţia obţinută şi îl înlocuim în a treia relaţie ş.a.m.d. Continuăm procedeul până la penultima relaţie din (3) de unde îl exprimăm pe $r_n = d$ şi astfel obţinem pe u şi v.

Exerciţiul 1. Să se arate că domeniul $\mathbb{Z}[i]$ al întregilor lui Gauss este euclidian şi să se determine:

a) c.m.m.d.c. şi c.m.m.m.c. al numerelor $z_1 = 12 - 3i$ şi $z_2 = 3 + 6i$ în $\mathbb{Z}[i]$;

b) câte un generator pentru fiecare dintre idealele $(z_1) \cap (z_2)$ şi (z_1, z_2).

Soluţie: Să remarcăm pentru început că funcţia $\delta : \mathbb{Z}[i] \to \mathbb{N}$, $\delta(z) = |z\overline{z}|$ este o restricţie a funcţiei $\delta_0 : \mathbb{Q}(i) \to \mathbb{Q}$, $\delta_0(z) = |z\overline{z}|$ care are, de asemenea, proprietatea

$$\delta_0(z_1z_2) = \delta_0(z_1)\delta_0(z_2), \ \forall z_1, z_2 \in \mathbb{Q}(i).$$

Fie $z_1 = a_1 + b_1i$, $z_2 = a_2 + b_2i \neq 0$, cu $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Arătăm că există numerele $q, r \in \mathbb{Z}[i]$ astfel încât $z_1 = z_2q + r$, unde $\delta(r) < \delta(z_2)$ (să observăm că această condiţie cuprinde şi posibilitatea ca $r = 0$). Avem $z = \dfrac{z_1}{z_2} \in \mathbb{Q}(i)$, adică $z = a + bi$ cu $a, b \in \mathbb{Q}$. Considerăm numerele întregi m, n cele mai apropiate de a, respectiv b, adică $m, n \in \mathbb{Z}$ astfel încât

$$|a - m| \leq \frac{1}{2} \text{ şi } |b - n| \leq \frac{1}{2}.$$

Luând $q = m + ni \in \mathbb{Z}[i]$ şi $z_3 = z - q = (a-m) + (b-n)i \in \mathbb{Q}(i)$ avem

$$z_1 = z_2 z = z_2 q + z_2(z-q) = z_2 q + z_2 z_3,$$

prin urmare $z_2 z_3 = z_1 - z_2 q \in \mathbb{Z}[i]$. Notăm $r = z_2 z_3$ şi avem:

$$\begin{aligned}\delta(r) = \delta(z_2 z_3) = \delta_0(z_2 z_3) = \delta_0(z_2)\delta_0(z_3) = \delta(z_2)\delta_0(z_3) = \delta(z_2)\left[(a-m)^2 + (b-n)^2\right] \\ \leq \delta(z_2)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{\delta(z_2)}{2} < \delta(z_2).\end{aligned}$$

a) Aplicăm algoritmul lui Euclid pentru a determina c.m.m.d.c. al lui z_1 şi z_2. Conform celor de mai sus, avem $z_1 = z_2 q + r$, unde $q, r \in \mathbb{Z}[i]$, cu $\delta(r) < \delta(z_2)$, se obţin astfel: din

$$\frac{z_1}{z_2} = \frac{12-3i}{3+6i} = \frac{4-i}{1+2i} = \frac{2}{5} - \frac{9}{5}\,i$$

rezultă $q = -2i$, prin urmare,

$$r = z_1 - z_2 q = (12-3i) + 2i(3+6i) = 3i.$$

Determinăm acum $q_1, r_1 \in \mathbb{Z}[i]$ cu $\delta(r_1) < \delta(r)$, astfel încât $z_2 = r q_1 + r_1$. Din

$$\frac{z_2}{r} = \frac{3+6i}{3i} = \frac{1+2i}{i} = 2 - i \in \mathbb{Z}[i]$$

rezultă $q_1 = \dfrac{z_2}{r}$ şi astfel $r_1 = z_2 - r q_1 = 0$. Prin urmare,

$$(z_1, z_2) = 3i \sim -3i \sim 3 \sim -3$$

şi $[z_1, z_2] \sim \dfrac{z_1 z_2}{(z_1, z_2)} = (12-3i)(2-i) = 30 - 18i$.

b) Toate idealele unui domeniu euclidian sunt principale. Aplicăm teorema 20 din cursul 5 şi avem

$$\begin{aligned}(z_1) \cap (z_2) = z_1\mathbb{Z}[i] \cap z_2\mathbb{Z}[i] = [z_1, z_2]\mathbb{Z}[i] = (30-18i)\mathbb{Z}[i] = (30-18i), \\ (z_1) + (z_2) = z_1\mathbb{Z}[i] + z_2\mathbb{Z}[i] = (z_1, z_2)\mathbb{Z}[i] = 3i\,\mathbb{Z}[i] = (3i).\end{aligned}$$

În cursul viitor vom începe să prezentăm mai în detaliu câteva aspecte care ţin de aritmetica inelelor de polinoame. Un rezultat important în studiul divizibilităţii polinoamelor cu coeficienţi într-un corp comutativ este următoarea teoremă, cunoscută ca **teorema împărţirii cu rest pentru polinoame**:

Teorema 9. Fie K este un corp comutativ. Pentru orice polinoame $f, g \in K[X]$, $g \neq 0$ există două polinoame $q, r \in K[X]$ unic determinate astfel încât

$$f = gq + r \text{ şi } \operatorname{grad} r < \operatorname{grad} g. \tag{4}$$

Demonstraţie. Fie $a_0, \ldots, a_n, b_0, \ldots, b_m \in K$, $b_m \neq 0$ şi

$$f = a_0 + a_1 X + \cdots + a_n X^n \text{ şi } g = b_0 + b_1 X + \cdots + b_m X^m.$$

Existenţa polinoamelor q şi r: Dacă $f = 0$ atunci $q = r = 0$ verifică (4).

Pentru $f \neq 0$ procedăm prin inducţie după $n = \operatorname{grad} f$. Dacă $n < m$ (întrucât $m \geq 0$ există polinoame f care verifică această condiţie), atunci $q = 0$ şi $r = f$ verifică pe (4).

Presupunem afirmaţia adevărată pentru polinoamele de grad mai mic decât $n \geq m$. Cum $a_n X^n$ este termenul de grad maxim al polinomului $a_n b_m^{-1} X^{n-m} g$, pentru polinomul $h = f - a_n b_m^{-1} X^{n-m} g$, avem $\operatorname{grad} h < n$ şi conform ipotezei există $q', r \in R[X]$ astfel încât

$$h = gq' + r \text{ şi } \operatorname{grad} r < \operatorname{grad} g.$$

Rezultă că $f = h + a_n b_m^{-1} X^{n-m} g = (a_n b_m^{-1} X^{n-m} + q')g + r = gq + r$ unde $q = a_n b_m^{-1} X^{n-m} + q'$. Deci existenţa polinoamelor q şi r care verifică pe (4) este demonstrată.

Unicitatea polinoamelor q şi r: Dacă mai avem

$$f = gq_1 + r_1 \text{ şi } \operatorname{grad} r_1 < \operatorname{grad} g,$$

atunci $gq + r = gq_1 + r_1$ de unde rezultă $r - r_1 = g(q_1 - q)$ şi $\operatorname{grad}(r - r_1) < \operatorname{grad} g$. Întrucât $g \neq 0$ urmează $q_1 - q = 0$ ceea ce implică $r - r_1 = 0$, adică $q_1 = q$ şi $r_1 = r$. □

Polinoamele q şi r din (4) se numesc **câtul**, respectiv **restul** împărţirii lui f la g.

Corolarul 10. Fie K este un corp comutativ şi $c \in K$. Atunci restul împărţirii unui polinom $f \in K[X]$ la polinomul $X - c$ este $f(c)$.

Într-adevăr, din (4) rezultă că restul r al împărţirii lui f la $X - c$ este un element din K, iar cum $f = (X - c)q + r$, se deduce că $r = f(c)$. Cazul $r = 0$ ne conduce imediat la:

Corolarul 11. Fie K este un corp comutativ. Un element $c \in K$ este rădăcină a lui f dacă şi numai dacă $(X - c) \mid f$.

Corolarul 12. Dacă K este un corp comutativ, atunci un polinom nenul $f \in K[X]$ de grad k are cel mult k rădăcini în K.

Într-adevăr pentru polinoamele de gradul zero afirmaţia este adevărată deoarece polinoamele de gradul zero nu au rădăcini. Presupunem $k > 0$ şi afirmaţia adevărată pentru polinoamele de grad mai mic decât k. Dacă $c_1 \in K$ este rădăcină a lui f, atunci $f = (X - c_1)q$ şi $\operatorname{grad} q = k - 1$. Conform ipotezei, polinomul q are cel mult $k-1$ rădăcini în K. Cum K este corp comutativ, $K[X]$ este domeniu de integritate şi din $f = (X - c_1)q$ rezultă că $c \in K$ este rădăcină a lui f dacă şi numai dacă $c = c_1$ sau c este rădăcină lui q. Deci f are cel mult k rădăcini în K.

Corolarul 13. Fie K un corp comutativ. Din teorema 9 rezultă că domeniul de integritate $K[X]$ împreună cu funcţia $\delta : K[X]^* \to \mathbb{N}$, $\delta(f) = \operatorname{grad} f$ este un domeniu euclidian.

Exemplul 14. Dacă luăm polinoamele $f = X^3 - 6X^2 + 9X + 3$ şi $g = X^2 - 6X + 8$ din $\mathbb{Q}[X]$, atunci, prin împărţiri succesive avem:

	$X = q_1$	$X - 9 = q_2$
$X^3 - 6X^2 + 9X + 3$	$X^2 - 6X + 8$	$X + 3$
$-X^3 + 6X^2 - 8X$	$-X^2 - 3X$	
$r_1 = X + 3$	$-9X + 8$	
	$9X + 27$	
	$r_2 = 35$	

adică

$$f = gq_1 + r_1 = g \cdot X + (X + 3) \text{ şi } g = r_1 q_2 + r_2 = (X + 3)(X - 9) + 35.$$

Evident, restul r_3 al împărţirii lui $r_1 = X + 3$ la $r_2 = 35$ în $\mathbb{Q}[X]$ este 0, aşadar, din algoritmul lui Euclid se deduce că 35 este un c.m.m.d.c. pentru f şi g. Dar cum 35 e inversabil în $\mathbb{Q}[X]$, putem scrie $(f, g) = 1$, adică f şi g sunt relativ prime. Cum

$$35 = r_2 = g - r_1(X-9) = g - (f - g \cdot X)(X-9) = -(X-9)f + [1 + X(X-9)]g,$$

rezulă că pentru $u = -\frac{1}{35}(X-9)$ şi $v = \frac{1}{35}(X^2 - 9X + 1)$ avem $uf + vg = 1$.

Observaţia 15. Din acest curs rezultă, printre altele, că domeniile de integritate $\mathbb{Z}$, $\mathbb{Z}[i]$ şi $K[X]$ (cu K corp comutativ) sunt domenii euclidiene. În consecinţă, aşa cum anticipam la finele cursului anterior, acestea sunt şi domenii cu ideale principale, deci sunt şi domenii factoriale.

Apendice (facultativ)

Fără dificultăţi deosebite se pot demonstra câteva proprietăţi ale lui

$$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{ a + b \cdot \frac{1+i\sqrt{19}}{2} \,\middle|\, a, b \in \mathbb{Z} \right\},$$

proprietăţi utile pentru o mai bună înţelegere a exerciţiilor rezolvate 2 şi 3. În primul rând, să observăm că numerele complexe $\theta = \frac{1+i\sqrt{19}}{2}$ şi $\theta' = \frac{1-i\sqrt{19}}{2}$ sunt soluţiile ecuaţiei

$$x^2 - x + 5 = 0,$$

care are coeficienţi în $\mathbb{Z}$. Pentru $z = a + b\theta$ cu $a, b \in \mathbb{Q}$, conjugatul lui z este $\overline{z} = a + b\theta'$, iar dacă $a, b \in \mathbb{Z}$ şi $z = a + b\theta$ atunci $z + \overline{z}$, $z\overline{z} \in \mathbb{Z}$ şi

$$z = 0 \Leftrightarrow a = b = 0 \Leftrightarrow \overline{z} = 0,$$

prin urmare, corespondenţa $z \mapsto |z \cdot \overline{z}|$ defineşte o funcţie $\delta : \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \to \mathbb{N}$.

Observaţia 16. i) Pentru funcţia $\delta : \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ avem:

1) $\delta(z_1 z_2) = \delta(z_1)\delta(z_2)$, $\forall z_1, z_2 \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$;
2) $\delta(z) = 0 \Leftrightarrow z = 0$;
3) $z \in U\left(\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]\right) \Leftrightarrow \delta(z) = 1$;
4) $z_1 | z_2 \Rightarrow \delta(z_1) | \delta(z_2)$;
5) $z_1 \sim z_2 \Leftrightarrow \delta(z_1) = \delta(z_2)$ şi $z_1 | z_2$;
6) dacă $\delta(z)$ e număr prim, atunci z este element ireductibil în $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$.

ii) Dacă $a, b \in \mathbb{Z}$ şi $z = a + b \cdot \frac{1+i\sqrt{19}}{2} = \frac{2a+b}{2} + \frac{b}{2}\sqrt{19}$ atunci

$$\delta(z) = 1 \Leftrightarrow (2a+b)^2 + 19b^2 = 4 \Leftrightarrow b = 0 \text{ şi } a \in \{-1, 1\},$$

prin urmare singurele elementele inversabile din $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ sunt -1 şi 1.

Exerciţiul 2. Să se demonstreze că domeniul $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ nu este euclidian.

Soluţie: Presupunem că există o funcţie $\gamma : \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \to \mathbb{N}$ care îndeplineşte condiţia din definiţia domeniilor euclidiene. Fie $x \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ neinversabil astfel încât $\gamma(x)$ ia cea mai mică valoare posibilă, i.e.

$$\gamma(x) \leq \gamma(y),\ \forall y \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \text{ neinversabil.}$$

Rezultă că există $q, r \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ astfel încât $2 = qx + r$ şi $\gamma(r) < \gamma(x)$ sau $r = 0$. Rezultă că dacă $r \neq 0$ atunci r este inversabil. Aşa cum rezultă din observaţia 16, un element este inversabil în $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ dacă şi numai dacă este ± 1.

Avem următoarele cazuri:

• $r = 0$, deci $x \mid 2$.

La fel ca în exerciţiile 4 şi 5 din cursul 7 se arată, folosind observaţia 16, că 2 este ireductibil. Rezultă că $x = \pm 2$.

• $r = -1$, deci $x \mid 3$.

La fel ca în exerciţiile 4 şi 5 din cursul 7 se arată, folosind observaţia 16, că 3 este ireductibil. Rezultă că $x = \pm 3$.

• $r = 1$, deci $x \mid 1$, ceea ce este imposibil pentru că x nu este inversabil.

De asemenea, există $q', r' \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ astfel încât

$$\frac{1+i\sqrt{19}}{2} = q'x + r' \text{ şi } \gamma(r') < \gamma(x) \text{ sau } r' = 0. \tag{5}$$

Din alegerea lui x rezultă că dacă $r' \neq 0$, atunci r' este inversabil. Deci r' poate fi doar 0 sau ± 1. Înlocuind în (5), se deduce că $x \in \{\pm 2, \pm 3\}$ divide unul din numerele $\frac{1+i\sqrt{19}}{2}$, $\frac{3+i\sqrt{19}}{2}$ sau $\frac{-1+i\sqrt{19}}{2}$, ceea ce conduce la o contradicţie.

Exerciţiul 3. Să se arate că domeniul $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ este cu ideale principale.

Soluţie: Fie I un ideal în $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ cu $0 \neq I \neq R$. Rezultă că există un element $x \in I$ (nenul) cu $|x|^2 \in \mathbb{N}^*$ (şi, implicit, $|x|$) minim.

Să presupunem, prin reducere la absurd, că $I \neq x\,\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$. Atunci există un element $y \in I \setminus x\,\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ şi

$$by - ax \in I,\ \forall a, b \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right].$$

Să notăm că

$$|by - ax| < |x| \;\Leftrightarrow\; \left|b \cdot \frac{y}{x} - a\right| < 1, \tag{6}$$

adică a compara $|by - ax|$ cu $|x|$ revine la a compara $\left|b \cdot \frac{y}{x} - a\right|$ cu 1, iar dacă găsim a şi b care satisfac (6), atunci, pentru a nu contrazice alegerea lui x, ar trebui să avem

$$|by - ax| = 0 \;\Leftrightarrow\; b \cdot \frac{y}{x} - a = 0. \tag{7}$$

Fără a restânge generalitatea, putem presupune că partea imaginară $v(\in \mathbb{R})$ a numărului complex $\frac{y}{x}$ este în intervalul $\left[-\frac{\sqrt{19}}{4}, \frac{\sqrt{19}}{4}\right]$.

În cazul în care aceasta nu are loc, cum intervalul $\left[\frac{2v}{\sqrt{19}} - \frac{1}{2}, \frac{2v}{\sqrt{19}} + \frac{1}{2}\right]$ are lungimea 1,

$$\exists m \in \mathbb{Z} : m \in \left[\frac{2v}{\sqrt{19}} - \frac{1}{2}, \frac{2v}{\sqrt{19}} + \frac{1}{2}\right] \;\Leftrightarrow\; \exists m \in \mathbb{Z} : \left|v - \frac{m\sqrt{19}}{2}\right| \leq \frac{\sqrt{19}}{4}.$$

Notăm $z = m \cdot \frac{1 + i\sqrt{19}}{2}$, iar cum $\frac{y - zx}{x} = \frac{y}{x} - z$ are partea imaginară $v - \frac{m\sqrt{19}}{2}$, îl putem lua pe y ca fiind $y_1 = y - xz$ deoarece acesta satisface şi celelalte condiţii impuse asupra lui y. Într-adevăr, cum I e ideal, $y_1 = y - xz \in I$ şi $y_1 = y - xz \notin x\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ (în caz contrar, $y = y_1 + xz$ ar aparţine idealului $x\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$, ceea ce contrazice alegerea iniţială a lui y).

Aşadar, pornind de la presupunerea că $I \neq x\,\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$, am găsit un $y \in I \setminus x\,\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ pentru care partea imaginară v a lui $\frac{y}{x}$ este în $\left[-\frac{\sqrt{19}}{4}, \frac{\sqrt{19}}{4}\right]$. Distingem următoarele cazuri:

Cazul 1: $-\frac{\sqrt{3}}{2} < v < \frac{\sqrt{3}}{2}$. Atunci

$$\exists k \in \mathbb{Z} : \left|\frac{y}{x} - k\right| < 1$$

(care este o inegalitate de forma (6)). Într-adevăr, considerăm reprezentarea geometrică a lui $\mathbb{C}$ într-un sistem de axe ortogonal xOy şi construim pornind din O, de o parte si de alta a axei Ox, dreptunghiuri adiacente cu latura orizontală $\frac{1}{2}$ pe Ox şi cea verticală $\frac{\sqrt{3}}{2}$. Punctul corespunzător lui $\frac{y}{x}$ se află fie în interiorul, fie pe una dintre laturile verticale ale unui astfel de dreptunghi. Concluzia urmează faptului că cea mai mare distanţa între două puncte din interiorul sau de pe frontiera acestui dreptunghi este lungimea diagonalei, care este 1.

Rezultă că $\frac{y}{x} - k = 0$, deci $y = kx \in x\,\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$, contradicţie.

Cazul 2: $\frac{\sqrt{3}}{2} \leq v \leq \frac{\sqrt{19}}{4}$. Atunci

$$0 \geq 2v - \frac{\sqrt{19}}{2} \geq \sqrt{3} - \frac{\sqrt{19}}{2} > \sqrt{3} - \frac{\sqrt{27}}{2} = -\frac{\sqrt{3}}{2},$$

iar cum $2v - \dfrac{\sqrt{19}}{2}$ este partea imaginară a lui $\dfrac{2y}{x} - \dfrac{1+i\sqrt{19}}{2}$, folosim cazul 1 şi deducem că există un $k \in \mathbb{Z}$ astfel încât $\left|\dfrac{2y}{x} - \dfrac{1+i\sqrt{19}}{2} - k\right| < 1$, de unde se obţine egalitatea de forma (7) aferentă:

$$\frac{2y}{x} - \frac{1+i\sqrt{19}}{2} - k = 0 \;\Leftrightarrow\; 2y + kx = \frac{1+i\sqrt{19}}{2}\, x.$$

a) Pentru $k \in 2\mathbb{Z}$ avem $2\left(y + \dfrac{k}{2}\, x\right) = \dfrac{1+i\sqrt{19}}{2}\, x$. Notăm $y + \dfrac{k}{2}\, x \in I$ cu y' şi avem

$$2y' = \frac{1+i\sqrt{19}}{2}\, x.$$

b) Pentru $k \in 1 + 2\mathbb{Z}$ avem $2\left(y + \dfrac{k-1}{2}\, x\right) = \dfrac{-1+i\sqrt{19}}{2}\, x$. Notăm $-y - \dfrac{k-1}{2}\, x \in I$ cu y' şi avem

$$2y' = \frac{1-i\sqrt{19}}{2}\, x.$$

Fie că suntem în subcazul a), fie în subcazul b), din

$$2y' = \frac{1 \pm i\sqrt{19}}{2}\, x\,,$$

prin înmulţire cu $\dfrac{1 \mp i\sqrt{19}}{4}$, obţinem

$$\frac{1 \mp i\sqrt{19}}{2}\, y' = \frac{5}{2}\, x \;\Leftrightarrow\; \frac{1 \mp i\sqrt{19}}{2}\, y' - 2x = \frac{1}{2}\, x,$$

şi astfel am găsit $\dfrac{1 \mp i\sqrt{19}}{2}\, y' - 2x \in I$ nenul cu

$$\left|\frac{1 \mp i\sqrt{19}}{2}\, y' - 2x\right| = \frac{1}{2}\, |x| < |x|,$$

ceea ce contrazice alegerea lui $x \in I$.

Cazul 3: $\dfrac{\sqrt{19}}{4} \le v \le \dfrac{\sqrt{3}}{2}$. Cazul se tratează în acelaşi mod ca şi cazul 2.