CURS 11+12 (facultativ)

Având în vedere că 17.04 (Vinerea Mare) si 1.05 au fost două zile de vineri libere, cursul nostru ar fi trebuit să se desfăşoare pe durata a 10 săptămâni. Totuşi, sunt câteva aplicaţii interesante care derivă din cursurile anterioare şi pe care le-am inclus sub forma unor exerciţii în acest material. Acestea se referă la rezolvarea unor ecuţii în $\mathbb{Z}$ care rezultă abordând problema în inele de forma $\mathbb{Z}[\theta]$, unde θ este o rădăcină a unui trinom cu coeficieţi întregi de forma $X^2 + pX + q$.

Preliminarii

Fie $p, q \in \mathbb{Z}$ şi ecuaţia

$$x^2 + px + q = 0. \tag{$*$}$$

Orice soluţie raţională a ecuaţiei $(*)$ este întreagă deoarece coeficientul dominant al polinomului $X^2 + pX + q \in \mathbb{Z}[X]$ este 1. Să considerăm că soluţiile ecuaţiei $(*)$ nu sunt raţionale, fie acestea $\theta, \theta' \in \mathbb{C} \setminus \mathbb{Q}$. Pentru $z = a + b\theta$ cu $a, b \in \mathbb{Q}$ numim $\overline{z} = a + b\theta'$ **conjugatul lui** z.

Exerciţiul 1. Fie $\theta, \theta' \in \mathbb{C} \setminus \mathbb{Q}$ soluţiile unei ecuaţii de forma $(*)$ (cu $p, q \in \mathbb{Z}$). Să se arate că:
a) dacă $a, b \in \mathbb{Q}$ atunci

$$z = a + b\theta = 0 \Leftrightarrow a = b = 0 \Leftrightarrow \overline{z} = 0;$$

b) dacă $a_1, a_2, b_1, b_2 \in \mathbb{Q}$ atunci

$$a_1 + b_1\theta = a_2 + b_2\theta \;\Rightarrow\; a_1 = a_2 \text{ şi } b_1 = b_2;$$

c) dacă $z = a + b\theta$ atunci:
i) $a, b \in \mathbb{Q} \;\Rightarrow\; z + \overline{z},\ z\overline{z} \in \mathbb{Q}$;
ii) $a, b \in \mathbb{Z} \;\Rightarrow\; z + \overline{z},\ z\overline{z} \in \mathbb{Z}$;
d) $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\}$ este cel mai mic subinel al lui $\mathbb{C}$ care conţine mulţimea $\{1, \theta\}$ (adică este subinelul lui $\mathbb{C}$ generat de $\{1, \theta\}$);
e) $\mathbb{Q}(\theta) = \{a + b\theta \mid a, b \in \mathbb{Q}\}$ este cel mai mic subcorp al lui $\mathbb{C}$ care conţine pe θ (adică este subcorpul lui $\mathbb{C}$ generat de θ);
f) $(\mathbb{Z}[\theta], +, \cdot)$ este un domeniu de integritate, iar $(\mathbb{Q}(\theta), +, \cdot)$ este un corp comutativ;
g) $\mathbb{Z}[\theta] = \mathbb{Z}[\theta']$ şi $\mathbb{Q}(\theta) = \mathbb{Q}(\theta')$;
h) dacă $z_1, z_2 \in \mathbb{Q}[\theta]$, atunci $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ şi $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.

Soluţie: a) Fie $a + b\theta = 0$. Presupunând $b \neq 0$ ar rezulta $\theta = -\dfrac{a}{b} \in \mathbb{Q}$, contradicţie. Prin urmare $b = 0$ şi, implicit, $a = 0$. Celelalte implicaţii sunt analoage sau evidente.
b) Se foloseşte a).
c) Relaţiile lui Viète aplicate ecuaţiei $(*)$ conduc la $\theta + \theta' = -p \in \mathbb{Z}$ şi $\theta\theta' = q \in \mathbb{Z}$, prin urmare

$$z + \overline{z} = 2a + b(\theta + \theta') \text{ şi } z\overline{z} = a^2 + ab(\theta + \theta') + b^2\theta\theta'.$$

Concluzia este imediată atât la i) cât şi la ii).
d) Evident $\mathbb{Z}[\theta] \neq \emptyset$. Pentru orice $z_1 = a_1 + b_1\theta,\ z_2 = a_2 + b_2\theta$ cu $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ avem

$$z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)\theta \in \mathbb{Z}[\theta] \text{ şi } z_1 z_2 = (a_1 a_2 + b_1 b_2 \theta^2) + (a_1 b_2 + a_2 b_1)\theta.$$

Din $\theta^2 = -p\theta - q$ rezultă că

$$z_1 z_2 = (a_1 a_2 - q b_1 b_2) + (a_1 b_2 + a_2 b_1 - p b_1 b_2)\theta \in \mathbb{Z}[\theta].$$

Deci $\mathbb{Z}[\theta]$ este subinel şi $1 = 1 + 0 \cdot \theta \in \mathbb{Z}[\theta]$. Arătăm că subinelul $\mathbb{Z}[\theta]$ este generat de $\{1, \theta\}$.
1) Evident $\{1, \theta\} \subseteq \mathbb{Z}[\theta]$.
2) Dacă A este un subinel al lui $(\mathbb{C}, +, \cdot)$ şi $\{1, \theta\} \subseteq A$ atunci $\mathbb{Z}[\theta] \subseteq A$. Într-adevăr, din $1 \in A$ şi din faptul că A este subgrup al lui $(\mathbb{C}, +)$ rezultă $\mathbb{Z} \subseteq A$. Analog, din $\theta \in A$ urmează $\mathbb{Z}\theta \subseteq A$, iar din $\mathbb{Z}, \mathbb{Z}\theta \subseteq A$ şi din stabilitatea lui A faţă de $+$ rezultă $\mathbb{Z} + \mathbb{Z}\theta \subseteq A$, adică $\mathbb{Z}[\theta] \subseteq A$.

Din 1) şi 2) deducem că $\mathbb{Z}[\theta]$ este cel mai mic subinel al lui $(\mathbb{C}, +, \cdot)$ care include pe $\{1, \theta\}$, adică $\mathbb{Z}[\theta]$ este subinelul generat de $\{1, \theta\}$.
e) Evident că $|\mathbb{Q}(\theta)| \geq 2$. Ca la d) se arată că pentru orice $z_1, z_2 \in \mathbb{Q}(\theta)$ avem $z_1 - z_2, z_1 z_2 \in \mathbb{Q}(\theta)$. Fie $z = a + b\theta \in \mathbb{Q}(\theta)$, $z \neq 0$. Aceasta înseamnă că $a, b \in \mathbb{Q}$ şi $z\overline{z} \in \mathbb{Q}^*$ şi astfel avem:

$$z^{-1} = \frac{1}{a + b\theta} = \frac{a + b\theta'}{z\overline{z}} = \frac{a + b(-p - \theta)}{z\overline{z}} = \frac{a - bp}{z\overline{z}} - \frac{b}{z\overline{z}}\theta \in \mathbb{Q}(\theta).$$

Deci $\mathbb{Q}(\theta)$ este subcorp. Arătăm că subcorpul $\mathbb{Q}(\theta)$ este generat de θ.
1) Evident $\theta \in \mathbb{Q}(\theta)$.
2) Dacă A este un subcorp al lui $(\mathbb{C}, +, \cdot)$ şi $\theta \in A$ atunci $\mathbb{Q}(\theta) \subseteq A$. Într-adevăr, din ipoteza că A este subcorp rezultă $1 \in A$ şi că A este subgrup al lui $(\mathbb{C}, +)$ ceea ce implică $\mathbb{Z} \subseteq A$. Tot din ipoteza că A este subcorp rezultă că A^* este subgrup în $(\mathbb{C}^*, \cdot)$ care, împreună cu $\mathbb{Z}^* \subseteq A^*$ implică $\mathbb{Q}^* \subseteq A^*$. Astfel am arătat că $\mathbb{Q} \subseteq A$, iar din $\theta \in A$, urmează $\mathbb{Q} + \mathbb{Q}\theta \subseteq A$, adică $\mathbb{Q}(\theta) \subseteq A$.

Din 1) şi 2) deducem că $\mathbb{Q}(\theta)$ este cel mai mic subcorp al lui $(\mathbb{C}, +, \cdot)$ care conţine pe θ, adică $\mathbb{Q}(\theta)$ este subcorpul generat de θ.
f) Din faptul că $\mathbb{Z}[\theta]$ este un subinel al corpului comutativ $(\mathbb{C}, +, \cdot)$ ce conţine pe 1 deducem că $\mathbb{Z}[\theta]$ este, împreună cu operaţiile induse, un inel (asociativ) nenul comutativ, cu unitate, fără divizori ai lui, iar din faptul că $\mathbb{Q}(\theta)$ este un subcorp al corpului comutativ $(\mathbb{C}, +, \cdot)$ deducem că $\mathbb{Q}(\theta)$ este, împreună cu operaţiile induse, un corp comutativ.
g) Din $\theta' = -p - \theta$ rezultă $\mathbb{Z}[\theta] \supseteq \mathbb{Z}[\theta']$ şi $\mathbb{Q}(\theta) \supseteq \mathbb{Q}(\theta')$. Analog rezultă incluziunile inverse.
h) Se verifică egalităţile folosind legăturile dintre θ şi θ' date de relaţiile lui Viète.

Observaţiile 1. a) Dacă $z = a(+0 \cdot \theta) \in \mathbb{Q}$ atunci $\overline{z} = a = z$, adică $\overline{z} = z$ pentru orice $z \in \mathbb{Q}$.
b) Să remarcăm că dacă θ este o soluţie (din $\mathbb{C} \setminus \mathbb{Q}$) a ecuaţiei $(*)$, atunci θ' este doar o notaţie pentru ,,cealaltă soluţie a ecuaţiei” $(*)$. Din acest punct de vedere, putem scrie $(\theta')' = \theta$ şi, implicit, avem $\overline{\overline{z}} = z$.

Exerciţiul 2. Fie $\theta \in \mathbb{C} \setminus \mathbb{Q}$ o soluţie a unei ecuaţii de forma $(*)$ cu $p, q \in \mathbb{Z}$. Să se arate că:
a) corespondenţa $z \mapsto |z \cdot \overline{z}|$ defineşte o funcţie de la $\mathbb{Z}[\theta]$ la $\mathbb{N}$;
b) funcţia $\delta : \mathbb{Z}[\theta] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$ are următoarele proprietăţi:
i) $\delta(z_1 z_2) = \delta(z_1)\delta(z_2)$ pentru orice $z_1, z_2 \in \mathbb{Z}[\theta]$;
ii) $\delta(z) = 0$ ($z \in \mathbb{Z}[\theta]$) dacă şi numai dacă $z = 0$;
iii) $z \in \mathbb{Z}[\theta]$ este inversabil în $\mathbb{Z}[\theta]$ dacă şi numai dacă $\delta(z) = 1$;
c) afirmaţiile i) şi ii) de la b) sunt adevărate şi pentru funcţia

$$\delta_0 : \mathbb{Q}(\theta) \to \mathbb{Q},\ \delta_0(z) = |z \cdot \overline{z}|.$$

Soluţie: a) Am văzut în problema anterioară că din relaţiile lui Viète aplicate ecuaţiei $(*)$ rezultă $\theta+\theta', \theta\theta' \in \mathbb{Z}$ şi $z\overline{z} = a^2 + ab(\theta+\theta') + b^2\theta\theta' \in \mathbb{Z}$.
b) i) $\delta(z_1z_2) = |z_1z_2\overline{z_1z_2}| = |z_1z_2\overline{z_1}\,\overline{z_2}| = |z_1\overline{z_1}||z_2\overline{z_2}| = \delta(z_1)\delta(z_2)$, $\forall z_1, z_2 \in \mathbb{Z}[\theta]$.
ii) Se aplică a) de la exerciţiul anterior.
iii) Dacă z este inversabil şi z^{-1} este inversul său atunci $\delta(z)\delta(z^{-1}) = 1$ în $\mathbb{N}$, ceea ce implică $\delta(z) = 1$. Reciproc, dacă $\delta(z) = 1$ atunci z este inversabil şi inversul lui z este $\overline{z}$ sau $-\overline{z}$.
c) Se demonstrează ca mai sus.

Exerciţiul 3. Fie $\theta \in \mathbb{C}\setminus\mathbb{Z}$ o soluţie a unei ecuaţii de forma $(*)$ şi $\delta : \mathbb{Z}[\theta] \to \mathbb{N}$, $\delta(z) = |z\cdot\overline{z}|$. Să se arate că pentru orice $z_1, z_2, z \in \mathbb{Z}[\theta]$ avem:

i) $z_1 \mid z_2 \;\Rightarrow\; \delta(z_1) \mid \delta(z_2)$;
ii) $z_1 \sim z_2 \;\Leftrightarrow\; \delta(z_1) = \delta(z_2)$ şi $z_1 \mid z_2$;
iii) dacă $\delta(z)$ e număr prim, atunci z este element ireductibil în $\mathbb{Z}[\theta]$.

Soluţie: i) Se foloseşte punctul b) i) al exerciţiului anterior.
ii) Dacă $z_2 = z_1z$ ($z \in \mathbb{Z}[\theta]$) atunci $\delta(z_2) = \delta(z_1)\delta(z)$. Din $\delta(z_1) = \delta(z_2)$ rezultă că $z_1 = z_2 = 0$ sau $\delta(z) = 1$, adică z e inversabil, prin urmare $z_1 \sim z_2$.
iii) Dacă $z = z_1z_2$ în $\mathbb{Z}[\theta]$ atunci $\delta(z) = \delta(z_1)\delta(z_2)$ în $\mathbb{N}$ cu $\delta(z)$ număr prim, prin urmare sau $\delta(z_1) = 1$ sau $\delta(z_2) = 1$.

Exerciţiul 4. Fie $\varepsilon \in \left\{\dfrac{1+i\sqrt{3}}{2}, \dfrac{1-i\sqrt{3}}{2}, \dfrac{-1+i\sqrt{3}}{2}, \dfrac{-1-i\sqrt{3}}{2}\right\}$. Să se determine elementele inversabile în inelul $\mathbb{Z}[\varepsilon]$.

Soluţie: Să observăm că

$$\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right] = \mathbb{Z}\left[\frac{1-i\sqrt{3}}{2}\right] = \mathbb{Z}\left[\frac{-1+i\sqrt{3}}{2}\right] = \mathbb{Z}\left[\frac{-1-i\sqrt{3}}{2}\right].$$

Prima şi ultima egalitate rezultă din punctul g) al exerciţiului 1, iar egalitatea din mijloc se obţine folosind din definiţia subinelului generat.

Fie atunci $\varepsilon = \dfrac{-1+i\sqrt{3}}{2}$. Numărul $z = a + b\varepsilon$ ($a, b \in \mathbb{Z}$) e inversabil în $\mathbb{Z}[\varepsilon]$ dacă şi numai dacă

$$\delta(z) = 1 \Leftrightarrow a^2 - ab + b^2 = 1 \Leftrightarrow (2a-b)^2 + 3b^2 = 4.$$

Avem $a, b \in \mathbb{Z}$ doar în următoarele cazuri:

- $(2a-b)^2 = 1$ şi $3b^2 = 3$;
- $(2a-b)^2 = 4$ şi $3b^2 = 0$,

de unde urmează $(a, b) \in \{(1,0), (-1,0), (0,1), (-1,-1), (1,1)\}$. Aşadar,

$$U(\mathbb{Z}[\varepsilon]) = \{1, -1, \varepsilon, -\varepsilon, -1-\varepsilon, 1+\varepsilon\}.$$

Observaţia 2. Din teorema împărţirii cu rest în $\mathbb{Z}$ rezultă că

$$\forall a, b \in \mathbb{Z},\; b \neq 0,\; \exists q', r' \in \mathbb{Z} :\; a = bq' + r' \text{ şi } |r'| \leq \frac{|b|}{2}.$$

Dacă q şi r sunt câtul şi restul împărţirii în $\mathbb{Z}$ a lui a la b şi $0 \leq r \leq \dfrac{|b|}{2}$, atunci $q' = q$ şi $r' = r$, iar dacă $\dfrac{|b|}{2} < r < |b|$ atunci $q' = q + \dfrac{|b|}{b}$ şi $r' = r - |b|$. Să observăm şi că, păstrând în această formă condiţia asupra lui r', numerele q', r' nu sunt unic determinate (de exemplu, $7 = 2\cdot 3 + 1 = 2\cdot 4 + (-1)$).

Exercițiul 5. Fie $p, q \in \mathbb{Z}$ cu $|p| + |q| < 3$. Considerăm $\theta \in \mathbb{C}$ o soluţie a ecuaţiei $(*)$, subinelul $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\}$ al lui $\mathbb{C}$ şi funcţia $\delta : \mathbb{Z}[\theta] \to \mathbb{N}$, $\delta(z) = |z \cdot \overline{z}|$. Să se arate că $(\mathbb{Z}[\theta], \delta)$ este un domeniu euclidian.

Soluţie: Dacă $\theta \in \mathbb{Q}$ atunci $\theta \in \mathbb{Z}$ şi $\mathbb{Z}[\theta] = \mathbb{Z}$, iar $\delta(z) = z^2 = (|z|)^2$ deoarece $\overline{z} = z$ pentru orice $z \in \mathbb{Z}$. Cum pentru orice $x, y \in \mathbb{Z}$,

$$\delta(x) < \delta(y) \;\Leftrightarrow\; |x| < |y|,$$

deducem că $\mathbb{Z}$ este un domeniu euclidian şi împreună cu funcţia δ.

Să considerăm acum că $\theta \in \mathbb{C} \setminus \mathbb{Q}$. Fie $z_1, z_2 \in \mathbb{Z}[\theta]$ cu $z_2 \neq 0$. Notăm $N(z_2) = z_2\overline{z_2}$. Atunci $N(z_2) \neq 0$ şi avem

$$\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{z_2\overline{z_2}} = \frac{z_3}{N(z_2)}\,, \text{ unde } z_3 = z_1\overline{z_2}\,.$$

Dar $z_3 \in \mathbb{Z}[\theta]$, prin urmare, există $m, n \in \mathbb{Z}$ astfel încât $z_3 = m + n\theta$. Folosind observaţia 2 deducem că există $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ astfel încât

$$m = N(z_2)q_1 + r_1,\ n = N(z_2)q_2 + r_2 \text{ şi } |r_1|, |r_2| \leq \frac{|N(z_2)|}{2}\,, \tag{1}$$

ceea ce implică

$$\frac{z_1}{z_2} = \frac{m + n\theta}{N(z_2)} = \frac{N(z_2)q_1 + r_1 + N(z_2)q_2\theta + r_2\theta}{N(z_2)} = (q_1 + q_2\theta) + \frac{r_1 + r_2\theta}{N(z_2)}.$$

Dacă notăm $Q = q_1 + q_2\theta$ şi $R = \dfrac{z_2(r_1 + r_2\theta)}{N(z_2)}$ atunci $Q \in \mathbb{Z}[\theta]$ şi $z_1 = z_2Q + R$. Urmează că

$$R = z_1 - z_2Q \in \mathbb{Z}[\theta],$$

iar cum $RN(z_2) = z_2(r_1 + r_2\theta)$ şi $\delta(z_2) = |N(z_2)|$, avem

$$\delta(R)[N(z_2)]^2 = \delta(R)\delta(N(z_2)) = \delta(z_2)\delta(r_1 + r_2\theta) = |N(z_2)|\delta(r_1 + r_2\theta).$$

Prin împărţire la $[N(z_2)]^2 \neq 0$ rezultă că

$$\delta(R) = \frac{\delta(r_1 + r_2\theta)}{\delta(z_2)} = \frac{1}{\delta(z_2)}\left|r_1^2 - pr_1r_2 + qr_2^2\right|.$$

Dar $\left|r_1^2 - pr_1r_2 + qr_2^2\right| \leq |r_1|^2 + |p||r_1||r_2| + |q||r_2|^2$ şi, folosind (1), avem

$$\delta(R) \leq \frac{1}{\delta(z_2)} \cdot \frac{\delta(z_2)^2}{4}\,(1 + |p| + |q|) = \delta(z_2) \cdot \frac{1 + |p| + |q|}{4}\,. \tag{2}$$

Dacă $|p| + |q| < 3$ atunci $\delta(R) < \delta(z_2)$ şi problema este rezolvată.

Observaţia 3. Domeniile euclidiene care se obţin din problema anterioară sunt

$$\mathbb{Z},\ \mathbb{Z}[i],\ \mathbb{Z}\left[\sqrt{2}\right],\ \mathbb{Z}\left[i\sqrt{2}\right],\ \mathbb{Z}\left[\frac{1 + i\sqrt{3}}{2}\right],\ \mathbb{Z}\left[\frac{1 + \sqrt{5}}{2}\right].$$

Rezolvarea unor ecuaţii în $\mathbb{Z}$

Exerciţiul 6. Să considerăm în $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ ecuaţia

$$x^2 + y^2 = z^2. \tag{1}$$

1) Să se arate că rezolvarea ecuaţiei (1) se poate reduce la cazul când x şi y sunt prime între ele.
2) Fie $x, y, z \in \mathbb{Z}$ care verifică (1) şi $(x, y) = 1$. Să se arate că x şi y nu pot fi ambele impare, iar dacă y este par atunci există $m, n \in \mathbb{Z}$ astfel încât

$$x = m^2 - n^2,\ y = 2mn \text{ şi } z = m^2 + n^2.$$

Soluţie: 1) Fie $d = (x, y)$ şi $x = dx'$, $y = dy'$. Atunci $(x', y') = 1$ şi din (1) rezultă $d \mid z$. Luăm $z = dz'$ şi avem

$$x^2 + y^2 = z^2 \Leftrightarrow x'^2 + y'^2 = z'^2.$$

2) **Soluţia 1:** Dacă x şi y sunt impare, adică $x \equiv 1(\text{mod } 2)$ şi $y \equiv 1(\text{mod } 2)$ se deduce că $x^2 + y^2 \equiv 2(\text{mod } 4)$ adică $z^2 \equiv 2(\text{mod } 4)$. Dar, dacă z este par atunci $z^2 \equiv 0(\text{mod } 4)$, iar dacă z este impar atunci $z^2 \equiv 1(\text{mod } 4)$, prin urmare congruenţa $z^2 \equiv 2(\text{mod } 4)$ nu poate avea loc.

Dacă x este impar şi y este par atunci z este impar şi $y^2 = (z + x)(z - x)$. Numerele $z + x$ şi $z - x$ sunt ambele pare şi 2 este singurul lor divizor comun prim. Într-adevăr, un alt divizor comun prim p al lor ar fi impar, ar divide pe y^2, pe $(z + x) + (z - x) = 2z$ şi pe $(z + x) - (z - x) = 2x$. Aşadar, am avea $p \mid x$ şi $p \mid y$, ceea ce contrazice condiţia $(x, y) = 1$.

Rezultă că $\dfrac{z + x}{2}$ şi $\dfrac{z - x}{2}$ sunt numere întregi prime între ele ale căror produs $\dfrac{y^2}{4} = \dfrac{z + x}{2} \cdot \dfrac{z - x}{2}$ este un pătrat perfect. Cum factorii primi din descompunerea lui $\dfrac{y^2}{4}$ au toţi exponenţi pari, pentru a nu contrazice condiţia $\left(\dfrac{z + x}{2}, \dfrac{z - x}{2}\right) = 1$ este necesar ca factorii primi din descompunerea lui $\dfrac{y^2}{4}$ să apară fie numai în descompunerea lui $\dfrac{z + x}{2}$, fie numai în descompunerea lui $\dfrac{z - x}{2}$, cu acelaşi exponent ca în descompunerea lui $\dfrac{y^2}{4}$. Prin urmare, $\dfrac{z + x}{2}$ şi $\dfrac{z - x}{2}$ sunt, de asemenea, pătrate perfecte, deci putem considera $z + x = 2m^2$ şi $z - x = 2n^2$, cu $m, n \in \mathbb{Z}$, şi astfel obţinem

$$x = m^2 - n^2,\ z = m^2 + n^2 \text{ şi } y = 2mn.$$

Se verifică uşor că dacă x, y, z au forma de mai sus, ele verifică ecuaţia $x^2 + y^2 = z^2$.

Soluţia 2: Evident, numerele x şi y nu sunt ambele pare şi z este impar. În $\mathbb{Z}[i]$ avem:

$$(x + yi)(x - yi) = z^2.$$

Dacă $d \in \mathbb{Z}[i]$ ar fi un divizor comun ireductibil pentru $x + yi$ şi $x - yi$ atunci $d \mid 2x$ şi $d \mid 2y$, prin urmare $d \mid (2x, 2y) = 2(x, y) = 2$ şi $\delta(d) \mid 4$. Cum $\delta(d) \mid \delta(z^2)$, cazurile $\delta(d) \in \{2, 4\}$ ar contrazice faptul că z e impar. Prin urmare, $(x + yi, x - yi) = 1$ în $\mathbb{Z}[i]$. Cum $\mathbb{Z}[i]$ este un domeniu factorial, rezultă că factorii ireductibili care apar (cu exponent par) în descompunerea lui z^2 sunt (asociaţi cu) factori care apar fie în descompunerea lui $x + yi$, fie în descompunerea lui $x - yi$. Aşadar, există $u \in \{\pm 1, \pm i\}$ şi $a, b \in \mathbb{Z}$ astfel ca $x + yi = u(a + bi)^2$. Rezultă că

$$x + yi = u(a^2 - b^2 + 2abi).$$

Pentru $u = 1$ se obţine $x = a^2 - b^2,\ y = 2ab$ şi $z = a^2 + b^2$. Pentru celelalte valori ale lui u se procedează analog şi se obţin forme similare pentru x, y, z, eventual cu roluri schimbate pentru x şi y (ceea ce se poate întâmpla dacă nu precizăm care dintre numerele x şi y este par).

Evident, dacă $a, b \in \mathbb{Z}$, $x = a^2 - b^2,\ y = 2ab$ şi $z = a^2 + b^2$ verifică ecuaţia din enunţ, ceea ce completează soluţia.

Exerciţiul 7. Să se rezolve în $\mathbb{Z} \times \mathbb{Z}$ ecuaţia lui Fermat

$$x^2 + 4 = y^3.$$

Soluţie: **Cazul 1:** x este impar. Ecuaţia dată se mai scrie

$$(2 + ix)(2 - ix) = y^3.$$

Cum $\mathbb{Z}[i]$ este un domeniu euclidian (vezi observaţia 3), prin urmare şi domeniu factorial, orice două elemente au un c.m.m.d.c. Fie $d = (2 + ix, 2 - ix)$ în $\mathbb{Z}[i]$, $d = m + ni$ $(m, n \in \mathbb{Z})$. Cum $d \mid (2+ix)+(2-ix) = 4$, rezultă $\delta(d) = m^2 + n^2 \mid 16$. Dar $d \mid 2 + ix$ implică $\delta(d) \mid \delta(2+ix)$, adică $m^2 + n^2 \mid 4 + x^2$. Cum x (şi, implicit, $4 + x^2$) e impar, $m^2 + n^2 = 1$. Aşadar, $(2 + ix, 2 - ix) = 1$ în $\mathbb{Z}[i]$. Dar $\mathbb{Z}[i]$ este domeniu factorial. Rezultă că factorii ireductibili ce apar (cu exponent multiplu de 3) în descompunerea lui y^3 sunt (asociaţi cu) factori ce apar fie în descompunerea lui $2 + ix$, fie în descompunerea lui $2 - ix$. Astfel, există $a, b \in \mathbb{Z}$ astfel ca

$$2 + ix \sim (a + bi)^3.$$

Cum $\pm 1 = (\pm 1)^3$ şi $\pm i = (\mp i)^3$, putem considera $2 + ix = (a + bi)^3$ şi astfel obţinem

$$a(a^2 - 3b^2) = 2 \text{ şi } 3a^2 b - b^3 = x.$$

Rezultă $a \in \{\pm 1, \pm 2\}$, ceea ce conduce la $x = \pm 11,\ y = 5$.
Cazul 2: x este par. Atunci şi y e par. Luând $x = 2u,\ y = 2v$ $(u, v \in \mathbb{Z})$ ecuaţia devine

$$u^2 + 1 = 2v^3 \Leftrightarrow (u + i)(u - i) = 2v^3.$$

Cum $i[(u-i)-(u+i)] = 2 = (-i)(1+i)^2$ (cu $-i$ şi i inversabile şi $1+i$ ireductibil (deci şi prim) în $\mathbb{Z}[i]$), rezultă că $1+i \mid u \pm i$. C.m.m.d.c. $(u+i, u-i)$ este divizor pentru $i[(u-i)-(u+i)] = 2$, dar $2 \nmid u \pm i$, prin urmare, $(u+i, u-i) = 1+i$. Deducem că există $a, b \in \mathbb{Z}$ astfel ca $u+i = (1+i)(a+bi)^3$. De aici se obţine

$$a^3 - 3a^2 b - 3ab^2 + b^3 = u \text{ şi } a^3 + 3a^2 b - 3ab^2 - b^3 = 1.$$

Dar $a^3 + 3a^2 b - 3ab^2 - b^3 = (a - b)(a^2 + 4ab + b^2)$. Atunci

$$a - b = 1 \text{ şi } a^2 + 4ab + b^2 = 1 \tag{1}$$

sau

$$a - b = -1 \text{ şi } a^2 + 4ab + b^2 = -1. \tag{2}$$

Sistemul (1) are soluţiile $(a, b) \in \{(1, 0), (0, -1)\}$, deci $(x, y) \in \{(2, 2), (-2, 2)\}$, iar sistemul (2) nu are soluţii deoarece restul împărţirii lui $a^2 + 4ab + b^2 = (a + 2b)^2 - 3b^2$ la 3 nu poate fi 2.

Exerciţiul 8. Să se arate că (toate) soluţiile din $\mathbb{Z} \times \mathbb{Z}$ ale ecuaţiei lui Fermat

$$y^2 + 2 = x^3$$

sunt $(3, 5)$ şi $(3, -5)$.

Soluţie: Cum $x^3 = y^2 + 2$, y este impar (în caz contrar, cum $y^2 + 2 \equiv 2 \pmod 4$ ar exista un cub perfect $x^3 \equiv 2 \pmod 4$, ceea ce nu e posibil), prin urmare şi x^3 este impar. În $\mathbb{Z}[i\sqrt{2}]$ avem:

$$x^3 = (y + i\sqrt{2})(y - i\sqrt{2})$$

Cum $\mathbb{Z}[i\sqrt{2}\,]$ este un domeniu euclidian (vezi observaţia 3), prin urmare şi domeniu factorial, orice două elemente au un c.m.m.d.c. Fie $d = (y + i\sqrt{2}, y - i\sqrt{2})$ în $\mathbb{Z}[i\sqrt{2}\,]$. Atunci d divide pe

$$y - i\sqrt{2} - (y + i\sqrt{2}) = -2i\sqrt{2} = (i\sqrt{2})^3.$$

Avem $U(\mathbb{Z}[i\sqrt{2}\,]) = \{-1, 1\}$ (vezi exemplul 3 d) din cursul 4) şi $i\sqrt{2}$ este ireductibil în $\mathbb{Z}[i\sqrt{2}\,]$ ($\delta(i\sqrt{2}) = 2$ şi aplicăm punctul iii) al exerciţiului 3), prin urmare $d = \pm(i\sqrt{2})^k$ cu $k \in \mathbb{N}$, $k \leq 3$. Dacă $k \neq 0$, $i\sqrt{2}$ este un divizor ireductibil al lui d, iar cum d divide pe

$$(y + i\sqrt{2})(y - i\sqrt{2}) = y^2 + 2 = x^3,$$

avem $i\sqrt{2} \mid x$ şi astfel $2 \mid x^3$, ceea ce contrazice faptul că x^3 este impar. Aşadar, $k = 0$ şi $d = \pm 1$. Cum $\mathbb{Z}[i\sqrt{2}]$ este domeniu factorial, rezultă că factorii ireductibili care apar (cu exponent multiplu de 3) în descompunerea lui x^3 sunt (asociaţi cu) factori care apar fie în descompunerea lui $y + i\sqrt{2}$, fie în descompunerea lui $y - i\sqrt{2}$. Astfel, există $a, b \in \mathbb{Z}$ astfel ca $y + i\sqrt{2} = (a + bi\sqrt{2})^3$ ceea ce este echivalent cu

$$y = a^3 - 6ab^2 \text{ şi } 1 = 3a^2b - 2b^3.$$

Din $1 = b(3a^2 - 2b^2)$ rezultă $b = \pm 1$. Atunci $a = \pm 1$, $y = \pm 5$ şi $x = 3$.

Notaţie. Pentru un domeniu factorial R, un element $r \in R$ şi un element ireductibil $p \in R$ notăm cu $v_p(r)$ exponentul maxim $k \in \mathbb{N}$ al lui p pentru care $p^k \mid r$.

Exerciţiul 9. Fie $\varepsilon = \dfrac{-1 + i\sqrt{3}}{2}$, $\alpha = 1 - \varepsilon$, $u \in \mathbb{Z}[\varepsilon]$ inversabil şi $x, y, z \in \mathbb{Z}[\varepsilon]$ cu

$$x^3 + y^3 = uz^3.$$

Să se arate că:

a) $\alpha \mid xyz$;

b) dacă $\alpha \nmid xy$ şi $\alpha \mid z$ atunci $\alpha^2 \mid z$.

Soluţie: În primul rând să reamintim că dacă $a, b \in \mathbb{Z}$ atunci $\delta(a + b\varepsilon) = a^2 - ab + b^2$. Ca atare, α este ireductibil deoarece $\delta(\alpha) = \delta(1 - \varepsilon) = 3$ care este număr prim.

Continuăm prin a arăta că orice $t \in \mathbb{Z}[\varepsilon]$ este de forma $q\alpha + r$ cu $q \in \mathbb{Z}[\varepsilon]$ şi $r \in \{-1, 0, 1\}$. Într-adevăr, cum $\varepsilon = 1 - \alpha$, dacă $a, b \in \mathbb{Z}$ şi $t = a + b\varepsilon = a + b - b\alpha$, atunci

$$\alpha \mid t - (a + b). \tag{1}$$

Dar $\alpha^2 = -3\varepsilon \sim 3$ şi, conform observaţiei 2, există $q', r \in \mathbb{Z}$ astfel ca $a + b = 3q' + r$ cu $r \in \{-1, 0, 1\}$, rezultă $\alpha \mid (a + b) - r$, ceea ce, împreună cu (1), implică $\alpha \mid t - r$.

a) Dacă $x = \alpha q + 1$ ($q \in \mathbb{Z}[\varepsilon]$) atunci

$$x^3 - 1 = (x - 1)(x - \varepsilon)(x - \varepsilon^2) = q\alpha(1 - \varepsilon + q\alpha)(1 - \varepsilon^2 + q\alpha).$$

Dar

$$1-\varepsilon^2+q\alpha=(1+\varepsilon)(1-\varepsilon)+q\alpha=-\varepsilon^2\alpha+q\alpha=\alpha(-\varepsilon^2+q)=\alpha(1-\varepsilon^2+q-1)$$
$$=\alpha[(1+\varepsilon)(1-\varepsilon)+q-1]=\alpha[(1+\varepsilon)\alpha+q-1]$$

şi $1-\varepsilon+q\alpha=\alpha+q\alpha=\alpha(1+q)$, prin urmare

$$x^3-1=\alpha^4q(1+q)(1+\varepsilon)+\alpha^3(q+1)q(q-1).$$

Cum q este suma unui multiplu de α cu $-1,0$ sau 1, al doilea termen al sumei de mai sus este multiplu de α^4 şi, astfel, $\alpha^4\mid x^3-1$.

Dacă $x=\alpha q-1$ atunci $-x=\alpha(-q)+1$ şi de mai sus rezultă că $\alpha^4\mid(-x)^3-1$ sau, echivalent, $\alpha^4\mid x^3+1$.

Presupunând că ar exista $x,y,z\in\mathbb{Z}[\varepsilon]$ cu

$$x^3+y^3=uz^3 \tag{2}$$

şi $\alpha\nmid xyz$, α nu ar divide nici pe x, nici pe y, nici pe z, prin urmare x, y şi z sunt de forma $q\alpha\pm1$. Din (2), folosind consideraţiile anterioare, ar rezulta că $\alpha^4|\pm1\pm1\mp u$. Folosind faptul că $\alpha^4\sim 9$, exerciţiul 4 şi aplicând pe δ se obţine câte o contradicţie pentru fiecare caz posibil.
b) Cum $\alpha\nmid xy$, α nu divide nici pe x, nici pe y, prin urmare x şi y sunt de forma $q\alpha\pm1$. Rezultă că $\alpha^4|\pm1\pm1\mp uz^3$. Aşa cum am văzut la a), z de forma $q\alpha\pm1$ conduce la o contradicţie, iar dacă $\alpha^4\mid uz^3$ atunci $3v_\alpha(z)=v_\alpha(uz^3)\ge4$, iar cum $v_\alpha(z)\in\mathbb{N}$, avem $v_\alpha(z)\ge2$, deci $\alpha^2\mid z$.

Exerciţiul 10. Fie $\varepsilon=\dfrac{-1+i\sqrt{3}}{2}$, $\alpha=1-\varepsilon$, $u\in U(\mathbb{Z}[\varepsilon])$ şi $x,y,z\in\mathbb{Z}[\varepsilon]$ cu $(x,y)=1$ în $\mathbb{Z}[\varepsilon]$ şi

$$x^3+y^3=uz^3.$$

Dacă $\alpha\nmid xy$ şi $v_\alpha(z)\ge2$ atunci există $x_1,y_1,z_1,u_1\in\mathbb{Z}[\varepsilon]$ cu u_1 inversabil şi $(x_1,y_1)=1$ în $\mathbb{Z}[\varepsilon]$, $\alpha\nmid x_1y_1$ şi $v_\alpha(z_1)=v_\alpha(z)-1$ astfel încât

$$x_1^3+y_1^3=u_1z_1^3.$$

Soluţie: Cum $uz^3=x^3+y^3=(x+y)(x+\varepsilon y)(x+\varepsilon^2y)$,

$$v_\alpha(x+y)+v_\alpha(x+\varepsilon y)+v_\alpha(x+\varepsilon^2y)=v_\alpha(uz^3)=3v_\alpha(z)\ge6.$$

Rezultă $v_\alpha(x+y)\ge2$ sau $v_\alpha(x+\varepsilon y)\ge2$ sau $v_\alpha(x+\varepsilon^2y)\ge2$. Cum ε este o rădăcină de ordinul 3 a unităţii, $y^3=(\varepsilon y)^3=(\varepsilon^2y)^3$, aşa că putem considera, fără a restrânge generalitatea, că $v_\alpha(x+y)\ge2$.

Cum $v_\alpha((1-\varepsilon)y)=v_\alpha(\alpha y)=1+v_\alpha(y)$ şi $\alpha\nmid y$ avem $v_\alpha((1-\varepsilon)y)=1$. Astfel,

$$v_\alpha(x+\varepsilon y)=v_\alpha(x+y-(1-\varepsilon)y)=\min(v_\alpha(x+y),v_\alpha((1-\varepsilon)y))=1,$$

iar cum $(1-\varepsilon^2)y=(1+\varepsilon)(1-\varepsilon)y$ şi $1+\varepsilon$ e inversabil,

$$v_\alpha(x+\varepsilon^2y)=v_\alpha(x+y-(1-\varepsilon^2)y)=\min(v_\alpha(x+y),v_\alpha((1-\varepsilon)y))=1.$$

Prin urmare, $v_\alpha(z)=v_\alpha(x+y)+v_\alpha(x+\varepsilon y)+v_\alpha(x+\varepsilon^2y)=v_\alpha(x+y)+2$, de unde

$$v_\alpha(x+y)=v_\alpha(z)-2.$$

Din $v_\alpha(x+y) \geq 2$ şi $v_\alpha(x+\varepsilon y) = v_\alpha(x+\varepsilon^2 y) = 1$ rezultă că α este un divizor comun pentru $x+y,\ x+\varepsilon y$ şi $x+\varepsilon^2 y$.

Dacă $p \in \mathbb{Z}[\varepsilon]$, $p \nsim \alpha$ ar fi un element ireductibil care divide pe $x+y$ şi $x+\varepsilon y$,

$$p \mid (x+y)-(x+\varepsilon y) = (1-\varepsilon)y = \alpha y \ \Rightarrow\ p \mid y,$$

ceea ce implică $p \mid (x+y)-y = x$ şi contrazice $(x,y)=1$. Aşadar, $(x+y, x+\varepsilon y) = \alpha$.

Analog se arată că $(x+y, x+\varepsilon^2 y) = \alpha = (x+\varepsilon y, x+\varepsilon^2 y)$.

Din cele de mai sus deducem şi că orice element ireductibil $p \in \mathbb{Z}[\varepsilon]$, cu $p \nsim \alpha$, divide (în $\mathbb{Z}[\varepsilon]$) cel mult unul dintre numerele $x+y,\ x+\varepsilon y$ şi $x+\varepsilon^2 y$. Dar

$$v_p(x+y)+v_p(x+\varepsilon y)+v_p(x+\varepsilon^2 y) = v_p(uz^3) = 3v_p(z),$$

prin urmare, p apare în descompunerea în factori ireductibili a cel mult unuia dintre numerele $x+y,\ x+\varepsilon y$ şi $x+\varepsilon^2 y$, iar când apare, exponentul său este un multiplu de 3.

Astfel, există $u', u'', u''' \in U(\mathbb{Z}[\varepsilon])$, $q_1, q_2, q_3 \in \mathbb{Z}[\varepsilon]$, cu

$$\alpha \nmid q_1,\ \alpha \nmid q_2,\ \alpha \nmid q_3,\ (q_1,q_2) = (q_1,q_3) = (q_2,q_3) = 1$$

şi

$$x+y = u' q_1^3 \alpha^{3v_\alpha(z)-2},\ x+\varepsilon y = u'' q_2^3 \alpha,\ x+\varepsilon^2 y = u''' q_3^3 \alpha. \tag{1}$$

Atunci

$$x+y = u' q_1^3 \alpha^{3v_\alpha(z)-2},\ \varepsilon x+\varepsilon^2 y = \varepsilon u'' q_2^3 \alpha,\ \varepsilon^2 x+\varepsilon y = \varepsilon^2 u''' q_3^3 \alpha, \tag{1'}$$

egalităţi care adunate dau

$$u' q_1^3 \alpha^{3v_\alpha(z)-2} + \varepsilon u'' q_2^3 \alpha + \varepsilon^2 u''' q_3^3 \alpha = 0 \Leftrightarrow u' q_1^3 \alpha^{3v_\alpha(z)-3} + \varepsilon u'' q_2^3 + \varepsilon^2 u''' q_3^3 = 0.$$

Considerăm $x_1 = q_2,\ y_1 = q_3,\ z_1 = q_1 \alpha^{v_\alpha(z)-1}$ şi obţinem

$$x_1^3 + u_2 y_1^3 = u_1 z_1^3, \tag{2}$$

cu $u_1, u_2 \in U(\mathbb{Z}[\varepsilon])$. Din $\alpha \nmid x_1$, $\alpha \nmid y_1$ şi $v_\alpha(z_1) = v_\alpha(z)-1 \geq 1$ rezultă $\alpha \mid x_1 \pm 1,\ \alpha \mid y_1 \pm 1$, avem

$$\alpha^4 \mid x_1^3 \pm 1,\ \alpha^4 \mid y_1^3 \pm 1,\ \alpha^3 \mid z_1^3,$$

prin urmare $\alpha^3 \mid \pm 1 \pm u_2$. Aplicând δ ajungem la concluzia că aceasta se poate întâmpla numai când $\pm 1 \pm u_2 = 0$, adică $u_2 \in \{-1, 1\}$.

Înlocuind, la nevoie, y_1 cu $-y_1$, egalitatea (2) devine

$$x_1^3 + y_1^3 = u_1 z_1^3$$

şi constatăm că u_1, x_1, y_1, z_1 satisfac condiţiile din enunţ.

Exerciţiul 11. Fie $\varepsilon = \dfrac{-1+i\sqrt{3}}{2}$ şi $u \in \mathbb{Z}[\varepsilon]$ inversabil. Să se arate că ecuaţia

$$x^3 + y^3 = uz^3$$

nu are nici o soluţie $(x,y,z) \in \mathbb{Z}[\varepsilon] \times \mathbb{Z}[\varepsilon] \times \mathbb{Z}[\varepsilon]$ cu $xyz \neq 0$.

Soluţie: Se observă uşor că putem considera $(x,y)=(y,z)=(x,z)=1$ în $\mathbb{Z}[\varepsilon]$. Presupunând că ecuaţia din enunţ ar avea o soluţie netrivială (x,y,z), α ar divide pe xyz (vezi exerciţiul 9 a)). Atunci fie

$$\alpha \mid xy \text{ şi } \alpha \nmid z, \tag{1}$$

fie

$$\alpha \nmid xy \text{ şi } \alpha \mid z. \tag{2}$$

În cazul (1), cum α este element ireductibil, este şi prim, prin urmare $\alpha \mid x$ sau $\alpha \mid y$. Să considerăm $\alpha \mid x$, $\alpha \nmid y$ şi $\alpha \nmid z$ (celălalt caz se tratează analog). Atunci $\alpha \mid x$, $\alpha^4 \mid y^3 \pm 1$ şi $\alpha^4 \mid z^3 \pm 1$, de unde $\alpha^3 | \pm 1 \pm u$. Aplicând δ rezultă că $u \in \{-1, 1\}$, prin urmare $(-y)^3 + (\pm z)^3 = x^3$, ceea ce ne plasează, după o schimbare de notaţie, în cazul (2).

În cazul existenţei unei soluţii netriviale ce verifică (2), aplicăm exerciţiul 9 b) şi exerciţiul 10 şi existenţa unei soluţii netriviale pentru ecuaţia din enunţ revine la existenţa unei soluţii netriviale ce verifică (2) pentru ecuaţia $x_1^3 + y_1^3 = u_1 z_1^3$ cu $v_\alpha(z_1) = v_\alpha(z) - 1$ şi putem aplica din nou exerciţiile 9 b) şi 10. Continuând procedeul obţinem un şir strict decrescător infinit de numere naturale $v_\alpha(z) > v_\alpha(z_1) > \cdots$, ceea ce nu este posibil.

Exerciţiul 12. Să se arate că ecuaţia lui Fermat

$$x^3 + y^3 = z^3$$

nu are soluţii $(x,y,z) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}^*$.

Soluţie: Cum $\mathbb{Z} \subseteq \mathbb{Z}[\varepsilon]$, concluzia rezultă imediat din exerciţiul 11.