6. FELADATLAP - GYŰRŰK

1. Legyen $M \neq \emptyset$ egy halmaz és $(R, +, \cdot)$ gyűrű. Az $R^M = \{f \mid f : M \to R\}$ függvények halmazán bevezetjük a következő műveleteket: $\forall\, f, g \in R^M$ $f + g : M \to R$, $f \cdot g : M \to R$, ahol $(f+g)(x) = f(x) + g(x)$ és $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in M$. Bizonyítsuk be, hogy $(R^M, +, \cdot)$ a függvények összeadásával és szorzásával gyűrű. Igaz-e, hogy ha R egységelemes (vagy kommutatív vagy integritástartomány), akkor R^M is az?

Megoldás. Fogjuk használni, hogy értelmezés szerint két $f, g : M \to R$ függvény egyenlő, ha minden pontban egyenlő értéket vesznek fel, vagyis

$$f = g \;\Leftrightarrow\; f(x) = g(x), \quad \forall\, x \in M.$$

Leellenőrizzük, hogy az $(R^M, +, \cdot)$ teljesíti a gyűrű axiómáit.

I. $(R^M, +)$ egy Abel-csoport:

- A megadott értelmezés szerint a függvények (pontokénti) összeadása egy belső művelet az R^M-en (az $M \to R$ függvények halmazán).
- A függvények összeadása asszociatív:
  minden $f, g, h \in R^M$ (vagyis $f, g, h : M \to R$ függvények) esetén
  $$\begin{aligned} & f + (g + h) = (f + g) + h \\ \overset{\text{ért.}}{\iff}\;& (f + (g + h))(x) = ((f + g) + h)(x), \quad \forall\, x \in M \\ \iff\;& f(x) + (g + h)(x) = (f + g)(x) + h(x), \quad \forall\, x \in M \\ \iff\;& f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x), \quad \forall\, x \in M, \end{aligned}$$
  amely teljesül, mert $f(x), g(x), h(x) \in R$ és az R gyűrűben az összeadás asszociatív.
- A függvények összeadása kommutatív:
  minden $f, g \in R^M$ (vagyis $f, g : M \to R$ függvények) esetén
  $$\begin{aligned} & f + g = g + f \\ \overset{\text{ért.}}{\iff}\;& (f + g)(x) = (g + f)(x), \quad \forall\, x \in M \\ \iff\;& f(x) + g(x) = g(x) + f(x), \quad \forall\, x \in M \end{aligned}$$
  amely teljesül, mert $f(x), g(x) \in R$ és az R gyűrűben az összeadás kommutatív.
- Létezik zéruselem (semleges elem az összeadásra nézve).
  Legyen $\theta \in R^M$, $\theta(x) = 0$, minden $x \in M$ esetén, ahol $0 \in R$ az $(R, +, \cdot)$ gyűrű zéruseleme. Tehát θ a konstans 0 függvény, vagyis $\theta \equiv 0$, ezért szokták egyszerűen 0-val jelölni.
  A konstans zéró függvény az R^M zéruseleme: minden $f \in R^M$ függvény esetén $f + \theta = \theta + f = f$. A kommutativitás alapján elég az ellenőrizni, hogy minden $f \in R^M$ esetén
  $$\begin{aligned} & f + \theta = f \\ \Leftrightarrow\;& (f + \theta)(x) = f(x), \quad \forall\, x \in M \\ \Leftrightarrow\;& f(x) + \theta(x) = f(x), \quad \forall\, x \in M \\ \Leftrightarrow\;& f(x) + 0 = f(x), \quad \forall\, x \in M, \end{aligned}$$
  amely teljesül, mert $f(x) \in R$ és az R gyűrűben 0 zéruselem.
- Minden függvénynek van ellentett függvénye, vagyis R^M-ben minden elemnek van szimmetrikusa az összeadásra nézve: minden $f \in R^M$ esetén létezik $(-f) \in R^M$, úgy, hogy $f + (-f) = (-f) + f = \theta \equiv 0$. Legyen $(-f) : M \to R$, $(-f)(x) = -f(x)$,

minden $x \in M$ esetén, vagyis a $(-f)$ ellentett függvény minden pontban az f-fel ellentétes értéket vesz fel. Az összeadás kommutativitása miatt elég ellenőrizni, hogy

$$\begin{aligned} & f+(-f)=\theta \\ \Leftrightarrow\ & (f+(-f))(x)=\theta(x), \quad \forall\, x \in M \\ \Leftrightarrow\ & f(x)+(-f)(x)=0, \quad \forall\, x \in M \\ \Leftrightarrow\ & f(x)+(-f(x))=0, \quad \forall\, x \in M, \end{aligned}$$

ami teljesül, mert az R gyűrűben az $f(x) \in R$ ellentettje $-f(x)$.

II. $(R^M, \cdot)$ félcsoport:

- A megadott értelmezés szerint a függvények (pontonkénti) szorzása egy belső művelet az R^M-en.
- A függvények összeadásához hasonlóan igazoljuk, hogy a függvények szorzása asszociatív: minden $f, g, h \in R^M$ (vagyis $f, g, h : M \to R$ függvények) esetén

$$\begin{aligned} & f \cdot (g \cdot h) = (f \cdot g) \cdot h \\ \overset{\text{ért.}}{\Longleftrightarrow}\ & (f \cdot (g \cdot h))(x) = ((f \cdot g) \cdot h)(x), \quad \forall\, x \in M \\ \Longleftrightarrow\ & f(x) \cdot (g \cdot h)(x) = (f \cdot g)(x) \cdot h(x), \quad \forall\, x \in M \\ \Longleftrightarrow\ & f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x), \quad \forall\, x \in M, \end{aligned}$$

amely teljesül, mert $f(x), g(x), h(x) \in R$ és az R gyűrűben a szorzás asszociatív.

III. A függvények szorzása disztributív a függvények összeadására nézve:
minden $f, g, h \in R^M$ (vagyis $f, g, h : M \to R$ függvények) esetén

$$f \cdot (g+h) = f \cdot g + f \cdot h \quad \text{és} \quad (g+h) \cdot f = g \cdot f + h \cdot f.$$

Valóban

$$\begin{aligned} & f \cdot (g+h) = f \cdot g + f \cdot h \\ \Leftrightarrow\ & (f \cdot (g+h))(x) = (f \cdot g + f \cdot h)(x), \quad \forall\, x \in M \\ \Leftrightarrow\ & f(x) \cdot (g+h)(x) = (f \cdot g)(x) + (f \cdot h)(x), \quad \forall\, x \in M \\ \Leftrightarrow\ & f(x) \cdot (g(x)+h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x), \quad \forall\, x \in M, \end{aligned}$$

amely teljesül, mert $f(x), g(x), h(x) \in R$ és az R gyűrűben a szorzás disztributív az összeadásra nézve. Hasonlóan

$$\begin{aligned} & (g+h) \cdot f = g \cdot f + g \cdot f \\ \Leftrightarrow\ & ((g+h) \cdot f)(x) = (g \cdot f + h \cdot f)(x), \quad \forall\, x \in M \\ \Leftrightarrow\ & (g+h)(x) \cdot f(x) = (g \cdot f)(x) + (h \cdot f)(x), \quad \forall\, x \in M \\ \Leftrightarrow\ & (g(x)+h(x)) \cdot f(x) = g(x) \cdot f(x) + h(x) \cdot f(x), \quad \forall\, x \in M, \end{aligned}$$

amely teljesül, mert $f(x), g(x), h(x) \in R$ és az R gyűrűben a szorzás disztributív az összeadásra nézve.

Ezzel beláttuk, hogy ha $(R, +, \cdot)$ gyűrű, akkor $(R^M, +, \cdot)$ is gyűrű.

- Ha az R gyűrű egységelemes (vagyis van semleges eleme a szorzásra nézve), ahol $1 \in R$ az egységelem, akkor R^M is egységelemes és a konstans 1 függvény lesz az egységelem. Valóban $\varepsilon : M \to R$, $\varepsilon(x) = 1$, minden $x \in M$ az R^M gyűrű egységeleme, mivel minden $f \in R^M$ esetén

$$\varepsilon \cdot f = f \cdot \varepsilon = f$$

$$\begin{aligned}
&\Leftrightarrow\ (\varepsilon \cdot f)(x) = (f \cdot \varepsilon)(x) = f(x), \quad \forall x \in M \\
&\Leftrightarrow\ \varepsilon(x) \cdot f(x) = f(x) \cdot \varepsilon(x) = f(x), \quad \forall x \in M \\
&\Leftrightarrow\ 1 \cdot f(x) = f(x) \cdot 1 = f(x), \quad \forall x \in M,
\end{aligned}$$

ami teljesül, mert $f(x) \in R$ és 1 az R gyűrű egységeleme. Megjegyezzük, hogy az általunk ε-vel jelölt konstans 1 függvényt általában egyszerűen csak 1-gyel jelölik.

- Ha $(R, +, \cdot)$ egy kommutatív gyűrű, vagyis R-ben a szorzás kommutatív, akkor az R értékű függvények (pontokénti) szorzása is kommutatív, tehát $(R^M, +, \cdot)$ is kommutatív gyűrű lesz. Valóban, minden $f, g \in R^M$ esetén

$$\begin{aligned}
&f \cdot g = g \cdot f \\
&\Leftrightarrow\ (f \cdot g)(x) = (g \cdot f)(x), \quad \forall x \in M \\
&\Leftrightarrow\ f(x) \cdot g(x) = g(x) \cdot f(x), \quad \forall x \in M,
\end{aligned}$$

amely teljesül, mert $f(x), g(x) \in R$ és az R gyűrűben a feltevés szerint a szorzás kommutatív.

- Egy gyűrű integritástartomány, ha egységelemes, kommutatív és zérusosztómentes. Az előző két alpontban igazoltuk, hogy ha egy R gyűrű egységelemes, illetve kommutatív, akkor R^M is egységelemes, illetve kommutatív. Ezért elég azt megvizsgálni, hogy ha az R gyűrű zérusosztómentes, akkor R^M is zérusosztómentes lesz-e.

  Ha az M halmaznak egyetlen eleme van, vagyis $|M| = 1$, akkor az R és R^M gyűrűk izomorfak, így ugyanolyan tulajdonsággal rendelkeznek, tehát ebben az esetben R^M is zérusosztómentes lesz.

  Ha az M halmaznak legalább két eleme van, akkor R^M már nem lesz zérusosztómentes annak ellenére, hogy R zérusosztómentes. Valóban, legyenek $x_1, x_2 \in M$, $x_1 \neq x_2$ az M halmaz két különböző rögzített eleme. Értelmezzük az $f_1, f_2 \in R^M$ függvények úgy, hogy

$$f_1(x) = \begin{cases} 1, & \text{ha } x = x_1 \\ 0, & \text{ha } x = x_2 \\ 0, & \text{ha } x \neq x_1, x_2 \end{cases} \quad \text{és} \quad f_2(x) = \begin{cases} 0, & \text{ha } x = x_1 \\ 1, & \text{ha } x = x_2 \\ 0, & \text{ha } x \neq x_1, x_2 \end{cases}.$$

  Ekkor f_1 és f_2 nem zérusfüggvények (vagyis nem konstans zérók), de az $f_1 \cdot f_2$ zérusfüggvény, mert

$$(f_1 \cdot f_2)(x) = f_1(x) \cdot f_2(x) = \begin{cases} 1 \cdot 0, & \text{ha } x = x_1 \\ 0 \cdot 1, & \text{ha } x = x_2 \\ 0 \cdot 0, & \text{ha } x \neq x_1, x_2 \end{cases} = 0, \quad \forall x \in M.$$

Megjegyzés. Az R itt nem a valós számok halmazát jelöli (annak jelölésére az $\mathbb{R}$ karaktert használjuk). A valós számok halmaza az összeadással és szorzással gyűrűt is alkot, így egy példa az $(R, +, \cdot)$ gyűrűre lehet az $(\mathbb{R}, +, \cdot)$. Egy másik példa az $(R, +, \cdot)$ gyűrűre az $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$, ahol $\mathcal{M}_n(\mathbb{R})$ az $(n \times n)$-es valós mátrixok halmaza. Ez utóbbi gyűrű egységelemes és ha $n > 1$, akkor nem kommutatív és vannak benne zérusosztók.

□

2. Bizonyítsuk be, hogy egy egységelemes (unitér) gyűrűben az összeadás kommutativitása következik az egységelem létezéséből.

Megoldás. Legyen $1 \in R$ a gyűrű egységeleme. A gyűrű értelmezésében többek között szerepel, hogy az összeadás kommutatív. Egy pillanatra elfelejtjük, hogy ezt feltételeztük és a többi tulajdonságokból, illetve az egységelem létezéséből fogunk rá következtetni.

Minden $x, y \in R$ esetén a $(1+x)(1+y)$ szorzatot a disztributivitás segítségével kétféleképpen számíthatjuk ki:

$$(1+x)\cdot(1+y) = (1+x)\cdot 1 + (1+x)\cdot y = (1\cdot 1 + x\cdot 1) + (1\cdot y + x\cdot y) = 1 + x + y + xy,$$
$$(1+x)\cdot(1+y) = 1\cdot(1+y) + x\cdot(1+y) = (1\cdot 1 + 1\cdot y) + (x\cdot 1 + x\cdot y) = 1 + y + x + xy,$$

ahonnan kapjuk, hogy

$$\begin{aligned} -1\backslash \quad 1 + x + y + xy &= 1 + y + x + xy \quad / - xy \\ \Leftrightarrow\ -1 + 1 + x + y + xy - xy &= -1 + 1 + y + x + xy - xy \\ \Leftrightarrow\ x + y &= y + x, \end{aligned}$$

tehát az összeadás kommutativitása következik a disztributivitás, asszociativitás, illetve az egységelem és ellentett elemek létezéséből is. $\square$

3. Bizonyítsuk be, hogy ha az R gyűrűben teljesül az $x^2 = x$ egyenlőség minden $x \in R$ elemre, akkor a gyűrű kommutatív.

Megoldás. Minden $x, y \in R$ esetén $(x+y)^2 = (x+y)(x+y) = (x+y)x + (x+y)y = x^2 + yx + xy + y^2$, továbbá a feltevést használva az $(x+y)$, illetve az x és y elemekre kapjuk, hogy

$$\begin{aligned} (x+y)^2 &= x + y \\ \Leftrightarrow\ x^2 + yx + xy + y^2 &= x^2 + y^2 \quad / - (x^2 + y^2) \\ \Leftrightarrow\ yx + xy &= 0 \\ \Leftrightarrow\ yx &= -xy. \end{aligned} \tag{1}$$

Ez utóbbi egyenlőségben x és y-t z-nek választva kapjuk, hogy $z^2 = zz = -zz = -z^2$, minden $z \in R$ esetén. A feltevést is felhasználva kapjuk, hogy $z = z^2 = -z^2 = -z$, minden $z \in R$ esetén, tehát

$$z = -z, \qquad \forall z \in R. \tag{2}$$

Az (1) és (2) összefüggések alapján minden $x, y \in R$ esetén $xy = -xy = xy$, vagyis az R gyűrű kommutatív. $\square$

4. Igazoljuk, hogy a következő struktúrák $\mathbb{C}$-vel izomorf testek:

(a) $(\mathbb{R} \times \mathbb{R}, +, \cdot)$, ahol $(x, y) + (a, b) = (x + a, y + b)$ és $(x, y)(a, b) = (xa - yb, ya + xb)$.

(b) $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$ a mátrixok összeadásával és szorzásával.

Megoldás.

(a) • $\mathbb{R} \times \mathbb{R}$-en a „+” asszociatív:
minden $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R} \times \mathbb{R}$ esetén

$$\begin{aligned} [(x_1, y_1) + (x_2, y_2)] + (x_3, y_3) &= (x_1 + x_2, y_1 + y_2) + (x_3, y_3) \\ &= ([x_1 + x_2] + x_3, [y_1 + y_2] + y_3) \\ &\overset{(*)}{=} (x_1 + [x_2 + x_3], y_1 + [y_2 + y_3]) \end{aligned}$$

$$= (x_1, y_1) + (x_2 + x_3, y_2 + y_3)$$
$$= (x_1, y_1) + [(x_2, y_2) + (x_3, y_3)],$$

ahol a $(*)$ egyenlőségbe kihasználtuk, hogy $x_1, x_2, x_3 \in \mathbb{R}$, $y_1, y_2, y_3 \in \mathbb{R}$ és az összeadás asszociatív az $\mathbb{R}$-en.

- $\mathbb{R} \times \mathbb{R}$-en a „+” kommutatív:
  minden $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$ esetén

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \overset{(\dagger)}{=} (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1),$$

  ahol a $(\dagger)$ egyenlőségbe kihasználtuk, hogy $x_1, x_2 \in \mathbb{R}$, $y_1, y_2 \in \mathbb{R}$ és az összeadás kommutatív az $\mathbb{R}$-en.

- Az $\mathbb{R} \times \mathbb{R}$-ben a $(0, 0)$ zéruselem (semleges elem az összeadásra nézve):
  minden $(x, y) \in \mathbb{R} \times \mathbb{R}$ esetén

$$(x, y) + (0, 0) = (x + 0, y + 0) = (x, y) = (0 + x, 0 + y) = (0, 0) + (x, y),$$

  mivel 0 az $\mathbb{R}$ zéruseleme (semleges elem az összeadásra nézve).

- Minden $(x, y) \in \mathbb{R} \times \mathbb{R}$ elemnek van ellentettje (szimmetrikus a „+” nézve), éspedig $-(x, y) := (-x, -y) \in \mathbb{R} \times \mathbb{R}$. Valóban

$$(x, y) + (-x, -y) = (x + (-x), y + (-y)) = (0, 0) = ((-x) + x, (-y) + y) = (-x, -y) + (x, y),$$

  mivel $(-x)$, illetve $(-y)$ az x, illetve y ellentettjei az $\mathbb{R}$-ben.

- $\mathbb{R} \times \mathbb{R}$-en a „$\cdot$” asszociatív:
  minden $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R} \times \mathbb{R}$ esetén

$$[(x_1, y_1) \cdot (x_2, y_2)] \cdot (x_3, y_3) = (x_1x_2 - y_1y_2, y_1x_2 + x_1y_2) \cdot (x_3, y_3) =$$
$$= ([x_1x_2 - y_1y_2]x_3 - [y_1x_2 + x_1y_2]y_3,\ [x_1x_2 - y_1y_2]y_3 + [y_1x_2 + x_1y_2]x_3) =$$
$$= (x_1x_2x_3 - y_1y_2x_3 - y_1x_2y_3 - x_1y_2y_3,\ x_1x_2y_3 - y_1y_2y_3 + y_1x_2x_3 + x_1y_2x_3),$$

  (felhasználtuk, hogy az $\mathbb{R}$-en a disztributivitást és a szorzás asszociativitását), illetve

$$(x_1, y_1) \cdot [(x_2, y_2) \cdot (x_3, y_3)] = (x_1, y_1) \cdot (x_2x_3 - y_2y_3, y_2x_3 + x_2y_3)$$
$$= (x_1[x_2x_3 - y_2y_3] - y_1[y_2x_3 + x_2y_3],\ y_1[x_2x_3 - y_2y_3] + x_1[y_2x_3 + x_2y_3]) =$$
$$= (x_1x_2x_3 - x_1y_2y_3 - y_1y_2x_3 - y_1x_2y_3,\ y_1x_2x_3 - y_1y_2y_3 + x_1x_2y_3 + x_1y_2x_3) =$$
$$= (x_1x_2x_3 - y_1y_2x_3 - y_1x_2y_3 - x_1y_2y_3,\ x_1x_2y_3 - y_1y_2y_3 + y_1x_2x_3 + x_1y_2x_3),$$

  (felhasználtuk, hogy az $\mathbb{R}$-en a disztributivitást, a szorzás asszociativitását és az összeadás kommutativitását), ahonnan következik, hogy

$$[(x_1, y_1) \cdot (x_2, y_2)] \cdot (x_3, y_3) = (x_1, y_1) \cdot [(x_2, y_2) \cdot (x_3, y_3)].$$

- $\mathbb{R} \times \mathbb{R}$-en a „$\cdot$” disztributív az „+” nézve:
  minden $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R} \times \mathbb{R}$ esetén

$$(x_1, y_1) \cdot [(x_2, y_2) + (x_3, y_3)] = (x_1, y_1) \cdot (x_2 + x_3, y_2 + y_3) =$$
$$= (x_1[x_2 + x_3] - y_1[y_2 + y_3],\ y_1[x_2 + x_3] + x_1[y_2 + y_3]) =$$
$$= (x_1x_2 + x_1x_3 - y_1y_2 - y_1y_3,\ y_1x_2 + y_1x_3 + x_1y_2 + x_1y_3) =$$
$$= (x_1x_2 - y_1y_2, y_1x_2 + x_1y_2) + (x_1x_3 - y_1y_3,\ y_1x_3 + x_1y_3) =$$
$$= (x_1, y_1) \cdot (x_2, y_2) + (x_1, y_1) \cdot (x_3, y_3)$$

  és hasonlóan

$$[(x_2, y_2) + (x_3, y_3)] \cdot (x_1, y_1) = (x_2 + x_3, y_2 + y_3) \cdot (x_1, y_1) =$$

$$= ([x_2 + x_3]x_1 - [y_2 + y_3]y_1,\ [x_2 + x_3]y_1 + [y_2 + y_3]x_1) =$$
$$= (x_2x_1 + x_3x_1 - y_2y_1 - y_3y_1,\ x_2y_1 + x_3y_1 + y_2x_1 + y_3x_1) =$$
$$= (x_2x_1 - y_2y_1, x_2y_1 + y_2x_1) + (x_3x_1 - y_3y_1,\ x_3y_1 + y_3x_1) =$$
$$= (x_2, y_2) \cdot (x_1, y_1) + (x_3, y_3) \cdot (x_1, y_1).$$

- Az $\mathbb{R} \times \mathbb{R}$ gyűrűben $(1,0)$ egységelem:
  minden $(x, y) \in \mathbb{R} \times \mathbb{R}$ esetén

$$(x, y) \cdot (1, 0) = (x \cdot 1 - y \cdot 0, y \cdot 1 + x \cdot 0) = (x, y) = (1 \cdot x - 0 \cdot y, 0 \cdot x + 1 \cdot y) = (1, 0) \cdot (x, y).$$

- Minden $(x, y) \in \mathbb{R} \times \mathbb{R}$, $(x, y) \neq (0, 0)$ elem invertálható, vagyis létezik $(x, y)^{-1} = (x', y') = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$ úgy, hogy $(x, y) \cdot (x', y') = (x', y') \cdot (x, y) = (1, 0)$. Valóban,

$$\begin{aligned}
(x, y) \cdot (x', y') &= (xx' - yy', xy' + yx') \\
&= \left(x\frac{x}{x^2+y^2} - y\frac{-y}{x^2+y^2},\ x\frac{-y}{x^2+y^2} + y\frac{x}{x^2+y^2}\right) \\
&= \left(\frac{x^2+y^2}{x^2+y^2}, \frac{-xy+yx}{x^2+y^2}\right) \\
&= (1, 0), \\
(x', y') \cdot (x, y) &= (x'x - y'y, x'y + y'x) \\
&= \left(\frac{x}{x^2+y^2}x - \frac{-y}{x^2+y^2}y,\ \frac{x}{x^2+y^2}y + \frac{-y}{x^2+y^2}x\right) \\
&= \left(\frac{x^2+y^2}{x^2+y^2}, \frac{xy-yx}{x^2+y^2}\right) \\
&= (1, 0).
\end{aligned}$$

Ezzel beláttuk, hogy $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ test.

Tekintsük az $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$, $f(x, y) = x + iy$ bijektív függvényt. Ekkor minden $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$ esetén

$$\begin{aligned}
f((x_1, y_1) + (x_2, y_2)) &= f(x_1 + x_2, y_1 + y_2) \\
&= (x_1 + x_2) + i(y_1 + y_2) \\
&= (x_1 + iy_1) + (x_2 + iy_2) \\
&= f(x_1, y_1) + f(x_2, y_2), \\
f((x_1, y_1) \cdot (x_2, y_2)) &= f(x_1x_2 - y_1y_2, y_1x_2 + x_1y_2) \\
&= (x_1x_2 - y_1y_2) + i(y_1x_2 + x_1y_2) \\
&= (x_1 + iy_1) \cdot (x_2 + iy_2) \\
&= f(x_1, y_1) \cdot f(x_2, y_2),
\end{aligned}$$

tehát $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ egy testizomorfizmus.

(b) A K az $(\mathcal{M}_2(\mathbb{R}), +, \cdot)$ gyűrű egy részgyűrűje, mert

- $O_2 = \begin{pmatrix} 0 & 0 \\ -0 & 0 \end{pmatrix} \in K$, ezért $K \neq \emptyset$;

- minden $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K$ esetén
$$A - B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -(b-d) & a-c \end{pmatrix} \in K;$$
- minden $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K$ esetén
$$A \cdot B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \in K.$$

A $(K, +, \cdot)$ gyűrű egységelemes, mert $I_2 = \begin{pmatrix} 1 & 0 \\ -0 & 1 \end{pmatrix} \in K$, továbbá minden $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq O_2$ esetén $A^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in K$. Tehát $(K, +, \cdot)$ egy test.

Végül, tekintsük a $g : K \to \mathbb{C}$, $g \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + ib$ bijektív függvényt. Ekkor minden $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in K$ esetén
$$\begin{aligned} g\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= g\begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \\ &= (a+c) + i(b+d) = (a+ib) + (c+id) \\ &= g\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + g\begin{pmatrix} c & d \\ -d & c \end{pmatrix}, \end{aligned}$$
illetve
$$\begin{aligned} g\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= g\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} \\ &= (ac-bd) + i(ad+bc) = (a+ib) \cdot (c+id) \\ &= g\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot g\begin{pmatrix} c & d \\ -d & c \end{pmatrix}, \end{aligned}$$
ezért $g : K \to \mathbb{C}$ egy testizomorfizmus.

□

5. Ha $k \in \mathbb{Z}$, legyen $A_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \middle| \, a, b \in \mathbb{Z} \right\}$. Igazoljuk,hogy:

(a) $(A_k, +, \cdot)$ kommutatív egységelemes gyűrű ($A_k \leq \mathcal{M}_2(\mathbb{Z})$).

(b) A_k integritástartomány $\Leftrightarrow$ k nem teljes négyzet.

Megoldás.

(a) • Minden $k \in \mathbb{Z}$ esetén $A_k \neq \emptyset$, mert $O_2 = \begin{pmatrix} 0 & 0 \\ k \cdot 0 & 0 \end{pmatrix} \in A_k$.

- Minden $B = \begin{pmatrix} a & b \\ kb & a \end{pmatrix}, C = \begin{pmatrix} c & d \\ kd & c \end{pmatrix} \in A_k$ mátrix esetén

$$B - C = \begin{pmatrix} a & b \\ kb & a \end{pmatrix} - \begin{pmatrix} c & d \\ kd & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ kb-kd & a-c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ k(b-d) & a-c \end{pmatrix} \in A_k.$$

- Minden $B = \begin{pmatrix} a & b \\ kb & a \end{pmatrix}, C = \begin{pmatrix} c & d \\ kd & c \end{pmatrix} \in A_k$ mátrix esetén

$$B \cdot C = \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ kd & c \end{pmatrix} = \begin{pmatrix} ac+bkd & ad+bc \\ kbc+akd & kbd+ac \end{pmatrix} = \begin{pmatrix} ac+kbd & ad+bc \\ k(ad+bc) & ac+kbd \end{pmatrix} \in A_k.$$

A fenti három pont alapján A_k részgyűrűje az $\mathcal{M}_2(\mathbb{Z})$ gyűrűnek.

Mivel az $\mathcal{M}_2(\mathbb{Z})$ gyűrű egységeleme felírható mint $I_2 = \begin{pmatrix} 1 & 0 \\ k \cdot 0 & 1 \end{pmatrix}$, ezért $I_2 \in A_k$, minden $k \in \mathbb{Z}$ esetén. Tehát A_k egységelemes gyűrű.

Minden $B = \begin{pmatrix} a & b \\ kb & a \end{pmatrix}, C = \begin{pmatrix} c & d \\ kd & c \end{pmatrix} \in A_k$ mátrix esetén

$$B \cdot C = \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ kd & c \end{pmatrix} = \begin{pmatrix} ac+bkd & ad+bc \\ kbc+akd & kbd+ac \end{pmatrix} = \begin{pmatrix} ac+kbd & ad+bc \\ k(ad+bc) & ac+kbd \end{pmatrix},$$

$$C \cdot B = \cdot \begin{pmatrix} c & d \\ kd & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ kb & a \end{pmatrix} = \begin{pmatrix} ca+dkb & cb+da \\ kda+ckb & kdb+ca \end{pmatrix} = \begin{pmatrix} ac+kbd & ad+bc \\ k(ad+bc) & ac+kbd \end{pmatrix},$$

ahonnan $BC = CB$, tehát az A_k gyűrű kommutatív.

(b) Az A_k gyűrű integritástartomány, ha kommutatív, egységelemes és nincsenek benne zérusosztók. Ez alapján elég igazolni, hogy A_k-ban nincsenek zérusosztók pontosan akkor, ha k nem teljes négyzet. Ez az állítás egyenértékű a következővel:

$$A_k\text{-ban vannak zérusosztók} \quad \Leftrightarrow \quad k \text{ teljes négyzet.}$$

$\boxed{\Rightarrow}$ Legyenek $B = \begin{pmatrix} a & b \\ kb & a \end{pmatrix}$, $C = \begin{pmatrix} c & d \\ kd & c \end{pmatrix} \in A_k$ úgy, hogy $B, C \neq O_2$, de $B \cdot C = O_2$ (vagyis B, C zérusosztók). Ekkor

(3) $$B \neq O_2 \;\Leftrightarrow\; (a,b) \neq (0,0), \quad \text{illetve} \quad C \neq O_2 \;\Leftrightarrow\; (c,d) \neq (0,0),$$

továbbá

$$B \cdot C = O_2 \;\Leftrightarrow\; \begin{pmatrix} ac+kbd & ad+bc \\ k(ad+bc) & ac+kbd \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(4) $$\Leftrightarrow\; ac + kbd = 0 \text{ és } ad + bc = 0.$$

Ki fogjuk fejezni a k-t az első egyenlőségből. Ehhez majd osztanunk kell bd-vel. Ha $b = 0$, akkor a (3) alapján $a \neq 0$ és a (4) alapján $ac = 0$ és $ad = 0$, ahonnan $c = 0$ és $d = 0$ adódik, ami ellentmond a $(c,d) \neq (0,0)$ feltevésnek. Tehát $b \neq 0$. Ha $d = 0$, akkor a (4) alapján $bc = 0$, továbbá $b \neq 0$, így $c = 0$, ami ellentmond a $(c,d) \neq (0,0)$ feltevésnek. Tehát $d \neq 0$. A (4) második egyenlőségéből kapjuk, hogy $c = -\dfrac{ad}{b}$, míg az első egyenlőségéből kapjuk, hogy

$$k = -\frac{ac}{bd} = \frac{a^2 d}{b^2 d} = \left(\frac{a}{b}\right)^2 \in \mathbb{Z}.$$

Mivel $k \in \mathbb{Z}$, ezért $\dfrac{a}{b} \in \mathbb{Z}$, tehát k teljes négyzet.

$\boxed{\Leftarrow}$ Ha $k = n^2$ teljes négyzet, akkor az A_{n^2} gyűrűben vannak zérusosztók:
$B = \begin{pmatrix} n & 1 \\ n^2 & n \end{pmatrix}$, $C = \begin{pmatrix} n & -1 \\ -n^2 & n \end{pmatrix} \in A_{n^2}$ és $B, C \neq O_2$, de

$$B \cdot C = \begin{pmatrix} n & 1 \\ n^2 & n \end{pmatrix} \cdot \begin{pmatrix} n & -1 \\ -n^2 & n \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

□

6. Legyen R egy gyűrű, $X \subseteq R$ nem üres részhalmaz és $C_R(X) = \{r \in R \,|\, rx = xr, \ \forall x \in X\}$ az X centralizátora. Igazoljuk, hogy $C_R(X) \leq R$, továbbá, hogy ha R test, akkor $C_R(X)$ résztest.

Megoldás.

- A $C_R(X)$ halmaz nem üres, mert $0 \cdot x = x \cdot 0 = 0$, minden $x \in X$ esetén.
- Minden $r_1, r_2 \in C_R(X)$ esetén értelmezés szerint fennállnak a következő összefüggések:

(5) $$r_1 x = x r_1, \quad \forall x \in X.$$

és

(6) $$r_2 x = x r_2, \quad \forall x \in X.$$

Az (5) és (6) összefüggések megfelelő oldalait kivonva egymásból kapjuk, hogy

$$r_1 x - r_2 x = x r_1 - x r_2, \quad \forall x \in X,$$

amely egyenértékű a disztributivitásss alapján az

$$(r_1 - r_2)x = x(r_1 - r_2), \quad \forall x \in X$$

relációval, ahonnan kapjuk, hogy $r_1 - r_2 \in C_R(X)$.
- Minden $r_1, r_2 \in C_R(X)$ esetén az (5) összefüggést jobbról szorozva r_2-vel és a (6) összefüggést pedig balról szorozva r_1-vel (a szorzás asszociativitása alapján) kapjuk, hogy

$$r_1 x r_2 = x r_1 r_2 \quad \text{és} \quad r_1 r_2 x = r_1 x r_2, \quad \forall x \in X,$$

ahonnan adódik, hogy $r_1 r_2 x = x r_1 r_2$, minden $x \in X$, vagyis $r_1 r_2 \in C_X(R)$.

A fenti három pont alapján a $C_X(R)$ részgyűrűje az R gyűrűnek.

Végül, ha R egy test és $1 \in R$ az egységeleme, akkor be látjuk, hogy $1 \in C_X(R)$, illetve minden $r \in C_R(X)$ esetén $r^{-1} \in C_R(X)$, tehát $C_X(R)$ részeste R-nek (s így sajátosan test is). Az egységelem tulajdonsága alapján $1 \cdot x = x \cdot 1 = x$, minden $x \in X$ esetén, tehát $1 \in C_R(X)$. Minden $r \in C_R(X)$ esetén értelmezés alapján

$$rx = xr, \quad \forall x \in X.$$

Ezt az összefüggést jobbról is és balról is szorozva r^{-1}-zel kapjuk, hogy

$$\underbrace{r^{-1}r}_{1} x r^{-1} = r^{-1} x \underbrace{r r^{-1}}_{1} \Leftrightarrow 1 \cdot x r^{-1} = r^{-1} x \cdot 1 \Leftrightarrow x r^{-1} = r^{-1} x, \quad \forall x \in X,$$

vagyis $r^{-1} \in C_R(X)$. □

7. Legyen $n \in \mathbb{N}$, $n \geq 2$ és a $(\mathbb{Z}_n, +, \cdot)$ gyűrű. Igazoljuk, hogy $\forall \widehat{a} \in \mathbb{Z}_n^*$ esetén $\widehat{a}$ invertálható $\Leftrightarrow$ lnko, $(a, n) = 1$. Igazoljuk azt is, hogy $(\mathbb{Z}_n, +, \cdot)$ akkor és csak akkor test, ha n prímszám.

8. Invertálható-e $\widehat{490}$ a $\mathbb{Z}_{2013}$ gyűrűben? Ha igen, adjuk meg az inverzét!

Megoldás. A $\widehat{490}$ pontosan akkor invertálható a $\mathbb{Z}_{2013}$ gyűrűben, ha $(490, 2013) = 1$ (vagyis relatív prímek). Kiszámoljuk a 490 és 2013 legnagyobb közös osztóját az euklidészi algoritmussal. Ehhez elosztjuk a 2013-at maradékosan 490-nel, majd megismételjük újra a maradékos osztást az osztóval és a maradékkal, ameddig 0 maradékot nem kapunk:

$$2013 = 4 \cdot 490 + 53, \tag{7}$$
$$490 = 9 \cdot 53 + 13, \tag{8}$$
$$53 = 4 \cdot 13 + 1, \tag{9}$$
$$13 = 13 \cdot 1 + 0. \tag{10}$$

Az utolsó nem nulla mararadék a legnagyobb közös osztó, vagyis $1 = (2013, 490)$, ezért a $\widehat{490}$ invertálható a $\mathbb{Z}_{2013}$ gyűrűben.

Az inverz kiszámításához a fenti maradékos osztásokból alulról felfele haladva kifejezzük a maradékokat, majd a kapott összefüggésekben sorra helyettesítjük a (baloldalon álló) legkisebb maradékot. A (9) egyenlőségből kifejezve a maradékot kapjuk, hogy

$$1 = 53 - 4 \cdot 13. \tag{11}$$

A (8) egyenlőségből kifejezzük a $13 = 490 - 9 \cdot 53$ maradékot és behelyettesítjük a (11) egyenlőségbe:

$$\begin{aligned} 1 &= 53 - 4 \cdot (490 - 9 \cdot 53) \\ &= -4 \cdot 490 + 37 \cdot 53. \end{aligned} \tag{12}$$

Most a (7) egyenlőségből kifejezzük az $53 = 2013 - 4 \cdot 490$ maradékot és behelyettesítjük a (13) egyenlőségbe:

$$\begin{aligned} 1 &= -4 \cdot 490 + 37 \cdot (2013 - 4 \cdot 490) \\ &= 37 \cdot 2013 - 152 \cdot 490. \end{aligned} \tag{13}$$

Tehát azt kaptuk, hogy $1 = 37 \cdot 2013 - 152 \cdot 490$, (ellenőrzésképpen a jobb oldalon elvégezve a műveleteket nézzük meg, hogy valóban teljesül-e az egyenlőség). Ez alapján írhatjuk, hogy

$$\begin{aligned} & \widehat{1} = \widehat{37} \cdot \widehat{2013} - \widehat{152} \cdot \widehat{490} \in \mathbb{Z}_{2013} \\ \Leftrightarrow\ & \widehat{1} = \widehat{-152} \cdot \widehat{490} \in \mathbb{Z}_{2013} \\ \Leftrightarrow\ & \widehat{1} = (\widehat{2013 - 152}) \cdot \widehat{490} \in \mathbb{Z}_{2013} \\ \Leftrightarrow\ & \widehat{1} = \widehat{1861} \cdot \widehat{490} \in \mathbb{Z}_{2013}. \end{aligned}$$

Az utolsó összefüggés azt jelenti, hogy $\widehat{490}^{-1} = \widehat{1861}$ a $\widehat{490}$ inverze a $\mathbb{Z}_{2013}$ gyűrűben. $\square$

9. Invertálhatók-e a következő elemek a megadott gyűrűben? Ha igen, számoljuk ki az inverzüket az euklideszi algoritmus segítségével.

(a) $\widehat{71} \in \mathbb{Z}_{1345}$;

Megoldás. Megvizsgáljuk, hogy invertálható-e a $\widehat{71}$ a $\mathbb{Z}_{1345}$ gyűrűben, vagyis 71 és 1345 relatív prímek-e:

$$\underline{1345} = 18 \cdot \underline{71} + \underline{67} \tag{14}$$
$$\underline{71} = 1 \cdot \underline{67} + \underline{4} \tag{15}$$
$$\underline{67} = 16 \cdot \underline{4} + \underline{3} \tag{16}$$
$$\underline{4} = 1 \cdot \underline{3} + \underline{1} \tag{17}$$
$$\underline{3} = 3 \cdot \underline{1} + \underline{0} \tag{18}$$

(Azért vannak az osztandók, osztók és maradékok aláhúzva, hogy az algoritmus második felébe ne végezzük el velük a szorzást.) Mivel az utolsó nem nulla maradék 1, ezért $(1345, 71) = 1$ és $\widehat{71}$ invertálható a $\mathbb{Z}_{1345}$ gyűrűben.

Az inverz kiszámításához a (17) egyenlőségből kifejezzük az 1 maradékot:

$$1 = \underline{4} - 1 \cdot \underline{3}.$$

A (16) egyenlőségből kifejezzük a 3 maradékot ($\underline{3} = \underline{67} - 16 \cdot \underline{4}$) és behelyettesítjük a fenti egyenlőségbe:

$$\begin{aligned} 1 &= \underline{4} - 1 \cdot (\underline{67} - 16 \cdot \underline{4}) \\ &= -1 \cdot \underline{67} + 17 \cdot \underline{4}. \end{aligned}$$

A (15) egyenlőségből kifejezzük a 4 maradékot ($\underline{4} = \underline{71} - 1 \cdot \underline{67}$) és behelyettesítjük a fenti egyenlőségbe:

$$\begin{aligned} 1 &= -1 \cdot \underline{67} + 17 \cdot (\underline{71} - 1 \cdot \underline{67}) \\ &= 17 \cdot \underline{71} - 18 \cdot \underline{67}. \end{aligned}$$

Végül a (14) egyenlőségből kifejezzük a 67 maradékot ($67 = \underline{1345} - 18 \cdot \underline{71}$) és behelyettesítjük a fenti egyenlőségbe:

$$\begin{aligned} 1 &= 17 \cdot \underline{71} - 18 \cdot (\underline{1345} - 18 \cdot \underline{71}) \\ &= -18 \cdot \underline{1345} + 341 \cdot \underline{71}. \end{aligned}$$

Tehát $1 = -18 \cdot 1345 + 341 \cdot 71$, ahonnan

$$\begin{aligned} & \widehat{1} = \widehat{-18} \cdot \widehat{1345} + \widehat{341} \cdot \widehat{71} \in \mathbb{Z}_{1345} \\ \Leftrightarrow\ & \widehat{1} = \widehat{341} \cdot \widehat{71} \in \mathbb{Z}_{1345}, \end{aligned}$$

ezért $\widehat{71}^{-1} = \widehat{341} \in \mathbb{Z}_{1345}$ az inverz. □

(b) $\widehat{71} \in \mathbb{Z}_{1346}$;

Megoldás. Megvizsgáljuk, hogy invertálható-e a $\widehat{71}$ a $\mathbb{Z}_{1345}$ gyűrűben, vagyis 71 és 1345 relatív prímek-e:

$$\begin{aligned} \underline{1346} &= 18 \cdot \underline{71} + \underline{68} \\ \underline{71} &= \ \ 1 \cdot \underline{68} + \underline{3} \\ \underline{68} &= 22 \cdot \underline{3} \ \ + \underline{2} \\ \underline{3} &= \ \ 1 \cdot \underline{2} \ \ + \underline{1} \\ \underline{2} &= \ \ 2 \cdot \underline{1} \ \ + \underline{0} \end{aligned}$$

(Azért vannak az osztandók, osztók és maradékok aláhúzva, hogy az algoritmus második felébe ne végezzük el velük a szorzást.) Mivel az utolsó nem nulla maradék 1, ezért $(1346, 71) = 1$ és $\widehat{71}$ invertálható a $\mathbb{Z}_{1346}$ gyűrűben.

Az inverz kiszámolásához ki fogjuk fejezni a legnagyobb közös osztót (az 1-et) az 1346 és 71 segítségével a következő módon:

$$\begin{aligned} 1 &= \underline{3} - 1 \cdot \underline{2} \\ &= \underline{3} - 1 \cdot (\underline{68} - 22 \cdot \underline{3}) \\ &= -1 \cdot \underline{68} + 23 \cdot \underline{3} \\ &= -1 \cdot \underline{68} + 23 \cdot (\underline{71} - 1 \cdot \underline{68}) \\ &= 23 \cdot \underline{71} - 24 \cdot \underline{68} \end{aligned}$$

$$= 23 \cdot \underline{71} - 24 \cdot (\underline{1346} - 18 \cdot \underline{71})$$
$$= -24 \cdot \underline{1346} + 455 \cdot \underline{71}.$$

Tehát azt kaptuk, hogy $1 = -24 \cdot 1346 + 455 \cdot 71$, ahonnan

$$\widehat{1} = \widehat{-24} \cdot \widehat{1346} + \widehat{455} \cdot \widehat{71} \in \mathbb{Z}_{1346}$$
$$\Leftrightarrow \ \widehat{1} = \widehat{455} \cdot \widehat{71} \in \mathbb{Z}_{1346},$$

tehát $\widehat{71}^{-1} = \widehat{455} \in \mathbb{Z}_{1346}$ az inverz. $\square$

(c) $\widehat{37} \in \mathbb{Z}_{2346}$;

Megoldás. Megvizsgáljuk, hogy invertálható-e a $\widehat{37}$ a $\mathbb{Z}_{2346}$ gyűrűben, vagyis 37 és 2346 relatív prímek-e:

$$\begin{aligned} \underline{2346} &= 63 \cdot \underline{37} + \underline{15} \\ \underline{37} &= \ \ 2 \cdot \underline{15} + \underline{7} \\ \underline{15} &= \ \ 2 \cdot \underline{7} \ \ + \underline{1} \\ \underline{7} &= \ \ 7 \cdot \underline{1} \ \ + \underline{0} \end{aligned}$$

(Azért vannak az osztandók, osztók és maradékok aláhúzva, hogy az algoritmus második felébe ne végezzük el velük a szorzást.) Mivel az utolsó nem nulla maradék 1, ezért $(2346, 37) = 1$ és $\widehat{37}$ invertálható a $\mathbb{Z}_{2346}$ gyűrűben.

Az inverz kiszámolásához ki fogjuk fejezni a legnagyobb közös osztót (az 1-et) az 2346 és 37 segítségével a következő módon:

$$\begin{aligned} 1 &= \underline{15} - 2 \cdot \underline{7} \\ &= \underline{15} - 2 \cdot (\underline{37} - 2 \cdot \underline{15}) \\ &= -2 \cdot \underline{37} + 5 \cdot \underline{15} \\ &= -2 \cdot \underline{37} + 5 \cdot (\underline{2346} - 63 \cdot \underline{37}) \\ &= 5 \cdot \underline{2346} - 317 \cdot \underline{37} \end{aligned}$$

Tehát azt kaptuk, hogy $1 = 5 \cdot 2346 - 317 \cdot 37$, ahonnan

$$\widehat{1} = \widehat{5} \cdot \widehat{2346} - \widehat{317} \cdot \widehat{37} \in \mathbb{Z}_{2346}$$
$$\Leftrightarrow \ \widehat{1} = \widehat{-317} \cdot \widehat{37} \in \mathbb{Z}_{2346}$$
$$\Leftrightarrow \ \widehat{1} = \widehat{(2346 - 317)} \cdot \widehat{37} \in \mathbb{Z}_{2346}$$
$$\Leftrightarrow \ \widehat{1} = \widehat{2029} \cdot \widehat{37} \in \mathbb{Z}_{2346},$$

tehát $\widehat{37}^{-1} = \widehat{2029} \in \mathbb{Z}_{2346}$ az inverz. $\square$

(d) $\widehat{741} \in \mathbb{Z}_{2423}$;

Megoldás. Megvizsgáljuk, hogy invertálható-e a $\widehat{741}$ a $\mathbb{Z}_{2423}$ gyűrűben, vagyis 741 és 2423 relatív prímek-e:

$$\begin{aligned} \underline{2423} &= 3 \cdot \underline{741} + \underline{200} \\ \underline{741} &= 3 \cdot \underline{200} + \underline{141} \\ \underline{200} &= 1 \cdot \underline{141} + \underline{59} \\ \underline{141} &= 2 \cdot \underline{59} \ \ + \underline{23} \\ \underline{59} &= 2 \cdot \underline{23} \ \ + \underline{13} \\ \underline{23} &= 1 \cdot \underline{13} \ \ + \underline{10} \end{aligned}$$

$$\begin{aligned}
\underline{13} &= 1 \cdot \underline{10} + \underline{3}\\
\underline{10} &= 3 \cdot \underline{3} + \underline{1}\\
\underline{3} &= 3 \cdot \underline{1} + \underline{0}.
\end{aligned}$$

(Azért vannak az osztandók, osztók és maradékok aláhúzva, hogy az algoritmus második felébe ne végezzük el velük a szorzást.) Mivel az utolsó nem nulla maradék 1, ezért $(2423, 741) = 1$ és $\widehat{741}$ invertálható a $\mathbb{Z}_{2423}$ gyűrűben.

Az inverz kiszámolásához ki fogjuk fejezni a legnagyobb közös osztót (az 1-et) az 2423 és 741 segítségével a következő módon:

$$\begin{aligned}
1 &= \underline{10} - 3 \cdot \underline{3}\\
&= \underline{10} - 3 \cdot (\underline{13} - 1 \cdot \underline{10})\\
&= -3 \cdot \underline{13} + 4 \cdot \underline{10}\\
&= -3 \cdot \underline{13} + 4 \cdot (\underline{23} - 1 \cdot \underline{13})\\
&= 4 \cdot \underline{23} - 7 \cdot \underline{13}\\
&= 4 \cdot \underline{23} - 7 \cdot (\underline{59} - 2 \cdot \underline{23})\\
&= -7 \cdot \underline{59} + 18 \cdot \underline{23}\\
&= -7 \cdot \underline{59} + 18 \cdot (\underline{141} - 2 \cdot \underline{59})\\
&= 18 \cdot \underline{141} - 43 \cdot \underline{59}\\
&= 18 \cdot \underline{141} - 43 \cdot (\underline{200} - 1 \cdot \underline{141})\\
&= -43 \cdot \underline{200} + 61 \cdot \underline{141}\\
&= -43 \cdot \underline{200} + 61 \cdot (\underline{741} - 3 \cdot \underline{200})\\
&= 61 \cdot \underline{741} - 226 \cdot \underline{200}\\
&= 61 \cdot \underline{741} - 226 \cdot (\underline{2423} - 3 \cdot \underline{741})\\
&= -226 \cdot \underline{2423} + 739 \cdot \underline{741}.
\end{aligned}$$

Tehát azt kaptuk, hogy $1 = -226 \cdot 2423 + 739 \cdot 741$, ahonnan

$$\begin{aligned}
&\widehat{1} = -\widehat{226} \cdot \widehat{2423} + \widehat{739} \cdot \widehat{741} \in \mathbb{Z}_{2423}\\
\Leftrightarrow\ &\widehat{1} = \widehat{871} \cdot \widehat{739} \in \mathbb{Z}_{2423},
\end{aligned}$$

tehát $\widehat{741}^{-1} = \widehat{739} \in \mathbb{Z}_{2423}$ az inverz. □

(e) $\widehat{429} \in \mathbb{Z}_{3553}$;

Megoldás. Megvizsgáljuk, hogy invertálható-e a $\widehat{429}$ a $\mathbb{Z}_{3553}$ gyűrűben, vagyis 429 és 3553 relatív prímek-e:

$$\begin{aligned}
\underline{3553} &= 8 \cdot \underline{429} + \underline{121}\\
\underline{429} &= 3 \cdot \underline{121} + \underline{66}\\
\underline{121} &= 1 \cdot \underline{66} + \underline{55}\\
\underline{66} &= 1 \cdot \underline{55} + \underline{11}\\
\underline{55} &= 1 \cdot \underline{11} + \underline{0}
\end{aligned}$$

Mivel az utolsó nem nulla maradék 11, ezért $(2346, 37) = 11 \neq 1$, ezért a $\widehat{429}$ nem invertálható a $\mathbb{Z}_{3553}$ gyűrűben. □

(f) $\widehat{428} \in \mathbb{Z}_{3553}$.

Megoldás. Megvizsgáljuk, hogy invertálható-e a $\widehat{428}$ a $\mathbb{Z}_{3553}$ gyűrűben, vagyis 428 és 3553 relatív prímek-e:

$$\begin{aligned}
\underline{3553} &= 8 \cdot \underline{428} + \underline{129} \\
\underline{428} &= 3 \cdot \underline{129} + \underline{41} \\
\underline{129} &= 3 \cdot \underline{41} \quad + \underline{6} \\
\underline{41} &= 6 \cdot \underline{6} \quad + \underline{5} \\
\underline{6} &= 1 \cdot \underline{5} \quad + \underline{1} \\
\underline{5} &= 5 \cdot \underline{1} \quad + \underline{0}.
\end{aligned}$$

(Azért vannak az osztandók, osztók és maradékok aláhúzva, hogy az algoritmus második felébe ne végezzük el velük a szorzást.) Mivel az utolsó nem nulla maradék 1, ezért $(3553, 428) = 1$ és $\widehat{428}$ invertálható a $\mathbb{Z}_{3553}$ gyűrűben.

Az inverz kiszámolásához ki fogjuk fejezni a legnagyobb közös osztót (az 1-et) az 3553 és 428 segítségével a következő módon:

$$\begin{aligned}
1 &= \underline{6} - 1 \cdot \underline{5} \\
&= \underline{6} - 1 \cdot (\underline{41} - 6 \cdot \underline{6}) \\
&= -1 \cdot \underline{41} + 7 \cdot \underline{6} \\
&= -1 \cdot \underline{41} + 7 \cdot (\underline{129} - 3 \cdot \underline{41}) \\
&= 7 \cdot \underline{129} - 22 \cdot \underline{41} \\
&= 7 \cdot \underline{129} - 22 \cdot (\underline{428} - 3 \cdot \underline{129}) \\
&= -22 \cdot \underline{428} + 73 \cdot \underline{129} \\
&= -22 \cdot \underline{428} + 73 \cdot (\underline{3553} - 8 \cdot \underline{428}) \\
&= 73 \cdot \underline{3553} - 606 \cdot \underline{428}
\end{aligned}$$

Tehát azt kaptuk, hogy $1 = 73 \cdot 3553 - 606 \cdot 428$, ahonnan

$$\begin{aligned}
& \widehat{1} = \widehat{73} \cdot \widehat{3553} - \widehat{606} \cdot \widehat{428} \in \mathbb{Z}_{3553} \\
\Leftrightarrow \ & \widehat{1} = -\widehat{606} \cdot \widehat{428} \in \mathbb{Z}_{2346} \\
\Leftrightarrow \ & \widehat{1} = (\widehat{3553 - 606}) \cdot \widehat{428} \in \mathbb{Z}_{2346} \\
\Leftrightarrow \ & \widehat{1} = \widehat{2947} \cdot \widehat{428} \in \mathbb{Z}_{3553},
\end{aligned}$$

tehát $\widehat{428}^{-1} = \widehat{2947} \in \mathbb{Z}_{3553}$ az inverz. □

10. Oldjuk meg a következő egyenleteket:

(a) $26x \equiv 29 \pmod{18}$;

Megoldás. Az $26x \equiv 29 \pmod{18}$ egyenlet átírható mint $8x \equiv 11 \pmod{18}$, amely egyenértékű a $\widehat{8} \cdot \widehat{x} = \widehat{11} \in \mathbb{Z}_{18}$ egyenlettel. Megvizsgáljuk, hogy invertálható-e $\widehat{8}$ a $\mathbb{Z}_{18}$ gyűrűben: nem invertálható, mert a legnagyobb közös osztójuk $(8, 18) = 2 \neq 1$. Megnézzük, hogy 2 osztja-e az egyenlet szabadtagját, 11-et. Mivel nem osztja ezért az egyenletnek nincs megoldása.

Úgy is látható, hogy a $8x \equiv 11 \pmod{18}$ egyenletnek nincs megoldása, hogy beszorozva $\frac{18}{(8,18)} = 9$-cel kapjuk, hogy

$$\begin{aligned}
& 8x \equiv 11 \pmod{18} \qquad / \cdot 9 \\
\Rightarrow \ & 9 \cdot 8x \equiv 9 \cdot 11 \pmod{18}
\end{aligned}$$

$$\begin{aligned} \Leftrightarrow\ 18 \cdot 4x &\equiv 9 \pmod{18} \\ \Leftrightarrow\ 0 \cdot 4x &\equiv 9 \pmod{18} \\ \Leftrightarrow\ 0 &\equiv 9 \pmod{18}, \end{aligned}$$

ami nem teljesül. □

(b) $8x \equiv 48 \pmod{18}$;

Megoldás. Az egyenlet átírható $8x \equiv 12 \pmod{18}$ alakra, mert $48 = 12+2\cdot 18$. Kiszámoljuk a 8 (az x együtthatója) és 18 legnagyobb közös osztóját: $(8, 18) = 2$. A legnagyobb közös osztó osztja a szabadtagot $12 = 2 \cdot 6$. Így az eredetivel egyenértékű egyenletet kapunk a következőképpen:

$$\begin{aligned} 8x &\equiv 48 \pmod{18} \\ \Leftrightarrow\ \frac{8}{2}x &\equiv \frac{12}{2} \pmod{\frac{18}{2}} \\ \Leftrightarrow\ 4x &\equiv 6 \pmod 9. \end{aligned}$$

Mostmár az x együtthatója relatív prím 9-vel, vagyis $(4, 9) = 1$, ezért létezik olyan k egész szám, hogy $k \cdot 4 \equiv 1 \pmod 9$, mert

$$k \cdot 4 \equiv 1 \pmod 9 \ \Leftrightarrow\ \widehat{k} \cdot \widehat{4} = \widehat{1} \in \mathbb{Z}_9 \ \Leftrightarrow\ \widehat{k} = \widehat{4}^{-1} \in \mathbb{Z}_9.$$

A bővített euklidészi algoritmussal kiszámolható a k:

$$\begin{aligned} \underline{9} &= 2 \cdot \underline{4} + \underline{1} \\ \underline{4} &= 4 \cdot \underline{1} + \underline{0}, \end{aligned}$$

tehát $1 = 9 - 2 \cdot 4$, ahonnan

$$\begin{aligned} &\Leftrightarrow\ \widehat{1} = \widehat{9} - \widehat{2} \cdot \widehat{4} \in \mathbb{Z}_9 \\ &\Leftrightarrow\ \widehat{1} = (\widehat{9-2}) \cdot \widehat{4} \in \mathbb{Z}_9 \\ &\Leftrightarrow\ \widehat{1} = \widehat{7} \cdot \widehat{4} \in \mathbb{Z}_9 \\ &\Leftrightarrow\ 1 \equiv 7 \cdot 4 \pmod 9. \end{aligned}$$

Ez alapján $k = 7$. (Megjegyezzük, hogy mivel 9 nem nagy szám, ezért próbálgatással is találhatunk olyan k számot, amire $k \cdot 4$-nek a 9-cel való osztási maradéka 1.)
Visszatérve a $4x \equiv 6 \pmod 9$ egyenlethez kapjuk, hogy

$$\begin{aligned} 7 \cdot \backslash\ 4x &\equiv 6 \pmod 9 \\ \Leftrightarrow\ 28x &\equiv 42 \pmod 9 \\ \Leftrightarrow\ x &\equiv 6 \pmod 9 \\ \Leftrightarrow\ x &= 6 + 9k,\ k \in \mathbb{Z} \\ \Leftrightarrow\ x &\in 6 + 9\mathbb{Z} = \{6 + 9k \mid k \in \mathbb{Z}\}. \end{aligned}$$

□

(c) $15x \equiv 27 \pmod{24}$;

Megoldás. Az egyenlet átírható $15x \equiv 3 \pmod{24}$ alakra. Kiszámoljuk a 15 (az x együtthatója) és a 24 legnagyobb közös osztóját: $(15, 24) = 3$. A legnagyobb közös osztó osztja a szabadtagot, a 3-at. Így az eredetivel egyenértékű egyenletet kaphatunk a következőképpen:

$$15x \equiv 3 \pmod{24}$$

$$\Leftrightarrow \frac{15}{3}x \equiv \frac{3}{3} \pmod{\frac{24}{3}}$$
$$\Leftrightarrow 5x \equiv 1 \pmod{8}.$$

Mostmár az x együtthatója relatív prím a 8-cal, vagyis $(5, 8) = 1$, ezért létezik olyan k egész szám, hogy $k \cdot 5 \equiv 1 \pmod{8}$ éspedig $k = 5$ (mivel $5 \cdot 5 = 3 \cdot 8 + 1$).

$$\begin{aligned} 5 \cdot \backslash\ 5x &\equiv 1 \pmod{8} \\ \Leftrightarrow 25x &\equiv 5 \pmod{8} \\ \Leftrightarrow x &\equiv 5 \pmod{8} \\ \Leftrightarrow x &= 5 + 8k,\ k \in \mathbb{Z} \\ \Leftrightarrow x &\in 5 + 8\mathbb{Z} = \{5 + 8k \mid k \in \mathbb{Z}\}. \end{aligned}$$

□

(d) $16x \equiv 12 \pmod{24}$;

Megoldás. Kiszámoljuk a 16 (az x együtthatója) és a 24 legnagyobb közös osztóját: $(16, 24) = 8$. A legnagyobb közös osztó nem osztja a szabadtagot, a 12-t, ezért az egyenletnek nincs megoldása. □

(e) $491x \equiv 3 \pmod{2020}$;

Megoldás. Kiszámoljuk a 491 (az x együtthatója) és a 2020 legnagyobb közös osztóját:

$$\begin{aligned} \underline{2020} &= 4 \cdot \underline{491} + \underline{56} \\ \underline{491} &= 8 \cdot \underline{56} + \underline{43} \\ \underline{56} &= 1 \cdot \underline{43} + \underline{13} \\ \underline{43} &= 3 \cdot \underline{13} + \underline{4} \\ \underline{13} &= 3 \cdot \underline{4} + \underline{1} \\ \underline{4} &= 4 \cdot \underline{1} + \underline{0}, \end{aligned}$$

ahonnan a legnagyobb közös osztó 1 (az utolsó nem nulla maradék). Tehát 491 és 2020 relatív prímek, ezért létezik $k \in \mathbb{Z}$ úgy, hogy $k \cdot 491 \equiv 1 \pmod{2020}$, vagyis $\widehat{k} = \widehat{491}^{-1} \in \mathbb{Z}_{2020}$. A bővített euklidészi algoritmussal számítjuk ki a k-t:

$$\begin{aligned} 1 &= \underline{13} - 3 \cdot \underline{4} \\ &= \underline{13} - 3 \cdot (\underline{43} - 3 \cdot \underline{13}) \\ &= -3 \cdot \underline{43} + 10 \cdot \underline{13} \\ &= -3 \cdot \underline{43} + 10 \cdot (\underline{56} - 1 \cdot \underline{43}) \\ &= 10 \cdot \underline{56} - 13 \cdot \underline{43} \\ &= 10 \cdot \underline{56} - 13 \cdot (\underline{491} - 8 \cdot \underline{56}) \\ &= -13 \cdot \underline{491} + 114 \cdot \underline{56} \\ &= -13 \cdot \underline{491} + 114 \cdot (\underline{2020} - 4 \cdot \underline{491}) \\ &= 114 \cdot \underline{2020} - 469 \cdot \underline{491}. \end{aligned}$$

Ez alapján $k = -469$.
Visszatérve a $491x \equiv 3 \pmod{2020}$ egyenlethez kapjuk, hogy

$$\begin{aligned} -469 \cdot \backslash\ 491x &\equiv 3 \pmod{2020} \\ \Leftrightarrow 1x &\equiv -1407 \pmod{2020} \end{aligned}$$

$$\begin{aligned}
&\Leftrightarrow\ x \equiv 2020 - 1407 \pmod{2020}\\
&\Leftrightarrow\ x \equiv 613 \pmod{2020}\\
&\Leftrightarrow\ x = 613 + 2020k,\ \ k \in \mathbb{Z}\\
&\Leftrightarrow\ x \in 613 + 2020\mathbb{Z} = \{613 + 2020k \mid k \in \mathbb{Z}\}.
\end{aligned}$$

□

(f) $490x \equiv 4 \pmod{2021}$.

Megoldás. Kiszámoljuk a 490 és a 2021 legnagyobb közös osztóját:

$$\begin{aligned}
\underline{2021} &= 4 \cdot \underline{490} + \underline{61}\\
\underline{490} &= 8 \cdot \underline{61} + \underline{2}\\
\underline{61} &= 30 \cdot \underline{2} + \underline{1}\\
\underline{2} &= 2 \cdot \underline{1} + \underline{0}
\end{aligned}$$

ahonnan a legnagyobb közös osztó 1 (az utolsó nem nulla maradék). Tehát 490 és 2021 relatív prímek, ezért létezik $k \in \mathbb{Z}$ úgy, hogy $k \cdot 490 \equiv 1 \pmod{2021}$, vagyis $\widehat{k} = \widehat{490}^{-1} \in \mathbb{Z}_{2021}$. A bővített euklidészi algoritmussal számítjuk ki a k-t:

$$\begin{aligned}
1 &= \underline{61} - 30 \cdot \underline{2}\\
&= \underline{61} - 30 \cdot (\underline{490} - 8 \cdot \underline{61})\\
&= -30 \cdot \underline{490} + 241 \cdot \underline{61}\\
&= -30 \cdot \underline{490} + 241 \cdot (\underline{2021} - 4 \cdot \underline{490})\\
&= 241 \cdot \underline{2021} - 994 \cdot \underline{490}
\end{aligned}$$

Ez alapján $k = -994$ (vagy $k = 2021 - 994 = 1027$ is jó).
Visszatérve a $490x \equiv 4 \pmod{2021}$ egyenlethez kapjuk, hogy

$$\begin{aligned}
-994 \cdot \backslash\ 490x &\equiv 4 \pmod{2021}\\
\Leftrightarrow\ 1x &\equiv -3976 \pmod{2021}\\
\Leftrightarrow\ x &\equiv 66 \pmod{2021}\\
\Leftrightarrow\ x &= 66 + 2021k,\ \ k \in \mathbb{Z}\\
\Leftrightarrow\ x &\in 66 + 2021\mathbb{Z} = \{66 + 2021k \mid k \in \mathbb{Z}\}.
\end{aligned}$$

□

11. Oldjuk meg a következő egyenletrendszert:

(a) $\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases}$;

Első megoldás. Az $\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_r} \end{cases}$, ($n_1, \dots, n_r$ páronként relatív prímek) egyenletrendszer megoldása

$$x \equiv \sum_{i=1}^{r} a_i N_i K_i \pmod{N}, \tag{19}$$

ahol

- $N = n_1 \cdot \ldots \cdot n_r$,
- $N_i = \dfrac{N}{n_i} = n_1 \cdot \ldots \cdot n_{i-1} \cdot n_{i+1} \cdot \ldots \cdot n_r$, minden $i = 1, \ldots, r$ esetén,
- $K_i = N_i^{-1} \pmod{n_i}$ (vagyis $\widehat{K_i} = \widehat{N_i}^{-1} \in \mathbb{Z}_{n_i}$), minden $i = 1, \ldots, r$ esetén.

A mi esetünkben $n_1 = 5$, $n_2 = 7$, $n_3 = 11$ páronként relatív prímek. Kiszámoljuk, hogy $N = n_1 \cdot n_2 \cdot n_3 = 5 \cdot 7 \cdot 11 = 385$, illetve $N_1 = \frac{N}{n_1} = 7 \cdot 11 = 77$, $N_2 = \frac{N}{n_2} = 5 \cdot 11 = 55$, $N_1 = \frac{N}{n_3} = 5 \cdot 7 = 35$.

A $K_1 \equiv N_1^{-1} \pmod{n_1}$ egy olyan szám, amelyre

$$\begin{aligned} K_1 N_1 &\equiv 1 \pmod{n_1} \Leftrightarrow \\ K_1 \cdot 77 &\equiv 1 \pmod{5} \Leftrightarrow \\ K_1 \cdot 2 &\equiv 1 \pmod{5}. \end{aligned}$$

Mivel $n_1 = 5$ kis szám, ezért $K_1 = 1, 2, 3, 4$ lehetséges értékek közül próbálgatással kapjuk, hogy $K_1 = 3$, mert $3 \cdot 1 = 6 = 5 + 1$. (Nagy n_1 esetén a K_1-et a bővített euklidészi algoritmussal számoljuk ki.)

A $K_2 \equiv N_2^{-1} \pmod{n_2}$ egy olyan szám, amelyre

$$\begin{aligned} K_2 N_2 &\equiv 1 \pmod{n_2} \Leftrightarrow \\ K_2 \cdot 55 &\equiv 1 \pmod{7} \Leftrightarrow \\ K_2 \cdot 6 &\equiv 1 \pmod{7}. \end{aligned}$$

Mivel $n_2 = 7$ kis szám, ezért $K_2 = 1, \ldots, 6$ lehetséges értékek közül próbálgatással kapjuk, hogy $K_2 = 6$, mert $6 \cdot 6 = 36 = 5 \cdot 7 + 1$.

A $K_3 \equiv N_3^{-1} \pmod{n_3}$ egy olyan szám, amelyre

$$\begin{aligned} K_3 N_3 &\equiv 1 \pmod{n_3} \Leftrightarrow \\ K_3 \cdot 35 &\equiv 1 \pmod{11} \Leftrightarrow \\ K_3 \cdot 2 &\equiv 1 \pmod{11}. \end{aligned}$$

Mivel $n_3 = 11$ kis szám, ezért $K_3 = 1, \ldots, 10$ lehetséges értékek közül próbálgatással kapjuk, hogy $K_3 = 6$, mert $6 \cdot 2 = 12 = 11 + 1$.

Végül a (19) képlet alapján kapjuk, hogy

$$\begin{aligned} x &\equiv \underbrace{2}_{a_1} \cdot \underbrace{77}_{N_1} \cdot \underbrace{3}_{K_1} + \underbrace{4}_{a_2} \cdot \underbrace{55}_{N_2} \cdot \underbrace{6}_{K_2} + \underbrace{5}_{a_3} \cdot \underbrace{35}_{N_3} \cdot \underbrace{6}_{K_3} \pmod{385} \\ &\equiv 462 + 1320 + 1050 \pmod{385} \\ &\equiv 2832 \pmod{385} \\ &\equiv 137 \pmod{385}, \end{aligned}$$

tehát $x = 137 + 385k$, $k \in \mathbb{Z}$, vagyis $x \in 137 + 385\mathbb{Z} = \{137 + 385k \mid k \in \mathbb{Z}\}$. (Az egyenletrendszer megoldásai olyan egész számok, amelyeknek a 385-tel való osztási maradéka 137.)

Megjegyzés. Könnyen leellenőrizhető, hogy helyes-e a megoldásunk, mivel elég megnézni, hogy 137 teljesíti-e az eredeti egyenletrendszert:

$$\begin{cases} 137 \equiv 27 \cdot 5 + 2 \equiv 2 \pmod{5} \\ 137 \equiv 19 \cdot 7 + 4 \equiv 4 \pmod{7} \\ 137 \equiv 12 \cdot 11 + 5 \equiv 5 \pmod{7} \end{cases}.$$

□

Második megoldás. Legyenek $n_1, \ldots, n_r$ páronként relatív prím természetes számok. Az

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_r} \end{cases}$$

egyenletrendszer megoldását

$$x = b_1 N_1 + \cdots + b_r N_r$$

alakban keresssük, ahol $N_i = \dfrac{n_1 \cdot \ldots \cdot n_r}{n_i}$, minden $i = 1, \ldots, r$ esetén. Ezt szerre behelyettesítve az egyenletrendszer egyenleteibe kiszámoljuk a $b_1, \ldots, b_r$ számokat.

A mi esetünkben az egyenletrendszer megoldását $x = b_1 \cdot 7 \cdot 11 + b_2 \cdot 5 \cdot 11 + b_3 \cdot 5 \cdot 7$ alakban keressük, amelyet behelyettesítve az egyenletrendszer első egyenletébe kapjuk, hogy

$$\begin{aligned} x &\equiv 2 \pmod{5} \;\Leftrightarrow \\ b_1 \cdot 7 \cdot 11 + b_2 \cdot 5 \cdot 11 + b_3 \cdot 5 \cdot 7 &\equiv 2 \pmod{5} \;\Leftrightarrow \\ b_1 \cdot 77 &\equiv 2 \pmod{5} \;\Leftrightarrow \\ 3 \cdot \backslash \quad 2b_1 &\equiv 2 \pmod{5} \;\Leftrightarrow \\ 6b_1 &\equiv 6 \pmod{5} \;\Leftrightarrow \\ b_1 &\equiv 1 \pmod{5}, \;\Leftrightarrow \\ b_1 &= 1 + 5k_1,\; k_1 \in \mathbb{Z} \end{aligned}$$

ahol a $c_1 = 0, 1, \ldots, 4$ lehetséges esetek közül próbálgatással megkapjuk, hogy $c_1 = 3$-mal kellett beszorzni a fenti egyenletet ahhoz, hogy a b_2 együtthatója 1 legyen (modulo 5). (Ha n_1 nagy szám, akkor a b_1 együtthatójának inverzét a bővített euklidészi algoritmussal számoljuk ki.)
Az x-et behelyettesítve a második egyenletbe kapjuk, hogy

$$\begin{aligned} x &\equiv 4 \pmod{7} \;\Leftrightarrow \\ b_1 \cdot 7 \cdot 11 + b_2 \cdot 5 \cdot 11 + b_3 \cdot 5 \cdot 7 &\equiv 4 \pmod{7} \;\Leftrightarrow \\ b_2 \cdot 55 &\equiv 4 \pmod{7} \;\Leftrightarrow \\ 6 \cdot \backslash \quad 6b_2 &\equiv 4 \pmod{7} \;\Leftrightarrow \\ 36b_2 &\equiv 24 \pmod{7} \;\Leftrightarrow \\ b_2 &\equiv 3 \pmod{7} \;\Leftrightarrow \\ b_2 &= 3 + 7k_2,\; k_2 \in \mathbb{Z}, \end{aligned}$$

ahol a $c_2 = 0, 1, \ldots, 6$ lehetséges esetek közül próbálgatással megkapjuk, hogy $c_2 = 6$-tal kellett beszorzni a fenti egyenletet ahhoz, hogy a b_2 együtthatója 1 legyen (modulo 7).
Az x-et behelyettesítve a harmadik egyenletbe kapjuk, hogy

$$\begin{aligned} x &\equiv 5 \pmod{11} \;\Leftrightarrow \\ b_1 \cdot 7 \cdot 11 + b_2 \cdot 5 \cdot 11 + b_3 \cdot 5 \cdot 7 &\equiv 5 \pmod{11} \;\Leftrightarrow \\ b_3 \cdot 35 &\equiv 5 \pmod{11} \;\Leftrightarrow \\ 6 \cdot \backslash \quad 2b_3 &\equiv 5 \pmod{11} \;\Leftrightarrow \\ 12b_3 &\equiv 30 \pmod{11} \;\Leftrightarrow \\ b_3 &\equiv 8 \pmod{11}, \;\Leftrightarrow \end{aligned}$$

$$b_3 = 8 + 11k_3,\ k_3 \in \mathbb{Z}$$

ahol a $c_3 = 0, 1, \ldots, 10$ lehetséges esetek közül próbálgatással megkapjuk, hogy $c_3 = 6$-gyel kellett beszorozni a fenti egyenletet ahhoz, hogy a b_3 együtthatója 1 legyen (modulo 11).

Végül azt kaptuk, hogy

$$\begin{aligned} x &= (1 + 5k_1) \cdot 7 \cdot 11 + (3 + 7k_2) \cdot 5 \cdot 11 + (8 + 11k_3) \cdot 5 \cdot 7 \\ &= 77 + 165 + 280 + \underbrace{(k_1 + k_2 + k_3)}_{k'} \cdot 385 \\ &= 522 + k' \cdot 385 \\ &= 137 + \underbrace{(k' + 1)}_{k} \cdot 385 \\ &= 137 + k \cdot 385, \end{aligned}$$

vagyis $x \in 137 + 385\mathbb{Z} = \{137 + 385k \mid k \in \mathbb{Z}\}$. □

Harmadik megoldás. Sorban megoldjuk az egyenleteket és a kapott megoldást behelyettesítjük a következőben. (Ennek a módszernek a hátránya az előzőekhez képest, hogy a számítások nem párhuzamosíthatók.)

$$\begin{aligned} x &\equiv 2 \pmod 5 \iff \\ x &= 2 + 5k_1,\ k_1 \in \mathbb{Z}. \end{aligned}$$

Ezt behelyettesítjük a második egyenletben:

$$\begin{aligned} -2 \setminus\ 2 + 5k_1 &\equiv 4 \pmod 7 \iff \\ 3 \cdot \setminus\ 5k_1 &\equiv 2 \pmod 7 \iff \\ 15k_1 &\equiv 6 \pmod 7 \iff \\ k_1 &\equiv 6 \pmod 7 \iff \\ k_1 &= 6 + 7k_2,\ k_2 \in \mathbb{Z}, \end{aligned}$$

ahonnan $x = 2 + 5k_1 = 2 + 5(6 + 7k_2) = 32 + 35k_2,\ k_2 \in \mathbb{Z}$. Ezt behelyettesítjük a harmadik egyenletbe:

$$\begin{aligned} 32 + 35k_2 &\equiv 5 \pmod{11} \iff \\ +1 \setminus\ -1 + 2k_2 &\equiv 5 \pmod{11} \iff \\ 6 \cdot \setminus\ 2k_2 &\equiv 6 \pmod{11} \iff \\ 12k_2 &\equiv 36 \pmod{11} \iff \\ k_2 &\equiv 3 \pmod{11} \iff \\ k_2 &= 3 + 11k_3,\ k_3 \in \mathbb{Z}. \end{aligned}$$

Végül azt kaptuk, hogy

$$\begin{aligned} & x = 32 + 35k_2 = 32 + 35(3 + 11k_3) = 137 + 385k_3,\ k_3 \in \mathbb{Z} \\ \iff\ & x \in 137 + 385\mathbb{Z}. \end{aligned}$$

□

(b) $\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod 9 \end{cases}$;

Első megoldás. Az $N_1 = 7 \cdot 9 = 63$ és a $K_1 \equiv N_1^{-1} \pmod 4$ egy olyan szám, amelyre

$$\begin{aligned} K_1 \cdot N_1 &\equiv 1 \pmod 4 \iff \\ K_1 \cdot 63 &\equiv 1 \pmod 4 \iff \\ K_1 \cdot 3 &\equiv 1 \pmod 4. \end{aligned}$$

A $K_1 = 1, 2, 3, 4$ lehetséges értékek közül próbálgatással kapjuk, hogy $K_1 = 3$, mert $3 \cdot 3 = 9 = 2 \cdot 4 + 1$.
Az $N_2 = 4 \cdot 9 = 36$ és a $K_2 \equiv N_2^{-1} \pmod 7$ egy olyan szám, amelyre

$$\begin{aligned} K_2 \cdot N_2 &\equiv 1 \pmod 7 \iff \\ K_2 \cdot 36 &\equiv 1 \pmod 7 \iff \\ K_2 &\equiv 1 \pmod 7, \end{aligned}$$

Az $N_3 = 4 \cdot 7 = 28$ és a $K_3 \equiv N_3^{-1} \pmod 9$ egy olyan szám, amelyre

$$\begin{aligned} K_3 \cdot N_3 &\equiv 1 \pmod 9 \iff \\ K_3 \cdot 28 &\equiv 1 \pmod 9 \iff \\ K_3 &\equiv 1 \pmod 9. \end{aligned}$$

Végül azt kapjuk, hogy

$$\begin{aligned} x &\equiv 1 \cdot 3 \cdot 63 + 2 \cdot 1 \cdot 36 + 3 \cdot 1 \cdot 28 \pmod{4 \cdot 7 \cdot 9} \\ &\equiv 189 + 72 + 84 \pmod{252} \\ &\equiv 345 \pmod{252} \\ &\equiv 93 \pmod{252}, \end{aligned}$$

tehát $x = 93 + 252k$, $k \in \mathbb{Z}$, vagyis $x \in 93 + 252\mathbb{Z} = \{93 + 252k \mid k \in \mathbb{Z}\}$. (Az egyenletrendszer megoldásai olyan egész számok, amelyeknek a 252-vel való osztási maradéka 93.)

Megjegyzés. Könnyen leellenőrizhető, hogy helyes-e a megoldásunk, mivel elég megnézni, hogy 93 teljesíti-e az eredeti egyenletrendszert:

$$\begin{cases} 93 \equiv 23 \cdot 4 + 1 \equiv 1 \pmod 4 \\ 93 \equiv 13 \cdot 7 + 2 \equiv 2 \pmod 7 \\ 93 \equiv 10 \cdot 9 + 3 \equiv 3 \pmod 9 \end{cases}.$$

$\square$

Második megoldás. Az egyenletrendszer megoldását $x = b_1 \cdot 7 \cdot 9 + b_2 \cdot 4 \cdot 9 + b_3 \cdot 4 \cdot 7$ alakban keressük. Az első egyenletből kapjuk, hogy

$$\begin{aligned} x &\equiv 1 \pmod 4 \iff \\ b_1 \cdot 63 &\equiv 1 \pmod 4 \iff \\ 3 \cdot \backslash \quad 3b_1 &\equiv 1 \pmod 4 \iff \\ 9b_1 &\equiv 3 \pmod 4 \iff \\ b_1 &\equiv 3 \pmod 4 \iff \\ b_1 &= 3 + 4k_1,\ k_1 \in \mathbb{Z}. \end{aligned}$$

A második egyenletből kapjuk, hogy

$$x \equiv 2 \pmod 7 \iff$$

$$\begin{aligned} b_2 \cdot 36 &\equiv 2 \pmod 7 \iff \\ b_2 &\equiv 2 \pmod 7 \iff \\ b_2 &= 2 + 7k_2,\ k_2 \in \mathbb{Z}. \end{aligned}$$

A harmadik egyenletből kapjuk, hogy

$$\begin{aligned} x &\equiv 3 \pmod 9 \iff \\ b_3 \cdot 28 &\equiv 3 \pmod 9 \iff \\ b_3 &\equiv 3 \pmod 9 \iff \\ b_3 &= 3 + 9k_3,\ k_3 \in \mathbb{Z}. \end{aligned}$$

Végül azt kaptuk, hogy

$$\begin{aligned} x &= (3 + 4k_1) \cdot 63 + (2 + 7k_2) \cdot 36 + (3 + 9k_3) \cdot 28 \\ &= 189 + 72 + 84 + \underbrace{(k_1 + k_2 + k_3)}_{k'} \cdot 252 \\ &= 345 + k' \cdot 252 \\ &= 93 + \underbrace{(k' + 1)}_{k} \cdot 252 \\ &= 93 + k \cdot 252, \end{aligned}$$

vagyis $x \in 93 + 252\mathbb{Z}$. □

Harmadik megoldás. Sorban megoldjuk az egyenleteket és a kapott megoldást behelyettesítjük a következőben.

$$\begin{aligned} x &\equiv 1 \pmod 4 \iff \\ x &= 1 + 4k_1,\ k_1 \in \mathbb{Z}. \end{aligned}$$

Ezt behelyettesítjük a második egyenletben:

$$\begin{aligned} -1 \setminus 1 + 4k_1 &\equiv 2 \pmod 7 \iff \\ 2 \cdot \setminus 4k_1 &\equiv 1 \pmod 7 \iff \\ 8k_1 &\equiv 2 \pmod 7 \iff \\ k_1 &\equiv 2 \pmod 7 \iff \\ k_1 &= 2 + 7k_2,\ k_2 \in \mathbb{Z}, \end{aligned}$$

ahonnan $x = 1 + 4k_1 = 1 + 4(2 + 7k_2) = 9 + 28k_2$, $k_2 \in \mathbb{Z}$. Ezt behelyettesítjük a harmadik egyenletbe:

$$\begin{aligned} 9 + 28k_2 &\equiv 3 \pmod 9 \iff \\ k_2 &\equiv 3 \pmod 9 \iff \\ k_2 &= 3 + 9k_3,\ k_3 \in \mathbb{Z}. \end{aligned}$$

Végül azt kaptuk, hogy

$$\begin{aligned} & x = 9 + 28k_2 = 9 + 28(3 + 9k_3) = 93 + 252k_3,\ k_3 \in \mathbb{Z} \\ \iff\ & x \in 93 + 252\mathbb{Z}. \end{aligned}$$

□

(c) $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 5 \pmod 8 \end{cases}$.

Első megoldás. Az $N_1 = 7 \cdot 8 = 56$ és a $K_1 \equiv N_1^{-1} \pmod 5$ egy olyan szám, amelyre

$$\begin{aligned} K_1 \cdot N_1 &\equiv 1 \pmod 5 \;\Leftrightarrow \\ K_1 \cdot 56 &\equiv 1 \pmod 5 \;\Leftrightarrow \\ K_1 &\equiv 1 \pmod 4). \end{aligned}$$

Az $N_2 = 5 \cdot 8 = 40$ és a $K_2 \equiv N_2^{-1} \pmod 7$ egy olyan szám, amelyre

$$\begin{aligned} K_2 \cdot N_2 &\equiv 1 \pmod 7 \;\Leftrightarrow \\ K_2 \cdot 40 &\equiv 1 \pmod 7 \;\Leftrightarrow \\ 3 \cdot \backslash\; 5K_2 &\equiv 1 \pmod 7 \Leftrightarrow \\ 15K_2 &\equiv 3 \pmod 7 \Leftrightarrow \\ K_2 &\equiv 3 \pmod 7, \end{aligned}$$

Az $N_3 = 5 \cdot 7 = 35$ és a $K_3 \equiv N_3^{-1} \pmod 8$ egy olyan szám, amelyre

$$\begin{aligned} K_3 \cdot 5 \cdot 7 &\equiv 1 \pmod 8 \;\Leftrightarrow \\ K_3 \cdot 35 &\equiv 1 \pmod 8 \;\Leftrightarrow \\ 3 \cdot \backslash\; 3K_3 &\equiv 1 \pmod 8 \;\Leftrightarrow \\ 9K_3 &\equiv 3 \pmod 8 \;\Leftrightarrow \\ K_3 &\equiv 3 \pmod 8. \end{aligned}$$

Végül azt kapjuk, hogy

$$\begin{aligned} x &\equiv 3 \cdot 1 \cdot 56 + 2 \cdot 3 \cdot 40 + 5 \cdot 3 \cdot 35 \pmod{5 \cdot 7 \cdot 8} \\ &\equiv 168 + 240 + 525 \pmod{280} \\ &\equiv 933 \pmod{280} \\ &\equiv 93 \pmod{280}, \end{aligned}$$

tehát $x = 93 + 280k$, $k \in \mathbb{Z}$, vagyis $x \in 93 + 280\mathbb{Z} = \{93 + 280k \mid k \in \mathbb{Z}\}$. (Az egyenletrendszer megoldásai olyan egész számok, amelyeknek a 280-nal való osztási maradéka 93.) □

Második megoldás. Az egyenletrendszer megoldását $x = b_1 \cdot 7 \cdot 8 + b_2 \cdot 5 \cdot 8 + b_3 \cdot 5 \cdot 7$ alakban keressük. Az első egyenletből kapjuk, hogy

$$\begin{aligned} x &\equiv 3 \pmod 5 \;\Leftrightarrow \\ b_1 \cdot 56 &\equiv 3 \pmod 5 \;\Leftrightarrow \\ b_1 &\equiv 3 \pmod 5 \;\Leftrightarrow \\ b_1 &= 3 + 4k_1,\; k_1 \in \mathbb{Z}. \end{aligned}$$

A második egyenletből kapjuk, hogy

$$\begin{aligned} x &\equiv 2 \pmod 7 \;\Leftrightarrow \\ b_2 \cdot 40 &\equiv 2 \pmod 7 \;\Leftrightarrow \\ 3 \cdot \backslash\quad 5b_2 &\equiv 2 \pmod 7 \;\Leftrightarrow \\ 15b_2 &\equiv 6 \pmod 7 \;\Leftrightarrow \end{aligned}$$

$$\begin{aligned} b_2 &\equiv 6 \pmod 7 \Leftrightarrow \\ b_2 &= 6 + 7k_2,\ k_2 \in \mathbb{Z}. \end{aligned}$$

A harmadik egyenletből kapjuk, hogy

$$\begin{aligned} x &\equiv 5 \pmod 8 \Leftrightarrow \\ b_3 \cdot 35 &\equiv 5 \pmod 8 \Leftrightarrow \\ 3 \cdot \backslash \quad 3b_3 &\equiv 5 \pmod 8 \Leftrightarrow \\ 9b_3 &\equiv 15 \pmod 8 \Leftrightarrow \\ b_3 &\equiv 7 \pmod 8 \Leftrightarrow \\ b_3 &= 7 + 8k_3,\ k_3 \in \mathbb{Z}. \end{aligned}$$

Végül azt kaptuk, hogy

$$\begin{aligned} x &= (3 + 4k_1) \cdot 56 + (6 + 7k_2) \cdot 40 + (7 + 8k_3) \cdot 35 \\ &= 168 + 240 + 245 + \underbrace{(k_1 + k_2 + k_3)}_{k'} \cdot 280 \\ &= 653 + k' \cdot 280 \\ &= 93 + \underbrace{(k' + 2)}_{k} \cdot 280 \\ &= 93 + k \cdot 280, \end{aligned}$$

vagyis $x \in 93 + 280\mathbb{Z}$. □

Harmadik megoldás. Sorban megoldjuk az egyenleteket és a kapott megoldást behelyettesítjük a következőben.

$$\begin{aligned} x &\equiv 3 \pmod 5 \Leftrightarrow \\ x &= 3 + 5k_1,\ k_1 \in \mathbb{Z}. \end{aligned}$$

Ezt behelyettesítjük a második egyenletben:

$$\begin{aligned} -3 \cdot \backslash\ 3 + 5k_1 &\equiv 2 \pmod 7 \Leftrightarrow \\ 3 \cdot \backslash\ 5k_1 &\equiv -1 \pmod 7 \Leftrightarrow \\ 15k_1 &\equiv -3 \pmod 7 \Leftrightarrow \\ k_1 &\equiv 4 \pmod 7 \Leftrightarrow \\ k_1 &= 4 + 7k_2,\ k_2 \in \mathbb{Z}, \end{aligned}$$

ahonnan $x = 3 + 5k_1 = 3 + 5(4 + 7k_2) = 23 + 35k_2$, $k_2 \in \mathbb{Z}$. Ezt behelyettesítjük a harmadik egyenletbe:

$$\begin{aligned} 23 + 35k_2 &\equiv 5 \pmod 8 \Leftrightarrow \\ +1 \cdot \backslash\ \ -1 + 3k_2 &\equiv 5 \pmod 8 \Leftrightarrow \\ 3 \cdot \backslash\ 3k_2 &\equiv 6 \pmod 8 \Leftrightarrow \\ 9k_2 &\equiv 18 \pmod 8 \Leftrightarrow \\ k_2 &\equiv 2 \pmod 8 \Leftrightarrow \\ k_2 &= 2 + 8k_3,\ k_3 \in \mathbb{Z}. \end{aligned}$$

Végül azt kaptuk, hogy

$$x = 23 + 35k_2 = 23 + 35(2 + 8k_3) = 93 + 280k_3,\ k_3 \in \mathbb{Z}$$

$\Leftrightarrow \; x \in 93 + 280\mathbb{Z}.$

$\square$