5.3 Комутативни прстени са јединицом

3.1 Затвореност за $+$. Нека је $a, b \in R$, тј. $a = \frac{m_1}{n_1}$ и $b = \frac{m_2}{n_2}$, за неке целе бројеве m_1, m_2, n_1 и n_2, при чему n_1 и n_2 нису дељиви са p. Тада је

$$a + b = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2},$$

па како $p \nmid n_1 n_2$, важи $a + b \in R$.

Затвореност за $\cdot$. Нека је $a, b \in R$, тј. $a = \frac{m_1}{n_1}$ и $b = \frac{m_2}{n_2}$, за неке целе бројеве m_1, m_2, n_1 и n_2, при чему n_1 и n_2 нису дељиви са p. Тада је $a \cdot b = \frac{m_1 m_2}{n_1 n_2}$, па како $p \nmid n_1 n_2$, важи $a \cdot b \in R$.

Неутрал за $+$. Како је $0 = \frac{0}{1}$, то је $0 \in R$.

Инверз за $+$. Нека је $a \in R$, тј. $a = \frac{m}{n}$, где $p \nmid n$. Тада је $-a = \frac{-m}{n}$, па како $p \nmid n$, важи $-a \in R$.

Неутрал за $\cdot$. Како је $1 = \frac{1}{1}$, то је $1 \in R$.

Како су операције $+$ и $\cdot$ асоцијативне, а $+$ и комутативна, закључујемо да је R потпрстен од $\mathbb{Q}$.

3.2 Означимо са N скуп свих нилпотентних елемената прстена R.

Нека је $x, y \in N$. Тада је $x^n = 0$ и $y^m = 0$, за неке $n, m \geqslant 1$. Како је R комутативан прстен у њему важи биномна формула[37], па је

$$(x + y)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} x^k y^{n+m-1-k}.$$

Посматрајмо произвољан сабирак на десној страни ове једнакости. Ако је $k \geqslant n$, тада је $x^k = 0$, па је и $x^k y^{n+m-1-k} = 0$; ако је $k < n$, тада је $n + m - 1 - k \geqslant n + m - 1 - n + 1 = m$, па је $y^{n+m-1-k} = 0$, тј. $x^k y^{n+m-1-k} = 0$. Дакле, сваки сабирак ове суме једнак је 0, па је $(x + y)^{n+m-1} = 0$, а самим тим и $x + y \in N$.

Нека је сада $x \in N$ и $r \in R$. Тада је $x^n = 0$, за неко $n \geqslant 1$. Како је R комутативан прстен важи $(rx)^n = r^n x^n = 0$, па је $rx \in N$.

3.3 Како је x нилпотентан елемент за неко $n \geqslant 1$ важи $x^n = 0$. Прстен R је комутативан, па важи (погледати и коментар)

$$1 = 1 - x^n = (1 - x)(1 + x + x^2 + \cdots + x^{n-1}),$$

тј. $1 + x + x^2 + \cdots + x^{n-1}$ је инверз елемента $1 - x$.

Коментар. У овом доказу смо користили да у комутативном прстену са јединицом R за све $a, b \in R$ и све $n \in \mathbb{N}$ важи

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

[37] Доказ се може извести на исти начин као у нпр. прстену $\mathbb{R}$.

Изведимо ову формулу. Важи:

$$\begin{aligned} a^n - b^n &= a^n - a^{n-1}b + a^{n-1}b - a^{n-2}b^2 + a^{n-2}b^2 - a^{n-3}b^3 + \cdots + ab^{n-1} - a^n \\ &= (a-b)a^{n-1} + (a-b)a^{n-2}b + (a-b)a^{n-3}b^2 + \cdots + (a-b)b^{n-1} \\ &= (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}). \end{aligned}$$

(у другој једнакости смо користили комутативност множења).

3.4 **Затвореност за $+$.** Нека је $x, y \in R$, тј. $x = a_1 + b_1\sqrt{2}$ и $y = a_2 + b_2\sqrt{2}$, за неке $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Тада је

$$x + y = a_1 + a_2 + (b_1 + b_2)\sqrt{2},$$

па како је $a_1 + a_2, b_1 + b_2 \in \mathbb{Q}$, то је $x + y \in R$.

Затвореност за $\cdot$. Нека је $x, y \in R$, тј. $x = a_1 + b_1\sqrt{2}$ и $y = a_2 + b_2\sqrt{2}$, за неке $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Тада је

$$x \cdot y = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2},$$

па како је $a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1 \in \mathbb{Q}$, то је $x \cdot y \in R$.

Инверз за $+$. Нека је $x \in R$, тј. $x = a + b\sqrt{2}$, где је $a, b \in \mathbb{Q}$. Тада је $-x = -a - b\sqrt{2}$, па је $-x \in R$.

Неутрал за $\cdot$. Како је $1 = 1 + 0 \cdot \sqrt{2}$, то је $1 \in R$.

Инверз за $\cdot$. Нека је $x \in R \setminus \{0\}$, тј. $x = a + b\sqrt{2}$, где је $a, b \in \mathbb{Q}$ и $(a, b) \neq (0, 0)$. Тада је[38] $a - b\sqrt{2} \neq 0$ и важи

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2} \cdot \sqrt{2},$$

па како је $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$, то је $\frac{1}{x} \in R$.

3.5 Скуп $I^2 + J^2$ је идеал прстена R (по ставу 3.13), па је довољно доказати да се 1 налази у $I^2 + J^2$ (погледати пример 3.20).

Из $I + J = R$ закључујемо да постоје $x \in I$ и $y \in J$ такви да је $x + y = 1$. Због комутативности прстена R, тада је и

$$1 = (x + y)^2 = x^2 + y^2 + 2xy,$$

па како $x^2 + y^2 \in I^2 + J^2$, да бисмо доказали да је $1 \in I^2 + J^2$, довољно је доказати да важи $2xy \in I^2 + J^2$. Важи

$$x^2y + xy^2 = (x + y)xy = xy,$$

па како је $x^2y \in I^2$ и $xy^2 \in J^2$, то је $xy \in I^2 + J^2$, а самим тим и $2xy \in I^2 + J^2$. Овим је тврђење доказано.

[38] У супротном је $\sqrt{2} = a/b \in \mathbb{Q}$, а знамо да је $\sqrt{2}$ ирационалан број.

3.6 Доказаћемо да је $S+I$ потпрстен прстена R.

Затвореност за $+$. Нека је $x, y \in S+I$. Тада је $x = s_1 + i_1$ и $y = s_2 + i_2$, за неке $s_1, s_2 \in S$ и $i_1, i_2 \in I$. Како је S потпрстен од R то је $s_1 + s_2 \in S$, а како је I идеал од R, то је $i_1 + i_2 \in I$, па важи

$$x + y = (s_1 + s_2) + (i_1 + i_2) \in S + I.$$

Затвореност за $\cdot$. Нека је $x, y \in R$. Тада је $x = s_1 + i_1$ и $y = s_2 + i_2$, за неке $s_1, s_2 \in S$ и $i_1, i_2 \in I$. Како је S потпрстен од R то је $s_1 \cdot s_2 \in S$, а како је I идеал од R, то је $s_2 \cdot i_1, s_1 \cdot i_2, i_1 \cdot i_2 \in I$, па и $s_2 \cdot i_1 + s_1 \cdot i_2 + i_1 \cdot i_2 \in I$. Одавде је

$$(s_1 + i_1)(s_2 + i_2) = s_1 \cdot s_2 + (s_2 \cdot i_1 + s_1 \cdot i_2 + i_1 \cdot i_2) \in S + I.$$

Неутрал за $+$. Како је $0 = 0 + 0$, а $0 \in S$ и $0 \in I$, то је $0 \in S + I$.

Инверз за $+$. Нека је $x \in S + I$, тј. $x = s + i$, где је $s \in S$ и $i \in I$. Тада је $-x = -s - i$, па како је $-s \in S$ и $-i \in I$, то је $-x \in S + I$.

Неутрал за $\cdot$. Како је $1 = 1 + 0$, а $1 \in S$ и $0 \in I$, то је $1 \in S + I$.

Како су операције $+$ и $\cdot$ асоцијативне, а $+$ и комутативна, закључујемо да је $S + I$ потпрстен од R.

3.7 Нека су S и T потпрстени прстена R. Докажимо да је $S \cap T$ потпрстен прстена R

Затвореност за $+$. Нека је $x, y \in S \cap T$. Тада је $x, y \in S, T$, па како су S и T потпрстени од R, то је $x + y \in S$ и $x + y \in T$. Одавде је $x + y \in S \cap T$, што је требало доказати.

Затвореност за $\cdot$. Нека је $x, y \in S \cap T$. Тада је $x, y \in S, T$, па како су S и T потпрстени од R, то је $x \cdot y \in S$ и $x \cdot y \in T$. Одавде је $x \cdot y \in S \cap T$, што је требало доказати.

Неутрал за $+$. Како је $0 \in S$ и $0 \in T$, то је $0 \in S \cap T$.

Инверз за $+$. Нека је $x \in S \cap T$. Тада је $x \in S, T$, па је $-x \in S, T$, а самим тим и $-x \in S \cap T$.

Неутрал за $\cdot$. Како је $1 \in S$ и $1 \in T$, то је $1 \in S \cap T$.

Докажимо сада да постоји прстен R и његови потпрстени S и T такви да $S \cup T$ није потпрстен од R.

Довољно је узети $R = \mathbb{R}$, $S = \mathbb{Q}(\sqrt{2})$ и $T = \mathbb{Q}(\sqrt{3})$. Тада S и T јесу потпрстени од R (погледати задатак 3.4), па је довољно доказати да $S \cup T$ није потпрстен од R.

Претпоставимо супротно. Тада из $\sqrt{2}, \sqrt{3} \in S \cup T$, следи $\sqrt{2} + \sqrt{3} \in S \cup T$, па је $\sqrt{2} + \sqrt{3} \in S$ или $\sqrt{2} + \sqrt{3} \in T$. Претпоставимо да је $\sqrt{2} + \sqrt{3} \in S$ (случај $\sqrt{2} + \sqrt{3} \in T$ се може анализирати аналогно). Тада за неке рационалне бројева a и b важи $a + b\sqrt{2} = \sqrt{2} + \sqrt{3}$, па је $a - \sqrt{3} = (1-b)\sqrt{2}$. Квадрирањем и сређивањем ове једнакости добијамо

$$a^2 + 3 - 2(1-b)^2 = 2a\sqrt{3},$$

па је $2a\sqrt{3} \in \mathbb{Q}$. Ово је могуће једино уколико је $a = 0$. Међутим, тада је $\sqrt{3} = (b-1)\sqrt{2}$, па је $\sqrt{3/2} \in \mathbb{Q}$, чиме је добијена контрадикција.

3.8 По примеру 3.16 важи

$$I = \langle \text{NZD}(45, 36) \rangle \cap \langle 12 \rangle = \langle 9 \rangle \cap \langle 12 \rangle = \langle \text{NZS}(9, 12) \rangle = \langle 36 \rangle.$$

3.9 По (3.1) елемент $a \in \mathbb{Z}_n$ је делитељ нуле ако и само ако није инвертибилан, тј. ако и само ако $a \notin \Phi(n)$. Дакле, $a \in \mathbb{Z}_n \setminus \{0\}$ је прави делитељ нуле ако и само ако је $\text{NZD}(a, n) > 1$.

а) Прави делитељи нуле у $\mathbb{Z}_{21}$ чине скуп $\{3, 6, 7, 9, 12, 14, 15, 18\}$.

б) Прави делитељи нуле у $\mathbb{Z}_{16}$ чине скуп $\{2, 4, 6, 8, 10, 12, 14\}$.

3.10 а) Скуп инвертибилних елемената у $\mathbb{Z}_{15}$ је

$$U(\mathbb{Z}_{15}) = \Phi(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

При томе, 1 је инверз од 1, 2 је инверз од 8, 4 је инверз од 4, 7 је инверз од 13, 11 је инверз од 11 и 14 је инверз од 14.

б) Скуп инвертибилних елемената у $\mathbb{Z}_{36}$ је

$$U(\mathbb{Z}_{36}) = \Phi(36) = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}.$$

При томе, 1 је инверз од 1, 5 је инверз од 29, 7 је инверз од 31, 11 је инверз од 23, 13 је инверз од 25, 17 инверз од 17, 19 инверз од 19 и 35 је инверз од 35.

3.11 Као у примеру 3.28 може се доказати да су сви идеали прстена $\mathbb{Z}_n$ облика $\langle m \rangle$ за неко $m \mid n$.

а) Идеали прстена $\mathbb{Z}_{24}$ су $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, $\langle 6 \rangle$, $\langle 8 \rangle$, $\langle 12 \rangle$ и $\langle 0 \rangle = \{0\}$.

б) Идеали прстена $\mathbb{Z}_{16}$ су $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 4 \rangle$, $\langle 8 \rangle$ и $\langle 0 \rangle = \{0\}$.

3.12 Докажимо да важи: уколико n дели m и $n \neq 1$, тада је пресликавање $f : \mathbb{Z}_m \to \mathbb{Z}_n$ задато са $f(x) = \rho(x, n)$ хомоморфизам комутативних прстена са јединицом. Нека је $m = nq$.

По дефиницији пресликавања f и операције $+_m$ важи

$$f(x +_m y) = \rho(x +_m y, n) = \rho(\rho(x + y, m), n).$$

Нека је $x + y = mk + r$, где је $0 \leqslant r < m$, те нека је $r = nl + s$, где је $0 \leqslant s < n$. По дефиницији, тада је $\rho(x + y, m) = r$ и $\rho(\rho(x + y, m), n) = \rho(r, n) = s$. Са друге стране,

$$f(x) +_n f(y) = \rho(x, n) +_n \rho(y, n) = \rho(\rho(x, n) + \rho(y, n), n),$$

па како је пресликавање $f_n : \mathbb{Z} \to \mathbb{Z}_n$ задато са $f_n(x) = \rho(x, n)$ хомоморфизам прстена (погледати пример 3.22), то је

$$\rho(\rho(x, n) + \rho(y, n), n) = f_n(x) +_n f_n(y) = f_n(x + y) = \rho(x + y, n).$$

Коначно, $x+y = mk+r = mk+nl+s = n(qk+l)+s$, па је $\rho(x+y,n) = s$, а самим тим важи

$$f(x +_m y) = \rho(\rho(x+y,m),n) = s = \rho(x+y,n) = f(x) +_n f(y),$$

што је и требало доказати.

Аналогно доказујемо да је $f(x \cdot_m y) = f(x) \cdot_n f(y)$. Како је $f(1) = \rho(1,n) = 1$, закључујемо да је f хомоморфизам комутативних прстена са јединицом.

а) Како $9 \mid 36$ пресликавање f јесте хомоморфизам комутативних прстена са јединицом. При томе важи

$$\begin{aligned}\operatorname{Ker}(f) &= \{x \in \mathbb{Z}_{36} : f(x) = 0\}\\ &= \{x \in \mathbb{Z}_{36} : \rho(x,9) = 0\}\\ &= \{x \in \mathbb{Z}_{36} : 9 \mid x\}\\ &= \{0,9,18,27\}.\end{aligned}$$

б) Како $6 \mid 36$ пресликавање f јесте хомоморфизам комутативних прстена са јединицом. При томе важи

$$\begin{aligned}\operatorname{Ker}(f) &= \{x \in \mathbb{Z}_{36} : f(x) = 0\}\\ &= \{x \in \mathbb{Z}_{36} : \rho(x,6) = 0\}\\ &= \{x \in \mathbb{Z}_{36} : 6 \mid x\}\\ &= \{0,6,12,18,24,30\}.\end{aligned}$$

в) Докажимо да f није хомоморфизам. Ово следи из

$$f(6 \cdot_{36} 6) = f(0) = 0 \quad \text{и} \quad f(6) \cdot_{10} f(6) = 6 \cdot_{10} 6 = 6.$$

3.13 а) Како је $\mathrm{NZD}(7,5) = 1$, то дату конгруенцију можемо помножити са 5 (множимо бројем 5, јер је $3 \cdot 5 \equiv 1 \pmod 7$), чиме добијамо $5 \cdot 3 \cdot x \equiv 5 \cdot 4 \pmod 7$, а самим тим $x \equiv 6 \pmod 7$. Сва решења дате конгрусенције су бројеви $x = 7k+6$, за $k \in \mathbb{Z}$.

б) У овом случају не можемо поступати као у делу под а), јер $\mathrm{NZD}(4,6) \neq 1$. Запишимо зато задату конгрусенцију у еквивалентном облику, тј. као $6 \mid 4x-2$. Како су „обе стране" у овој релацији дељиве са 2, то можемо „скратити" са 2, чиме добијамо $3 \mid 2x-1$. Ово је еквивалентно са $2x \equiv 1 \pmod 3$. Приметимо да важи $\mathrm{NZD}(3,2) = 1$, па сада можемо поступати као у делу под а). Множењем ове конгруенције са 2 добијамо $x \equiv 2 \pmod 3$, па су сва решења почетне конгруенције бројеви $x = 3k+2$, за $k \in \mathbb{Z}$.

в) Важи $\mathrm{NZD}(15,10) = 5 \neq 1$, па дату конгрусенцију записујемо као $10 \mid 15x-4$. Међутим, $5 \mid 10$ и $5 \mid 15x$, па како $5 \nmid 4$, то $10 \nmid 15x-4$, а самим тим дата конгруенција нема решења.

г) Важи $\mathrm{NZD}(12,15) = 3 \neq 1$, па дату конгрусенцију записујемо као $15 \mid 12x - 21$. Обе стране ове релације дељиве су са 3, па можемо скратити са 3, чиме добијамо $5 \mid 4x - 7$, тј. $4x \equiv 7 \pmod 5$. Како је $\mathrm{NZD}(4,5) = 1$ ову конгруенцију можемо помножити са 4, чиме добијамо $x \equiv 3 \pmod 5$. Дакле, сва решења почетне конгруенције су бројеви $x = 5k + 3$, за $k \in \mathbb{Z}$.

3.14 а) Конгрусенција $x \equiv 3 \pmod 7$ сквивалентна је са $x = 7k + 3$, за неко $k \in \mathbb{Z}$. Заменом у другу конгрусенцију добијамо $7k + 3 \equiv 5 \pmod 8$, тј. $7k \equiv 2 \pmod 8$. Како је $\mathrm{NZD}(7,8) = 1$, ову конгруенцију можемо помоножити са 7 чиме добијамо $k \equiv 6 \pmod 8$, па је $k = 8l + 6$, за неко $l \in \mathbb{Z}$. Коначно, сва решења овог система конгруенција су бројеви $x = 7k + 3 = 7(8l + 6) + 3 = 56l + 45$, за $l \in \mathbb{Z}$.

б) Конгрусенција $x \equiv 5 \pmod{13}$ сквивалентна је са $x = 13k + 5$, за $k \in \mathbb{Z}$. Заменом у другу конгрусенцију добијамо $13k + 5 \equiv -1 \pmod 8$, тј. $5k \equiv 2 \pmod 8$. Како је $\mathrm{NZD}(5,8) = 1$, ову конгруенцију можемо помоножити са 5 чиме добијамо $k \equiv 2 \pmod 8$, па је $k = 8l + 2$, за $l \in \mathbb{Z}$. Дакле, $x = 13k + 5 = 13(8l + 2) + 5 = 104l + 31$, па заменом у последњу конгрусенцију добијамо

$$104l + 31 \equiv 4 \pmod 7.$$

Како је $104 \equiv 6 \pmod 7$ и $31 \equiv 3 \pmod 7$, ова конгрусенција сквивалентна је са $6l \equiv 1 \pmod 7$. Како је $\mathrm{NZD}(6,7) = 1$, ову конгруенцију можемо помоножити са 6 чиме добијамо $l \equiv 6 \pmod 7$, па је $l = 7r + 6$, за $r \in \mathbb{Z}$. Коначно, сва решења овог система конгруенција су бројеви

$$x = 104l + 31 = 104(7r + 6) + 31 = 728r + 655, \text{ за } r \in \mathbb{Z}.$$

в) Решимо прво дате три конгруенције. То можемо урадити тако што прву конгруенцију помножимо са 4, другу са 7, а трећу са 9, чиме добијамо сквивалентан систем конгусенција

$$x \equiv 4 \pmod 7, \quad x \equiv 5 \pmod 9, \quad x \equiv 5 \pmod{11}.$$

Прва конгрусенција сквивалентна је са $x = 7k + 4$, за $k \in \mathbb{Z}$. Заменом у другу конгрусенцију добијамо $7k + 4 \equiv 5 \pmod 9$, тј. $7k \equiv 1 \pmod 9$. Како је $\mathrm{NZD}(4,9) = 1$, ову конгруенцију можемо помоножити са 4 чиме добијамо $k \equiv 4 \pmod 9$, па је $k = 9l + 4$, за $l \in \mathbb{Z}$. Дакле, $x = 7k + 4 = 7(9l + 4) + 4 = 63l + 32$, па заменом у последњу конгруенцију добијамо

$$63l + 32 \equiv 5 \pmod{11}.$$

Како је $63 \equiv 8 \pmod{11}$ и $32 \equiv -1 \pmod{11}$, ова конгрусенција сквивалентна је са $8l \equiv 6 \pmod{11}$. Како је $\mathrm{NZD}(7,11) = 1$, ову конгрусенцију можемо помоножити са 7 чиме добијамо $l \equiv 9 \pmod{11}$, па је $l = 11r + 9$, за $r \in \mathbb{Z}$. Коначно, сва решења овог система конгруенција су бројеви

$$x = 63l + 32 = 63(11r + 9) + 32 = 693r + 599, \text{ за } r \in \mathbb{Z}.$$

3.15 Приметимо да је $2^3 \equiv 1 \pmod 7$, па 2 није примитивни корен по модулу 7. Број 3 јесте примитивни корен по модулу 7, што доказује следећа таблица:

n	0	1	2	3	4	5
$3^n \bmod 7$	1	3	2	6	4	5

из које читамо и вредности $\mathrm{ind}_3(n)$:

n	1	2	3	4	5	6
$\mathrm{ind}_3(n)$	0	2	1	4	5	3

.

Примитивни корени по модулу 7 су тачно они елементи $n \in \mathbb{Z}_7 \setminus \{0\}$ за које је НЗД$(\mathrm{ind}_3(n), 6) = 1$, па из претходне табеле налазимо да су једини примитивни корени по модулу 7 бројеви 3 и 5.

Сваки број из $\mathbb{Z}_7 \setminus \{0\}$ се на јединствен начин (по модулу 7) може записати као 3^y, па у свакој од наведених конгруенција уводимо смену $x \equiv 3^y \pmod 7$.

а) Коришћењем описане смене и таблице за $\mathrm{ind}_3(n)$ конгруенција $4x \equiv 3 \pmod 7$ своди се на $3^4 3^y \equiv 3^1 \pmod 7$, тј. на $3^{y+3} \equiv 1 \pmod 7$. Како је $3^n \equiv 1 \pmod 7$ ако и само ако $n \equiv 0 \pmod 6$ (јер је 3 примитивни корен по модулу 7), закључујемо да је дата конгруенција еквивалентна са $y \equiv 3 \pmod 6$. Дакле, $x \equiv 3^3 \equiv 6 \pmod 7$, па су сва решења дате конгруенције бројеви $x = 7k + 6$, за $k \in \mathbb{Z}$.

б) На сличан начин, конгруенција $x^2 \equiv 2 \pmod 7$ своди се на

$$3^{2y-2} \equiv 1 \pmod 7,$$

па је дата конгруенција еквивалентна са $2y \equiv 2 \pmod 6$. Као у задатку 3.13 може се добити да је решење ове конгруенције $y \equiv 1 \pmod 3$, тј. $y \equiv 1 \pmod 6$ или $y \equiv 4 \pmod 6$. Дакле, важи $x \equiv 3^1 \equiv 3 \pmod 7$ или $x \equiv 3^4 \equiv 4 \pmod 7$, па су сва решења дате конгруенције бројеви $x = 7k + 3$ и $x = 7k + 4$, за $k \in \mathbb{Z}$.

в) Конгруенција $x^3 \equiv 2 \pmod 7$ своди се на $3^{3y-2} \equiv 1 \pmod 7$, па је дата конгруенција еквивалентна са $3y \equiv 2 \pmod 6$. Како НЗД$(3, 6) = 3$ не дели 2 закључујемо да ова конгруенција нема решења.

г) Конгруенција $x^4 \equiv 3 \pmod 7$ своди се на $3^{4y-1} \equiv 1 \pmod 7$, па је дата конгруенција еквивалентна са $4y \equiv 1 \pmod 6$. Како НЗД$(4, 6) = 2$ не дели 1 закључујемо да ни ова конгруенција нема решења.

3.16 Следећа таблица доказује да је број 2 примитивни корен по модулу 11:

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

из које читамо и вредности $\mathrm{ind}_2(n)$:

n	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2(n)$	0	1	8	2	4	9	7	3	6	5

Примитивни корени по модулу 11 су тачно они елементи $n \in \mathbb{Z}_{11} \setminus \{0\}$ за које је НЗД$(\mathrm{ind}_2(n), 10) = 1$, па из претходне табеле налазимо да су примитивни корени по модулу 11 бројеви 2, 6, 7 и 8.

Сваки број из $\mathbb{Z}_{11} \setminus \{0\}$ се на јединствен начин (по модулу 11) може записати као 2^y, па у свакој од наведених конгруенција уводимо смену $x \equiv 2^y \pmod{11}$.

а) Коришћењем описане смене и таблице за $\mathrm{ind}_2(n)$ конгруенција $4x \equiv 3 \pmod{11}$ своди се на $2^2 2^y \equiv 2^8 \pmod{11}$, тј. на $2^{y-6} \equiv 1 \pmod{11}$. Како је $2^n \equiv 1 \pmod{11}$ ако и само ако $n \equiv 0 \pmod{10}$ (јер је 2 примитивни корен по модулу 11), закључујемо да је дата конгруенција еквивалента са $y \equiv 6 \pmod{10}$. Даклe, $x \equiv 2^6 \equiv 9 \pmod{11}$, па су сва решења дате конгруенције бројеви $x = 11k + 9$, за $k \in \mathbb{Z}$.

б) На сличан начин, $x^2 \equiv 3 \pmod{11}$ своди се на $2^{2y-8} \equiv 1 \pmod{11}$, па је почетна конгруенција еквивалентна са $2y \equiv 8 \pmod{10}$. Као у задатку 3.13 добијамо да је решење ове конгруенције $y \equiv 4 \pmod{5}$, тј. $y \equiv 4 \pmod{10}$ или $y \equiv 9 \pmod{10}$. Даклe, $x \equiv 2^4 \equiv 5 \pmod{11}$ или $x \equiv 2^9 \equiv 6 \pmod{11}$, па су сва решења дате конгруенције бројеви $x = 11k + 5$ и $x = 11k + 6$, за $k \in \mathbb{Z}$.

в) Конгруенција $x^3 \equiv 2 \pmod{7}$ своди се на $2^{3y-1} \equiv 1 \pmod{11}$, па је дата конгруенција еквивалентна са $3y \equiv 1 \pmod{10}$. Као у задатку 3.13 добијамо да је решење ове конгруенције $y \equiv 7 \pmod{10}$. Даклe, важи $x \equiv 2^7 \equiv 7 \pmod{11}$, па су сва решења дате конгруенције бројеви $x = 11k + 7$, за $k \in \mathbb{Z}$.

г) Конгруенција $x^4 \equiv -3 \equiv 8 \pmod{11}$ своди се на $2^{4y-3} \equiv 1 \pmod{11}$, па је еквивалентна са $4y \equiv 3 \pmod{10}$. Као НЗД$(4, 10) = 2 \nmid 3$ закључујемо да ова конгруенција нема решења.