Algebra liniowa 2

dr Joanna Jureczko

Zestaw zadań nr 3

Pierścień Pierścienie klas reszt
Pierścień $\mathbb{Z}_n$
Małe Twierdzenie Fermata
Chińskie Twierdzenie o resztach

3.1. Które z poniższych zbiorów są pierścieniami ze względu na dodawanie i mnożenie? Odpowiedź uzasadnić.

a) $\{a + b\sqrt{5} \colon a, b \in \mathbb{Z}\}$,

b) $\mathbb{N}$,

c) $\{a + b\sqrt{2} + c\sqrt{3} \colon a, b, c \in \mathbb{Z}\}$,

d) $\{a + b\sqrt[3]{2} \colon a, b \in \mathbb{Q}\}$,

e) wszystkie macierze 2×2 z zerowym wyznacznikiem,

f) wszystkie liczby wymierne, które można zapisać z mianownikiem 2,

g) wszystkie liczby wymierne, które można zapisać z mianownikiem będącym liczbą nieparzystą.

3.2. Wyznaczyć grupę elementów odwracalnych i dzielniki zera pierścienia: a) $\mathbb{Z}_4$, b) $\mathbb{Z}_{10}$, c) $\mathbb{Z}_{16}$.

3.3. Wyznaczyć wszystkie odwracalne klasy reszt modulo 25 i obliczyć ich elementy odwrotne.

3.4. Rozwiązać równania

a) $5x^2 + 5x + 1 = 0$ w $\mathbb{Z}_{11}$, b) $x^2 + x + 3 = 0$ w $\mathbb{Z}_5$

c) $2x^2 + 2x + 2 = 0$ w $\mathbb{Z}_{13}$ d) $2x^3 + 3x^2 + x + 3 = 0$ w $\mathbb{Z}_7$.

3.5. Rozwiązać układy równań

a) $\begin{cases} 3x + 5y = 2 \\ 4x + 9y = 4 \end{cases}$ w $\mathbb{Z}_7$ i $\mathbb{Z}_{13}$, b) $\begin{cases} 5x + 4y = 1 \\ 4x + 3y = 1 \end{cases}$ w $\mathbb{Z}_5$ i $\mathbb{Z}_{11}$.

3.6. Rozwiązać układy równań

a) $\begin{cases} 2x + 7y + 3z + t = 6 \\ 3x + 5y + 2z + 2t = 4 \\ 9x + 4y + z + 7t = 2 \end{cases}$ w $\mathbb{Z}_{11}$, b) $\begin{cases} 6x + 3y + 2z + 3t + 4w = 5 \\ 4x + 2y + z + 2t + 3w = 4 \\ 4x + 2y + 3z + 2t + w = 0 \\ 2x + y + 7z + 3t + 2w = 1 \end{cases}$ w $\mathbb{Z}_{11}$.

3.7. Każdy z następujących układów rozwiązać w $\mathbb{Z}_p$ dla $p = 5, 7, 11$

a) $\begin{cases} x + 4y + 3z = 2 \\ 3x + 2y + 4z = 3 \\ 4x + y + z = 0 \end{cases}$ b) $\begin{cases} 2x + 3y + z = 1 \\ x + 4y + 3z = 3 \\ 4x + 3z = 2 \end{cases}$

3.8. Obliczyć wyznaczniki macierzy

a) $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 5 & 3 \\ 1 & 3 & 2 & 4 \\ 2 & 2 & 1 & 4 \end{bmatrix}$ w $\mathbb{Z}_7$ b) $\begin{bmatrix} 1 & 1 & 1 & 2 \\ 1 & 3 & 1 & 3 \\ 1 & 1 & 4 & 3 \\ 3 & 0 & 8 & 10 \end{bmatrix}$ w $\mathbb{Z}_{11}$.

3.9. Obliczyć wartości funkcji Eulera dla n, gdy a) $n = 37$, b) $n = 243$, c) $n = 333$, d) $n = 10!$, e) $n = 1001$, f) $n = 46189$.

3.10. Obliczyć a) 2^{20} $(mod\ 7)$, b) 67^{43} $(mod\ 14)$, c) 67^{43} $(mod\ 17)$, d) 67^{43} $(mod\ 16)$, e) 345^{679} $(mod\ 16)$, f) 114^{273} $(mod\ 25)$.

3.11. Niech a będzie liczbą całkowitą dodatnią taką, że $NWD(a, n) = 1$. Wyznaczyć k, dla których zachodzi $n|a^k - a$, gdy a) $n = 7$, b) $n = 21$, c) $n = 81$, d) $n = 105$, e) $n = 10395$.

3.12. Stosując Małe Twierdzenie Fermata (lub jego uogólnienie) obliczyć a) $13^{101}(mod 16)$, b) $7^{137}(mod 23)$, c) $63^{111}(mod 17)$, d) $4^{288}(mod 13)$, e) $5^{555}(mod 7)$.

3.13. Rozwiązać kongruencje:

a) $19x \equiv 9\ (mod\ 79)$,

b) $17x \equiv 9\ (mod\ 83)$,

c) $18x \equiv 97\ (mod\ 107)$.

3.14. Rozwiązać kongruencje:

a) $949x \equiv 348\ (mod\ 53^2)$,

b) $739x \equiv 1226\ (mod\ 13^3)$.

3.15. Rozwiązać układ kongruencji $x \equiv 1(mod\ p)$, gdzie $p \in \{2, 3, 5, 7\}$.

3.16. Rozwiązać układ kongruencji:

a) $\begin{cases} x \equiv 3\ (mod\ 7) \\ x \equiv 7\ (mod\ 20) \end{cases}$ b) $\begin{cases} x \equiv 0\ \ (mod\ 14) \\ x \equiv 10\ (mod\ 17) \end{cases}$ c) $\begin{cases} x \equiv 4\ (mod\ 9) \\ x \equiv 1\ (mod\ 22) \end{cases}$

3.17. Rozwiązać układ kongruencji:

a) $\begin{cases} x \equiv 4\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \\ x \equiv 7\ (mod\ 8) \end{cases}$ b) $\begin{cases} x \equiv 2\ (mod\ 7) \\ x \equiv 8\ (mod\ 10) \\ x \equiv 4\ (mod\ 13) \end{cases}$

3.18. Rozwiązać układ kongruencji:

a) $\begin{cases} 11x \equiv 17\ (mod\ 20) \\ 13x \equiv 11\ (mod\ 35) \end{cases}$ b) $\begin{cases} 5x \equiv 13\ \ (mod\ 18) \\ 17x \equiv 11\ (mod\ 20) \\ 23x \equiv 19\ (mod\ 30) \end{cases}$

3.19. Wskazać i rozwiązać odpowiedni układ kongruencji równoważny z daną kongruencją

a) $58x \equiv 137\ (mod\ 143)$,

b) $1793x \equiv 765\ (mod\ 2448)$,

c) $87x \equiv 202\ (mod\ 221)$.

3.20.* Udowodnić małe twierdzenie Fermata.

3.21.* Udowodnić chińskie twierdzenie o resztach.

Odpowiedzi:

3.1. a) tak, b) nie, c) nie, d) tak, e) nie, f) tak, g) tak.

3.2. a) NWD(a, 4)= 1, $1 + 4\mathbb{Z}$, b) NWD(a, 10) =1, $1 + 10\mathbb{Z}, 3 + 10\mathbb{Z}, 7 + 10\mathbb{Z}, 9 + 10\mathbb{Z}$, c) NWD(a, 16) = 1, $1 + 16\mathbb{Z}, 3 + 16\mathbb{Z}, 5 + 16\mathbb{Z}, 7 + 16\mathbb{Z}$.

3.3. NWD(a, 25) =1, $1 + 25\mathbb{Z}, 2 + 25\mathbb{Z}, 3 + 25\mathbb{Z}, 4 + 25\mathbb{Z}, 6 + 25\mathbb{Z}, 7 + 25\mathbb{Z}, 8 + 25\mathbb{Z}, 9 + 25\mathbb{Z}, 11 + 25\mathbb{Z}, 12 + 25\mathbb{Z}, 13 + 25\mathbb{Z}, 14 + 25\mathbb{Z}, 16 + 25\mathbb{Z}, 17 + 25\mathbb{Z}, 18 + 25\mathbb{Z}, 19 + 25\mathbb{Z}, 21 + 25\mathbb{Z}, 22 + 25\mathbb{Z}, 23 + 25\mathbb{Z}, 24 + 25\mathbb{Z}$.

3.4. a) 1,9, b) 1,3, c) 3,9, d) brak rozwiązań.

3.5. a) w $\mathbb{Z}_7$ brak rozwiązań; w $\mathbb{Z}_{13}$ $x = 9, y = 8$, b) w $\mathbb{Z}_5$ $x = 1, y = 4$; w $\mathbb{Z}_{11}$ $x = 1, y = 10$.

3.6. Układy mają nieskończenie wiele rozwiązań. Wskazówka: zastosować twierdzenie Kroneckera-Capellego.

3.7. a) w $\mathbb{Z}_5$ brak rozwiązań, w $\mathbb{Z}_7$ nieskończenie wiele rozwiązań, w $\mathbb{Z}_{11}$ $x = 6, y = 4, z = 8$, b) w $\mathbb{Z}_7$ brak rozwiązań, w $\mathbb{Z}_5$ nieskończenie wiele rozwiązań, w $\mathbb{Z}_{11}$ $x = 3, y = 8, z = 4$,

3.8. a) 1, b) 1.

3.9. a) $\varphi(37) = 36$, b) $\varphi(243) = 3^4 \cdot 2$, c) $\varphi(333) = 6 \cdot 36$, d) $\varphi(110!) = 2^{10} \cdot 3^3 \cdot \cdot 5$, e) $\varphi(1001) = 6 \cdot 10 \cdot 12$, f) $\varphi(46189) = 10 \cdot 12 \cdot 16 \cdot 18$.

3.10. a) $2^{20} = 4(mod\ 7)$, b) 11, c) 16, d) 11, e) 9, f) 19.

3.11. Wskazówka: zastosować Małe Tiwerdzenie Fermata $a^{\varphi(m)} \equiv 1(mod\, m) \leftrightarrow a^{\varphi(m)-1} - a \equiv 0(mod\, m) \leftrightarrow m|a^{\varphi(m)+1} - a \leftrightarrow k = \varphi(m)+1$, a) $k = \varphi(7)+1 = 7$, b) $k = \varphi(21)+1 = 13$, c) $k = \varphi(81) + 1 = 55$, d) $k = \varphi(105) + 1 = 49$, e) $k = \varphi(10395) + 1 = 4321$.

3.12. a) 40, b) 17, c) 10, d) 1, e) 6.

3.13. a) $x \equiv 67(mod\ 79)$, b) $x \equiv 64(mod\ 83)$, c) $x \equiv 47(mod\ 107)$.

3.14. a) $x \equiv 471(mod\ 53^2)$, b) $x \equiv 843(mod\ 13^3)$.

3.15. $x \equiv 1(mod\ 20)$.

3.16. a) $x \equiv 87(mod\ 140)$, b) $x \equiv 112(mod\ 238)$, c) $x \equiv 67(mod\ 198)$.

3.17. a) $x \equiv 159(mod\ 280)$, b) $x \equiv 758(mod\ 910)$.

3.18. a) $x \equiv 87(mod\ 140)$, b) $x \equiv 143(mod\ 180)$.

3.19. a) $x \equiv 64(mod\ 143)$, b) $x \equiv 765(mod\ 2448)$, c) $x \equiv 203(mod\ 221)$.