

Zadania podstawowe

- Rozstrzygnij, czy $\mathbb{F}_5[\gamma]$, gdzie γ spełnia podane równanie, jest ciałem.
(a) $\gamma^3 + 3\gamma^2 + 4\gamma + 4 = 0$, (c) $\gamma^3 + 3\gamma^2 + 2\gamma + 4 = 0$, (e) $\gamma^3 + 2\gamma + 1 = 0$.
(b) $\gamma^3 + 3\gamma^2 + 3 = 0$, (d) $\gamma^3 + \gamma + 1 = 0$.
- W ciele $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, gdzie γ spełnia $\gamma^2 + 2\gamma + 2 = 0$, oblicz (tzn. przedstaw w postaci $a + b\gamma$, $a, b \in \mathbb{F}_3$):
(a) $(2\gamma + 1) \cdot (\gamma + 2)$, (c) $(2\gamma + 1)/(\gamma + 1)$, (e) $(\gamma + 1)^9$,
(b) $(\gamma + 2) \cdot (\gamma + 1)$, (d) $\gamma/(2\gamma + 1)$, (f) $(\gamma + 2)^9$.
- W ciele $\mathbb{F}_{27} = \mathbb{F}_3[\gamma]$, gdzie γ spełnia $\gamma^3 + 2\gamma + 1 = 0$, oblicz (tzn. przedstaw w postaci $a + b\gamma + c\gamma^2$, $a, b, c \in \mathbb{F}_3$):
(a) $(2\gamma^2 + 1) \cdot (\gamma + 2)$, (c) $(2\gamma + 1)/(\gamma + 1)$, (e) $(\gamma + 1)^{27}$,
(b) $(\gamma^2 + 2) \cdot (\gamma + 1)$, (d) $\gamma/(2\gamma + 1)$, (f) $(\gamma + 2)^{27}$.
- Niech $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, gdzie $\gamma^2 + 2\gamma + 2 = 0$. Wykaż, że γ jest generatorem, tzn. że $\mathbb{F}_9 \setminus \{0\} = \{1, \gamma, \gamma^2, \dots, \gamma^7\}$.
- Element $s \in \mathbb{F}_{p^n}$ nazywamy pierwiastkiem (pierwotnym) z jedynki stopnia m , jeżeli $s^m = 1$ oraz $s^k \neq 1$ dla $0 < k < m$.
(a) Znajdź pierwiastki pierwotne z jedynki stopnia 4 w $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, gdzie $\gamma^2 + 2\gamma + 2 = 0$.
(b) Wykaż, że $\mathbb{F}_{p^n}$ zawiera pierwiastki (pierwotne) z jedynki stopnia m wtw. gdy $m|p^n - 1$.
- (a) Rozwiąż w $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, gdzie $\gamma^2 + 2\gamma + 2 = 0$, równanie $x^3 = \gamma$.
(b) Wykaż, że dla dowolnego $a \in \mathbb{F}_{p^n}$ równanie $x^p = a$ ma dokładnie jedno rozwiązanie w ciele $\mathbb{F}_{p^n}$.
(Wskazówka: wykaż, że funkcja $x \mapsto x^p$ jest różnowartościowa. Co można powiedzieć o funkcji różnowartościowej $f : X \rightarrow X$, gdzie $|X| < \infty$?)
- Wykaż, że ciała $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, gdzie $\gamma^2 + 2\gamma + 2 = 0$ oraz $\mathbb{F}'_9 = \mathbb{F}_3[\gamma']$, gdzie $(\gamma')^2 + \gamma' + 2 = 0$, są "takie same". (Wskazówka: jakie pierwiastki ma wielomian $x^2 + x + 2$ w ciele $\mathbb{F}_9$? Znajdź pierwiastek postaci $a + b\gamma$)
- Niech $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, gdzie $\gamma^2 + 2\gamma + 2 = 0$. Sprawdź, że mnożenie przez γ "przestawia" niezerowe elementy $\mathbb{F}_9$. Z czego to wynika?
- Wykaż, że ciała $\mathbb{F}_p[\sqrt{c_1}]$ oraz $\mathbb{F}_p[\sqrt{c_2}]$, gdzie $c_1, c_2 \in \mathbb{F}_p$ są dowolnymi nieresztami kwadratowymi, są "takie same".
(Wskazówka: wykaż, że $c_1 = a^2 \cdot c_2$ dla pewnego $a \in \mathbb{F}_p$)

Zadania bardziej zaawansowane

- Charakterystyką ciała nazwiemy najmniejszą liczbę $n \geq 1$ taką, że $\underbrace{1 + 1 + \dots + 1}_n = 0$.
(a) Znajdź charakterystykę ciała $\mathbb{F}_p$.
(b) Wykaż, że charakterystyka dowolnego ciała skończonego jest liczbą pierwszą.
(c) Wykaż, że jeżeli istnieje ciało n -elementowe, to n jest potęgą liczby pierwszej.
(Wskazówka: skorzystaj z tw. Cauchy'ego – jeżeli $\oplus$ jest "ładnym" działaniem na zbiorze n -elementowym X , 0 jest elementem neutralnym $\oplus$, oraz $q \in \mathbb{P}$, $q|n$, to istnieje $x \in X$, $x \neq 0$ taki że $\underbrace{x \oplus x \oplus \dots \oplus x}_q = 0$.)
- (a) Wykaż, że $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ wtw. gdy $n|m$.

(Wskazówka: skorzystaj z tego, że $\mathbb{F}_{p^n} = \{\alpha : \alpha^{p^n} = \alpha\}$)

(b) Wykaż, że $\mathbb{F}_{p^{1!}} \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \mathbb{F}_{p^{4!}} \subset \dots$

(c) Niech $\overline{\mathbb{F}}_p := \mathbb{F}_{p^{1!}} \cup \mathbb{F}_{p^{2!}} \cup \mathbb{F}_{p^{3!}} \cup \mathbb{F}_{p^{4!}} \cup \dots$. Wykaż, że $\overline{\mathbb{F}}_p$ jest (nieskończonym) ciałem oraz że dowolny wielomian $f \in \mathbb{F}_p[x]$ ma pierwiastek w $\overline{\mathbb{F}}_p$.

3. (a) Rozłóż $x^9 - x \in \mathbb{F}_3[x]$ na czynniki nierozkładalne. Sprawdź bezpośrednio, że wielomian ten jest iloczynem wszystkich nierozkładalnych wielomianów stopnia 1 oraz 2 o najwyższym współczynniku równym 1.

(b) Wykaż, że $x^{p^n} - x \in \mathbb{F}_p[x]$ jest iloczynem wszystkich wielomianów nierozkładalnych $f \in \mathbb{F}_p[x]$ o najwyższym współczynniku n oraz takich, że $\deg f | n$.

Wskazówka: skorzystaj z następującego faktu – jeżeli $f \in \mathbb{F}_p[x]$ jest wielomianem nierozkładalnym, $a \in \mathbb{F}_{p^n}$ jego pierwiastkiem, zaś $g \in \mathbb{F}_p[x]$ spełnia $g(a) = 0$, to $f | g$.

4. Oblicz $Z(t) := \prod_P (1 - t^{\deg P})^{-1}$, gdzie iloczyn ten przebiega wszystkie wielomiany nierozkładalne $P \in \mathbb{F}_q[t]$ o współczynniku przy najwyższej potędze równym 1. Jest to tzw. **funkcja dzeta** ciała skończonego.

(Wskazówka: rozwiń czynniki w szeregi geometryczne)

5. (a) Wykaż, że jeżeli $\gamma \in \mathbb{F}_{p^k}$ jest pierwiastkiem wielomianu $x^p - x - a \in \mathbb{F}_p[x]$, to $\gamma + 1, \gamma + 2, \dots, \gamma + (p-1)$ również są pierwiastkami tego wielomianu.

(b) Wykaż, że wielomian $x^p - x - a \in \mathbb{F}_p[x]$ jest nierozkładalny.

(c) Wykaż, że jeżeli wielomian $x^{p^n} - x - a$ jest nierozkładalny dla $a \in \mathbb{F}_p$, to $n = 1$ lub $n = p = 2$.

6. Niech $p \neq q$ będą liczbami pierwszymi. Wykaż, że wielomian $1 + x + \dots + x^{q-1}$ rozkłada się modulo p na $(q-1)/f$ czynników stopnia f , gdzie $f := \text{ord}_q(p)$ (tzn. $f = \min\{n : p^n \equiv 1 \pmod{q}\}$).

(Wsk. zrób zadanie o pierwiastkach z jedynki. Jakie jest najmniejsze n takie, że q -ty pierwiastek z jedynki należy do $\mathbb{F}_{p^n}$?)

7. Celem zadania jest dowód prawa wzajemności reszt kwadratowych. Niech $p \neq q$ będą liczbami pierwszymi. Dla uproszczenia przyjmijmy, że $4 | q-1$. Chcemy wówczas pokazać, że q jest resztą kwadratową mod p wtw. gdy p jest resztą kwadratową mod q . Rozważmy wielomian Gaussa:

$$g_q(x) := \sum_{k=1}^{q-1} \left(\frac{k}{q} \right) x^k \in \mathbb{F}_p[x].$$

(a) Wykaż, że $g_q(\omega)^p = \left(\frac{p}{q} \right) \cdot g_q(\omega)$.

(b) Wykaż, że jeżeli $\omega \in \mathbb{F}_{p^n}$ jest pierwiastkiem pierwotnym stopnia q , to $g_q(\omega)^2 = q$.

(Wsk. możesz skorzystać z równości $\sum_{k=0}^{q-1} \left(\frac{k \cdot (t-k)}{q} \right) = 0$ dla $t \neq 0$)

(c) Wykaż, że q jest resztą kwadratową mod p wtw. gdy $g_q(\omega) \in \mathbb{F}_p$ wtw. p jest resztą kwadratową mod q .

(Wsk. dla $g \in \mathbb{F}_{p^n}$ mamy $g \in \mathbb{F}_p$ wtw. gdy $g^p = g$)

8. Niech $(F_n)_n$ będzie ciągiem Fibonacciego, tzn.

$$F_0 = 0, F_1 = 1, F_{n+2} = F_n + F_{n+1}.$$

Okresem $(F_n)_n$ modulo p nazywamy najmniejszą liczbę $r > 0$ taką, że $F_n \equiv F_{n+r} \pmod{p} \forall n \geq 0$.

(a) Znajdź okres ciągu Fibonacciego modulo 7.

(b) Skąd wiadomo, że dla każdego p ciąg ten posiada okres?

(c) Wykaż, że okres ciągu Fibonacciego dzieli $p^2 - 1$ oraz że dla $p \equiv \pm 1 \pmod{5}$ okres ten dzieli $p - 1$.

Wskazówka: skorzystaj ze wzoru Bineta: $F_n = \frac{A^n - B^n}{A - B}$, gdzie A oraz B są pierwiastkami równania $x^2 - x - 1 = 0$. Przejdź do ciała skończonego, w którym to równanie ma rozwiązanie.