Lista 14

Zadanie 1. Niech $\mathbb{F}$ będzie ciałem skończonym o n elementach. Pokaż, że w $\mathbb{F}[x]$ prawdziwa jest zależność:

$$x^n - x = \prod_{a \in \mathbb{F}} (x - a) \ .$$

Wskazówka: Porównaj pierwiastki obydwu wielomianów oraz ich wiodące współczynniki.

Zadanie 2. Pokaż, że dla liczby pierwszej p istnieje wielomian nierozkładalny stopnia 2 w $\mathbb{Z}_p[x]$.

Wskazówka: Zliczyć wszystkie wielomiany stopnia 2 w $\mathbb{Z}_p[x]$ oraz wszystkie rozkładalne wielomiany stopnia 2 w $\mathbb{Z}_p[x]$: zauważ, że muszą się one rozkładać na wielomiany stopnia 1.

Zadanie 3. Operację różniczkowania wielomianów nad ciałem $\mathbb{F}$ definiujemy analogicznie, jak w przypadku liczb rzeczywistych, tzn. $\left(\sum_{i=0}^{n} a_i x^i\right)' = \sum_{i=1}^{n} i a_i x^{i-1}$, formalnie

$$(a_0, a_1, a_2, \ldots, a_n) \mapsto (a_1, 2a_2, 3a_3, \ldots, na_n, 0)$$

przy czym „i" w „ia_i" rozumiemy tu jako element w $\mathbb{F}$ uzyskany poprzez i-krotne dodanie 1 (elementu neutralnego mnożenia) w ciele $\mathbb{F}$, tzn. $i = \underbrace{1 + 1 + \cdots + 1}_{i \text{ razy}}$.

Udowodnij, że w dowolnym pierścieniu wielomianów $\mathbb{F}[x]$ o współczynnikach z ciała $\mathbb{F}$ różniczkowanie ma te same własności, co w przypadku współczynników rzeczywistych, tzn.:

- jest liniowe: $(\alpha f + \beta g)' = \alpha f' + \beta g'$ dla $\alpha, \beta \in \mathbb{F}$, $f, g \in \mathbb{F}[x]$;
- $(fg)' = f'g + fg'$ dla $f, g \in \mathbb{F}[x]$;
- $(x - \alpha)^k = k(x - \alpha)^{k-1}$;
- $(f \circ g)' = (f' \circ g) \cdot g'$.

W zależności od metody, dwa ostatnie punkty być może wolisz pokazać w odwrotnej kolejności.

Wskazówka: Przy dowodzeniu drugiego punktu skorzystaj z punktu pierwszego i sprowadź problem do przypadku, w którym $f = x^k$, $g = x^\ell$.

Zadanie 4. Udowodnij, że dla wielomianu $f \in \mathbb{F}[x]$ jeśli liczba $\alpha \in \mathbb{F}$ jest pierwiastkiem k-krotnym tego wielomianu, to

$$\overline{f}(\alpha) = \overline{f'}(\alpha) = \overline{f''}(\alpha) = \cdots = \overline{f^{(k-1)}}(\alpha) = 0 \ .$$

Zadanie 5. Rozważmy wielomiany o współczynnikach z ciała $\mathbb{F}$. Dla jakich a, b wielomian

$$X^5 + aX^3 + b$$

ma pierwiastek podwójny (dopuszczamy większe krotności), jeśli

- $\mathbb{F} = \mathbb{R}$?
- $\mathbb{F} = \mathbb{Z}_3$?
- $\mathbb{F} = \mathbb{Z}_5$?

Możesz skorzystać z Zadania 4, nawet jeśli nie umiesz go udowodnić.

Wskazówka: Rozważ osobno przypadki $a = 0$ oraz $b = 0$. Pomocne też może być Zadanie 1. Ponadto dla ciał skończonych być może konieczne będzie sprawdzenie dla ustalonych a, b wszystkich potencjalnych pierwiastków ręcznie.

Zadanie 6. Znajdź wielomiany najniższego możliwego stopnia, spełniające warunki

- $\overline{f}(-1) = -12$, $\overline{f}(0) = -7$, $\overline{f}(1) = -6$ (w $\mathbb{R}$);
- $\overline{g}(0) = 3$, $\overline{g}(1) = 4$, $\overline{g}(4) = 3$ (w $\mathbb{Z}_5$);
- $\overline{h}(0) = 1$, $\overline{h}(1) = 2$, $\overline{g}(h) = 0$ (w $\mathbb{Z}_3$);
- $\overline{i}(1) = 3$, $\overline{i}(2) = 6$, $\overline{i}(4) = 2$ (w $\mathbb{Z}_7$);
- $\overline{j}(1) = 3$, $\overline{j}(2) = 10$, $\overline{j}(3) = 23$ (w $\mathbb{R}$).

Zadanie 7 (* nie liczy się do podstawy)**.** Udowodnij, że nie istnieją kody korygujące błędy, które poprawiają więcej błędów, niż kody Reeda-Salomona.

W tym celu pokaż, że jeśli w $\mathbb{F}^n$, które traktujemy jako n-elementowe wektory elementów z $\mathbb{F}$, mamy wybrane $|\mathbb{F}|^k$ wektorów, to któreś dwa z nich różnią się na najwyżej $n-k+1$ pozycjach.

Wskazówka: Podziel całe $\mathbb{F}^n$ na "stożki": jeden stożek ma ustalone pierwsze k współrzędnych i dowolne $u-k$ dalsze współrzędne.

Zadanie 8. Opisz konstrukcję ciała $\mathbb{F}_8$ o ośmiu elementach. Wskaż generator grupy multiplikatywnej $\mathbb{F}_8^*$ (np. zgadując go i sprawdzając, że rzeczywiście jest generatorem).

Zadanie 9. W ciele $\mathbb{F}$ rozważmy kolejne sumy

$$1, 1+1, 1+1+1, \dots \ ,$$

gdzie 1 jest elementem neutralnym dodawania. Niech k będzie najmniejszą taką liczbą, że $\underbrace{1+1+\cdots+1}_{k \text{ razy}} = 0$. Pokaż, że jeśli takie skończone k istnieje, to jest liczbą pierwszą. (Może nie istnieć, np. w liczbach wymiernych).

Zadanie 10. Znajdź wszystkie wielomiany nierozkładalne stopnia 2 w $\mathbb{Z}_3[x]$. Dla każdego z nich opisz konstrukcję ciała o dziewięciu elementach. Wskaż izomorfizmy między tymi ciałami.

Zadanie 11. Pokaż, że podgrupa $H \leq G$ grupy cyklicznej G jest cykliczna.

Wskazówka: Niech $G = \langle g \rangle$, w H wybierz g^u o minimalnym niezerowym u. Dowód jest taki sam dla skończonego i nieskończonego G.

Możesz też skorzystać z tego, że G jest izomorficzne z $(\mathbb{Z}_u, +_u)$ lub z $(\mathbb{Z}, +)$.