Lista 16

Zadanie 1. Wyznacz największy wspólny dzielnik par wielomianów (o ile nie jest napisane inaczej: w $\mathbb{R}[x]$)

- $x^4 - 2x^3 - 19x^2 + 8x + 60$ oraz $x^4 + 5x^3 + 5x^2 - 5x - 6$;
- $x^4 + x^3 + 2x^2 + 2x$ oraz $x^4 + 2x^3 + 2x^2 + x$ (w $\mathbb{Z}_3[x]$)
- $f = x^p + 1$, $g = x + 1$ (w $\mathbb{Z}_p[X]$ dla p—pierwszego).

Wyraź nwd jako kombinację podanych wielomianów.

Wskazówka: Do ostatniego: policz, ile wynosi $(x+1)^p$ w $\mathbb{Z}_p$.

Rozwiązanie Niech $f =, x^4 - 2x^3 - 19x^2 + 8x + 60$.

$$\begin{array}{r|l} & 1 \\ \hline x^4 - 2x^3 - 19x^2 + 8x + 60 & x^4 + 5x^3 + 5x^2 - 5x - 6 \\ & -x^4 + 2x^3 + 19x^2 - 8x - 60 \\ \hline & 7x^3 + 24x^2 - 13x - 66 \end{array}$$

Czyli

$$f' = f - g = 7x^3 + 24x^2 - 13x - 66$$

oraz $\mathrm{nwd}(f, g) = \mathrm{nwd}(f', g)$.

$$\begin{array}{r|l} & \frac{1}{7}x - \frac{38}{49} \\ \hline 7x^3 + 24x^2 - 13x - 66 & x^4 - 2x^3 - 19x^2 + 8x + 60 \\ & -x^4 - \frac{24}{7}x^3 + \frac{13}{7}x^2 + \frac{66}{7}x \\ \hline & -\frac{38}{7}x^3 - \frac{120}{7}x^2 + \frac{122}{7}x + 60 \\ & \frac{38}{7}x^3 + \frac{912}{49}x^2 - \frac{494}{49}x - \frac{2508}{49} \\ \hline & \frac{72}{49}x^2 + \frac{360}{49}x + \frac{432}{49} \end{array}$$

$$g - (\frac{x}{7} - \frac{38}{49})f' = \frac{72}{49}(x^2 + 5x + 6)$$

Przekształcając mamy

$$x^2 + 5x + 6 = \frac{1}{72}(49g - (7x - 38)f')$$

I dalej

$$\begin{array}{r|l} & 7x - 11 \\ \hline x^2 + 5x + 6 & 7x^3 + 24x^2 - 13x - 66 \\ & -7x^3 - 35x^2 - 42x \\ \hline & -11x^2 - 55x - 66 \\ & 11x^2 + 55x + 66 \\ \hline & 0 \end{array}$$

Czyli największy wspólny dzielnik to $x^2 + 5x + 6$. Wstawiając wyrażanie na f' dostajemy

$$\frac{1}{72}(49g - (7x - 38)(f - g)) = \frac{7x + 11}{72}g - \frac{7x - 38}{72}f$$

W drugim przykładzie, oznaczmy pierwszy wielomian przez f a drugi przez g. Wtedy

$$g' = g - f = x^3 + x$$

Potem

W ostatnim przykładzie zauważmy, że

$$(x+1)^p =_p \sum_{i=0}^{p} \binom{n}{i} x^i$$

Zauważmy, że $\binom{p}{i}$ dzieli się przez p dla $i \notin \{0, p\}$, czyli

$$(x+1)^p =_p x^p + 1$$

I w takim razie $\mathrm{nwd}(x^p + 1, x + 1) = x + 1$.

Zadanie 2. Korzystając z tw. Bezout rozłóż poniższe wielomiany z $\mathbb{Z}_2[x]$ na czynniki nierozkładalne

$$x^5+x^3+x+1, \quad x^4+x^3+x^2+1, \quad x^5+x^2+x, \quad x^4+x^2+1, \quad x^4+x^2+x \ .$$

Potraktuj powyższe wielomiany jako wielomiany z $\mathbb{Z}_3[x]$ i również rozłóż je na czynniki nierozkładalne.

Wskazówka: Być może konieczne też będzie osobne zastanowienie się, które wielomiany drugiego stopnia są nierozkładalne.

Rozwiązanie Rozpatrzmy wielomian x^5+x^3+x+1 jako wielomian o współczynnikach z $\mathbb{Z}_2$. Zauważmy, że jeśli jest on rozkładalny, to ma czynnik stopnia najwyżej 2. Sprawdźmy najpierw czynniki liniowe, czyli policzmy wartość w $0, 1$. Łatwo sprawdzić, że wartość w 1 to 1. Wartość w 0 to 0, czyli dzieli się przez $x+1$. Można podzielić, albo zauważyć

$$x^5+x^3+x+1 = x^5+2x^4+x^3+x+1 = (x+1)(x^4+x^3+1)$$

Wielomian x^4+x^3+1 ma wartość 1 w 1, nie dzieli się więc przez $x+1$. Pozostaje sprawdzić, czy dzieli się przez x^2+x+1 (jedyny nierozkładalny stopnia 2). Jedynym możliwym rozkładem jest $(x^2+x+1)^2$:

$$(x^2+x+1)^2 = x^4+x^2+1$$

czyli x^4+x^3+1 jest nierozkładalny.

Zadanie 3. Wielomian f ma resztę z dzielenia przez $x - c_1$ równą r_1 oraz resztę z dzielenia przez $x - c_2$ równą r_2. Ile wynosi reszta z dzielenia f przez $(x - c_1)(x - c_2)$?

Wystarczy, że zapiszesz zależność na współczynniki tego wielomianu, nie musisz jej rozwiązywać.

Wskazówka: Skorzystaj z tw. Bezout.

Rozwiązanie Reszta jest postaci $ax + b$, tj.

$$f = (x - c_1)(x - c_2) + ax + b$$

Przy czym

$$f(c_1) = r_1 \quad f(c_2) = r_2$$

Co daje układ równań liniowych na a, b:

$$ac_1 + b = r_1 \quad ac_2 + b = r_2$$

Zadanie 4. Niech f, g, f', g', a będą niezerowymi wielomianami z pierścienia wielomianów $\mathbb{F}[x]$ o współczynnikach z ciała $\mathbb{F}$. Załóżmy, że $f = af'$ oraz $g = ag'$.

- Jeśli $h' = \operatorname{nwd}(f', g')$, to ile wynosi $\operatorname{nwd}(f, g)$? Jeśli $h' = a'f' + b'g'$ dla pewnych wielomianów $a', b' \in \mathbb{F}[x]$, to jak wyraża się $\operatorname{nwd}(f, g)$ poprzez wielomiany f, g?
- Jeśli h', r' są ilorazem oraz resztą z dzielenia f' przez g', to ile wynosi iloraz, a ile reszta z dzielenia f przez g?

Rozwiązanie Jeśli

$$f' = h'g' + r'$$

to

$$f'a = h'(g'a) + r'a$$

oraz

$$\deg r'a = \deg r' + \deg a < \deg g' + \deg a = \deg g'a = \deg g$$

czyli iloraz to h' a reszta $r'a$.

Zauważmy teraz, że z tego wynika, że $\operatorname{nwd}(f, g) = a \operatorname{nwd}(f', g')$: W odpowiadających krokach algorytmu Euklidesa dla f, g oraz f', g' dla f, g wywołujemy dla wielomionów dla f', g' przemnożonych przez a. W szczególnośc na końcu dostajemy $\operatorname{nwd}(f', g')$ oraz $a \operatorname{nwd}(f', g')$.

Zadanie 5. Dane są dwa niezerowe wielomiany $f, g \in \mathbb{F}[x]$ z pierścienia wielomianów o współczynnikach z ciała $\mathbb{F}$. Załóżmy, że $f = f'f''$ oraz $\text{nwd}(f', g) = 1$. Celem zadania jest pokazanie, jak odtworzyć reprezentację $\text{nwd}(f, g)$ jako kombinacji wielomianów f, g z analogicznych reprezentacji dla f'', g oraz f', g.

- Pokaż, że $\text{nwd}(f, g) = \text{nwd}(f'', g)$.
- Niech $\text{nwd}(f'', g) = af'' + bg$ oraz $1 = \text{nwd}(f', g) = cf' + dg$ dla odpowiednich wielomianów $a, b, c, d \in \mathbb{F}[x]$. Wyraź $\text{nwd}(f, g)$ jako kombinację wielomianów f, g; kombinacja ta może używać kombinacji wielomianów spośród a, b, c, d, f', f'' jako współczynników.

Rozwiązanie Z Zadania 10, jeśli

$$\text{nwd}(f, g) = \prod_i p_i^{\alpha_i}$$

gdzie p_i są nierozkładalne, to istnieją α_i', α_i'' takie że $\alpha_i = \alpha_i' + \alpha_i''$ oraz $p_i^{\alpha_i'} | f'$ oraz $p_i^{\alpha_i''} | f''$. Ponieważ $\text{nwd}(g, f') = 1$, to $\alpha_i' = 0$ dla każdego i. Czyli $\alpha_i'' = \alpha_i$ i tym samym $\text{nwd}(f, g) | f''$, czyli też $\text{nwd}(f, g) | \text{nwd}(f'', g)$. Jako że $f'' | f$ to oczywiście $\text{nwd}(f'', g) | \text{nwd}(f, g)$. Czyli $\text{nwd}(f, g) = \text{nwd}(f'', g)$.

Niech

$$\text{nwd}(f', g) = 1 = a'f' + b'g \quad \text{nwd}(f'', g) = a''f'' + b''g$$

Łącząc dostajemy

$$\begin{aligned} \text{nwd}(f'', g) &= a''f'' + b''g \\ &= (a'f' + b'g)a''f'' + b''g \\ &= a'f'f'' + (b'a''f'' + b'')g \end{aligned}$$

co daje reprezentację $\text{nwd}(f, g)$ w żądanej postaci.

Zadanie 6. Oblicz wartości podanych wielomianów w punktach w odpowiednich pierścieniach:

$$x^4 + 3x^2 - 2x + 1 \text{ w } 2, \text{ w } \mathbb{Z}_7; \quad 2x^3 - x^2 + x - 2 \text{ w } 1, \text{ w } \mathbb{Z}_3; \quad 3x^4 - 3x^3 + 4x - 5 \text{ w } 2, \text{ w } \mathbb{Z}_6$$

Zadanie 7. Podaj wszystkie nierozkładalne wielomiany stopnia 2 oraz 3 w $\mathbb{Z}_2[x]$ oraz wszystkie nierozkładalne wielomiany stopnia 2 w $\mathbb{Z}_3[x]$.

Wskazówka: Jeśli $f = gh$, to przynajmniej jeden z nich ma stopień 1.

Rozwiązanie Rozważmy najpierw wielomiany stopnia 2 w $\mathbb{Z}_2[x]$:

$$x^2, x^2 + 1, x^2 + x, x^2 + x + 1$$

Pierwszy dzieli się przez x, drugi to $(x + 1)^2$, trzeci to $x(x + 1)$. Czwarty jest nierozkładalny: gdyby był rozkładalny, to na czynniki liniowe, czyli musiałby mieć pierwiastek w 0 lub 1, a łatwo sprawdzić, że nie ma.

W przypadku wielomianów stopnia 3 zauważmy, że jeśli wielomian stopnia 3 jest rozkładalny, to dzieli się przez wielomian stopnia 1, czyli ma pierwiastek. Jest 8 wielomianów stopnia 3 w $\mathbb{Z}_2[x]$:

$$x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1 \ .$$

Należy teraz sprawdzić, który ma pierwiastek w 0 lub 1, pozostałe są nierozkładalne. tzn.

$$x^3 + x + 1, x^3 + x^2 + 1 \ .$$

są nierozkładalne.

W $\mathbb{Z}_3[x]$ jest 9 wielomianów stopnia 2:

$$x^2, x^2 + 1, x^2 + 2, x^2 + x, x^2 + x + 1, x^2 + x + 2, x^2 + 2x, x^2 + 2x + 1, x^2 + 2x + 2.$$

Ponownie sprawdzamy, który ma pierwiastek. Pozostają:

$$x^2 + 1, x^2 + x + 2, x^2 + 2x + 2.$$

Zadanie 8 (* Nie liczy się do podstawy)**.** Celem tego zadania jest pokazanie, że wielomiany nierozkładalne w $\mathbb{R}[x]$ są stopnia najwyżej 2. Możesz korzystać z (nie tak prostego) twierdzenia, że wielomiany nierozkładalne nad $\mathbb{C}[x]$ są stopnia najwyżej 1. W tym zadaniu utożsamiamy wielomian z jego wartościowaniem a $\overline{x}$ będzie oznaczać sprzężenie (w $\mathbb{C}$) liczby zespolonej x.

Ustalmy wielomian $f \in \mathbb{R}[x]$.

- Pokaż, że dla liczby zespolonej c zachodzi $f(\overline{c}) = \overline{f(c)}$.
- Wywnioskuj z tego, że jeśli $c \in \mathbb{C}$ jest miejscem zerowym wielomianu f, to jest nim też $\overline{c}$.
- Pokaż, że wielomian $(x-c)(x-\overline{c})$ ma współczynniki rzeczywiste.
- Wywnioskuj z tego, że jeśli f jest nierozkładalny (w $\mathbb{R}[x]$), to jest stopnia najwyżej 2.

Rozwiązanie Łatwo sprawdzić, że $\overline{a+b} = \overline{a} + \overline{b}$ oraz $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$.
Dla wielomianu $f = \sum_i f_i x^i$ zdefinujmy

$$\overline{f} = \sum_i \overline{f_i} x^i.$$

Wtedy $\overline{f \cdot g} = \overline{f} \cdot \overline{g}$.
Ponadto

$$\overline{f}(\overline{a}) = \sum_i \overline{f_i}\overline{a^i} = \overline{\sum_i f_i a^i} = \overline{f(a)}$$

W takim razie, jeśli $f \in \mathbb{R}[x]$ to oczywiście $\overline{f} = f$ i w takim razie

$$f(\overline{a}) = \overline{f(a)}.$$

Jeśli

$$f(\alpha = 0)$$

to

$$f(\overline{\alpha}\text{‘}) = \overline{0} = 0$$

Jeśli α jest pierwiastkiem $f \in \mathbb{R}[x]$ to $f = (x-\alpha)g$ i nakładając obustronnie sprzężenie dostajemy $f = (x-\overline{\alpha})\overline{g}$. Czyli

$$f = (x-\alpha)(x-\overline{\alpha})h$$

Ponownie nakładając sprzężenie:

$$f = \overline{(x-\alpha)}(x-\overline{\alpha})\overline{h} = (x-\alpha)(x-\overline{\alpha})\overline{h}.$$

Czyli $h = \overline{h}$ i tym samym ma współczynniki rzeczywiste. Ponadto

$$\overline{(x-\alpha)(x-\overline{\alpha})} = (x-\overline{\alpha})(x-\alpha)$$

czyli ma współczynniki rzeczywiste.

Jeśli $f \in \mathbb{R}[x]$ jest nierozkładalny i stopnia większego niż 1, to ma pierwiastek zespolony, powiedzmy α. Ale wtedy $(x-\alpha)(x-\overline{\alpha})|f$, czyli $f = c(x-\alpha)(x-\overline{\alpha})$ dla pewnej stałej c.

Zadanie 9. Pokaż, że jeśli $\mathbb{F}$ jest ciałem, to w pierścieniu wielomianów $\mathbb{F}[x]$ o współczynnikach z ciała $\mathbb{F}$ zachodzi *prawo skreśleń*: dla $f, g, h \in \mathbb{F}[x]$, gdzie $f \neq 0$, zachodzi

$$fg = fh \implies g = h \ .$$

Wywnioskuj z tego, że analogiczne prawo zachodzi też dla podzielności: dla $f, g, h \in \mathbb{F}[x]$, gdzie $f \neq 0$, zachodzi

$$fg | fh \implies g | h \ .$$

Rozwiązanie Przenosząc na jedną stronę dostajemy

$$f(g - h) = 0$$

Jako że $\deg 0 = \deg f + \deg(g - h)$ dostajemy, że $g - h = 0$, czyli $g = h$.

Zadanie 10. Udowodnij uogólnienia twierdzenia z wykładu:

> Niech $\mathbb{F}$ będzie ciałem, f będzie wielomianem nierozkładalnym a $p_1, p_2, \ldots, p_\ell$ wielomianami w pierścieniu wielomianów $\mathbb{F}[x]$ o współczynnikach z $\mathbb{F}$ oraz $f^k | p_1 p_2 \ldots p_\ell$. Wtedy istnieją liczby $n_1, n_2, \ldots, n_\ell$, takie że $\sum_i n_i \geq k$ oraz dla każdego i zachodzi $f^{n_i} | p_i$.

Wskazówka: Skorzystaj z Zadania 9, nawet jeśli nie potrafisz go rozwiązać.

Rozwiązanie Indukcja po k, dla $k = 1$ zostało pokazane na wykładzie.

Niech $f^{k+1} | p_1 p_2 \ldots p_\ell$, w szczególności $f^k | p_1 p_2 \ldots p_\ell$. Z założenia indukcyjnego istnieją takie $n_1, \ldots, n_\ell$, że $p_i = f^{n_i} p_i'$ oraz $\sum_i n_i = k$.

Skoro $f^{k+1} | p_1 p_2 \ldots p_\ell$ to dla pewnego h mamy

$$f^{k+1} h = f^k p_1' p_2' \ldots p_\ell'.$$

Po skróceniu (Zadanie 9) dostajemy

$$fh = p_1' p_2' \ldots p_\ell'.$$

I teraz dostajemy, że f dzieli któreś p_i'm czyli $f^{n_i+1} | p_i$, co daje tezę.

Zadanie 11. Niech $\mathbb{F}$ będzie ciałem zaś $\mathbb{F}[x]$ pierścieniem wielomianów o współczynnikach z tego ciała. Udowodnij, że każdy wielomian $f \in \mathbb{F}[x]$ da się przedstawić jednoznacznie (z dokładnością do kolejności czynników) w postaci $f = c \cdot f_1 \cdot f_2 \cdots f_k$, gdzie $c \in \mathbb{F}$ jest stałą, a każde $f_i \in \mathbb{F}[x]$ jest wielomianem nierozkładalnym o wiodącym współczynniku równym 1.

Wskazówka: Założenie o współczynniku równym 1 jest tylko po to, by uniknąć arbitralności w wyborze współczynnika wiodącego, co prowadzi do "różnych" rozkładów.

Możesz skorzystać z Zadań 9–10, nawet jeśli nie potrafisz ich udowodnić.