LISTA 14 ZAD 3

Pokaż, że w $\mathbb{F}[x]$ zachodzi prawo skreśleń: jeśli $f, g, h \in \mathbb{F}[x]$ spełniają $f \neq 0$, $fg = fh \Rightarrow g = h$.

Przenosząc na jedną stronę dostajemy

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

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

LISTA 14 ZAD 4

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

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

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

Rozpatrzmy wielomian x^5+x^3+x+1 jako wielomian o współczynnikach z $\mathbb{Z}_2$. Zauważmy, że jeśli jest on rozkładalny, to ma czynniki 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.

LISTA 14 ZAD 5

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.

Reszta jest postaci $ax+b$, tj.

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

Przy czym $f(c_1) = r_1$, $f(c_2) = r_2$

Co daje układ równań liniowych na a, b:

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

LISTA 14 ZAD 6

Niech f, g, f', g', a będą niezerowymi wielomianami z pierścienia wielomianów $F[x]$. Załóżmy, że $f = af'$ oraz $g = ag'$.

- Jeśli $h' = \text{nwd}(f', g')$, to ile wynosi $\text{nwd}(f, g)$?
- Jeśli h', r' są ilorazem oraz resztą z dzielenia

f' przez g', to ile wynosi iloraz, a ile reszta z dzielenia f przez g?

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 wyniku, że $nwd(f,g) = a\, nwd(f',g')$: w odpowiadających krokach algorytmu Euklidesa dla f, g oraz f', g' dla f, g występujemy dla wielomianów dla f', g' przemnożonych przez a. W szczególności na końcu dostajemy $nwd(f',g')$ oraz $a\, nwd(f',g')$.

LISTA 14 ZAD 10

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

Wszystkich wielomianów stopnia 2 o współczynniku wiodącym 1 w $\mathbb{Z}_p[x]$ jest p^2 (po p wyborów na każdy z dwóch pozostałych współczynników). Wielomian rozkładalny jest postaci $(x-\alpha)(x-\beta)$ dla $\alpha, \beta \in \mathbb{Z}_p$. Jest p takich wielomianów dla $\alpha = \beta$ oraz $p(p-1)/2$ dla $\alpha \neq \beta$ (dzielimy przez dwa, bo kolejność nie gra roli) czyli $p(p+1)/2 < p^2$. Czyli jest jakiś wielomian nierozkładalny stopnia 2.