Zadanie: Wielomiany nierozkładalne i ciało $GF(9)$

Podpunkt 1: Znajdź wszystkie unormowane nierozkładalne wielomiany 2. stopnia nad ciałem $\mathbb{Z}_3$.

Unormowany wielomian 2. stopnia nad ciałem $\mathbb{Z}_3$ ma postać x^2+ax+b, gdzie $a, b \in \mathbb{Z}_3 = \{0, 1, 2\}$. Wielomian jest nierozkładalny, jeśli nie ma pierwiastków w $\mathbb{Z}_3$. Sprawdzimy to dla każdego z 9 możliwych wielomianów, podstawiając $0, 1, 2$ za x i sprawdzając, czy wynik jest równy 0 (mod 3).

1. $w(x) = x^2$: $w(0) = 0^2 = 0$. Pierwiastek to 0. **Rozkładalny**.
2. $w(x) = x^2 + 1$: $w(0) = 0^2 + 1 = 1 \neq 0$ $w(1) = 1^2 + 1 = 2 \neq 0$ $w(2) = 2^2 + 1 = 4 + 1 = 5 \equiv_3 2 \neq 0$ Brak pierwiastków. **Nierozkładalny**.
3. $w(x) = x^2 + 2$: $w(0) = 0^2 + 2 = 2 \neq 0$ $w(1) = 1^2 + 2 = 3 \equiv_3 0$. Pierwiastek to 1. **Rozkładalny** (np. $(x-1)(x+1) = (x+2)(x+1) = x^2+3x+2 \equiv x^2+2 \pmod 3$).
4. $w(x) = x^2 + x$: $w(0) = 0^2 + 0 = 0$. Pierwiastek to 0. **Rozkładalny**.
5. $w(x) = x^2+x+1$: $w(0) = 0^2+0+1 = 1 \neq 0$ $w(1) = 1^2+1+1 = 3 \equiv_3 0$. Pierwiastek to 1. **Rozkładalny** (np. $(x-1)(x-1) = (x+2)^2 = x^2+4x+4 \equiv x^2+x+1 \pmod 3$).
6. $w(x) = x^2 + x + 2$: $w(0) = 0^2 + 0 + 2 = 2 \neq 0$ $w(1) = 1^2 + 1 + 2 = 4 \equiv_3 1 \neq 0$ $w(2) = 2^2 + 2 + 2 = 4 + 2 + 2 = 8 \equiv_3 2 \neq 0$ Brak pierwiastków. **Nierozkładalny**.
7. $w(x) = x^2 + 2x$: $w(0) = 0^2 + 2(0) = 0$. Pierwiastek to 0. **Rozkładalny**.
8. $w(x) = x^2+2x+1$: $w(0) = 0^2+2(0)+1 = 1 \neq 0$ $w(1) = 1^2+2(1)+1 = 4 \equiv_3 1 \neq 0$ $w(2) = 2^2 + 2(2) + 1 = 4 + 4 + 1 = 9 \equiv_3 0$. Pierwiastek to 2. **Rozkładalny** (np. $(x-2)^2 = (x+1)^2 = x^2 + 2x + 1 \pmod 3$).
9. $w(x) = x^2+2x+2$: $w(0) = 0^2+2(0)+2 = 2 \neq 0$ $w(1) = 1^2+2(1)+2 = 1+2+2 = 5 \equiv_3 2 \neq 0$ $w(2) = 2^2 + 2(2) + 2 = 4 + 4 + 2 = 10 \equiv_3 1 \neq 0$ Brak pierwiastków. **Nierozkładalny**.

Unormowane nierozkładalne wielomiany 2. stopnia nad ciałem $\mathbb{Z}_3$ to:

- $x^2 + 1$
- $x^2 + x + 2$
- $x^2 + 2x + 2$

Podpunkt 2: Rozważmy ciało $GF(9) = \mathbb{Z}_3[x]/(p(x))$. Znajdź α^2 i α^3 w $GF(9)$ dla $\alpha = x^2 + x$. Jaka jest charakterystyka ciała $GF(9)$?

Wybieramy jeden ze znalezionych wielomianów nierozkładalnych, np. $p(x) = x^2 + x + 2$. W ciele $GF(9) = \mathbb{Z}_3[x]/(x^2 + x + 2)$, elementy to klasy reszt z dzielenia wielomianów przez $p(x)$. Możemy je reprezentować przez wielomiany stopnia mniejszego niż stopień $p(x)$, czyli stopnia co najwyżej 1. Zatem elementy mają postać $ax + b$, gdzie $a, b \in \mathbb{Z}_3$.

Z definicji pierścienia ilorazowego, $p(x) \equiv 0 \pmod{p(x)}$. Oznacza to, że: $x^2+x+2 \equiv 0 \pmod{x^2+x+2}$ $x^2 \equiv -x-2 \pmod{x^2+x+2}$ Ponieważ działamy w $\mathbb{Z}_3$, gdzie $-1 \equiv_3 2$ i $-2 \equiv_3 1$, nasza reguła redukcji to: $x^2 \equiv 2x+1 \pmod{x^2+x+2}$

Mamy dany element $\alpha = x^2 + x$. Musimy znaleźć jego reprezentację w ciele $GF(9)$. Podstawiamy regułę redukcji: $\alpha = x^2 + x \equiv (2x+1) + x \pmod{x^2+x+2}$ $\alpha \equiv 3x+1 \pmod{x^2+x+2}$ Ponieważ $3 \equiv_3 0$, mamy: $\alpha \equiv 0x+1 \pmod{x^2+x+2}$ $\alpha \equiv 1 \pmod{x^2+x+2}$

Zatem, w ciele $GF(9)$, element α jest równy 1 (jedynce ciała). Teraz możemy łatwo obliczyć α^2 i α^3: $\alpha^2 = 1^2 = 1$ $\alpha^3 = 1^3 = 1$

Charakterystyka ciała $GF(9)$

Charakterystyka ciała $GF(p^n)$ jest zawsze liczbą pierwszą p. W tym przypadku, ciało $GF(9)$ może być zapisane jako $GF(3^2)$, gdzie $p = 3$ i $n = 2$. Zatem charakterystyka ciała $GF(9)$ wynosi **3**.