Algebra Komputerowa

Rozkład Bezkwadratowy Wielomianu [1, 2]

Filip Zieliński

2025

Spis Treści

Założenia

- Przez całą prezentacje zakładamy, że K jest ciałem **charakterystyki zero**, bądź ciałem **skończonym**.
- Uwaga! Przedstawione twierdzenia nie muszą zachodzić dla ciał nieskończonych o skończonej charakterystyce.
- Mówiąc o pierścieniu, musimy mówić o pierścieniu z jednoznacznością rozkładu.
- Zazwyczaj myślimy o pierścieniu wielomianów jednej zmiennej $K[x]$.

KOŁO NAUKOWE

Definicja

Niech R będzie pierścieniem oraz $a \in R$ elementem tego pierścienia. a nazywamy *bezkwadratowym*, jeżeli nie jest podzielny przez kwadrat żadnego elementu nieodwracalnego.

Obserwacja

Niech $f \in K[x]$ będzie wielomianem o rozkładzie

$$f = \varepsilon \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_m}$$

gdzie ε jest elementem odwracalnym, a $p_1, \ldots, p_m$ są różnymi wielomianami unormowanymi nierozkładalnymi.
Następujące warunki są równoważne

1. f jest bezkwadratowy,
2. $\alpha_1 = \ldots = \alpha_m = 1$,
3. rozważając f w swoim ciele rozkładu, f posiada jedynie pierwiastki jednokrotne.

Lemat

Niech $f \in K[x]$ będzie wielomianem, a z pierwiastkiem f o krotności k. Jeżeli $k > 1$ to $f'(z) = 0$.

Pierwiastki wielokrotne wielomianu

Elementy bezkwadratowe

KOŁO NAUKOWE

Lemat

Niech $f \in K[x]$ będzie wielomianem, a z pierwiastkiem f o krotności k. Jeżeli $k > 1$ to $f'(z) = 0$.

Twierdzenie

Niech $f \in K[x]$ będzie wielomianem jednej zmiennej o współczynnikach z ciała K. Zachodzi

$$f \text{ jest bezkwadratowy} \Leftrightarrow \mathrm{NWD}(\mathrm{f}, \mathrm{f}') = 1$$

Niech $f \in K[x]$ będzie wielomianem o rozkładzie

$$f = \varepsilon \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_m}.$$

Oznaczmy $k = \max\{\alpha_1, \dots \alpha_{,m}\}$. Pogrupujmy czynniki względem ich krotności, tzn

$$g_i = \prod_{j \leqslant m,\ \alpha_j = i} p_j \quad i \leqslant k$$

Definicja

Rozkładem bezkwadratowym wielomianu f nazywamy zapisanie go w postaci

$$f = \varepsilon \cdot g_1^1 \cdot g_2^2 \cdots g_k^k$$

Definicja

Niech $f \in K[x]$ będzie wielomianem o rozkładzie postaci

$$f = \varepsilon \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_m}.$$

Radykałem wielomianu f nazywamy wielomian

$$\mathrm{rad}(f) = p_1 \cdots p_m.$$

Definicja

Niech $f \in K[x]$ będzie wielomianem o rozkładzie postaci

$$f = \varepsilon \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_m}.$$

Radykałem wielomianu f nazywamy wielomian

$$\mathrm{rad}(f) = p_1 \cdots p_m.$$

Twierdzenie

Niech f będzie wielomianem o współczynnikach z **ciała charakterystyki zero**. Zachodzi

$$\mathrm{rad}(f) = g_1 \cdots g_k = \frac{f}{\mathrm{NWD(f, f')}}$$

Założenia: K – ciało charakterystyki zero.
Wejście: $f \in K[x]$
Wyjście: $g_1, \ldots, g_k$ takie, że $f = \varepsilon \prod_{i=1}^{k} g_i^i$
Kroki:

1. Przypisz $a_0 := f$, $a_1 := \mathrm{NWD}(a_0, a_0')$, $b_1 = \frac{a_0}{a_1}$, $i := 1$.
2. Dopóki $b_i \neq 1$, wykonuj:
   - Wylicz $a_{i+1} = \mathrm{NWD}(a_i, a_i')$.
   - Wylicz $b_{i+1} = \frac{a_i}{a_{i+1}}$.
   - Wylicz $g_i = \frac{b_i}{b_{i+1}}$.
3. Zwróć $g_1, \ldots, g_k$.

Algorytm Tobeya - Horowitza jest **najstarszym** znanym algorytmem rozkładania bezkwadratowego wielomianu. Został wymyślony w latach 1967/1969.

Algorytm Tobeya - Horowitza jest **najstarszym** znanym algorytmem rozkładania bezkwadratowego wielomianu. Został wymyślony w latach 1967/1969.

- Drobna modyfikacja tego algorytmu, sprawia, że działa on na wielomianach nad ciałami skończonymi.

Algorytm Tobeya - Horowitza jest **najstarszym** znanym algorytmem rozkładania bezkwadratowego wielomianu. Został wymyślony w latach 1967/1969.

- Drobna modyfikacja tego algorytmu, sprawia, że działa on na wielomianach nad ciałami skończonymi.
- Istnieje szereg szybszych algorytmów
  1. algorytm Mussera (1971),
  2. algorytm Yuna (1976),
  3. algorytm Gerharda (2001),
  4. algorytm Guersenzvaiga-Szechtmana (2012/2017).

Źródła

Prezentacja jest mocno oparta o wykład autorstwa *Przemysława Koprowskiego*, który można obejrzeć pod tym linkiem

[1] Joachim Von Zur Gathen and Jurgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[2] Przemysław Koprowski. *Lectures on Computational Mathematics*. 2022.

Pytania, wątpliwości, uwagi ?