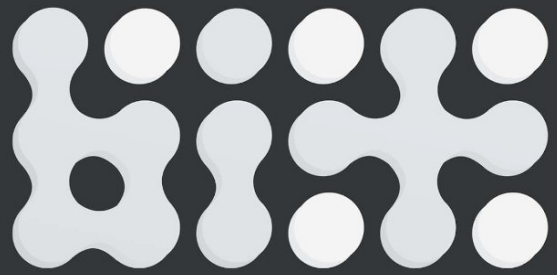

Algebra Komputerowa

Rozkład Wielomianu nad Ciałem Skończonym [1, 2]

Filip Zieliński

2025

Spis Treści

Oznaczenia

Ciało skończone liczności q oznaczmy przez $\mathbb{F}_q$.
Oczywiście $q = p^m$ dla pewnego p będącego liczbą pierwszą i dla dodatniego całkowitego wykładnika m.
Zachodzi $char(\mathbb{F}_q) = p$.

Algorytm dzielenia wielomianów nad ciałem skończonym dzielimy na trzy etapy,

1. *Squarefree factorization* (rozkład ze względu na krotność).
2. *Distinct-degree factorization* (podział ze względu na stopień)
3. *Equal degree factorization* (ostateczny rozkład)

Algorytm dzielenia wielomianów nad ciałem skończonym dzielimy na trzy etapy,

1. *Squarefree factorization* (rozkład ze względu na krotność).
2. *Distinct-degree factorization* (podział ze względu na stopień)
3. *Equal degree factorization* (ostateczny rozkład)

Temat rozkładu bezkwadratowego wielomianu poruszała poprzednia prezentacja. Dzięki temu możemy rozważać problem rozkładu wielomianu g, który jest bezkwadratowy.

Rozważmy bezkwadratowy unormowany wielomian $g \in \mathbb{F}_q[x]$ o rozkładzie

$$g = p_1 \cdots p_m.$$

Oznaczmy $s = \max\{\deg p_i \mid i \leqslant m\}$. Pogrupujmy czynniki g względem stopnia, znaczy się

$$h_k = \prod_{\deg p_i = k} p_i \quad \text{dla } k \leqslant s.$$

Definicja

Rozkładem *distinct-degree* wielomianu g nazywamy wyrażenie

$$g = h_1 \cdots h_s.$$

Kluczowe twierdzenie

Distinct-degree factorization

KOŁO NAUKOWE

Twierdzenie

Ustalmy liczbę całkowitą $d \geqslant 1$ oraz niech $p_1, \ldots, p_t \in \mathbb{F}_q[X]$ będą **wszystkimi** unormowanymi nierozkładalnymi wielomianami o współczynnikach z $\mathbb{F}_q$ o takim stopniu, że $\deg(p_i) \mid d$ dla każdego i. Zachodzi

$$p_1 \cdots p_t = x^{q^d} - x.$$

Założenia: $g \in \mathbb{F}_q[x]$ – wielomian unormowany bezkwadratowy.
Wejście: Wielomian $g \in \mathbb{F}_q[x]$.
Wyjście: Wielomiany $h_1, \ldots, h_s \in \mathbb{F}_q[x]$, takie że

$$g = h_1 h_2 \cdots h_s,$$

gdzie każdy h_i jest iloczynem nierozkładalnych czynników stopnia dokładnie i.
Kroki:

1. Przypisz $f_0 := x$, $g_1 := g$, $k := 1$.
2. Dopóki g_k jest wielomianem niebędącym stałą, wykonuj:
   - Oblicz $f_k := f_{k-1}^q \bmod g_k$.
   - Oblicz $h_k := \mathrm{nwd}(g_k, f_k - x)$.
   - Zwiększ $k := k + 1$.
   - Przypisz $g_k := \frac{g_{k-1}}{h_{k-1}}$.
3. Zwróć $h_1, \ldots, h_k$.

Pozostałości

Equal degree factorization

Musimy teraz rozłożyć wielomian f stopnia n o współczynnikach z ciała $\mathbb{F}_q$, o rozkładzie

$$f = p_1 \cdots p_m$$

gdzie $\deg(p_i) = d$ dla każdego p.

Musimy teraz rozłożyć wielomian f stopnia n o współczynnikach z ciała $\mathbb{F}_q$, o rozkładzie

$$f = p_1 \cdots p_m$$

gdzie $\deg(p_i) = d$ dla każdego p. Oznaczmy sobie $R = \mathbb{F}_q[x]/\langle f \rangle$ oraz $K_i = \mathbb{F}_q/\langle p_i \rangle$.
Zauważmy, że K_i jest rozszerzeniem ciała $\mathbb{F}_q$ stopnia d dla każdego K_i. Tak więc $K_i \cong K_j$ dla każdego i, j.
Dodatkowo, zauważmy, że $R \cong \mathbb{F}_q[x]_{\leqslant n-1}$.

Obserwacja

Z chińskiego twierdzenia o resztach wynika istnienie izomorfizmu Φ, takiego, że

$$\Phi : R \leftarrow K_1 \times \ldots \times K_m.$$

Algortym Cantora - Zassenhausa (19
Equal degree factorization

KOŁO NAUKOWE

Rozważmy g względnie pierwsze z f. Oznaczmy $\tilde{g} = g \pmod{f}$. Mamy

$$\Phi(\tilde{g}) = (\tilde{g_1}, \ldots, \tilde{g}_m)$$

ustalmy $e = \frac{q^d - 1}{2}$. Zauważmy, że

$$\Phi(\tilde{g}^e) = (\tilde{g_1}^e, \ldots, \tilde{g}_m^e) = (\pm 1, \ldots, \pm 1)$$

Rozważmy g względnie pierwsze z f. Oznaczmy $\tilde{g} = g \pmod{f}$. Mamy

$$\Phi(\tilde{g}) = (\tilde{g_1}, \ldots, \tilde{g_m})$$

ustalmy $e = \frac{q^d - 1}{2}$. Zauważmy, że

$$\Phi(\tilde{g}^e) = (\tilde{g_1}^e, \ldots, \tilde{g_m^e}) = (\pm 1, \ldots, \pm 1)$$

Twierdzenie

Niech h będzie resztą z dzielenia $g^e - 1$ przez f. Jeżeli jest takie $i \neq j$, że $\tilde{g_i}^e = 1$ oraz $\tilde{g_j}^e = -1$, to $\mathrm{NWD(h, f)}$ jest nietrywialnym dzielnikiem f.

[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 ?