# 7 - Pierwiastki wielomianu X^q - X stanowią ciało

Wednesday, 19 June 2024 21:13

Niech $Q = p^k$. Dane jest ciało $\mathbb{F}$ charakterystyki $p$.

Jeśli wielomian $X^Q - X$ ma $Q$ pierwiastków to stanowią one ciało.

Wystarczy pokazać, że zbiór $A = \{a \in \mathbb{F} : a^Q = a\}$ jest zamknięty na $+, \cdot$.

- $-1, 0, 1 \in A$ w oczywisty sposób.

- Jeśli $a, b \in A$, to $a \cdot b \in A$:

$$(a \cdot b)^Q = a^Q \cdot b^Q = a \cdot b$$

- $a \in A \Rightarrow a \cdot (-1) = -a \in A$

- $a \in A \Rightarrow a^{-1} \in A$: $(a^{-1})^a \cdot a = a^{-a} \cdot a^a = 1 \Rightarrow a^{-1} = a^{-a}$

- $a, b \in A \Rightarrow a + b \in A$:

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j} = a^p + b^p$$ bo pozostałe dwumiany są podzielne przez $p$, a $\mathbb{F}$ jest charakterystyki $p$.

Zatem $(a+b)^{p^k} = a^a + p^a$

Algorytmiczna konstrukcja

Dla $k \in \mathbb{N}$ liczba unormowanych wielomianów nierozkładalnych nad $\mathbb{Z}_p$ jest $\geq \frac{p^k}{2k}$.

Zatem jeśli potrafimy sprawdzić, czy wielomian jest nierozkładalny to wystarczy losować.

Jak sprawdzić?

$X^{p^k} - X$ jest iloczynem wszystkich nierozkładalnych wielomianów o stopniu dzielącym $k$.

Zatem wystarczy sprawdzać $gcd(W, X^{p^d} - X)$ □