



Ciało na p^2 elementach

Antoni Łuczak

10.04.2025

Teoria

Definicja 1 ($\mathbb{F}_{p^2}$)

Dana jest nieparzysta liczba pierwsza p oraz nierozkładalna kwadratowa d modulo p . Definiujemy $\mathbb{F}_p(\sqrt{d})$ jako zbiór składający się z elementów postaci $a + b\sqrt{d}$, gdzie $a, b \in \{0, \dots, p-1\}$ wraz z dodawaniem oraz mnożeniem zdefiniowanymi w następujący sposób:

$$(a + b\sqrt{d}) + (x + y\sqrt{d}) = a + x + (b + y)\sqrt{d}$$

$$(a + b\sqrt{d})(x + y\sqrt{d}) = ax + byd + (ay + bx)\sqrt{d}.$$

Okazuje się, że każdy niezerowy element α takiego zbioru posiada odwrotność multiplikatywną α^{-1} spełniającą $\alpha\alpha^{-1} = 1$. Otrzymujemy w ten sposób ciało skończone na p^2 elementach.

Ćwiczenie 1. Niech $a \in \{0, \dots, p-1\}$. Udowodnij, że $\mathbb{F}_p(\sqrt{d})$ zawiera pewien element x spełniający $x^2 = a$. Wywnioskuj stąd, że wybór d nie ma znaczenia i że wszystkie ciała na p^2 elementach są "takie same".

W związku z powyższym ćwiczeniem często nie precyzujemy wartości d , tylko rozpatrujemy dowolne ciało na p^2 elementach oznaczane $\mathbb{F}_{p^2}$

Twierdzenie 1

Dane są dwa elementy $a, b \in \mathbb{F}_{p^2}$. Wtedy spełniona jest równość

$$(a + b)^p = a^p + b^p.$$

Wniosek 1. Dany jest taki element $x \in \mathbb{F}_{p^2}$, że x^2 jest nierozkładalą kwadratową modulo p . Wtedy dla dowolnych $a, b \in \{0, \dots, p-1\}$ zachodzi

$$(a + bx)^p = a - bx.$$

Wniosek 2. Dla a, b, x tak jak wyżej zachodzi

$$(a + bx)^{p^2-1} = 1,$$

o ile $a, b \neq 0$.

Zadania

Zadanie 1. Dana jest nieparzysta liczba pierwsza $p \neq 5$. Niech dodatkowo f_n oznacza n -tą liczbę Fibonacciego. Udowodnić, że liczby f_{p^2-1} oraz $f_p^2 - 1$ są podzielne przez p .

Zadanie 2 (61OM-3-5). Liczba pierwsza $p > 3$ daje resztę 2 z dzielenia przez 3. Niech

$$a_k = k^2 + k + 1 \text{ dla } k = 1, 2, 3, \dots, p-1.$$

Wykazać, że iloczyn $a_1 a_2 a_3 \dots a_{p-1}$ daje resztę 3 z dzielenia przez p .

Zadanie 3. Udowodnić, że wielomian

$$x^5 - x + 2137$$

jest nierozkładalny nad liczbami wymiernymi.

Zadanie 4 (ISL). Ciąg $a_0, a_1, a_2, \dots$ jest zdefiniowany przez warunki

$$a_0 = 2, \quad a_{k+1} = 2a_k^2 - 1.$$

Udowodnić, że jeśli nieparzysta liczba pierwsza p dzieli a_n , to 2^{n+3} dzieli $p^2 - 1$.

Zadanie 5 (Test Lucasa-Lehmery). Ciąg $x_0, x_1, x_2, \dots$ jest zdefiniowany przez warunki

$$x_0 = 4, \quad x_{k+1} = x_k^2 - 2.$$

Udowodnić, że dla nieparzystej liczby pierwszej p , liczba $n = 2^p - 1$ jest pierwsza wtedy i tylko wtedy, gdy n dzieli x_{p-2} .