

CIAŁA SKOŃCZONE

PASJONACI MATEMATYKI

PRZYPOMNIENIE

Reszta kwadratowa: $2 \equiv 3^2 \pmod{7}$.

($\frac{p-1}{2}$ niezerowych reszt kwadratowych i $\frac{p-1}{2}$ reszt kwadratowych)

Definicja 1.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p|a, \\ 1, & p \nmid a, a \text{ jest resztą kwadratową}, \\ -1, & a \text{ jest nieresztą kwadratową}. \end{cases}$$

Fakt 2.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Wniosek 3.

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{a \cdot b}{p}\right).$$

Twierdzenie 4 (prawo wzajemności reszt kwadratowych). $p, q \in \mathbb{P}, p, q > 2 \Rightarrow$

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

oraz $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$

Przykład 5.

$$\left(\frac{6}{47}\right) = \left(\frac{2}{47}\right) \cdot \left(\frac{3}{47}\right) = (-1)^{\frac{47^2-1}{8}} \cdot (-1)^{\frac{3-1}{2} \cdot \frac{47-1}{2}} \left(\frac{47}{3}\right) = 1 \cdot (-1) \cdot \left(\frac{2}{3}\right) = 1.$$

Motywacje:

- rozwiązywanie równań w liczbach całkowitych,
- badanie liczb pierwszych: np. istnieje niesk. wiele liczb pierwszych $p \equiv 1 \pmod{8}$.

Zadanie: Wykaż, że wielomian $(x^2 - 2)(x^2 - 3)(x^2 - 6)$ ma pierwiastek modulo dowolna liczba pierwsza, ale nie ma pierwiastka całkowitego.

CIAŁA SKOŃCZONE

Ciało – zbiór z działaniami dodawania, odejmowania, mnożenia i dzielenia (przez niezerowe elementy). Przykłady: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{F}_2 = \{0, 1\}$ (gdzie $1 + 1 = 0$, $0 \cdot 1 = 0$, $1 \cdot 1 = 1$).

Pytanie: dla jakich n istnieje ciało n -elementowe?

Motywacja: kryptografia, teoria liczb.

Przykład: $\mathbb{Z}/n := \{0, 1, \dots, n-1\}$ – reszty z dzielenia przez n z działaniami dodawania i mnożenia mod n .

$\mathbb{Z}/n$ jest ciałem wtw. gdy n jest liczbą pierwszą. Istotnie, jeżeli $n = n_1 \cdot n_2$ to $n_1 \cdot n_2 \equiv 0 \pmod{n}$, zatem n_1 oraz n_2 nie mają odwrotności. Dla $n = p$ każda niezerowa reszta ma odwrotność mod p .

Dlatego piszemy: $\mathbb{F}_p := \mathbb{Z}/p$.

Fakt 6. Jeżeli istnieje ciało n -elementowe, to n jest potęgą liczby pierwszej.

Dowód. Ćwiczenie. □

Pytanie: Jak skonstruować ciała p^k -elementowe?

Pomysł: $\mathbb{Q} \rightsquigarrow \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

- $\mathbb{F}_9 = \mathbb{F}_3[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{F}_3\}$,
- $\mathbb{F}_7[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{F}_7\}$ – nie jest ciałem, bo $(3 - \sqrt{2}) \cdot (3 + \sqrt{2}) = 9 - 2 \equiv 0 \pmod{7}$.

Stąd: $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{c}]$, gdzie c jest nierozkładalną kwadratową!

Pytanie: Jak skonstruować ciało 4 elementowe?

Pomysł: $\{a + b\gamma : a, b \in \mathbb{F}_2\} = \{0, 1, \gamma, 1 + \gamma\}$, gdzie $\gamma^2 + \gamma + 1 = 0$. Jak dodawać elementy? Tabela mnożenia: $\gamma \cdot (\gamma + 1) = \gamma^2 + \gamma = 1$, $\gamma^2 = \gamma + 1$, $(\gamma + 1)^2 = \gamma$.

Twierdzenie 7. Ciało p^k -elementowe jest postaci:

$$\mathbb{F}_p[\gamma] = \{a_0 + a_1\gamma + \dots + a_{k-1}\gamma^{k-1} : a_0, \dots, a_{k-1} \in \mathbb{F}_p\},$$

gdzie γ spełnia równanie:

$$b_k\gamma^k + \dots + b_1\gamma + b_0 = 0,$$

zaś $P(x) := b_kx^k + \dots + b_1x + b_0 \in \mathbb{F}_p[x]$ – nierozkładalny.

(np. $P(x) = x^2 - 2 = (x - 3) \cdot (x + 3) \in \mathbb{F}_7[x]$).

Pytanie: jak udowodnić, że istnieje wielomian nierozkładalny stopnia n dla każdego n ?

Fakt 8. Jeżeli $a, b \in \mathbb{F}_{p^n}$ to $(a + b)^p = a^p + b^p$.

Stwierdzenie 9. Jeżeli $\alpha \in \mathbb{F}_{p^k}$ to $\alpha^{p^k} = \alpha$.

Przykład 10. W $\mathbb{F}_4$:

$$(1 + \gamma)^4 = \gamma^2 = 1 + \gamma.$$

Dowód. Niech $\mathbb{F}_{p^k} \setminus \{0\} = \{\alpha_1, \dots, \alpha_{p^k-1}\}$. Wtedy $\{\alpha \cdot \alpha_1, \dots, \alpha \cdot \alpha_{p^k-1}\} = \{\alpha_1, \dots, \alpha_{p^k-1}\}$, zatem:

$$\alpha\alpha_1 \cdot \dots \cdot \alpha\alpha_{p^k-1} = \alpha_1 \cdot \dots \cdot \alpha_{p^k-1},$$

czyli $\alpha^{p^k-1} = 1$. □

Uwaga 11. *Inny opis ciała p^k -elementowego:*

$$\mathbb{F}_{p^k} := \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^k} - \alpha = 0\}$$

$(\overline{\mathbb{F}_p})$ to pewien duży zbiór, w którym każdy wielomian ma pierwiastek).

Twierdzenie 12. *Istnieje element g (generator ciała) taki, że $\mathbb{F}_{p^k} \setminus \{0\} = \{g^0, g^1, \dots, g^{p^k-2}\}$.*

Przykład 13. $1 + \gamma$ jest generatorem w $\mathbb{F}_4$: $1, 1 + \gamma, (1 + \gamma)^2 = 1 + 2\gamma + \gamma^2 = \gamma$.