

---

ДОМАШНЯ РОБОТА №11  
З ПРЕДМЕТУ  
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”  
ФІ-12 Бекешева Анастасія

---

1. Нормований поліном  $f(x) = x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0, \alpha_i \in \mathbb{Z}_3, \alpha_0 \neq 0$ . Всього  $1 \cdot 3 \cdot 3 \cdot 2 = 18$  комбінацій, отже переберемо поліноми

- $x^3 + 2$  - звідний
- $x^3 + 1$  - звідний
- $x^3 + 2x^2 + 1$  - незвідний

Нормований поліном  $f(x) = x^5 + \alpha_4 x^4 + \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0, \alpha_i \in \mathbb{Z}_3, \alpha_0 \neq 0 \Leftrightarrow \alpha_0 = 1$ . Переберемо

- $x^5 + 1$  - звідний
- $x^5 + x + 1$  - звідний
- $x^5 + x^2 + 1$  - незвідний

2. Кількість примітивних елементів у  $F_{625} : \varphi(624) = \varphi(2^4 \cdot 3 \cdot 13) = (2^4 - 2^3) \cdot 2 \cdot 12 = 192$

3. Кількість примітивних елементів у  $F_{37} : \varphi(36) = \varphi(2^2 \cdot 3^2) = 2 \cdot 6 = 12$ . Перевіримо, чи є 2 примітивним елементом поля:  $h = 36 = 2^2 \cdot 3^2, 2^{18} \bmod 36 \neq 1, 2^{12} \bmod 36 \neq 1, \text{ord}(2) = 36$ . 2 - примітивний елемент. Знайдемо інші примітивні елементи, вони матимуть вигляд:  $2^\alpha, 0 \leq \alpha \leq 36, \gcd(36, \alpha) = 1$ . Отже примітивні елементи  $2^\alpha, \alpha \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$ .

4. Коренів буде 5, вони будуть знаходитись у полі  $F_{35}$ . Якщо  $\alpha$  - корінь, усі інші коріні -  $\alpha^3, \alpha^{3^2}, \alpha^{3^3}, \alpha^{3^4}$ .

5. Квадратичний лишок  $a = x^2 \bmod p$ , за теоремою Ойлера, критерієм Ойлера та властивостями функції Ойлера  $a^{\frac{p-1}{2}} = a^{\frac{\varphi(p)}{2}} = x^{\varphi(p)} = 1 \bmod p$ , а отже порядок  $a$  не може дорівнювати  $\varphi(p)$ .