ДОМАШНЯ РОБОТА №12
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

vec	in basis	ind	ord	min polynomial
(0,0)	0			x
(0,1)	1	α^8	1	$x+2$
(1,0)	α	α^1	8	x^2+x+2
(1,1)	$\alpha+1$	α^7	8	x^2+2x+2
(0,2)	2	α^4	2	$x+1$
(2,0)	2α	α^5	8	x^2+x+1
(1,2)	$a+2$	α^6	4	x^2+1
(2,1)	$2\alpha+1$	α^2	4	x^2+1
(2,2)	$2\alpha+2$	α^3	8	x^2+x+2

1. $x^9 - x = x^9 + 2x = x^{3^2} + 2x = x(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)(x^3+x+1)$

2. F_{p^n} - розширення полінома $g(x) = x^{p^n} - x$. Будь-який нормований незвідний поліном степеня n ділить g. Отже $[F_{p^n} : F_p]$ і більше розширень немає. Отже кожен незвідний поліном, що ділить g має бути степеня n або 1. Так як кожен лінійний поліном над F_p ділить g і g має корені, ми маємо p різних поліномів що ділять g. Якщо перемножити усі незвідні нормовані поліноми що ділять g ми отримаємо g і сума їх степенів буде дорівнювати p^n. Позначимо кількість незвідних нормованих поліномів степеня n як m і отримаємо $mn + p = p^n$. Отже $m = \dfrac{p^n - p}{n}$. Існує $m = \dfrac{3^7 - 3}{7} = 312$ незвідних нормованих поліномів степіня 7.

3. Переберемо можливі значення у $F_4(\{0, 1, \beta, \beta+1\})$:

   0: $0^2 + 0 \cdot \beta + 1 = 1 \neq 0$

   1: $1^2 + 1 \cdot \beta + 1 = \beta \neq 0$

   β: $\beta^2 + \beta^2 + 1 = 1 \neq 0$

$\beta+1$: $\beta^2 + 2\beta + 1 + \beta^2 + \beta + 1 = \beta \neq 0$

   Отже поліном $x^2 + \beta x + 1$ мав би корені, якби $\beta = 0$, але воно таким не є, адже це корінь $x^2 + x + 1$ над F_2. Поліном $x^2 + \beta x + 1$ незвідний над F_4.