ДОМАШНЯ РОБОТА №13
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

		ind	ord	$\mathrm{Tr}_{F_{16}}$	Tr_{F_{16}/F_4}
(0000)				0	0
(0001)			1	0	0
(0010)			15	1	$\alpha^3+\alpha+1$
(0011)			5	1	$\alpha^3+\alpha+1$
(0100)			15	1	$\alpha^3+\alpha$
(0101)			5	1	$\alpha^3+\alpha$
(0110)			15	0	1
(0111)			15	0	1
(1000)			5	1	$\alpha^3+\alpha+1$
(1001)			15	1	$\alpha^3+\alpha+1$
(1010)			3	0	0
(1011)			3	0	0
(1100)			15	0	1
(1101)			15	0	1
(1110)			15	1	$\alpha^3+\alpha$
(1111)			5	1	$\alpha^3+\alpha$

1.

2. Незвідні поліноми матимуть вигляд ax^2+bx+c. Переберемо усі можливі значення у $F_4(\{0,1,\beta,\beta+1\})$. Зазначимо, що $a\neq 0$ (інакше поліном буде першого степеню) і $c\neq 0$ (інакше поліном точно звідний).

   (Вибачте, дуже багато переписувати, тому чернетку як я перебирала усе це я прикріплю іншим файлом)

   Випишемо незвідні поліноми $x^2+x+1, x^2+\beta x+1, \beta x^2+1, \beta x^2+x+1, \beta x^2+\beta x+1,$ $(\beta+1)x^2+1, (\beta+1)x^2+x+1, (\beta+1)x^2+(\beta+1)x+1, x^2+\beta, x^2+x+\beta, x^2+\beta x+\beta,$ $\beta x^2+x+\beta, \beta x^2+\beta x+\beta, \beta x^2+(\beta+1)x+\beta, (\beta+1)x^2+\beta, (\beta+1)x^2+\beta x+\beta,$ $(\beta+1)x^2+(\beta+1)x+\beta, x^2+(\beta+1), x^2+x+(\beta+1), x^2+(\beta+1)x+(\beta+1), \beta x^2+(\beta+1),$ $\beta x^2+\beta x+(\beta+1), \beta x^2+(\beta+1)x+(\beta+1), (\beta+1)x^2+x+(\beta+1), (\beta+1)x^2+\beta x+(\beta+1),$ $(\beta+1)x^2+(\beta+1)x+(\beta+1)$.

3. Контрприклад x^2+2x

4. $f(x)=x^5+x^4+1=(x^2+x+1)(x^3+x+1)$. Нехай α - корінь x^2+x+1.
   $\alpha^2=\alpha+1$, $\alpha^3=\alpha^2+1=1$. Тоді $\mathrm{ord}\,(\alpha)=3 \Longrightarrow \mathrm{ord}\,(x^2+x+1)=3$. Нехай β - корінь x^3+x+1. $\beta^4=\beta\cdot\beta^3=\beta(\beta+1)=\beta^2+\beta\neq 1 \Longrightarrow \mathrm{ord}\,(\beta)=7$.
   Знайдемо $t=\min\{s|2^s\geq\max\{1,1\}\}=0$. $\mathrm{ord}\,(f(x))=2^0\ \mathrm{lcm}\,(3,7)=21$

5. $\dfrac{\varphi(5^5-1)}{5}=\dfrac{1}{5}\cdot\varphi(3124)=\dfrac{1}{5}\cdot\varphi(2^2\cdot 11\cdot 71)=\dfrac{1400}{5}=280$