ДОМАШНЯ РОБОТА №9
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

1. $g(x) = x^2 + 2x + 4, \quad f(x) = 4x^5 + 2x^4 + x^3 + 1$
   $f(x) = (4x^3 + 4x^2 + 2x)g(x) + (2x + 1)$
   $g(x) = (3x + 2)(2x + 1) + (2)$
   $2 = g(x) - (2x + 1)(3x + 2) = g(x) - (3x + 2)(f(x) - (4x^3 + 4x^2 + 2x)g(x)) =$
   $= (-3x - 2)f(x) + (12x^4 + 20x^3 + 14x^2 + 4x + 1)g(x)$
   $g^{-1} \mod f(x) = 2x^4 + 4x^2 + 4x + 1$

2. Фактор кільце є полем, тоді й тільки тоді, коли поліном є незвідним. У випадку з $x^2 + k$, поліном є незвідним коли в нього нема коренів. Тобто перевіримо $x^2 + k$, $k \in \mathbb{Z}_7$.

   (0) $(0^2 + k) \mod 7 = 0 \Rightarrow k = 0$

   (1) $(1^2 + k) \mod 7 = 0 \Rightarrow k = 6$

   (2) $(2^2 + k) \mod 7 = 0 \Rightarrow k = 3$

   (3) $(3^2 + k) \mod 7 = 0 \Rightarrow k = 4$

   (4) $(4^2 + k) \mod 7 = 0 \Rightarrow k = 5$

   (5) $(5^2 + k) \mod 7 = 0 \Rightarrow k = 3$

   (6) $(6^2 + k) \mod 7 = 0 \Rightarrow k = 6$

   Отже нам підходять усі k, окрім $k \in \{0, 3, 4, 5, 6\}$. Тобто $k = 1, 2$

3.

векторна ф-ма	(0,0,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
поліноми	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x^2	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+1
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$