Самборский Иван М4138
09.11.2015

Глава 5.

Задача 1.

$\forall n$ будет существовать порождающий полином $g(x) = 1,\ (n, n),\ R = 1,\ d = 1,\ \nexists g^{\perp}(x)$.

А также $g(x) = x^{n-1} + x^{n-2} + \cdots + 1,\ (n, 1),\ R = \frac{1}{n}, d = n,\ g^{\perp}(x) = x + 1$.

И $g(x) = x + 1,\ (n, n-1), R = \frac{n-1}{n}, d = 2, g^{\perp}(x) =\ x^{n-1} + x^{n-2} + \cdots + 1$.

1) $n = 3$

$x^3 + 1 = (x + 1)(x^2 + x + 1)$

Все возможные порождающие полиномы приведены выше в общем виде.

2) $n = 4$

$x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1) = (x + 1)^2(x^2 + 1)$

$g(x)$	(n, k)	R	d	$g^{\perp}(x)$
$x^2 + 1$	$(4, 2)$	$\frac{1}{2}$	2	$x^2 + 1$

3) $n = 5$

$x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x^1 + 1)$

Все возможные порождающие полиномы приведены выше в общем виде.

4) $n = 6$

$x^6 + 1 = (x + 1)(x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 1)^2(x^4 + x^2 + 1) = (x + 1)^2(x^2 + x + 1)^2$

$g(x)$	(n, k)	R	d	$g^{\perp}(x)$
$x^4 + x^2 + 1$	$(6, 2)$	$\frac{1}{3}$	3	$x^2 + 1$
$x^2 + x + 1$	$(6, 4)$	$\frac{2}{3}$	2	$x^4 + x^3 + x + 1$
$x^2 + 1$	$(6, 4)$	$\frac{2}{3}$	2	$x^4 + x^2 + 1$
$x^3 + 1$	$(6, 3)$	$\frac{1}{2}$	2	$x^3 + 1$
$x^4 + x^3 + x + 1$	$(6, 2)$	$\frac{1}{3}$	4	$x^2 + x + 1$

5) $n = 7$

$x^7 + 1 = (x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$

$g(x)$	(n,k)	R	d	$g^{\perp}(x)$
x^3+x^2+1	$(7,4)$	$\frac{4}{7}$	3	$x^4+x^3+x^2+1$
x^3+x+1	$(7,4)$	$\frac{4}{7}$	3	x^4+x^2+x+1
x^4+x^2+x+1	$(7,3)$	$\frac{3}{7}$	4	x^3+x+1
$x^4+x^3+x^2+1$	$(7,3)$	$\frac{3}{7}$	4	x^3+x^2+1

6) $n=8$

$x^8+1=(x+1)(x^7+x^6+x^5+x^4+x^3+x^2+x+1)=(x+1)^2(x^6+x^4+x^2+1)=$
$(x+1)^2(x^3+x^2+x+1)^2=(x+1)^6(x^2+1)$

$g(x)$	(n,k)	R	d	$g^{\perp}(x)$
x^2+1	$(8,6)$	$\frac{3}{4}$	2	$x^6+x^4+x^2+1$
x^3+x^2+x+1	$(8,5)$	$\frac{5}{8}$	2	x^5+x^4+x+1
x^4+1	$(8,4)$	$\frac{1}{2}$	2	x^4+1
x^5+x^4+x+1	$(8,3)$	$\frac{3}{8}$	4	x^3+x^2+x+1
$x^6+x^4+x^2+1$	$(8,2)$	$\frac{1}{4}$	4	x^2+1

7) $n=9$

$x^9+1=(x+1)(x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)=(x+1)(x^2+x+1)(x^6+x^3+1)$

$g(x)$	(n,k)	R	d	$g^{\perp}(x)$
x^2+x+1	$(9,7)$	$\frac{7}{9}$	2	$x^7+x^6+x^4+x^3+x+1$
x^6+x^3+1	$(9,3)$	$\frac{1}{3}$	3	x^3+1
x^3+1	$(9,6)$	$\frac{2}{3}$	2	x^6+x^3+1
$x^7+x^6+x^4+x^3+x+1$	$(9,2)$	$\frac{2}{9}$	6	x^2+x+1

Задача 2.

Построим все поля $GF(2^3)$. Для этого необходимо найти все простые полиномы $p(x)$. Таких полиномов всего два: x^3+x^2+1 и x^3+x+1.

Самборский Иван М4138
09.11.2015

	$p(x) = x^3 + x^2 + 1$	$p(x) = x^3 + x + 1$
$-\infty$	0	0
x^0	1	1
x	$x^2 + 1$	x
x^2	$x^2 + x$	x^2
x^3	x^2	$x + 1$
x^4	$x + 1$	$x^2 + x$
x^5	x	$x^2 + x + 1$
x^6	$x^2 + x + 1$	$x^2 + 1$

Генерирующие элементы

Пусть $f: F_1 \to F_2$ — изоморфизм, сопоставляющие одинаковые степени генератора. Покажем, что $f(x_i) + f(x_j) = f(x_i + x_j)$ и $f(x_i)f(x_j) = f(x_i \cdot x_j)$.

$f(x_i + x_j) = f(x_i + x_i x_{j-i}) = f\left(x_i \cdot (1 + x_{j-i})\right) = f(x_i) f(1 + x_{j-i}) =$

	$f(1) + f(x_i)$	$f(1 + x_i)$
0	$1 + 0 = 1$	1
1	$1 + 1 = 0$	0
$x^2 + 1$	$1 + x = 1 + x$	$x + 1$
$x^2 + x$	$1 + x^2 = 1 + x^2$	$x^2 + 1$
x^2	$1 + (x + 1) = x$	x
$x + 1$	$1 + (x^2 + x) = 1 + x + x^2$	$x^2 + x + 1$
x	$1 + (x^2 + x + 1) = x^2 + x$	$x^2 + x$
$x^2 + x + 1$	$1 + (x^2 + 1) = x^2$	x^2

$= f(x_i)\left(f(1) + f(x_{j-i})\right) = f(x_i)\left(1 + f(x_{j-i})\right) = f(x_i) + f(x_i) f(x_{j-i}) = f(x_i) + f(x_j)$

Последний переход докажем, с помощью доказательства второго свойства изоморфизма. Что тривиально, так как произведение элементов поля эквивалентно произведению степеней генерирующего элемента в данном поле.

Задача 3.

1) $GF(2)$

Элемент поля	Порядок
0	
1	1

2) $GF(3)$

Элемент поля	Порядок
0	
1	1
2	2

3) $GF(2^2), p(x) = x^2 + x + 1$

	Элемент поля	Порядок
$-\infty$	0	

x^0	1	1
x^1	x	3
x^2	$x+1$	3

$\boldsymbol{x^3} = (x+1)\cdot x = x^2 + x = 2x + 1 = 1$
$(\boldsymbol{x+1})^{\boldsymbol{3}} = (x^2+1)(x+1) = x(x+1) = x^2 + x = x + x + 1 = 1$

4) $GF(5)$

Элемент поля	Порядок
0	
1	1
2	4
3	4
4	2

5) $GF(7)$

Элемент поля	Порядок
0	
1	1
2	3
3	6
4	3
5	6
6	2

6) $GF(2^3), p(x) = x^3 + x + 1$

	Элемент поля	Порядок
$-\infty$	0	
x^0	1	1
x^1	x	7
x^2	x^2	7
x^3	$x+1$	7
x^4	x^2+x	7
x^5	x^2+x+1	7
x^6	x^2+1	7

$\left(\boldsymbol{x^2}\right)^{\boldsymbol{7}} = (x^2+1)^2x^2 = (x^4+1)x^2 = (x^2+x+1)x^2 = x^4 + x^3 + x^2 = x^2 + x + x + 1 + x^2 = 1$
$(\boldsymbol{x+1})^{\boldsymbol{7}} = (x^2+1)^3(x+1) = (x^4+1)(x^3+x+x^2+1) = (x^2+x+1)(x+1+x+x^2+1) =$
$x^4 + x^3 + x^2 = x^2 + x + x + 1 + x^2 = 1$
…

Самборский Иван М4138
09.11.2015

7) $GF(3^2), p(x) = x^2 + x + 1$

	Элемент поля	Порядок
$-\infty$	0	
x^0	1	1
x^1	x	8
x^2	$x+1$	4
x^3	$2x+1$	8
x^4	2	2
x^5	$2x$	8
x^6	$2x+2$	4
x^7	$x+2$	8

Задача 4.

$GF(2^4), p(x) = 1 + x + x^4$

	Элемент поля	Обратный элемент
$-\infty$	0	—
x^0	1	1
x^1	x	x^3+1
x^2	x^2	x^3+x^2+1
x^3	x^3	x^3+x^2+x+1
x^4	$x+1$	x^3+x^2+x
x^5	x^2+x	x^2+x+1
x^6	x^3+x^2	x^3+x
x^7	x^3+x+1	x^2+1
x^8	x^2+1	x^3+x+1
x^9	x^3+x	x^3+x^2
x^{10}	x^2+x+1	x^2+x
x^{11}	x^3+x^2+x	$x+1$
x^{12}	x^3+x^2+x+1	x^3
x^{13}	x^3+x^2+1	x^2
x^{14}	x^3+1	x

Задача 5.

$GF(2^4), p(x) = 1 + x + x^2 + x^3 + x^4$

	Элемент поля	Обратный элемент
$-\infty$	0	—
x^0	1	1
x^1	$x+1$	x^3+x
x^2	x^2+1	x^2+x
x^3	x^3+x^2+x+1	x
x^4	x^3+x^2+x	x^3+x+1
x^5	x^3+x^2+1	x^3+x^2
x^6	x^3	x^2
x^7	x^2+x+1	x^3+1

Самборский Иван М4138
09.11.2015

x^8	x^3+1	x^2+x+1
x^9	x^2	x^3
x^{10}	x^3+x^2	x^3+x^2+1
x^{11}	x^3+x+1	x^3+x^2+x
x^{12}	x	x^3+x^2+x+1
x^{13}	x^2+x	x^2+1
x^{14}	x^3+x	$x+1$