

Типовой расчет по дискретной математике

2 курс 3 семестр

1. Постройте рекуррентную последовательность с периодом $k = \text{const}$.

Замечание!: Поле содержащее элемент нужного порядка должно содержать подполе.

1) Построить поле в котором существует элемент порядка K .

$$F_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\} - \text{подполе.}$$

$F_p[x] = \{a_\infty x^\infty + a_{\infty-1} x^{\infty-1} + x^{\infty-2} \dots + a_0 \mid a_\infty, a_{\infty-1}, \dots, a_0 \in F_p\}$ – множество всевозможных многочленов, коэффициенты которых берутся из F_p .

Что означает эта запись: $F_p[x]/(x^q \dots)$ - ?

Из теории: $F_p[x]/(x^q \dots) = \{A_1 x^{q-1} + A_2 x^{q-2} + \dots + A_n \mid A_1, A_2, \dots, A_n \in F_p\}$

Пример № 1:

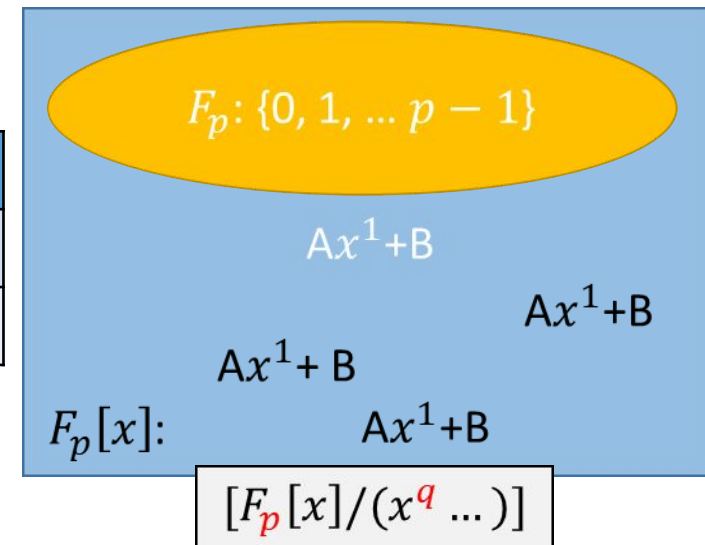
$$(x^3 + x^2 + 1)/(x^2 + x + 1) = (A_1 x^1 + A_0)$$

Пример № 2:

$$(x^7 + x^2 + 1)/(x^2 + x + 1) = (A_5 x^5 + A_4 x^4 + \dots + A_0)$$

$$(x^7 + x^2 + 1)/(x^2 + x + 1) \approx (x^7 + x^2 + 1) \% (x^2 + x + 1) = (A_1 x^1 + A_0)$$

0			
1			



Вывод:

$$F_p[x]/(x^q \dots) \approx F_p[x] \% (x^q \dots) = \{A_1 x^{q-1} + A_2 x^{q-2} + \dots + A_n \mid A_1, A_2, \dots, A_n \in F_p\}$$

$F_p[x]/(x^q \dots)$ – поле над подполем F_p .

$[F_p[x]/(x^q \dots)]$ – фактор-группа. ~ (Поле)

p^q – число элементов в поле, которое имеет подполе F_p

$p^q - 1 =$ максимальным порядком (+Индивидуальные порядки элем'с.). Поля $[F_p[x]/(x^q \dots)]$, кол. Во обратимых.

$$p^q - 1 = C = S_1 \cdot S_2 \cdot S_3$$

$p^q - 1 = C = S_1 \cdot S_2 \cdot \dots \cdot K \cdot S_n = K \cdot S$, где $S = S_1 \cdot S_2 \cdot \dots \cdot S_n$ и $K \cdot S, S_1, S_2, \dots, S_n$ – делители числа C . т. е. индивидуальные порядки для определенных элементов поля $[F_p[x]/(x^q \dots)]$.

$a^K = e$ – В мультипликативной терминологии.

$q\lambda = e$ – В аддитивной терминологии порядок.

1. Постройте рекуррентную последовательность с периодом $k = 31$

Замечание!: Поле содержащее элемент нужного порядка должно содержать подполе.

$$F_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\} - \text{подполе.} \quad p^q - 1 = C = K \cdot S \quad p^q - 1 = C = 31 \cdot S \quad p^q = 31 \cdot S + 1$$

$$F_p[x]/(x^q \dots) = \{A_1 x^{q-1} + A_2 x^{q-2} + \dots + A_n \mid A_1, A_2, \dots, A_n \in F_p\}$$

$$p^q = 1 : S = 0$$

$$p^q = 32 = 2^5 = 31 \cdot 1 + 1 : S = 1$$

$$F_2[x]/(x^5 \dots) = \{A_4 x^4 + A_3 x^3 + A_2 x^2 + A_1 x^1 + A_0 x^0 \mid A_0, A_1, \dots, A_4 \in F_2\}$$

$$p = 2, q = 5$$

$(F_2[a], a^5 = a^3 + 1) = F_2[a]$, где a корень многочлена $(x^5 + x^3 + 1) = F_2[x]/(x^5 + x^3 + 1) = \{A_4 x^4 + A_3 x^3 + A_2 x^2 + A_1 x^1 + A_0\}$

$$x^5 + x^3 + 1 = 0 \quad a^5 = -a^3 - 1 = a^3 + 1 \quad b = A_4 x^4 + A_3 x^3 + A_2 x^2 + A_1 x^1 + A_0$$

$$a^5 = a^3 + 1$$

$$p^q = 32 \quad b^{31} = 1$$

$$b = x^4 + x^3 + x^2 + x^1 + 1$$

$p^q - 1 =$ максимальным порядком (+Индивидуальные порядки элем's.). Поля $[F_p[x]/(x^q \dots)]$, кол. Во обратимых.

$$C = p^q - 1 = 31 \quad b^{31} = b \quad b = a^4 + a^3 + a^2 + a^1 + 1$$

$$b = x^4 + x^3 + x^2 + x^1 + 1$$

$$x^i$$

$$x_{n+3} + x_{n+2} + x_{n+1} + x_n + x_{n-1} = 0$$

$$1. x^4 + x^3 + x^2 + x^1 + 1 = 0 \mid F_2$$

$$x_{n+(i-1)}$$

$$x_{n+3} = -x_{n+2} - x_{n+1} - x_n = x_{n+2} + x_{n+1} + x_n + x_{n-1}$$

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

$$[0 \quad 0 \quad 0 \quad 0 \quad -a_0 \quad 1]$$

$$x_{n+3} = x_{n+2} + x_{n+1} + x_n + x_{n-1}$$

										30																			
0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0
1	22	23	24	25	26	27	28	29	30	31																			

$n \in \mathbb{N}$

$$x_0 = x_{n+3} = x_{n+2} + x_{n+1} + x_n + x_{n-1}$$

$$n + 3 = 0$$

$$n = -3$$

$n \in \mathbb{N}$

$$x_0 = x_{-1} + x_{-2} + x_{-3} + x_{-4} = 0 + 0 + 0 + 0 = 0$$

$$n + 3 = 1$$

$$n = 1 - 3 = -2$$

$$x_1 = x_0 + x_{-1} + x_{-2} + x_{-3} = 0 + 0 + 0 \mid \text{Пусть } x_1 = 1$$

$$n + 3 = 1$$

$$n = -2$$

$$n = 1 - 3 = -2$$

$$x_2 = x_1 + x_0 + x_{-1} + x_{-2} = 1 + 0 + 0 = 1$$

$$n + 3 = 2$$

$$n = 2 - 3$$

$$n = -1$$

$$x_3 = x_{n+3} = x_{n+2} + x_{n+1} + x_n = x_2 + x_1 + x_0 + x_{-1} = 1 + 1 + 0 + 0 = 0$$

$$n + 3 = 3 \quad n = 0$$

$$x_4 = x_{n+2} + x_{n+1} + x_n = x_3 + x_2 + x_1 + x_0 = 1 + 0 + 0 = 0$$

$$n = 4 - 3 = 1$$

$$n + 3 = 4$$

2. Определить период последовательности сдвигового регистра, задаваемого многочленом.

- $A_1x^{q-1} + A_2x^{q-2} + \dots + A_n$;
- $F_p[x]/(x^q \dots) = \{A_1x^{q-1} + A_2x^{q-2} + \dots + A_n \mid A_1, A_2, \dots, A_n \in F_p\}$

p^q – число элементов в поле, которое имеет подполе F_p .

$p^q - 1$ = максимальным порядком (+ Индивидуальные порядки элем's.). Поля $[F_p[x]/(x^q \dots)]$, кол. Во обратимых.

$$p^q - 1 = C = S_1 \cdot S_2 \cdot S_3 \cdot \dots \cdot S_n$$

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & \dots & -a_0 \\ 1 & 0 & 0 & 0 & \dots & -a_1 \\ 0 & 1 & 0 & 0 & \dots & -a_2 \\ 0 & 0 & 1 & 0 & \dots & -a_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 1 & -a_{n-1} \end{bmatrix} -$$

$$M^{S_i} = M, \text{ где } S_i \in \{S_1, S_2, S_3, \dots, S_n\}$$

$$M^{S_i-1=r} = E, \text{ где } S_i \in \{S_1, S_2, S_3, \dots, S_n\}, S_i = r + 1;$$

2. Определить период последовательности сдвигового регистра, задаваемого многочленом.

$$F_p[x]/(x^q \dots) = \{a = x^3 + 2x + 2 \mid A_1, A_2, \dots, A_n \in F_3\}$$

$$K = F_3, a = x^3 + 2x + 2$$

$$p^q = 3^4 = 81$$

$$p^q - 1 = 3^4 - 1 = 81 - 1 = 80$$

p^q – число элементов в поле, которое имеет подполе F_p

$$p^q - 1 = C = S_1 \cdot S_2 \cdot S_3$$

$$F_3[x]/(x^4 \dots) = \{b = x^3 + 2x + 2, A_3x^3 + A_2x^2 + A_1x + A_0 \mid A_1, A_2, \dots, A_3 \in F_3\}$$

$$F_3[a]/(a^4 + 1) = \{b = a^3 + 2a + 2, A_3x^3 + A_2x^2 + A_1x + A_0 \mid A_1, A_2, \dots, A_3 \in F_3\}$$

$p^q - 1$ = максимальным порядком (+Индивидуальные порядки элем'с.). Поля $[F_p[x]/(x^q \dots)]$, кол. Во обратимых.

$$p^q - 1 = 80 = 1 \cdot 2^4 \cdot 5 = \{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$$

$$a^4 = (-1) = 2$$

$$b(a) = a^3 + 2a + 2 \quad b = a^3 + 2a + 2$$

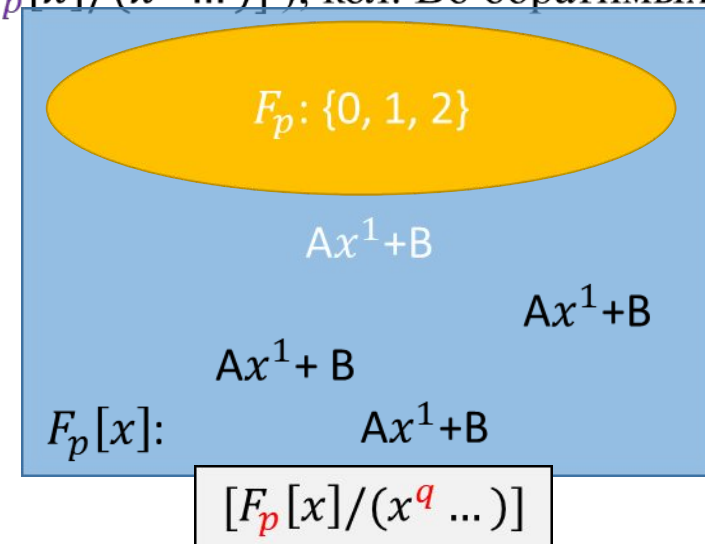
$$b^k = 1, k \in \{2, 4, 5, 8, 10, 16, 20, 40\}$$

$$(a^3 + (2a + 2))^k = 1$$

$$[a^3]^k + (2a + 2)^k = 1$$

$$(2a + 2)^k = (2a)^k + 2^k$$

0	1		
1	2		
2	2		



2. Определить период последовательности сдвигового регистра, задаваемого многочленом.

$$F_p[x]/(x^q \dots) = \{a = x^3 + 2x + 2 \mid A_1, A_2, \dots, A_n \in F_3\}$$

$$K = F_3, a = x^3 + 2x + 2$$

$$p^q = 3^4 = 81$$

$$p^q - 1 = 3^4 - 1 = 81 - 1 = 80$$

p^q — число элементов в поле, которое имеет подполе F_p

$$p^q - 1 = C = S_1 \cdot S_2 \cdot S_3$$

$$F_3[x]/(x^5 \dots) = \{b = x^3 + 2x + 2, A_3x^3 + A_2x^2 + A_1x + A_0 \mid A_1, A_2, \dots, A_3 \in F_3\}$$

$$F_3[a]/(a^4 + 1) = \{b = a^3 + 2a + 2, A_3x^3 + A_2x^2 + A_1x + A_0 \mid A_1, A_2, \dots, A_3 \in F_3\}$$

$p^q - 1 =$ максимальным порядком (+Индивидуальные порядки элем'с.). Поля $[F_p[x]/(x^q \dots)]$, кол. Во обратимых.

$$p^q - 1 = 80 = 1 \cdot 2^4 \cdot 5 = \{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$$

$$a^4 = (-1) = 2$$

$$b(a) = a^3 + 2a + 2 \quad b = a^3 + 2a + 2$$

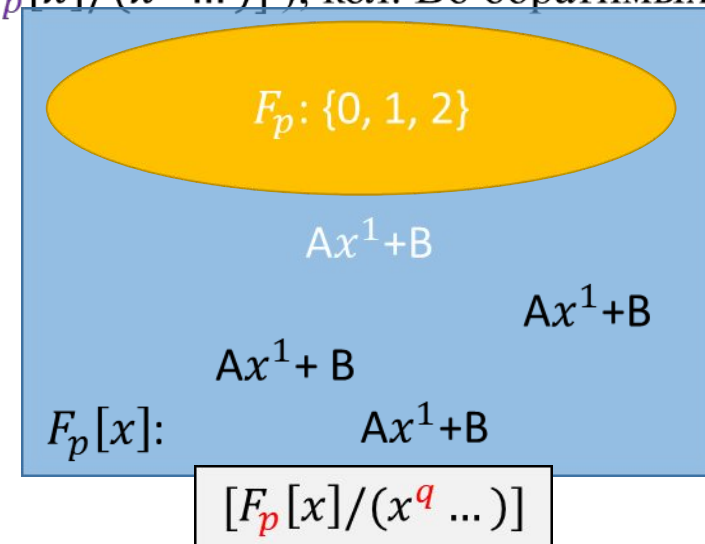
$$b^k = 1, k \in \{2, 4, 5, 8, 10, 16, 20, 40\}$$

$$(a^3 + (2a + 2))^k = 1$$

$$[a^3]^k + (2a + 2)^k = 1$$

$$(2a + 2)^k = (2a)^k + 2^k$$

0	1		
1	2		
2	2		



$$(a^3 + 2a + 2)^{80} = \left((a^3 + 2a + 2)^5 \right)^{16} =$$

$$a^4 = 2$$

- $(a^3 + 2a + 2)^5 = (a^3 + 2a + 2)^2 \cdot (a^3 + 2a + 2)^2 \cdot (a^3 + 2a + 2) =$
- $= (a^3 + (2a + 2))^2 = 2a^2 + 2 + 4a^3 + (2a + 2)^2 = a^3 + 2a$
- $(2a + 2)^2 = 4a^2 + 8a + 4 = a^2 + 2a + 1$
- $= (a^3 + 2a)^{16} = a^{16} \cdot (a + 2)^{16} = a^{16} \cdot (a + 2)^{16}$

$$K = F_7, b = x^2 + 6x + 2$$

$$F_7[x]/(x^3 \dots) = \{b = x^2 + 6x + 2 \mid A_1, A_2, \dots, A_n \in F_7\}$$

$$7^3 - 1 = 7 \cdot 7 \cdot 7 - 1 = 49 \cdot 7 - 1 = 343 - 1 = 342 = \{1, 2, 3, 6, 9, 18, 19, 38, 57, 114, 171, 342\}.$$

$$F_7[a]/(a^q \dots) = \{b = a^2 + 6a + 2 = 0 \cdot a^3 + a^2 + 6a + 2 \mid A_1, A_2, \dots, A_n \in F_7\}$$

$$a^3 = 5 \quad b^k = 1$$

F_7

0	2	
1	3	
2	3	
3	1	
4	3	
5	1	$4 \cdot 5 + 2 = 22 = 1$
6	1	$1 \cdot 6 + 2 = 8 = 1$

$$k = 2: b^2 = (a^2 + (6a + 2))^2 = 12a^3 + 40a^2 + 29a + 4 = 5a^3 + 5a^2 + a + 4 = 5a^2 + a + 1$$

$$k = 3: b^3 = (a^2 + 6a + 2)^3 = (a^2 + (6a + 2))^2 (a^2 + 6a + 2) = (5a^2 + a + 1)(a^2 + 6a + 2) = (4a + 3 + 9a^2) = 2a^2 + 4a + 3$$

$$k = 6: b^6 = (b^3)^2 = (2a^2 + 4a + 3)^2 = 2a + 5$$

$\{1, 2, 3, 6, 9, 18, 19, 38, 57, 114, 171\}$

$$k = 9: b^9 = (b^3)^3 = b^6 b^3 = (2a + 5)(2a^2 + 4a + 3) = 5a + 4a^2 = a(4a + 5)$$

$$k = 18: b^{18} = (b^9)^2 = (a(4a + 5))(a(4a + 5)) = a^2(4a + 5)^2 = (3a + 1 + 4a^2)$$

$$k = 19: b^{19} = b^{18} \cdot b = (4a^2 + 3a + 1)(a^2 + 6a + 2) = (11a + 4 + 6a^2) = 6a^2 + 11a + 4$$

3	5	
4	5	
5	3	
6	2	

$$K = F_7, b = x^2 + 6x + 2$$

$$F_7[x]/(x^4 \dots) = \{ b = x^2 + 6x + 2 \mid A_1, A_2, \dots, A_n \in F_7 \}$$

$$7^4 - 1 = 7 \cdot 7 \cdot 7 \cdot 7 - 1 = 2401 - 1 = 2400 = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 25, 30, 32, 40, 48, 50, 60, 75, 80, 96, 100, 120, 150, 160, 240, 300, 400, 480, 600, 800, 1200, 2400\}$$

$$F_7[a]/(a^4 \dots) = \{ b = a^2 + 6a + 2 = 0 \cdot a^3 + a^2 + 6a + 2 \mid A_1, A_2, \dots, A_n \in F_7 \}$$

$$a^4 = 6 \quad b^k = 1$$

$$b^k = (a^2 + 6a + 2)^k = (a^2)^k + (6a)^k + 2^k = 1 \quad \boxed{F_7}$$

$$k = 2: b^2 = (a^2 + 6a + 2)^2 = (a^2)^2 + (6a)^2 + 2^2 = 4 + a^2 + 6 = a^2 + 3$$

$$8 \cdot 27 = 216 = 6^3 \quad k = 3: b^3 = (a^2 + 6a + 2)^3 = (a^2)^3 + (6a)^3 + 2^3 = 8 + 6a^2 + 4 = 6a^2 + 12 = 6a^2 + 5$$

$$(b^2)^2 = (a^2 + 3)^2 = a^4 + 9 = 6 + 9 = 6 + 2 = 8 = 1 \quad k = 4$$

$$k = 4: b^4 = (a^2 + 6a + 2)^4 = (a^2)^4 + (6a)^4 + 2^4 = (a^4)^2 + (a^4) + 2 = 36 + 6 + 2 = 1 + 6 + 2 = 9 = 2$$

$$k = 3: b^3 = (a^2 + 6a + 2)^3 = (a^3)^2 + (6a)^3 + 2^3 = 1 + 2 + 4 = 0$$

$$k = 6: b^6 = (a^2 + 6a + 2)^6 = ((a^2 + 6a + 2)^3)^2 = 0^2 = 0$$

{1, 2, 3, 6, 9, 18, 19, 38, 57, 114, 171}

$$\{7,9,1,21,3,63\} = 2^6 - 1 = p^q = 9 \cdot S + 1 \quad p^q - 1 = 15 \cdot S \quad p^q = 15 \cdot S + 1 \quad \text{Макс порядок}$$

$$F_2 \quad p^q = 15 \cdot S + 1 \quad q = 3$$

$$\{1,3,5,15\} = 15 - p \quad \text{Макс порядок}$$

$$F_2[a], a^4 = a + 1 \in F_2[a], \text{ где } a \text{ — корень многочлена } x^4 + x + 1 = [F_2[x]/(x^4 + x + 1)] = \{A + Bx + Cx^2 + Dx^3 : A, B, C, D \in F_2\}$$

14														14															
1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0

$$[F_2[x]/(x^4 + x + 1)] = \{Ax^3 + Bx^2 + Cx + D : A, B \in F_2\} \quad x^4 = x + 1 \quad x^4 + x + 1 = 0$$

$$x^3 + x + 1 \quad B^{15} = B$$

$$b = x^3 + x + 1 \quad b^{15} = b^5 \cdot b^5 \cdot b^5 \quad b^5 =$$

$$b = x^3 + x + 1 = x^3 + a_2 \cdot x^2 + a_1 x + a_0 \quad b = x^3 + x + 1 - \text{минимальным многочленом } B$$

$$x^3 + x + 1 - \text{неприводимы}$$

$$N(B) = B^3 + B + E = 0$$

$$B = \begin{bmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} - \text{НФФ} \quad x_{n+2} + x_n + x_{n-1} = 0$$

$$x_{n+2} = x_n + x_{n-1} \quad 1,0,1,1,1, 0, 0, 1,0,1,1,1,0,0,1,0, \quad n + 2 = 1$$

$$x_0 = x_{-2} + x_{-3} = 1 \quad x_3 = x_1 + x_0 = 1 \quad x_7 = x_{n+2} = x_5 + x_4 = 1 \quad x_{13} = x_{n+2} = x_{11} + x_{10} = 0 \quad n + 2 = 4$$

$$x_1 = x_{-1} + x_{-2} = 0 \quad x_4 = x_{n+2} = x_2 + x_1 = 1 \quad x_8 = x_{n+2} = x_6 + x_5 = 0 \quad x_{14} = x_{n+2} = x_{12} + x_{11} = 0 \quad n + 2 = 5$$

$$x_2 = x_0 + x_{-1} = 1 \quad x_5 = x_{n+2} = x_3 + x_2 = 0 \quad x_9 = x_{n+2} = x_7 + x_6 = 1 \quad x_{15} = x_{n+2} = x_{13} + x_{12} = 0 \quad n + 2 = 6$$

$$x_6 = x_{n+2} = x_4 + x_3 = 0 \quad x_{10} = x_{n+2} = x_8 + x_7 = 1 \quad x_{16} = x_{n+2} = x_{14} + x_{13} = 0$$