Министерство науки и высшего образования Российской Федерации
Российский технологический университет - МИРЭА

Институт кибернетики
Кафедра высшей математики

Типовой расчёт
по предмету: «Дискретная математика»
III семестр

Вариант 18

Выполнил студент группы КМБО-02-19
Проскуряков Иван

№	1	2

Москва 2020

Содержание

Теоретическая справка

Зададим рекуррентную последовательность по следующему принципу:

1. Пусть длина последовательности будет m, период τ.

2. Члены последовательности будут меняться по правилу:

$$\begin{aligned}
&X_{\text{нач}} = (x_0, x_1, \cdots, x_{m-1}) \text{ - некоторое начальное состояние последовательности}\\
&X'_{\text{нов}} = \left(x'_0, x'_1, \cdots, x'_{m-1}\right) \text{ - следующее состояние системы}\\
&x'_0 = a_0 x_m\\
&x'_1 = x_0 + a_1 x_{m-1}\\
&x'_2 = x_1 + a_2 x_{m-1}\\
&\cdots\\
&x'_{m-1} = x_{m-2} + a_{m-1} x_{m-1}
\end{aligned} \tag{1}$$

Теперь запишем (1) в матричном виде:

$$X^T_{\text{нов}} = BX^T_{\text{нач}}, \text{ где B - матрица нормальной Фробениусовой формы}$$

$$B = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & 1 & a_{m-1} \end{bmatrix} \tag{2}$$

Тогда для N-го такта имеем:

$$X_N = B^N X_{\text{нач}} \tag{3}$$

Из (3) видно, что последовательность зациклится, если $B^N = E$, тогда $X_N = X_{\text{нач}}$, т.е. для нахождения периодна последовательности достаточно найти порядок матрицы B.

Искать $ordB$ как порядок элемента $gl(m, \mathbb{F}_p)$ сложно и долго, поэтому рассмотрим $\mathbb{F}_p[B] \subset gl(m, \mathbb{F}_p)$, где

$$\mathbb{F}_p[B] = \left\{x_o B^0 + x_1 B^1 + \ldots + x_{m-1} B^{m-1} | x_i \in \mathbb{F}_p\right\}$$

$\mathbb{F}_p[B]$ будет алгеброй над $\mathbb{F}_p$ (коммутативной, ассоциативной, с единицей), при этом $\mathbb{F}_p[B]$ будет полем, если $\mu_B(x)$ - минимальный многочлен матрицы B - окажется неприводим. Тогда можно заняться поиском порядка матрицы $B^{m \times m}$ уже в получившемся поле.

Чтобы найти некоторую матрицу B вида 2 с коэффициентами $a_i \in \mathbb{F}_p$ заданного порядка τ, достаточно рассмотреть $\mathbb{F}_p[q]$, где q - корень некоторого неприводимого над $\mathbb{F}_p$ многочлена. При этом $|\mathbb{F}_p[q]^*| \vdots T$, т.е. в $\mathbb{F}_p[q]$ может найтись элемент порядка τ.

Если такой элемент β найдётся, и его минимальный многочлен окажется неприводим на $\mathbb{F}_p$, то можно утверждать, что матрица вида 2 восстановится по $\mu_\beta(x)$ и будет иметь порядок τ.

Задача 1

Постройте рекуррентную последовательность с периодом $k = 8$. Замечание: поле, содержащее элемент нужного порядка, должно содержать подполе.

Решение:

1. Рассмотрим $\mathbb{F}_7[\alpha]$, где $\alpha^2 = -1$. $\mathbb{F}_7[\alpha]$ - поле (т.к. многочлен $x^2 + 1$ очевидно неприводим над $\mathbb{F}_7$), при этом $\mathbb{F}_7 \subset \mathbb{F}_7[\alpha]$, т.е. в поле $\mathbb{F}_7[\alpha]$ $\exists$ нетривиальное подполе.

   Пояснение. *Если бы x^2+1 был приводим над $\mathbb{F}_7$, то тогда бы он разлагался в произведение двух многочленов первого порядка вида $(x-a)(x-b)$, где $a, b \in \mathbb{F}_7$, т.е. имел бы корни над $\mathbb{F}_7$, что, очевидно, не выполнено.*

2. В $\mathbb{F}_7[\alpha]$ найдём элемент 8-го порядка:

   - Т.к. $|\alpha^*| = 48$ и $48 \vdots 8$, то в этом поле вполне может найтись элемент заданного порядка (каждый элемент образует циклическую группу, а порядок подгруппы должен быть делителем порядка группы).
   - Рассмотрим элемент $\alpha - 1$:
     Возможные порядки для него: $\{2, 3, 4, 6, 8, 12, 16, 24, 48\}$

     $$\begin{aligned}
     &(\alpha-1)^2 = -2\alpha \\
     &(\alpha-1)^3 = 2(\alpha+1) \\
     &(\alpha-1)^4 = (-2\alpha)^2 = 4\alpha^2 = -4 \\
     &(\alpha-1)^8 = (\alpha-1)^4(\alpha-1)^4 = 2 \\
     &(\alpha-1)^{24} = ((\alpha-1)^8)^3 = 2^3 = 1
     \end{aligned}$$

     Отсюда $\Rightarrow ord(\alpha-1)^3 = 8$, $(\alpha-1)^3 = 2(\alpha+1) = \beta$.

3. Т.к. β линейно не выражается через свою нулевую степень, попробуем выразить линейно β^2 через β^1, β^0:

   $$\begin{aligned}
   &(2(\alpha+1))^2 = 4(-1+2\alpha+1) = \alpha = 4(2(\alpha+1)) - 1 \\
   &\beta^2 = 4\beta - 1
   \end{aligned}$$

   Тогда β является корнем многочлена $x^2 - 4x + 1$

4. Имеем $\mu_\beta(x) = x^2 - 4x + 1$ - неприводим над $\mathbb{F}_7$ (по тем же соображениям, что и в **Пояснении** выше).

   Наблюдение 1. *Данный многочлен можно было получить и другим путём. Т.к. β является корнем некоторого неприводимого над $\mathbb{F}_7$ многочлена второй степени (доказывалось на семинаре), то корнем этого многочлена также является $\Phi(\beta)$ - значение отображения Фробениуса от β. Получим многочлен:*

   $$(x - 2(\alpha+1))(x - 2\Phi(\alpha+1)) = (x - 2(\alpha+1))(x - 2(1-\alpha)) = x^2 - 4x + 1$$

5. Соответствующая многочлену $\mu_\beta(x) = x^2 - 4x + 1$ матрица нормальной Фробениусовой формы запишется:

   $$B = \begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}$$

   Т.к. порядок этой матрицы равен 8, то она задаст рекуррентную последовательность периода 8 по правилу 1.

Задача 2

Определите период последовательности сдвигового регистра, задаваемого многочленом:

I. $\mathbb{K} = \mathbb{F}_2,\ P(x) = x^6 + x^4 + x^3 + x^2 + x + 1$

II. $\mathbb{K} = \mathbb{F}_3,\ P(x) = x^3 + 2x^2 + 1$

Решение:

I. 1. Проверим $P(x)$ на приводимость:

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

Многочлен x^4+x+1 является неприводимым, т.к. он не имеет корней над $\mathbb{F}_2$ и не делится на единственный неприводимый над $\mathbb{F}_2$ многочлен второй степени (x^2+x+1, $x^4+x+1 = x^2 + x + \dfrac{1}{x^2+x+1}$).

2. $\mathbb{F}_2[\alpha], \alpha^6 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \backsim \mathbb{F}_2[x]/(P(x)), \Rightarrow |\mathbb{F}_2[\alpha]^*| = |\mathbb{F}_2[x]/(P(x))^*|$

$$|\mathbb{F}_2[x]/(P(x))^*| = \quad |\mathbb{F}_2[x]/(x^2-1)^*| \quad * \quad |\mathbb{F}_2[x]/(x^4+x+1)^*|$$

$$|\mathbb{F}_2[x]/(x^2-1)^*| = 2$$

$$|\mathbb{F}_2[x]/(x^4+x+1)^*| = 15$$

$$|\mathbb{F}_2[x]/(P(x))^*| = 2 * 15 = 30$$

3. Приступим к поиску порядка элемента α:
Возможные порядки (исходя из порядка мультипликативной группы кольца $\mathbb{F}_2[\alpha]$ - см. предыдущее действие): $\{2, 3, 5, 6, 10, 15, 30\}$

$$\underline{\alpha^6} = \underline{\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1}$$
$$\underline{\alpha^9} = \alpha^3(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = \alpha(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) +$$
$$+ (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + \alpha^5 + \alpha^4 + \alpha^3 = \underline{\alpha^4 + \alpha^3 + 1}$$
$$\underline{\alpha^{10}} = \underline{\alpha^5 + \alpha^4 + \alpha}$$
$$\underline{\alpha^{15}} = (\alpha^4 + \alpha^3 + 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = \alpha^2(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) +$$
$$+ 2\alpha^7 + 2\alpha^6 + 2\alpha^5 + 2\alpha^4 + \alpha^3 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) +$$
$$+ \alpha^5 + \alpha^3 + \alpha + 1 = \underline{\alpha^5 + \alpha^4 + \alpha^2}$$
$$\underline{\alpha^{30}} = \alpha^{10} + (\alpha^4 + \alpha^2)^2 = \alpha^{10} + \alpha^8 + \alpha^4 = \alpha^4(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + \alpha^8 + \alpha^4 =$$
$$= \alpha(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + \alpha^5 = \underline{1}$$

$ord\alpha = 30$, следовательно порядок матрицы вида 2, соответствующей данному многочлену и задающей данную последовательность сдвиговых регистров, будет равен 30.

II. 1. Проверим $P(x)$ на приводимость:
Если он приводим, то разлагается на произведение многочленов второй и первой степеней, следовательно, он должен иметь корни над $\mathbb{F}_3$. Но он их, очевидно, не имеет. Отсюда заключаем, что $P(x)$ неприводим.

2. Рассмострим $\mathbb{F}_3[\alpha]$, где $\alpha^3 = 2\alpha^2 + 1$. Необходимо найти порядок элемента α в данном поле, т.к. он будет определять порядок матрицы вида 2, задающей период последовательности сдвигового решистра.

Найдём $ord\alpha$:

- $|\mathbb{F}_3[\alpha]^*| = 26, \Rightarrow \{1, 2, 13, 26\}$ - возможные порядки элементов в $\mathbb{F}_3[\alpha]$
-

$$\alpha^2 \neq 1$$

$$\underline{\alpha^{13}} = (\alpha^3)^4\alpha = (2\alpha^2+1)^4\alpha = \alpha(2\alpha^2+1)(2\alpha^6+1) = \alpha(2\alpha^2+1)(2(2\alpha^2+1)^2+1) =$$
$$= (\alpha^2+2+\alpha)(2(\alpha^4+\alpha^2+1)+1) = 2(\alpha^2+\alpha+2)(2\alpha^3+\alpha+2) =$$
$$= 2(2\alpha^4+\alpha^3(1+2)+\alpha^2(2+1+1)+\alpha(2+2)+1) = \alpha^4+2\alpha^2+2\alpha+2 =$$
$$= 2\alpha^3+\alpha+2\alpha^2+2\alpha+2 = \alpha^2+2+2\alpha^2+2 = \underline{1}$$

$ord\alpha = 13, \Rightarrow$ искомый период равен 13.

Пояснение. *Во втором пункте решения есть вычислительная ошибка: на самом деле* $\alpha^3 = \alpha^2 + 2$. *Хотя это и не влияет на идею решения, рекомендуем провести вычисления, согласуясь с вскрывшейся ошибкой.*