Лекции по фундаментальной и компьютерной алгебре.

Печатала: Ткаченко Анастасия

7 июня 2018 г.

3 семестр.

18 сентября 2017г.

Краткий обзор основных алгебраических понятий.

Определение.

Бинарной алгебраической операцией на множестве A, называется отображение $f : A * A \to A$ (Из прямого произведения в себя).

Если $f : A^n \to A$, то операция называется n-арной и ей занимается полиномиальная алгебра.

Пример.

det матрицы размерности $n \times n$, можно рассматривать как n-ую операцию, если разбить матрицу на строки или столбцы. И можно рассматривать как n^2-арную, если рассмотреть матрицу поэлементно. При $n = 1$, т.е. когда $f : A \to A$, операция называется унарной. Взятие обратного элемента - унарная операция.

Определение.

Бинарная операция, когда двум элементам множества A, ставится в соответствие третий элемент этого множества. $f : (a, b) \mapsto C$

Вместо длинных слов: бинарная алгебраическая операция, обычно говорят: умножение или сложение.

Операция называется коммутативной, если: $\forall a, b \in A\ f(a, b) = f(b, a)$ $ab = ba$

Коммутативную операцию, обычно называют сложением, но не всегда.

Виды колец:

1. Если умножение ассоциативное, то кольцо называется ассоциативным.

Примеры.

Кольцо целых чисел, кольцо многочленов от любого числа переменных, кольцо матриц над ассоциативным кольцом.

2. Не ассоциативные кольца.

Примеры.

Трёхмерное пространство векторов, где сложение - это сложение векторов, а умножение - это векторное произведение, называется кольцом кольцом Ли, Ёрдановы кольца, Мардоновы.

Т.к. суперпозиция функций - ассоциативная, а большинство процессов в природе и науке - это отображение, то чаще всего встречается ассоциативные кольца.

3. Ассоциативное кольцо с коммутативным умножением, называется коммутативным кольцом.

Пример.

Кольцо матрицы размером > 1, всегда не коммутативное.

Определение.

Если в кольце ненулевые элементы по умножению, образуют некоммутативную группу, то такое кольцо называется телом.

Полю действительных чисел добавим мнимую единицу:

$$R; i, j, k$$

$$i^2 = j^2 = k^2 = -1$$

$$i - j = k$$

$$j \cdot k = i$$

$$j \cdot i = -k$$

25 сентября 2017г.

1. Абстрактное строение.

Рассмотрим идеал порождённый множеством $f(x)$, т.е. $I = u \cdot g(f(x))$ - это главный идеал состоящий из всех кратных многочленов $f(x)$

$I = ug(f(x)) = \{L(x)|l(x) = f(x) \cdot h(x),\, h(x) \in p[x]\}$

Рассмотрим фактор-кольцо $p[x]/ug(x)$ (По этому идеалу).

По теореме о построении поля разложения, у нас получится поле в котором многочлен $f(x)$, имеет хотя бы один корень, мы можем считать, что это наш α.

2. Символьное описание простого расширения.

У нас есть поле p и символ α, который является корнем многочлена, т.е. $f(\alpha) = 0$. Рассмотрим степени $\alpha, 1, \alpha, \alpha^2, \ldots, (\alpha)^(n-1)$. Т.к. многочлен $f(x)$, имеет n-ую степень, то возникает соотношение: $\alpha^n + a_(n-1)(\alpha)^(n-1) + \ldots + a_0 = 0$, отсюда α^n можно выразить через элементы меньшей степени, таким образом поля $P(\alpha) = \{b_0 + b_1\alpha + \ldots + b_(n-1)\alpha^(n-1)|b_i \in p\}$ или другими словами является векторным пространством размерности n над полем P. Базис $1, \alpha, \ldots, \alpha^(n-1)$.

$\alpha^n = -a_(n-1)\alpha^(n-1) - \ldots - a_0$ - это соотношение задаёт умножение в поле. Степени выше n, получаются при умножении на α этого равенства с последующим использованием этого же равенства.

Теорема 1.

Простое алгебраическое расширение $P(\alpha)$ - изоморфно $\approx P[x]/ug(f(x))$, где $f(x)$ - минимальный многочлен $f(x)$ и $P(\alpha) = a_(n-1)\alpha^(n-1) - \ldots a$.

Теорема 2.

$\forall$ p - простое число и $\forall n \in N$ $\exists$ поле $GF(p)$, содержащие p^n элементов.

Теорема 3 (О структуре подполей поля Галуа).

Пусть $GF(p^n)$ - некоторое поле Галуа, а $CF(p^n)$ - какое-нибудь другое поле, тогда $CF(p^n) \geq GF(p^n) \iff$, чтобы $m|n$, т.е. структура подполей определяется структурой делителей числа n.

9 октября 2017г.

Теорема (Описание неприводимых многочленов).

Пусть $f(x) \in GF(p)[x]$ - неприводимый многочлен, его степень $f(x) = m$.

Утверждение.

Многочлен $f(x) \iff$ делит множество $(x^(p^m) - x)$, когда $m|n$

Вывод из теоремы.

Все неприводимые многочлены степени m, если $m|n$, находятся как сомножители $b(x^(p^m) - x)$.

Доказательство.

1. Пусть $f(x)|(x^(p^m) - x)$, значит его поле разложения $GF(p^m)$ - сходится внутри поля разложения $GF(p^n)$, т.е. $GF(p^m) \triangle GF(p^n) \Rightarrow m|n$

Обратно: пусть $m|n$, тогда поле разложения $GF(p^m) < GF(p^n)$, значит все корни множества f, являются корнями большего многочлена, значит он делит его.

Пример.

Пусть $p = 3, n = 2$

Рассмотрим многочлен $(x^(3^2) - x)$ над $GF(3)$. Перечислим все неприводимые многочлены второй степени над полем $GF(3)$. Они имеют вид: $x^2 + \alpha x + \beta$, α и $\beta \in GF(3)$

Если многочлен второй степени - неприводим, значит у него нет корня.

Теорема о примитивном элементе.

Определение.

Порождающий элемент мультипликативной группы поля, называется примитивным.

Теорема.

В любом конечном поле $GF(p^n) \exists$ примитивный элемент, т.е. мультипликативная группа этого поля - циклична.

Доказательство.

$h = p^n - 1$ - порядок мультипликативной группы. $h = p^n - 1 = p^(\alpha_1)_1 - p^(\alpha_5)_5$ - разложение на простые множители. Для каждого i, рассмотрим многочлен $x^(h/p_i) - 1$. Т.к. этот многочлен, имеет степень $< h$, то не все ненулевые элементы, являются его корнями. Пусть a_i - не корень, т.е.

$$a^(h/p_i)_i \neq 1$$

$$b_i = a^(\frac{h}{p_i k_i})_i$$

. По теореме Лагранжа: каждый элемент в степени равной порядку группы, равен 1. $b^(p^(\alpha_i)_i)_i = 1$, но его порядок, может быть и меньше, однако если $b^(p^(\alpha_(i-1))_i)_i = a^(h/p_i)_i \neq 1 \Rightarrow$ порядок элементов $p_i = p^(\alpha_i)_i$

Элемент $b = b_1 b_2 \dots b_5$ и есть примитивный элемент. Т.к. порядки всех b - взаимно просты между собой, то их НОК равно: $h = p^n - 1 = p^(\alpha_1)_1 \dots p^(\alpha_5)_5$

Если по этой теореме искать примитивный элемент, то нужно перебрать все элементы в поле (ЖУТЬ).

Алгоритм нахождения примитивного элемента.

1. Порядок мультипликативной группы h, раскладывается на простые множители $h = p^n - 1 = p^(\alpha_1)_1 \dots p^(\alpha_5)_5$

Если находимся в простом поле $GF(p)$, то по порядку перебираем $g = 2, 3, 5, 7, 11, 13, 17$

$$g^(\frac{h}{p_i})$$

, $i = 1 \dots 5$

5 раз возвести в степень $\frac{h}{p_i}$. Тот элемент, для которого эти степени $\neq 1$ и будет примитивным.

Сколько примитивных элементов ?

Ответ: $\varphi(h-1)$

Задачи.

1.

$$p = 19$$

$$p - 1 = 18 = 2 \cdot 3^2$$

Нужно проверить $g^(3^2) = g^9; g^6$

$$2^2 = 4$$

$$2^4 = 4^2 = 16$$

$$2^8 = 2^3 \cdot 2 = 9 \cdot 2 = 18$$

$$2^6 = 2^4 \cdot 2^2 = 64 = 7 \neq 1$$

$$GF(2)$$

$$x^2 + x + 1$$

Т.к. все многочлены данной степени делят многочлен $x^p - x$, то какой бы из них мы не взяли, поля разложения будут одинаковыми.

$$x^3 + x + 1$$

$$GF(2^3) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

Добавим корень обозначенный через α.

$$\alpha, \alpha^2, \alpha^4$$

$$\alpha, \alpha^2, \alpha^2 + \alpha$$

Соотношения

$$\alpha^3 + \alpha + 1$$

$$\alpha^4 = \alpha^2 + \alpha$$

Т.к. в поле ненулевых элементов 7 и 7 - простое число $\Rightarrow$ примитивным элементом, будет любой не единичный

$$(\alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1)$$

30 октября 2017г.

Нахождение примитивных элементов. Логарифм Якоби. Решения уравнения в конечных полях.

Теорема.

Если поле P, содержит u элементов, то количество разложений примитивных элементов $\varphi(q-1)$

Функция Эйлера - мультипликативна, т.е. если $n = m \cdot k$ $(m, k) = 1$ (взаимно простые), то $\varphi(n) = \varphi(m)\varphi(k)$, поэтому $n = p(\alpha_1)_1 \ldots p(\alpha_5)_5$, то $\varphi(n) = \varphi(p(\alpha_1)_1 \ldots \varphi(p(\alpha_5)_5$

Несложно заметить, что каждое p-ое число делится на p, значит: $\varphi(p^\alpha) = p^\alpha - p(\alpha - 1)$

$$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8$$

Таким образом: в $GF(17)$, примитивным является каждый второй ненулевой элемент.

Возьмём поле $GF(2)$, его расширение $x^3 + x + 1$ - неприводимо, т.к. нет корней. Пусть $\alpha^3 = \alpha + 1$, α - его корень.

$$GF(2^3) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

, в этом поле, примитивными будут все кроме 0 и 1.

$$GF(3)$$

$$x^2 + 1$$

$$\alpha^2 = 2$$

$$GF(3^2) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

, тогда мультипликативная форма: $|GF^*(3^2)| = 8$

$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$$

- приводимых.

Для нахождения приводимого $a^n \neq 1$

$$\alpha, \alpha^2 = 2$$

,

$$\alpha^4 = \alpha^2 = 1$$

Как строится поле расширения ?

Берём неприводимый многочлен (не раскладывая на множители) и добавляем формальный корень (например α)

$$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$$

$$(\alpha+1)^4 = (2\alpha)^2 = 1 \cdot \alpha^2 = 2 \neq 1$$

В алгоритме AES:

$$GF(2^2)$$

$$x^8 + x^4 + x^2 + x + 1$$

Логарифм Якоби.

Пусть P - поле, a - примитивный элемент, тогда любой ненулевой элемент этого поля, может быть представлен в виде: $b = a^i$, $0 < i < |p|$.

Операцию умножения всегда стремятся заменить сложением и примитивный элемент - идеальное средство. $= a^j \ bc = a^(i+j)$

При использовании примитивного элемента, умножение сводится к сложению показателей.

Определение.

Если a - примитивный элемент: $b = a^i$, то $\log_a b = i$

Возникает проблема со сложением $b + c = a^i + a^j = a^i(1 + a^(j-i)$

Проблема: чему равняется $1 + a^k = a^L(k)$

$L(k)$ - Логарифм Якоби.

31 октября 2017г.

$$GF(7)$$

$$a = 3$$

$$GF(3^2)$$

$$\alpha^2 = 2$$

$$a = \alpha + 1$$

Вторая строка - это показатель степени 3 в случае, когда степень равна соответствующему элементу поля GF(17).

Таблица Якоби

3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
$L(i)$	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8	#

$$3^1 = 3, 3^2 = 9, 3^3 = 9 \cdot 3 = 27 \ldots 10$$

$$3^4 = 10 \cdot 3 = 30 = 13$$

(по |17|)

$$3^5 = 13 \cdot 3 = 39 = 5$$

$$3^6 = 5 \cdot 3 = 15$$

$$3^7 = 15 \cdot 3 = 45 = 11$$

$$3^8 = 11 \cdot 3 = 33 = 16 = -1$$

$$3^9 = -1 \cdot 3 = -3 = 14$$

$$3^{10} = -3 \cdot 3 = -9 = 8$$

$$3^{11} = 8 \cdot 3 = 7$$

$$3^{12} = 7 \cdot 3 = 21^{-17} = 4$$

$$3^{13} = 4 \cdot 3 = 12$$

$$3^{14} = 12 \cdot 3 = 36 = 2$$

$$3^{15} = 2 \cdot 3 = 6$$

$3^1 + 1 = 4 = 3^12$
$L(1) = 12$
$3^2 + 1 = 2^8 + 1 = 16 + 1 = 0$
$L(8) = \#$ - не существует.

Применение логарифма Якоби.

1. Примитивный элемент умноженный по модулю P, сводит к сложению по модулю p-1. Алгоритм Якоби мат. сложения, заменяет сложением показателей.

$GF(17)$ $x^2 + 2x + 11$ $x = \frac{-2+\sqrt{2^2-4\cdot 11}}{2}$

1. Все элементы заменяем на степени через примитивные:
$-2 = 15 = 3^6$
$2 = 3^14$, $2^{-1} = 3^2$
$4 = 2^{12}$
$-4 - 13 = 3^{14}$, $11 = 3^7$
$(3^6 + \sqrt{2^{12} + 3^4 \cdot 3^7}) \cdot 3^2 = 3^8 + 3^2\sqrt{3^7}$
$3^{12} + 3^{11} = 3^{11}(3^1 + 1) = 3^{11} \cdot 3^{12} = 3^{23}(-16) = 3^7$
Если $\sqrt{3^7}$ - корень извлекается, то такой $a \leq x < 16$, что
$(3^x)^2 = 3^{17}$
$2x = 7(16)$
$GF(3^2)$
$\alpha^2 = 2$

$a = \alpha + 1$	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
i	8	4	6	1	7	2	3	5
$L(i)$	4	#	1	7	6	3	5	2

$(\alpha+1)^1 = \alpha + 1$
$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$
$(\alpha+1)^3 = 2\alpha \cdot (\alpha+1) = 2\alpha^2 + 2\alpha = 1 + 2\alpha$

$(\alpha+1)^4 = (2\alpha+1)(\alpha+1) = 2\alpha^2+\alpha+2\alpha+1 = 4+1 = 2$
$(\alpha+1)^5 = 2(\alpha+1) = 2\alpha+2^2$
$(\alpha+1)^6 = (2\alpha+2)(\alpha+1) = 2\alpha^2+2\alpha+2\alpha+2 = \alpha$
$(\alpha+1)^7 = \alpha(\alpha+1)\alpha^2+\alpha = \alpha+2$
Считаем L(1):
$(\alpha+1)^1+1 = \alpha = (\alpha+1)^6$
$LogTo("Test.gap");$
$M := [1,1,01,0,0];$
$Length(M);$
$Ni := Set(M);$
Матрица задаётся построчно и разделяется между собой запятыми.
$n := [[1,2,2017]];$
$[0,1,2^A0],[0,1,17];$
$B := A^n(-1);$

6 ноября 2017г.

Алгебраически числа.

x^3+x+1 Рассмотрим над полем $GF(2)$ (Самое маленькое).
Добавим $\alpha^3 = \alpha+1$
$GF(2^3) = \{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$
Многочлен после добавления, разложится на: $(x-\alpha)(x-\alpha^2)(x-\alpha^4)$ $\alpha^4 = \alpha^2+\alpha$

Предположим, что этот многочлен над полем $Q : y = x^3+x+1$ $\alpha = -0,0162$

У этого многочлена есть единственный корень $\approx -0,0162$

Построим поле разложения для этого многочлена: $\frac{x^3+x+1}{x-\alpha} = x^2+\alpha x+(a+\alpha^2)$

$x^3+x+1 = (x^2+\alpha x+a+\alpha^2)$
$\beta = \frac{-\alpha\pm\sqrt{\alpha^2-4-4\alpha^2}}{2} = -\frac{\alpha}{2}\pm\frac{\sqrt{-4-3\alpha^2}}{2} =$
$Q(\alpha) = \{a_2, a^2+a, \alpha+a_4, \ldots \in Q\}$

Поэтому добавляя один корень неприводимого многочлена 3 степени, 2 группа у нас автоматически не появится. $= -\frac{\alpha}{2}\pm i\sqrt{3\alpha^2+4}$

$|Q(\alpha,\beta) : Q| = 6$

Норма и след элементов в конечном поле.

Пусть α - корень некоторого неприводимого многочлена характеристики р, тогда $\alpha, \alpha^p, \alpha^{p^2}, \ldots \alpha^{p^{n-1}}$ - остаточные корни.

Нормой: α $N(\alpha) = \alpha\alpha^p\ldots\alpha^{p^{n-1}} \in \Gamma$

След: $Tr(\alpha) = \alpha+\alpha^p+\ldots+\alpha^{p^{n-1}} \in \Gamma$

Несложно проверить, что и след, и норма принадлежат исходному полю расширения которых $f(x) \in P[x]$

$N(\alpha,\beta) = N(\alpha)N(\beta)$
$Tr(\alpha+\beta) = Tr(\alpha)+Tr(\beta)$
$P(\alpha)$

$1, \alpha, \ldots \alpha^{n-1}$ - базис этого поля над полем Р. Тогда при помощи элемента α, мы можем задать линейное отображение $\alpha : p(\alpha) \to p(\alpha)$

$\alpha : x \mapsto \alpha x$

6 ноября 2017г.

Пусть P - Некоторое поле. $S_0, S_1, \dots$ - некоторая последовательность. Последовательность называется рекуррентной k, если $S_{n+k} = a_{k-1} \cdot S_{n+k-1} + \dots$

Т.к. первые k элементов, не связаны никакими ограничениями, то вектор $\overline{S_0} = (S_0, S_1, \dots S_{k-1}$, называют вектором инициализации. Разных векторов инициализации может быть q^k.

Матричная запись регистра сдвига.

A=МАТРИЦА

$\overline{S_n} = S_0 A^n$

Если матричная степень степень станет единичной, то последовательность станет $= 0$ (будет повторяться).

Теорема.

Если D не делит b, то уравнение не имеет решения, если делит< то решений будет d штук.

Доказательство.

1 Случай.

Если d не делит b, то вычитая из ax любое кратное число n, всегда будет получаться число делящееся на d. Значит b никогда не получится.

2 Случай.

$a = da_0$

$b = db_0$

$n = dn_0$

$a_0 x = b_0(n_0) \Rightarrow$ т.к. НОД $(a_0, n_0) = 1$, то по следствию из алгоритма Евклида, у a_0, есть обратный по умножению.

$x_0 = a_0^{-1} b_0(n_0)$

Непосредственно проверяется, что все суммы вида $x = x_0 + in_0$ $0 \leq i < d$, является корнем $ax = b(n)$

Система из k уравнений по различным модулям:

$a_1 x = b_1(n_1)$

$a_2 x = b_2(n_2)$

$\dots$

$a_n x = b_n(n_n)$ - ЭТО СИСТЕМА

27 ноября 2017г.

Пример.

$\underline{S_{n+1}} = S_{n+3} + S_{n+2} + S_{n+1} + S_n$ $GF(2)$

$\overline{S_0} = (1, 0, 0, 0)$

$x^4 + x^3 + x^2 + x + 1 \neq (x^2 + ax + 1)(x^2 + bx + 1)$

В нашем случае многочлен - неприводим, т.е. у него нет множителей второго порядка. Поэтому по теореме о корнях неприводимого многочлена, его корнями будут: $\alpha, \alpha^2, \alpha^4, \alpha^8$

$\alpha^4 = \alpha^3 + \alpha^2 \neq \alpha + 1$

$\alpha^8 = \alpha^3$ $\alpha^5 = 1$

Т.к. мультипликативная группа поля, значит α, не является примитивным элементом. Что делать, если многочлен разложения в произведение двух неприводимых многочленов, как найти корни ?

Пример.

$|GF(2^4)^*| = 15$

$GF(3)$

$x^2 + 1$ - неприводимый

$x^2 + x + 2$ - неприводимый (т.к. нет корней из GF(3))

Допустим если характеристический многочлен $f(x) = (x^2+1)(x^2+x+2)$

По теореме о корнях неприводимых многочленов поля Галуа ... все остальные многочлены многочлены данной степени. Из соображений удобства вычислений полю GF(3), мы добавляем корень α первого многочлена, который будет удовлетворять: $\alpha^2 = 2$. По теореме о корнях неприводимого многочлена, корнями будут α и α^3

$GF(3^2) = \{0, 1, 2, \alpha, 2\alpha, \alpha + 1, 2\alpha + 1, 2\alpha + 2; \alpha + 2\}$

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

Теперь среди 9 элементов поля $GF(3^2)$, нужно найти корни второго многочлена.

1 Способ.

Просто перебрать все 6 элементов не принадлежащих $GF(3^2)$, подствить их в многочлен и проверить кто корень.

2 Способ.

Найти корни по формуле квадратного уравнения:

$\frac{-1+\sqrt{1^2-4^2}}{2} = (2 + \sqrt{2}) = 1 + 2\sqrt{2}$

$\sqrt{2}$ - принадлежит полю $GF(3^2)$

$\sqrt{2}$ - это такой элемент a, что $a^2 = 2$, значит $\sqrt{2}$ - это α

$x_{1,2} = 1 \pm 2\alpha$

$x + x + 2 = (x - 1 - \alpha)(x - 1 - +\alpha)$

$x_1 = 1 + 2\alpha$

$x_1 = 1 - 2\alpha$

$GF(2^4)$

$\alpha, \alpha^2, \alpha^3, \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$; $\alpha^5 = 1$

$15 = 5 \cdot 3$ $g^3 \neq 1, g^5 \neq 1$

$\varphi(15) = \varphi(3)\varphi(5) = \varphi \cdot 4 = 8$

Примитивных элементов: 8 штук.

$g = \alpha + 1$ $g^2 = (\alpha + 1)^2 = \alpha^2 + 1$

$g^3 = (\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1 \neq 1$

$g^4 = (\alpha + 1)^2\alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1 + 1 = \alpha^3 + \alpha^2 + \alpha + 1$

$g^5 = (\alpha^3 + \alpha^2 + \alpha)(\alpha + 1) = \alpha^4 + \alpha = \alpha^2 + \alpha + 1\alpha = \alpha^3 + \alpha^2 + 1 + 1$

Теперь нужно составить таблицу его степеней, чтобы записать все элементы поля $GF(2^4)$

3	1	2	3	4	5	6	7	8	9	1
$(\alpha+1)^i$	$\alpha+1$	α^2+1	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+1$	α^3	$\alpha^2+\alpha+\alpha$	α^3+1	α^2	α^3 -

Будем использовать упрощение, что самый длинный элемент равен α^4, причём $\alpha^5 = 1$

Для нахождения n-ого члена рекурентной последовательности, нам необходимо решить систему из 4 неизвестных, в которой столбец свободных членов - вектор инициализации, в нашем случае импульсная функция.

$\alpha, \alpha^2, \alpha^4, \alpha^8$

$\alpha_1 = \alpha$ $\alpha_2 = \alpha^2$ $\alpha_2 = \alpha^3$ $\alpha_1 = \alpha^4$

$\beta_1 + \beta_2 + \beta_3 + \beta_4 = 1$

$\beta_1\alpha_1 + \beta_2\alpha_2 + \beta_3\alpha_3 + \beta_4\alpha_4 = 0$

$\beta_1\alpha_1^2 + \beta_2\alpha_2^2 + \beta_3\alpha_3^2 + \beta_4\alpha_4^2 = 0$

$\alpha^4 + \alpha^3 = \alpha^2 + \alpha + 1$ Во второй строчке