КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ
И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра системного анализа и информационных технологий

Ш.. ИШМУХАМЕТОВ, Р.Г. РУБЦОВА

ВЫЧИСЛЕНИЯ В КОНЕЧНЫХ ПОЛЯХ

Учебно-методическое пособие

Казань - 2019

УДК 512.624
ББК 22.144

Принято на заседании кафедры системного анализа и информационных технологий
Протокол № 7 от 6 марта 2019 года

Принято на заседании учебно-методической комиссии Института Вычислительной математики и информационных технологий
Протокол № 7 от 14 марта 2019 года

Рецензенты:
доктор технических наук, профессор,
заведующий кафедрой САИТ **Р.Х. Латыпов;**
кандидат физико-математических наук,
доцент кафедры теоретической кибернетики **В.С. Кугураков**

Ишмухаметов Ш.Т., Рубцова Р.Г.
Вычисления в конечных полях: Учебно-методическое пособие/
Ш.Т. Ишмухаметов, Р.Г. Рубцова.– Казань: Казанский ун-т, 2019.– 23 с.

В учебном пособии изучаются базовые понятия, связанные с конечными полями, вводятся основные определения из теории полей, выполняется разбор учебных примеров, изучаются приложения к криптографии и теории чисел. Рассматриваются расширения конечных полей, операции с многочленами над конечными полями, алгоритмы поиска неприводимых и примитивных многочленов над конечными полями.

Пособие предназначено для подготовки по курсу "Математические основы информационной безопасности".

Содержание

1. Группы

Алгебраической структурой называется пара, состоящая их непустого множества M и набора, заданных на элементах множества M операциях. Одной из наиболее известных алгебраических структур является группа.

Определение. Группой называется пара $< G, * >$, где G – непустое множество, а $*$ – бинарная операция, удовлетворяющая следующим трем аксиомам:

1. Ассоциативность:
   $(\forall a,\, b,\, c \in G) \quad a * (b * c) = (a * b) * c,$
2. Существование единичного (нейтрального) элемента:
   $(\exists \mathbf{e} \in G)(\forall a \in G) \quad a * \mathbf{e} = \mathbf{e} * a = a,$
3. Существование обратного элемента:
   $(\forall a \in G)(\exists b \in G) \quad a * b = b * a = \mathbf{1}.$

Наиболее часто операция $*$ является операцией сложения или умножения чисел. В этом случае обратный по сложению к a элемент обозначается через $(-a)$, а по умножению a^{-1}.

Если в группе $< G, + >$ выполняется свойство коммутативности $a+b = b+a$, то группа называется *коммутативной* или *абелевой*. Очевидно, что группа по сложению кольца $\mathbf{Z}_n$ является абелевой группой.

Примерами групп являются:

(1) Множество целых чисел Z с операций сложения и нейтральным элементом $\mathbf{0}$.

(2) Множество всех действительных или комплексных чисел без нулевого элемента относительно операции умножения.

(3) Множество невырожденных квадратных матриц размерности $n\ x\ n$ относительно умножения и единичной матрицей в качестве нейтрального элемента.

(4)Множество $F_p = \{1, 2, \ldots, p-1\}$, где p – простое число относительно умножения по модулю числа p и нейтральным элементом $\mathbf{1}$.

Поле является алгебраической структурой с двумя бинарными операциями – операцией сложения и операцией умножения. Поскольку, для элементов поля по каждой из этих операций существует обратный элемент, то в поле определены 4 арифметических операции – сложение, вычитание, умножение и деление.

Конечные поля исследовал знаменитый французский математик Эварист Галуа (1811–1832), поэтому в его честь конечные поля называются полями

Галуа и обозначаются $GF(q)$(от Galois Fields), где q-размерность конечного поля.

2. Простейшие конечные поля

Простейшее поле состоит ровно из p элементов, где p-произвольное простое число, включая $p = 2$:

$$GF(p) = \{0, 1, 2, \ldots, p-1\}.$$

Число p называется характеристикой поля. На элементах множества $GF(p)$ можно выполнять арифметических действия, беря от результата остаток по модулю p. Деление элементов поля выполняется с помощью формулы

$$\frac{a}{b} = a \cdot b^{-1},$$

где обратный к b определяется как такой элемент $c \in GF(p)$, что выполняется $b \cdot c \equiv 1 \bmod p$. Например, в поле $GF(7)$ обратный к $b = 5$ будет $c = 3$, т.к. $5 \cdot 3 = 15 \equiv 1 \bmod 5$.

Очевидно, что три действия (сложение, вычитание, умножение) над элементами поля определены корректно. Надо показать, что и деление определено верно. Деление в поле выполняется с помощью обратного элемента

$$\frac{a}{b} = a * b^{-1} \bmod p,$$

поэтому достаточно доказать, что для каждого ненулевого элемента $a < p$ найдется элемент $b = a^{-1} \bmod p$.

Пример. Пусть $p = 11$. Выполним действия с элементами $a = 4$ и $b = 7$:

$$a+b = 5+7 \bmod 11 = 1, \quad a-b = 5-7 \bmod 11 = 9, \quad a*b = 5*7 \bmod 11 = 3,$$

$$a/b = 5/7 \bmod 11 = 5 * 7^{-1} \bmod 11 = 5 * 8 \bmod 11 = 7.$$

Обратный элемент $7^{-1} \bmod 11$ был найден подбором из условия $7 \cdot x \bmod 11 = 1$. Для больших значений обратный элемент ищется с помощью расширенного алгоритма Евклида.

3. Расширенный алгоритм Евклида

Пусть даны числа A и B. Надо найти обратный к B элемент по модулю A. Напомним, что для существования такого элемента числа A и B должны быть взаимно-простыми. В случае конечных полей модуль $A = p$ – простое число, поэтому для $1 \leq a < p$ это условие выполняется автоматически. Покажем, как вычислить $15^{-1} \bmod 26$:

№	A	B	$A \bmod B$	[A/B]	x	y
1	26	15	11	1	-4	7
2	15	11	4	1	3	-4
3	11	4	3	2	-1	3
4	4	3	1	1	1	-1
5	3	1	0	-	0	1

Напомним, что сначала заполняются первые 4 столбца последовательно сверху вниз, перенося значения в столбцах B и $A \bmod B$ вниз и влево пока не дойдем до строки с 0 в столбце $A \bmod B$. Это – прямой ход алгоритма Евклида.

После выполнения прямого хода алгоритма Евклида значение в нижней позиции столбца B окажется равным НОД исходных чисел A и B. Если оно отлично от 1, то обратного значения $B^{-1} \bmod A$ не существует.

На следующем этапе начинаем заполнять столбцы x, y, двигаясь снизу вверх. В нижней строке всегда помещаем значения 0 и 1. Заполним строку с номером $i+1$, заполняем значения строки i по формулам:

$$\begin{cases} x_i = y_{i+1} \\ y_i = x_{i+1} - y_{i+1} \cdot [A/B]_i \end{cases}$$

Значение $y = 7$, находящееся в верхней строке, является искомым обратным элементом: $15^{-1} \bmod 26 = 7$. Проверим вычисление $15 \cdot 7 \bmod 26 = 105 \bmod 26 = 1$. Числа 15 и 7 – взаимно-обратные по модулю 26, значит, вычисление верно.

Теперь можно завершить выполнение упражнение:

$$\frac{22}{15} = 22 \cdot 15^{-1} \bmod 26 = 22 \cdot 7 \bmod 26 = 154 \bmod 26 = 24.$$

Замечание. При вычислении обратного элемента с помощью алгоритма Евклида значение y в первой строке может оказаться отрицательный, тогда к значению y надо прибавить значение модуля A.

4. Поля

Полем называется алгебраическая структура $< F, +, * >$, состоящая из непустого множества и двух бинарных операция. Поле является группой по сложению и группой по умножению (обратный элемент по умножению рассматривается для ненулевых элементов), связанных аксиомами дистрибутивности ($\forall a,\ b,\ c \in F$):

$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Более подробные сведения о конечных полях может найти в монографии Лидла и Нидеррайтера «Конечные поля» [2].

Теорема 4.1. *Кольцо вычетов* $\mathbf{Z}_p = \{1, 2, \ldots, p-1\}$, *где* p – *простое число, является полем.*

Доказательство. Необходимо доказать, что для каждого ненулевого элемента a найдется обратный к нему по умножению элемент b, $a * b \bmod p = 1$. Умножим все элементы $\mathbf{Z}_p^*$ на элемент a (умножение выполняется по модулю p). Получим:

$$a\mathbf{Z}_p^* = \{a,\ 2a,\ \ldots, (p-1)a\}.$$

Покажем, что все элементы этого списка – различные, т.е. $ia = ja$ влечет $i = j$. Предположим противное, тогда $ia - ja = (i-j)a = 0$, т.е. $(i-j) * a \bmod p = 0$, откуда, $(i-j) \bmod p = 0$, что противоречит выбору i и j.

Значит, последовательность $a \cdot \mathbf{Z}_p^*$ – это просто перестановка множества $\mathbf{Z}_p^*$ и должна содержать 1. Отсюда, для некоторого i $i * a = 1$, т.е. $i = a^{-1}$, и теорема доказана.

Пусть $< G, * >$–произвольная группа по умножению.

Определение 4.1. *Порядком элемента* a *группы* G *(обозначается* $ord_G(a)$*) называется* наименьшее *число* k *такое, что* $a^k = 1$. *Порядком группы называется число ее элементов.*

Пример. Рассмотрим кольцо $\mathbf{Z}_{11}$. Число $n = 11$ является простым, поэтому кольцо $\mathbf{Z}_{11}$ является полем. Каждый элемент $\mathbf{Z}_{11}$ имеет порядок по сложению и порядок по умножению. Порядок по сложению любого элемента, кроме 0, равен 11. Порядок по умножение равен наименьшему t такому, что $a * a * \ldots * a = a^t \bmod 11 = 1$. Например, порядок $a = 10$ равен 2, т.к. $10^2 \bmod 11 = 100 \bmod 11 = 1$.

Следующее свойство, связывающее порядки элементов с порядком группы, широко используется в различных алгоритмах, описанных ниже. Эта теорема была доказана знаменитым французским математиком Жозефом Луи Лагранжем (1736–1813).

Теорема 4.2. (Лагранж). *Порядок любого элемента конечной группы является делителем порядка группы.*

Доказательство. Пусть элемент a конечной группы $< G, \cdot >$ имеет порядок $k > 1$. Тогда элементы a, a^2, ... , a^{k-1}, $a^k = 1$ различны и сами образуют группу A, содержащую k элементов и являющуюся подгруппой G. Различные смежные классы $b \cdot A$ для $b \in G$ имеют также мощность k, а

объединение их дает в совокупности группу G. Значит, число элементов G равно $k \cdot m$, где m–число смежных классов, откуда вытекает утверждение теоремы.

Пример. Рассмотрим кольцо $\mathbf{Z}_p$ при $p = 29$. Ненулевые элементы этого кольца образуют группу по умножению, порядок которой равен $p - 1 = 28$. По теореме Лагранжа порядок любого элемента a этой группы является делителем 28, т.е. может принимать одно из следующих значений: 1, 2, 4, 7, 14 и 28.

5. Примитивные элементы поля

Порядком (по умножению) ненулевого элемента a поля F_p называется наименьшая степень t такая, что выполняется условие

$$a^t \mod p = 1.$$

Элемент $a \in G$ называется *примитивным* элементом или *генератором* группы, если его порядок $ord_G(a)$ равен порядку группы. Не любая группа имеет генератор. Группа, в которой есть генератор, порождается одним элементом и называется *циклической.*

Теорема 5.1. *Группа по умножению поля F_p является циклической.*

Эта теорема доказывается в пособии "Введение в теорию чисел". Там приводится более сильная теорема о том, что в конечном поле существует ровно $\varphi(d)$ элементов порядка d для каждого делителя d числа $p - 1$ (это порядок поля F_p без нулевого элемента). В частности, примитивные элементы имеют порядок $p - 1$, значит, в конечном поле существует ровно $\varphi(p-1)$ примитивных элементов. Рассмотрим в качестве примера поле F_7.

Упражнение. Найти порядки всех ненулевых элементов поля F_7.

Решение. В поле F_7 имеется 6 ненулевых элементов По теореме Лагранжа порядком элемента могут быть только делители 6, т.е. числа $Del(6) = \{1, 2, 3, 6\}$. Порядок 1 имеет только $a = 1$, а порядок 2 имеет наибольший элемент поля $a = 6$. Все остальные элементы имеют порядок 3 или 6. Будем вычислять значение $a^3 \mod 7$ для всех a от 2 до 5. Если $a^3 \mod 7 = 1$, то порядок a равен 3, иначе, 6:

a	2	3	4	5
$ord(a)$	3	6	3	6

Элементами максимального порядка являются $a = 3$ и $a = 5$. Они и являются примитивными элементами поля F_7.

6. Теорема о примитивном элементе конечного поля

В этом разделе мы вернемся к вопросу о существовании примитивных элементов (генераторах) конечного поля Напомним, что элемент $g \in F$ называется примитивным для поля F, если все ненулевые элементы F являются степенями этого элемента. Докажем теорему о том, что каждое конечное поле содержит хотя-бы один примитивный элемент

Теорема 9.1. Пусть F_p– конечное поле. Поле F_p для каждого делителя $d|(p-1)$ содержит ровно $\varphi(d)$ элементов порядка d. В частности, F_p содержит $\varphi(p-1)$ элементов порядка $p-1$ (все такие элементы являются генераторами поля F_p).

Доказательство. Пусть d – произвольный делитель $p-1$, и пусть a – элемент порядка d. Рассмотрим степени этого элемента

$$a, a^2, \ldots, a^{\varphi(d)} = 1.$$

(последняя степень равна 1 согласно теореме Эйлера).

Если степень t не имеет общих делителей с d, то элемент $b = a^t$ имеет также порядок d. Поэтому, в полк F либо нет ни одного элемента порядка d, любо ровно $\varphi(d)$ таких элементов.

Предположим, что найдется такое $d|(p-1)$, что в F_p нет элемента порядка d. Каждый ненулевой элемент F_p имеет порядок, являющийся делителем $p-1$. Общее количество ненулевых элементов равно $p-1$. По теореме Эйлера о делителях натурального числа n

$$p - 1 = \sum_{d|(p-1)} \varphi(d)$$

С другой стороны, количество ненулевых элементов поля равно сумме $\varphi(d)$, где сумма берется по тем делителям d, для которых найдется элемент порядка d. В силу нашего предположения, такая сумма строго меньше суммы $\varphi(d)$, вычисленной по всем делителям $p-1$. Но тогда число ненулевых элементов поля строго меньше $p-1$, что невозможно. Значит, предположение не верно, и теорема доказана.

7. Расширения конечных полей

Определение. Пусть F–поле. Многочлен $P_n(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, где все $a_i \in F$, называется неприводимым над полем F, если его нельзя представить в виде произведения многочленов меньшей степени с коэффициентами из поля F.

Пример. 1. Многочлен $P_2(x) = x^2 - 2$ является неприводимым над полем F_5, так как в F_5 уравнение $P_2(x) = x^2 - 2 = 0$ не имеет решения, так как нет

элементов, квадрат которых равен 2. Многочлен $P_2(x) = x^2 + 4$ является приводимым в этом поле $x^2 + 4 = (x + 1)(x + 4)$.

2. Многочлен $P_2(x) = x^2 - 5$ – неприводим в поле $\mathbf{Q}$ рациональных чисел, однако приводим в более широком поле действительных чисел $\mathbf{R}$.

Определение. Пусть F–поле. Элемент a называется *алгебраическим элементом степени* n над полем F, если он удовлетворяет уравнению $P_n(a) = 0$, где $P_n(x)$ – неприводимый многочлен над полем F.

Примеры. 1. Все элементы самого поля F являются алгебраическими элементом степени 1 над полем F, так как каждый элемент $a \in F$ удовлетворяет уравнению 1-й степени $x - a = 0$.

2. Уравнение $x^2 - 2 = 0$ в поле F_5 является неприводимым, так как ни один элемент $a \in F$, будучи возведенным в квадрат, не равен 2. Поэтому корень этого уравнения $\sqrt{2}$ является алгебраическим элементом степени 2 над полем F.

3. Мнимая единица $i = \sqrt{-1}$ является алгебраическими элементом степени 2 над полем действительных чисел $\mathbf{R}$.

Определение. Группа $< G, * >$ называется циклической, если найдется элемент a, называемый примитивным элементом или генератором группы, такой, что любой другой элемент b группы G равен некоторой степени элемента a: $b = a^k$.

Множество всех корней неприводимого многочлена образует циклическую группу, то есть найдется примитивный корень θ, такой что все другие корни являются степенями этого элемента. В качестве примера можно привести группу комплексных корней n-й степени из 1. Например, для $n = 4$ найдется один примитивный корень $\theta = \cos(\pi/4) + i \cdot \sin(\pi/4)$.

Пусть F – какое-нибудь поле, а элемент x является примитивным корнем неприводимого многочлена $P_k(x)$, степени $k > 1$ с коэффициентами из F. Добавим элемент x к полю F и построим наименьшее поле F', расширяющее $F \cup \{a\}$.

Теорема 7.1. *Наименьшее поле F', расширяющее $F \cup \{a\}$, состоит из всевозможных многочленов $P_i(x)$ степени меньшей k с коэффициентами из поля F.*

Доказательство. Действительно, вместе с элементов x добавляются их произведения и степени $x^2, x^3, \ldots$. Также добавляются произведения этих степеней на элементы исходного поля ax^i. Поскольку, x удовлетворяет уравнению $P_k(x) = x^k + a_1x^{k-1} + \ldots + a_k = 0$, то $x^k = -a_1x^{k-1} - \ldots - a_k$, то есть x^k можно выразить через многочлен меньшей степени. Такое

представление возможно для всех старших степеней $x^n,\ n \geq k$ и их произведений на элементы базового поля. После такой подстановки останутся только слагаемые степеней строго меньших k. Теорема доказана.

Пример 1. Рассмотрим конечное поле F_5 и добавим к нему элемент x, являющийся примитивным корнем уравнения $x^2 = 2$. Достроим множество $F_5 \cup \{x\}$ до поля. Получим множество многочленов вида $ax+b$, где $a, \in F_5$. Операции сложения, вычитания, умножения таких многочленов выполняются с помощью обычных правил арифметических действий с многочленами с приведением результата сначала по модулю 5, потом по модулю $x^2 - 2$. Пусть $A = 3x + 4, B = 2x + 3$:

$$
\begin{aligned}
&A \ + \ B = (3x + 4) + (2x + 3) \bmod 5 = 5x + 7 \bmod 5 = 2,\\
&A \ - \ B = x + 1.\\
&A \ \cdot \ B = (3x + 4)(2x + 3) = (6x^2 + 17x + 12) \bmod 5 =\\
&= x^2 + 2x + 2 = 2x + 4.
\end{aligned}
$$

(в выражении $x^2 + 2x + 2$ просто заменили x^2 на 2, так как $x^2 - 2 = 0$ и привели подобные члены по модулю 5).

Вычисление отношения многочленов немного сложнее и состоит в нахождении обратного многочлена по модулю заданного неприводимого многочлена с применением расширенного алгоритма Евклида. Для $k = 2$ этот алгоритм немного проще и состоит в домножении дроби на многочлен, сопряженный к знаменателю:

$$\frac{3x+4}{2x+3} = \frac{(3x+4)(2x-3)}{(2x+3)(2x-3)} = \frac{6x^2-x-12}{4x^2-9} = \frac{x^2+4x+3}{4x^2-4} = \frac{4x}{4} = x.$$

(опять в вычислении заменяем x^2 на 2).

Пример 2. Дано кубическое поле, полученное добавлением к полю F_7 корня x неприводимого многочлена x^3+x+1. По теореме это полу состоит из многочленов 2-й степени с коэффициентами из F_7. Найти отношение элементов этого поля $P_1 = 2x^2 + x + 3$ и $P_2 = 3x^2 + 2x + 1$.

Решение. Сначала необходимо найти $P_2^{-1} \bmod x^3 + x + 1$. Используем для этого расширенный алгоритм Евклида. Первый шаг состоит в делении

с остатком $x^3 + x + 1$ на P_2:

$$\begin{array}{rl} x^3 \quad + x + 1 & \mid 3x^2 + 2x + 1 \\ - & \hline 15x^3 + 10x^2 + 5x & \mid 5x - 1 \\ \hline -10x^2 - 4x + 1 & \\ - & \\ -3x^2 - 2x - 1 & \\ \hline -2x + 2 & \end{array}$$

В следующем действии поделим $3x^2 + 2x + 1$ на остаток $-2x + 2$:

$$\begin{array}{rl} x^2 + 2x + 1 & \mid -2x + 2 \\ - & \hline -4x^2 + 4x & \mid 2x + 1 \\ \hline -2x + 1 & \\ - & \\ -2x + 2 & \\ \hline -1 & \end{array}$$

Занесем полученные данные в таблицу расширенного алгоритма Евклида. Заполним столбцы u, v, помещая в нижнюю строку значения 0 и $(-1)^{-1} \bmod 7 = -1$ и поднимаясь вверх по тем же формулам, как в обычном алгоритме:

A	B	$A \bmod B$	$A \; div \; B$	u	v
$x^3 + x + 1$	$3x^2 + 2x + 1$	$-2x + 2$	$5x - 1$	$2x + 1$	$-1 - (5x - 1)(2x + 1)$
$3x^2 + 2x + 1$	$-2x + 2$	-1	$2x + 1$	-1	$2x + 1$
$-2x + 2$	-1	0	$-$	0	-1

Обратный элемент находится в правом верхнем углу. Преобразуем его:

$$P_2^{-1} = -1 - (5x - 1)(2x + 1) = -1 - (10x^2 + 3x - 1) = 4x^2 + 4x$$

Проверим вычисление, перемножив P_2 и P_2^{-1}:

$$(3x^2 + 2x + 1)(4x^2 + 4x) = 12x^4 + 20x^3 + 12x^2 + 4x =$$
$$= 12x(-x - 1) - (-x - 1) + 12x^2 + 4x = 1.$$

Произведение равно 1, значит, обратный элемент вычислен верно. Закончим вычисление, вычисляя произведение $P_1 \cdot P_2^{-1}$:

$$(2x^2 + x + 3)(4x^2 + 4x) = 8x^4 + 12x^3 + 16x^2 + 12x =$$
$$= x(-x - 1) + 5(-x - 1) + 2x^2 + 12x = x^2 + 6x + 2$$

8. Неприводимые многочлены над произвольным полем

Согласно следующей теореме неприводимые многочлены произвольной степени $n \geq 2$ можно найти над любым конечным полем.

Теорема 8.1. *Пусть F_p–конечное поле. Для любого $n \geq 2$ найдется неприводимый многочлен степени n.*

1. Покажем, как найти неприводимые многочлены 2-й степени. Рассмотрим произвольное конечное поле F_p. Вычислим всевозможные квадраты элементов из F_p. Полученные элементы называются квадратичными вычетами, а оставшиеся элементы - квадратичными невычетами. Поскольку квадраты элементов $a \neq 0$ и $p - a$ совпадают, то квадратичными вычетами будет ровно половина ненулевых элементов. Выберем любой невычет a. Многочлен $P(x) = x^2 - a$ является неприводимым над полем F_p.

2. $k = 3$. В поле F_p вычислим кубы всех элементов, например, для $p = 7$ получим:

a	1	2	3	4	5	6
a^3	1	1	6	1	6	6

Кубическими вычетами являются числа 1 и 6. Остальные элементы - невычеты, т.е. уравнение $x^3 = 2$ не имеет решения в F_7 и многочлен $x^3 - 2$ - неприводимый.

Примечание 1. При $p \bmod 3 = 2$ (например, если $p = 11$), степени x^3 всех элементов – различны, поэтому кубических невычетов - нет. В этом случае, надо строить таблицу значений многочлена $x^3 + x$ (или подобного ему), и искать для какого a уравнение $x^2 + x = a$ неразрешимо, тогда многочлен $x^2 + x - a$ - неприводимый.

Примечание 2. Для степеней $n > 3$ данный способ не подходит, т.к. многочлен 4-й степени можно разложить в произведение двух неприводимых многочленов 2-й степени, поэтому он не будет иметь ни одного корня из исходного поля, но будет приводимым.

Следующие результаты относятся к полям характеристики 2 ($p = 2$).

9. Неприводимые многочлены над полем $F_2 = \{0, 1\}$

Теорема 9.1. *Пусть $P_n(x) = x^n + a_1 x^{n-1} + \ldots + a_n$–неприводимый многочлен степени n над полем $F_2 = \{0, 1\}$. Тогда свободный член $P_n(x)$ равен 1, и число ненулевых слагаемых этого многочлены – нечетно.*

Доказательство. Если многочлен $P_n(x)$ – неприводим, он не обращается в 0 при подстановке вместо x элементов поля, то есть $P_n(0) \neq 0$ и $P_n(1) \neq 0$.

Но $P_n(0) = a_n$, а $P_n(1)$ – есть сумма по модулю 2 ненулевых коэффициентов этого многочлена. Эта сумма не равна 0, если количество слагаемых – нечетно. Теорема доказана.

Для степеней $n = 2$ и $n = 3$ эти условия являются и достаточными. Для $n \geq 4$ этих условий недостаточно, так как некоторые многочлены с нечетным числом слагаемых и ненулевым свободным членом могут раскладываться в произведение неприводимых многочленов степени 2 или больше. Например, многочлен $x^4 + x^2 + 1$ – приводим, $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

Найдем неприводимые многочлены 2-й, 3-й и 4-й степеней. Многочленами с ненулевым свободным членом и нечетным числом слагаемых являются следующие:

1. $n = 2:\ x^2 + x + 1$
2. $n = 3:\ x^3 + x + 1,\ \ x^3 + x^2 + 1$
3. $n = 4:\ x^4 + x + 1,\ \ x^4 + x^2 + 1,\ \ x^4 + x^3 + 1,\ \ x^4 + x^3 + x^2 + x + 1$

Как было отмечено выше, многочлен x^4+x^2+1 – приводим. Все остальные многочлены в списке - не приводимы. Ниже мы укажем алгоритм для проверки, является ли многочлен неприводимым.

Пусть $\mu(n)$ – функция Мебиуса. Напомним ее определение:

$$\mu(n) = \begin{cases} 1,\ n = 1 \\ (-1)^k,\ \text{если } n \text{ – произведение } k \text{ различных простых сомножителей,} \\ 0,\ \ \text{иначе.} \end{cases}$$

Обозначим через $T_{p,n}(x)$ произведение всех неприводимых многочленов степени n над полем F_p.

Теорема 9.2. *Для каждого простого p и $n \geq 2$ $T_{p,n}(x)$ равно произведению*

$$T_{p,n}(x) = \prod_{d|n} (x^{p^{n/d}} - x)^{\mu(d)}, \tag{1}$$

где произведение вычисляется по всем делителям d степени n.

Пример. Вычислим произведение всех неприводимых многочленов степени 3 над полем F_2. Делителями $n = 3$ являются числа 1 и 3, поэтому в произведении будут два сомножителя:

$$T_{2,3}(x) = (x^{2^{3/1}} - x)^{\mu(1)} (x^{2^{3/3}} - x)^{\mu(3)} = \frac{x^8 - x}{x^2 - x} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Аналогично, произведение всех неприводимых многочленов 4-й степени над полем F_2 равно

$$T_{2,4}(x) = (x^{2^{4/1}}-x)^{\mu(1)}(x^{2^{4/2}}-x)^{\mu(2)}(x^{2^{4/4}}-x)^{\mu(4)} = \frac{x^{16}-x}{x^4-x} = x^{12}+x^9+x^6+x^3+1.$$

(сомножитель в степени $\mu(4)$ равно 1, так как $\mu(4) = 0$).

Из полученных примеров следует, что над полем F_2 найдется ровно два неприводимых многочлена степени 3 (так как произведение этих многочленов имеет степень 6) и три неприводимых многочлена степени 4.

Отсюда ясно, что неприводимыми многочлена степени n надо полем F_p являются в точности многочлены - делители $T_{p,n}(x)$. Поэтому проверка любого такого многочлена на неприводимость возможна путем деления многочлена $T_{p,n}(x)$ на проверяемый.

10. Примитивные многочлены над конечным полем

Полным аналогом примитивного элемента простого поля в расширенном поле являются примитивные многочлены. Начнем с определения порядка многочлена, являющееся аналогом порядка элемента простого поля.

Определение. Порядком называется наименьшее число e такое, что многочлен $x^e - 1$ делится на $P_n(x)$ (деление выполняется по модулю p).

Найдем порядок многочлена $P_n(x) = x^2 + x + 1$ над полем F_2. Очевидно, возможный порядок больше 2. Поделив x^3-1 на x^2+x+1, получим остаток 0. Значит, порядок многочлена $P_n(x) = x^2 + x + 1$ равен 3.

Напомним, что порядками элементов простого поля F_p могут быть по теореме Лагранжа только делители $p - 1$. Сформулируем аналог этого теоремы для полей многочленов.

Теорема 10.1. *Порядками многочленов степени n над простым полем F_p являются в точности делители $p^n - 1$.*

Пример. Многочлен $x^4 + x + 1$ над полем F_2 больше 4 и по теореме является делителем $2^4 - 1 = 15$. Полином $x^5 - 1$ не делится на $x^4 + x + 1$, значит, его порядок равен 15.

Напомним, что многочлен со старшим коэффициентом, равным 1, называется нормированным.

Определение. Неприводимый нормированный многочлен степени n над полем F_p называется *примитивным*, если его порядок равен наибольшему возможному значение $p^n - 1$.

Многочлен $x^4 + x + 1$ над полем F_2 является примитивным, поскольку его порядок равен наибольшему возможному значению 15.

11. Приложение теории многочленов над конечными поля. Генераторы псевдослучайных последовательностей

Одним из наиболее важных приложений теории многочленов является построение псевдослучайных последовательностей, используемых в потоковых алгоритмах шифрования. Рассмотрим генератор пседвослучайной последовательности, построенный на основе *регистра сдвига с линейной обратной связью.*

В общем случае регистр сдвига представляет собой последовательность некоторых элементов конечного поля. Наиболее часто применяются битовые регистры сдвига (то есть основным полем является поле F_2). Длина такого регистра выражается числом битов. При каждом извлечении бита все биты регистра сдвигаются вправо на одну позицию. Новый старший бит рассчитывается как булева функция всех остальных битов регистра. Выходом обычно является младший значащий бит. Периодом регистра сдвига называют длину выходной последовательности до начала ее повторения.

Простейший тип регистров сдвига – регистр сдвига с линейной обратной связью (РСЛОС или ЛРС). Обратная связь – простая операция XOR над некоторыми битами регистра. Перечень этих битов определяется характеристическим многочленом и называется последовательностью отводов. Иногда такую схему называют конфигурацией Фибоначчи.

Дадим более подробное описание линейного регистра над конечным полем F_p. Пусть заданы число $n > 0$ и рекуррентное соотношение.

$$S_{n+i} = a_{n-1}S_{n+i-1} + a_{n-1}S_{n+i-1} + \ldots + a_0 S_i,\ i = 0, 1, 2, \ldots. \tag{2}$$

Последовательность $\{S_i\}$ полностью определяется начальными n значениями. Суммирование выполняется по модулю числа p. Обычно p берется равным 2, тогда последовательность S_i состоит из 0 и 1.

Свяжем с этой последовательностью многочлен над полем F_p:

$$P_n(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^{n-2} - \ldots - a_0.$$

Этот многочлен называется характеристическим многочленом рекуррентной последовательности $\{S_i\}, i = 0, 1, 2, \ldots$.

Пример. Рассмотрим регистр длины 4 над полем F_2. Сопоставим ему характеристический многочлен $P(x) = x^4 - x^3 - 1$. Ненулевыми коэффициентами многочлена (кроме старшего) являются a_3 и a_0. Тогда соотношение (2) запишется так:

$$S_{i+4} = S_{i+3} \oplus_2 S_i.$$

Зададим начальное слово длины $n = 4$, равным $(S_0, S_1, S_2, S_3) = (1, 1, 1, 1)$. Следующие значение равны:

$S_4 = S_3 \oplus_2 S_0 = 1 \oplus_2 1 = 0$,

$S_5 = S_4 \oplus_2 S_1 = 0 \oplus_2 1 = 1$ и т.д.

Продолжая вычисление, получим:

$$S = (1, 1, 1, 1,)0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, (1, 1, 1, 1,) \dots$$

Назовем текущим состоянием регистра на i такте последние вычисленные n-значений, то есть слово $(S_{i+3}, S_{i+2}, S_{i+1}, S_i)$.

Мы видим, что текущее состояние регистра совпало с начальным состоянием на 15-м такте. Поскольку каждое последующее значение зависит только от $n = 4$ предыдущих, то дальше последовательность будет повторяться. Наименьшее значение i, при котором текущее состояние регистра совпало с начальным, называется периодом работы регистра, а пройденная последовательность состояний – циклом работы регистра. Среди пройденных состояний встречаются все слова длины 4, кроме нулевого слова $(0, 0, 0, 0)$. Поскольку нулевое слово порождает только нулевые, то цикл, начинающийся с любой ненулевого слова, имеет максимальную длину $2^n - 1 = 15$.

Очевидно, чем больше период генератора, тем больше текста можно закодировать с помощью одной последовательности. Значит, надо выбирать генераторы с максимальным периодом. Следующая теорема объясняет, как строить такие регистры.

Теорема 11.1. *Регистр сдвига с линейной обратной связью над полем F_2 размерности n имеет максимальный период, равный $2^n - 1$, тогда и только тогда, когда его характеристический многочлен является примитивным.*

Упражнение. Проверить, является ли многочлен $P_5(x) = x^5 - x - 1$ примитивным над полем F_2 и построить для него цикл, начинающийся с единичного слова.

12. Регистры сдвига над полем F_3

Рассмотрим трехэлементное поле $F_3 = \{0, 1, 2\}$. Построим неприводимые многочлены над этим полем размерности 3. Будем рассматривать нормированные многочлены, т.е. многочлены со старшим коэффициентом, равным 1. Произвольный нормированный многочлен 3-й степени имеет общий вид

$$P(x) = x^3 - a_2x^2 - a_1x - a_0.$$

Как и в случае 2-элементного поля, неприводимые многочлены $P(x)$ не должен обращаться в ноль при подстановке вместо x элементов 0,1 и 2.

Отсюда получим три условия:

$$P(0) \neq 0 \ \to a_0 \neq 0,$$
$$P(1) \neq 0 \ \to (a_0 + a_1 + a_2) \bmod 3 \neq 1,$$
$$P(2) \neq 0 \ \to 8 - 4a_2 - 2a_1 - a_0 \neq 0, \ \to \ (a_0 + 2a_1 + a_2) \bmod 3 \neq 2$$

Теорема 12.1. *Многочлен $P(x) = x^3 - x - 1$ является неприводимым над полем F_3.*

Доказательство. Выбранный многочлен $P(x)$ имеет коэффициенты $a_2 = 0, \ a_1 = 1, \ a_0 = 1$. Они удовлетворяют приведенным выше неравенствам. Если бы многочлен $P(x)$ был приводимым, он делился бы на двухчлен $x-b$, где $b \in \{0, 1, 2\}$, значит, $P(x)$ обращался бы в 0 при подстановке $x = b$. Это противоречит выбору коэффициентов. Теорема доказана.

Согласно теореме 9.2, произведение неприводимых многочленов 3-й степени над полем F_3 равно

$$T_{3,3} = (x^{3^{3/1}} - x)^{\mu(1)}(x^{3^{3/3}} - x)^{\mu(3)} = \frac{x^{27} - x}{x^3 - x} = x^{24} + x^{22} + \ldots \ + x^2 + 1.$$

Значит над полем F_3 существует ровно 8 неприводимых многочленов. Одним из факторов $T_{3,3}$ является $P(x) = x^3 - x - 1$.

Построим регистр сдвига над полем F_3 длины 3, взяв в качестве характеристического многочлена многочлен $x^3 - x - 1$. Функция обратной связи в этом случае равна

$$S_{i+3} = S_{i+1} \oplus_3 S_i$$

Построим цепочку слов, вырабатываемую этим регистром, начиная со слова $(0, 0, 1)$:

$$(0, 0, 1), 0, 1, 1, 1, 2, 2, 0, 1, 2, 1, (0, 0, 1).$$

На 13-м шаге повторилось исходное слово. Период последовательности равен 13 – половина максимального периода $3^3 - 1 = 26$.

Таким образом для поля F_3 аналог теоремы 11.1 не выполняется.

13. Алгоритмы вычисления наибольшего общего делителя

Вычисление наибольшего общего делителя и обратных элементов по заданному модулю обычно выполняется с помощью расширенного алгоритма Евклида. Этот алгоритм подробно описан в параграфе 3 данного пособия. Приведем пример вычисления НОД с помощью этого алгоритма для чисел $A = 406$, $B = 387$:

N	A	B	$A \bmod B$
1	406	387	19
2	387	19	7
3	19	7	5
4	7	5	2
5	5	2	1
6	2	1	0

Итак, НОД(406, 387)=1 и был вычислен за 6 итераций. Рассмотрим альтернативные варианты для вычисления НОД и нахождения обратных по модулю элементов.

13.1. **Бинарный алгоритм вычисления НОД.** Алгоритм был известен еще в Китае 1-го века, но опубликован был лишь в 1967 году израильским физиком и программистом Джозефом Стайном. Он основан на использовании следующего свойства НОД (английское greatest common divisor GCD):

$$GCD(2^m \cdot A, 2^n \cdot B) = 2^k \cdot GCD(A, B), \quad k = min\{m, n\}, \quad A,\ B - \text{ нечетны}.$$

Вычисление НОД(A, B) по этому алгоритму выполняется следующим образом:

1. Выделяем нечетные части из множеств A и B: $A = 2^{r_1}A_0$, $B = 2^{r_2}B_0$, $r = min\{r_1, r_2\}$.

2. Далее в цикле по $n = 1, 2, \ldots$ строим новые пары (A_n, B_n) до тех пор, пока C_n не станет равным нулю. Тогда B – искомый НОД. Рассмотрим $n + 1$-шаг алгоритма:

2.1. Вычисляем разность $C_n = A_n - B_n$.

2.2. Сокращаем C_n на 2 до тех пор, пока C_n не станет нечетным.

2.3. Определим новую пару (A_{n+1}, B_{n+1}), полагая $(A_{n+1}, B_{n+1}) = (B_n, C_n)$, если $B_n > C_n$ или $(A_{n+1}, B_{n+1}) = (C_n, B_n)$, иначе.

2.4. Переход к следующему шагу.

3. Продолжим выполнение шага 2 до тех пор, пока C не станет равным 0 (или раньше, если B станет равно 1, тогда НОД=1). Последнее значение B равно искомому НОД, умноженному на общую четную часть 2^r, сокращенную на 1-м шаге.

Рассмотрим пример вычисления НОД тех же чисел 406 и 387 по бинарному алгоритму. На первом шаге вытаскиваем четные делители из чисел A и B и

сокращаем их. Получим пару $(A_0, B_0) = (387, 203)$. Продолжим вычисление по основному алгоритму:

N	A	B	$A - B$	C
1	387	203	184	23
2	203	23	180	45
3	45	23	22	11
4	23	11	12	3
5	11	3	8	1
6	3	1	2	1
7	1	1	0	0

Вычисление можно было уже закончить на шаге 5, когда было найдено значение C, равное 1.

13.2. k-арный алгоритм вычисления НОД. .

k-арный алгоритм вычисления НОД был разработан в начале 90-х годов 20 столетия Д. Соренсоном [5]. Этот алгоритм обобщает бинарный алгоритм. Пусть дано $k = 2^s$ и два числа A и B, $A > B > 1$. Будем предполагать, что эти числа являются нечетными, иначе сократим их на четные делители.

По теореме Соренсона если числа A и B взаимно-просты с k, то существуют целые числа x и y, удовлетворяющие условию $1 \le x \le \sqrt{k}$ и $-\sqrt{k} \le y \le \sqrt{k}$ такие, что выполнено тождество

$$Ax + By \equiv 0 \mod k.$$

Основное вычисление k-арного алгоритма состоит в том, что для заданной пары (A, B) ищется пара чисел x, y, удовлетворяющая теореме Соренсона, после чего вычисляется $C = |Ax + By|/k$. Если C останется четным, то оно дополнительно сокращается на 2, пока не станет нечетным. После чего переходят к новой паре (B, C).

Поиск пары x, y, удовлетворяющей теореме Соренсона, можно выполнять перебором. Из условия $Ax+By \equiv 0 \mod k$ можно получить эквивалентное условие $y \equiv -qx \bmod k$, где $q = AB^{-1} \bmod k$.

В цикле по x от 1 до $\sqrt{k}$ будем вычислять два значения y: $y_1 = -(qx \bmod k)$ и $y_2 = y_1 + k$, первое из которых отрицательно, а второе – положительно, и проверять, будет ли одно из них лежать в интервале $[-\sqrt{k}; \sqrt{k}]$.

Когда такое y найдется, вычислим $C = |Ax + By|/k$ и перейдем к новой паре (B, C) (или (C, B), если $C > B$). Вычисление продолжается до тех пор, пока не будет получено $C = 0$. Последнее значение B дает нам исходный НОД$=d = GCD(A, B)$ или его кратное md. Последний случай возникает

из-за того, что при вычислении $C = (Ax + By)/k$ в C может появиться дополнительный множитель, не входящий в НОД исходных A и B, поэтому на последнем шаге k-арного алгоритма выполняют дополнительную прогонку с помощью классического алгоритма Евклида КАЕ:

$$GCD(A, B) = KAE(B, KAE(A, d')),$$

где d'– НОД, полученный с помощью k-арного алгоритма, A, B – исходные числа.

Приведем пример вычисления НОД по описанному алгоритму при $k = 16$:

N	A	B	q	x	y	$(Ax + By)/k$	C
1	387	203	9	2	-2	23	23
2	203	23	13	1	3	17	17
3	23	17	7	2	2	5	5
4	17	5	13	1	3	2	1

13.3. **Аппроксимирующий k-арный алгоритм вычисления НОД.** Аппроксимирующий k-арный алгоритм был разработан Ш.Т.Ишмухаметовым в 2017 году [6]. Основная идея алгоритма состоит в улучшении схемы Соренсона выбора пары x и y таким образом, чтобы значение $C = |Ax + By|/k$ было наименьшим. Пусть по-прежнему заданы нечетные числа A и B, $k = 2^s$ и $q = AB^{-1} \bmod k$. Из условия $y \equiv -qx \bmod k$ следует, что $y = -qx + ks$ для некоторого целого s. Выполним следующие преобразования:

$$\frac{Ax + By}{k} = \frac{Ax + B(-qx + ks)}{k} = B \cdot \left| \frac{A/B - q}{k} \cdot x + s \right|$$

Обозначим дробь $(A/B - q)/k$ через α. Тогда получим:

$$\frac{Ax + By}{k} = |\alpha x + s|. \tag{3}$$

Поскольку $A/B > 1$ и $0 < q < k$, значение $\alpha > -1$. Оно окажется больше 1, если $A/B > k + q$. В этом случае, $A >> B$, и применение k-арного алгоритма не эффективно. Лучше в таких случаях использовать обычную итерацию классического алгоритма Евклида, вычисляя $C = A \bmod B$.

Пусть β – произвольное действительное число, находящееся в интервале от 0 до 1, и задано некоторое натуральное число $k > 2$. Дробью Фарея для заданного β называется правильная дробь m/n с целыми $m < k$ и $n < k$ такая, что разность

$$\left| \beta - \frac{m}{n} \right| - \text{ минимальна.}$$

Иначе говоря, дробь Фарея является наилучшим приближением действительного числа β в классе дробей с ограниченным числителем и знаменателем.

Присвоим переменной x значение равное знаменателю дроби Фарея m/n $x = n$. Значение y равным $y = -qx - km$.

Определим $C = (Ax + By)/k$. Если C – четно, выполним его сокращение на 2, пока C не станет нечетным. Перейдем к новой паре (B, C).

Покажем как найти дробь Фарея на примере. Пусть $\beta = 0,403$, $k = 16$.

1. Строим исходную последовательность дробей:

$$0 < \frac{1}{k-1} < \frac{1}{k-2} < \ldots < \frac{1}{3} < \frac{1}{2} < \frac{2}{3} < \ldots < \frac{k-2}{k-1} < 1.$$

2. Находим интервал, в котором находится наше число β: $\beta \in (1/3; 1/2)$.

3. Выполняем в цикле следующее вычисление. Предположим, что в данный момент β находится в интервале $(m_1/n_1;\ m_2/n_2)$.

3.1. Вычисляем медиану

$$\frac{m}{n} = \frac{m_1 + m_2}{n_1 + n_2}.$$

3.2. Проверяем условие $n_1 + n_2 \geq k$. Если оно выполняется, выходим из цикла. Иначе, сравниваем β с m. Если $\beta < m$, перейдем к новому интервалу $[m_1/n_1; m/n]$, иначе, к интервалу $[m/n; m_2/n_2]$.

4. После выхода из цикла получим интервал значений, приближающих наше число.

Выполним наше вычисление поиска дроби Фарея для $\beta = 0,403$:

$$\beta \in \left(\frac{1}{3}; \frac{1}{2}\right),\ m = \frac{2}{5} < \beta \to \beta \in \left(\frac{2}{5}; \frac{1}{2}\right),\ m = \frac{3}{7} > \beta \to$$

$$\beta \in \left(\frac{2}{5}; \frac{3}{7}\right),\ m = \frac{5}{12} < \beta \to \beta \in \left(\frac{2}{5}; \frac{5}{12}\right) = (0,4;\ 0,417).$$

Значит, искомой дробью Фарея является дробь $2/5 = 0,4$.

Выполним теперь полное вычисление НОД$(387, 203)$ с использованием аппроксимирующего k-арного алгоритма:

N	A	B	q	α	m	n	x	y	$(Ax + By)/k$	C
1	387	203	9	$-0,443$	-4	9	9	-17	2	1

Значение y было вычислено по формуле $y = -qx - km = -9 \cdot 9 + 16 \cdot 4 = -17$. НОД=1 был вычислен за одну итерацию аппроксимирующего алгоритма.

Литература

[1] Крэндалл Р., Померанс К. *Простые числа. Криптографические и вычислительные аспекты* // М.: URSS – Springer–Verlag, Berlin, 2011, 665 p.

[2] Лидл Р. *Конечные поля*/Р. Лидл,Г. Нидеррайтер.– Т. 1, 2. М.: Мир, 1988, 428 с.

[3] Ишмухаметов Ш.Т. *Методы факторизации натуральных чисел: учебное пособие.* – Казанский федеральный университет, Казань, 2011. – 190 с.

[4] Галуев Г.А. *Математические основы криптологии: Учебно-методическое пособие.*– Таганрог: Изд-во ТРТУ, 2003.-120 с.

[5] Sorenson, J. *Two Fast GCD Algorithms*// Journal of Algorithms, V.16, **1**, 1994, p. 110-144

[6] 4. Ishmukhametov S.T. *An approximating k-ary GCD Algorithm.* // Lobachevskii Journal of Mathematics 37 (6), 2017, 723-729