Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

# Неприводимые многочлены над конечными полями и их связь с теорией кодирования

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 227 группы

направления 02.04.01 - Математика и компьютерные науки

механико-математический факультет

Хомич Екатерины Александровны

Научный руководитель
доцент, к.ф.-м.н., доцент Е.В. Сецинская

Зав. кафедрой
зав. каф., к.ф.-м.н. А. М. Водолазов

Саратов 2017

# ВВЕДЕНИЕ

Работа посвящена исследованию объектов конечных полей, алгоритмам решения алгебраических уравнений, разложения на неприводимые многочлены и проверки неприводимости многочленов, а также циклическим кодам.

**Актуальность темы.** В настоящее время все больше операций различного характера, предусматривающие обмен конфиденциальными данными, возможны через интернет. В связи с этим необходимо защищать передаваемую информацию, а также следить за целостностью переданных данных, так как интернет это открытый канал связи. Именно поэтому сейчас активно развиваются прикладные аспекты теории конечных полей, которая была построена в работах Ферма, Эйлера, Лежандра, Гаусса, Галуа, Диксона и других выдающих ученых, и развивалась как область чистой математики до последний четверти 20-го века, пока не возникла надобность данной теории в криптографии и теории кодирования. Свойства неприводимых многочленов позволяют максимизировать эффективность компьютерной реализации арифметике в конечных полях. Таковы, например, реализация электронной цифровой подписи на эллиптических кривых, коды Рида-Маллера, Рида-Соломона и другие.

Начиная с 20 века многочлены стали использоваться для новых целей. Нужно было быстро и эффективно передавать информацию. Сообщение должно было содержать в себе последовательность символов, которое потом передали по каналу связи. Рассмотрим пример использования многочленов при передаче сообщения. Пусть мы хотим передать число «2017», в двоичной записи числу «2017» эквивалентно число «11111100001», и обозначает многочлен 10-й степени $x^{10}+x^9+x^8+x^7+x^6+x^5+1$. Так как мы всегда можем преобразовать двоичную запись сообщения в многочлен $n-$ой степени, мы можем использовать различные операции с многочленами, для выполнения необходимых действий над данными. С помощью теории многочленов мы можем проверить передаваемую информацию на целостность, для этого используются циклические коды.

Неприводимые многочлены, корни которых образуют базис для представления элементов конечных полей, аналогичны простым числам. Они нашли

свое применение в различных областях математики, информационной техники и защите информации. К примеру, симметричные многочлены(у которых коэффициенты симметричны относительно центрального бита.), которые применяются в теории кодирования, имеют максимально возможный порядок $p - 2^{2^k} + 1$, где степень многочлена $N = 2^{k+1}$. Это сближает их с тематикой простых чисел Ферма, которые рассчитываются по формуле $p = 2^{2k+1}$. Данные числа интересны как пример больших простых чисел, имеющих мало единичных битов в своей двоичной записи. Числа Ферма имеют всего два таких битов - старший и младший это минимально возможное количество.

Порядок примитивных многочленов степени $n$, равный $p = 2^n - 1$, сближает их с простыми числами Мерсенна. В настоящее время найдено 48 таких чисел и поиск их продолжается. Построение алгоритма эквивалентного поиска примитивных многочленов степени $n$ могло бы упростить или хотя бы систематизировать процедуру поиска чисел Мерсенна. В защите информации эти числа применяются в генераторе псевдослучайных чисел «вихрь Мерсенна».

Криптографические приложения основаны преимущественно на теоретико-сложностных проблемах алгебраической теории чисел. А одной из таких сложных задач является поиск всех неприводимых многочленов заданной степени $n$ над некоторым конечным полем $F_p$ или $GF(p)$. В нахождении таких многочленов заинтересованы криптографические службы всего мира, они ведут активную работу, но эти работы засекречены. Однако, Эварист Галуа (1811 -1832 гг.) доказал существование неприводимых многочленов сколь угодно большой степени и создал теорию поля Галуа. Построение таких многочленов производится подбором, то есть вероятностными алгоритмами, что требует временных затрат и объемных вычислений, что находит применение в криптографии. Использование теоретико-сложностных проблем в криптографии приобрело особую значимость только после того, как в 1976 году Диффи и Хеллман открыли принципиально новый тип криптосистем и изобрели «криптографию с открытым ключом». Данная криптосистема не позволяет по ключу шифрования найти ключ дешифрования, избежав чрезвычайно длинных вычислений.

Также к числу сложных задач, которые применяются в криптографии, относится задача разложения многочлена на неприводимые многочлены. Имеется много эффективных алгоритмов решения этой задачи, если конечное поле малого размера. Когда рассматриваем поля больших размеров, то поставленная задача усложняется в разы. Находя разложения на неприводимые многочлены, будут отыскиваться новые неприводимые многочлены больших степеней.

**Объект изучения** – элементы конечных полей (неприводимые многочлены, циклические коды) и их свойства.

**Предмет изучения** – алгоритм разложения многочлена на неприводимые множители.

**Цель.** Главной целью настоящей работы является изучение неприводимых многочленов в конечных полях и из связь с теорией кодирования.

Для достижения поставленной цели потребовалось решить следующие задачи:

1) Рассмотреть неприводимые многочлены в конечных полях: основные понятия, теоремы, алгоритмы.

2) Изучить применение неприводимых многочленов в циклических кодах.

3) Изучить алгоритм Берлекэмпа и его усовершенствования.

4) Изучить алгоритм Берлекэмпа-Месси для его реализации.

Магистерская работа состоит из введения, четырех разделов, заключения, списка использованных источников и приложений.

В разделах работы приведены основные понятия и алгоритмы связанные с неприводимыми многочленами над конечными полями, а также рассмотрено их применение в криптографии и приведены подробные примеры.

Рассмотрим основные положения из работы.

**Алгоритм решения** $f(x) = 0$ **в** $GF(p)$.

**1 шаг.** Вычислить

$$g(x) = \text{НОД}(f(x), x^p - x) \in GF(p)[x].$$

Заметим, что все корни $f(x)$ в $GF(p)$ являются корнями многочлена $g(x)$ кратности 1, и других корней у $g(x)$ нет. Если $deg\ g(x) = 0$, то корней у

$f(x)$ в $GF(p)$ нет. Если $deg\ g(x) = 1, g(x) = x - a$, то $a$ – единственный корень $f(x)$ в поле $GF(p)$(без учета кратности). Далее мы предполагаем, что $2 \leqslant deg\ g(x) < p$, ищем корни $g(x)$ в $GF(p)$.

**2 шаг.** Случайным образом выбрать элемент $\sigma \in GF(p)$ и вычислить

$$d(x) = \text{НОД}((x + \sigma)^{\frac{p-1}{2}} - 1, g(x)).$$

**3 шаг.** Если $d(x) = 1$ или $d(x) = g(x)$, то вернуться на шаг 2. Если $deg\ d(x) = 1, d(x) = x - b$, то $b$ – корень многочлена $f(x)$; мы заносим его в список найденных корней, заменяем $g(x)$ на $g(x)/(x - b)$ и возвращаемся на шаг 2. Аналогично, при $deg\ d(x) = deg\ g(x) - 1$ мы находим $x - b = \frac{g(x)}{d(x)}$, заносим $b$ в список корней, заменяем $g(x)$ на $d(x)$ и возвращаемся на 2-й шаг. Если $2 \leqslant deg\ d(x) < deg\ g(x) - 1$, то мы рассматриваем вместо $g(x)$ два его делителя – многочлены $d(x)$ и $g(x)/d(x)$, и к каждому из них мы применяем 2 и 3 шаги алгоритма, чтобы найти их корни.

**Конец алгоритма**

Рассмотрим алгоритм Тонелли-Шэнкса для решения уравнения $x^2 \equiv a(mod p)$, в случае $p \equiv 1(mod 4)$. В нем $p-1 = 4k = 2^{s+1} \cdot t = 2^e \cdot t; N$ – какой-либо известный нам квадратичный невычет по модулю $p$. Мы считаем, что $\left(\frac{a}{p}\right) = \pm 1$.

**Алгоритм Тонелли-Шэнкса.**

**1 шаг.** Вычисляем следующие значения:

$$y := N^t (mod\, p), \quad r := e, \quad x := a^{(t-1)/2} (mod\, p),$$

$$b := ax^2 (mod\, p), \quad x := ax (mod\, p).$$

**2 шаг.** Если $b \equiv 1(mod\, p)$, то $x$ является искомым решением уравнения, и алгоритм останавливается.

**3 шаг.** Находим наименьшее $m \in \mathbb{N}$ такое, что $b^{2m} \equiv 1(mod\ p)$. Оно удовлетворяет неравенству $a \leqslant m \leqslant r - 1$.

**4 шаг.** Вычисляем значения

$$l := y^{2^{r-m-1}} (mod\, p), \quad y := l^2, \quad r := m,$$

$$x := xl(mod\, p), \quad b := by(mod\, p)$$

и возвращаемся на 2-й шаг.

**Конец алгоритма.**

**Алгоритм Берлекэмпа.** На входе алгоритма задан унитарный многочлен $f(x) \in GF(q)[x], deg\ f(x) = n \geqslant 2$, про который известно, что он не имеет кратных неприводимых множителей. На выходе — разложение $f(x)$ на неприводимые множители.

**1 шаг.** Вычислить матрицу $B$.

**2 шаг.** Найти базис пространства решений системы линейных уравнений

$$B_1 \begin{pmatrix} x_0 \\ ... \\ x_{n-1} \end{pmatrix} = 0, \tag{1}$$

где $B_1 = (B - l_n)^T, l_n$ — единичная матрица, знак $(\cdot)^T$ означает транспортирование. Пусть $\bar{e}_1 = (1, 0, ..., 0), \bar{e}_2, ..., \bar{e}_k$ — найденный базис.

Поскольку $x^{iq} \equiv 1(mod\ f(x))$ при $i = 0$, то в матрице $B$ первая строка всегда имеет вид $(1, 0, ..., 0)$, и первый столбец матрицы $B_1$ будет нулевым. Поэтому $\bar{e}_1 = (1, 0, ..., 0)$ будет присутствовать в базисе пространства решений.

**3 шаг.** При $k = 1$ многочлен $f(x)$ неприводим; вообще, найденное значение $k$ равно количеству неприводимых делителей $f(x)$ в $GF(q)[x]$. При $k > 1$ надо взять $\bar{e}_2 = (h_{2,0}, ..., h_{2,n-1})$ и построить $f$ — разлагающий многочлен $h_2(x) = \sum\limits_{i=0}^{n-1} h_{2,i}x^i$. С его помощью, то есть вычисляя НОД$(f(x), h_2(x) - c)$ при $c \in GF(q)$, найти разложение

$$f(x) = g_1(x)...g_l(x),$$

где $g_i(x) \in GF(q)[x], l \geqslant 2$. Если $l = k$, алгоритм останавливается. Если $l < k$, то мы берем $\bar{e}_3 = (h_{3,0}, ..., h_{3,n-1})$, строим $h_3(x) = \sum\limits_{i=0}^{n-1} h_{3i}x^i$; вычисляя НОД$(g_i(x), h_3(x) - c)$ для найденных $g_i(x)$, мы получаем дальнейшее разложение $f(x)$, и т.д. Алгоритм закончит работу, когда мы переберем все базисные векторы $\bar{e}_2, ..., \bar{e}_k$, и для соответствующих им многочленов

$h_i(x)$ вычислим наибольшие общие делители найденных множителей $f(x)$ с $h_i(x) - c, c \in GF(q)$.

Алгоритм останавливается, как только мы найдем разложение $f(x)$ на $k$ множителей, где $k = n - rang\, B_1$.

**Конец алгоритма.**

Алгоритм Берлекэмпа имеет реализацию в системе компьютерной алгебры PARI/GP и может быть использован посредством команды $factormod$. PARI/GP — это система компьютерной математики с собственным $C-$подобным интерпретируемым языком, ориентированная на вычислительную теорию чисел. Также можно проверить многочлен на неприводимость командой $polisirreducible(f)$ или найти унитарный неприводимый многочлен степени $n$ с переменной $w$ над конечным полем $F_p$ с помощью команды $ffinit(p, n, w)$.

Наиболее интересен для реализации алгоритм Берлекэмпа-Месси. Это алгоритм поиска кратчайшего регистра сдвига с линейной обратной связью для поданной на вход бинарной последовательности. Также алгоритм позволяет найти минимальный многочлен поданной на вход линейной рекуррентной последовательности над произвольным полем. Алгоритм был открыт Элвином Берлекэмпом (англ.) в 1968 году. Джеймс Мэсси в следующем году нашел применение алгоритма к линейным кодам. Это стало ключом для практического применения кодов Рида — Соломона, которые широко используются для восстановления в случае повреждений, в помехоустойчивом кодировании.

Рассмотрим усовершенствование алгоритма Берлекэмпа.

**Метод Кантора-Цассенхауза** Зафиксируем простое число $p$. Пусть $f(x) \in \mathbb{Z}/p\mathbb{Z}[x], f(x)$ унитарен и не имеет кратных неприводимых множителей. Ниже мы опишем алгоритм, который для заданного $d \in \mathbb{N}$ находит произведение всех неприводимых делителей $f(x)$, имеющих степень $d$. Предварительно рассмотрим лемму.

**Лемма 1.** Пусть $g(x) \in \mathbb{Z}/p\mathbb{Z}[x], f(x)$ — унитарный неприводимый многочлен.

1. Если $deg\, g(x) = d$, то $g(x)$ делит $x^{p^d} - x$.

2. Если $g(x)$ делит $x^{p^d} - x$ и $g(x)$ не делит $x^{p^e} - x$ для всех $e < d$, то $deg\, g(x) = d$.

**Замечание 1.** Этот алгоритм нахождения произведений всех неприводимых делителей $f(x)$, имеющих фиксированную степень, можно применять до того, как мы применяем алгоритм Берлекэмпа для факторизации $f(x)$.

Далее мы считаем, что $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$, $f(x)$ бесквадратен, и все его неприводимые делители имеют одинаковую степень $d$, известную нам. Следующие две теоремы описывают **метод Кантора-Цассенхауза** для факторизации $f(x)$. В нем различаются случаи $p = 2$ и $p > 2$.

**Теорема 1.** Если $p > 2$, то для любого многочлена $T = T(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ справедливо равенство

$$f(x) = \text{НОД}(f(x), T)\text{НОД}(f(x), T^{(p^d-1)/2} + 1)\text{НОД}(f(x), T^{(p^d-1)/2} - 1).$$

**Теорема 2.** Пусть $p = 2, U(x) = x + x^2 + x^4 + ... + x^{2^{d-1}} \in \mathbb{Z}/2\mathbb{Z}[x]$. Тогда для любого многочлена $T = T(x) \in \mathbb{Z}/2\mathbb{Z}[x]$ справедливо равенство

$$f(x) = \text{НОД}(f(x), U(T))\text{НОД}(f(x), U(T) + 1).$$

Также представляет большой теоретический интерес следующий метод, в основе которого лежим матрица из многочленов, то есть матрица, элементами которой являются многочлены из кольца $\mathbb{F}_q[x]$.

**Теорема 3.** Пусть $f = f_1...f_k$, где $f_1, ..., f_k$ – различные нормированные неприводимые многочлены из $\mathbb{F}_q[x]$, и пусть $h_2, ..., h_k \in \mathbb{F}_q[x]$ – нормированные многочлены степени меньшей степени многочлена $f(x)$, которые вместе с $h_1 = 1$ являются линейно независимыми над полем $\mathbb{F}_q$ решениями сравнения

$$h^q \equiv h (mod\, f), deg\,(h) < deg\,(f). \tag{2}$$

Тогда диагональная матрица из многочленов

$$D = \begin{pmatrix} f_1 & 0 & ... & 0 \\ 0 & f_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & f_k \end{pmatrix}$$

эквивалентна матрице из многочленов

$$A = \begin{pmatrix} f & 0 & 0 & ... & 0 \\ h_2 - 1 & -1 & 0 & ... & 0 \\ h_3 & 0 & -1 & ... & 0 \\ ... & ... & ... & ... & ... \\ h_k & 0 & 0 & ... & -1 \end{pmatrix}.$$

Приведенная выше теорема обеспечивает теоретическую возможность нахождения неприводимых делителй многочлена $f$ путем приведения матрицы $A$ к диагональному виду. Сама же матрица $A$ (число $k$ и многочлены $h_2, ..., h_k$ из ее первого столбца) строится с помощью алгоритма Берлекэмпа. Однако алгоритм, с помощью которого производится диагонализация матрицы $A$ довольно сложен.

**Заключение.** Работа посвящена конечным полям и неприводимым многочленам. В ней были даны основные определения и теоремы, связанные с неприводимыми многочленами, которые как и простые числа активно применяются в теории кодирования. Также было изучено применение неприводимых многочленов в циклических кодах

Рассмотрим пример. В современном алгоритме шифрования AES, пришедшем на смену DES, используется конечное поле Галуа $GF(2^8)$. Это поле является расширением самого маленького поля $GF(2)$, которое состоит из двух нейтральных элементов $\{0, 1\}$. Неприводимый многочлен, с помощью которого оно строится, согласно стандарту США $FIPS - 197$, имеет вид $f(x) = x^8 + x^4 + x^3 + x + 1$. Данный многочлен неприводим. Пусть $g(x) = x^7 + x^3 + x + 1$. Этот остаток задает, согласно $FIPS - 197$, байт со следующими битами 10001011. Одно из основных криптографических преобразований алгоритма AES состоит в том, что элемент поля $g(x)$ преобразуется в обратный к нему по умножению $g^{-1}(x)$. Для этого используют алгоритм Евклида. После того как найдем такие остатки $u, v$, что $ug + vf = 1$. Получим, что $u = x^7 + x^6 + x^4 + x^3 + 1, v = x^6 + x^5 + x^3 + x + 1$, то есть $g^{-1}(x) = x^7 + x^6 + x^4 + x^3 + 1$ и, значит, байт 10001011 под действие одного шага алгоритма AES перейдет в байт 11011001.

В работе дан обзор методов решения алгебраический уравнений в конечных полях. Одним из таких методов является алгоритм Тонелли-Шэнкса, он находит решение квадратного уравнения $x^2 \equiv a(mod\ p)$. Также были рассмотрены алгоритмы факторизации многочленов. Одним из основных алгоритмов является алгоритм Берлекэмпа. Также Берлекэмпом был предложен алгоритм разложения с помощью диагонализации матриц из многочленов. Помимо обоснования алгоритма также приводится ряд его усовершенствований. Одним из них является алгоритм Берлекэмпа-Месси, диаграмму данного алгоритма и его реализации можно найти в приложении. Там же есть пример выполнения созданной программы.

В работе рассмотрен метод Кантора-Цассенхауза, который находит произведение всех неприводимых делителей многочлена, имеющих фиксированную степень. Его можно применять до того, как мы применяем алгоритм Берлекэмпа. Алгоритмы дополнены примерами.

В последнем разделе приводится вероятностный алгоритм проверки неприводимости многочленов над конечным полями.

Приведенные здесь алгоритмы находят практическое применение в теории кодирования, протоколах шифрования, программировании дискретных устройств.

Для достижения поставленной цели, а именно изучения неприводимых многочленов в конечных полях и их связи с теорией кодирования, были изучены различные источники в том числе английская литература. Следует отметить, что работа оснащена множеством примеров. И полностью соответствует поставленным задачам.