ВВЕДЕНИЕ

Теория чисел — раздел математики, занимающийся изучением чисел непосредственно как таковых, их свойств и поведения в различных ситуациях. В теории чисел, естественно, выделяются и рассматриваются в первую очередь те проблемы, которые глубоко и достаточно непосредственно связаны с изучаемыми объектами и важны для построения математики в ее целом. Некоторые теоретико-числовые задачи возникают уже в рамках школьного курса арифметики. В настоящее время в теорию чисел включают более широкий круг вопросов, выходящих за рамки изучения натуральных чисел.

Конечное поле — поле, состоящее из конечного числа элементов. Конечные поля стали изучаться в начале XIX в. Этому предшествовали исследования выдающихся математиков таких как Гаусс и Галуа. Длительное время конечные поля изучались и находили применения только в алгебре и теории чисел, однако в последние десятилетия грани соприкосновения теории конечных полей с разными областями математики и ее прикладными разделами существенно расширились. Конечные поля обладают такими свойствами, которые присущи далеко не всем алгебраическим объектам.

В данной работе первая глава посвящена основным определениям и понятиям. Вторая глава занимает центральное место в работе, в ней мы приводим несколько алгоритмов разложения многочленов на множители над конечными полями (а именно алгортим Берлекемпа и Цессенхауза), алгоритмы нахождения корней многочленов в полях большой малой характеристики. В последней третьей главе мы рассмотрим методы решения систем линейных уравнений, наиболее часто используемые в современных алгоритмах факторизации и дискретного логарифмирования и приводим несколько алгоритмов.

Краткое содержание работы:

В **Разделе 1** рассматриваются основные определения и понятия, которые используются в последующих разделах. Такие как:

Определение 1. Множество F с двумя бинарными операциями $+$ (сложение) и $\cdot$ (умножение)называется полем, если оно образует коммутативную группу по сложению, все его не нулевые элементы образуют коммутативную группу по умножению, и выполняется свойство дистрибутивности $a(b+c) = ab + ac$.

Определение 3. Пусть a и b — произвольные целые числа и n — натуральное число. Будем говорить, что a сравнимо с b по модулю n и будем писать $a \equiv b \pmod{n}$, если разность $a - b$ делится на n, т.е. если $a = b + kn$ для некоторого целого числа k.

Определение 10. Пусть R — произвольное кольцо. Многочленом (или полиномом) над R называется выражение вида

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n, .$$

где n — неотрицательное целое число, коэффициенты $a_i, 0 \leqslant i \leqslant n,$ — элементы кольца R, а x — некоторый символ, не принадлежащий кольцу R, называемый переменной (или неизвестной) над R.

Многочлены

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{и} \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

над R считаются равными тогда и только тогда, когда $a_i = b_i$ для $0 \leqslant i \leqslant n$. Определим сумму многочленов $f(x)$ и $g(x)$ равенством

$$f(x) + f(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

а произведение многочленов

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} c_k x_k, \quad \text{где } c_k = \sum_{i+j=k} a_i b_j, 0 \leqslant i \leqslant m, 0 \leqslant j \leqslant n$$

Определение 11. Кольцо, образованное многочленами над кольцом R с веденными выше операциями, называется кольцом многочленов над R и обозначается через $R[x]$.

Определение 17. Элемент α в некотором расширении K, содержащем F, называется алгебраическим над F, если существует многочлен с коэффициентами из F, обращающийся в 0 при подстановке в него α. В этом случае существует единственный нормированный неприводимый многочлен в $F[x]$, корнем которого является α (и всякий другой многочлен из $F[x]$ корнем которого является α, должен делится на этот приведенный неприводимый многочлен). Если этот нормированный неприводимый многочлен имеет степень d, то любой элемент $F(\alpha)$ (т.е. любое рациональное выражение, включает в себя степени α и элементы из F) можно представить как линейную комбинацию степеней $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$. Таким образом, эти степени α образуют базис поля $F(\alpha)$ над F, и степень расширения, полученного присоединением α, равна степени нормированного неприводимого многочлена с корнем α. Любой другой корень α' того же неприводимого многочлена называется сопряженным к α над F.

Китайская теорема об остатках для многочленов. Пусть k — поле и $u_1(x), \ldots, u_r(x)$ — попарно взаимно простые многочлены из $k[x]$. Для любого набора $a_1(x), \ldots, a_r(x)$ многочленов из $k[x]$ существует многочлен $c(x)$ такой, что $c(x) \equiv a_i(x) \pmod{u_i(x)}$ для любого $i = 1, \ldots, r$. Условием $\deg c(x) < \sum_{i=1}^{r} \deg u_i(x)$ число $c(x)$ определяется однозначно.

Малая теорема Ферма. Если p — простое число, то для любого $a \in \mathbb{Z}$ выполняется сравнение $a^p \equiv a \pmod{p}$.

Раздел 2 — основной в данной работе. В нем рассматривается две задачи:
1.Разложить $f(x)$ на неприводимые множители над полем F.
2.Найти все корни $f(x)$, принадлежащие f.

Вторая задача есть частный случай первой. Тем не менее здесь мы укажем алгоритм, сводящий решение первой задачи ко второй, и покажем, как может быть решена вторая задача. Основными алгоритмами и теоремами в данном разделе являются:

Алгоритм 2.1(Берлекемп) Данные: Многочлен $f(x) \in F[x]$ без кратных корней.

Найти: Разложение $f(x)$ на неприводимые множители.

1. Вычислить матрицу $B = \|b_{ij}\|_{0 \leqslant i,j < n}$ с помощью равенств (2.6 ($x^{iq} \equiv \sum_{i=0}^{n-1} b_{ij} x^j \pmod{f(x)}$)).

2. Решая систему (2.7 ($\vec{a} \cdot (B - I) = 0$)), найти многочлены $h_1(x) = 1, h_2(x), \ldots, h_k(x)$, составляющие базис пространства $\mathfrak{L}$. Если $k = 1$, то СТОП, многочлен $f(x)$ неприводим.

3. Положить $M = \{f\}$.

4. Для каждого $j = 2, \ldots, k$ и для каждого $c \in F$ до тех пор, пока не выполняется мощность$M = k$, проделать следующее:
для каждого $u \in M$ вычислить

$$p(x) = (u(x), h_j(x) - c.$$

и, если $0 < \deg p(x) < \deg u(x)$, исключить $u(x)$ из M и заменить его парой многочленов $p(x),\ u(x)/p(x)$.

5. Если мощность $M = k$, СТОП. Множество M содержит все неприводимые делители $f(x)$.

Теорема 2.1 Алгоритм находит разложение многочлена $f(x)$ на неприводимые множители. Для этого ему требуется $O(qn^3)$ арифметических операций в поле F.

Пример. Данный пример взят из монографии Кнута [5].

Пусть $u(x) = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8,\ p = 13$. Непосредственными вычислениями проверяется, что НОД$(u(x), u'(x)) = 1$. Следовательно, $u(x)$ свободен от квадратов. Далее, $x^0 \equiv 1 \pmod{u(x)}$, значит первая строка матрицы B равна $(1, 0, \ldots, 0)$. Вычислим вторую строку, т.е. $x^{13} \pmod{u(x)}$. Ниже приводятся вычисления.

k	$a_{k,7}$	$a_{k,6}$	$a_{k,5}$	$a_{k,4}$	$a_{k,3}$	$a_{k,2}$	$a_{k,1}$	$a_{k,0}$
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0
2	0	0	0	0	0	1	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	1	0	0	0	0	0
6	0	1	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0
8	0	12	0	3	3	5	11	5
9	12	0	3	3	5	11	5	0
10	0	4	3	2	8	0	2	8
11	4	3	2	8	0	2	8	0
12	3	11	8	12	1	2	5	7
13	11	5	12	10	11	7	1	2

Получим вторую строку матрицы B, записанную в обратном порядке.Продолжая подобным образом получим остальные строки матрицы B:

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 7 & 11 & 10 & 12 & 5 & 11 \\ 3 & 6 & 4 & 3 & 0 & 4 & 7 & 2 \\ 4 & 3 & 6 & 5 & 1 & 6 & 2 & 3 \\ 2 & 11 & 8 & 8 & 3 & 1 & 3 & 11 \\ 6 & 11 & 8 & 6 & 2 & 7 & 10 & 9 \\ 5 & 11 & 7 & 10 & 0 & 11 & 7 & 12 \\ 3 & 3 & 12 & 5 & 0 & 11 & 9 & 12 \end{bmatrix}$$

Вычитая единичную матрицу, получим:

$$B - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 7 & 11 & 10 & 12 & 5 & 11 \\ 3 & 6 & 3 & 3 & 0 & 4 & 7 & 2 \\ 4 & 3 & 6 & 4 & 1 & 6 & 2 & 3 \\ 2 & 11 & 8 & 8 & 2 & 1 & 3 & 11 \\ 6 & 11 & 8 & 6 & 2 & 6 & 10 & 9 \\ 5 & 11 & 7 & 10 & 0 & 11 & 6 & 12 \\ 3 & 3 & 12 & 5 & 0 & 11 & 9 & 11 \end{bmatrix}$$

Ранг данной матрицы равен 5. Находим три линейно независимых решения соответствующей системы линейных однородных уравнений.

Первая строка нулевая, таким образом, получаем решение $v[1] = (1, 0, \ldots, 0)$. Выбирая в качестве свободных параметров, выбираем последние две координаты, получим еще два решения: $v[2] = (0, 5, 5, 0, 9, 5, 1, 0)$ и $v[3] = (0, 9, 11, 9, 10, 12, 0, 1)$.

Им соответствуют многочлены

$$v[2](x) = x^6 + 5x^5 + 9x^4 + 5x^2 + 5x,$$

$$v[3](x) = x^7 + 12x^5 + 10x^4 + 9x^3 + 11x^2 + 9x.$$

Находим НОД$(u(x), v[2](x) - s)$. Получаем

$$\text{НОД}(u(x), v[2](x) - 0) = x^5 + 5x^4 + 9x^3 + 5x + 5$$

$$\text{НОД}(u(x), v[3](x) - 2) = x^3 + 8x^2 + 4x + 12$$

При всех s отличных от 0 и 2 получаем НОД$(u(x), v[2](x) - s) = 1$. Поскольку размерность пространства решений $r = 3$, продолжаем поиск неприводимых множителей. Находи, что при $s = 6$

$$\text{НОД}(v[3](x) - s, x^5 + 5x^4 + 9x^3 + 5x + 5) = x^4 + 2x^3 + 3x^2 + 4x + 6$$

при $s = 8$

$$\text{НОД}(v[3](x) - s, x^5 + 5x^4 + 9x^3 + 5x + 5) = x + 3,$$

при остальных значениях s этот НОД равен 1.

Таким образом, мы нашли все три неприводимых сомножителя, на которые исходный многочлен $u(x)$ разлагается в поле вычетов по модулю 13.

Алгоритм 2.2 (Цассенхауз) Данные: Многочлен $f(x) \in F[x]$ без кратных корней.

Найти: Разложение $f(x)$ на неприводимые множители над полем F.

1. Вычислить матрицу B, число k и многочлены $h_1(x) = 1, h_2(x), \ldots, h_k(x)$, как в алгоритме Берлекемпа. Положить $M = \{f(x)\}$.

2. Для каждого $j = 2, \ldots, k$ проделать следующие операции.

2.1 Вычислить наименьшееd такое,что векторы

$$\vec{c_l} = (c_{l,0}, \ldots, c_{l,n-1}) \in F^n, \quad l = 0, \ldots, d,$$

определенные сравнениями

$$h_j(x)^l = \sum_{i=0}^{n-1} c_{l,i} x^i \qquad (\mathrm{mod}\ f(x))$$

линейно зависимы над F.

2.2 Вычислить коэффициенты $b_0, \ldots, b_d \in F$ такие, что

$$b_0\vec{c}_0 + \cdots + b_d\vec{c}_d = 0, \qquad d_d = 1.$$

Обозначить $g_j(y) = b_0 + b_1 y + \cdots + b_d y^d$.

2.3 Найти множество $\mathcal{R}_j$ корней многочлена $g_j(y)$, принадлежащих F.

2.4 Для каждого $c \in \mathcal{R}_j$ и каждого $u \in M$ вычислить

$$p(x) = (u(x), h_j(x) - c)$$

и, если $1 \leqslant \deg p(x) < \deg u(x)$, исключить $u(x)$ из M и заменить его парой многочленов $p(x),\ u(x)/p(x)$.

2.5 Если мощность $M = k$, СТОП. Множество M содержит все неприводимые делители $f(x)$.

Приведенный выше алгоритм отличается от алгоритма 2.1 лишь тем, что в нем вычисляются многочлены $p(x) = (u(x), h_j(x) - c)$ только в том случае, когда $c \in \mathcal{R}_j$,т.е. когда $p(x) \neq 1$. Обоснование его справедливо совпадает с обоснование для алгоритма 2.1. Сложность алгоритма 2.2, сводящего задачу разложения на множители к вычислению корней в том же поле, есть, как легко видеть, $O(n^2(k^2 + \ln q))$.

Алгоритм 2.2. сводит задачу разложения $f(x) \in F[x]$ на неприводимые над F множители к нахождению корней в поле F некоторой совокупности многочленов $g_j(x) \in F[x]$.

Раздел 3. В этом разделе мы рассмотрим методы решения систем линейных уравнений над конечными полями, наиболее часто используемые в современных алгоритмах факторизации и дискретного логарифмирования. Кроме того мы опишем методы решения систем линейных уравнений в целых числах. Основные алгоритмы:

Алгоритм Ланцоша: Алгоритм Ланцоша работает следующим образом. Мы вычисляем последовательность векторов $\boldsymbol{\omega}_0 = \boldsymbol{b}, \boldsymbol{\omega}_1, \boldsymbol{\omega}_2, \ldots,$ пользуясь

формулами (3.20 ($\begin{cases} \boldsymbol{\omega}'_0 = \boldsymbol{s}_0 = \boldsymbol{b}, \\ \boldsymbol{\omega}'_1 = A\boldsymbol{\omega}'_0 - \lambda_{10}\boldsymbol{\omega}'_0, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \boldsymbol{\omega}'_i = A\boldsymbol{\omega}'_{i-1} - \sum\limits_{j=0}^{i-1} \alpha_{ij}\boldsymbol{\omega}'_j, \\ \cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$)), (3.22 ($\alpha'_{ij} = \frac{(A\boldsymbol{\omega}'_{i-1}, \boldsymbol{\omega}'_j)_A}{(\boldsymbol{\omega}'_j, \boldsymbol{\omega}'_j)_A}$.)), (3.24 ($\boldsymbol{\omega}_I = A\boldsymbol{\omega}_{i-1} - \frac{(\boldsymbol{\omega}_{i-1}, A\boldsymbol{\omega}_{i-1})_A}{(\boldsymbol{\omega}_{i-1}, \boldsymbol{\omega}_{i-1})_A}\boldsymbol{\omega}_{i-1} - \frac{(\boldsymbol{\omega}_{i-1}, A\boldsymbol{\omega}_{i-2})_A}{(\boldsymbol{\omega}_{i-2}, A\boldsymbol{\omega}_{i-2})_A}\boldsymbol{\omega}_{i-2},$)). если на некотором шаге будет построен вектор $\boldsymbol{\omega}_i \neq 0$ такой, что $(\boldsymbol{\omega}_i, \boldsymbol{\omega}_i)_A = 0$, то мы не сможем найти решение (3.12 ($A\boldsymbol{x} = \boldsymbol{b}$)) этим методом. Если же будет построен вектор $\boldsymbol{\omega}_m = 0$, то решение $\boldsymbol{x}$ мы находим по формуле (3.18 ($\boldsymbol{x} = \sum\limits_{i=0}^{r} \frac{(\boldsymbol{\omega}_i, \boldsymbol{b})}{(\boldsymbol{\omega}_i, \boldsymbol{\omega}_i)}\boldsymbol{\omega}_i$)) при $r = m - 1$.

Алгоритм Видемана:

Алгоритм 1.

1 шаг: Присвоить $\boldsymbol{b}_0 := \boldsymbol{b},\ k := 0,\ \boldsymbol{y}_0 := 0,\ d_0 := 0.$

2 шаг: Если $\boldsymbol{b}_k = 0$, то решение (3.26 ($A\boldsymbol{x} = \boldsymbol{b}, \quad \boldsymbol{b} \neq 0$)) равно $\boldsymbol{x} = -\boldsymbol{y}_k$, и алгоритм завершает работу.

3 шаг: Выбрать случайный вектор $\boldsymbol{u}_{k+1} \in \mathbb{K}^n, \boldsymbol{u}_{k+1} \neq 0.$

4 шаг: Вычислить первые $2(n - d_k)$ членов последовательности $\left\{(\boldsymbol{u}_{k+1}, A^i\boldsymbol{b}_k)\right\}_{i=0,1,2,\ldots}$

5 шаг: С помощью алгоритма Берлекэмпа–Месси вычислить минимальный многочлен $f_{k+1}(z)$ последовательности шага 4, нормализованный так, что бы его свободный член равнялся 1.

6 шаг: Присвоить

$$\boldsymbol{y}_{k+1} := \boldsymbol{y}_k + \hat{f}_{k+1}(A)\boldsymbol{b}_k,$$

$$\boldsymbol{b}_{k+1} := \boldsymbol{b}_0 + A\boldsymbol{y}_{k+1},$$

$$d_{k+1} := d_{k+1} + \deg f_{k+1}(z).$$

7 шаг: Присвоить $k := k + 1$ и вернуться на шаг 2.

Конец алгоритма.

Алгоритм 2.

1 шаг: Вычислить $A^i\boldsymbol{b},\ i = 0, 1, \ldots, 2n - 1.$

2 шаг: Присвоить $k := 0, g_0(z) := 1.$

3 шаг: Присвоить $\boldsymbol{u}_{k+1} := (0, \ldots, 0, 1, 0, \ldots, 0)$ (единица стоит на $k+1$-м месте).

4 шаг: Используя результаты 1-ого шага, вычислить последовательность

$$(\boldsymbol{u}_{k+1}, A^i\boldsymbol{b}), \quad i = 0, 1, \ldots, 2n-1.$$

5 шаг: Вычислить последовательность

$$(\boldsymbol{u}_{k+1}, g_k(A))A^i\boldsymbol{b}), \quad i = 0, 1, \ldots, 2n-1-\deg g_k(z).$$

6 шаг: Найти (с помощью Берлекэипа–Месси) минимальный многочлен $f_{k+1}(z)$ для последовательности, полученной на 5-ом шаге (свободный член $f_{k+1}(z)$ равен 1).

7 шаг: Присвоить $g_{k+1}(z) := f_{k+1}(z)g_k(z)$.

8 шаг: Присвоить $k := k+1$. Если $\deg g_k(z) < n$ и $k < n$, то идти на 3-й шаг.

9 шаг: Для многочлена $f(z) = g_k(z)$ с помощью найденных на 1-м шаге значений $A^i\boldsymbol{b}$ найти решение $\boldsymbol{x}$ системы (3.26 ($A\boldsymbol{x} = \boldsymbol{b}, \quad \boldsymbol{b} \neq 0$)) по формуле (3.27 ($\boldsymbol{x} = -\sum\limits_{i=1}^{d} f[i]A^{i-1}\boldsymbol{b}$)).

Конец алгоритма.

ЗАКЛЮЧЕНИЕ

В настоящей работе был рассмотрен один из разделов теории чисел: разложение многочленов на множители над конечными полями, приведены соответствующие алгоритмы. В данной работе первая глава посвящена основным определениям и понятиям. Во второй главе, которая занимает центральное место в работе, мы рассмотрели несколько алгоритмов разложения многочленов на множители над конечными полями. В последней третьей главе мы рассмотрели методы решения систем линейных уравнений, наиболее часто используемые в современных алгоритмах факторизации и дискретного логарифмирования, последние рекорды в области дискретного логарифмирования в простых полях были достигнуты с помощью алгоритма Ланцоша, который приводится в данной главе. Таким образом, основная цель данной работы — познакомиться с теорией чисел, а именно с таким разделом, как разложение многочленов на множители над конечными полями, показать разнообразие алгоритмов, использующиеся в теории чисел была достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 О.Н. Герман, Ю.В. Нестеренко, Теоретико — числовые методы в криптографии.

2 С.Г. Гандикин, Малая теорема Ферма. — МЦНМО Редакция журнала «Квант».

3 О.Н. Василенко, Теоретико — Числовые Алгоритмы В Криптографии. — М.: МЦНМО, 2003.

4 Е.В. Панкратьев, А.Е. Панкратьев, Алгебраические алгоритмы и их сложность. — Механико-математический факультет МГУ.

5 Д. Кнут, Искуство программирования на ЭВМ. Т.2, Получисленные алгоритмы. — Москва: Мир. 1977.

6 Лидл Р., Нидеррайтер Г. Конечные поля: в 2х томах. Т.1. Пер. с англ. — М.: Мир,1988.

7 Лидл Р., Нидеррайтер Г. Конечные поля: в 2х томах. Т.2. Пер. с англ. — М.: Мир,1988.

8 Н. Коблиц, Курс теории чисел и криптографии. — Москва: Научное изд-во ТВП, 2001.

9 Ю.В. Нестеренко, Теория чисел. — М.: Издательский центр «Академия», 2008.

10 А.Г. Ростовцев, Е.Б. Маховенко, Теоретическая криптография. — НПО «Профессионал» , Санкт-Петербург.

11 Р. Блейхут, Теория и практика кодов, контролирующие ошибки. Перевод с английского : И.И. Грушко, В.М. Блиновский. Под редакцией: К.Ш. Загангирова — М.: Мир, 1986.

12 А.А. Бухштаб, Теория чисел. — «Просвещение», Москва.

13 А.И. Мальцев, Основы линейной алгебры.

14 Б. Л. Ван-дер-Варден, Алгебра. — М.: Мир, 1975.

15 З.И. Боревич, И.Р. Шафаревич, Теория чисел. — М.: Наука, 1985.

16 Ю.В. Нестеренко, Теория чисел, 2008.

17 А.Г. Курош, Курс высшей алгебры. — М.: Наука, 1965.

18 Н. Коблиц, Р-адические числа, р-адический анализ и дзета-функции. — Мир, 1982.

19 И.М. Виноградов, Основы теории чисел. — М.-Л., Гостехиздат, 1952.

20 Д. Кокс, Дж. Литтл, Д. О’ши, Идеалы,многообразия и алгоритмы. — Перевод на русский язык «Мир», 2000.