

ОГЛАВЛЕНИЕ

Предисловие	11
-------------------	----

Часть I. Решение линейных систем уравнений

Введение	14
----------------	----

Глава 1. Скалярные алгоритмы и приближения Паде	17
---	----

1.1. Приближения Паде	17
-----------------------------	----

1.1.1. Алгоритм Евклида	19
-------------------------------	----

1.1.2. Подходящие дроби как решения систем линейных уравнений	21
--	----

1.1.3. Промежуточные дроби	23
----------------------------------	----

1.1.4. Алгоритм Берлекемпа – Мессис	26
---	----

1.2. Алгоритм Видемана	29
------------------------------	----

1.2.1. Алгоритм Видемана и приближения Паде	29
---	----

1.3. Алгоритм Ланцоша	31
-----------------------------	----

1.3.1. Алгоритм Ланцоша и приближения Паде	35
--	----

1.3.2. Схема Горнера и ортогональные многочлены	43
---	----

Глава 2. Блочный алгоритм Видемана – Копперсмита	51
--	----

2.1. Описание алгоритма	51
-------------------------------	----

2.2. Построение матричных приближений Паде	53
--	----

2.2.1. Приведенный базис	57
--------------------------------	----

2.2.2. Сдвиг степеней	62
-----------------------------	----

2.3. Вероятность получения ненулевого решения	64
---	----

2.3.1. Обзор многомерного случая	65
--	----

2.3.2. Одномерный случай	68
--------------------------------	----

Глава 3. Параллельные алгоритмы Видемана и Ланцоша	76
--	----

3.1. Краткое описание алгоритмов	76
--	----

3.1.1. Алгоритм Видемана	76
--------------------------------	----

3.1.2. Алгоритм Ланцоша	77
3.1.3. Блочные алгоритмы над полем $GF(2)$	78
3.1.4. Вычислительные вопросы	79
3.2. Последовательные версии алгоритмов.	80
3.2.1. Алгоритмы Видемана	80
3.2.2. Алгоритмы Ланцоша	82
3.3. Параллельные версии алгоритмов.	84
3.3.1. Параллельное умножение матрицы на вектор.	85
3.3.2. Параллельный алгоритм Видемана	94
3.3.3. Параллельный алгоритм Ланцоша	96
3.4. Некоторые замечания.	97

Часть II. Алгоритм просеивания и его применения

Введение	100
Глава 1. Разложение на множители больших чисел	102
1.1. Алгоритм факторизации методом решета числового поля	102
1.2. Порядок A и его свойства	105
1.2.1. Простые идеалы первой степени в кольце A	109
1.2.2. Показатели	111
1.2.3. Расширение идеалов кольца A	118
1.3. Оценка индекса порядка A	122
1.4. Обоснование алгоритма	132
1.5. Извлечение квадратного корня в поле алгебраических чисел	135
Глава 2. Алгоритм дискретного логарифмирования	142
2.1. λ -функции и виртуальные логарифмы.	143
2.1.1. λ -функции	143
2.1.2. Чистая образующая главного идеала	145
2.1.3. Определение виртуального логарифма идеала	147
2.1.4. Основная теорема	148
2.2. Алгоритм дискретного логарифмирования методом решета числового поля	152
2.3. Комментарии и обоснование алгоритма.	157
2.3.1. Разложение простых чисел в произведение простых идеалов	157
2.3.2. Уравнения системы	158
2.3.3. Вычисление индивидуальных логарифмов	159

Глава 3. Просеивание	164
3.1. Просеивание на решетках	164
Глава 4. Выбор многочленов	171
4.1. Характеристики многочленов	173
4.1.1. Размер многочлена	173
4.1.2. Гладкость многочлена	174
4.1.3. Функции Мерфи E и e	177
4.2. Классические алгоритмы	178
4.2.1. Разложение по основанию m	178
4.2.2. Алгоритм Монтгомери	179
4.3. Современные алгоритмы	181
4.3.1. Алгоритм Монтгомери – Мерфи	181
4.3.2. Алгоритм Кляйнюнга	183
4.3.3. Оптимизация многочленов	189
 Часть III. Эллиптические кривые над полем рациональных чисел	
Введение	193
Глава 1. Рациональные точки на эллиптических кривых	196
1.1. Основные определения	196
1.2. Точки кручения	199
1.3. Высоты и их свойства	211
1.4. Редукция по простому модулю	218
Глава 2. Нахождение ранга эллиптической кривой	222
2.1. Алгоритм Берча – Суиннертон-Дайера и его обоснование	222
2.2. Реализация алгоритма Берча – Суиннертона-Дайера	232
2.2.1. Отыскание 2-накрытий	232
2.2.2. Отбор неэквивалентных 2-накрытий	232
2.2.3. Поиск p -адических точек на 2-накрытиях	235
2.2.4. Поиск рациональных точек на 2-накрытиях и эллиптических кривых	237
Глава 3. Построение базиса группы рациональных точек	242
3.1. Общая схема алгоритма	242

3.2. Нахождение высот рациональных точек	243
3.2.1. Разложение канонической высоты в сумму локальных высот	243
3.2.2. Вычисление локальной высоты в архимедовом случае	246
3.2.3. Замена параметра	248
3.2.4. Оценка ошибки при вычислении локальной высоты	253
3.2.5. Вычисление локальной высоты в неархимедовом случае	257
3.3. Работа с 2-накрытиями	259
3.4. Факторгруппа $E(\mathbb{Q})/2E(\mathbb{Q})$	261
3.5. Оценка нижней границы высот рациональных точек	263
3.5.1. Вычисление эллиптических логарифмов	264
3.5.2. Вычисление суммы $D_E(n)$	274
3.5.3. Вычисление константы α	277
3.5.4. Основной алгоритм	280
3.6. Выделение базиса из полного набора независимых точек	283
3.7. Поиск рациональных корней многочленов	288
Глава 4. Задача дискретного логарифмирования на эллиптической кривой	291
Введение	291
4.1. Обзор некоторых методов	292
4.2. Исчисление “xedni”	297
Список литературы	303