

ОГЛАВЛЕНИЕ

Предисловие	3
Введение	4
Глава 1. Элементы теории чисел	7
1.1. Делимость целых чисел. Алгоритм Евклида	7
1.2. Простые числа, основная теорема арифметики	11
1.3. Функция Эйлера и ее свойства	13
1.4. Сравнения	14
1.5. Сравнения с одним неизвестным	17
1.6. Первообразные корни и индексы	22
1.7. Цепные дроби	26
1.8. p -адические числа	32
1.9. Алгебраические числа	42
Глава 2. Быстрые алгоритмы	51
2.1. Алгоритм Евклида	51
2.2. Символы Лежандра и Якоби	53
2.3. Быстрый алгоритм возведения в степень	58
2.4. Вероятностные алгоритмы	60
2.5. Решение квадратичных сравнений (алгоритм Шенкса)	64
2.6. Вероятностные методы отсеивания составных чисел	67
2.7. Быстрые алгоритмы умножения и деления целых чисел	79
Глава 3. Разложение многочленов на множители над конечными полями	91
3.1. Алгоритм Берлекемпа	92
3.2. Сведение задачи разложения на неприводимые множители к нахождению корней (алгоритм Цассенхауза)	96
3.3. Нахождение корней многочленов в полях малой характеристики	99
3.4. Нахождение корней многочленов в полях большой характеристики	102
Глава 4. Алгоритмы, распознающие простоту чисел	106
4.1. Условный алгоритм Миллера	106
4.2. $(N - 1)$ -методы доказательства простоты чисел	110
4.3. Построение больших простых чисел	116
4.4. $(N + 1)$ -методы доказательства простоты чисел	120

4.5. Алгоритм Коэна — Ленстры	128
4.6. Полиномиальный алгоритм проверки чисел на простоту . . .	150
Глава 5. Разложение целых чисел на множители	161
5.1. Алгоритмы экспоненциальной сложности	162
5.2. Субэкспоненциальные алгоритмы	172
5.3. Общий алгоритм просеивания в полях алгебраических чисел	189
Глава 6. Дискретное логарифмирование	201
6.1. Метод Гельфонда	201
6.2. Метод Полига — Хеллмана	203
6.3. Линейное решето	206
Глава 7. LLL-алгоритм и его применения	209
7.1. Решетки	209
7.2. LLL-алгоритм	219
7.3. Применения LLL-алгоритма	228
Глава 8. Криптографические применения	246
8.1. Алгоритм Диффи — Хеллмана обмена ключами	247
8.2. Алгоритм RSA	248
8.3. Электронная цифровая подпись	250
8.4. Об уязвимости системы RSA	251
Упражнения	259
Список литературы	268