Предисловие
Введение
Глава 1. Элементы теории чисел
1.1. Делимость целых чисел. Алгоритм Евклида
1.2. Простые числа, основная теорема арифметики
1.3. Функция Эйлера и ее свойства
1.4. Сравнения
1.5. Сравнения с одним неизвестным
1.6. Первообразные корни и индексы
1.7. Цепные дроби
1.8. p-адические числа
1.9. Алгебраические числа
Глава 2. Быстрые алгоритмы
2.1. Алгоритм Евклида
2.2. Символы Лежандра и Якоби
2.3. Быстрый алгоритм возведения в степень
2.4. Вероятностные алгоритмы
2.5. Решение квадратичных сравнений (алгоритм Шенкса)
2.6. Вероятностные методы отсеивания составных чисел
2.7. Быстрые алгоритмы умножения и деления целых чисел
Глава 3. Разложение многочленов на множители
над конечными полями
3.1. Алгоритм Берлекемпа
3.2. Сведение задачи разложения на неприводимые множители
к нахождению корней (алгоритм Цассенхауза)
3.3. Нахождение корней многочленов в полях малой
характеристики
3.4. Нахождение корней многочленов в полях большой
характеристики
Глава 4. Алгоритмы, распознающие простоту чисел
4.1. Условный алгоритм Миллера
4.2. (N − 1)-методы доказательства простоты чисел
4.3. Построение больших простых чисел
4.4. (N + 1)-методы доказательства простоты чисел
4.5. Алгоритм КоэнаЛенстры
4.6. Полиномиальный алгоритм проверки чисел на простоту
Глава 5. Разложение целых чисел на множители
5.1. Алгоритмы экспоненциальной сложности
5.2. Субэкспоненциальные алгоритмы
5.3. Общий алгоритм просеивания в полях алгебраических чисел
Глава 6. Дискретное логарифмирование
6.1. Метод Гельфонда
6.2. Метод ПолигаХеллмана
6.3. Линейное решето
Глава 7. LLL-алгоритм и его применения
7.1. Решетки
7.2. LLL-алгоритм
7.3. Применения LLL-алгоритма
Глава 8. Криптографические применения
8.1. Алгоритм ДиффиХеллмана обмена ключами
8.2. Алгоритм RSA
8.3. Электронная цифровая подпись
8.4. Об уязвимости системы RSA
Список литературы