

ВЫСШЕЕ ОБРАЗОВАНИЕ

ВВЕДЕНИЕ В ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

М. М. Глухов
И. А. Круглов
А. Б. Пичкур
А. В. Черемушкин



E.LANBOOK.COM

ОГЛАВЛЕНИЕ

Введение	5
<i>Глава 1</i>	
Оценка сложности арифметических операций	8
1.1. Сложность арифметических операций с целыми числами	8
1.1.1. Сложность базовых целочисленных алгоритмов	9
1.1.2. Быстрые алгоритмы умножения чисел	14
1.1.3. Алгоритм возведения в степень	15
1.2. Сложность вычисления наибольшего общего делителя чисел	16
1.2.1. Алгоритм Евклида нахождения наибольшего общего делителя двух чисел	16
1.2.2. Расширенный алгоритм Евклида	18
1.2.3. Другие алгоритмы вычисления наибольшего общего делителя	19
1.3. Сложность арифметических операций в кольцах вычетов	22
1.3.1. Стандартные алгоритмы	22
1.3.2. Алгоритм Монгмери	22
Алгоритм 1.1	23
Алгоритм 1.2	24
1.3.3. Использование китайской теоремы об остатках	28
<i>Глава 2</i>	
Решение уравнений в кольцах вычетов	32
2.1. Строение мультипликативной группы кольца вычетов	32
2.1.1. Критерий цикличности мультипликативной группы кольца вычетов	32
2.1.2. Первообразные корни по модулю N	36
2.2. Решение уравнений в кольцах вычетов	40
2.2.1. Сведение к простому модулю	40

2.2.2.	Случай простого модуля	43
	Алгоритм 2.1	43
2.3.	Исследование квадратных сравнений. Квадратичные вычеты и невычеты	47
	Алгоритм 2.2	54
2.4.	Решение некоторых типов уравнений в кольцах вычетов	55
2.4.1.	Извлечение квадратного корня в кольцах вычетов	55
	Алгоритм 2.3	56
	Алгоритм 2.4	59
	Алгоритм 2.5	62
	Алгоритм 2.6	63
2.4.2.	Извлечение корня в кольцах вычетов	64
	Алгоритм 2.7	66
	Алгоритм 2.8	68
2.4.3.	Показательные сравнения. Сведение к простому модулю	69
<i>Глава 3</i>		
	Цепные дроби	74
3.1.	Представление действительных чисел цепными дробями	74
3.1.1.	Конечные и бесконечные цепные дроби и их свойства	74
3.1.2.	Представление действительных чисел цепными дробями над \mathbb{Z}	79
3.2.	Представление квадратичных иррациональностей периодическими цепными дробями	82
3.3.	Приложения цепных дробей	91
3.3.1.	Подходящие дроби как наилучшие приближения	91
3.3.2.	Применение цепных дробей к решению линейных сравнений	94
3.3.3.	Применение цепных дробей к решению уравнения Пелля	96
<i>Глава 4</i>		
	Простые числа	102
4.1.	Характеры конечных абелевых групп и суммы Гаусса	102
4.1.1.	Характеры конечных полей и суммы Гаусса	102
4.1.2.	Доказательство квадратичного закона взаимности	108
4.1.3.	Приложение характеров и сумм Гаусса к нахождению оценок числа решений уравнений над конечными полями	110
4.2.	Распределение простых чисел в натуральном ряду	114
4.2.1.	Теорема Чебышева	114

4.2.2.	Понятие об аналитических методах в теории чисел	121
4.2.3.	Теорема Мертенса	126
4.3.	Критерии простоты.	
	Числа Ферма и числа Мерсенна	131
4.3.1.	Критерии простоты	131
4.3.2.	Числа Ферма и числа Мерсенна	143
<i>Глава 5</i>		
	Проверка простоты целых чисел	146
5.1.	Вероятностные тесты простоты	146
5.1.1.	Тест простоты на основе малой теоремы Ферма	147
	Алгоритм 5.1	147
5.1.2.	Тест Соловея–Штрассена	152
	Алгоритм 5.2	152
5.1.3.	Тест Миллера–Рабина	155
	Алгоритм 5.3	155
5.2.	Полиномиальный тест распознавания простоты	161
	Алгоритм 5.4	162
5.3.	Применение характеров и сумм Гаусса для проверки простоты целых чисел	166
	Алгоритм 5.5	176
5.4.	Построение больших простых чисел	181
	Алгоритм 5.6	181
5.4.1.	Теорема Поклинттона	184
5.4.2.	Метод Маурера генерации простых чисел	188
5.4.3.	Сильно простые числа	193
<i>Глава 6</i>		
	Разложение целых чисел на множители	196
6.1.	Экспоненциальные алгоритмы факторизации	199
6.1.1.	Метод пробных делений	199
6.1.2.	ρ -метод Полларда	200
	Алгоритм 6.1	201
	Алгоритм 6.2	201
6.1.3.	Метод Ферма	205
	Алгоритм 6.3	206
6.1.4.	$(p - 1)$ -метод Полларда	207
	Алгоритм 6.4	207
6.1.5.	$(p + 1)$ -метод Вильямса	209
	Алгоритм 6.5	210
6.2.	Субэкспоненциальные алгоритмы факторизации	211
6.2.1.	Алгоритм Диксона	216
	Алгоритм 6.6	216
6.2.2.	Алгоритм Бриллихарт–Моррисона	222
6.2.3.	Метод решета построения B -гладких чисел	225
	Алгоритм 6.7	226
6.2.4.	Метод квадратичного решета	230
	Алгоритм 6.8	231

Глава 7

Эллиптические кривые	240
7.1. Эллиптические кривые над конечными полями	240
Алгоритм 7.1	250
Алгоритм 7.2	251
7.2. Эллиптические конфигурации	256
7.3. Факторизация целых чисел с помощью эллиптических кривых	262
Алгоритм 7.3	265
7.4. Проверка целых чисел на простоту с помощью эллиптических кривых	272
Алгоритм 7.4	273

Глава 8

Методы вычисления дискретных логарифмов	279
8.1. Алгоритмы дискретного логарифмирования в произвольной конечной циклической группе	280
8.1.1. Алгоритм Гельфонда–Шенкса	280
Алгоритм 8.1	280
8.1.2. Метод сведения к собственным подгруппам	282
8.1.3. Метод Сильвера–Полига–Хеллмана	284
Алгоритм 8.2	285
8.1.4. ρ -метод Полларда и его распараллеливание	289
Алгоритм 8.3	290
Алгоритм 8.4	295
8.2. Алгоритмы дискретного логарифмирования в конечном простом поле	297
8.2.1. Индекс-метод логарифмирования в конечном простом поле	297
Алгоритм 8.5	298
8.2.2. Метод линейного решета	305
Первый этап метода линейного решета	307
Алгоритм 8.6	307
Второй этап метода линейного решета	311
Алгоритм 8.7	313
Модификация первого этапа метода линейного решета	316
Алгоритм 8.8	316
8.3. Алгоритмы дискретного логарифмирования в конечном неп простом поле	320
Алгоритм 8.9	320
Метод Д. Копперсмита логарифмирования в полях $GF(2^n)$	322

Глава 9

Методы геометрии чисел	326
9.1. Решетки в евклидовом пространстве	326
9.1.1. Основные определения	326
9.1.2. Целочисленные решетки и матрицы	331
Алгоритм 9.1	336
9.2. Редуцированный по Минковскому базис решетки	340

9.2.1. Редуцированный по Минковскому базис решетки	340
Алгоритм 9.2	342
9.2.2. Редукция решеток размерности 2. Алгоритм Гаусса	343
Алгоритм 9.3	343
9.2.3. Редукция решеток размерности 3	347
Алгоритм 9.4	347
9.3. Последовательные минимумы. Теорема Минковского о выпуклом теле	351
9.3.1. Последовательные минимумы	351
9.3.2. Теорема Минковского о выпуклом теле	358
9.4. LLL-алгоритм и его приложения	362
9.4.1. Алгоритм Ловаца (LLL-алгоритм)	362
Алгоритм 9.5	365
9.4.2. Приложения алгоритма Ловаца	370
1. Вычисление кратчайшего вектора решетки	370
2. Целочисленное линейное программирование с ограниченным числом неизвестных	372
Алгоритм 9.6	372
3. Алгоритм Бабаи	378
Алгоритм 9.7	378
Список литературы	382