

ОГЛАВЛЕНИЕ

Введение	7
Глава 1. О делимости чисел	12
1.1. Свойства делимости целых чисел	13
1.2. Наименьшее общее кратное и наибольший общий делитель	15
1.3. Алгоритм Евклида	19
1.4. Решение в целых числах линейных уравнений ..	23
Глава 2. Простые и составные числа	36
2.1. Простые числа. Решето Эратосфена. Бесконечность множества простых чисел	36
2.2. Основная теорема арифметики	39
2.3. Теоремы Чебышёва	50
2.4. Дзета-функция Римана и свойства простых чисел .	59
Глава 3. Арифметические функции	69
3.1. Мультипликативные функции и их свойства	69
3.2. Функция Мёбиуса и формулы обращения	71
3.3. Функция Эйлера	76
3.4. Сумма делителей и число делителей натурального числа	78
3.5. Оценки среднего значения арифметических функций	80
Глава 4. Числовые сравнения	87
4.1. Сравнения и их основные свойства	87
4.2. Классы вычетов. Кольцо классов вычетов по данному модулю	89
4.3. Полная и приведённая системы вычетов	94
4.4. Теорема Вильсона	95
4.5. Теоремы Эйлера и Ферма	96

4.6. Представление рациональных чисел бесконечными десятичными дробями	98
4.7. Проверка на простоту и построение больших простых чисел	100
4.8. Разложение целых чисел на множители и криптографические применения	112
Глава 5. Сравнения с одним неизвестным	116
5.1. Основные определения	116
5.2. Сравнения первой степени	118
5.3. Китайская теорема об остатках	120
5.4. Полиномиальные сравнения по простому модулю	124
5.5. Полиномиальные сравнения по составному модулю	131
Глава 6. Сравнения второй степени	137
6.1. Сравнения второй степени по простому модулю . .	137
6.2. Символ Лежандра и его свойства	139
6.3. Квадратичный закон взаимности	141
6.4. Символ Якоби и его свойства	147
6.5. Суммы двух и четырёх квадратов	150
6.6. Представление нуля квадратичными формами от трёх переменных	157
Глава 7. Первообразные корни и индексы	164
7.1. Показатель числа по заданному модулю	164
7.2. Существование первообразных корней по простому модулю	166
7.3. Построение первообразных корней по модулям p^k и $2p^k$	170
7.4. Теорема об отсутствии первообразных корней по модулям, отличным от 2, 4, p^k и $2p^k$	173
7.5. Индексы и их свойства	176
7.6. Дискретное логарифмирование	180
7.7. Двучленные сравнения	187
Глава 8. Цепные дроби	191
8.1. Теорема Дирихле о приближении действительных чисел рациональными	193

8.2. Конечные цепные дроби	195
8.3. Цепная дробь действительного числа	199
8.4. Наилучшие приближения	205
8.5. Эквивалентные числа	208
8.6. Квадратичные иррациональности и цепные дроби	212
8.7. Использование цепных дробей для решения некоторых диофантовых уравнений	217
8.8. Разложение числа e в цепную дробь	227
Глава 9. Алгебраические и трансцендентные числа . . .	231
9.1. Поле алгебраических чисел	231
9.2. Приближения алгебраических чисел рациональными. Существование трансцендентных чисел	239
9.3. Иррациональность чисел e^r и π	245
9.4. Трансцендентность числа e	249
9.5. Трансцендентность числа π	251
9.6. Невозможность квадратуры круга	258
Глава 10. Решение задач в Wolfram Mathematica	264
10.1. Уравнения, неравенства и сравнения	265
10.1.1. Диофантовы уравнения и неравенства	265
10.1.2. Целочисленное программирование	272
10.1.3. Сравнения	273
10.1.4. Решение сравнений	276
10.1.5. Системы сравнений	277
10.2. Простые и составные числа	279
10.2.1. Простые числа	279
10.2.2. Генерация больших простых чисел	282
10.2.3. Разложение чисел на множители	284
10.3. Теоретико-числовые функции	285
10.3.1. Элементарные функции	285
10.3.2. Суммы по делителям: число делителей и суммы их степеней	287
10.3.3. Функция Мёбиуса	289
10.3.4. Функция Эйлера	290
10.3.5. Показатель числа и первообразные корни	292
10.4. Диофантовы приближения	293
10.4.1. Цепные дроби	294
10.4.2. Разложение чисел в цепные дроби	294

10.4.3. Цепные дроби квадратичных иррациональностей .	296
10.4.4. Разложение алгебраических чисел степени, большей 2	298
10.4.5. Разложение трансцендентных чисел	299
10.5. Алгебраические числа	301
10.5.1. Задание алгебраических чисел, радикалы, арифметические операции, минимальный многочлен и степень	301
10.5.2. Поле алгебраических чисел	304
Ответы и указания	312
Литература	316