

УДК 519.7
ББК 22.176
A18

Рецензенты:

Калягин В. А. — доктор физико-математических наук, профессор НИУ ВШЭ
Ульянов М. В. — доктор технических наук, профессор,
 ведущий научный сотрудник института проблем управления
 им. В. А. Трапезникова РАН

Научный редактор:

Захаров В. А. — доктор физико-математических наук,
 профессор МГУ им. М. В. Ломоносова

Авдошин С. М., Набебин А. А.
 А18 Дискретная математика. Модулярная алгебра, криптография, кодирование. — М.: ДМК Пресс, 2017. — 352 с.: ил.

ISBN 978-5-97060-408-3

Книга содержит необходимые сведения из универсальных и классических алгебр, системы аксиом для основных алгебраических структур (группоид, моноид, полугруппы, группы, частичные порядки, кольца, поля). Описываются основные криптографические алгоритмы. Рассматриваются ставшие классическими помехоустойчивые коды — линейные, циклические, БЧХ. Приводятся алгоритмы проектирования таких кодов.

В основу книги положен многолетний опыт преподавания авторами дисциплины «Дискретная математика» на факультете бизнес-информатика, на факультете компьютерных наук Национального исследовательского университета Высшая школа экономики и на факультете автоматизации и вычислительной техники Национального исследовательского университета Московский энергетический институт.

Книга предназначена для студентов бакалавриата, обучающихся по направлениям 09.03.01 «Информатика и вычислительная техника», 09.03.02 «Информационные системы и технологии», 09.03.03 «Прикладная информатика», 09.03.04 «Программная инженерия», а также для ИТ-специалистов и разработчиков программных продуктов.

УДК 519.7
ББК 22.176

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-5-97060-408-3

© Авдошин С. М., Набебин А. А., 2017
 © Оформление, издание, ДМК Пресс, 2017

Содержание

Предисловие	11
Введение	13
1. Множество	13
2. Функция	14
3. Отношение	16
4. Отношение эквивалентности	17
5. Каноническое разложение функции.....	18
6. Мощность множества. Счетные и несчетные множества	19
7. Мощность континуума	20
8. Кардинальные числа. Сравнение мощностей.....	21
Часть I. МОДУЛЯРНАЯ АЛГЕБРА	25
Глава 1. Делимость	26
1.1. Позиционная система счисления	26
1.2. Простые числа	28
1.3. Факторизация целых чисел	29
1.4. Наибольший общий делитель.....	30
1.4.1. Алгоритм Евклида вычисления наибольшего общего делителя.....	31
1.4.2. Расширенный алгоритм Евклида вычисления наибольшего общего делителя	34
1.5. Наименьшее общее кратное.....	35
1.6. Непрерывные (цепные) и подходящие дроби.....	37
1.6.1. Вычисление подходящих дробей.....	38
1.6.2. Алгоритм вычисления подходящих дробей	39
Глава 2. Функции Мебиуса и Эйлера	41
2.1. Функции $\lfloor x \rfloor$, $ x $, $\{x\}$ для вещественного x	41
2.2. Мультипликативные функции	42
2.3. Функция и формула обращения Мебиуса	43
2.4. Функция Эйлера	47
Глава 3. Сравнения	49
3.1. Сравнение целых чисел.....	49
3.2. Свойства сравнений	49
3.3. Полная система вычетов.....	51

4 ❖ Содержание

Операции над классами	51
3.4. Приведенная система вычетов.....	53
3.5. Теоремы Эйлера и Ферма.....	54
3.6. Классы целых чисел по модулю m , взаимно простых с модулем m	54
3.7. Модулярные арифметические операции	55
3.7.1. Алгоритм вычисления мультипликативно обратного элемента $a^{-1} \pmod{n}$ в \mathbb{Z}_n	56
3.7.2. Алгоритм вычисления модулярной степени в \mathbb{Z}_n	56
3.7.3. Алгоритм вычисления генератора мультипликативной циклической группы \mathbb{Z}_p^* при простом p (перебор).....	57
Глава 4. Сравнения с одной переменной	58
4.1. Решение сравнения с переменными	58
4.2. Сравнения первой степени	60
4.3. Система сравнений первой степени.....	61
4.3.1. Попарно взаимно простые модули	61
4.3.2. Алгоритм Гаусса для системы сравнений $x \equiv c_1 \pmod{m_1}, \dots,$ $x \equiv c_k \pmod{m_k}$ с попарно взаимно простыми модулями.....	62
4.3.3. Произвольные модули	63
4.4. Сравнения любой степени с простым модулем	64
4.5. Сравнения произвольной степени по составному модулю	65
Алгоритм решения сравнения $f(x) \equiv 0 \pmod{p^a}$	68
Глава 5. Сравнения второй степени	69
5.1. Квадратичные вычеты по простому модулю	69
5.2. Символ Лежандра	70
5.3. Символ Якоби.....	74
Алгоритм вычисления символа Якоби (и символа Лежандра) $JACOBI(a, n)$	76
5.4. Квадратичные вычеты по составному модулю	77
Глава 6. Прimitивные корни и индексы	80
6.1. Экспонента, примитивные корни, индексы.....	80
6.1.1. Число классов вычетов данной экспоненты.....	82
6.1.2. Индексы (дискретные логарифмы).....	83
6.2. Прimitивные корни по модулям p^a и $2p^a$	83
6.3. Вычисление примитивных корней по модулям p^a и $2p^a$	87
6.4. Индексы по модулям p^a и $2p^a$	88
6.5. Индексы и вычеты	88
6.6. Индексы по модулю 2^a	89
6.7. Индексы по любому составному модулю	91

Глава 7. Универсальные алгебры.....93

7.1. Алгебры, подалгебры, гомоморфизм алгебр	93
7.2. Конгруэнции	96

Глава 8. Абстрактная алгебра99

8.1. Полугруппы.....	99
8.2. Циклические полугруппы	101
8.3. Группы	103
8.3.1. Циклические группы	107
8.3.2. Смежные классы. Разложение группы по подгруппе	107
8.3.3. Конечные группы и теорема Лагранжа	109
8.3.4. Конечные циклические группы	109
8.3.5. Алгоритм вычисления всех подгрупп конечной циклической группы.....	111
8.4. Нормальные подгруппы, фактор-группы, теорема о гомоморфизме групп.....	111
8.5. Кольцо	114
8.6. Поле.....	117
8.7. Полиномиальные кольца.....	120
8.8. Идеал кольца.....	121
8.8.1. Главный идеал	122
8.8.2. Разностное кольцо (кольцо классов вычетов). Сравнения.....	122
8.9. Линейное векторное пространство	124
8.10. Булева алгебра	126
8.11. Решетка.....	126

Глава 9. Конечные поля 128

9.1. Представление конечного поля множеством классов вычетов по модулю неприводимого полинома	128
9.2. Поле разложения полинома $x^{p^m} - x$	130
9.3. Циклическость мультипликативной группы поля.....	130
9.4. Задание поля корнем неприводимого полинома	131
9.5. Строение конечных полей.....	133
9.5.1. Минимальный полином	136
9.5.2. Вычисление минимального полинома	137
9.5.3. Подполя конечного поля	139
9.5.4. Круговые полиномы.....	142
9.5.5. Алгоритм факторизации полинома $x^{p^m-1} - 1$ на круговые полиномы из $\text{GF}(q)$	144
9.6. Изоморфизм полей Галуа.....	145
9.7. Автоморфизмы поля Галуа	146

9.8. Основные алгоритмы для конечных полей.....	147
9.8.1. Алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$	149
9.8.2. Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$	150
9.8.3. Мультипликативный обратный элемент в \mathbb{F}_{p^m}	153
9.8.4. Модулярная степень в \mathbb{F}_{p^m}	153
9.8.5. Тестирование полинома из $\mathbb{Z}_p[x]$ на неприводимость	153
9.8.6. Порождение случайного неприводимого полинома над \mathbb{Z}_p	153
9.8.7. Тестирование неприводимого полинома на примитивность	154
9.8.8. Порождение случайного нормированного примитивного полинома над \mathbb{Z}_p	154
9.8.9. Вычисление порядка элемента конечной группы (метод Гаусса)	154
9.8.10. Вычисление генератора конечной циклической группы (метод Гаусса).....	154

Часть II. КРИПТОГРАФИЯ..... 156

Глава 10. Модулярная алгебра в криптографии..... 157

10.1. Криптография и ее цели	157
10.1.1. Хэш-функция	160
10.1.2. Алгоритм MASH-1	161
10.2. Проблема факторизации целых чисел.....	162
10.2.1. ρ -алгоритм Полларда факторизации целых чисел	162
10.2.2. $(p - 1)$ -алгоритм Полларда факторизации целых чисел	163
10.2.3. Алгоритм квадрат-решета факторизации целых чисел.....	164
10.3. Проблема RSA.....	165
10.4. Проблема квадратичного вычета.....	166
10.4.1. Алгоритм вычисления дискретного квадратного корня по простому модулю p	166
10.4.2. Алгоритм вычисления дискретного квадратного корня по простому модулю p , где $p \equiv 3 \pmod{4}$	167
10.4.3. Алгоритм вычисления дискретного квадратного корня по простому модулю p , где $p \equiv 5 \pmod{8}$	167
10.4.4. Алгоритм вычисления дискретного квадратного корня по простому модулю p при большом s	167
10.4.5. Алгоритм вычисления дискретного квадратного корня по модулю $n = p \cdot q$, где p и q есть простые числа	167
10.5. Проблема дискретного логарифма	168
10.5.1. Алгоритм «малый шаг – большой шаг» вычисления дискретного логарифма	168
10.5.2. ρ -алгоритм Полларда вычисления дискретного логарифма.....	169
10.5.3. Алгоритм Полига-Хеллмана вычисления дискретного логарифма	171

10.6. Проблема подмножества суммы	172
10.6.1. Наивный (переборный) алгоритм решения проблемы суммы.....	172
10.6.2. Алгоритм «встреча посередине» решения проблемы подмножества суммы.....	172
10.7. Проблема факторизации полиномов над конечным полем	173
10.7.1. Бесквадратная факторизация.....	173
10.7.2. Q-матричный алгоритм Берлекампа	174
10.8. Криптосистема RSA.....	175
10.8.1. Шифросистема RSA	175
10.8.2. Электронная цифровая подпись RSA с использованием хэш-функции	177
10.8.3. Электронная цифровая подпись RSA с извлечением сообщения	179
10.9. Криптосистема Эль-Гамала.....	180
10.9.1. Шифросистема Эль-Гамала над числовым полем Галуа $GF(p)$	180
10.9.2. Электронная цифровая подпись Эль-Гамала над числовым полем Галуа $GF(p)$	182
10.9.3. Шифросистема Эль-Гамала над полиномиальным полем Галуа $GF(p^m)$	184
10.9.4. Электронная цифровая подпись Эль-Гамала над полиномиальным полем Галуа $GF(p^m)$	187
10.10. Электронная цифровая подпись DSA.....	189
10.11. Криптографическая система Рабина	192
10.11.1. Шифросистема Рабина.....	192
10.11.2. Электронная цифровая подпись Рабина с извлечением сообщения.....	194
10.11.3. Модифицированная цифровая подпись Рабина с извлечением сообщения.....	195
10.12. Рюкзачная схема шифрования Меркле–Хеллмана.....	198
10.13. Рюкзачная схема шифрования Хора–Ривеста.....	199
10.14. Вероятностные схемы шифрования с открытым ключом.....	203
10.14.1. Вероятностная схема шифрования Голдвассер–Микали	204
10.14.2. Вероятностная схема шифрования Блума–Голдвассер.....	206
10.15. Электронная цифровая подпись Фейге–Фиат–Шамира	208
10.16. Электронная цифровая подпись GQ.....	210
10.17. Электронная цифровая подпись Шнорра с хэш-функцией	211
10.18. Электронная цифровая подпись Ниберга–Рюппеля с извлечением сообщения.....	213

Глава 11. Криптография на эллиптических кривых над конечными полями	215
11.1. Эллиптические кривые.....	215

11.2. Эллиптические кривые над полем вещественных чисел	216
11.3. Эллиптические кривые в конечных полях.....	218
11.4. Сложение точек эллиптической кривой $E(F)$ $y^2 = x^3 + ax + b$ над полем F характеристики $\text{char}(F) > 3$	219
11.5. Сложение точек эллиптической кривой $E(F)$ $y^2 = x^3 + ax^2 + bx + c$ с над полем F характеристики $\text{char}(F) = 3$	220
11.6. Сложение точек суперсингулярной эллиптической кривой $E(F)$ $y^2 + cy = x^3 + ax + b$ над полем F характеристики $\text{char}(F) = 2$	222
11.7. Сложение точек несуперсингулярной эллиптической кривой $E(F)$ $y^2 + xy = x^3 + ax^2 + b$ над полем F характеристики $\text{char}(F) = 2$	224
11.8. Вычисление $k \cdot P$	226
11.9. Порядок группы точек эллиптической кривой	226
11.9.1. Алгоритм вычисления порядка элемента группы точек эллиптической кривой (метод Гаусса)	228
11.9.2. Алгоритм вычисления генератора циклической группы точек эллиптической кривой (метод Гаусса)	228
11.10. Криптосистемы на эллиптических кривых над числовым конечным полем	229
11.10.1. Шифросистема Эль-Гамала на эллиптических кривых над числовым конечным полем.....	229
11.10.2. Электронная цифровая подпись (ЭЦП) Эль-Гамала на эллиптических кривых над числовым конечным полем	232

Глава 12. Шифросистема NTRU на конечных полиномиальных кольцах..... 235

12.1. Проблема кратчайшего вектора в целочисленной решетке	235
12.2. Шифросистема NTRU	236

Глава 13. Блочные и потоковые шифры..... 241

13.1. Блочный шифр RC5-S.....	241
13.2. Потоковые шифры.....	245
13.2.1. Линейный регистр сдвига с обратной связью.....	245
13.2.2. Расшифровка линейного регистра сдвига	247

Часть III. КОДИРОВАНИЕ 250

Глава 14. Линейные коды 251

14.1. Линейные пространства над полями Галуа.....	251
14.2. Расстояние Хэмминга.....	252
14.3. Порождающая и проверочная матрицы.....	253
14.4. Декодирование в ближайшее кодовое слово.....	255

14.5. Расстояние и корректирующая способность кода.....	256
14.6. Каноническая форма базисных матриц систематического кода.....	256
14.6.1. Каноническая проверочная матрица	256
14.6.2. Каноническая кодирующая матрица	257
14.6.3. Алгоритм систематизации несистематического линейного кода.....	260
14.7. Декодирование линейного кода (декодер).....	261
14.8. Бинарный код Хэмминга.....	263

Глава 15. Циклические коды 266

15.1. Порождающая и проверочная матрицы циклического кода	266
15.2. Канонические порождающая и проверочная матрицы циклического кода.....	268
15.3. Систематический кодер циклического кода.....	270

Глава 16. Коды Боуза–Чоудхури–Хоквингема (коды БЧХ) 271

16.1. Построение кодов БЧХ.....	271
16.2. Декодер Питерсона–Горенштейна–Цирлера	276
16.3. Алгоритм Питерсона–Горенштейна–Цирлера БЧХ-кода с исправлением t и менее ошибок	281

Глава 17. Коды сжатия информации 298

17.1. Алфавитное кодирование.....	298
17.2. Кодирование с минимальной избыточностью.....	299
17.3. Алгоритм Фано построения разделимой префиксной схемы алфавитного кодирования, близкого к оптимальному	300
17.4. Оптимальное кодирование.....	301
17.5. Алгоритм Хаффмана оптимальной разделимой префиксной схемы алфавитного кодирования	303
17.6. Кодер и декодер Прюфера для деревьев	309

Глава 18. Основы теории информации 311

18.1. Количество информации и энтропия	311
18.1.1. Равновероятность знаков алфавита.....	311
18.1.2. Разновероятность знаков алфавита. Формулы Шеннона	313
18.2. Свойства энтропии.....	313
18.3. Энтропия при непрерывном сообщении	316
18.4. Условная энтропия	319
18.5. Взаимная энтропия	326

Приложения	327
1. Множества, функции, отношения	327
2. Модулярная алгебра.....	334
3. Криптография.....	341
4. Кодирование.....	342
5. Информация и энтропия.....	345
Литература.....	347
Обозначения.....	349