

О Г Л А В Л Е Н И Е

Введение	3
1. Множество	3
2. Мощность множества. Счетные и несчетные множества	5
3. Мощность континуума	7
4. Кардинальные числа. Сравнение мощностей	8
5. Шкала мощностей	11
6. Унарные функции	12
7. Отношения	14
8. Отношение эквивалентности	14
9. Каноническое разложение функции	16
10. Определение группы, кольца, поля	17
Часть 1. МОДУЛЯРНАЯ АРИФМЕТИКА	20
1. Делимость	20
1.1. Позиционная система счисления	20
1.1.1. Алгоритм вычисления n -ричной записи 10-ричного числа a	22
1.2. Простые числа	22
1.3. Факторизация целых чисел	24
1.4. Наибольший общий делитель	25
1.4.1. Алгоритм Евклида вычисления наибольшего общего делителя	26
1.4.2. Расширенный алгоритм Евклида вычисления наибольшего общего делителя	29
1.4.2.1. Расширенный алгоритм Евклида вычисления $d = \text{нод}(a, b)$, $a \geq b$, и чисел u, v , для которых $d = ua + vb$	30
1.5. Наименьшее общее кратное	31
1.6. Непрерывные (цепные) и подходящие дроби	33
1.6.1. Вычисление подходящих дробей	34
1.6.2. Алгоритм вычисления подходящих дробей	35
2. Функции Мебиуса и Эйлера	36
2.1. Функции $[x]$, $\{x\}$ для вещественного x	36
2.2. Мультипликативные функции	37
2.3. Функция Мебиуса и формула обращения Мебиуса	39
2.4. Функция Эйлера	45

3. Сравнения	47
3.1. Сравнение целых чисел	47
3.2. Свойства сравнений	48
3.3. Полная система вычетов	49
3.3.1. <i>Операции над классами</i>	50
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. <i>Алгоритм вычисления мультипликативно обратного элемента $a^{-1} \pmod{n}$ в \mathbb{Z}_n</i>	56
3.7.2. <i>Алгоритм вычисления модулярной степени в \mathbb{Z}_n</i>	57
3.7.3. <i>Алгоритм вычисления генератора мультипликативной циклической группы \mathbb{Z}_p^* при простом p (перебор)</i>	57
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	62
4.3.1. <i>Попарно взаимно простые модули</i>	62
4.3.2. <i>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</i>	63
4.3.3. <i>Произвольные модули</i>	64
4.4. Сравнения любой степени с простым модулем	65
4.5. Сравнения произвольной степени по составному модулю	66
4.5.1. <i>Алгоритм решения сравнения $f(x) \equiv 0 \pmod{p^a}$</i>	69
5. Сравнения второй степени	70
5.1. Квадратичные вычеты по простому модулю	70
5.2. Символ Лежандра	72
5.3. Символ Якоби	77
5.3.1. <i>Алгоритм вычисления символа Якоби (и символа Лежандра)</i>	79
5.4. Квадратичные вычеты по составному модулю	80

6. Прimitives корни и индексы	83
6.1. Экспонента и примитивные корни	83
6.1.1. Число классов данной экспоненты	85
6.1.2. Индексы (дискретные логарифмы)	87
6.2. Примитивные корни по модулям p^α и $2p^\alpha$	87
6.3. Вычисление примитивных корней по модулям p^α и $2p^\alpha$	91
6.4. Индексы по модулям p^α и $2p^\alpha$	92
6.5. Индексы и вычеты	93
6.6. Индексы по модулю 2^α	95
6.7. Индексы по любому составному модулю	97
7. Группа, кольцо, поле	99
7.1. Группа	99
7.2. Кольцо	101
7.3. Поле	101
7.4. Полиномиальные кольца	102
7.5. Векторное пространство	104
7.6. Конечные поля	106
7.6.1. Основные свойства полей	106
7.6.2. Алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$	109
7.6.3. Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$	110
7.6.4. Мультипликативный обратный элемент в \mathbb{F}_{p^m}	112
7.6.5. Модулярная степень в \mathbb{F}_{p^m}	112
7.6.6. Тестирование полинома из $\mathbb{Z}_p[x]$ на неприводимость	113
7.6.7. Порождение случайного неприводимого полинома над \mathbb{Z}_p	113
7.6.8. Тестирование неприводимого полинома на примитивность	114
7.6.9. Порождение случайного нормированного примитивного полинома над \mathbb{Z}_p	114
7.6.10. Вычисление порядка элемента конечной группы	114
7.6.11. Вычисление генератора конечной циклической группы (алгоритм Гаусса)	115

8. Применение модулярной арифметики в криптографии	115
8.1. Криптография и ее цели	115
8.1.1. Хэш-функция	119
8.1.2. Алгоритм MASH	120
8.2. Проблема факторизации целых чисел	121
8.2.1. <i>Rho-алгоритм Полларда факторизации целых чисел</i>	122
8.2.2. <i>(p-1)-алгоритм Полларда факторизации целых чисел</i>	122
8.2.3. <i>Алгоритм квадрат-решета факторизации целых чисел</i>	123
8.3. Проблема RSA	125
8.4. Проблема квадратичного вычета	126
8.4.1. <i>Алгоритм вычисления квадратного корня по простому модулю p</i>	126
8.4.2. <i>Алгоритм вычисления квадратного корня по простому модулю p, где $p \equiv 3 \pmod{4}$</i>	127
8.4.3. <i>Алгоритм вычисления квадратного корня по простому модулю p, где $p \equiv 5 \pmod{8}$</i>	127
8.4.4. <i>Алгоритм вычисления квадратного корня по простому модулю p при большом s</i>	127
8.4.5. <i>Вычисление квадратного корня по модулю n, если p и q есть, простые факторы в n</i>	128
8.5. Проблема дискретного логарифма	128
8.5.1. <i>Алгоритм "малый шаг - большой шаг" вычисления дискретного логарифма</i>	129
8.5.2. <i>Rho алгоритм Полларда вычисления дискретного логарифма</i>	130
8.5.3. <i>Алгоритм Полига-Хеллмана вычисления вычисления дискретного логарифма</i>	132
8.6. Проблема подмножества суммы	133
8.6.1. <i>Наивный (переборный) алгоритм решения проблемы суммы</i>	133
8.6.2. <i>Алгоритм "встреча посередине" решения проблемы суммы</i>	134
8.7. Факторизация полиномов над конечным полем	134
8.7.1. <i>Бескватратная факторизация</i>	135
8.7.2. <i>Алгоритм бескватратной факторизации</i>	135
8.7.3. <i>Q-матричный алгоритм Берленкампа</i>	136

8.7.4. <i>Q</i> -матричный алгоритм Берленкампа факторизации полиномов над конечным полем	136
8.8. Криптосистема RSA	137
8.9. Электронная цифровая подпись RSA с извлечением сообщения	138 139
8.9.1. Электронная цифровая подпись RSA с использованием хэш-функции	142
8.10. Криптосистема ЭльГамала	142
8.11. Электронная цифровая подпись ЭльГамала	144
8.12. Обобщенная криптосистема ЭльГамала с мультипликативной группой G поля Галуа $GF(p^m)$	146
8.13. Обобщенная электронная цифровая подпись ЭльГамала с мультипликативной группой G поля Галуа $GF(p^m)$	150
8.14. Электронная цифровая подпись DSA	153
8.15. Криптосистема Рабина	156
8.16. Электронная цифровая подпись Рабина с извлечением сообщения	158
8.17. Модифицированная цифровая подпись Рабина с извлечением сообщения	159
8.18. Криптосистема МакЭлиса	162
8.19. Рюкзачная схема шифрования Меркле-Хеллмана	164
8.19.1. Базовая рюкзачная схема шифрования Меркле-Хеллмана	164
8.20. Рюкзачная схема шифрования Хора-Ривеста	166
8.21. Вероятностное шифрование с открытым ключом	170
8.22. Вероятностная схема шифрования Голдвассера-Микали	171
8.23. Вероятностная схема шифрования Блома-Голдвассера	174
8.24. Электронная цифровая подпись Фейге-Фиат-Шамира	176
8.25. Электронная цифровая подпись GQ	178
8.26. Электронная цифровая подпись Шнорра	180
8.27. Электронная цифровая подпись Ниберга-Рюппеля с извлечением сообщения	182
9. Рекуррентные последовательности в \mathbb{R}	183
9.1. Конечные разности	183

9.1.1. Свойства конечных разностей	183
9.2. Рекуррентные уравнения	186
9.3. Линейные рекуррентные уравнения с переменными коэффициентами	188
9.3.1. Метод Лагранжа вариации произвольных постоянных вычисления частного решения неоднородного уравнения	196
9.4. Линейные рекуррентные уравнения с постоянными коэффициентами	204
Часть 2. ЭЛЕМЕНТЫ КОМБИНАТОРИКИ	211
10. Порождение комбинаторных конфигураций и их пересчет	211
10.1. Размещения, перестановки, сочетания	211
10.2. Правило суммы и правило произведения	212
10.3. Подсчет числа размещений, перестановок, сочетаний	212
10.3.1. Число размещений без повторений	212
10.3.2. Число размещений с повторениями	213
10.3.3. Число сочетаний без повторений	213
10.3.4. Число сочетаний с повторениями	213
10.3.5. Число перестановок данной спецификации	214
10.3.6. Число размещений данной спецификации	215
11. Производящие функции для комбинаторных конфигураций и их чисел	216
11.1. Аппарат формальных степенных рядов	216
11.2. Производящие функции для сочетаний	216
11.2.1. Сочетания без повторений	216
11.2.2. Сочетания с повторениями с ограничениями на число повторений	218
11.2.3. Сочетания с повторениями без ограничений на число повторений	219
11.3. Производящие функции для размещений с повторениями	221
12. Комбинаторно логический аппарат	223
12.1. Включения и исключения	223
12.2. Приложения формулы включений и исключений	226
12.2.1. Задача о беспорядках	226
12.2.2. Задача о встречах	228

Часть 3. АЛГЕБРА ЛОГИКИ И ПРЕДИКАТЫ	229
13. Алгебра логики	229
13.1. Функции алгебры логики	229
13.2. Формулы. Реализация функций формулами	230
13.3. Равносильные преобразования формул	233
13.4. Нормальные формы	235
13.4.1. Совершенные нормальные формы	236
13.5. Минимизация нормальных форм	239
13.5.1. Алгоритм Куайна построения сокращенной ДНФ	241
13.5.2. Алгоритм построения сокращенной ДНФ с помощью КНФ	243
13.5.3. Построение всех тупиковых ДНФ	244
13.5.4. Алгоритм минимизации функций в классе ДНФ	247
13.5.5. Алгоритм минимизации функций в классе КНФ	247
13.5.6. Алгоритм минимизации функций в классе нормальных форм	247
13.6. Минимизация частично определенных функций	250
13.6.1. Алгоритм минимизации частично определенных функций в классе ДНФ	251
13.6.2. Алгоритм минимизации частично определенных функций в классе КНФ	251
13.7. Двойственные функции	253
13.7.1. Принцип двойственности	254
13.8. Линейные функции	255
13.9. Монотонные функции	259
13.10. Теорема Поста о функциональной полноте	261
13.10.1. Предполные классы	262
14. Функции k-значной логики	264
14.1. Функции и отношения	264
14.2. Самодвойственные функции	268
14.3. Монотонные функции	269
14.4. Линейные функции	269
14.5. Функции, сохраняющие разбиение	270
14.6. Классы типа \mathbb{C}	270
14.7. Классы типа \mathbb{B}	271

14.8. Сравнение функций двузначной и многозначной логик	272
15. Частично упорядоченные множества, решетки, булевы алгебры	272
15.8. Отношение частичного порядка	272
15.9. Решетки	276
15.10. Изоморфизм решеток	279
15.11. Булевы алгебры	280
16. Синтез схем из функциональных элементов	284
16.1. Схема из функциональных элементов	284
16.2. Функции Шеннона	287
16.3. Элементарные методы синтеза схем	287
16.4. Синтез мультиплексоров	290
16.5. Элементы функциональной декомпозиции	292
16.6. Обнаружение неисправностей в схемах	298
17. Логика предикатов	302
17.1. Предикаты, кванторы	302
17.2. Выполнимость, невыполнимость, общезначимость, опровержимость формул логики предикатов	304
17.3. Равносильность формул	309
17.3.1. Релятивизованные кванторы	311
17.4. Префиксная нормальная форма	312
17.5. Проблема разрешимости в логике предикатов	313
17.5.1. Проблема разрешимости \exists -формул	314
17.5.2. Проблема разрешимости \forall -формул	315
17.5.3. Проблема разрешимости логики одноместных предикатов	316
17.6. Отношения	318
17.7. Суперпозиция функций	321
17.8. Операции Мальцева над функциями	321
17.9. Алгебра отношений (реляционная алгебра)	322
17.9.1. Операции Мальцева над отношениями	322
17.10. Алгебра отношений k -значной логики	324
Часть 4. АЛГОРИТМЫ НА ГРАФАХ	325
18. Способы задания графов	325
18.1. Графы, мультиграфы, псевдографы	325

18.2. Задание графов	327
18.3. Операции над графами	328
18.4. Маршруты, цепи, циклы, связность	329
18.4.1. Помечивающий алгоритм (Дейкстры) поиска кратчайшего (с наименьшим весом) пути между двумя вершинами s и t в связном нагруженном ориентированном графе	330
18.4.1.1. Вычисление наименьшего веса пути от s к t	330
18.4.1.2. Построение наименьшего пути от s к t	331
19. Обходы графов	338
19.1. Эйлеровы графы	338
19.2. Полные циклы и последовательности де Брейна	340
19.3. Гамильтоновы графы	343
19.4. Коды Грея	344
20. Деревья	345
20.1. Деревья и лес	345
20.2. Характеристические свойства деревьев	345
20.3. Каркасы и хорды в связном графе	348
21. Циклы в графах	351
21.1. Линейное пространство двоичных наборов	351
21.2. Линейное пространство подграфов данного графа	352
21.3. Подпространство четных подграфов	353
21.4. Циклический ранг графа	357
21.5. Матричная теорема о деревьях	360
22. Двудольные графы и паросочетания	361
22.1. Двудольные графы	361
22.2. Паросочетания	363
22.2.1. Алгоритм построения совершенного паросочетания для двудольного графа	364
22.3. Системы различных представителей	366
23. Планарные графы	370
23.1. Плоские графы	370

23.2.	Формула Эйлера	371
23.3.	Критерий планарности Понтрягина–Куратовского	374
23.3.1.	<i>Алгоритм построения плоского изображения графа</i>	374
24.	Раскраска графов	377
24.1.	Хроматическое число и хроматический класс	377
24.2.	Раскраска вершин	378
24.3.	Верхняя и нижняя оценки хроматического числа. Внутренне и внешне устойчивые множества вершин графа	379
24.3.1.	<i>Внутренне устойчивые множества вершин графа</i>	379
24.3.2.	<i>Алгоритм вычисления всех наибольших внутренне устойчивых множеств вершин графа $G = (V, E)$</i>	380
24.3.3.	<i>Внешне устойчивые множества вершин графа</i>	381
24.3.4.	<i>Алгоритм вычисления всех наименьших внешне устойчивых множеств вершин графа $G = (V, E)$</i>	382
24.4.	Оптимальная раскраска вершин графа	383
24.4.1.	<i>Алгоритм оптимальной раскраски (p, q)-графа $G = (V, E)$</i>	384
24.5.	Раскрашивание планарных графов	385
25.	Потоки в транспортных сетях	387
15.1.	Двухполюсные сети	387
25.2.	Дивергенция	388
25.3.	Потоки в сетях	389
25.4.	Сечения в сетях	390
25.5.	Величина потока и пропускная способность сети	391
25.6.	Максимальный поток	392
25.6.1.	<i>Алгоритм вычисления максимального потока в транспортной сети</i>	394
25.6.2.	<i>Помечивающий алгоритм Дейкстры вычисления максимального потока в транспортной сети</i>	398

26. Перечисление графов	404
26.1. Число помеченных графов	404
26.2. Число помеченных деревьев	405
26.3. Графы и группы подстановок	407
26.3.1. Группы подстановок и лемма Бернсайда	407
26.3.2. Теорема Пойа	412
26.3.3. Раскраска вершин куба	416
26.3.4. Составление ожерелий	418
Часть 5. МОНАДИЧЕСКАЯ ЛОГИКА И КОНЕЧНЫЕ АВТОМАТЫ	421
27. Конечные автоматы	421
27.1. Автоматы Мили и Мура	421
27.2. Источники	425
27.2.1. Алгоритм детерминизации источника	430
27.3. Регулярные языки	431
27.4. Теоремы замкнутости для класса автоматов представимых языков	434
27.5. Минимизация числа состояний автомата с выходом	437
27.5.1. Склеивание неразличимых состояний	439
27.5.2. Алгоритм минимизации автомата	440
27.5.3. Алгоритм разбиения множества состояний на классы неотличимых состояний	444
28. Автоматы и сверхязыки	446
28.1. Макроавтоматы	446
28.2. Конкатенация языка и сверхязыка	449
28.3. Сверхитерация автоматных языков	451
28.4. Детерминизация макроисточника	455
28.4.1. Общерегулярные сверхязыки	454
29. Проблема униформизации	457
29.1. Языки и операторы	457
29.1.1. Униформизация	461
29.2. Игры	461
29.2.1. Игры с конечным числом состояний	464
29.3. Стратегии	465
29.4. Униформизация конечно автоматных языков	468

29.4.1. <i>Порядковые векторы и порядковые стратегии</i>	468
29.4.2. <i>Теоремы о порядковых стратегиях</i>	471
29.4.3. <i>Пример построения выигрывающего автомата</i>	476
30. Монадическая логика	479
30.1. Логика одноместных предикатов	479
30.2. Выразимость в ЛОП	482
30.2.1. <i>Макросточники и ЛОП</i>	483
30.2.2. <i>Регулярные языки и ЛОП</i>	484
30.2.3. <i>Общерегулярные языки и ЛОП</i>	485
30.3. Специальная префиксная форма	485
30.4. Синтез автомата по формуле ЛОП	487
Список сокращений и знаков	492
Литература	494