
Оглавление

Предисловие	11
1. Целочисленные алгоритмы	13
1.1. Арифметика целых чисел	13
1.1.1. Деление с остатком	13
1.1.2. Наибольший общий делитель, наименьшее общее кратное и их свойства	14
1.1.3. Простые числа	17
1.1.4. Решето Эратосфена. Разложение числа на простые множители	19
1.1.5. Позиционная запись натуральных чисел	27
1.1.6. Алгоритмы арифметических действий с p -ичными записями натуральных чисел	29
1.1.7. Алгоритмы перевода p -ичной записи натурального числа в q -ичную	31
1.1.8. Алгоритм эффективного возведения числа в натуральную степень	32
Задачи и вопросы	34
1.2. Алгоритм Евклида и цепные дроби	36
1.2.1. Классический алгоритм Евклида	36
1.2.2. Бинарный алгоритм Евклида	37
1.2.3. Линейное представление наибольшего общего делителя	39
1.2.4. Обобщенный алгоритм Евклида	40
1.2.5. Разложение числа в цепную дробь	42
1.2.6. Свойства подходящих дробей и их вычисление	45
1.2.7. Цепные дроби и анализ алгоритма Евклида	46
1.2.8. Бесконечная цепная дробь и ее вычисление	51
1.2.9. Наилучшие приближения	58
1.2.10. Некоторые применения цепных дробей	60
1.2.11. Диофантовы уравнения	61
1.2.12. Числа Фибоначчи	66
Задачи и вопросы	70
1.3. Арифметика остатков	71
1.3.1. Алгебраические структуры	71
1.3.2. Арифметика и свойства сравнений	73
1.3.3. Функция Эйлера и ее свойства	77

1.3.4.	Линейные сравнения	85
1.3.5.	Китайская теорема об остатках	89
1.3.6.	Система остаточных классов	93
1.3.7.	Применение теоремы Эйлера в криптографии. Система шифрования RSA	94
1.3.8.	Простейшие атаки на систему RSA	99
1.3.8.1.	Схема с нотариусом	100
1.3.8.2.	Метод бесключевого чтения RSA, или циклическая атака	100
1.3.9.	Другие примеры использования RSA	101
1.3.9.1.	Электронная подпись	101
1.3.9.2.	Электронные деньги	102
	Задачи и вопросы	104
1.4.	Арифметика многочленов	106
1.4.1.	Основные операции и свойства	106
1.4.2.	Схема Горнера	114
1.4.3.	Алгоритм Евклида для многочленов. Линейное представление НОД	116
1.4.4.	Интерполяционная формула Лагранжа	118
1.4.5.	Разложение многочлена на свободные от квадратов множители	120
1.4.6.	Разложение многочленов на неприводимые множители	122
1.4.6.1.	Приводимость над полем рациональных чисел	123
1.4.6.2.	Связь неприводимости многочленов с целыми коэффициентами над \mathbb{Z}_p и \mathbb{Q}	125
	Задачи и вопросы	126
1.5.	Базисы Гребнера	128
1.5.1.	Задачи на доказательство и многочлены	128
1.5.2.	Случай многочленов одной переменной	129
1.5.3.	Понятие идеала	130
1.5.3.1.	Идеалы в кольце многочленов одной переменной	132
1.5.4.	Линейные многочлены многих переменных. Понятие базиса Гребнера	132
1.5.5.	Алгоритм Бухбергера	135
1.5.5.1.	Главный член многочлена с несколькими переменными	135

1.5.5.2.	Редукция многочлена с несколькими переменными	136
1.5.5.3.	Построение S -многочленов	139
1.5.5.4.	Построение базиса Гребнера	140
	Задачи и вопросы	145
1.6.	Теория множеств и комбинаторика	147
1.6.1.	Вводные задачи	147
1.6.1.1.	Принцип умножения	147
1.6.1.2.	Принцип сложения	148
1.6.1.3.	Использование взаимно однозначного соответствия множеств	150
1.6.1.4.	Различные способы рассуждений	152
1.6.1.5.	Принцип использования разных языков описания	153
1.6.1.6.	Принцип формального оперирования алгебраическими объектами вместо комбинаторных рассуждений	154
1.6.1.7.	Принцип Дирихле	155
1.6.2.	Размещения и сочетания	157
1.6.3.	Биномиальные коэффициенты	160
1.6.4.	Кодирование с исправлением ошибок. Граница Хемминга	162
1.6.5.	Полиномиальное кодирование	165
1.6.6.	Код Шеннона — Фано и алгоритм Хаффмана	171
1.6.7.	Лексикографический порядок. Генерация подмножеств	173
1.6.8.	Перечислительная комбинаторика	175
1.6.8.1.	Перечисление подмножеств	176
1.6.8.2.	Перечисление элементов декартова произведения множеств	180
1.6.8.3.	Перечисление перестановок	182
1.6.9.	Бинарный код Грея	188
1.6.9.1.	Код Грея и задача о Ханойских башнях	189
1.6.10.	Числа Стирлинга первого и второго родов	190
1.6.11.	Числа Каталана	193
1.6.12.	Разбиения чисел	198
1.6.13.	Введение в динамическое программирование. Задача о рюкзаке	202
1.6.14.	Принцип включения-исключения	205
1.6.15.	Обращение Мебиуса	210

1.6.16.	Понятие о группе: теорема Бернсайда	214
1.6.16.1.	Самосовмещения правильного тетраэдра	214
1.6.16.2.	Подгруппы и классы смежности	217
1.6.16.3.	Теорема Бернсайда	222
	Задачи и вопросы	228
1.7.	Производящие функции и рекуррентные уравнения	231
1.7.1.	Производящие функции	231
1.7.2.	Решение однородного линейного рекуррентного уравнения	236
1.7.3.	Решение неоднородного линейного рекуррентного уравнения	243
1.7.4.	Производящая функция для чисел Каталана	245
1.7.5.	Число многочленов заданной степени, неприводимых над полем вычетов	247
	Задачи и вопросы	250
1.8.	Элементы дискретной теории вероятностей	251
1.8.1.	Основные определения	251
1.8.2.	Условные вероятности и формула Байеса	253
1.8.3.	Дискретные случайные величины. Математическое ожидание и дисперсия	258
	Задачи и вопросы	262

2. Графы и бинарные отношения 263

2.1.	Основные понятия теории графов	263
2.1.1.	Простейшие определения и свойства	263
2.1.2.	Машинное представление графов	270
2.1.2.1.	Матрица инцидентности	270
2.1.2.2.	Матрица смежности	271
2.1.2.3.	Списки инцидентности	272
2.1.2.4.	Список ребер	273
2.1.3.	Поиск в глубину и ширину в графе	273
2.1.4.	Связность	278
2.1.5.	Эйлеровы графы	289
2.1.6.	Графы де Брюина	298
2.1.7.	Гамильтоновы графы	303
2.1.8.	Турниры	308
2.1.9.	Деревья	310
2.1.10.	Корневые деревья	313
2.1.11.	Код Прюфера	317
2.1.12.	Главные циклы и коциклы	320

2.1.13. Двудольные графы	329
2.1.14. Клики и независимые множества	333
2.1.15. Планарность	337
2.1.16. Раскраска графов	345
2.1.17. Хроматические многочлены	354
Задачи и вопросы	362
2.2. Алгоритмы на графах	367
2.2.1. Построение наибольшего паросочетания	367
2.2.2. Построение минимальных стягивающих деревьев	373
2.2.3. Задача нахождения кратчайших путей в графе	385
2.2.4. Алгоритм Форда — Беллмана	386
2.2.5. Алгоритм Форда — Беллмана для нахождения дерева кратчайших путей	391
2.2.6. Алгоритм Дейкстры	396
2.2.7. Сравнительный анализ трудоемкости алгоритмов Форда — Беллмана и Дейкстры	402
2.2.8. Алгоритм Флойда	403
2.2.9. Волновой алгоритм	411
2.2.10. Алгоритм Форда — Фалкерсона	414
2.2.11. Перебор с возвратом	426
2.2.12. Метод ветвей и границ	430
Задачи и вопросы	433
2.3. Бинарные отношения	436
2.3.1. Введение. Постановка задачи	436
2.3.2. Свойства бинарных отношений	437
2.3.3. Способы задания отношений	440
2.3.4. Отношения эквивалентности и толерантности	442
2.3.5. Отношения предпорядка и порядка	444
2.3.6. Алгоритм топологической сортировки	447
2.3.7. Частично упорядоченные множества. Диаграмма Хассе	450
2.3.8. Транзитивное замыкание бинарного отношения. Алгоритм Уоршелла	452
2.3.9. Примеры на бинарные отношения	458
2.3.10. Введение в семантические сети	459
Задачи и вопросы	460

3. Математическая логика и теория алгоритмов 463

3.1. Логика высказываний	463
------------------------------------	-----

3.1.1.	Основные понятия логики высказываний	463
3.1.2.	Равносильность формул логики высказываний	470
3.1.3.	Принцип двойственности	473
3.1.4.	Логическое следствие	475
3.1.5.	Нормальные формы в логике высказываний	479
3.1.6.	Контактные схемы	488
3.1.7.	Метод минимизирующих карт	491
3.1.8.	Метод Куайна — Мак-Класки	498
3.1.9.	Метод резолюций в логике высказываний	503
3.1.10.	Стратегии метода резолюций	508
3.1.11.	Линейная резолюция	512
3.1.12.	Решетки, булевы алгебры, кольца	513
	Задачи и вопросы	519
3.2.	Булевы функции	521
3.2.1.	Основные понятия	521
3.2.2.	Замкнутость и полнота	526
3.2.3.	Полиномы Жегалкина и линейные функции	529
3.2.4.	Быстрое вычисление полинома Жегалкина	536
3.2.5.	Булевы функции в криптографии	538
3.2.6.	Самодвойственные функции	539
3.2.7.	Монотонные функции	544
3.2.8.	Теорема Поста	548
3.2.9.	Разложение Шеннона	555
3.2.10.	Бинарные диаграммы решений	556
	Задачи и вопросы	563
3.3.	Логика предикатов	566
3.3.1.	Основные определения	566
3.3.2.	Семантика логики предикатов	569
3.3.3.	Примеры и задачи на выразительность логики предикатов	571
3.3.4.	Равносильность формул логики предикатов	573
3.3.5.	Логическое следствие	576
3.3.6.	Нормальные формы	578
3.3.7.	Примеры и задачи на приведение к ПНФ и СНФ	582
3.3.8.	Метод резолюций в логике предикатов	583
3.3.8.1.	Подстановка и унификация	584
3.3.8.2.	Метод резолюций	588
3.3.9.	Метод резолюций и ПРОЛОГ	593
	Задачи и вопросы	596

3.4. Нечеткая логика	599
3.4.1. Нечеткие множества	599
3.4.1.1. Введение в нечеткие множества	599
3.4.1.2. Основные понятия	602
3.4.1.3. Операции над нечеткими множествами	606
3.4.1.4. Мера нечеткости множеств	611
3.4.1.5. Функции принадлежности	613
3.4.1.6. Методы построения функций принадлежности	617
3.4.2. Нечеткие бинарные отношения	619
3.4.2.1. Основные понятия	619
3.4.2.2. Свойства нечетких бинарных отношений	622
3.4.3. Нечеткая логика высказываний	624
3.4.3.1. Нечеткие высказывания	624
3.4.3.2. Нечеткие формулы логики высказываний	627
Задачи и вопросы	629
3.5. Теория алгоритмов	631
3.5.1. Машина Тьюринга и функции, вычислимые по Тьюрингу	631
3.5.2. Примеры и задачи на построение машин Тьюринга	637
3.5.3. Операции над машинами Тьюринга	641
3.5.4. Проблема останова машины Тьюринга	643
3.5.5. Частично рекурсивные функции	646
3.5.6. Нормальные алгорифмы Маркова	649
3.5.7. Примеры и задачи на нормальные алгорифмы Маркова	653
3.5.8. Вычислительная сложность алгоритма	656
3.5.9. Сложностные классы задач	658
Задачи и вопросы	660
3.6. Формальные языки и грамматики	662
3.6.1. Основные определения порождающих грамматик	663
3.6.2. Классификация грамматик	665
3.6.3. Контекстно-свободные грамматики	667
3.6.4. Синтаксический анализатор	670
3.6.5. Преобразования контекстно-свободных грамматик	673
3.6.6. Примеры на построение грамматик	676
3.6.7. Префиксная и постфиксная записи формул	677

3.6.8.	Алгоритмы обработки скобочных записей	682
	Задачи и вопросы	685
3.7.	Конечные автоматы-распознаватели	688
3.7.1.	Введение	688
3.7.2.	Автоматы Мили и Мура	689
3.7.3.	Примеры автоматов Мили и Мура	691
3.7.4.	Эквивалентность автоматов Мили и Мура	692
3.7.5.	Основные понятия автоматов-распознавателей	696
3.7.6.	Примеры автоматов-распознавателей	697
3.7.7.	Недетерминированные автоматы-распознаватели. Детерминизация	699
3.7.8.	Теорема о разрастании для автоматных языков	703
3.7.9.	Автоматы и автоматные грамматики	706
3.7.10.	Минимизация автоматов-распознавателей	710
3.7.11.	Конечные автоматы с эпсилон-переходами	714
3.7.12.	Конечные автоматы и регулярные выражения	715
	Задачи и вопросы	721

Список литературы	725
--------------------------	------------

Список алгоритмов	731
--------------------------	------------

Предметный указатель	734
-----------------------------	------------

