

ВЫСШЕЕ ОБРАЗОВАНИЕ

В. М. Фомичёв, Д. А. Мельников

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

ЗАЩИТЫ ИНФОРМАЦИИ

Часть 1. Математические аспекты

Под редакцией В. М. Фомичёва

УЧЕБНИК



СООТВЕТСТВУЕТ
ПРОГРАММАМ
ВЕДУЩИХ НАУЧНО-
ОБРАЗОВАТЕЛЬНЫХ
ШКОЛ

УМО ВО рекомендует

юрайт
издательство

Оглавление

Список основных обозначений.....	7
Предисловие	9
Глава 1. Множества, функции, алгоритмы.....	12
1.1. Понятие множества и функции	12
1.2. Операции над множествами	14
1.3. Схемы и методы комбинаторики	16
1.3.1. Основные правила перечисления	16
1.3.2. Схемы выборок, биномиальные коэффициенты	16
1.3.3. Покрытия и разбиения множеств, принцип включения- исключения.....	18
1.4. Многочлены, формальные степенные ряды, нумераторы.....	20
1.5. Понятие об алгоритмах и сложности вычислений	22
<i>Задачи и упражнения</i>	25
Глава 2. Алгебраические структуры	28
2.1. Полугруппы и группы.....	28
2.2. Кольца, поля, векторные пространства.....	30
2.3. Кольца матриц	32
2.4. Кольцо целых чисел, простые числа, алгоритм Евклида.....	33
2.5. Кольца вычетов, сравнения.....	37
2.6. Кольца многочленов, делимость	38
2.7. Проблема Фробениуса.....	42
<i>Задачи и упражнения</i>	44
Глава 3. Бинарные отношения	47
3.1. Отношения эквивалентности и конгруэнтности.....	47
3.2. Частичный порядок на множествах	48
3.3. Полурешетки и решетки.....	50
3.4. Начала теории графов.....	53
3.5. Графы функций и преобразований.....	58
<i>Задачи и упражнения</i>	59
Глава 4. Полугруппы, группы, конечные поля.....	63
4.1. Определяющие свойства дискретных функций	63
4.2. Преобразования и подстановки.....	65
4.3. Задание полугруппы и группы системой образующих элементов.....	67
4.4. Порядки групп, подгрупп, элементов.....	67
4.5. Конечные поля.....	70
4.6. Характеристики полугрупп и их элементов.....	74

4.7. Сопряженные элементы в моноидах и в группах	75
4.8. Транзитивность групп преобразований	76
4.9. Эквиваленция функций относительно групп подстановок	78
<i>Задачи и упражнения</i>	78
Глава 5. Решение сравнений	81
5.1. Функции теории чисел	81
5.2. Непрерывные дроби	85
5.3. Решение линейных сравнений	87
5.4. Нелинейные сравнения общего вида	88
5.5. Решение нелинейных двучленных сравнений	89
5.6. Первообразные корни и индексы	94
<i>Задачи и упражнения</i>	96
Глава 6. Функции алгебры логики	99
6.1. Элементарные булевы функции	99
6.2. Представление функций формулами	100
6.3. Полнота и замкнутость классов	102
6.4. Основные способы задания булевых функций	106
6.4.1. Табличное задание	106
6.4.2. Геометрическое и графическое задание	106
6.4.3. Многочлен Жегалкина	106
6.4.4. Тензорное произведение матриц, спектральное представление	108
6.5. Связь различных представлений функций	111
6.6. Понятие о классификации двоичных функций	114
<i>Задачи и упражнения</i>	118
Глава 7. Сбалансированность и биективность функций	122
7.1. Критерии сбалансированности функций	123
7.2. Алгебраическая зависимость системы функций	124
7.3. Обратимость функций из некоторых классов	125
7.3.1. Аффинные функции векторных пространств	125
7.3.2. Аффинные преобразования кольца вычетов	126
7.3.3. Регистры сдвига	126
7.3.4. Треугольные преобразования	129
<i>Задачи и упражнения</i>	130
Глава 8. Периодические последовательности	133
8.1. Алгебра последовательностей	133
8.2. Определяющие свойства периодов последовательностей	135
8.3. Период усложненной последовательности	137
8.4. Характеристики периодичности преобразования	137
8.5. Полноцикловые преобразования	139
8.6. Линейные регистры сдвига и линейные рекуррентные последовательности	142
8.7. Линейная сложность последовательностей	146
8.8. Нормальные периодические последовательности	148
8.9. Аффинные преобразования максимального периода	149
<i>Задачи и упражнения</i>	150

Глава 9. Конечные автоматы Мили	153
9.1. Основные определения, виды автоматов	153
9.2. Способы задания автоматов Мили.....	155
9.3. Отношения и операции с автоматами	156
9.4. Различимость состояний и входов	157
9.5. Периодичность и линейная сложность в конечных автоматах	160
<i>Задачи и упражнения</i>	<i>163</i>
Глава 10. Статистическое тестирование последовательностей	166
10.1. Случайные и псевдослучайные последовательности	166
10.2. Генераторы последовательностей.....	168
10.3. Критерии оценки ПСП.....	169
10.4. Статистическое тестирование последовательностей.....	170
10.5. Пакеты статистических тестов и тестируемые характеристики.....	174
10.6. Комбинирование тестов.....	177
<i>Задачи и упражнения</i>	<i>179</i>
Глава 11. Аналитические свойства функций	180
11.1. Свойство совершенности функции и его усиления	180
11.2. Матрично-графовый подход к оценке перемешивающих свойств	183
11.3. Прimitивность графов и неотрицательных матриц	184
11.4. Прimitивность систем матриц и систем графов.....	188
11.5. Локальная примитивность матриц и графов.....	190
11.6. Алгебраические характеристики нелинейности.....	192
11.7. Приближения нелинейных отображений.....	195
<i>Задачи и упражнения</i>	<i>196</i>
Библиографический список	198
Ответы и решения	200
Предметный указатель.....	204