

УДК 511+519.6
ББК 22.13+22.18+22.19
С79

А

Степанов, Александр А.
С79 От математики к обобщенному программированию / А. А. Степанов, Д. Роуз ; пер. с англ. А. А. Слинкина. — 2-е изд., эл. — 1 файл pdf : 266 с. — Москва : ДМК Пресс, 2023. — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10". — Текст : электронный.

ISBN 978-5-89818-306-6

В этой основательной и вместе с тем доступной книге авторы объясняют принципы обобщенного программирования и стоящее за ними понятие математической абстракции.

Любой достаточно квалифицированный программист, умеющий логически мыслить, уже обладает достаточными знаниями для прочтения этой книги. Авторы на удивление доходчиво сообщают необходимые сведения из общей алгебры и теории чисел. Они объясняют, какие проблемы должны были разрешить математики, и показывают, как найденные ими решения переводятся на язык обобщенного программирования и позволяют создать эффективный и элегантный код.

Читая эту книгу, вы освоите мыслительный процесс, необходимый для правильного программирования, и научитесь обобщать найденные для частного алгоритмы с целью расширить область их полезного применения без потери эффективности. Вы также постигнете, в чем состоит ценность математики для программирования, — и это понимание пригодится вне зависимости от того, на каком языке вы пишете и какую парадигму применяете.

УДК 511+519.6
ББК 22.13+22.18+22.19

Электронное издание на основе печатного издания: От математики к обобщенному программированию / А. А. Степанов, Д. Роуз ; пер. с англ. А. А. Слинкина. — Москва : ДМК Пресс, 2016. — 264 с. — ISBN 978-5-97060-379-6. — Текст : непосредственный.

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.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

В соответствии со ст. 1299 и 1301 ГК РФ при устранении ограничений, установленных техническими средствами защиты авторских прав, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации.

ISBN 978-5-89818-306-6

© 2015 Pearson Education, Inc.
© Оформление, перевод, ДМК Пресс, 2016

А

Содержание

Благодарности	9
Об авторах	10
От авторов.....	11
Предисловие автора к русскому изданию	12
Глава 1. О чем эта книга	13
1.1. Программирование и математика	13
1.2. Исторические справки.....	14
1.3. Требования к читателю.....	15
1.4. План книги.....	15
Глава 2. Первый алгоритм	17
2.1. Египетское умножение.....	18
2.2. Улучшение алгоритма.....	21
2.3. Заключительные мысли.....	24
Глава 3. Теория чисел в Древней Греции	25
3.1. Геометрические свойства целых чисел	25
3.2. Просеивание простых чисел.....	28
3.3. Реализация и оптимизация кода.....	30
3.4. Совершенные числа.....	35
3.5. Пифагорейская программа	38
3.6. Фатальный изъян в программе	40
3.7. Заключительные мысли.....	44
Глава 4. Алгоритм Евклида	45
4.1. Афины и Александрия.....	45
4.2. Алгоритм Евклида нахождения наибольшей общей меры.....	47
4.3. Тысяча лет без математики	51
4.4. Странная история нуля	52
4.5. Алгоритмы нахождения частного и остатка	54
4.6. Повторное использование кода.....	57
4.7. Доказательство правильности алгоритма.....	60
4.8. Заключительные мысли.....	61
Глава 5. Зарождение современной теории чисел	62
5.1. Простые числа Мерсенна и Ферма	62
5.2. Малая теорема Ферма	66
5.3. Сокращение.....	69
5.4. Доказательство малой теоремы Ферма	72

5.5. Теорема Эйлера	74
5.6. Применение арифметики по модулю	78
5.7. Заключительные мысли.....	79

Глава 6. Абстракция в математике 80

6.1. Группы	80
6.2. Моноиды и полугруппы.....	83
6.3. Некоторые теоремы о группах.....	86
6.4. Подгруппы и циклические группы	88
6.5. Теорема Лагранжа	90
6.6. Теории и модели	94
6.7. Примеры категоричных и некатегоричных теорий.....	97
6.8. Заключительные мысли.....	99

Глава 7. Вывод обобщенного алгоритма 102

7.1. Осмысление требований к алгоритму.....	102
7.2. Требования к А	103
7.3. Требования к N	106
7.4. Новые требования.....	108
7.5. От умножения к возведению в степень	109
7.6. Обобщение операции.....	111
7.7. Вычисление чисел Фибоначчи.....	114
7.8. Заключительные мысли.....	117

Глава 8. Еще об алгебраических структурах 118

8.1. Стевин, полиномы и НОД	118
8.2. Геттинген и немецкая математика	123
8.3. Нётер и рождение общей алгебры.....	128
8.4. Кольца	129
8.5. Умножение матриц и полукольца.....	132
8.6. Приложение: социальные сети и кратчайшие пути	134
8.7. Евклидовы кольца.....	136
8.8. Поля и другие алгебраические структуры.....	137
8.9. Заключительные мысли.....	138

Глава 9. Организация математических знаний 141

9.1. Доказательства	141
9.2. Первая теорема.....	144
9.3. Евклид и аксиоматический метод	147
9.4. Альтернативы евклидовой геометрии.....	148
9.5. Формалистический подход Гильберта.....	151
9.6. Пеано и его аксиомы	153
9.7. Построение арифметики.....	156
9.8. Заключительные мысли.....	159

Глава 10. Основные понятия программирования	160
10.1. Аристотель и абстракции	160
10.2. Значения и типы	162
10.3. Концепции	163
10.4. Итераторы	166
10.5. Категории, операции и характеристики итераторов	167
10.6. Диапазоны	171
10.7. Линейный поиск	173
10.8. Двоичный поиск	174
10.9. Заключительные мысли	178
Глава 11. Алгоритмы перестановки	179
11.1. Перестановки и транспозиции	179
11.2. Обмен диапазонов	182
11.3. Циклическая перестановка	185
11.4. Использование циклов	188
11.5. Обращение	192
11.6. Пространственная сложность	196
11.7. Алгоритмы, адаптирующиеся к объему памяти	197
11.8. Заключительные мысли	198
Глава 12. Обобщения НОД	199
12.1. Аппаратные ограничения и более эффективный алгоритм	199
12.2. Обобщение алгоритма Штайна	202
12.3. Теорема Безу	204
12.4. Расширенный алгоритм Евклида	208
12.5. Применения НОД	212
12.6. Заключительные мысли	213
Глава 13. Реальное приложение	215
13.1. Криптология	215
13.2. Проверка простоты	217
13.3. Тест Миллера–Рабина	220
13.4. Алгоритм RSA: как и почему он работает	222
13.5. Заключительные мысли	225
Глава 14. Заключение	226
Дополнительная литература	228
Приложение А. Обозначения	233
Приложение В. Стандартные приемы доказательства	236
В.1. Доказательство от противного	236
В.2. Доказательство по индукции	237

В.3. Принцип Дирихле	238
----------------------------	-----

Приложение С. Язык C++ для программистов на других языках239

С.1. Шаблонные функции.....	239
С.2. Концепции	240
С.3. Синтаксис объявлений и типизированные константы	241
С.4. Объекты-функции.....	241
С.5. Предусловия, постусловия и утверждения	242
С.6. Алгоритмы и структуры данных STL.....	243
С.7. Итераторы и диапазоны	244
С.8. Использование using для псевдонимов типов и функций типов в C++11	245
С.9. Списки инициализаторов в C++11	246
С.10. Лямбда-функции в C++11	246
С.11. Замечание о ключевом слове inline.....	247

Библиография248

Предметный указатель252