

# Лекции по дискретной математике

А. Шень    М. Вялый    В. Подольский    А. Рубцов    Д. Шварц

Черновой вариант от 8 сентября 2015 г.

# Оглавление

Предисловие	7
<b>I Начальные примеры</b>	<b>9</b>
<b>1 Математическая индукция</b>	<b>10</b>
1.1 Задача о раскраске плоскости . . . . .	10
1.2 Формулировка принципа математической индукции . . . . .	13
1.3 Доказательство формул суммирования по индукции . . . . .	17
1.4 Доказательство неравенств . . . . .	18
1.5 Ненулевые решения однородной линейной системы . . . . .	20
1.6 Коды Грея . . . . .	22
1.7 Ханойская башня . . . . .	24
1.8 Теорема Холла о представителях . . . . .	27
1.9 Задачи для самостоятельного решения . . . . .	28
<b>2 Подсчёты</b>	<b>31</b>
2.1 Правило суммы . . . . .	31
2.2 Рекуррентное соотношение: пример . . . . .	35
2.3 Рекуррентное соотношение: число путей . . . . .	38
2.4 Слова и правило произведения . . . . .	40
2.5 Выбор с ограничениями . . . . .	43
2.6 Подсчёты с кратностью . . . . .	45
2.7 Подмножества и числа сочетаний . . . . .	47
2.8 Ещё о числах сочетаний . . . . .	50
2.8.1 Симметрия . . . . .	50
2.8.2 Сумма чисел в строке . . . . .	51
2.8.3 Знакопеременная сумма . . . . .	52
2.8.4 Слова о включениях и исключениях . . . . .	53
2.8.5 Пути, подмножества, слова . . . . .	54
2.8.6 Соседние числа в строке . . . . .	55
2.8.7 Монеты и перегородки . . . . .	57
2.9 Бином Ньютона и производящие функции . . . . .	58

2.10	Числа Каталана . . . . .	67
2.10.1	Правильные последовательности скобок . . . . .	67
2.10.2	Рекуррентная формула . . . . .	69
2.10.3	Вычисление с помощью отражений . . . . .	71
2.10.4	Вычисление с производящей функцией . . . . .	73
2.10.5	Вычисление с теорией вероятностей и поворотами . . . . .	74
2.10.6	Доказательство по индукции с дробными параметрами . . . . .	76
2.10.7	Неассоциативные произведения, триангуляции и стековый калькулятор . . . . .	77
2.11	Что дальше? . . . . .	81
<b>3</b>	<b>Графы</b>	<b>82</b>
3.1	Какие бывают графы . . . . .	82
3.2	Примеры графов . . . . .	86
3.3	Степени вершин . . . . .	88
3.4	Подграфы . . . . .	92
3.5	Или густо, или пусто. Теорема Рамсея . . . . .	93
3.6	Правильные раскраски . . . . .	95
3.7	Ещё о двудольных графах. Теорема Холла о представителях . . . . .	96
3.8	Достижимость и компоненты связности . . . . .	99
3.9	Деревья . . . . .	103
3.10	Ориентированные графы и перестановки . . . . .	108
3.11	Эйлеровы циклы . . . . .	110
3.12	Задачи для самостоятельного решения . . . . .	114
<b>4</b>	<b>Арифметика остатков</b>	<b>115</b>
4.1	Чётные и нечётные числа . . . . .	115
4.2	Деление на 3 и остатки . . . . .	116
4.3	Деление с остатком . . . . .	117
4.4	Сравнения по модулю . . . . .	120
4.5	Таблицы сложения и умножения по модулю $N$ . . . . .	121
4.6	Обратимые элементы по модулю $N$ . . . . .	123
4.7	Обратимые элементы и диофантовы уравнения . . . . .	126
4.8	Алгоритм Евклида . . . . .	127
4.9	Алгоритм Евклида и диофантовы уравнения . . . . .	129
4.10	Однозначность разложения на множители . . . . .	132
4.11	Китайская теорема об остатках . . . . .	134
4.12	Малая теорема Ферма . . . . .	135
4.13	Функция Эйлера и теорема Эйлера . . . . .	138
4.14	Что дальше? . . . . .	139

<b>II Основные конструкции</b>	<b>141</b>
<b>5 Множества</b>	<b>142</b>
5.1 Основные свойства множеств и операции с множествами . . . . .	142
5.2 Теоретико-множественные тождества . . . . .	147
<b>6 Множества и логика</b>	<b>150</b>
6.1 Логические переменные, логические связки . . . . .	150
6.2 Какие связки необходимы? . . . . .	155
6.2.1 Подсчёт составных высказываний . . . . .	156
6.2.2 Полнота дизъюнкции, конъюнкции и отрицания . . . . .	157
6.2.3 Полнота конъюнкции и отрицания . . . . .	158
6.2.4 Алгебраическое доказательство теоремы 6.1 . . . . .	159
6.3 Формула включений-исключений . . . . .	160
6.3.1 Первое доказательство . . . . .	161
6.3.2 Второе доказательство . . . . .	161
6.3.3 Формула для симметрической разности . . . . .	162
<b>7 Функции</b>	<b>163</b>
7.1 Пример . . . . .	164
7.2 Функции и связанные с ними понятия . . . . .	164
7.2.1 Терминология и обозначения . . . . .	165
7.2.2 Образ множества, полный прообраз . . . . .	167
7.3 Декартово произведение множеств и графики функций . . . . .	169
7.4 Инъекции, сюръекции и биекции . . . . .	172
7.4.1 Определения . . . . .	172
7.4.2 Биекции и сравнение множеств . . . . .	175
7.5 Композиции функций . . . . .	177
7.5.1 Определение . . . . .	177
7.5.2 Ассоциативность . . . . .	179
7.5.3 Обратная функция . . . . .	179
7.5.4 Степени композиций . . . . .	181
7.6 Подсчёты . . . . .	182
7.7 Задачи для самостоятельного решения . . . . .	184
<b>8 Отношения и их графы</b>	<b>186</b>
8.1 Отношения в естественном языке . . . . .	186
8.2 Отношения с точки зрения математики . . . . .	188
8.3 Свойства бинарных отношений . . . . .	189
8.4 Графы, матрицы и бинарные отношения . . . . .	191
8.5 Отношения эквивалентности . . . . .	192
8.6 Композиция отношений . . . . .	194
8.7 Отношения: что дальше? . . . . .	197
8.8 Задачи для самостоятельного решения . . . . .	198

<b>9</b>	<b>Мощность множеств</b>	<b>199</b>
9.1	Равномощные множества . . . . .	199
9.1.1	Определение равномощности . . . . .	199
9.1.2	Свойства равномощности . . . . .	200
9.1.3	Примеры равномощных множеств . . . . .	201
9.2	Счётные множества . . . . .	203
9.2.1	Определение и простейшие примеры . . . . .	203
9.2.2	Свойства счётных множеств . . . . .	204
9.3	Несчётные множества . . . . .	208
9.3.1	Интервал и отрезок равномощны . . . . .	208
9.3.2	Добавление счётного множества . . . . .	209
9.3.3	Числа и последовательности . . . . .	210
9.3.4	Отрезок и квадрат . . . . .	211
9.4	Теорема Кантора–Бернштейна . . . . .	212
9.5	Диагональный аргумент Кантора и сравнение мощностей . . . . .	214
9.5.1	Несчётность отрезка . . . . .	214
9.5.2	Сравнение мощностей . . . . .	216
9.6	Что дальше? . . . . .	218
<b>10</b>	<b>Упорядоченные множества</b>	<b>220</b>
10.1	Отношения порядка . . . . .	220
10.1.1	Отношения строгого частичного порядка . . . . .	220
10.1.2	Строгие и нестрогие порядки . . . . .	221
10.2	Примеры . . . . .	222
10.3	Операции над частично упорядоченными множествами . . . . .	225
10.4	Операции с порядками . . . . .	225
10.5	Какие порядки считать «одинаковыми»? . . . . .	227
10.6	Конечные линейные порядки . . . . .	228
10.7	Порядки и индукция . . . . .	229
10.8	Антицепи . . . . .	230
<b>11</b>	<b>Вероятность: первые шаги</b>	<b>233</b>
11.1	Элементарная теория вероятностей: определения . . . . .	233
11.2	Вероятностный метод . . . . .	236
11.3	Условные вероятности . . . . .	238
11.4	Случайная величина, математическое ожидание . . . . .	241
11.5	Частота орлов при подбрасывании монеты и биномиальные коэффициенты . . . . .	247
11.6	Большие отклонения: неравенство Чернова . . . . .	250
11.7	Подробности для любознательных . . . . .	253
11.7.1	Ещё одна элементарная оценка отношения биномиальных коэффициентов . . . . .	253
11.7.2	Другое доказательство неравенства Чернова . . . . .	254

<b>12 Комбинаторные игры</b>	<b>256</b>
12.1 Позиции . . . . .	256
12.2 Стратегии . . . . .	259
12.3 Разбор с конца . . . . .	261
12.4 Симметричные стратегии . . . . .	265
12.5 Ним . . . . .	269
12.6 Сумма игр и функция Шпрага–Гранди . . . . .	272
<b>III Вычислимость</b>	<b>275</b>
<b>13 Разрешающие деревья</b>	<b>276</b>
13.1 Задача об угадывании числа. Деление пополам. Мощностная нижняя оценка . . . . .	276
13.2 Формализация модели . . . . .	278
13.3 Угадывание числа, неадаптивный вариант задачи . . . . .	279
13.4 Ограниченные модели деревьев разрешения. Сортировка, взвешивания, булевы функции . . . . .	280
13.5 Рассуждение с противником . . . . .	283
<b>14 Булевы схемы и формулы</b>	<b>287</b>
14.1 Булевы схемы . . . . .	287
14.2 Формулы . . . . .	295
<b>15 Вычислимые функции. Перечислимые и разрешимые множества</b>	<b>300</b>
15.1 Вычислимые функции . . . . .	300
15.2 Универсальные вычислимые функции . . . . .	303
15.3 Перечислимые и разрешимые множества . . . . .	305
15.4 Перечислимые множества в терминах вычислимых функций . . . . .	308
15.5 Проекция и графики . . . . .	311
15.6 Перечислимые неразрешимые множества . . . . .	312
15.7 Главные нумерации . . . . .	314
15.8 Рекурсия и теорема о неподвижной точке . . . . .	316
15.9 Теорема Успенского–Райса . . . . .	319
<b>16 Машины Тьюринга. Тезис Чёрча – Тьюринга</b>	<b>320</b>
16.1 Машины Тьюринга . . . . .	320
16.2 Тезис Чёрча – Тьюринга . . . . .	323
16.3 Использование машин Тьюринга в доказательствах . . . . .	324
16.4 Композиция функций, вычислимых МТ, и уборка мусора . . . . .	326
16.5 Многоленточные машины Тьюринга . . . . .	329
16.6 Моделирование многоленточной МТ на одноленточной . . . . .	331
16.7 Универсальная машина Тьюринга . . . . .	333
16.8 Универсальная 3-ленточная машина для 1-ленточных машин . . . . .	335

16.9	Соответствие между абстрактной теорией алгоритмов и МТ . . . . .	338
<b>17</b>	<b>Примеры неразрешимых задач</b>	<b>341</b>
17.1	Почему важна проблема остановки? . . . . .	341
17.2	FRACSTRAN . . . . .	343
17.3	Язык программирования . . . . .	344
17.4	Сведение проблемы остановки: от программ к пасьянсам . . . . .	348
17.5	Задача достижимости на графе подстановок слов . . . . .	350
17.6	Неразрешимость задачи достижимости для графа подстановок слов . . . . .	352

# Предисловие

Слова «дискретная математика», входящие в название этой книжки, употребляют в разных значениях. Иногда противопоставляют «дискретную» математику, говорящую о конечных или по крайней мере хорошо различимых объектах, и «непрерывную», где речь идёт о действительных числах, пределах, непрерывности, производных и т.п. Хотя это противопоставление условно и не всегда применимо (скажем, странно было бы разделять «дискретные» алгебраические кривые над конечным полем и «непрерывные» алгебраические кривые над полем комплексных чисел), некоторый смысл оно имеет.

Говоря о «советской школе дискретной математики», имеют в виду немного другое — прежде всего пионерские работы 1950-х и 1960-х годов (О.Б. Лупанов и его школа) по анализу булевых функций, их классов, обобщений на многозначную логику и др.

Наконец, «дискретная математика» как учебный предмет на младших курсах — это сборная солянка из разных понятий и результатов, которые являются частью базовой математической культуры и необходимы будущим математикам и программистам, но не входят в традиционно сложившиеся курсы начального математического цикла (анализ, алгебра, линейная алгебра).

Именно в этом смысле слова «дискретная математика» используются в названии этой книжки, представляющей собой расширенные записки лекций, читавшихся на факультете компьютерных наук Высшей школы экономики. Получилась она разнородной: некоторые темы (скажем, про математическую индукцию или про комбинаторику) — это то, что вполне могло бы изучаться в школе и даже когда-то изучалось.<sup>1</sup> В других случаях целью является освоение некоторого языка (скажем, что такое пересечение множеств или бинарное отношение). Или это может быть прологом к рассказу о некоторой математической теории, попыткой выделить какое-то минимальное содержательное начало, которое имело бы смысл рассказать даже тем, кто в дальнейшем с этим не столкнётся. Или просто какой-то красивый результат, который трудно найти доступно изложенным.

---

<sup>1</sup> «Гимназист бойко выводил какую-то формулу, со стуком ломая мел о доску, и все писал, несмотря на то, что профессор уже сказал ему: „Довольно“, — и велел нам взять билеты. „Ну что, ежели достанется теория сочетаний!“ — подумал я, доставая дрожащими пальцами билет из мягкой кипы нарезанных бумажек.» (Лев Толстой, *Юность* из цикла *Детство. Отрочество. Юность*, глава XI, *Экзамен математики*. Странно, но потом герой повести с успехом отвечает про бином Ньютона.)

В каждую «лекцию» (в реальности это могло быть несколько лекций) мы старались включить и достаточно трудный материал, чтобы студентам не было скучно. При этом мы не рассчитывали на то, что все это сразу поймут. Такие более трудные места можно и нужно пропускать, если они кажутся непонятными, и двигаться дальше.

Изложение сопровождается задачами; часть из них — это вопросы к слушателям для проверки понимания на лекциях, другие разбирались на семинарах и включались в домашние задания, третьи могут быть предметом самостоятельной работы для заинтересовавшихся студентов и указанием на возможное развитие темы. В общем, как говорил классик, *прими собрание пёстрых глав...*