

# Классические

## НАПРАВЛЕНИЯ В МАТЕМАТИКЕ

Ю. И. МАНИН, А. А. ПАНЧИШКИН

# Введение в современную теорию чисел

Издание 3-е, стереотипное

Москва  
МЦНМО  
2020

15+



УДК 511  
ББК 122.130  
М23

Издано при поддержке  
Фонда развития теоретической  
физики и математики «БАЗИС»

**Манин Ю. И., Панчишкин А. А.**

М23 Введение в современную теорию чисел.— 3-е изд., стереотип.—  
М.: МЦНМО: НМУ, 2020.— 552 с.: ил.

ISBN 978-5-4439-1460-2

Предлагаемая читателю книга — это переработанная и дополненная версия книги «Теория чисел I. Введение в теорию чисел» Ю. И. Манина и А. А. Панчишкина (М.: ВИНТИ, 1989) и ее английского перевода (Encyclopaedia of Mathematical Sciences, v. 49, Springer-Verlag, 1995). Книга состоит из вводных глав к различным разделам теории чисел. Все главы объединены общей концепцией: вместе с читателем пройти от наглядных примеров теоретико-числовых объектов и задач, через общие понятия и теории, развитые на протяжении долгого времени, к некоторым новейшим достижениям и видениям современной математики и наброскам для дальнейших исследований. Новые разделы, написанные для данного издания, включают в себя сжатое изложение доказательства Уайлса великой теоремы Ферма, недавно открытый полиномиальный алгоритм проверки на простоту числа, обзор счета рациональных точек на многообразиях и другие сюжеты; заключительная часть книги посвящена арифметическим когомологиям и некоммутативной геометрии.

Предыдущее издание книги вышло в 2013 г.

ББК 122.130

12+

Научное издание

*Юрий Иванович Манин, Алексей Алексеевич Панчишкин*

ВВЕДЕНИЕ В СОВРЕМЕННУЮ ТЕОРИЮ ЧИСЕЛ

Редактор С. О. Горчинский

Подписано в печать 14.11.2019 г. Формат 60 × 90 1/16. Бумага офсетная.

Печать офсетная. Печ. л. 34,5. Тираж 1500 экз. Заказ № 1285,1287.

Издательство Московского центра непрерывного математического образования.

119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-08-04.

Отпечатано с электронных носителей издательства.



ОАО «Тверской полиграфический комбинат». 170024, г. Тверь, пр-т Ленина, 5.

Телефон: (4822) 44-52-03, 44-50-34. Телефон/факс: (4822) 44-42-15.

Home page: [www.tverpk.ru](http://www.tverpk.ru) Email: [sales@tverpk.ru](mailto:sales@tverpk.ru)

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,  
Москва, Большой Власьевский пер., д. 11. Тел. (499) 241-72-85. E-mail: [biblio@mccme.ru](mailto:biblio@mccme.ru)

ISBN 978-5-4439-1460-2

© Манин Ю. И., Панчишкин А. А., 2013.

© МЦНМО, 2020.

## Оглавление

Предисловие . . . . .	11
Введение . . . . .	13
<b>Часть I. Задачи и приемы</b>	
<b>Глава 1. Элементарная теория чисел . . . . .</b>	<b>21</b>
§1.1. Задачи о целых числах. Делимость и простота . . . . .	21
1.1.1. Системы счисления . . . . .	21
1.1.2. Простые и составные числа . . . . .	22
1.1.3. Основная теорема арифметики и алгоритм Евклида . . . . .	24
1.1.4. Вычисления с классами вычетов . . . . .	26
1.1.5. Квадратичный закон взаимности и распознавание простоты числа . . . . .	29
1.1.6. Распределение простых чисел . . . . .	32
§1.2. Диофантовы уравнения первой и второй степени. . . . .	37
1.2.1. Уравнение $ax + by = c$ . . . . .	37
1.2.2. Диофантовы системы линейных уравнений . . . . .	38
1.2.3. Уравнения второй степени . . . . .	40
1.2.4. Принцип Минковского—Хассе для квадратичных форм . . . . .	42
1.2.5. Уравнение Пелля . . . . .	45
1.2.6. Представление целых чисел и квадратичных форм квадратичны- ми формами . . . . .	46
1.2.7. Связь с аналитической теорией чисел . . . . .	51
1.2.8. Эквивалентность бинарных квадратичных форм . . . . .	54
§1.3. Кубические уравнения . . . . .	56
1.3.1. Проблема существования рационального решения . . . . .	56
1.3.2. Сложение точек на кубической кривой . . . . .	57
1.3.3. Строение группы рациональных точек на кубической кривой . . . . .	59
1.3.4. Кубические сравнения по простому модулю . . . . .	66
§1.4. Задачи о континууме: приближения и непрерывные дроби . . . . .	68
1.4.1. Диофантовы приближения иррациональных чисел . . . . .	68
1.4.2. Ряды Фарея . . . . .	69
1.4.3. Непрерывные (цепные) дроби . . . . .	70
1.4.4. $SL_2$ -эквивалентность чисел . . . . .	71
1.4.5. Периодические цепные дроби. Решение уравнения Пелля . . . . .	72
§1.5. Диофантовы приближения и иррациональность . . . . .	73
1.5.1. Идеи доказательства иррациональности числа $\zeta(3)$ . . . . .	73

1.5.2.	Мера иррациональности числа	74
1.5.3.	Теорема Туэ—Зигеля—Рота, трансцендентные числа, диофантовы уравнения	75
1.5.4.	Вывод тождеств (1.5.1) и (1.5.2)	77
1.5.5.	Рекуррентные последовательности $a_n$ и $b_n$	78
1.5.6.	Трансцендентные числа и седьмая проблема Гильберта	80
1.5.7.	Работа Ю. В. Нестеренко о $e^\pi$ [610]	80
<b>Глава 2. Некоторые приложения элементарной теории чисел</b>		<b>81</b>
§2.1.	Разложение и кодирование с открытым ключом	81
2.1.1.	Временные затраты для разложения чисел	81
2.1.2.	Односторонние функции и кодирование с открытым ключом	81
2.1.3.	Криптосистема с открытым ключом	82
2.1.4.	Статистика и массовое производство простых чисел	84
2.1.5.	Вероятностные методы проверки на простоту	85
2.1.6.	Проблема дискретного логарифма и протокол обмена ключами Диффи—Хеллмана	86
2.1.7.	Вычисление дискретного логарифма для эллиптических кривых над конечными полями (ECDLP)	86
§2.2.	Детерминированные проверки на простоту	87
2.2.1.	Тест на простоту Адлемана—Померанса—Румели: основные идеи	88
2.2.2.	Гауссовы суммы и их использование в тестах на простоту	89
2.2.3.	Детальное описание теста на простоту	93
2.2.4.	Простые числа лежат в классе P	97
2.2.5.	Алгоритм М. Агравала, Н. Каяла и Н. Саксены	100
2.2.6.	Практические и теоретические доказательства простоты. Алгоритм ECPP (Elliptic Curve Primality Proving), построенный Ф. Мореном [142]	101
2.2.7.	Арифметические прогрессии из простых чисел	102
§2.3.	Разложение больших чисел на множители	103
2.3.1.	Сравнение сложности тестов на простоту и разложения чисел на множители	103
2.3.2.	Разложение чисел и квадратичные формы	104
2.3.3.	Вероятностный алгоритм CLASNO	105
2.3.4.	Метод цепных дробей (CFRAC) и вещественные квадратичные поля	107
2.3.5.	Использование эллиптических кривых	110

## Часть II. Идеи и теории

<b>Глава 3. Индукция и рекурсия</b>		<b>115</b>
§3.1.	Элементарная теория чисел с точки зрения логики	115
3.1.1.	Элементарная теория чисел	115
3.1.2.	Логика	116
§3.2.	Диофантовы множества	117

3.2.1.	Перечислимость и диофантовы множества	117
3.2.2.	Диофантовость перечислимых множеств	117
3.2.3.	Свойства диофантовых множеств	118
3.2.4.	Диофантовость и уравнение Пелля	119
3.2.5.	График экспоненты диофантов	119
3.2.6.	Диофантовость и биномиальные коэффициенты	120
3.2.7.	Биномиальные коэффициенты как остатки	120
3.2.8.	Диофантовость факториала	120
3.2.9.	Факториал и алгоритм Евклида	120
3.2.10.	Дополнительные результаты	121
§3.3.	Частично рекурсивные функции и перечислимые множества	122
3.3.1.	Частичные функции и вычислимые функции	122
3.3.2.	Простейшие функции	122
3.3.3.	Элементарные операции над частичными функциями	122
3.3.4.	Частично рекурсивное описание функций	123
3.3.5.	Другие рекурсивные функции	125
3.3.6.	Дальнейшие свойства рекурсивных функций	127
3.3.7.	Связь с множествами уровня	127
3.3.8.	Связь с проекциями множеств уровня	128
3.3.9.	Теорема Матияевича	128
3.3.10.	Существование некоторых биекций	128
3.3.11.	Операции на примитивно перечислимых множествах	130
3.3.12.	Функция Гёделя	130
3.3.13.	Свойства перечислимых множеств	131
§3.4.	Диофантовы множества и алгоритмическая неразрешимость	131
3.4.1.	Алгоритмическая нераспознаваемость и неразрешимость	131
3.4.2.	План доказательства теоремы Матияевича	132
<b>Глава 4. Арифметика алгебраических чисел</b>		<b>134</b>
§4.1.	Алгебраические числа: реализации и геометрия	134
4.1.1.	Присоединение корней многочленов	134
4.1.2.	Расширения Галуа и элементы Фробениуса	136
4.1.3.	Тензорное произведение полей и геометрическое изображение алгебраических чисел	138
4.1.4.	Единицы, логарифмическое отображение и регулятор	140
4.1.5.	Точки решетки в выпуклом теле	142
4.1.6.	Вывод теоремы о единицах из леммы о выпуклом теле	144
§4.2.	Разложение простых идеалов, дедекиндовы кольца и нормирования	145
4.2.1.	Простые идеалы и однозначность разложения на множители	145
4.2.2.	Конечность числа классов	147
4.2.3.	Разложение простых идеалов в расширениях	148
4.2.4.	Разложение простых идеалов в циклотомических полях	150
4.2.5.	Простые идеалы, показатели и нормирования	152
§4.3.	Локальные и глобальные методы	154
4.3.1.	$p$ -адические числа	154
4.3.2.	Приложения $p$ -адических чисел к решению сравнений	158

4.3.3.	Символ Гильберта	159
4.3.4.	Алгебраические расширения поля $\mathbb{Q}_p$ и поля Тэйта	161
4.3.5.	Нормализованные нормирования	163
4.3.6.	Точки числовых полей. Формула произведения	165
4.3.7.	Адели и иделы	167
4.3.8.	Геометрия аделей и иделов	169
§4.4.	Теория полей классов	174
4.4.1.	Абелевы расширения поля рациональных чисел	174
4.4.2.	Элементы Фробениуса числовых полей и отображение взаимности Артина	177
4.4.3.	Теорема Чеботарева о плотности простых идеалов	179
4.4.4.	Закон разложения и отображение взаимности	179
4.4.5.	Ядро отображения взаимности	180
4.4.6.	Символ Артина	181
4.4.7.	Глобальные свойства символа Артина	181
4.4.8.	Связь символа Артина и локальных символов	183
4.4.9.	Свойства локального символа	184
4.4.10.	Явная конструкция абелевых расширений локального поля и вычисление локального символа	185
4.4.11.	Абелевы расширения числовых и функциональных полей	188
§4.5.	Группа Галуа в арифметических задачах	191
4.5.1.	Деление круга на $n$ равных частей	191
4.5.2.	Расширения Куммера и символ степенного вычета	195
4.5.3.	Когомологии Галуа	198
4.5.4.	Когомологическое определение локального символа	201
4.5.5.	Группа Брауэра, закон взаимности и принцип Минковского—Хассе	203
<b>Глава 5.</b>	<b>Арифметика алгебраических многообразий</b>	<b>209</b>
§5.1.	Арифметические многообразия: схемы конечного типа над кольцом целых чисел	209
5.1.1.	Решение уравнений и кольца	209
5.1.2.	Множество решений систем	209
5.1.3.	Пример: «язык сравнений»	209
5.1.4.	Эквивалентность систем уравнений	210
5.1.5.	Решения системы как гомоморфизмы $K$ -алгебр	210
5.1.6.	Спектр кольца	211
5.1.7.	Функции на спектрах	211
5.1.8.	Топология пространства $\text{Spec } A$	212
5.1.9.	Схемы	215
5.1.10.	Точки схемы со значениями в кольцах	217
5.1.11.	Решения уравнений и точки схем	217
5.1.12.	Теорема Шевалле	218
5.1.13.	Некоторые геометрические понятия	219
§5.2.	Геометрические методы изучения диофантовых уравнений	221
5.2.1.	Основные вопросы	221

5.2.2.	Геометрическая классификация	223
5.2.3.	Существование рациональных точек и препятствия к принципу Хассе	224
5.2.4.	Конечные и бесконечные множества решений	227
5.2.5.	Число точек ограниченной высоты	229
5.2.6.	Высота и геометрия Аракелова	233
5.2.7.	Рациональные многообразия	234
§5.3.	Эллиптические кривые, абелевы многообразия и линейные группы	236
5.3.1.	Алгебраические кривые и римановы поверхности	236
5.3.2.	Эллиптические кривые	238
5.3.3.	Кривая Тэйта и ее точки конечного порядка	245
5.3.4.	Теорема Морделла—Вейля и когомологии Галуа	247
5.3.5.	Абелевы многообразия и якобианы	252
5.3.6.	Формула Зигеля и числа Тамагавы	259
§5.4.	Диофантовы уравнения и представления Галуа	266
5.4.1.	Модуль Тэйта эллиптической кривой	266
5.4.2.	Теория комплексного умножения	268
5.4.3.	Характеры $l$ -адических представлений	271
5.4.4.	Представления в характеристике $p$	272
5.4.5.	Модуль Тэйта числового поля	273
§5.5.	Теорема Фальтингса и проблемы конечности в диофантовой геометрии	276
5.5.1.	Сведение гипотезы Морделла к гипотезе Шафаревича	276
5.5.2.	Теорема Шафаревича	278
5.5.3.	Переход к абелевым многообразиям	279
5.5.4.	Проблемы конечности и гипотеза Тэйта	281
5.5.5.	Сведение гипотез Тэйта к свойству конечности для изогений	282
5.5.6.	Высота Фальтингса—Аракелова	284
5.5.7.	Гипотеза Т и поведение высоты при изогениях	287
<b>Глава 6.</b>	<b>Дзета-функции и модулярные формы</b>	<b>289</b>
§6.1.	Дзета-функции арифметических схем	289
6.1.1.	Определение дзета-функций	289
6.1.2.	Аналитическое продолжение дзета-функций	291
6.1.3.	Схемы над конечным полем и теорема Делиня	291
6.1.4.	Дзета-функции и тригонометрические суммы	295
§6.2.	$L$ -функции, теория Тэйта и явные формулы	300
6.2.1.	$L$ -функции рациональных представлений Галуа	300
6.2.2.	Формализм Артина	302
6.2.3.	Пример: дзета-функция Дедекинда	305
6.2.4.	Характеры Гекке и теория Тэйта	306
6.2.5.	Явные формулы	314
6.2.6.	Группа А. Вейля и ее представления	316
6.2.7.	Дзета-функции, $L$ -функции и мотивы	318
§6.3.	Модулярные формы и эйлеровы произведения	324
6.3.1.	Связь между алгебраическими многообразиями и $L$ -функциями	324
6.3.2.	Классические модулярные формы	325

6.3.3.	Приложение: кривая Тэйта и полустабильные эллиптические кривые	327
6.3.4.	Аналитические семейства эллиптических кривых и конгруэнц-подгруппы	329
6.3.5.	Модулярные формы относительно конгруэнц-подгрупп	329
6.3.6.	Теория Гекке	332
6.3.7.	Примитивные формы	337
6.3.8.	Обратная теорема в форме Вейля	339
§6.4.	Модулярные формы и представления Галуа	344
6.4.1.	Сравнения Рамануджана и представления Галуа	344
6.4.2.	Связь с конструкцией Эйхлера—Шимуры	346
6.4.3.	Гипотеза Шимуры—Таниямы—Вейля	347
6.4.4.	Гипотеза Берча—Свиннертон-Дайера	348
6.4.5.	Гипотеза Артина и параболические формы	355
6.4.6.	Модулярные представления над конечными полями	358
§6.5.	Автоморфные формы и программа Ленглендса	359
6.5.1.	Связь классических модулярных форм с теорией представлений	359
6.5.2.	Автоморфные $L$ -функции	363
6.5.3.	Принцип функториальности Ленглендса	366
6.5.4.	Автоморфные формы и гипотезы Ленглендса	367
<b>Глава 7.</b>	<b>Великая теорема Ферма и семейства модулярных форм</b>	<b>369</b>
§7.1.	Гипотеза Шимуры—Таниямы—Вейля и высшие законы взаимности	369
7.1.1.	Задача Пьера де Ферма (1601—1665)	369
7.1.2.	Ошибка Г. Ламе	370
7.1.3.	Краткий обзор замечательного доказательства Уайлса	371
7.1.4.	STW-гипотеза	373
7.1.5.	Связь с квадратичным законом взаимности	373
7.1.6.	Полное доказательство STW-гипотезы	374
7.1.7.	Модулярность полустабильных кривых	377
7.1.8.	Структура доказательства теоремы 7.13 (полустабильной STW-гипотезы)	378
§7.2.	Теорема Ленглендса—Туннелла и модулярность по модулю 3	380
7.2.1.	Представления Галуа: подготовка	380
7.2.2.	Модулярность по модулю $p$	382
7.2.3.	Переход от параболических форм веса один к параболическим формам веса два	383
7.2.4.	Предварительный обзор этапов доказательства теоремы 7.13 о модулярности	384
§7.3.	Модулярность представлений Галуа и универсальные кольца деформаций	385
7.3.1.	Представления Галуа над локальными нётеровыми алгебрами	385
7.3.2.	Деформации представлений Галуа	386
7.3.3.	Модулярные представления Галуа	388
7.3.4.	Допустимые деформации и модулярные деформации	390
7.3.5.	Универсальные кольца деформаций	392

§7.4.	Основная теорема Уайлса и критерии изоморфизма локальных колец	394
7.4.1.	Идеи доказательства основной теоремы 7.33	394
7.4.2.	Сюръективность отображения $\varphi_{\Sigma}$	395
7.4.3.	Построения универсального кольца деформаций $R_{\Sigma}$	396
7.4.4.	Набросок построения универсального кольца модулярных деформаций $T_{\Sigma}$	397
7.4.5.	Универсальность и теорема плотности Чеботарева	399
7.4.6.	Критерии изоморфизма локальных колец	399
7.4.7.	Второй критерий изоморфизма локальных колец и $I$ -структуры	400
§7.5.	Шаг индукции по Уайлсу: применение критериев и когомологии Галуа	401
7.5.1.	Шаг индукции по Уайлсу при доказательстве основной теоремы 7.33	401
7.5.2.	Формула, связывающая $\#\Phi_{R_{\Sigma}}$ и $\#\Phi_{R_{\Sigma'}}$ : подготовка	403
7.5.3.	Группа Зельмера и $\Phi_{R_{\Sigma}}$	404
7.5.4.	Инфинитезимальные деформации	404
7.5.5.	Деформации типа $\mathcal{D}_{\Sigma}$	406
§7.6.	Относительный инвариант, основное неравенство и минимальный случай	410
7.6.1.	Относительный инвариант	410
7.6.2.	Основное неравенство	412
7.6.3.	Минимальный случай	414
§7.7.	Окончание доказательства Уайлса и теорема об абсолютной неприводимости	416
7.7.1.	Теорема об абсолютной неприводимости	416
7.7.2.	От $p = 3$ к $p = 5$	419
7.7.3.	Семейства эллиптических кривых с фиксированным $\bar{\rho}_{3,E}$	420
7.7.4.	Окончание доказательства	422

### Часть III. Аналогии и видения

<b>Глава III-0.</b>	<b>Вводный очерк части III: мотивировки и общее описание</b>	<b>427</b>
§III.1.	Аналогии и различия между числами и функциями: точка на бесконечности, архимедовы свойства и т. д.	427
III.1.1.	Формула Коши о вычетах и формула произведения	427
III.1.2.	Арифметические многообразия	428
III.1.3.	Бесконечно малые окрестности слоев	428
§III.2.	Геометрия Аракелова, слой над бесконечностью, циклы и функции Грина (по Жилле—Суле)	429
III.2.1.	Арифметические группы Чжоу	430
III.2.2.	Арифметическая теория пересечений и теорема Римана—Роха	431
III.2.3.	Геометрическое описание замкнутых слоев над бесконечностью	433
§III.3.	Теория дзета-функций, локальные множители для $\infty$ , $\Gamma$ -множители Серра и общее описание дзета-функций как определителей арифметических Фробениусов: программа Денингера	435
III.3.1.	Архимедовы $L$ -множители	437
III.3.2.	Формулы Денингера	437

§III.4. Предположение, что недостающие геометрические объекты — некоммутативные пространства. . . . .	438
III.4.1. Типы и примеры некоммутативных пространств и как с ними обращаться. Некоммутативная геометрия и арифметика . . . . .	438
III.4.2. Общие сведения о спектральных тройках . . . . .	442
III.4.3. Содержание части III: описание основных этапов данной программы . . . . .	443
<b>Глава 8. Геометрия Аракелова и некоммутативная геометрия (по К. Конзани и М. Марколли, [278]) . . . . .</b>	<b>446</b>
§8.1. Униформизация Шоттки и геометрия Аракелова. . . . .	446
8.1.1. Мотивировки и контекст работы Конзани—Марколли . . . . .	446
8.1.2. Аналитическая конструкция вырождающихся кривых над полными локальными полями и геометрия Аракелова (по Мамфорду, см. [601]) . . . . .	447
8.1.3. Группы Шоттки и новые перспективы в геометрии Аракелова . . . . .	452
8.1.4. Гиперболические тела с ручками . . . . .	456
8.1.5. Геометрия Аракелова и гиперболическая геометрия . . . . .	459
§8.2. Когомологические конструкции, архимедов оператор Фробениуса и регуляризованные определители. . . . .	463
8.2.1. Архимедовы когомологии . . . . .	463
8.2.2. Локальный множитель и архимедовы когомологии . . . . .	467
8.2.3. Когомологические конструкции . . . . .	468
8.2.4. Дзета-функция специального слоя и кручение Райдемайстера . . . . .	469
§8.3. Спектральные тройки, динамика и дзета-функции. . . . .	472
8.3.1. Динамическая теория на бесконечности . . . . .	475
8.3.2. Гомотопический фактор . . . . .	476
8.3.3. Фильтрация . . . . .	478
8.3.4. Гильбертово пространство и градуировка . . . . .	479
8.3.5. Алгебра Кунца—Кригера . . . . .	479
8.3.6. Арифметические поверхности: гомологии и когомологии . . . . .	482
8.3.7. Архимедовы множители с точки зрения динамики . . . . .	484
8.3.8. Динамическая теория для кривых Мамфорда . . . . .	484
8.3.9. Когомологии пространства $\mathcal{W}(\Delta/\Gamma)_T$ . . . . .	488
8.3.10. Спектральные тройки и кривые Мамфорда . . . . .	491
§8.4. Редукция по модулю $\infty$ . . . . .	492
8.4.1. Гомотопические факторы и «редукция по модулю бесконечности» . . . . .	492
8.4.2. Отображение Баума—Конна . . . . .	494
Литература . . . . .	496
Предметный указатель . . . . .	546