

ЗИБОРЕВИЧ ИРШАФАРЕВИЧ

ТЕОРИЯ ЧИСЕЛ



З. И. БОРЕВИЧ, И. Р. ШАФАРЕВИЧ

ТЕОРИЯ ЧИСЕЛ

ИЗДАНИЕ ВТОРОЕ



ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1972

517.1

Б 82

УДК 511.2

Теория чисел. Боревич Э. И., Шафаревич И. Р. Главная редакция физико-математической литературы изд-ва «Наука», 1972.

В книге излагается ряд методов современной теории чисел. Изложение иллюстрируется рассмотрением большого числа конкретных теоретико-числовых вопросов, относящихся главным образом к неопределенным уравнениям. Основное внимание уделено алгебраическим методам, но заметное место занимают также геометрический и аналитический методы. В книге изложены как классические вопросы, так и некоторые новейшие достижения.

Книга рассчитана на студентов, аспирантов и научных работников, работающих в области алгебры и теории чисел. Для ее понимания достаточно знакомства с математикой в объеме первых двух курсов физико-математических факультетов университетов или педагогических институтов.

ОГЛАВЛЕНИЕ

Предисловие	7
Глава I. Сравнения	9
§ 1. Сравнения по простому модулю	11
1. Суммы степеней вычетов (11). 2. Теоремы о числе реше- ний сравнений (12). 3. Квадратичные формы по простому модулю (14).	
§ 2. Тригонометрические суммы	17
1. Сравнения и тригонометрические суммы (17). 2. Суммы степеней (20). 3. Модуль гауссовой суммы (23).	
§ 3. p -адические числа	27
1. Целые p -адические числа (27). 2. Кольцо целых p -адических чисел (30). 3. Дробные p -адические числа (34). 4. Сходи- мость в поле p -адических чисел (35).	
§ 4. Аксиоматическая характеристика поля p -адических чисел	42
1. Метризованные поля (42). 2. Метрики поля рациональных чисел (47).	
§ 5. Сравнения и целые p -адические числа	51
1. Сравнения и уравнения в кольце O_p (51). 2. О разре- шимости некоторых сравнений (53).	
§ 6. Квадратичные формы с p -адическими коэффициентами	60
1. Квадраты в поле p -адических чисел (60). 2. Представ- ление нуля p -адическими квадратичными формами (62). 3. Бинарные формы (65). 4. Эквивалентность бинарных форм (69). 5. Замечания о формах высших степеней (70).	
§ 7. Рациональные квадратичные формы	76
1. Теорема Минковского — Хассе (76). 2. Формы от трех переменных (77). 3. Формы от четырех переменных (84). 4. Формы от пяти и более переменных (86). 5. Рациональ- ная эквивалентность (87). 6. Замечания о формах высших степеней (88).	
Глава II. Представление чисел разложимыми формами	92
§ 1. Разложимые формы	94
1. Целочисленная эквивалентность форм (94). 2. Постро- ение разложимых форм (95). 3. Модули (98).	
§ 2. Полные модули и их кольца множителей	101
1. Базис модуля (101). 2. Кольца множителей (105). 3. Едини- цы (107). 4. Максимальный порядок (109). 5. Дискриминант полного модуля (111).	
§ 3. Геометрический метод	114
1. Геометрическое изображение алгебраических чисел (114). 2. Решетки (119). 3. Логарифмическое пространство (123). 4. Геометрическое изображение единиц (124). 5. Первые све- дения о группе единиц (126).	

§ 4. Группа единиц	127
1. Критерий полноты решетки (127). 2. Лемма Минковского (128). 3. Структура группы единиц (133). 4. Регулятор (135).	
§ 5. Решение задачи о представлениях рациональных чисел полными разложимыми формами	138
1. Единицы с нормой $+1$ (138). 2. Общий вид решений уравнения $N(\mu) = a$ (139). 3. Эффективное построение системы основных единиц (140). 4. Числа модуля с данной нормой (144).	
§ 6. Классы модулей	145
1. Норма модуля (145). 2. Конечность числа классов (148).	
§ 7. Представление чисел бинарными квадратичными формами	151
1. Квадратичные поля (151). 2. Порядки в квадратичном поле (152). 3. Единицы (154). 4. Модули (158). 5. Соответствие между модулями и формами (161). 6. Представление чисел бинарными формами и подобие модулей (164). 7. Подобие модулей в мнимом квадратичном поле (167).	
<i>Глава III. Теория делимости</i>	178
§ 1. Некоторые частные случаи теоремы Ферма	178
1. Связь теоремы Ферма с разложением на множители (178). 2. Кольцо $Z[\zeta]$ (180). 3. Теорема Ферма в случае однозначности разложения на множители (184).	
§ 2. Разложение на множители	188
1. Простые множители (188). 2. Однозначность разложения (189). 3. Примеры неоднозначного разложения (191).	
§ 3. Дивизоры	194
1. Аксиоматическое описание дивизоров (194). 2. Единственность (196). 3. Целозамкнутость колец с теорией дивизоров (199). 4. Связь теории дивизоров с показателями (200).	
§ 4. Показатели	207
1. Простейшие свойства показателей (207). 2. Независимость показателей (208). 3. Продолжение показателей (211). 4. Существование продолжений (216).	
§ 5. Теория дивизоров для конечного расширения	220
1. Существование (220). 2. Норма дивизоров (221). 3. Степень инерции (225). 4. Конечность числа разветвленных простых дивизоров (231).	
§ 6. Дедекиндовы кольца	236
1. Сравнения по модулю дивизора (236). 2. Сравнения в дедекиндовых кольцах (237). 3. Дивизоры и идеалы (239). 4. Дробные дивизоры (241).	
§ 7. Дивизоры в полях алгебраических чисел	246
1. Абсолютная норма дивизора (246). 2. Классы дивизоров (250). 3. Приложение к теореме Ферма (254). 4. Вопросы эффективности (257).	
§ 8. Квадратичное поле	267
1. Простые дивизоры (267). 2. Закон разложения (270). 3. Представление чисел бинарными квадратичными формами (273). 4. Роды дивизоров (279).	
<i>Глава IV. Локальный метод</i>	286
§ 1. Поля, полные относительно показателей	286
1. Пополнение поля по показателю (286). 2. Представление элементов в виде рядов (288). 3. Конечные расширения полного поля с показателем (291). 4. Целые элементы (293). 5. Поля формальных степенных рядов (297).	

§ 2. Конечные расширения поля с показателем	302
§ 3. Разложение многочленов на множители в полном поле с показателем	308
§ 4. Метрики поля алгебраических чисел	313
1. Описание метрик (313). 2. Соотношение между метриками (318).	
§ 5. Аналитические функции в полных полях	319
1. Степенные ряды (319). 2. Показательная и логарифмическая функция (323).	
§ 6. Метод Сколема	327
1. Представление чисел неполными разложимыми формами (328). 2. Связь с локальными аналитическими многообразиями (329). 3. Теорема Туэ (333). 4. Замечания о формах с большим числом переменных (338).	
§ 7. Локальные аналитические многообразия	341
Глава V. Аналитический метод	349
§ 1. Аналитическая формула для числа классов дивизоров	349
1. Дзета-функция Дедекинда (349). 2. Фундаментальная область (353). 3. Вычисление объема (356). 4. Принцип Дирихле (361). 5. Тожество Эйлера (364).	
§ 2. Число классов дивизоров кругового поля	366
1. Неприводимость кругового многочлена (367). 2. Закон разложения в круговом поле (368). 3. Выражение h через значения L -рядов (370). 4. Суммирование рядов $L(1, \chi)$ (374). 5. Ряды $L(1, \chi)$ для примитивных характеров (377).	
§ 3. Простые дивизоры первой степени	381
1. Существование простых дивизоров первой степени (381). 2. Характеризация нормальных расширений законами разложения простых дивизоров первой степени (383). 3. Теорема Дирихле о простых числах в арифметической прогрессии (386).	
§ 4. Число классов дивизоров квадратичного поля	389
1. Формула для числа классов дивизоров (389). 2. Характер квадратичного поля (395). 3. Гауссовы суммы для квадратичных характеров (396).	
§ 5. Число классов дивизоров поля деления круга на простое число частей	404
1. Разложение числа h на два множителя (404). 2. Множитель h_0 (408). 3. Множитель h^* (411). 4. Условие взаимной простоты h^* с l (415). 5. Замечание об операторной структуре группы классов дивизоров (417).	
§ 6. Условие регулярности	420
1. Поле \mathbb{I} -адических чисел (420). 2. Некоторые вспомогательные сравнения (424). 3. Базис вещественных целых \mathbb{I} -адических чисел в случае $(h^*, l) = 1$ (427). 4. Критерий регулярности и лемма Куммера (429).	
§ 7. Второй случай теоремы Ферма для регулярных показателей	431
1. Теорема Ферма (431). 2. Бесконечность числа иррегулярных простых чисел (435).	
§ 8. Числа Бернулли	436
Алгебраическое дополнение	444
§ 1. Квадратичные формы над произвольным полем характеристики $\neq 2$	444
1. Эквивалентность квадратичных форм (444). 2. Прямая сумма квадратичных форм (446). 3. Представление элементов поля (447). 4. Бинарные квадратичные формы (449).	

§ 2. Алгебраические расширения	451
1. Конечные расширения (451). 2. Норма и след (454). 3. Се- парабельные расширения (457). 4. Нормальные рас- ширения (460).	
§ 3. Конечные поля	462
§ 4. Некоторые сведения о коммутативных кольцах	466
1. Делимость в кольцах (466). 2. Идеалы (467). 3. Целые элементы (469). 4. Дробные идеалы (471).	
§ 5. Характеры	473
1. Строение конечных абелевых групп (473). 2. Характеры конечных абелевых групп (473). 3. Числовые характеры (477).	
Таблицы	481
Предметный указатель	494