



**Уральский
федеральный
университет**

имени первого Президента
России Б.Н.Ельцина

**Институт радиоэлектроники
и информационных
технологий**

**Б. М. ВЕРЕТЕННИКОВ
М. М. МИХАЛЕВА**

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Часть I

Учебное пособие

Министерство образования и науки Российской Федерации
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина

Б. М. Веретенников, М. М. Михалева

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Часть I

*Рекомендовано методическим советом УрФУ
в качестве **учебного пособия** для студентов,
обучающихся по направлению подготовки
010500.68 – Теоретические основы информатики*

Екатеринбург
Издательство Уральского университета
2014

УДК 511+512(075.8)
ББК 22.13я73+22.14я73
В31

Рецензенты:

кафедра Прикладной математики Уральского государственного экономического университета; протокол №1 от 29.08.2013 г. (завкафедрой, канд. физ.-мат. наук, доц. Ю. Б. Мельников);

И. Н. Белоусов, канд. физ.-мат. наук (Институт математики и механики УрО РАН)

Научный редактор – канд. физ.-мат. наук, доц. Н. В. Чуксина

Веретенников, Б. М.

В31 Алгебра и теория чисел : учебное пособие / Б. М. Веретенников, М. М. Михалева. – Екатеринбург : Изд-во Урал. ун-та, 2014. – Ч. 1. – 52 с.

ISBN 978-5-7996-1193-4 (ч. 1)

ISBN 978-5-7996-1166-8

Учебное пособие включает в себя такие разделы курса «Алгебра и теория чисел», как элементарная теория чисел, теория сравнений, цепные и непрерывные дроби, p -адические числа. Предназначено для студентов института радиоэлектроники и информационных технологий – РТФ.

Библиогр.: 8 назв.

УДК 511+512(075.8)

ББК 22.13я73+22.14я73

ISBN 978-5-7996-1193-4 (ч. 1)
ISBN 978-5-7996-1166-8

© Уральский федеральный
университет, 2014

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
ГЛАВА I. ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ЧИСЕЛ	5
§ 1. Основные теоремы	5
§ 2. Наибольший общий делитель целых чисел (НОД)	6
§ 3. Взаимно простые числа	8
ГЛАВА II. ТЕОРИЯ СРАВНЕНИЙ.....	9
§ 4. Основные понятия.....	9
§ 5. Алгебраические действия с классами вычетов.....	10
§ 6. Обратимые элементы в $\mathbb{Z}/n\mathbb{Z}$	12
§ 7. Функция Эйлера и ее свойства.....	15
§ 8. Решение линейных сравнений с помощью функции Эйлера....	18
§ 9. Китайская теорема об остатках.....	18
§ 10. Обобщение китайской теоремы об остатках	21
§ 11. Примеры решения задач по теории сравнений	21
ГЛАВА III. ЦЕПНЫЕ И НЕПРЕРЫВНЫЕ ДРОБИ	28
§ 12. Разложение рационального числа в цепную дробь.....	28
§ 13. Подходящие дроби	29
§ 14. Применение цепных дробей к решению линейных сравнений	31
§ 15. Непрерывные дроби	33
§ 16. Разложение по степеням двучлена по схеме Горнера.....	37
§ 17. Применение цепных дробей к приближенному решению уравнений.....	38
ГЛАВА IV. СРАВНЕНИЯ ПО МОДУЛЮ p^k И p -АДИЧЕСКИЕ ЧИСЛА.....	41
§ 18. Решение сравнений по модулю p^k	41
§ 19. p -адические числа	44
СПИСОК ЛИТЕРАТУРЫ	48

ВВЕДЕНИЕ

Данное пособие базируется на лекциях, которые читались первым автором на радиотехническом факультете, сейчас ИРИТ–РтФ, студентам специальности МОАИС (математическое обеспечение и администрирование информационных систем) в течение ряда лет. В предлагаемой читателям первой части этого пособия рассматриваются элементарная теория чисел, теория сравнений, цепные и непрерывные дроби и немного теории p -адических чисел. Почти все теоремы приведены с доказательствами, разобрано много примеров вычислительного характера и приведено достаточно задач для самостоятельного решения. Мы надеемся, что усвоив методы, изложенные в пособии, читатель сможет применять их в различных областях математики и информатики, а также будет готов к изучению следующих разделов теории чисел: квадратичные вычеты, первообразные корни, алгебраическая теория чисел и т. д. Пособие может быть использовано в учебном процессе студентами и преподавателями Уральского федерального университета.