

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П. КОРОЛЕВА»

В.М. ЧЕРНОВ, А.О.КОРЕПАНОВ

ТЕОРЕТИКО-ЧИСЛОВЫЕ
ПРЕОБРАЗОВАНИЯ В ЗАДАЧАХ
ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

*Утверждено Редакционно-издательским советом университета
в качестве учебного пособия*

САМАРА
Издательство СГАУ
2006

УДК 519.2
ББК 22.343
Ч493



**Инновационная образовательная программа
"Развитие центра компетенции и подготовка
специалистов мирового уровня в области аэро-
космических и геоинформационных технологий"**

Рецензенты: д-р. техн. наук, проф. В.Г. Карташевский,
д-р. физ.-мат. наук, проф. А.И. Жданов.

Чернов В.М.

Ч493 **Теоретико-числовые преобразования в задачах цифровой
обработки сигналов: учеб. пособие / В.М. Чернов, А.О. Коре-
панов – Самара: Изд-во Самар. гос. аэрокосм. ун-та, 2006. –
112 с.**

ISBN 5-7883-0398-2

Содержание пособия относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел).

Специалисты в области анализа и обработки цифровой информации давно и успешно используют алгебраические и теоретико-числовые методы, прежде всего в таких областях, как криптография, корректирующие коды, синтез быстрых алгоритмов дискретных ортогональных преобразований. Несмотря на это, существует относительно мало доступной монографической литературы, охватывающей не только одну или несколько из указанных уже традиционных областей применения методов абстрактной алгебры и теории чисел к решению задач информатики, но и рассматривающей относительно новые приложения указанных математических методов и теорий к решению перспективных задач анализа цифровых сигналов. Ряд монографий отечественных или зарубежных авторов давно уже стал библиографической редкостью, а книги, изданные за рубежом, практически недоступны широкому кругу специалистов. Данное пособие ставит своей целью частичное восполнение указанного пробела.

Предназначено для студентов специальностей и направлений «Прикладные математика и физика», «Прикладные математика и информатика».

УДК 519.2
ББК 22.343

ISBN 5-7883-0398-2

© Чернов В.М., Корепанов А.О., 2006
© Самарский государственный
аэрокосмический университет, 2006

ОГЛАВЛЕНИЕ

Введение	6
Часть 1. Модулярная арифметика и быстрое "безошибочное"	
вычисление свертки	8
1.1. Постановка задачи, основные идеи	8
1.1.1. Теоретико-числовые преобразования и целочисленные	
свертки	8
1.2. Реализация арифметических операций для модулей	
специального вида	11
1.2.1. Арифметика в полях по модулю числа Мерсенна	11
1.2.2. Арифметика в полях по модулю числа Ферма	13
1.2.3. Арифметика в полях по модулю числа Голomba	15
1.3. Редуцированные системы счисления в конечных полях	16
1.3.1. Двоично-избыточная система счисления	16
1.3.2. Редуцированные системы счисления в комплексном поле	
Мерсенна	19
1.4. Алгоритмы вычисления свертки в полях p -адических	
чисел	24
1.4.1. p -адические числа	24
1.4.2. Вычисление свертки с помощью ТЧП по модулю степени	
простого числа	27
1.4.3. Реализация арифметических операций в кольце классов	
вычетов по модулю степени числа Мерсенна	30
1.4.4. Реализация арифметических операций в кольце классов	
вычетов по модулю степени числа Ферма	31
1.5. Алгоритмы вычисления свертки в расширениях	
неархимедово нормированных полей	33
1.5.1. Продолжение p -адических нормирований на	
квадратичные расширения поля \mathbb{Q}	33
1.5.2. Метрическая форма китайской теоремы об остатках	34