

# С Ъ Д Ъ Р Ж А Н И Е

<b>Глава 1. Аритметика</b>	5
1.1. Аксиоми на Пеано. Делимост и деление с остатък.	5
1.2. Най-голям общ делител. Алгоритъм на Евклид.	10
1.3 Прости числа. Основна теорема на аритметиката.	15
1.4 Бройни системи. Сложност на аритметичните операции.	18
<b>Глава 2. Разпределение на простите числа.</b>	25
2.1. Аритметични функции.	25
2.2. Разпределение на простите числа.	34
<b>Глава 3. Сравнения</b>	39
3.1. Елементарни свойства на сравненията.	39
3.2. Линейни сравненията. Китайска теорема за остатъците.	43
3.3. Сравненията от втора и по-висока степен.	46
3.4. Примитивни корени и индекси.	52
3.5. Съществуване на примитивен корен.	55
<b>Глава 4. Квадратични остатъци.</b>	59
4.1. Квадратични и $k$ -степенни остатъци.	59
4.2. Квадратичен закон за реципрочност.	64
4.3. Представяне в сума от квадрати.	66
<b>Глава 5. Криптография.</b>	69
5.1. Цели, задачи и основни понятия.	69
5.2. Криптографски примитиви и механизми.	74
5.3. Електронен подпис.	81
5.4. Генериране на големи прости числа.	83
<b>Глава 6. Теоретико-числови преобразования.</b>	89
6.1. Дискретно преобразование на Фурие.	89
<b>Глава 7. Нелинейни диофантови уравнения.</b>	95
7.1. Диофантови уравнения от втора степен.	95
7.2. Уравнения от вида $x^2 - Dy^2 = F$ .	98
<b>Литература.</b>	107

## ПРЕДГОВОР

Предложените на вниманието на читателя “Лекции по теория на числата” представляват съдържанието на курса “Увод в теория на числата” четен от автора във Факултета по математика и информатика на СУ “Св. Климент Охридски”.

Използвам случая да изразя благодарност към колегите от катедра “Алгебра” за предоставената ми възможност да чета този курс и за оказваното от тях съдействие.

Н. Манев