

С Ъ Д Ъ Р Ж А Н И Е

Глава 1. Аритметика	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
1.5. Верижни дроби.	24
Глава 2. Разпределение на простите числа.	31
2.1. Аритметични функции.	31
2.2. Разпределение на простите числа.	40
Глава 3. Сравнения	45
3.1. Елементарни свойства на сравненията.	45
3.2. Линейни сравненията. Китайска теорема за остатъците.	49
3.3. Сравненията от втора и по-висока степен.	52
3.4. Примитивни корени и индекси.	59
3.5. Съществуване на примитивен корен.	62
Глава 4. Квадратични остатъци.	65
4.1. Квадратични и k -степенни остатъци.	65
4.2. Квадратичен закон за реципрочност.	70
4.3. Представяне в сума от квадрати.	72
Глава 5. Нелинейни диофантови уравнения.	75
5.1. Диофантови уравнения от втора степен.	75
5.2. Уравнения от вида $x^2 - Dy^2 = F$.	78
Глава 6. Криптография.	85
6.1. Цели, задачи и основни понятия.	85
6.2. Криптографски примитиви и механизми.	90
6.3. Електронен подпис.	97
6.4. Генериране на големи прости числа.	99
Глава 7. Теоретико-числови преобразования.	105
7.1. Дискретно преобразование на Фурие.	105
Глава 8. Модулярна аритметика.	111

8.1. Извличане на квадратен корен по модул степен на нечетно просто.	111
8.2. Метод на Монгомери за умножение и повдигане в степен.	114
Глава 9. Разлагане на прости множители.	117
9.1. Метод на верижните дроби.	117
9.2. Метод на квадратичното решето.	118
9.3. Методи на John M. Pollard.	122
9.4. Метод Number Field Sieve (NFS).	124
Глава 10. Елиптични криви и криптография.	125
10.1. Проективно пространство и елиптични криви.	125
10.2. Криптографски протоколи основани на елиптични криви.	130
Литература.	131

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