СУ "Св. Климент Охридски" - ФМИ

2005-2006 г.

Конспект на курса "Увод в теорията на числата"

1. Аксиоми на Пеано. Делимост и деление с остатък.
2. Най-голям общ делител. Алгоритъм на Евклид.
3. Прости числа. Основна теорема на аритметиката.
4. Бройни системи. Сложност на аритметични операции.
5. Аритметични функции I.
6. Аритметични функции II.
7. Разпределение на простите числа.
8. Елементарни свойства на сравненията.
9. Линейни сравнения. Китайска теорема за остатъците.
10. Сравнения от втора и по-високи степени.
11. Примитивни корени и индекси.
12. Съществуване на примитивен корен. Циклична ли е $\mathbb{Z}^n$?
13. Квадратични и многостепенни остатъци.
14. Квадратичен закон за реципрочност.
15. Криптографски примитиви и механизми.
16. Електронен подпис.
17. Генериране на големи прости числа.
18. Диофантови уравнения от втора степен.
19. Уравнение на Пел.

Май 2006 г., София

ст. н.с. Николай Манев