

Тема: Алгоритми елементарне теорије бројева и неке њихове примене

Наставник: **Бојана Боровићанин**

У мастер раду ће бити представљени основни алгоритми елементарне теорије бројева и неке њихове могуће примене, укључујући Еуклидов алгоритам, проширени Еуклидов алгоритам, алгоритам за развој броја у верижни разломак, као и Фермаов и Милеров тест за испитивање да ли је неки број прост. Биће приказана примена алгоритама за решавање линеарних конгруенција, система линеарних конгруенција, као и примена у РСА криптографским системима. За приказане алгоритме биће одређена временска и меморијска сложеност.

Литература

1. E. Bach, J. Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, The MIT Press, 1996.
2. J. Buhler, S. Wagon, *Basic algorithms in number theory*, Algorithmic Number Theory MSRI Publications, Volume 44, 2008.
3. A. Dujella, *Увод у теорију бројева* - скрипта, Природословно-математички факултет, Свеучилиште у Загребу, 2003.
4. H. M. Edwards, *Higher arithmetic: an algorithmic introduction to number theory*, AMS, 2008.
5. В. Мићић, З. Каделбург, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2001.
6. М. Станић, Н. Икодиновић, *Теорија бројева*, збирка задатака, Завод за уџбенике и наставна средства, Београд, 2004.
7. Р. Тошић, В. Вукославчевић, *Елементи теорије бројева*, Алеф, Нови Сад, 1995.