Криптографија

Упуство за припрему првог колоквијума

Следеће теме могу бити укључене у први колоквијум:

1. **Дјељивост. НЗД и НЗС.**
   Појмови. Особине. Примјери.

2. **Еуклидов алгоритам. Проширени Еуклидов алгоритам.**
   Обавезно урадити неколико примјера док се не стекне потребна рутина.

3. **Модуларна аритметика. Кинеска теорема о остацима.**
   Особине. Примјери. Конгруентне једначине (конгруенције).
   Рјешавање помоћу система помоћу Кинеске теореме о остацима.

4. **Прости бројеви. Факторизација бројева на просте чиниоце.**
   Обратити пажњу на резултате који слиједе из чињенице јединствености факторизације природних бројева на просте чиниоце.

5. **Фермаова и Ојлерова теорема. Ојлерова функција - мултипликативност. Вилсонова теорема.**
   Обновити доказе наведених теорема и особина Ојлерове функције.

6. **Елементи теорије група. Цикличне групе. Лагранжова теорема.**
   Обратити пажњу на појмове као што су: неутрални елемент, инверзни елементм ред елемента, ред групе, подгрупа...
   Утврдити везе између резултата из Теорије група и Теорије бројева које смо обрађивали. Примјер: Фермаова теорема у вези са редом елемента у цикличној групи.