ICTP DIPLOMA PROGRAMME IN MATHEMATICS 2013-14

Introduction to Number Theory
A. Sofer (10 lectures : 20 hrs)

The main objective of this class is to practice and improve math communication skills in English. The emphasis will be on problem solving.

Contents

1. Divisibility in Z; Division Algorithm; Greatest Common Divisor; Euclidean Algorithm; Linear Diophantine Equations.

2. Prime Numbers; Fundamental Theorem of Arithmetic.

3. Congruences; Linear Congruence Equations; Wilson's Theorem; Fermat's Little Theorem.

4. Polynomial Congruence Equations.

5. Euler's Phi Function; Euler's Theorem.

6. Public-Key Cryptography: RSA.