

ICTP DIPLOMA PROGRAMME IN MATHEMATICS 2014-15

Introduction to Number Theory

A. Sofer (15 lectures : 22.5 hrs)

1. Divisibility in \mathbb{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.