4. PMAT 603.36: Advanced Number Theory - Analytic and Algebraic

Instructor: Dr. R. Mollin
Offered Winter 2013
Prerequisite: Pure Mathematics 315 and PMAT 427 of consent of the Department.

I propose to offer a graduate course that will encompass ADNT. The topics will draw strongly from both the analytic and algebraic and analytic sides. The topics to be covered are delineated on the following table of contents. This will provide a unique opportunity to learn cutting-edge material with applications of both analytic and algebraic number theory to cryptology and other exciting areas to which number theory may be applied.

Required Text: Advanced Number Theory with Applications: (ADNTA), R.A. Mollin, Taylor and Francis Group/CRC, Boca Raton, New York, London, Tokyo (2010); ISBN # 978-1-4200-8328-6.

Recommended Auxiliary Text: Algebraic Number Theory -- Second Edition: (ANT2), R.A. Mollin, Chapman & Hall/CRC, Boca Raton, New York, London, Tokyo (2011). ISBN # 978-1-4398-4598-1.

FACULTY OF SCIENCE

Pure Mathematics 603.36 -- Advanced Number Theory
Winter 2013 - R.A. Mollin

SYLLABUS

REQUIRED TEXT: ADVANCED NUMBER THEORY WITH APPLICATIONS by Richard A. Mollin; (2010) CRC Press/Taylor and Francis Group Publishers.

Topics:

Ch. 1. Algebraic Number Theory: Algebraic number fields; The Gaussian field; Euclidean and other quadratic fields; applications of unique factorization.

Ch. 2. Ideals: Arithmetic in quadratic fields; Dedekind domains; applications to factoring.

Ch. 3. Binary quadratic Forms: composition; class group; ambiguity; genus; representation.

Ch. 4. Diophantine Approximation: algebraic and transcendental numbers; transcendence; Minkowski's convex body theorem.

Ch. 5. Arithmetic Functions: The Euler-Maclaurin summation formula; average orders; The Riemann zeta function;

Ch. 6. P-adic analysis: Solving mod p^n; valuations; representation.

Ch. 7. Dirichlet Characters: Dirichlet L-Functions; Dirichlet Density.

Ch. 8. Diophantine Equations: Lucas-Lehmer Theory; Ramanujan-Nagell equations; Bachet's equation; Fermat's equation; Catalan and the ABC conjecture.

Ch. 9. Elliptic Curves: Mazur, Siegel, and reduction; factoring and primality testing; elliptic curve cryptography.

Ch. 10. Modular Forms: Modular group, forms, and reduction; applications to elliptic curves; Shimura-Tanayama-Weill and proof of FLT—time permitting.