Math 567 **Elementary Number Theory**

Spring 2000

Jim Propp (813 Van Vleck, x3-5148, propp@math.wisc.edu)

Tuesdays and Thursdays, 2:00-3:45; B223 Van Vleck.

Textbook: David M. Burton, *Elementary Number Theory*, fourth edition

Course description

Homework assignments will be given every week (except when one of the two take-home exam is being given). Homework counts towards 60% of one's course-grade; each of the two take-homes is worth an additional 20%. (On homework assignments, students may work together or seek help from me; on take-home exams, they may not do so.) Students taking the course for credit will be expected to attend regularly.

Provisional syllabus

I. Divisibility and Primes: the division algorithm, the Euclidean algorithm, unique factorization

II. Congruences: linear congruences, the Chinese Remainder Theorem, polynomial congruences, counting solutions, Fermat's "little" theorem and Euler's generalization, applications to factoring and cryptography, perfect numbers, Mersenne primes, Fermat primes

III. Quadratic reciprocity: the Legendre symbol, two proofs of QR, primitive roots

IV. Arithmetical functions: $\phi(n)$, $\sigma(n)$, multiplicative functions, Möbius inversion, counting necklaces

V. Diophantine equations: use of congruences, the method of descent, Pythagorean triples, Fermat's two-squares theorem, quadratic forms, Fermat's Last Theorem for exponents 3 and 4, Lagrange's four-squares theorem

VI. Continued fractions: rational numbers, quadratic irrationals, approximation of real numbers, Farey fractions

(more)

VII. Distribution of prime numbers: infinitude, Tchebychef's inequalities, primes in arithmetic progressions, the Riemann zeta-function

VIII. Elliptic curves: the congruent number problem, Fermat's Last Theorem, applications to factoring