MATH 465/565
Theory of Numbers (3 units)

Course Outline

Sections	Topics	# of weeks
2.1–2.5	**Basic Divisibility:** Review of divisibility, gcd's, primes, and unique factorization from Math 267.	1.0
3.1–3.7	**Congruences:** Definition and basic properties (review from Math 267); linear congruences; the Chinese Remainder Theorem; polynomial congruences; the theorems of Fermat, Euler and Wilson.	2.0
4.1–4.3	**Primitive Roots:** Existence of primitive roots; index calculus.	2.0
5.1–5.6	**Quadratic Residues:** Quadratic congruences to a composite modulus; the Legendre symbol and its properties; the law of quadratic reciprocity; applications; the Jacobi symbol.	3.0
6.1–6.10	**Arithmetic Functions:** Multiplicative functions; the functions $\sigma(n)$, $\tau(n)$, $\phi(n)$, and $[n]$; the Möbius function; order estimation; sums over primes; Chebyshev's inequalities; the order of magnitude of σ, ϕ and τ.	3.5
7.1–7.6	**Sums of Squares:** Representations of the integers as sums of two squares; Gaussian integers; the function $r_2(n)$; Lagrange's theorem on sums of four squares.	1.5
	Exams	1.0

Textbook: *Topics in Number Theory*, Dover edition, by William J. LeVeque.

Adopted: January 2012.