MATH342: Number Theory

Syllabus

- *4 lectures* Recap: Divisors, primes, Euclidean algorithm, greatest common divisor, Fundamental Theorem of Arithmetic, arithmetic modulo n.
- *1 lecture* Perfect numbers. Euler's classification of even perfect numbers.
- *2 lectures* The number $\pi(n)$ of primes $\leq n$, the Riemann zeta function, the Prime Number Theorem (no proof), Chebyshev's estimates.
- *3 lectures* The Euler function $\varphi(n)$, the group of units modulo n, the order of an element, congruences.
- *8 lectures* Fermat's theorem on the order of elements modulo a prime, Fermat's primality test and pseudo-primes. Euler's theorem. Primitive roots. The number and sum of divisors of an integer. The Miller-Rabin test. Carmichael numbers. Testing Mersenne primes.
- *6 lectures* Quadratic residues part 1. Groups, rings, fields. Euclidean rings and unique factorisation. Pythagorean triples. The group of units in a quadratic number field.
- *5 lectures* Legendre symbols. Quadratic residues part 2. Gauss' reciprocity law.
- *4 lectures* More applications of quadratic residues and Gauss' reciprocity, including some lower order cases of Fermat's Last Theorem.
- *3 lectures* Revision.

Networked texts

These are networked texts in the university library.

- *Elementary number theory: primes, congruences and secrets, a computational approach*, William Stein, Springer, 2009.

- *Elementary number theory in nine chapters*, James J. Tattersall, Mcgraw Hill 2007

- *Introductory algebraic number theory* by Saban Alaca and Kenneth S. Williams. Cambridge University Press 2004. This is more advanced, and hence does not cover "elementary" topics such as quadratic reciprocity (a major component of the course). Algebraic structures are very much in the foreground, which has advantages.

- *Problems in algebraic number theory*, M. Ram Myrty and Jody Esmonde, Springer 2005. This is actually aimed at graduate students, but is very practical, crammed full of problems, and well worth looking at.

- *A Primer of Analytic Number Theory: from Pythagoras to Riemann*, J. Stopple, Cambridge University Press 2003. This is analytic number theory, but is worth looking at for the Prime Number Theorem.

Other texts

- *Primes and programming*, P.J. Giblin, Cambridge University Press 1993

- *Algebra*, Serge Lang, Addison-Wesley 1965 (or any newer edition)

- *A course in arithmetic*, J-P. Serre (first chapter only) Graduate Texts in Mathematics no. 7 Springer-Verlag 1973