

Sheet1

Fermat's Little Theorem	Sec 3-2		Oct
Wilson's Theorem	Sec 3-3		Oct
card shuffling	Sec 4-3		Oct
solving congruences	Sec 5-1, 5-2		Oct
chinese remainder theorem	Sec 5-3		Nov
Mu, phi, d and sigma	Sec 6-1, 6-2		Nov
multiplicative functions	Sec 6-3		Nov
Möbius inversion	Sec 6-4		Nov
primitive roots	Sec 7-1, 7-2		Nov
distrib. primes & Tchebychev's ineq	Sec 8-1, 8-2		Nov
Jacobi and Legendre symbols	Sec 9-1, 9-2		Dec
quadratic reciprocity	Sec 9-3		Dec
Intro to Elliptic curves	Not in book		Jan
pseudo-primality testing	Not in book		Jan
RSA	Not in book		Jan
Digital Signatures (coord with RSA)	Not in book		Feb
Factorization algorithms	Not in book		Feb
Sum of 4 squares theorem	Sec 11-2		Feb
Fermat's Last Theorem and A. Weil	Not in book (sec 11-2)		Feb
Jacobi triple product identity	Sec 13-2		Jan ?
Ferrer's diagrams and partition ident.	Sec 12-4		Jan ?
partitions which fit in a rectangle	Not in book		March
Topic in the history of number theory	Not in book		Anytime
Unsolved problems in number theory	Not in book (sec 8-3)		Anytime
Suggest a topic			Anytime