

> Contents

Introduction	1
1 Primes and Factors	3
1.1 Prime numbers	3
1.2 Prime factors	8
1.3 Euler's phi function	10
1.4 Common factors	11
1.5 More about prime factors	16
2 Continued Fractions and Rational Approximations	21
2.1 Continued fractions	21
2.2 Good approximations	23
2.3 The continued fraction algorithm	25
2.4 The convergents of a continued fraction	30
2.5 The convergents are good approximations	35
2.6 The limit of the convergents	41
2.7 Approximating with mediants	45
3 Modular Arithmetic	52
3.1 Congruences	52
3.2 Elementary operations with congruences	55
3.3 Complete sets of residues	56
3.4 Using division in a congruence	57
3.5 Polynomial congruences	59
3.6 Successive powers of a number	62
3.7 A result due to Fermat	64
3.8 Euler's generalisation of Fermat's theorem and the number lambda	66

4	Cryptography	70	
4.1	Enciphering and deciphering	70	
4.2	Using the cryptography program	72	
4.3	Increasing the security of our system	74	
4.4	Public-key cryptography	76	
Appendix 1		Fields	78
Appendix 2		Common ASCII code numbers	79
Appendix 3		User notes	80
Bibliography			84
Index			85