Square roots and factoring

10.1. Square roots modulo n

10.2. Cryptosystems

10.3. RSA

10.4. Certificates and the complexity classes P and NP

10.5. Polynomial time primality testing

10.6. Factoring methods

10.7. Additional Exercises: Questions on factoring and primality testing

Appendix 10A. Pseudoprime tests using square roots of 1

10.8. The difficulty of finding all square roots of 1

Appendix 10B. Factoring with squares

Random squares

Euler's sum of squares method

The Continued fractions method

10.9. Factoring with polynomial values

The large prime variation

Appendix 10C. Identifying primes of a given size

Pseudoprime tests

10.10. The Proth-Pocklington-Lehmer primality test

Appendix 10D. Carmichael numbers

10.11. Constructing Carmichael numbers

10.12. Erdős's construction

The computational evidence

Appendix 10E. Cryptosystems based on discrete logarithms

10.13. The Diffie-Hellman key exchange

10.14. The El Gamal cryptosystem

Appendix 10F. Running times of algorithms

10.15. P and NP

10.16. Difficult problems

Appendix 10G. The AKS test

10.17. A computationally quicker characterization of the primes

10.18. A set of extraordinary congruences

Appendix 10H. Factoring algorithms for polynomials

10.19. Testing polynomials for irreducibility

10.20. Testing whether a polynomial is squarefree

10.21. Factoring a squarefree polynomial modulo p