

Power residues

7.1. Generating the multiplicative group of residues

7.2. Fermat's Little Theorem

7.3. Special primes and orders

7.4. Further observations

7.5. The number of elements of a given order, and primitive roots

7.6. Testing for composites, pseudoprimes, and Carmichael numbers

7.7. *Divisibility tests, again*

7.8. *The decimal expansion of fractions*

7.9. Primes in arithmetic progressions, revisited

7.10. Additional Exercises: Primes in arithmetic progressions, revisited

Appendix 7A. Card shuffling and Fermat's Little Theorem

7.11. Card shuffling and orders modulo n

7.12. The "necklace proof" of Fermat's Little Theorem

7.13. Taking powers efficiently

7.14. Running time: The desirability of polynomial time algorithms

Appendix 7B. Orders and primitive roots

7.15. Constructing primitive roots modulo p

7.16. Indices / Discrete Logarithms

7.17. Primitive roots modulo prime powers

7.18. Orders modulo composites

Appendix 7C. Finding n th roots modulo prime powers

7.19. n th roots modulo p

7.20. Lifting solutions

7.21. Finding n th roots quickly

Appendix 7D. Orders for finite groups

7.22. Cosets of general groups

7.23. Lagrange and Wilson

7.24. Normal subgroups

Appendix 7E. Constructing finite fields

7.25. Classification of finite fields

7.26. The product of linear forms in \mathbb{F}_q

Appendix 7F. Sophie Germain and Fermat's Last Theorem

7.27. Fermat's Last Theorem and Sophie Germain

Appendix 7G. Primes of the form $2^n + k$

7.28. Covering sets of congruences

7.29. Covering systems for the Fibonacci numbers

A Fibonacci covering system

7.30. The theory of covering systems

Appendix 7H. Further congruences

7.31. Fermat quotients

Binomial coefficients

Bernoulli numbers modulo p

Sums of powers of integers modulo p^2

The Wilson quotient

Beyond Fermat's Little Theorem

7.32. Frequency of p -divisibility

Fermat quotients

Bernoulli numbers

Appendix 7I. Primitive prime factors of recurrence sequences

7.33. Primitive prime factors

Prime power divisibility of second-order linear recurrence sequences

7.34. Closed form identities and sums of powers

7.35. Primitive prime factors and second-order linear recurrence sequences