

## The basic algebra of number theory

3.1. The Fundamental Theorem of Arithmetic

3.2. Abstractions

3.3. Divisors using factorizations

3.4. Irrationality

3.5. Dividing in congruences

3.6. Linear equations in two unknowns

3.7. Congruences to several moduli

3.8. Square roots of  $1 \pmod{n}$

3.9. Additional Exercises: More questions on congruences

Appendix 3A. Factoring binomial coefficients and Pascal's triangle modulo  $p$

3.10. The prime powers dividing a given binomial coefficient

3.11. Pascal's triangle modulo 2

Appendix 3B. Solving linear congruences

3.12. Composite moduli

3.13. Solving linear congruences with several unknowns

3.14. The Chinese Remainder Theorem in general

When the moduli are not coprime

Appendix 3C. Groups and rings

**3.15. A direct sum**

**3.16. The structure of finite abelian groups**

Appendix 3D. Unique factorization revisited

**3.17. The Fundamental Theorem of Arithmetic, clarified**

**3.18. When unique factorization fails**

**3.19. Defining ideals and factoring**

**3.20. Bases for ideals in quadratic fields**

Appendix 3E. Gauss's approach

**3.21. Gauss's approach to Euclid's Lemma**

Appendix 3F. Fundamental theorems and factoring polynomials

**3.22. The number of distinct roots of polynomials**

**The Euclidean algorithm for polynomials**

**3.23. Interpreting resultants and discriminants**

**3.24. Other approaches to resultants and gcds**

Appendix 3G. Open problems

**3.25. The Frobenius postage stamp problem, II**

**3.26. Egyptian fractions for  $3/b$**

**3.27. The  $3x + 1$  conjecture**