CAMBRIDGE

Cambridge University Press
978-0-521-72236-0 - The Higher Arithmetic: An Introduction to the Theory of Numbers, Eighth Edition
H. Davenport
Table of Contents
More information

CONTENTS

Introduction *page* viii

I Factorization and the Primes 1
1. The laws of arithmetic 1
2. Proof by induction 6
3. Prime numbers 8
4. The fundamental theorem of arithmetic 9
5. Consequences of the fundamental theorem 12
6. Euclid's algorithm 16
7. Another proof of the fundamental theorem 18
8. A property of the H.C.F 19
9. Factorizing a number 22
10. The series of primes 25

II Congruences 31
1. The congruence notation 31
2. Linear congruences 33
3. Fermat's theorem 35
4. Euler's function $\phi(m)$ 37
5. Wilson's theorem 40
6. Algebraic congruences 41
7. Congruences to a prime modulus 42
8. Congruences in several unknowns 45
9. Congruences covering all numbers 46

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-72236-0 - The Higher Arithmetic: An Introduction to the Theory of Numbers, Eighth Edition
H. Davenport
Table of Contents
More information

III Quadratic Residues 49
1. Primitive roots 49
2. Indices 53
3. Quadratic residues 55
4. Gauss's lemma 58
5. The law of reciprocity 59
6. The distribution of the quadratic residues 63

IV Continued Fractions 68
1. Introduction 68
2. The general continued fraction 70
3. Euler's rule 72
4. The convergents to a continued fraction 74
5. The equation $ax - by = 1$ 77
6. Infinite continued fractions 78
7. Diophantine approximation 82
8. Quadratic irrationals 83
9. Purely periodic continued fractions 86
10. Lagrange's theorem 92
11. Pell's equation 94
12. A geometrical interpretation of continued fractions 99

V Sums of Squares 103
1. Numbers representable by two squares 103
2. Primes of the form $4k + 1$ 104
3. Constructions for x and y 108
4. Representation by four squares 111
5. Representation by three squares 114

VI Quadratic Forms 116
1. Introduction 116
2. Equivalent forms 117
3. The discriminant 120
4. The representation of a number by a form 122
5. Three examples 124
6. The reduction of positive definite forms 126
7. The reduced forms 128
8. The number of representations 131
9. The class-number 133

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-72236-0 - The Higher Arithmetic: An Introduction to the Theory of Numbers, Eighth Edition
H. Davenport
Table of Contents
More information

VII Some Diophantine Equations 137
1. Introduction 137
2. The equation $x^2 + y^2 = z^2$ 138
3. The equation $ax^2 + by^2 = z^2$ 140
4. Elliptic equations and curves 145
5. Elliptic equations modulo primes 151
6. Fermat's Last Theorem 154
7. The equation $x^3 + y^3 = z^3 + w^3$ 157
8. Further developments 159

VIII Computers and Number Theory 165
1. Introduction 165
2. Testing for primality 168
3. 'Random' number generators 173
4. Pollard's factoring methods 179
5. Factoring and primality via elliptic curves 185
6. Factoring large numbers 188
7. The Diffie–Hellman cryptographic method 194
8. The RSA cryptographic method 199
9. Primality testing revisited 200

Exercises 209
Hints 222
Answers 225

Bibliography 235

Index 237

© Cambridge University Press www.cambridge.org