

## CONTENTS

CHAPTER	PAGE
<p>I. FUNDAMENTAL THEOREMS ON DIVISIBILITY . . .</p> <p style="padding-left: 2em;">Greatest common divisor. Relatively prime integers. Prime numbers. Infinitude of primes. Congruent numbers. Least residues. Fermat's theorem and Euler's generalization. Euler's <math>\phi</math> function.</p>	1
<p>II. THEORY OF CONGRUENCES . . . . .</p> <p style="padding-left: 2em;">Linear congruences. Chinese remainder theorem. Number of roots. Belonging to an exponent. Primitive roots. Residual polynomials and congruences. Indices.</p>	10
<p>III. QUADRATIC RESIDUES AND RECIPROCITY LAW . .</p> <p style="padding-left: 2em;">Legendre's symbol. Gauss's lemma. Quadratic reciprocity law. Geometrical proof. Jacobi's symbol</p>	30
<p>IV. INTRODUCTION TO DIOPHANTINE EQUATIONS . .</p> <p style="padding-left: 2em;">Historical note. All integral solutions of <math>Ax^2 + y^2 = z^2</math>. Impossibility of <math>x^4 + y^4 = z^2</math>. All rational and all integral solutions of <math>ax^2 + bxy + cy^2 = ez^2</math>. Sets of integers having equal sums of like powers. All rational solutions of <math>x^3 + y^3 + z^3 + w^3 = 0</math>. Equal sums of two fourth powers.</p>	40
<p>V. BINARY QUADRATIC FORMS . . . . .</p> <p style="padding-left: 2em;">Transformation. Equivalence. Definite and reduced forms. Neighboring forms. No two reduced forms are equivalent. Ambiguous and opposite forms. Automorphs. Proper representations. Sum of two squares. Kronecker's symbol. Number of representations by positive forms. Characters and genera. Table of positive reduced forms with a single class in each genus. Criterion for equivalence.</p>	63
<p>VI. CERTAIN DIOPHANTINE EQUATIONS . . . . .</p> <p style="padding-left: 2em;">All integral solutions of <math>x^2 - my^2 = zw</math> and of <math>ax^2 + bxy + cy^2 = zw</math>. Method of Euler and Lagrange.</p>	91

CHAPTER	PAGE
VII. INDEFINITE BINARY QUADRATIC FORMS . . . . .	99
Relations between the roots of equivalent forms. Reduced forms. Their chains and periods. Continued fractions. Equivalent, reduced forms. Lower bound of numbers represented by a form. Automorphs. All integral solutions of $t^2 - du^2 = 4$ . Proper representations. Indefinite, ambiguous forms.	
VIII. SOLUTION OF $ax^2 + by^2 + cz^2 = 0$ IN INTEGERS . . . . .	117
IX. COMPOSITION AND GENERA OF BINARY QUADRATIC FORMS . . . . .	134
Classes which admit composition. Number of genera. Number of ambiguous classes. Gauss's celebrated theorem on duplication.	
X. DIOPHANTINE EQUATIONS WITH ONLY A FINITE NUMBER OF INTEGRAL SOLUTIONS . . . . .	151
Recent theorems of Thue and Siegel on $H(x, y) = c$ , $H(x, y) = G(x, y)$ , $ay^2 + by + c = dx^n$ , and the rational approximation to a root of an algebraic equation.	
XI. MINIMA OF REAL, INDEFINITE, BINARY QUADRATIC FORMS . . . . .	175
INDEX . . . . .	181