

Carl Friedrich Gauss

DISQUISITIONES ARITHMETICAE

Translated by Arthur A. Clarke

Revised by William C. Waterhouse
with the help of Cornelius Greither and
A. W. Grootendorst



Springer-Verlag
New York Berlin Heidelberg Tokyo

CONTENTS

	page
Translator's Preface	v
Bibliographical Abbreviations	vii
Dedication	xv
Author's Preface	xvii
Section I. Congruent Numbers in General	1
Congruent numbers, moduli, residues, and nonresidues, art. 1 ff.	
Least residues, art. 4	
Elementary propositions regarding congruences, art. 5	
Certain applications, art. 12	
Section II. Congruences of the First Degree	5
Preliminary theorems regarding prime numbers, factors, etc., art. 13	
Solution of congruences of the first degree, art. 26	
The method of finding a number congruent to given residues relative to given moduli, art. 32	
Linear congruences with several unknowns, art. 37	
Various theorems, art. 38	
Section III. Residues of Powers	29
The residues of the terms of a geometric progression which begins with unity constitute a periodic series, art. 45	
If the modulus = p (a prime number), the number of terms in its period is a divisor of the number $p - 1$, art. 49	
Fermat's theorem, art. 50	
How many numbers correspond to a period in which the number of terms is a given divisor of $p - 1$, art. 52	
Primitive roots, bases, indices, art. 57	
Computation with indices, art. 58	
Roots of the congruence $x^a \equiv A$, art. 60	
Connection between indices in different systems, art. 69	

Bases adapted to special purposes, art. 72	
Method of finding primitive roots, art. 73	
Various theorems concerning periods and primitive roots, art. 75	
A theorem of Wilson, art. 76	
Moduli which are powers of prime numbers, art. 82	
Moduli which are powers of the number 2, art. 90	
Moduli composed of more than one prime number, art. 92	
Section IV. Congruences of the Second Degree	63
Quadratic residues and nonresidues, art. 94	
Whenever the modulus is a prime number, the number of residues less than the modulus is equal to the number of nonresidues, art. 96	
The question whether a composite number is a residue or nonresidue of a given prime number depends on the nature of the factors, art. 98	
Moduli which are composite numbers, art. 100	
A general criterion whether a given number is a residue or a nonresidue of a given prime number, art. 106	
The investigation of prime numbers whose residues or non- residues are given numbers, art. 107	
The residue -1 , art. 108	
The residues $+2$ and -2 , art. 112	
The residues $+3$ and -3 , art. 117	
The residues $+5$ and -5 , art. 121	
The residues $+7$ and -7 , art. 124	
Preparation for the general investigation, art. 125	
By induction we support a general (fundamental) theorem and draw conclusions from it, art. 130	
A rigorous demonstration of the fundamental theorem, art. 135	
An analogous method of demonstrating the theorem of art. 114, art. 145	
Solution of the general problem, art. 146	
Linear forms containing all prime numbers for which a given number is a residue or nonresidue, art. 147	
The work of other mathematicians concerning these in- vestigations, art. 151	
Nonpure congruences of the second degree, art. 152	
Section V. Forms and Indeterminate Equations of the Second Degree	108

- Plan of our investigation; definition of forms and their notation, art. 153
- Representation of a number; the determinant, art. 154
- Values of the expression $\sqrt{(b^2 - ac)} \pmod{M}$ to which belongs a representation of the number M by the form (a, b, c) , art. 155
- One form implying another or contained in it; proper and improper transformation, art. 157
- Proper and improper equivalence, art. 158
- Opposite forms, art. 159
- Neighboring forms, art. 160
- Common divisors of the coefficients of forms, art. 161
- The connection between all similar transformations of a given form into another given form, art. 162
- Ambiguous forms, art. 163
- Theorem concerning the case where one form is contained in another both properly and improperly, art. 164
- General considerations concerning representations of numbers by forms and their connection with transformations, art. 166
- Forms with a negative determinant, art. 171
- Special applications for decomposing a number into two squares, into a square and twice a square, into a square and three times a square, art. 182
- Forms with positive nonsquare determinant, art. 183
- Forms with square determinant, art. 206
- Forms contained in other forms to which, however, they are not equivalent, art. 213
- Forms with 0 determinant, art. 215
- The general solution by integers of indeterminate equations of the second degree with two unknowns, art. 216
- Historical notes, art. 222
- Distribution of forms with a given determinant into classes, art. 223
- Distribution of classes into orders, art. 226
- The partition of orders into genera, art. 228
- The composition of forms, art. 234
- The composition of orders, art. 245
- The composition of genera, art. 246
- The composition of classes, art. 249
- For a given determinant there are the same number of classes in every genus of the same order, art. 252

- Comparison of the number of classes contained in individual genera of different orders, art. 253
- The number of ambiguous classes, art. 257
- Half of all the characters assignable for a given determinant cannot belong to any properly primitive genus, art. 261
- A second demonstration of the fundamental theorem and the other theorems pertaining to the residues -1 , $+2$, -2 , art. 262
- A further investigation of that half of the characters which cannot correspond to any genus, art. 263
- A special method of decomposing prime numbers into two squares, art. 265
- A digression containing a treatment of ternary forms, art. 266 ff.
- Some applications to the theory of binary forms, art. 286 ff.
- How to find a form from whose duplication we get a given binary form of a principal genus, art. 286
- Except for those characters for which art. 263, 264 showed it was impossible, all others will belong to some genus, art. 287
- The theory of the decomposition of numbers and binary forms into three squares, art. 288
- Demonstration of the theorems of Fermat which state that any integer can be decomposed into three triangular numbers or four squares, art. 293
- Solution of the equation $ax^2 + by^2 + cz^2 = 0$, art. 294
- The method by which the illustrious Legendre treated the fundamental theorem, art. 296
- The representation of zero by ternary forms, art. 299
- General solution by rational quantities of indeterminate equations of the second degree in two unknowns, art. 300
- The average number of genera, art. 301
- The average number of classes, art. 302
- A special algorithm for properly primitive classes; regular and irregular determinants etc., art. 305
- Section VI. Various Applications of the Preceding Discussions 375
- The resolution of fractions into simpler ones, art. 309
- The conversion of common fractions into decimals, art. 312
- Solution of the congruence $x^2 = A$ by the method of exclusion, art. 319
- Solution of the indeterminate equation $mx^2 + ny^2 = A$ by exclusions, art. 323

Another method of solving the congruence $x^2 \equiv A$ for the case where A is negative, art. 327

Two methods for distinguishing composite numbers from primes and for determining their factors, art. 329

Section VII. Equations Defining Sections of a Circle

407

The discussion is reduced to the simplest case in which the number of parts into which the circle is cut is a prime number, art. 336

Equations for trigonometric functions of arcs which are a part or parts of the whole circumference; reduction of trigonometric functions to the roots of the equation $x^n - 1 = 0$, art. 337

Theory of the roots of the equation $x^n - 1 = 0$ (where n is assumed to be prime), art. 341 ff.

Except for the root 1, the remaining roots contained in (Ω) are included in the equation $X = x^{n-1} + x^{n-2} + \dots + x + 1 = 0$; the function X cannot be decomposed into factors in which all the coefficients are rational, art. 341

Declaration of the purpose of the following discussions, art. 342

All the roots in (Ω) are distributed into certain classes (periods), art. 343

Various theorems concerning these periods, art. 344

The solution of the equation $X = 0$ as evolved from the preceding discussions, art. 352

Examples for $n = 19$ where the operation is reduced to the solution of two cubic and one quadratic equation, and for $n = 17$ where the operation is reduced to the solution of four quadratic equations, art. 353, 354

Further discussions concerning periods of roots, art. 355 ff.

Sums having an even number of terms are real quantities, art. 355

The equation defining the distribution of the roots (Ω) into two periods, art. 356

Demonstration of a theorem mentioned in Section IV, art. 357

The equation for distributing the roots (Ω) into three periods, art. 358

Reduction to pure equations of the equations by which the roots (Ω) are found, art. 359

Application of the preceding to trigonometric functions, art. 361 ff.	
Method of finding the angles corresponding to the individual roots of (Ω), art. 361	
Derivation of tangents, cotangents, secants, and cosecants from sines and cosines without division, art. 362	
Method of successively reducing the equations for trigono- metric functions, art. 363	
Sections of the circle which can be effected by means of quadratic equations or by geometric constructions, art. 365	
Additional Notes	461
Tables	463
Gauss' Handwritten Notes	467
List of Special Symbols	470
Directory of Terms	471