

Carl Friedrich Gauss

Disquisitiones Arithmeticae

English Edition

算术探究 英文版

Springer

世界图书出版公司
www.wpcbj.com.cn

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

图书在版编目 (CIP) 数据

算术探究 = Disquisitiones Arithmeticae English Edition : 英文 / (德) C. F. 高斯
(Carl Friedrich Gauss) 著 . — 北京 : 世界图书出版公司北京公司 , 2016.5
ISBN 978-7-5192-1470-8

I . ①算… II . ①高… III . ①代数—英文 IV . ① O15

中国版本图书馆 CIP 数据核字 (2016) 第 119577 号

著 者 : Carl Friedrich Gauss
责任编辑 : 刘 慧 高 蓉
装帧设计 : 任志远

出版发行 : 世界图书出版公司北京公司
地 址 : 北京市东城区朝内大街 137 号
邮 编 : 100010
电 话 : 010-64038355 (发行) 64015580 (客服) 64033507 (总编室)
网 址 : <http://www.wpebj.com.cn>
邮 箱 : wpebjst@vip.163.com
销 售 : 新华书店
印 刷 : 三河市国英印务有限公司
开 本 : 787mm × 1092mm 1/16
印 张 : 31
字 数 : 595 千
版 次 : 2016 年 7 月第 1 版 2016 年 7 月第 1 次印刷
版权登记 : 01-2015-5157
定 价 : 115.00 元

版权所有 翻印必究

(如发现印装质量问题 , 请与所购图书销售部门联系调换)

DISQUISITIONES ARITHMETICAE

AMS Classifications: 10-01, 01A55

Library of Congress Cataloging-in-Publication Data
Gauss, Carl Friedrich, 1777-1855.

Disquisitiones arithmeticae.

Essentially a reprint of the ed. published in 1966
by Yale University Press. Cf. Pref.

Translated from the ed. of 1870, edited by E. C. J.
Schering.

1. Numbers, Theory of. I. Waterhouse, William C.

II. Title.

QA241.G2613 1986 512 85-27753

The first Springer edition of this book, published in 1986, was reprinted
from the 1966 edition by Yale University Press, New Haven and London.

© 1966 by Yale University Press.

All rights reserved. No part of this book may be translated or reproduced in
any form without written permission from the copyright holder.

Reprint from English language edition:

Disquisitiones Arithmeticae

by Carl Friedrich Gauss

Copyright © 1986 Springer New York

Springer New York is a part of Springer Science+Business Media

All Rights Reserved

This reprint has been authorized by Springer Science & Business Media for distribution in
China Mainland only and not for export therefrom.

TRANSLATOR'S PREFACE

IT IS EXTRAORDINARY that one hundred and sixty-four years should have passed between the publication of Gauss' *Disquisitiones Arithmeticae* and its translation into English. No other reason need be offered to justify this enterprise now save the Olympian stature of the author himself, although it is no great presumption to believe that in such a work by such a man there are still hidden profound insights which may yet, after so many years, inspire new discoveries in the field of mathematics.

An apology may be needed for carrying over into English much of the flavor of Gauss' Ciceronian style. I made this decision because I felt that any scholar interested in this work is more concerned with Gauss' thought than in a pithy paraphrase of it. Those fortunate enough to be able to read the original have been satisfied with this for a century and a half. It would be somewhat arbitrary to separate the modern reader too much from the style of the master.

This translation was made from the second edition, edited by Schering for the Königlichen Gesellschaft der Wissenschaften at Göttingen, and printed in 1870 by Dietrich. The reader will find that some footnotes are identified by numerals, others by letters of the alphabet. The former refer to notes that I have inserted, the latter to Gauss' own footnotes. I have also added for the reader's convenience a list of abbreviations of the bibliographical works cited in the text, a list of special symbols used by Gauss with the page numbers where they are defined, and a directory of important terms.

Schering's notes for the second edition read, in part: "In the year 1801 seven sections of the *Disquisitiones Arithmeticae* were published in octavo. The first reprint was published under my direction in 1863 as the first volume of Gauss' *Works*. That edition

has been completely sold out, and a new edition is presented here. The eighth section, to which Gauss makes frequent reference and which he had intended to publish with the others, was found among his manuscripts. Since he did not develop it in the same way as the first seven sections, it has been included with his other unpublished arithmetic essays in the second volume of this edition of his *Works*. . . . The form of this edition has been changed to allow for ease of order and summary. I believed that this was justified because Gauss had made such a point of economizing on space. Many formulae which were included in the running text have been displayed to better advantage."

Dr. Herman H. Goldstine first suggested that I undertake this translation, and I am grateful to him for his suggestion and for his continued interest.

ARTHUR A. CLARKE, S.J.

*Fordham University
New York, New York
June 1965*

PREFACE TO THE SPRINGER EDITION

THIS IS ESSENTIALLY a reproduction of the 1966 edition, but it has been possible to introduce small changes at a number of places where a more precise rendering of the original text seemed to be required. I bear the responsibility for these changes, but I have made substantial use of careful notes prepared by A. A. Clarke, C. Greither, and A. W. Grootendorst.

WILLIAM C. WATERHOUSE

*Pennsylvania State University
August 1985*

TRANSLATOR'S BIBLIOGRAPHICAL ABBREVIATIONS

In the text the dates in brackets represent the years during which the papers were delivered; the unbracketed dates are the years of publication.

<i>Acta acad. Petrop.</i>	<i>Acta academiae scientiarum imperialis Petropolitanae</i> , St. Petersburg
<i>Algebra</i>	Leonhard Euler, <i>Vollständige Anleitung zur Algebra</i> , St. Petersburg, 1770
<i>Appel au public</i>	Samuel König, <i>Appel au public du jugement de l'Académie de Berlin sur un fragment de lettre de Mr. de Leibniz, cité par Mr. König</i> , Leiden, 1752.
<i>Comm. acad. Petrop.</i>	<i>Commentarii academiae scientiarum imperialis Petropolitanae</i> , St. Petersburg
<i>Hist. de l'Ac. de Prusse</i>	See below
<i>Hist. Acad. Berlin</i>	<i>Histoire de l'Académie royale des sciences et belles-lettres avec les mémoires</i> , Berlin [popularly called <i>Histoire de l'Académie de Prusse</i>]
<i>Hist. Acad. Paris</i>	<i>Histoire de l'Académie royale des sciences avec les mémoires de mathématique et physique</i> , Paris
<i>Nouv. mém. Acad. Berlin</i>	<i>Nouveaux mémoires de l'Académie de Berlin</i> , Berlin
<i>Nova acta erudit.</i>	<i>Nova acta eruditorum</i> , Leipzig
<i>Nova acta acad. Petrop.</i>	<i>Nova acta academiae scientiarum imperialis Petropolitanae</i> , St. Petersburg

- Novi comm. acad. Petrop.* *Novi commentarii academiae scientiarum imperialis Petropolitanae*, St. Petersburg
- Opera Mathem.* Pierre de Fermat, *Varia opera Mathematica D. Petri de Fermat, Senatoris Tolosani*, Toulouse, 1679
- Opera Mathem. Wall.* *Opera Mathematica*, ed. Johannes Wallis, Oxford, 1693
- Opuscula Analytica* Leonhard Euler, St. Petersburg, 1783

TO THE MOST SERENE
PRINCE AND LORD
CHARLES WILLIAM FERDINAND
DUKE OF BRUNSWICK AND LUNEBURG

MOST SERENE PRINCE,

I consider it my greatest good fortune that YOU allow me to adorn this work of mine with YOUR most honorable name. I am bound by a sacred duty to offer it to YOU. Were it not for YOUR favor, Most Serene Prince, I would not have had my first introduction to the sciences. Were it not for YOUR unceasing benefits in support of my studies, I would not have been able to devote myself totally to my passionate love, the study of mathematics. It has been YOUR generosity alone which freed me from other cares, allowed me to give myself to so many years of fruitful contemplation and study, and finally provided me the opportunity to set down in this volume some of the results of my investigations. And when at length I was ready to present my work to the world, it was YOUR munificence alone which removed all the obstacles that continually delayed its publication. Such has been YOUR bounty toward me and my work that I can only contemplate it with most grateful mind and silent wonder; I cannot pay it the tribute it justly deserves. For not only do I feel myself hardly equal to such an office, but also everyone knows YOUR extraordinary liberality to all who devote themselves to the higher disciplines. And everyone knows that YOU have never excluded from YOUR patronage those sciences which are commonly regarded as being too recondite and too removed from ordinary life. YOU YOURSELF in YOUR supreme wisdom are well aware of the intimate and necessary bond that unites all sciences among themselves and with whatever pertains to the prosperity of the human society. Therefore I present this book as a witness to my profound regard for YOU and to my

dedication to the noblest of sciences. Most Serene Prince, if you judge it worthy of that extraordinary favor which you have always lavished on me, I will congratulate myself that my work was not in vain and that I have been graced with that honor which I prize above all others.

MOST SERENE PRINCE

Your Highness' most dedicated servant

Brunswick, July 1801

C. F. GAUSS

AUTHOR'S PREFACE

THE INQUIRIES which this volume will investigate pertain to that part of Mathematics which concerns itself with integers. I will rarely refer to fractions and never to surds. The Analysis which is called indeterminate or Diophantine and which discusses the manner of selecting from the infinitely many solutions for an indeterminate problem those that are integral or at least rational (and usually with the added condition that they be positive) is not the discipline to which I refer but rather a quite special part, related to it roughly as the art of reducing and solving equations (Algebra) is related to the whole of Analysis. Just as we include under the heading ANALYSIS all discussion that involves quantity, so integers (and fractions in so far as they are determined by integers) constitute the proper object of ARITHMETIC. However what is commonly called Arithmetic hardly extends beyond the art of enumerating and calculating (i.e. expressing numbers by suitable symbols, for example by a decimal representation, and carrying out arithmetic operations). It often includes some subjects which certainly do not pertain to Arithmetic (like the theory of logarithms) and others which are common to all quantities. As a result it seems proper to call this subject Elementary Arithmetic and to distinguish from it Higher Arithmetic which includes all general inquiries about properties special to integers. We consider only Higher Arithmetic in the present volume.

Included under the heading "Higher Arithmetic" are those topics which Euclid treated in Book VIII^{ff}. with the elegance and rigor customary among the ancients, but they are limited to the rudiments of the science. The celebrated work of Diophantus, dedicated to undetermined problems, contains many results which excite a more than ordinary regard for the ingenuity and proficiency of the author because of their difficulty and the subtle devices he uses, especially if we consider the few tools that he had at hand for

his work. However, these problems demand a certain dexterity and skillful handling rather than profound principles and, because the questions are too specialized and rarely lead to more general conclusions, Diophantus' book seems to mark an epoch in the history of Mathematics more because it presents the first traces of the characteristic art and Algebra than because it enriched Higher Arithmetic with new discoveries. Far more is owed to modern authors, of whom those few men of immortal glory P. de Fermat, L. Euler, L. Lagrange, A. M. Legendre (and a few others) opened the entrance to the shrine of this divine science and revealed the abundant wealth within it. I will not recount here the individual discoveries of these geometers since they can be found in the Preface to the appendix which Lagrange added to Euler's *Algebra* and in the recent volume of Legendre (which I shall soon cite). I shall also cite many of them in the proper places in these pages.

The purpose of this volume, whose publication I promised five years ago, was to present my investigations into Higher Arithmetic, both those begun by that time and later ones. Lest anyone be surprised that I start almost at the very beginning and treat anew many results that had been actively studied by others, I must explain that when I first turned to this type of inquiry in the beginning of 1795 I was unaware of the modern discoveries in the field and was without the means of discovering them. What happened was this. Engaged in other work I chanced on an extraordinary arithmetic truth (if I am not mistaken, it was the theorem of art. 108). Since I considered it so beautiful in itself and since I suspected its connection with even more profound results, I concentrated on it all my efforts in order to understand the principles on which it depended and to obtain a rigorous proof. When I succeeded in this I was so attracted by these questions that I could not let them be. Thus as one result led to another I had completed most of what is presented in the first four sections of this work before I came into contact with similar works of other geometers. Once I was able to study the writings of these men of genius, I recognized that the greater part of my meditations had been spent on subjects already well developed. But this only increased my interest, and walking in their

footsteps I attempted to extend Arithmetic further. Some of these results are embodied in Sections V, VI, and VII. After a while I began to consider publishing the fruits of my investigations. And I allowed myself to be persuaded not to omit any of the early results, because at that time there was no book that brought together the works of other geometers, scattered as they were among Commentaries of learned Academies. Besides, many results were new, most were treated by new methods, and the later results were so bound up with the old ones that they could not be explained without repeating from the beginning.

Meanwhile there appeared an outstanding work by a man to whom Higher Arithmetic already owed much, Legendre's "Essai d'une théorie des nombres." Here he collected together and systematized not only all that had been discovered up to that time but also many new results of his own. Since this book came to my attention after the greater part of my work was already in the hands of the publishers, I was unable to refer to it in analogous sections of my book. I felt obliged, however, to add Additional Notes on a few passages and I trust that this understanding and illustrious man will not be offended.

The publication of my work was hindered by many obstacles over a period of four years. During this time I continued investigations which I had already undertaken and deferred to a later date so that the book would not be too large, and I also undertook new investigations. Similarly, many questions which I touched on only lightly because a more detailed treatment seemed less necessary (e.g. the contents of art. 37, 82 ff., and others) have been further developed and have led to more general results that seem worthy of publication (cf. the Additional Note on art. 306). Finally, since the book came out much larger than I expected, owing to the size of Section V, I shortened much of what I first intended to do and, especially, I omitted the whole of Section *Eight* (even though I refer to it at times in the present volume; it was to contain a general treatment of algebraic congruences of arbitrary rank). All these things, which will easily fill a book the size of this one, will be published at the first opportunity.

In several difficult discussions I have used synthetic proofs and have suppressed the analysis which led to the results. This was

necessitated by brevity, a consideration that had to be consulted as much as possible.

The theory of the division of a circle or of regular polygons treated in Section VII *of itself* does not pertain to Arithmetic but the *principles* involved depend solely on Higher Arithmetic. Geometers may be as surprised at this fact itself as (I hope) they will be pleased with the new results that derive from this treatment.

These are the things I wanted to warn the reader about. It is not my place to judge the work itself. My greatest hope is that it pleases those who have at heart the development of science, either by supplying solutions that they have been looking for or by opening the way for new investigations.

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 $x^n \equiv A$, 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