Goldstein · Schappacher · Schwermer

The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae

Catherine Goldstein
Norbert Schappacher
Joachim Schwermer *Editors*

The Shaping of Arithmetic

after C. F. Gauss's Disquisitiones Arithmeticae

With 36 Figures

Springer

Catherine Goldstein
Histoire des sciences mathématiques
Institut de mathématiques de Jussieu
175 rue du Chevaleret
75013 Paris, France
E-mail: cgolds@math.jussieu.fr

Joachim Schwermer
Fakultät für Mathematik
Universität Wien
Nordbergstraße 15
1090 Wien, Austria
E-mail: joachim.schwermer@univie.ac.at

Norbert Schappacher
UFR de mathématique
et d'informatique / IRMA
7 rue René Descartes
67084 Strasbourg Cedex, France
E-mail: schappa@math.u-strasbg.fr

Library of Congress Control Number: 2006932291

ISBN 978-3-540-20441-1 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable for prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typeset by the editors
Production: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Cover design: WMXDesign GmbH, Heidelberg

Printed on acid-free paper 44/3100/YL 5 4 3 2 1 0

In memoriam

MARTIN KNESER
1928 – 2004

Foreword

In 1998, the editors convinced themselves that it was the right time to take stock of recent research concerning the modern history of number theory, and to evaluate in its light our comprehension of the development of this discipline as a whole. One issue at stake was to bring together historiographical results coming from different disciplines and linguistic domains which, we felt, had remained too often unaware of each other.

We organized two meetings at the *Mathematisches Forschungsinstitut Oberwolfach* : first a small RIP-workshop held June 14–19, 1999, among historians of number theory and historians of related topics, and then a larger conference which took place June 17–23, 2001, two hundred years after the publication of Carl Friedrich Gauss's *Disquisitiones Arithmeticae*. The latter brought together historians and philosophers of mathematics with number theorists interested in the recent history of their field. Two further meetings, organized by one of us in Vienna and Zürich the following years, continued our venture.

Two concrete projects arose from these activities. One concerned the creation of resources, for scholars and students: we initiated a bibliography of secondary literature on the History of Number Theory since 1800.[1]

The present volume is the second result of our work. It aims at answering the question, already raised during the first workshop, on the role of Gauss's *Disquisitiones Arithmeticae* in the definition and evolution of number theory. This role is here appraised in a comparative perspective, with attention both to the mathematical reception of the treatise, and to its role as a model for doing mathematics. The volume is the result of a collective work. Although all authors have kept their proper voices, they have also accepted quite a bit of editorial interference with a view to making the volume as coherent as possible. We have nonetheless left room for original analyses and results, including newly discovered documents.

1. A preliminary version of this bibliography has been kindly put on line by Franz Lemmermeyer on a website hosted by the University of Heidelberg (http://www.rzuser.uni-heidelberg.de/∼hb3/HINTbib.html).

During its rather long elaboration, the present book has greatly profited from the help of many individuals and institutions which we here gratefully acknowledge: the *Mathematisches Forschungsinstitut Oberwolfach* and its director at the time of the meetings, Matthias Kreck; the *Erwin-Schroedinger International Institute for Mathematical Physics* at Vienna; the ETH at Zürich, and special encouragement provided by Urs Stammbach; the CIRM at Luminy, which gave us a week's refuge for our editorial work in the summer of 2003; the *Laboratoire de mathématiques de l'Université Paris-Sud*, the *Institut de mathématiques de Jussieu*, as well as the *Institut de la recherche mathématique avancée* at Strasbourg which actively supported our joint work for the preparation of this book. Special thanks go to the *Abteilung Handschriften und Alte Drucke der Niedersächsischen Staats- und Universitätsbibliothek Göttingen*, and in particular to Jürgen Rohlfing, for the expert collaboration which made so many documents available to us, some of them as high quality scans. We also express our sincere gratitude to Springer-Verlag and their associated staff at Heidelberg and Leipzig, especially to Joachim Heinze, who believed in this project at an early stage. Our warmest thanks go to Frazer Jarvis for linguistic work on the texts, and to Jim Ritter for constant technical and moral support.

And last but not least, we thank all the participants of the Oberwolfach meetings who have shared their insights and knowledge with us for the benefit of the project: besides the authors of this book, Leo Corry, Hélène Gispert, Jeremy Gray, Ralf Haubrich, Helmut Koch, Martina Schneider, Takase Masahito, Erhard Scholz, Urs Stammbach, and Hans Wussing.

One of the participants at the 2001 conference was Martin Kneser. Despite his serious illness, his intense, visible passion for number theory and its history was a challenging inspiration to all of us, historians and mathematicians alike. Martin Kneser died on February 16, 2004. We dedicate this book to his memory.

July 2006

Catherine Goldstein
Norbert Schappacher
Joachim Schwermer

Table of Contents

Foreword vii
Table of Contents ix
Editions of C. F. Gauss's *Disquisitiones Arithmeticae* xi

Part I. A Book's History 1

Chapter I.1 A Book in Search of a Discipline (1801–1860) 3
Catherine Goldstein & Norbert Schappacher

Chapter I.2 Several Disciplines and a Book (1860–1901) 67
Catherine Goldstein & Norbert Schappacher

Part II. Algebraic Equations, Quadratic Forms, Higher Congruences: Key Mathematical Techniques of the *Disquisitiones* 105

Chapter II.1 The *Disquisitiones Arithmeticae* and the Theory of Equations 107
Olaf Neumann

Chapter II.2 Composition of Binary Quadratic Forms and the Foundations of Mathematics 129
Harold M. Edwards

Chapter II.3 Composition of Quadratic Forms: An Algebraic Perspective 145
Della Fenster & Joachim Schwermer

Chapter II.4 The Unpublished Section Eight: On the Way to Function Fields over a Finite Field 159
Günther Frei

Part III. The German Reception of the *Disquisitiones Arithmeticae:* Institutions and Ideas 199

Chapter III.1 A Network of Scientific Philanthropy: Humboldt's Relations with Number Theorists 201
Herbert Pieper

Chapter III.2 Ὁ Θεὸς Ἀριθμητίζει: The Rise of Pure Mathematics as Arithmetic with Gauss 235
José Ferreirós

Part IV. Complex Numbers and Complex Functions in Arithmetic 269

Chapter IV.1 From Reciprocity Laws to Ideal Numbers: An (Un)Known Manuscript by E.E. Kummer 271
Reinhard Bölling

Chapter IV.2 Elliptic Functions and Arithmetic 291
Christian Houzel

Part V. Numbers as Model Objects of Mathematics 313

Chapter V.1 The Concept of Number from Gauss to Kronecker 315
Jacqueline Boniface

Chapter V.2 On Arithmetization 343
Birgit Petri & Norbert Schappacher

Part VI. Number Theory and the *Disquisitiones* in France after 1850 375

Chapter VI.1 The Hermitian Form of Reading the *Disquisitiones* 377
Catherine Goldstein

Chapter VI.2 Number Theory at the *Association française pour l'avancement des sciences* 411
Anne-Marie Décaillot

Part VII. Spotlighting Some Later Reactions 429

Chapter VII.1 An Overview on Italian Arithmetic after the *Disquisitiones Arithmeticae* 431
Aldo Brigaglia

Chapter VII.2 Zolotarev's Theory of Algebraic Numbers 453
Paola Piazza

Chapter VII.3 Gauss Goes West: The Reception of the *Disquisitiones Arithmeticae* in the USA 463
Della Fenster

Part VIII. Gauss's Theorems in the Long Run: Three Case Studies 481

Chapter VIII.1 Reduction Theory of Quadratic Forms: Toward *Räumliche Anschauung* in Minkowski's Early Work 483
Joachim Schwermer

Chapter VIII.2 Gauss Sums 505
Samuel J. Patterson

Chapter VIII.3 The Development of the Principal Genus Theorem 529
Franz Lemmermeyer

List of Illustrations 563
Index 565
Authors' Addresses 577

Editions of Carl Friedrich Gauss's *Disquisitiones Arithmeticae*

The *Disquisitiones Arithmeticae* has been omitted from the list of references of the individual chapters: we list underneath its various editions. Throughout this book, passages from Gauss's *Disquisitiones Arithmeticae* are referred to only by the article number. The title of Gauss's work is routinely abbreviated as "D.A." For all works, a mention of [Author 1801a] refers to the item "AUTHOR. 1801a" in the bibliography, a mention of [Author 1801/1863] refers to the 1863 edition in this item.

1801. *Disquisitiones Arithmeticae*. Leipzig: Fleischer. Repr. Bruxelles: Culture et civilisation, 1968. Repr. Hildesheim: Olms, 2006. Rev. ed. in *Werke*, vol. 1, ed. Königliche Gesellschaft zu Göttingen [E. Schering]. Göttingen: Universitäts-Druckerei, 1863; 2nd rev. ed., 1870; repr. Hildesheim: Olms, 1973.

http://gallica.bnf.fr
http://dz-srv1.sub.uni-goettingen.de/cache/toc/D137206.html

1807. *Recherches arithmétiques*. French transl. A.-C.-M. Poullet-Delisle. Paris: Courcier. Repr. Sceaux: Gabay, 1989.

http://gallica.bnf.fr

1889. *Arithmetische Untersuchungen*. German transl. H. Maser. In *Untersuchungen über höhere Arithmetik*, pp. 1–453. Berlin: Springer. Repr. New York: Chelsea, 1965; 2nd ed., 1981.

http://dz-srv1.sub.uni-goettingen.de/cache/toc/D232699.html

1959. *Arifmetičeskie issledovaniya*. Russian transl. V. B. Dem'yanov. In *Trudi po teorii čisel* [Works on number theory], ed. I. M. Vinogradov, B. N. Delone, pp. 7–583. Moscow: Academy of Sciences USSR.

1966. *Disquisitiones Arithmeticae*. English transl. A. A. Clarke. New Haven: Yale University Press. Rev. ed. W. C. Waterhouse. New York: Springer, 1986.

1995. *Disquisitiones Arithmeticae*. Spanish transl. H. Barrantes Campos, M. Josephy, A. Ruiz Zùñiga. Colección Enrique Pérez Arbelaez 10. Santa Fe de Bogotá: Academia Colombiana de Ciencias Exactas, Fisicas y Naturales.

1995. *Seisuu ron*. Japanese transl. Takase Masahito. Tokyo: Asakura-Shoten.

1996. *Disquisicions aritmètiques*. Catalan transl. G. Pascual Xufré. Barcelona: Institut d'Estudis Catalans, Societat Catalana de Matemàtiques.

DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

Fig. I. Title page of *Disquisitiones Arithmeticae*, 1801 edition
(Private copy)

Part I

A Book's History

Welche Wichtigkeit Gauß: *Disquisitiones Arithmeticae für die Entwicklung der Mathematik gehabt haben, darüber existiert wohl kein Zweifel. Es ist ein Werk, das ungefähr in der Mathematik dieselbe Stellung einnimmt, wie die Kritik der reinen Vernunft von* Kant *in der Philosophie.*

Carl Itzigsohn, March 23, 1885

SCIENCES.

Recherches arithmétiques, par M. C. Fr. Gauss [de Brunswick], traduites par A. C. M. Poullet-Delisle, professeur de mathématiques au Lycée d'Orléans. — Paris 1807.

Au titre modeste de cet ouvrage, quelques personnes pourraient croire d'abord que l'auteur n'y considère que les questions les plus simples. Mais ces Recherches arithmétiques sont au fond, des recherches très-savantes sur les *propriétés générales* des nombres, et sur l'*analyse indéterminée* à laquelle elles se lient : matière profonde, inépuisable, la plus neuve et la plus ardue peut-être de toutes les parties des mathématiques.

L'arithmétique élémentaire n'est guères autre chose, comme on sait, que l'art de la numération qui peut s'établir d'une infinité de manières, suivant l'échelle ou la base que l'on veut choisir. Mais les nombres, considérés en eux-mêmes, ont des propriétés qui ne dépendent point du tout de la manière dont on les représente. Ainsi il y a des nombres qui ne peuvent être divisés par aucun autre, et qu'on appelle *premiers* ou simples, parce que tous les autres s'en composent par la multiplication ; il y a les nombres *figurés* qu'on nomme *triangles*, *quarrés*, *pentagones*, *exagones*, etc. selon que leurs unités considérées comme des points, par exemple, pourraient être arrangées symétriquement en triangle, en quarré, en pentagone, etc. Il y a les différentes *puissances* des nombres qu'on produit en les multipliant par eux-mêmes, et une foule d'autres formés par diverses lois et par toutes les combinaisons régulières de celles-là. Or tous ces nombres et leurs propriétés demeurent toujours les mêmes dans tous les systèmes possibles de numération ; et de-là résulte un certain genre de spéculations mathématiques d'où naissent plusieurs vérités ou théorèmes qui, avec le peu qu'on sait trouvé jusqu'ici de l'art de se conduire dans ces recherches, constituent cette arithmétique transcendante qu'on nomme aujourd'hui la théorie des nombres.

Ni les bornes, ni la nature de cette feuille ne nous permettraient des développemens bien étendus sur cette matière. Pour ceux d'ailleurs qui voudraient l'approfondir, les détails seraient toujours insaisissans, et pour les autres, superflus. Nous ferons seulement observer que les propriétés qu'on étudie aujourd'hui dans les nombres, n'ont aucun rapport à ces vertus merveilleuses qu'y cherchaient les anciens philosophes. Elles ne regardent que leurs simples manières d'être les uns à l'égard des autres, comme sous le point de vue, des diviseurs qu'ils peuvent avoir, des résidus qu'ils laissent ; et en général, on les peut rapporter à certaines possibilités ou impossibilités de décomposer les nombres formés par une certaine loi, en d'autres formés par une loi différente, ou par la même. Elles peuvent donc se partager naturellement en deux grandes classes ; les propriétés positives et les propriétés négatives ; dont on peut se faire une idée par les théorèmes suivans :

Un nombre quelconque est toujours décomposable en trois triangles, ou en quatre quarrés, ou en cinq pentagones, ou en six exagones, et ainsi à l'infini : (zéro pouvant quelquefois être compté dans cette décomposition comme un nombre figuré.)

Une puissance quelconque au-dessus de la seconde, ne peut jamais se décomposer en deux puissances semblables. Ainsi aucun cubes ne peuvent former un cube ; deux bi-quarrés n'en font point quarré, et de même à l'infini.

L'élégante simplicité de ces théorèmes, leur expression si claire et si bien terminée qu'on les voit d'abord du premier coup-d'œil ; et cependant l'extrême difficulté qui se fait bientôt sentir quand on en veut essayer la démonstration rigoureuse, peuvent expliquer le singulier attrait de ces questions de ce genre, et l'espèce de passion avec laquelle on y livre, dès qu'une fois on a commencé de s'en occuper. Cette science d'ailleurs nous presse, toujours nouvelle et renaissant à chaque pas des découvertes. Les progrès de l'algèbre, et l'invention des nouveaux calculs ont mis successivement les géomètres en état de vaincre les plus hautes difficultés de la géométrie et de la mécanique. Un fleux aujourd'hui résout facilement des problèmes qui ont arrêté les plus rigoureux génies ; et c'est ce qui fait que l'on ne peut exactement comparer les géomètres séparés l'un d'un peu longs intervalles. Mais ces mêmodes, dit-on, ont si bien fait asservir et mesurer toutes les affections des grandeurs continues, ne nous ont presque rien appris sur le calcul et les combinaisons des quantités discrètes. On ne sait guère y appliquer jusqu'ici plus d'Analyse que n'en avait Fermat il y a deux siècles ; et comme ce génie n'était fait sans doute, pour y pénétrer, quelqu'art nouveau dont le secret ne nous est point parvenu, personne n'y a pu rétablir encore toutes les démonstrations perdues de la plupart de ses théorèmes, et entre autres, celles des deux précédens qui sont dûs à cet homme extraordinaire. Ainsi, quand les autres branches des mathématiques se sont élevées par degrés à la perfection, et que les géomètres y ont si bien réalisé cette allégorie, qu'un *enfant monte sur les épaules d'Hercule qui plus loin que lui-même*, la doctrine des nombres, malgré leurs travaux, est restée, pour ainsi dire, immobile : comme pour eux, dans tous les temps, l'épreuve de leurs forces et la mesure de la pénétration de leur esprit.

C'est pourquoi M. *Gauss*, par un ouvrage aussi profond et aussi neuf que ses *Recherches arithmétiques*, n'annonce certainement comme une des meilleures têtes mathématiques de l'Europe. Il paraît, dans sa préface, qu'en 1795, où il entra pour la première fois ses méditations du côté des nombres, il n'avait encore aucune idée de ce qui avait été fait avant lui sur cette matière,

I.1

A Book in Search of a Discipline (1801–1860)

CATHERINE GOLDSTEIN and NORBERT SCHAPPACHER

Carl Friedrich Gauss's *Disquisitiones Arithmeticae* of 1801 has more than one claim to glory: the contrast between the importance of the book and the youth of its author; the innovative concepts, notations, and results presented therein; the length and subtlety of some of its proofs; and its role in shaping number theory into a distinguished mathematical discipline.

The awe that it inspired in mathematicians was displayed to the cultured public of the *Moniteur universel ou Gazette nationale*[1] as early as March 21, 1807, when Louis Poinsot, who would succeed Joseph-Louis Lagrange at the Academy of Sciences six years later, contributed a full page article about the French translation of the *Disquisitiones Arithmeticae*:

> The doctrine of numbers, in spite of [the works of previous mathematicians] has remained, so to speak, immobile, as if it were to stay for ever the touchstone of their powers and the measure of their intellectual penetration. This is why a treatise as profound and as novel as his *Arithmetical Investigations* heralds M. Gauss as one of the best mathematical minds in Europe.[2]

1. This French newspaper, created by Charles-Joseph Panckoucke in the first months of the French Revolution, had the goal of informing its readers of administrative, political, and cultural events and of promoting French achievements. It opened its columns regularly to reviews of books recommended by the *Institut national des sciences et des arts.*

2. *Gazette nationale ou Le Moniteur universel* 80 (1807), 312: *La doctrine des nombres malgré leurs travaux [antérieurs] est restée, pour ainsi dire, immobile ; comme pour être dans tous les tems, l'épreuve de leurs forces et la mesure de la pénétration de leur esprit. C'est pourquoi Monsieur Gauss, par un ouvrage aussi profond et aussi neuf que ses* Recherches arithmétiques *s'annonce certainement comme une des meilleures têtes mathématiques de l'Europe.*

A long string of declarations left by readers of the book, from Niels Henrik Abel to Hermann Minkowski, from Augustin-Louis Cauchy to Henry Smith, bears witness to the profit they derived from it. During the XIXth century, its fame grew to almost mythical dimensions. In 1891, Edouard Lucas referred to the *Disquisitiones Arithmeticae* as an "imperishable monument [which] unveils the vast expanse and stunning depth of the human mind,"[3] and in his Berlin lecture course on the concept of number, Leopold Kronecker called it "the Book of all Books."[4] In the process, new ways of seeing the *Disquisitiones* came to the fore; they figure for instance in the presentation given by John Theodore Merz in his celebrated four-volume *History of European Thought in the Nineteenth Century*:

> Germany … was already an important power in the Republic of exact science which then had its centre in Paris. Just at the beginning of the nineteenth century two events happened which foreboded for the highest branches of the mathematical sciences a revival of the glory which in this department Kepler and Leibniz had already given to their country. … The *first* was the publication of the 'Disquisitiones Arithmeticae' in Latin in 1801.[5] … [Gauss] raised this part of mathematics into an independent science of which the 'Disquisitiones Arithmeticae' is the first elaborate and systematic treatise.… It was … through Jacobi, and still more through his contemporary Lejeune-Dirichlet … that the great work of Gauss on the theory of numbers, which for twenty years had remained sealed with seven seals, was drawn into current mathematical literature… The seals were only gradually broken. Lejeune-Dirichlet did much in this way, others followed, notably Prof. Dedekind, who published the lectures of Dirichlet and added much of his own.[6]

Gauss's book (hereafter, we shall often use the abbreviation "the D.A." to designate it) is now seen as having created number theory as a systematic discipline in its own right, with the book, as well as the new discipline, represented as a landmark of German culture. Moreover, a standard history of the book has been elaborated. It stresses the impenetrability of the D.A. at the time of its appearance and integrates it into a sweeping narrative, setting out a continuous unfolding of the book's content, from Johann Peter Gustav Lejeune-Dirichlet and Carl Gustav Jacob Jacobi on.

In this history modern algebraic number theory appears as the natural outgrowth of the discipline founded by the *Disquisitiones Arithmeticae*. Historical studies have accordingly focused on the emergence of this branch of number theory, in particular on the works of Dirichlet, Ernst Eduard Kummer, Richard Dedekind, Leopold Kronecker, and on the specific thread linking the D.A. to the masterpiece of algebraic number theory, David Hilbert's *Zahlbericht* of 1897. In addition, they have also explored the fate of specific theorems or methods of the D.A. which are relevant for number theorists today.

Yet a full understanding of the impact of the *Disquisitiones Arithmeticae*, at

3. [Lucas 1891], p. vi: *Ce livre, monument impérissable dévoile l'immense étendue, l'étonnante profondeur de la pensée humaine.*
4. [Kronecker 1891/2001], p. 219: *das Buch aller Bücher.*
5. The second event alluded to by Merz is the computation of Ceres's orbit, also by Gauss.
6. [Merz 1896–1914], vol. I, pp. 181, 181–182 (footnote), 187–188 and 721.

all levels, requires more than just a "thicker description"[7] of such milestones; it requires that light be shed on other patterns of development, other readers, other mathematical uses of the book – it requires a change in our questionnaire. We need to answer specific questions, such as: What happened to the book outside Germany? What were the particularities, if any, of its reception in Germany? Which parts of it were read and reworked? And when? Which developments, in which domains, did it stimulate – or hamper? What role did it play in later attempts to found mathematics on arithmetic?

Such questions suggest narrower foci, which will be adopted in the various chapters of the present volume. In this first part, however, we take advantage of the concrete nature of our object of inquiry – a book – to draw a general map of its tracks while sticking closely to the chronology. That is to say, instead of going backwards, seeking in the *Disquisitiones Arithmeticae* hints and origins of more recent priorities, we will proceed forwards, following Gauss's text through time with the objective of surveying and periodizing afresh its manifold effects.[8]

But let us start, first, at the beginning of all beginnings…

1. The Writing and the Architecture of the *Disquisitiones Arithmeticae*

Gauss began to investigate arithmetical questions, at least empirically, as early as 1792, and to prepare a number-theoretical treatise in 1796 (i.e., at age 19 and, if we understand his mathematical diary correctly, soon after he had proved both the constructibility of the 17-gon by ruler and compass and the quadratic reciprocity law). An early version of the treatise was completed a year later.[9] In November 1797, Gauss started rewriting the early version into the more mature text which he would give to the printer bit by bit. Printing started in April 1798, but proceeded very slowly for technical reasons on the part of the printer. Gauss resented this very much, as his letters show; he was looking for a permanent position from 1798. But he did use the delays to add new text, in particular to sec. 5 on quadratic forms, which had roughly doubled in length by the time the book finally appeared in the summer of 1801.[10]

---

7. The reference is to Gilbert Ryle and Clifford Geertz, in particular [Geertz 1973].
8. We have systematically tracked mentions of the D.A. in the main nineteenth-century journals, and then in the complete works – if published – of the mathematicians encountered. For want of space (in the text or in the margin …), only part of the evidence used to establish our main claims can be presented here.
9. Parts of the manuscript, known as *Analysis residuorum*, were published posthumously in Gauss's *Werke*; other parts were identified as such in 1980 by Uta Merzbach in different German archives; see [Merzbach 1981], also for a global comparison of the early version with the printed book; for detailed comparisons of specific parts, in particular sec. 2, see [Bullynck 2006a] and [Bullynck 2006b], appendices A and B. See also [Schlesinger 1922], sec. III.
10. Basic data on the genesis of the *Disquisitiones* can be derived from Gauss's mathematical diary, [Gauss 1796–1814], and from his correspondence. Our quick summary here is based on [Merzbach 1981]. What exactly Gauss found in his predecessors and how he was influenced by them remains a difficult question, in spite of his own historical

1.1. The First Sections: Congruences to the Fore

Let us skim through the contents of the *Disquisitiones Arithmeticae* as they appeared in 1801.[11] Although it may make somewhat tedious reading, we think it useful to indicate the full variety of matters treated by Gauss. The 665 pages and 355 articles of the main text are divided unevenly into seven sections. The first and smallest one (7 pp., 12 arts.) establishes a new notion and notation which, despite its elementary nature, modified the practice of number theory:

> If the number a measures[12] the difference of the numbers b, c, then b and c are said to be *congruent according to* a; if not, *incongruent*; this a we call the *modulus.* Each of the numbers b, c are called a *residue* of the other in the first case, a *nonresidue* in the second.[13]

The corresponding notation $b \equiv c \pmod{a}$ is introduced in art. 2. The remainder of sec. 1 contains basic observations on convenient sets of residues modulo a and on the compatibility of congruences with the arithmetic operations. To consider numbers or equations up to a given integer was not new with Gauss.[14] His innovation was to turn this occasional computational device into a topic in its own right.

Section 2 (33 pp., 32 arts.) opens with several theorems on integers including the unique prime factorization of integers (in art. 16), and then treats linear congruences in arts. 29–37, including the Euclidean algorithm and what we call the Chinese remainder theorem. At the end of sec. 2, Gauss added a few results for future reference which had not figured in the 1797 manuscript, among them: (i) properties

---

remarks. We do not go into it here, referring for a first orientation and survey of Gauss's obvious predecessors, in particular Euler, Lagrange and Legendre, to [Weil 1984]; the less-expected tradition of German arithmetical textbooks and the more general impact of Lambert's and Hindenburg's works are explored in the original thesis of Maarten Bullynck, [Bullynck 2006b].

11. The reader is invited to go back and forth between our rough summary and Gauss's original detailed table of contents which we reproduce on the double page 10–11. In the present section, expressions in quotation marks, with no explicit reference attached, are the English translations of key words from this Latin table of contents. The table is copied from the 1801 edition of the D.A. except that, for the sake of readability, we have modified the letters "u" and "v" according to current Latin spelling. Other surveys of the book are proposed in [Bachmann 1911], [Rieger 1957], [Neumann 1979–1980], [Bühler 1981], chap. 3, [Neumann 2005].

12. Along with this classical Euclidean term "to measure" (*metiri*), which, as well as "modulus" (small measure), reminds us of the additive flavour of Euclidean division, Gauss also used "to divide" (*dividere*) as of sec. 2, art. 13, in the context of a product of natural integers. This diversity of expressions was not always maintained in translations.

13. Our translation of the opening paragraph of D.A., art. 1: *Si numerus a numerorum b, c differentiam metitur, b et c* secundum *a* congrui *dicuntur, sin minus,* incongrui*: ipsum a* modulum *appellamus. Uterque numerorum b, c, priori in casu alterius* residuum*, in posteriori vero* nonresiduum *vocatur.*

14. Gauss acknowledged this fact in the footnote to art. 2, noticing that Legendre had used a simple equality in such situations, and pleading at the same time for his own, unequivocal notation. Other authors are discussed in [Bullynck 2006b], appendix A.

of the number $\varphi(A)$ of prime residues modulo A (arts. 38–39); (ii) in art. 42, a proof that the product of two polynomials with leading coefficient 1 and with rational coefficients that are not all integers cannot have all its coefficients integers;[15] and (iii) in arts. 43 and 44, a proof of Lagrange's result that a polynomial congruence modulo a prime cannot have more zeros than its degree.[16]

Section 3 (51 pp., 49 arts.) is entitled "On power residues." As Gauss put it, it treats "geometric progressions" $1, a, a^2, a^3, \ldots$ modulo a prime number p (for a number a not divisible by p), discusses the "period" of a modulo p and Fermat's theorem, contains two proofs for the existence of "primitive roots" modulo p, and promotes the use of the "indices" of $1, \ldots, p-1$ modulo p with respect to a fixed primitive root, in analogy with logarithm tables.[17] After a discussion, in arts. 61–68, of n^{th} roots mod p from the point of view of effective computations, the text returns to calculations with respect to a fixed primitive root, and gives in particular in arts. 75–78 two proofs – and sketches a third one due to Lagrange – of Wilson's theorem, $1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}$. The analogous constructions and results for an odd prime power are discussed in arts. 82–89, the exceptional case of the powers of $p = 2$ in arts. 90–91. Finally, integers n for which there exists a primitive root modulo n are characterized in art. 92.

Section 4 (73 pp., 59 arts.), "On congruences of degree 2," develops a systematic theory of "quadratic residues" (i.e., residues of perfect squares). It culminates in the "fundamental theorem" of this theory, from which "can be deduced almost everything that can be said about quadratic residues,"[18] and which Gauss stated as:

> If p is a prime number of the form $4n+1$, then $+p$, if p is of the form $4n+3$, then $-p$, will be a [quadratic] residue, resp. nonresidue, of any prime number which, taken positively, is a residue, resp. nonresidue of p.[19]

Gauss motivated this *quadratic reciprocity law* experimentally, gave the general statement and formalized it in tables of possible cases (arts. 131 and 132), using the notation aRa', resp. aNa', to mean that a is a quadratic residue, resp. nonresidue, modulo a'.[20] He also gave here the first proof of the law, an elementary one by

15. This is one of several results known today as "Gauss's lemma."
16. See [Bullynck 2006a], for a closer study of sec. 2 in comparison to Gauss's earlier manuscript of the D.A.
17. In modern terms, the period is the order of the element a in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$, Fermat's theorem states that this order divides $p-1$, a primitive root is a generator of the group and the index of an element is the corresponding exponent with respect to the chosen generator.
18. D.A., art. 131: … *omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur.*
19. Our translation of D.A., art. 131: *Si p est numerus primus formae* $4n+1$*, erit* $+p$*, si vero p formae* $4n+3$*, erit* $-p$ *residuum vel non residuum cuiusuis numeri primi qui positive acceptus ipsius p est residuum vel non residuum.* The supplementary theorems about the quadratic residue behaviour of -1 and 2 are treated in parallel.
20. Today one usually sees this quadratic reciprocity law written in terms of Legendre's symbol. It is defined, for any integer a and p a prime number not dividing a, by

induction.[21] A crucial nontrivial ingredient (used in art. 139) is a special case of a theorem stated in art. 125, to the effect that, for every integer which is not a perfect square, there are prime numbers modulo which it is a quadratic nonresidue.[22]

1.2. Quadratic Forms

The focus changes in sec. 5 of the D.A., which treats "forms and indeterminate equations of the second degree," mostly binary forms, in part also ternary. With its 357 pp. and 156 arts., this section occupies more than half of the whole *Disquisitiones Arithmeticae*. Leonhard Euler, Joseph-Louis Lagrange, and Adrien-Marie Legendre had forged tools to study the representation of integers by quadratic forms. Gauss, however, moved away from this Diophantine aspect towards a treatment of quadratic forms as objects in their own right, and, as he had done for congruences, explicitly pinpointed and *named* the key tools. This move is evident already in the opening of sec. 5:

> The form $axx + 2bxy + cyy$,[23] when the indeterminates x, y are not at stake, we will write like this, (a, b, c).[24]

Gauss then immediately singled out the quantity $bb - ac$ which he called the "determinant"[25] – "on the nature of which, as we will show in the sequel, the prop-

---

$\left(\frac{a}{p}\right) = \pm 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$, that is, 1 if a is quadratic residue modulo p, -1 if not; see [Legendre 1788], p. 186, and D.A., art. 106, for the last congruence. Given distinct odd prime numbers p, q, the quadratic reciprocity law then says that $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$. Notwithstanding Dirichlet's criticism (published after Gauss's death) of the D.A. as lacking a notational calculus for quadratic residues, [Dirichlet 1889–1897], vol. 2, p. 123, one may point out that Gauss's formulation stresses the normalization of $\pm p$, a phenomenon that would recur with higher reciprocity laws; see [Neumann 2005], p. 308.

21. In the late 1960s, John Tate "lifted directly from the argument which was used by Gauss in his first proof of the quadratic reciprocity law" his determination of the second K-group of the field of rational numbers $K_2(\mathbf{Q})$; see [Milnor 1971], p. 102. More generally, Gauss's argument is seen to provide an inductive procedure to determine successively the local factors at all primes p of a given Steinberg symbol on $\mathbf{Q}^* \times \mathbf{Q}^*$, and the decomposition of the universal continuous Steinberg symbol with values in $\{\pm 1\}$ is tantamount to the reciprocity law. See [Milnor 1971], p. 101–107; cf. [Tate 1971], § 3.

22. This follows easily from the reciprocity law; Gauss does not even bother to give the details. The difficulty is to prove it *directly* (arts. 125–129) in a special case which then makes the proof by complete induction of the reciprocity law work: that every $\pm p$, for a prime p of the form $4n + 1$, is a quadratic nonresidue modulo some prime $q < p$.

23. Gauss's convention that the coefficient of the mixed term be even is original and its advantages and drawbacks have been much in debate; see J. Schwermer's chap. VIII.1.

24. D.A., art. 153: *Formam $axx + 2bxy + cyy$, quando de indeterminatis x, y non agitur, ita designabimus (a, b, c).* In [Kronecker 1891/2001], p. 235, this move is heralded as the first time in history that a system of three discrete quantities was introduced.

25. Nowadays called, sometimes up to a constant, the *discriminant* of the form. For the various normalizations and names of this quantity in the XIX$^{\text{th}}$ century, see [Dickson 1919–1923], vol. 3, p. 2. We will usually employ Gauss's word in this chapter.

erties of the form chiefly depend"[26] – showing that it is a quadratic residue of any integer primitively represented[27] by the form (art. 154).

The first part of sec. 5 (arts. 153–222, 146 pp.) is devoted to a vast enterprise of a finer classification of the forms of given determinant, to which the problem of representing numbers by forms is reduced. Gauss defined two quadratic forms (art. 158) to be equivalent if they are transformed into one another under substitutions of the indeterminates, changing (x, y) into $(\alpha x+\beta y, \gamma x+\delta y)$, for integral coefficients $\alpha, \beta, \gamma, \delta$, with $\alpha\delta-\beta\gamma = +1$ or $= -1$.[28] Two equivalent forms represent the same numbers. If $\alpha\delta-\beta\gamma = +1$, the equivalence is said to be "proper," if $\alpha\delta-\beta\gamma = -1$, "improper." While integral invertible substitutions were already used by Lagrange, this finer distinction is due to Gauss and greatly exploited by him. After generalities relating to these notions and to the representation of numbers by forms – in particular (art. 162), the link between the problem of finding *all* transformations between two, say, properly equivalent forms, when one is known, and the solutions of the equation $t^2 - Du^2 = m^2$, where D is the determinant of the forms and m the greatest common divisor of their coefficients – the discussion then splits into two very different cases according to whether the determinant is negative or positive. In each case, Gauss showed that any given form is properly equivalent to a so-called "reduced" form (art. 171 for negative, art. 183 for positive discriminants), not necessarily unique, characterized by inequalities imposed on the coefficients.[29] The number of reduced forms – and thus also the number of equivalence classes of forms – of a given determinant is finite. Equivalence *among reduced forms* is studied – in particular, the distribution of the reduced forms of given positive determinant into "periods" of equivalent reduced forms, art. 185 – and a general procedure is given to determine if two binary quadratic forms with the same determinant are (properly or improperly) equivalent and to find all transformations between them. Using this, Gauss settled the general problem of representing integers by quadratic forms (arts. 180–181, 205, 212), as well as the resolution in integers of quadratic equations with two unknowns and integral coefficients (art. 216). The first half of sec. 5 closes with a brief historical reminder (art. 222).

The classification of forms also ushers the reader into the second half of sec. 5, entitled "further investigations on forms." Art. 223 fixes an algorithm to find a good representative for every (proper equivalence) class of quadratic forms of a given determinant. Representing classes by reduced forms avoids working with the infinite classes abstractly, just as Gauss never worked with our field $\mathbf{Z}/p\mathbf{Z}$, the elements of which are infinite sets of integers, but with conveniently chosen residues modulo p.

---

26. D.A., art. 154: *Numerum bb − ac, a cuius indole proprietates formae* (a, b, c) *imprimis pendere, in sequentibus docebimus,* determinantem *huius formae vocabimus.*
27. I.e., which can be written as $axx + 2bxy + cyy$, for two *coprime* integers x and y.
28. Gauss also handled the general case of arbitrary substitutions with integral coefficients transforming a form into another one which is then said to be "contained" in the first.
29. A reduced form (A, B, C) of determinant $D < 0$ is such that $A \le 2\sqrt{-D/3}$, $B \le A/2$, $C \ge A$. A reduced form of determinant $D > 0$ is such that $0 \le B < \sqrt{D}$, $\sqrt{D} - B \le |A| \le \sqrt{D} + B$.

Original Table of Contents of the *Disquisitiones Arithmeticae*

Dedicatio. Praefatio.

Sectio prima. De numerorum congruentia in genere.

Numeri congrui, moduli, residua et non residua, art. 1 sq. Residua minima, 4. Propositiones elementares de congruis, 5. Quaedam applicationes, 12.

Sectio secunda. De congruentiis primi gradus.

Theoremata praeliminaria de numeris primis, factoribus etc. 13. Solutio congruentiarum primi gradus, 26. De inveniendo numero secundum modulos datos residuis datis congruo 32. Congruentiae lineares quae plures incognitas implicant 37. Theoremata varia 38.

Sectio tertia. De residuis potestatum.

Residua terminorum progressionis geometricae ab unitate incipientis constituunt seriem periodicam, 45. *Considerantur primo moduli qui sunt numeri primi.* Ponendo modulum $= p$, multitudo terminorum in periodo metitur numerum $p - 1$ art. 49. Fermatii theorema, 50. Quot numeris respondeant periodi, in quibus terminorum multitudo est divisor datus numeri $p - 1$ art. 52. Radices primitivae, bases, indices, 57. Algorithmus indicum, 58. De radicibus congruentiae $x^n \equiv A$, art. 60. Nexus indicum in systematibus diversis, 69. Bases usibus peculiaribus accommodatae, 72. Methodus radices primitivas assignandi, 73. Theoremata varia de periodis et radicibus primitivis, 75. (Theorema Wilsonianum, 76). *De modulis qui sunt numerorum primorum potestates, 82. Moduli qui sunt potestates binarii, 90. Moduli e pluribus primis compositi, 92.*

Sectio quarta. De congruentiis secundi gradus.

Residua et nonresidua quadratica art. 94. Quoties modulus est numerus primus, multitudo residuorum ipso minorum multitudini nonresiduorum aequalis, 96. Quaestio, utrum numerus compositus residuum numeri primi dati sit an nonresiduum, ab indole factorum pendet, 98. De modulis, qui sunt numeri compositi, 100. Criterium generale, utrum numerus datus numeri primi dati residuum sit an nonresiduum, 106. *Disquisitiones de numeris primis quorum residua aut non residua sint numeri dati* 107 sqq. Residuum -1 art. 108. Residua $+2$ et -2, art. 112. Residua $+3$ et -3, art. 117. Residua $+5$ et -5 art. 121. De ± 7 art. 124. Praeparatio ad disquisitionem generalem, 125. Per inductionem theorema generale (*fundamentale*) stabilitur, conclusionesque inde deducuntur 130. Demonstratio rigorosa huius theorematis, 135. Methodus analoga, theorema art. 114 demonstrandi, 145. Solutio problematis generalis 146. De formis linearibus omnes numeros primos continentibus, quorum vel residuum vel non residuum est numerus quicunque datus 147. De aliorum laboribus circa has investigationes 151. De congruentiis secundi gradus non puris 152.

Sectio quinta. De formis aequationibusque indeterminatis secundi gradus.

Disquisitionis propositum; formarum definitio et signum 153. Numerorum repraesentatio; determinans 154. Valores expr. $\sqrt{(bb - ac)}$ (mod. M) ad quos repraesentatio numeri M per formam (a, b, c) pertinet, 155. Forma aliam implicans, sive sub alia contenta; transformatio, propria et impropria, 157. Aequivalentia, propria et impropria 158. Formae oppositae 159, contiguae 160. Divisores communes coëfficientium formarum 161. Nexus omnium transformationum similium formae datae in formam datam 162. Formae ancipites 163. Theorema circa casum ubi forma sub alia simul proprie et improprie contenta est 164. Generalia de repraesentationibus numerorum per formas, earumque nexu cum transformationibus 166. *De formis determinantis negativi* 171. Applicationes speciales ad discerptionem numerorum in quadrata duo, in quadratum simplex et duplex, in simplex et triplex 182. *De formis determinantis positivi non-quadrati* 183. *De formis determinantis quadrati* 206. Formae sub aliis contentae quibus tamen non aequivalent 213. *Formae determinantis* 0 art. 215. Solutio generalis omnium aequationum indeterminatarum secundi gradus duas incognitas implicantium per numeros integros 216. Annotationes historicae 222.

DISQUISITIONES ULTERIORES DE FORMIS. Distributio formarum determinantis dati in classes 223; classium in ordines 226. Ordinum partitio in genera 228. *De compositione formarum* 238. Compositio ordinum 245, generum 246, classium 249. Pro determinante dato in singulis generibus eiusdem ordinis classes aeque multae continentur 252. Comparantur multitudines classium in singulis generibus ordinum diversorum contentarum 253. De multitudine classium ancipitum 257. Certe semissi omnium characterum pro determinante dato assignabilium genera proprie primitiva (positiva pro det. neg.) respondere nequeunt 261. Theorematis fundamentalis et reliquorum theorematum ad residua -1, $+2$, -2 pertinentium demonstratio secunda 262. Ea characterum semissis, quibus genera respondere nequeunt, propius determinantur 263. Methodus peculiaris, numeros primos in duo quadrata decomponendi 265. DIGRESSIO CONTINENS TRACTATUM DE FORMIS TERNARIIS 266 sqq. *Quaedam applicationes ad theoriam formarum binariarum.* De invenienda forma e cuius duplicatione forma binaria data generis principalis oriatur 286. Omnibus characteribus, praeter eos, qui in artt. 262, 263 impossibiles inventi sunt, genera revera respondent 287, III. Theoria decompositionis tum numerorum tum formarum binariarum in tria quadrata 288. Demonstratio theorematum Fermatianorum, quemvis integrum in tres numeros trigonales vel quatuor quadrata discerpi posse 293. Solutio aequationis $axx + byy + czz = 0$ art. 294. De methodo per quam ill. Le Gendre theorema fundamentale tractavit 296. Repraesentatio cifrae per formas ternarias quascunque 299. Solutio generalis aequationum indeterminatarum secundi gradus duas incognitas implicantium per quantitates rationales 300. De multitudine mediocri generum 301, classium 302. Algorithmus singularis classium proprie primitivarum; determinantes regulares et irregulares etc. art. 305.

Sectio sexta. Variae applicationes disquisitionum praecedentium.

Resolutio fractionum in simpliciores 309. Conversio fractionum communium in decimales 312. Solutio congruentiae $xx \equiv A$ per methodum exclusionis 319. Solutio aequationis indeterminatae $mxx + nyy = A$ per exclusiones 323. Alia methodus congruentiam $xx \equiv A$ solvendi pro eo casu ubi A est negativus 327. Duae methodi, numeros compositos a primis dignoscendi, illorumque factores investigandi, 329.

Sectio septima. De aequationibus, circuli sectiones definientibus.

Disquisitio reducitur ad casum simplicissimum, ubi multitudo partium, in quas circulum secare oportet, est numerus primus 336. Aequationes pro functionibus trigonometricis arcuum qui sunt pars aut partes totius peripheriae; reductio functionum trigonometricarum ad radices aequationis $x^n - 1 = 0$ art. 337. *Theoria radicum huius aequationis* (ubi supponitur, n esse numerum primum). Omittendo radicem 1, reliquae (Ω) continentur in aequatione $X = x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$. Functio X resolvi nequit in factores inferiores, in quibus omnes coëfficientes sint rationales 341. Propositum disquisitionum sequentium declaratur 342. Omnes radices Ω in certas classes (periodos) distribuuntur 343. Varia theoremata de his periodis 344 sqq. His disquisitionibus superstruitur solutio aequationis $X = 0$ art. 352. Exempla pro $n = 19$, ubi negotium ad duas aequationes cubicas unamque quadraticam, et pro $n = 17$, ubi ad quatuor quadraticas reducitur artt. 353, 354. *Disquisitiones ulteriores de hoc argumento.* Aggregata, in quibus terminorum multitudo par, sunt quantitates reales 355. De aequatione, per quam distributio radicum Ω in *duas* periodos definitur 356. Demonstratio theorematis in sect. IV commemorati 357. De aequatione pro distributione radicum Ω in *tres* periodos 338. Aequationum, per quas radices Ω inveniuntur reductio ad puras 359. *Applicatio disquisitionum praecedentium ad functiones trigonometricas.* Methodus, angulos quibus singulae radices Ω respondeant dignoscendi 361. Tangentes, cotangentes, secantes et cosecantes e sinubus et cosinubus absque divisione derivantur 362. Methodus, aequationes pro functionibus trigonometricis successive deprimendi 363. Sectiones circuli, quas per aequationes quadraticas sive per constructiones geometricas perficere dicet 365.

Additamenta.

Tabulae.

In art. 226, certain classes are grouped together into an "order" according to the divisibility properties of their coefficients.[30] There follows (arts. 229–233) a finer grouping of the classes within a given order according to their "genus." Gauss showed that, for every odd prime divisor p of the determinant of a form (with coprime coefficients), integers prime to p that can be represented by the form (and thus by all forms of its class) are either all quadratic residues, or all nonresidues modulo p: recording this information, as well as similar information at $p = 2$ for even discriminants, defines the "character" of the form (or of the class of the form). Classes with the same character are put into the same genus. The principal genus for a determinant D is that of the principal form $(1, 0, -D)$.[31]

In art. 235, Gauss defined a form $F(X, Y) = AXX+2BXY+CYY$ to be a "composite" of $f(x, y) = axx + 2bxy + cyy$ and $f'(x', y') = a'x'x' + 2b'x'y' + c'y'y'$, if $F(B_1, B_2) = f(x, y) \cdot f'(x', y')$, for certain transformations of the indeterminates $B_i(x, y; x', y')$, bilinear, as we would say, in x, y and x', y'. While this definition generalizes time-honoured relations like the following,[32] with $F = f = f'$:

$$(xx' - Nyy')^2 + N(xy' + yx')^2 = (x^2 + Ny^2) \cdot (x'^2 + Ny'^2),$$

the generality of the concept allowed Gauss to enter uncharted territory, for instance, to check – by elaborate computations – formal properties like the commutativity and associativity of the operation, as far as it is defined on the level of forms (arts. 240–241). In the end, the concept yields a multiplicative structure on the set of orders (art. 245) and of genera, with the principal genus acting like a neutral element (arts. 246–248), and indeed of classes (art. 239 and art. 249) of the same determinant.[33]

This rich new structure gave Gauss a tremendous leverage: to answer new questions, for instance, on the distribution of the classes among the genera (arts. 251–253); to come back to his favourite theorem, the quadratic reciprocity law, and derive a second proof of it from a consideration of the number of characters that actually correspond to genera of a given discriminant (arts. 261–262); to solve a long-standing conjecture of Fermat's (art. 293) to the effect that every positive integer is the sum of three triangular numbers. For this last application, as well as for deeper insight into the number of genera, Gauss quickly generalized (art. 266 ff.) the basic theory of reduced forms, classes etc., from binary to ternary quadratic forms. This

30. It is with explicit reference to this terminology that Richard Dedekind would later introduce the notion of order into algebraic number theory in [Dedekind 1930–1932], vol. 1, pp. 105–158.

31. See also §2 of F. Lemmermeyer's chap. VIII.3 below. Such classificatory schemes, then part and parcel of the natural sciences, already existed in mathematics, with variants, see Hindenburg's classification in [Bullynck 2006b], pp. 259–260. Note, however, that Gauss put classes below genera and orders.

32. [Weil 1986]. Cf. the blackboard in [Weil 1979], vol. III, p. ii.

33. This particularly difficult theory of the composition of forms has been reformulated several times by Gauss's successors; two different perspectives, emphasizing different aspects of its history and of its current relevance, are proposed in chaps. II.2 and II.3 below, by H.M. Edwards and by D. Fenster and J. Schwermer.

gave him in particular explicit formulae for the number of representations of binary quadratic forms, and of integers, by ternary forms, implying especially that every integer $\equiv 3 \pmod 8$ can be written as the sum of three squares, which is tantamount to Fermat's claim.[34] Sec. 5 closes (arts. 305–307) by open-ended reflections on the analogy between the multiplicative structure of the prime residue classes modulo an integer and of the classes of quadratic forms.[35]

Sec. 5 sometimes displays, and often hides, a tremendous amount of explicit computations performed by Gauss,[36] of numbers of classes, genera, or representations. To mention just one striking example of such extensive computations, which had an intriguing long term history, Gauss observed that any given "classification," that is, any given pair of numbers, one for the number of genera (which Gauss wrote as a Roman numeral) and one for the number of classes contained in a single genus (Arabic numeral), is realized by at most finitely many negative determinants:

> It seems beyond doubt that the sequences written down do indeed break off, and by analogy the same conclusion may be extended to any other classification. For instance, since in the whole tenth thousand of determinants there is none corresponding to a class number less than 24, it is highly probable that the classifications I.23, I.21 etc.; II.11; II.10 etc.; IV.5; IV.4; IV.3; IV.2 stop already before -9000, or at least that they contain extremely few determinants beyond -10000. However, *rigorous* proofs of these observations appear to be most difficult.[37]

---

34. The entry in Gauss's mathematical diary about this problem is the only one accompanied by Archimedes's exclamation "EYPHKA"; see [Gauss 1796–1814], July 10, 1796.

35. This as well as the composition of orders and genera alluded to above would provide one of the sources for the later development of the abstract concept of group, see [Wussing 1969], I, § 3.3, and [Wussing 2001].

36. Examples relative to the composition of forms are displayed in H.M. Edwards's chap. II.2 below, who argues that such computations play a crucial role in Gauss's conception of a well-founded theory. See also Gauss's addition to art. 306 at the end of the 1801 edition and the tables in [Gauss 1863/1876], pp. 399–509. Gauss discussed how much numerical material on quadratic forms ought to be published *in extenso* in an 1841 letter to H. C. Schumacher, translated in [Smith 1859–1865], §119. Cf. [Maennchen 1930] and [Neumann 1979–1980], p. 26.

37. Our translation of D.A., art. 303: *Nullum dubium esse videtur, quin series adscriptae revera abruptae sint, et per analogiam conclusionem eandem ad quasuis alias classificationes extendere licebit. E.g. quum in tota milliade decima determinantium nullus se obtulerit, cui multitudo classium infra 24 responderit: maxime est verisimile, classificationes I.23, I.21 etc.; II.11; II.10 etc.; IV.5; IV.4; IV.3; IV.2 iam ante* -9000 *desiisse, aut saltem perpaucis determinantibus ultra* -10000 *comprendere. Demonstrationes autem* rigorosae *harum observationum perdifficiles esse videntur.* Indeed, for one of the simplest constellations of numbers of classes and genera (corresponding to "orders of class number one" in imaginary quadratic fields, in Richard Dedekind's terminology of 1877), the proof that the list of determinants found by Gauss (art. 303) is actually complete was given by Kurt Heegner only in 1954 – and at first not accepted – by a method which subsequently would greatly enrich the arithmetic of elliptic curves. A book on Heegner by H. Opolka, S.J. Patterson, and N. Schappacher is in preparation.

1.3. Applications

Explicit calculations had evidently been part and parcel of number theory for Gauss ever since he acquired a copy of [Lambert 1770] at age 15, and launched into counting prime numbers in given intervals in order to guess their asymptotic distribution.[38] In these tables, Johann Heinrich Lambert made the memorable comment:

> What one has to note with respect to all factorization methods proposed so far, is that primes take longest, yet cannot be factored. This is because there is no way of knowing beforehand whether a given number has any divisors or not.[39]

The whole D.A. is illustrated by many non-trivial examples and accompanied by numerical tables. Section 6 (52 pp., 27 arts.) is explicitly dedicated to computational applications. In the earlier part of sec. 6, Gauss discussed explicit methods for partial fraction decomposition, decimal expansion, and quadratic congruences. Its latter part (arts. 329–334) takes up Lambert's problem and proposes two primality tests: one is based on the fact that a number which is a quadratic residue of a given integer M is also a quadratic residue of its divisors and relies on results of sec. 4; the second method uses the number of values of $\sqrt{-D} \bmod M$, for $-D$ a quadratic residue of M, and the results on forms of determinant $-D$ established in sec. 5.

The final Section 7 on cyclotomy (74 pp., 31 arts.) is probably the most famous part of the *Disquisitiones Arithmeticae*, then and now, because it contains the conditions of constructibility of regular polygons with ruler and compass. After a few reminders on circular functions – in particular (art. 337), the fact that trigonometric functions of the angles kP/n, for a fixed integer n and for $k = 0, 1, 2, \ldots n-1$, where $P = 2\pi$ denotes "the circumference of the circle," are roots of equations of degree n – Gauss focused on the prime case and the irreducible[40] equation

$$X = 0, \quad \text{where } X = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 \; ; n > 2 \text{ prime},$$

which his aim is to "decompose *gradually* into an increasing number of factors in such a way that the coefficients of these factors can be determined by equations of as

38. See Gauss's letter to Johann Franz Encke of December 24, 1849 in [Gauss 1863/1876], pp. 444–447. In [Biermann 1977], pp. 7–18, it is established that the page of Gauss's mathematical diary which follows the last entry of July 9, 1814, records the dates when Gauss counted prime numbers in certain intervals. On the influence of Lambert's and Hindenburg's tables on Gauss's sec. 6, see [Bullynck 2006b]. See also [Maennchen 1930], in particular pp. 27–35.

39. [Lambert 1770], pp. 29–30: *Was übrigens bey allen bißher erfundenen Methoden, die Theiler der Zahlen aufzusuchen, zu bemerken ist, besteht darinn, daß man bey Primzahlen am längsten aufsuchen muß, und zuletzt doch nichts findet, weil man nicht voraus weiß, ob eine forgegebene Zahl Theiler hat oder nicht.* Lambert went on to propose Fermat's Little Theorem as a first necessary criterion for primality.

40. D.A., art. 341. The word "irreducible" was established a few decades later. Cf. O. Neumann's chap. II.1 below.

low a degree as possible, until one arrives at simple factors, i.e., at the roots Ω of X."[41] Art. 353 illustrates the procedure for $n = 19$, which requires solving two equations of degree three and one quadratic equation (because $n - 1 = 3 \cdot 3 \cdot 2$); art. 354 does the same for $n = 17$ which leads to four quadratic equations ($n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$).[42]

All roots of $X = 0$ are powers r^i of one of them, but to solve the equation, Gauss replaced the natural sequence of the exponents i, that is $1, 2, \ldots, n-1$, by the more efficient bookkeeping provided by sec. 3:

> But in this [natural] form of the roots there is presented no means of distributing them into cyclical periods, nor even of ascertaining the existence of such periods or of determining their laws. It was the happy substitution of a geometrical series formed by the successive powers of a primitive root of n in place of the arithmetical series of natural numbers, as the indices [i.e., exponents] of r, which enabled [Gauss] to exhibit not merely all the different roots of the equation $\frac{x^n-1}{x-1}$, but which also made manifest the cyclical periods which existed among them. Thus if α was a primitive root of n and $n - 1 = mk$, then in the series $r, r^\alpha, r^{\alpha^2}, \ldots, r^{\alpha^{k-1}}, \ldots, r^{\alpha^{mk-1}}$ the m successive series which are formed by the selection of every k^{th} term, beginning with the first, the second … are periodical.[43]

Complementary results on the auxiliary equations, i.e., those satisfied by the sums over all the roots of unity in a given period, are given in art. 359, applications to the division of the circle in the final arts. 365 and 366. As a byproduct of his resolution of $X = 0$, Gauss also initiated a study of what are today called "Gauss sums," i.e., certain (weighted) sums of roots of unity, like the sum of a period, or of special values of circular functions. For instance, he proved (art. 356) that, for an odd prime n and an integer k not divisible by n,

$$\sum_R \cos \frac{kRP}{n} - \sum_N \cos \frac{kNP}{n} = \pm\sqrt{n} \quad \text{or} \quad 0,$$

according to whether $n \equiv 1$ or $n \equiv 3 \bmod 4$. Here, R varies over the quadratic residues, N over the quadratic non-residues modulo n.[44]

1.4. The Disquisitiones Arithmeticae as a System

In the preface of the D.A., Gauss explicitly restricted the objects of arithmetic to be the rational integers; he wrote:

---

41. Our translation of D.A., art. 342: *Propositum disquisitionum sequentium … eo tendit, ut X in factores continuo plures* GRADATIM *resolvatur, et quidem ita, ut horum coëfficientes per aequationes ordinis quam infimi determinentur, usque dum hoc modo ad factores simplices sive ad radices* Ω *ipsas perveniatur.*

42. For Gauss's early annoucements of these results and details on the case of the 17-gon, see [Reich 2000]. The impact on the theory of equations is discussed in O. Neumann's chap. II.1.

43. [Peacock 1834], p. 316. Gauss described his view in his letter to Christian Gerling of January 6, 1819; see [Gauss & Gerling 1927/1975], p. 188.

44. The sign of $\sqrt{n}$ depends on whether k is or is not a quadratic residue modulo n, but Gauss did not succeed in proving this fact in the D.A. See S.J. Patterson's chap. VIII.2 below.

> The theory of the division of the circle … which is treated in sec. 7 does not belong *by itself* to arithmetic, but its *principles* can only be drawn from higher arithmetic.[45]

In sec. 7 itself, he promised that the "intimate connection" of the topic with higher arithmetic "will be made abundantly clear by the treatment itself."[46] There is of course the technical link mentioned above, that is, the bookkeeping of the roots of unity via sec. 3. But the "intimate connection" that Gauss announced goes further and also concerns the systemic architecture of the treatise.

Despite the impressive theoretical display of sec. 5, one cannot fully grasp the systemic qualities of the D.A. from the torso that Gauss published in 1801. At several places in the D.A. and in his correspondence a forthcoming volume II is referred to. The only solid piece of evidence we have is what remains of Gauss's 1796–1797 manuscript of the treatise. This differs from the structure of the published D.A. in that it contains an (incomplete) 8$^{\text{th}}$ chapter (*caput octavum*), devoted to higher congruences, i.e., polynomials with integer coefficients taken modulo a prime and modulo an irreducible polynomial.[47] Thus, according to Gauss's original plan, sec. 7 would not have been so conspicuously isolated, but would have been naturally integrated into a greater, systemic unity. The division of the circle would have provided a model for the topic of the *caput octavum*, the theory of higher congruences; it would have appeared as part of a theory which, among many other insights, yields two entirely new proofs of the quadratic reciprocity law.[48]

The treatise would thus have come full circle in several respects: beginning with ordinary congruences and ending with higher congruences; encountering various periodic structures along the way: prime residues, periods of reduced quadratic forms of positive discriminant, classes of quadratic forms which are all multiples of one class, cyclotomic periods and their analogues mod p; and proving quadratic reciprocity four separate times in the process.

That scientificity ought to be expressed by way of a system was a widespread idea in Germany in the second half of the XVIII$^{\text{th}}$ century. Lambert, whose works were well represented in Gauss's library, wrote, besides his scientific *œuvre*, several philosophical texts developing this idea, at least two of which Gauss owned personally.[49] German idealist philosophers from Immanuel Kant to Georg Wilhelm Friedrich Hegel, for instance Johann Gottlieb Fichte, Friedrich Wilhelm Joseph von

45. Our translation of D.A., *praefatio: Theoria divisionis circuli …, quae in Sect. VII tractatur,* ipsa *quidem* per se *ad Arithmeticam non pertinet, attamen eius* principia *unice ex Arithmetica Sublimiori petenda sunt.*

46. D.A., art. 335: *tractatio ipsa abunde declarabit, quam intimo nexu hoc argumentum cum arithmetica sublimiori coniunctum sit.*

47. We summarize in this paragraph G. Frei's analysis, in chap. II.4 below, of the *caput octavum* and its importance for the economy of the whole treatise that Gauss originally planned.

48. Gauss published them later independently; see G. Frei's chap. II. 4 below.

49. Maarten Bullynck has drawn our attention to [Lambert 1764] and [Lambert 1771]; see [Bullynck 2006b], p. 278. Unfortunately, the dates of acquisition for these items are not known.

Schelling, Karl Leonhard Reinhold, and Jakob Friedrich Fries, cultivated various systemic programmes. Starting with Fichte, a system with a circular instead of linear architecture – returning to its initial point which thereby receives its higher justification – is called upon to provide a self-justifying foundation for the unfolding of self-consciousness. With Hegel this would become the unfolding of reason; in his first philosophical publication, which appeared in the same year as Gauss's D.A., Hegel wrote that "the method of the system, which may be called neither analytical nor synthetical, is realized most purely if it appears as the development of reason itself."[50]

The systemic design of Gauss's original plan for his arithmetic fits those ambient ideas remarkably well.[51] It makes it possible, for instance, to appreciate the four proofs of the quadratic reciprocity law originally planned for the treatise in a dual way: deducing a theorem at a certain place of the systemic development endows it with a specific theoretical meaning;[52] on the other hand, the various proofs of the same result connect these theoretical frameworks into a system which is not simply a deduction of increasingly complicated theorems from initial axioms. In Gauss's words,

> It is the insight into the marvellous interlinking of the truths of higher arithmetic which constitutes the greatest appeal of these investigations.[53]

Another systemic cyclicity is created precisely by the already mentioned recurrence of periodic structures throughout the treatise. Gauss himself insisted on the analogy between what we call cyclic components of class groups and the multiplicative structure of residues modulo a prime number:

> The proof of the preceding theorem will be found to be completely analogous to the proofs of arts. 45, 49, and the theory of the multiplication of classes actually has a very great affinity in every respect with the argument of sec. 3.[54]

---

50. [Hegel 1801], p. 35: *Am reinsten gibt sich die weder synthetisch noch analytisch zu nennende Methode des Systems, wenn sie als eine Entwicklung der Vernunft selbst erscheint.* For a general orientation about the philosophical ideas alluded to in this paragraph, see [Ritter, Gründer 1998], art. "System," pp. 835–843.

51. In spite of Gauss's philosophical interests – e.g., he is said to have read Kant's *Critique of Pure Reason* several times; see [Dunnington 1955], p. 315; cf. J. Ferreirós's chap. III.2 and J. Boniface's chap. V.1 below – we have no evidence of a direct and conscious inspiration; later mentions of Hegel by Gauss are rather critical; see for instance [Gauss & Schumacher 1862], vol. 4, n° 944, p. 337. A reference to Gauss's idea of science as a system in the not very reliable biographical essay [Waltershausen 1856], p. 97, suggests only a banal deductive structure.

52. From the philosophical point of view, cf. [Hartmann 1972], p. 106: "The point easily lost sight of is that the [systemic] methodological structure provides a new meaning to categories that already have a meaning."

53. Our translation of [Gauss 1817], p. 160: *Dann ist gerade die Einsicht in die wunderbare Verkettung der Wahrheiten der höhern Arithmetik dasjenige, das einen Hauptreiz dieses Studiums ausmacht, und nicht selten wiederum zur Entdeckung neuer Wahrheiten führt.*

54. Our translation of D.A., art. 306: *Demonstratio theor. praec. omnino analoga invenietur*

Gauss thus drew the attention of the reader to the fact that sec. 3 was not only instrumental for decomposing the cyclotomic equation in sec. 7 but also linked the theory of forms to the rest. He also significantly called "irregular" a determinant whose principal genus was not cyclic, i.e., not constituted by the multiples of a single class of forms.

Half a century later, the mathematician Ernst Eduard Kummer reflected upon a suitable system for "the more recent mathematics," and concluded that it should not be linear but

> rather like the system of the universe; its goal would be to give not just the deduction of the mathematical truths, but an insight into all the essential relations among them.[55]

As mentioned above, the subject of the *Disquisitiones Arithmeticae* was natural numbers and Gauss's proofs were anchored in intricate computations, both formal (as in the sec. 5) and numerical, ultimately based on integers. The tension between this anchorage of the book and the striving towards a wider theoretical scope, as illustrated in the last section of the D.A., will be a recurring theme in what follows. It explains why the question of the reception of the book is tightly linked to the shaping of number theory as a specific discipline.

2. The Early Years of the *Disquisitiones Arithmeticae*

Gauss's own impressions of the early reception of the *Disquisitiones Arithmeticae* are scattered in his correspondence. A letter of June 16, 1805, to Antoine-Charles Marcel Poullet-Delisle, his French translator,[56] summarizes them well:

> It is for me as sweet as it is flattering that the investigations contained in my Work, to which I devoted the best part of my youth, and which were the source of my sweetest pleasures, have acquired so many friends in France; a fate quite different from what

---

demonstrationibus in arts. 45, 49, reveraque theoria multiplicationis classium cum argumento in Sect. III tractato permagnam undique affinitatem habet. Cf. the note on D.A., art. 306.IX: "Démonstration de quelques théorèmes concernant les périodes des classes des formes binaires du second degré," [Gauss 1863/1876], pp. 266–268, where Gauss used, of course informally, the word "group" (*groupe*) referring to all classes of forms of given determinant.

55. [Kummer 1975], vol. 2, p. 697: *die neuere Mathematik … wird sich erst später ihr eigenthümliches System schaffen, und zwar wol nicht mehr nur ein in einer Linie fortlaufendes, dessen Vollkommenheit allein darin liegt, dass das Folgende überall durch das Vorhergehende begründet werde, sondern ein dem Weltsysteme ähnlicheres, dessen Aufgabe es sein wird, über die blosse Begründung der mathematischen Wahrheiten hinausgehend, eine allseitige Erkenntnis der wesentlichen Beziehungen derselben zueinander zu geben.* In [Kummer 1975], vol. 2, p. 687, the parallel is made explicit between Hegel's principle of the systemic "self-interpretation of content" (*Sichselbstauslegen des Inhalts*) and the system required for the new mathematics since Gauss.

56. On his life, see [Boncompagni 1882].

> they found in Germany where a taste for the most difficult parts of pure mathematics is the property of a very small number of persons.[57]

The *Disquisitiones Arithmeticae* had in fact been mentioned at the French Academy at least as early as January 1802:

> Citizen Legendre communicates a geometrical discovery, made in Germany by M. Charles Frédéric Bruce [sic], from Brunswick, and published by him in his work entitled *Disquisitiones arithmeticae*, Leipsik, 1801,[58]

and was commented upon very positively from all quarters.[59] The project of a French translation was supported by arguably the most prominent mathematician of the time, Pierre-Siméon Laplace, and on May 31, 1804, Joseph-Louis Lagrange wrote to Gauss:

> Your *Disquisitiones* have put you at once among the first mathematicians, and I consider the last section as one which contains the most beautiful analytic discovery made in a long time. Your work on planets will moreover have the merit of the importance of its topic.[60]

The beginning of this praise is often quoted, but taken in its entirety, the citation provides important clues about the early reception of the D.A. First, attention focused on the last section, the resolution of $x^n - 1 = 0$ through auxiliary equations and its consequences for the constructibility of regular polygons; this is the part of the book which borders both on the general theory of equations and on geometry. Second, Gauss's innovation was described as "analytical." Finally, number theory (and more generally pure mathematics) was considered a subsidiary subject compared to astronomy or mathematical physics.

---

57. Letter published by Ernest Fauque de Jonquières in 1896, *Comptes rendus de l'Académie des sciences* 122, p. 829: *Il m'est aussi doux que flatteur que les recherches contenues dans mon Ouvrage, auxquelles j'avais dévoué la plus belle partie de ma jeunesse, et qui ont été la source de mes plus douces jouissances, aient acquis tant d'amis en France; sort bien inégal à celui qu'elles ont trouvé en Allemagne où le goût pour les parties plus difficiles des mathématiques pures n'est la propriété que d'un fort petit nombre de personnes.* In the letter, Gauss also expressed his hopes to publish the sequel of the D.A., a project he described as delayed for lack of time and printer.

58. *Procès verbaux de l'Académie des sciences*, registre 114, vol. II, séance du 6 pluviôse an 10 (26 janvier 1802), p. 457: *Le Citoyen Legendre communique une découverte géométrique, faite en Allemagne par M. Charles Frédéric Bruce, de Brunswick, et publiée par lui dans son ouvrage intitulé* Disquisitiones arithmeticae*, Leipsik, 1801.*

59. Gauss's fame in France was decisive for his connection to Alexander von Humboldt (then in Paris), and for establishing on the German scene, through Humboldt, a place for himself and, afterwards, for other number theorists; see H. Pieper's chap. III.1 in this volume.

60. [Lagrange 1867–1892], vol. 14, p. 299: *Vos Disquisitiones vous ont mis tout de suite au rang des premiers géomètres et je regarde la dernière section commme contenant la plus belle découverte analytique qui ait été faite depuis longtemps. Votre travail sur les planètes aura de plus le mérite de l'importance de son objet.* "Geometer" (*géomètre*) remains a standard terminology for "mathematician" in French during the XIX$^{\text{th}}$ century.

This challenges the disciplinary position of the *Disquisitiones Arithmeticae* both in its mathematical and cultural aspects. Two situations typified the first generation of its readers:[61] either their involvement with the book, even if significant and fruitful, occupied only a small part within all their mathematical activities, or they themselves occupied a marginal position in the mathematical community. Augustin-Louis Cauchy is a good example of the first category, and Sophie Germain of the second.[62] And Gauss himself, after all, turned to astronomy and geodesy to secure a position.

This does not mean, however, that the reading of the D.A. at the time was restricted to one section, nor that it remained superficial and did not lead at all to innovative work. Sophie Germain displayed in her papers a thorough knowledge of all the sections: those on congruences of course which she used freely in her work on Fermat's Last Theorem as well as in her new proof of the quadratic residue behaviour of the prime 2, but also the difficult sec. 5, and specifically the composition of forms and the theory of ternary forms.[63] In his memoir on symmetric functions, presented to the *Institut* on November 30, 1812, Cauchy relied on concepts and a notation which he borrowed directly from the D.A., such as the idea of an adjoint and the notion of determinant, to prove that if a function of n quantities takes less than p distinct values, where p is the greatest prime divisor of n, then it can take at most 2 values, and furthermore to develop his theory of combinations and of determinants, seen with hindsight as key steps towards the development of group theory.[64]

However, as Lagrange's quote suggested, the D.A. was first of all taken up for its treatment of $x^n - 1$ and therefore mostly in treatises on algebra. For instance, Sylvestre François Lacroix included in the third edition of his *Complément des Élemens d'algèbre* (1804) a discussion of Gauss's results in the section on binomial equations.[65] Lagrange's second edition of his *Traité de la résolution des équations*

61. Different aspects of this early reception have been documented in [Neumann 1979–1980], [Reich 1996], [Reich 2000], [Goldstein 2003], and [Neumann 2005].

62. On the shifting professional status of number theory and number theorists, and the characteristics of the craft at different moments, see [Goldstein 1989].

63. See for instance Bibliothèque Nationale de France, Manuscripts f.fr 9118, pp. 40–41, 86; f.fr. 9114, pp. 92–94. On Germain's work, see [Edwards 1977], pp. 61–65, and [Laubenbacher, Pengelley 1998].

64. See [Cauchy 1815], where Cauchy – perhaps significantly – refers to Gauss's "Recherches analytiques" [sic]; cf. [Belhoste 1991], pp. 32–35. Between 1813 and 1815, Cauchy also published, in [Cauchy 1813–1815], his proof of Fermat's general claim to the effect that each natural number is the sum of no more than n n-gonal numbers. Gauss had shown in passing how to reduce the case $n = 4$ (already proved by Lagrange) to his theorem for $n = 3$; see end of D.A., art. 293. Cauchy then managed to reduce the cases $n \geq 5$ to those proven by Gauss; the most original elements of this proof, however, seem quite independent of the D.A.

65. [Lacroix 1804], p. 92: *M. Gauss, dans un ouvrage très-remarquable, intitulé Disquisitiones Arithmeticae, a fait voir que* toute équation à deux termes, dont l'exposant est un nombre premier, peut être décomposée rationnellement en d'autres équations dont les degrés sont marqués par les facteurs premiers du nombre qui précède d'une unité ce