C.F. Gauss's Re-Writing of Section II De congruentiis primi gradus

Materials on the Genesis of the Disquisitiones Arithmeticae, Part III

Maarten Bullynck

Mathematical texts have the inclination to obscure the preparatory steps and stages of proofs and theories. In this respect, C.F. Gauss is renowned for removing traces of his earlier hard work. However, through a comparison of Gauss's *Disquisitiones Arithmeticae* (DA) with a draft of the DA, some aspects of this writing and re-writing process can be recovered. Especially an analysis of Section II reveals a re-grouping of results and procedures that ultimately changed the general aspect of the DA, making it one of the first truly "modern" mathematical works.

Contents

1 Introduction

Relatively little is known on the genesis of Carl Friedrich Gauss's number-theoretic opus magnum, the *Disquisitiones Arithmeticae* (DA) Gauss 1801a, now published more than 200 years ago in 1801. In the vein of his dictum "pauca, sed matura", Gauss was very reticent about incomplete results and even heuristic methods that preceded and prepared the 1801 publication. There are references throughout the DA to other authors (mainly Euler, Lagrange and Legendre); there are succinct remarks in the DA on the genesis of its text, but all these taken together, neither the subsequent structuring and polishing of the DA, nor Gauss's *ars inveniendi*[1] could be reconstructed.

After Gauss's death in 1855, the edition of his collected works brought together both texts from the *Nachlass*, letters and Gauss's scientific journal. Based on this material Bachmann, Schlesinger, Maennchen and others wrote the essays that ultimately should have led to a scientific biography of Gauss under the direction of Felix Klein, and were published as supplements in volumes X and XI of Gauss's *Gesammelte Werke* Gauss 1863-1929. These essays could reconstruct part of the chronology of Gauss's important results (using the letters and the retrieved scientific journal) and also revealed the importance of the large number tables Gauss compiled and which led him to the discovery of many relationships between numbers.

The present article uses yet another source to shed some light into the genesis of Gauss's *Disquisitiones*: A manuscript consisting of 7 chapters that may be considered a first draft of the *Disquisitiones*, the *Analysis Residuorum* (Gauss 1797 = AR)[2] Chapters 1, 3, 4 and 7 of this manuscript are near identical with Sections I, III, IV and VI of the DA, whereas chapters 6 and 8 were omitted in the DA, excepting a small part of Chapter 6 that was integrated in Section VII. This change of plan was most certainly motivated by Gauss's more intensive lecture of Euler, Lagrange and Legendre as well as by his own progressions during the period 1797-99. Thus, in the writing process itself, the AR turned into the DA, from a book with an emphasis on the theory of congruences to a book including a very substantial part on quadratic forms.

As we will argue, this re-focussing of the original set-up is mirrored in the re-writing of AR's chapter 2 into DA's Section II. A detailed comparison of the manuscript with the printed version reveals several expansions and additions to the already written articles.[3] As the analysis will show these changes mainly fall into two categories: 1) a refinement of the exposition's form both on the level of "didactics" and content; 2) a re-arrangement of theorems, moving certain basic but crucial results from backmatter to frontmatter.

---

[1] The term is due to Leibniz, and is e.g. used in Neumann 1979-1980, 24.

[2] The parts of this manuscript are disseminated over three libraries: Berlin-Brandenburgische Akademie der Wissenschaften, Staatsbibliothek zu Berlin and Niedersächsische Staats- und Universitätsbibliothek Göttingen. The first two parts of the manuscript were discovered 1981 by Uta Merzbach in the "Nachlass" of J.P.G. Lejeune-Dirichlet. In Merzbach 1981, she showed that these two parts match up with an already known manuscript in the Göttingen Universitätsbibliothek. The manuscript was most probably written down in Summer/Autumn 1797, during Gauss's first years at Göttingen university (Merzbach 1981, 173). The title Gauss had given to this manuscript was *Doctrina de residuis numerorum*, but because the manuscript in Göttingen was known as *De Analysis Residuorum* (= AR) and indicated as such in the edition of Gauss's *Werke*, it seems most convenient to stick to this title. The parts discovered in Dirichlet's *Nachlass* contain 4 chapters that correspond to the first 4 sections of the DA, the manuscript breaking off within Gauss's first proof of quadratic reciprocity. The part that was conserved in Göttingen contains three more chapters: a treatment of the cyclotomic congruence and equation ($x^m - 1 \equiv 0$ and $x^m - 1 = 0$) (Chapter 6), applications (Chapter 7) and a general theory of congruences, introducing prime functions and two more proofs of the law of quadratic reciprocity (Chapter 8). Chapter 7 was quite literally taken over as Section VI, the second part of Chapter 6 as Section VII in the DA, cfr. Dedekind's remarks in Gauss 1863-1929, II, 240. Chapter 8 corresponds to a section VIII Gauss refers to in the DA, but that was never published during his lifetimes. They were posthumously included in the *Werke* (Gauss 1863-1929, II, 199–242, edited by Dedekind).

Lacking in the extant manuscript are quadratic forms, corresponding to Section V of the DA. Gauss learnt about quadratic forms by reading Euler, Lagrange and Legendre, i.e., from 1796 onwards, when he could borrow their works from the Göttingen university library, cfr.Bachmann 1911, 16; Schlesinger 1912, 17. Consequently, the first part of Section V may however have been partly treated in the AR manuscript, but DA's articles 234-305 on the composition of quadratic forms were certainly written from Autumn 1798 onwards only (cfr. DA 234 + handwritten note Gauss 1863-1929, I, 476.).

[3] U. Merzbach merely notices the absence of article 42, which Gauss only proved August 1797, as well as some differences in style (Merzbach 1981, 171-3), and eventually considers AR chapter 2 near identical to DA Section II. Actually, six articles (35, 36, 37, 40, 41 and 42) of the DA are lacking in the AR.

2 The general build-up of Section II

Before moving to the analysis, it is important to consider the role of this second part on linear congruences within the AR and DA. Its build-up was a very deliberate one: If one compares the AR with the DA, the ordering of the items and the motivation Gauss gives for its order remain unaltered. In modern terms, one could name this chapter "Basic notions and lemmata“ providing the essential background for further reading. It should be remembered that in his introduction Carl Friedrich Gauss stresses that his *Disquisitiones Arithmeticae* are not solely concerned with Diophantine problems, but is the science of the natural numbers. This science consists of two parts: Elementary arithmetic and higher arithmetic that Euclid founded in Book VII of his *Elements* (DA, VII-VIII). This set-up is different from his precessors and contemporaries, from Lagrange, Euler and Legendre, who were mostly but interested in the Diophantine number problems. With the exception of Euler's posthumously published *Tractatus de numerorum doctrina* (Euler 1862b, cfr. Weil 1984, 193-5) Gauss's work is the first attempt to compile all results related to integral numbers in one theory, the theory of numbers.

The need to construct such a coherent theory of numbers, covering both elementary and enhanced topics, had been signalled by Lambert. In the introduction to his *Zusätze zu den logarithmischen und trigonometrischen Tabellen* (1770) J.H. Lambert regrets the dispersed procedures and results that treat of prime numbers, factorisation and the like, and marks out the need for a more general framework:

> Ich habe mich [...] um die Theorie der Primzahlen näher umgesehen, und da fand ich freylich nur einzelne abgebrochne Stücke, ohne sonderlichen Anschein, daß dieselbe so bald sollten zusammengehängt und zum förmlichen System gemacht werden können. Euclid hat wenig, Fermat einzelne meist unbewiesene Sätze, Euler einzelne Fragmente, die ohnehin von den ersten Anfängen weiter entfernet sind und zwischen sich und den Anfängen Lücken lassen. (Lambert 1770, 20, part of this statement is also quoted in Kästner 1758/1791-4, I, 2, 552)

Many of these topics were treated under the name *Anatomia numerorum*, a concept that seems to stem from Poethius in 1728 (Kästner 1758/1791-4, I, 2, 556) and occurs in essays by Euler and Lambert himself (Lambert 1769).

The only example of a systematic and fully proof-based part of number theory being Euclid's Book VII, Gauss thus had to reiterate and supplement these results in the modern language of algebra to start off his *Disquisitiones.* The need for exact and algebraic proof - even for Euclid's propositions - is characteristic for the turn of the century, and more especially in the German states. Due to the importance of logic and proof in the Leibniz-Wolffian philosophy (cfr. Peckhaus 1997), German mathematicians as Lambert in his *Neues Organon*, Kästner in his *Anfangsgründen* and Hindenburg devoted serious attention to the epistemological status and the various constructions and possibilities of proof. In particular, the algebraic translation of Euclidean proofs were dicussed, because they were considered as an important cutting edge between antique rigour and modern analytical methods (cfr. Bullynck 2005a).

In Section II, articles 13-20 of the DA (17-20 of the AR) provide quite exactly this translation: They formulate and prove algebraically the basic theorems on primes, and end with the unique prime factorisation (cfr. Göcksel and Örkan 2001). The comment in article 14, proving that if p does not divide a and b, then it does not divide ab either, is noteworthy. Although this theorem has been known since Euclid, "we did not want to omit it, because not a few of recent [works] have sold a vague procedure for proof (DA 14).[4] For Gauss, vague arguments should not be sold for proof.[5] Turning from these results to "the to our aims more nearly related“ ones, the articles 21

---

[4] In the Latin original: "nos tamen ommittere eam noluimus, tum quod recentiorum complures seu ratiocina vage pro demonstratione vendativerunt“ (DA 14).

[5] In the AR, the statement is less sharp: "in libris nostris arithmeticis etiam optimis plerumque desideratur“ (AR 18), "even in our best arithmetical books there is much left to be desired“.

and 22 just repeat the proven theorems in the language of congruences - using the "appropriate notation" of Section I, ≡ (mod.), that "marks an epoch in the development of the science of arithmetic"(Matthews 1892, quoted after Cajori 1928/29, II, 34).
After this warming-up, Gauss proceeds to the treatment of linear congruences, first the single case (DA 23-31), then systems of congruences (DA 32-37), closing his Section II with a staccato of at first sight nearly unrelated, though important results that can be regarded as lemmata. These include theorems on the Euler-function (DA 38-39), some more lemmata (DA 40-41) and the fundamental theorem for the number of solutions of a congruence (DA 42-3) - that Euler still lacked in his attempt at a systematic exposition, and Lagrange proved in 1770 (Weil 1984, 193–6) - ending with a historical note (44). The AR contains the same parts, but both the treatment of single and systems of linear congruences get expanded (growing from 23-33 to 23-37), and the lemmata 40-42 are added only in the final version. We will consider these two groups of changes separately, because they show the two different aspects of the re-writing process.

3 The Re-Writing of Section II: Part I

The first group of changes connects with the general and very obvious difference between the AR and the DA on the level of presentation: A tightening of the exposition, visible in the numerical examples, the notations and proofs, and stylistic improvements of the Latin text (Merzbach 1981, 171 and 174). Whereas the AR advanced the algorithms for the solution of congruences through worked-out numerical examples, a didactical method quite common in the 18th Century, the DA reduces these to compact examples, giving only the outcomes of some mediary steps.[6] Instead of this, an algebraic and more abstract formulation of the algorithm can be found in the DA (cfr. 3.1, 5). These re-writings are especially remarkable in the treatment of solution methods for first degree congruences. Instead of a numerical example, mediating the algorithm, a formalistic framework, a "calculi algorithmus" is introduced by Gauss to simplify the treatment of congruence forms and reduce the calculations for articles 27, 31 (linear congruences) and 33 (systems of linear congruences).

3.1 Calculi for special cases - linear congruences (art. 23-31)

For the solution of simple congruences, both with prime and composite modulos, the comparison of the AR with the DA shows interesting shifts. Let us consider the prime case first: The AR gives us a general discussion of the conversion of a congruence $ax \equiv \pm 1$ (mod. f) into an indeterminate equation $ax = fy \pm 1$, then proceeds with a numerical example $83x = 16y \pm 1$, because "it suffices for those who do not know the method to add an example" (AR 26). Its treatment in the DA starts off with the same general statements (very close to the wordings in the AR), but then proceeds to a transcription of the "algorithm of calculation", using the squared brackets notation:

> If the quantities A, B, C, D, E etc. depend from α, β, γ, δ etc. in the following way: $A = \alpha$, $B = \beta A + 1$, $C = \gamma B + A$, $D = \delta C + B$, $E = \epsilon D + C$ etc., we will designate it for the sake of brevity as follows, $A = [\alpha]$; $B = [\alpha, \beta]$; $C = [\alpha, \beta, \gamma]$, $D = [\alpha, \beta, \gamma, \delta]$ etc. (DA 27)

As Gauss notes, this algorithm may be derived from Euler's and Lagrange's methods, but it avoids the cumbersome notation of continued fractions, and uses the squared brackets notation instead,

---

[6] This partially answers a question that was raised during the conference "years *Disquisitiones Arithmeticae*", viz., on "the role of numerical examples" in the DA (Conference Report 2001, 1). Gauss's compression of examples, apart from the pressure of printing costs, can certainly be linked to the symbolic trend in German mathematics, as sketched in Bullynck 2005a, cfr. also Jahnke 1990, 161-232. As to the influence "on later authors" (Conference Report 2001, 1), the intermediate form Gauss developed for his DA does not seem to have been pursued further: In two of the major treatises on number theory after Gauss, Tschebyscheff 1845/1889 returns to long, didactal examples, whereas Lejeune-Dirichlet 1863/1894 almost lacks any numerical examples.

which is a "relation [that] can be considered more generally, as we do on another occasion" (DA 27 & 28). Only in DA's article 202, as a kind of afterthought or correction, Gauss remarks in a footnote, that the same notation (together with some rules for calculation) had already been used by Euler, but "[w]e neglected to note it at that time." (DA 202)[7]

Indeed, compared with the method of substitution which was still used in the AR's example, this notation has the advantage of being compact and reducing combinations of sums to a set of expressions that can be manipulated according to certain formulae. Those formulae are given in footnotes (DA 27, note; DA 177, note), Euler even mentions a few more (cfr. Euler 1765/7, 92). A brief survey of Section V makes clear that the algorithms Gauss indicates for converting quadratic forms (a, b, c) into other forms rests mainly upon this same algorithm (cfr. DA 177, 188). They are, however, not described using the square bracket notation, this notation only appears in the "added" commentaries to the algorithm, either in a footnote (DA 177) or in a discussion (DA 189) together with the remark that "[b]y means of these formulae [...] the calculation involved can be done very quickly." (DA 189)[8]

This kind of optimisation of algorithms through the introduction of an appropriate notation or symbolism reappears in the solution of a single congruence with a composite modulo. The AR again gives the general treatment and then a numerical example (AR 30-31), in the DA the form $ax \equiv b$ mod. mn is reworked into $x \equiv v$ mod. $\frac{m}{\delta}$, with δ the least common divisor of m and n.

> In the same way that the root of the equation $ax = b$ can be expressed as $\frac{b}{a}$, we will designate by $\frac{b}{a}$ a root of the congruence $ax \equiv b$ and join to it the modulus of the congruence to distinguish it. Thus, e.g., $\frac{19}{17}$ (mod. 12) denotes any number that is $\equiv 11$ (mod. 12). (DA 31)

Associated with this notation an algorithm is given, making calculation with roots of linear congruences "very like that for common fractions".

Curiously enough, this same fractional notation already appears in the third chapter of the AR discussing the use of indices to calculate roots of higher congruences: "Index quotientis $\frac{a}{b}$ (significatione generaliori §) congruus est secundum $(t-1)$ differentiae indicum numeratoris et denominatoris." (AR 55)[9] Indeed, the DA give the same formula, Ind.$\frac{a}{b}$ = Ind. a - Ind. b, with reference to article 31 (DA 59), the reference in the AR, however, is an empty §. The re-writing of article 31 is thus but a consequent addition making the DA more coherent, adding in the mean time a simple notation to facilitate both comprehension and calculation.

3.2 Calculi for special cases - systems of congruences (art. 32-35)

The problem to find a solution satisfying multiple congruences is an important one, since it will "prove to be very useful in what follows" (DA 32, cfr. AR 33). The solution for this problem (nowadays mostly called the Chinese Remainder Problem, hereafter CRT) is a successive application and combination of the solution method for single congruences. Again, the AR proceeds with general discussion (AR 32) followed by a numerical, worked-out example (AR 33). In saying that another congruence can be added to the system, not the word 'congruence' is used, but the word 'condition' (AR 32), a word that was also used by Euler and Kästner in this context. Indeed does the addition of a third, fourth, etc. congruence condition the space of solutions of the first and second congruence.

This analogy is pursued further in the DA, where the discussion of the CRT rather drastically expands from two articles to four. Instead of a successive combination of solutions, the treatment

---

[7] The reference is to Euler 1765/7. Cfr. also Bullynck 2005b.

[8] For the same reason Gosper advocated the use of continued fraction on computers in Beeler et al. 1972 (39-44), cfr. also the theory and comments on continued fractions (356-359), as well as formulae to manipulate continued fractions (Exercises 5-10 and 15 on pages 374-5) in Knuth 1969.

[9] Translation: "The index of the quotient $\frac{a}{b}$ (in the generalised sense of paragraph) is congruent to the difference of the indices of the numerator and denominator modulo $(t-1)$."

is consequently built around the concept of 'condition'. These can "combined into one" (DA 32), or "resolved in many conditions" (DA 33) if the modulo can be factorised. As Gauss remarks:

> This observation opens to us not only a method of discovering the impossibility when it exists, but also a more satisfactory way of calculating. (DA 33)

Resolving A into its factors A', A'', etc. , a congruence $x \equiv a$ (mod. A) can be substituted by $x \equiv a$ (mod. A'), $x \equiv a$ (mod. A''), etc. Impossibility of solution is thus quickly observed, if two conditions exist, $x \equiv a$ resp. b (mod. $A' = B'$), with a not $\equiv b$ (mod. $A' = B'$). If a is congruent to b, however, one of both conditions can be "rejected'. Gauss calls the first case the detection of "inconsistent" conditions, the second, of "superfluous" conditions (DA 34). It is this second case that enhances calculation: "it is not a matter of indifference, so far as brevity of calculation is concerned, which superfluous conditions are rejected." (DA 35)

Considering the re-writing of these 3 problems (single congruences with both prime and composite modulo, systems of congruences), an intermediary conclusion can be proposed.[10] In all 3 cases a new formalism or a new concept is presented that makes the treatment of the problem more concise and the form of the problem more manipulable. Although Gauss is renowned for his saying that the truth of theorems should come "ex notionibus", not "ex notationibus" (DA 76), it seems that he did not hesitate to introduce new notations if this made both exposition and calculation more transparent. More particularly, through the introduction of the squared brackets, the fractions and the 'conditions', the "calculi algorithmus" becomes a rather formal device. It is formal in precisely this way: The algorithm consists of 1) a set of rules to combine, to calculate formal expressions; 2) an interpretation of those formal expression into the numeric solution. Hence, in a first stage, the algorithm avoids numerical (and possibly involved) calculations, only in a second stage, a reduced form of the problem has to be numerically evaluated.

Together with the rather frustrating remark that "it is not our intention to treat of these details or of other practical artifices that can be learned more easily by usage than by precept" (e.g. DA 35), the demand for brevity of calculation is one of two mantras that occur throughout the whole of the *Disquisitiones*. The introduction of the formal algorithms in the subsequent re-writing of the AR is thus a consequent choice, or even an imperative for the style and presentation Gauss had in mind (cfr. letter to Zimmermann, 5).

3.3 The special case: Article 36's Calendar Problem[11]

Although connected with the three preceding cases, the DA's "new" article 36 stands a bit apart and deserves special attention. It introduces a practical method for combined congruences if one has to solve "many of these problems ... for which the modulos A, B, C retain their values" (DA 36). In this special case, the algorithm can be simplified to a formula. If given 3 congruences:

$$\begin{aligned} X &\equiv a \pmod A \\ X &\equiv b \pmod B \\ X &\equiv c \pmod C \end{aligned}$$

then solve these three for $a = 1, b = 0, c = 0$; then for $a = 0, b = 1, c = 0$ and for $a = 0, b = 0, c = 1$; let the 3 solutions be α, β, γ, then the formula to calculate all solutions for a certain triple (a, b, c) is: $X = \alpha a + \beta b + \gamma c$. Compared with an explicit calculation through the CRT, this is indeed a practical shortcut for this class of problems.[12]

---

[10] How Gauss's treatment these problems relate to a tradition of presenting remainder problems is analysed in Bullynck 2005b. The present article focuses mainly on aspects of the writing-process that fall within Gauss's own evolution.

[11] A more detailed historical analysis of article 36 in Bullynck 2006.

[12] Indeed, a variant of this method is given as an optimal algorithm for conversion of modular number presentations into decimal presentation in Knuth 1969 (284-292, algorithm 291), although Knuth gives no reference to Gauss at all.

And then follows an example, the only instance of a concrete problem out of "elementary mathematics" in the whole text of the DA, the calculation of year's number in a Julian period:

> This usage arises in the problem of chronology when we seek to determine what Julian year it is whose indiction, golden number, and solar cycle are given. Here $A = 15$, $B = 19$, $C = 28$; ... and the number we seek will be the least residue of the number $6916a + 4200b + 4845c$, where a is the indiction, b the golden number, c the solar cycle. (DA 36)

The use of the variables indiction, sun cycle and golden number for solving this calender problem goes back to Clavius (cfr. Lichtenberg 1997, 441) and their tabulation has a long standing tradition of being included in handbooks of chronology (cfr. Grotefend 1905, overview 4-8, tables 95-104). Finding the year starting from these variables was thus mostly done by looking up the respective numbers in tables.

The simple formula Gauss deduces in DA's article 36 (with the constant numbers 6916, 4200 and 4845) is, however, not new. It was quite intensively studied and debated in the period 1750-1800 among German mathematicians. J. Bernouilli was the first to indicate these constant numbers (6916, 4200 and 4845), an analytical justification was given by Kästner in his *Mathematische Anfangsgründe*(Kästner 1758/1791-4, II, 437-441, cfr. Hindenburg 1786, 302). Apart from Kästner's long and rather explicative proof, C.F. Hindenburg in 1786 also provided a deduction of the formula (along with a general treatment of CRT problems) in his article "Verbindungsgesetz cyklischer Perioden; Natur und Eigenschaften derselben; Ihr Gebrauch in der diophantischen oder unbestimmten Analytik" (Ibid. 301-302) in the *Leipziger Magazin für reine und angewandte Mathematik*.

It is known that Gauss possessed a copy of Kästner's work when he started studying in Göttingen (cfr. Reich 2005, 46; Gauss-Bibliothek 2005), but he may have been even familiar with the problem in Braunschweig. Both Drude, Gauss's professor at the Collegium Carolinum, and Zimmermann, Gauss's protector in Braunschweig, were subscribers to the *Leipziger Magazin*, first series (cfr. subscription list in Subskribentenliste 1781), moreover, Gauss also borrowed the *Magazin* at the Göttingen University Library in December 1795 (Dunnington 1955, 398). [13] All in all, article 36 is one of the very rare instances in the DA where Gauss's early mathematical education in the German tradition surfaces, though not explicitly mentioned.

Of course, the addition of this calendar problem to the *Disquisitiones* in between 1796-7 (the AR) and 1801 (publication of the DA) seems also to be quite naturally be linked to to end of 1799, beginning of 1800, when Gauss published his Easter formula. The first occupation with this problem seems to stem from 1799 (cfr. the first calculation in Gauss 1863-1929, XI, 206-7), its publication in *Zach's monatliche Correspondenz* in August 1800 (Gauss 1863-1929, VI, 73-79), *Braunschweigisches Magazin* in 1806 (Ibid., 80-86) and a correction in 1816 (Gauss 1863-1929, XI, 201-2) indicate the lasting interest Gauss took in the calendar problem. Although the first calculation from 1799 uses double modulo's to calculate sun cycle, indiction and golden number, these are absent from the 1800-publication. Because the reasons for the formulae "lie in higher arithmetics" and Gauss has not yet "not published on the topic", he cannot use its formalism for a "simple" deduction (Gauss 1863-1929, VI, 75).

The example in the DA is thus the correlate of the 1800-article: The latter gives formulae to calculate the 3 variables (sun cycle, indiction, golden number) explicitly, instead of looking them up in tables; the DA-example on the contrary analytically proves a simple formula with three constant numbers to calculate the year in a Julian period, assuming that these 3 variables are known. As

---

[13] For the respective importances of Drude, Zimmermann and Kästner for the young Gauss, cfr. Hänselmann 1878, 33 & 24-6 & Poser 1987, 20-27, Gauss's letters to Zimmermann, regarding Kästner. A study into the importance of C.F. Hindenburg for the young Gauss still is a desideratum. We restrict ourselves for the moment to noting that Hindenburg's journals together with the works of the Newtonian school, present in the library of the Collegium Carolinum, were the first "professional" works of mathematics - apart from *Rechenbücher* - Gauss could get hold of.

well as the previously discussed articles, article 36 is notable for its algorithmic optimisation, but more than that alone, it also offers a glimpse into the diverse traditions Gauss absorbed, into one of the more remote layers, his school education (for more details, Bullynck 2006, Bullynck 2005a).[14]

4 The Re-Writing of Section II: Part II

As mentioned in the introduction, DA's Section II ends with 3 lemmata not present in the AR. Although lemmata 40 and 41 are not very remarkable or new results from the mathematical point of view, it will be argued that their inclusion helps to structure the following sections of the DA. They are mainly used to abbreviate the longer proofs of later sections. Lemma 42 is a different case altogether, as U. Merzbach already remarked (cfr. 1), Gauss having it only proven late 1797 and thus forbidding inclusion in the early part of the AR. The theorem is, however, also a useful one to shorten the exposition of Section VII. Epecially in the discussion of these lemmata will the re-structuring of the DA come to the foreground, shedding some, if slightly defocussed, light on the genesis of the DA.

4.1 Lemma 40

Article 40 proposes to proof the following theorem:

> Let the greatest common divisor of the numbers A, B, C, D etc. be $= \mu$; We can always determine the numbers a, b, c, d, etc. such that $aA + bB + cC +$ etc. $= \mu$ (DA 40)

For just two prime numbers A and B this theorem ($aA+bB=1$) is now known as Bezout's theorem (cfr. Chabert 1999, 122-126), Gauss's version is more general. Its proof consists of successive applications of the solution method for simple congruences $A \equiv \nu \pmod{B}$, proven in article 30. When searching for occurrences resp. applications of lemma 40 throughout the DA, one is struck by its absence before coming to article 162, where all similar transformations of one quadratic form into another have to be calculated. This implies a long and tedious proof running over some five pages of long combinations and calculations on equations. The lemma is used to generate the coefficients $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$ that are applied (i.e. multiplied and combined) two times to a system of 6 equations, which in the end leads to a solution. In quite the same way, it is applicated in article 164, though only once. Afterwards, it only reappears in articles 215 and 218 to find the right substitution, although there is no explicit reference to article 40. Once, however, the part on the composition of forms starts, the lemma is continuously and explicitly used to prove both composition and decomposition of quadratic forms (DA 234-36, 240, 242). It starts with a lemma to find the multipliers to 4 series of integers (234), than proceeds to find the decomposition (235) and ends with the composition of 2 forms (236) - in this last case lemma 40 is applied even 2 times.

Considering the part on ternary quadratic forms, it is worthwhile looking at article 279:

> 279. Lemma. Given any three integers a, a', a'' (not all $= 0$): to find six others B, B', B'', C, C', C'' so disposed that
> $B'C'' - B''C' = a, \quad B''C - BC'' = a', \quad BC' - B'C = a''$

Its solution uses two successive applications of lemma 40 and Gauss remarks: "we have to omit here the analysis by which we found this solution and the method of finding all of them from one solution.“ (DA 279) But the lemma 279 in itself can be viewed as the analogon of lemma 40 for the theory of ternary forms. Indeed, the following articles 280, 284 II, 294 II, 299 II all use lemma 279 in proofs that can be considered more or less analoguous to the ones on binary forms.

---

[14] The addition of article 37 is not discussed in this paper, but in Bullynck 2005b, since it is a transformed version of traditional *Rechenbuch*-problems.

4.2 Lemma 41

As article 40, article 41 is a lemma that was only included late into the DA, and it could have served a similar purpose in the whole of the DA, if the eighth Section on congruences would have been included. Its formulation is clear, as is its provenience, being a lemma on combination and permutations, already proven in J. Bernouilli's *Ars conjectandi* which Gauss already acquired in 1793, cfr. Schlesinger 1912, 17 and Reich 2005, 47.

> If p is a prime number and we have p elements, among which as many as we please can be equal so long as not all are equal, then the number of permutations of these elements will be divisible by p. (DA 41)

Typically, Gauss mentions that the proof using the theory of permutations is easy, but gives an alternative demonstration by exhaustion - one of Gauss's favourite proof techniques.[15]

Looking for applications of this lemma, none but one is found. The one instance is a proof of $(a + b + c + \ldots)^p \equiv (a^p + bp + c^p + \ldots)$ (mod. p), with p prime. This generalisation of Fermat's little theorem ”will also prove useful for further investigations“ (DA 51), but never reappears in the DA. The inclusion of these two affiliated lemmata can, however, be explained, if one takes into account that a Section VIII was originally planned in the DA. The trace of these two theorems can indeed be pursued in the posthumously published AR's Chapter 8 and a much later 'spin-off' from the *Disquisitiones.*

Consider the eighth chapter of the AR, articles 340 to 365, where prime functions are defined and rules for the factorisation of equations given. In articles 341 through 343 arguments from the theory of combinations abound, more specifically we find: ”p res diversas admissis repetitionibus $\frac{p \cdot p+1}{1.2}$ modis divers combinari posse.“ (AR 342)[16] Quite close to the wording in DA's lemma 41, though without proof and generalisation, the use of combinations in the AR is quite often invoked, be it more in an ad hoc fashion. Proceeding through these articles, the AR also offers two theorems, viz. 350 and 356, that, although different, are closely allied to lemma 51.

As a matter of fact, the only explicit reference to lemma 51 in Gauss's writings occurs 17 years later in the sixth proof of quadratic reciprocity[17], given in *Theorema fundamentalis in Doctrina de Residuis Quadraticis Demonstrationes et Ampliationes novae* (1818) nr. 5 (Gauss 1863-1929, II, 57). As Bachmann remarks, this 1818-proof is affiliated with the seventh and eighth (resp. third and fourth) proof given in *De Analysis Residuorum* (articles 365-7) (Bachmann 1911, 50-1). Discovered 1796, but published only in 1863, these twin proofs rely exactly on the already mentioned articles 350 and 356.

Summarising our findings, it seems that the inclusion of lemmata 41 and 51 were part of a plan to rewrite AR's chapter 8 and add it to the bulky DA. Because of printing costs this never happened, though some materials from it were subsequently published in Gauss's 1818 paper. Once again, Gauss tried to make his presentation more coherent and transparent by moving some basic and widely useful theorems to the front of the DA, instead of having to prove them further on. Unfortunately, due to the circumstances, this re-structuring missed its goal, chapter 8 was only published posthumously.

4.3 Lemma 42

The insertion of lemma 42 is the only addition that has been discussed in the literature so far. The theorem states that the product of two functions in x, both with rational (but not all integer)

---

[15] Gauss's proof of Fermat's little theorem has the same rhetorics: Proofs using the binomium are mentioned, but the proof given is by exhaustion, cfr. DA 50. The term 'proof by exhaustion' should not be confused with e.g. Eudoxos's or Archimedes's method of exhaustion. These use exhaustion over a continuum through inclusion within upper and lower bounds, whereas Gauss's method of exhaustion runs over discrete elements, i.e., by 'counting'.

[16] Translation: ”p different things can be combined in $\frac{p \cdot p+1}{1.2}$ different ways, admitting repetition.“

[17] Or eighth proof, depending on the chronology of either publication, or discovery, cfr. Bachmann 1911, 50.

coefficients, is a new function, that cannot have all its coefficients integral (DA 42). Gauss's scientific journal dates the discovery of this proof on July 23d 1797, i.e., probably during the writing of the AR chapters 6-8 (cfr. Gauss 1863-1929, X, 519-20, Journal-fragment nr. 69; Merzbach 1981, 171, 173). As is visible in the entries of his scientific journal, Gauss worked on the articles 237-375 (i.e. chapters 6-8) during July till begin September 1797 (Gauss 1863-1929, X, 519-523), accumulating new results as well as noting opportunities to clarify and shorten his ideas.

Gauss's original treatment of cyclotomic equations most probably started off with the modular case $\frac{x^p-1}{x-1} \equiv 0 \pmod{p}$, treated in AR 237-251 (Bachmann 1911, 33-34). It seems, however, that during the writing of chapter 8 Gauss noticed that his exposition might be re-structured, using DA's lemma 42, that originally pertained to this general discussion on congruences. Considering that this general discussion never got rewritten and published, the inclusion of 42 is mainly needed for DA's Section VII. There, the lemma is used in article 341 only (Dedekind 1930, II, 28), which proofs that a cyclotomic equation with prime degree needs to have factors of a degree higher than unity.[18]

5 Conclusions

The ultimate redaction of the DA seems to have two distinct characteristics: 1) a refinement of the exposition's form; 2) a re-arrangement of theorems due to results found during the writing process. Characteristic 1 is most clearly observed in DA's 27, 31 and 33, characteristic 2 in the lemmata 40-42.

As to characteristic 1: The refinement is marked by the introduction of new forms and concepts and apart from the advantage they represent for the clearness of exposition, they also entail computational concision. In this light, the following quote from a letter to Schumacher is a succinct but clear statement of Gauss's considerations:

> Überhaupt verhält es sich mit allen solchen Calculs so, dass man durch sie nichts leisten kann, was nicht auch ohne sie zu leisten wäre; der Vortheil ist aber der, dass wenn ein solcher Calcul dem innersten Wesen vielfach vorkommender Bedürfnisse correspondirt, jeder der sich ihn ganz angeeignet hat, auch ohne die gleichsam unbewussten Inspirationen des Genies, die niemand erzwingen kann, die dahin gehörigen Aufgaben lösen, ja selbst in so verwickelten Fällen gleichsam mechanisch lösen kann, wo ohne eine solche Hülfe auch das Genie ohnmächtig wird. So ist es mit der Erfindung der Buchstabenrechnung überhaupt; so mit der Differentialrechnung gewesen, so ist es auch (wenn auch in partielleren Sphaeren) mit Lagranges Variationsrechnung, mit meiner Congruenzenrechnung und mit Möbius' Calcul. (Gauss an Schumacher, 15.05.1843, Nr. 1307, Peters 1850–1865, III, 107)

Gauss's much celebrated formalism for congruences $a \equiv b \pmod{c}$ is a prime example of this, but our analysis shows that the impulse for these "corresponding" formalisms owes much to subsequent application of modulo problems in more complex or more general problems. The neatest example of this is the regressive introduction of the fractional notation for roots of a congruence (DA 31), that was first used in the part on the calculation of indices (AR 55).

Another aspect of these formalisms is the computational advantage. It is repeated throughout the DA that brevity of calculation is ambitioned. Even in the more abstract parts of the DA, Gauss never looses sight of this aspect. E.g. even within the part on the composition of forms Gauss notices: "it is more advantageous to use one method consistently so that the operations involved can be reduced to a fixed algorithm" (DA 272 IV), in much the same way, he advises the reader to calculate the roots of a cyclotomic equation "from a table of sines" to distinguish the individual roots according to their magnitude (DA 352). The many formalisms Gauss introduces

---

[18] As the commentators of Gauss's scientific journal, Klein and Loewy, remark, Gauss's earlier proof of lemma 341, implied by nr. 40 of Gauss's journal (Gauss 1863-1929, X, 507), must have been either incomplete, or based on other principles (Ibid., 520).

play not an unimportant role in this regard. As we have seen, the squared brackets notation, e.g., in combination with the transformation formulae is quite advantaguous for solving both linear equations and Pell's equation, or for finding transformations of quadratic forms. Instead of Euler's and Lagrange's long substitution and/or continued fractions, Gauss delays his numerical evaluation of combined $[a, b, c, \ldots]$'s until a simple or a final form is reached, simple and final being defined relative to the application. Algorithmically speaking, division and multiplication are avoided during intermediary steps and are replaced by additions and subtractions, as can be observed in the notes to DA's 27 and 177.

Next to this internal motivation for the introduction of new formalisms, this leads us to an external factor. It was a common lamentation in 18th century mathematics that the calculations and notations got too involved. Instances may be quoted from Hindenburg 1786 on Euler, from Kästner 1758/1791-4 on Lagrange and from Delambre 1810 on Legendre.[19] The Combinatorial School, e.g., considered recursive formulae too involved, instead, they advocated explicit, independent formulae ("Lokalzeichen"), which led them to a focus on form (cfr. Jahnke 1990, 161-232, especially 189-90; Bullynck 2005a).

This concern (although not the combinatorial solution) was shared by Gauss. In a lettre to his protector Zimmermann during the time of the AR's writing, Gauss says:

> Daß ich diesen Entwürf nicht zu groß gemacht habe [ein Alphabet = 24 Bogen][20], sondern vielmehr manches dem Leser zu entwickln zu überlassen genöthigt bin, werden Sie daraus schließen können, das ich nothwendig das Wesentliche der Untersuchungen meiner Vorgänger habe mitnehmen müssen, und die von Euler zusammen ungefehr 50, die von La Grange etwa 30 und eine einzige Abhandlung von Le Gendre 12 Bogen beträgt. Ich würde eine Unmöglichkeit unternehmen, wenn hierunter nicht manche Wiederholungen wären und durch meine Methoden die weitläufigsten Rechnungen sehr zusammengezogen würden. (Gauss an Zimmermann, 12.03.1797, Poser 1987, 27)

This reduction ranged not only over extensive calculations but also over extensive proofs. Gauss's congruence notation clarified and simplified in this way lots of problems from indeterminate analysis. Another device that helped to reduce the exposition is Gauss's much discussed use of representants of classes to both calculate and prove results. Instances of this are the least residues (DA 4), and the primitive classes of binary quadratic forms: "For brevity we use the representing forms instead of the classes whose place they take." (DA 226, note)[21]

As to the reduction of the bulk of proofs, this immediately connects with our second characteristic. As we have shown lemma 40 repeatedly occurs in that part of DA's Section V which was written after 1798 and mainly reduces the bulk of the proofs on the composition of forms. In much the same way, lemma 41 together with the allied lemma 51 might have structured an eighth chapter on the factorisation of general congruences greatly. The same holds true for lemma 42, although it is indeed applied once, in the proof on the prime factors of the cyclotomic equation.

Lemmata 40 and 41 are by no means "new" or hard to prove theorems within mathematics, but they are fundamental and basic results. This certainly motivated Gauss to move them to the DA's frontmatter. As for lemmata 51 and 42, these are not as obvious to prove, hence, for lemma 42 the date of discovery is well recorded in Gauss's scientific journal. Most probably we have to date lemma 51 in the same period, since it clearly belongs to chapter 8 of the AR. The fact that lemma 42 was certainly (and lemma 51 probably) proven during the writing of the AR's final chapters, clearly shows how Gauss moved on and accumulated more results and insights into his arithmetical theory.

---

[19] For the exact references and quotes, as well as a broader discussion, we refer to Bullynck 2005a.

[20] Finally, the DA were 43 "Bogen" thick.

[21] There is in respect to this device a complex discussion on the date of emergence of equivalence classes, cfr. HM 2003, especially the remarks of G. Moore.

Considering once more the lemmata 40, 41 and 42, it is remarkable that all three have survived until nowadays in a near unaltered form (although they may have been transformated in theorems on ideals or groups), which emphasises their fundamental nature.[22] The subsequent polishing and clarifying C.F. Gauss devoted to his *Disquisitiones Arithmeticae* by carefully singling out essential theorems from the bulk of his results and placing them in an obvious place, Section II, has certainly borne fruits

References

Bachmann, P. (1911), *Über Gauss' Zahlentheoretische Arbeiten*, in: Gauss 1863-1929, Bd. X/2.

Beeler, M.; Gosper, R. and Schroeppel, R. (eds.) (1972), *HAKMEM*, MIT Artificial Intelligence Memo nr. 239.

Bullynck, M. (2005a), "Aspects of 18th Century Mathematical Socialisation. The Case of C.F. Gauss", (forthcoming).

— (2005b), "C.F. Gauss's Re-Writing of Section II *De congruentiis primi gradus*", (forthcoming).

— (2006), "A Note on article 36 in Gauss's *Disquisitiones.* A Ramificated Story in the Margin of the Re-Writing of Section II", *Simon Stevin - Bulletin of the Belgian Mathematical Society*, (to appear March 2006).

Cajori, F. (1928/29), *A History of Mathematical Notations, 2 Bd.*, La Salle, nachdruck im Einband, New York, 1993.

Chabert, J.-L. (ed.) (1999), *A History of Algorithms. From the Pebble to the Microchip*, Springer, Berlin.

Conference Report (2001), "Two Hundred Years of Number Theory after Carl-Friedrich Gauss' Disquisitiones Arithmeticae, June 17th - June 23rd", Report No. 26/2001, verfügbar unter: www.mfo.de/programme/schedule/2001/25b/Report_26_01.ps.

Dauben, J. e. (1981), *Mathematical Perspectives. Essays on Mathematics and Its Historical Development*, Academic Press, New York.

Dedekind, R. (1930), *Gesammelte mathematische Werke*, Vieweg, Braunschweig, hg. von Fricke, Noether und Ore, 3 Bde.

Delambre, M. (1810), *Rapport Historique sur le progres des sciences mathématiques depuis 1789 et sur leur état actuel*, Paris.

Dunnington, G. (1955), *Carl Friedrich Gauss. Titan of Science*, Exposition Press, New York.

Euler, L. (1765/7), "De usu novi algorithmi in problemate Pelliano solvendo", In: Euler 1907, Bd. 2, 74–111.

— (1862a), *Opera Postuma*, Teubner, Leipzig, Berlin, hg. von Rudio, Krazer und Stäckel.

— (1862b), *Tractatus de numerorum doctrina Capita XVI, quae supersunt*, in: Euler 1862a, Bd. 1, 3–75.

---

[22] It is not by accident that Dedekind dedicated an essay to Gauss's lemma 42 (Dedekind 1930, II, 28-39).

— (1907), *Commentationes Arithmeticae (2 Vol. = Leonhardi Euleri Opera Omnia. Series I. Volumen II & III)*, Teubner, Leipzig, Berlin.

Gauss, C. (1797), "Elementa doctrina Residuorum", Handschrift: Artikel 1-18, 23-38, 50-75, 79-85 im NL Dirichlet 31 (Berlin-Brandenburgische Akademie der Wissenschaften - Akademiearchiv); Artikel 39-50 im NL Dirichlet, Vermischtes (Staatsbibliothek zu Berlin - Handschriftenabteilung); Artikel 237-251; 253-302; 330-375 in NL Gauss, Manuskripte 50, 51, [De Analysis Residuorum] (Niedersächsische Staats- und Universitätsbibliothek Göttingen), partly published in Gauss 1863-1929, II, 199–242, with commentaries by Dedekind.

— (1801a), *Disquisitiones Arithmeticae*, Fleischer, Leipzig, nachdruck Culture et Civilisation, Bruxelles 1968 (also Gauss 1863-1929, I).

— (1863-1929), *Werke*, Göttingen, nachdruck Hildesheim, New York, 1973.

Gauss-Bibliothek (2005), "C.F. Gauss: Bibliothekbestand", Zusammengestellt mittels der OPAC der heutigen Niedersächsische Staats- und Universitätsbibliothek Göttingen (Suchbedingungen: Signatur [Gauss Bibl.]).

Göcksel, A. and Örkan, E. (2001), "A Historical Survey of the Fundamental Theorem of Arithmetics", *Historia Mathematica*, 28 (3), pp. 207–214.

Grotefend, H. (1905), *Taschenbuch der Zeitrechnung*, Hahn, Hannover und Leipzig, 2. Auflage.

Hänselmann, L. (1878), *Karl Friedrich Gauß. Zwölf Kapitel aus seinem Leben*, Leipzig.

Hindenburg, C. (1786), "Verbindungsgesetz cyklischer Perioden; Natur und Eigenschaften derselben; Ihr Gebrauch in der diophantischen oder unbestimmten Analytik", *Leipziger Magazin für reine und angewandte Mathematik*, 1 (3), pp. 281–324, hrsg. von Bernouilli, J. und Hindenburg, C.F.

HM (2003), "Concept of Equivalence Relation", *Historia Matematica (mailing list)*, Volume 05 (Number 095), (Thursday, September 25).

Jahnke, H. (1990), *Mathematik und Bildung in der Humboldtschen Bildungsreform*, Vandenhoeck & Ruprecht, Göttingen.

Kästner, A. (1758/1791-4), *Der mathematischen Anfangsgründe*, Vandenhoek & Ruprecht, Göttingen, 4 Teile, 4. Auflage (1. Auflage, 1758).

Knuth, D. E. (1969), *The Art of Computer Programing, Vol. 2: Seminumerical Algorithms*, Addison-Wesley, New York, third Edition. Addison-Wesley, 1997.

Lambert, J. (1769), "Adnotata quaedam de numeris, eorumque anatomia", *Nova Acta Eruditorum*, LXIX, pp. 107–128.

— (1770), *Zusätze zu den Logarithmischen und Trigonometrischen Tabellen*, Spener'sche Buchhandlung, Berlin.

Lejeune-Dirichlet, P. (1863/1894), *Vorlesungen über Zahlentheorie*, Vieweg, Braunschweig, hg. von R. Dedekind, 1. Auflage 1863, 4. Auflage 1894.

Lichtenberg, H. (1997), "Zur Interpretation der Gaußschen Osterformel und ihrer Ausnahmeregeln", *Historia Mathematica*, (24).

Merzbach, U. (1981), “An early version of Gauss’s Disquisitiones Arithmeticae”, In: Dauben 1981, 167–178.

Mittler, E. (ed.) (2005), *”Wie der Blitz einschlägt, hat sich das Räthsel gelöstÒ Carl Friedrich Gauß in Göttingen*, Niedersächsische Staats- und Universitätsbibliothek Göttingen, Göttingen, (=Göttinger Bibliotheksschriften 30).

Neumann, O. (1979-1980), “Bemerkungen aus heutiger Sicht über Gauß’ Beiträge zu Zahlentheorie, Algebra und Funktionentheorie, 1. Teil”, *NTM-Schriften zur Geschichte der Naturwissenschaften, Technik und Medezin*, 16 (2), pp. 22–39.

Peckhaus, V. (1997), *Logik, Mathesis Universalis und die allgemeine Wissenschaft: Leibniz und die Wiederentdeckung der formalen Logik im 19. Jahrhundert*, Akademie-Verlag, Berlin.

Peters, C. (ed.) (1850–1865), *Gauss C.F. - Schumacher H.C.: Briefwechsel*, Esch, Altona, reprint: Hildesheim, New York: Olms Verlag, 1975.

Poser, H. (ed.) (1987), *Briefwechsel zwischen Carl Friedrich Gauß und Eberhard August Wilhelm von Zimmermann*, Vandenhoeck & Ruprecht, Göttingen.

Reich, K. (2005), *Der junge Gauß und seine Welt der Mathematikbücher*, in: Mittler 2005, 35–47.

Schlesinger, L. (1912), *Über Gauss’ Arbeiten zur Funktionentheorie*, in: Gauss 1863-1929, Bd.X/2.

Subskribentenliste (1781), “Liste der Subskribenten”, *Leipziger Magazin zur Naturkunde, Mathematik und Oekonomie*, 1, nicht-paginiertes Vorwort.

Tschebyscheff, P. (1845/1889), *Theorie der Kongruenzen*, Mayer & Müller, Berlin, deutsche übersetzung von H. Schapira.

Weil, A. (1984), *Number Theory: An Approach through History from Hammurapi to Legendre*, Birkhäuser, Boston.