

Mathematical Tables and other Ways to Gauss and Computation

The U.S. reception of C.F. Gauss's number theoretical work (1938-1989)

Maarten Bullynck¹ *

IZWT, Bergische Universität Wuppertal, Gaußstraße 20, 42119 Wuppertal, Germany

Received: date / Revised version: date

Abstract The 20th century reception of C.F. Gauss's computational work in number theory is sketched. In particular, the involvement of the U.S. American mathematicians Derrick Henry Lehmer and Daniel Shanks with Gauss's work is analyzed, especially their continuation of work on topics as arccotangents, factors of $n^2 + a^2$, composition of binary quadratic forms.

1 Introduction

[John Selfridge]: "How old is [D.H.] Lehmer?"
[Daniel Shanks]: "He's 83. he was born on Feb. 23, 1905. Gauss died on Feb. 23, 1855 and I used to ask Lehmer, 'Where were you that whole 50 years?'" [Shanks(1989), p. 194]

Without going as far as jokingly suggesting a transmigration of souls, there is indeed a transmigration of ideas and attitudes between C.F. Gauss (1777-1855) and the American mathematicians Derrick Henry Lehmer (1905-1991) and Daniel Shanks (1917-1996). Both often pointed out the lineage that runs from Gauss to their own work, and their reception of Gauss's work in number theory and its computational aspects is an important and

* I would like to thank the Alexander-von-Humboldt-Stiftung for funding this research. For their comments I would like to thank Catherine Goldstein, Norbert Schappacher and especially John Brillhart. *Present address: Krijgslaan 57, 9000 Gent, Belgium.*

innovative phase in the history of number theory. Moreover, it is a part of the birth of computational mathematics as a discipline in its own right.¹

The reception of Carl Friedrich Gauss's masterpiece, the *Disquisitiones Arithmeticae* [Gauss(1801), Gauss(1965)], was an intricate process running over many decades. From its publication in 1801 onwards, its reception has left its deep marks in the history of mathematics, but also, the *Disquisitiones* have been interpreted and reinterpreted as mathematics and number theory itself changed. With citation networks (using the *Jahrbuch über die Fortschritte der Mathematik* from the years 1870 until the First World War) Catherine Goldstein has recently shown that work pursuing Gauss can be roughly divided in three categories [Goldstein and Schappacher(2007), p. 71–75]. There is a Dirichlet-cluster, involved in analytical number theory, a Hermite-Kronecker-cluster, expanding the theory of binary quadratic, ternary and other forms. Finally a third cluster, the Legendre-Gauss-cluster, takes up various issues in number theory (congruences and quadratic reciprocity e.g.) without recourse to analysis or the theory of forms. The last two traditions have so far been mostly underrepresented in the historiography of mathematics, especially the third tradition, because it falls somewhat outside the realm of research journals, though it is quantitatively by far the greatest.

Looking specifically at the reception of Gauss in the U.S., two different aspects of reception can be discerned, already from the time that E.H. Moore (1862-1932) built up the first research-oriented mathematics department in American history at Chicago University. Before then, an American had to go to Europe to learn how to do mathematical research [Parshall and Rowe(1994)]. These two different strands are personified by two of E.H. Moore's students who went on to work in number theory, the first and best-known being Leonard E. Dickson (1874-1954), the second one Derrick N. Lehmer (1867-1938). Della Fenster has shown how L.E. Dickson's *Introduction to the Theory of Numbers* follows the lay-out of Gauss's *Disquisitiones*. Also, in his monumental *History of Number Theory* Gauss's work figures prominently [Fenster(2007)]. However, another strand in the U.S. reception of Gauss's number-theoretical work would avail himself of great importance in the years after 1930. This reception focused more on the computational side of Gauss's work, a side often neglected in the traditional interpretation of the *Disquisitiones*, though very present in the Legendre-Gauss-cluster of reception. Derrick N. Lehmer's work on tables of divisors may serve as an example of such orientation. "Lehmer [was] alive to the significance of theory and viewing the table [of divisors] as a contribution to it" [Putnam(1939), p. 209], and disliked the 'modern' tendency to reformulate long-known theorems in number theory as theorems in group theory.²

¹ D.H. Lehmer's involvement with computational number theory on the ENIAC and on the SWAC has recently attracted academic interest, see [De Mol and Bullynck(2008), Corry(2008)].

² According to his son D.H. Lehmer (personal communication by John Brillhart).

Interestingly enough, this rediscovery of the computational Gauss runs parallel to and is deeply intertwined with another important development that has had and is having an enormous impact on mathematics: The birth of the digital computer. From the beginnings (the 1930ies) onwards, the main actors of this history were deeply interested in computational work, paper work if needed, mechanized work if possible, as well as in mathematical tables. This particular strand in the reception of Gauss's work in number theory is therefore also a witness of the changing goals and interests within mathematics, is also a part of the emergence of the digital computer and its influence on mathematics.

2 Gauss's Tables from the *Nachlass*

The magistral edition of C. F. Gauss's *Collected Works* [Gauss(1863-1929)], begun 1863 and finished 1929, was an important factor in rekindling the interest in Gauss's work. Many of the collaborators of the edition, such as Ernest C.J. Schering, Richard Dedekind, Paul Bachmann, Philipp Maennchen, as well as others invested much effort in editing Gauss's *Nachlass* (unpublished notes and manuscripts) and it might even be said that this effort was not without influence on their own mathematical work. The publication of the 12 volumes also aroused interest in the U.S., especially the volumes 2 (1863, 2nd expanded edition 1876³) and 10 (1917), that contained much of Gauss's computational work and extensive mathematical tables.

Raymond Clare Archibald (1875–1950) had studied mathematics in Europe and was since 1908 associated with the mathematics department of Brown University. He helped build up a vast mathematical library at Brown and from 1921 to 1941 also supervised the growth of the library of the American Mathematical Society. He was also a historian of mathematics, contributing to the newly found journal *Isis* as well as to *Osiris* and *Scripta Mathematica*, serving as (co-)editor on the boards of these journals [Sarton(1956)]. Archibald had particular interest in mathematical tables. Apparently, he collected tables on his summer trips to Europe, bringing together an impressive table library at Brown, and publishing many notes and papers on historically important tables and table makers (collected in [Archibald(1948)]). He shared this interest with the mathematician Derrick Henry Lehmer, D.N. Lehmer's son, who had studied under Dickson in Chicago (1929–1930), and under Archibald at Brown University (1930–1932) [Lehmer(1973), p. 1]. During these student days Lehmer helped Archibald to identify obscure mathematical tables and when Archibald be-

³ "Volume 2 in its 2nd edition of 1876 had been somewhat enlarged by Schering: The tables on pages 484–495 were spread out (without change of contents) on pages 484–496, additional material was added on pp. 497–518, and Schering's "Bemerkungen" as well as the table of contents (formerly pp. 496–504, now pp. 519–528) were properly adjusted." (C.J. Scriba on MathSciNet).

came the Chairman of the Committee on Mathematical Tables and other Aids to Computation in 1939, Lehmer joined him in this venture.

In 1941 the Committee published Lehmer's report on tables in the theory of numbers [Lehmer(1941)], that listed all known auxiliary tables in number theory, large and small, including lists of known errors. C.F. Gauss is the fourth most quoted table-maker in Lehmer's report, immediately after the notorious table-makers A.J.C. Cunningham (1842-1928), M. Kraitchik (1882-1957) and D.H. Lehmer himself. With this result, Gauss is on about the same level with J.W.L. Glaisher and D.N. Lehmer, authors of large factor tables. The entries on Gauss's tables show that Lehmer inspected them with care, adding comments on their use and purpose that are not to be found in the *Werke*.

In 1943 Archibald could convince the National Research Council to finance the publication of a periodical, documenting the evolution of mathematical tables, computing machines and techniques of calculation [Lehmer(1969), Lehmer(1973), p. 13-15 & 13-14]. Archibald would serve as the chief editor of *Mathematical Tables and other Aids to Computation*⁴ until his death in 1950, D.H. Lehmer taking over the editorship in the fifties (1950 to 1959). Through this journal and personal contacts, both of them organized a network where an interest for computational procedures and tables was fostered and where a reception of the computational Gauss slowly grew.⁵

The first rediscovery of Gauss's techniques happened around 1938, with the publication of two articles. Both were published in the *Mathematical Monthly*, one by John Wrench Jr. and one by D. H. Lehmer [Wrench(1938), Lehmer(1938)]. These papers are a continuation of the tables on *Cyclotechnie* in Gauss's *Nachlass* [Gauss(1863-1929), II, p. 477-495]. These tables list the divisors smaller than 200 for 2452 numbers of the forms $aa + 1$, $aa + 4$, $aa + 9$, \dots , $aa + 81$. Gauss had started these calculations at the time of writing his *Disquisitiones Arithmeticae* (from 1797 to 1801), but had returned to these late in his life (1846-7), drawing up extensive and, as far as possible, complete tables.

The editor of this second volume, Ernest Schering, had written in the commentaries [Gauss(1863-1929), II, p. 523-525] that these tables had their foremost use in calculating arcs whose cotangents are rational numbers and could hence be used for finding formulae approximating π . In Philipp Maennchen's essay on Gauss's calculations, accompanying the 10th volume of the *Werke*, the tables are discussed from another viewpoint [Maennchen(1918), p. 36-46]. Maennchen suspected Gauss was interested in finding the distribution of divisors of numbers of the form $aa + bb$. Both interpretations are mentioned by D.H. Lehmer in his *Guide to Tables* [Lehmer(1941), p. 32].

Lehmer's and Wrench's articles focus on the generation of arc(co)tangent relations suitable for an accurate and speedy calculation of π . The main idea is that it is possible to write $\arctan(n)$ as a finite sum of smaller \arctan 's,

⁴ Henceforth abbreviated as *MTAC*, 4 (29), 1.

⁵ For the history of the journal see also [Polachek(1995)].

using results from Diophantine analysis. Because $\arctan(n)$ is equal to

$$\frac{i}{2} \log \frac{1 - ni}{1 + ni}$$

a decomposition of $\arctan(n)$ into $\sum \lambda_i \arctan(n_i)$ comes down to finding solutions to

$$(1 + ni) = (p/q) \prod (1 + n_i i)^{\lambda_i}$$

with p and q integers. Thus, one has to solve the quadratic diophantine equation

$$(1 + n^2)q^2 = \prod (1 + n_i^2)^{\lambda_i} p^2$$

For instance, to find a decomposition of $\arctan(3)$, which we write as (3) hereafter, into (1) and (2), one has to solve $10q^2 = 2^r 5^s p^2$. $r = 3, s = 1$ being the solution, (3) can be written as $3(1) - (2)$. Using Gauss's tables of factorisations of $n^2 + 1$ or Cunningham's binomial factorisations [Cunningham and Woodall(1925)], such decompositions can be easily found. Among the formulae thus generated one finds (using arccotan for convenience) Euler's formula, $\pi/4 = (1) = [2] + [3]$, and Machin's often used formula, $\pi/4 = (1) = 4[5] - [239]$, writing $[n]$ for arccotan (n) .

Applying this theory, Wrench derives 4 new identities for calculating π , especially suited for machine calculation (i.e. desk calculators), hence using arctangents of powers of ten [Wrench(1938), p. 109]. As a follow-up paper to Wrench, Lehmer returns to the question of these arctangent identities, indicating a formula to determine the time complexity of the calculation. Assuming the Gregory series⁶ is used for evaluation of \arctan , Lehmer defines his measure for the amount of calculation labor required by [Lehmer(1938), p. 657]⁷:

$$\sum \frac{1}{\log n_i}$$

Since the calculation of [10] is much simpler than predicted by this measure (due to shortcuts possible in the decimal number system), Lehmer sets this measure equal to $\frac{1}{2}$. Similarly, arccotangents that are powers of previously calculated arccotangents have measure zero because they can be easily recopied from the earlier calculations.⁸ Using this definition, one obtains measure 5.41778 for Euler's formula, 1.8511 for Machin's formula, 1.9644, 1.5513 and 1.5860 for the formulae Wrench recommended. Lehmer also shows that this measure can be made arbitrarily small, though the numbers involved get unreasonably large for easy calculation. As the 'best' formula, having a small measure and involving small numbers, Klिंगenstierna's $[1] = 8[10] - [239] - 4[515]$ (measure 1.2892) is recommended.

⁶ I.e., $\arctan x = \sum_{n=0}^{\infty} (-1)^n (2n+1)^{-1} x^{2n+1}$.

⁷ The \log is the common logarithm with base 10, since calculations at that time were done in decimal format. When changing the number base to n , the \log should be replaced with \log_n . As Lehmer shows, all results hold for other number bases.

⁸ Lehmer makes a conservative estimate on $\operatorname{arccotan} 10 = \arctan \frac{1}{10}$, giving it measure 0.5, probably, 0.25 would be closer to the truth, cfr. the time estimate in [Shanks and Wrench(1962), p. 77].

3 Enter the Digital Computer: Calculating π

December 1945 John Wrench was commissioned by R.C. Archibald, in his function as head of the Committee for Mathematical Tables, to undertake a new calculation of π (with desk calculators) to check on William Shanks's 707-digit computation (1854). Using Machin's formula, Wrench computed the [5] part, whereas Levi Smith computed the [239] part [Wrench(1947), p. 245]. Their report describes in detail the procedures and the check routines used and found Shanks in error from the 527th digit onwards. In the course of this calculation, Wrench made up two auxiliary tables: A table of the consecutive powers of 2 and a table of all reciprocals of the form $r/(2n-1)$, n less than 425 [Wrench(1947), p. 246]. This latter table was later used by Wrench to check Gauss's extensive tables of decimal periods [Gauss(1863-1929), II, p. 412-434], finding 22 errors [Wrench(1950)].⁹

Wrench's effort, however, is about the last computation of π without the help of digital computers. During the Second World War, not only mechanical computers were much improved upon, but the first electronic digital general-purpose computer, the ENIAC, had been constructed, working at a speed a factor of ten upto hundred times faster than their mechanical or relay-based counterparts [Goldstine and Goldstine(1946), Hoffleit(1949)]. These technological innovations had sparked a new interest in computational methods and apart from the people around the journal *MTAC* several research groups in the U.S. devoted their time to find and construct faster computational methods suited for digital computers. One such center was the Institute for Numerical Analysis (INA) founded by the National Bureau of Standards (NBS) in 1947 that (partially) grew out of the Mathematical Table Project started in 1939 [Todd(1975b)].

In 1946 J.C.P. Miller, involved in a similar table project in the U.K., posted two queries on inverse tangents and their interrelations, information that was useful to Miller for computing a large table of the gamma function [Miller(1946), Johnston and Miller(1946)]. John Todd, at that time employed at the recently founded INA in California, responded to these queries with a note in *MTAC* and a more extended paper in the *Monthly* [Todd(1947), Todd(1949)].¹⁰ Todd's papers returned to Gauss's work in the *Nachlass* and Lehmer's papers, but established a criterium to find out whether a certain rational arc(co)tangent is irreducible or not, i.e., an arc(co)tangent is irreducible if it cannot be written as the sum of smaller arc(co)tangents. An arctangent (N) is irreducible if and only if N^2+1 has a prime factor which is not a factor of a number n^2+1 with $n < N$, or also, if N^2+1 has no prime factors smaller than $2N$. This meets Gauss's own definition of irreducible within the range of his tables, since Gauss had called

⁹ Wrench also corrected Gauss's tables of the lemniscate function [Wrench(1948)], using arctangent relationships. Compare also [Lehmer(1948), Todd(1975a)].

¹⁰ See also Lehmer's review of Todd's article, [Lehmer(1950)].

those numbers $a^2 + 1$ irreducible that have no prime divisors under 200. As a side-result, Todd spotted an error in Gauss's table for arccotangents.¹¹

When in 1949 John von Neumann and Nick Metropolis suggested to George Reitwiesner to calculate e and π on the ENIAC, this string of papers on arctangents provided the basis for choosing an efficient computation procedure. Reitwiesner listed three arccotangent formulae, among them Machin's classic and the Klängenstierna formula recommended by Lehmer.

$$4[5] - [239] \text{ (Lehmer measure 1.8511)}$$

$$8[10] - [239] - 4[515] \text{ (Lehmer measure 1.2892)}$$

Although Klängenstierna's formula was listed as a possible candidate, Reitwiesner rejected it, and used Machin's formula so that "identical programming apply for all series employed" [Reitwiesner(1950), p. 13]. Indeed, the Lehmer measure for Klängenstierna's formula is small, because it is assumed that the evaluation of $[10]$ is advantageous, can be shortcut in the decimal system. Although the ENIAC was a decimal machine, this shortcut would imply that two routines had to be programmed on the computer: One for the general Gregory series for evaluating $[n]$ and a special one for $[10]$. Given the limited memory of the ENIAC and the difficulty of programming it, Reitwiesner's choice is understandable. Or: Commodity of programming apparently excludes shortcuts.

e was calculated on a Fourth of July weekend, π on a Labor Day weekend in 1949 [Reitwiesner(1950)]. Since many digits of e and π were desired, the size of the storage rings (10 digits, or 20 digits if coupled) had to be circumvented. Therefore the division process was split up: A number i of digits to be calculated per run was determined, the i digits found by division and the remainders were stored separately, these last ones printed out on punch cards. After all first i digits of all terms in the formulae for e and π were calculated and added up (and stored on another punch card), the process was restarted, but this time starting from the remainders on the punch cards, to get at the next i digits etc. At last, all digit punch cards were added (in the case of e), or all digit cards were added term-wise, and the terms subsequently added (for π). The sequence of commands was quite straightforward to program with the new converter code [Clippinger(1948)]. The formula for e uses only multiplication, division and addition, and is thus easy to program, certainly with the lookup table of elementary operations. π is different, since the arctan implies powers n , -1 and $2n + 1$ and is thus a little more intricate.

The first digital computation of π to 2035 digits eclipsed Wrench's 808-digit-determination only 2 years earlier. Connecting with another recently developed mathematical device, pseudo-random number generators [von Neumann(1951)], von Neumann suggested to check on the distribution

¹¹ It may be remarked that parallel to the rediscovery of the cyclotechnic formulae, Gauss's work on the computation of linear systems was rediscovered as well. George Forsythe found a relaxation method in Gauss's letters and improved on the method in the years 1951-2 [Forsythe(1951), Forsythe and Motzkin(1952)].

of the digits in π and e . The analysis showed that the distribution of the digits of π seem to obey to a normal distribution, and are thus 'random', whereas the digits of e diverge from a normal distribution, and are not random [Metropolis et al.(1950)Metropolis, Reitwiesner and von Neumann]. This was confirmed by later computations [Gruenberger(1952)].

In the following years, some other computations of π on digital computers were executed, all using Machin's formula [Shanks and Wrench(1962), p. 76]. The next big step in obtaining more digits was in 1962 on a IBM 7090 system. Daniel Shanks together with π -veteran John Wrench returned to the arctangent relations, deriving the following equation: $\pi = 24[8] + 8[57] + 4[239]$ due to Størmer.¹² The calculation was checked with a formula due to Gauss: $\pi = 48[18] + 32[57] - 20[239]$. The IBM 7090 being a binary machine, Shanks and Wrench did use the obvious shortcut on [8], where binary shift can be used instead of costly division. Moreover, they compressed the series used to evaluate the arctangents, saving 27 percent in operations. Finally, they obtained 333,075 bits or 100,265 decimal digits of π .

Shanks and Wrench's computation is the last one using Gauss's arctangent formulae. As they discuss at the end of the paper, arctangent formulae allow only for small improvements on the time of calculation. They suggest that computing the reciprocal of π might be more advantageous, using Ramanujan's formula [Shanks and Wrench(1962), p. 78]. This would essentially become the most important method in the years to come (from the 1970ies onwards).

Daniel Shanks also contributed in a different way to the theory of arctangents. He took up the question of the density of irreducibles, posed by Todd and Chowla [Chowla and Todd(1949)], as well as Gauss's original questions (according to Maennchen), viz., the relation of factorisations of $n^2 + 1$ to the Gaussian primes, and the factors of $n^2 + a^2$ [Shanks(1959)]. To this end, Shanks used an IBM 704 to sieve through all numbers $n^2 + 1$ from $n = 1$ to 180,000. Using the statistics obtained by this method, Shanks checked on various conjectures related to primes, irreducibles and p-adic roots of -1 .

4 Factorisation

There is another strand figuring prominently in Gauss's work, both in his published work and the *Nachlass*, that is revived in the years 1930–1960: Factor tables and factorisation.¹³ Gauss was intimately familiar with the construction of large factor tables, as his reviews of Chernac and Burckhardt's tables show [Gauss(1863-1929), II, 181–186]. Moreover, in his *Disquisitiones Arithmeticae*, Section VI on applications, Gauss had described

¹² The formula has a Lehmer measure of 2.0973 on a decimal computing machine, but only a measure of 1.2400 on a binary machine, where $\frac{1}{3}$ of the divisions can be shortcut as binary shifts.

¹³ For the prominence of this theme in Gauss's work, see [Bullynck(2008b)].

at length two new procedures to factor large numbers, using his theoretical results from the preceding sections. As D.H. Lehmer had noted when describing Gauss's tables of quadratic forms:

the representation of a large number N by the form $x^2 - Dy^2 = N$ [...] was at once seen to be a key to the question of factoring large numbers N and it was with this application in mind that Gauss began his epoch-making investigation into the theory of binary quadratic forms. [Lehmer(1941), p. 68]

Gauss's two methods both connect to binary quadratic forms.

The first method, explained in articles 330 to 332, is the exclusion method of residues. Given a number N and r_i quadratic residues of N , one can gradually sieve out half of possible divisors of N (\sqrt{N} numbers in the first step, half of that in the second, a fourth in the third etc.) by checking the residues. Since a residue r of N is also a residue of a divisor of N , this sieving process eliminates possible divisors, especially if a table of residues of numbers upto 997 (in Gauss's table from the *Nachlass*) is accessible. The second method (articles 333–334) relies upon the values of $\sqrt{D} \bmod N$ (D being the determinant of a quadratic form). The greatest common divisor of N and the differences of these values correspond to the factors of N . This method can in essence be found in Fermat, who used the quadratic form $x^2 - y^2$, but it becomes only efficient with other, suitably chosen quadratic forms, the 'suitably chosen' depending on the form of the number N that has to be factorised. The theory that enables this suitable choice was developed by Euler, Legendre and Gauss.

For the first method, Gauss indicated a means of mechanizing the procedure:

The table should distinguish prime numbers which have each (r) as residue from those for which they are nonresidues. [...] the maximum utility would result if the individual vertical columns were removable and could be reassembled on plates or rods (like those of Napier). [...] If these are properly placed next to the first column of the table which contains the moduli (i.e. in such a way that the position in each of the rods which corresponds to the same number in the first column is placed in the corresponding horizontal line) those prime numbers that remain after the exclusions [...] can be recognized immediately by inspection. [Gauss(1965), art. 331]

A specimen of a table giving all residues of the moduli upto 97 is printed as appendix II in the *Disquisitiones*. As Maennchen recounts, tin rods as described in this quote were found in Gauss's *Nachlass* [Maennchen(1918), p. 34]. Together with Legendre's method [Legendre(1798), pp. 313–320] based on linear divisors of quadratic forms and the continued fraction expansion, these were the best general factoring methods available during the 19th century (cfr. [Dickson(1919–1927), I, p. 355–374]).

Though these factoring methods were known in the literature, nobody seemed to have used them in the construction of a large factor table. E.g.,

J.W.L. Glaisher [Glaisher(1878)] essentially used J.K. Burckhardt's stencil method [Burckhardt(1814)]. This again, is actually a refinement of C. F. Hindenburg's paper-and-ink sieve method [Hindenburg(1776)], that in itself is an improved implementation of Eratosthenes's sieve. Only in the beginning of the 20th century were Legendre's and Gauss's methods taken up again. Derrick Norman Lehmer (Derrick Henry Lehmer's father) published on Legendre's method of linear divisors and published factor stencils for factoring numbers upto 2 billion [Lehmer(1926), Lehmer(1927), Lehmer(1929)]. Around the same time Kraitchik promoted Gauss's first method again in his *Théorie des Nombres* [Kraitchik(1922)]. Finally, Derrick Henry Lehmer mechanized his father's factor stencils. Substituting the paper strips with (bicycle) chains, Lehmer built a sieve mechanism in 1928 [Lehmer(1928)]. Later, in 1933, he speeded up the machine by rebuilding it with mechanical rotating gears and a photo-electric eye [Lehmer(1933a), Lehmer(1933b)]. Again later, with the birth of digital electronic computers, Lehmer described in detail how to set up various number sieves, both the linear sieve (Eratosthenes's sieve) and the quadratic sieve (the linear divisors method) [Lehmer(1953)].

In 1974, when efficient factoring methods had become an important topic once again, D.H. Lehmer and his wife, Emma Trotskaïa Lehmer, took up parts of Gauss's second method and ideas from Legendre and Kraitchik [Lehmer and Lehmer(1974)]. Given a number N , take its residue n modulo 24 and select three quadratic forms according to the following table:

n	1	5	7	11	13	17	19	23
selection	<i>BDI</i>	<i>AHJ</i>	<i>CDG</i>	<i>BFH</i>	<i>ADE</i>	<i>ABC</i>	<i>BDI</i>	<i>CFJ</i>

with

$$\begin{array}{llll}
 (A) & N = x^2 + y^2 & (B) & N = x^2 + 2y^2 \\
 (C) & N = x^2 - 2y^2 & & \\
 (D) & N = x^2 + 3y^2 & (E) & N = x^2 - 3y^2 \\
 (F) & -N = x^2 - 3y^2 & & \\
 (G) & N = x^2 + 6y^2 & (H) & 2N = x^2 + 6y^2 \\
 (I) & N = x^2 - 6y^2 & & \\
 (J) & -N = x^2 - 6y^2 & &
 \end{array}$$

Using Gauss's method to solve quadratic congruences with exclusion moduli, the Lehmers solve two of these forms for N , three if one of the two fails to generate a solution. This gives at least two solutions, (x_1, y_1) and (x_2, y_2) , for N . Computing the greatest common divisor of N and $x_1y_2 - x_2y_1$ then gives a factor of N .¹⁴

¹⁴ As J. Brillhart pointed out to me, it should be noted that this method was already less performant at the time of its publication than Morrison and Brillhart's algorithm, first described 1969 by D.E. Knuth [Knuth(1969), p. 396–401] and explained with computational detail in 1975 [Morrison and Brillhart(1975)]. The Lehmers' method is, however, useful for other jobs in number theory, such as finding pseudo-squares.

5 Daniel Shanks's reading of Gauss's *Disquisitiones Arithmeticae*

Daniel Shanks, whom we already mentioned because of his work on π and on divisors of $n^2 + 1$, apparently got involved in computational number theory through his 1959-article on the distribution of primes under the form $n^2 + 1$ [Williams(1997), p. 930]. This article, in which heuristics (computations and tables), fast algorithms and conjectures are of paramount importance, returns to Gauss's original objectives with the cyclotechnic tables. These researches prompted Shanks to pursue related issues, amongst them a Hardy-Littlewood conjecture on the distribution of primes under the form $n^2 + a$, and to devise fast algorithms to evaluate the Dirichlet L -functions [Shanks(1960), Shanks and Wrench(1963), Shanks(1963)]. To compute this last function, one needs to evaluate the class number, $h(d)$, of the discriminant d of a quadratic form ($ax^2 + bxy + c^2$, $d = b^2 - 4ac$). In the course of investigating class numbers, their algorithms and the quadratic forms they are related to, Shanks eventually went back to the famous Section V on quadratic forms in Gauss's *Disquisitiones Arithmeticae*. Shanks's work between 1969 and 1975 is written in close dialogue with Gauss's original text, and the series of articles published in these years may be said to constitute a sagacious reading, comment and actualisation of Gauss's Section V.¹⁵

Shanks's Gauss-lecture must have started in the 1960ies, as Chapter II of his idiosyncratic but wonderful introduction to number theory attests. This book, *Solved und unsolved problems in number theory* [Shanks(1993)], was published 1962, and republished in 1977, 1985 and 1993 with an additional Chapter IV, 'Progress', that discusses progress in computational number theory. Chapter II, 'The Underlying Structure', deals with residue classes, congruences, primitive roots and related questions. In contrast to Chapter I that starts from perfect numbers and proceeds to the quadratic reciprocity law (from Pythagoras over Euclid, Fermat, Euler to Legendre so to say), Chapter II focuses on the modern *structures* within number theory, as introduced by Gauss in his *Disquisitiones*. The problem that starts off this discussion is the problem of periodic decimals, i.e. the fact that fractions of two integers a and b (if b is not of the form $2^n 5^m$) have infinitely repeating periods of certain lengths, with the repeating digits in a certain order. Shanks rightly points out (pp. 53-57 & 203-4) that this problem most probably inspired the young Gauss and led him to many of the early number-theoretic discoveries that one can find in Sections I to III and Section VI (art. 309-318) of the *Disquisitiones*.¹⁶ Shanks's Chapter II is thus genetically rooted in the same problems that Gauss tackles in the early

¹⁵ Perhaps Shanks's work in the 20th century is not unlike Lejeune-Dirichlet's, who, as Kummer tells in his obituary [Kummer(1860)], never left his copy of the *Disquisitiones Arithmeticae* on the shelf and never travelled without it. Some say Dirichlet's *Vorlesungen zur Zahlentheorie* are a running commentary on the *Disquisitiones*.

¹⁶ Shanks does not provide historical evidence, but one can consult [Bullync(2008a)].

sections of his number-theoretical magnum opus. An important innovation that Shanks adds to this exposition are the cycle graphs, that visualize the ‘underlying structure’ (viz. the cycles of primitive roots resp. the finite associative groups) of a residue class modulo m , \mathfrak{M}_m . Shanks treats not only the case where m is prime (as do most textbook authors), but discusses at length the structure for composite m , parallel to articles 82 to 93 in Gauss.

An even more intense involvement with Gauss’s *Disquisitiones*, especially its Section V on quadratic forms, seems to start around 1969 when Shanks publishes an article on Gauss’s class-number problems [Shanks(1969b)]. Probably sparked by H.M. Stark’s recent result on class-number one [Stark(1966)]¹⁷ and his own work on computing class-numbers, Shanks offers an explicit rereading of the final articles of the *Disquisitiones*’ Section V, presenting a round-up of solved and unsolved problems that Gauss had formulated.

Let us first introduce some notation. A quadratic form $Ax^2 + Bxy + Cy^2$ has a discriminant $\Delta = B^2 - 4AC$; Gauss, however, writes the quadratic form as $ax^2 + 2bxy + cy^2$ with a determinant D equal to $b^2 - ac$ (thus $\Delta = 4D$). Given a quadratic form $ax^2 + 2bxy + cy^2$, or (a, b, c) in shorthand, all transformations

$$x = \alpha x' + \beta y' \quad \& \quad y = \gamma x' + \delta y'$$

$$\text{with } (\alpha\delta - \beta\gamma)^2 = 1$$

transform (a, b, c) into an equivalent quadratic form (a', b', c') with the discriminant/determinant remaining invariant. Gauss, however, introduces the additional specification that two forms are properly equivalent if $\alpha\delta - \beta\gamma = 1$, improperly equivalent if $\alpha\delta - \beta\gamma = -1$ (art. 157). Moreover, if a form is both properly and improperly equivalent to itself (which happens if a divides $2b$), it is called an ambiguous form (originally *anceps*, opposed) (art. 163 & 165).

The transformations between quadratic forms determine an equivalence relation, and thus class is defined as all forms with determinant D that can be transformed into one another. This would be the modern version. In Gauss’s version, a class is defined more narrowly, as containing all forms that are properly, resp. improperly, resp. both properly and improperly equivalent to each other (art. 223–224). Such a class may be represented by

¹⁷ The same result was obtained independently and with other methods by Baker [Baker(1966)]. Also, 15 years earlier, Kurt Heegner [Heegner(1952)] had offered a proof, but its validity had remained a point of discussion. N. Schappacher (Strasbourg), S.J. Patterson and H. Opolka (Braunschweig) are engaged in an ongoing project that studies Heegner’s *Nachlass*. They plan a book with biographical details, posthumous papers and an analysis of Heegner’s work in the near future.

the reduced form of this class.¹⁸ A modern ‘class’ can therefore either be equal to a Gauss class, or be equal to three Gauss classes.¹⁹

This distinction might seem superfluous, but it belongs to the core material Gauss needs to construct his many algorithms, devices and concepts in the theory of quadratic forms.

This distinction between proper and improper equivalences seems almost trifling, or pedantic, when one first reads it [...] Yet, it is all-important. Without this distinction, the class number comes out wrong, composition collapses, the class group disappears. [Shanks(1975b), p. 24]

The class-number $h(\Delta)$ is an integral number equal to the number of different classes of a quadratic form, having a discriminant equal to Δ . For negative discriminants/determinants ($\Delta < 0$; $D < 0$) the following hold. The class-number $h(\Delta)$ is equal to $h(D = \frac{\Delta}{4})$ if $\Delta = 8k - 1$, and is equal to $3h(D)$ if $\Delta = 8k + 3$ (articles 265, IV–VI & 303; [Shanks(1969b), p. 151–152]). If $\Delta = 8k + 5$ then, depending on the question if

$$x^2 - \Delta y^2 = 4 \quad \& \quad x \equiv y \equiv 1 \pmod{2}$$

has a solution or not, $h(\Delta) = h(D)$ respectively $h(\Delta) = 3h(D)$ [Shanks(1969a)].

Gauss puts yet another classification on top of these classes, the genera (art. 230–233). Forms with a determinant D (or discriminant $\Delta = 4D$) can represent only numbers that have a certain relationship to this D .²⁰ These relationships are called characters, and display the residuacity²¹ of these numbers modulo all factors of D and their value modulo 8 or 4. For instance, the determinant -161 (=7.23) has four genera specified by the following total characters: 1 mod 4 R7 R23; 3 mod 4 N7 R23; 3 mod 4 R7 N23; 1 mod 4 N7 N23 (art. 307). It is clear that, combinatorially exhausting the possible characters, the determinant -161 might have 8 genera, but it has only 4. This fact, that the genera of D correspond to exactly half of the possible total characters of D , has been proven by Gauss (art. 261, 263 & 287) and is now known as the *Hauptgeschlechtssatz*.

After these preliminaries on Gaussian vocabulary, we are ready to pursue Daniel Shanks’s round-up of Gauss’s class-number problems. Gauss had computed the number of genera and classes per genus for all D between 0 and -1000 [Gauss(1863-1929), II, pp. 449–476]. After giving a sample of his

¹⁸ A reduced quadratic form (p, q, r) has p smaller than q , r smaller than $\sqrt{4d/3}$ and can function as the ‘representative’ of an equivalence class. In Gauss’s original text, such reduced forms are interpreted as ‘representatives’ of their class, or as a kind of ‘shorthand’, ‘shortcut’ or ‘logarithm’, though nowadays this is easily recognized as an equivalence class.

¹⁹ If there are both proper and improper transformations, there always exist ambiguous forms, art. 165, hence always three classes.

²⁰ As a special case the coefficients of a form (a, b, c) are such numbers.

²¹ I.e., if they are a quadratic residue of p or not, abbreviated as Rp and Np, residue of p and non-residue of p .

list of genera and classes for certain negative D 's, Gauss conjectured that for each classification $A.a$ (A being the number of genera, a the number of classes per genus) there exists a finite list of D 's that have this classification (art. 303). Moreover, Gauss notices that some classifications do not occur, and particularly that 'as the number of genera increases, more classifications will disappear'. This comes down to a conjecture that as A increases, a also increases. For positive determinants, Gauss remarks that most genera have only one class, though certain have more (art. 304).

H.M. Stark had shown 1966 that indeed the modern classification $I.1$ (one genus and one class per genus) occurs only for a finite list of Δ 's, viz., only the negative discriminants 1, 2, 3, 4, 7, 11, 19, 23, 27, 31, 43, 67, 163 have class number one.²² Under Gauss's definitions, the modern $I.1$ consists of $I.1$ and part of $I.3$ (for the $\Delta = 8k + 3$). Shanks completes Stark's proof so as to match up with Gauss's original conjecture and then proceeds with the other questions and conjectures of Gauss. First of all, Shanks shows that the list of all negative determinants having class numbers $h = 6n \pm 1$ is indeed finite, and that these determinants can be constructively found. The method uses Gauss's composition of quadratic forms, the easier case (i.e. duplication), which Shanks will develop later on, or as he remarks page 159: 'Our point is that the idea of composition, used extensively above, is useful not only theoretically, but also computationally.'

Another conjecture raised by Gauss, if his and Euler's list of idoneal numbers, i.e. determinants having only one class per genus (the numbers of genera is arbitrary), is complete, remains, even after Stark and Shanks's efforts, unsettled. Shanks generalizes this question into a more modern one:

Which Abelian groups occur as composition groups for negative determinants? [Shanks(1969b), p. 156]

The question of the idoneal numbers thus becomes equivalent to the question if Abelian groups of order 2^n with $n > 4$ (being a direct product of 2-groups) occur as class groups. Yet another Gauss conjecture, as Shanks remarks, remains unsettled, viz., if the ratio of positive determinants D having class number 1 to those having a higher class number has a fixed limit as D approaches infinity.

Finally, Shanks takes up Gauss's distinction between regular and irregular determinants (art. 306, VIII), which had been largely ignored by subsequent scholarship. A principal class of determinant $-D$ is of the form $(1, 0, D) = K$. By exponentiating (i.e. repeated self-composition) this form K^m , one obtains all members of the principal class, and for a certain n , $K^n = K$. In non-principal classes, there also exist forms L that generate either the whole class or a fraction of it, and where for a certain m , $L^m = L$. If for a given determinant all m are equal to n , the determinant is regular; if the m 's divide n , irregular. Gauss gives examples of irregular negative determinants with ratios m/n equal to 2 and 3, and adds that, although no irregularity exponents over 3 occur under the determinants greater than

²² We omitted the minus for ease of writing.

-10.000, one can find determinants with arbitrary exponent beyond this limits. For positive determinants, irregulars are much rarer, though infinitely many have exponent 2, but – Gauss has to admit – he did not find an example of an irregular positive determinant equal to 3 or another odd number.

Shanks computed an example that answered the latter question, the determinant 32009 with irregularity exponent 3. As Shanks learned subsequently while the article was proofread, Gordon Pall [Pall(1936)] had already found one such example, $D = 62501$, 33 years earlier. As a matter of fact, Shanks rewords Gauss's concept of irregularity into the language of groups. E.g., the class group of Shanks's example $\Delta = 32009$ is $C(3) \times C(3) \times C(3)$, that of Pall has a class group $C(3) \times C(9)$, but both have a Gauss irregularity exponent equal to 3.²³ The examples show that Gauss's original question lacks some sophistication, and Shanks lists this as one of Gauss's 'errors' [Shanks(1989), p. 174]. The questions on irregular negative determinants are not pursued in the 1969-article, though many of Shanks's later articles, often written in collaboration, deal with these.²⁴ These studies all fall within the frame of Shanks's modernized question: Which Abelian groups occur as composition groups for negative determinants? More specific questions in this context are: How many 2-Sylow-, 3-Sylow-subgroups etc. occur, or equivalently, what is the 2-rank, 3-rank, etc. of the composition group of D ?

6 Improving on Gauss's algorithms

One of the most important points in Shanks's 1969-paper is the rediscovery of Gauss's composition of quadratic forms. As Shanks recounts,

In 1968, the Lehmers and I were looking for $Q(\sqrt{d})$ with very small or very large Dirichlet functions $L(1, \chi)$.²⁵ [...] By punching in a program, the Lehmers computed many $h(d)$ for large negative d . They used the well-known formula of Dirichlet for h as a sum of Jacobi Symbols. This requires $O(d)$ operations and a $|d|$ around 10^9 required a full day's computation. But then D.H. Lehmer used his sieve to construct some promising larger $|d|$ around 10^{12} . They no doubt had smaller $L(1, \chi)$ but each would require 1000 days computation by this method. Emma Lehmer asked me if I could think of a method to compute these large class numbers. [...] I decided that I could. [...] So this became CLASNO which computes h , the class group and the factorisation of the discriminant. [Shanks(1989), p. 176]

Used in the joint paper with the Lehmers, announced in the paper on Gauss's class number problems: CLASNO. CLASNO is Shanks's algorithm

²³ $C(n)$ is the cyclic groups with n elements.

²⁴ See [Shanks and Weinberger(1972), Shanks(1972c), Shanks and Serafin(1973), Neild and Shanks(1974), Shanks(1976)].

²⁵ This refers to [Lehmer et al.(1970)Lehmer, Lehmer and Shanks].

to compute the class number of large d 's, and takes its inspiration from Gauss's composition. It is described in the famous paper, 'Class number, a theory of factorisation, and genera' [Shanks(1971a)].

6.1 CLASNO

To compute a class number $h(d)$, as long as d is not too large, one can use a method essentially due to Lagrange, viz., compute all reduced quadratic forms having discriminant d . Alternately, one can use Dirichlet sums of Jacobi Symbols. Both procedures have a time measure $O(d)$, linear to d and become unfeasible for large d . Using the fact that the reduced forms (resp. equivalence classes) form an Abelian group under composition, Shanks devises his CLASNO that can compute a class number with $O(d^{1/4})$ operations.

A quadratic binary form $F = (A, B, C)$ is the composition of two other binary quadratic forms, $f = (a, b, c)$ and $f' = (a', b', c')$ if there exist substitutions

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$

$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

that transform F into the product ff' (art. 235). By many lengthy and involved calculations, Gauss deduces the properties of composition. Amongst them the fact that composition is associative, commutative and under what conditions determinant, order, genus and class remain invariant (art. 236–241 & 245–252). This is what Shanks calls Composition I. Now, by the properties of composition just derived, if one composes two opposite reduced forms having the same determinant (or class representatives), they are equal to a principal class which functions as unity in the class group.²⁶ More specifically, an ambiguous form (where a divides b) composed with itself gives a principal class, since an ambiguous form is opposed to itself. In shorthand, if K is an ambiguous form, $K^2 = I$ (with I a principal class).²⁷ In general again, every (reduced) form K composed with itself and iterating this process, leads to a principal form, thus there exists an m for which $K^m = I$. This iterated self-composition or exponentiation is central to the speed of Shanks's CLASNO. The second composition method, that uses the

²⁶ A principal class has a representative form $(1, 0, d)$, with $-d$ the determinant

²⁷ Gauss writes composition as an addition, $K + K = 2K = I$, because he considers the operation as a shortcut for multiplication, hence the logarithm of a multiplication which is addition. Poulet-Delisle's French translation of the *Disquisitiones* (1807) changes the addition sign into a multiplication sign, a change generally adopted by later writers. Shanks poses the not uninteresting and so far unsolved historical question if this change is due to Gauss or to the French translators [Shanks(1989), p. 168–169]. As papers from Gauss's *Nachlass* [Gauss(1863-1929), II, pp. 269–291] show (which Shanks apparently never checked), Gauss used his addition sign upto 1834, so the change is most likely due to the translators.

group structure of the equivalence classes (reduced forms) in the form of either composition of opposite classes or the exponentiation of ambiguous classes (all having the same determinant) is Composition II (art. 242–243 & 257–259). As Shanks admits, ‘I did not need the representations of Composition I, and I therefore merely modified Composition II. In fact, I did not even read Gauss’s Composition I.’ [Shanks(1989), p. 194]

First of all, Shanks gives a routine to calculate the easy composition, only bothering about the class of the composed form, not of its representation.²⁸ This algorithm, COMPOS, computes F_1F_2 , with $F_1 = (A_1, B_1, C_1)$ and $F_2 = (A_2, B_2, C_2)$, taking [Shanks(1971a), 434–435]

$$D = \gcd(A_1, A_2) \quad ; \quad S = \frac{1}{2}(B_1 + B_2) \quad ; \quad N = B_2 - S$$

$$\text{and } D_1 = \gcd(D, S)$$

Take $V_1 = A_1/D_1$, $V_2 = A_2/D_1$ and $X = C_2D_1$. Compute the solutions to the indeterminate linear equations:

$$A_2Y_1 - A_1X_1 = D \quad ; \quad SX_2 - DY_2 = D_1$$

Put $R = Y_1Y_2N - X_2C_2 \pmod{V_1}$. Then, finally, the composed form (A_3, B_3, C_3) can be calculated:

$$A_3 = V_1V_2 \quad ; \quad B_3 = B_2 + 2V_2R \quad \text{and} \quad C_3 = (X + R(B_2 + V_2R))/V_1$$

This yields an efficient composition algorithm, especially if F_1 equals F_2 .

CLASNO now proceeds as follows. One computes solutions B_p of

$$-\Delta \equiv B_p^2 \pmod{p}$$

for each p , obtaining quadratic forms (p, B_p, C_p) , with $\Delta + B_p^2 = 4pC_p$ and having discriminant $-\Delta$.²⁹ The stock of forms thus obtained is used to compute the class number, the class group and factorisations of Δ .

Now use an estimate H of the class number h , and express it in binary. Now, the class number h is equal to the largest exponent n for which $K^n = I$ for a given K with determinant D . The binary representation makes clear that one mainly needs to repeatedly square a form $F_p = (p, B_p, C_p)$, to obtain F_p^H , since F_p^H can be written as the sum of $F_p^{2^m}$'s. On each recursive step, the form G_n should be reduced. Here again, Shanks indicates an efficient reduction method, that essentially is Gauss’s (art. 188–9), but goes back to Lagrange. If F_p^H is a principal form I then H is the class number h , if not, one can use the first s powers n of F_p that are still in store to compute the right h by trial-and-error. Either one such F_p^n is equal to F_p^H

²⁸ Remark that Shanks uses discriminants in the following algorithm, not Gauss’s determinants.

²⁹ Shanks also devised an efficient routine to do this, which is not in Gauss, viz. RESSOL and QUPAPR. This was published only in 1972 and immediately upgraded to SQROAP [Shanks(1972a)].

or will be equal to a F_p^{H+2sr} (computed in steps $2s$), this gives a form F_p^{H-n} resp. $F_p^{H+2sr-n}$ equal to I . This is known as the baby steps (the n 's going per 1), giant steps (the r 's going per s) algorithm, though – from a different perspective – it is also analogous to Gauss's trial-and-error procedure to compute primitive roots modulo p (art. 73–74).³⁰ This procedure gives the right class number. Using the first part of this same algorithm (the squaring part) with other forms F_p , one can obtain smaller cycles of length e , that are the p -Sylow-subgroups of the class group with $h/e = p^i$.

Since in this way, one is able to determine the 2-Sylow-subgroups of the class group, one can compute the ambiguous classes (or reduced forms F_a) of discriminant $-\Delta$ that are exactly the 2-Sylow-subgroups, because $F_a^2 = I$. These ambiguous classes have either the form $(A, 0, C)$, (A, A, C) , or (A, B, A) which determine all factorisations of Δ , viz. $\Delta = 4AC$ or $\Delta = A(4C - A)$, or $\Delta = (2A - B)(2A + B)$. Using the structure of the class groups obtained earlier (or in the algorithm: at the same time), it becomes possible to factor a given number Δ in $O(\Delta^{1/4})$ operations. Although the coefficient to $O(\Delta^{1/4})$ is rather large (due to the expensive composition and euclidean algorithm), this algorithm is superior to the classical sieve method, either Eratosthenes's or the quadratic sieve, once the numbers are larger than a certain limit value. The old sieve methods have $O(\Delta^{1/2})$ with a small coefficient (due to optimisations of the methods), and are thus more efficient for smaller numbers.

6.2 GATESR

Daniel Shanks did not restrict his reading of the *Disquisitiones* to the part on composition, but also went through the part on ternary forms. Gauss added this part rather late in the process of publishing the *Disquisitiones* (the years 1798–1799) mainly to provide a proof for the important theorem that the genera of a quadratic form with determinant d correspond to exactly half of the possible characters of d . Gauss's theory of ternary quadratic forms is very condensed, contains many long calculations, and brings an outline of the theory of ternary forms, constructed parallel to the extensive one on binary forms.

Shanks's factorisation method, imbedded in CLASNO, assumes the class number h and its class group can be computed in a realistic time frame. For very large numbers, this may not be the case, but using Gauss's theory on ternary forms, it is possible to gather information on the 2-Sylow subgroups without computing h or the complete class group. One needs, however, the complete factorisation of Δ in advance. To get at the 2-Sylow-part of the

³⁰ There, one computes the complete powers of a few small numbers, say 2^n , 3^n modulo p (these are the baby steps), determines their periods (that are divisors of p) and then combines them into a new number q which has a period equal to the least common multiple of the small number periods. Repeating this combination (going in giant steps), one rather quickly obtains a primitive root of p .

class group, one needs the ambiguous forms only, or in Gauss's terms, one needs the square root of the principal class, i.e., a form F with $F^2 = I$ (art. 268). In Gauss's set-up, computing the square roots of the principal class determines all genera, an important step towards proving his principal genus theorem.

First, Gauss expands his binary quadratic form into a ternary one,

$$t = a_1x^2 + a_2y^2 + a_3z^2 + 2b_1yz + 2b_2xz + 2b_3xy$$

that should have a determinant D

$$D = b_1^2a_1 + b_2^2a_2 + b_3^2a_3 - a_1a_2a_3 - 2b_1b_2b_3$$

equal to $+1$.³¹ To compute these extra terms, Gauss goes on to define an adjoint form of t , $t^A = T$, fulfilling the relationship $(t^A = T)^A = t$. This adjoint form gives a set of relations from which one can calculate a_3, b_1, b_2 [Shanks(1971b), p. 841]. This is the first subroutine of the algorithm GATESR (for GAUSS TERNARY SQUARE ROOT) which Shanks calls COMTAT.

A second subroutine turns the ternary form t into an equivalent one of the form $x^2 - yz$. Essentially, the algorithm (art. 271–273) is the equivalent for ternary forms of the reduction of binary quadratic forms, in fact, it even makes use of the algorithm of binary forms. The algorithm is an intricate but elegant one, bearing the mark of Gauss's craftsmanship in devising computational procedures. Given a ternary form

$$t = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

calculate its adjoint

$$T = \begin{pmatrix} A_1 & A_2 & A_3 \\ B_1 & B_2 & B_3 \end{pmatrix}$$

The binary quadratic form imbedded in t is $f = (a_1, b_3, a_2)$. Reduce this embedded form f using the Lagrange-Gauss procedure to f' . Expand this again to a ternary form t' , calculate its adjoint T' and then take the binary form embedded in the adjoint, $F' = (A_3, B_1, A_2)$. Reduce this binary form into an equivalent one F'' , and recalculate the corresponding ternary form t'' and its adjoint T'' . Alternate this procedure until

$$a_1^{(n)} \leq \sqrt{\frac{4}{3}A_2^{(n)}} \quad \text{and} \quad A_2^{(n)} \leq \sqrt{\frac{4}{3}a_1^{(n)}D}$$

This is the reduced ternary form.

Shanks adapts this algorithm, simplifying some steps and throwing away some information not needed for obtaining the ambiguous forms. Since Shanks only needs ternary forms with D equal to $+1$, he can spell out an

³¹ Gauss abbreviates a ternary form to $\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$.

‘endgame’, listing the five possible outcomes of the algorithm [Shanks(1971b), p. 843]. With these modifications, Shanks baptises the second part of his GATESR-algorithm GAURED for GAUSS REDuction [Shanks(1971b), pp. 842–843].

6.3 Further applications of CLASNO: The infrastructure

The algorithm CLASNO, or in general: the rediscovery of composition, found many further applications in Shanks’s later work in the 70ies. Just as GATESR investigates the 2-Sylow-subgroups, one can investigate other p -Sylow-subgroups by looking not at the structure of the class group, but at the structure of the equivalence classes making up the class group. This comes down to investigating periods of forms that are not in the principal class. Instead of studying the structure of a principal form $K^n = I$, with n the class number, one can study smaller periods that occur within the non-principal genera, where $K^m = I$, with m dividing n . Shanks calls this the infrastructure of the class group.³² These ideas about infrastructure were used in an algorithm for computing the regulator of a quadratic field [Shanks(1972b)].

In 1975 Shanks started to work on an analysis of Morrison and Brillhart’s factoring algorithm. In 1969-1970, Morrison and Brillhart had taken up an old algorithm developed by D.H. Lehmer and R.A. Powers [Lehmer and Powers(1931)], refined it, adapted it meticulously to a digital computer and had used it (amongst other things) to show that the seventh Fermat number ($2^{2^7} - 1$) is composite [Morrison and Brillhart(1975)]. The algorithm was formulated in the language of continued fractions, and Shanks tried to translate the ideas behind the algorithm into quadratic forms to analyze and improve it.

Shanks’s analysis, though of value in itself, had missed an important point of Morrison and Brillhart’s algorithm and could thus not improve upon it, as Brillhart pointed out to Shanks upon receiving a first draft of the analysis [Shanks(1975a)]. However, the analysis and the discussion led Shanks to think about infrastructure and squares occurring in the continued fraction expansion. Ultimately, Shanks devised a new algorithm, rethinking the algorithm and using the information generated by the structure of quadratic classes, it is called SQUFOF [Shanks(1975b)]. Again, the algorithm embeds many of Gauss’s rediscovered concepts: Composition, periods of principal and non-principal classes, ambiguous forms and the square root of a principal class.³³

³² One might note that Gauss gives a sketch of these ideas in articles 305–308. His idea is to investigate the structure of the forms with determinant D by looking at the periods of reduced quadratic forms in the different genera.

³³ I thank John Brillhart for his comments on this section.

7 Composition again

One of Daniel Shanks's last papers is entitled 'On Gauss and Composition' [Shanks(1989)] and is a very sympathetic overview of his involvement with Gauss's *Disquisitiones*. In a way, this paper is an essay towards a larger study on Gauss, a study announced in the 3rd edition of Shanks's *Solved and unsolved problems in number theory* as well as in this paper. The study unfortunately never materialized, but the fragments gathered in this 1989-paper still offer a fascinating panorama.

The paper, in two parts, is an emphatic defense of what Shanks calls Gauss's greatest discovery, and – we might add - Shanks's greatest rediscovery: The composition of quadratic forms. The first part of the paper gives an overview of Gauss's composition and lists arguments why composition is so important, although it has often been neglected by mathematicians. The second part is a research paper, recurring again on the COMPOS-algorithm.

The COMPOS-algorithm, based upon Gauss's Composition II, runs in $O(\Delta)$ time, with Δ the discriminant. Shanks endeavours to bring the composition algorithm down to $O(\sqrt{\Delta})$ time. To obtain this running time, he assembles an ingenious 2 times 4 matrix that intrinsically contains all information on the forms to be composed, but avoids to process this information (i.e. to multiply and add them) until necessary, to keep the numbers smaller. This restriction is dictated by the computer: This algorithm needs only single-precision words, not double- or multi-precision words, and can thus be implemented without further ado on any computer or calculator.³⁴

We have the following 2×4 -matrix [Shanks(1989), p. 181]:

$$M = \begin{pmatrix} a & b & c & d \\ e & f & g & h \end{pmatrix}$$

Through the entries and the determinants of the minors of this matrix, both the composed form $F = (A_3, B_3, C_3)$ as its two constituent forms, $f = (A_1, B_1, C_1)$ and $f' = (A_2, B_2, C_2)$ (with $F = ff'$) are accessible. We have on the one hand:

$$A_3 = ab + cd \quad , \quad C_3 = ef + gh \quad , \quad B_3 = af + be + ch + dg$$

And on the other hand, with $|M_{ij}|$ the minor of the i -th and j -th column of M :

$$A_1 = |M_{14}| \quad , \quad A_2 = |M_{24}|$$

$$C_1 = |M_{23}| \quad , \quad C_2 = |M_{13}|$$

$$B = (B_2 - B_1)/2 = |M_{12}| \quad , \quad B' = (B_2 + B_1)/2 = |M_{34}|$$

³⁴ Let us note that the names of Shanks's algorithms are restricted in the same way by the devices used: They are all six-letter-combinations, corresponding to the storage space reserved for a file or routine name on a HP-25 hand calculator.

How now to assemble this matrix? Using the same notations as above for the forms f and f' that are to be composed, one starts with a matrix [Shanks(1989), pp. 185–9]:

$$\mu = \begin{pmatrix} A_1 & A_2 & B & 0 \\ \alpha & \beta & \gamma & 1 \end{pmatrix} \quad \text{with} \quad B = (B_1 + B_2)/2$$

The minors that output A_1, A_2 and B already work, but we should get the minors working that output C_1, C_2 or B' . Thus, e.g. $A_1\gamma - B\alpha = C_2$, one solves this indeterminate equation using the euclidean algorithm and gets γ and α . Using one more equation one easily determines β . This matrix already contains the unreduced composition of f and f' . Taking the C_3 and B_3 coefficients of this unreduced form, one applies the euclidean algorithm on B_3/C_3 recording the quotients n_i . By multiplying the second row of μ with n_1 and subtracting the first row one gets a third row, again, multiply this third row by n_2 and subtract the second row. Iterate this process until the n_i run out. The last two rows that are obtained constitute the matrix M , containing the coefficients of f, f' and the reduced composed form F .

After explaining this new composition algorithm, baptized NUCOMP, Shanks returns to the topic of his paper, Gauss. He suggests the NUCOMP algorithm embeds some of the features of Gauss's Composition I [Shanks(1989), p. 184]. This is indeed the case: The third conclusion of Gauss's art. 235 states that the coefficients of (a, b, c) , i.e. the first form entering into the composition, are in proportion to the minors of the substitution operations that compose ff' into F . This quite exactly matches up with Shanks's matrix.

8 Conclusion: We all admire Gauss

Summarizing, it was the publication of Gauss's *Werke*, containing many materials from the *Nachlass*, especially the many tables, that initially renewed the interest in Gauss's work. Philipp Maennchen in Germany, J.C.A. Cunningham in the U.K. and R.C.A. Archibald and D.H. Lehmer in the U.S. played an important role in increasing the recognition of the computational aspect of Gauss's work. Although this aspect of Gauss had never been completely forgotten, even more, that many 19th century mathematicians commented on or complained about 'tedious, complicated calculations and deductions' (Eisenstein as quoted in [Schmitz(2004)]), Gauss's computations lay more or less buried under the many 19th and 20th century developments in mathematics. E.g., as Daniel Shanks pointed out in the 1970ies, the composition of binary quadratic forms was a rather badly known method, abandoned in favour of (amongst others) ideal theory.

The efforts of R.C.A. Archibald and D.H. Lehmer, promoting work on mathematical tables and constants, and editing the journal *Mathematical Tables and other Aids to Computation* cleared the way for a generation of mathematicians to become involved with computational number theory.

The invention of digital computers, only two years after the first issue of this journal, added even more impetus to this development. Thus, the U.S. knew a continuous interest in and development of computational number theory from the 1930ies onwards, ultimately leading up to the present prominence of the mathematics of computation.

The recognition and refinement of Gauss's methods went hand in hand with this development. Amongst them, one may cite improvements on the relaxation method Gauss described to Gerling [Forsythe and Motzkin(1952)] and the rediscovery of the fast fourier transformation by Cooley and Tukey but already present in a 1805-*Nachlass*-paper by Gauss on interpolation [Heidemann et al.(1984)Heidemann, Johnson and Burrus]. In number theory, Gauss's arctangent formulae to compute π and the factoring methods by exclusion moduli were exploited and improved. Often, these improvements adapted Gauss's methods to the peculiarities of the computers used (the binary notation, the parallelism).

The most continuous and insistent exploitation of Gauss's *Disquisitiones Arithmeticae* is due to Daniel Shanks. Many topics, but seldomly discussed in the literature, were excavated, and turned into performative algorithms. Especially the composition of quadratic binary forms got into the focus of research again. Shanks's lecture of Gauss's magnum opus in many ways also restored this text to its original meanings: Periodic decimals, factoring, distribution of numbers of certain forms, calculation of periods of quadratic forms, classification issues in quadratic forms ... All these problems are at the heart of Gauss's writing and research, but have sometimes been obscured by subsequent work that focused on related though different problems.

References

- [Archibald(1948)] Archibald, R. (1948), *Mathematical Table Makers. Portraits, Paintings, Busts, Monuments, Bio-Bibliographical Notes*, Scripta Mathematica Studies 3, Scripta Mathematica.
- [Baker(1966)] Baker, A. (1966), "Linear forms in the logarithms of algebraic numbers", *Mathematika*, 13, pp. 204–216.
- [Bullynck(2008a)] Bullynck, M. (2008a), "Decimal Periods and their Tables: A Research Topic (1765-1801)", 30pp., accepted for publication in *Historia Mathematica*.
- [Bullynck(2008b)] — (2008b), "From Anatomia Numerorum to Higher Arithmetics A History of Factor Tables with Notes on the Birth of Number Theory 1668-1817", 68 pp., submitted to *Revue d'histoire des mathématiques*.
- [Burckhardt(1814)] Burckhardt, J. K. (1814), *Table des diviseurs pour tous les nombres du deuxième million, ou plus exactement depuis 1020000 à 2028000, avec les nombres premiers qui s'y trouvent*, Courcier, Paris.
- [Chowla and Todd(1949)] Chowla, S. D. and Todd, J. (1949), "The density of reducible integers", *Canadian Journal of Mathematics*, 1, pp. 297–299.
- [Clippinger(1948)] Clippinger, R. F. (1948), *A Logical Coding System Applied to the ENIAC*, BRL 673, Ballistic Research Laboratories, Aberdeen Proving Ground.

- [Corry(2008)] Corry, L. (2008), “Number crunching vs. number theory: computers and FLT, from Kummer to SWAC (1850–1960), and beyond”, *Archive for the History of Exact Sciences*, URL <http://www.springerlink.com/content/47wpg1878r26h6hr>.
- [Cunningham and Woodall(1925)] Cunningham, A. J. C. and Woodall, H. J. (1925), *Factorisation of $y^n \pm 1$, $y = 2, 3, 4, 5, 6, 7, 10, 11, 12$ up to high powers (n)*, Hodgson, London.
- [Dickson(1919–1927)] Dickson, L. (1919–1927), *History of the Theory of Numbers*, Carnegie Institute, Washington, 3 Vol.
- [Fenster(2007)] Fenster, D. (2007), “Gauss Goes West: The Reception of the *Disquisitiones Arithmeticae* in the USA”, in: “The Shaping of Arithmetic after C. F. Gauss’s *Disquisitiones Arithmeticae*”, , edited by Goldstein, C.; Schappacher, N. and Schwermer, J., pp. 463–479, Springer.
- [Forsythe(1951)] Forsythe, G. E. (1951), “Gauss to Gerling on relaxation (Translation)”, *Mathematical Tables and Other Aids to Computation*, 5 (36), pp. 255–258.
- [Forsythe and Motzkin(1952)] Forsythe, G. E. and Motzkin, T. S. (1952), “An extension of Gauss’s transformation for improving the condition of systems of linear equations”, *Mathematical Tables and Other Aids to Computation*, 6 (37), pp. 9–17.
- [Gauss(1801)] Gauss, C. F. (1801), *Disquisitiones Arithmeticae*, Fleischer, Leipzig, reprint Culture et Civilisation, Bruxelles 1968 (also *C.F. Gauss, Werke*, volume I).
- [Gauss(1863-1929)] — (1863-1929), *Werke*, Göttingen, 12 volumes, reprint Hildesheim, New York, 1973.
- [Gauss(1965)] — (1965), *Disquisitiones Arithmeticae*, Yale University Press, New Haven, London, translation of *Disquisitiones Arithmeticae* (1801) by A.A. Clarke, 1965.
- [Glaisher(1878)] Glaisher, J. (1878), “On factor tables, with an account of the mode of formation of the factor table for the fourth million”, *Proceedings of the Cambridge Philosophical Society*, 3, pp. 99–138.
- [Goldstein and Schappacher(2007)] Goldstein, C. and Schappacher, N. (2007), “Several Disciplines and a Book (1860–1901)”, in: “The Shaping of Arithmetic after C. F. Gauss’s *Disquisitiones Arithmeticae*”, , edited by Goldstein, C.; Schappacher, N. and Schwermer, J., pp. 67–104, Springer.
- [Goldstine and Goldstine(1946)] Goldstine, H. and Goldstine, A. (1946), “The Electronic Numerical Integrator and Computer (ENIAC)”, *Mathematical Tables and Other Aids to Computation*, 2 (15), pp. 97–110.
- [Gruenberger(1952)] Gruenberger, F. (1952), “Further statistics on the digits of e ”, *Mathematical Tables and Other Aids to Computation*, 6 (38), pp. 123–124.
- [Heegner(1952)] Heegner, K. (1952), “Diophantische Analysis und Modulfunktionen”, *Mathematische Zeitschrift*, 56, pp. 227–253.
- [Heidemann et al.(1984)] Heidemann, Johnson and Burrus] Heidemann, M. T.; Johnson, D. H. and Burrus, C. S. (1984), “Gauss and the history of the fast Fourier transform”, *IEEE ASSP Magazin*, 1 (4), pp. 14–21.
- [Hindenburg(1776)] Hindenburg, C. (1776), *Beschreibung einer ganz neuen Art, nach einem bekannten Gesetze fortgehende Zahlen, durch Abzählen oder Abmessen bequem und sicher zu finden, nebst Anwendung der Methode auf verschiedene Zahlen, besonders auf eine darnach zu fertigende Factorentafel, mit eingestreuten, die Zahlenberechnung überhaupt betreffenden Anmerkungen*, Crusius, Leipzig.

- [Hoffleit(1949)] Hoffleit, D. (1949), “A Comparison of Various Computing Machines Used in the Reduction of Doppler Observations”, *Mathematical Tables and Other Aids to Computation*, 3 (25), pp. 373–377.
- [Johnston and Miller(1946)] Johnston, S. and Miller, J. C. P. (1946), “Tables of $TAN^{-1}(m/n)$ ”, *Mathematical Tables and Other Aids to Computation*, 2 (15), pp. 147–148.
- [Knuth(1969)] Knuth, D. E. (1969), *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, Addison-Wesley, New York, third edition. Addison-Wesley, 1997.
- [Kraitchik(1922)] Kraitchik, M. (1922), *Théorie des Nombres*, Gauthier-Villars, Paris.
- [Kummer(1860)] Kummer, E. E. (1860), “Gedächtnissrede auf Gustav Peter Lejeune-Dirichlet”, in: “G. Lejeune Dirichlet’s Werke”, , edited by Kronecker, L. and Fuchs, L., vol. 2, pp. 309–343, Georg Reimer.
- [Legendre(1798)] Legendre, A.-M. (1798), *Essai sur la Théorie des nombres*, Courcier, Paris, 2nd revised Ed. 1808, 3rd revised Ed. 1830.
- [Lehmer(1928)] Lehmer, D. H. (1928), “The Mechanical Combination of Linear Forms”, *American Mathematical Monthly*, 35 (3), pp. 114–121.
- [Lehmer(1933a)] — (1933a), “A machine for combining sets of linear congruences”, *Mathematische Annalen*, 109, pp. 661–667.
- [Lehmer(1933b)] — (1933b), “A Photo-Electric Number Sieve”, *American Mathematical Monthly*, 40 (7), pp. 401–406.
- [Lehmer(1938)] — (1938), “On Arccotangent Relations for π ”, *American Mathematical Monthly*, 45 (10), pp. 657–664.
- [Lehmer(1941)] — (1941), *Guide to Tables in the Theory of Numbers*, no. 105 in Bulletin of the National Research Council, National Research Council, Washington, D. C., committee on Mathematical Tables and Aids to Computation, Report 1: Report of the Subcommittee on Section F: Theory of Numbers.
- [Lehmer(1948)] — (1948), “The lemniscate constant”, *Mathematical Tables and Other Aids to Computation*, 3 (23), pp. 550–551.
- [Lehmer(1950)] — (1950), “J. Todd, “A problem on arctangent relations” (Review)”, *Mathematical Tables and Other Aids to Computation*, 4 (30), p. 85.
- [Lehmer(1953)] — (1953), “The Sieve Problem for All-Purpose Computers”, *Mathematical Tables and Other Aids to Computation*, 7 (41), pp. 6–14.
- [Lehmer(1969)] — (1969), “Interview with Derrick H. Lehmer, 8 October 1969, interviewed by Uta Merzbach”, Interview transcript, Computer Oral History Collection, 1969–1973, Archives Center, National Museum of American History.
- [Lehmer(1973)] — (1973), “Interview with Derrick H. Lehmer, 18 April 1973, interviewed by Robina Mapstone”, Interview transcript, Computer Oral History Collection, 1969–1973, Archives Center, National Museum of American History.
- [Lehmer and Lehmer(1974)] Lehmer, D. H. and Lehmer, E. (1974), “A new factorization technique using quadratic forms”, *Mathematics of Computation*, 28 (126), pp. 625–635.
- [Lehmer et al.(1970)Lehmer, Lehmer and Shanks] Lehmer, D. H.; Lehmer, E. and Shanks, D. (1970), “Integer Sequence having prescribed quadratic character”, *Mathematics of Computation*, 24 (110), pp. 433–451.
- [Lehmer and Powers(1931)] Lehmer, D. H. and Powers, R. E. (1931), “On factoring large numbers”, *Proceedings of the National Academy of Sciences*, pp. 770–776.

- [Lehmer(1926)] Lehmer, D. N. (1926), “On the construction of factor stencils”, *Bulletin of the American Mathematical Society*, 32 (2), pp. 149–150.
- [Lehmer(1927)] — (1927), “A theorem on factorization”, *Bulletin of the American Mathematical Society*, 33 (1), pp. 35–36.
- [Lehmer(1929)] — (1929), “An announcement regarding factor stencils”, *Bulletin of the American Mathematical Society*, 35 (5), pp. 684–686.
- [Maennchen(1918)] Maennchen, P. (1918), “Gauss als Zahlenrechner”, in: “C. F. Gauss Werke”, vol. X/2 (Ergänzungsband), Göttingen.
- [Metropolis et al.(1950)Metropolis, Reitwiesner and von Neumann] Metropolis, N.; Reitwiesner, G. and von Neumann, J. (1950), “Statistical Treatment of Values of First 2,000 Decimal Digits of e and of π Calculated on the ENIAC”, *Mathematical Tables and Other Aids to Computation*, 4 (30), pp. 109–111.
- [Miller(1946)] Miller, J. C. P. (1946), “Tables of $TAN^{-1}(m/n)$ ”, *Mathematical Tables and Other Aids to Computation*, 2 (13), pp. 62–63.
- [De Mol and Bullynck(2008)] De Mol, L. and Bullynck, M. (2008), “A week-end off. The first extensive number-theoretical computation on the ENIAC”, in: *Computability in Europe 2008 Logic and Theory of Algorithms Logic and Theory of Algorithms, Fourth Conference on Computability in Europe, CiE 2008, Athens, Greece, June 2008, Proceedings*, edited by Beckmann, A.; Dimitracopoulos, C. and Löwe, B., vol. 5028 of *Lecture Notes in Computer Science*, pp. 121–131.
- [Morrison and Brillhart(1975)] Morrison, M. A. and Brillhart, J. (1975), “A method of factoring and the factorization of F7”, *Mathematics of Computation*, 29 (129), pp. 183–205.
- [Neild and Shanks(1974)] Neild, C. and Shanks, D. (1974), “On the 3-rank of quadratic fields and the Euler product”, *Mathematics of Computation*, 28, pp. 279–291.
- [von Neumann(1951)] von Neumann, J. (1951), “Various techniques used in connection with random digits”, *Monte Carlo Method*, National Bureau of Standards, Applied Mathematics Series 12, 36–38. Also in *Collected Works*, Vol. 5, Pergamon Press, New York, 1963, 768–770.
- [Pall(1936)] Pall, G. (1936), “Note on irregular determinants”, *Journal of the London Mathematical Society*, 11, pp. 34–35.
- [Parshall and Rowe(1994)] Parshall, K. H. and Rowe, D. E. (1994), *The emergence of the American mathematical research community, 1876-1900 : J. J. Sylvester, Felix Klein, and E. H. Moore*, American Mathematical Society, Providence.
- [Polachek(1995)] Polachek, H. (1995), “History of the journal Mathematical Tables and other Aids to Computation, 1959-1965”, *Annals of the History of Computing IEEE*, 17 (3), pp. 67–74.
- [Putnam(1939)] Putnam, T. M. (1939), “Derrick Norman Lehmer – In Memoriam”, *Bulletin of the American Mathematical Society*, 45 (3), pp. 209–212.
- [Reitwiesner(1950)] Reitwiesner, G. (1950), “An ENIAC Determination of π and e to more than 2000 Decimal Places”, *Mathematical Tables and Other Aids to Computation*, 4 (29), pp. 11–15.
- [Sarton(1956)] Sarton, G. (1956), “Raymond Clare Archibald”, *Osiris*, 12, pp. 4–34.
- [Schmitz(2004)] Schmitz, M. (2004), “The life of Gotthold Ferdinand Eisenstein”, *Res. Lett. Inf. Math. Sci.*, 6, pp. 1–13.

- [Shanks(1959)] Shanks, D. (1959), “A Sieve Method for Factoring Numbers of the Form $n^2 + 1$ ”, *Mathematical Tables and Other Aids to Computation*, 13 (66), pp. 78–86.
- [Shanks(1960)] — (1960), “On the conjecture of Hardy and Littlewood concerning the number of primes of the form $n^2 + a$ ”, *Mathematics of Computation*, 14 (321–332).
- [Shanks(1963)] — (1963), “Supplementary data and remarks concerning a Hardy-Littlewood conjecture”, *Mathematics of Computation*, 17, pp. 188–193.
- [Shanks(1969a)] — (1969a), “Class Number of Primes of the Form $4n + 1$ by K. E. Kloss; M. Newman; E. Ordman (Review)”, *Mathematics of Computation*, 23 (105), pp. 213–214.
- [Shanks(1969b)] — (1969b), “On Gauss’s Class Number Problems”, *Mathematics of Computation*, 23 (105), pp. 151–163.
- [Shanks(1971a)] — (1971a), “Class number, a theory of factorization, and genera”, in: “Proceedings of the 1969 Summer Institute on Number Theory”, , edited by Lewis, D., vol. 20 of *Symposia in Pure Mathematics*, pp. 415–440, American Mathematical Society, Providence.
- [Shanks(1971b)] — (1971b), “Gauss’s Ternary Form Reduction and the 2-Sylow Subgroup”, *Mathematics of Computation*, 25 (116), pp. 837–853, corrigenda in *MoC 32* (144), Oct. 1978, 1328–1329.
- [Shanks(1972a)] — (1972a), “Five number-theoretic algorithms”, in: “Proceedings of the second Manitoba conference on numerical mathematics”, , edited by Thomas, R. and Williams, H., vol. 7 of *Congressus Numerantium*, pp. 51–72, Utilitas Mathematica, Winnipeg.
- [Shanks(1972b)] — (1972b), “The infrastructure of a real quadratic field and its applications”, in: “Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)”, pp. 217–224.
- [Shanks(1972c)] — (1972c), “New types of quadratic fields having three invariants divisible by 3”, *Journal of Number Theory*, 4, pp. 537–556.
- [Shanks(1975a)] — (1975a), “Analysis and improvement of the continued fraction method of factorization”, URL web.usna.navy.mil/wdj/mcmath/, unpublished manuscript, typed into latex by Stephen McMath, March 2004.
- [Shanks(1975b)] — (1975b), “SQUFOF notes”, URL web.usna.navy.mil/wdj/mcmath/, unpublished manuscript, typed into latex by Stephen McMath, March 2004.
- [Shanks(1976)] — (1976), “Class groups of the quadratic fields found by F. Diaz y Diaz”, *Mathematics of Computation*, 30 (133), pp. 173–178, corrigenda in *MoC 30* (136), p. 900.
- [Shanks(1989)] — (1989), “On Gauss and composition. I & II”, in: “Number Theory and Applications”, , edited by Mollin, I., pp. 163–184, Kluwer Academic Publishers, Dordrecht.
- [Shanks(1993)] — (1993), *Solved and unsolved problems in number theory*, Chelsea, New York, (1st ed., Spartan Books, Washington, DC, 1962).
- [Shanks and Serafin(1973)] Shanks, D. and Serafin, R. (1973), “Quadratic fields with four invariants divisible by 3”, *Mathematics of Computation*, 27, pp. 183–187, corrigenda in *MoC 27*, p. 1012.
- [Shanks and Weinberger(1972)] Shanks, D. and Weinberger, P. (1972), “A quadratic field of prime discriminant requiring three generators for its class group, and related theory”, *Acta Arithmetica*, 21, pp. 71–87.
- [Shanks and Wrench(1962)] Shanks, D. and Wrench, J. W. (1962), “Calculation of π to 100,000 Decimals”, *Mathematics of Computation*, 16 (77), pp. 76–99.

- [Shanks and Wrench(1963)] — (1963), “The calculation of certain Dirichlet series”, *Mathematics of Computation*, 17, pp. 136–154.
- [Stark(1966)] Stark, H. M. (1966), “On complex quadratic fields with class-number equal to one”, *Transactions of the American Mathematical Society*, 122, pp. 112–119.
- [Todd(1947)] Todd, J. (1947), “Tables of $TAN^{-1}(m/n)$ ”, *Mathematical Tables and Other Aids to Computation*, 2 (18), pp. 287–288.
- [Todd(1949)] — (1949), “A Problem on Arc Tangent Relations”, *American Mathematical Monthly*, 56 (8), pp. 517–528.
- [Todd(1975a)] — (1975a), “The lemniscate constants”, *Communications of the ACM*, 18 (1), pp. 14–19.
- [Todd(1975b)] — (1975b), “Numerical Analysis at the National Bureau of Standards”, *SIAM Review*, 17 (2), pp. 361–370.
- [Williams(1997)] Williams, H. C. (1997), “Daniel Shanks (1917–1996)”, *Mathematics of Computation*, 66 (219), pp. 929–934.
- [Wrench(1938)] Wrench, J. W. (1938), “On the Derivation of Arctangent Equalities”, *American Mathematical Monthly*, 45 (2), pp. 108–109.
- [Wrench(1947)] — (1947), “A new approximation to π ”, *Mathematical Tables and Other Aids to Computation*, 2 (18), pp. 245–248.
- [Wrench(1948)] — (1948), “C. F. Gauss Werke v.3 1866 “De curva lemniscata”, p.413–432 (Errata)”, *Mathematical Tables and Other Aids to Computation*, 3 (23), pp. 201–203.
- [Wrench(1950)] — (1950), “C. .F. Gauss, “Tafel zur Verwandlung gemeiner Brüche mit Nennern aus dem ersten Tausend in Decimalbrüche”, Werke p.2, p. 412–434 (Errata)”, *Mathematical Tables and Other Aids to Computation*, 4 (32), pp. 222–223.