Modular Arithmetics before C.F. Gauss.

Maarten Bullynck

Modular Arithmetic before C.F. Gauss. Systematisations and discussions on remainder problems in 18th century Germany

Maarten Bullynck

IZWT, Bergische Universität Wuppertal, Gaußstraße 20, 42119 Wuppertal, Germany
Forschungsstipendiat der Alexander-von-Humboldt-Stiftung
Email: Maarten.Bullynck@kuttaka.org

Abstract

Remainder problems have a long tradition and were widely disseminated in books on calculation, algebra and recreational mathematics from the 13th century until the 18th century. Many singular solution methods for particular cases were known, but Bachet de Méziriac was the first to see how these methods connected with the Euclidean algorithm and with Diophantine analysis (1624). His general solution method contributed to the theory of equations in France, but went largely unnoticed elsewhere. Later Euler independently rediscovered similar methods, while von Clausberg generalised and systematised methods which used the greatest common divisor procedure. These were followed by Euler's and Lagrange's continued fraction solution methods, and Hindenburg's combinatorial solution. Shortly afterwards, Gauss, in the *Disquisitiones Arithmeticae*, proposed a new formalism based on his method of congruences and created the modular arithmetic framework in which these problems are posed today.

2000 Mathematics Subject Classification: 01A50; 11A05; 11D04

Key words: Remainder problems, modular arithmetic, euclidean algorithm, Euler, Hindenburg, Gauss

1 Introduction: Remainder Problems

There is a certain class of elementary mathematical problems involving division and remainders [1] that has, for example, the following form:

> There are an unknown number of things. Three by three, two remain; five by five, three remain; seven by seven, two remain. How many things? [Li and Shen, 1987, 93]

This example from Sun Tzu's *Suan Ching* belongs to an old tradition in Chinese mathematics. A general rule to solve these problems (*tái yen*), the oldest extant formulation being in Sun Tzu's work in the 3rd or 4th century A.D., was proposed on the basis of special cases [Dickson, 1919–1927; Li and Shen, 1987, II, 57–59; 92–94]. An affiliated though different rule, called *kuttaka* (the pulveriser), was known in 7th century India [Srinivasiengar, 1967, 95–109]. Because the earliest example of this general rule comes from ancient China, the general solution method to this class of problems is today called the Chinese Remainder Theorem.

This paper traces the tradition of this kind of problem and some affiliated ones, which we will call remainder problems. After a short discussion of the origins and transmission of these problems in Western traditions, we will discuss the first general framework created to deal with them, that of Claude Gaspard Bachet de Méziriac (1624). We will then mainly focus upon their treatment in 18th century Germany. Many systematisations were attempted, first by Christlieb von Clausberg (1732) and Leonhard Euler (1734), and later, in the last third of the century, by Joseph Louis Lagrange and Abraham Kästner, and by Euler again. These last three recognised the central role of the greatest common divisor algorithm in solving remainder problems and thereby provided a general framework, essentially equivalent to Bachet's, in which to treat them. Remarkably, however, at the end of the 1700s two other formally different general frameworks were created, the first by Carl Friedrich Hindenburg in the context of Diophantine problems, and the second by Carl Friedrich Gauss in his *Disquisitiones Arithmeticae*.

The analysis of these frameworks will not only show how a rather disconnected collection of textbook remainder problems was integrated into a general theory, but also how discussions on theoretical and computational issues played a role in the invention of new frameworks, in this case discussions on the application range of the Euclidean algorithm and on the efficiency of its computa-

[1] In this text I deal only with the case of linear remainder problems, not with the quadratic case or with power residues. Modular arithmetic in the title should thus be understood as (linear) modular arithmetic. For the history of power residues, in particular the strand pertaining to decimal periods, see [Bullynck, 2008b].

tion. Finally, it will also shed some new light on the discourses that nurtured Gauss's *Disquisitiones Arithmeticae*, especially its second section, thus allowing a richer understanding of the environment in which Gauss's treatise was written and of one of Gauss's significant innovations, modular arithmetic.

2 From *Rechenbücher* and recreational mathematics to 18th century Textbooks

2.1 Examples and first instances of remainder problems

In continental Europe, remainder problems show up for the first time in medieval manuscripts on calculation, perhaps through the mediation of Italian merchants returning from China, perhaps through Arabic translations of Indian sources. The oldest extant problems in the Latin tradition can be found in Leonardo Pisano's *Liber Abaci*. Pisano's examples are particular instances of the Chinese Remainder Problem, presented as 'tricks' to guess a number someone has in mind. By asking the person to give the remainders of their chosen number after division by 3, 5 and 7, the number is found by forming the products of the respective remainders with 70, 21 and 15, adding these up and keeping the remainder of this number after division by 105 [Pisano, 1202, 428–9]. Another problem of the same kind is the egg-woman problem. An unknown number of eggs are broken, and by grouping the remaining eggs by 2, 3, 4, 5, 6 and 7, and registering the remainders (1, 1, 1, 1, 1, 0), the question is, how many eggs are left? [Pisano, 1202, 402–403]. [2] Similar 'tricks' are described for other divisors, but proofs and a general procedure are lacking.

Pisano's examples were copied by other writers, often with the same numbers, sometimes with different numbers, and sometimes with some explanation on how to find the multiplicands (70, 21 and 15 in the above example). As previously collected data on several of these remainder problems show [3], examples exist in Italian algebra books, French, Dutch and German books of calculation, and in Cossist works of the 15th and 16th centuries. During this period there seems to have been little or no attempt at generalisation and almost no novel solutions were produced, with one notable exception: Michael Stifel's

[2] Pisano formulates this problem without the narrative. Note that this problem introduces the added difficulty, that the problem can have no solutions (since the divisors are not relatively prime).

[3] See [Tropfke, 1980, 636–642] and David Singmaster's *Sources in recreational mathematics. An annotated bibliography*, 8th preliminary edition. The part on arithmetic problems, including a long list of Chinese remainder problems through the ages, is available at http://us.share.geocities.com/mathrecsources/7.htm.

rule. Christoph Rudolff's *Coss* [1525] contains some of the first occurrences of Pisano's problems in Germany (after the *Algorismus Ratisbonensis*, a 15th century *Rechenbuch* [Vogel, 1954]). In 1553 Michael Stifel published a new enhanced edition of Rudolff's *Coss*, not only reproducing the original text, but adding long commentaries and new examples. One of these additions contains a general rule for a specific remainder problem. Again, this problem is put in the form of guessing a number by its remainders, and involves two divisors, α and $\alpha + 1$ (thus relatively prime), and two remainders. The solution is obtained as follows: multiply the smaller divisor's remainder with the larger divisor, then add the product of the remainder of the larger divisor with the square of the smaller divisor, and lastly calculate the remainder of this sum after division by the product of two divisors [Stifel, 1553, 15^v – 16^r]. [4]

An affiliated class of problems, known under the rule for their solution, is the *regula coeci* (rule of the blind) or the *regula virginum* (rule of the virgins), a different form of which is known as the hundred fowls problem. Again the origin of these problems is not completely clear; Leonardo Pisano has some examples on alloying metals [Pisano, 1202, 240–257]. One of the forms that would later become classic in German books, but which was often found in 15th and 16th century works, is the tavern-problem (also known as *Zechrechnen*). [5] This problem is of the following form, the specific example given here being derived from Adam Riese (1544),:

> A group of 20 persons, men, women and virgins, drink in a tavern, together they spend 18 Thaler. The men drink for 3 Thaler a person, the women for 2 Thaler and the virgins for half a Thaler. How many men, women and virgins were in the drinking party? [6]

In modern terms, this type of problem leads to two linear equations to be solved in integers, but involving three unknowns. [7] The problem, if fractional and negative solutions are excluded, can have a finite number of solutions, an infinite number of solutions or no solutions. After deriving equations in one

[4] The problem can also be found in Stifel's *Arithmetica Integra* [1544, book I fol. 38^v]. From the algebraic form of this solution, $r_1(\alpha + 1) + r_2\alpha^2$ (r_1, r_2 being remainders, α being the divisor), it is immediately clear that after division by α, r_1 is left over, and after division by $\alpha + 1$ (because of the alternate form $r_1(\alpha + 1) + r_2.(\alpha^2 - 1) + r_2$) r_2 is left over.

[5] See the previously quoted David Singmaster's *Sources in recreational mathematics. An annotated bibliography*, 8th preliminary edition. The part 7.P.1 "Hundred Fowls and other linear problems" lists this and affiliated questions.

[6] Adapted from [Riese, 1522, 104–106], 1544 edition.

[7] The three unknowns add up to a given number n, thus this problem can be reformulated as a partition of the number n with restrictions. In this case, $20 = x + y + z$ with restriction $36 = 6x + 4y + z$. This form is present in Diophantus's work, as indicated in section 2.2 on Bachet.

parameter (say t) from the problem (either in words or in symbolic form), most books describe a trial-and-error process. Setting t to 1, 2, 3, etc. and checking whether the sum of the unknowns becomes equals to a number n (in the example 20) leads in a limited number of steps to a solution. In the example given above, the triple $(1, 5, 14)$ satisfying the problem is found.

2.2 Remainder problems in recreational mathematics

In the 17th century, books on recreational mathematics came into vogue, starting with Claude Gaspard Bachet de Méziriac's *Problèmes plaisans et delectables* [1612] in France, and Daniel Schwenter's *Mathematische Erquickstunden* [1636], edited by G. Ph. Harsdörffer from Schwenter's papers in Germany. These books contained problems from the Italian algebra books, German Cossist books, as well as manuals of arithmetic, for the diversion of the readership. Remainder problems were a particular class of problems that were always included in these works.

Bachet, in his *Problèmes plaisans et delectables*, relied upon many earlier books, notably Chuquet's *Le Triparty en la Science des Nombres* [1484], as sources for his problems. In its turn his book became the source and model for nearly all subsequent books on recreational mathematics. These include the *Récréations Mathématiques* [Leurechon, 1624] which was the main source for Schwenter's and Harsdörffer's *Deliciae Physico-Mathematica* [1636] and William Leybourn's *Pleasure with Profit* [1694]. [8] These recreational mathematic books mostly kept the rhetorical framework of the problems (the narrative) and described the solution not in symbolic or algebraic terms but in words. In this respect, the books on recreational mathematics provide an important link in the transmission of remainder problems from the 16th century into the 18th century, though they seldomly add anything new to the original formulations and solutions, and often (because of the sole reliance on words) made the solution less transparent.

However, Bachet's work is the notable exception to this rule. Bachet was also the translator and commentator of Diophantus's *Arithmetica*, published 1621 [Bachet, 1621]. This work is well-known to have triggered Pierre de Fermat's interest in Diophantine problems. Interest in these problems then spread in the mathematical community of Western Europe through Fermat's correspondance with various other mathematicians (1636-1660) and through his notes in Bachet's translation, posthumously edited by his son. [9] In the second edition

[8] See [Heeffer, 2006] for a detailed study of the *Récréations Mathématiques* [1624] often ascribed to Jean Leurechon. The paper also contains much information on Bachet's sources.

[9] See e.g. [Weil, 1984, Ch. 3], or for a more modern treatment [Goldstein, 2004].

of the *Problèmes plaisans et delectables* in 1624, Bachet did not restrict himself to the problems and their solutions, but added notes (*Advertissements*), discussing and generalising the problems, as well as providing proofs of the solutions and indicating connections with the work of Euclid and Diophantus. To this end, Bachet, in his introduction, included 26 propositions that served him as building blocks for the proofs. Moreover, Bachet comments extensively upon the solution methods in his sources, shedding light upon the earlier perception of these problems.

Bachet's Problem 6 is exactly Pisano's example of the Chinese Remainder problem, described at the beginning of section 2.1. As Bachet reveals in his *Advertissement* to this problem, he omitted the proof of the solution in the first edition,

> because I did not want to expand it [the book] with 12 propositions, that I have been forced to add, just for this topic alone, & because I expect to publish one day my *Elemens Arithmetiques*, from which I drew these propositions. [Bachet, 1624, 88] [10]

The solution of this problem is actually a transliteration of the 'word-version' of the problem. Using algebraic letters within a running text, Bachet explains every step of the procedure, relying on a construction to find a number that is a multiple of A and B and surpasses by one a multiple of C (using the 20th proposition stated in the introduction). Bachet then uses the 24th and 25th propositions (that if a given number after division by b leaves a, one can subtract b's from this number and after division by b it will still leave a) [Bachet, 1624, 85–7]. In the *Advertissement* Bachet discusses 'proofs' given by Forcadel in his annotations to Gemma Frisius's *Arithmetica Practica* (published 1582) and by G. Gosselin in his translation of Tartaglia's *De Arte Magna* (published 1577). Forcadel only proves the case where the difference between the two divisors is one (i.e. Stifel's case), whereas Gosselin, according to Bachet, proves nothing [Bachet, 1624, 87–88].

Bachet's propositions in the introduction as well as his comment in the *Advertissement* (explaining why it is necessary to use divisors that are relatively prime and how to find them) refer constantly to Euclid's *Elements*, books VII to IX. The crucial proposition, Euclid VII, 2, to find the greatest common divisor (g.c.d.) of two numbers that are relatively prime (nowadays known as the Euclidean algorithm) [11] is invoked to prove Bachet's propositions 18 and

[10] Original: "à cause que ie ne voulus pas le grossir des douze propositions, que i'ay esté constraint d'y aiouster, presque pour ce seul subject, & que ie pensois de publier au premier iourmes Elemenis Arithmetiques [sic], dont i'ay tiré lesdictes propositions."

[11] The ancient Greek called this procedure *anthyphairesis*. For the transmission of this procedure from the Greek to the Islamic mathematicians in the Middle Ages

20 [Bachet, 1624, 18–24]. In proposition 20, Bachet constructs a solution to the problem of finding a multiple of $n-1$ numbers that exceeds by a unit an n^{th} number (all numbers relatively prime). Proposition 18 is the first general solution to the linear Diophantine problem $ax - by = 1$ (a and b relatively prime). Essentially this proposition comes down to applying the Euclidean algorithm to a and b, keeping track of the remainders and quotients (which Bachet does using letters), until the algorithm stops and the g.c.d. 1 is arrived at, and then working back up again until a solution of the form $1 = ax - by$ is reached. Because the process is arithmetically complex and often rather tedious, Bachet also suggests a simple trial and error procedure, namely, generating multiples of a until the total is one more than a multiple of b.

The problems added to the second edition include more remainder problems. Two of these [Bachet, 1624, 199–206] are egg-woman problems. Bachet gives the general structure of the solution referring to Problem 6 and proposition 18, but adds that the trial-and-error procedure is usually faster. He also comments upon the additional difficulty that the divisors are not relatively prime, but remarks that since division by 2, 3, 4, 5, 6, 7 leaves 1, 1, 1, 1, 1, 0 (in the second example 1, 2, 3, 4, 5, 0), it suffices that 7 is relatively prime to the other divisors. It is thus sufficient to find a multiple of 2, 3, 4, 5 and 6 that exceeds by one (in the second example, is one less than) a multiple of 7 [Bachet, 1624, 200; 204]. Bachet credits this shortcut to Cardano in his *Practica Arithmetica* (1539), but is critical of the fact that it comes down to a *petitio principii* because Cardano gives no general procedure to find a multiple of a that exceeds a multiple of b by one [Bachet, 1624, 201–202]. Bachet also notes that neither Sfortunat, Tartaglia nor Cardano found a general rule to solve the second problem, and that Sfortunat even claimed it was impossible to find a solution [Bachet, 1624, 204]. It must be added, that Bachet does not give (even implicitly) a general criterium for the (im)possibility of a solution to this problem.

The final additional problem, the last in the book, belongs to the *regula virginum* class [Bachet, 1624, 237–247]. Prior to Bachet this question had tortured many mathematicians (among them Tartaglia and Etienne de la Roche) all of whom failed to find a general solution and had to restrict themselves to the trial-and-error solution given above. Bachet, however, remarks that this problem is related to the 41st question of the 4th book of Diophantus, and proceeds to solve it using the method described in his translation of Diophantus [Bachet, 1621, 261–6]. Bachet introduces a *Racine* (an unknown x in modern terms) into the problem corresponding to the number of persons paying the most. After some manipulations he arrives at:

thus we have in algebraic terms the number of men equal to 1 Rac., the

see [Hogendijk, 2002].

number of women equal to $9\frac{7}{8}1\frac{3}{2}$ Rac. that of children equal to 31 $\frac{1}{8}$ + $\frac{3}{8}$ Rac. of which the sum is exactly 41 [Bachet, 1624, 240] [12]

Setting the *Racine* equal to a number gives one of many solutions, although one has to check for 'impossible' solutions, i.e., negative solutions and – in certain cases – fractional solutions (since half a man is no man).

This final additional problem in Bachet's text marks the arrival of the algebraic method that will be dominant for the rest of the 17th century and all of the 18th century.

2.3 Bachet's reception in French and English algebra books and its absorption in the theory of equations (a brief sketch)

Bachet's work on the linear Diophantine equation $ax - by = 1$ was transmitted mainly in new algebra textbooks, appearing in France and England during the 17th and 18th century. In these works, the link with the older remainder problems slowly disappears, and the references are rather to Diophantus and to the then emerging general theory of equations. Also, the indeterminate equations figure marginally by comparison with determinate equations, they serve more as examples for the power of the algebraic method than as a topic *per se*. Among these books are John Kersey's *Elements of Algebra* [1673], Michel Rolle's *Traité d'algebre* [1690] and Thomas Simpson's *A Treatise of Algebra* [1745]. [13] The authors of these books pursued the algebraisation of the problem, eventually linking it up with the important theory of equations, and adding their comments on Bachet's solution method. Kersey called the method "tedious and obscure" and returned to the trial-and-error method of forming multiples, which Bachet himself had proposed [Kersey, 1673, 301]. Rolle sticks to the solution method, but makes it somewhat clearer and points out that it is advantageous to use the lesser of the two numbers as the divisor.

Variants on Bachet's methods were given by Thomas Fantet de Lagny in his *Analyse Générale; ou méthodes nouvelles pour résoudre les problèmes de tous les Degrez à l'infini* [1733], posthumously edited by Richet, and by the blind mathematician Nicholas Saunderson in his *Elements of algebra* [1740]. The latter devised a scheme that avoids the double work of first finding the divisors and then substituting them again. Instead, Saunderson starts from two equations $1A - 0B = p$ and $0A - 1B = q$, the quotient of p and q determining how many times to subtract the second equation from the first. This process is

[12] Original: "par ainsi nous avons en termes Algebriques le nombre des hommes qui est 1.Rac. celuy des femmes qui est $9\frac{7}{8}1\frac{3}{2}$ Ra. Celuy des enfans 31 $\frac{1}{8}$ + $\frac{3}{8}$ Rac. dont la somme est iustement 41."

[13] See [Dickson, 1919–1927, II, 45–46].

then repeated with $0A - 1B = q$ and the new equation and so on. Eventually, this leads to an equation of the form $aA - bB = \pm 1$ [Saunderson, 1740, 275–279].

De Lagny's treatise is an ambitious work emphasising computational issues, and proposing a general method for solving equations numerically, both determinate and indeterminate. To this end, he develops a general theory of relations between two numbers (*théorie des rapports*). He points out that all relations between two integers a and b are based on the numbers generated by the g.c.d. procedure (i.e. the quotients and remainders) applied to a and b [Lagny, 1733, 523–530]. Using this insight, he develops his *triangle des rapports*, that lists all the quotients and remainders of two numbers, and generalises the idea to all quantities, using infinite series [Lagny, 1733, 552–568]. In modern terms, Lagny (re-)invents the method of continued fractions to approximate the relation between any two numbers which occur in the solving of equations. He also indicates the limits of accuracy, if such a triangle is broken off at a certain point, giving estimates of the error involved [Lagny, 1733, 568–575]. [14]

Using *triangles des rapports*, de Lagny proceeds to solve the linear Diophantine case, including Chinese Remainder problems, and examples of the *regula virginum* (actually Diophantus's problems from Book 4) [Lagny, 1733, 587–595; 602–607]. Given the equation $y = (ax + q)/p$, Lagny applies the g.c.d. procedure in the following way. Reduce a and q to a' and q' so that they are smaller than p (i.e. modulo p), then divide px by $a'x + q'$ and write the remainder down, $a''x + q''$. Then, divide $a'x + q'$ by $a''x + q''$ and write down the remainder, and so on, until a remainder of the form $x + q^{(n)}$ is reached. The solution for x is then $-q^{(n)}$. For examples of the *regula virginum*, Lagny uses his procedure twice for the equations $y = (ax + q)/p$ and $z = (ax + q)/p$ and then checks if they have solutions in common. Lagny seems to be one of the first to apply Euclid's procedure to equations (with integer coefficients).

Finally, in France, Etienne Bézout made Bachet's solution method for the linear Diophantine equation part of a general theory of equations. Bézout had included problems of the form $ax - by = c$ as examples of the application of algebra to arithmetic in his famous textbook series *Cours de Mathématiques* [Bézout, 1766, 118–121]. Later on, in the process of writing his general theory of equations [15], Bézout generalised Bachet's identity $ax + by = \pm 1$ (there exists integer solutions to this equation if a and b are relatively prime) to polynomials: if $P(x)$ and $Q(x)$ are two polynomials, then there exist two other polynomials $A(x)$ and $B(x)$ such that $A(x)P(x) + B(x)Q(x) = g.c.d(P, Q)$,

[14] Shallit [1994, 404–405] remarks that de Lagny also comments on the worst case of the g.c.d. scheme, some hundred years before Lamé.
[15] See [Alfonsi, 2007].

when $P(x)$ and $Q(x)$ are relatively prime.[16] This identity is now commonly known as Bézout's identity.

2.4 Remainder problems in early 18th century Germany: Early Systematisations

Although Bachet connected the tradition of remainder problems with the Diophantine (and more generally, ancient Greek) tradition, in Germany these two lines of tradition remained rather separated during the 17th century and for most of the 18th century. The remainder problems remained accessible to a larger public in Cossist works, manuals of arithmetic (*Rechenbücher*) and in works on recreational mathematics, but work on Diophantine problems, or on the theory of equations were rather rare or were published in academic journals or books which did not refer to the more common remainder problems.

Thus, the group of remainder problems remained largely a fragmented set of specific problems, often reproduced and often solved in a way that suggested a more general procedure to solve the whole class. However, their embedding in recreational works and their spurious appearance in *Rechenbücher* obscured this more general procedure, as witnessed in a striking letter from H.W.M. Olbers, the Altona astronomer, to C.F. Gauss, dated 26 Nov. 1810 [Schilling and Kramer, 1900, I, 460]:

> Recently I discovered, on leafing through Schwenter's *Mathematische Erquickstunden*, a piece of paper with my handwriting [...] It dealt with Schwenter's arithmetical recreation of the so-called pronic numbers. Schwenter shows how to guess every number smaller than $a^2 + a$ if one is given the remainders of both divisions, i.e., if one divides it first by a and then by $a + 1$. Schwenter's procedure to find this number is very impractical and tedious, because he needs two multiplications, an addition and a cumbersome division; on the bit of paper was shown how a subtraction, a multiplication and an addition suffice.[17]

[16] Independently, Gauss had written down the same result in 1796 in his scientific diary [Gauss, 1863-1929, X, 500]. He included the result in the section on the general theory of congruences (section VIII), originally planned to be part of the *Disquisitiones Arithmeticae*, but only published posthumously [Gauss, 1863-1929, II, 215].

[17] The full quote in the original: "Neulich fiel mir, da ich von ungefähr Schwenter's "Mathematische Erquickstunden" durchblätterte, die ich schon von meiner Jugend her besitze, ein Papier in die Hände, das ich wenigstens schon vor 35 Jahren beschrieben oder vielmehr bekritzelt hatte, und das mir ganz wieder aus dem Gedächtniss gekommen war. Nur mit Mühe konnte ich mir den Inhalt der Zahlen und Formeln enträthseln. Es betraf die von Schwenter angegebene arith-

Olbers indicates that the exercise can be generalised easily but that there was unfortunately nobody in his environment at that time (c. 1775) who could further his study of such problems.

Olbers's experience was not an isolated one and could even be termed characteristic for the average reader in late 17th and early 18th century Germany. In most 17th century books reproducing remainder problems, there was no effort to elucidate the solution method nor to systematise and/or generalise the results. This situation changed in the early 18th century with the publication of Christian Wolff's influential *Anfangsgründe aller mathematischen Wissenschaften* [1710], a book that programmatically called for more systematisation. Two salient points in this program were: 1) reduction of the many special rules; 2) proof of the remaining rules within arithmetic. [18] Most of the early textbooks inspired by Wolff's approach did not cover remainder problems, since these belonged to the 'special cases'. One exception to this stands out, Christlieb von Clausberg's *Demonstrative Rechenkunst worinnen gemeine und kaufmännische Rechnungsarten* [1732]. Around the same time, the young Leonhard Euler, as a child arithmetically socialised with Stifel's edition of Rudolff's *Coss* [1553] [19], devoted one of his contributions to the St Petersburg *Commentarii* to an essay in systematising remainder problems [Euler, 1734/5].

Christlieb (sometimes Christian) von Clausberg (1689–1751) was a *Rechenmeister* who studied in Danzig, then taught in Hamburg, Lübeck and Leipzig

---

metische Belustigung mit den sogenannten Proniczahlen. Schwenter lehrt, wie man jede Zahl, die kleiner ist als a^2+a errathen kann, wenn man sie erst mit a, und dann mit $A+1$ divideren [sic], und sich die beiden Ueberreste der Division angeben lässt. Schwenter's Verfahren, die Zahl zu finden, ist sehr unbequem und weitläufig, da er zwei Multiplikationen, eine Addition und eine beschwerliche Division gebraucht; auf dem Papier war gezeigt, dass man mit einer Subtraktion, einer Multiplikation und einer Addition ausreiche. Ueberdem hatte ich schon damals bemerkt, dass diese Eigenschaft, durch die Reste zweier Divisionen die Zahl zu bestimmen, gar nicht auf die Proniczahlen beschränkt sei, sondern dass man jede Zahl errathen könne, die kleiner ist als $a^2 + ap$, wenn man sie mit ma und mit $na + np$ dividiren, und sich die beiden Reste angeben lässt, wobei m, n, a, und p willkührlich sind, nur muss a und p keine gemeinschaftlichen Faktor haben. – Ich führe Ihnen dies Unbedeutende nur an, um zu zeigen, dass ich vielleicht in früher Jugend, wenigstens vor 34 oder 35 Jahren, eine Neigung zur höheren Arithmetik hatte, die nur durch einen Lehrer wie Sie hätte unterhalten und ausgebildet werden müssen. ".
The reference is to [Schwenter and Harsdörffer, 1636, I, 41]. This is of course the problem that can be solved with Stifel's rule.

[18] For an account of Wolff's desiderata and some topics that were influential on the style of 18th century German textbooks, see [Müller, 1904, 68–72]. For specific issues on the presentation of arithmetic operations [Bullynck, 2008a; Sterner, 1891, 323–347].

[19] See Euler's autobiography in [Fellmann, 1995, 11].

before entering the services of the Danish king in Copenhagen [ADB, 1875-1912, 4, 285]. His *Demonstrative Rechenkunst worinnen gemeine und kaufmännische Rechnungsarten* first published in 1732 in four parts was often reprinted during the 18th century. It is virtually encyclopedic and it presents the content of many *Rechenbücher* of previous centuries in an orderly and precise manner. In it, Clausberg adopts the demonstrative manner upon which Christian Wolff had insisted:

> I have deemed it necessary [...], to teach in my book arithmetic in the *demonstrative* way, i.e., *convincing* and with complete *certainty*. This is displayed by the word *Science* that I use in the title. [Clausberg, 1732, Introduction] [20]

However, Clausberg did not proceed exactly in Wolff's rigid manner, but rather provided intuitively convincing arguments, or transpositions into algebraic terms, to account for the validity of the rules. Nevertheless, his work was still an advance on that of earlier writers in Germany.

In spite of Wolff's desideratum, that the mass of arithmetic rules should be reduced, Clausberg endeavoured to include all the tricks and rules advantageous in arithmetic, "allerhand vortheilhafte Rechnung" [Clausberg, 1732, Introduction]. Among these are a number of rules to solve particular remainder problems, all included in the fourth part. Due to the encyclopedic character of the work, Clausberg reproduced older problems and variants including their solution methods prior to introducing his newer perspectives. He solves two cases of the Chinese Remainder Problem with two divisors (div. 8, 10 and rem. 7, 7; div. 7, 15 and rem. 0, 10) by trial-and-error first concluding that this method is successful in the first case, but "einen harten Knoten" (a difficult knot to untie) in the second case [Clausberg, 1732, §1343]. [21] In a later section, however, he introduces a more general treatment of these problems. In §1491 Stifel's rule is described and proven, and the next paragraph refers to the problems treated earlier and includes the remark that it is possible "to find [these numbers] not by mere trying out, but by regulated calculation" [Clausberg, 1732, §1492]. [22] The principle regulating these calculations is the procedure for finding the g.c.d. which Clausberg explains without proof and without reference to Euclid.

Similarly, Clausberg solves examples of the *regula virginum* by trial-and-error

[20] Original: "So habe ich es vor höchst nöthig erachtet [...], die Rechenkunst auch in meinem Buche *demonstrativ*, das ist *überführend* und mit völliger *Gewißheit* vorzutragen. Eben dieses zeiget das Wort *Wissenschaft* an, dessen ich mich im Titel bediene."

[21] Cases with more than two divisors do not appear in Clausberg.

[22] Original: "dass nicht durch blosses Tentiren, sondern regulirte Rechnung [solche Zahlen] auszufinden sind"

[Clausberg, 1732, §1355 – §1366], remarking that because there are an infinity of solutions, it is difficult to find the desired answer, "or it has to be blindly by pure coincidence, hence the old Arithmeticians have called this Coeci or Blind Calculation." [Clausberg, 1732, §1356]. [23] However, Clausberg finds the correct viewpoint, remarking that the problem of partition (*Zerstreuung*) of numbers is intimately connected with these problems, though difficult to solve in all generality [Clausberg, 1732, §1360]. Although Clausberg did not add much theoretically to the solving of remainder problems, he was one of the first German writers to bring some systematic perspective to these problems.

Mathematically much more interesting is a paper by the young Euler, written 1734/5, published 1740. In this paper, "Solutio problematis arithmetici de inveniendo numero qui per datos numeros divisus relinquat data residu" [Euler, 1734/5] [24], Euler collects problems from the 'recreative' and the *Rechenbuch*-traditions ("vulgaribus arthmeticorum libris"). His aim is to get rid of the many special rules (some even false), and to perfect the method of solution, just as Lahire and Sauveur had done for problems on magic squares [Euler, 1734/5, 18]. The problems Euler concentrates on are all variants of Chinese Remainder problems, the *regula virginum* is not one of his objectives. His exposition is clear and is a considerable advance on that of earlier writers (except Bachet, whom Euler apparently does not know).

Euler starts by showing how problems with many divisors depend on the solution of the problem with two divisors. He then proceeds to show how the algorithm to find the g.c.d. correlates with the solution of the case with two divisors (see Figure 1), and that (when working with integers) the series of remainders in the algorithm must produce either 0 or 1. Euler proves that the remainder thus found is indeed the g.c.d., using the property that the g.c.d. of a remainder and a divisor is also the g.c.d. of the divisor and the dividend [Euler, 1734/5, 19–22]. Euler also points out the advantage of using negative numbers to reduce calculations, e.g., taking the remainder -1 instead of the remainder that is one less than the divisor. He then shows how to use the case with two divisors to solve cases with many divisors. In this respect, his exposition is more general than that of Bachet.

[include Figure 1 (EulerCRT.ps) with caption here]

After some examples, Euler explains how this general method for solving (Chinese) remainder problems can produce special rules. With reference to Stifel [1553], Euler derives an even more general form of Stifel's rule. Instead of divisors a and $a + 1$ Euler takes a and $na + 1$ which leads to the formula:

[23] Original: "es müßte denn blindlings hin und von ohngefehr geschehen; als hat es den alten Arithmeticis beliebet, dieselbe Cöci oder Blindrechnung zu benamen."
[24] Translation of the title: Solution of arithmetic problems where a number has to be found that leaves given remainders after division by given divisors .

$x = mna^2 + ma + (na + 1)q - nap$, with q remainder of the sought number x after division by a and p remainder after division by $na + 1$; m is a parameter that generates for each value $(=\ldots, -2, -1, 0, 1, 2, \ldots)$ a solution x [Euler, 1734/5, 27–29]. Another classic example follows: find a number that leaves 1 after division by 2, 3, 4, 5, 6, and 0 when divided by 7 [Euler, 1734/5, 30].

As a final classic example, Euler considers the formula for the Julian year [Euler, 1734/5, 30]. The problem is to find the year in the Gregorian calendar corresponding to the year in the Julian calendar. To this end, Clavius, who was one of the architects of the calendar reform (1579–1583), had devised a table in which, for every Julian year, three numbers were listed: indiction, lunar and solar cycle. Using these numbers, the corresponding Gregorian year could be retrieved in another table. John Wallis [1656-1657, II, 451–5] had empirically derived the following formula from the tables: 6916 Ind. + 4200 Lun. Cycl. + 4845 Sol. Cycle (modulo 7980). [25] However, since indiction, lunar and solar cycle indicate a position in a returning (circular) order [26], the problem can be seen as a remainder problem involving three divisors, which is exactly how Euler saw it and, using the formulae he derived earlier, he proved Wallis's formula.

The paper ends with a general solution for the problem of finding a number that has remainders $p, q, r, \ldots$ after division by $a, b, c, \ldots$ (relatively prime). This solution is

$$Ap + Bq + Cr + \ldots + mabc\ldots$$

where A is the number that leaves 1 (respectively 0) after division by a (respectively $bc\ldots$) [Euler, 1734/5, 31]. This formula, which Euler never mentioned in any other work, would later be included in the works of Hindenburg and Gauss, who apparently never saw Euler's paper. [27]

3 The second half of the 18th century: On the role of the Euclidean algorithm

In 1767 Lagrange published the first of a series of articles on Diophantine quadratic problems. Improving on Euler's work, Lagrange gave a general so-

[25] Note that England only adopted the Gregorian Calendar in 1753.
[26] Indiction was a Roman tax cycle.
[27] Well before Euler, William Beveridge in his *Instutionum Chronologicarum* [1669] includes a derivation of the formula for three divisors and a treatment of calendar problems. Beveridge proceeds neatly along Euclidean lines and, as Bachet had done before him, adds some extra axioms to prove that the g.c.d.-based solution method answers the Chinese remainder problem [Beveridge, 1669, 252–257].

lution method for Pell's equation $x^2 - Dy^2 = a$. This was the most important Diophantine problem in the second half of the 18th century. Pierre de Fermat and John Wallis (with Brouncker) had given solutions for special cases, but it was only during 1765-1770 that both Euler and Lagrange came up with a general solution. Both noticed, as Wallis and Brouncker had done for a restricted case, that the development of $\sqrt{D}$ in continued fractions (using the substitution $x = a + \frac{1}{y}$) solved the problem. The series of convergents towards the square root of D, say $\frac{m}{n}, \frac{m'}{n'}, \ldots$, produced pairs $(m, n), (m', n'), \ldots$ that satisfied the equation. Euler's first solution was through successive substitutions [Euler, 1765/7], Lagrange's solution was through an equivalent of these substitutions expressed in continued fractions [Lagrange, 1767a; 1768], the substitutions $p_0 = a_0p_1 + p_2$; $p_1 = a_1p_2 + p_3$; ... corresponding to the continued fraction $\frac{1}{a_0+\frac{1}{a_1+\frac{1}{\ddots}}}$. Recursively filling in all substitutions, or finding the smallest common denominator for the continued fraction, ultimately gives the n^{th} solution. This solution method brought coherence to the treatment of both linear and quadratic Diophantine equations with two unknowns. In the linear case $px - qy = n$, the series of substitutions and continued fractions end if p_n becomes 0. In the quadratic case, the coefficients become periodic.

Apart from substitutions and continued fractions, Euler introduced another slightly different formalism, midway between substitions and continued fractions: $(a_0, a_1, \ldots)$, where the a_n have the same meaning as above. At first sight this new formalism appears to be an abbreviation of the substitution (or continued fraction) formalism. However, it contains only relevant information (the p_n's are left out) and at the same time avoids the typographical disaster of long diagonally proceeding continued fractions. Furthermore, its straightforward form, amounting to a horizontally smoothed continued fraction, allows for some simple and practical formulae that can be easily memorised:

(v, a, b, c, d, e) = v (a, b, c, d, e) + (b, c, d, e),
(v, a, b, c, d, e) = (v, a) (b, c, d, e) + v (c, d, e),
(v, a, b, c, d, e) = (v, a, b) (c, d, e) + (v, a)(d, e),
(v, a, b, c, d, e) = (v, a, b, c) (d, e) + (v, a ,b) (e) [Euler, 1765/7, 92]

Finally, fractional notation can be used, $\frac{(v,a,b,c,d,e)}{(a,b,c,d,e)}$, to indicate the successive approximations to a solution. [28]

In his follow-up paper, Lagrange stresses that he is the first to solve the quadratic case, with the help of his beloved continued fractions, but he also reflects on the solution for the linear case ($px - qy = n$) [Lagrange, 1767b, 659–661; 696–699] and remarks:

[28] Today Euler's (and Gauss's) notational procedure is called a *continuant*. For a modern treatment of continuants see [Graham et al., 1994, 301–309]. These authors remark that Euler's procedure is essentially the same as de Lagny's.

> M. Bachet is, as we have remarked before, the first to have solved the preceding problem; his method, though independent of continued fractions, comes down to essentially the same thing as the method we have just presented; and, in general, all other methods that other Geometers have imagined after him reduce to the same principles. [Lagrange, 1767b, 698] [29]

Earlier in the same text, Lagrange draws a parallel between Bachet as the solver of the linear case of Diophantine equations and himself as the solver of the quadratic case.

In general, it seems that Lagrange was well acquainted with earlier work on the linear Diophantine case, although the sparsity of references in Lagrange's work forbids positive confirmation. As Dickson [1919–1927, II, 46] remarks, Lagrange repeated Saunderson's procedure in a later essay written at the Ecole Polytechnique [Lagrange, 1798, 307–309]. Moreover, the general idea behind de Lagny's computational perspective in his *théorie générale des rapports*, seems to herald much of Lagrange's approach. Both in handling Diophantine questions and in his numerical methods to solve equations, Lagrange relied heavily on continued fractions, exactly as de Lagny had relied on his *rapports*.

3.1 Euler's and Kästner's textbooks

Euler's and Lagrange's work clearly showed how to solve the linear Diophantine equation and explained the role played by the Euclidean algorithm in its solution. This helped to stabilise the presentation of the solution, and later when two widely read and reprinted textbooks including remainder problems appeared, they each systematised the problems in a similar way, i.e., by showing their connection with indeterminate (Diophantine) linear problems through use of the g.c.d. procedure. [30] The first of these textbooks is Euler's famous *Algebra* [1770], the second is the first additional volume to the first part of Kästner's series *Anfangsgründe der Mathematik* [1786]. [31] Again, these

[29] Original: "M. Bachet est, comme nous l'avons déjà remarqué, le premier qui ait résolu le Problème précédent; sa méthode, quoique indépendante des fractions continues, revient cependant au même pour le fond que celle que nous venons d'exposer; et, en général, toutes celles que d'autres Géomètres ont imaginées après lui se réduisent aux mêmes principes."

[30] I know of no other textbooks in Germany 1770–1790 that deal with remainder problems. Karsten [1776, I, 2, 62–70] gives an example of the *regula virginum*, but this is almost a word for word repetition of Clausberg's text.

[31] I.e., the 'zweyte Abtheilung' of the 'erster Theil' (dealing with arithmetic, geometry, trigonometry and perspective) being additions to the part on arithmetic published earlier in 1758.

textbooks re-use earlier works [32] but present the information from a somewhat different perspective. Although both works stress examples, systematisation and proof, Euler tries to connect traditional algebra with analysis [Euler, 1770, 6], whereas Kästner's aim is partly didactical, providing proofs, and partly historical, adding notes on earlier books. [33]

In both books, the special cases disappear in favour of the general method of substitution that, formulated analytically, leads to a general solution of Chinese Remainder problems with two divisors. Kästner gives only one example solvable by a short search and solves all other examples using the general method [Kästner, 1786, 515–522]. In Euler's *Algebra* the substitution method is the only one used, although Euler didactically proceeds from "intuitive" examples to the general solution [Euler, 1770, II, 220-228; 231-235]. All examples in Euler and Kästner are restricted to the case of one equation with two unknowns (or to a remainder problem with two divisors), although Kästner notes that the Julian Calendar problem is an instance of the problem with three divisors [Kästner, 1786, 522].

Kästner gives a solution for the calendar problem, though not in his chapter on indeterminate analysis but in the chapter on chronology in the second part of his series *Anfangsgründe* [1759]. Its solution runs over four pages and applies substitution. Of the three unknowns Q, R and S, Q is calculated first, by successive subsitution, then R and S are deduced "in a similar way" [Kästner, 1759, 437-441]. Given the length of the deduction, it is not surprising that this kind of example is not included in elementary textbooks. In fact, Kästner includes this problem and its analytical derivation only because Joh. III Bernoulli had given the solution (after J.H. Lambert suggested the problem) but without proof [Kästner, 1759, 441].

With the introduction of this general and algebraic solution, however, a new problem arises: the length of the solution. As Euler remarks:

> The solution of such questions rests on the relation of the two numbers by which we are to divide and depending on the nature of this relationship, the solution becomes sometimes shorter, sometimes longer. [Euler, 1770, II, 223] [34]

[32] [Heeffer, 2007] shows Euler's dependence on [Stifel, 1553]; Kästner's work is full of references to earlier writers.

[33] Kästner's interest in the history and bibliography of mathematics is later pursued in [Kästner, 1796].

[34] Original: "Die Auflösung solcher Fragen beruhet auf das Verhältnis der beyden Zahlen, wodurch getheilt werden soll, und nach der Beschaffenheit derselben wird die Auflösung bald kürzer bald weitläufiger." This question, the length of the Euclidean algorithm, would only be developed on a theoretical level much later, see [Shallit, 1994; Schreiber, 1995].

He follows this with a short example (using 6 and 13) solved with only one substitution (since $13 = 2.6 + 1$), and then a longer one (39 and 56), for which five substitutions are needed. In the remaining examples the limit of five substitutions is never exceeded [Euler, 1770, II, 223–227, 230-235]. Kästner's examples vary between one step and six steps, though he mentions a case "where one has to divide 54 times, before one finds the greatest common measure" [Kästner, 1786, 528]. [35]

Lastly, both Euler Euler [1770, II 235–246] and Kästner Kästner [1786, 529–539] treat instances of the *regula virginum*. In these works, the *regula virginum* or *coeci* appears immediately after the remainder problems involving one linear equation and two unknowns, indicating that both classes of problems are related. However, neither Kästner nor Euler propose a general solution method embracing the complete class of problems and each remain faithful to the treatment given in earlier books such as Clausberg. Essentially, this comes down to Bachet's algebraic solution, reducing the problem to x, y, z's and substituting values for x (up to a certain limit specified by the problem), and excluding the solutions with fractional or negative x, y, z's.

3.2 Discussions on Euclid's procedure

As Bachet and Clausberg had noted much earlier, the procedure for finding the g.c.d. is the key technique for solving the fundamental example of remainder problems with two divisors, which (in algebraic notation) amounts to solving $ax - by = c$ in integers. Both Euler and Kästner acknowledge the pivotal role of the Euclidean algorithm, and both refer to Euclid VII, 2. Kästner, however, remarks:

> I had to think about this rule [the Euclidean algorithm] because of the similarity of the method in (21) [example with div. 7, 15 and rem. 0, 10], where we also divide remainders by preceding numbers. M. Euler has also remarked on this similarity in his Anl. zur Algebra 231 S. but he did not develop the proof of the resolution.[Kästner, 1786, 528] [36]

Kästner did not include the procedure for finding the g.c.d. in the first part of his *Anfangsgründe* [1758] because it seemed "entbehrlich" (dispensable), but he now develops it in full [Kästner, 1786, 523–4]. Kästner's proof is actu-

[35] This is actually a classic "recreational" problem, originally from Pisano, with the goal of astounding the reader with the solution [Dickson, 1919–1927, I, 60].

[36] Original: "Mich erinnerte an ihr [the Euclidean algorithm], die Aehnlichkeit ihres Verfahrens mit dem (21) wo auch immer Reste mit vorhergehenden dividirt werden. Hr. Euler hat auch diese Aehnlichkeit bemerkt Anl. zur Algebra 231 S. aber den Beweis der Auflösung nicht entwickelt."

ally quite similar to the argument given by Euler [1734/5, 19–22], which we described earlier.

Kästner's critique, that Euler did not develop his proof in full, is part of a more general critique regarding the absence or incompleteness of proof in Euler's work. Kästner had earlier regretted Euler's slackness in proofs in the *Introductio in Analysin infinisitorum* [Müller, 1904, 116] and repeated this critique when reviewing Euler's posthumously published *Opuscula Analytica* [1783-1785] for the *Göttinger Gelehrte Anzeigen* [Kästner, 1785, 539], pointing out that "die Induction hier nicht allemal sicher ist" (the induction is not always on sure footing). J.H. Lambert equally complained that Euler rather "shows the fundamentals than explain them completely" ("die Gründe mehr anzeigt als vollständig vorlegt") when he reviewed Euler's *Algebra* for the *Allgemeine deutsche Bibliothek* [Lambert, 1770b, 544].

These criticisms can be better interpreted if Kästner's and Lambert's view on mathematics is taken into account. For both, Euclid remains the model of mathematical exposition and correctnesss. Kästner's preface to the first volume of his *Anfangsgründe* takes a programmatic stance [37]:

> All concepts within arithmetic are in my view based upon those of integer numbers; fractions are integer numbers, whose unity is a part of the original whole, then perceived as unity; and one should imagine irrational quantities as fractions, that have a variable unity, a smaller and smaller part of the whole. It is a major methodical error that Freiherr von Wolff bases the doctrine of fractions on the doctrine of proportions, because the larger part of proportions have fractions in their exponents. Therefore, I have tried to derive everything in the 1st chapter of the Arithmetik starting from the concepts of integer numbers; and I have been careful to prove how theorems follow from this, that are apparent in the case of integer numbers, and have been generally admitted without suitable justification, even by writers who prove meticulously. [Kästner, 1758, preface] [38]

[37] Compare also with [Folta, 1973; Bullynck, 2006, 194–234]. For Lambert's more complicated though similar view on this topic, see [Lambert, 1771, Parts II and IV].
[38] Original: "Alle Begriffe der Arithmetik gründen sich meines Erachtens auf die von ganzen Zahlen; Brüche sind ganze Zahlen, deren Einheit ein Stück des anfangs für die Einheit angenommenen Ganzen ist, und Irrationalgrössen muß man sich als Brüche vorstellen, die diese Einheit veränderlich, immer ein kleineres und kleineres Stück des Ganzen ist. Daß der Freyh. v. Wolf die Lehre von den Brüchen auf die von den Verhältnissen gründet, ist ein grosser Fehler wieder die Methode, weil die größte Menge der Verhältnisse, Brüche zu Exponenten hat. Daher habe ich im I. Cap. der Arithmetik alles aus den Begriffen ganzer Zahlen herzuleiten gesucht; und dabey sorgfältig gewiesen, wie hieraus Sätze folgen, die bey ganzen Zahlen augenscheinlich sind, und auch von Schriftstellern, die scharf erweisen, meiner Einsicht nach ohne zulängliche Rechtfertigung allgemein angenommen werden."

Indeed, Wolff proves the Euclidean algorithm in his *Elementa Matheseos* [Wolff, 1732, 60–61] in the chapter on fractions assuming his numbers are integers which is systematically unsound. Moreover, in transferring Euclid's proposition from continuous geometry to finite quantities (or an arithmetic based on integers), one has to re-prove Euclid's proposition in the same rigorous manner. This had already been noted by Wenceslaus J. G. Karsten, the mathematics professor of Halle university, who had provided a different proof (similar to Kästner's and Euler's argument of 1734) in his *Lehrbegriff* [Karsten, 1776, I, 1, 87–89]. [39]

This discussion becomes more concrete if one considers the use Lambert made of the Euclidean algorithm. In his famous article that proves the irrationality of π [Lambert, 1767], Lambert comments on the range of application allowed for by the Euclidean algorithm. The proof proposes to show that the arc of a circle is incommensurable to its tangent and it therefore makes use of an extended interpretation of Euclid VII, 2, i.e., the Euclidean algorithm. Since Lambert uses an infinite series in continued fraction form to calculate the tangent, the question arises whether the Euclidean algorithm is applicable to the infinite series:

> One should remark that, whereas Euclid applies his method only to integral and rational numbers, I need to use it in another way, because I have to apply it to quantities of which it is not known in advance if they are rational or not. [...] Although [the progression of remainders] continues to infinity, we will nevertheless be able to apply Euclid's proposition. [Lambert, 1767, 267, 276] [40]

The condition Lambert finds for the application of Euclid VII, 2 is that the progression of residues (i.e., of the denominators of the continued fractions) has to be strictly convergent. In fact, Lambert proves it is more convergent than a geometric progression. [41] Similar applications of continued fractions to infinite series accompanied by an explicit concern for the convergence of such procedures are also described in the essay "Verwandlung der Brüche", contained in Lambert's *Beyträge* [Lambert, 1765-1772, II, 75ff.].

---

[39] Later, the mathematics professor Johann Pasquich from Presburg (Bratislava) would provide yet another proof [Pasquich, 1787].

[40] Original: "[I]l convient die remarquer que, tandis que *Euclide* ne l'applique qu'à des nombres entiers et rationels, il faudra que je m'en serve d'une autre façon, lorsqu'il s'agit d'en faire l'application à des quantités, dont on ignore encore si elles seront rationelles ou non? [...] Quoique [la progression des résidus] continue à l'infini, nour pourrons néanmoins y appliquer la proposition d'*Euclide*."

[41] A more detailed analysis of this proof, including remarks on the 'modern' convergence of the series, can be found in A. Speiser's foreword to [Lambert, 1946-1948, I, XIII–XVI].

This contemporary example clarifies Kästner's somewhat cryptic description of "fractions, that have a variable unity". In the extended use of the proposition in the theory of continued fractions or in Lambert's essay, it becomes difficult to determine whether one is dealing with a convergent or divergent series. In the 18th century, it was usual to interpret an infinite series as corresponding to a quantity, but this quantity might be impossible, i.e., have no value when evaluated. Therefore, given the law behind the members of a series, one had "to determine the nature of the quantity defined by this series" [Lambert, 1758, 16].[42] The only method then available to show that the number was indeed possible was the classical (Greek) method of exhaustion, forcing the number between an upper and lower limit whose difference could be made arbitrarily small . In Euler's work, the control on the produced 'numbers' (i.e. to check if an occurring series is convergent or not) was often lacking, a fact criticised by both Kästner and Lambert.

4 Hindenburg's *Verbindungsgesetz Cyklischer Perioden* (1786)

However, Euler's general solution for linear Diophantine equations, using substitions, did not satisfy everyone:

> A general solution of problem (11) was also given by M. Euler. But the length of solution, that already occurs if one transposes his method for two divisors and remainders to three, shows the complexity, that inevitably has to occur if more divisors and remainders are involved. [Hindenburg, 1786, 318][43]

In this quotation, Carl Friedrich Hindenburg is criticising the sometimes involved nested series of substitutions that can occur with Euler's solution method. To avoid these substitutions Hindenburg developed an alternative general system based on finite, combinatorial principles and on a 'direct' and 'efficient' production of the solution. He presented the system in an article "Verbindingsgesetz cyklischer Perioden" [Hindenburg, 1786], although he had announced the idea some ten years before [Hindenburg, 1776, 34].

Hindenburg does not start from equations, but from combinations of numbers:

> **Combinatory Law of Cyclic Periods** 1. Explanation. The series of nat-

[42] Original: "invenire naturam quantitatis, ex qua series formatur".
[43] Original: "Eine allgemeine Auflösung der Aufgabe (11) hat auch Herr Euler gegeben. Aber die Weitläufigkeit, auf die man schon verfällt, wenn man das für zwey Divisoren und Reste gelehrte Verfahren auf drey überträgt, läßt die Verwickelung voraus übersehen, in die man bey mehrern Divisoren und Resten nothwendig gerathen muß."

ural numbers, starting from 1, in their natural order, up to α; β; γ; δ; etc. should be written in vertical columns one next to the other

α-	β-	γ-	δ-	columns
1,	1,	1,	1,	&c.
2,	2,	2,	2,	&c
3,	3,	3,	3,	&c
.	.	.	.	&c
α	.	.	.	&c
.	β	.	.	&c
.	.	γ	.	&c
.	.	.	δ	&c
.	.	.	.	&c
.	.	.	.	&c
&c	&c	&c	&c	&c
α	β	γ	δ	&c
1,	1,	1,	1,	&c.

as above, so that if one arrives at the largest numbers α, β, γ, δ, &c. of the individual vertical rows, one repeats from there, each in their order, to write (from 1 onwards), and continues, until one arrives at the highest or largest Complexion α, β, γ, δ, &c. (the last horizontal member of the row) [Hindenburg, 1786, 283–4] [44]

In this construction, every line makes up a *Complexion*, to which an *Ordnungszahl* (index) can be assigned. A complete cyclic period consists of a number of complexions equal to the least common multiple of the α, β, γ, δ, ... As an example, the full system of cyclic periods for 2, 3, 4 is as follows:

(1) 1, 1, 1 (5) 1, 2, 1 (9) 1, 3, 1

[44] Original: "**Verbindungsgesetz cyklischer Perioden** 1. Erklärung. Die Reihe der natürlichen Zahlen, von 1 an, in ihrer Ordnung, bis α; β; γ; δ; u.s.w. schreibe man in senkrechten Colonnen nebeneinander [...] dergestalt, daß, wenn man auf die größten Zahlen α, β, γ, δ, &c. der einzelnen senkrechten Reihen gekommen ist, man von da an diese Reihen, jede in ihrer Ordnung, von vorne (von 1 an) zu schreiben wieder anfängt, und damit so lange fortfährt, bis man einmal auf die höchste oder größte Complexion α, β, γ, δ, &c. (das letzte horizontale Glied der gesamten Reihe) verfällt."

(2) 2, 2, 2	(6) 2, 3, 2	(10) 2, 1, 2
(3) 1, 3, 3	(7) 1, 1, 3	(11) 1, 2, 3
(4) 2, 1, 4	(8) 2, 2, 4	(12) 2, 3, 4

Note that Hindenburg's construction has a double ordering. Firstly there are the complexions themselves which Hindenburg considered as a new kind of number, defining addition and subtraction (though not multiplication). The components of complexions are added (or subtracted) within each column and if in any column the result exceeds the number of the column, say α, the least remainder respective to α is written down, and if the least remainder is zero, α is used instead of zero. (It is important to note that there is no carry between the columns.) Secondly there are the indices of the complexions which can be added and subtracted from one another in the usual way [Hindenburg, 1786, 287–291]. [45]

As Hindenburg noted, the component of a complexion may take on different forms, it can even be a negative number:

> If one takes a smaller number for the quotient as one might do, then the remainder becomes as large or larger than the divisor; if one takes 0 for the quotient, then the remainder is equal to the dividend; if one takes a larger number than the quotient can be after normal division, then the remainder becomes negative. [Hindenburg, 1786, 293 footnote] [46]

Thus, a single number can be represented in infinitely many different though equivalent ways, e.g., a number with 2 in the 7-column can also have 9 or -5 in this column. Although to us it appears a rather trivial observation, Hindenburg emphasises this property [Hindenburg, 1786, 289, 292–3, 307, 313, 315] and makes good use of it to abbreviate his calculations.

The first conversion problem is from index to complexion: a complexion with index n is always of the form $n, n, n, n, \ldots$, though if n exceeds α (or β or $\gamma \ldots$), instead of n, the least remainder of n after division by $\alpha \ldots$ is written down [Hindenburg, 1786, 293–4]. The second conversion problem, to find the index of a given complexion, is more difficult. One method is the decomposition of

[45] This kind of notation system has been often reinvented. In the computer age, Valach [1955] was the first to present this system, specifically to avoid carry in addition and multiplication, though Lehmer [1933] had described the system earlier. No reference is ever made to Hindenburg, his system seems to be forgotten, though Gauss's congruences are always mentioned.

[46] Original: "Nimmt man eine kleinere Zahl zum Quotienten, als man nehmen könnte, so wird der Rest so groß oder größer als der Divisor; nimmt man 0 für den Quotienten, so wird der Rest dem Dividendus gleich; nimmt man eine größere Zahl, als der Quotient nach der gewöhnlichen Division seyn kann, so wird der Rest negativ"

the complexion $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$ into the sum of complexions with known index. From the definition of addition we know that n times 1, β, γ, δ, ... (index i) is equal to n, β, γ, δ, ... and has an index ni. A given complexion $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$ can thus be written as:

$\mathfrak{a}$ times $1, \beta, \gamma, \delta, \ldots +$
$\mathfrak{b}$ times $\alpha, 1, \gamma, \delta, \ldots +$
$\mathfrak{c}$ times $\alpha, \beta, 1, \delta, \ldots +$
$\mathfrak{d}$ times $\alpha, \beta, \gamma, 1, \ldots +$
...

If one knows (i.e. has calculated in advance) the indices for $1, \beta, \gamma, \delta, \ldots$; $\alpha, 1, \gamma, \delta, \ldots$ etc., one can easily calculate the index of $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$

It is clear that the *Verbindungsgesetz* implies a general solution to a class of remainder problems. That is, the problem of finding all numbers that leave $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$ after division by $\alpha, \beta, \gamma, \delta, \ldots$, is equivalent to the problem of finding the index of the complexion $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \ldots$ within a cyclic period consisting of $\alpha, \beta, \gamma, \delta, \ldots$ [Hindenburg, 1786, 312–316]. As a special case, the solution of $ax + by = c$ can also be found through this construction [Hindenburg, 1786, 316–318].

The advantage of Hindenburg's (and [Euler, 1734/5]) solution method is obvious when one has to solve many remainder problems in which the divisors are constant and the remainders variable. Such a case is the formula for the calculation of Julian years, which is derived in Hindenburg's paper in four different, though related ways [Hindenburg, 1786, 299–305]. Other advantages are the polyformity of the complexions (i.e., the fact that using Hindenburg's notation a number can be represented in an infinite number of ways) and the symmetry of the derived formula. Two remarks close Hindenburg's paper which are instructive with respect to the context of his work. Firstly, Hindenburg mentions Stifel's special rule and remarks that similar rules may be derived easily from his cyclic periods, but "to teach such rules here, would be fully superfluous." [Hindenburg, 1786, 320] Hindenburg's purpose in including this remark is to show the power of his system, namely that it can even generate the earlier rules of computation and to emphasize the generality of his method.[47] The second remark indicates potential generalisations of his cyclic periods. To this end, non-decadic systems may also be used, or even:

> Instead of the series of numbers 1, 2, 3, ..., α; 1, 2, 3, ..., β; 1, 2, 3, ..., γ; etc. in which the numbers proceed in natural order, one could also use

[47] If Hindenburg had read Euler's paper from 1734, the remark might also refer to Euler. Hindenburg's formula would then also be copied from Euler. Normally, however, Hindenburg refers quite faithfully to his sources, both in his own works and in his editorial comments in his journals.

other numerical series, in which the given numbers or even just single digits, can follow any previously determined, even if apparently irregular, order. [Hindenburg, 1786, 321] [48]

This observation fits within his general and ambitious idea of using combinatorial analysis as a universal tool for solving mathematical problems. In this scheme, tables play an important role [Hindenburg, 1786, 322–324] and the idea of automation is clearly hinted at.

Hindenburg's paper, although it fell into obscurity in the next century, was very well known in its own time. Both the *Allgemeine deutsche Bibliothek*, one of the two most important general review journals in Northern Germany, and the *Göttinger Gelehrten Anzeigen*, probably the most important review journal for scientific work at that time, devoted several pages to a review of the first issue of the *Leipziger Magazin für reine und angewandte Mathematik*, which contained Hindenburg's paper and was edited by Hindenburg and Jean III Bernoulli. [49] The *Göttinger Gelehrten Anzeigen* even indicated the gist of Hindenburg's novel method. [50]

When Hindenburg's combinatorial analysis became fashionable in Germany, from 1794 onwards, some of his students pursued the idea of cyclic periods, publishing their results in *Archiv für reine und angewandte Mathematik*, which Hindenburg edited during the years 1795 to 1800. Johann Karl Burckhardt used Hindenburg's method to construct a table for Julian years according to their characteristics [Burckhardt, 1798], A.F. Lüdicke showed how to apply the procedure to a problem with seven divisors [Lüdicke, 1798], and finally, J.W. Becker supplemented Hindenburg's original essay by showing how to deal with periods that are not relatively prime [Becker, 1798]. [51] Hindenburg, in his typical editorial fashion, added copious notes and remarks to Lüdicke's

[48] Original: "Statt der Zahlenreihen 1, 2, 3, ..., α; 1, 2, 3, ..., β; 1, 2, 3, ..., γ; u.s.w., bey denen die Zahlen in natürlicher Ordnung fortgehen, könnte man auch jede andere Zahlenreihen gebrauchen, wo gegebene Zahlen oder auch nur einzelne Ziffern, nach jeder vorher bestimmten, an sich auch noch so unregelmäßig scheinenden Ordnung auf einander folgen."

[49] The other most important general review journal in Northern Germany was the *Allgemeine Litteratur-Zeitung* which displayed only the contents of the issue.

[50] See *Göttinger Gelehrte Anzeigen*, 5. Stück 8. Jan. 1787, pp. 47–48. The review is by Kästner.

[51] References to these articles in the *Archiv* are missing in [Dickson, 1919–1927, II], though Lüdicke appears, together with Kästner, on p. 62. Lüdicke [1798] and Kästner [1759] are quoted from a secondary source, and it seems Dickson or his source got the information garbled. Dickson assigns both works to the year 1745 and says Lüdicke deals with the calendar problem, whereas it is Hindenburg who deals with that problem. Most probably his information on Hindenburg's paper is also quoted from a secondary source, see his note 108 p. 63.

essay, repeating the main points of his original work [Lüdicke, 1798, 216–220]. Notably Hindenburg takes the opportunity to correct his own historical remarks on the problem. Instead of the contemporary "standard" references (Clausberg, Kästner's *Anfangsgründe* and Euler's *Algebra*, all quoted in his article from 1786), Hindenburg now mentions that Bachet had solved the problem in 1624 and refers to Lagrange's work on Diophantine equations [52], where he probably found the Bachet reference.

Another of Hindenburg's 1798 editorial comments is significant because it touches on a topic added by Gauss to his *Disquisitiones Arithmeticae* some time between 1797 and 1799 (as will be shown in the following section). Lüdicke had noted that his indeterminate problem contained superfluous information and that this information was best discarded before computation. [53] Hindenburg added in a footnote that this can be generalised. It is advantageous if "all conditions are put next to one another from the beginning onwards, to compare them", so that conditions [i.e. a mod b] can be discarded if they appear more than once [Lüdicke, 1798, 210, note]. [54]

5 Gauss's Modular Arithmetic (1797-1801)

From 1797 onwards, a third attempt was made at constructing a general framework in which all remainder problems could be solved. The author of this system was Carl Friedrich Gauss, an avid reader of Lambert and Hindenburg as well as of Euler and Lagrange. Gauss had received copies of Kästner's work in 1791, of Lambert's *Zusätze zu den logarithmischen und Trigonometrischen Tafeln* [1770a] and of Hindenburg's *Beschreibung* [1776] in 1793, and acquired Clausberg's work in 1794. [55] Upon arriving at Göttingen University (1796), the three volumes of Lambert's *Beyträge zum Gebrauch der Mathematik* [1765-1772] were the first books he borrowed from the library. Later on (1797) he also borrowed the *Mémoires* of the St Petersburg and Berlin Academies, which contained Lambert's, Euler's and Lagrange's essays [Dunnington, 1955, 398–404]. Since Hindenburg's journals, both the *Magazin* and the *Archiv*, were the only journals solely devoted to mathematics in Germany, one can assume

[52] The reference is to [Lagrange, 1767b, 220–222] and [Lagrange, 1767a, 294–295] or [Lagrange, 1867-1892, II, 519–520, 698], that deal mostly with the quadratic case.
[53] The problem is to find the number that leaves 1, 2, 4, 5, 5, 9, 0 after division by 2, 3, 5, 6, 9, 10 and 0, where, e.g., the 5 mod 5 and the 9 mod 9 may be discarded.
[54] Original: "Es werden bey ihr [der Abkürzung] die sämtlichen Bedingungen gleich Anfangs, zur näheren Vergleichung, neben einander gestellt."
[55] These are Gauss-B460, Gauss-B199, Gauss-B440 and Gauss-B340 in Gauss's personal library (now at the Göttingen University Library) with handwritten dates of acquisition.

Gauss read them frequently. Two of Gauss's professors at the Collegium Carolinum, Zimmermann and Drude, were on the list of subscribers of the original *Magazin* [Subskribentenliste, 1781], so Gauss may have had access to Hindenburg's *Magazin* from 1792 onwards. In any case, Gauss's letters make it clear that Gauss read the *Archiv* on a regular basis between 1797 and 1799 while studying in Göttingen. [56] Although it is not certain that Gauss read Hindenburg's 1786 article, he must have been familiar with the gist of it through the 1798 resumé in the *Archiv*.

Being intimately familiar with the general literature on remainder problems from 1791 onwards, and with the professional literature from 1796 onwards, Gauss drafted a formalism (A), written during the summer and autumn of 1797. The final version (B) appeared in Sections I and II of the *Disquisitiones Arithmeticae* (1801). Version B is an augmentation and partial transformation of Version A. Whereas Version A introduces the fundamental concept of congruences, Version B is a richer and more mature version of the same topic, going beyond Euler.

5.1 Version A (1797)

Gauss's early version of 1797 was discovered in 1981 by U. Merzbach in Dirichlet's *Nachlass* [Merzbach, 1981]. This draft of (the first four sections of) the *Disquisitiones Arithmeticae* contains the major innovations Gauss added to the already existing treatment of remainder problems. These are the concept of congruence and the associated modulus sign $x \equiv a \pmod{p}$.

> **Definitions.** If a certain number, which we will call the **modulus**, measures the difference of two numbers, we will call these numbers **congruent**

[56] A letter to Zimmermann regarding a contribution Gauss planned to send to Hindenburg's *Archiv* [Poser, 1987, 27] and a letter to Bolyai [Schmidt, 1899, 37 and the note p. 188] mentioning an article Gauss read in Hindenburg's journal determine the years 1797 and 1799. The contribution mentioned in the first letter is on a theorem of Lagrange [Gauss, 1863-1929, VIII, 76], concerning an important issue within combinatorial analysis. With respect to this letter, it is important to clear up some confusion. Waltershausen [1856, 22] claims Hindenburg had died before Gauss's essay arrived, but this is erroneous as Hindenburg died only in 1808. This was pointed out by Schlesinger [Gauss, 1863-1929, X, 444] and later, without reference to Schlesinger, by [Jahnke, 1990, 205]. Since the mediator for the contact with Hindenburg was Kästner, one may assume that, in accordance with contemporary custom, Gauss's contribution and letter would have been enclosed in a letter from Kästner to Hindenburg, since the two of them were already in regular correspondence. Kästner, however, died in 1800, so Waltershausen probably substituted Hindenburg for Kästner in his account.

to the modulus, if not, **incongruent**. In the first case one of the two numbers will be called the **residue** of the other, in the second case, a **non-residue**. E.g. 32 and 11 will be called congruent to the modulus 7, because the difference of these numbers, 21, is divisible by 7.
Denoting congruent numbers by a sign is very useful for abbreviating calculations: thus, because of the analogy with equality between numbers, we will use as a sign, this sign $\equiv$, the modulus can be added in brackets to avoid ambiguity if it is considered necessary. For example §.1. can be written in this way as $32 \equiv 11 \pmod 7$; $-19 \equiv +1 \pmod 5$. [Gauss, 1797, Art. 1 and 5] [57]

The introduction of the concept of a congruence and the appropriate notation makes the treatment of linear, quadratic and higher Diophantine problems formally and theoretically coherent. Moreover, the $\equiv$ sign, as Gauss indicates, abbreviates calculation.

Directly related to this, is Gauss's use of "representatives", i.e., the least positive or negative residue of a congruence.

If the given number is -17, modulus 5, we will have a progression of residues $\ldots, -22, -17, -12, -7, -2, +3, +8, \ldots$ Here, -2 will be the minimal negative residue and the absolute minimum, $+3$ the minimal positive residue. [Gauss, 1797, art. 5] [58]

In article 6 Gauss proves the "transitivity" of the congruence relation, that is if two numbers are both congruent to a third number, then they are congruent to each other. [59] The concept of least residue and the transitivity property taken together provide one of the main techniques for abbreviating calcula-

[57] Original: "**Definitiones**. Si numerus aliquis, quem **moduli** nomine denotabimus, duorum numerorum differentiam metitur, hi **secundum illum congrui** dicentur, sin minus, **incongrui**. Priori casu alteruter numerorum alterius **residuum** vocatur, posteriori non-**residuum**. Ita numeri 32, 11 congrui dicentur secundum modulum 7, quippe quorum differentia 21 per 7 dividitur.
Maiorem utilitatem afferret ad calculos contrahendo numeros congruos signo denotare: ad quod ob insignam inter eos et quantitates aequales analogiam hoc utemur $\equiv$, modulo quando ad ambiguitatem evitandam necessarium videbitur clausulis apposito. Exempla §.1. igitur tali modo exhibentur $32 \equiv 11 \pmod 7$; $-19 \equiv +1 \pmod 5$)."
[58] Original: "Sit numerus datus -17, modulus 5, habebimus progressionem residuorum $\ldots, -22, -17, -12, -7, -2, +3, +8, \ldots$ Hic itaque -2 erit residuum minimum negativum simulque absolute minimum, $+3$ residuum minimum positivum."
[59] This property (or theorem) was a standard ingredient in 'algebraic' proofs of the Euclidean algorithm, in Euler, Kästner and Karsten as well as in Lambert's theorems on primes, included in [Lambert, 1770a, 21–22; 28–48]. Of course, Bachet had already discerned this property in his propositions 24 and 25.

tions in solving congruences. As Gauss often remarks, an intelligent choice of the representative can make computation much easier. This connects with Hindenburg's comments on the useful polyformity of his complexions. [60]

Chapter 2 of the draft, "De residuis functionum primi gradus", describes the solution of a first degree congruence. Given a congruence $ax + b \equiv c$ modulo a prime number p, it can always be transformed into an indeterminate equation $ax = fy \pm 1$ through a suitable substitution. As Gauss remarks, the solution of this equation is well known, thus it is sufficient to add an example for those who do not yet know the solution [Gauss, 1797, art. 26].

> If an indeterminate equation is given ... $83x = 16y \pm 1$. Divide the greatest coefficient 83 by the least coefficient 16, the quotient will be 5, throw away what is left and make $y = 5x + p$ which after substition in the first equation gives $3x = 16p \pm 1$. [Gauss, 1797, art. 26] [61]

Gauss's method is clearly substitution based upon the g.c.d. algorithm. He gives Euler the credit for first discovering this general solution method, and indicates that the continued fractions method of Lagrange is a variant of it [Gauss, 1797, art. 27].

As to remainder problems with many moduli, these are considered as sets of congruences: $x \equiv \alpha$ (mod. A) and $x \equiv \beta$ (mod. B) which can be combined into $By + \beta \equiv \alpha$ (mod. A) [Gauss, 1797, art. 32]. Because the problem of finding all numbers that have given remainders after division by given divisors "occurs throughout this book very often" [Gauss, 1797, art. 33], Gauss adds an example, where a set of three congruences is solved: $5x + 2 \equiv 0$ (mod. 9); $6x + 15 \equiv 0$ (mod. 21); $3x + 3 \equiv 0$ (mod. 4). These congruences have the respective solutions 5, 1 and 1, and through the substitutions $x = 9y + 5$ and $x = 63z + 50$ the solution for the set is obtained: $x \equiv 113$ (mod. 252).

[60] The introduction in Gauss's *Disquisitiones* of the congruence relation has, from late 19th century onwards, been described as the first definition of an equivalence-relation in modern mathematics, although the use of the word "equivalence" itself must surely be considered anachronistic in this case. For a discussion, see [HM, 2003]. It seems, however, from the material presented here, that at least a small part of the credit should be attributed to Hindenburg.

[61] Original: "Sit data aequatio indeterminata ... $83x = 16y \pm 1$. Dividatur coefficiens maior 83 per minorem 16, et quum quotiens fit 5, neglecto quod superest, faciamus $y = 5x + p$ quo valore substituto prodibit aequotio priori similis $3x = 16p \pm 1$."

Apart from the concept of a congruence and the notation, Gauss's treatment of remainder problems in the draft version does not go much beyond the textbook exposition of Kästner and Euler. However, in his exposition on the topic in the 1801 *Disquisitiones* [Gauss, 1801] he does go some steps beyond the draft. In particular he makes improvements to both the concept and the notation that help to abbreviate the calculation of solutions, and he adds more cases and generalisations of problems.

The first addition is the square bracket notation, equivalent to Euler's round bracket notation. This notation is introduced in a footnote to article 27 but without reference to Euler, a lapse that is corrected in a footnote to article 202. In contrast to Euler, Gauss hints at a more general use of this notation and indicates two formulae that are at the basis of this generalisation:

$$[\alpha,\beta,\gamma,\ldots,\lambda,\mu].[\beta,\gamma,\ldots,\lambda]-[\alpha,\beta,\gamma,\ldots,\lambda].[\beta,\gamma,\ldots,\lambda,\mu]=\pm 1$$
$$[\alpha,\beta,\gamma,\ldots,\lambda,\mu]=[\mu,\lambda,\ldots,\gamma,\beta,\alpha]$$ [Gauss, 1801, 27 footnote] [62]

As can be deduced from articles 177 (footnote) and 202 (comment), where this method is recommended for faster calculation of transformations between quadratic forms, the use of square brackets must have been a rather late addition to the *Disquisitiones*.

The solution of the remainder problem with more than one modulus is given in more general terms than in the draft, but essentially remains the same. To calculate the solutions more conveniently, Gauss again takes up an idea, "condition", present in Euler's work (e.g. [Euler, 1770, II, 230]) and implicit in Hindenburg's 1798 comments on Lüdicke's paper. Each line in the remainder problem defined by

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

can be interpreted as a "condition" on the set of solutions. Each new line can then be considered a further condition limiting this set. The interesting part is, however, that a condition can be "factorised" into two or more conditions (or "multiplied" into one condition): $X \equiv a \pmod{A.B} \rightarrow X \equiv a \pmod{A}$ and $X \equiv a \pmod{B}$ (if a has no common divisor with A or B, see [Gauss,

[62] $\overline{[\alpha,\beta,\ldots,\mu]}$ corresponds to the continued fraction $\frac{1}{\alpha+\frac{1}{\beta+\ldots+\frac{1}{\mu}}}$. Gauss's formulae can be easily proved using properties of continued fractions. For a proof see [Stern, 1833, 13].

1801, art. 33]). This makes it easy to see whether the problem does or does not have a solution, and helps to reduce the number of calculations required when the problem does have a solution.

A third addition is article 36, which proves Euler's and/or Hindenburg's formula for remainder problems with constant moduli and provides an application of it to the Julian year calendar problem. The proof is formulated with congruences, but the proof procedure is very similar to Euler's and Hindenburg's derivation [Bullynck, 2007].

Most puzzling at first sight is the final addition to the part on systems of linear congruences, article 37, that gives a general method to determine if a set of equations involving as many unknowns as equations has solutions or not. In the case of three equations:

$$\begin{aligned} ax + by + cz &\equiv f \pmod{m} \\ a'x + b'y + c'z &\equiv f' \pmod{m} \\ a''x + b''y + c''z &\equiv f'' \pmod{m} \end{aligned}$$

Gauss proceeds by calculating ζ, ζ', ζ'' such that $b\zeta + b'\zeta' + b''\zeta'' = 0$ and $c\zeta + c'\zeta' + c''\zeta'' = 0$, and by determining ν, ν', ν'' and μ, μ', μ'' in a similar way, i.e. so that $a\nu + a'\nu' + a''\nu'' = 0$ and $c\nu + c'\nu' + c''\nu'' = 0$, etc. This reduces the given system of congruences to: $\sum(a\zeta)x \equiv \sum(f\zeta)$; $\sum(b\nu)y \equiv \sum(f\nu)$; $\sum(c\mu)z \equiv \sum(f\mu)$, all mod m. This is of course an application of the classic method for calculating solutions of a system of n equations with n unknowns [Gauss, 1801, art. 37].

Two cases need to be distinguished: if $\sum(a\zeta), \sum(b\nu), \sum(c\mu)$ are prime relative to m, then the solution is the classic one, if not, then let α, β, γ be the g.c.d. of m and $\sum(a\zeta), \sum(b\nu), \sum(c\mu)$ respectively. If α, β, γ divide $\sum(f\zeta)$, $\sum(f\nu)$, $\sum(f\mu)$ respectively, then a solution exists, if not, no solution exists [Gauss, 1801, art. 37]. The second case is explained using a page long example.

The motivation to include article 37 in the *Disquisitiones* cannot be traced to an application of the article later on in the book, as Gauss himself admits in the preface [Gauss, 1801, XI], but it can be linked with the tradition of *Rechenbuch* problems. As mentioned before, both Euler and Kästner treated *regula virginum* problems immediately after Chinese Remainder problems, though they neither explained the connection nor proposed a general method. Gauss could do both, but merged the *regula virginum* problems into the more general problem of article 37, second case. If we apply Gauss's method to Riese's instance of the *regula virginum* (discussed in Section 2) the connection becomes clearer [63] :

[63] Gauss uses a different and in fact easier example.

$$4x + 2y + z = 36$$
$$x + y + z = 20$$

Turning these equations into congruences modulo 12 (because in Riese's example we multiplied the first equation by 12 to get integers) and then tripling the first congruence (to get a third congruence independent of the first two), we get three (conditional) congruences:

$$4x + 2y + z \equiv 0 \pmod{12}$$
$$x + y + z \equiv 8 \pmod{12}$$
$$6y + 3z \equiv 0 \pmod{12}$$

Using Gauss's elimation method, the congruences are transformed into the simpler congruences $12x \equiv 0$, $4y \equiv 4$ and $6z \equiv 0$ all (mod 12). The g.c.d.'s of the coefficients with 12 are 12, 4, 6 respectively, which divide the remainders 0, 4 and 0 respectively, thus the system has solutions. These solutions depend upon the solutions of the simpler congruences, i.e., $x = t$, $y = 3u + 1$ and $z = 2v$ (for integers t, u, v).

In his text Gauss remarks that all solutions of the proposed congruences will be found among these equations in integers t, u, v, but that not all combinations of t, u, v satisfy the problem, but "only those whose interconnection can be shown by one or more of the conditional congruences." [Gauss, 1801, art. 37] This is indeed the classic difficulty in the algebraic solution of the *regula virginum*, also Gauss refrains from giving a complete solution, but gives "some idea of it" by an example. Gauss substitutes the x, y, z with their solutions in t, u, v. The tricky point (on which Gauss does not expand) is that to solve these congruences, one cannot always divide, or that one risks dividing by 0. In Gauss's example, these congruences all nicely reduce to (mod 4); in the example we took from Riese it does not. Therefore, we turn to the original equations and, subtracting the second from the first, we get $y = 16 - 3x$. From this, it follows that x cannot have all values $0, 1, \ldots, 11$ but only half of them $(0, 1, \ldots, 5)$, y and z are determined then by $y = 16 - 3x$ and $z = 2x + 4$. This generates all six triples that solve the problem. [64]

Though somewhat involved, Gauss's solution method has no need for trial-and-error and is more general than the common examples of the *regula virginum* in which the first coefficient of one of the equations is usually constrained to be one. Although in our example, the problem can be solved more easily by the classical method (Bachet's and Euler's), Gauss's method has the advantage that it can deal with larger systems of equations, and that it can derive the (im)possibility of solution without trial and error.

Thus Gauss homogenises the treatment of remainder problems with Diophan-

[64] This is essentially returning to Bachet's and Euler's solution.

tine problems through congruences, much after the fashion begun by Euler, but adding ideas of his own and some from Hindenburg. In the mature version of the *Disquisitiones* some new problems, notably the Julian year problem and the *regula virginum*, are integrated and some new formalisms to abbreviate computation are included. The synthesis and homogenisation thus achieved is not only elegant but also provides a variety of "tools" for abbreviating the computation of solutions to both general and special cases.

6 Conclusions

Solutions and frameworks for solving remainder problems attracted special interest in the late 18th century. One of the reasons for this seems to be that these old remainder problems provided a bridge between earlier traditions and modern and/or advanced mathematics. In France, Bachet's solution was used as an example to display the application of algebra to arithmetic problems, but it was also integrated in the theory of equations, one of the main research topics of the period. In Germany, other aspects of these problems, notably their link with the Diophantine tradition and with Euclidean proof, were developed.

Euler independently rediscovered Bachet's solution in a slightly more general form in 1734. Later, Lagrange gave due credit to Bachet for solving the linear Diophantine problem when publishing his own solution to the quadratic case during 1766–1770. In the late 18th century, the general solution method for remainder problems was included in textbooks by Euler and Kästner. This was mainly to show the application of the g.c.d. procedure and to point out some difficulties, namely the length of the solution and the need to prove the Euclidean algorithm. Both difficulties reflect important issues in the German mathematical community of that time: computational problems and discussions on the foundation of arithmetic and the form of proof.

For Hindenburg and Gauss, both of the above issues were important motivations for developing new frameworks for solving remainder problems. Hindenburg's complexions are computationally interesting. Although more work needs to be done in advance than with the other frameworks, the final calculation can be done very quickly. Furthermore, since the complexions only involve integers, they avoid methodological problems with the Euclidean algorithm. Finally, Gauss's congruences, functioning as an equation, a relationship and a tool for abbreviating calculation, reshaped this fragmented field of mathematics (which had come from old algebra books, Rechenbücher, recreational mathematics, equation theory and Diophantus) into a coherent theory. All singular problems, previously treated by Euler and Hindenburg, appear in Section II of the *Disquisitiones Arithmeticae*, and are aptly solved using congruences, with many indications on how to abbreviate the calculations.

Acknowledgments

The author would like to thank Catherine Goldstein for comments on an earlier version of this paper and for her continuing support; Liesbeth De Mol for many discussions; Anthony Moore, Julian Rohrhuber and Renate Wieser for inviting me to Hamburg and Cologne to discuss remainder arithmetic; two anonymous referees for many valuable suggestions. Finally, I would like to thank June Barrow-Green for editing my text.

Added in Proof

In addition to Stifel's rule, Simon Jacob's treatment of remainder problems with more than two divisors deserves mention. Simon Jacob (1510–1564) was an apprentice to the *Rechenmeister* Johann Neudörffer the Elder (1497–1563) in Nürnberg. Jacob wrote a *Rechenbuch* that was edited posthumously by his brother as *Ein New und Wol-gegründt Rechenbuch, auff den Linien und Ziffern* [Jacob, 1565]. As an apprentice of Neudörffer, Jacob had had access to a circle of mathematicians and reformers, amongst them the famous publisher of mathematical texts Johann Petreius who was married to Neudörffer's sister. Petreius had published Copernicus, Schöner, Rheticus and Stifel and others. [65]

Jacob's book contained 7 problems of remainders after division, all with more than two divisors [Jacob, 1565, 240v–243v]. With this set of examples Jacob indicated how to solve the general case. His procedure came down to the following. Given three divisors A, B and C and respective remainders a, b and c, multiply a with BC, b with AC, c with AB, add them and take the remainder of this sum after division by ABC. [66]

Jacob's method in these examples was later explicitated and put in an algebraic and clearer format by Nicolaas Huberts van Persijn. Frans van Schooten the Younger (1615–1660) published van Persijn's treatment in his *Exercitationes Mathematicae* 1657, fifth part on Miscellanea, chapter VII. [67] This fifth part of the *Exercitationes* contained many number problems, some from Stifel, some from Jacob, some from Bachet's Diophantus edition, etc. This collection of problems were all presented in algebraic garments and accompanied by a

[65] For more details on Jacob, see Gebhardt [1999], on Petreius and his environment Keunecke [1982].
[66] Jacob had examples up to five divisors, always relatively prime to each other. However, Jacob did not explicitly enunciate this as a necessary condition for his procedure to work.
[67] These are pages 407–410 or pages 379–382 in the Dutch (original) edition [1659].

praise of the Cartesian method.[68] Van Schooten's Miscellanea section (or at least a part of it) may therefore stand as one of the 17th century attempts to get at something like a general approach in problems with integer numbers. Van Schooten's text lines up with the more systematic attempts at solving the linear Diophantine case in Bachet's 1624 edition of the *Problèmes plaisans et delectables* and in Beveridge's *Institutionum Chronologicorum* (1669). Van Schooten's *Exercitationes* were widely read and Isaac Newton and Leonhard Euler were among those who worked through van Schooten's book to learn the new algebra.

References

ADB, 1875-1912. Allgemeine deutsche Biographie. Historische Commission bei der Kgl. Akademie der Wissenschaften, Leipzig, 56 volumes.

Alfonsi, L., 2007. Algebraic analysis and the use of indeterminate coefficients by Etienne Bézout (1730-1783). Bulletin of the Belgian Mathematical Society – Simon Stevin 13 (5), 933–936.

Bachet de Méziriac, C. G., 1612. Problèmes plaisants et délectables, qui se font par les nombres. Partie recueillis de divers autheurs, partie inventez de nouveau avec leur demonstration. Rigaud, Lyon.

Bachet de Méziriac, C. G., 1621. Diophanti Alexandrini Arithmeticorum Libri sex et de Numeris Multangulis Liber unus. Drouart, Paris.

Bachet de Méziriac, C. G., 1624. Problèmes plaisants et délectables, qui se font par les nombres. Partie recueillis de divers autheurs, partie inventez de nouveau avec leur demonstration. Rigaud, Lyon. Second and enlarged edition.

Becker, J. W., 1798. Zusatz zu Prof. Hindenburgs Abhandlung über die cyklischen Perioden. Archiv der reinen und angewandten Mathematik 2 (8), 481–486.

Beveridge, W., 1669. Institutionum Chronologicarum. Roycroft, London.

Bézout, E., 1766. Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine. Troisième partie: L'algèbre. Musier, Paris.

Bullynck, M., 2006. Vom Zeitalter der Formalen Wissenschaften. Anleitung zur Verarbeitung von Erkenntnissen anno 1800, vermittelst einer parallelen Geschichte. PhD-Thesis, University of Gent, Belgium. Defended 22.3.2006, accessible under www.kuttaka.org/ZfW.pdf.

Bullynck, M., 2007. A note on article 36 in Gauss's *Disquisitiones*. A ramificated story in the margin of the re-writing of section II. Bulletin of the Belgian Mathematical Society – Simon Stevin 13 (5), 945–947.

Bullynck, M., 2008a. The transmission of numeracy. Integrating reckoning in protestant North-German elementary education (1770-1810). (Historia Paedagogica, in print).

[68] See in particular [Schooten, 1659, 390–391 and 459–462].

Bullynck, M., 2008b. Decimal periods and their tables: A German research topic (1765-1801) (Historia Mathematica, forthcoming).

Burckhardt, J. K., 1798. Tafel, um jedes Jahr der Julian. Periode aus seinen Kennzeichen zu finden. Archiv der reinen und angewandten Mathematik 2 (5), 58–59.

Chuquet, N., 1484. Le Triparty en la Science des Nombres (Manuscript, Lyon). First part transcribed by A. Marre, Le Triparty en la Science des Nombres par Maistre Nicolas Chuquet, Parisien d'après le manuscrit Fond francaise n. 1346, Bulletino di Bibliografia e di Storia della Scienze Matematiche e Fisiche, Tomo XIII, 1880, 593-658, 693-814. The appendix partially transcribed by A. Marre, Appendice au Triparty en la science des nombres de Nicolas Chuquet Parisien, Bulletino di Bibliografia e di Storia della Scienze Matematiche e Fisiche, Tomo XIV, 1881, 413-460.

Clausberg, C. v., 1732. Demonstrative Rechenkunst, oder Wissenschaft, gründlich und kurz zu rechnen; Worinnen nicht nur sowohl die gemeinen, als allerhand vortheilhafte Rechnungs=arten überhaupt, nebst sehr compendiösen Proben, sondern auch die Wechsel=, Arbitragen= und andere kaufmännische Rechnungen auf eine sonderbare, kurze Manier gründlich und deutlich gelhret, anbey eine Beschreibung der Europäischen Münzen, Wechsel=Arten und Usanzen, auch Vergleichung der Gewichte und Ellen=Maasse; nicht weniger die wahre Berechnung des Interusurii, wie auch unterschiedene andere Mathematische und curiöse Rechnungen; imgleichen eine Probe einer bus auf 32 Ziffern verfertigten neuen Logarithmischen Tabelle. Auf Kosten des Autoris gedruckt, Leipzig, reprints until 1795.

Dickson, L., 1919–1927. History of the Theory of Numbers. Carnegie Institute, Washington, 3 Vol.

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

Euler, L., 1734/5. Solutio problematis arithmetici de inveniendo numero qui per datos numeros divisus relinquat data residua. Comm. Ac. Petrop. 7 (1734/5), 1740, 46–66, also in: Euler 1907, vol. 1, 18–32.

Euler, L., 1765/7. De usu novi algorithmi in problemate pelliano solvendo. N. Comm. Ac. Petrop. 11 (1765), 1767, 28–66, also in: Euler 1907, vol. 2, 74–111.

Euler, L., 1770. Vollständige Anleitung zur Algebra, 2 Bde. Kays. Acad. der Wissenschaften St. Petersburg, St. Petersburg.

Euler, L., 1783 and 1785. Opuscula Analytica, 2 volumes (1783 and 1785). Kays. Acad. der Wissenschaften St. Petersburg, St. Petersburg.

Euler, L., 1907. Commentationes Arithmeticae. Teubner, Leipzig, Berlin (2 Vol. = Leonhardi Euleri Opera Omnia. Series I. Volumen 2 and 3).

Fellmann, E., 1995. Leonhard Euler. Rowohlt, Reinbeck.

Folta, J., 1973. Remarks on the axiomatic development of mathematics in the second half of the Eighteenth Century (A.G. Kästner, J.H. Lambert) (in czech). DVT-Dejiny Ved a Techniky 6, 189–205.

Gauss, C. F., 1797. Elementa doctrina residuorum. Handschrift: Artikel 1-18,

23-38, 50-75, 79-85 in NL Dirichlet 31 (Berlin-Brandenburgische Akademie der Wissenschaften - Akademiearchiv); Artikel 39-50 in 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.

Gauss, C. F., 1801. Disquisitiones Arithmeticae. Fleischer, Leipzig. (Reprint Bruxelles: Culture et Civilisation, 1968) Also [Gauss, 1863-1929, Vol. 1].

Gauss, C. F., 1863-1929. Werke. Göttingen, Königliche Gesellschaft der Wissenschaften zu Göttingen. (Reprint Hildesheim, New York: Olms, 1973)

Gebhardt, R., 1999. Simon Jacob (1510–1564). In: Gebhardt, R. (ed.): Rechenbücher und mathematische Texte der frühen Neuzeit. Schriften des Adam-Ries-Bundes Annaberg-Buchholz Bd. 11. Adam-Ries-Bund, Annaberg-Buchholz, pp. 151–166

Goldstein, C., 2004. L'arithmétique de Pierre Fermat dans le contexte de la correspondance de Mersenne : Une approche micro-sociale. Sciences et techniques en perspective 8, 14–47, IIe séries.

Graham, R. L., Knuth, D. E., Patashnik, O., 1994. Concrete Mathematics. A Foundation for Computer Science. Addison-Wesley, Reading, Massachusetts, 2nd Edition.

Heeffer, A., 2006. Récréations mathématiques (1624) a study of its authorship, sources and influence. Gibecière 1 (2), 79–170.

Heeffer, A., 2007. The origin of problems in Euler's Algebra. Bulletin of the Belgian Mathematical Society – Simon Stevin 13 (5), 949–952.

Hindenburg, C. F., 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.

Hindenburg, C. F., 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), 281–324.

HM, 2003. Concept of equivalence relation. Historia Matematica (mailing list) Volume 05 (Number 095), (Thursday, September 25).

Hogendijk, J., 2002. Anthyphairetic ratio theory in medieval islamic mathematics. In: Y. Dold-Samplanius, J.W. Dauben, M. Folkerts and B. van Dalen (Ed.), *From China to Paris: 2000 years transmission of mathematical ideas*. Stuttgart, Franz Steiner Verlag, 187–202.

Jacob, S., 1565. Ein New und Wolgegründt Rechenbuch Auff den Linien vnd Ziffern, sampt der Welschen Practic vnd allerley Vortheilen, neben der Extraction Radicum, vnd von den Proportionen; mit vielen lustigen Fragen vnd Auffgaben, [et]c.; Deßgleichen ein vollkommener Bericht der Regel Falsi, mit

newen Inuentionibus, Demonstrationibus, vnd Vortheilen, so bi anher für vnmüglich geschetzt, gebessert, dergleichen noch nie an Tag kommen; Vnd dann von der Geometria, wie man mancherley Felder vnd Ebne, auch allerley Corpora, Regularia vnd Jrregularia, messen, Aream finden vnd rechnen sol. Matthes Becker, Frankfurt-am-Main, Second edition 1600.

Jahnke, H.-N., 1990. Mathematik und Bildung in der Humboldtschen Bildungsreform. Vandenhoeck & Ruprecht, Göttingen.

Karsten, W. J. G., 1776. Lehrbegriff der gesamten Mathematik. Anton Ferdinand Röse, Greifswald, 2. Auflage.

Kästner, A. G., 1758. Anfangsgründe der Arithmetik, Geometrie, ebenen und sphärischen Trigonometrie und Perspectiv. Theil I, Abth. 1 of Anfangsgründe der Mathematik. Vandenhoeck, Göttingen.

Kästner, A. G., 1759. Anfangsgründe der angewandten Mathematik. Theil II of Anfangsgründe der Mathematik. Vandenhoeck, Göttingen.

Kästner, A. G., 1785. Euler, Opuscula Analytica, Rezension. Göttingische Anzeigen von Gelehrten Sachen, 1785, 54. St., 539–542.

Kästner, A. G., 1786. Fortsetzung der Rechenkunst in Anwendungen auf mancherley Geschäffte. Theil 1, Abth. 2 of Die mathematischen Anfangsgründe. Vandenhoeck, Göttingen.

Kästner, A. G., 1796. Geschichte der Mathematik seit der Wiederherstellung der Wissenschaften bis an das Ende des achtzehnten Jahrhunderts. Vandenhoek & Ruprecht, Göttingen, 3 Teile.

Kersey, J., 1673/ The elements of that mathematical art commonly called algebra expounded in four books. John Kersey, London.

Keunecke, H.-O., 1982. Johann Petreius (1497–1550). Mitteilungen des Vereins für Geschichte der Stadt Nrnberg 69, 110–129.

Lagny, T. F. de, 1733. Analyse générale ou Methodes nouvelles pour resoudre les problemes de tous les Genres & de tous les Degrez à l'infini. Vol. 11 of Memoires de l'Académie Royale des Sciences (Année 1720). Paris.

Lagrange, J. de, 1767a. Sur la solution des Problèmes indéterminés du second degré. Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlin 2, 165–310, also in: Lagrange 1867-1892, vol. 2, 377–539.

Lagrange, J. de, 1767b. Sur la résolution des équations numériques. Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlin 2, 311–352, also in: Lagrange 1867-1892, vol. 2, 539–578.

Lagrange, J. de, 1768. Addition au Mémoire sur résolution des équations numériques. Histoire de l'Académie Royale des Sciences et des Belles-Lettres de Berlin 3, 111–180, also in: Lagrange 1867-1892, vol. 2, 581–655.

Lagrange, J. de, 1798. Essai d'analyse numérique sur la transformation des fractions. Journal De l'école Polytechnique 2, 93–115, also in: Lagrange 1867-1892, vol. 7, 291–316.

Lagrange, J. de, 1867-1892. Oeuvres. Ed. by M.J.-A Serret. Gauthier-Villars, Paris, 14 volumes. (Reprint: Hildesheim, New York: Olms Verlag, 1973)

Lambert, J. H., 1758. Observationes variae in mathesin puram. Acta Helvetica 3, 128–168, also in [Lambert, 1946-1948, I, 16–51].

Lambert, J. H., 1765-1772. Beyträge zum Gebrauche der Mathematik und deren Anwendung. Buchhandlung der Realschule, Berlin, 3 Teile, davon 2. Teil in 2 Abschnitten (1765, 1770, 1772).

Lambert, J. H., 1767. Mémoire sur quelques propriétés remarquables des quantités transcendentes circulaires et logarithmiques. Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin XVII, 265–322.

Lambert, J. H., 1770. Zusätze zu den Logarithmischen und Trigonometrischen Tabellen. Spener'sche Buchhandlung, Berlin.

Lambert, J. H., 1770. Euler, Algebra, Rezension. Allgemeine deutsche Bibliothek, 1770, 13. Bd., 2. St., 544.

Lambert, J. H., 1771. Anlage zur Architectonic, oder Theorie des Ersten und des Einfachen in der philosophischen und mathematischen Erkenntniß. Hartknoch, Riga, reprint: Lambert 1965, Band III and IV.

Lambert, J. H., 1946-1948. Opera Mathematica. Ed. by A. Speiser. Orell Füßli, Zürich, 2 volumes.

Lambert, J. H., 1965. Philosophische schriften. Ed. by H.-W. Arndt, 7 Vol. (I-IV, VI-VII and IX). Olms, Hildesheim.

Lehmer, D. H., 1933. Numerical notations and their influence on mathematics. Mathematics News Letter 7 (6), 8–12.

Leurechon, J., 1624. Recreation Mathematique. Jean Appier Hanzelet, Pont-à-Mousson.

Leybourn, W., 1694. Pleasure with profit consisting of Recreations of Diverse Kinds, also a treatise to Algebra. Baldwin and Dunton, London.

Li, Y., Shen, K., 1987. Chinese Mathematics. Clarendon, Oxford.

Lüdicke, A. F., 1798. Eine bestimmte Aufgabe aus der unbestimmten Analytik, nebst einem Zusatze des Herausgebers. Archiv der reinen und angewandten Mathematik 2 (6), 206–220.

Merzbach, U., 1981. An early version of Gauss's Disquisitiones Arithmeticae. In: Dauben, J. (Ed.), 1981, *Mathematical Perspectives. Essays on Mathematics and Its Historical Development*. Academic Press, New York, 167–178.

Müller, C., 1904. Studien zur Geschichte der Mathematik insbesondere des mathematischen Unterrichts an der Universität Göttingen im 18. Jahrhundert. Abhandlungen zur Geschichte der Mathematischen Wissenschaften mit Einschluss ihrer Anwendungen 18, 51–143.

Pasquich, J., 1787. Über das größte gemeinschaftliche Maaß zwoer ganzen Zahlen. Leipziger Magazin für reine und angewandte Mathematik (1), 97–104.

Pisano, L., 1202. Liber Abaci. Translated by L.E. Sigler (2002), *Fibonacci's Liber Abaci. Leonardo Pisano's Book of Calculation*. Springer, New York, Berlin.

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

Riese, A., 1522. Rechnung auff der Linien unnd Federn. Erfurt, later, revised and expanded editions in 1544 and 1574.

Rolle, M., 1690. Traité d'algèbre, ou principes generaux pour resoudre les questions de mathematique. Michallet, Paris.

Rudolff, C., 1525. Behend vnnd Hubsch Rechnung durch die kunstreichen regeln Algebre so gemeinlicklich die Coss genent werden. Darinnen alles so treulich an tag gegeben, das auch allein auss vleissigem lesen on allen mundtliche vnterricht mag begriffen werden, etc. Vuolfius Cephaleus Joanni Jung, Strassburg.

Saunderson, N., 1740. Elements of Algebra. Cambridge University Press, Cambridge.

Schilling, C., Kramer, J. (Eds.), 1900. Carl Friedrich Gauss – Heinrich Wilhelm Matthias Olbers Briefwechsel. Springer, Berlin, 2 volumes. (Reprint Hildesheim: Olms Verlag, 1976)

Schmidt, F. and Stäckel, P. (Eds.), 1899. Briefwechsel zwischen Carl Friedrich Gauss und Wolfgang Bolyai. Teubner, Leipzig.

Schooten, F. van, 1657. Exercitationes Mathematicae. Elsevier, Leiden.

Schooten, F. van, 1659. Mathematische oeffeningen, begrepen in vijf boecken. Goedesbergh, Amsterdam.

Schreiber, P., 1995. A supplement to J. Shallit's paper 'Origins of the analysis of the Euclidean algorithm'. Historia Mathematica 22, 422–424.

Schwenter, D., Harsdörffer, G. P., 1636. Deliciae Physico-Mathematicae. Oder Mathematische vnd philosophische Erquickstunden. ... Darinnen Sechshundert Drey vnd Sechzig Schöne, Liebliche vnd Annehmliche Kunststücklein, Auffgaben vnd Fragen auß der Rechenkunst, Landtmessen, Perspectiv, Naturkündigung vnd andern Wissenschafften genommen, begriffen seindt. Allen Kunstliebenden zu Ehren, Nutz, Ergötzung des Gemüths vnd sonderbahren Wolgefallen am tag gegeben. Dümler, Nürnberg.

Shallit, J., 1994. Origins of the analysis of the Euclidean algorithm. Historia Mathematica 21, 401–419.

Simpson, Th., 1745. A Treatise of Algebra. John Nourse, London.

Srinivasiengar, C., 1967. The history of Ancient Indian Mathematics. World Press Private, Calcutta.

Stern, M., 1833. Theorie der Kettenbrüche und ihre Anwendung. Journal für die reine und angewandte Mathematik 10 (1), 1–22.

Sterner, M., 1891. Principielle Darstellung des Rechenunterrichts auf historischer Grundlage. I. Teil. Geschichte der Rechenkunst. Oldenbourg, München & Leipzig.

Stifel, M., 1544. Arithmetica Integra. Johann Petreius, Nürnberg.

Stifel, M., 1553. Die Coss Christoffe Rudolffs mit schönen Exempeln der Coss. Alexandrus Lutomyslensis, Königsberg.

Subskribentenliste, 1781. Liste der subskribenten. Nicht-paginiertes Vorwort, Leipziger Magazin zur Naturkunde, Mathematik und Oekonomie 1 (1).

Tropfke, J., 1980. Geschichte der Elementarmathematik. Bd. 1: Arithmetik und Algebra. De Gruyter, Berlin, New York, 4. Auflage, vollst. neu bearb. von Kurt Vogel, Karin Reich und Helmuth Gericke.

Valach, M., 1955. Vznik kodu a ciselné soustavy zbytkových tríd. Stroje na

zpracování informací 3, 211–245.
Vogel, K. (ed.), 1954. Die Practica des Algorismus Ratisbonensis. Ein Rechenbuch des Benediktinerklosters St. Emmeram aus der Mitte des 15. Jahrhunderts nach den Handschriften der Munchner Staatsbibliothek und der Stiftsbibliothek St. Florian. C.H. Beck, München.
Wallis, J., 1656-1657. Operum Mathematicorum. Lichfield, London, 2 Volumes.
Waltershausen, S. v., 1856. Gauss zum Gedächtnis. Hirzel, Wiesbaden.
Weil, A., 1984. Number Theory: An Approach through History from Hammurapi to Legendre. Birkhäuser, Boston.
Wolff, C., 1710. Anfangsgründe aller mathematischen Wissenschaften. Halle.
Wolff, C., 1732. Elementa Matheseos Universae. Tomus Primus qui commentationem de methodo mathematica, arithmeticam, geometram, trigonometriam planam & analisim, tam finitorum quam infinitorum complectitur. Bousquet, Genève, second revised and augmented edition.

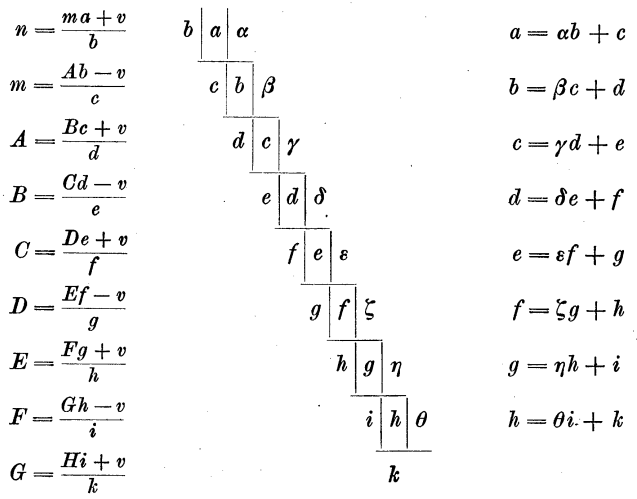

Figure 1: Euler's solution to the linear case (division procedure)