HISTORIA MATHEMATICA 21 (1994), 401–419

Origins of the Analysis of the Euclidean Algorithm

JEFFREY SHALLIT*,†

Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

The Euclidean algorithm for computing the greatest common divisor of two integers is, as D. E. Knuth has remarked, "the oldest nontrivial algorithm that has survived to the present day." Credit for the first analysis of the running time of the algorithm is traditionally assigned to Gabriel Lamé, for his 1844 paper. This article explores the historical origins of the analysis of the Euclidean algorithm. A weak bound on the running time of this algorithm was given as early as 1811 by Antoine-André-Louis Reynaud. Furthermore, Lamé's basic result was known to Émile Léger in 1837, and a complete, valid proof along different lines was given by Pierre-Joseph-Étienne Finck in 1841.

L'algorithme d'Euclide pour le calcul du plus grand commun diviseur de deux entiers est, comme l'a remarqué D. E. Knuth, "le plus ancien algorithme non trivial qui ait survécu à ce jour." C'est traditionnellement à Gabriel Lamé que l'on attribue la première analyse du temps de calcul de cet algorithme dans son article de 1844. Ici, on examine les origines historiques de l'analyse de l'algorithme d'Euclide. Antoine-André-Louis Reynaud a donné un majorant du temps de calcul de cet algorithme dès 1811. De plus, le résultat de base de Lamé était connu d'Émile Léger en 1837, et Pierre-Joseph-Étienne Finck en a donné une preuve complète et correcte, par des méthodes différentes en 1841.

Der Euklidische Algorithmus, um den größten gemeinsamen Teiler zweier ganzer Zahlen zu berechnen, ist, wie D. E. Knuth festgestellt hat, „der älteste nichttriviale Algorithmus, der bis zum heutigen Tage überlebt hat." Anerkennung für die erste Untersuchung der Laufzeit des Algorithmus wird traditionsgemäß Gabriel Lamé für seine Schrift aus dem Jahr 1844 gezollt. In vorliegendem Artikel wird den historischen Ursprung der Untersuchung des Euklidischen Algorithmus dargelegt. Antoine-André-Louis Reynaud hatte bereits vor 1811 eine grobe Schranke der Laufzeit dieses Algorithmus. Außerdem war Lamés grundlegendes Ergebnis bereits 1837 Émile Léger bekannt, und Pierre-Joseph-Étienne Finck hatte 1841 mit anderen Methoden einen kompletten, stichhaltigen Beweis gefunden.

MSC 1991 subject classifications: 01A50, 01A55, 01A70, 11A05
KEY WORDS: analysis of algorithms, Euclidean algorithm

1. INTRODUCTION

By the *analysis* of an algorithm we mean the determination of good bounds (especially upper) for the algorithm's consumption of resources, such as time and space. Such bounds are generally expressed in terms of the *size* of the inputs, or in the case of integer inputs, in terms of the inputs themselves. The analysis of

* Supported in part by a grant from NSERC. Partial support from NSF Grant DCR 920-8639 and the Wisconsin Alumni Research Foundation.
† E-mail: shallit@graceland.uwaterloo.ca.

0315-0860/94 $6.00

algorithms has become a fundamental field of study in computer science. As D. E. Knuth said in 1970:

> The advent of high-speed computing machines, which are capable of carrying out algorithms so faithfully, has led to intensive studies of the properties of algorithms, opening up a fertile field for mathematical investigations. Every reasonable algorithm suggests interesting questions of a "pure mathematical" nature; and the answers to these questions sometimes lead to useful applications, thereby adding a little vigor to the subject without spoiling its beauty. [40, 269]

Despite the emergence in the last thirty years of the analysis of algorithms as a field in its own right, there has been relatively little historical discussion of the origins of this field. Questions such as *Who was the first to recognize that algorithms could be analyzed?* and *Who was the first to give an analysis of an algorithm?* are legitimate subjects for historical inquiry.

Of course, the answers to these questions are necessarily fuzzy, because of the vagueness of the definitions of "algorithm" and "analysis." For example, algorithms were given by the Babylonians as early as 1800 B.C.E. [51, 42], but they apparently did not discuss the "running time" of their algorithms. The Greeks contributed Euclid's algorithm (ca. 300 B.C.E.) and the sieve of Eratosthenes (ca. 250 B.C.E.) for creating a list of prime numbers, but no explicit evidence survives to suggest that they considered the number of operations required. In the early 13th century, Fibonacci observed that to determine if a number n is prime, it suffices to divide by the integers $\leq \sqrt{n}$ [21, 38]; here, merely stating the result implies a complexity bound on the problem of testing primality.

Closer to the present day, Gauss's *Disquisitiones* is sprinkled with remarks about efficiency of algorithms. But his remarks are always qualitative, rather than quantitative in nature. For example, in discussing Euler's criterion for determining the quadratic character of a modulo p, Gauss wrote: ". . . as soon as the numbers we are examining are even moderately large this criterion is practically useless because of the amount of calculation involved." [31, Art. 106].

In this paper, I will focus on one particular algorithm of great importance, the Euclidean algorithm for computing the greatest common divisor of two integers, and discuss some 19th-century attempts to analyze this algorithm, one as early as 1811. I know of no other algorithm that received any analysis before this date.

The article will focus on four French mathematicians of the early 19th century. For a thorough examination of this period, see [34].

I will first mention the work of Gabriel Lamé, to whom the credit for analyzing the Euclidean algorithm is usually given. Then I will discuss the life and work of four other French mathematicians, Antoine-André-Louis Reynaud, Émile Léger, Pierre-Joseph-Étienne Finck, and Jacques Philippe Marie Binet, all of whom analyzed algorithms for the greatest common divisor before Lamé.

It may be worth reminding the reader of the details of the Euclidean algorithm.[1] Let u_0 and u_1 be positive integers. Write

[1] Of course, the greatest common divisor of two numbers u and v may also be determined by first computing their prime factorizations $u = p_1^{e_1} \cdots p_k^{e_k}$ and $v = p_1^{f_1} \cdots p_k^{f_k}$, and then using the formula $\gcd(u, v) = p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)}$. This method is not currently practical for large numbers, since there is no known fast algorithm for integer factorization.

$$\begin{aligned} u_0 &= q_0 u_1 + u_2 \\ u_1 &= q_1 u_2 + u_3 \\ &\vdots \\ u_{n-1} &= q_{n-1} u_n + u_{n+1}, \end{aligned}$$

where $0 = u_{n+1} < u_n < \cdots < u_2 < u_1$. Then $u_n = \gcd(u_0, u_1)$.

We define $E(u_0, u_1)$ to be the number of *division steps* performed by the algorithm on input (u_0, u_1), and we see that $E(u_0, u_1) = n$. It can be proved by induction that if $u > v > 0$, $E(u, v) = n$, and u is as small as possible, then $(u, v) = (F_{n+2}, F_{n+1})$, where F_k denotes the kth Fibonacci number, defined by $F_0 = 0$; $F_1 = 1$; and $F_{k+2} = F_{k+1} + F_k$ for $k \geq 0$.

The Euclidean algorithm appeared in Euclid's *Elements*, Book VII, Proposition 2 [37]; also see Book X, Propositions 1–4. However, the idea is likely to have been known previously. Quoting Knuth again, "[w]e might call it the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day" [41, 318]. (For a brief discussion of modern work on the analysis of the Euclidean algorithm, see [42].)

2. GABRIEL LAMÉ

Gabriel Lamé (see Fig. 1) was a famous French mathematician who was primarily interested in geometry, thermodynamics, applied mechanics, and number theory. Since the life and work of Lamé has been covered at length elsewhere in easily available sources (such as [9; 32, 601–602; 13]), I will not discuss it further here.

In his well-known 1844 paper [45], Lamé proved that if $u > v > 0$, then the number of division steps $E(u, v)$ performed by the Euclidean algorithm is always less than 5 times the number of decimal digits in v.

The method of proof used by Lamé was as follows: first, he proved that, for all k, there are at most five Fibonacci numbers whose decimal expansions contain k digits.[2] Then, given an arbitrary input u_0 and u_1 to the algorithm, he considered how the sequence $u_2, u_3, \ldots, u_n$ of remainders determined by the algorithm are distributed among the intervals given by successive Fibonacci numbers, $[F_k, F_{k+1}]$. He showed (i) no more than two remainders can appear between successive Fibonacci numbers and (ii) when two such remainders appear in an interval $[F_k, F_{k+1}]$, the following interval $[F_{k-1}, F_k]$ contains no remainder. The result now follows.

Lamé's result, though correct, can nevertheless be criticized on several grounds. First, he did not explicitly note that the "worst case" of the Euclidean algorithm (in the sense of the lexicographically least pair (u, v) with $u > v > 0$ such that the Euclidean algorithm performs n steps) occurs when the inputs are successive Fibonacci numbers. Second, his proof is much more cumbersome than necessary.

[2] Of course, Lamé did not call them "Fibonacci numbers"; it was Édouard Lucas (1842–1891) who popularized the name.

FIG. 1. Gabriel Lamé (courtesy David Eugene Smith collection, Columbia University).

For a simpler proof, see, for example, [36]. Third, the number 5 is somewhat artificial. It is actually possible to show, for example, that $E(u, v) < 4.79 \log_{10} v$, for all v sufficiently large. (Here "4.79" is an approximation to $1/\log_{10} \alpha$, where $\alpha = (1 + \sqrt{5})/2$.)

In modern terms, the result of Lamé would typically be expressed as follows: if $u > v > 0$, then $E(u, v) = O(\log v)$. With the modern approach of asymptotic analysis of algorithms, it is the $\log v$ term that matters; the constant in front of this term is regarded as relatively unimportant.

3. PREVIOUS ANALYSIS OF THE EUCLIDEAN ALGORITHM

Although Lamé is generally recognized as the first to analyze the Euclidean algorithm in his 1844 paper, in fact there was much previous work on this problem.

For example, as pointed out in [33, 290], in 1733 Thomas Fantet de Lagny (1660–1734) (see Fig. 2) described his *"théorie générale des rapports"*; this was essentially based on the terms of the simple continued fraction expansion of the quotient of two integers. He divided the *rapports* into different *genres*, depending on the length of the continued fraction expansion. He also introduced a method of calculation that is essentially what we call *continuants* today. As an example, de Lagny gave (what would now be called) the series of convergents to $(1 + \sqrt{5})/2$:

FIG. 2. Thomas Fantet de Lagny (courtesy Bibliothèque Municipale de Lyon). (B. M. Lyon Coste 13 896; Cliché B. M. Lyon (Didier Nicole))

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \frac{89}{55}, \frac{144}{89}, \ldots$$

and remarked:

> Pour démontrer *à priori* que cette série comprend les rapports les plus simples de tous les genres à l'infini, il suffit de démontrer qu'un rapport quelconque, par exemple, celui du cinquième genre 13/8: or cela est évident par la formation, puisqu'il contient tous les rapports les plus simples que le précédent & qu'il les surpasse: car il contient & surpasse le plus simple rapport du quatrième genre 8/5; & en rétrogradant de même jusqu'à l'origine, on trouvera qu'il contient & surpasse le rapport du troisième genre 5/3, celui du second genre 3/2, celui du premier genre d'inégalité 2/1, & enfin qu'il contient & surpasse 1/1 qui est le rapport d'égalité, le premier & le plus simple de tous les rapports.

> Comme la même chose se trouve dans chacun des rapports de cette série, il suit delà que la série continuée à l'infini comprend par ordre les rapports les plus simples de tous les genres à l'infini.
>
> On démontrera encore la même chose *à posteriori* par la division: car on trouvera que chacun des rapports pris à discrétion dans la série, comme ici le rapport du cinquième genre 13/8, contient tous les rapports les plus simples des genres précédens dans la série, & il est évident que chacun de ces rapports est le premier & le plus simple de son genre, puisque chaque quotient est l'unité, excepté le dernier quotient 2, qui ne put être moindre dans le rapport d'inégalité, ce qui est de l'essence du rapport d'inégalité. [43, 363–364]

To modern eyes, de Lagny's argument is not rigorous, but it seems clear that he was attempting to argue that the quotients of adjacent Fibonacci numbers provided the "simplest" fraction that resulted in a continued fraction expansion having a given length. In other words, the inputs $(u, v) = (F_{n+2}, F_{n+1})$ elicit the worst-case behavior of the Euclidean algorithm. However, de Lagny did not explicitly make the connection between his results and the Euclidean algorithm, and therefore cannot really be said to have "analyzed an algorithm."

For biographical details on de Lagny, see [32, 558–559].

Moving into the 19th century, let us recall that the opening sentence of Lamé's 1844 paper reads as follows:

> Dans les traités d'Arithmétique, on se contente de dire que le nombre des divisions à effectuer, dans la recherche du plus grand commun diviseur entre deux entiers, *ne pourra pas surpasser la moitié du plus petit.* [45, 867]

In modern notation, we understand that Lamé is referring to some previous observation that $E(u, v) \leq v/2$. An interesting question is: which *"traité d'Arithmétique"* did Lamé have in mind? His paper gives no explicit clue, but it is certainly reasonable to believe it was a well-known work available in France in 1844.

In attempting to answer this question, one problem is immediate: the French term *"arithmétique"* is ambiguous. It can refer either to the English "arithmetic" or to "number theory." Which did Lamé intend? Most likely, he meant introductory books on arithmetic, such as those intended to prepare students for admission to the *École Polytechnique*. There were very few books available in France at that time on pure number theory, and none of them seems to discuss the running time of the Euclidean algorithm.

However, publication records (e.g., [7; 8]) reveal that at least 40 books on arithmetic were published in France between 1780 and 1844. Most of these discussed Euclid's algorithm in a section on the arithmetic of rational fractions, since it is useful for placing fractions in lowest terms. A method based on trial division by prime numbers was also frequently discussed.

Some books of the period compared the relative efficiency of these two methods. For example, the English mathematician, Peter Barlow, wrote in 1811 that

> . . . this method [for computing the greatest common divisor by means of the prime factorization] is, however, rather theoretical than practical, being by no means so ready in application as the rule generally given [i.e., the Euclidean algorithm] for this purpose in books of arithmetic. [6, 22]

Of the arithmetics of the time and place, one stands out above all others: the *Arithmétique* of Étienne Bezout (1730–1783). Bezout was one of the most renowned French mathematicians of the period, and his *Cours de mathématiques à l'usage des gardes du pavillon et de la marine* first appeared in 1764. The first volume of this work was entitled *Arithmétique,* and it went through dozens of editions, first under Bezout's own direction, and, after his death, at the hands of others. According to Crosland [15, 11], even Napoleon I learned mathematics from Bezout's books.

Contemporary views of Bezout's *Arithmétique* varied. For example, the possibly pseudonymous author, Prince, remarked in the introduction to his 1812 edition [55], "[l]'arithmétique de Bezout est certainement une des meilleures, sur-tout pour la clarté . . . ." Peyrard was less generous, remarking [53] that "[i]l y a dans Bezout des démonstrations qui manquent de clarté . . . ." Nevertheless, it is clear that Bezout's *Arithmétique* was the standard by which arithmetics of the time were measured.

We will see below that Antoine-André-Louis Reynaud remarked that $E(u, v) < v/2$ in his 1821 edition of Bezout's *Arithmétique*. Is there any reason to believe that this was the *"traité d'arithmétique"* that Lamé had in mind? The answer is almost certainly yes. First, Reynaud's various editions of Bezout's *Arithmétique* were extraordinarily popular in France, with one going through at least 26 different editions. (His major competitor was Silvestre-François Lacrois, whose *Traité élémentaire d'arithmétique* went through at least 18 editions. For more information on French mathematical textbooks of the time, see [17–19].) Second, very few other books of the time on arithmetic (including Lacroix's) contained any discussion of the number of division steps in the Euclidean algorithm. The only exceptions I am aware of are the books of P.-F. Amadieu [1, 200, Remarque III], Prince's edition of Bezout's *Arithmétique* [55, 107, Note 54], and Finck's books [22; 24] (discussed below). Third, the wording used by Lamé coincides very closely with that used by Reynaud.

4. ANTOINE-ANDRÉ-LOUIS REYNAUD

4.1. Life of Reynaud[3]

Antoine-André-Louis Reynaud was born on September 12, 1771,[4] in Paris, the son of a well-known lawyer at the Paris parliament. As a young man he distinguished himself for his literary studies, writing dramatic compositions at the age of 15 and later, a patriotic play on the subject of the taking of Toulon.

Reynaud enthusiastically embraced the principles of the French Revolution. In 1790 he was named *Capitaine au Régiment d'Élèves.* In 1792, he entered the *Garde Nationale.* He wished to pursue a military career, but following the wishes

[3] The account of Reynaud's life that follows is based on archives of the *École Polytechnique* and the contemporary work of Sarrut and Saint-Edme [63, Tome III, 2^{e} partie, 156–161]. Also see [30, 188–189; 38, Vol. 41, 77–79; 46, Vol. 10, 1135; 56, Vol. VII, 567–568].

[4] Some sources, such as [56] and the files of the *École Polytechnique,* give a birth year of 1777.

of his family, he instead began a career as an accountant in the *Compatibilité Nationale,* where he was employed for four years. However, not finding the work to his liking, he spent his evenings studying mathematics on his own, and in 1796 he was admitted to the *École Polytechnique.*

Reynaud was first in his graduating class of 1798, and was assigned to the *corps des Ponts et Chaussées* on December 28 of that year. However, he was allowed to spend a third year at the *École Polytechnique,* where he was *chef de brigade* until November 22, 1799.

In 1800, Butet de la Sarthe founded the *École Polymathique* [15, 197], intended to prepare students for the *École Polytechnique,* and Reynaud, without salary, took on the duties of teaching mathematics at this school. He also taught at the *lycée du Palais-Royal.*

On November 22, 1804, Reynaud was appointed *répétiteur d'analyse* at the *École Polytechnique,* a position he filled until August 28, 1814. In 1806, Reynaud was put in charge of the public land-survey in France. He also published a manual containing the mathematics necessary for surveyors. In 1809 he was named as a temporary admissions examiner for the *École Polytechnique.* This post was made permanent on August 28, 1814, and Reynaud continued performing these duties until July 1, 1837, when he began his retirement.

In the years 1808 and 1811 Reynaud assisted Gaspard de Prony with a course in mechanics. It was here that Reynaud may have gained an interest in efficient computation, since de Prony had directed a huge project to compute mathematical tables [35]. Between 1812 and 1814, he gave a *cours d'analyse* in place of Louis Poinsot. (This course was given the next year by Cauchy [29].)

Tired of the conflicts that followed the French Revolution, Reynaud decided in 1814 that liberal institutions sponsored by Louis XVIII would be best for the future of France, and he devoted himself to these. He therefore showed no enthusiasm for the return of Napoleon during the Hundred Days.

Reynaud received many honors, including being named *docteur de la Faculté des Sciences* in 1812; member of the *Académie des Sciences et Belles-Lettres* of Lyon in 1813; *chevalier de la Légion d'Honneur* on December 13, 1814; member of the *Académie des Sciences et Belles-Lettres* at Le Mans in 1817; Tours in 1824; *chevalier de l'Ordre de Saint-Michel* on March 22, 1823; Baron in 1823; etc. In 1824 he was chosen by the Marquis of Bouthillier to head the new Forestry School at Nancy.

In his later years, Reynaud devoted himself to such projects as the improvement of the *École Navale* at Brest (1834), entrance examination of students at the *Marine Royale,* and similar duties. He became an officer of the *Légion d'Honneur* on May 30, 1837. He published many books, including (in addition to those mentioned previously) *Traité d'algèbre, Trigonométrie rectiligne et sphérique, Théorèmes et problèmes de géométrie,* and *Traité de statistique.*

Reynaud died in Paris on February 24, 1844.

4.2. Work of Reynaud

In 1811, Reynaud made the following observation:

> Le nombre de divisions à effectuer, pour obtenir le plus grand commun diviseur entre deux nombres, ne peut jamais excéder le plus petit des deux nombres proposés, car chaque reste étant un nombre entier moindre que le diviseur, les restes diminuent au moins d'une unité à chaque division; de sorte qu'on parviendra au reste zéro, après un nombre de divisions tout au plus égal au plus petit des deux nombres proposés. [58, 34, Note 60]

In modern terms, Reynaud proved that $E(u, v) \leq v$. Today, this bound would be regarded as trivial. The result is noteworthy nevertheless because it seems to be the *first explicit analysis* of the Euclidean algorithm. Reynaud's 1804 book [57] does *not* contain a similar remark, so we may suppose that Reynaud first considered the quantity $E(u, v)$ between 1804 and 1811.

In 1821, in the 9th edition of his *Traité d'arithmétique*, Reynaud improved his result as follows:

> Le nombre de divisions à effecteur pour obtenir le plus grand commun diviseur, ne peut jamais excéder la moitié du plus petit des deux nombres proposés; car lorsqu'on parvient à deux restes consécutifs dont la différence est l'unité, la division de ces deux restes l'un par l'autre conduit au reste 1, ce qui indique que les nombres donnés n'ont pas de facteurs communs; et par conséquent, toutes les fois que les nombres proposès ont un plus grand commun diviseur, les restes successifs diminuent au moins de deux unités à chaque division. [60, Section 27, 367]

An essentially identical paragraph also appears in [61, 36]. (No such improvement appeared in [59], the 8th edition of *Traité d'arithmétique*, so we may suppose that Reynaud improved his result sometime between 1816 and 1821.)

This paragraph, which seems to claim a proof of the inequality $E(u, v) \leq v/2$, requires some clarification. Although the general idea is valid, the inequality $E(u, v) \leq v/2$ actually is false! (This was observed by Lamé [45].) Several small counterexamples, such as $E(5, 3) = 3$ and $E(8, 5) = 4$, are easily produced. A more careful reading, however, suggests that Reynaud actually proposed a slight *modification* to Euclid's algorithm: namely, that when two consecutive remainders differing by 1 are encountered, then the algorithm should be terminated immediately. Under this interpretation, Reynaud actually claimed $E(u, v) \leq v/2 + 2$, a correct inequality.

This interpretation of a modified Euclid's algorithm is supported by a similar result given by P.-F. Amadieu in 1839:

> *Le plus grand nombre de divisions que l'on puisse faire en cherchant le plus grand commun diviseur de deux nombres est égal à la moitié du plus petit nombre.*
>
> En effet, si deux restes consécutifs ne différaient que d'une unité, ces restes seraient premiers entre eux, et les nombres donnés le seraient aussi: il serait donc inutile de continuer l'opération. Ainsi, tant que l'opération ne sera pas arrêtée, deux restes consécutifs différeront au moins de deux unités. Dès-lors le premier reste sera au plus égal au plus petit nombre diminué de deux unités, et les restes suivans diminueront à chaque division au moins de deux unités. Donc, le nombre de ces restes ou le nombre des divisions qu'on aura à effectuer sera au plus égal au nombre de fois que 2 sera contenu dans le plus petit nombre, c'est-à-dire à la moitié du plus petit nombre. C. Q. F. D. [1, 200, Remarque III]

5. ÉMILE LÉGER

5.1. Life of Léger[5]

Émile Léger was born in Lagrange-aux-Bois, France, on August 15, 1795, son of Claude Léger, a humanist and literary figure. After his father obtained a chair in rhetoric at the *Lycée de Mayence,* Léger studied for two years under Olry Terquem, editor of the *Nouvelles annales de mathématiques.* In 1813, he was admitted to the *École Polytechnique.* Napoleon Bonaparte returned to Paris in March 1815 (the "Hundred Days"), and the students of the *École Polytechnique* were called to defend the capital [29, 330]. Léger received *"trois coups de lance"* while defending a post on the *route de Vincennes.* In 1816, he left the *École Polytechnique* and returned to live with his family at Montmorency, where his father, Claude, had started an educational institution. When Claude became too old to continue his teaching duties, Émile took over with enthusiasm. Each year, the school sent students to prestigious schools such as the *École Polytechnique.* During his short career, Léger published four brief papers (see [62, Vol. III, 932]). He died in Paris on December 15, 1838, at the age of 43.

5.2. Work of Léger

Émile Léger appears to have been the first (or the second, if the work of de Lagny mentioned above is counted) to recognize that the worst case of the Euclidean algorithm occurs when the inputs are consecutive Fibonacci numbers.

In a short paper of 1837, published seven years before the paper of Lamé, Léger discussed the continued fraction

$$1+\cfrac{1}{1+\cfrac{1}{1+\cdots+\cfrac{1}{1}}} \tag{1}$$

and wrote

> Le fraction continue (1) conduit à la solution d'un problème curieux: Dans la recherche du plus grand commun diviseur de deux nombres donnés, quel est le plus grand nombre d'opérations qu'on puisse avoir à faire?
> Les réduites de la fraction (1)
>
> $$\frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \frac{89}{55}, \text{etc.} \tag{2}$$
>
> sont les fractions qui conduisent au plus grand nombre d'opérations; il suffit donc, étant donnée une fraction quelconque, de déterminer la première de ces réduites qui a un dénominateur plus grand que cette fraction donnée, le rang de cette réduite fera connaître la limite cherchée. [47]

However, Léger did not give any rigorous proof of his assertions.

[5] This account of Léger's life is taken from the obituary by Olry Terquem [65], with details added from the archives of the *École Polytechnique.*

6. PIERRE-JOSEPH-ÉTIENNE FINCK

6.1. Life of Finck[6]

Pierre-Joseph-Étienne Finck was born in Lauterbourg, a small town in what is now the department of the Bas-Rhin in France, adjacent to the German border, on October 15, 1797 (24 vendémiaire an VI) at five in the morning [4, #22]. His father, Jean-Pierre Finck (b. ca. 1758), was a civil registrar (*"receveur de l'enregistrement"*) who died on October 2, 1810 in Klingenmünster. His mother was Françoise Eléonore Catherine Bailleul; she died on April 24, 1810. Thus left an orphan at age 12, Finck was adopted by a wholesaler (*"négociant"*) named Botta [39, 373] from the town of Landau in der Pfalz.

In 1815, Finck was admitted to the *École Polytechnique* in Paris. His rank was sixth upon admission. He was named corporal for the school year 1815–1816. Finck was graduated in 1817, with a class rank of 19 from a total of 72 students. He was admitted to the service of the *Artillerie de Terre* on 10 December 1817, the third on a list of 25 students.

However, the Artillery School was apparently not to Finck's liking, for he wrote to the Comte de Gouvion Saint-Cyr on March 25, 1818, expressing his desire to leave the school in order to enter into a light-cavalry regiment of the Royal Guard. Accompanying this request was a letter from a superior officer, which explained that Finck found his studies boring, and complaining about his frivolous behavior (*"conduite légère"*). Finck's request was turned down. On July 21, 1818, Finck reiterated his request to obtain the rank of second lieutenant in the Royal Guard, saying that if this request could not be fulfilled, then he would submit his resignation. The resignation was accepted on July 30, 1818.

A year later, on March 22, 1819, Finck wrote once again to the Comte de Gouvion Saint-Cyr, explaining that his resignation in 1818 from the Artillery School was, in fact, due to a trial in Landau that necessitated his presence (a reason not mentioned at all in his previous requests), and requesting readmission to the Artillery School. (Finck's military record contains a skeptical note appended to this letter, penned by an officer examining Finck's request.) However, this request was also turned down.

Finck moved back to Strasbourg sometime before 1821, and later resumed his education, enrolling in the *Faculté des Sciences de Strasbourg,* and receiving the degree of *bachelier à sciences mathématiques* on August 28, 1827 [3]. On November 13, 1827, he received the degree of *licencié ès sciences mathématiques* for a thesis entitled *Les machines en mouvement*. Later, on July 25, 1829 (one source gives a different date of September 12, 1829), he received the degree of *docteur ès sciences mathématiques*. The title of his doctoral thesis was *Sur les mouvements de l'équateur terrestre* [4, #112].

[6] This account of Finck's life is based on records of the *École Polytechnique;* French military records; the *Archives municipales* of Strasbourg; the *Archives départementales du Bas-Rhin* [2; 3]; the *Archives Nationales* in Paris [4]; and the biographies in [64, 497; 5, 941; 16, Vol. 13, 1369; 44, Vol. 17, 484–485].

Sometime before 1821, Finck married Madeleine Weiss, the Landau-born daughter of Simon Weiss, a custom shoemaker, and Catherine Bollinger; they had six children. However, Madeleine died on July 9, 1840, at the age of 41, of uterine cancer. Finck was remarried on April 21, 1841, to Fanny de Fuchsamberg (born November 10, 1797, in Besançon). They had no children.

Finck became *répetiteur de mathématiques* at the *École d'Artillerie de Strasbourg* on January 21, 1825, and was promoted to *professeur* on May 1, 1827. He also was appointed to teach a course of *mathématiques spéciales* at the *Collège de Strasbourg,* beginning October 9, 1827, as a replacement for the retiring Jean-Joseph Bedel (b. March 23, 1767). On September 8, 1829, Finck was provisionally promoted to *professeur de mathématiques spéciales* at the *Collège de Strasbourg,* an appointment which was made permanent on October 2, 1833.

Like most Frenchmen, Finck apparently would have preferred an appointment at Paris [4, #58]. But the French *cumul* system, which allowed him to simultaneously hold posts at the *École d'Artillerie* and the *Collège de Strasbourg,* afforded him a degree of financial security at Strasbourg that he would have had difficulty matching in the capital.

On February 26, 1842, Finck was provisionally appointed to replace Jorlin in the position of *professeur de mathématiques appliquées* of the *Faculté des Sciences de Strasbourg.* When Jorlin retired on January 1, 1847, the *Faculté des Sciences* instituted a search for a new chair of applied mathematics. The search narrowed to four candidates, including Finck, Louis-Auguste-Jean Banet, and Alexandre-Charles-Augustin Guiot, and Finck was appointed to this position on May 6, 1847.

During his academic career, Finck wrote more than 20 papers which appeared in the *Journal de mathématiques pures et appliquées, Nouvelles annales de mathématiques,* and the *Comptes rendus de l'Académie des Sciences de Paris.* Several of his papers refer to efficient methods of calculation; see, for example, [25; 26; 28]. A nearly complete list can be found in [62, Vol. II, 612].[7] Finck also wrote seven textbooks, including *Éléments d'algèbre, Géométrie élémentaire basée sur la théorie des infiniments petits, Mécanique rationnelle,* and *Principes de l'analyse infinitésimale.* His *Algèbre* won praise from Olry Terquem, who called it *"le seul ouvrage français où l'on explique ces logarithmes* [*de Gauss*]."

Finck was a patron of the literary arts at Strasbourg; the *Renseignements confidentiels* form of 1862 noted that

> M. Finck est un des rares mathématiciens qui attachent une grande importance aux études littéraires. [4, #35]

He also loved languages, and in addition to French, spoke and wrote German, and read English, Danish, Swedish, and Italian [4, #40].

Finck was highly respected as a scholar and teacher in Strasbourg. Comments in his personnel file include *"esprit de justice et d'impartialité"* (1859); *"savant*

[7] One paper missing from this list is [12]. For some mysterious reason, Finck's first initial is erroneously given as "B" in the Royal Society list, as well as in some of the papers he published.

estimé, professeur consciencieux, enseignement solide et méthodique" (1864). The only negative evaluations related to his blunt manner: "*caractère actif, droit, ferme, mais toujours trop brusque*" (1844–1845); "*parait avoir un peu corrigé la brusquerie qu'on lui reprochait avec tout de raison*" (1845–1846).

Finck's *Notice individuelle* of 1858 [4, #43] claims that he was awarded the *chevalier de la Légion d'Honneur* on March 14, 1857, but no independent confirmation of this has been found.

According to his *Notice individuelle* for 1863 [4, #33], Finck began to suffer ill health in 1862. On December 9, 1866 he was given the right to take sick leave for the school year 1866–1867, a request which was renewed the following year. Finck retired on December 1, 1868 [4, #3].

Finck died at Strasbourg on July 27, 1870, at the age of 72 years and 8 months, just eight days after the beginning of the Franco-Prussian war. The cause of death was given as senility ("*ramollissement cérébrale*").

6.2. *Work of Finck*

In his 1841 book, *Traité élémentaire d'arithmétique à l'usage des candidats aux écoles spéciales,* Finck discusses the Euclidean algorithm for computing the greatest common divisor of two integers:

> Chaque reste est moindre que la moitié du dividende: car si le diviseur est égal à la moitié du dividende, le reste est 0; si le diviseur est plus grand que cette moitié, le quotient est 1, et le reste, devant faire avec le diviseur une somme égale au dividende, sera moindre que cette même moitié; enfin, si le diviseur est plus petit que la moitié du dividende, le reste le sera aussi comme étant moindre que le diviseur. De là il suit que si l'on nomme A et B les deux nombres dont on cherche le p. g. c. d., A étant $> B$, les restes successifs sont respectivement moindres que $A/2, B/2, A/4, B/4, A/8, B/8, \ldots, A/2^n, B/2^n$; l'opération se terminera donc au plus tard lorsque $B/2^n \leq 2$, ou $B < 2^{n+1}$; car alors le reste moindre que $B/2^n$ sera au plus $= 1$, qui est le dernier diviseur; mais alors le nombre des divisions faites serait $2n + 1$. Ainsi, cherchez l'exposant de la plus petite puissance de 2, qui surpasse B, diminuez-le d'une unité, doublez le reste et ajoutez 1, ce sera une limite du nombre des opérations qu'il y aura à faire pour trouver le p. g. c. d. de A et B.
>
> Soit, pour exemple, les nombres 89 et 55: la plus petite puissance de 2, qui surpasse 55 est 64 ou 2^6; donc $n + 1 = 6$, $n = 5$ et $2n + 1 = 11$; et, en effet, dans ce cas, il faut neuf opérations. On a, du reste, $n + 1 > (\log B)/(\log 2)$, d'où $n > \frac{\log B}{\log 2} - 1$, et on peut remarquer que la limite est toujours moindre que $\frac{1}{2} B$.... [22, 44, Remarque 1]

In modern terms, then, Finck observed that if $u = qv + r$, then $r \leq u/2$. By iterating this observation, he proved the following bound on the number of division steps in the Euclidean algorithm: $E(u, v) \leq 2 \log_2 v + 1$. This bound is not quite as good as that given by Lamé (since $(2 \log_2 v)/(5 \log_{10} v) \doteq 1.329$). Nevertheless, in his 1841 book, Finck gave the first rigorous analysis of the Euclidean algorithm, and proved the fundamental result that $E(u, v) = O(\log v)$. Furthermore, the use of the consecutive Fibonacci numbers 89 and 55 in his example computation suggests strongly that Finck knew what the worst-case inputs to the algorithm really were.

Finck's proof has the great virtue of simplicity, a trait that led to its rediscovery by several others; for example, see [68, 141–143].

The final remark by Finck quoted above shows that he was well aware that his bound was superior to the bound $E(u, v) \leq v/2 + 2$ given previously in the book of Reynaud.

In 1842, Finck published a letter in which he drew attention to the problem of determining the number of operations required to compute the greatest common divisor of two numbers. He said:

> Dans ce même ouvrage . . . , j'ai entre autres questions, que l'on ne trouve pas dans les livres élémentaires, traité un problème qui est susceptible d'une solution plus complète: il a pour objet de déterminer le nombre des opérations de la recherche du p. g. c. d. de deux nombres entiers.
>
> On peut, pour arriver à ce but, suivre deux marches: l'une conduit aux séries récurrentes et à une équation exponentielle fort compliquée. Elle est fondée sur ce que le cas le plus défavorable est celui où tous les quotients sont égaux à l'unité, le dernier étant 2; de là on est amené à chercher le terme général de la suite
>
> $$1,\ 1 \cdot 1 + 1,\ (1 \cdot 1 + 1)1 + 1, \text{ etc.}$$
>
> Je ne m'arrêterai pas à développer ce calcul.
>
> La second manière est la suivante. . . . [23]

He then proceeded to give a slightly different analysis of the problem, based on the general idea of his 1841 exposition. (The difference occurs because he observed that if $u = qv + r$, then we actually have $r < u/2$, not simply $r \leq u/2$.)

This same analysis was then reproduced in the second edition of his *Traité élémentaire d'arithmétique*, published in 1843 [24]. On pp. 57–58 we find the analysis, which results in the bound $E(u, v) \leq 2[\log_2((v + 1)/2)]$.

The paper of Lamé, published the following year, did not escape Finck's attention. Indeed, he must have been slightly miffed that Lamé, a fellow *polytechnicien* who had already established a reputation far superior to Finck's,[8] made no reference to his work. In an 1845 paper [27], Finck called attention to the analysis in his 1842 paper and his 1843 book. He admitted that his bound is not quite as good as Lamé's, but he also pointed out that the number 5 in Lamé's theorem could be replaced with 1/.204, but with no number smaller than 1/.209.

Despite this lobbying by Finck on behalf of his own results, Lamé has traditionally received the credit for the analysis of the Euclidean algorithm. Of books that discuss analysis of algorithms, or the Euclidean algorithm, only Lucas [50, 335] makes any reference to Finck's work. And Terquem, in an 1849 paper [66], chastised Bertrand for not mentioning Lamé by name in his *Traité d'arithmétique*—even though Finck's simpler proof was published three years before Lamé's.

[8] There is even a street in Paris named for Lamé.

7. JACQUES PHILIPPE MARIE BINET

7.1. Life of Binet[9]

The mathematician and astronomer, Jacques Philippe Marie Binet, was born on February 2, 1786, in Rennes. He entered the *École Polytechnique* on November 22, 1804, and graduated two years later, entering into the service of the *corps des Ponts et Chaussées* in November 1806.

On November 10, 1807, Binet was appointed *adjoint aux répétiteurs de mathématiques* at the École Polytechnique, and *répétiteur d'analyse appliquée et de géométrie descriptive* on April 21, 1808. In 1814 he was appointed *examinateur temporaire* in descriptive geometry. On November 3, 1815, he became *instituteur de mécanique* at the École Polytechnique, where he replced Poisson. He also became *inspecteur des études* on September 5, 1816. That same year, he helped edit the 1816 edition of the *Mécanique analytique* of Lagrange. Binet was also appointed *professeur d'astronomie* at the Collège de France in 1823.

Following the July Revolution of 1830 and the installation of Louis Philippe on the French throne, Binet was removed from his appointment as *inspecteur des études* on November 13, 1830, due to his attachment to the previous regime of Charles X.

Binet wrote more than 50 papers during the period 1808–1851. He received the decoration of *chevalier de la Légion d'Honneur* on May 1, 1821. He was elected to the *Académie des Sciences* in 1843.

Binet died in Paris on May 12, 1856.

7.2. Work of Binet

In an 1841 paper [10], Binet discussed a slightly modified version of the Euclidean algorithm for the calculation of the greatest common divisor. Today this method is called the *least-remainder algorithm:* at each division step, one writes $a = qb + r$, where $|r|$ is as small as possible. Since r can be chosen such that $|r| \leq b/2$, it follows that the number of division steps is $O(\log b)$.

Binet wrote as follows (we have corrected two minor typographical errors);

> La limite $\frac{\log a}{\log(2)}$ est aussi celle du dénombrement des divisions consécutives qu'exige la recherche du plus grand diviseur de A et a, lorsque, pour simplifier le calcul, on a soin d'admettre des résidus positifs ou négatifs, afin de n'employer que des diviseurs moindres que la moitié des dividendes correspondants, à partir de la seconde division. L'utilité de cette marche est manifeste, et je pense que l'on a dû en faire la remarque, quoique je ne la trouve dans aucun Traité. Alors les divisions seront représentées successivement par les formules
>
> $$A = aq \pm \alpha_1,\ a = \alpha_1 q_1 \pm \alpha_2,\ \alpha_1 = \alpha_2 q_2 \pm \alpha_3,\ \text{etc.},\ \alpha_{n'-1} = \alpha_{n'} q_{n'},$$
>
> $n' + 1$ étant le nombre des divisions; et d'après le décroissement des résidus, on aura

[9] This brief account of Binet's life is based on files of the *École Polytechnique* and the accounts in [44, Vol. 16, 885; 38, Vol. 5, 101; 54, Vol. 6, 495; 46, Vol. 2, 753; 30, 148; 34, Sect. 4.2.3]. (The eulogy given by Cauchy [14] unfortunately contains no information of interest.)

$$a > 2\alpha_1 > 2^2\alpha_2 > 2^3\alpha_3 > \cdots > 2^{n'}\alpha_{n'}.$$

On tire de là, comme ci-dessus,

$$n' < \frac{\log(a) - \log(\alpha_n)}{\log(2)}.$$

On sait que cette série de divisions fournit les quotients, positifs ou négatifs, dont se composerait la fraction continue représentant la fraction numérique $\frac{a}{A}$. La fraction continue ainsi composée serait, en général, moins étendue que celle dont on fait ordinairement usage, et où l'on n'emploie que des quotients positifs. [10, 454]

Binet's analysis is surprisingly modern in presentation. It may have been overlooked because his 1841 paper [10] started by analyzing a *different* algorithm that is *not* guaranteed to produce the greatest common divisor. However, Lionnet [48] claimed that Binet's bound "est déjà ancienne et depuis longtemps du domaine public."

In a paper written after Lamé's [11], Binet brought attention to his 1841 paper, and observed that the number of steps in the least-remainder algorithm to compute the gcd on inputs of α digits is bounded by $(10/3)\alpha$, which is superior to Lamé's bound of 5α for the ordinary Euclidean algorithm. A similar remark was later given by Nievengloski [52] and Lionnet [49].

A more complete worst-case analysis of the least-remainder algorithm was given by Dupré in 1846 [20]. Later, Vahlen [67] proved that the least-remainder algorithm provides the shortest continued fraction expansion among any algorithms that choose between the ordinary remainder and the least-remainder at each step; this result is stronger than Binet's claim.

8. CONCLUSIONS

I have traced some of the early work on the analysis of the Euclidean algorithm, starting with Reynaud's elementary remarks in 1811. The remarks of Reynaud, Léger, and Finck show that the "running time" of the Euclidean algorithm was of interest to mathematicians before the appearance of Lamé's paper on the subject in 1844; furthermore, Finck gave an excellent bound on the number of division steps prior to Lamé. While the work of Reynaud, Léger, Finck, and Binet had essentially no influence on the development of the analysis of algorithms as a field, these pioneers nevertheless deserve our respect and admiration.

ACKNOWLEDGMENTS

I am indebted to Fabrice Jaubert, Naji Mouawad, Michel Mendès France, and Jean-Paul Allouche for their help with the French language. Paul Campbell, Donald Knuth, Michael Somos, Eric Bach, Jean-Paul Allouche, Ivor Grattan-Guinness, A. K. Lenstra, and H. W. Lenstra, Jr. read a draft of this paper and made many useful comments. I am particularly grateful to D. H. Fowler for his careful reading and expertise. Shyamala Balgopal of the Reference Library of the University of Illinois at Urbana–Champaign provided assistance in locating some of the early work of Finck. I also thank Claudine Billoux of the *Service des Archives, École Polytechnique,* Jean-Christophe Ton-That and Jean Favier of the *Archives Nationales,* Marie-Annick Hepp, *Conservateur en Chef et Chef de la Division Archives du Service historique de l'Armée de Terre,* and Jacques d'Orléans, *Directeur des*

Archives départementales du Bas-Rhin, for their extensive assistance in providing copies of original documents relating to the lives of Reynaud, Léger, and Finck.

REFERENCES

1. P.-F. Amadieu, *Traité d'arithmétique, à l'usage spécial des élèves qui se préparent aux écoles du gouvernement,* Paris: Hachette, 1839.

2. Archives départementales du Bas-Rhin, Dossier 1TP/SUP99, containing items on Pierre-Joseph-Étienne Finck; Strasbourg, France.

3. Archives départementales du Bas-Rhin, Dossier 1TP/SUP 95, Registre des gradués en sciences; Strasbourg, France.

4. Archives Nationales, Dossier F/17/20741, containing 119 items on Pierre-Joseph-Étienne Finck; Paris, France.

5. C. Baechler and J.-P. Kintz (Eds.), *Nouveau dictionnaire de biographie alsacienne,* Vol. 11, Strasbourg: Fédération des Sociétés d'Histoire et d'Archéologie d'Alsace, 1988.

6. P. Barlow, *An Elementary Investigation of the Theory of Numbers,* London: Johnson and Co., 1811.

7. A. J. Q. Benchot (Ed.), *Bibliographie de l'Empire Français,* Paris, 1811–1814.

8. A. J. Q. Benchot (Ed.), *Bibliographie de la France; ou, Journal général de l'imprimerie et de la librairie,* Paris, 1814–1857.

9. J. Bertrand, C. Combes, and V. Puiseux, Mélanges. Funérailles de M. Lamé, le mardi 3 mai 1870, *Bulletin des sciences mathématiques et astronomiques* **1** (1870), 189–195, 224–228.

10. J. Binet, Recherches sur la théorie des nombres entiers et sur la résolution de l'équation indéterminée du premier degré qui n'admet que des solutions entières, *Journal de mathématiques pures et appliquées* **6** (1841), 449–494.

11. J. Binet, Note sur le nombre des divisions à effecteur pour obtenir le plus grand diviseur commun de deux nombres eniters; suivie d'une remarque sur une classe de séries récurrentes, *Comptes rendus des séances de l'Académie des Sciences* **19** (1844), 937–941.

12. E. Bobillier and P.-J.-E. Finck, Solution des deux problèmes de statique proposés à la page 296 du précédent volume, *Annales de mathématiques* **17** (1827–1828), 59–68.

13. M. Bradley, Franco–Russian Engineering Links: The Careers of Lamé and Clapeyron, 1820–1830, *Annals of Science* **38** (1981), 291–312.

14. A. Cauchy, Discours de M. Augustin Cauchy, *Archiv der Mathematik und Physik* **27** (1856), 483–484.

15. M. P. Crosland, *The Society of Arcueil: A View of French Science at the Time of Napoleon I,* London: Heinemann, 1967.

16. Roman D'Amat (Ed.), *Dictionnaire de biographie française,* Paris: Librairie Letouzey et Ané, 1975.

17. J. Dhombres, French Textbooks in the Sciences 1750–1850, *History of Education* **13** (1984), 153–161.

18. J. Dhombres, French Mathematical Textbooks from Bézout to Cauchy, *Historia Scientiarum,* No. 28 (1985), 91–137.

19. J. Dhombres, Mathématisation et communauté scientifique française (1775–1825), *Archives internationales d'histoire des sciences* **36** (1986), 249–293.

20. A. Dupré, Sur le nombre de divisions à effectuer pour obtenir le plus grand commun diviseur entre deux nombres entiers, *Journal de mathématiques pures et appliquées* **11** (1846), 41–64.

21. Leonardo Pisano Fibonacci, *Scritti di Leonardo Pisano,* Vol. I, Rome: Baldassare Boncompagni, 1857.

22. P. J. E. Finck, *Traité élémentaire d'arithmétique à l'usage des candidats aux écoles spéciales,* Strasbourg: Derivaux, 1841.

23. P. J. E. Finck, Lettre, *Nouvelles annales de mathématiques* **1** (1842), 353–355.

24. P. J. E. Finck, *Traité élémentaire d'arithmétique à l'usage des candidats aux écoles spéciales,* 2nd ed., Strasbourg: Derivaux, 1843.

25. P.-J.-E. Finck, De la division abrégée, *Nouvelles annales de mathématiques* **4** (1845), 328–331.

26. P.-J.-E. Finck, Division abrégée, *Nouvelles annales de mathématiques* **4** (1845), 658–659.

27. P.-J.-E. Finck, Observations sur le théorème de M. Lamé, relativement au plus grand commun diviseur, et nouvelle démonstration de ce théorème, *Nouvelles annales de mathématiques* **4** (1845), 71–74.

28. P.-J.-E. Finck, Note sur la division abrégée, *Nouvelles annales de mathématiques* **5** (1846), 599–603.

29. A. Fourcy, *Histoire de l'École Polytechnique,* Paris: L'Auteur, 1828.

30. A. Fourcy, *Histoire de l'École Polytechnique,* Paris: Belin, 1987. Introduction et appareil critique par Jean Dhombres.

31. C. F. Gauss, *Disquisitiones arithmeticae,* Leipzig: G. Fleischer, 1801; [English trans.] by A. A. Clarke, New York: Springer-Verlag, 1986.

32. C. C. Gillispie (Ed.), *Dictionary of Scientific Biography,* Vol. VII. New York: Scribner's, 1973.

33. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics,* Reading, MA: Addison–Wesley, 1989.

34. I. Grattan-Guinness, *Convolutions in French Mathematics, 1800–1840,* 3 vols., Basel: Birkhäuser, 1990.

35. I. Grattan-Guinness, Work for the Hairdressers: The Production of de Prony's Logarithmic and Trigonometric Tables, *Annals of the History of Computing* **12** (1990), 177–185.

36. H. Grossman, On the Number of Divisions in Finding a G. C. D., *American Mathematical Monthly* **31** (1924), 443.

37. T. L. Heath, *The Thirteen Books of Euclid's Elements,* 3 vols., New York: Dover, 1956.

38. J. C. F. Hoefer (Ed.), *Nouvelle biographie générale depuis les temps les plus reculés jusqu'à nos jours,* Paris: Firmin Didot Frères, 1855–1862.

39. A. Kaltenbach, *Orientation et définition du patriotisme allemand chez un historien de l'Allemagne du Sud: le Palatin-Badois Ludwig Haeusser (1818–1867),* Ph.D. thesis, Université de Paris, 1963. Also published as *Ludwig Haeusser, historien et patriote 1818–1867; Contribution à l'étude de l'histoire politique et culturelle franco–allemande au XIXe–siècle,* Paris: Presses Universitaires de France, 1965.

40. D. E. Knuth, The Analysis of Algorithms, in *Actes du Congrès International des Mathématiciens, 1970,* Paris: Gauthier–Villars, 1971, 3:269–274.

41. D. E. Knuth, *The Art of Computer Programming. Volume 2: Seminumerical Algorithms* (2nd ed.), Reading, MA: Addison–Wesley, 1981.

42. D. E. Knuth, Algorithmic Themes, in *A Century of Mathematics in America, Part I,* (P. Duren, Ed.), Providence: American Mathematical Society, 1988, pp. 439–445.

43. T. F. de Lagny, Analyse générale, ou méthodes nouvelles pour résoudre les problèmes de tous les genres & de tous les degrés à l'infini, *Mémoires de l'Académie Royale des Sciences (Paris),* **11** (1733).

44. C.-A. Laisant *et al.* (Eds.), *La grande encyclopédie, inventaire raisonné des sciences, des lettres et des arts,* Paris: H. Lamirault et Compagnie, 1895.

45. G. Lamé, Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers, *Comptes rendus des séances du l'Académie des Sciences* **19** (1844), 867–870.

46. P. Larousse, *Grand dictionnaire universel du XIX^e siècle,* Paris: Administration du Grand dictionaire universel, 1867; reprint ed., Slatkine, Genève-Paris, 1982.

47. E. Léger, Note sur le partage d'une droite en moyenne et extrême, et sur un problème d'arithmétique, *Correspondance mathématique et physique* **9** (1837), 483–485.

48. E. Lionnet, Sur la limite du nombre des divisions à faire pour trouver le plus grand commun diviseur de deux nombres entiers, *Nouvelles annales de mathématiques* **4** (1845), 617–626.

49. E. Lionnet, Note sur le plus grand commun diviseur, *Nouvelles annales de mathématiques* **10** (1851), 85–86.

50. E. Lucas, *Théorie des nombres,* Paris: Gauthier–Villars, 1891.

51. O. Neugebauer, *The Exact Sciences in Antiquity,* Princeton: University Press, 1952.

52. G.-H. Nievengloski, Sur la limite supérieure du nombre de divisions à faire pour trouver le plus grand commun diviseur de deux nombres, *Nouvelles annales de mathématiques* **4** (1845), 568–573.

53. F. Peyrard, *Cours de mathématiques à l'usage de la marine et de l'artillerie, par Bezout. Édition originale, revue et augmentée par Peyrard et renfermant toutes les connaissances mathématiques nécessaires pour l'admission à l'École Polytechnique,* Paris: Louis, 1803.

54. M. Prevost and Roman D'Amat (Eds.), *Dictionnaire de biographie française,* Paris: Librarie Letouzey et Ané, 1954.

55. Prince, *Arithmétique de Bezout,* Lyon: Boursy, 1812.

56. J.-M. Quérard, *La France littéraire, ou Dictionnaire bibliographique des savants, historiens et gens de lettres de la France, ainsi que des littérateurs étrangers qui ont écrit en francais, plus particulièrement pendant les XVIII^e et XIX^e siècles,* Paris: Firmin Didot Père et Fils, 1835; reprint ed., G.-P. Maisonneuve & Larose, Paris, 1964.

57. A.-A.-L. Reynaud, *Traité d'arithmétique à l'usage des ingénieurs du cadastre et des élèves qui se destinent à l'École Polytechnique, à la marine, à l'artillerie et au commerce,* Paris: Courcier, 1804.

58. A.-A.-L. Reynaud, *Traité d'arithmétique à l'usage des élèves qui se destinent à l'École Polytechnique,* 6th ed., Paris: Courcier, 1811.

59. A.-A.-L. Reynaud, *Traité d'arithmétique à l'usage de la marine et de l'artillerie, par Bezout; avec des notes et des tables de logarithmes,* 8th ed., Paris: Courcier, 1816.

60. A.-A.-L. Reynaud, *Traité d'arithmétique à l'usage de la marine et de l'artillerie, par Bezout; avec des notes et des tables de logarithmes,* 9th ed., Paris: Courcier, 1821.

61. A.-A.-L. Reynaud, *Traité d'arithmétique à l'usage des élèves qui se destinent à l'École Royale Polytechnique et à l'École Spéciale Militaire,* 10th ed., Paris: Courcier, 1821.

62. Royal Society of London, *Catalogue of Scientific Papers (1800–1863),* London: Her Majesty's Stationery Office, 1868–1869.

63. G. Sarrut and B. Saint-Edme, *Biographie des hommes du jour,* Paris: Henri Krabbe, 1837.

64. E. Sitzmann, *Dictionnaire de biographie des hommes célèbres de l'Alsace,* Vol. I, Alsace: Rixheim, 1909.

65. O. Terquem, Notice biographique, *Nouvelles annales de mathématiques* **5** (1846), 205–207.

66. O. Terquem, Questions sur la numération et sur le plus grand commun diviseur, *Nouvelles annales de mathématiques* **8** (1849), 358–362.

67. K. Th. Vahlen, Über Näherungswerthe und Kettenbrüche, *Journal für die Reine und Angewandte Mathematik* **115** (1895), 221–233.

68. H. S. Wilf, *Algorithms and Complexity,* Englewood Cliffs, NJ: Prentice-Hall, 1986.