Lagrange and the four-square theorem

Jenny Boucard

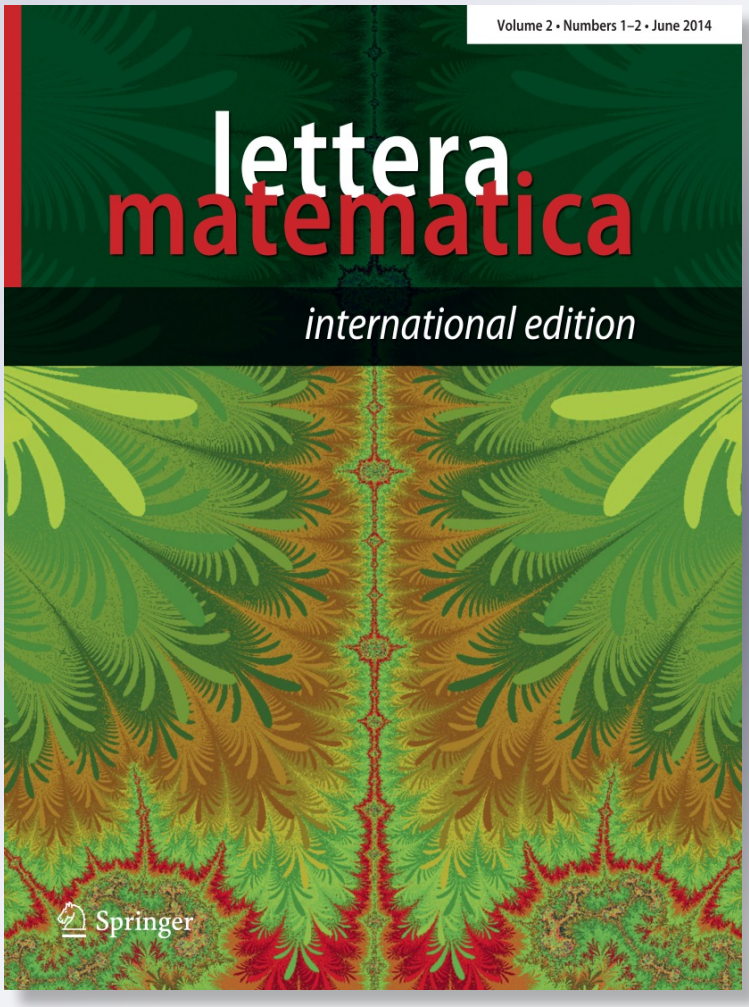
Lagrange and the four-square theorem

Jenny Boucard

Lettera Matematica
International edition

ISSN 2281-6917
Volume 2
Combined 1-2

Lett Mat Int (2014) 2:59-66
DOI 10.1007/s40329-014-0052-2



Springer

Lett Mat Int (2014) 2:59–66
DOI 10.1007/s40329-014-0052-2

Lagrange and the four-square theorem

Jenny Boucard

Published online: 22 May 2014

Abstract In this article we will first provide an overview of Lagrange's arithmetic work, written between 1768 and 1777. We then focus on the proof of the four-square theorem published in 1772, and shed light on the context of its implementation by relying on other memoirs by Lagrange and Leonhard Euler. By means of this analysis, our goal is to give a concrete vision of the arithmetic, algebraic and analytical methods and tools used by Lagrange in number theory and place his arithmetic practice in the context of the second half of the eighteenth century.

Keywords Number theory · Remainders · Lagrange · Euler · Indeterminate equations · Four-square theorem

1 Introduction

Joseph-Louis Lagrange is regularly presented as one of the scholars who contributed to the renewal of number theory in eighteenth century, especially due to his proposal of novel proof methods:

> Together with Euler, Lagrange brings new prestige to number theory, neglected since Fermat's time; he is the first to prove several theorems that seventeenth-century arithmeticians had just stated, including the theorem by J. Wilson, reported by Waring; his work on Pell equation and on general second-degree indeterminate analysis, in which the role of the discriminant of quadratic forms is emphasised, paved the way to Legendre and Gauss [1, p. 69].

Lagrange's research in arithmetic are usually described as just a synthesis of a series of results obtained by Pierre de Fermat and Leonhard Euler, as well as an anticipation of the theory of quadratic forms developed by Adrien-Marie Legendre and Carl Friedrich Gauss at the beginning of nineteenth century.

After a short presentation of Lagrange's arithmetical work, the goal of this article is to provide a concrete idea of the methods and techniques he used in number theory and to situate his activity within the second half of eighteenth century. To this end, we put particular emphasis on his proof of the four-square theorem[1] as well as on some works that will help us to understand better how this proof came to be.

2 Lagrange and number theory: an outline

With the works of Euler, Lagrange, and Legendre, the second half of eighteenth century is often described as a period of transition in the history of number theory [6]. In the sixteenth and seventeenth centuries[2], indeed, it is mostly judges, aristocrats, diplomats, and members of the clergy who became interested in problems about numbers; they had epistolary exchanges, often in the form of mathematical challenges. The Toulouse magistrate Pierre de Fermat was particularly renowned, due to the arithmetic questions he posed: he associated a specific object with

J. Boucard (✉)
Centre François Viète, UFR des Sciences et des Techniques de Nantes, 2 rue de la Houssinière, BP 92 208,
44322 Nantes Cedex 3, France
e-mail: jenny.boucard@univ-nantes.fr

[1] According to this theorem, every integer number can be written as a sum of four squares. Our analysis of its proof relies on [2–5].

[2] We rely here on the analysis in [7] and quote from it some excerpts from correspondences.

arithmetic and encouraged his contemporaries to tackle it: "Arithmetic has nevertheless its own domain, that is, the theory of integer numbers; this theory was but drafted by Euclid and was not that much expanded by his successors …; arithmeticians have then to develop, or at least, revive it".[3] Some played along; others instead, and most of them, refused it [7, p. 418]. As we shall see with Lagrange, ambiguous remarks about the utility of number theory recur in the letters of later centuries. However, by the nineteenth century the situation had changed: number theory was the topic of a prize awarded by the French Academy of Sciences; it was taught in several German universities; and some scholars, among whom Ernst Eduard Kummer, were officially recognised for their contributions to this area.

In the history of number theory in the eighteenth century certain names[4] appear frequently, such as Christian Goldbach and Leonhard Euler, who exchanged letters about arithmetic starting in 1730. Euler also published several papers about this topic.[5] At the turn of the century, Legendre published his *Essai sur la théorie des nombres*, where he summarises several results in "indeterminate analysis" studied by previous mathematicians. Lagrange, for his part, presented about ten arithmetic memoirs between 1768 and 1777.

So, it was while at the Academy of Berlin that Lagrange produced the whole of his research in arithmetic.[6] At that time, he was in a very favourable position that allowed him to devote himself fully to his scientific work. During the same period Johann Heinrich Lambert was also at the Academy of Berlin; starting in 1770, he embarked on a project to construct a factor table and strongly solicited the academia regarding the importance of the development of an autonomous number theory [8]. Lagrange was thus working in a climate in which number theory seems not to have been completely ignored. Moreover, he maintained a regular correspondence with d'Alembert and Euler, discussing arithmetic questions with the latter.

Among Lagrange's works, the best known and most quoted in the history of number theory are undoubtedly those concerning second-degree indeterminate problems [9–12] and quadratic forms [13, 14].[7] From 1768 to 1771, Lagrange gave some methods to solve Pell-Fermat equation[8] and, more in general, second-degree indeterminate problems. These questions had already been studied previously. For instance, in the case of Pell-Fermat equation, Euler had proved the existence of infinitely many solutions, starting from a single given solution. In the case of these indeterminate equations, Lagrange's remarkable originality lies in determining a particular solution (if one exists) and deducing from it the whole set of solutions. In several of his works, he devotes himself to simplifying and unifying his methods of solution. In 1775 and 1777, Lagrange published a study of the numbers that can be represented in the form $Bt^2 + Ctu + Du^2$. Often considered in the histories of number theory as Lagrange's most significant contribution in that field, these works are often read through the lens of the later works by Legendre and Gauss about quadratic forms [6, 15]. Remarking on this work, Lagrange wrote to d'Alembert on 6 July 1775: "I would not be surprised if you were unsatisfied with what you will find in this volume, since I am myself. My research in arithmetic is the thing that cost me the most and that is perhaps worth the least"[16, p. 301].

Lagrange also published the first complete proofs of some particular results, including the four-square theorem [17] and Wilson's theorem[9] [18], as well as the solution of the Diophantine equation $z^2 = 2x^4 - y^4$ [19]. These memoirs are shorter than the others and might appear isolated. However, we are going to show that, in the case of the four-square theorem, Lagrange uses tools and methods that he had already honed in the course of his research on the second-degree indeterminate problems, as well as some of writings by Euler who, in his turn, would rely on Lagrange's work to obtain a new proof.

3 The four-square theorem from Bachet to Lagrange: some historical references

Lagrange's proof of the four-square theorem appeared in 1772. As he himself remarks in his historical introduction, the "theorem by Mr Bachet" [17, p. 190] has been the subject of previous research. Claude-Gaspard Bachet de Méziriac is well known for his *Problèmes plaisans et*

[3] In what follows, unless otherwise noted, the numbers we shall consider are integers.

[4] Obviously, these names do not include all amateur number theorists. Indeed, as we are reminded by C. Goldstein: "These famous names allow us to trace the evolution of the methods. If Goldbach repeatedly recalls Fermat's hypotheses in a letter to Euler, this is due to the fact that along seventeenth and eighteenth centuries some number lovers kept existing, who transmitted this corpus and prevented it to fall into oblivion" [7, p. 438].

[5] However, Euler's writings about arithmetic occupy "just" four out of seventy volumes constituting his *Opera Omnia*.

[6] Let us recall that Lagrange lived in three cities: Turin (1736–1766), Berlin (1766–1787) and Paris (1787–1813).

[7] For this survey of Lagrange's works in number theory, we rely on several surveys and analyses of his work; among them, [6, chap. IV] and [3].

[8] This problem asks for the resolution in integers of the equation $x^2 - Ay^2 = 1$, where A is a non-square integer number.

[9] Here is the statement of Wilson's theorem, as found in Lagrange: if n is an arbitrary prime number, then the number $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \ldots \cdot (n-1) + 1$ is always divisible by n.

délectables qui se font par les nombres, published in 1612 and then again in 1624, which would become an important source about arithmetic questions in later centuries. He also published, in 1621, a translation from Latin of Diophantus's *Arithmetica*, adding a commentary where, in his remarks about a Diophantine problem, Bachet stated the four-square theorem and verified it for the integers from 1 to 325.

It is from this work that, some years later, Fermat learned about the four-square theorem. He made mention of this problem in his correspondence starting in the 1630s. Thus he wrote to Digby in 1658: "I announce to your illustrious correspondents that I found a complete proof of it". No proof by Fermat has been found, but some clues can be found in a letter to Pierre de Carcavi written in 1659, where Fermat claims there that the four-square theorem belongs to a series of *a priori* unconnected arithmetic questions that can be proved using the "method of infinite descent". He describes this technique in the case of a negative proposition: it amounts to assuming that the problem admits a positive integer solution and to proving that it is possible to derive from it another, strictly smaller, positive integer solution. Hence we may construct a decreasing sequence of positive integers, leading to a contradiction. Fermat suggests applying this procedure to positive propositions too, again relying on a proof by absurdum. He describes explicitly the idea of his method, but he does not give the details of a procedure to construct the decreasing sequence of integer numbers that satisfy the required conditions. We shall see that this method will be the core of Lagrange's and Euler's proofs in their papers about sums of squares.[10]

As we have mentioned above, Euler's research in number theory seems to have begun with his correspondence with Goldbach. Goldbach sent Euler two letters, in December 1729 and May 1730, detailing some conjectures by Fermat and a few of his own results; Euler replied on 4 June 1730, confirming his interest in number theory and in particular in the "not inelegant theorem" stating that every number can be written as a sum of four squares. From 1730 to 1750 the two mathematicians had regular exchanges about their results on sums of squares. Between 1749 and 1751, Euler presented several memoirs about sums of squares, including a proof of a weak version of the four-square theorem [23]: every integer number is a sum of at most four integer or rational squares.

Lagrange finally gives a complete proof of the four-square theorem in a dozen-page memoir [17]. Unlike Euler, he has not published other texts about sums of squares. At the time, the two scholars were engaged in a regular correspondence,[11] in which they often discussed arithmetical questions, but never the four-square theorem. So, it is harder, in the case of Lagrange, to learn about his path towards the formulation of his final proof. On the one hand, focussing on this proof and on its context allows us to concretely understand the difficulties arising in the close study of Lagrange's writings and, on the other, to emphasise the diverse methods—algebraic, analytic, arithmetic—marshalled by Lagrange (especially) in his writings about number theory. Taking into account a sample of memoirs by Euler and Lagrange also underlines both their mutual influences as well as their peculiarities within number theory.

4 Outline of the proof of the four-square theorem given by Lagrange

In general, this result by Lagrange relies on long sequences of algebraic manipulations that may be hard to follow. We sketch here the outline of the proof, then we dwell on the two methods used by Lagrange to prove the two main theorems of his paper. As Lagrange himself recalls in the introduction to his memoir, the structure of his proof depends on what Euler had already discovered in his works on the sums of squares. To begin with, a product of two sums of four squares is itself a sum of four squares: so we may restrict ourselves to prime numbers. Hence, in order to prove that every prime number is a sum of four squares, Lagrange, following Euler, presents two steps:

(I) Every prime number p divides a sum of two or three squares, the quotient of this division being less than p;
(II) If a product is a sum of four squares, and one of the factors is of the same form, then the other factor is again a sum of four squares.[12]

As Lagrange remarks, Euler had already given a proof of step (I). Now Lagrange gives proofs for both steps, starting with slightly different statements.

Lagrange begins by proving that every prime number dividing a sum of four squares while not dividing any of the squares is necessarily a sum of four squares. To this end, he proves that: "if the sum of four squares is divisible

[10] For some historical background about the use of the method of infinite descent, we refer to [20–22].

[11] They exchanged at least five letters from December 1769 to December 1770.

[12] Assume now that there are prime numbers that cannot be written as sums of four squares: let p be the smallest of these numbers. Then there are integers a, b, and c such that $a^2 + b^2 + c^2 = np$, where $n < p$. Hence the prime factors of n are smaller than p and are sums of four squares; so n, and hence p, are sums of four squares, a contradiction.

by a prime number greater than the square root of the sum itself, then this number is necessarily equal to the whole sum" [17, p. 193]. To prove this, Lagrange uses the method of infinite descent we recalled above in speaking of Fermat. Thus, after showing that it is possible to restrict ourselves to the case where the four square summands are relatively prime, he considers the equation $Aa = p^2 + q^2 + r^2 + s^2$, where p, q, r, and s are relatively prime and A is a prime number such that $A > \sqrt{p^2 + q^2 + r^2 + s^2}$. Three pages of manipulations of algebraic identities and of facts about divisibility allow Lagrange to establish that there exist integer numbers a', p', q', r', and s' such that $Aa' = p'^2 + q'^2 + s'^2 + r'^2$ and $a' < a$ if $a > 1$. Applying the method of infinite descent, he can conclude:

> It follows that if Aa is a sum of four squares, then Aa' is too …; so, if a is greater than 1, then a' is necessarily smaller than a; and if a' is still greater than 1, it can be proved in the same way that Aa'' is again a sums of four squares, with a'' smaller than a'; and so on. So, since the numbers a, a', a'' are integer, none of which equal to zero, …and since they get smaller and smaller, it is clear that we shall arrive to one of them being equal to one, so A will be equal to the sum of four integer squares [17, p. 197].

Hence, unlike what we know about Fermat's work, with the method of infinite descent Lagrange is able to show that the number A is indeed a sum of four squares, without a proof by absurdum.

Lagrange proves next the first step by obtaining a result more general than Euler's: "If A is a prime number and B and C are arbitrary positive or negative numbers not divisible by A, then I claim that we can always find two numbers p and q such that the number $p^2 - Bq^2 - C$ is divisible by A" [17, p. 198]. It is sufficient to set $B = C = -1$ to establish a theorem about sums of three squares analogous to the one proved by Euler.

Lagrange restricts himself to the case where there is no q such that $Bq^2 + C$ is divisible by A, and then sets $Bq^2 + C = b$. He next introduces some expressions depending on b and p: $P = p^{A-3} + bp^{A-5} + b^2p^{A-7} + \cdots + b^{\frac{A-3}{2}}$ and $Q = b^{\frac{A-1}{2}} + 1$, thus obtaining an equality in which he can apply Fermat's little theorem:[13] $(p^2 - Bq^2 - C)PQ = Q(p^{A-1} - 1) - (b^{A-1} - 1)$. So, the two sides of this equality are divisible by A; now he just has to prove that there exist integers p and q such that A does not divide P nor Q. Lagrange appeals to the "known theory of differences"[14] [17, p. 199] in order to show that, by denoting by P', P'', …, $P^{(A-2)}$ the values of P for $p = 1, 2, \ldots, A-2$, then we have

$$P' - (A-3)P'' + \frac{(A-3)(A-4)}{2}P''' - \cdots + P^{(A-2)} = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (A-3).$$

Now, since A does not divide $(A-3)!$, there exists a p such that A does not divide P. He proceeds analogously for the expression Q, and then conclude.

5 Towards Lagrange's proof of the four-square theorem

In his memoir titled *Novae demonstrationes circa resolutionem numerorum in quadrata* submitted to the Academy of St. Petersburg in 1772, but published in the *Acta eruditorum* only in 1780, Euler happily announces that he has finally managed to find a complete proof of the four-square theorem, very different from Lagrange's and, above all, less laboured. Before describing his work, Euler briefly recalls the steps of Lagrange's proof and stresses his own goal: to give a new proof which is, in his opinion, clearer and more concise. Lagrange's proof actually involves long, non-intuitive calculations. Nevertheless, it is possible to detect links between this short memoir and some earlier works by Euler and by Lagrange: some of these were explicitly acknowledged by Lagrange, while others seem to reflect established mathematical practise. In this section we shall focus on some of these links.

5.1 Euler and the two-square theorem: "I have at long last found a conclusive proof"[15]

Thanks to his correspondence with Goldbach, it is possible to reconstruct Euler's path through sums of squares. For instance, in 1748, Euler proved the fundamental identity

[13] Let us recall Fermat's little theorem: if p is a prime number and a is a number not divisible by p, then $a^{p-1} - 1$ is divisible by p.

[14] The theory of finite differences, already known to Leibniz, was expounded by Euler in Volume I of his *Institutiones calculi differentialis cum eius usu in analysi finitorum ac doctrina serierum* (1755). He considers a function f, a fixed increment ω, and works on the sequences $x, x+\omega, x+2\omega, \ldots$, and $f(x), f(x+\omega), f(x+2\omega), \ldots$

Then he defines the sequence of first differences: $\Delta f(x) = f(x+\omega) - f(x)$, $\Delta f(x+\omega) = f(x+2\omega) - f(x+\omega)$ and so on. Then he considers the second differences $\Delta^2 f(x) = \Delta f(x+\omega) - \Delta f(x)$, $\Delta^2 f(x+\omega) = \Delta f(x+2\omega) - \Delta f(x+\omega)$, …

More in general, Euler shows that: $\Delta^n f(x) = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} f(x+j\omega)$. In particular, he proves that, in the case of a polynomial of degree n, $\Delta^n f(x) = \omega^n n(n-1)(n-2)\cdots 2 \cdot 1$. This is the result used by Lagrange.

[15] This quotation is from the letter Euler wrote to Goldbach on 12 April 1749: "Nunmehr habe ich endlich einen bündigen Beweis gefunden".

about the product of sums of four squares mentioned above. On 12 April 1749, Euler wrote to Goldbach to let him know that he has found a proof of the two-square theorem. It is in the same letter that he presents his proof of a weak form of the four-square theorem.

In the case of sums of two squares, the outline of Euler's proof is not too different from the one Lagrange would adopt for sums of four squares. First, he shows that the product of two sums of two squares is a sum of two squares, then that the divisors of sums of two relatively prime squares are themselves sums of two squares, and finally he deduces the two-square theorem: every prime number of the form $4n + 1$ is a sum of two squares. Euler's first memoir about the two-square theorem, presented on 20 March 1749 at the Academy of Berlin [24], only contains a *Tentamen demonstrationis*, completed in a second memoir presented on 15 October 1750 [25]. In both texts, methods and tools similar to those used by Lagrange can be found. Thus, in order to show that the divisors of sums of two relatively prime squares are sums of two squares, Euler relies on the method of infinite descent: he assumes that there exists a sum of two squares that is divisible by a number p that is not a sum of two squares and constructs a decreasing sequence of sums of two squares admitting a divisor that is not a sum of two squares, which is impossible (since we necessarily get to a sum of two squares which is a prime number or 1).

In order to derive the two-square theorem, Euler finally proves that every prime number of the form $4n + 1$ divides a sum of two squares using Fermat's little theorem: the number $4n + 1$ divides the difference $a^{4n} - b^{4n}$ if it is relatively prime to a and b, so it divides one of the factors $a^{2n} - b^{2n}$ or $a^{2n} + b^{2n}$. It suffices to prove that there exist numbers a and b that are relatively prime to $4n + 1$ and such that $4n + 1$ does not divide the difference $a^{2n} - b^{2n}$: this is the subject of Euler's second memoir, in which he uses the method of finite differences. He considers the sequence 1, 2^{2n}, 3^{2n}, ... , $(4n)^{2n}$ and assumes that all first differences $2^{2n} - 1, 3^{2n} - 2^{2n}, \ldots, (4n)^{2n} - (4n - 1)^{2n}$ are divisible by $4n + 1$. In this case, the second, third, ..., $2n$-th differences are again divisible by $4n + 1$. Now, the $2n$-th difference equals $(2n)!$, so it cannot possibly be divisible by $4n + 1$, a prime number. Hence, at least one of the first differences is not divisible by $4n + 1$ and there are two numbers a and b such that $a^{2n} - b^{2n}$ is not divisible by $4n + 1$.

This proof of the two-square theorem already involves several results and tools that Lagrange will use too; this is for instance the case for Fermat's little theorem, the method of infinite descent, and finite differences. Nevertheless, these last two methods will not be used by Lagrange in the same way.

5.2 A weak version of the four-square theorem by Euler: elaboration of a theory of residues

In the memoir that Euler read at the Academy of Berlin in 1751, containing his proof of a weak version of the four-square theorem [23], he works with sums of squares in a very different way. A large part of this text is devoted to what Euler calls the *residua*, which are in this memoir the remainders of squares after being divided by a composite or prime number p. He also introduces the notion of complement of a residue, which is the difference between a given residue and the divisor p. So he finds several properties of these residues and their complements. Starting with his Theorem 14, Euler links residues and sums of squares. This way, Euler proves that, for every prime number p, it is always possible to find a sum of three (or fewer) squares that is divisible by p (which amounts to the first step of Lagrange's proof, given above), by means of considerations on residues (Euler distinguishes the cases whether or not -1 is a residue). Euler next deduces the weak version of the four-square theorem, using an argument by contradiction.

In the proofs of these two theorems we find the outline of the proof and the tools that will be further developed by Lagrange—Fermat's little theorem and finite differences. But finite differences no longer appear in Euler's memoir about sums of four squares; they are replaced by an increasingly important use of residues. This is consistent with what Euler explicitly states in [23]: he advocates direct proofs about sums of two squares, that is, based on arithmetic tools, without resorting to results "extraneous" to number theory.

5.3 Lagrange and the second-degree indeterminate problems

As we mentioned in the introduction, Lagrange began working on second-degree indeterminate problems[16] in 1768 and published several memoirs about this topic between 1769 and 1773.

We shall dwell here on the solution of the equation $A = u^2 - Bt^2$ in integer numbers as presented by Lagrange in his text entitled "Sur la solution des problèmes indéterminés du second degré" [10]. This method of solution is described in some fifty pages. To link it to his proof of the four-square theorem, we focus on Lagrange's use of the methods of infinite descent and of finite differences.

Lagrange restricts the problem to the case $A = p^2 - Bq^2$ where A, B and p, q are two pairs of relatively prime numbers. He shows that it is necessary to determine integer

[16] We shall not discuss them here, but continued fractions are central to the methods developed by Lagrange for these subjects.

numbers α, A_1, p_1, and q_1, such that $AA_1 = \alpha^2 - B$ and $A_1 = p_1^2 - Bq_1^2$. So we get a new equation $A_1 = p_1^2 - Bq_1^2$ with $A_1 < A$. Hence, the original equation can be solved in the integers if the equation $A_1 = p_1^2 - Bq_1^2$ can be solved and if the expressions of p as functions of p_1, q_1, α, A, and B are given by integers.

He obtains a double sequence of equations such that the A_is and the α_is form two decreasing sequences of positive numbers:

$$\begin{cases} AA_1 = \alpha^2 - B, & \alpha < \dfrac{A}{2} \\ A_1A_2 = \alpha_1^2 - B, & \alpha_1 = \mu_1 A_1 \pm \alpha < \dfrac{A_1}{2} \\ A_2A_3 = \alpha_2^2 - B, & \alpha_2 = \mu_2 A_2 \pm \alpha_1 < \dfrac{A_2}{2} \\ \ldots\ldots\ldots\ldots, \end{cases} \qquad \begin{cases} A = p^2 - Bq^2, \\ A_1 = p_1^2 - Bq_1^2, \\ A_2 = p_2^2 - Bq_2^2, \\ A_3 = p_3^2 - Bq_3^2, \\ \ldots\ldots\ldots\ldots \end{cases}$$

Thus Lagrange uses here the method of infinite descent to approach an increasingly simpler equation that he is able to solve, allowing him to deduce from it the solutions to all previous equations (if possible).

A later paragraph of this work is devoted to finding a number α such that $\alpha^2 - B$ is divisible by A, when the number A is prime.[17] So Lagrange shows that $\alpha^2 - B$ is divisible by A if and only if $B^{\frac{A-1}{2}} - 1$ is too. To this end, he sets $P = \alpha^{2(m-1)} + \alpha^{2(m-2)}B + \alpha^{2(m-3)}B^2 + \cdots + B^{m-1}$, where $m = \frac{A-1}{2}$, obtaining:

$$\begin{aligned}(\alpha^2 - B)P &= \alpha^{2m} - B^m = \alpha^{A-1} - B^m \\ &= \alpha^{A-1} - 1 - (B^m - 1).\end{aligned}$$

The similarity with the expressions used by Lagrange in the case of the four-square theorem is striking: here, he applies in a similar way Fermat's little theorem and finite differences to prove that if $B^m - 1$ is divisible by A, then there is a number α such that A divides $\alpha^2 - B$.

6 Lagrange, Euler and the four-square theorem

All of the above shows a series of methods and tools used by our two scholars in several of their works and then exploited by Lagrange in his proof of the four-square theorem.

Euler responded quickly to Lagrange's proof of the four-square theorem and, while congratulating him on his complete proof, remarks that the text is lengthy and laboured. Euler proposed a shorter, simpler proof [26], along the same lines we have seen. In order to obtain the step (II), he again relies on the method of infinite descent: to prove that a number N that divides a sum of squares but does not divide any of the squares is itself a sum of four squares, Euler constructs a decreasing sequence of positive integers n, n', n'', ... such that Nn, Nn', Nn'', ... are sums of squares. So we necessarily get to $N \cdot 1$, itself a sum of four squares. So Euler again uses the method of infinite descent "à la Lagrange". However the calculations involved are distinctly shorter than Lagrange's, due to some clever algebraic substitutions. Euler then proves the step (I) in the form: for all prime number N, there exist infinitely many sums of three squares that are divisible by N. For this theorem he gives, once more, a proof based on the theory of residues.

This shows well the mutual influence between Euler and Lagrange, on several levels: the two scholars followed the same outline for their proofs and several methods and tools are shared among the different texts (method of infinite descent, method of finite differences, manipulation of algebraic identities, Fermat's little theorem, divisibility arguments). However, the ways these methods are used evolve. This is for instance the case of the method of infinite descent: first applied by Euler in arguments by contradiction, it is later used by Lagrange (and later on again by Euler) to show directly the existence of a solution to the problem under examination.

On the other hand, each of the two mathematicians shows his own practical approaches. In the case of step (I) of the proof of the four-square theorem, Euler and Lagrange propose successively new proofs, constructed by mean of specific tools. Thus the method of finite differences no longer appear in Euler's research on four squares: he develops instead a set of results on quadratic residues that allows him to get purely arithmetic proofs. Lagrange, for his part, gives new proofs, using a variety of analytic, algebraic, arithmetic tools, for the results already proved by Euler using residues.

7 Lagrange and number theory seen in their context

Starting from the four-square theorem, we have emphasised different aspects of Lagrange's arithmetic activity and of the way methods and tools circulated among the texts we have considered. However, we could enlarge our corpus in order to show other facets of arithmetic practice in the second half of the eighteenth century.

On the one hand, in the same period and earlier, a consideration of other works by Lagrange shows some points in common: for instance, in his memoir about the solution of numerical equations [27], Lagrange also uses the theory of finite differences. We have examined here only the works by Lagrange and Euler, but taking into account more authors and traditions would make evident even more elements in the progressive establishment of an autonomous number theory. We have already mentioned

[17] This amounts in fact to determining if B is a quadratic residue modulo A; however, Lagrange systematically presents such questions in terms of divisibility.

the work by Lambert and his attempts to promulgate number theory.

In [28], Bullynck shows that the circulation of medieval problems gave rise to different traditions: some problems about remainders, of Chinese and Indian origin, were transmitted from the fifteenth to the seventeenth centuries in Italian algebra books, French and German calculus books, the works of La Coss, and later in the books about recreational mathematics, which were very successful in the seventeenth century. An important example is the collection of *Problèmes plaisans et délectables qui se font par les nombres* by Bachet mentioned above. The work by Bachet is then transmitted in the seventeenth and eighteenth centuries to France and England, mostly via algebra handbooks. Progressively, the references become limited to Diophantus's *Arithmetica* and to the theory of equations, while the problems about remainders tend to disappear. On the other hand, the Diophantine tradition and the problems about remainders are covered separately in German works, in the seventeenth and most of the eighteenth century. The problems about remainders find their place in arithmetic handbooks (*Rechenbücher*) and books of recreational mathematics, while Diophantine problems and questions about the theory of equations, far rarer, appear in academic journals. In the second half of the eighteenth century, the general solution to the problems of (linear) remainders is incorporated in textbooks, especially by Euler and Abraham Kästner. Now, we have seen that these two alternatives—respectively centred on indeterminate equations and on the remainders—are partially echoed in Lagrange and Euler.

Then, after their proofs of the four-square theorem, Lagrange and Euler tried their hands at proving Wilson's theorem, once more corresponding with each other. Lagrange proposed two proofs based on several algebraic, arithmetic (such as Fermat's little theorem), and analytic (finite differences) tools, while Euler's proof relied on the theory of residues. In his further work, Lagrange never used results about residues, but continues including results from branches different from arithmetic: so, in order to solve the Diophantine equation $z^2 = 2x^4 - y^4$ [19], he relies on results from differential calculus. Lagrange did not further pursue his research in number theory after 1777. His position, somewhat ambiguous with respect to this area, is reflected in the letter he sent to young Gauss in order to congratulate him for the publication of his *Disquisitiones Arithmeticae*: "Your *Disquisitiones* made of you all at once one of the foremost geometers, and I consider the last section as containing the most beautiful analytic discovery made in a long time. The merit of your work about planets, moreover, is augmented by the importance of his subject".[18]

For his part, Euler wrote more memoirs about residues and a draft of a treatise about number theory, mainly centred on these residues [29]: originally tools to be used in research, residues become a subject in themselves. Thus he paved the way for new methods and new concepts in number theory, no longer limited to Diophantine analysis as in Lagrange. Euler's work, in a sense, promotes Gauss's treatise.[19]

Euler and Lagrange are, in a way, typical of contrasting arithmetic practices: Euler, with a number theory showing an increasing desire for autonomy and proofs based on arithmetic arguments; Lagrange, with an arithmetic focussed on indeterminate equations and disregarding the use of residues. Lagrange nonetheless succeeded in proving the same results as Euler, without using residues, simultaneously developing other research directions. A similar alternative is again found between Legendre and Gauss [2]; more in general, it must be taken into account to put in context the arithmetic work by French mathematicians at the beginning of the nineteenth century.

Acknowledgments Translated from the French by Daniele A. Gewurz

References

1. Andoyer, H., Humbert, P.: Les mathématiques pures de Descartes à Cauchy. In: Hanotaux, G. (éditeur) Histoire de la nation française, vol. XIV, pp. 23–80. Plon, Paris (1924)
2. Boucard, J.: Un "rapprochement curieux de l'algèbre et de la théorie des nombres" : études sur l'utilisation des congruences de 1801 à 1850. Thèse de doctorat, Université Paris 6, Paris (2011)
3. Buraux-Bourgeois, B.: La théorie des nombres dans l'oeuvre de Lagrange. Thèse de doctorat. Université de Paris-Nord, Paris (1990)
4. Buraux-Bourgeois, B.: L'analyse diophantienne chez Lagrange. Cahier du séminaire d'histoire des mathématiques **3**, 13–23 (1993)
5. Pieper, H.: On Euler's contributions to the Four-Squares Theorem. Historia Mathematica **20**, 12–18 (1993)
6. Weil, A.: Number Theory: An Approach through History from Hammurapi to Legendre. Birkhäuser, Boston (1984)
7. Goldstein, C.: Le métier des nombres aux XVII^{e} et XIX^{e} siècles. In: Serres, M. (éditeur) Éléments d'histoire des sciences, pp. 274–295. Bordas, Paris (1989)
8. Bullynck, M.: A History of Factor Tables with Notes on the Birth of Number Theory 1668–1817. Revue d'histoire des mathématiques **16**(2), 133–216 (2010)
9. Lagrange, J.-L.: Solution d'un problème d'arithmétique. Miscellanea Taurinensia, **4**:41–97, 1773. Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. I, Gauthier-Villars, Paris, pp. 671–731 (1867)
10. Lagrange, J.-L.: Sur la solution des problèmes indéterminés du second degré. Mémoires de l'Académie royale des sciences et des belles-lettres de Berlin, Année 1767, 165–310 (1769). Repr. in

[18] The last section of Gauss's work covers the solution of binomial equations, so it pertains to algebra.

[19] Euler nevertheless published further arithmetic memoirs, not centred on residues and using a variety of methods.

Œuvres de Lagrange, ed. J.-A. Serret, t. 2, Gauthier-Villars, Paris, pp. 377–535 (1868)
11. Lagrange, J.-L.: Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers. Mémoires de l'Académie royale des sciences et des belles-lettres de Berlin, Année 1768, pp. 181–250 (1770). Repr. in Œuvres de Lagrange, J.-A. Serret, ed., t. 2, Gauthier-Villars, Paris, pp. 655–726 (1868)
12. Lagrange, J.-L.: Additions. de l'analyse indéterminée. In Élémens d'Algèbre d'Euler, traduits de l'allemand, avec des notes et des additions, vol. 2, pp. 369–658. Bruyset–Desaint, Lyon–Paris (1773). Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. VII, Gauthier-Villars, Paris, pp. 5–180 (1869)
13. Lagrange, J.-L.: Recherches d'arithmétique. Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1773, pp. 265–312 (1775). Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. 3, Gauthier-Villars, Paris, pp. 695–758 (1869)
14. Lagrange, J.-L.: Suite des recherches d'arithmétique imprimées dans le volume de l'année 1773. Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1775, pp. 323–356 (1777). Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. 3, Gauthier-Villars, Paris, pp. 759–795 (1869)
15. Aubry, A.: Sur les travaux arithmétiques de Lagrange, de Legendre et de Gauss. L'Enseignement mathématique **11**, 430–450 (1909)
16. Lagrange, J.-L.: Œuvres de Lagrange, ed. J.-A. Serret, vol. 14. Gauthier-Villars, Paris (1867–1892)
17. Lagrange, J.-L.: Démonstration d'un théorème d'arithmétique. Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1770, pp. 123–133 (1772). Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. 3, Gauthier-Villars, Paris, pp. 189–201 (1869)
18. Lagrange, J.-L.: Démonstration d'un théorème nouveau concernant les nombres premiers. Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1771, pp. 125–137 (1773). Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. 3, Gauthier-Villars, Paris, pp. 425–438 (1869)
19. Lagrange, J.-L.: Sur quelques problèmes de l'analyse de Diophante. Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin, Année 1777, pp. 140–154 (1779). Repr. in Œuvres de Lagrange, ed. J.-A. Serret, t. 4, Gauthier-Villars, Paris, pp. 377–398 (1869)
20. Goldstein, C.: Descente infinie et analyse diophantienne : programmes de travail et mises en œuvre chez Fermat, Levi, Mordell et Weil. Cahiers du séminaire d'histoire des mathématiques **3**, 25–49 (1993)
21. Goldstein, C.: L'arithmétique de Pierre Fermat dans le contexte de la correspondance de Mersenne : une approche microsociale. Sciences et techniques en perspective **8**(1), 14–47 (2004)
22. Bussotti, P.: From Fermat to Gauss: Indefinite Descent and Methods of Reduction in Number Theory. Erwin Rauner Verlag, Augsburg (2006)
23. Euler, L.: Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum. Novi Commentarii academiae scientiarum Petropolitanae **5**, 13–58 (1760)
24. Euler, L.: De numeris, qui sunt aggregata duorum quadratorum. Novi Commentarii academiae scientiarum Petropolitanae **4**, 3–40 (1758)
25. Euler, L.: Demonstratio theorematis Fermatiani omnem numerum primum formae 4n+1 esse summam duorum quadratorum. Novi Commentarii academiae scientiarum Petropolitanae **5**, 3–13 (1760)
26. Euler, L.: Novae demonstrationes circa resolutionem numerorum in quadrata. Acta Eruditorum (1777), 193–211 (1780)
27. Lagrange, J.-L.: Sur la résolution des équations numériques. Mémoires de l'Académie royale des sciences et belles-lettres de Berlin, pp. 311–352 (1769). Repr. in Œuvres de Lagrange, J.-A. Serret, ed., t. 2, Gauthier-Villars, Paris, pp. 539–578 (1868)
28. Bullynck, M.: Modular Arithmetic Before C. F. Gauss : Systematizations and Discussions on Remainder Problems in 18th-Century Germany. Historia Mathematica **36**, 48–72 (2009)
29. Euler, L.: Tractatus de numerorum doctrina capita sedecim, quae supersunt. In: Rudio, F. (ed.) Commentationes arithmeticae, pp. 503–575. Teubner, Berlin (1849)

Jenny Boucard born in 1981, is a lecturer in the history of sciences at the University of Nantes, and a member of the Centre François Viète. Her work regards the history of number theory in the eighteenth and nineteenth centuries. In particular, she has studied the reception of the arithmetic notion of congruence in France during the first half of the nineteenth century. She is the author of "Cyclotomie et formes quadratiques dans l'oeuvre arithmétique d'Augustin-Louis Cauchy (1829–1840)" in the *Archive for History of Exact Science* (vol. 67 (4), 2013).