Foundations of Science (2020) 25:671–702
https://doi.org/10.1007/s10699-019-09642-3

Historical and Foundational Details on the Method of Infinite Descent: Every Prime Number of the Form $4n+1$ is the Sum of Two Squares

Paolo Bussotti[1] · **Raffaele Pisano**[2,3,4]

Published online: 3 January 2020

Abstract
Pierre de Fermat (1601/7–1665) is known as the inventor of modern number theory. He invented–improved many methods useful in this discipline. Fermat often claimed to have proved his most difficult theorems thanks to a method of his own invention: the *infinite descent* (Fermat 1891–1922, II, pp. 431–436). He wrote of numerous applications of this procedure. Unfortunately, he left only one almost complete demonstration and an outline of another demonstration. The outline concerns the theorem that every prime number of the form $4n+1$ is the sum of two squares. In this paper, we analyse a recent proof of this theorem. It is interesting because: (1) it follows all the elements of which Fermat wrote in his outline; (2) it represents a good introduction to all logical nuances and mathematical variants concerning this method of which Fermat spoke. The assertions by Fermat will also be framed inside their historical context. Therefore, the aims of this paper are related to the history of mathematics and to the logic of proof-methods.

Keywords Fermat · Infinite descent · Number theory · Foundations of mathematics · Relationship logic-mathematics

1 Introduction

The *Infinite Descent* is a mathematical method used in the theory of numbers. It is based on the third excluded principle and relies on the fact that the natural numbers are a well-ordered set. For example, given a certain known equation, typically a Diophantine one, while looking for its solutions, finally one can arrive to claim that it has no solution supposing that it has solutions and showing that under this hypothesis, an infinite descent in integers might be constructed. This is absurd. Hence, the equation has no solution. Nowadays, this mathematical

✉ Raffaele Pisano
raffaele.pisano@univ-lille.fr

Paolo Bussotti
paolo.bussotti@uniud.it

[1] Udine University, Udine, Italy

[2] IEMN, Lille University, Lille, France

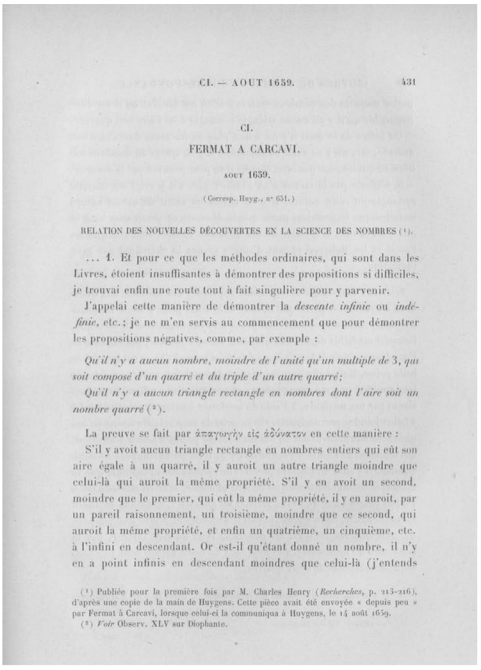
[3] Affiliated to (2015–2019) School/SCFS, Sydney University, Sydney, Australia

[4] Affiliated to CPNSS, LSE, London, UK

argument is used in the Number Theory and in other branches of mathematics as abstract algebra. Pierre de Fermat[1] (1601/7–1665) produced important results on this subject.

Along his childhood, Fermat followed the tradition of his family as dealer and then he was lawyer in Toulouse (Kline 1999, I, pp. 320–321). He wrote remarkable argumentations and results including several aspects of mathematics, as probability calculus, geometry and their applications to physics (cfr. Pisano and Capecchi 2013, 2015; Pisano and Bussotti 2013, 2016, 2017). Though he gave such important contributions to mathematics and science, he published few of his results. For, they are known thanks to several letters addressed to numerous scientific correspondents/friends. Such letters concern a vast panorama: number theory, infinitesimal calculus, geometry of coordinates, probability, optic (see e.g., the *principle of least time* or simply called *Fermat's principle*). Among his many original contributions, probably the most outstanding ones regard number theory. Particularly his *method of Infinite Descent* is the specific object of this paper.

The method was invented by Fermat and written as *descente infinie ou indéfinie* (Fermat 1891–1922, II Correspondence, August 1659, p. 431; see also p. 213) in a letter entitled *Relation des nouvelles découvertes en la science des nombre* (*Ivi*, pp. 431–436) and addressed to Huygens (1629–1695) by the intermediation of Pierre de Carcavi (1600?1603?–1684) (Fig. 1a). It is also well known that the *Diophantine equations* were crucial references for Fermat. He read *Arithmetica*—written by Diophantus of Alexandria (fl. AD 201–215; fl. AD 285–299) in the third century AD—as translated into Latin (1621) by Claude-Gaspard Bachet de Méziriac (1581–1638) (Fig. 1b).



CI. — AOUT 1659. 431

CI.

FERMAT A CARCAVI.

AOUT 1659.

(Corresp. Huyg., n° 631.)

RELATION DES NOUVELLES DÉCOUVERTES EN LA SCIENCE DES NOMBRES (1).

... 1. Et pour ce que les méthodes ordinaires, qui sont dans les Livres, étoient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir.

J'appelai cette manière de démontrer la *descente infinie* ou *indéfinie*, etc.; je ne m'en servis au commencement que pour démontrer les propositions négatives, comme, par exemple :

Qu'il n'y a aucun nombre, moindre de l'unité qu'un multiple de 3, *qui soit composé d'un quarré et du triple d'un autre quarré;*

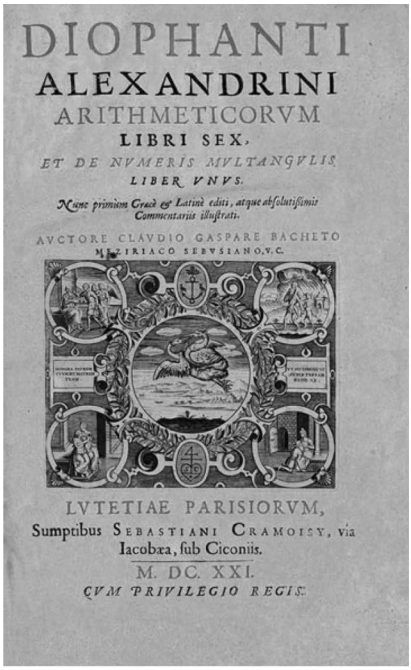
Qu'il n'y a aucun triangle rectangle en nombres dont l'aire soit un nombre quarré (2).

La preuve se fait par ἀπαγωγὴν εἰς ἄδύνατον en cette manière :

S'il y avoit aucun triangle rectangle en nombres entiers qui eût son aire égale à un quarré, il y auroit un autre triangle moindre que celui-là qui auroit la même propriété. S'il y en avoit un second, moindre que le premier, qui eût la même propriété, il y en auroit, par un pareil raisonnement, un troisième, moindre que ce second, qui auroit la même propriété, et enfin un quatrième, un cinquième, etc. à l'infini en descendant. Or est-il qu'étant donné un nombre, il n'y en a point infinis en descendant moindres que celui-là (j'entends

(1) Publiée pour la première fois par M. Charles Henry (*Recherches*, p. 215-216), d'après une copie de la main de Huygens. Cette pièce avait été envoyée « depuis peu » par Fermat à Carcavi, lorsque celui-ci la communiqua à Huygens, le 14 août 1659.
(2) *Voir* Observ. XLV sur Diophante.

(a)



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.

LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

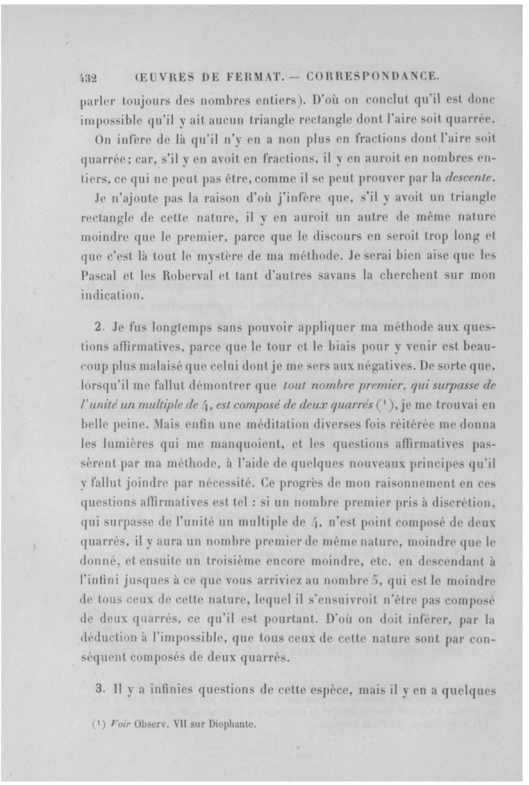
(b)

Fig. 1 **a** The *Infinite Descent* (Fermat 1891–1922, II Correspondence to Carcavi, August 1659, pp. 431 [431–436]). *Source*: With kind permission of *Gallica–National French Library* (BnF). **b** Diophantus' *Arithmetica*. (Bachet de Méziriac 1621). *Source*: Commons licensed | Public domain

[1] de Fermat's date (hereafter Fermat) of birth seems to be commonly accepted as established in 1601. But, Barner (2001) indicates that such a date is more probably 1607 or 1608. We assume no position on that.

Fermat, in his *Observations sur Diophante*, did not offer explicit roots to any Diophantine equation. Nevertheless, in the margin of this edition, Fermat wrote several annotations (posthumously published, 1670); among them, one also referred to what nowadays is called *Fermat's Last Theorem*.

For our aim, we are interested in the theorem on the primes of the form $4n+1$ (Fig. 2)[2,3]. The proposition we are facing is the following:



432 ŒUVRES DE FERMAT. — CORRESPONDANCE.

parler toujours des nombres entiers). D'où on conclut qu'il est donc impossible qu'il y ait aucun triangle rectangle dont l'aire soit quarrée.

On infère de là qu'il n'y en a non plus en fractions dont l'aire soit quarrée; car, s'il y en avoit en fractions, il y en auroit en nombres entiers, ce qui ne peut pas être, comme il se peut prouver par la *descente*.

Je n'ajoute pas la raison d'où j'infère que, s'il y avoit un triangle rectangle de cette nature, il y en auroit un autre de même nature moindre que le premier, parce que le discours en seroit trop long et que c'est là tout le mystère de ma méthode. Je serai bien aise que les Pascal et les Roberval et tant d'autres savans la cherchent sur mon indication.

2. Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y venir est beaucoup plus malaisé que celui dont je me sers aux négatives. De sorte que, lorsqu'il me fallut démontrer que *tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux quarrés* (1), je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquoient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité. Ce progrès de mon raisonnement en ces questions affirmatives est tel : si un nombre premier pris à discrétion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux quarrés, il y aura un nombre premier de même nature, moindre que le donné, et ensuite un troisième encore moindre, etc. en descendant à l'infini jusques à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivroit n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux quarrés.

3. Il y a infinies questions de cette espèce, mais il y en a quelques

(1) *Voir* Observ. VII sur Diophante.

Every prime number of the form $4n+1$ *is the sum of two squares*

Fig. 2 Fermat's Theorem on Sums of Two Squares (Fermat 1891–1922, II Correspondence to Carcavi, August 1659, pp. 432). *Source*: With kind permission of *Gallica–National French Library* (BnF)

[2] […] tout nombre premier, qui surpasse l'unité d'un multiple de 4, est composé de deux quarrés […]" (Fermat 1891–1922, II, p. 432). This $4n+1$ theorem is also called *Girard's theorem*. See below.

[3] [1891] *Œuvres de Fermat*, t. I, Œuvres mathématiques diverses – Observations sur Diophante, éd. P. Tannery et C. Henry, Paris, Gauthier-Villars; [1894], *Œuvres de Fermat*, t. II, Correspondance, éd. P. Tannery et C. Henry, Paris, Gauthier-Villars; [1896], *Œuvres de Fermat*, t. III, Traductions des écrits latins de Fermat; de l'*Inventum novum* de J. de Billy; du *Commercium epistolicum* de Wallis par P. Tannery, éd. P. Tannery et C. Henry, Paris, Gauthier-Villars; [1912], *Œuvres de Fermat*, t. IV, Compléments par P. Tannery, éd. P. Tannery et C. Henry, Paris, Gauthier-Villars; [1922], *Œuvres de Fermat*, supp. T. I-IV par M. C. de Waard, éd. P. Tannery et C. Henry, Paris, Gauthier-Villars.

Fermat often mentioned this theorem:

Observations sur Diophante, (Fermat 1891–1922, I, 7, pp. 293–297).
Letter to Mersenne on 25 December 1640 (*Ivi*, II, p. 213).
Letter to Frenicle on 15 June 1641 (*Ivi*, II, p. 221).

Where for an odd prime a of the for $4n+1$ this statement can be written as:

$a=b^2+c^2$ (where b and c are integers $\leftrightarrow$ a$\equiv -1$ (mod. 4) (for example see Pythagorean case study).

For example, we have:

$$13 = 2^2 + 3^2.$$

Nevertheless, other prime numbers like 3, 7, 11, 19, 23 and 31 cannot be calculated (decomposed) as sum of two squares.[4] As Albert Girard (1595–1632) remarked: no number of the form $4n+3$ is the sum of two squares, which is, anyway, a trivial truth. He also realized that, to use modern terms, necessary condition for an odd number to be the sum of two squares is that it is congruous -1 modulus 4. Dickson suggested that Girard dealt with both positive integral and prime numbers proving their determination by a sum of two squares of positive integers (Dickson [1919] 1920 [1923], II, p. 227–228). On our side we wonder: *how is it possible to determinate a number* $(4n+1)$ *in order to prove that any prime of the form* $4n+1$ *is the sum of two squares?* In other words, it is necessary to determinate the kind of number (a propriety) and its related equation (a form). Fermat faced this theorem by the *Infinite Descent* method. He left only an outline of his proof. Thus, a final question arises: *how might the infinite descent method be applied to Fermat's problem?*

For example, let us consider the following decompositions of 17 and 29:

$$17 = 4^2 + 1^2 \text{ and } 29 = 5^2 + 2^2$$

Fermat conceived an idea like this: By means of *Infinite Descent* method let us suppose that a prime p of the form $4n+1$ which does not have this propriety exists, that is, it is not the sum of two squares. If, given this hypothesis, it would be possible to show that, starting from p, a decreasing series of numbers (a descent, in fact) should exist until reaching numbers as 29 or 17, which, according to the descent should not be the sum of two squares, but, indeed, are, this would imply a contradiction. Such contradiction depends on the fact that p had been supposed not to be the sum of two squares.[5] Hence, p is the sum of two squares. Fermat applied the outlined reasoning not to 17 or 29, but to 5. For, when $n=1$, we obtain the number 5, which can be written as:

$$5 = 2^2 + 1^2$$

However, the prime number 5 should not have this propriety. But, effetely, the prime number 5 is *uniquely* determinable as the sum of two squares: 2^2+1^2. Thus, the assertion is valid for any prime of form $4n+1$ (see Fermat's correspondence to Huygens/Carcavi).

[4] Generally speaking, it depends on the congruence to 0 or to -1 (mod. 4).

[5] One might also claim that another smaller number exists, which does not have that property. But n is an arbitrary number, so *descending infinitely* to all n–positive integers, one arrives at $n=1$. In other words, the descending sequence starting from p has, so to say, a natural less number, that is the smallest number of the prime $4n+1$, namely 5, assuming $n=1$.

Even if it could be considered similar, it is necessary to precise that Fermat's *Infinite Descent* is different from mathematical induction method for the following mathematical reasons.[6] In the *Infinite Descent*:

- Just after having claimed the *ad absurdum* hypothesis for a certain value of n, then it is possible to find another smaller number, having the same propriety; and this number must not be necessarily the immediately next number along the *series of the natural number* (*descending*).
- The method is able to falsify some assumptions. This is the main use of it.

Leonhard Euler (1707–1783), basing on Fermat's *Infinite Descent*, proposed—maybe—the first published and complete proof of the $4n+1$ primes theorem. It is in letters (1747, April 6th and 1749, April 12th) to Christian Goldbach (1690–1764) and then it was published in two articles (Euler 1752–1753, pp. 3–40, 1754–1755, pp. 3–13).

Fermat's studies on number theory were the theoretical base for many scholars (Euler, Lagrange, Gauss, Dedekind, Minkowski, etc.).

2 The Aim of this Paper

Since this paper aims at explaining the logic of the infinite or indefinite descent, an application of this method concerning the $4n+1$-*primes* theorem and dating back to the beginning of the twenty first century will be proposed because it is particularly significant in order to:

(1) Show the general features of the method;
(2) Specify the mathematical and logical differences among the possible uses of the descent.

The proof on which we will focus has been explained by Sergio Paolini (1938–2009).[7] By his reasoning, it is possible to analyse and re–interpret the steps that characterize an application based on Fermat's method. The core of this paper has the following structure:

(1) Initial section in which the general logic of the descent is expounded;
(2) A historical outline of the theorems enunciated by Fermat and proved by infinite descent after Fermat;
(3) A detailed summary of the way in which Paolini proved the $4n+1$ primes theorem;
(4) A deeper explanation of the logic connoting the infinite descent as a consequence of the analysis carried out in the previous sections.

[6] The problem of the logical relations between *infinite descent* and the various forms of mathematical induction (ordinary mathematical induction, Noetherian induction, and so on) will be faced if the sixth section of this paper. The three items we add in the running text need only as a description of the differences between the mathematical application of infinite descent and ordinary induction. For the moment we do not enter the logical questions connected to the relations between the two methods. In addition and generally speaking, it is not necessary to claim a specific case for which the theorem is satisfied; it is only necessary to prove that the basic case ($n=1$) contradicts.

[7] One of us (PB) translated Paolini's work into English (Bussotti 2006, pp. 481–554; for the proofs on the binary quadratic forms, see pp. 481–507, pp. 496–499; on Fermat see pp. 17–184). On Paolini see: Bussotti and Paolini 1997; Bussotti 2000; Bussotti 2008, pp. 63–112.

The foundational reasons behind this article are historical–mathematical and logical (Pisano and Gaudiello 2009).

From a historical point of view, Paolini's proof of the $4n+1$ primes theorem follows step by step the scarce indications left by Fermat. This is a novelty.

From a mathematical point of view this proof exploits methods, which were available to Fermat.

From a logical standpoint, it allows to spread a light on a rather obscure subject: the different applications of the method invented by Fermat.

3 The Logical Structure of the *Infinite Descent*

The infinite descent is a method of *reductio ad absurdum*. For example, let us suppose that a theorem T has to be proved. Let us assume (*ad absurdum*) that $\neg T$ is true. If it is possible to demonstrate that $\neg T$ implies the existence of an infinity of integers between n and 1 (or 0), this is absurd. Therefore $\neg T$ is false and T is true. The smallest limit of the descent is not necessarily 0 or 1. It can be an integer $m < n$. In this case $\neg T$ would imply the existence of an infinite quantity of numbers between[8] m and n.

A quite easy example of a theorem that can be proved by descent was proposed by Euclid in his *Elements* (VII, 31) where he proved that every composite number p is divided by a prime number. The proof runs as follows:

Let be $p = p_1p_2$. Both p_1 and p_2 are composite numbers, otherwise the theorem is true. Both p_1 and p_2 divide p and are greater than 1 because p is composite. Hence they are smaller than p. Euclid considered then $p_1 = p_3p_4$, once again p_3 and p_4 are composite numbers and they are smaller than p_1 and greater than 1. But if we want to deny the truth of the theorem, we would admit an infinite descent $p < p_1 < p_3 < \cdots < 1$ in integers. This is absurd, hence the theorem is true.

This proof by Euclid is interesting because it represents the first case of a complete proof by descent in mathematical literature. On the other hand, the application is so elementary that it is sufficient to create an easy descent based on a reduction from p to p_1 and from p_1 to p_3 in order to obtain the proof, whereas the application of the descent to more difficult theorems is often complicated and the reduction from a value to a smaller value for which the theorem is supposed false can be problematic. However, Euclid's proof is a useful introduction to the subject.

4 On the Theorems Proved by *Infinite Descent*

In the letter[9] above mentioned sent to Christian Huygens through Pierre de Carcavi and entitled *Relation des nouvelles découvertes en la science des nombres* (Fermat 1891–1922, II, pp. 431–436) Fermat pointed out that the classical methods used in arithmetic were not sufficient to deal with the most difficult theorems. He had been able to invent a new

[8] From a theoretical point of view, it would be sufficient to show that, if the theorem was false, then more than $m - n - 1$ numbers would exist between m and n, which is absurd.

[9] With regard to the discovery of this letter by Fermat to Huygens, see: Henry 1879 in Fermat 1879, pp. 737–740; Bussotti 2006, p. 5, ft. 4.

method, which allowed him to solve a series of complicate problems. This method is exactly the infinite descent. We read:

> 1. And since the ordinary methods explained in the Books, are not sufficient to prove so difficult propositions, finally I have found a particular way to reach the demonstration. I will call this method of proof *infinite descent* or *indefinite* [*descente infinie* ou *indéfinie*]; at the beginning, I used it in order to prove negative propositions as for example […] *there is no right triangle in numbers* [that is a Pythagorean triangle] *of which the area is equal to the square of an integer number* […].
> The proof is based on the *απαγωγην εις αδυνατον* [*reductio ad absurdum*] […][10]

By these words, Fermat declared himself to be the inventor of the infinite descent (*Ibidem*). Certainly, he knew Euclid's work, but the Euclidean proof by descent is not quite indicative insofar as it is applied to a very elementary proposition. Furthermore, it is not part of a context in which the descent has a primary role: it is an application. On the contrary, Fermat claimed that a great part of his most significant theorems could be proved by descent. But which are the "difficult propositions" (*Ibidem*) of which Fermat was speaking? In the aforementioned letter to Huygens we find the answer. Fermat explained four different kinds of applications of his method:

(a) To *ordinary*[11] negative propositions. He quoted two theorems in this category:

(1) The mentioned theorem concerning the fact that the area of a Pythagorean triangle is never the square of an integer[12];
(2) No number of the form $3n-1$ is of the form x^2+3y^2.

The case of this last theorem is interesting from a historical point of view because its demonstration is really easy. It is enough to write the numbers mod.3 and to see that the square of a number which is not a multiple of 3 is of the form $3n+1$. In this sense, no descent is necessary. Fermat was one of the first mathematicians who fully understood the importance to write the numbers in function of a modulus k and a remainder h, that is, in the form[13] $kn+h$. However, the science of numbers was at the beginning of its development, so we

[10] "1. Et pour ce que les méthodes ordinaires, qui sont dans les Livres, étoient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir. J'appelai cette manière de démontrer la *descente infinie ou indéfinie*, etc." je ne m'en servis au commencement que pour démontrer les propositions négatives, comme, par exemple: […] *Qu'il y a aucun triangle rectangle en nombres dont l'aire soit un nombre quarré* […] (Fermat 1891–1922, II, p. 431; see also pp. 212–217). Our translation.

[11] Fermat did not write the word *ordinary*. We use it because it expresses epistemologically–synthetically the thought of Fermat that there are four different ways in which his method can be applied.

[12] This proposition is the only one of which Fermat left an almost complete demonstration in his *Observations sur Diophante* (observation 45; Fermat 1891–1922, I, p. 340. See also Bussotti and Paolini 1997, pp. 36–39 and 55–71; Edwards 1977, chapter 1.6.; Goldstein 1995; Mahoney 1973, 1994, pp. 352–354; Weil 1984, chapter 2, paragraph X.

[13] To write a class of numbers in the form $kn+h$ means, in modern terms, to write such a class in function of the modulus k and the remainder or residue h. Fermat, Euler, Lagrange and Legendre were well aware of this way of writing and of the concepts of modulus and of residue. However, the mathematician who fully developed the whole potential of the notion of congruence based and a modulus and on a residue was Gauss in his *Disquisitiones Arithmeticae* (Gauss 1801). Gauss gave the formal definition of two congruent numbers in respect to a modulus (first section of the *Disquisitiones*) and based the entire, magnificent theory expounded in his masterpiece on the concept of congruence between two numbers.

cannot exclude that the inventor of the modern way to conceive a number had not completely explored the potentiality of this way of writing. Therefore, we should not be surprised that Fermat claimed to have used the descent for theorems, which are difficult nowadays, too, and for theorems, which are very easy in a modern perspective. Exactly the perspectives were different.

(b) To *affirmative propositions*. Here the use of the descent is quite more difficult and—following Fermat's words—new principles are necessary. Fermat included in this category his theorems concerning the binary quadratic forms. That is:

(1) Every prime numbers of the form $4n+1$ is the sum of two squares, namely it is of the form x^2+y^2.

In this letter, Fermat claimed: "3. There are infinite questions of this kind […]".[14] It is almost sure he was referring to the problems concerning the binary quadratic forms of the prime numbers. In particular, in a letter to Blaise Pascal (1623–1662) on 25 September 1654, Fermat argued that[15] (Fermat 1891–1922, II, p. 313):

(2) Every prime of the form $8n+1$ and every prime of the form $8n+3$ are the sum of a square and of the double of another square. This means that these two classes of primes are of the form x^2+2y^2;
(3) Every prime number of the form $6n+1$ is the sum of a square and of the triple of another square. It can hence be written as x^2+3y^2.

He wrote cryptal words with regard to the $4n+1$ primes theorem. We will mention them at the beginning of the next section and show that they can be understood in the light of Paolini's proof which we will explain in Sect. 5.

(c) To particularly difficult affirmative propositions. Here Fermat mentioned two problems:

(1) Every integer is the sum of four integer squares;
(2) the equation $Ny^2 = x^2 - 1$ (N is not a square) has always an infinite number of integer solutions.[16]

[14] "3. Il y a infinies questions de cette espèce […]" (Fermat 1891–1922, II, p. 432). Our translation.

[15] He repeated these theorems concerning the decomposition of the primes of the forms $4n+1$, $6n+1$, $8n+1$, $8n+3$ in a letter to Digby on June 1658 (Fermat 1891–1922, II, p. 403; see also Bussotti 2006, pp. 177–180).

[16] Fermat dealt with the polygonal numbers theorem on many occasions. The general proposition (every integer is the sum of three triangulars, of four squares, of five pentagonals, of six hexagonals, on so on) was, for example, mentioned in *Observations sur Diophante* (Fermat 1891–1922, I, p. 305), in a letter to Mersenne in September/October 1636 (Fermat 1891–1922, II, pp. 65–66). In the letter to Pascal on 25 September 1654 (*Ivi*, pp. 312–313). In the letter to Digby on 19 June 1658 (*Ivi*, pp. 403–404). For the proofs given by Paolini of the three triangulars and four squares theorem with methods available to Fermat, see Paolini (Bussotti 2006, Appendix, pp. 507–534 and 534–547 respectively). For the explanation of the used methods, see: Bussotti 2006, pp. 109–171. The reference to Pell equation dates to a late phase of Fermat's "mathematical career". Beyond the letter to Huygens, Fermat spoke of this equation starting from February 1657, for example in a letter to Frenicle in that month (Fermat, 1891–1922, II, p. 333). A letter to Brouncker dates to the same month (*Ivi*, p. 335). For the relations between Fermat and the English mathematicians as to the solution of this equation see Bussotti 2006, pp. 77–109. On so called Pell–Fermat equation see: Barbeau 2003; Hofmann 1944; Konen 1901; Selenius 1963; Weil 1977.

This is the famous so wrongly called Pell (1611–1685) equation.[17] The correct name would be Fermat equation.

(d) To particularly difficult negative propositions. Fermat mentioned the following ones:

(1) The cubic case of Fermat's last theorem, that is $x^3 + y^3 \neq z^3$, with x, y, z positive integers[18];
(2) The equation $x^2 + 2 = y^3$ has only the integral solution (5,3);
(3) The equation $x^2 + 4 = y^3$ has only the integral solutions (2, 2); (11, 5);
(4) Every number of the form $2^{2^n} + 1$ is prime.

The last proposition (4) is false as Euler proved (Euler 1732–1738).

Therefore, Fermat—in the above mentioned letter (Fermat 1891–1922, II, pp. 431–436)—claimed that there are four different ways to apply the infinite descent. Unfortunately, he left only one complete demonstration: that concerning the Pythagorean triangle and the indications relative to the theorem on the primes of the form $4n+1$ that we will refer to.

After Fermat, as above cited, Euler tried to reconstruct Fermat's results (Euler 1732–1738)[19] and methods and supplied many demonstrations by descent, also considering some Diophantine problems not mentioned by Fermat. However, Euler's most important applications of the method regard the propositions by Fermat. Particularly Euler proved:

(1) Three theorems concerning the divisors of the binary quadratic forms and precisely: the form $x^2 + Ay^2$, with x and y mutually prime and $A = 1$, 2 or 3, can be divided only by numbers of its same form[20];
(2) Fermat's last theorem for the exponent[21] 3 (Euler 1770, Ch. 15, § 243).

[17] John Pell (1611–1685) has nothing to do with the equation. The name was inaccurately attributed by Euler (Euler 1765).

[18] It is well known that Fermat mentioned more than once the impossibility to solve in integers the two equations $x^3 + y^3 = z^3$ and $x^4 + y^4 = z^4$, but he mentioned the impossibility to solve in integers the general equation $x^n + y^n = z^n$—apart from the trivial solutions – only in *Observations sur Diophante*, question 2 (Fermat 1891–1922 I, p. 291). The proof of the impossibility to solve in integers the equation $x^4 + y^4 = z^4$ (to be precise $x^4 + y^4 = z^2$) is included in the theorem that no Pythagorean triangle has the area equal to the square of an integer, while we have no demonstration left by Fermat of the impossibility to solve in integers the equation $x^3 + y^3 = z^3$.

[19] See also Goldbach 1747, April 6th and 1749, April 12th; Euler 1752–1753, pp. 3–40, 1754–1755, pp. 3–13.

[20] Euler used two methods to prove these theorems on the binary quadratic form $x^2 + Ay^2$ ($A = 1, 2, 3$). We call a first demonstration (see above Sect. 5.2) *reduction-descent*. It was given for the form $x^2 + y^2$ (Euler 1752–1753); form $x^2 + 2y^2$ (Euler 1756-1757); form $x^2 + 3y^2$ (Euler 1760–1761). We call a second version of the proof as *ordinary reduction* (see below; Euler 1773).

[21] It is well known that Euler's proof is based on some assumptions not demonstrated by Euler. Anyway, for the assumed assumptions it is possible to make Euler's proof more rigorous. Euler used $Q\left(\sqrt{-3}\right)$. Johann Carl Friedrich Gauß (1777–1855) proved this theorem by means of a *reversed induction* using $Z\left(\sqrt[3]{1}\right)$. Cfr. Gauss posthumous works (Gauss posthumous, *Werke* II, pp. 387–391). Weil reworked Euler's proof without using $\sqrt{-3}$ (Weil 1984, chapter 1, paragraph XVI; see also Bussotti 2006, pp. 279–287; Macys 2007). For commentary on Gauss' proof see Dickson [1919] 1920 [1923], p. 548; Ribenboim 1979, p. 39; Bussotti 2006, pp. 434–437. For reconstructions based on the descent but on principles different from Euler's see: Paolini (Bussotti 2006, Appendix, pp. 547–554; pp. 171–176) and Piyadasa (Piyadasa 2010; in this proof $\sqrt[3]{1}$ is used).

(3) Every integer that divides the sum of four mutually prime squares is the sum of four squares[22] (Euler 1773). By means of this theorem, he was also able to prove that every integer is the sum of four squares. Nevertheless, in this case, Lagrange (1736–1813) had preceded Euler (Lagrange 1770).

The theorems in (1) were used by Euler as lemmas in order to prove Fermat's theorems on binary quadratic forms.

The theorem in (3) is a lemma to prove that every integer is the sum of four integer squares.

Euler proposed two different versions of the theorems in (1) and in (3) (see note 20 and Sect. 5 of this paper). The first version is not expounded in a complete manner, but it can be made complete (Bussotti 2006, pp. 222–226). From a historical standpoint, it is maybe more interesting than the second one, because the procedure used by Euler is—in the first version—closer to Fermat's assertions. However, Fermat claimed to have used the descent in the proof of $4n+1$ primes itself and not in a lemma, although—in Euler's procedure—the theorem on the divisors of the binary quadratic forms is a fundamental step to prove the decompositions of such forms in sum of squares. This is one of the reasons why it is difficult to ascribe Euler's proof to Fermat. After Euler, Lagrange played a fundamental role in the history of number theory. His contributions are less numerous than Euler's, but they are very important. As Euler, Lagrange was interested in reconstructing and using Fermat's method. We find different applications in:

(1) *Sur la solution des problèmes indéterminés du second degré* (Lagrange 1769), where he solved all undetermined equations of second degree with two unknowns;
(2) Some argumentations in the context of the proof that every integer is the sum of four squares (1770).
(3) *Sur quelques problèmes de l'analyse de Diophante* (Lagrange 1777), where the solution of some Diophantine equations is expounded.
(4) Given a binary quadratic form, a reduced binary quadratic form with the same determinant exists (both cases of positive and negative determinants). These two are the only proofs[23] (Bussotti 2006, pp. 293–417) by descent given in the *Recherches d'Arithmétique* (1773 and 1775).

Therefore, Euler and Lagrange had an interest in rediscovering and applying Fermat's method and in the reconstruction of Fermat's number theory. After Lagrange there were

[22] As to the works dedicated to the the sums of four squares (Cfr. Euler 1754–1755; see also Pieper 1993; Bussotti 2006, pp. 261–273).

[23] As to Lagrange's demonstration of the four squares theorem see also Boucard 2014. For a story of the polygonal number theorem from the Greek period to Cauchy, also including Gauss' proof that every integer is the sum of three triangulars see Bussotti and Scimone 2009. With regard to Lagrange's *Recherches d'arithmétique* and the use of the descent, see: Lagrange 1773–1775, pp. 723–737; Bussotti 2006, pp. 362–396; Pisano and Capecchi 2013.

many applications of this procedure in number theory and in algebra,[24] but a complete methodological research on this subject was still missing.[25]

Given this reference frame, the demonstrations by Paolini are interesting for the following reasons:

(1) For the first time Fermat's theorems concerning the binary quadratic forms are proved by descent. We mean the method is not used to prove lemmas, but it is exploited in the theorems themselves;
(2) This method can be extended to a wide class of numbers of the form $x^2 + Ay^2$, while Euler's method is valid only when $A = 1, 2, 3$;
(3) The single steps of the descent are well clarified;
(4) It is possible to give a sense to some of Fermat's assertions, which, without an explanation and interpretation, seem strange or even absurd;
(5) The descent, or in any case *infinitary* methods similar to the descent, are the centre of an *arithmetical world* because as Paolini proved (Cfr. Bussotti 2006, Appendix, pp. 507–547; for the commentaries, pp. 109–171) by these methods it is possible to prove that every integer is the sum of three triangular numbers and of four squares in the context of enquiries concerning the polygonal numbers.

Furthermore he also supplied a proof of Fermat's last theorem for the exponent 3 without using $\sqrt{-3}$. For all these reasons, it seems to us that such demonstrations have a mathematical, a methodological and a historical interest. Let us now explain and comment the main reasoning carried out in Paolini's proof that every prime number of the form $4n + 1$ is the sum of two squares. This proof is a prototype for the other theorems concerning the binary quadratic forms and proved by Paolini (*Ibidem*).

5 The Proof: Every Prime Numbers of the Form $4n + 1$ is the Sum of Two Squares

This is the first proposition on the binary quadratic forms enunciated by Fermat. In a sense, this theorem opens the modern theory of numbers.

5.1 What Fermat Wrote

In the letter to Huygens, Fermat wrote as to the $4n + 1$ primes theorem (Table 1):

[24] For the theorems proved by descent, see i.e.,: Bussey 1918; Bussotti and Paolini 1997; Bussotti 2000; Bussotti 2006; Cassinet 1980; Conrad (s.d.); Dickson [1919] 1920 [1923] (many references); Genocchi 1855; Genocchi 1883; Hofmann 1960–1962; Lemmermeyer 2003; Piyadasa 2010; Shirali 2003; Tat–Wing 2005; Vacca 1927-1928; Vandiver 1932. For interesting methodological considerations see Brotherston and Simpson 2007; Smith 1992, Wirth 2004, Wirth 2010.

[25] For a research concerning the applications in Fermat, Euler, Lagrange and Gauss see Bussotti (Bussotti 2006). On Lagrange methods see Pisano and Capecchi (2013).

Table 1 What Fermat wrote on the demonstration of the $4n + 1$ primes theorem

2. Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y venir est beaucoup plus malaisé que celui dont je me sers aux négatives. De sorte que, lorsqu'il me fallut démontrer que *tout nombre premier qui surpasse de l'unité un multiple de 4, est composé de deux quarrés*, je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquoient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité. Ce progrès de mon raisonnement en ces questions affirmatives est tel: si un nombre premier pris à discrétion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux quarrés, il y aura un nombre premier de la même nature, moindre que le donné, et ensuite un troisième encore moindre, etc. en descendant à l'infini jusque à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivroit n'être pas composé de deux quarrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont par conséquent composés de deux quarrés	2. For a long time I was not able to apply my method to affirmative questions, because the way and the means to obtain this application are more difficult than those I use for the negative ones. Therefore, when I had to prove that *every prime number, which is bigger by one than a multiple of 4, is composed of two squares*, I found myself in great difficulty. But finally a meditation, which I repeated several times, brought me the light that I lacked, and affirmative questions entered my method with the addition of some new principles, which I had necessarily to add. This progress of my reasoning in these affirmative questions is such: if any prime number, which is bigger by one than a multiple of 4 were not composed of two squares, there would exist another prime number of the same nature, which is less than the given one, and a third number less than the second and so on, descending infinitely till arriving at the number 5, which is the smallest of all the numbers of that nature. This number should not be composed of two squares, but, in fact, it is. From this reasoning, it is possible to infer, by the deduction to the impossible, that all the numbers of this nature are consequently composed of two squares
Fermat 1891–1922, II, p. 432	Author's translation

A reconstruction of the proof, which could be ascribed to Fermat, should explain:

(1) Which are the new principles connoting the application of the descent to affirmative propositions.
(2) The way in which it is possible to pass from a prime number which is—*ad absurdum*—supposed not to be the sum of two squares, to a smaller number, which should not be the sum of two squares.

Furthermore, this proof should be based only upon mathematical means available to Fermat.

In this section, we will answer the latter question, while dealing with the former in the next section. A clarification with regard to Fermat's words: when he claimed that the descent should be continued infinitely till reaching 5, these words make in themselves no sense because if a descent in integers reaches any number (in this case 5) it cannot be infinite. However, what Fermat claimed is clear, as the mechanism of the descent can be continued until reaching 5.

5.2 Paolini's Proof that Every Prime of the Form $4n + 1$ is the Sum of Two Squares

In order to understand how Paolini applies the descent, it is useful to present a brief picture of the preliminary definitions and assertions that are necessary to demonstrate the theorem. Almost all the elementary proofs of this proposition start from the fact that -1 is a quadratic residue of the primes of the form $4n+1$. The proof we are analysing starts from this property, as well.

Since the value -1 is a quadratic residue of the prime numbers of the form $p=4n+1$ (that is, the congruence $x^2 \equiv -1(\mathrm{mod}.p)$ has solutions), the equation

$$kp = x^2 + 1$$

has solutions for $k<x<p$, which is the form in which Paolini presents this property (Bussotti 2006, Appendix, Theorem 1, Sect. 3, pp. 484–485). The second passage consists in defining the notion of *resolving fraction* associated to an integer number m. We read (see also Table 2):

> I associate the fraction $\frac{m}{x}$ to an integer number m [m is not necessarily a prime number] such that $km = x^2 + 1$, with $m>x$. I develop this fraction in a continued fraction and I invert the convergents. Let g_n be the biggest of the g_i such that $g_i^2 < m$. It is possible that there is a convergent $\frac{f_n}{g_n}$ such that $m = g_n^2 + (xg_n - mf_n)^2$. If such a convergent exists, then I define $\frac{m}{x}$ as a *resolving fraction* of m, in the sense that m is the sum of two squares.[26]

Table 2 Explanation of the role of the resolving fractions to decompose a number in sum of two squares

Let us consider the identity $5 \cdot 34 = 13^2 + 1$. Then the fraction associated to 34 is $\frac{34}{13}$. Its convergents are $2, 3, \frac{5}{2}, \frac{8}{3}, \frac{13}{5}, \frac{34}{13}$. If we invert these convergents, we obtain: $\frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \frac{5}{13}, \frac{13}{34}$. The biggest g_i such that $g_i^2 < 34$ is 5, so that $f_n = 2$, with $x=13$ and $m=34$. It is $34=5^2 + (13 \cdot 5 - 34 \cdot 2)^2 = 5^2 + 3^2$. So that $\frac{34}{13}$ is *resolving* of 34. The latter 34 is not a prime number. It is possible to consider the convergent directly by inverting the role of f_n and g_n. The result is clearly the same one.

[26] We have slightly modified the definition. Paolini offered two proofs of the $4n+1$ primes theorem: the former (*Ivi*, pp. 492–495) based on the concept of *even continued fraction* is inspired by Lucas (Lucas 1891, pp. 250–251). The latter is the one we are expounding. This is easier than the former and can be generalized to other binary quadratic forms, whereas the former is valid only for the primes of the form $4n+1$.

That is, a number is a sum of two squares if and only if its associated fraction is resolving.

Paolini's idea consists in proving that, if m is a prime number of the form $4n+1$, then a resolving fraction associated to m exists. The resolving fractions have three properties, proved in the following Paolini's Theorems 2, 3 and 4. To prove these properties, it is sufficient to know how to pass from a convergent of order $n-1$ to a convergent of order n. In order to demonstrate the Theorem 3, an argument that is based on complete induction is used. Here we refer to these propositions without the proof. It is possible to check the proofs in Paolini's mentioned work.[27]

(1) (Theorem 2): *If* $km = x^2 + 1\ (m > x)$ *and if and only if m/x is a resolving fraction of m, then the fraction* $\frac{m-x}{m}$ [or better $\frac{m}{m-x}$] *is resolving of* m *too. This fraction is defined as complementary fraction of m/x.*

(2) (Theorem 3): *Given an integer number m such that* $km = x^2 + 1$, $k<x<m$, *let* $\frac{x^2+1}{kx}$ *be developed in continued fraction and let* $q_0, q_1, \ldots, q_{n-1}, q_n$ *be its incomplete quotients, then the incomplete quotients of the continued fraction* $\frac{(x+k)^2+1}{k(x+k)}$ *are the same as* $\frac{x^2+1}{kx}$, *if we exclude the first one, which is* $q_0 + 1$ *and the last one.*

(3) (Theorem 4): *Let m be an integer and k and x integers such that* $k<x<m$. *Let us suppose that the equation* $km = x^2 + 1$ *has solutions and that* $\frac{m}{x}=\frac{x^2+1}{kx}$ *is a resolving fraction of* m. *Then the number* $m' = m+2x+k$ *is such that* $km' = (x + k)^2 + 1$ *and the fraction* $\frac{(x+k)^2+1}{k(x+k)}$ *is resolving of m'.*

In the following additional applications of previous theorems (Table 3):

Table 3 Example of an application of the Theorem 2 and of the Theorem 4

Theorem 2: Let us consider the identity $5 \cdot 29 = 12^2 + 1$, with $m=29$, $k=5$, $x=12$. Let us develop the fraction $\frac{29}{12}$ in continued fraction. It is $\frac{29}{12} = 2 + \frac{1}{2+\frac{1}{2+\frac{1}{2}}}$, so that the convergents are $2, \frac{5}{2}, \frac{12}{5}, \frac{29}{12}$. Let us invert them, obtaining $\frac{1}{2}, \frac{2}{5}, \frac{5}{12}, \frac{12}{29}$. The biggest g_i such that $g_i^2 < 29$ is 5. In this case the formula $m = g_n^2 + (xg_n - mf_n)^2$ is applicable because the identity $5^2 + (12 \cdot 5 - 29 \cdot 2)^2 = 5^2 + 2^2 = 29$ holds. Hence $\frac{29}{12}$ is resolving of 29. Since $m=29$ and $x=12$, the Theorem 2 asserts that also the fraction $\frac{29}{17}$ is resolving of m. For, if 12 is a solution of the congruence $x^2 \equiv -1(\mathrm{mod}.29)$, the other solution is $y = 29 - 12 = 17$. So that we have the identity $10 \cdot 29 = 17^2 + 1$, with $y=17$ and $k' = 10$. Let us consider the fraction $\frac{29}{17} = 1 + \frac{1}{1+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}}$. The convergents are $1, 2, \frac{5}{3}, \frac{12}{7}, \frac{29}{17}$. If we invert them, we have $\frac{1}{1}, \frac{1}{2}, \frac{3}{5}, \frac{7}{12}, \frac{17}{29}$. The biggest g_i such that $g_i^2 < 29$ is 5, and $5^2 + (17 \cdot 5 - 29 \cdot 3)^2 = 5^2 + 2^2 = 29$. Therefore $\frac{29}{17}$ is resolving of 29, as Theorem 2 claims.

Theorem 4: let us consider again the identity $5 \cdot 29 = 12^2 + 1$. Then $m' = m + 2x + k = 29 + 2 \cdot 12 + 5 = 58$ and $5 \cdot 58 = 17^2 + 1$. The Theorem 4 claims that the fraction $\frac{58}{17}$ is resolving of 58. If we develop this fraction in a continued fraction, we obtain: $\frac{58}{17} = 3 + \frac{1}{2+\frac{1}{2+\frac{1}{3}}}$. The convergents are $3, \frac{7}{2}, \frac{11}{3}, \frac{58}{17}$ and, inverted, they are $\frac{1}{3}, \frac{2}{7}, \frac{3}{11}, \frac{17}{58}$. The biggest g_i such that $g_i^2 < 58$ is 7, and, being $k = 5$ and $x' = 17$, it follows that $7^2 + (17 \cdot 7 - 58 \cdot 2)^2 = 7^2 + 3^2 = 58$ so that $\frac{58}{17}$ is resolving of 58.

[27] Theorem 2 (Bussotti 2006, pp. 488–490 for the first version; p. 497 for the second one). Theorem 3 (*Ivi*, pp. 491–492 for the first version; pp. 497–498 for the second one). Theorem 4 (*Ivi*, pp. 498–499).

The Theorem 3 is used only to prove the Theorem 4.

The conceptual basis of Paolini's argument consists in excluding the cases, in which the theorem is trivially proved. The general structure of the reasoning is like this.

Paolini considers a prime p of the form $4n+1$ and the two complementary fractions associated to p. He supposes *ad absurdum* that p is not the sum of two squares. This means that the two fractions associated to p, let us indicate them by A and A_1, are not resolving. From A or A_1, it is possible to deduce a fraction B which is associated to a number m less than p. The fraction B is not resolving of m otherwise, by means of the Theorem 4, the fraction associated to p from which B derives, should be resolving of p. Hence, p would be the sum of two squares. Because of Theorem 2, neither the fraction associated to m nor the complementary of B—let us indicate by B_1—are resolving of m. This process can be iterated finding a decreasing sequence of numbers $m_n < m_{n-1} < \cdots m < p$ the associated fractions to which are note resolving, otherwise those associated to p should be resolving. But the fraction associated to the "small"—the meaning of this word will be clarified in the proof—number m_n is in fact resolving. Then—by means of the Theorem 4—one concludes that the fractions associated to p are resolving, as well. Against the hypothesis that p is not the sum of two squares. This *absurdum* proves that p is the sum of two squares.

Let us see the proof in detail.

If p is a prime number of the form $4n+1$, the equation $kp = x^2 + 1$ has always solutions. If $k=1$, the number p is the sum of the two squares x^2 and 1.

If $k=2$, in an argument by *reductio ad absurdum*, it is necessary to suppose that no one of the two complementary fractions associated to p are resolving of p, otherwise p would be the sum of two squares.

If $k=2$, it is possible to subtract progressively the multiples of k (that is of 2) from x, at the condition that $k < \frac{x_n}{2}$.[28] In this way, we obtain a series of numbers, which can be indicated by m, for which the identity[29]

$$2m = (x - 2l)^2 + 1 \text{ is valid.}$$

None of the fractions $\frac{m}{x-2l}$ is resolving, otherwise the fractions associated to p would be resolving and p would be the sum of two squares (Theorem 4). Neither their complementary fractions $\frac{m}{m-(x-2l)}$ are resolving (Theorem 2). By subtracting progressively 2 from x, one arrives at

$$k = 2, x_{n+1} = 3, \text{ with } k > \frac{x_{n+1}}{2}.$$

The fraction $\frac{3^2+1}{2\cdot 3} = \frac{5}{3}$ is associated to 5 ($2\cdot 5 = 3^2+1$) and it is resolving of 5 because if we develop $\frac{5}{3}$ in a continued fraction, its convergents are: 1, 2, $\frac{5}{3}$. Inverting them one has $\frac{1}{1}, \frac{1}{2}, \frac{3}{5}$. Applying the already explained method, one obtains $5 = (3 \cdot 2 - 1 \cdot 5)^2 + 2^2$, where 2 is the biggest g_i such that $g_i^2 < 5$. Then the Theorems 2 and 4 ensure that every step of the descent is in fact composed of numbers to which resolving fractions are associated. Therefore, the fractions associated to p are resolving, hence p is the sum of two squares. But our hypothesis was that p was not. This contradiction proves the theorem. One could claim:

[28] The succession of the x_n is given by $x\text{-}k = x_1$, $x - 2\,k = x_2, \ldots$, $x\text{-}nk = x_n$.

[29] So, for example, starting from $2 \cdot 41 = 9^2 + 1$, we obtain

$$2 \cdot 25 = (9-2)^2 + 1 = 7^2 + 1$$
$$2 \cdot 13 = (7-2)^2 + 1 = (9 - 2 \cdot 2)^2 + 1 = 5^2 + 1$$
$$2 \cdot 5 = (5-2)^2 + 1 = (7 - 2 \cdot 2)^2 + 1 = (9 - 2 \cdot 3)^2 + 1 = 3^2 + 1$$

since the fractions associated to the *small numbers* are resolving and since it is possible to *ascend* backwards from the fractions associated to the small numbers to those associated to p, these fractions are resolving, but they should not be.

Contradiction, hence the theorem is true. This logical scheme in which, given a proposition A, it is (Cfr. Bellissima and Pagli 1996):

$$(\neg A \rightarrow A) \rightarrow A$$

is called *Consequentia mirabilis*.

Paolini's demonstration continues analysing the cases in which $k>2$. We will see that it is possible to construct a descent that can be continued without limits from a theoretical point of view. But this descent has an end at 5 or before 5. The descent—or more appropriately the reduction—has its end with a number, to which a resolving fraction is associated, so that also p is the sum of two squares.

Let k be an even number bigger than 2. The reasoning starts, as always, from the equation

$$kp = x^2 + 1 \tag{1}$$

The first important consideration concerns the value of k. If $k = \frac{x}{2}$, replacing this value in the equation, it follows that the possible solutions for p and x are respectively (4.1) and (5.2). But p is bigger than 5. Thus $k \neq \frac{x}{2}$. In addition, Paolini proves that if $k > \frac{x}{2}$, then in the identity

$$k'p = (p - x)^2 + 1 = y^2 + 1 \tag{2}$$

(identity that is the complementary of $kp = x^2 + 1$), one has $k' < \frac{y}{2}$ (this part of the demonstration is not difficult). Using the same technique as in the case $k=2$, one subtracts progressively k from x till $k < x - nk$ and $k > \frac{x-nk}{2}$. Posing $x - nk = x_n$, it is $k \neq \frac{x_n}{2}$ because k is even and x_n is odd. Thus, we have the following equation

$$km_1 = x_n^2 + 1 \tag{3}$$

It is trivial to prove that $x_n < m_1 < 2x_n$.

Now, let us pose $y_n = m_1 - x_n$. It is $m_1 > 2y_n$ and from Eq. 3), one obtains the equation

$$k_1 m_1 = y_n^2 + 1 \tag{4}$$

Since $k > \frac{x_n}{2}$, it is $1 \leq k_1 \leq \frac{y_n}{2}$.

Furthermore $x_n > y_n$ and therefore $k_1 < k$. All these conditions ensure that the descent can be continued, that is, the two equations

$$kp = x^2 + 1$$

and

$$k_1 m_1 = y_n^2 + 1 \tag{5}$$

have the same formal properties, but the components of the first equation are bigger than the corresponding components of the second one. It is necessary to precise that:

(1) if in $k_1 m_1 = y_n^2 + 1$, $k_1 = 1$, then the fraction $\frac{y_1^2+1}{y_1}$ is resolving of m_1 and hence m_1 is the sum of two squares. By applying the Theorem 2, also the fraction $\frac{m_1}{x_n} = \frac{x_n^2+1}{kx_n}$ (the com-

plementary fraction of $\frac{y_1^2+1}{y_1}$) is resolving of m_1, and applying the Theorem 4, one reaches the conclusion that the fraction $\frac{p}{x} = \frac{x^2+1}{kx}$ is resolving of p, so that p is the sum of two squares.

(2) If $k_1 = \frac{y_n}{2}$, it is $m_1 = 5$. In this case $y_n = 2$ is the only solution that is compatible with the fact that m_1, y_n and k are integer numbers. But in this case one has the equation $1 \cdot 5 = 2^2 + 1$. The fraction $\frac{5}{2}$ is resolving of 5, and according to Theorem 2, the fraction $\frac{5}{3}$ is resolving of 5, as well. Thus, by applying the Theorem 4, one returns to p which, for this reason, is the sum of two squares. So, really (2) is a particular case of (1).

When $k_1 < \frac{y_n}{2}$ the descent continues. But this descent cannot be infinite, so we reach either the case 1), or the case 2) or an $y^*=3$, for which one has $2 \cdot 5 = 3^2 + 1$. This fraction is resolving of 5, and the reasoning is the same as the one analysed if $k=2$.

The cases for which in the equation $kp = x^2 + 1$ the number k is odd, can be dealt with a completely similar technique.

Finally, every prime number of the form $4n+1$ is the sum of two squares.

In the following we propose an example of descent in order to see how this procedure is applied in a specific case (Table 4).

Table 4 *An application to a specific case of the explained procedure*

Let us start from the identity

(1) $10 \cdot 73 = 27^2 + 1$

It is $p=73$, $x=27$, $k=10$. So $k < \frac{x}{2}$. Therefore the first step of the descent is obtained with $k=10$ and $x_1 = (27 - 10) = 17$. The value of m_1 can be calculated or obtained automatically from the equation at the end of the Theorem 4. In this case the equation is $p = m_1 + 2x_1 + k$, that is $73 = m_1 + 2 \cdot 17 + 10$, so that $m_1 = 29$. Hence we have the identity

(2) $10 \cdot 29 = 17^2 + 1$

Here $k > \frac{x_1}{2}$. But in the complementary identity, obtained posing $y_1 = m_1 - k = 29 - 17 = 12$, we have

(3) $5 \cdot 29 = 12^2 + 1$

Hence $k_1 = 5$, and $k_1 < \frac{y_1}{2}$. So the descent continues. Now with $k_1 = 5$, $y_1 = 12$ and $m_1 = 29$, we obtain $y_2 = 12 - 5 = 7$. So that, in order to obtain m_2, the equation $m_1 = m_2 + 2y_2 + k_1$ can be applied, that is $29 = m_2 + 14 + 5$, so that $m_2 = 10$ and one gets the identity

(4) $5 \cdot 10 = 7^2 + 1$.

Now $k_1 > \frac{y_2}{2}$, but the complementary identity, that is obtained as in the previous case, is

(5) $1 \cdot 10 = 3^2 + 1$.

Here $k_1' = 1$ and the descent is ended. But the fraction $\frac{m_2}{x_2} = \frac{10}{3}$ is resolving of 10. For, developing it in continued fraction, it is $\frac{10}{3} = 3 + \frac{1}{3}$, the convergents are 3, $\frac{10}{3}$ and inverted they are $\frac{1}{3}$, $\frac{3}{10}$. The biggest g_i such that $g_i^2 < 10$, is 3, and, since it is $m_2 = 10$, $x_2 = 3$, $f_n = 1$, it holds $g_n^2 + (x_2 \cdot g_n - m \cdot f_n)^2 = 3^2 + (3 \cdot 3 - 10 \cdot 1)^2 = 3^2 + 1^2 = 10$. Thence $\frac{10}{3}$ is resolving of 10. But, for the Theorem 2, also the complementary fraction of $\frac{10}{3}$, that is $\frac{10}{7}$ (Identity 4) is resolving of 10, and for the Theorem 4, the fraction from which $\frac{10}{7}$ derives, that is $\frac{29}{12}$ (Identity 3) is resolving of 29, and again for the Theorem 2, also $\frac{29}{17}$ (Identity 2) is resolving of 29, and, finally, for the theorem 4, $\frac{73}{27}$ (Identity 1) is resolving of 73, that is 73 is the sum of two squares. Now we summarize the procedure in a diagram:

$$
\begin{array}{c}
10 \cdot 73 = 27^2 + 1 \\
\downarrow \\
10 \cdot 29 = 17^2 + 1 \leftrightarrow 5 \cdot 29 = 12^2 + 1 \\
\updownarrow \\
5 \cdot 10 = 7^2 + 1 \leftrightarrow 1 \cdot 10 = 3^2 + 1
\end{array}
$$

5.3 Relations between Fermat's Assertions and Paolini's Proof

After Fermat, the elementary demonstrations concerning the form $x^2 + Ay^2$ ($A = 1, 2, 3$), in which the descent or a reduction is used and which are not inscribed inside a general theory of the binary quadratic forms as Lagrange's or Gauss' (1777–1855) are of two types (both derive from Euler's ideas):

1. Given a number p which divides the sum of two coprime squares, then p is the sum of two squares. In the case of $x^2 + y^2$, starting from the identity $n \cdot p = x^2 + y^2$, the number n is progressively reduced until reaching 1 in identities of the form $n_i \cdot p = x_i^2 + y_i^2$. Since it is possible to reach $n_i = 1$, then p is the sum of two squares. If p is a prime of the form $4n + 1$, due to the congruence $x^2 \equiv -1(\mathrm{mod}.p)$, p divides the sum of two squares and hence it is the sum of two squares. *Mutatis mutandis*, the reasoning when $A = 2,3$ is the same (Euler 1773; Conrad s.d., p. 13).

This argumentation cannot be attributed to Fermat because there is no *reduction ad absurdum*, n is reduced until reaching 1, but no *apagoge eis adynaton*, to use Fermat's words, exists. Furthermore, n is reduced, but not p, while, according to Fermat's words, p has to be reduced.

2. In a phase of his career as a number theoretician which dates back about to the period 1750–1755, Euler had not yet fully developed his ideas and methods on the quadratic residues. In this phase a theorem was discovered, proved and used by him as a lemma to prove the $4n + 1$ primes theorem: "a number which is the sum of two coprime squares can be divided only by numbers which are the sum of two coprime squares". Here the reasoning is similar to what Fermat could have been thought: the "little" numbers which are the sum of two mutually prime squares are either primes or can be divided only by numbers which are the sum of two mutually prime squares. This is an inductive basis. Let us now suppose, *ad absurdum*, that $a^2 + b^2$, $(a, b) = 1$, is divided by a number p which is not the sum of two coprime squares. Euler was able to prove that a number $c^2 + d^2$, which is less than $a^2 + b^2$, exists $(c, d) = 1$, and is divided by a number which is not the sum of two squares. The process can be iterated until reaching the "small" numbers which are the sum of two coprime squares. But these numbers are divided only by numbers which are the sum of two squares, while, they should not be. This contradiction proves the theorem.[30]

Here the resort to the *reductio ad absurdum* exists, but the reasoning is applied to an important lemma to prove the $4n + 1$ primes theorem, not to the theorem itself. Therefore, even if Euler's proof is likely close to Fermat's way of thinking, it is difficult to ascribe it to Fermat. The proof given by Paolini gets all the elements Fermat spoke about:

[30] We have here summarized a reasoning which is rather refined and which – in the form given by Euler – is not completely satisfying, but the basis of Euler's argument is correct at all. On the forms $a^2 + b^2$, $a^2 + 2b^2$ and $a^2 + 3b^2$ (Bussotti 2006, pp. 222–226; 238–242; p. 246 respectively).

(a) It is conceived as a *reductio ad absurdum*
(b) It is applied directly in the proof of the theorem, not in a lemma.
(c) Given the identity $k \cdot p = x^2 + 1$, the reduction we have seen acts either reducing k, or reducing p, according to the specific conditions characterizing every step of the process. Therefore either a value $k_i = 1$ is reached before $m_i = 5$ or $m_j = 5$ is reached, as Fermat claimed.
(d) The continued fractions were well known and used in Fermat's time and the properties of the continued fractions exploited in the shown proof are elementary and need no mathematical element extraneous to Fermat's way of thinking (Bussotti 2006, pp. 68–77).
(e) Fermat wrote of new principles of the infinite descent applied to affirmative propositions and, as we will see in the next section, new principles exist in Paolini's proof: (1) there is an inductive basis for which the theorem is true, the *small numbers*; (2) after the descent there is an *ascent* which permits to prove that the fractions associated to p, are resolving. The reasoning is an example of *consequantia mirabilis*.

Given this picture, we think that this proof can be reasonably ascribed to Fermat. This is clearly an epistemological consequence based on the historical-logical reconstruction. However it is important—from a mathematical and methodological standpoint—that, in the historical-epistemological reconstruction of Fermat's methods; a procedure which fits with almost all his assertions has been found. Therefore, two further remarks are necessary:

(a) Fermat wrote that all numbers of the descent are prime of the form $4n+1$. This seems difficult to admit because in this manner Fermat would have found a series consisting only of primes, a result which was, maybe, more important than the theorem in itself. It is enough to admit that every step of the descent contains numbers which should not be—*ad absurdum*—the sum of two squares, without the further request they are prime. A posteriori, since the proof shows that every number of the descent is in fact the sum of two squares, and has -1 as a quadratic residue, such numbers have no factor of the form $4n+3$, but this truth is known only a posteriori.

(b) By means of the method of the resolving fractions it is possible to decompose in the form $x^2 + Ay^2$ a wider class of prime numbers than those belonging to the forms $4n+1$, $6n+1$, $8n+1$ and $8n+3$, the classes of which Fermat spoke and whose properties can be proved by Euler's methods. For example, it is possible to prove that every prime of the form $20n+1$ is of the form $x^2 + 5y^2$(Fermat did not deal with this form). A theoretical research concerning all the classes of primes to which this technique can be applied is still missing.

6 Intermezzo: A logical Variant of the *Infinite Descent* and the *New Principles*

In this section, after having provided a symbolization of the proposed proof, the variants of the descent will be analysed.

6.1 The logical structure of the proposed proof

First, let us specify the logical scheme of this demonstration. Let us denote:

By p the proposition "the two fractions associated to the prime number $4n+1$ are not resolving".

By p_1 the proposition "the two fractions associated to the first number of the descent are not resolving".

By p_n the proposition "the two fractions associated to the n-th number of the descent are not resolving".

By p_{n+1} the proposition "the two fractions associated to 5 are not resolving". The argument by descent proves that

$$((p \to p_1) \wedge (p_1 \to p_2) \wedge \ldots \wedge (p_n \to p_{n+1}))$$

But

$$((p \to p_1) \wedge (p_1 \to p_2) \wedge \ldots \wedge (p_n \to p_{n+1})) \to (p \to p_{n+1})$$

is a tautology. Therefore, we deduce $(p \to p_{n+1})$ by *modus ponens*. On the other hand, $\neg p_{n+1}$ is true, so that we have, applying *modus tollens*:

$$\begin{array}{l} p \to p_{n+1} \\ \neg p_{n+1} \\ \hline \neg p \end{array}$$

That is, every prime number of the form $4n+1$ has a resolving fraction and therefore it is the sum of two squares.

6.2 The Variants of the Infinite Descent

In every argument by descent, the presence of a *form*, that has the same formal properties with different order of size, is an essential element. Also in Paolini's reasoning there is such a form and it is represented by the two identities $kp = x^2 + 1$ and $k'p = y^2 + 1$. The identities that we obtain in the descent have the same formal properties of these two, but they represent numbers which become progressively smaller. The same reasoning is valid for the fraction that are associated to the numbers p, m, $m_1, \ldots, 5$. All of them are constructed in the same way. The existence of numerical forms having the same formal properties, but representing, in the descent, progressively decreasing numbers, are typical of all the arguments in which this method is applied. However, the ways in which the reasoning is developed are so different case by case that Fermat was justified to speak of *new principles*.

Let us start from the application to what, following the distinction by Fermat, one could call the *application to ordinary negative propositions*. An appropriate and paradigmatic example is given by the only proposition of which Fermat left an almost complete proof: *the area of a Pythagorean triangle is not the square of an integer*. Given a Pythagorean

triple (*x,y,z*), the area of the triangle whose sides are *x, y, z* is $\frac{xy}{2}$. In the two triples (0,0,0) and (1,0,1), it is $\frac{xy}{2}=0$ and 0 is the square of an integer. Clearly no triangle can have a side equal to 0, nevertheless it is important to take into account this property of the triples (0,0,0) and (1,0,1). At the beginning of the demonstration, it is necessary to suppose—*ad absurdum*—that a Pythagorean triple (x, y, z), which is different from (0,0,0) and (1,0,1), exists, such that $\frac{xy}{2}$ is equal to the square of an integer. But one proves that, given some properties of the Pythagorean triples and the particular conditions of the theorem, it is possible to construct a triple (x_1, y_1, z_1) such that $z_1 < z$ but $z_1 > 1$ with the condition that $\frac{x_1 y_1}{2}$ is the square of an integer. This procedure can be iterated, obtaining a value $z_2 < z_1$ and $z_2 > 1$, being $\frac{x_2 y_2}{2}$ the square of an integer.

Under these conditions, an infinite descent in integers would be given because an infinite quantity of integers would exist between z and 1, this is absurd and hence the theorem is true. There are three fundamental steps in this demonstration:

1. To show that the *hypotenuses* of the hypothetical triangles have an invariant form.
2. To prove that the sequence of the hypotenuses is decreasing.
3. To prove that every hypotenuse is bigger than 1.

The latter is an important condition because if the descent reached the triple $1^2 + 0^2 = 1^2$, this descent would not have been *infinite*, but *finite* and, by repeating this finite process backwards, a set of Pythagorean triangles would have been obtained *whose area would be equal to the square of an integer*. That is, the opposite of Fermat's assertion. But since $1 < \cdots z_n \cdots < z$ and the process can be iterated, an infinite descent is constructed. Therefore the existence of a lower limit, in this case the triples (0,0,0) and (1,0,1), *which cannot be reached* is fundamental for the application of the infinite descent to negative propositions. For what Fermat called the affirmative propositions, things work in another manner:

1. There is a set of values—which can be considered *small*—for which the theorem T to prove is true.
2. Supposing that T is not true for a certain value *V*, it is possible to construct an algorithm which proves T to be false for a value *W* less than *V*. This algorithm can be iterated, but not *indefinitely*, it is a finite algorithm which reaches the small values with the condition that for such values the theorem T should be false, whereas it is true. This contradiction, deriving from the supposition that T is false for a certain number, proves that T is, in fact, true for every number. In some cases, as the analysed one, an *ascent* follows the descent.

The logical scheme of the *consequentia mirabilis* is applied.

Here the final point of the descent is reached, which is the opposite of the application to negative propositions and the algorithm, though it can be indefinitely prosecuted from a formal point of view, is in fact finite. Therefore, the *reductio ad absurdum* is used; the algorithm is potentially infinite, but really finite.

At all appearances, these are the new principles of which Fermat spoke. Now Fermat's words have a complete interpretation. We have called this application to affirmative propositions *reduction-descent* because the algorithm is a reduction rather than an infinite descent.

In what follows we will clarify the differences between the reduction-descent and the procedure we call *ordinary reduction*. It is worth underlining that affirmative propositions exist which are proved by applications of the descent, based on the same principles as those characterizing the application to negative propositions. Lagrange and Gauss offer examples of these demonstrations (Lagrange 1773–1775, pp. 723–737; Gauss 1801, p. 146).

With regard to the ordinary reduction, let us consider the way in which John Wallis (1616–1703) and William Brouncker (1620–1684) solved Pell equation. For, it is based on a *reduction*. That is, given Pell equation $x^2 = Ny^2 + 1$, the two English mathematicians constructed a series of equations having a solution if and only if $x^2 = Ny^2 + 1$ has solutions.

Furthermore the possible solutions of the n-th equation are smaller than the ones of the $(n-1)$-th. But from this reduction it is not absolutely possible to conclude that there is an infinite descent and that therefore Pell equation has no solutions. On the contrary, Wallis and Brouncker reached the solution (1,1) and therefore Pell's equations *has always solution*. In this case, a *definite descent* has been obtained. We call this method *ordinary reduction.* From a methodological point of view, the second version of Euler proofs that if a number divides the form $x^2 + Ay^2$, with $A = 1$, 2 or 3, $(x,y) = 1$, then it has the same form as the dividend, and that if a number divides the sum of four squares, then it is the sum of four squares are based on ordinary reductions. Here there is neither a *reductio ad absurdum* nor an infinite descent. It is difficult to say if, when Fermat thought of the particularly difficult affirmative propositions, he was referring to this method. The lack of a *reductio ad absurdum* can induce to think he was not. Hence three different applications of procedures based on a reduction can be identified:

1. *Infinite descent in a proper sense*, supposing **T** to be false, the existence of an infinity of integers between two integers m and n follows.
2. *Reduction descent*, when the theorem is true for an initial segment of integers and denying that it is valid for any integer, we are able to construct a procedure which obliges to admit it is false for the initial segment. This contradiction proves the theorem.
3. *Ordinary reduction*, when one is able to prove that a theorem is true for any value if and only if it is true for *small values*, but for small values it is true, hence it is true for any value.

The reduction descent, with its resort to an *ad absurdum reasoning*, can be used when an ordinary reductions fails. For example in case of Paolini's proof, if he had proved that if the fractions associated to a number p are resolving, then also the fractions associated to a number less than p are, then an ordinary reduction could have been applied. But he proved that if the fraction associated to p is resolving than the fraction associated to a number which is greater, no less, than p is resolving. This proposition can be used only in a demonstration *ad absurdum*—as the one explained—not in a direct proof of the $4n + 1$ primes theorem.

6.3 Internal and External Logic

In this section[31] three methods have been analysed:

[31] The features of this section are different from those of the other sections, where we have presented the final results of a research, while this section has to be interpreted as an outline and a proposal for a new research rather than the explanation of final results.

(1) *Infinite descent* in a proper sense;
(2) *Reduction descent*;
(3) *Ordinary reduction*.

In some way, all three can be connected to Fermat and to the problems and theorems he posed and discovered. There is a method which is strictly correlated to 1) and 2): the principle of the smallest integer. It is based on the idea that if a problem has solutions in integers, then it has a solution which is the smallest one. Therefore—dealing with integers –, in a reasoning by *reductio ad absurdum* for the theorem **T**, it is possible to hypothesize that a certain value or set of values are the smallest ones for which ¬ **T** is true and, after that, to show that a smaller value or set of values exist. This contradiction proves **T** is true. The first mathematician who used explicitly the method of the smallest integer was probably Lagrange.[32] This way of reasoning can be applied both while dealing with *infinite descent* or *reduction descent*. These methods can hence be included inside the more general scheme of the *principle of the smallest integer*, even if some doubts might be expressed on the fact that this inclusion embraces all the cases in which *infinite descent* and *reduction descent* are applied (Cfr. Bussotti 2006, pp. 451–456).

The relation between infinite descent, reduction descent and principle of the smallest integer introduces an important problem: *what is the role of formal logic in mathematics?* It is well known that, from the point of view of the mathematical logic all the methods we have analysed are logically equivalent to mathematical induction. However, in history and in practice of mathematics these methods have been used for different classes of problems: for example, no demonstration by mathematical induction exists of the fact that every prime of the form $4n+1$ is the sum of two squares or that the equation $x^3 + y^3 = z^3$ has no integral solutions if we exclude the trivial ones. This is true for most theorems proved by the methods we have expounded. The question is*: does a general mechanism **M** which allows us to transcribe a proof by descent into a proof by mathematical induction, so that, after having obtained this proof, we can avoid to consider all the steps of **M** and obtain a proof by mathematical induction which seems independent of its deduction from the proof by descent*? This is exactly what happens in projective geometry: for example, in space projective geometry the law of duality permits to obtain (for axioms and theorems) and demonstrate (for theorems) a graphical proposition from another one replacing the word "point" by "plane", the word "to cut" by "to project" and leaving unmodified the word "straight line" (Table 5).

Table 5 One of the most elementary examples in which the duality law is applied

Three points *a, b, c* which do not belong to a straight line determine a *triangle*, which is composed of three points (vertices), of the three straight lines *ab, ac, bc* and by the plane *abc*.	Three planes *α, β, γ* which do not belong to a straight line [that is, which do not belong to a pencil of planes] determine a *trihedral angle*. The figure is composed of three planes (faces), of the three straight lines they determine *αβ*, *αγ*, *βγ* (edges) and of the point *αβγ*.

[32] See, for example the admirable demonstrations by Lagrange that all the solutions of Pell equation $t^2 - Du^2 = 1$ are of the form $t = \frac{(t_1+u_1\sqrt{D})^m+(t_1-u_1\sqrt{D})^m}{2}$; $u = \frac{(t_1+u_1\sqrt{D})^m+(t_1-u_1\sqrt{D})^m}{2\sqrt{D}}$ (Lagrange 1774, Sects. 72–75; Bussotti 2006, pp. 352–362).

It would be interesting to determine whether such automatic transformation of a proof given by descent in a proof given by mathematical induction can exist. In any case, though from the point of view of the formal logic the analysed methods are equivalent to mathematical induction, their *internal* logic is different (Cfr. Gauthier 1991, 2002):

(1) As far as mathematical logic is concerned, the distinction between affirmative and negative propositions makes no sense because an affirmative proposition can be transformed into a negative one and viceversa. Any deductive scheme is a tautology. But for a mathematician this distinction can be significant because the way in which a proposition is presented can open the possibility to a proof which—otherwise—could not have been conceived.
(2) The possibility to use the *reductio ad absurdum* can also open perspectives of proof, which are excluded otherwise. Therefore, even if from a logical point of view, schemes of proof by *reductio ad absurdum* are proved to be logically equivalent to schemes in which the *reductio* is not used, in the practice of mathematics these schemes can be applied to different kinds of situations.
(3) *Infinite descent, reduction descent and principle of the smallest integer* allow us "to go backwards", that is given a value, they are based on the construction of a smaller value, whereas the mathematical induction allows us "to go forwards". This feature can also represent a great difference from a mathematical point of view, because the first three methods permit to exploit the property that, given two integers, only a finite number of integers can exist between them, while this is not the case with mathematical induction.

Finally, the internal logic of the infinite descent and of the mathematical induction is different because these methods are based on different properties of the mathematical objects (the integers, in this case) and on different ways of thinking of the mathematicians. The internal logic can highlight properties of the mathematical methods and of mathematics as an activity carried out by human beings, with their hard work, their failures and their successes, which, with a mere formal approach, might remain obscure. Mathematical logic provides an external approach to mathematics. It is quite useful to classify methods, theorems and problems and to avoid logical mistakes, but it cannot be confused with the internal logic of mathematics. These methods are hence different from a mathematical standpoint, even if they are logically equivalent.

7 Conclusion

The seventeenth century is well–known as the century of the scientific revolution. For, several fields of the human knowledge—especially in relation to exact sciences—were either created or improved in a substantial manner. Taking into account this context, new interests raised in the *Scientia de ponderibus*, ballistic, practical geometry (Pisano and Capecchi 2015) until new Mechanics (Bussotti and Pisano 2014). This new movement of ideas stimulated the parallel developing of mathematical science: the use and theory of the equations in geometry, symbolism, pure calculus and obviously its relationship with physical science (Pisano and Capecchi 2013).

The modern theory of numbers also dates back to the seventeenth century and it has to be inscribed, generally speaking, within the outlined picture. Fermat was the main protagonist of this new mathematical current of studies. However, he provided no publication in

which his statements and proofs were explained. Rather, he suggested several arguments close to the modern Number Theory within several letter to his scientific correspondents.

7.1 An Assumption

From a historical–mathematical viewpoint, the infinite descent has often been used in the context of the Diophantine analysis in order to determine the possible solutions of certain equations or classes of equations achieved through this method. It is a particular kind of proof by contradiction based on the *well–ordering principle*.

One might assume that Fermat might have created an entire number theoretical construction and that the $4n+1$ theorem represented, in a sense, the core of Fermat's number theory. For, it is connected with several of his most profound researches.

With regard to the problem of the Pythagorean triples, the fact that every prime number of the form $4n+1$ is the sum of two squares allowed Fermat to grasp the class of numbers which can be the hypotenuse of a Pythagorean triangle and how many times a composite number can be hypotenuse (Bussotti, 2006, pp. 177–180). Fermat, for example, wrote in a letter to Frenicle (15 June 1641):

> The fundamental proposition of the right triangles is that every prime number which exceeds by a unity a multiple of 4 is composed of two squares.[33]

Therefore, this fundamental theorem is the basis to solve the traditional Diophantine problems concerning the right triangles. Furthermore, it is the basic statement for the theory of binary quadratic forms of the kind Ax^2+By^2. Fermat dealt with the form x^2+By^2 ($A=1$, $B=1,2,3$). The form x^2+y^2 is a prototype for the study of the others. Moreover, the theorem is also connected with the following equation:

$$x^2 - Ny^2 = -1$$

faced by Fermat, too. This equation is the easiest extension of Pell's equation. But, in contrast to the latter, there is a precise necessary condition for the equation to have a solution. For, it is necessary that N has –1 as a quadratic residue, that is, if it is a prime number, it must be of the form $4n+1$.

Fermat also assumed that the $4n+1$ primes theorem is necessary to prove the polygonal numbers theorem. This theorem is stated both in *Observations sur Diophante* (Fermat 1891–1922, I, Observation XVIII, p. 305; in order to comment Diophantus' *quaestio* XXXI, Book IV), and in many letters and is considered by Fermat as one of the most significant and general in number theory. It is worth pointing out that it appears in Fermat's correspondence from 1637 (Fermat 1891–1922, II), while the $4n+1$-primes theorem appears from 1640 (*Ibidem*). Therefore, one could conjecture that

Fermat first proved the three "triangles" theorem and on its basis the four squares theorem, and then the general theorem on the polygonal numbers.

[33] "La proposition fondamentale des triangles rectangles est que tout nombre premier, qui surpasse de l'unité un multiple de 4, est compose de deux quarrés". (Fermat 1891–1922, II, p. 221; Author's translation).

Why? Because it can also historically–epistemologically justify that:

(a) In a phase of the proof of the three triangulars theorem, the property according to which *every prime number of the form* $4n + 1$ *is the sum of two squares* might be necessary (Cfr. Paolini, in Bussotti 2006, pp. 507–534 and, for an explanation see Bussotti, 2006, pp. 129–142).
(b) Fermat declared that he had to prove—"[…] lorsqu'il me fallut démontrer […]" (Fermat 1891–1922, II, p. 432)—the theorem on the prime numbers of the form $4n + 1$; as if this proposition represented a lemma for proving other propositions.

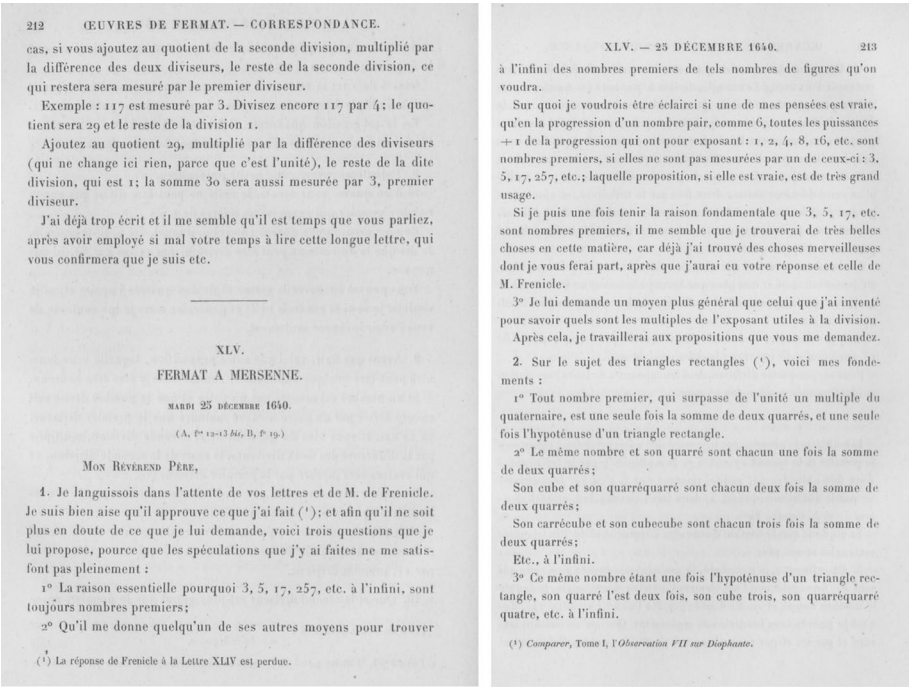
This could be a reasonable–so–possible reconstruction of Fermat's work. Following these conjectural assumptions:

(c) Fermat could have also assumed this property $4n + 1$ primes as hypothesis delaying its proof some years later.
(d) The relations between the $4n + 1$ theorem and the polygonal numbers theorem are historically consistent with Fermat's assertions (cfr. Letter to Pascal in 1654; Fermat 1891–1922, II) and with a recent proof (also given by Paolini) in which the $4n + 1$-primes theorem is used to prove the three triangulars theorem, which, in its turn, is exploited to demonstrate the other assertions on the polygonal numbers Theorem.

For, Fermat's edifice of number theory acquires an admirable inner coherence and interconnection.

7.2 Concluding Remarks

In the letter to Mersenne, dating to 1640, 23rd December (Fig. 3), Fermat claimed (Fermat 1891–1922, II, pp. 212–213) that the prime numbers of the form $4n + 1$ and its square are the sum of two squares, and that this decomposition is possible in only one way. Thus, of any prime of the form $4n + 1$ cube and bi-square are obtained in two ways only, as sum of two square, and so on to the infinitum (Fig. 3).



212 ŒUVRES DE FERMAT. — CORRESPONDANCE.

cas, si vous ajoutez au quotient de la seconde division, multiplié par la différence des deux diviseurs, le reste de la seconde division, ce qui restera sera mesuré par le premier diviseur.

Exemple : 117 est mesuré par 3. Divisez encore 117 par 4; le quotient sera 29 et le reste de la division 1.

Ajoutez au quotient 29, multiplié par la différence des diviseurs (qui ne change ici rien, parce que c'est l'unité), le reste de la dite division, qui est 1; la somme 30 sera aussi mesurée par 3, premier diviseur.

J'ai déjà trop écrit et il me semble qu'il est temps que vous parliez, après avoir employé si mal votre temps à lire cette longue lettre, qui vous confirmera que je suis etc.

XLV.

FERMAT A MERSENNE.

MARDI 25 DÉCEMBRE 1640.

(A, f^os 12-13 bis, B, f^o 19.)

MON RÉVÉREND PÈRE,

1. Je languissois dans l'attente de vos lettres et de M. de Frenicle. Je suis bien aise qu'il approuve ce que j'ai fait (1); et afin qu'il ne soit plus en doute de ce que je lui demande, voici trois questions que je lui propose, pource que les spéculations que j'y ai faites ne me satisfont pas pleinement :

1° La raison essentielle pourquoi 3, 5, 17, 257, etc. à l'infini, sont toujours nombres premiers;

2° Qu'il me donne quelqu'un de ses autres moyens pour trouver

(1) La réponse de Frenicle à la Lettre XLIV est perdue.

XLV. — 25 DÉCEMBRE 1640. 213

à l'infini des nombres premiers de tels nombres de figures qu'on voudra.

Sur quoi je voudrois être éclairci si une de mes pensées est vraie, qu'en la progression d'un nombre pair, comme 6, toutes les puissances + 1 de la progression qui ont pour exposant : 1, 2, 4, 8, 16, etc. sont nombres premiers, si elles ne sont pas mesurées par un de ceux-ci : 3, 5, 17, 257, etc.; laquelle proposition, si elle est vraie, est de très grand usage.

Si je puis une fois tenir la raison fondamentale que 3, 5, 17, etc. sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière, car déjà j'ai trouvé des choses merveilleuses dont je vous ferai part, après que j'aurai eu votre réponse et celle de M. Frenicle.

3° Je lui demande un moyen plus général que celui que j'ai inventé pour savoir quels sont les multiples de l'exposant utiles à la division.

Après cela, je travaillerai aux propositions que vous me demandez.

2. Sur le sujet des triangles rectangles (1), voici mes fondements :

1° Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle.

2° Le même nombre et son quarré sont chacun une fois la somme de deux quarrés;

Son cube et son quarréquarré sont chacun deux fois la somme de deux quarrés;

Son carrécube et son cubecube sont chacun trois fois la somme de deux quarrés;

Etc., à l'infini.

3° Ce même nombre étant une fois l'hypoténuse d'un triangle rectangle, son quarré l'est deux fois, son cube trois, son quarréquarré quatre, etc. à l'infini.

(1) *Comparer*, Tome I, l'*Observation VII sur Diophante*.

Fig. 3 Fermat's Letter to Mersenne on the Sums of Two Squares (Fermat 1891–1922, II Correspondence to Mersenne, December 1640, pp. 212–213). *Source*: With kind permission of *Gallica–National French Library* (BnF)

For example, when $n = 1$, we have:

$$5 = 2^2 + 1^2$$
$$5^2 = 3^2 + 4^2$$
$$5^3 = 2^2 + 11^2$$

and

$$5^3 = 5^2 + 10^2$$

and so on.

Fermat did not deal only with the sums of two squares, but also with other binary quadratic forms such as:

$$x^2 + 2y^2$$
$$x^2 + 3y^2$$
$$x^2 - 2y^2$$

In this sense, each prime number can be represented as follows:

$$6n + 1 \text{can be represented by the form } x^2 + 3y^2$$
$$8n + 1 \text{can be represented by the form } x^2 + 2y^2$$
$$8n + 3 \text{can be represented by the form } x^2 + 2y^2$$

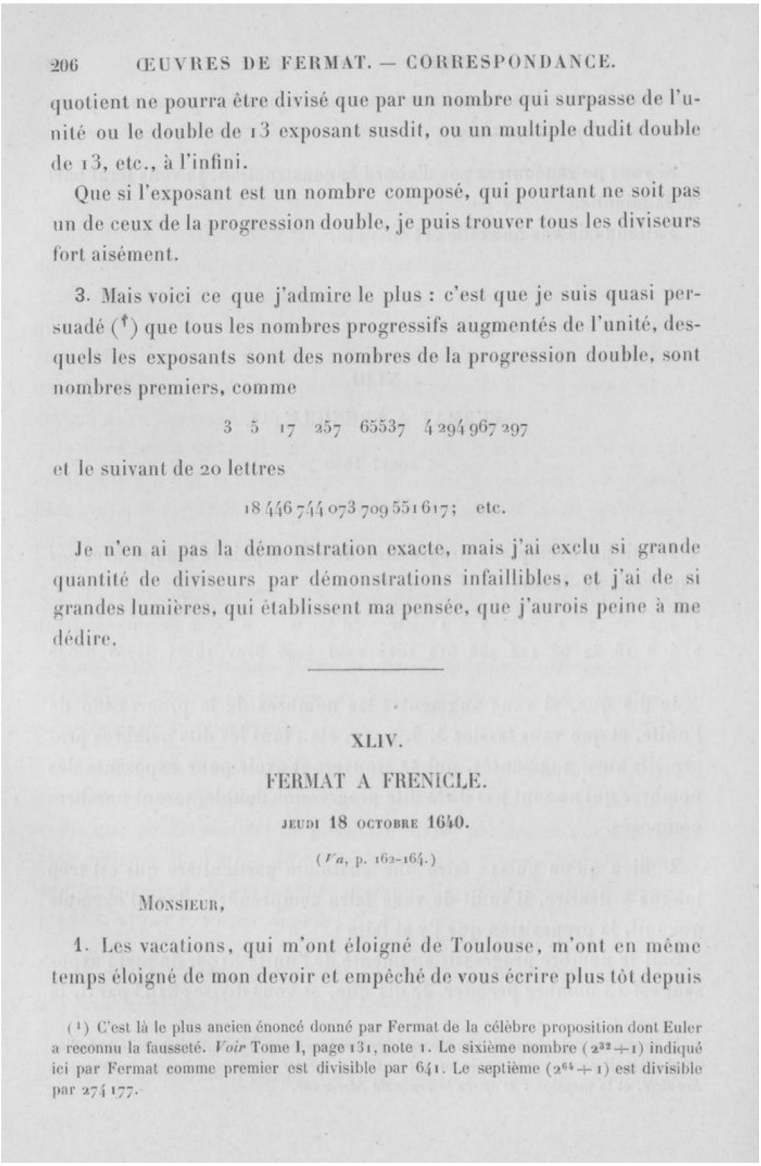
By the way, it was known from a long time that, since the squares are the sum of the successive odd numbers, every odd number—therefore both prime and composite numbers—can be represented as the difference of two squares (Cfr. Pisano and Capecchi 2015, 2013).

We should remark that Fermat thought to have found a general formula in order to determine prime numbers for each arbitrary value of n. However, this argument lacked of proofs. For, Fermat's statement is false; so, epistemologically, it also loses its general supposed evidence.

As a matter of fact, since 1640, in another letter (Fig. 4), Fermat believed to have found a series exclusively composed of prime numbers. Such series is

$$(2)^{2^n} + 1$$

In an initial phase, he admitted not to be able to prove such a proposition (Fermat 1891–1922, II, p. 206),—which hence—he proposed as a conjecture (Fig. 4), but, afterwards, in the above mentioned letter to Huygens (1659) via Carcavi he claimed to have proved his statement, which is impossible (Fermat 1891–1922, II, p. 431–432).



206 ŒUVRES DE FERMAT. — CORRESPONDANCE.

quotient ne pourra être divisé que par un nombre qui surpasse de l'unité ou le double de 13 exposant susdit, ou un multiple dudit double de 13, etc., à l'infini.

Que si l'exposant est un nombre composé, qui pourtant ne soit pas un de ceux de la progression double, je puis trouver tous les diviseurs fort aisément.

3. Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé (†) que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme

3 5 17 257 65537 4 294 967 297

et le suivant de 20 lettres

18 446 744 073 709 551 617; etc.

Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurois peine à me dédire.

XLIV.

FERMAT A FRENICLE.

JEUDI 18 OCTOBRE 1640.

(*Fa*, p. 162-164.)

MONSIEUR,

1. Les vacations, qui m'ont éloigné de Toulouse, m'ont en même temps éloigné de mon devoir et empêché de vous écrire plus tôt depuis

(†) C'est là le plus ancien énoncé donné par Fermat de la célèbre proposition dont Euler a reconnu la fausseté. *Voir* Tome I, page 131, note 1. Le sixième nombre $(2^{32}+1)$ indiqué ici par Fermat comme premier est divisible par 641. Le septième $(2^{64}+1)$ est divisible par 274 177.

Fig. 4 Fermat's Letter to Frenicle on the Sums of Two Squares (Fermat 1891–1922, II Correspondence to Frenicle, August (?) 1640, p. 206) *Source*: With kind permission of *Gallica–National French Library* (BnF)

Until nowadays, we know that for the above formula the primes are the first following numbers only: 3, 5, 17, 257, 65,537 (Fermat 1891–1922, II, XLIII, p. 206). However, as above mentioned, he claimed (letter to Huygens; *Ibidem*) to have proved this proposition, which is impossible, as this proposition is false, as Euler proved (Euler 1752-1753, pp. 3–40, 1754–1755, pp. 3–13).

Fermat also dealt with other questions that he solved by *infinite descent*. As above said, his most remarkable one concerns the theorem according to which the area of

a Pythagorean triangle is not the square of an integer. Particularly, Fermat proposed an almost complete proof (Fermat 1891–1922, I, p. 340, III, p. 271) based on *Infinite Descent* concerning this theorem. A corollary of such a theorem by Fermat is that the following equation, by means of integers only, is impossible:

$$x^4 + y^4 = z^4$$

It has no integral solution.

To conclude, this paper has to be considered as a contribution to the following problems:

(1) *History of mathematics*: it is possible to prove Fermat's theorems on binary quadratic forms following the scarce indications left by Fermat and by means of methods, which were available to him.
(2) *Explanations on mathematical methods*: under the name *infinite descent* are, in general, included three different methods: infinite descent, reduction descent, ordinary reduction. We have clarified their differences and shown that, following these differences, many assertions by Fermat, which seemed difficult to be understood, are subject to a reasonable interpretation.
(3) *Difference between internal and external logic of mathematics*. This is connected with the relations between mathematical logic and mathematics. This is an interesting research field on which still many specifications and clarifications have to be given by the scholars.
(4) Inner connections of Fermat's number theory. Fermat was working to a whole number-theoretical edifice in which the $4n + 1$-*primes* theorems was one of the fundamental bases and the polygonal numbers theorem was the most relevant result.

Acknowledgements We acknowledge *Gallica National French Library* (BnF) for its kind permission and we address our gratitude to anonymous referees for their valuable remarks, which have been of great help.

References

Barbeau, E. (2003). *Pell's equation*. New York: Springer.
Barner, K. (2001). Das Leben Fermats. *DMV Mitteilungen, 3,* 12–26.
Bellissima, F., & Pagli, P. (1996). *Consequentia mirabilis: una regola logica tra matematica e filosofia*. Olschki: Firenze.
Boucard, J. (2014). Joseph-Louis Lagrange e il teorema dei quattro quadrati. *Lettera Matematica Pristem, 88*(89), 59–69.
Brotherston, J., Simpson, A. (2007). Complete Sequent Calculi for Induction and Infinite Descent. In *Proceedings of logic in computer science. 22nd annual IEEE symposium on logic in computer science (LICS 2007)* (pp. 51-62). Los Alamos: IIEE.
Bussey, W. H. (1918). Fermat's method of infinite descent. *The American Mathematical Monthly, 25*(8), 333–337.
Bussotti, P. (2000). "Ogni numero primo della forma 4n + 1 è la somma di due quadrati": storia dei metodi dimostrativi usati per provare un teorema. *L'insegnamento della matematica e delle scienze integrate, 23A,* 27–63.
Bussotti, P. (2006). *From Fermat to Gauss. Indefinite descent and methods of reduction in number theory*. Augsburg: Rauner.
Bussotti, P. (2008). *Problems and methods at the origin of the theory of numbers*. Napoli: Giannini.
Bussotti, P., & Paolini, S. (1997). *Pierre de Fermat e la discesa indefinite*. Pisa: ETS.

Bussotti, P., & Pisano, R. (2014). Newton's Philosophiae Naturalis Principia Mathematica "Jesuit" Edition: The Tenor of a Huge Work. *Accademia Nazionale Lincei Rendiconti Lincei Matematica e Applicazioni, 25*(4)*,* 413–444.

Bussotti, P., & Scimone, A. (2009). *Sulle orme di Fermat. Il teorema dei numeri poligonali e la sua dimostrazione*. Lugano: Agorà-Lumieres internationales.

Cassinet, R. (1980). Histoire de la descente infinie da Campanus à Hilbert. *Cahiers du Séminaire d'Histoire des Mathématiques de Toulouse, 2/B,* 1–25.

Conrad, K. (s. d). *Proofs by descent*. Retrieved http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/descent.pdf.

de Fermat, P. (1891–1922). *Œuvres, four volumes plus Supplément aux tomes I–IV.* Paris: Gauthier–Villars.

Dickson, L. E. ([1919] 1920 [1923]). *History of the theory of numbers* (Vol. 3 Vol). Washington: Carnegie Institution of Washington.

Edwards, H. M. (1977). *Fermat's last theorem: A genetic introduction to algebraic number theory*. New York: Springer.

Euler, L. (1732–1738). *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*. Commentarii academiae scientiarum Petropolitanae 6, pp. 103–107. In OO, Ser. I, II, pp. 1–5.

Euler, L. (1752–1753). *De numeris qui sunt aggregata duorum quadratorum*. Novi commentarii academiae scientiarum Petropolitanae, 4, pp. 3–40. In OO, Ser. 1, II, pp. 295–327.

Euler, L. (1754–1755). *Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*. Novi commentarii academiae scientiarum Petropolitanae 5, pp. 13–58. In OO, Ser. 1, II, pp. 338–372.

Euler, L. (1756–1757). *Specimen de usu observationum in mathesi pura*. Novi commentarii academiae scientiarum Petropolitanae, 6, pp. 185–230. In OO, Ser. 1, II, pp. 459–492.

Euler, L. (1760–1761). *Supplementum quorundam theorematum arithmeticorum quae in nonnullis demonstrationibus supponuntur*. Novi commentarii academiae scientiarum Petropolitanae, 8, pp. 105–128. In OO, Ser. 1, II, pp. 556–575.

Euler, L. (1765). *De usu novi algorithmi in problemate Pelliano solvendo*. Novi commentarii academiae scientiarum Petropolitanae, 11, pp. 28–66. In OO, Ser. 1, III, pp. 73–111.

Euler, L. (1770). *Algebra*. Petersburg. In OO, Ser. 1, I.

Euler, L. (1773). *Novae demonstrationes circa resolutionem numerorum in quadrata*. Nova acta eruditorum, pp. 193–211. In OO, Ser. 1, III, pp. 218–239.

de Fermat, P. (1879). Relation des nouvelles découvertes en la science des nombres. *Bullettino di bibliografia, XII,* 737–740.

Gauss, C. F. (1801). *Disquisitiones arithmeticae*. Leipzig. In Gauss [1870] 1876 (Vol. I).

Gauss, C. F. ([1870] 1876). *Werke* (Vol. I–II). Göttingen-Berlin, Gesellschaft der Naturwissenschaften zu Göttingen.

Gauss, C. F. (posthumous). *Zur Theorie der complexen Zahlen. Neue Theorie der Zerlegung der Cuben (Nachlass)*. In Gauss [1870] 1876 (Vol. I, pp. 387–391).

Gauthier, Y. (1991). *La logique interne*. Paris: Vrin.

Gauthier, Y. (2002). *Internal logic. Foundations of mathematics from Kronecker to Hilbert*. Dordrecht: Kluwer.

Genocchi, A. (1855). Sopra tre scritti inediti di Leonardo Pisano pubblicati da B. Boncompagni. *Annali di scienze matematiche e fisiche VI*. Roma, Tipografia delle Belle Arti, pp. 161–185, pp. 218–251, pp. 273–320, pp. 345–362.

Genocchi, A. (1883). Intorno a un manoscritto di Pietro Fermat testè pubblicato. *Rivista scientifico–industriale delle principali scoperte ed invenzioni fatte nelle scienze e nelle industrie* (pp. 148–151) [French translation: Fermat, Oeuvres, supplément aux tomes I–IV, pp. 152–157].

Goldstein, C. (1995). *Un théorème de Fermat et ses lecteurs*. Saint Denis: Presses Universitaires de Vincennes.

Hofmann, J. E. (1944). *Studien zur Zahlentheorie Fermats (Über die Gleichung $x^2 = py^2 + 1$)*. Berlin: Verlag der Akademie der Wissenschaften.

Hofmann, J. E. (1960-62). Über zahlentheoretische Methoden Fermats und Eulers, ihre Zusammenhänge und ihre Bedeutung. *Archive for History of Exact Sciences, I*, 122–159.

Kline, M. (1999). *Storia del pensiero matematico* (Vol. 2). Torino: Einaudi.

Konen, H. (1901). *Geschichte der Gleichung t^2–$Du^2 = 1$*. Leipzig: Hirzel.

Lagrange, J. L. (1769). Sur la solution de problèmes indéterminés du second degré, in Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin, t. XXIII. In *Fermat 1891–1922* (II, pp. 375–535).

Lagrange, J. L. (1770). Démonstration d'un théorème d'arithmétique. Nouveaux Mémoires de l'Académie royale des Sciences et Belles–Lettres de Berlin. In *Fermat 1891–1922* (III, pp. 187–201).
Lagrange, J. L. (1774). *Additions aux Eléments d'Algèbre d'Euler*. In., 7, pp. 3-180. See also: Euler, OO, 1, I, pp. 499–651 with the title *Additions à l'analyse indéterminée*.
Lagrange, J. L. (1777). Sur quelques problèmes de l'analyse de Diophante. Nouveaux Mémoires de l'Académie royale des Sciences et Belles–Lettres de Berlin. In *Fermat 1891–1922* (IV, pp. 375–398).
Lagrange, J. L. (1870–1873). *Œuvres de Lagrange*. Seconde édition. Paris : Courcier (ed), XIV vols. (in X) Paris: Gauthier–Villars.
Lagrange, J. L. ([1773] 1775). Recherches d'arithmétique. Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin". In *Fermat 1891–1922* (III, pp. 693–758, 759–795) [first and second part respectively].
Lemmermeyer, F. (2003). *Higher descent on Pell conics. I. From Legendre to Selmer*. http://www.fen.bilkent.edu.tr/~franz/publ/pell-a-pdf.
Lucas, E. (1891). *Théorie des nombres*. Paris: Gauthier-Villars.
Macys, J. J. (2007). On Euler's hypothetical proof. *Mathematical Notes, 82*(3), 352–356.
Mahoney, M. S. ([1973] 1994). *The mathematical career of Pierre de Fermat 1601–1665*. Princeton: Princeton University Press.
OO Euler, L. ([1911, 1913, 1915, 1917] 1941). *Opera Omnia, Series 1*. Vols. I, X, II, III, IV. Leipzig and Berlin: Teubner.
Pieper, H. (1993). On Euler's contribution to the four–squares theorem. *Historia Mathematica, 20,* 12–18.
Pisano, R., Agassi, J., & Drozdova, D. (Eds.). (2017). *Hypothesis and perspective in history and philosophy of science. Homage to Alexandre Koyré 1892–1964*. Dordrecht: Springer.
Pisano, R., Bussotti, P. (2013). On popularization of scientific education in Italy between 12th and 16th centuries. In *Problems of education in the 21st century* (Vol. 57, pp. 90–101).
Pisano, R., & Bussotti, P. (2016). A Newtonian tale details on notes and proofs in Geneva Edition of Newton's Principia. *Bulletin of the British Society for the History of Mathematics, 31*(3), 160–178.
Pisano, R., & Bussotti, P. (2017). On the conceptualization of force in Johannes Kepler's corpus: an interplay between physics/mathematics and metaphysics. *Pisano, Agassi and Drozdova 2017,* 295–346.
Pisano, R., & Capecchi, D. (2013). Conceptual and mathematical structures of mechanical science in the western civilization around 18th century. *Almagest, 4*(2), 86–121.
Pisano, R., & Capecchi, D. (2015). *Tartaglia's science weights. Mechanics in XVI century. Selections from Quesiti et inventioni diverse*. Dordrecht: Springer.
Pisano, R., & Gaudiello, I. (2009). Continuity and discontinuity. An epistemological inquiry based on the use of categories in history of science. Polish Academy of Sciences. *Organon, 41,* 245–265.
Piyadasa, R. A. D. (2010). Method of infinite descent and proof of Fermat's last theorem for n = 3. *Canadian Journal of Computing in Mathematics, Natural Sciences, Engineering and Medicine, 1*(6), 181–186.
Ribenboim, P. (1979). *13 Lectures on Fermat's last theorem*. New York: Springer.
Selenius, C. O. (1963). Kettenbruchtheoretische Erklärung der zyklischen Methode zur Lösung der Bhashare–Pell- Gleichung. *Acta Academiae Aboensis. Mathematica et Physica, XXIII,* 3–44.
Shirali, S. A. (2003). Infinite descent—but not into Hell. *Resonance, 2,* 42–55.
Smith, S. T. (1992). Quadratic residues and $x^3 + y^3 = z^3$ in models of IE1 and IE2. *Notre Dame Journal of formal logic, 34*.
Tat-Wing, L. (2005). The method of infinite descent. *Mathematical Excalibur*, *10*(11), 1–2, 4.
Vacca, G. (1927–1928). Sul principio della discesa di Fermat e sulle dimostrazioni dell'esistenza degli irrazionali quadratici. *Atti della reale accademia delle scienze di Torino*, *63*, 241–252.
Vandiver, H. S. (1932). On the method of infinite descent in connection with Fermat's last theorem for regular primes. *Commentarii Mathematici Elvetici, 4,* 1–8.
Weil, A. (1977). Fermat et l'équation de Pell. *ΠΡΙΣΜΑΤΑ. Naturwissenschaftgeschichtliche Studien* (pp. 441–447). Wiesbaden: Franz Steine Verlag.
Weil, A. (1984). *Number theory: an approach through history from Hammurapi to Legendre*. Boston: Birkhäuser.
Wirth, C. P. (2004). Descente infinie + deduction. *Logic journal of the IGPL, 12*(1), 1–96.
Wirth, C. P. (2010). A self–contained and easily accessible discussion of the method of descente infinie and FERMAT's only explicitly known proof by descente infinie. *Seki Working-paper SWP-2006-02*. arXiv :0902.3623