German Research Center for Artificial Intelligence

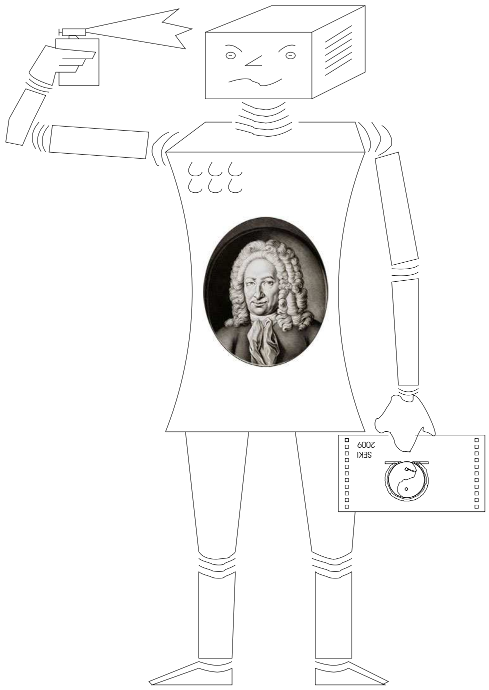
JACOBS UNIVERSITY

UNIVERSITÄT DES SAARLANDES

SEKI Working-Paper

http://www.dfki.de/seki

ISSN 1860-5931



A Self-Contained and Easily Accessible Discussion of the Method of *Descente Infinie* and Fermat's Only Explicitly Known Proof by *Descente Infinie*

Claus-Peter Wirth

Dept. of Computer Sci., Saarland Univ., D–66123 Saarbrücken, Germany

wirth@logic.at

SEKI Working-Paper SWP–2006–02

SEKI is published by the following institutions:

German Research Center for Artificial Intelligence (DFKI GmbH), Germany

- Robert Hooke Str. 5, D–28359 Bremen
- Trippstadter Str. 122, D–67663 Kaiserslautern
- Campus D 3 2, D–66123 Saarbrücken

Jacobs University Bremen, School of Engineering & Science, Campus Ring 1, D–28759 Bremen, Germany

Universität des Saarlandes, FR 6.2 Informatik, Campus, D–66123 Saarbrücken, Germany

SEKI Editor:

Claus-Peter Wirth
E-mail: `wirth@logic.at`
WWW: `http://www.ags.uni-sb.de/~cp`

Please send surface mail exclusively to:

DFKI Bremen GmbH
Safe and Secure Cognitive Systems
Cartesium
Enrique Schmidt Str. 5
D–28359 Bremen
Germany

This SEKI Working-Paper was internally reviewed by:

Paolo Bussotti
Via Paolo Lilla 66, 57122 Livorno, Italy
E-mail: `paolo.bussotti@alice.it`

A Self-Contained and Easily Accessible Discussion of the Method of *Descente Infinie* and FERMAT's Only Explicitly Known Proof by *Descente Infinie*

CLAUS-PETER WIRTH

Dept. of Computer Sci., Saarland Univ., D–66123 Saarbrücken, Germany

wirth@logic.at

Submitted: 2006, Aug. 20. First Print Edition: 2006, Nov. 2.
Thoroughly Revised Second Edition: 2010, Dec. 14

Abstract

We present the only proof of PIERRE FERMAT by *descente infinie* that is known to exist today. As the text of its Latin original requires active mathematical interpretation, it is more a proof *sketch* than a proper mathematical proof. We discuss *descente infinie* from the mathematical, logical, historical, linguistic, and refined logic-historical points of view. We provide the required preliminaries from number theory and develop a self-contained proof in a modern form, which nevertheless is intended to follow FERMAT's ideas closely. We then annotate an English translation of FERMAT's original proof with terms from the modern proof. Including all important facts, we present a concise and self-contained discussion of FERMAT's proof sketch, which is easily accessible to laymen in number theory as well as to laymen in the history of mathematics, and which provides new clarification of the Method of *Descente Infinie* to the experts in these fields. Last but not least, this paper fills a gap regarding the easy accessibility of the subject.

Keywords: Descente Infinie, Foundations of Mathematics, Pierre Fermat, MSC03-03, MSC01A45

Résumé

Nous présentons la seule preuve de Pierre Fermat par descente infinie qui est connue aujourd'hui. Car le texte de son origine latine exige une interprétation mathématique active, il est plus un croquis de preuve qu'une preuve mathématique complète. Nous discutons la descente infinie par les points de vues mathématique, logique, historique, linguistique et par un point de vue logique-historique raffiné. Nous fournissons les préliminaires nécessaires à partir de la théorie des nombres et nous développons une preuve en forme moderne, qui se satisfait à elle-même et qui suit pourtant de près les idées de Fermat. Nous continuons par annoter une traduction anglaise de la preuve originale de Fermat avec les termes de la preuve moderne. Y compris tous les faits importants, nous présentons une discussion concise et cohérente du croquis de preuve de Fermat, qui est facilement compréhensible pour des profanes en théorie des nombres ainsi pour des profanes en l'histoire des mathématiques, et qui offre des explications nouvelles de la méthode de descente infinie aux experts dans ces domaines. Finalement ce document comble une lacune en ce qui concerne la compréhensibilité du sujet.

Contents

1 Introduction and Motivation

It seems that — for pedagogical as well as political reasons — myth has to surround the truly paradigmatic figures in the history of science with fictitious association disconnected from the historical facts. GALILEO GALILEI (1564–1642) is the primary example for this; cf. [FEYERABEND, 1975], [PRAUSE, 1986b]. But also the most famous mathematician PIERRE FERMAT is a subject of myth. For instance, on the one hand, one has tried to turn FERMAT into a model for mankind, cf. [STEPHEN, 1960]. On the other hand, FERMAT was accused to be a rogue:

> "Actions, however, speak louder than words. The fact that none of the many letters of FERMAT which survive gives any real indication of his methods surely means that, consciously or unconsciously, he was very jealous, secretive, and competitive about his work, as were all of his contemporaries."
>
> [EDWARDS, 1977, § 1.6, p.11]

The myth on FERMAT even continues with his name and his life time, for a funny collection cf. [GOLDSTEIN, 1995], § 1. The most famous mathematician PIERRE FERMAT was born not in 1601 as usually claimed, but either in 1607 or in January 1608. The PIERRE FERMAT born in 1601 died before his stepbrother, our most famous PIERRE FERMAT was born. Our FERMAT was a competent lawyer and devoted judge of the parlement of Toulouse (*conseilleur au parlement de Toulouse*), a position which he bought and by which he was admitted the title *éculier*. Thus, PIERRE *de* FERMAT is the address to the noble judge.

The mathematician PIERRE FERMAT only existed in the very rare leisure time of this most busy judge. What would mathematics be like today if this incredible genius would not have put mathematics behind family, profession, social status, and commerce? For more up-to-date information on FERMAT's life we recommend [BARNER, 2001] instead of the better known [MAHONEY, 1994], as the latter provides reliable information only on the mathematics of FERMAT.

All what is important for us here, is that the field of *number theory* as we know it today, was basically created by the mathematician PIERRE FERMAT (1607?–1665). He built and improved on DIOPHANTUS OF ALEXANDRIA (3rd century?), who had looked for rational solutions of a large number of problems in number theory. In number theory, FERMAT left the classical association to geometry behind (but was more ingenious than FRANÇOIS VIÈTE (1540–1603)) and insisted on integer solutions for the problems. FERMAT's mathematical work on number theory seems to have taken place during his very rare leisure time in his easy chair, from which he avoided to get up to fetch paper. Instead, he scribbled his ideas into his copy of DIOPHANTUS' *Arithmetic* in the commented bilingual Greek and Latin edition [DIOPHANTUS, 1621] of Claude Gaspard Bachet de Méziriac (1581–1638). It is not surprising that these notes — intended for the most skilled and ingenious problem-solver FERMAT himself to reconstruct his findings — are very short and hard to understand. In his letters to contemporary mathematicians, however, he used to be just as short or even shorter. The reason seems to be that FERMAT wanted his correspondents to do number theory on their own and to find out how much fun it is, cf. [MAHONEY, 1994]. Reporting piecemeal on his results and his methods, but hiding his theorems in their most general form and his proofs, he became a most famous but lonely mathematician.

The Method of *Descente Infinie* is the standard induction method of the working mathematician from the ancient Greeks until today. It got lost in the Middle Ages and was reinvented and named by FERMAT, cf. § 2.

FERMAT's marginal notes in his copy of DIOPHANTUS' *Arithmetic* were published in 1670 only a few years after his death, and in this paper we will have a look at a text passage of Observation XLV of these *Observations on* DIOPHANTUS; cf. [DIOPHANTUS, 1670, Vol. VI, p. 338f.], [FERMAT, 1891ff., Vol. I, p. 340f.]. This passage contains the only proof of FERMAT by the *Method of Descente Infinie* explicitly known today. Already by this fact, Observation XLV is a most important and precious piece of mathematics. It becomes even more important by the fact that it paradigmatically exemplifies the Method of *Descente Infinie* and exhibits this method's conceptual aspects and technical problems in a multitude which is truly surprising for such a short text. All in all, FERMAT's Observation XLV is the primary example for the Method of *Descente Infinie*, historically, conceptually, and pedagogically.

As FERMAT's original proof is hard to understand, we first have to grasp the mathematical ideas implicitly expressed in this proof. Note that this cognitive process is similar to the interpretation of a music passage from its notes in the following sense: If we perceive a gestalt of the passage, this gestalt will be meaningful, but not necessarily the original one of the author. After projecting our image onto the original passage, we can then evaluate its adequacy. When we look at a text of the 17th century today, we are very likely to interpret something into it, however, which FERMAT's contemporaries would not have done. Nevertheless, I may hope that this paper is not infected by more modern number theory simply for the following reason: I did not do number theory seriously the last twenty years. And I did not use any further material on number theory beside EUCLID's *Elements*, but did everything on my own without getting out of my easy chair. It took me a couple of days, but it was an incredible lot of fun. This indicates that FERMAT was right and his contemporaries should not have neglected his challenges; cf. [MAHONEY, 1994].

My mixed motivations for writing this paper were actually the following:

1. There was no concise presentation of the subjects including all important facts and being easily accessible to laymen in the history of mathematics.

2. Regarding FERMAT's proof, there was no easily comprehensible self-contained presentation suited for a student in computer science with a minor knowledge in number theory. This paper should enable him to carry out a case study with our inductive theorem proving software system QUODLIBET; cf. [AVENHAUS &AL., 2003], [SCHMIDT-SAMOA, 2006a; 2006b; 2006c], [WIRTH, 2004; 2005; 2010].

3. I wanted to have fun and to construct a naïve interpretation of FERMAT's proof that has a good chance to be more in the style of the 17th century than interpretations of modern experts in number theory.

4. Moreover, with my expertise in logic and automated theorem proving, I had to clarify some methodological aspects of *Descente Infinie* and to make some minor contributions to the interpretation of FERMAT's proof.

2 *Descente Infinie*

2.1 Working Mathematician's Point of View

In everyday mathematical practice of an advanced theoretical journal the frequent inductive arguments are hardly ever carried out explicitly. Instead, the proof just reads something like "by structural induction on n, q.e.d." or "by induction on (x, y) over $<$, q.e.d.", expecting that the mathematically educated reader could easily expand the proof if in doubt. In contrast, very difficult inductive arguments, sometimes covering several pages, such as the proofs of HILBERT's *1st ε-theorem*, GENTZEN's *Hauptsatz*, or confluence theorems such as the ones in [GRAMLICH & WIRTH, 1996] and [WIRTH, 2009] still require considerable ingenuity and *will* be carried out! The experienced mathematician engineers his proof roughly according to the following pattern:

> He starts with the conjecture and simplifies it by case analysis. When he realizes that the current goal becomes similar to an instance of the conjecture, he applies the instantiated conjecture just like a lemma, but keeps in mind that he has actually applied an induction hypothesis. Finally, he searches for some well-founded ordering in which all the instances of the conjecture he has applied as induction hypotheses are smaller than the original conjecture.

The hard tasks of proof by mathematical induction are

(Hypotheses Task)
: to find the numerous induction hypotheses (as, e.g., in the proof of GENTZEN's Hauptsatz on Cut-elimination in [GENTZEN, 1935]) and

(Induction-Ordering Task)
: to construct an *induction ordering* for the proof, i.e. a well-founded ordering that satisfies the ordering constraints of all these induction hypotheses in parallel. (For instance, this was the hard part in the elimination of the ε-formulas in the proof of the 1st ε-theorem in [HILBERT & BERNAYS, 1968/70, Vol. II], and in the proof of the consistency of arithmetic by the ε-substitution method in [ACKERMANN, 1940]).

The soundness of the above method for engineering hard induction proofs is easily seen when the argument is structured as a proof by contradiction, assuming a counterexample. For FERMAT's historic reinvention of the method, it is thus just natural that he developed the method itself in terms of assumed counterexamples. He called it "*descente infinie ou indéfinie*". Here is this *Method of Descente Infinie* in modern language, very roughly speaking: A proposition Γ can be proved by *descente infinie* as follows:

> *Show that for each assumed counterexample of Γ there is a smaller counterexample of Γ w.r.t. a well-founded ordering $<$, which does not depend on the counterexamples.*

2.2 Logical Point of View

At FERMAT's time, natural language was still the predominant tool for expressing terms and equations in mathematical writing, and it was too early for a formal axiomatization. Moreover, note that an axiomatization captures only validity, but in general does neither induce a method of proof search nor provide the data structures required to admit both a formal treatment and a human-oriented proof search. The formalizable logic part, however, of *descente infinie* can be expressed in what is called the (second-order) *Theorem of* NOETHER*ian Induction* (N), after EMMY NOETHER (1882–1935). This is not to be confused with the *Axiom of Structural Induction*, which is generically given for any inductively defined data structure, such as the *Axiom* (S) *of Structural Induction for the natural numbers inductively defined by the constructors zero* $\mathsf{0}$ *and successor* s. Moreover, we need the definition $(\mathsf{Wellf}(<))$ of well-foundedness of a relation $<$.

$$(\mathsf{Wellf}(<)) \qquad \forall Q.\ \Big(\ \exists x.\ Q(x) \quad\Rightarrow\quad \exists m.\ \big(\ Q(m) \wedge \neg\exists w{<}m.\ Q(w)\ \big)\ \Big)$$

$$(\mathsf{N}) \qquad \forall P.\ \left(\ \forall x.\ P(x) \quad\Leftarrow\quad \exists{<}.\ \left(\begin{array}{l} \quad \forall v.\ \big(\ P(v) \quad\Leftarrow\quad \forall u{<}v.\ P(u)\ \big) \\ \wedge\ \ \mathsf{Wellf}(<) \end{array}\right)\ \right)$$

$$(\mathsf{S}) \qquad \forall P.\ \Big(\ \forall x.\ P(x) \quad\Leftarrow\quad P(\mathsf{0})\ \wedge\ \forall y.\ \big(\ P(\mathsf{s}(y)) \Leftarrow P(y)\ \big)\ \Big)$$

$$(\mathsf{nat1}) \qquad \forall x.\ \big(\ x = \mathsf{0}\ \vee\ \exists y.\ x = \mathsf{s}(y)\ \big)$$

$$(\mathsf{nat2}) \qquad \forall x.\ \ \mathsf{s}(x) \neq \mathsf{0}$$

$$(\mathsf{nat3}) \qquad \forall x, y.\ \big(\ \mathsf{s}(x) = \mathsf{s}(y)\ \Rightarrow\ x = y\ \big)$$

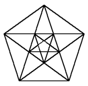
Let $\mathsf{Wellf}(\mathsf{s})$ denote $\mathsf{Wellf}(\lambda x, y.\, (\mathsf{s}(x) = y))$, which implies the well-foundedness of the ordering of the natural numbers. The natural numbers can be specified up to isomorphism either by (S), $(\mathsf{nat2})$, and $(\mathsf{nat3})$, or else by $\mathsf{Wellf}(\mathsf{s})$ and $(\mathsf{nat1})$. The first alternative follows RICHARD DEDEKIND (1831–1916) and is named after GUISEPPE PEANO (1858–1932). The second follows MARIO PIERI (1860–1913). As the instances for P and $<$ in (N) are often still easy to find when the instances for P in (S) are not, the second alternative together with (N) is to be preferred in theorem proving for its usefulness and elegance. Cf. [WIRTH, 2004] for more on this.

The proposition Γ of § 2.1 is represented in (N) by $\forall x.\ P(x)$. Roughly speaking, a *counterexample* for Γ is an instance a for which $\neg P(a)$ holds, but we should be more careful here because this is actually a semantical notion and not a syntactical one; cf. [WIRTH, 2004], § 2.3.2. To treat counterexamples properly, we need a logic that actually models the mathematical process of proof search by *descente infinie* itself and directly supports it with the data structures required for a formal treatment, and thus requires a semantical treatment of free variables. The only such logic can be found in [WIRTH, 2004].

2.3 Historical Point of View

2.3.1 Early Greek History

Although we do not have any original Greek mathematical documents from the 5th century B.C. and only fragments from the following millennium, the first known occurrence of *descente infinie* in history seems to be the proof of the irrationality of the golden number $\frac{1}{2}(1+\sqrt{5})$ by the Pythagorean mathematician Hippasus of Metapontum (Italy) in the middle of the 5th century B.C., cf. [Fritz, 1945]. This proof is carried out geometrically in a pentagram, where the golden number gives the proportion of the length of a line to the length of the side of the enclosing pentagon:



Under the assumption that this proportion is given by $m : n$ with natural numbers m and n, it can be shown that the proportion of the length of a line of a new pentagram drawn inside the inscribed pentagon to the length of the side of this pentagon is $m{-}n : 2n{-}m$, with $0 \prec m{-}n \prec m$, and so forth since the new inscribed pentagram is similar to the original one. A myth says that the gods drowned Hippasus in the sea, as a punishment for destroying the Pythagoreans' belief that everything is given by positive rational numbers; and this even with the pentagram, which was the Pythagoreans' sign of recognition amongst themselves. The resulting confusion seems to have been one of the reasons for the ancient Greek culture to shift interest in mathematics from theorems to proofs.

2.3.2 Euclid's Elements

Proof by Generalizable Example In the famous collection "*Elements*" of Euclid of Alexandria (ca. 300 B.C.), we find several occurrences of *descente infinie*. In the Elements, the verbalization of a proof by *descente infinie* has the form of a *generalizable example* in the sense that a special concrete counterexample is considered — instead of an arbitrary one — but the existence of a smaller counterexample is actually shown independently of this special choice. Similarly, the induction step of a structural induction may also be presented in the form of a generalizable example. Such proofs via a generalizable example are called *quasi-general* in [Freudenthal, 1953]. We would not accept a quasi-general proof as a proper proof from our students today because the *explicit* knowledge and the *explicit* verbalization of methods of mathematical induction have become standard during the last centuries. And we may ask why the Elements proceed by generalizable examples. For this question it is interesting to see that already in a text of Plato (427–347 B.C.) (Athens) we find a proof by structural induction with a proper verbalization of a general induction step without resorting to generalizable examples, cf. [Acerbi, 2000]. As the theorem of this proof is mathematically trivial ("$n{+}1$ terms in a list have n contacts"), the intention of this proof seems to be the explicit demonstration of the activity of structural induction itself, though no instance of the Axiom of Structural Induction (S) is explicitly mentioned. Moreover, the verbalization of a variable number and even the comprehension of a non-concrete example and a general induction proof seems to have been a challenge for an ancient Greek student; cf. [Unguru, 1991, p. 279ff.]. Thus, the presentation of induction proofs via generalizable examples in the Elements may well have had pedagogical reasons.

Let us have a look at two proofs from the Elements.

Proof by *Descente Infinie* In [EUCLID, ca. 300 B.C., Vol. VII, Proposition 31], we find the following proof by *descente infinie*:

> Proposition VII.31: Any composite number is measured by some prime number.
>
> Proof of Proposition VII.31: Let A be a composite number. I say that A is measured by some prime number. Since A is composite, therefore some number B measures it. Now, if B is prime, then that which was proposed is done. But if it is composite, some number measures it. Let a number C measure it. Then, since C measures B, and B measures A, therefore C also measures A. And, if C is prime, then that which was proposed is done. But if it is composite, some number measures it. Thus, if the investigation is continued in this way, then some prime number will be found which measures the number before it, which also measures A. If it is not found, then an infinite sequence of numbers measures the number A, each of which is less than the other, which is impossible in numbers. Therefore some prime number will be found which measures the one before it, which also measures A. Q.e.d. (Proposition VII.31)

Proof by Structural Induction Taking into account that the ancient Greeks were not familiar with an actually infinite set of natural numbers, in accordance with [FREUDENTHAL, 1953] I consider the proof of Proposition IX.8 of the Elements to be obviously a proof by structural induction, whereas [UNGURU, 1991] rejects this opinion and [ACERBI, 2000] even claims that there are no proofs by structural induction in EUCLID's Elements at all. Thus, let us have a look at this proof to give the reader a chance to judge on his own.

> Proposition IX.8: If as many numbers as we please beginning from a unit are in continued proportion, then the third from the unit is square as are also all those which successively leave out one, and the fourth is cubic as are also all those which leave out two, and the seventh is both cubic and square as are also all those which leave out five.
>
> Proof of Proposition IX.8: Let there be as many numbers as we please, A, B, C, D, E, and F, beginning from a unit and in continued proportion. I say that B, the third from the unit, is square as are all those which leave out one; C, the fourth, is cubic as are all those which leave out two; and F, the seventh, is both cubic and square as are all those which leave out five. Since the unit is to A as A is to B, therefore the unit measures the number A the same number of times that A measures B. But the unit measures the number A according to the units in it, therefore A also measures B according to the units in A. Therefore A multiplied by itself makes B, therefore B is square. And, since B, C, and D are in continued proportion, and B is square, therefore D is also square. For the same reason F is also square. Similarly we can prove that all those which leave out one are square. I say next that C, the fourth from the unit, is cubic as are also all those which leave out two. Since the unit is to A as B is to C,

therefore the unit measures the number A the same number of times that B measures C. But the unit measures the number A according to the units in A, therefore B also measures C according to the units in A. Therefore A multiplied by B makes C. Since then A multiplied by itself makes B, and multiplied by B makes C, therefore C is cubic. And, since C, D, E, and F are in continued proportion, and C is cubic, therefore F is also cubic. But it was also proved square, therefore the seventh from the unit is both cubic and square. Similarly we can prove that all the numbers which leave out five are also both cubic and square. Q.e.d. (Proposition IX.8)

2.3.3 Recovering from the Dark Middle Ages

After EUCLID, in the following eighteen centuries until FERMAT, I do not know of *descente infinie* (except that EUCLID's Elements where copied again and again), but of *structural induction* only. Structural induction was known to the Muslim mathematicians around the year 1000 and occurs in a Hebrew book of LEVI BEN GERSON (1288–1344) (Orange and Avignon) in 1321, cf. [KATZ, 1998]. BLAISE PASCAL (1623–1662) (Paris) knew structural induction from "*Arithmeticorum Libri Duo*" of FRANCISCO MAUROLICO (MAUROLYCUS) (1494–1575) (Messina) written in 1557 and published posthumously in 1575 in Venice, cf. [BUSSEY, 1917]. PASCAL used structural induction for the proofs of his "*Traité du Triangle Arithmétique*" written in 1654 and published posthumously in 1665. While these induction proofs are still presented as "generalizable examples", in the demonstration of "Conséquence XII" we find — for the first time in known history — a correct verbalization of the related instance of the Axiom of Structural Induction (S); cf. [PASCAL, 1954, p. 103], [ACERBI, 2000, p. 57].

2.3.4 Revival

In the 1650s, BLAISE PASCAL (1623–1662) (Paris) exchanged letters on probability theory and *descente infinie* with PIERRE FERMAT (1607?–1665) (Toulouse), who was the first to describe the *Method of Descente Infinie* explicitly. FRANÇOIS VIÈTE (1540–1603) (Paris) had already given a new meaning to the word *analysis* by extending the analysis of concrete mathematical problems to the algebraic analysis of the process of their solution. FERMAT improved on VIÈTE:

Instead of a set of rules that sometimes did find a single solution to the "double equations" of DIOPHANTUS OF ALEXANDRIA (3rd century?) and sometimes did not, he invented a *method* to enumerate an infinite set of solutions, which is described in the "*Inventum Novum*" by the number theoretician JACQUES DE BILLY (1602–1679); for a French translation cf. [FERMAT, 1891ff., Vol. III, pp. 325–398]; for a discussion see [MAHONEY, 1994, § VI.III.B].

Much more than that, FERMAT was the first who — instead of just proving a theorem — analyzed the *method* of proof search. This becomes obvious from the description of the *Method of Descente Infinie* in a letter for CHRISTIAAN HUYGENS (1629–1695) (Den Haag) entitled "*Relation des nouvelles découvertes en la science des nombres*"; cf. [FERMAT, 1891ff., Vol. II, pp. 431–436]. This letter, in which FERMAT also lists some theorems and claims to have proved them by *descente infinie*, was sent to PIERRE DE CARCAVI in August 1659. Moreover, in his letter for HUYGENS and in [DIOPHANTUS, 1670], FERMAT was also the first to provide a correct verbalization of proofs by *descente infinie* and to overcome their presentation as "generalizable examples". *Methodological* considerations seem to have been FERMAT's primary concern.

2.4 Linguistic and Refined Logic-Historical Points of View

The level of abstraction of our previous discussion of *descente infinie* is well-suited for the description of the structure of mathematical proof search in two-valued logics, where the difference between a proof by contradiction and a positive proof of a given theorem is only a linguistic one and completely disappears when we formalize these proofs in a state-of-the-art modern logic calculus, such as the one of [WIRTH, 2004]. An investigation into the history of mathematics, however, also has to consider the linguistic representation and the exact logical form of the presentation.

2.4.1 An Inappropriate Refinement by UNGURU and ACERBI

Such a linguistic and logic-historical refinement can easily go over the top. For instance, from the above-mentioned fact that we find — for the first time in known history — a correct verbalization of the related instance of the Axiom of Structural Induction (S) in PASCAL's publications, it is not sound to conclude that PASCAL was the first to do structural induction (as claimed in [UNGURU, 1991]) or the first to do it *consciously* (as claimed in [ACERBI, 2000]). These claims are just as abstruse to most working mathematicians as the claim that FERMAT was the first to do *descente infinie*. And [FOWLER, 1994] is perfectly right to object to this view on the basis of a deeper understanding of the mathematical activity, although we have to be careful not to interpret modern thinking into the historical texts.

Mathematics is mostly a top-down procedure and when we do not formalize and explicate every bit of it, we may have good reasons and be well aware of what we do. Human mathematical activity includes subconscious elements, but this does not mean that their application is unconscious. Just as music is not captured by notes and not necessarily invented as notes, mathematical activity cannot be captured by its formalization and is not necessarily well-expressed in natural or formal language. (Actually, formalization is a dangerous step for a mathematician because afterward there is hardly any way back to his original intuition.)

2.4.2 Our Suggestion for an Unproblematic Classification Scheme

All in all, for our subject here there is actually no need to discuss the working mathematician's consciousness: It suffices to speak of

1. quasi-general proofs (i.e. proofs by generalizable examples),
2. general proofs (i.e. proofs we would accept from our students in an examination today),
3. proofs with an explicit statement of the related instance of an induction axiom or theorem, and
4. proofs with an explicit statement of an induction axiom or theorem itself.

2.4.3 An Appropriate Refinement by Paolo Bussotti

There is evidence that such a linguistic and logic-historical refinement is necessary to understand the fine structure of historical reasoning in mathematics. For instance, in Euclid's Elements, Proposition VIII.7 is just the contrapositive of Proposition VIII.6, and this is just one of several cases that we find a proposition with a proof in the Elements, where today we just see a corollary. Moreover, even Fermat reported in his letter for Huygens (cf. § 2.3.4) that he had had problems to apply the Method of *Descente Infinie* to positive mathematical statements.

> "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." [Fermat, 1891ff., Vol. II, p. 432]

> "For a long time I was not able to apply my method to affirmative conjectures because the ways and means of achieving this are much more complicated than the ones I am used to for negative conjectures. Such that, when I had to show that any prime number which exceeds 1 by a multiple of 4 is the sum of two squares, I found myself pretty much in trouble. But finally oft-repeated meditation gave me the insight I lacked, and affirmative questions yielded to my method with the aid of some new principles which had to be added to it."

Because of the work of Frege and Peano, these logical differences may be considered trivial today. Nevertheless, they were not trivial before, and to understand the history of mathematics and the fine structure in which mathematicians reasoned, the distinction between affirmative and negative theorems and between direct and apagogic methods of demonstration is important.

Therefore, it is well justified when in [Bussotti, 2006], following the above statement of Fermat, the Method of *Descente Infinie* is subdivided into *indefinite descent* (ID) and *reduction-descent* (RD):

$$\text{(ID)}\quad \forall P.\ \left(\ \forall x.\ P(x) \quad \Leftarrow \quad \exists{<}.\ \left(\begin{array}{ll} & \forall v.\ \big(\ \neg P(v) \ \Rightarrow\ \exists u{<}v.\ \neg P(u)\ \big) \\ \wedge & \mathsf{Wellf}(<) \end{array}\right)\right)$$

$$\text{(RD)}\quad \forall P.\ \left(\ \forall x.\ P(x) \quad \Leftarrow \quad \exists{<}.\ \exists S.\ \left(\begin{array}{ll} & \forall u.\ \big(\ S(u) \ \Rightarrow\ P(u)\ \big) \\ \wedge & \forall v.\ \left(\begin{array}{l} \quad \neg S(v) \wedge \neg P(v) \\ \Rightarrow\ \exists u{<}v.\ \neg P(u) \end{array}\right) \\ \wedge & \mathsf{Wellf}(<) \end{array}\right)\right)$$

Actually, "$\mathsf{Wellf}(<)$" does not occur in [Bussotti, 2006] because for Fermat the Method of *Descente infinie* was actually restricted to the well-founded ordering of the natural numbers.

Although (N), (ID), and (RD) are logically equivalent in two-valued logics, according to [Bussotti, 2006] *descente infinie* does not subsume proofs by Noetherian or structural induction. This is in opposition to our more coarse-grained discussion above. With this fine-grained distinction, on Page 2 of [Bussotti, 2006], we find the surprising claim that there is only a single proof by indefinite descent in the whole Elements, namely the before-cited Proof of Proposition VII.31. Indeed, at least all those proofs in the Elements beside VII.31 which I reexamined and which proceed by mathematical induction, actually proceed by reduction-descent or structural induction, but not by indefinite descent: The correctness proofs of the Euclidian Algorithm (Proposition VII.2 and Proposition X.3) are reduction-descents with a horrible linguistic surface structure. Similarly, the proofs of Propositions IX.12 and IX.13 are reduction-descents with superfluous sentences confusing the proof idea.

Note that, as already repeatedly expressed above, a logical formalization cannot capture a mathematical method. Moreover, as also already expressed above, logical equivalence of formulas does not imply the equivalence of the formalized methods. For an interesting discussion of this difficult subject see [Bussotti, 2006, Chapter 7].

Nevertheless, (N), (ID), and (RD) sketch methods of proof search equivalent for the working mathematician of today. Indeed: (ID) — roughly speaking — is the contrapositive of (N), which means that in two-valued logics the methods only differ in verbalization. Moreover, a proof by (ID) is a proof by (RD) when we set S to the empty predicate. Finally, a proof by (RD) can be transformed into a proof by (ID) as follows: Suppose we have proofs for the statements in the conjunction of the premise of (RD). The proofs of $\forall u.\ \big(\ S(u) \ \Rightarrow\ P(u)\ \big)$ and $\forall v.\ \left(\begin{array}{l} \quad \neg S(v) \wedge \neg P(v) \\ \Rightarrow\ \exists u{<}v.\ \neg P(u) \end{array}\right)$ give a proof of $\forall v.\ \left(\begin{array}{l} \quad \neg S(v) \wedge \neg P(v) \\ \Rightarrow\ \exists u{<}v.\ (\neg S(v) \wedge \neg P(u)) \end{array}\right)$. Instantiating the P in (ID) via $\{P \mapsto \lambda z.\ (S(z) \vee P(z))\}$, the latter proof can be schematically transformed into a proof of $\forall x.\ (S(x) \vee P(x))$ by (ID). And then from the proof of $\forall u.\ \big(\ S(u) \ \Rightarrow\ P(u)\ \big)$ again, we get a proof of $\forall x.\ P(x)$, as intended. Thus, in any case, the resulting proof does not significantly differ in the mathematical structure from the original one.

Note that this is contrary to the case of NOETHERian vs. structural induction, where the only transformation I see from the former to the latter (the other direction is trivial, cf. [WIRTH, 2004], § 1.1.3) is to show that the *axiom* (S) implies $\mathsf{Wellf}(\mathsf{s})$, and then leave the application of (N) unchanged. This transformation, however, is not complete because it does not remove the application of (N), which is a *theorem* anyway.

All in all, this shows that — while structural and NOETHERian induction vastly differ in practical applicability — for a working mathematician today it is not important for his proof search to be aware of the differences between NOETHERian induction (N), indefinite descent (ID), and reduction-descent (RD). And thus, we will continue to subsume all the three under the Method of *Descente Infinie*.

2.4.4 A Further Refinement

For the soundness of WALSH's interpretation of FERMAT's proof in our § 4.7, we have to invent the following further refinement to the logic-historical discussion of *descente infinie*.

The predicate P in the theorem (ID) of § 2.4.3 may actually vary in the indefinite descent, in the sense that — for a function P from natural numbers to predicates — we have the following theorem:

$$(\mathsf{ID}') \qquad \forall P. \left(\begin{array}{l} \forall x.\ P_0(x) \\ \Leftarrow\ \exists{<}.\ \left(\begin{array}{l} \forall i \in \mathbf{N}.\ \forall v.\ \left(\ \neg P_i(v) \ \Rightarrow\ \exists u{<}v.\ \neg P_{i+1}(u)\ \right) \\ \wedge\ \mathsf{Wellf}(<) \end{array} \right) \end{array} \right)$$

For a sufficiently expressible logic, this again makes no difference: Indeed, to prove theorem (ID′) and even to use theorem (ID) instead of it without a significant change of the structure of the proof, it suffices to instantiate theorem (ID) according to

$$\{\ P \ \mapsto\ \lambda x.\ \forall i \in \mathbf{N}.\ P_i(x)\ \}.$$

Typically — as in the example of § 4.7 — the set $\{\ P_i \mid i \in N\ \}$ is finite. In this case, the universal quantification in $\forall i \in \mathbf{N}.\ P_i(x)$ can be replaced with a finite conjunction.

3 Prerequisites from Number Theory

In this § 3, we list the propositions and the proofs that I found in my easy chair without any help beside EUCLID's Elements.

If the reader is experienced in number theory or wants to have the pleasure of doing some exercises in elementary number theory on his own, he should skip this § 3 and continue directly with § 4. Moreover, we generally recommend to skip this § 3 on a first reading.

We follow the Elements quite closely, but occasionally deviated from them if an alternative course is more efficient. As we address modern readers, the language of our presentation, however, is a modern one, most atypical for the 17^{th} century. Furthermore, in this § 3, we follow the historical proof ideas only very roughly and are not seriously concerned with historical authenticity. Nevertheless, as expressed already in § 1, we hope that our reconstruction of elementary number theory in this § 3 does not essentially differ from what FERMAT's contemporary mathematicians could have achieved if FERMAT had been able to interest them in his new number theory. This aspect becomes crucial, however, only for FERMAT's proof in § 4.

The proofs missing here can be found § A of the appendix.

3.1 From the Elements, Vol. VII

Let all variables range over the set of natural numbers $\mathbf{N}$ (including 0), unless indicated otherwise. Let '$\prec$' denote the (irreflexive) ordering and '$\preceq$' the reflexive ordering on $\mathbf{N}$. Let $\mathbf{N}_+ := \{\, n \in \mathbf{N} \mid 0 \neq n \,\}$.

Definition 3.1 (Divides)
x divides y (written: $x \mid y$) if there is a k such that $kx = y$.

Corollary 3.2 *The binary relation $\mid$ is a reflexive ordering on the natural numbers with minimum 1 and maximum 0. Moreover, $(x \mid y) \wedge (y \neq 0)$ implies $x \preceq y$.*

Corollary 3.3 *Let us assume $x \mid y_0$. Then $x \mid y_1$ iff $x \mid y_0 + y_1$.*

Corollary 3.4 $(x = 0) \vee (y \mid z)$ *iff* $xy \mid xz$.

Definition 3.5 (Coprime)
$l_1, \ldots, l_n$ are *coprime* if $\forall x.\ \big(\ \forall i \in \{1, \ldots, n\}.\ (x \mid l_i) \quad \Rightarrow \quad x = 1\ \big)$.

Corollary 3.6 *If p, q are coprime and $p \succeq q$, then $p \succ q$ or $p = q = 1$.*

Lemma 3.7 (EUCLID**'s Elements, Propositions VII.20 and VII.21, generalized)**
Let $x_0y_1 = y_0x_1$ *with* $x_0, x_1, y_0, y_1 \in \mathbf{N}_+$.
Then the following holds:

(i) *For every* z_0, z_1, *we have:* $y_0z_1 = z_0y_1$ *iff* $x_0z_1 = z_0x_1$.

Moreover, the following two cases are equivalent:

(ii) y_0, y_1 *are coprime.*

(iii) y_0 *is* $\preceq$*-minimal such that there is a* $y'_1 \in \mathbf{N}_+$ *with* $x_0y'_1 = y_0x_1$.

Furthermore, in each of the two cases (ii) and (iii), the following holds:

(iv) *There is a* $k \in \mathbf{N}_+$ *with* $ky_i = x_i$ *for* $i \in \{0, 1\}$.

Lemma 3.8 (EUCLID**'s Elements, Proposition VII.23)**
If y, z *are coprime and* $x \mid y$, *then* x, z *are coprime, too.*

Lemma 3.9 (EUCLID**'s Elements, Proposition VII.24, generalized)**
If x_i, z *are coprime for* $i \in \{1, \ldots, m\}$, *then* $\prod_{i=1}^m x_i$, z *are coprime, too.*

Lemma 3.10 (EUCLID**'s Elements, Proposition VII.26, generalized)**
If x_i, y_j *are coprime for* $i \in \{1, \ldots, m\}$ *and* $j \in \{1, \ldots, n\}$, *then* $\prod_{i=1}^m x_i$, $\prod_{i=1}^n y_i$ *are coprime, too.*

Corollary 3.11 (EUCLID**'s Elements, Proposition VII.27)**
If y, z *are coprime, then* y^n, z^m *are coprime, too.*

Definition 3.12 (Prime)
A number p is *prime* if $p \neq 1$ and $(x \mid p) \Rightarrow x \in \{1, p\}$ for all x.

Corollary 3.13 *If* p *is prime, then* $2 \preceq p$.

Lemma 3.14 (EUCLID**'s Elements, Proposition VII.29)**
If p *is prime and* $p \nmid x$, *then* p, x *are coprime.*

The following lemma is popular today under the label of "EUCLID*'s Lemma*":

Lemma 3.15 (EUCLID**'s Elements, Proposition VII.30)**
If p *is prime and* $p \mid x_1x_2$, *then* $p \mid x_1$ *or* $p \mid x_2$.

The following lemma will be applied exclusively in the proofs of Lemmas A.2, 3.22, and 3.24.

Lemma 3.16 (EUCLID**'s Elements, Proposition VII.31)**
For any $x \neq 1$, *there is some prime* p *such that* $p \mid x$.

3.2 From the Elements, Vol. VIII

Definition 3.17 (Continued Proportion)
$x_0, \ldots, x_{n+1}$ are in *continued proportion* if $\forall i \in \{0, \ldots, n{+}1\}.\ (x_i \in \mathbf{N}_+)$ and $\forall i \in \{1, \ldots, n\}.\ (x_{i-1}x_{i+1} = x_i^2)$.

The following lemma will be applied exclusively in the proof of Lemma 3.19.

Lemma 3.18 (EUCLID**'s Elements, Proposition VIII.1, generalized)**
If $x_0, \ldots, x_{n+1}$ and $y_0, \ldots, y_{n+1}$ are in continued proportion, if $x_0y_1 = y_0x_1$, and if x_0, x_{n+1} are coprime, then there is some $k \in \mathbf{N}_+$ with $kx_i = y_i$ for $i \in \{0, \ldots, n{+}1\}$.

The following lemma will be applied exclusively in the proof of Lemma 3.21.

Lemma 3.19 (EUCLID**'s Elements, Proposition VIII.2, generalized)**
If $x_0, \ldots, x_{n+1}$ are in continued proportion, then there are $k \in \mathbf{N}_+$ and coprime $y, z \in \mathbf{N}_+$ such that $y^{n+1}z^0, \ldots, y^{n+1-i}z^i, \ldots, y^0z^{n+1}$ are in continued proportion, too, $x_0(y^nz^1) = (y^{n+1}z^0)x_1$, $ky^{n+1-i}z^i = x_i$ for $i \in \{0, \ldots, n{+}1\}$, and, moreover, in case that x_0, x_{n+1} are coprime, $k = 1$.

Lemma 3.20 (EUCLID**'s Elements, Proposition VIII.14)**
$x \mid y$ iff $x^2 \mid y^2$.

3.3 Further Simple Lemmas for FERMAT's Proof

Lemma 3.21 *If a, b are coprime and $ab = x^2$, then there are coprime y, z with $a = y^2$, $b = z^2$, and $x = yz$.*

Lemma 3.22 *$l_1, \ldots, l_n$ are not coprime iff $\exists p$ prime. $\forall i \in \{1, \ldots, n\}.\ (p \mid l_i)$.*

Lemma 3.23 *Let a, b be coprime. Let p be a prime number.*

(1) Either pa, b are coprime or a, pb are coprime.

(2) If $pab = v^2$ for some v, then there are $m \in \mathbf{N}$ and $k \in \mathbf{N}_+$ such that pm, k are coprime and $\{pm^2, k^2\} = \{a, b\}$.

Lemma 3.24 *Suppose $a \succeq b$, $x \mid a{-}b$, and $x \mid a{+}b$. Then we have:*

(1) $x \mid 2a$ and $x \mid 2b$.

(2) If a, b are coprime, then $x \preceq 2$.

Lemma 3.25
If p, q are coprime with $p \succeq q$, then pq, $p^2{-}q^2$ are coprime, and pq, $p^2{+}q^2$ are coprime.

3.4 Roots of $x_0^2 + x_1^2 = x_2^2$

Lemma 3.26 *$x_0^2 + x_1^2 = x_2^2$ iff for some $i \in \{0,1\}$, there are a, b such that $a \succeq b$, $x_i = 2\sqrt{ab}$, $x_{1-i} = a - b$, and $x_2 = a + b$.*

Proof of Lemma 3.26 The "if"-direction is trivial. Let us assume $x_0^2 + x_1^2 = x_2^2$ to show the "only if"-direction. Suppose $x_i = 2y_i + 1$ for $i \in \{0,1\}$. Then $x_0^2 + x_1^2 = (2y_0+1)^2 + (2y_1+1)^2 = 4y_0^2 + 4y_0 + 1 + 4y_1^2 + 4y_1 + 1 = 2(2(y_0^2 + y_0 + y_1^2 + y_1) + 1)$. As the square of an even number divides by 4 and the square of an odd number is odd, this would mean that $x_0^2 + x_1^2$ is not a square. Thus, there is some $i \in \{0,1\}$ and some c with $x_i = 2c$. But then $x_2 \pm x_{1-i}$ must be even too, because $(x_2 + x_{1-i})(x_2 - x_{1-i}) = x_2^2 - x_{1-i}^2 = x_i^2 = 4c^2$ means that one of them must be even by Lemma 3.15, and then the other is even, too. Thus, there are a, b such that $x_2 + x_{1-i} = 2a$ and $x_2 - x_{1-i} = 2b$. This implies $2x_2 = 2a + 2b$, $2x_{1-i} = 2a - 2b$, and $2a2b = 4c^2$, and then $x_2 = a + b$, $x_{1-i} = a - b$, and $ab = c^2$. **Q.e.d. (Lemma 3.26)**

Note that in Lemma 3.26 we cannot require any of a and b to be a square in general. For instance, for $x_0 = 12 \wedge x_1 = 9 \wedge x_2 = 15$, we have $x_0^2 + x_1^2 = x_2^2$, but necessarily get $\sqrt{ab} = 6$ (as x_1 is odd), and then, if any of a or b is a square, we have $(a = 9 \wedge b = 4) \vee (a = 36 \wedge b = 1)$, i.e. $(x_2 = 13 \wedge x_1 = 5) \vee (x_2 = 37 \wedge x_1 = 35)$, which are PYTHAGOREAN triangles not similar to the original $x_2 = 15 \wedge x_1 = 9$. But $a = 12 \wedge b = 3$ provide the generators for $x_0 = 12 \wedge x_1 = 9 \wedge x_2 = 15$, whose existence is guaranteed by Lemma 3.26.

If x_0, x_1, x_2 are coprime, however, then a, b must be coprime (as $(y \mid a) \wedge (y \mid b) \Rightarrow \forall i \in \{0,1,2\}.\ (y \mid x_i)$) and one even and one odd (as otherwise $\forall i \in \{0,1,2\}.\ (2 \mid x_i)$). And then they must be squares because of $x_i = 2\sqrt{ab}$ and Lemma 3.21; say $a = p^2$ and $b = q^2$. Then p, q are coprime and one even and one odd, too. All in all, we get as a corollary of Lemma 3.26:

Corollary 3.27 *If $x_0^2 + x_1^2 = x_2^2$ and x_0, x_1, x_2 are coprime, then, for some $i \in \{0,1\}$, there are coprime p, q such that one of them is odd and one of them is even, $p \succ q$, $x_i = 2pq$, $x_{1-i} = p^2 - q^2$, and $x_2 = p^2 + q^2$.*

Note that in Corollary 3.27 we cannot require $q \in \mathbf{N}_+$ because for the case of $(x_0, x_1, x_2) = (1, 0, 1)$ we have $x_0^2 + x_1^2 = x_2^2$ and x_0, x_1, x_2 are coprime, but $i \in \{0,1\}$, $p \succ q$, $x_i = 2pq$, $x_{1-i} = p^2 - q^2$, and $x_2 = p^2 + q^2$ implies $q = 0$.

Lemma 3.28 ([FRÉNICLE, 1676, Proposition XXXVIII], generalized)
Let $x_0^2 + x_1^2 = x_2^2$ and x_0, x_1, x_2 be coprime. Then exactly one of x_0, x_1 is even, say x_i. If $x_i = v^2$ for some v, then there are $m \in \mathbf{N}$ and $k \in \mathbf{N}_+$ such that $2m, k$ are coprime, $(m = 0) \Leftrightarrow (x_0 = 0)$, and $(2m^2)^2 + (k^2)^2 = x_2$.

Proof of Lemma 3.28 By Corollary 3.27, there are $j \in \{0,1\}$ and coprime p, q such that one of them is odd and one of them is even, $p \succ q$, $x_j = 2pq$, $x_{1-j} = p^2 - q^2$, and $x_2 = p^2 + q^2$. We have assumed x_i to be the even one in $\{x_0, x_1\}$, i.e. $i = j$. Thus, $2pq = v^2$ by assumption. By Lemma 3.23(2), there are $m \in \mathbf{N}$ and $k \in \mathbf{N}_+$ such that $2m, k$ are coprime and $\{2m^2, k^2\} = \{p, q\}$. Moreover the following are logically equivalent: $x_0 = 0$, $q = 0$, $m = 0$. Finally, $(2m^2)^2 + (k^2)^2 = p^2 + q^2 = x_2$. **Q.e.d. (Lemma 3.28)**

3.5 Roots of $x_0^2 + 2x_1^2 = x_2^2$

Lemma 3.29
$x_0^2 + 2x_1^2 = x_2^2$ *iff there are* a, b *such that* $a \succeq b$, $x_0 = a - b$, $x_1 = \sqrt{2ab}$, *and* $x_2 = a + b$.

Proof of Lemma 3.29 The "if"-direction is trivial. Let us assume $x_0^2 + 2x_1^2 = x_2^2$ to show the "only if"-direction. $(x_2 + x_0)(x_2 - x_0) = x_2^2 - x_0^2 = 2x_1^2$ means that one of $x_2 \pm x_0$ must be even by Lemma 3.15, and then the other is even, too. Thus, there are a, b with $x_2 + x_0 = 2a$, and $x_2 - x_0 = 2b$. But then $2x_2 = 2a + 2b$, $2x_0 = 2a - 2b$, and $2a2b = 2x_1^2$, i.e. $x_2 = a + b$, $x_0 = a - b$, and $2ab = x_1^2$. **Q.e.d. (Lemma 3.29)**

If x_0, x_1, x_2 are coprime, however, then a, b must be coprime. By Lemma 3.23(2), then there are $m \in \mathbf{N}$ and $k \in \mathbf{N}_+$ such that $2m, k$ are coprime and $\{2m^2, k^2\} = \{a, b\}$. All in all, we get as a corollary of Lemma 3.29:

Corollary 3.30 *If* $x_0^2 + 2x_1^2 = x_2^2$ *and* x_0, x_1, x_2 *are coprime, then there are* $m \in \mathbf{N}$ *and* $k \in \mathbf{N}_+$ *such that* $2m, k$ *are coprime,* $2m^2 \neq k^2$, $x_0 = |2m^2 - k^2|$, $x_1 = 2mk$, *and* $x_2 = 2m^2 + k^2$.

Note that in Corollary 3.30 we cannot require $m \in \mathbf{N}_+$ because for the case of $(x_0, x_1, x_2) = (1, 0, 1)$ we have $x_0^2 + 2x_1^2 = x_2^2$ and x_0, x_1, x_2 are coprime, but $x_2 = 2m^2 + k^2$ implies $m = 0$.

4 Fermat's Proof

In this § 4, we first state Fermat's theorem of Observation XLV in [Diophantus, 1670] in modern notation (§ 4.1). Then, we present Fermat's original short French announcement of the theorem (and the idea of proving it by *descente infinie*), and translate it into English (§ 4.2).

In § 4.3, we present Fermat's original Latin proof.

As this proof is hard to understand, we first have to grasp the mathematical ideas implicitly expressed in this proof. Therefore, in § 4.4, we continue with a simple, self-contained, modern English proof of the theorem. Afterward, in § 4.5, we present our translation of the Latin proof, annotated with our interpretation, which is more or less standard.

Note that the cognitive process behind this annotation seems to be similar to the interpretation of a music passage from its notes in the following sense: If we perceive a gestalt of the passage, this gestalt will be meaningful, but not necessarily the original one of the author. After projecting our image onto the original passage, we can then evaluate its adequacy. Therefore, we look at interpretations of Fermat's proofs in the literature and discuss similar interpretations in § 4.6, and Walsh's alternative interpretation in § 4.7.

Finally, § 4 closes with Frénicle's more elegant proof of the theorem in § 4.8.

4.1 Fermat's Theorem of Observation XLV in [Diophantus, 1670]

Fermat's theorem simply says that the area of a Pythagorean triangle with positive integer side lengths is not the square of an integer, or in modern formulation:

Theorem 4.1 *If* $x_0, x_1 \in \mathbf{N}_+$ *and* $x_2, x_3 \in \mathbf{N}$ *and* $x_0^2 + x_1^2 = x_2^2$, *then* $x_0 x_1 \neq 2x_3^2$.

Note that we cannot generalize Theorem 4.1 by admitting $0 \in \{x_0, x_1\}$ because we have

$$(x_0, x_1, x_2, x_3) \in \{(0,0,0,0), (0,1,1,0), (1,0,1,0)\} \quad \text{iff} \quad (x_0^2 + x_1^2 = x_2^2) \wedge (x_0 x_1 = 2x_3^2).$$

4.2 French Abstract of the Theorem and its Proof Idea

Fermat summarized his original proof (which we will quote in § 4.3) in his letter for Huygens (which we have already discussed in § 2.3.4):

> "S'il y avoit aucun triangle rectangle en nombres entiers qui eût son aire égale a 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 le second, qui auroit la même propriété, et enfin un quatrième, un cinquième, &c. à l'infini en descendant." [Fermat, 1891ff., Vol. 1, p. 431f.]

"If there were any right-angled triangle in whole numbers that had its area equal to a square, there would be another triangle smaller than that one, which would have the same property. If there were a second, smaller than the first, which had the same property, there would be, by a similar reasoning, a third, smaller than the second, which would have the same property, and finally a fourth, a fifth, &c., descending to infinity."

4.3 FERMAT's Original Latin Proof

FERMAT wrote in Observation XLV on DIOPHANTUS' Problem XX of his *Observations on* DIOPHANTUS; cf. [DIOPHANTUS, 1670, Vol. VI, p. 339] (there is a manipulated facsimile in [WEIL, 1984, p. 78] and a true one in [GOLDSTEIN, 1995, p. 60]) and [FERMAT, 1891ff., Vol. I, p. 340f.]:

Si area trianguli esset quadratus, darentur duo quadratoquadrati quorum differentia esset quadratus; unde sequitur dari duo quadratos quorum et summa et differentia esset quadratus. Datur itaque numerus, compositus ex quadrato et duplo quadrati, aequalis quadrato, ea conditione ut quadrati eum componentes faciant quadratum.

Sed, si numerus quadratus componitur ex quadrato et duplo alterius quadrati, eius latus similiter componitur ex quadrato et duplo quadrati, ut facillime possumus demonstrare.

Unde concludetur latus illud esse summam laterum circa rectum trianguli rectanguli, et unum ex quadratis illud componentibus efficere basem, et duplum quadratum aequari perpendiculo.

Illud itaque triangulum rectangulum conficietur a duobus quadratis quorum summa et differentia erunt quadrati. At isti duo quadrati minores probabuntur primis quadratis primo suppositis, quorum tam summa quam differentia faciunt quadratum:

Ergo, si dentur duo quadrati quorum summa et differentia faciunt quadratum, dabitur in integris summa duorum quadratorum eiusdem naturae, priore minor.

Eodem ratiocinio dabitur et minor ista inventa per viam prioris, et semper in infinitum minores invenientur numeri in integris idem praestantes: Quod impossibile est, quia, dato numero quovis integro, non possunt dari infiniti in integris illo minores.

Demonstrationem integram et fusius explicatam inserere margini vetat ipsius exiguitas.

Note that the separation into paragraphs is not original, but intended to simplify the comparison with the English translation in § 4.5, which follows the same separation into paragraphs. Moreover, we have omitted the beginning and the end of Observation XLV, which state the theorem and that it is proved indeed, respectively.

4.4 A Simple Self-Contained Modern Proof of Theorem 4.1

We show Theorem 4.1 by *descente infinie*, more precisely by indefinite descent (ID, cf. p.14).

Assuming the existence of x_0, x_1, x_2, x_3 with $x_0, x_1 \in \mathbf{N}_+$ and $x_0^2 + x_1^2 = x_2^2$ and $x_0 x_1 = 2x_3^2$, we will show the existence of y_0, y_1, y_2, y_3 with $y_0, y_1 \in \mathbf{N}_+$ and $y_0^2 + y_1^2 = y_2^2$, $y_0 y_1 = 2y_3^2$, and $y_2 \prec x_2$.

First, let us consider the case that there is some prime number z that divides x_0, x_1, i.e. that there are y_i with $x_i = z y_i$ for $i \in \{0, 1\}$. Then we have $z^2(y_0^2 + y_1^2) = x_2^2$, i.e. $z^2 \mid x_2^2$. By Lemma 3.20, we get $z \mid x_2$. Thus, there is some $y_2 \in \mathbf{N}_+$ with $x_2 = z y_2$. Then we also have $z^2(y_0^2 + y_1^2) = z^2 y_2^2$, i.e. $y_0^2 + y_1^2 = y_2^2$. Moreover, we have $z^2 y_0 y_1 = 2x_3^2$, i.e. $z^2 \mid 2x_3^2$. As z is prime, from the latter we get $z \mid 2$ or $z \mid x_3^2$ by Lemma 3.15. By Corollary 3.4, $z = 2$ and $z^2 \mid 2x_3^2$ implies $z \mid x_3^2$. Thus, we have $z \mid x_3^2$ in both cases, and then $z \mid x_3$ by Lemma 3.15 again. Thus, there is some y_3 with $x_3 = z y_3$. Then $z^2 y_0 y_1 = 2x_3^2 = z^2 2 y_3^2$, i.e. $y_0 y_1 = 2y_3^2$. From $x_0, x_1 \in \mathbf{N}_+$, we get $x_2 \in \mathbf{N}_+$. For each $i \in \{0, 1, 2\}$, we get $y_i \in \mathbf{N}_+$ from $x_i \in \mathbf{N}_+$. Finally, we have $y_2 \prec x_2$ because of $x_2 = z y_2$. This completes this case by *descente infinie*.

Thus, we may assume x_0, x_1 to be coprime by Lemma 3.22, and — a fortiori — x_0, x_1, x_2 to be coprime, too.

Claim I: There are coprime p, q such that one of them is odd and one of them is even, $p \succ q$, and there are some c, e, f with $x_2 \succ e \succ f \succ 0$ such that

$$p = e^2, \quad q = f^2, \quad \text{and} \quad p^2 - q^2 = c^2.$$

Proof of Claim I: By Corollary 3.27 there are coprime p and q such that one of them is odd and one of them is even and, for some $i \in \{0, 1\}$, $p \succ q$, $x_i = 2pq$, $x_{1-i} = p^2 - q^2$, and $x_2 = p^2 + q^2$. Because of $x_i \in \mathbf{N}_+$, we have $p, q \in \mathbf{N}_+$. From $x_0 x_1 = 2x_3^2$, we get $2pq(p^2 - q^2) = 2x_3^2$, i.e. $pq(p^2 - q^2) = x_3^2$. By Lemma 3.25, we know that pq and $p^2 - q^2$ are coprime, too. Thus, by Lemma 3.21 there must be some coprime $b, c \in \mathbf{N}_+$ with $x_3 = bc$, $pq = b^2$, and $p^2 - q^2 = c^2$. By the coprimality of p, q, because of $pq = b^2$, by Lemma 3.21 there must be some coprime $e, f \in \mathbf{N}_+$ with $b = ef$, $p = e^2$, and $q = f^2$. Moreover $e \succ f \succ 0$, as $e \preceq f$ would imply the contradictory $p \preceq q$, and $f = 0$ would imply the contradictory $x_i = 0$. Furthermore, from $q \in \mathbf{N}_+$, we get $x_2 = p^2 + q^2 \succ p^2 = e^4 \succeq e$.

Q.e.d. (Claim I)

Claim II: There are coprime $g, h \in \mathbf{N}_+$ and some e, f with $x_2 \succ e \succ f \succ 0$ such that

$$e^2 + f^2 = g^2 \quad \text{and} \quad e^2 - f^2 = h^2.$$

Proof of Claim II: Note we will not use any information on the current proof state beside Claim I here. By Claim I, $p+q, p-q \in \mathbf{N}_+$. By Claim I and Lemma 3.24(2), the only prime that may divide both $p+q$ and $p-q$ is 2; but this is not the case because one of p, q is even and one is odd. Thus, by Lemma 3.22, $p+q, p-q$ are coprime and because of $(p+q)(p-q) = p^2 - q^2 = c^2$, by Lemma 3.21, there are coprime $g, h \in \mathbf{N}_+$ with $c = gh$, $p+q = g^2$, $p-q = h^2$.

Q.e.d. (Claim II)

As the induction hypothesis in Fermat's original proof does not seem to be Theorem 4.1, but Claim II instead, let us forget anything about the current proof state here beside Claim II. The following two claims are trivial in the context of Claim II:

Claim IIa: $h^2 + 2f^2 = g^2$.

<u>Claim IIb:</u> $h^2+f^2=e^2$.

As g,h are coprime (according to Claim II), h,f,g are coprime, a fortiori. Thus, by Claim IIa and Corollary 3.30, there are m,k such that $2m,k$ coprime, $h=|2m^2-k^2|$, $f=2mk$, and $g=2m^2+k^2$. Set $y_0{:=}2m^2$, $y_1{:=}k^2$, $y_2{:=}e$, $y_3{:=}mk$. By Claim II we have $x_2\succ y_2\succ 0$. As $f\in\mathbf{N}_+$ by Claim II, we have $m,k\in\mathbf{N}_+$, and $y_0,y_1\in\mathbf{N}_+$. Moreover, we have $y_0y_1=2y_3^2$, $g=y_0+y_1$, and $f^2=2y_0y_1$. Finally, by Claim IIa and Claim IIb, we have $y_0^2+y_1^2 = (y_0+y_1)^2-2y_0y_1 = g^2-f^2 \underset{\text{(IIa)}}{=} h^2+2f^2-f^2 = h^2+f^2 \underset{\text{(IIb)}}{=} e^2 = y_2^2$. This completes also this remaining case by *descente infinie*.

Q.e.d. (Theorem 4.1)

4.5 An Annotated Translation of FERMAT's Original Proof

The following English translation of FERMAT's original proof (cf. § 4.3) roughly follows the translation found in [MAHONEY, 1994, p. 352f.], but has several improvements. Moreover — to refer to the proof of Theorem 4.1 in § 4.4 explicitly — we have added several annotations. (Brackets [...] enclose these annotations, which are typeset in italics.)

> If the area of a [*right-angled*] triangle were a square, there would be given two squares-of-squares [e^4, f^4] of which the difference would be a square [*Claim I*]; whence it follows that two squares [e^2, f^2] would be given, of which both the sum and the difference would be squares [*Claim II*]. And thus a number would be given, composed of a square and the double of a square, equal to a square [*Claim IIa*], under the condition that the squares composing it make a square [*Claim IIb*].
>
> However, if a square number is composed of a square and the double of another square [$g^2 = h^2 + 2f^2$], its side [*i.e. its square root* g] is similarly composed of a square and the double of a square [$g = k^2 + 2m^2$], as we can most easily demonstrate [*Corollary 3.30*].
>
> Whence one concludes that this side [g] is the sum of the sides [y_0, y_1] about the right angle of a right-angled triangle [$g = y_0 + y_1$, $y_0^2 + y_1^2 = y_2^2$], and that one of the squares composing it constitutes the base [$k^2 = y_1$], and the double square is equal to the perpendicular [$2m^2 = y_0$].
>
> [*Instead of applying Theorem 4.1 as an induction hypothesis now (or, dually, using its negation as the pattern for the descente infinie),* FERMAT *seems to descend the inductive reasoning cycle until the negation of Claim II can be applied as an induction hypothesis (or, dually, Claim II can be used as the pattern for the descente infinie).*] Hence, this right-angled triangle is generated [*(in the sense of § 3.4)*] by two squares, of which the sum and difference are squares. These two squares, however, will be proved to be smaller than the first squares initially posited, of which the sum as well as the difference also made squares:
>
> Therefore, if two squares [e^2, f^2] are given of which the sum and the difference are squares [*Claim II*], there exists in integers the sum of two squares of the same nature, less than the former [$e^2 + f^2$].
>
> [*Finally* FERMAT *illustrates the Method of Descente Infinie.*] By the same argument there will be given in the prior manner another one less than this, and smaller numbers will be found indefinitely having the same property. Which is impossible, because, given any integer, one cannot give an infinite number of integers less than it.
>
> The smallness of the margin forbids to insert the proof completely and with all detail. [*This is roughly the sentence following* FERMAT*'s Last Theorem in Observation II ([*FERMAT, *1891ff., Vol. I, p. 291], cf. our § 6), which drove generations of mathematicians crazy: "Hanc marginis exiguitas non caperet."*]

4.6 Similar Interpretations of the Proof in the Literature

My interpretation of FERMAT's proof being completed, it is now time to have a look into the literature of its interpretation. The interpretation of FERMAT's proof in [DICKSON, 1919ff., Vol. 2, p. 615f.], (looked up only after my interpretation was already completed) is roughly similar to my interpretation, but a little less structured and less similar to FERMAT's original proof. The interpretation of the proof in [EDWARDS, 1977, § 1.6], (looked up only after my interpretation was already completed) claims to follow [DICKSON, 1919ff., Vol. 2, p. 615f.], but makes things only worse and is not at all convincing.

> "It is the next two sentences [*our 2nd and 3rd paragraphs*] that are the difficult ones to follow [*for Edwards*]." [EDWARDS, 1977, § 1.6, p. 13]

The briefest interpretation of the proof in [WEIL, 1984, Chapter X] (looked up only after my interpretation was already completed) is quite in accordance with my interpretation when we apply the substitution $\{x{\mapsto}e, y{\mapsto}f, u{\mapsto}g, v{\mapsto}h, z{\mapsto}c, r{\mapsto}k, s{\mapsto}m\}$ to Weil's interpretation.

The interpretation of the proof in [MAHONEY, 1994, Chapter VI.VI] is less brief, but mathematically strange in the sense that there are some steps in it which I do not clearly understand (such as "we may set $f^2 = 4k^2m^2$."). As [MAHONEY, 1994] is the standard work on the mathematics of FERMAT, however, we have renamed our variables in accordance to it, such that the proof of [MAHONEY, 1994] is already roughly in accordance with our presentation here, without any renaming of variables.

The discussion of the proof in [BUSSOTTI, 2006, Chapter 2.2.3, pp. 39–46] follows the interpretation of [MAHONEY, 1994], but elaborates the ways and means of the induction-hypothesis application, or more precisely, the indefinite descent. We read:

> "From this demonstration, it is possible to deduce one of the most important properties inherent in every argument by indefinite descent: there is an *invariable form* with different orders of sizes [...]. [BUSSOTTI, 2006, p. 45]

As we have already discussed in § 2.4.4, from a refined logic-historical point of view, this "*invariable form*" may actually vary. This will become important in § 4.7 below, where we will discuss the only interpretation of FERMAT's original proof that significantly differs from my presentation here, namely the one in [WALSH, 1928].

4.7 WALSH's Alternative Interpretation

The only interpretation of FERMAT's original proof that significantly differs from our presentation here is the one in [WALSH, 1928]. With the missing details added and the unconvincing parts removed, we may describe WALSH's interpretation roughly as follows.

Suppose that the clean-up of § 4.4 up to Claim I has been done. Then we continue as follows.

Claim III: There are some $e, f, g, h \in \mathbf{N}_{+}$ with g, h coprime and $x_2 \succeq e \succ f \succ 0$ such that

$$e^2{+}f^2 = g^2 \quad \text{and} \quad e^2{-}f^2 = h^2.$$

Proof of Claim III: Set $e := x_2$, $f := 2x_3$, $g := x_0{+}x_1$, and $h := |x_0{-}x_1|$. Then we have $e^2{\pm}f^2 = x_2^2{\pm}4x_3^2 = x_0^2{+}x_1^2{\pm}2x_0x_1 = (x_0{\pm}x_1)^2$. Moreover, we have $e \succ f$ by the following indirect proof: Otherwise, we would have $0 \succeq e^2{-}f^2 = (x_0{-}x_1)^2$, i.e. $x_0 = x_1$, and as x_0, x_1 are coprime, we would get $x_0 = x_1 = 1$, i.e. the contradictory $2 = x_2^2$. Finally, to show that g, h are coprime suppose $z \mid x_0{+}x_1$ and $z \mid |x_0{-}x_1|$. As x_0, x_1 are coprime, we get $z \preceq 2$ by Lemma 3.24(2). By Corollary 3.27 we know that $x_0{+}x_1$ is odd. Thus, we get $z = 1$, as was to be shown. Q.e.d. (Claim III)

Compared to Claim II of § 4.4, the weakness of Claim III is that it only states $x_2 \succeq e$ instead of $x_2 \succ e$. This weaker statement, however, does not admit us to apply our induction hypothesis as before. This is not by chance and another weight function cannot help us, because the new triangle is actually the same as before: Indeed, we have $x_2 = e = y_2$ and $\{x_0, x_1\} = \{\frac{g \pm h}{2}\} = \{2m^2, k^2\} = \{y_0, y_1\}$. This means that — to arrive in proof state with a smaller weight — we actually have to descend the inductive reasoning cycle by proving Claim I and Claim II. The interesting aspect is that — as noted already in § 4.5 — this is exactly what FERMAT does in his proof. While these steps are superfluous according to all other interpretations, they are necessary according to the interpretation in [WALSH, 1928].

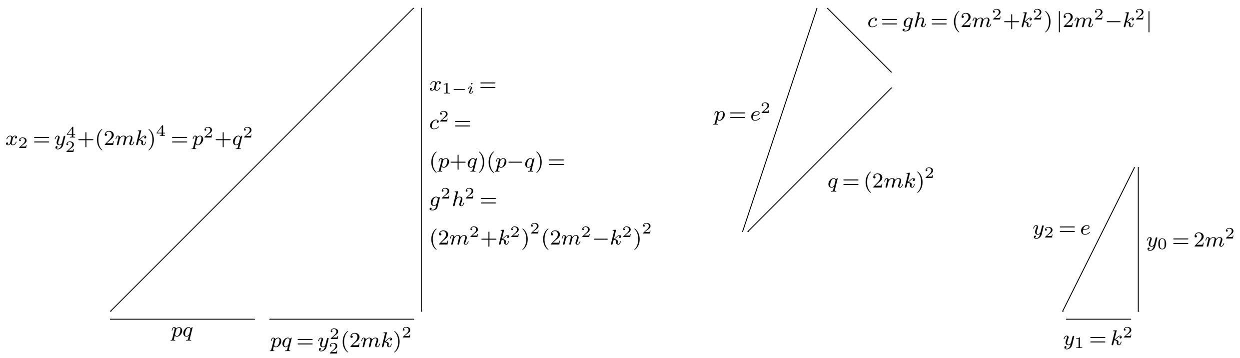
Note that, according to § 2.4.4, WALSH's proof is actually sound w.r.t. the following instantiation: In (ID′) of § 2.4.4, roughly speaking, we set P_0 to Theorem 4.1, and P_i to Claim II for all $i \in \mathbf{N}_{+}$. We measure P_0 with the weight $x_2^2{+}(2x_3)^2{+}1$. And we measure P_i with the weight $e^2{+}f^2$ for $i \in \mathbf{N}_{+}$, just as FERMAT has described the weight in his original proof, cf. the 4th paragraph of our annotated translation in § 4.5. From P_0 to P_1 the weight decreases by 1. And from P_i to P_{i+1} the weight also decreases for $i \in \mathbf{N}_{+}$. A simpler way to see the soundness of this proof is to model it as a deductive proof of Theorem 4.1 with Claim II as a lemma, plus an inductive proof of Claim II.

We cannot decide whether the interpretation of WALSH [1928] for the first step of FERMAT's proof (i.e. the Proof of Claim III) reflects FERMAT's intentions regarding his original proof better than our presentation in §§ 4.4 and 4.5. The interpretation of the actual indefinite descent of FERMAT, however, is superior in WALSH's version. Moreover, note that — considering FERMAT's extreme conciseness in general — it is very likely that FERMAT had believed the additional descent to be actually necessary. We cannot decide, however, whether this belief, which he contradicts in his letter for HUYGENS in 1659 (cf. § 4.2), means that WALSH's interpretation is the correct one. This belief may be simply based on FERMAT's inexperience with *descente infinie* at the time when he wrote his Observation XLV, more than 20 years before his death in 1665. The following dating of the Observations very roughly agrees with [GOLDSTEIN, 1995, § 11]:

> "The dates of the various notes on DIOPHANTUS are not known; but it is probable that this Note [*Observation XLV*] was written sometime between 1636 and 1641, or at least, in round numbers twenty years before the Letter [*for* HUYGENS]. This is important; for the Note and the Letter do not agree — at least in appearance [*of the induction-hypothesis application*]." [WALSH, 1928, p. 412]

4.8 FRÉNICLE's More Elegant Version of FERMAT's Proof

Note that geometric illustration cannot help much to understand the Proof of Theorem 4.1 in § 4.4. The following seems to be the best we can get:



The leftmost triangle is the originally assumed one and the rightmost triangle is the one to which the modern Proof of Theorem 4.1 in § 4.4 descends. Although the one in the middle is rectangular by Claim I, it is not explicitly noted in FERMAT's proof. In the proof of the same theorem in [FRÉNICLE, 1676], however, BERNARD FRÉNICLE DE BESSY (1605?–1675) (Paris) descends to the same rightmost triangle but completely avoids application of Corollary 3.30 by an application of Lemma 3.28 to the rectangular triangle depicted in the middle. Omitting Claim II and all the following, the proof of Proposition XXXIX in [FRÉNICLE, 1676] continues roughly as follows: We have (Claim I) $q^2+c^2=p^2$, c is odd, $p=e^2$, $q=f^2$, $x_2 \succ e \succ f \succ 0$, and p, q are coprime. By Lemma 3.28, there are $m, k \in \mathbf{N}_+$ such that $(2m^2)^2+(k^2)^2=p=e^2$. q.e.d. This is more elegant than FERMAT's proof with an obviously and definitely different lemmatization, which, however, was sometimes neglected:

> "FRÉNICLE follows this proof [*of* FERMAT] faithfully, with little more than verbal changes [...]. [WEIL, 1984, § X, p. 77]

As we are already exceeding the scope of this little paper and our margins are too small, we ask the reader who is interested in more information on the subject to have a look at [GOLDSTEIN, 1995], which is a whole book dedicated to the history of Theorem 4.1, including a discussion of different interpretations of FERMAT's Latin original and much more.

5 Conclusion

Fermat gave his readers a hard time with his notes. His proof sketch of his Observation XLV, which we have studied in this paper in some detail, is hard to understand, interpret, and disambiguate; for the readers of the 21st century just as well as for readers of 17th century. Without expertise in number theory, it takes some days to construct a consistent interpretation of this short proof sketch.

Fermat named the method of this proof *descente infinie*. This method and its variants are of outstanding importance in mathematics.

In § 2, we have discussed the Method of *Descente Infinie* from the mathematical, logical, historical, linguistic, and refined logic-historical points of view, and we have presented all its aspects with novel clearness, precision, and detail.

As Fermat wanted people to have fun with number theory, we have suggested that our § 3 could be skipped by the readers and have put its less interesting proofs into the appendix (§ A); so a reader who is not an expert in number theory may choose between the fun of exercise or the relief of solution.

Regarding the aspects of both pedagogical presentation and the interpretation of critical texts in the history of mathematics, we consider it to be advantageous to present the following three in the given order:

1. the Latin original proof (§ 4.3),
2. a modern self-contained proof (§ 4.4),
3. and an English translation of the Latin original (§ 4.5).

This paper is (to the best of our knowledge) unique already in presenting these three items.

Moreover, this paper is (again to the best of our knowledge) unique in annotating the English translation with references to a more explicit modern proof and not vice versa. Although we have been quite laconic with our comments in the translation, we are confident that the mathematical gestalt of Fermat's proof sketch is perceivable with the help of the sparse annotations in the translation in § 4.5, building on the detailed presentation of the modern proof in § 4.4. We believe that this perception is easier and deeper than what can arise from the standard procedure of presenting a modern proof with annotations from (a translation of) the original, and that the usefulness of our procedure for interpreting critical texts in the history of mathematics is higher than that of the standard procedure.

All in all, including all important facts, we have presented a concise and self-contained discussion of Fermat's proof sketch, which is easily accessible to laymen in number theory as well as to laymen in the history of mathematics, and which provides new clarification of the Method of *Descente Infinie* to the experts in these fields. Last but not least, this paper fills a gap regarding the easy accessibility of the subject.

6 Aftermath

Finally, note that FERMAT's proof sketch omits the little but important details of the proof, such as being positive, being coprime, or $2 \nmid p{-}q$, which are essential parts of our modern proof in § 4.4. Moreover, he does not at all explicate the underlying theory, which we tried to reconstruct in § 3.

As he seems to have found his proofs without pen and paper just in his imagination, he may have had some subconscious subroutines taking care of this. Such subroutines are error-prone and would explain FERMAT's only claim that we know to be wrong, namely to have proved $\forall n \in \mathbf{N}.\ (2^{2^n}{+}1 \text{ prime})$, contradicted by $5 = \mu n.\ \neg(2^{2^n}{+}1 \text{ prime})$ because of $2^7 5{+}1 \mid 2^{2^5}{+}1$. This claim of a proof occurs in that same letter for HUYGENS, which we quoted in § 4.2 and discussed in § 2.3.4. Five years before, in a letter to PASCAL in August 1654, he had admitted that the proof was still incomplete; cf. [FERMAT, 1891ff., Vol. II, p. 309f.].

Whether the proof FERMAT claimed to have found for "FERMAT's Last Theorem"

$$\forall n \succeq 3.\ \forall x, y, z \in \mathbf{N}_{+}.\ (x^n{+}y^n \neq z^n)$$

was also faulty for bigger n, or whether FERMAT, the methodologist who after eighteen centuries was the first to apply the Method of *Descente infinie* again, invented yet another method for this proof, is still an open question.

Acknowledgments

I would like to thank PAOLO BUSSOTTI for a list of suggestions for improvement on an earlier version of this paper, for some profound help, and for much more.

I would also like to thank CATHERINE GOLDSTEIN for some information on the sophistication of the publications of L'Académie Royale des Sciences, Paris.

Furthermore, I would like to thank STEPHAN UNVERZAGT for some alternative translations of FERMAT's Latin text, which were especially useful because they did not take the mathematical content into account.

Finally, I would like to thank MARC WAGNER for some help with the French language, and for much more.

A Missing Proofs and Additional Lemmas

Proof of Lemma 3.7

Let us assume $x_0 y_1 = y_0 x_1$ with $x_0, x_1, y_0, y_1 \in \mathbf{N}_+$.

(i): We show the "only if"-direction, the "if"-direction is symmetric. $x_0 z_1 y_0 = x_0 y_0 z_1 = x_0 z_0 y_1 = z_0 x_0 y_1 = z_0 y_0 x_1 = z_0 x_1 y_0$. Thus, dividing by y_0, we get $x_0 z_1 = z_0 x_1$.

(iii)⇒(ii): Assume (iii). If y_0, y_1 were not coprime, there would be some $k \succeq 2$ and $y''_i \in \mathbf{N}_+$ with $k y''_i = y_i$ for $i \in \{0,1\}$. Then we would have $x_0 k y''_1 = k y''_0 x_1$, and then $x_0 y''_1 = y''_0 x_1$. This would contradict the $\preceq$-minimality of y_0.

(iii)⇒(iv): Assume (iii). Dividing x_i by y_i, we get $k_i, r_i \in \mathbf{N}$ with $x_i = k_i y_i + r_i$ and $r_i \prec y_i$ for $i \in \{0,1\}$. Then $k_0 y_0 y_1 + r_0 y_1 = (k_0 y_0 + r_0) y_1 = x_0 y_1 = y_0 x_1 = y_0 (k_1 y_1 + r_1) = k_1 y_0 y_1 + r_1 y_0$ with $r_i y_{1-i} \prec y_0 y_1$ for $i \in \{0,1\}$. Thus, dividing $x_0 y_1$ by $y_0 y_1$, we get k_0 with remainder $r_0 y_1$ as well as k_1 with remainder $r_1 y_0$. Thus, $k_0 = k_1$ and $r_0 y_1 = r_1 y_0$. Then $x_0 r_1 y_0 = x_0 r_0 y_1 = x_0 y_1 r_0 = y_0 x_1 r_0 = r_0 x_1 y_0$. Thus, we have $x_0 r_1 = r_0 x_1$. But as $r_0 \prec y_0$ and as y_0 is the least number such that there is a $y'_1 \in \mathbf{N}_+$ with $x_0 y'_1 = y_0 x_1$, we have $r_0 = 0$. This implies $r_1 = 0$. Thus, $x_i = k_0 y_i$ for $i \in \{0,1\}$.

(ii)⇒(iii): Assume (ii). As $y_0 z_1 = z_0 y_1$ has the solution $(z_0, z_1) = (x_0, x_1) \in \mathbf{N}_+ \times \mathbf{N}_+$, let z_0 be $\preceq$-minimal such that there is a $y'_1 \in \mathbf{N}_+$ with $y_0 y'_1 = z_0 y_1$. Then $z_0 \in \mathbf{N}_+$. Let $z_1 \in \mathbf{N}_+$ be given such that $y_0 z_1 = z_0 y_1$. Applying (iii)⇒(iv) to the sentence $y_0 z_1 = z_0 y_1$, we infer that there is a $k \in \mathbf{N}_+$ such that $k z_i = y_i$ for $i \in \{0,1\}$. Thus, $k \mid y_i$ for $i \in \{0,1\}$. As y_0, y_1 are coprime, we have $k = 1$. Thus, $z_0 = y_0$. Thus, y_0 is $\preceq$-minimal such that there is a y'_1 with $y_0 y'_1 = y_0 y_1$. By (i), y_0 is $\preceq$-minimal such that there is a y'_1 with $x_0 y'_1 = y_0 x_1$. **Q.e.d. (Lemma 3.7)**

Proof of Lemma 3.8 Assume $u \mid x$ and $u \mid z$. By transitivity of $\mid$ according to Corollary 3.2, from $x \mid y$ we have $u \mid y$. From y, z being coprime we get $u = 1$. **Q.e.d. (Lemma 3.8)**

Proof of Lemma 3.9 For $m = 0$, the lemma holds as 1 is the minimal element of the reflexive ordering $\mid$ according to Corollary 3.2. Thus, let us show that the lemma holds for $m{+}1$ under the induction hypothesis that it holds for m. If there is some $i \in \{1, \ldots, m{+}1\}$ with $x_i = 0$, then we have $z = 1$, and the lemma holds for $m{+}1$. In case of $z = 0$, we have $x_i = 1$ for all $i \in \{1, \ldots, m{+}1\}$, and the lemma holds again for $m{+}1$. Thus we may assume $x_0, \ldots, x_{m+1}, z \in \mathbf{N}_+$. Assume $u \mid \prod_{i=1}^{m+1} x_i$ and $u \mid z$. By the first there is some k' with $x_{m+1} \prod_{i=1}^{m} x_i = k' u$ and $k', u \in \mathbf{N}_+$. By the second, by x_{m+1}, z being coprime, and by Lemma 3.8, we get that x_{m+1}, u are coprime. Thus, by Lemma 3.7, there is some $k \in \mathbf{N}_+$ with $k u = \prod_{i=1}^{m} x_i$. But then $u \mid \prod_{i=1}^{m} x_i$. By our induction hypothesis, $\prod_{i=1}^{m} x_i$, z are coprime. Thus, we get $u = 1$. **Q.e.d. (Lemma 3.9)**

Proof of Lemma 3.10 For $m+n=0$, the lemma holds as 1 is the minimal element of the reflexive ordering $|$ according to Corollary 3.2. Thus, suppose the lemma holds for arbitrary $m+n$ to show that it holds for $m+n+1$. By symmetry, we may assume that x_i, y_j are coprime for $i \in \{1,\ldots,m\}$ and $j \in \{1,\ldots,n+1\}$. By Lemma 3.9 y_{n+1}, $\prod_{i=1}^{m} x_i$ are coprime. By induction hypothesis, $\prod_{i=1}^{n} y_i$, $\prod_{i=1}^{m} x_i$ are coprime. All in all, by Lemma 3.9 $y_{n+1}\prod_{i=1}^{n} y_i$, $\prod_{i=1}^{m} x_i$ are coprime, i.e. $\prod_{i=1}^{m} x_i$, $\prod_{i=1}^{n+1} y_i$ are coprime.
Q.e.d. (Lemma 3.10)

Proof of Lemma 3.14 Assume $k \mid p$ and $k \mid x$. As p is prime, we have $k \in \{1,p\}$. As $p \nmid x$, we have $k \neq p$. Thus, $k=1$. **Q.e.d. (Lemma 3.14)**

Proof of Lemma 3.15 We may assume $p \nmid x_1$ and $x_0, x_1 \in \mathbf{N}_+$. Then p, x_1 are coprime by Lemma 3.14. Because of $p \mid x_1x_2$, there is some k with $kp = x_1x_2$. Then $k \in \mathbf{N}_+$. By Lemma 3.7, we get $p \mid x_2$. **Q.e.d. (Lemma 3.15)**

Proof of Lemma 3.16

We show this by *descente infinie*, more precisely by indefinite descent (ID, cf. p.14).

Suppose that there is some $x \neq 1$ not divided by any prime. We look for an $x' \neq 1$ not divided by any prime with $x' \prec x$. As the relation $|$ is reflexive and has maximum 0 according to Corollary 3.2, x is not prime and $x \succeq 2$. Thus, there must be some $x' \notin \{1,x\}$ with $x' \mid x$. As the relation $|$ is transitive according to Corollary 3.2, x' is not divided by any prime. Moreover, there is a k such that $kx' = x$. From $x \succeq 2$ and $x' \notin \{1,x\}$, we thus get $k \succeq 2$ and $x' \succeq 2$. Thus, $x' \prec x$. **Q.e.d. (Lemma 3.16)**

Proof of Lemma 3.18

<u>Claim 1:</u> $x_0y_i = y_0x_i$ and $x_{i-1}y_i = y_{i-1}x_i$ for all $i \in \{1,\ldots,n+1\}$.
<u>Proof of Claim 1:</u> For $i=1$ this holds by assumption of the lemma. Suppose it holds for $i \in \{1,\ldots,n\}$. Then $x_0y_{i+1} = \frac{x_0y_i^2}{y_{i-1}} = \frac{y_0x_iy_i}{y_{i-1}} = \frac{y_0x_i^2}{x_{i-1}} = y_0x_{i+1}$ and $x_iy_{i+1} = \frac{x_iy_i^2}{y_{i-1}} = \frac{x_i^2y_i}{x_{i-1}} = y_ix_{i+1}$.
<u>Q.e.d. (Claim 1)</u>

From Claim 1 we get $x_0y_{n+1} = y_0x_{n+1}$. As x_0, x_{n+1} are coprime, by Lemma 3.7 there is some $k \in \mathbf{N}_+$ with $kx_i = y_i$ for $i \in \{0, n+1\}$. By Claim 1 this holds for all $i \in \{0,\ldots,n+1\}$ because of $kx_i = \frac{kx_0y_i}{y_0} = \frac{y_0y_i}{y_0} = y_i$. **Q.e.d. (Lemma 3.18)**

Proof of Lemma 3.19 Let y be minimal with $x_0z = yx_1$ for some $z \in \mathbf{N}_+$. By Lemma 3.7, $y \in \mathbf{N}_+$, y, z are coprime, and there is some $k' \in \mathbf{N}_+$ with $k'y = x_0$ and $k'z = x_1$. Thus, $x_0(y^nz^1) = k'y^{n+1}z^1 = (y^{n+1}z^0)x_1$. Moreover, $y^{n+1}z^0, \ldots, y^{n+1-i}z^i, \ldots, y^0z^{n+1}$ are in continued proportion. By Corollary 3.11, y^{n+1}, z^{n+1} are coprime, too. Applying Lemma 3.18, we get a $k \in \mathbf{N}_+$ with $ky^{n+1-i}z^i = x_i$ for $i \in \{0,\ldots,n+1\}$. In case that x_0, x_{n+1} are coprime, we get by Lemma 3.18 a $k'' \in \mathbf{N}_+$ with $k''x_i = y^{n+1-i}z^i$. This means $x_i \preceq y^{n+1-i}z^i$, i.e. $k=1$. **Q.e.d. (Lemma 3.19)**

Below we will prove Proposition VIII.14 of EUCLID's Elements, but we give a proof that is shorter and more modern than the one in the Elements, which recursively requires a large number of additional propositions. Instead we need the following two lemmas.

The following lemma will be applied exclusively in the proofs of Lemmas A.2 and 3.20.

Lemma A.1 *If p is prime and $p^m \mid x_0x_1$, then there are n_0 and n_1 such that $m=n_0+n_1$, $p^{n_0} \mid x_0$, and $p^{n_1} \mid x_1$.*

Proof of Lemma A.1

We show this by *descente infinie*, more precisely by indefinite descent (ID, cf. p.14).

Let p be prime. Suppose that $p^m \mid x_1x_2$, but there are no n_1 and n_2 such that $m=n_1+n_2$, $p^{n_1} \mid x_1$, and $p^{n_2} \mid x_2$. Then $m, x_0, x_1 \in \mathbf{N}_+$. By Lemma 3.15, there is an $i \in \{0,1\}$ such that $p \mid x_i$. Thus, there is some $x'_i \in \mathbf{N}_+$ with $x'_i p = x_i$. Set $x'_{1-i} := x_{1-i}$. There is some $k \in \mathbf{N}_+$ with $kp^m = x_0x_1$. Thus, $kp^m = x'_{1-i}x'_i p$. Thus, $kp^{m-1} = x'_{1-i}x'_i$. But there cannot be any n'_1 and n'_2 such that $m-1=n'_1+n'_2$, $p^{n'_1} \mid x'_1$, and $p^{n'_2} \mid x'_2$, because this leads to a contradiction when we set $n_i := n'_i+1$ and $n_{1-i} := n'_{1-i}$. **Q.e.d. (Lemma A.1)**

The following lemma will be applied exclusively in the proof of Lemma 3.20.

Lemma A.2 $x \mid y$ *iff* $\forall p$ *prime.* $\forall n \in \mathbf{N}_+.\ \big(\ (p^n \mid x) \ \Rightarrow\ (p^n \mid y)\ \big)$.

Proof of Lemma A.2 The "only if"-direction follows directly from the transitivity according to Corollary 3.2. We show the other direction by *descente infinie*, more precisely by indefinite descent: Suppose that there are x, y such that $\forall p$ prime. $\forall n \in \mathbf{N}_+$. $\big(\ (p^n \mid x) \ \Rightarrow\ (p^n \mid y)\ \big)$, but $x \nmid y$. We find x', y' of the same kind with $y' \prec y$. According to Corollary 3.2, we have $x \neq 1$ and $y \neq 0$. By Lemma 3.16, there is some prime p such that $p \mid x$. Then we have $p \mid y$ by our assumption (setting $n := 1$). Thus, we have $y \succeq 2$. Moreover, there is some $y' \in \mathbf{N}_+$ with $y'p = y$. Thus $y' \prec y$. Moreover, there is some x' with $x'p = x$. Then $x' \nmid y'$. It suffices to show that for any prime number q and any $n \in \mathbf{N}_+$ with $q^n \mid x'$ we have $q^n \mid y'$.
$\underline{q=p}$: From $p^n \mid x'$ we get $p^{n+1} \mid x$, and then $p^{n+1} \mid y$, i.e. $p^{n+1} \mid y'p$. By Corollary 3.4, we get $p^n \mid y'$.
$\underline{q \neq p}$: From $q^n \mid x'$ we get $q^n \mid x$, and then $q^n \mid y$, i.e. $q^n \mid y'p$. By Lemma A.1, we get $q^n \mid y'$. **Q.e.d. (Lemma A.2)**

Proof of Lemma 3.20 The "only if"-direction is trivial. For the "if"-direction, assume $x^2 \mid y^2$ and $p^n \mid x$ for arbitrary prime number p and $n \in \mathbf{N}_+$. By Lemma A.2 it suffices to show $p^n \mid y$. But from $p^n \mid x$ we get $p^{2n} \mid x^2$, and then $p^{2n} \mid y^2$. By Lemma A.1, we get $p^n \mid y$. **Q.e.d. (Lemma 3.20)**

Proof of Lemma 3.21 If any of a, b is equal to 0, then the other divides both and thus (as a, b are coprime) must be equal to 1; and $x=0$; in which case the lemma follows by $y := a$ and $z := b$. If none of a, b is equal to 0, then also x is not equal to 0 and a, x, b are in continued proportion; so the lemma follows from Lemma 3.19 by setting its $n := 1$. **Q.e.d. (Lemma 3.21)**

Proof of Lemma 3.22 The "if"-direction is trivial. For the "only if"-direction let us assume that $l_1, \ldots, l_n$ are not coprime. Then there is some $x \neq 1$ such that $x \mid l_i$ for all $i \in \{1, \ldots, n\}$. By Lemma 3.16 there is some prime number p with $p \mid x$. By transitivity of $\mid$ according to Corollary 3.2, we get $p \mid l_i$ for all $i \in \{1, \ldots, n\}$. **Q.e.d. (Lemma 3.22)**

Proof of Lemma 3.23

(1): Suppose neither pa, b nor a, pb coprime. By Lemma 3.22 there are two prime numbers x, y with $x \mid pa$, $x \mid b$, $y \mid a$, $y \mid pb$. As a, b coprime, $x \nmid a$. As x is prime, by Lemma 3.15 we get $x \mid p$ and thus $x = p$, as p is prime. Similarly we get $y = p$. Thus $p \mid b$ and $p \mid a$, contradicting being a, b being coprime.

(2): If pa, b are coprime, they must be squares by Lemma 3.21, say $pa = l^2$ and $b = k^2$. By Lemma 3.15, there is some m with $pm = l$, i.e. $a = pm^2$. By Lemma 3.8, pm, k are coprime. Thus, $k \in \mathbf{N}_+$ because $pm \neq 1$. Moreover, $\{pm^2, k^2\} = \{a, b\}$. Similarly, if a, pb are coprime, they must be squares by Lemma 3.21, say $a = k^2$ and $pb = l^2$. By Lemma 3.15, there is some m with $pm = l$, i.e. $b = pm^2$. Then again we have $k \in \mathbf{N}_+$, pm, k are coprime, and $\{pm^2, k^2\} = \{a, b\}$. **Q.e.d. (Lemma 3.23)**

Proof of Lemma 3.24

(1): By Corollary 3.3 we get $x \mid (a+b) \pm (a-b)$, i.e. $x \mid 2a$ and $x \mid 2b$.

(2): By (1) we have $x \mid 2a$ and $x \mid 2b$. Assume $x \succ 2$ to show a contradiction. If $2 \mid x$, then there is some $k \succeq 2$ with $2k = x$, and then we have $k \mid a$ and $k \mid b$, contradicting a, b being coprime. Otherwise, if $2 \nmid x$, then by Lemma 3.16 there is some prime number $p \succ 2$ with $p \mid x$. Then $p \mid 2a$. By Lemma 3.15 we get $p \mid a$. Similarly $p \mid b$. This again contradicts a, b being coprime. **Q.e.d. (Lemma 3.24)**

The following lemma will be applied exclusively in the proof of Lemma 3.25.

Lemma A.3 *If* $p \succeq q$ *and* $x \mid 2pq$, *then* $x \mid p^2 - q^2$ *iff* $x \mid p^2 + q^2$.

Proof of Lemma A.3 As $x^2 \mid 4p^2q^2$ by Lemma 3.20, the following are logically equivalent by Corollary 3.3 and Lemma 3.20: $x \mid p^2 - q^2$; $x^2 \mid (p^2 - q^2)^2$; $x^2 \mid p^4 - 2p^2q^2 + q^4$; $x^2 \mid p^4 + 2p^2q^2 + q^4$; $x^2 \mid (p^2 + q^2)^2$; $x \mid p^2 + q^2$. **Q.e.d. (Lemma A.3)**

Proof of Lemma 3.25 Suppose the contrary. Then by Lemma 3.22 there is a prime number x with $x \mid pq$ and $(x \mid p^2 + q^2) \vee (x \mid p^2 - q^2)$. Then we have $x \mid 2pq$, and then, by Lemma A.3, we have $(x \mid p^2 + q^2) \wedge (x \mid p^2 - q^2)$. Moreover, by Lemma 3.24(1), we have $x \mid 2p^2$ and $x \mid 2q^2$. As p, q are coprime, one of them is odd. Thus, one of pq and $p^2 + q^2$ is odd. Thus, as x divides both, $x \neq 2$. Thus, as x is prime, we have $x \nmid 2$. By Lemma 3.15, we get $x \mid p^2$ and $x \mid q^2$, and then $x \mid p$ and $x \mid q$, contradicting p, q being coprime. **Q.e.d. (Lemma 3.25)**

References

[Acerbi, 2000] Fabio Acerbi. Plato: Parmenides 149a7–c3. a proof by complete induction? *Archive for History of Exact Sciences*, 55:57–76, 2000.

[Ackermann, 1940] Wilhelm Ackermann. Zur Widerspruchsfreiheit der Zahlentheorie. *Mathematische Annalen*, 117:163–194, 1940. Received Aug. 15, 1939.

[Avenhaus &al., 2003] Jürgen Avenhaus, Ulrich Kühler, Tobias Schmidt-Samoa, and Claus-Peter Wirth. How to prove inductive theorems? QuodLibet! 2003. In [Baader, 2003, pp. 328–333], `http://www.ags.uni-sb.de/~cp/p/quodlibet`.

[Baader, 2003] Franz Baader, editor. *19th Int. Conf. on Automated Deduction, Miami Beach (FL), 2003*, number 2741 in Lecture Notes in Artificial Intelligence. Springer, 2003.

[Barner, 2001] Klaus Barner. Das Leben Fermats. *DMV-Mitteilungen*, 3/2001:12–26, 2001.

[Becker, 1965] Oscar Becker, editor. *Zur Geschichte der griechischen Mathematik*. Wissenschaftliche Buchgesellschaft, Darmstadt, 1965.

[Berka & Kreiser, 1973] Karel Berka and Lothar Kreiser, editors. *Logik-Texte – Kommentierte Auswahl zur Geschichte der modernen Logik*. Akademie-Verlag, Berlin, 1973. 2nd rev. ed. (1st ed. 1971; 4th rev. rev. ed. 1986).

[Bussey, 1917] W. H. Bussey. The origin of mathematical induction. *American Mathematical Monthly*, XXIV:199–207, 1917.

[Bussotti, 2006] Paolo Bussotti. *From* Fermat *to* Gausz*: indefinite descent and methods of reduction in number theory.* Number 55 in Algorismus. Dr. Erwin Rauner Verlag, Augsburg, 2006.

[Dickson, 1919ff.] Leonard Eugene Dickson. *History of the Theory of Numbers*. Carnegie Inst. of Washington, 1919ff..

[Diophantus, 1621] Diophantus of Alexandria. *Diophanti Alexandrini Arithmeticorum Libri Sex, Et De Numeris Multangulis Liber Unus. Nunc primum Graece & Latine editi, atque absolitissimis Commentariis illustrati. Auctore Claudio Gaspare Bacheto Meziriaco Sebusiano, V. C.* Sébastien Cramoisy, Paris, 1621.

[Diophantus, 1670] Diophantus of Alexandria. *Diophanti Alexandrini Arithmeticorum Libri Sex, Et De Numeris Multangulis Liber Unus. Cum Commentariis C. G. Bacheti V. C. & observationibus D. P. de* Fermat *Senatoris Tolosani. Accessit Doctrinae Analyticae inventum novum, collectum ex variis eiusdem D. de* Fermat *Epistolis*. Bernard Bosc, Toulouse, 1670.

[Edwards, 1977] Herold M. Edwards. Fermat*'s Last Theorem — A Genetic Introduction to Algebraic Number Theory*. Springer, 1977.

[Euclid, ca. 300 b.c.] Euclid of Alexandria. *Elements*. ca. 300 b.c.. Web version without the figures: `http://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.01.0085`. English translation: Thomas L. Heath (ed.). *The Thirteen Books of* Euclid*'s Elements*. Cambridge Univ. Press, 1908; web version without the figures: `http://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.01.0086`. English web version (incl. figures): D. E. Joyce (ed.). Euclid*'s Elements*. `http://aleph0.clarku.edu/~djoyce/java/elements/elements.html`, Dept. Math. & Comp. Sci., Clark Univ., Worcester (MA).

[Fermat, 1891ff.] Pierre Fermat. *Œuvres de* Fermat. Gauthier-Villars, Paris, 1891ff.. Ed. by Paul Tannery, Charles Henry.

[Feyerabend, 1975] Paul Feyerabend. *Against Method*. New Left Books, London, 1975.

[Fowler, 1994] David Fowler. Could the Greeks have used mathematical induction? Did they use it? *Physis*, XXXI(1):253–265, 1994.

[Frénicle, 1676] Bernard Frénicle de Bessy. *Traité des Triangles Rectangles en Nombres*. E. Michallet, Paris, 1676. Also in: Recueil de plusieurs traitez de mathematique de L'Académie Royale des Sciences, Imprimerie Royale, Paris, 1676f.. Also in: Mémoires de L'Académie Royale des Sciences, depuis 1666 jusqu'en 1699 **V**, pp. 127–206, Compagnie des Libraires, Paris, 1729.

[Freudenthal, 1953] Hans Freudenthal. Zur Geschichte der vollständigen Induktion. *Archives Internationales d'Histoire des Sciences*, 6:17–37, 1953.

[Fritz, 1945] Kurt von Fritz. The discovery of incommensurability by Hippasus of Metapontum. *Annals of Mathematics*, 46:242–264, 1945. German translation: *Die Entdeckung der Inkommensurabilität durch* Hippasos von Metapont in [Becker, 1965, pp. 271–308].

[Gentzen, 1935] Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210,405–431, 1935. Also in [Berka & Kreiser, 1973, pp. 192–253]. English translation in [Gentzen, 1969].

[Gentzen, 1969] Gerhard Gentzen. *The Collected Papers of* Gerhard Gentzen. North-Holland (Elsevier), 1969. Ed. by Manfred E. Szabo.

[Gillman, 1987] Leonard Gillman. *Writing Mathematics Well*. The Mathematical Association of America, 1987.

[Goldstein, 1995] Catherine Goldstein. *Un Théorème de* Fermat *et ses Lecteurs*. Histoires de Science. Presses Universitaires de Vincennes, Saint-Denis, 1995.

[Gramlich & Wirth, 1996] Bernhard Gramlich and Claus-Peter Wirth. Confluence of terminating conditional term rewriting systems revisited. In *7^{th} Int. Conf. on Rewriting Techniques and Applications, New Brunswick (NJ), 1996*, number 1103 in Lecture Notes in Computer Science, pages 245–259. Springer, 1996.

[Hilbert & Bernays, 1968/70] David Hilbert and Paul Bernays. *Die Grundlagen der Mathematik*. Springer, 1968/70. 2^{nd} rev. ed. (1^{st} ed. 1934/39).

[HUTTER & STEPHAN, 2005] Dieter Hutter and Werner Stephan, editors. *Mechanizing Mathematical Reasoning: Essays in Honor of Jörg H. Siekmann on the Occasion of His 60th Birthday*. Number 2605 in Lecture Notes in Artificial Intelligence. Springer, 2005.

[KATZ, 1998] Victor J. Katz. *A History of Mathematics: An Introduction*. Addison-Wesley, 1998. 2nd ed..

[MAHONEY, 1994] Michael Sean Mahoney. *The Mathematical Career of* PIERRE *de* FERMAT *1601–1665*. Princeton Univ. Press, 1994. 2nd rev. ed. (1st ed. 1973).

[PASCAL, 1954] Blaise Pascal. *Œuvres Complètes*. Gallimard, Paris, 1954. Jacques Chevalier (ed.).

[PRAUSE, 1986a] Gerhard Prause. *Niemand hat Kolumbus ausgelacht*. Econ Verlag, Vienna, 1986.

[PRAUSE, 1986b] Gerhard Prause. GALILEI war kein Märtyrer. 1986. In [PRAUSE, 1986a, pp. 167–187].

[SCHMIDT-SAMOA, 2006a] Tobias Schmidt-Samoa. An even closer integration of linear arithmetic into inductive theorem proving. *Electronic Notes in Theoretical Computer Sci.*, 151:3–20, 2006. http://www.ags.uni-sb.de/~cp/p/evencloser, http://dx.doi.org/10.1016/j.entcs.2005.11.020.

[SCHMIDT-SAMOA, 2006b] Tobias Schmidt-Samoa. *Flexible Heuristic Control for Combining Automation and User-Interaction in Inductive Theorem Proving*. PhD thesis, Univ. Kaiserslautern, 2006. http://www.ags.uni-sb.de/~cp/p/samoadiss.

[SCHMIDT-SAMOA, 2006c] Tobias Schmidt-Samoa. Flexible heuristics for simplification with conditional lemmas by marking formulas as forbidden, mandatory, obligatory, and generous. *Journal of Applied Non-Classical Logics*, 16:209–239, 2006. http://dx.doi.org/10.3166/jancl.16.208-239.

[STEPHEN, 1960] Marie Stephen. Monsieur FERMAT. *The Mathematics Teacher*, March 1960:192–195, 1960. ISSN 0025-5769.

[UNGURU, 1991] Sabetai Unguru. Greek mathematics and mathematical induction. *Physis*, XXVIII(2):273–289, 1991.

[WALSH, 1928] C. M. Walsh. FERMAT's Note XLV. *Annals of Mathematics*, 29:412–432, 1928.

[WEIL, 1984] André Weil. *Number Theory*. Birkhäuser (Springer), 1984.

[WIRTH, 2004] Claus-Peter Wirth. Descente Infinie + Deduction. *Logic J. of the IGPL*, 12:1–96, 2004. http://www.ags.uni-sb.de/~cp/p/d.

[WIRTH, 2005] Claus-Peter Wirth. History and future of implicit and inductionless induction: Beware the old jade and the zombie! 2005. In [HUTTER & STEPHAN, 2005, pp. 192–203], http://www.ags.uni-sb.de/~cp/p/zombie.

[Wirth, 2009] Claus-Peter Wirth. Shallow confluence of conditional term rewriting systems. *J. Symbolic Computation*, 44:69–98, 2009. http://dx.doi.org/10.1016/j.jsc.2008.05.005.

[Wirth, 2010] Claus-Peter Wirth. *Progress in Computer-Assisted Inductive Theorem Proving by Human-Orientedness and Descente Infinie?* SEKI-Working-Paper SWP–2006–01 (ISSN 1860–5931). SEKI Publications, Saarland Univ., 2010. Rev. ed. http://arxiv.org/abs/0902.3623.