Diophantus of Alexandria : a Text and its History

Norbert Schappacher*

April 2005

Abstract. Diophantus's *Arithmetica* is one of the most influential works in the history of mathematics. For instance, it was in the margin of his edition of Diophantus that Pierre de Fermat, some day between 1621 and 1665, wrote the statement of his so-called Last Theorem (which was proved only a few years ago). But Fermat was not the first to derive inspiration from Diophantus's collection of algebraic/arithmetic problems: the Arabs had profited from reading the *Arithmetica* when developing Algebra as a mathematical discipline. Nor was he the last: at the end of this paper we present the example of a Berkeley Ph.D. thesis of 1998 which is directly inspired by a problem of Diophantus.

But for all the influence that this author had on various mathematicians at various times, we know almost nothing about him, and even the text of the "Arithmetica" betrays very little of what Diophantus actually knew — or did not know.

We first present views of well-known historians who speculated on who Diophantus was, then go on to describe some salient features of the *Arithmetica*, and finally we survey the main different readings of this text that have been given over the centuries: first in the Arab world in the 9th and 10th century, and during the Byzantine Renaissance (11th to 13th century); then during the 16th and 17th century in Western Europe (Viète, Fermat), up to the 20th century way of looking at Diophantus.

The present text is a substantially enriched and reworked English version of my article "Wer war Diophant?" (*Mathematische Semesterberichte* **45/2** (1998), 141–156).

* I.R.M.A., 7 rue René Descartes, 67084 Strasbourg, France; `schappa@math.u-strasbg.fr`

Table of contents

1. Dating Diophantus. Two works have come upon us under the name of *Diophantus of Alexandria*: a very extensive collection of solved problems entitled "*Arithmetica*," and a short, more theoretical treatise on polygonal numbers, which is rather euclidean in style.[1] The *Arithmetica* are essentially *self-contained*: at least as far as we know them, they do not contain any explicit reference to other mathematical authors.[2]

On the other hand, we know of only one mathematician of the pre-Arabic and pre-Byzantine era who quotes from Diophantus's *Arithmetica*: *Theon of Alexandria*,[3] father of *Hypatia*, the best-known woman scientist of (late) antiquity, who however owes her fame not least to the fact that she was gruesomely murdered by street gangs of the Bishop and Early Father of the Curch Cyril in 415 AD.[4] Theon of Alexandria thus belongs to the middle of the fourth century AD, and this gives us an upper bound for the dating of the *Arithmetica*, and of their presumed author Diophantus.

If we accept, and we might as well, that the same Diophantus was indeed also the author of the treatise on polygonal numbers, then we obtain a lower bound because in this work there is a quote from *Hypsicles* who lived around 150 BC—see [Tannery 1893/95], vol. I, 470 (27).

The known works of Diophantus thus provide us with an interval of 500 years for their composition, and this is about all that we may be certain of when it comes to dating Diophantus of Alexandria. No reliable biographical information about him is available.[5]

The great French classical scholar (and mathematician) Paul Tannery (1843–1904), to whom we owe (among other standard works of reference

---

[1] For the treatise on polygonal numbers, see the Greek-Latin edition [Tannery 1893/95], vol. I, 450–481. Polygonal numbers are: triagonal numbers, i.e., numbers that can be arranged in triangular shape, like $1, 3, 6, 10, 15, 21, \ldots$, or perfect squares, or pentagonal numbers like $1, 5, 12, 22, 35, \ldots$, etc. Thus in general, the sequence of a-fold polygonal numbers is given by the rule $\frac{n}{2}\{2 + (n-1)(a-2)\}$, for $n = 1, 2, 3, \ldots$.

[2] At three places, which all occur in book "V" from the Byzantine tradition (see below for the numbering of the books) the text refers to "porisms": see [Tannery 1893/95], vol. I, 316 (6), 320 (2), and 358 (5). It is not clear whether these results were part of another book of the *Arithmetica* which is now lost, or if the references are to an independent treatise (by Diophantus, or simply known to Diophantus's intended readers?) of which no other trace has come upon us. See also our discussion of general statements in the *Arithmetica* in section 4. below.

[3] See [Tannery 1893/95], vol. II, 35 (9-11), cf. vol. I, 8 (13–15).

[4] The year 415 is undisputed. There are, however, diverging opinions about the age at which Hypatia met her tragic death. See for instance [Dzielska 1995]. Cf. the insightful discussion of the principal sources and speculations about Hypatia, which in particular tries to reconstruct her writings, her teachings, and the political reasons for her murder, in [Cameron & Long], pp. 39–62.

[5] Note that, even though such an uncertainty of dates may seem enormous for the historic mediterranean cultures, in the history of Indian culture and science, for instance, even larger intervals of uncertainty are the rule rather than the exception—see for example [Gupta 1995], p. 263f.

of the time—see for instance his [Fermat]) the monumental critical edition [Tannery 1893/95] of the six books of the *Arithmetica* which we have from the Byzantine tradition, discovered in the library of the Escurial a letter of the Byzantine intellectual Michael Psellus[6] which has been used to date Diophantus more precisely—see [Tannery 1893/95], vol. II, 37–42. In this letter, Psellus mentions work on arithmetic (the "Egyptian method of numbers," as he calls it) by a certain Anatolios which was dedicated to Diophantus.[7] Tannery identified this author with the historically known Anatolius of Alexandria, a philosopher who was the Bishop of Laodicea (an ancient town on today's Syrian coast) around 270/280 AD, and who was indeed the author of a treatise on arithmetic of which we have fragments. Assuming a treatise can be 'dedicated' only to a person still alive, this would put Diophantus in the third century AD.

But considering the late date and the nature of the Psellus source (the sentence itself which mentions the dedication is slightly corrupt in the manuscript), one may want to be sceptical about these conclusions. It actually seems that Tannery got somewhat carried away with this letter that he had discovered; he used it as his only basis for emending the single most important methodological statement of the *Arithmetica*, in which Diophantus introduces his symbol for the one and only unknown that he can handle in his notation.[8]

Still, independently of the Psellus letter, the fact that, as far as we know, nobody before Theon mentions Diophantus, and also the fact that the problems of the *Arithmetica* are rather unusual in classical Greek mathematics, make it probable that Diophantus wrote his works rather towards the end of the 500 year interval. Today, he is generally said to have lived around 250

---

[6]   Michael Psellus, 1018–1081(?), was for many years a philosopher at the court of Byzantium and authored a great number of works on a broad variety of subjects, from philosophy and theology to the sciences and alchimy. Aside from numerous letters he was maybe best known for his Lives of various Emperors and politicians, which take a psychological approach to the personalities portrayed. He liked to present himself as influential although he and his group lost their leading position under Constatin IX in 1054. At times he lived as a monk.

[7]   See [Tannery 1893/95], vol. II, 38 (22) – 39 (1). But see also Knorr's criticism of Tannery's treatment of Psellus's sentence in [Knorr 1993], 184.

[8]   See [Tannery 1893/95], vol. I, 6 (3–5). Instead of leaving this sentence as it reads in all the manuscripts, i.e., as defining the $\alpha\lambda o\gamma o\varsigma \ \alpha\rho\iota\theta\mu o\varsigma$, the *untold number*, the number which is as yet unknown, to be "what has none of these special properties [that were discussed in the preceding lines, like the property of being a square, cube, etc.], but simply holds some multitude of units," Tannery wanted us to read (in Yvor Thomas's English translation, [Thomas 1941], p. 523): "The number which has none of these characteristics, but merely has in it an undetermined multitude of units, is called *arithmos*." But the untranslated last word of the Greek sentence that Tannery created simply means 'number,' thus rendering the statement at least very awkward. This criticism of Tannery's 'correction' of the crucial sentence was made in a very convincing way by Rashed and Allard—see the note on the Arabic word for the unknown, "šay", in [Rashed 1984], tome III, 120–123.

AD, as Tannery's argument suggested. There is also a mathematical papyrus in Greek from the third century, not by Diophantus, but which uses the same symbol for the unknown that we also find in the Byzantine manuscripts of the *Arithmetica*.[9]

But one ought not to forget the basic uncertainty in all these conjectures. In fact, a lot can be and has been said in favour of relating Diophantus closely to *Heron of Alexandria*, a fairly encyclopedic author of texts on questions of mathematics, and in particular on applications of mathematics. Heron also discusses problems similar to those of Diophantus, and both use the same notation for the minus sign. If one assumes a close relationship between the two, one may even wonder, as Sir Thomas Heath did, whether the *Dionysius* to whom the *Arithmetica* are formally addressed was maybe identical with the addressee Dionysius of Heron's book on Geometric Definitions and of his Elements of Arithmetic.[10] The dates of Heron, after having been hotly debated for a long time and in a large interval, are today usually considered to have been settled by Neugebauer who computed the date of a certain lunar eclipse in Rome which is mentioned in Heron's treatise on the diopter in the context of a determinantion of the distance between Alexandria and Rome; according to Neugebauer, Heron was alive in 62 AD.[11] One may — such is the inherent uncertainty of the history of hellenistic science — doubt even this dating because it rests on the assumptions that Heron himself put the reference into the text, and that the event described was a contemporary event for him. These assumptions could well both be wrong; Heron's texts are known to have been greatly modified and extended over the centuries. But if we are not so sceptical and suppose that Heron has indeed lived in the first century AD, should this not lead us to place Diophantus up to two centuries earlier than is generally done today?

A little mathematical poem which claims to be the inscription on Diophantus's tomb almost strikes me as a parody of our ignorance. It determines the length of Diophantus's life by a linear equation to 84 years.[12] There are

---

[9]   Pap. Michigan 620. I owe this reference to [Gericke 1984], p. 143.

[10]   Wilbur Knorr has recently argued that both these treatises usually attributed to Heron are in fact due to Diophantus. See [Knorr 1993], esp. pp. 184–186; an exciting paper to read which, however, does of course not settle the matter conclusively. — For earlier accounts of the relation between Heron and Diophantus, see [Heath 1921], p. 306, note 1, as well as the long footnote 149 in [Klein 1992], 244–248.

[11]   Neugebauer's argument was published in 1938, after Heath and after the original German version of Klein's book. See [Neugebauer 1975], p. 846f. I thank Menso Folkerts for pointing out Neugebauer's paper to me in a letter.

[12]   See [Tannery 1893/95], vol. II, 60f. In Y. Thomas's translation [Thomas 1941], p. 513: *This tomb holds Diophantus. Ah, what a marvel. And the tomb tells scientifically the measure of his life. God vouchsafed that he should be a boy for the sixth part of his life; when a twelfth was added, his cheeks acquired a beard; He kindled for him the light of marriage after a seventh, and in the fifth year after his marriage He granted him a son. Alas! late-begotten and miserable child, when he had reached the measure of half his*

obituary notices also for Nicolas Bourbaki. So this poem need not deter anyone from speculating that 'Diophantus' was in fact the name of a collective author. On the other hand, there is no positive reason to embark on such a speculation, and most of all: I do not see how any of the difficult questions related to Diophantus would thereby become easier to answer.

2. Speculations on Diophantus's origins. Just as the precise dates of his life, Diophantus's ethnic or religious affiliation is open only to speculations. The possibility to speculate has been extensively used by many authors. Let us give some examples:

Hermann Hankel in his work on the history of mathematics in ancient and medieval time, adopts an almost poetic tone when he comes to Diophantus:[13]

> Here, in the midst of this sad and barren landscape of the Greek accomplishments in arithmetic, suddenly springs up a man with youthful energy: Diophantus. Where does he come from, where does he go to? Who were his predecessors, who his successors? We do not know. It is all one big riddle. He lived in Alexandria. If a conjecture were permitted, I would say he was not Greek; ... if his writings were not in Greek, no-one would ever think that they were an outgrowth of Greek culture....

Around the same time, the German historian of mathematics **Moritz Cantor**[14] confessed that, to him,

---

father's life, the chill grave took him. After consoling his grief by this science of numbers for four years, he reached the end of his life. It is a poem from the *Anthologia Palatina* of mathematical problems in poetic garb. The interpretation which Harder admits in [Harder 1995], 267f, to the effect that the solution is $65 + \frac{1}{3}$ years rather than 84 is compatible with the German translation that Harder uses, but not with the Greek original.

[13]   [Hankel 1874], 157. The original German quotation reads: *Da mitten in dieser traurigen Oede [der griechischen Leistungen im Bereich der Arithmetik] erhebt sich plötzlich ein Mann mit jugendlicher Schwungkraft: Diophant. Woher, wohin, wer sind seine Vorgänger, wer seine Nachfolger? — wir wissen es nicht — alles ein Räthsel. ... Er lebte in Alexandrien; sein Geburtsland ist unbekannt; wäre eine Conjectur erlaubt, ich würde sagen, er war kein Grieche; vielleicht stammte er von den Barbaren, welche später Europa bevölkerten; wären seine Schriften nicht in griechischer Sprache geschrieben, Niemand würde auf den Gedanken kommen, daß sie aus griechischer Cultur entsprossen wären...* — Hankel is of course also remembered as a mathematician, for instance for his integral for the gamma function (Habilitationsschrift Leipzig 1863), and by his "Untersuchungen über unendlich oft oscillierende und unstetige Funktionen," Math. Annalen **20**, 1882.

[14]   [Cantor 1907], 396. The first edition of Cantor's work dated from 1880. — *Diophant mit seinem in Griechenland mehrfach vorkommenden Namen [war] wirklicher Grieche, Schüler griechischer Wissenschaft, wenn auch ein solcher, der weit über seine Zeitgenossen hervorragt, Grieche in dem, was er leistet, wie in dem, was er zu leisten nicht vermag. Eines wollen wir dabei keineswegs ausgeschlossen haben ...: daß nämlich die griechische Wissenschaft, wie sie von Alexandria aus nach Westen und nach Osten erobernd vordrang ... von den gleichen Eroberungszügen auch neuen Werth an Ideen mit nach Hause brachte, dass die griechische Mathematik als solche nie aufgehört hat, sich anzueignen, was sie da oder dort Aneignenswerthes fand.*

Diophantus, with this name which is frequent in Greece, was a true Greek, disciple of Greek science, if one who towers high above his contemporaries. He was Greek in what he accomplished, as well as in what he was not able to accomplish. But we must not forget that Greek science, as it conquered the East from Alexandria ..., brought new ideas back home from these campaigns, that Greek mathematics as such has never ceased to pick up whatever it found worth picking up here and there.

Paul Tannery himself did not speculate on the ethnic origin of Diophantus. However, he suggested one may identify that Dionysius to whom the *Arithmetica* are addressed as Dionysius, Bishop of Alexandria, and deduce from this that Diophantus was christian.[15]

For **Oswald Spengler**, the author of the most successful, and terribly politically influential German book of the 1920s: "Der Untergang des Abendlandes", "The Decline of the Occident," Diophantus was a crucial indicator of the change of culture that, according to Spengler, took place in late antiquity. Much like Toynbee after him, Spengler undertook a parallel, cyclic description of the big cultures of world history, in each of which he claimed to be able to recognize the same morphological developments. Spengler battled the idea of universally valid mathematics. For him, the mathematics developed by a culture are a particularly telling indicator of the type of this culture. Late antiquity for him was no longer part of the classical culture, but belonged already to the Arab culture which, according to Spengler, was characterized by the *magisches Weltgefühl*, the magic apprehension of the world. This culture would later on find its religion in Islam. The Pantheon in Rome for instance was thus diagnosed by Spengler as "the earliest of all mosques."

Now, Diophantus's *Arithmetica* stand out because of their formal, algebraic rather than geometric treatment of quantities, which prompts Spengler to comment:[16]

This is indeed not an enrichment, but a complete negation of the *Weltgefühl* of antiquity. This alone should have sufficed to prove that Diophantus is no longer part of classical culture. A new *Zahlengefühl*, a new notion of number ... is at work in him. What an *undetermined* number a, an *unnamed* number 3 is—both neither

---

[15] See [Tannery 1912], 527–539. Cf. [Knorr 1993], 187.

[16] [Spengler 1923], 96–97. — *Das ist allerdings nicht eine Bereicherung, sondern eine vollkommene Überwindung des antiken Weltgefühls, und allein dies hätte beweisen sollen, daß Diophant der antiken Kultur nicht mehr angehört. Ein neues Zahlengefühl ... ist in ihm tätig. ... Was eine* unbestimmte *Zahl a und was eine* unbenannte *Zahl 3 ist — beides weder Größe, noch Maß, noch Strecke — hätte ein Grieche gar nicht angeben können. ... Diophant lebte um 250 n. Chr., also im dritten Jahrhundert der arabischen Kultur.*

quantity, nor measure, nor line segment—a Greek would have not been able to say. ... Diophantus lived around 250 AD, i.e., in the third century of Arab culture.

Spengler, who must have had his own way of recognizing truly great works, unperturbed by detailed mathematical scrutiny, had his personal view on the mathematical qualities of Diophantus; he would not let himself be impressed by a collection of tricky problems that have but inspired later writers:[17]

> To be sure, Diophantus was not a great mathematician. Most of what his name stands for is not in his writings, and what there is, is surely not quite his own invention. His accidental importance lies in the fact that, as far as we know, he was the first in whose works the new *Zahlengefühl* is recognizable beyond any doubt.

Diophantus being a clear representative of the new, 'magic' culture, Spengler even proceeded to make him comply racially with this role. While Spengler categorized the philosopher Spinoza as the "latest representative of the magic *Weltgefühl*, in fact a latecomer," for the simple reason that "he came from the ghetto," i.e., since he was Jewish,[18] he turned this argument around in the case of Diophantus, whom he had already introduced as the first representative of the magic *Zahlengefühl*, forgetting even that he had previously said that Diophantus was not a great mathematician:[19]

> How many of the great Alexandrians may have been Greek only in the *magic sense*? Were Plotin and Diophantus maybe of Jewish or Chaldaic origins?

David M. Burton. The most absurd statement about Diophantus's origins that I have been able to find generously conflates different historical eras and transposes the often conjectured influence of Babylonian problems on those found in the *Arithmetica* into ethnic categories. In "Burton's History of Mathematics" from 1991 one reads:[20]

> Diophantos was most likely a Hellenized Babylonian.

---

[17]   [Spengler 1923], 98/99. — *Nicht als ob Diophant ein großer Mathematiker gewesen wäre. Das meiste, woran bei seinem Namen erinnert wird, steht nicht in seinen Schriften, und was darin steht, ist sicherlich nicht ganz sein Eigentum. Seine zufällige Bedeutung liegt darin, daß — nach dem Stande unseres Wissens — bei ihm als dem ersten das neue Zahlengefühl unverkennbar vorhanden ist.*
[18]   Cf. [Spengler 1923], 391. Cf. the sarcastic comments on this passage by Leonard Nelson in [Nelson 1921], 115–117.
[19]   [Spengler 1923], 770. — *Wie viele unter den großen Alexandrinern mögen aber Griechen nur im magischen Sinne gewesen sein? Waren Plotin und Diophant vielleicht der Geburt nach Juden oder Chaldäer?* — The Chaldaic dynasty, the last Babylonian dynasty, as of 626 BC, consisted of Aramaic families that were generally respected as learned people.
[20]   [Burton 1991/95], 223.

3. ... and the mathematical text ? All these quotes use the absence of biographical information in order to make metaphorical statements about the *Arithmetica* by way of speculating on the origin of their author. I claim that the same phenomenon which we see here with respect to Diophantus's biography repeats itself with respect to his mathematics. The *Arithmetica* are almost as elusive as their author. The way in which mathematicians through the centuries have read and used the *Arithmetica* is always a reliable expression of their proper ideas; but never can we be sure of what these readings tell us about the text itself. The *Arithmetica* are probably the most striking example of a mathematical text which, on the one hand, has inspired, and continues to inspire, generations of mathematicians at various different moments of the history of algebra and number theory; but which, on the other hand, has never, for all that we know, be developed further as such.

At least mathematicians tend to find it hard to admit this. We are convinced, are we not, that, if we peruse the text sufficiently carefully, we can practically look over Diophantus's shoulder while reading the *Arithmetica*. But this text, with its unique history of different readings over the centuries, provides a particularly good example to demonstrate the problems of this naively optimistic mathematical attitude.

I will thus succinctly survey four major historic occasions on which a group of mathematicians or learned people rediscovered the *Arithmetica*. In fact, since we have no original parts of the text, nor any direct knowledge of what happened to it between its first writing and the 9th century AD, all we can talk about are *re*-discoveries of a text that had slipped into oblivion. Such a rediscovery may conveniently be called a *renaissance of Diophantus* for the time and place where it occurs. I will suggest that there were four major such renaissances of Diophantus so far, or more precisely, two times two. All the parts of the *Arithmetica* which we possess today go back no further than to the first double renaissance, the two chapters of which took place in Bagdad, resp. in Byzantium, between the ninth and the thirteenth century. The twofold second renaissance comprises the appropriation of the *Arithmetica* in Europe and the Western world as of the sixteenth and seventeenth century.

4. A few observations on the text of the *Arithmetica.* Before turning to the first renaissance and its two chapters, however, let us try to take a brief look at "the text itself." Of course, strictly speaking, this is impossible. There is no original text of Diophantus which has not somehow passed at least through the first double renaissance. And from the main thesis I am defending here it should be clear that I have no illusions whatsoever about

the feasibility of "simply reading the text."[21]

This being said, one does of course have to look at it. And the reader of Diophantus then finds himself in a situation somewhat analogous to that of Hardy and Littlewood when they were perusing Ramanujan's manuscripts sent to them from India.[22] Both texts clearly show a virtuoso author who is able to solve problems some of which, in the case of Diophantus, are not easy to solve today for, say, a good first year university student of mathematics. For Ramanujan the level is of course even higher. But both texts are also written in a way very different from what we are used to, and, above all, they contain notoriously few hints at the underlying general methods that the author has employed to find his solutions. This makes it extremely hard to pin down explicitly "what he knew."

But it will be convenient for the reader if we briefly point out a few properties of the *Arithmetica* which are good to have in mind when looking at the further voyage of this text through history.

Let us take as a very easy example problem I.28: *Find two numbers whose sum and the sum of whose squares are given numbers.* The context reveals that by "number" Diophantus always means: positive rational number. Before solving this problem, Diophantus states a necessary condition: *twice the sum of the squares minus the square of the sum of the two numbers has to be a square* (of a positive rational number).

Nowadays, using algebraic notation and knowledge which dates back at most to the sixteenth century, we would probably reconstruct this somewhat like this: We look for X and Y such that $X + Y = a$ and $X^2 + Y^2 = b$. Then $2b - a^2 = (X - Y)^2 = (Y - X)^2$ does indeed have to be a square. And a moment's thought shows us today that this condition is also sufficient; for $Y = a - X$ transforms $X^2 + Y^2 = b$, divided by 2, into the quadratic equation

$$X^2 - aX + \frac{a^2 - b}{2} = 0 \quad \text{of discriminant} \quad \frac{2b - a^2}{4}.$$

If we want, we can then find the two rational solutions of this equation expressed in terms of a and b, from the formula we have learnt at school.

Diophantus has no such notation, nor was there any general notion or theory of quadratic equations that he could have been taught at school. It is also not completely clear whether he understands his necessary condition (which is clearly stated as such) in fact as a necessary and sufficient condition

---

[21]   Note the subtle way in which André Weil seems to indirectly acknowledge this problem in his book [Weil 1983]: his brief chapter on Diophantus is placed in Chapter I: "Protohistory" (§X, pp. 24–29). This allows Weil to treat Diophantus essentially by way of various looks cast back on the *Arithmetica* from later developments of number theory.

[22]   I am indebted to Don Zagier for this nice comparison.

for the solubility of the problem.[23] All he does is 'solve the problem,' and here is what 'solving' means for him: first he chooses the value 20 for what we have called a, and he chooses the value 208 for what we have called b. (Note in passing that $2 \times 208 - 20^2 = 4^2$ is indeed a perfect square, so the necessary condition is respected.)

Then Diophantus proceeds to use his only notation for one (and only one at a time) unknown quantity.[24] Following Tannery, let us write x for this unique unknown that Diophantus can handle notationally. Diophantus then writes the difference of the two numbers (the bigger one minus the smaller one) in the form $2x$. In other words, $x + 10$ will be the bigger, and $10 - x$ the smaller of the two numbers we want. Then, noting explicitly that 10 is half the first given sum, this leaves him with the following equation:[25]

$$208 = (x + 10)^2 + (10 - x)^2 = 2x^2 + 200.$$

Note that it very conveniently does not have a linear term, and therefore immediately yields $x^2 = 4$, i.e., $x = 2$ since only positive solutions are allowed by Diophantus. The two numbers sought are then 12 and 8.

A generous mathematician's way of reading this 'solution' would be to say that Diophantus shows here a general method to deal with quadratic equations, and it is only his restricted notation which does not allow him to spell things out in appropriate generality. He is thus led to choose more or less generic values for the constants, and also for those unknowns which are not covered by x.

It is true that Diophantus commands the technique of choosing numerical values to perfection, never losing sight, even in the most involved problems, of which choices have been made at which stage of the argument, and not hesitating to go back and correct such a choice if it becomes apparent that it would lead him to an irrational or negative solution of the principal problem, or of some auxiliary problem along the way.[26]

---

[23] The necessary conditions stated for other problems of the *Arithmetica* tend to be necessary and sufficient to insure the general solvability of the problem as stated in positive rational numbers. But at times the divergence of the generality of the statement and the particularity of the given solution make the logic more involved. The first such instance occurs with problem I.21, and was already remarked as such by Bachet. Cf. also footnote 34 below.

[24] According to a generally accepted hypothesis of Heath's, his sign for this was probably originally a contraction of the first two letters, $\alpha\rho$, of the Greek word for number, $\alpha\rho\iota\theta\mu o\varsigma$.

[25] To be quite precise, for Diophantus what we write as $+$ and $-$ are not on the same footing: addition of terms he handles by simple juxtaposition, and in every expression all terms prefixed by a minus are collected together at the end.

[26] It also happens in the later books that Diophantus can actually use a quadratic equation for his unknown which, as he notes expcitly, has only an irrational solution for the deduction of a rational solution to the problem he is solving. See the four problems "IV".9 through "IV".12, [Tannery 1893/95], vol. I, 204, (19); 208, (7); 210 (1); and 212 (5) − (7), as well as problem "IV".31, "IV".32, [Tannery 1893/95], vol. I, p. 264f; 270, (5).

However, it is not clear whether Diophantus was aware, for instance, of a general notion of "quadratic equation." He does, in the later books, occasionally indicate more or less general recipes for handling various types of quadratic equations.[27] But the only overriding principle that he seems to have at heart is a ranking of expressions according to *species*, i.e. essentially, according to powers of x, which occur in them, with a view to transforming the equations at hand in such a way that one is finally left with an equation between two multiples of the same power of x—see the explanations in the introductions to books I and IV.[28]

And yet more seriously, one begins to suspect that there may be more to those 'generic choices' of numerical values than our understanding with its anticipated generality made us guess at first sight, when it comes to what we call indeterminate problems, i.e., problems that do not, like the previous one, have a unique solution in positive rational numbers. In fact, in most cases there is nothing in Diophantus's usual treatment of indeterminate problems that shows any difference from the case of determinate problems. Once a single solution in positive rational numbers is obtained, the problem is considered done and Diophantus moves on to the next one.

Let us take as example the famous problem II.8, in the all too narrow margin of which Fermat inscribed the statement (but not his would-be wonderful proof) of what came then to be called "Fermat's Last Theorem."[29] The problem reads: *Partition a given square into two squares.* Diophantus takes the given square to be 16, and writes the first square of the required partition as x^2. He therefore has to make $16 - x^2$ a square, which we might write y^2 in our modern notation. In order to do this, Diophantus will use the *Ansatz*: $y = 2x - 4$. This works well because $x^2 + y^2 = 16$ then becomes $5x^2 = 16x$, i.e., $x = \frac{16}{5}$, and we have divided 16 into the sum of the two squares $\frac{256}{25}$ and $\frac{144}{25}$.

---

[27] See in the first place "IV".39, [Tannery 1893/95], vol. I, 304, (5) − (10), for an instance of $bx + c = ax^2$. Similarly "VI".6, in particular [Tannery 1893/95], vol. I, 402, (14) − (16), for an instance of $ax^2 + bx = c$. Cf. also the remark in "VI".22, [Tannery 1893/95], vol. I, 444, (23) − (24), on an equation of type $bx = ax^2 + c$.

[28] See the end of the introduction to book I, [Tannery 1893/95], vol. I, 14 (11ff), which is taken up again in the introduction to Book IV, [Rashed 1984], tome III, p. 2–3; cf. the commentary about the term species in [Rashed 1984], tome III, p. 104–105.

[29] Fermat's oft-quoted note reads: *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.* — That is: "To split a cube into two cubes, or a biquadrate into two biquadrates, or in general, to infinity, any power higher than the square into two powers of the same order, is impossible. Of this fact I have discovered a truly extraordinary proof. The exiguity of the margin would not hold it." — In one of the manuscripts, which dates from the 13th century, there is also a note in the margin of this same problem II.8, by an unhappy reader who curses Diophantus for the difficulty of his text—see [Tannery 1893/95], vol. I, 84, and [Tannery 1893/95], vol. II, 260.

This is a fair description of how Diophantus *usually* treats indeterminate problems, giving one special solution which depends on numerical choices and specializations made along the way. The fact that other linear substitutions $y = tx - 4$ would have yielded a solution to the original problem as well, tends not to be mentioned. Nor, to be sure, does he ever show any indication of being aware of the geometric interpretation of this or similar problems as that of finding rational points on a circle of rational radius, and of his operations, as intersecting the circle with the line $y = 2x - 4$.[30]

In the peculiar, exceptional case of problem II.8, however, there is one sentence which, for once, expresses greater generality: Before the substitution of $2x - 4$ for the root of the second square, we read: *Let us take the square of some multiple of x minus the number whose square makes 16.* In other words, it is suggested that any substitution of the form $tx - \sqrt{16}$ for y will yield a solution. And we seem to be referred back to this observation when we read later on, in problem III.19: *We have learned how to decompose the given square into two squares in an infinite number of ways.*[31]

It is well worth to dwell a bit on this problem III.19. In fact, in all the *Arithmetica* as far as we possess them today, III.19 is the most outspoken passage in the way of allusions to general mathematical facts around the decomposition of squares into two squares. But it is not theoretical in the sense of a systematic general treatise. It rather strikes us as a particularly virtuoso, surprising, and dense solution, which is interspersed with hints at general insights, a true 'Champagne Aria' among the problems of the *Arithmetica*. We may assume with Tannery that III.19 originally marked the end, and indeed the climax, of the first three books of the *Arithmetica*, which bring the art of Diophantus up to equations involving the square of the unknown.[32]

Problem III.19 itself is a mouthful, asking for eight conditions to be satisfied simultaneously: *Find four numbers such that the square of the sum of all four, plus or minus any one of the numbers, is a square.*

---

[30]   Examples of indeterminate problems in the *Arithmetica* which Diophantus treats in such a way that they become definite abound—see for instance the group of problems II.21, II.22, II.23, II.25.

[31]   [Tannery 1893/95], vol. I, 184 (3–4). Here and in the following discussion of III.19, I translate, resp. paraphrase, myself directly from the Tannery edition. — Note that Diophantus does not give any explicit reference to an ealier problem here, nor does he ever take the time to actually prove that infinitely different choices of what we have called t in our discussion of II.8 do indeed produce infinitely many different partitions of the given square.

[32]   See [Tannery 1893/95], vol. I, p. 187, footnote, where it is suggested that the two subsequent problems III.20 and III.21, which mark the end of book III in the manuscripts, are later additions. If we discuss III.19 in detail, we do so assuming, at least for the sake of the argument, that this problem and its solution is indeed an original part of the *Arithmetica*.

Diophantus's solution of this problem starts with a general observation which, for once, is not a necessary condition, but presents a preliminary problem to which the given one will be reduced: *Since the square of the hypotenuse of any right triangle, plus or minus twice the product of the two sides around the right angle, makes a square, I first look for four right triangles that have the same hypotenuse.* In modern terminology, Diophantus proposes to look for four different (positive rational) solutions to

$$(\triangle) \qquad\qquad a_i^2 + b_i^2 = c^2 \qquad (i = 1, 2, 3, 4)$$

because then he will have, for $i = 1, 2, 3, 4$, that $c^2 \pm 2a_i b_i = (a_i \pm b_i)^2 =$ a square.

Having stated this auxiliary problem in terms of right triangles, Diophantus immediately goes on to remark that this is really the same as what the reader is supposed to know, for instance from II.8: *This is the same as decomposing a given square into two squares [in four ways], and we have learned how to decompose the given square into two squares in an infinite number of ways.*[33] But this sentence, the way it is inserted here into the solution of III.19, is a mere aside; we will see how Diophantus will actually go about finding a concrete solution to the auxiliary problem without directly invoking the method of II.8. Does this maybe suggest that the infinitely many solutions whose existence we may be sure of, are not as such easy to make explicit for Diophantus, or at least that he finds it too difficult for pedagogical reasons to follow this approach here? Or is it merely the overflowing abundance of ideas of the true virtuoso which prompts him to solve the auxiliary problem in another way?

Be that as it may, having made his general observation, here is how Diophantus actually solves his auxiliary problem:

> *So let us now exhibit two right triangles on smallest numbers, namely (3,4,5), (5,12,13), and multiply all sides of each triangle with the hypotenuse of the other triangle; then the first triangle becomes (39,52,65), the second (25,60,65). These are right [triangles] having the same hypotenuse. But 65 is naturally partitioned into squares in two ways; as 16 plus 49, and as 64 plus 1. This is so because the number 65 is the product of 13 and 5, and each of these can be decomposed into two squares. I now take the roots of the said 49 and 16, i.e., 7 and 4, and form the right triangle from the two numbers 7 and 4: (33,56,65). Similarly, 64 and 1 have the roots 8 and 1; so I form again a right triangle, from these numbers, whose sides are (16,63,65).*

---

[33]   [Tannery 1893/95], vol. I, 184 (1–4). Our parenthesis *[in four ways]* indicates a slight insecurity in the text which, however, causes no trouble for understanding the sentence.

There are several general facts used or alluded to in this passage. First, Diophantus knows how to systematically produce right triangles with integer sides. More precisely, given positive integers, in our notation $p > q$, he knows how to, as he he calls it, "form the right triangle from these numbers," i.e., in our notation, he knows how to write down the right triangle $(p^2 - q^2, 2pq, p^2 + q^2)$ (or with the two first sides permuted), and also multiples $((p^2 - q^2)\lambda, 2pq\lambda, (p^2 + q^2)\lambda)$ of it. Such a *forming* of right triangles from two numbers is what is treated nowadays—apparently as a late echo of a historical attribution made in the fifth century AD by Proclus—under the name of 'pythagorean triples.' This basic technique is used by Diophantus in many places, in particular in the problems of book "VI". It is by no means surprising to find such knowledge in Diophantus, given that the famous Babylonian tablet Plimpton 322 which is believed to be certainly not more recent than 1600 B.C. already contains a list of fifteen 'pythagorean triples.'[34] But note that it is not evident from the text of the *Arithmetica*, whether Diophantus knew that *all* right triangles with rational sides can be obtained in this way (a fact which we 'simply' like to see today as the parametrization of the rational points on the unit circle via stereographic projection from a chosen rational point P: the rational points on the unit circle are the second points of intersections with the circle of lines with rational slope passing through P). This kind of statement, aiming at exhausting all solutions of a problem, seems in fact alien to the very style of Diophantus's problems.

The other striking observation in the text at hand is the remark about 65 being the sum of two squares in two different ways, because it is the product of the two integers 5 and 13, each of which is the sum of two squares. This indicates knowledge on the multiplicativity of the property of being decomposable into two squares, i.e., something like what we would indicate by the formulae[35]

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (bc - ad)^2 + (bd + ac)^2.$$

Such knowledge in Diophantus seems more remarkable than that about constructing right triangles.

At any rate, following this ingenious play with different right triangles, Diophantus has now at hand, as he says, *four right triangles having the same hypotenuse.* Or in terms of what we called $(\triangle)$: $65^2 = 33^2 + 56^2 = 16^2 + 63^2 = 39^2 + 52^2 = 25^2 + 60^2$. So he may continue: *Let us therefore go back to the original problem. I put the sum of the four numbers equal to $65x$, and the individual ones equal to x^2 times four times the areas of the triangles.*

---

[34]   See for instance [Weil 1984], p. 8f.
[35]   See also [Weil 1983], p. 24f.

Let us transfer this to our general setup: Suppose we have found c and the four pairs (a_i, b_i) satisfying $(\triangle)$. Note in passing that Diophantus's *four times the area of the right triangle* (a_i, b_i, c) is precisely the quantity $2a_i b_i$ which, when added to or deducted from c^2, each time makes a square. Now, there is of course no reason to assume that we will also have $c = 2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3 + 2a_4 b_4$, as we would wish in order to solve the original problem. So, Diophantus suggests that we scale the four triangles: we may multiply all a_i, b_i, c by the same factor x, and still have four solutions to the homogeneous equation $(\triangle)$. Then, all we have to do is to choose x such that $(2a_1 b_1 + 2a_2 b_2 + 2a_3 b_3 + 2a_4 b_4)x^2 = cx$. This is achieved by the rational value $x = \frac{c}{2(a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)}$, and thus we obtain a solution to the original problem.

This is what Diophantus executes for his numerical values.[36] The solution of the original problem that he thus winds up with is given by the four numbers $\frac{17136600}{163021824}$, $\frac{12675000}{163021824}$, $\frac{15615600}{163021824}$, and $\frac{8517600}{163021824}$.

To sum up: the disparity between the general formulation of problems and certain restrictive conditions, as well as some very rare general comments on the one hand, and the particularity of the presented solutions on the other, make it hard if not impossible to judge with any kind of precision the 'theoretical' algebraic knowledge that Diophantus had at his disposal. There is also never a statement to the effect that *all* solutions of a problem have been found.[37]

If one just looks for statements or general methods described as such in the *Arithmetica*, there are some to be found in the introductions to books I and IV. For instance, Diophantus gives the abstract rule for handling the 'minus'-operation ($\lambda\epsilon\iota\psi\iota\varsigma$): in our notation, $(-) \cdot (-) = +$.[38] Furthermore,

---

[36] See the end of his solution to III.19, [Tannery 1893/95], vol. I, 186 (1) – (9). Note that the editors' corrections of some of the numbers in this final passage of III.19 appear to be straightforward.

[37] Bašmakova, who is always ready to attribute advanced knowledge to Diophantus of which there is no explicit trace in the text, draws up a list of more general solutions of problems in the *Arithmetica* [Bašmakova 1974], 40–42. Apart from III.19 just cited, she quotes four problems of book "IV" which are to be solved *in indeterminato* ($\epsilon\nu$ $\tau\omega$ $\alpha o\rho\iota\sigma\tau\omega$): "IV".19, "IV".33, lemma, "IV".34, lemma, "IV".35, lemma. Here we find indeed that the text explains one-parameter families of solutions, but a careful analysis of the text would have to try to explain: why here and not elsewhere? Finally, Bašmakova quotes from the book "VI", which treats primarily problems involving rational right triangles, a domain where we have already seen that the *Arithmetica* contain statements that go beyond particular solutions to indeterminate problems. First she points to "VI".11, second lemma, which does make an infinity claim which is reduced to those listed before. And then she mentions the "lemma" preceding problem "VI".15, which according to Bašmakova has a "much more general character" than the other quotes. But as a matter of fact, Diophantus treats it by specialization as usual, concluding once a special solution is found.

[38] [Tannery 1893/95], vol. I, 12 (19–21).

within the problems, some more or less general approaches are given special names; for example, the double equation ($\delta\iota\pi\lambda o\iota\sigma o\tau\eta\varsigma$), in our notation:[39]

$$x + a = u^2$$
$$x + b = v^2$$

where Diophantus tries to write $a - b = u^2 - v^2 = pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$.

Roughly 15% of the approximately 300 problems that we currently know of the *Arithmetica* contain so-called *diorisms*, i.e., necessary conditions like the one on $2b - a^2$ being square which we encountered in our first example, II.8, above. Their generality tends to be close to that of the statement of the problem.[40] Among these are the six problems of whose necessary condition we read that "This is $\pi\lambda\alpha\sigma\mu\alpha\tau\iota\kappa o\nu$" (plasmatikon). Reading this reminds the modern mathematician of remarks of the sort "this is trivial," but who knows what this word held for Diophantus? A lot of ink has been spilled about this question. It may well be unanswerable.[41]

Finally, there is one famous diorism in which Diophantus may have recorded that a (squarefree) odd number can only be decomposed as a sum of two squares, if it has no factor of the form $4n - 1$. But the text in the

---

[39]   See for instance problem I.11 in [Tannery 1893/95], vol. I, 96 (8–14).

[40]   I am thinking of the following 46 problems, of which I put in brackets those which Sesiano, in his list [Sesiano 1982], 461–483, does not recognize as problems with diorisms: I.5, I.6, I.8, I.9, I.14, I.16, I.17, I.19, I.21, I.27, I.28, I.30; II.6, II.7, (III.16), (III.19) [see the discussion above]; IV.17, IV.18, IV.19, IV.20, IV.21, IV.22; V.7, V.8, V.9, V.10, V.11, V.12; (VI.21), VII.6, (VII.16), (VII.17), (VII.18); ("IV".7), ("IV".14), "IV".34, "IV".35; ("V".3 ["porism"]), ("V".5 ["porism"]), ("V".6, 2. lemma), ("V".7), ("V".8), "V".9, "V".11, "V".16 ["porism"]; "VI".11, 2. lemma.

[41]   The six problems are I.27, I.28, I.30; IV.17, IV.19; V.7. Already the various translations that have been proposed over the centuries give an idea of what one is up against: from Xylander's (1575) "effictum aliunde," and Nesselmann's (1842) "das läßt sich aber bewerkstelligen," via Tannery's (1893) "hoc est formativum", Heath's (1910) "This is of the nature of a formula (easily obtained)", Ver Eecke's (1959) "chose qui est figurative," Sesiano's (1972) "constructible," the spectrum goes all the way to Wertheim's (1890) "und man kann immer solche Zahlen als gegeben annehmen, daß diese Bedingung erfüllt ist," or Rashed's (1984) "Ceci est un problème convenablement déterminé." Probably the biggest obstacle to solving the problem lies in the fact that, as far as we know today, this word or its Arabic equivalent occurs only six times in the *Arithmetica* (and the text in the first Arabic occurence is also problematic), and it does *not* occur with many diorisms where we would expect it according to the interpretations given by Rashed ([Rashed 1984], tome III, 133–138) or Sesiano ([Sesiano 1982], 192). Ver Eecke—see [Ver Eecke 1959], p. 37, footnote—thought that these words are remarks made by some early reader of Diophantus, which slid into the text after copying. (But he could not know about the three occurences in books IV and V, from the Arabic translation discovered in the 1970s. And this translation is based on a tradition of the text of the *Arithmetica* which is different from the one that led to the Greek manuscripts we know.) In [Caveing 1997], 389–393, on the other hand, the Greek expression is used as evidence for a geometric background of Diophantus's algebra. (But serious doubts remain whether the jargon of a working mathematician is accessible to Caveing's refined philology.)

manuscripts is obviously corrupt. Jacobi tried to correct it (yielding, of course, the statement we would very much like to credit Diophantus with), and it is touching to see how he tries to reconstruct the way in which the original text may have been deformed by copists who were unable to understand its meaning.[42]

5. The first renaissance of Diophantus took place in the world of Islam; it began probably in the 70s of the ninth century. Qusṭā ibn Lūqā, a Greek christian whose mother probably called him Kostas, worked for the better part of his life as a translator and commentator at the court of Bagdad. Thus he also translated Diophantus from Greek into Arabic (and wrote a commentary which we do not have), probably the first seven books of the *Arithmetica*. The books IV through VII from this translation resurfaced around 1971 in the Astan Quds Library in Meshed (Iran) in a copy from 1198 AD.[43] It was not catalogued under the name of Diophantus (but under that of Qusṭā ibn Lūqā) because the librarian was apparently not able to read the main line of the cover page where Diophantus's name appears in geometric Kufi calligraphy.

This discovery, and the subsequent editions and translations by Roshdi Rashed and Jaques Sesiano substantially changed our view of the *Arithmetica*. Before, the six books of the *Arithmetica* which have come upon us through Byzantine copies (see below, the second renaissance of Diophantus) had been taken to be the first six books of the work.[44] But now we have to count them like this: I, II, III, "IV", "V", "VI". The first seven books of the *Arithmetica* are: the first three books I, II, III from the Greek sources, and then books IV through VII of which we have the Arabic translation. The remaining Greek books "IV", "V", and "VI" come somewhere between VIII

---

[42] Problem "V".9, [Tannery 1893/95], vol. I, 332 (17)–334 (2). See [Jacobi 1847]. His proposed corrected version reads: $\delta\epsilon\iota\ \delta\eta\ \tau o\nu\ \delta\iota\delta o\mu\epsilon\nu o\nu\ \mu\eta\tau\epsilon\ \pi\epsilon\rho\iota\sigma\sigma o\nu\ \epsilon\iota\nu\alpha\iota, \mu\eta\tau\epsilon\ o$ $\delta\iota\pi\lambda\alpha\sigma\iota\omega\nu\ \alpha\upsilon\tau o\upsilon\ \kappa\alpha\iota\ \mu^{\circ}\ \overline{\alpha}\ \mu\epsilon\iota\zeta\omega\nu\ \epsilon\chi\eta\ \mu\epsilon\rho o\varsigma\ \tau\epsilon\tau\rho\alpha\chi\eta\ \mu\epsilon\tau\rho\epsilon\iota\sigma\vartheta\alpha\iota\ \pi\alpha\rho\alpha\ \tau\eta\nu\ \overline{\alpha}\ \mu^{\circ}$. That is : "It is necessary that the given quantity be neither odd, nor that any part of twice the given quantity plus 1 be measured four-fold next to 1." This is meant, according to Jacobi, to express a necessary condition for 'twice the given quantity plus 1' being a sum of two squares. Jacobi also proves this necessary condition at length in a way which, he thinks, was accessible to Diophantus. Tannery's reconstruction of this difficult sentence expresses the (equivalent) condition that no *prime* divisor p of 'twice the given quantity plus 1' should be such that 4 divides $p + 1$. It has the advantage of leaving the word 'prime number,' which occurs in some manuscripts, intact. The same reading, without philological anlysis, had already been suggested by Fermat on mathematical grounds—see [Fermat II], p. 203f.

[43] See [Rashed 1984], cf. [Sesiano 1982].

[44] See for instance [Ver Eecke 1959], p. XII–XV, for a survey of different views concerning the part of the complete *Arithmetica* that the six Greek books were supposed to represent by various authors, before the discovery of the Arabic books. Ver Eecke even tries to convince the reader that no other books than those known in Greek ever existed in Arabic translation: p. XIVf.

and XIII, but we do not know where.

Qusṭā ibn Lūqā's translation was made about half a century after al-Khwārizmi had created, also in Bagdad, Algebra as a mathematical discipline, through his famous book. Now, al-Khwārizmi's book is the exact opposite of Diophantus's *Arithmetica* in that it is on the one hand more elementary, treating only linear and quadratic equations whereas Diophantus has a lot of problems involving cubes, and other higher powers up to x^9 occur. But the novelty (and other difference with Diophantus) of al-Khwārizmi lies in his extremely systematic treatment, aiming at a general classification of linear and quadratic equations, and at general methods of solving them which are established with proofs. Thus, by translating the *Arithmetica*, Qusṭā ibn Lūqā implanted them into an active scientific environment which was marked by a systematic development of the young discipline of algebra.

This not only meant that Diophantus's work was now occasionally referred to as his "Art of Algebra," and that Qusṭā ibn Lūqā used the new Arabic algebraic terminology for his translation. But the translation was read and used as inspiration by working mathematicians who had their own mathematical notions and interests to put it into place. Thus abū-Kāmil in Cairo, for instance, wrote a book on algebra hardly ten years after Qusṭā ibn Lūqā's translation, which discusses the existence of infinitely many solutions to equations which we recognize as defining conic sections, provided they admit at least one rational solution.[45]

And there was yet another line of research which began to be cultivated by mathematicians of the world of Islam during the second half of the tenth century, and for which Diophantus's problems were as interesting as they were *a priori* differently conceived: I mean *the number theoretic movement in Arabic algebra* which Roshdi Rashed in particular has drawn attention to and analyzed. This is usually described as the discipline which asks for solutions in (positive) integers, rather than, as Diophantus does, in (positive) rational numbers, of polynomial equations in two or more variables. This description is slightly awkward in that the rational solutions to a given equation in n variables (say, $x^3 + y^3 = 1$) correspond to integer solutions of the homogenized equation in $n + 1$ variables ($x^3 + y^3 = z^3$). So it is better to describe the difference between the algebraic and the arithmetic line of research differently. What strikes us in tenth century arithmetic, in contrast to Diophantus's *Arithmetica*, is the *new notion of unsolvability* that makes its appearance.

All problems in the *Arithmetica* are not only solvable but actually solved. Difficulties with the solvability in positive rational numbers, which naturally

---

[45] Here we follow Rashed's account in the chapter *Analyse combinatoire, analyse numérique, analyse diophantienne et théorie des nombres* of [Rashed 1997], in particular pp. 72–85. See also the literature quoted there.

come up in the course of the work, occur for Diophantus when an equation would lead either to a nonpositive, or to an irrational solution. These difficulties are systematically avoided by going back and choosing other numerical values for the data of the problem. Just as he never discusses systematically *all* solutions of a given problem, he also never proposes problems that have no solution in positive rational numbers.

But around 940 al-Khāzin refuted an argument that abū-M. al-Khujandī had proposed to show that the equation (in our notation) $x^3 + y^3 = z^3$ has no solution in positive integers, and this discussion was carried on further involving also Abdallāh ben Alī.[46] And it is also in al-Khāzin, and not in the *Arithmetica*, that we find the genuinely number theoretical problem which has become over the past 15 years among arithmetic algebraic geometers a favourite topic of lectures for a wider audience :

6. The Congruent Number Problem. *Decide whether a given square-free positive integer is a congruent number.*

Here are two equivalent ways to define congruent numbers :

Definitions. (1) A positive rational number k is called **congruent**, if there is a rational square d^2 such that both $d^2 + k$ and $d^2 - k$ are rational squares.[47]

(2) Equivalently, a positive rational number k is called **congruent**, if there exists a right triangle with rational sides—say a, b, c, with $a^2 + b^2 = c^2$—whose area is k, i.e., such that $k = \frac{ab}{2}$.

The second definition implies the first one because, for $d = \frac{c}{2}$, one finds

$$d^2 \pm k = \left(\frac{c}{2}\right)^2 \pm k = \left(\frac{a^2 + b^2}{4}\right) \pm \frac{ab}{2} = \left(\frac{a \pm b}{2}\right)^2.$$

To see that the first definition implies the second one, we may write $d^2 + k = u^2$ and $d^2 - k = v^2$ and set $a = u + v$ and $b = u - v$. Then $a^2 + b^2 = (2d)^2$, which we call c^2, and $ab = 2k$ as desired.

It was apparently by some such argument, and using knowledge about generating right triangles with integer sides, that al-Khāzin established the equivalence of both definitions of congruent numbers.[48] This type of problem and argument looks very diophantian at first sight.[49] And it certainly

---

[46]   See [Anbouba 1979], 136f; cf. [Rashed 1979], [Rashed 1997], 80–85.

[47]   This definition appears to be at the origin of the terminology; the three squares $d^2 - k, d^2, d^2 + k$ form a three term progression with step, or *congruum* k.

[48]   I have not seen al-Khāzin's text myself, but rely on [Rashed 1997], 82.

[49]   Recall for instance from section 4 above problem II.8, which taught us how to write a given rational square as a sum of two squares in arbitrarily many ways. And note that the big problem III.19, discussed at length in section 4 above, produces a rational square d^2 with respect to which four different numbers k have the congruent property from definiiton (1).

remains diophantian in spririt as long as one tries to produce congruent integers by listing right triangles with integer sides. The first congruent number which everyone encounters in this way is 6, the area of the right triangle with sides $(3, 4, 5)$. Checking that $k = 5$ is also congruent takes only marginally longer: it suffices to scale down by the factor 6 the triangle $(9, 40, 41)$ whose area is $180 = 5 \cdot 6^2$. An anonymous Arab manuscript[50] written before the year 972 contains a table yielding 34 congruent numbers k.

The novel aspect of the problem, the one which takes us beyond Diophantus, emerges as soon as one wants to show that a certain k—say, a squarefree positive integer—which has refused to show up in the tables is actually *not a congruent number*. That tabulating areas of integral right triangles is a poor guide to deciding the congruent number problem is probably felt by everybody who experiments with it. A particularly striking example was computed a few years ago by Don Zagier: $k = 157$ is a congruent number, but one has to wait very long indeed for it to show up in the tables, because the simplest rational right triangle with area 157 has the sides

$$a = \frac{6{,}803{,}298{,}487{,}826{,}435{,}051{,}217{,}540}{411{,}340{,}519{,}227{,}716{,}149{,}383{,}203}$$

$$b = \frac{411{,}340{,}519{,}227{,}716{,}149{,}383{,}203}{21{,}666{,}555{,}693{,}714{,}761{,}309{,}610}$$

$$c = \frac{224{,}403{,}517{,}704{,}336{,}969{,}924{,}557{,}513{,}090{,}674{,}863{,}160{,}948{,}472{,}041}{8{,}912{,}332{,}268{,}928{,}859{,}588{,}025{,}535{,}178{,}967{,}163{,}570{,}016{,}480{,}830} \cdot$$

I do not know whether the group of mathematicians with whom al-Khāzin was in contact also discussed would-be proofs of the fact that certain k are not congruent numbers. Leonardo di Pisa, better known as Fibonacci, in the first half of the 13th century, after having established that $k = 5$ is congruent in his *Liber quadratorum*, did ponder (in vain) the problem to show that $k = 1$ is not congruent. Number theoretical research from the World of Islam found its way into Fibonnacci's works, for instance via the direct exchange with the Arab speaking world that was practised at the Sicilian court of Frederic II. This exchange did not make Diophantus directly accessible to the Occident. But it did contribute to making the congruent number problem known in the West.

The theorem that 1 *is not a congruent number* is tantamount to saying that the area of a right triangle with rational sides can never be a square, or to the fact the equation $x^4 + y^4 = z^2$ has no solution in positive integers, so that it contains the special case $n = 4$ of the so-called Fermat's Last Theorem. It was first proved by Fermat with his technique of descent (*descente infinie*).[51] The Arab number theorists have opened up mathematics for this kind of

---

[50]   Translated and commented by F. Woepcke in Atti Accad. Pont. Nuovi Lincei **14** (1860–61), 250–259. — Here I quote from [Dickson 1923], p. 459.
[51]   The proof is sketched, and constitutes the only explicit sketch by Fermat of a proof

problem. In doing so they were surely inspired by Diophantus, but showed the way to a number theory which lies well beyond the *Arithmetica*.

The congruent number problem is still unsolved, although we today have a very simple and effective conjectural criterion for integers to be congruent, which is known to be necessary, and the sufficiency of which is a consequence of the famous Conjecture of Birch and Swinnerton-Dyer for a certain family elliptic curves over $\mathbf{Q}$. The starting point of this is the observation that congruent numbers (which up to scaling by rational squares may be assumed to be squarefree integers) may also be defined like this:

Definition. (3) A positive squarefree integer k is **congruent**, if the elliptic curve $E_k : y^2 = x^3 - k^2x$ has at least one rational point $(x, y) \in \mathbf{Q}^2$ such that $y \neq 0$.[52]

Now, if we knew the Conjecture of Birch & Swinnerton-Dyer for all elliptic curves $E_k : y^2 = x^3 - k^2x$, where k varies over all squarefree positive integers, then it would follow that such a k is a congruent number, if and only if $\sum(-1)^n = 0$, where the sum is taken over all possible ways of writing k in the form $\ell^2 + 2m^2 + 8n^2$ (if k is odd), resp. over all possible ways of writing $\frac{k}{2}$ in the form $\ell^2 + 4m^2 + 8n^2$ (if k is even), with integers ℓ, m, n. This criterion makes serious use of very recent developments in arithmetic algebraic geometry.[53] Enough has already been proved towards the Conjecture of Birch & Swinnerton-Dyer to ascertain that : if k is a congruent number, then the corresponding sum $\sum(-1)^n$ has to vanish.

Let us explain the criterion by checking a few cases. If $k = \ell^2 + 2m^2 + 8n^2$ is odd, then it is necessarily $\equiv 1, 3 \pmod 8$, and any odd[54] integer $\frac{k}{2}$ of

---

by descent that we have, in a note in the margin of his Bachet edition of Diophantus, following some number theoretical problems that Bachet has added at the end of book VI of the *Arithmetica*. See the fundamental book [Goldstein 1995], which incidentally has suggested the basic thesis of this paper. For the nature of Bachet's edition, cf. below, the third renaissance.

[52]   It is not hard to show, that the group law on E_k will then produce infinitely many such points—see [Koblitz 1984], 44–46. To prove the equivalence of this definition with those given above, observe that k is congruent if and only if there exist positive integers a, b, c, e, such that $\gcd(a, b, c) = 1$, $a^2 + b^2 = c^2$, and $ab = 2ke^2$. Parametrizing the "primitive pythagorean triple" $(a, b, c) = (p^2 - q^2, 2pq, p^2 + q^2)$ by relatively prime integers $p > q > 1$ such that $p - q$ is odd, and abbreviating $\alpha = p/q$, we find that k being congruent amounts to the existence of $1 < \alpha \in \mathbf{Q}$ and $c, e \in \mathbf{Z}$ such that $(\alpha^3 - \alpha)(c/(\alpha^2 + 1))^2 = ke^2$. Via $x = k\alpha$, $y = k^2(\alpha^2 + 1)e/c$, this becomes : $\exists x, y \in \mathbf{Q}$, $y \neq 0 : y^2 = x^3 - k^2x$.

[53]   The result, in a slightly different formulation, is due to J. Tunnel, A classical diophantine problem and modular forms of weight 3/2, Inventiones Mathematicae **72** (1983), 323–334 : k is congruent if and only if there are exactly twice as many integer representations of k, resp. $\frac{k}{2}$, by the given ternary quadratic forms, as there are such representations with n even. Cf. [Koblitz 1984], 221.

[54]   Remember we assume k squarefree. So if k is even, $\frac{k}{2}$ will be odd.

the form $\ell^2 + 4m^2 + 8n^2$ will be $\equiv 1, 5 \pmod 8$. Therefore, when $k \equiv 5, 6, 7 \pmod 8$, there are no representations at all to look at, the sum is therefore empty, i.e., $= 0$. The Conjecture of Birch & Swinnerton-Dyer then indicates that these k should all be congruent numbers. This can usually be verified without too much trouble for a given k in computational range with today's theoretical and computational apparatus.

For $k = 1, 2, 3, 10$ on the other hand, there are exactly:

two representations of $1 = (\pm 1)^2 + 2 \cdot 0^2 + 8 \cdot 0^2$;
two representations of $1 = (\pm 1)^2 + 4 \cdot 0^2 + 8 \cdot 0^2$;
four representations of $3 = (\pm 1)^2 + 2 \cdot (\pm 1)^2 + 8 \cdot 0^2$;
four representations of $5 = (\pm 1)^2 + 4 \cdot (\pm 1)^2 + 8 \cdot 0^2$.

In all these cases, this yields a nonzero multiple of $(-1)^0 = 1$ for the corresponding sum $\sum (-1)^n$, and this proves unconditionally, in the style of the late twentieth century, that $k = 1, 2, 3, 10$ are not congruent. For $k = 11$, one finds

$$11 = (\pm 1)^2 + 2 \cdot (\pm 1)^2 + 8 \cdot (\pm 1)^2 = (\pm 3)^2 + 2 \cdot (\pm 1)^2 + 8 \cdot 0^2,$$

so the sum adds up to $4 \cdot \big((-1)^1 + (-1)^{-1} + (-1)^0\big) = -4 \neq 0$, which again proves that 11 is not a congruent number. The only three values of $k \equiv 1, 2, 3 \pmod 8$ which are < 100 and whose corresponding sums $\sum (-1)^n$ do vanish, are $k = 34, 41, 65$. That 34 and 65 are indeed congruent, already follows from the table in the anonymous Arabic manuscript mentioned above. But to find a rational right triangle with area 41 would have also been still within reach of mathematicians of the tenth century, or indeed of Diophantus himself: $(a, b, c) = (\frac{123}{20}, \frac{40}{3}, \frac{881}{60})$.[55]

But we have been getting ahead of ourselves ...

7. The second renaissance of Diophantus, or more precisely, the second chapter of the first renaissance, took place during the intellectual revival of the Byzantine empire between the 11th and the 13th century. It is linked to the first chapter in that it was to a large extent the interest of the world of Islam for old Greek manuscripts which finally triggered the growing interest of the Byzantines in their intellectual heritage. It is this Byzantine awareness of heritage to which we owe the manuscripts (copies of copies) of the six books I, II, III, "IV", "V", "VI" of the *Arithmetica*, which have come upon us in Greek.[56] The oldest of these manuscripts themselves are thought to date from the 13th century. The whole Byzantine tradition of the text does

---

[55] Cf. G. Kramarz, All congruent numbers less than 2000, Mathematische Annalen **273** (1986), 337–340.
[56] See the table in [Tannery 1893/95], vol. II, p. XXIII.

not go back to the same original 'edition' of the *Arithmetica* as the Greek text from which Qusṭā ibn Lūqā had translated. The latter is richer in commenting the solutions given, and also places a standard sentence at the end of each solved problem which sums up the solution obtained. There have been discussions whether Qusṭā ibn Lūqā's copy was maybe Hypatia's "commentary" on Diophantus which existed according to the Byzantine encyclopedia Suda ($\Sigma o\upsilon\delta\alpha$).[57]

If the Byzantine interest in Diophantus and other ancient mansucripts was mainly motivated by a sense of cultural heritage, and not by active mathematical interests comparable to those of the scholars in the Arab world, this is of course not to say that the Byzantine scholars did not study their Diophantus. The historian of mathematics Christianidis has recently proposed a reading of Diophantus via the theory of proportions, which is a direct generalization of a commentary by Maximus Planudes on problem II.8—see section 4 above for our brief discussion of this problem.[58] Thus Christianidis explains Planudes's way of reconstructing Diophantus: if we extend the notation which we used above in section 4 to state the general problem II.8 in the form $x^2 + y^2 = a^2$, then the substitution "$y = tx - a$" is obviously equivalent to saying that t equals the proportion $(a + y) : x$. And Christianidis shows how similar reconstructions in terms of proportions can be given for Diophantus's solutions of other indeterminate problems in a mathematically coherent way.

But there is no shortage of such mathematically coherent reconstructions of Diophantus's alleged method. Bašmakova's account in [Bašmakova 1974], or its echo in Zagier's presentation [Zagier 1991], who proceeds with the modern classification of the problems according to the genus of algebraic curves in mind, provide other examples. Christianidis draws our attention to a Byzantine way of looking at Diophantus. Short of assuming a particular communication of souls between Diophantus and Planudes over some seven

---

[57]   This entry of the Suda is included in [Tannery 1893/95], vol. II, 36 (20–25). There, Tannery suggests a questionable modification of the text of the manuscript. The Suda is a compilation of compilations dating from about 1000 AD. Tannery reproduces the old erroneous reading of the name of this encyclopedia as the name of a person, "Suidas." [Cameron & Long 1993], pp. 44–49, discuss this and other evidence about Hypatia's writings and concludes that she (in part guided by her father) authored textbook editions of: (i) Ptolemy's *Almagest* starting wth Book III; (ii) Ptolemy's *Handy Tables*; (iii) (at least parts of) Diophantus's *Arthmetica*; and (iv) possibly Apollonius's *Conics*. More specifically for Hypatia's commentary on Diophantus, see [Bašmakova *et al.* 1978], as well as [Sesiano 1982], 71–75. These hypotheses about a "major commentary" which would have been the basis of Qusṭā ibn Lūqā's translation have been violently rejected by Rashed and his circle—see for instance [Rashed 1984], tome III, the end of the long footnote 63, on page LXII.

[58]   [Christianidis 1998]. The Byzantine monk Maximus Planudes (appr. 1255–1305) was the Byzantine scholar to whom the most important class of Greek manuscripts of the *Arithmetica* which we have today goes back to. Cf. also Knorr's comments on the related papers [Christianidis 1991] and [Waterhouse 1993], in [Knorr 1993], 181.

centuries or more, there is no reason to grant this reading any more authority than other reconstructions. But as a Byzantine reading it might actually be relevant to understand particularities of the Byzantine manuscripts on which our knowledge of the Greek books of the *Arithmetica* depends.

8. The third renaissance of Diophantus, or the first chapter of the second double renaissance, was started by the humanist Johannes Müller, better known as Regiomontanus, who discovered at the end of 1463 one of the Byzantine manuscripts of Diophantus in Venice.[59] Giovanna Cifoletti[60] has shown that, over the following 200 years, Diophantus's *Arithmetica* was taken on the one hand as the ultimate proof for the creators of the new Algebra like Gosselin, Stevin, Pelletier, Viète, and others that algebra was not an Arab invention, but that it had existed with the Greeks as a pure science, whereas the barbaric Arabs had humiliated it into an applied discipline.[61] On the other hand, we see in this third renaissance almost a repetition of what we found in the Arab world during the first renaissance: a number theory movement sets in which starts to rival the algebraic approach to the *Arithmetica*.

Thus, the first European edition, of the (six Greek books of the) *Arithmetica*[62] realized as a Latin translation in 1575 at Basel by the humanist Wilhelm Holzmann (1532–1576), who called himself *à la grecque* Xylander, was soon followed by another one, in Greek with Latin translation, done with great care and lots of remarks and added problems by the 'lover of numbers' Bachet de Méziriac (Paris 1621).[63] This was the edition of Diophantus which Pierre de Fermat studied and into which he inscribed his

---

[59]   For Regiomontanus in general see [Zinner 1968], cf. also [Mett 1996] and [Belyi 1985]. Regiomontanus describes his discovery of this Greek work on Algebra in a letter to Bianchini dated 11 February 1464. There he says in particular, quite characteristically for a humanist at the time, that he would like to translate this text into Latin and publish it, but not before he has found the remaining 7 of the 13 books...

[60]   [Cifoletti 1996], cf. also [Morse 1981].

[61]   See Viète, preface to his Zététiques [Vaulézard 1986], p. 271: "L'art que je produis aujourd'hui est un art nouveau, ou du moins tellement dégradé par le temps, tellement sali et souillé par les barbares, que j'ai cru nécessaire de lui donner une forme entièrement neuve." — Viète has a nice way of describing the difference between Diophantus's method of choosing generic numerical values when solving his problems—something he calls *Algèbre* ot *Logistica numerosa*, and his own formal algebra, the *Logistica speciosa*: (always in Vaulezard's translation, p. 51) "Diophante a traité du Zetetique tres subtilement entre tous autres, aux livres qu'il a escrits de l'Arithmetique, mais comme il a donné son institut par les nombres et non par especes (desquels toutefois il s'est servi) c'est en quoy la subtilité et l'ingeniosité de son esprit est grandement à admirer, puis ce qu'au Logistice numerique les choses aparoissent plus subtiles et difficiles à concevoir, qu'au specifique auquel auquels elles sont plus familieres et facilement trouvées et rencontrées."

[62]   This is not counting Bombelli's Algebra from 1579 which contained many problems taken from Diophantus.

[63]   To cite but one famous example of Bachet's numerous comments on the possibility of decomposing numbers as sums of 2, 3, or 4 perfect squares, on the occasion of problem

famous marginal notes. Now, as we mentioned above, Fermat introduced as a major novelty into arithmetic the technique of infinite descent. But for a descent argument (i.e., for the contradiction at the end) to work it is essential that one deals with (hypothetical) solutions to the problem which are measured by positive integers, and not just by rational numbers or other non-discrete quantities. Therefore Fermat was unhappy about the algebraic tendencies of his time, in particular Viète's success, but also with Diophantus, and tried to rally support for number theoretic investigations in his style. In fact, it seems that this danger, as he saw it, of the new algebra of his time to move from integer variables to rational numbers, or even to continuous quantities without having to change notation, prompted Fermat not to use algebraic notation, but Latin prose, when he was doing number theory, in particular via descent (no wonder then, that the margin was often too small). But of course he was well aware of how much inspiration he had received from Diophantus for his number theory, and thus he once speculated whether among the 7 books of the *Arithmetica* unknown to him, there might not be one or several that would treat problems looking for integer solutions instead of rational ones. This speculation strikes us as very unlikely today; it is a marvellous example for the many different ways in which Diophantus has been approached over the centuries.[64]

To give yet another example of a reading of Diophantus in a certain historic context, let us quote d'Alembert's entry on Diophantus in the great *Encyclopédie* [d'Alembert 1784]. There he soon points out the usefulness of Diophantus's methods for the transformation of integrals of algebraic functions, and thus finds the occasion to quote a paper of his which he had published in 1746 in the *Berliner Monatsberichte*.

---

problem IV.29. This remark triggered the general claim in the margin by Fermat, that any number is the sum of at most a a-polygonal numbers, which was subsequently proven by Lagrange, Legendre, Gauss for squares ($a = 4$), and for general a by Cauchy.

[64]   See Fermat [II], no. LXXXI, *Second défi de Fermat aux mathématiciens,* Février 1657; p. 334f (our translation): "Arithmetical questions—there is almost no-one proposing them, almost no-one understanding them. Or isn't this the reason why arithmetic has been hitherto treated geometrically rather than arithmetically? This is in fact what most of the books of ancient as well as recent authors suggest; this is what Diophantus himself suggests. Even though he stood a bit more apart from geometry than others, in that he restricts to analysis with only rational numbers. This domain, however, is not completely free from geometry, as is proved over and over by Viète's Zetetica in which Diophantus's method is extended to the continuous quantity, and thereby to geometry. Thus it is the theory [*doctrina*] of integers that arithmetic claims as its proper patrimony. This theory, which is already, if only with a light touch, sketched in Euclid's Elements, and which has not been sufficiently developed by those who followed (if a substantial amount of it is not hidden in those books of Diophantus which the adverse course of time has withdrawn from us)—the students of arithmetic should strive to advance or renew."

9. Diophantus in the twentieth century. And nowadays? The renaissance initiated by Regiomontanus, Viète, and Fermat has been brought to a certain conclusion by the classical scholarly work on Diophantus (as well as on Fermat) done by Heath and Tannery around the turn of the century. In the twentieth century I see a new renaissance of Diophantus which began even before the discovery of the four Arabic books in the 1970s. If a date has to be given to mark the transition from the third to the **fourth renaissance of Diophantus**, I would propose Poincaré's research programme [Poincaré 1901] where he indicates how the arsenal of birational algebraic geometry, which had seen such a formidable progress in the nineteenth century, should be systematically brought to bear on diophantine problems. Poincaré's programme suggests that we turn to the theory of algebraic curves to understand the *Arithmetica*; that we use the genus as the classifying invariant for Diophantus's problems; that we see chords and tangents in many places where Diophantus chooses numerical values. Algebraic geometry has provided the modern language for discussing Diophantus. The impressive success story of Arithmetic algebraic geometry in the twentieth century has given it an additional momentum.

What I find most intriguing in the current situation is the strange convergence of two tendencies which are really opposed to each other: At first sight, the historical-philological approach seems to be neatly separated today from the creative mathematical one, as it naturally ought to be. For instance, if one compares Rashed's edition of the Arabic books [Rashed 1984] with Tannery's classical edition of the Greek books [Tannery 1893/95], the main difference is that Rashed and his collaborators separate the mathematical commentary clearly from the pure, literal translation, whereas Tannery amalgamated translation and notational retranscription in his Latin text, thus avoiding a separate mathematical commentary altogether. This should be seen as a natural progress over the past 100 years of the philological care taken also with scientific texts. After all, archeologists do also no longer imitate Evans's behaviour while unearthing the Knossos palace in Crete, who simply threw many fragments away if they did not come from the 'classical' stratum that interested him. It may also be an indication that our current algebro-geometric frame of interpretation for Diophantus is farther removed from the text than that of Fermat, even though the current editions have not yet adopted Grothendieck's language of schemes; Lachaud, who prepared the commentary for the Rashed edition, compromised for the language of Weil's *Foundations of Algebraic Geometry* from 1946.

But in spite of this crystal clear separation of the historical text from the modern interpretation, certain historians of mathematics try to surpass the mathematicians in blending modern inspiration with Diophantus's alleged thoughts. The worst example of this thoughtless tendency is given by the

Russian historian of mathematics Bašmakova in her book on Diophantus [Bašmakova 1974]. To give but one telling example, she claims that Diophantus uses also negative numbers, in spite of the obvious fact that he only accepts positive rational solutions. To substantiate her claim[65] she analyzes a problem (II.9) in terms of the chord and tangent process, according to which Diophantus draws "a line through the point $(2, -3)$." That neither the line nor that point are mentioned in Diophantus does not seem to distract this author who continuously confuses her own mathematical interpretation with the content of the text.

Contrary to the historian, a mathematician cannot be asked to separate his creative ideas from the text. After all, his duty is not to do history of mathematics, but to use Diophantus as a sort of virtual colleague in the quest for new problems and theorems. To conclude, let us take a look at Joseph L. Wetherell's 1998 Berkeley thesis: "Bounding the number of rational points on certain curves of high rank".[66] This work takes off from problem VI.17 of the third Arabic book, which was suggested to Wetherell by Hendrik Lenstra: "Find three squares which when added give a square, and such that the first one is the side (i.e., the squareroot) of the second, and the second is the side of the third."[67] Call the first number, which has to be a square, x^2, then the second is x^4, and the third x^8, and we want that $x^2 + x^4 + x^8$ be a square, which in modern notation we may write as y^2. Diophantus solves this problem by taking y as $x^4 + \frac{1}{2}$. This gives the equation

$$x^2 + x^4 + x^8 = x^8 + x^4 + \frac{1}{4},$$

in which he may, according to the first principles of the *Arithmetica*, simplify terms of equal order. This gives

$$x^2 = \frac{1}{4},$$

and therefore (since only positive rational numbers are acceptable) the solution $x = 1/2$. Thus the first number sought is $1/4$, the second (which had to be the square of the first) "the half of one eighth", as Diophantus says, and the third is $1/256$. Their sum is $81/256$, which is indeed a square. This finishes this problem of the *Arithmetica*, which clearly belongs to the less complicated ones.

---

[65] [Bašmakova 1974], 36.

[66] I thank Wetherell (`jlwether@alum.mit.edu`, oder: `wetherel@math.usc.edu`) for promptly sending me the files.

[67] See [Rashed 1984], tome IV, 65. Cf. [Sesiano 1982], 149f. Apparently because this problem does not fit into any group of problems in an obvious way, it is simply omitted from the *Conspectus* of all the problems in Rashed's edition: [Rashed 1984], tome IV, 129.

Its special role when viewed through our current spectacles comes from the observation that *today we* instinctively substitute in the equation

$$y^2 = x^8 + x^4 + x^2$$

$y = xw$, and thus obtain the hyperelliptic curve

$$w^2 = x^6 + x^2 + 1.$$

Blowing up at infinity resolves this into a smooth projective curve of genus 2. According to Gerd Faltings's theorem from 1983 (the former Mordell Conjecture), such a curve can only have finitely many rational points.[68] Thus Wetherell writes in his introduction:

> This work was motivated by a problem from the *Arithmetica* of Diophantus. In problem 17 of book 6 of the Arabic manuscript, Diophantus poses a problem which comes down to finding positive rational solutions to $y^2 = x^6 + x^2 + 1$. This equation describes a genus 2 curve which we will call C. Diophantus provides the solution $(1/2, 9/8)$ and a natural question is whether there are any other positive rational solutions. It clearly will suffice to find all rational points on C. In addition to the solution given by Diophantus and the 3 obvious variations obtained by negating the x and y-coordinates, we have the 4 trivial solutions $(0, 1)$, $(0, -1)$, ∞^+, and ∞^-. Here ∞^+ and ∞^- are the points on the non-singular curve which lie over the point at infinity in the hyperelliptic plane model for C.
>
> There are several reasons why C is intriguing. First, it appears to be the only curve of genus greater than one in the ten known books of the *Arithmetica*.[69] Since the genus is greater than one, we know by Faltings' theorem that C has only finitely many rational points. So it makes sense to ask if Diophantus had found all of the positive rational solutions. In other words, are the 8 solutions we have described the only rational points on C?
>
> Second, while C has many pleasant properties, it is just outside of reach for the usual methods of determining the set of rational points on a genus 2 curve. In particular, C covers two elliptic curves:
> $$E_1 : y^2 = x^3 + x + 1,$$
> $$E_2 : y^2 = x^3 + x^2 + 1.$$

---

[68] Cf. the allusions to this in [Rashed 1984], tome IV, p. LXXVIII.

[69] *Note by N. Sch.:* This is not true. There is one other example in the Greek books which lie past book VII of the *Arithmetica*: problem "IV".18.

If either of these elliptic curves had only finitely many rational points, it would be a short calculation to find the set of rational points on C; however, both E_1 and E_2 have rank 1. Along the same lines, if $J = \text{Jac}(C)$ had rank 0, then it would be a finite calculation to determine $C(\mathbf{Q})$. If J had rank 1, then it would be possible to bound the number of points in $C(\mathbf{Q})$ by using Flynn's explicit description of Chabauty calculations on genus 2 curves. But J is isogenous to the product $E_1 \times E_2$, so that J has rank 2.

Using a refinement and strengthening of Chabauty's method, Wetherell finally succeeds in showing that the equation $y^2 = x^6 + x^2 + 1$ has indeed only the six obvious solutions (x, y) with x, y rational.

It is exciting to see how a problem which is over 1700 years old can suggest an interesting research topic today. It is clear that our mathematical interest in Wetherell's work is not in the result but in the refined method he applies. And if we care for a bit of historical perspective, we should not forget that the diophantine problem solved here—namely, to determine *all* rational solutions of the given equation—is of the sort that Diophantus would not have been able to express.

References

J. Le Rond d'Alembert (1784), "Diophante", *in:* Encyclopédie méthodique. Mathématiques, tome premier, Paris (Planckoucke) / Liège (Plomteux), p. 533–534

A. Anbouba (1979), Un traité d'Abū Ja'far [al-Khāzin] sur les triangles rectangles numériques, Journal for the History of Arabic Science (Aleppo, Syrien) **3** (1), 134–156

I.G. Bašmakova (1974), Diophant und Diophantische Gleichungen, Berlin (VEB Deutscher Verlag der Wissenschaften)

I.G. Bašmakova, E.I. Slavoutine, B.A. Rosenfeld (1978), The Arabic version of the *Arithmetica* of Diophantus (in Russian), Istor. Mat. Issledov., Moskau, **13**

Iu.A. Belyi (1985), Regiomontan (in Russian), Moskau (NAUKA)

D.M. Burton (1991/95), History of Mathematics, Dubuque, IA (Wm.C. Brown Publishers)

A. Cameron, J. Long (with a contribution by L. Sherry) (1993), Barbarians and Politics at the Court of Arcadius, Berkeley CA (U Cal. Press)

M. Cantor (1907), Vorlesungen über Geschichte der Mathematik, vol. I (von den ältesten Zeiten bis zum Jahre 1200 n. Chr.), 3rd edition, Leipzig (Teubner)

M. Caveing (1997), La figure et le nombre. Recherches sur les premières mathématiques des Grecs. La constitution du type mathématique de l'idéalité dans la pensée grecque, Paris (Septentrion)

G. Cifoletti (1996), The creation of the history of algebra in the 16th century; *in:* L'Europe Mathématique — Mathematical Europe (Goldstein, Ritter, Gray, ed.s), Paris (MSH), 123–142

J. Christianidis (1991), $A\rho\iota\theta\mu\eta\tau\iota\kappa\eta \ \Sigma\tau o\iota\chi\epsilon\iota\omega\sigma\iota\varsigma$: Un traité perdu de Diophante d'Alexandrie?, Historia Math. **18**, 239–246

J. Christianidis (1998), Une interprétation byzantine de Diophante, Historia Math. **25**, 22–28

L.E. Dickson (1923), History of the Theory of Numbers, Volume II, Diophantine Analysis, The Carnegie Institute of Washington

M. Dzielska (1995), Hypatia of Alexandria (translated by F. Lyra), Revealing Antiquity **8**, Cambridge, Mass., London (Harvard University Press)

P. de Fermat [I – IV], Œuvres de Fermat, publiées par P. Tannery et Ch. Henry; Paris (Gauthier-Villars), 1891–1912

H. Gericke (1984), Mathematik in Antike und Orient, Heidelberg etc. (Springer Verlag); quoted from the reedition Wiesbaden (Fourier Verlag) 1992, which also contains Gericke's: Mathematik im Abendland von den römischen Feldmessern bis zu Descartes.

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

R.C. Gupta (1995), Ancient Indian mathematics: some highlights; *in:* Science in the West and India, Some Historical Aspects, edited by B.V. Subbarayappa, N. Mukunda, Bombay etc. (Himalaya Publ. House)

H. Hankel (1874), Zur Geschichte der Mathematik im Altertum und Mittelalter, Leipzig — we quote from the second edition, edited by J.E. Hofmann, Hildesheim (Olms) 1965

G. Harder (1995), Diophantische Gleichungen: ein zweitausend Jahre altes Thema der Mathematik, Jahrbuch 1994 der Deutschen Akademie der Naturforscher Leopoldina **40**, 267–278

T. Heath (1921), A History of Greek Mathematics, volume II: from Aristarchus to Diophantus, Oxford (Clarendon Press)

C.G.J. Jacobi (1847), Über die Kenntnisse des Diophantus von der Zusammensetzung der Zahlen aus zwei Quadraten nebst Emendation der Stelle Probl. Arith. V.12, Monatsbericht Akad. Wiss. Berlin August 1847, 265–278 [= Gesammelte Werke VII, 332–344]

J. Klein (1968), Greek Mathematical Thought and the Origin of Algebra (translated from German by Eva Brann), Cambridge, Mass. (MIT Press) — I quote the Dover-reprint of 1992

W.R. Knorr (1993), *Arithmêtikê stoicheiôsis:* On Diophantus and Hero of Alexandria, Historia Math. **20**, 180–192

N. Koblitz (1984), Introduction to Elliptic Curves and Modular Forms, Springer GTM **97**: New York etc.

R. Mett (1996), Regiomontanus, Wegbereiter des neuen Weltbildes, Einblicke in die Wissenschaft, Stuttgart, Leipzig (Teubner)

J. Morse (1981), The reception of Diophantus' "Arithmetic" in the Renaissance, Ph.D. thesis, Ann Arbor, Michigan

L. Nelson (1921), SPUK, Einweihung in das Geheimnis der Wahrsagerkunst Oswald Spenglers und sonnenklarer Beweis der Unwiderleglichkeit seiner Weissagungen nebst Beiträgen zur Physiognomik des Zeitgeistes. Eine Pfingstausgabe für alle Adepten des metaphysischen Schauens, Leipzig (Verlag der Neue Geist, Dr. P. Reinhold)

O. Neugebauer (1975), A history of ancient mathematical astronomy, Part Two, Berlin - Heidelberg - etc. (Springer)

H. Poincaré (1901), Sur les propriétés arithmétiques des courbes algébriques, *Journal de Mathématiques*, $5^{ème}$ série, t. **7**, fasc. III, 1901, 161–233) = Œuvres **V**, 483–550.

R. Rashed (1979), L'analyse diophantienne au Xe siècle, l'exemple de al-Khāzin, Revue d'Histoire des Sciences **XXXII/3**, 193–222

R. Rashed (1984), Diophante. Les Arithmétiques, tome III (livre IV) et tome IV (livres V, VI, VI). Texte établit et traduit par Roshdi Rashed, Paris (Les Belles Lettres)

R. Rashed (1997), Histoire des Sciences Arabes, sous la direction de Roshdi Rashed avec la collaboration de Régis Morelon, tome 2.: Mathématiques et physique; Paris (Seuil)

N. Schappacher (1989), Neuere Forschungsergebnisse in der Arithmetik elliptischer Kurven, *Didaktik der Mathematik* **17** (1989), 149–158

J. Sesiano (1982), Books IV to VII of Diophantus' *Arithmetica* in the Arabic Translation Attributed to Qusṭā ibn Lūqā, New York - Heidelberg - Berlin (Springer)

O. Spengler (1923), Der Untergang des Abendlandes (2 Bände), we quote from the 'Gesamtausgabe,' dtv, 1972

P. Tannery (1893/95), Diophantus Alexandrinus, opera omnia, I & II, Leipzig (Teubner); I am using the reprint Stuttgart (Bbibliotheca Teubneriana) 1974

P. Tannery (1912), Mémoires Scientifiques de Paul Tannery, publiés par J.L. Heiberg et H.G. Zeuthen (five volumes); tome II, Paris (Gauthier-Villars)

I. Thomas (1941), Selections Illustrating the History of Greek Mathematics, vol. II, Loeb Classical Library, Cambridge (Mass.) and London

J.-L. de Vaulézard (1986), *Introduction en l'art analytic ou nouvelle algèbre,* and: *Les cinq livres des zététiques* de François Viète; French translation by Vaulézard, first edition: 1630; *New edition realized by:* Jean-Robert Armogathe *in:* Corpus des œuvres de philosophie en langue française, Paris (Fayard)

P. Ver Eecke (1959), Diophante d'Alexandrie, les six livres arithmétiques et le livre des nombres polygones, œuvres traduites pour la première fois du grec en français avec une introduction et des notes; nouveau tirage 1959, Paris (Blanchard)

W.C. Waterhouse (1993), Harmonic means and Diophantus, Historia Math. **20**, 89–91

A. Weil (1983), Number Theory. An approach through history. From Hammurapi to Legendre; Boston, etc. (Birkhäuser)

D. Zagier (1991), Lösungen von Gleichungen in ganzen Zahlen; *in:* Miscellanea Mathematica (eds. Hilton, Hirzebruch, Remmert), Berlin - Heidelberg - etc. (Springer); 311–326

E. Zinner (1968), Leben und Wirken des Johannes Müller von Königsberg (2nd edition), Osnabrück (Otto Zeller)