CO 480 Lecture 3

Diophantus of Alexandria, Arithmetica and Diophantine Equations

May 9th, 2017

This Day In History (May 9th, 1694)

Johann Bernoulli wrote Leibniz, introducing the method of "separation of variables" or "separation of indeterminates." He would publish the method in Acta eruditorum in November of 1694.

New Classroom!

- EIT 1015 from now on WITH EXCEPTIONS:
- Thursday May 25th (STC 0010 with Alain)
- Tuesday May 30th (STC 0010 with Alain)
- Tuesday June 6th and July 25th Quizzes will be in M3 1006!

Announcements

- Course Project Proposal due next Tuesday (Watch for a Crowdmark link on Thursday evening!)
- Assignment 1 due a week Thursday (Again watch for a Crowdmark link on Thursday!)
- Please submit the correct file to the correct link!
- Add this course! Add to Piazza as well.
- Added restriction to Project: Alain Gamache is doing Édouard Lucas

Diophantus of Alexandria

This week, we'll be discussing Diophantus of Alexandria. We will be talking about Alexandria, its foundation, the Library of Alexandria and problems in Diophantine Equations.

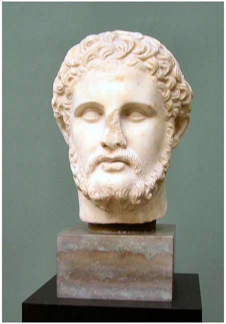
Where Are We This Week?

$\sim 350BCE - 350AD$ in Macedon

https://commons.wikimedia.org/wiki/File:Map_Macedonia_336_BC-en.svg

History of Alexander the Great

- Battle of Chaeronea (won by Philip II of Macedon) in 338 BCE
- Marked the end of the golden age of Greek mathematics.
- Philip was succeeded by his son Alexander the Great.



https://commons.wikimedia.org/wiki/File:Filip_II_Macedonia.jpg

Alexander the Great

- Lived from 356 until 323 BCE (died at age 33)
- Conquered much of the world between 334 BCE to 323 BCE
- Spread Greek culture around the world (his armies were usually Greek)
- Tutored by Aristotle (343 BCE)

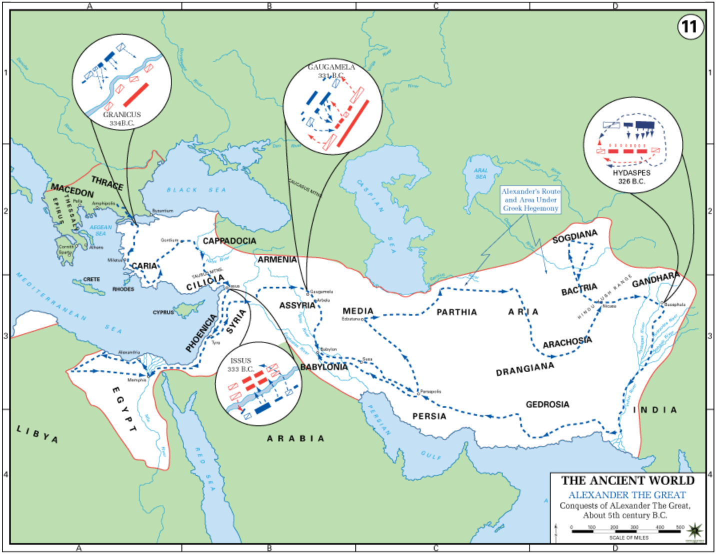
https://en.wikipedia.org/wiki/File:Alexander1256.jpg

Alexander the Conqueror (334 BCE-323 BCE)

Courtesy:
`http://www.ancient.eu/timeline/Alexander_the_Great/`

- 334 BCE - Invaded Persian Empire; liberated Ephesos, Baalbek (renamed Heliopolis)
- 333 BCE - Conquered Sidon, Aleppo
- 332 BCE - Conquers Tyre (injures shoulder), Syria (turns to Egypt)
- 331 BCE - Egypt is conquered by Alexander with little resistance including Susa
- 331 BCE - Founds Alexandria at port town of Rhakotis.

Map of Conquered Areas



Alexandria After Alexander

- Once Alexander left Egypt (shortly after creating Alexandria say 331-330 BCE), control passed to his viceroy Cleomenes (died 322 BCE)
- Upon Alexander's death in 323 BCE, Cleomenes remained as a satrap (political leader) in Alexandria under viceroy Ptolemy who then ordered him to be killed on the suspicion of the embezzlement of 8000 talents. (see Pollard and Reid 2007, enough to pay for 66000 years for one labourer)
- Note: Talent is a unit of weight; usually for gold or silver. One talent of gold currently is worth $1.25 million USD.
- Note: Some references rumour the execution was for spying for Perdiccas.

Ptolemy I Soter

- Lived from 367 BCE - 283 BCE (or 282 BCE)
- One of Alexander's most trusted guards and greatest generals [McLeod]
- Defended from a siege of Perdiccas in 321 BCE (his own men betrayed Peridiccas)
- Ptolemic rule until $\sim$ 80BCE
- As Ptolemic rule progressed, Alexandria began to deteriorate

https://commons.wikimedia.org/wiki/File:Ptolemy_I_Soter_Louvre_Ma849.jpg

Roman Annexation

- Rome annexed Alexandria around 80 BCE.
- Brought back a revitalization of Alexandria.
- Alexandria was under Roman rule until 616AD when it was seized by the Persians.
- During this period is when Diophantus lived in Alexandria

Musaeum

- The Ptolomies wanted Alexandria to be a cornerstone of education.
- Began and finished construction of the Musaeum or Mouseion or Museion at Alexandria (Institution of the Muses).
- Where our 'museum' comes from.
- Arts of the muses included science, philosophy, drama, music, fine art, and mathematics.
- (I couldn't find even an artist's rendition of a picture of the Musaeum!)

Muses

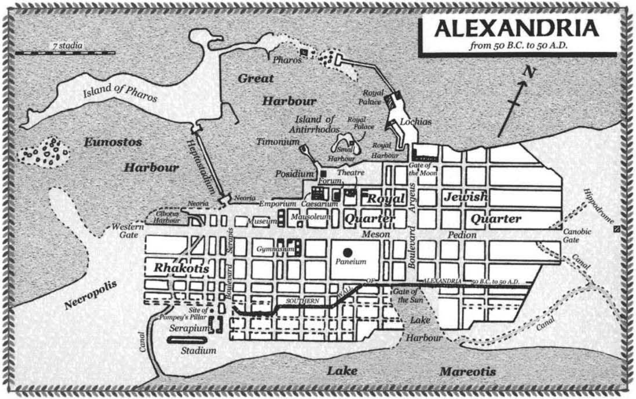
- Goddesses of science, literature and arts in Greek mythology
- Clio - Goddess of history.
- Nine Muses (according to greek poet Hesiod $\sim 750 - 650$ BCE)
- History, Epic Poetry, Love Poetry, Lyric Poetry (music, song), Tragedy, Hymns, Dance, Comedy, Astronomy

https://en.wikipedia.org/wiki/File:Car_of_history.jpg

Books

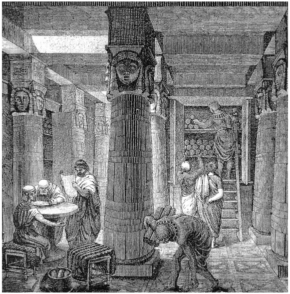
- If Alexandria was to become a great intellectual centre, scholars would need books (back then manuscripts).
- Adjacent to the Musaeum was the great Library of Alexandria.
- Books were stored in the *biblion* (place of books) in the library.
- Library also consisted of other smaller libraries and shrines.

Alexandria (The Library of Alexandria - McLeod)



THE LIBRARY OF ALEXANDRIA

Library at Alexandria



https://en.wikipedia.org/wiki/File:Ancientlibraryalex.jpg

Library of Alexandria

- Most workers were translators called scribblers (*charakitai*) [McLeod].
- Wrote on papyrus.
- Was a place not just for study but for all forms of artistic display.
- Further, was not just a collection of scrolls but rather a research centre full of life and exuberance.
- Library had little consideration for intellectual property or even property rights (see next slide)

Books

- Ptolemy III (246-221BCE) is said to have written across the world asking to borrow books for copying.
- Athens obliged and Alexandria copied the books but kept the originals forfeiting fifteen talents deposited as a bond

https://commons.wikimedia.org/wiki/File:Octadrachm_Ptolemy_III_BM_CMBMC103.jpg

- Ships coming into Alexandria also had all their books confiscated and if travelers were lucky, would be given copies of the originals. (Galen - Roman writer)
- 310-240 BCE - library contained 400,000 mixed scrolls and 90,000 single scrolls!

Great Fire of Alexandria

http:
//www.ancient-origins.net/sites/default/files/field/image/library-alexandria-destruction.jpg

Great Fire of Alexandria

- Great Fire occurred in Alexandria in 48 BCE (Julius Caesar).
- Burned down docks and storehouses of grains.
- “Dio Cassius says that the Great Library was burned as well but Caesar himself says in his account of the Civil War that he burned all the vessels in the harbour which had come to support Pompey plus 22 warships which had usually been on guard at Alexandria.” [McLeod p. 50]
- Highly contested if and how many times the library had burned down.
- Accounts by Plutarch, Aulus Gellius, Ammianus Marcellinus, and Orosius suggest that troops ‘accidentally’ burnt the library down during the Siege of Alexandria. [Pollard and Reid]
- Also may have burnt down between 270 and 275AD during an Egyptian revolt...
- ... and again in 391AD when Theodosius I ordered that pagan temples should be destroyed.

A Brief Digression

https://www.youtube.com/watch?v=sIMu2FmLtdM

Famous people to have worked in Alexandria

- Archimedes of Syracuse ("Eureka", area, volumes, basics of calculus)
- Erathostenes (sieve for prime numbers, geometry)
- Euclid (geometry)
- Hypsicles
- Heron
- Menelaus
- Ptolemy (Claudius Ptolemaeus)
- Diophantus of Alexandria
- Pappus
- Theon and daughter Hypatia

Diophantus of Alexandria

- Alexandrian Greek mathematician known as the "father of Algebra".
- Probably born sometime between 201 and 215 AD and died sometime probably between 285 AD and 299 AD.

Diophantus of Alexandria

- Probably born sometime between 201 and 215 AD and died sometime probably between 285 AD and 299 AD.
- Heath claims that “He was later than Hypsicles... and earlier of Theon of Alexandria” which limits the range of dates certainly to between 150 BCE and 350 AD.
- A letter of Michael Psellus in the 11th century reports that Anatolius, Bishop of Laodicea since 280 AD [Heath p.545], dedicated a treatise on Egyptian computation to his friend Diophantus [Tannery p. 27-42] [Heath p.545]
- Mention of friend ‘Dionysius’ who was probably St. Dionysius, lead a Christian school in Alexandria beginning in 231AD and eventually in 247AD became bishop of Alexandria [Heath (Arithmetica) p. 129][Tannery, in his Mèmoires scientifiques, II, 536 ff.]

Epigram of Diophantus (dated back to 4th century [Burton p.217])

From the "Greek Anthology" (see [Tannery p. 60] or [Heath (Arithmetica) p. 113)

> *His boyhood lasted for* 1/6 *of his life; his beard grew after* 1/12 *more; after* 1/7 *more, he married and his son was born* 5 *years later; the son lived to half his father's age and the father died* 4 *years after his son.*

Letting x be Diophantus' age at death. We see that...

Epigram of Diophantus (dated back to 4th century [Burton p.217])

From the "Greek Anthology" (see [Tannery p. 60] or [Heath (Arithmetica) p. 113)

> *His boyhood lasted for* 1/6 *of his life; his beard grew after* 1/12 *more; after* 1/7 *more, he married and his son was born* 5 *years later; the son lived to half his father's age and the father died* 4 *years after his son.*

Letting x be Diophantus' age at death. We see that...

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

Solving gives...

Epigram of Diophantus (dated back to 4th century [Burton p.217])

From the "Greek Anthology" (see [Tannery p. 60] or [Heath (Arithmetica) p. 113)

> *His boyhood lasted for* 1/6 *of his life; his beard grew after* 1/12 *more; after* 1/7 *more, he married and his son was born* 5 *years later; the son lived to half his father's age and the father died* 4 *years after his son.*

Letting x be Diophantus' age at death. We see that...

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

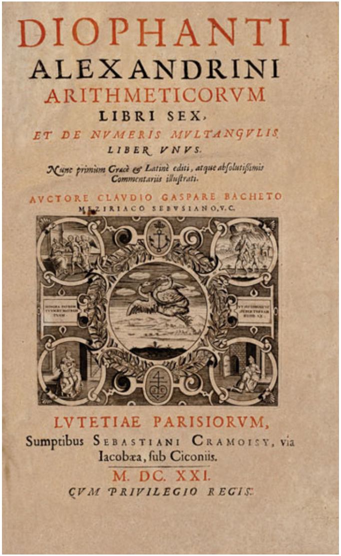
Solving gives... $x = 84$.

Diophantus of Alexandria

Four major contributions:

- Arithmetica (we will discuss later)
- Moriastica (computations with fractions)
- On Polygonal Numbers (only a fragment survives today - see assignment 2 for a sample problem. not original work but used geometric proofs)
- Porisms (completely lost - only know of its existence from references made in Arithmetica)

Arithmetica



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

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

Arithmetica

- A series of 13 books (as mentioned in the introduction of Arithmetica).
- Six have survived due to efforts by the Greeks
- The other 7 were believed to have been lost however recently, four more have been found due to efforts by the Arabs. This was the doctoral thesis work of Jacques Sesiano in 1975 at Brown University.
- Sesiano found 4 more books bringing the total to 10/13 books found.
- Note in Burton p. 219 didn't know of the existence of the 4 arabic books that Sesiano did.

Controversy of the Numbering of Books in Arithmetica

- The numbering of the books has recently been brought to question from the work of Jacques Sesiano.
- Heath claims to have books I to VI however, Book IV must come right after I-III as is confirmed by the Arabic sources.
- Heath's book IV-VI in all likelihood come after the books IV-VII from Sesiano based on the fact that the four books seem to be sequential.
- Thus, we believe to have all of books I-VII and three of the books from VIII-XIII. (I won't speculate as to which books we have from that list).

Language of Arithmetica - Variable powers

- Greek. Bachet translated to Latin in 1621.
- Diophantus used ς for unknown linear quantities.
- Δ^{Υ} represented unknown squares.
- K^{Υ} represented cube. (Kappa, not 'K')
- $\Delta^{\Upsilon}\Delta$, ΔK^{Υ} and $K^{\Upsilon}K$ for fourth, fifth and sixth powers respectively.
- Also has a notation for fractions (won't discuss here)
- See [Heath p.458]

Language of Arithmetica

Alpha	Beta	Gamma	Delta	Epsilon	Digamma	Zeta	Eta	Theta
α	β	γ	δ	ϵ	$\digamma$	ζ	η	θ
1	2	3	4	5	6	7	8	9

Iota	Kappa	Lambda	Mu	Nu	Xi	Omicron	Pi	Koppa
ι	κ	λ	μ	ν	ξ	o	π	ϟ
10	20	30	40	50	60	70	80	90

Rho	Sigma	Tau	Upsilon	Phi	Chi	Psi	Omega	Sampi
ρ	σ	τ	υ	ϕ	χ	ψ	ω	ϡ
100	200	300	400	500	600	700	800	900

How to Translate

- For example, $\alpha = 1$, $\beta = 2$, $\gamma = 3$, $\delta = 4$,
- $K^{\Upsilon}\lambda\epsilon$ meant $35x^3$ and $M\alpha$ would be $+1$. (Abbreviation of *monades*, Greek for units).
- Subtraction was ⩚ (upside-down psi) and positive terms appeared before negative terms.
- For example, $x^3 - 2x^2 + 3x - 4$ was

How to Translate

- For example, $\alpha = 1$, $\beta = 2$, $\gamma = 3$, $\delta = 4$,
- $K^{\Upsilon}\lambda\epsilon$ meant $35x^3$ and $M\alpha$ would be $+1$. (Abbreviation of *monades*, Greek for units).
- Subtraction was $\pitchfork$ (upside-down psi) and positive terms appeared before negative terms.
- For example, $x^3 - 2x^2 + 3x - 4$ was

$$K^{\Upsilon}\alpha\varsigma\gamma\pitchfork\Delta^{\Upsilon}\beta M\delta$$

Try some conversions to/from Greek

1. $x^3 + 13x^2 + 5x + 2$
2. $\Delta^{\Upsilon}\Delta\text{ϡϟ}\digamma M\Xi\Lambda K^{\Upsilon}\iota\epsilon$
3. $-x^2 + 2x - 3$

This Day In History (May 11th, 1610)

Matteo Ricci died in Peking, China. An Italian Jesuit who studied with Christopher Clavius in Rome during the 1570s, he translated The First Six Books of Euclid into Chinese in 1607.

Announcements

- Reminder that the Tutte Road naming ceremony is tomorrow! Come to get a perspective on the history of William Tutte! Check the CO 480 webpage for more information.
- Crowdmark Links will be posted today. Check your inboxes tomorrow if you do not have two links from Crowdmark (One for the Project Proposal and one for Assignment 1) Please email me immediately with which one you're missing!
- Everyone must submit the Project Proposal and groups should each submit the same one!
- Posted history assignment question rubric.

Problems and What a Solution Was In Arithmetica

- Entire world consists of positive rational solutions to problems.
- A solution was considered solved when a single solution was found (either integer or rational).
- There were no negative solutions. For example, in (Greek) Book V Problem 2, we find the equation

$$4x + 20 = 4$$

  which he labels as "absurd because the 4 ought to be some number greater than 20" [Heath (Arithmetica) p.200] [Burton p. 220]

Typical Question in Diophantus' Arithmetica

Book I Problem VII

From the same (required) number to subtract two given numbers so as to make the remainders have to one another a given ratio.

Modern Day Solution

> *From the same (required) number to subtract two given numbers so as to make the remainders have to one another a given ratio.*

Let a, b be the first two given numbers and let the ratio be $c : d$ (or c/d). Then:

$$\begin{aligned} \frac{x-a}{x-b} &= \frac{c}{d} \\ d(x-a) &= c(x-b) \\ (d-c)x &= ad-bc \\ x &= \frac{ad-bc}{d-c} \end{aligned}$$

What Diophantus Did [Heath (Arithmetica) p.132]

> *From the same (required) number to subtract two given numbers so as to make the remainders have to one another a given ratio.*

Given numbers $100, 20$ given ratio $3:1$. Required number x. Therefore $x - 20 = 3(x - 100)$ and $x = 140$.

Major Differences

- Diophantus was pleased with solving a specific instance of a problem
- Came up with algorithms for solving these types of problems.
- Often wrote down a ‘necessary’ condition to make the problem work.

Definition

Diophantine Equations

A *Diophantine Equation* is a polynomial equation over the integers in n variables where we want to classify all integer (or rational) solutions to the problem.

In Diophantus' case, he required only one positive rational solution to exist. We however often want to show such equations either have no solutions, finitely many (then enumerate them) or to find a parameterization for infinitely many (like Linear Diophantine Equations in Math 135).

Rough Contents

- Book I: All Linear Diophantine Equations
- Books II onward: Introduces quadratic terms
- Book IV (arabic) and beyond: Introduces cubic and higher terms.

Interesting Implicit Results in Diophantus' Arithmetica

I will discuss two results in Arithmetica that aren't formally proven.

- Quadratic Equations. It is clear that Diophantus knew of a way to solve quadratic equations (though it is likely not he who knew of these methods first)
- Integers as the sum of two squares. Again it is unclear that he knew the result we will prove but he seemed to avoid it very mindfully.

Quadratic Equations

- $ax^2 + bx = c$ Greek Book VI Problem 6 (or VI.6)
- $ax^2 = bx + c$ Greek Book IV Problem 39 (or IV.31)
- $ax^2 + c = bx$ Greek Book V Problem 10 (or IV.22)

Notice that Diophantus has 3 cases because he does not have a notion of negative numbers. Diophantus never was explicit in solving this generally but he knew the general method as was manifest in Book V Problem 30

29. To find three squares such that the sum of their squares is a square.

Let the squares be x^2, 4, 9 respectively[1].

Therefore $x^4 + 97 =$ a square $= (x^2 - 10)^2$, say;

whence $x^2 = \frac{3}{20}$.

If the ratio of 3 to 20 were the ratio of a square to a square, the problem would be solved; but it is not.

Therefore *I have to find two squares* (p^2, q^2, *say*) *and a number* (m, *say*) *such that* $m^2 - p^4 - q^4$ *has to* $2m$ *the ratio of a square to a square.*

Let $p^2 = z^2$, $q^2 = 4$ and $m = z^2 + 4$.

Therefore $m^2 - p^4 - q^4 = (z^2+4)^2 - z^4 - 16 = 8z^2$.

Hence $8z^2/(2z^2+8)$, or $4z^2/(z^2+4)$, must be the ratio of a square to a square.

Put $z^2 + 4 = (z+1)^2$, say;

therefore $z = 1\frac{1}{2}$, and the squares are $p^2 = 2\frac{1}{4}$, $q^2 = 4$, while $m = 6\frac{1}{4}$;

or, if we take 4 times each, $p^2 = 9$, $q^2 = 16$, $m = 25$.

Starting again, we put for the squares x^2, 9, 16;

then the sum of the squares $= x^4 + 337 = (x^2 - 25)^2$, and $x = \frac{12}{5}$.

The required squares are $\frac{144}{25}$, 9, 16.

30. [The enunciation of this problem is in the form of an epigram, the meaning of which is as follows.]

A man buys a certain number of measures (χόες) of wine, some at 8 drachmas, some at 5 drachmas each. He pays for them a *square* number of drachmas; and if we add 60 to this number, the result is a square, the side of which is equal to the whole number of measures. Find how many he bought at each price.

Let $x =$ the whole number of measures; therefore $x^2 - 60$ was the price paid, which is a square $= (x - m)^2$, say.

If now k^2, l^2, m^2 represent three numbers satisfying the conditions of the present problem of Diophantus, put for the second of the required numbers $2kx + k^2$, for the third $2lx + l^2$, and for the fourth $2mx + m^2$. These satisfy three conditions, since each of the last three numbers added to the first $(x^2 + a)$ less the number a gives a square. The remaining three conditions give a triple-equation.

[1] "Why," says Fermat, "does not Diophantus seek *two* fourth powers such that their sum is a square? This problem is in fact impossible, as by my method I am in a position to prove with all rigour." It is probable that Diophantus knew the fact without being able to prove it generally. That neither the sum nor the difference of two fourth powers can be a square was proved by Euler (*Commentationes arithmeticae*, I. pp. 24 sqq., and *Algebra*, Part II. c. XIII.).

Now $\frac{1}{5}$ of the price of the five-drachma measures $+ \frac{1}{8}$ of the price of the eight-drachma measures $= x$;

so that $x^2 - 60$, the total price, has to be divided into two parts such that $\frac{1}{5}$ of one $+ \frac{1}{8}$ of the other $= x$.

We cannot have a real solution of this unless

$$x > \tfrac{1}{8}(x^2 - 60) \text{ and } < \tfrac{1}{5}(x^2 - 60).$$

Therefore $5x < x^2 - 60 < 8x$.

(1) Since $x^2 > 5x + 60$,

$x^2 = 5x +$ a number greater than 60,

whence x is[1] *not less than* 11.

(2) $x^2 < 8x + 60$

or $x^2 = 8x +$ some number less than 60,

whence x is[1] *not greater than* 12.

Therefore $11 < x < 12$.

Now (from above) $x = (m^2 + 60)/2m$;

therefore $22m < m^2 + 60 < 24m$.

Thus (1) $22m = m^2 +$ (some number less than 60),

and therefore m is[2] *not less than* 19.

(2) $24m = m^2 +$ (some number greater than 60),

and therefore m is[2] *less than* 21.

Hence we put $m = 20$, and

$$x^2 - 60 = (x - 20)^2,$$

so that $x = 11\frac{1}{2}$, $x^2 = 132\frac{1}{4}$, and $x^2 - 60 = 72\frac{1}{4}$.

Thus we have to divide $72\frac{1}{4}$ into two parts such that $\frac{1}{5}$ of one part *plus* $\frac{1}{8}$ of the other $= 11\frac{1}{2}$.

Let the first part be $5z$.

Therefore $\frac{1}{8}$ (second part) $= 11\frac{1}{2} - z$,

or second part $= 92 - 8z$;

therefore $5z + 92 - 8z = 72\frac{1}{4}$,

and $z = \frac{79}{12}$.

Therefore the number of five-drachma χόες $= \frac{79}{12}$.

" " " " eight-drachma " $= \frac{59}{12}$.

[1] For an explanation of these limits see p. 60, *ante*.

[2] See p. 62, *ante*.

The Equation $a^2x + bx = c$

In Book VI Problem 6, Diophantus mentions that $6x^2 + 3x = 7$ cannot be solved because "(half the coefficient of x) squared plus a product of the coefficient of x^2 and the absolute term should be a square"

This algebraically would be $(b/2)^2 + ac = (1/4)(b^2 - 4a(-c))$ and rearranging this in the abstract equation, we see that Diophantus was speaking of the discriminant being a positive rational square.

Thus, since $(3/2)^2 + 6 \cdot 7$ is not a square, he claims the above equation has no solution.

Sum of Two Squares

Diophantus seemed to have known the following theorem (see discussions [Heath p.482-483]).

Theorem

If a number when subtracted by 3 is divisible by 4, then the number cannot be written as the sum of two squares.

or reworded

Theorem

If $n \in \mathbb{Z}$ satisfies $n \equiv 3 \mod 4$, then there do not exist integers x and y satisfying $x^2 + y^2 = n$.

Arithmetica (Greek) Book V Problem 9 [Heath p. 206]

9. To divide unity into two parts such that, if the same given number be added to either part, the result will be a square.

Necessary condition. The given number must not be odd and the double of it + 1 must not be divisible by any prime number which, when increased by 1, is divisible by 4 [*i.e.* any prime number of the form $4n - 1$][1].

Given number 6. Therefore 13 must be divided into two squares each of which > 6. If then we divide 13 into two squares the difference of which < 1, we solve the problem.

[1] For a discussion of the text of this condition see pp. 107–8, *ante*.

Proof

$$n \in \mathbb{Z} \land n \equiv 3 \mod 4 \Rightarrow \neg \exists x, y \in \mathbb{Z}, x^2 + y^2 = n$$

Proof: Assume towards a contradiction that there exists integers x and y such that $x^2 + y^2 = n$. Since this holds over the integers, it must hold in $\mathbb{Z}_4$, that is,

$$x^2 + y^2 \equiv 3 \mod 4$$

Now, squaring each of $0, 1, 2, 3$ modulo 4 yields $0, 1, 0, 1$ respectively. Since each of $x, y \in \{0, 1, 2, 3\}$ modulo 4, we see that $x^2 + y^2$ modulo 4 must be one of $0 + 0$, $0 + 1$, $1 + 0$ or $1 + 1$. These numbers are $0, 1, 2$, none of which give you 3 modulo 4, a contradiction.

Arithmetica (Greek) Book V Problem 11 [Heath p. 206]

11. To divide unity into three parts such that, if we add the same number to each of the parts, the results are all squares.

Necessary condition[3]. The given number must not be 2 or any multiple of 8 increased by 2.

In other words, a number of the form $24n + 7$ for any $n \in \mathbb{N}$ cannot be written as the sum of three integer squares. (See assignment 1)

What about...

... numbers as the sum of four squares?

Arithmetica (Greek) Book IV Problem 29 [Heath p. 200]

29. To find four square numbers such that their sum added to the sum of their sides makes a given number[1].

[1] On this problem Bachet observes that Diophantus appears to assume, here and in some problems of Book v., that any number not itself a square is the sum of two or three or four squares. He adds that he has verified this statement for all numbers up to 325, but would like to see a scientific proof of the theorem. These remarks of Bachet's are the occasion for another of Fermat's famous notes: "I have been the first to discover a most beautiful theorem of the greatest generality, namely this: Every number is either a triangular number or the sum of two or three triangular numbers; every number is a square or the sum of two, three, or four squares; every number is a pentagonal number or the sum of two, three, four or five pentagonal numbers; and so on *ad infinitum*, for hexagons, heptagons and any polygons whatever, the enunciation of this general and wonderful theorem being varied according to the number of the angles. The proof of it, which depends on many various and abstruse mysteries of numbers, I cannot give here; for I have decided to devote a separate and complete work to this matter and thereby to advance arithmetic in this region of inquiry to an extraordinary extent beyond its ancient and known limits."

Unfortunately the promised separate work did not appear. The theorem so far as it relates to squares was first proved by Lagrange (*Nouv. Mémoires de l'Acad. de Berlin*, année 1770, Berlin 1772, pp. 123–133; *Oeuvres*, III. pp. 189–201), who followed up results obtained by Euler. Cf. also Legendre, *Zahlentheorie*, tr. Maser, I. pp. 212 sqq. Lagrange's proof is set out as shortly as possible in Wertheim's Diophantus, pp. 324–330. The theorem of Fermat in all its generality was proved by Cauchy (*Oeuvres*, II[e] série, Vol. VI. pp. 320–353); cf. Legendre, *Zahlentheorie*, tr. Maser, II. pp. 332 sqq.

Lagrange's Four Square Theorem

Lagrange's Four Square Theorem

Any non-negative integer can be expressed as the sum of four [integer] perfect squares.

Problems in Diophantus' Arithmetica

Let's look at a few more problems.

Book I Problem 17

To find four numbers such that the sums of all sets of three are given numbers.

Book I Problem 17

To find four numbers such that the sums of all sets of three are given numbers.
Let's say the sums of three are 20, 22, 24 and 27 respectively.

Book I Problem 17

To find four numbers such that the sums of all sets of three are given numbers.
Let's say the sums of three are $20, 22, 24$ and 27 respectively.
Let x be the sum of all four numbers.

Book I Problem 17

To find four numbers such that the sums of all sets of three are given numbers.
Let's say the sums of three are $20, 22, 24$ and 27 respectively.
Let x be the sum of all four numbers.
Then the numbers are $x - 22$, $x - 24$, $x - 27$, $x - 20$. Therefore, $4x - 93 = x$ and so $x = 31$. Thus, the numbers are $4, 7, 9$ and 11.

Book I Problem 18

To find three numbers such that the sum of any pair exceeds the third by a given number.

Book I Problem 18

To find three numbers such that the sum of any pair exceeds the third by a given number.
Given excesses 20, 30 and 40.

Book I Problem 18

To find three numbers such that the sum of any pair exceeds the third by a given number.
Given excesses 20, 30 and 40.
Let x_1, x_2 and x_3 be the three numbers. So $x_1 + x_2 = x_3 + 20$, $x_2 + x_3 = x_1 + 30$ and $x_3 + x_1 = x_2 + 40$. Summing these gives

$$2(x_1 + x_2 + x_3) = (x_1 + x_2 + x_3) + 90$$

and so $x_1 + x_2 + x_3 = 90$. Thus, $2x_3 = 70$ or $x_3 = 35$ and $2x_1 = 60$ or $x_1 = 30$ and $2x_2 = 50$ and so $x_2 = 25$.

Note about Book I Problem 18

Usually Diophantus solves problems using one variable when he can. In this problem, we see that he wasn't able to and did use multiple variables to help.

Book II Problem 8

To divide a given square number into two squares. (Recall: Rational Squares) Perhaps the most famous of Diophantus' problems

3. To find two numbers such that their product is to their sum or their difference in a given ratio [cf. I. 34].

4. To find two numbers such that the sum of their squares is to their difference in a given ratio [cf. I. 32].

5. To find two numbers such that the difference of their squares is to their sum in a given ratio [cf. I. 33].

6[1]. To find two numbers having a given difference and such that the difference of their squares exceeds their difference by a given number.

Necessary condition. The square of their difference must be less than the sum of the said difference and the given excess of the difference of the squares over the difference of the numbers.

Difference of numbers 2, the other given number 20.

Lesser number x. Therefore $x+2$ is the greater, and

$$4x+4=22.$$

Therefore $x=4\frac{1}{2}$, and

the numbers are $4\frac{1}{2}$, $6\frac{1}{2}$.

7[1]. To find two numbers such that the difference of their squares is greater by a given number than a given ratio of their difference[2]. [*Difference assumed.*]

Necessary condition. The given ratio being 3 : 1, the square of the difference of the numbers must be less than the sum of three times that difference and the given number.

Given number 10, difference of required numbers 2.

Lesser number x. Therefore the greater is $x+2$, and

$$4x+4=3\,.\,2+10.$$

Therefore $x=3$, and

the numbers are 3, 5.

8. To divide a given square number into two squares[3].

[1] The problems II. 6, 7 also are considered by Tannery to be interpolated from some ancient commentary.

[2] Here we have the identical phrase used in Euclid's *Data* (cf. note on p. 132 above): the difference of the squares is τῆς ὑπεροχῆς αὐτῶν δοθέντι ἀριθμῷ μείζων ἢ ἐν λόγῳ, literally "greater than their difference by a given number (more) than in a (given) ratio," by which is meant "greater by a given number than a given proportion or fraction of their difference."

[3] It is to this proposition that Fermat appended his famous note in which he enunciates what is known as the "great theorem" of Fermat. The text of the note is as follows:

"On the other hand it is impossible to separate a cube into two cubes, or a

Given square number 16.

x^2 one of the required squares. Therefore $16-x^2$ must be equal to a square.

Take a square of the form[1] $(mx-4)^2$, m being any integer and 4 the number which is the square root of 16, *e.g.* take $(2x-4)^2$, and equate it to $16-x^2$.

Therefore $4x^2-16x+16=16-x^2$,

or $5x^2=16x$, and $x=\frac{16}{5}$.

The required squares are therefore $\frac{256}{25}$, $\frac{144}{25}$.

9. To divide a given number which is the sum of two squares into two other squares[2].

biquadrate into two biquadrates, or generally *any power except a square into two powers with the same exponent.* I have discovered a truly marvellous proof of this, which however the margin is not large enough to contain."

Did Fermat really possess a proof of the general proposition that $x^m+y^m=z^m$ cannot be solved in rational numbers where m is any number >2? As Wertheim says, one is tempted to doubt this, seeing that, in spite of the labours of Euler, Lejeune-Dirichlet, Kummer and others, a general proof has not even yet been discovered. Euler proved the theorem for $m=3$ and $m=4$, Dirichlet for $m=5$, and Kummer, by means of the higher theory of numbers, produced a proof which only excludes certain particular values of m, which values are rare, at all events among the smaller values of m; thus there is no value of m below 100 for which Kummer's proof does not serve. (I take these facts from Weber and Wellstein's *Encyclopädie der Elementar-Mathematik*, I_2, p. 284, where a proof of the formula for $m=4$ is given.)

It appears that the Göttingen Academy of Sciences has recently awarded a prize to Dr A. Wieferich, of Münster, for a proof that the equation $x^p+y^p=z^p$ cannot be solved in terms of positive integers not multiples of p, if 2^p-2 is not divisible by p^2. "This surprisingly simple result represents the first advance, since the time of Kummer, in the proof of the last Fermat theorem" (*Bulletin of the American Mathematical Society*, February 1910).

Fermat says ("Relation des nouvelles découvertes en la science des nombres," August 1659, *Oeuvres*, II. p. 433) that he proved that *no cube is divisible into two cubes* by a variety of his method of *infinite diminution* (*descente infinie* or *indéfinie*) different from that which he employed for other negative or positive theorems; as to the other cases, see Supplement, sections I., II.

[1] Diophantus' words are: "I form the square from any number of ἀριθμοί *minus* as many units as there are in the side of 16." It is implied throughout that m must be so chosen that the result may be *rational* in Diophantus' sense, *i.e.* rational and positive.

[2] Diophantus' solution is substantially the same as Euler's (*Algebra*, tr. Hewlett, Part II. Art. 219), though the latter is expressed more generally.

Required to find x, y such that

$$x^2+y^2=f^2+g^2.$$

If $x \gtrless f$, then $y \lessgtr g$.

Put therefore $x=f+pz$, $y=g-qz$:

Book II Problem 8

To divide a given square number into two squares.
Given square number 16.

Book II Problem 8

To divide a given square number into two squares.
Given square number 16.
Let x^2 be one of the required squares. Therefore $16 - x^2$ must be equal to a square.
Take a square of the form $(mx - 4)^2$, m being any integer and 4 the number which is the square root of 16, e.g. take $(2x - 4)^2$ and equate it to $16 - x^2$.
Therefore $4x^2 - 16x + 16 = 16 - x^2$ or $5x^2 = 16x$ and $x = 16/5$.
The required squares are therefore 256/25 and 144/25.

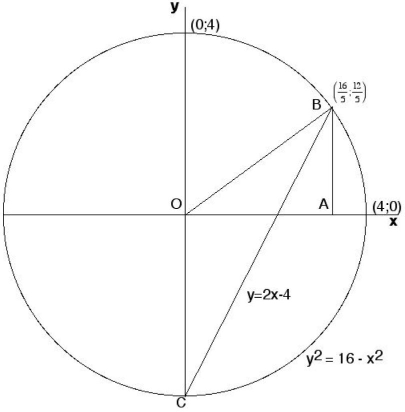
Geometric Interpretation

Set $y = mx - 4$. Plug this into $x^2 + y^2 = 16$. We know one root of the corresponding quadratic is rational, namely $(0, -4)$. In fact,

$$16 = x^2 + (mx - 4)^2 = (1 + m^2)x^2 - 8mx + 16$$

and so, $x = 0$ or $x = 8m/(1 + m^2)$ which is also rational so long as m is. Hence, infinitely many rational points can be found and in fact, given a rational point, joining the line from $(0, -4)$ to that point gives a unique m value.

Geometric Interpretation



https://en.wikipedia.org/wiki/Diophantus_II.VIII#/media/File:Diophantus_1_jpg.jpg

Byzantine scholar - John Chortasmenos (1370-1437)

Famous margin notes beside this problem [Herrin p.322]

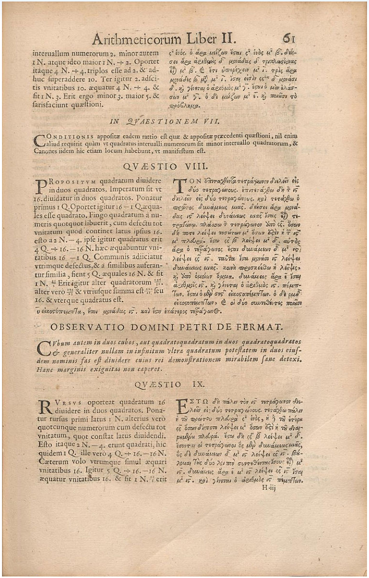
> *Thy soul, Diophantus, be with Satan because of the difficulty of your other theorems and particularly of the present theorem*

Pierre de Fermat's Margin Note

A more famous margin quote:

> *If an integer n is greater than 2, then $a^n + b^n = c^n$ has no solutions in non-zero integers a, b and c. I have a truly marvelous proof of this proposition which this margin is too narrow to contain.*

Original version of book is lost but Fermat's son edited the next edition in Diophantus published in 1670 to include the annotation.



interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem rattio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. [illegible] erit

https://en.wikipedia.org/wiki/File:Diophantus-II-8-Fermat.jpg

Book II Problem 13

From the same (required) number to subtract two given numbers so as to make both remainders squares.

Book II Problem 13

From the same (required) number to subtract two given numbers so as to make both remainders squares.
Given the numbers 6 and 7.
Seek a number which exceeds a square by 6, say $x^2 + 6$.

Book II Problem 13

From the same (required) number to subtract two given numbers so as to make both remainders squares.
Given the numbers 6 and 7.
Seek a number which exceeds a square by 6, say $x^2 + 6$.
Thus, $x^2 + 6 - 7 = x^2 - 1$ must also be a square.

Book II Problem 13

From the same (required) number to subtract two given numbers so as to make both remainders squares.
Given the numbers 6 and 7.
Seek a number which exceeds a square by 6, say $x^2 + 6$.
Thus, $x^2 + 6 - 7 = x^2 - 1$ must also be a square.
Say this is equal to $(x - 2)^2$.

Book II Problem 13

From the same (required) number to subtract two given numbers so as to make both remainders squares.
Given the numbers 6 and 7.
Seek a number which exceeds a square by 6, say $x^2 + 6$.
Thus, $x^2 + 6 - 7 = x^2 - 1$ must also be a square.
Say this is equal to $(x - 2)^2$.
Solving gives $x = 5/4$ and so the required number is

$$x^2 + 6 = \frac{25}{16} + 6 = \frac{121}{16}$$

(Diophantus actually gives two ways to solve this problem!)

Book II Problem 20

To find two numbers such that the square of either added to the other gives a square.

Book II Problem 20

To find two numbers such that the square of either added to the other gives a square.

Let x and $2x + 1$ be the numbers so that they satisfy one condition ($x^2 + 2x + 1$ is a square).

Book II Problem 20

To find two numbers such that the square of either added to the other gives a square.

Let x and $2x+1$ be the numbers so that they satisfy one condition (x^2+2x+1 is a square).

The other condition gives $4x^2+5x+1$. This is a square, say $(2x-2)^2$. Therefore, $x = 3/13$ and $2x+1 = 19/13$.

Book III Problem 21

To divide a given number into two parts and to find a square which, when added to either of the parts, gives a square. We will give the number 20 and the square $x^2 + 2x + 1$.

Book III Problem 21

To divide a given number into two parts and to find a square which, when added to either of the parts, gives a square. We will give the number 20 and the square $x^2 + 2x + 1$.
What polynomials can be added to $x^2 + 2x + 1$ to give another square?

Book III Problem 21

To divide a given number into two parts and to find a square which, when added to either of the parts, gives a square. We will give the number 20 and the square $x^2 + 2x + 1$.
What polynomials can be added to $x^2 + 2x + 1$ to give another square?
Let $2x + 3$ and $4x + 8$ be the squares. Then $6x + 11 = 20$ and so $x = 3/2$ whence 6 and 14 are the parts and the square is 25/4.

Arabic Book IV Problem 26

We wish to find two numbers one cubic and the other square such that the difference of their squares is a square number.

Arabic Book IV Problem 26

We wish to find two numbers one cubic and the other square such that the difference of their squares is a square number.
Let x^3 be the cube and $4x^2$ be the square.

Arabic Book IV Problem 26

We wish to find two numbers one cubic and the other square such that the difference of their squares is a square number.
Let x^3 be the cube and $4x^2$ be the square.
Set $x^6 - 16x^4$ to be $(3x^2)^2$.

Greek Book IV Problem 18

To find two numbers such that the cube of the first added to the second gives a cube and the square of the second added to the first gives a square.

Greek Book IV Problem 18

To find two numbers such that the cube of the first added to the second gives a cube and the square of the second added to the first gives a square.
Diophantus shows some of the discovery:
Let x be the first number. therefore the second is a cube number minus x^3, say $8 - x^3$. Then

$$(8 - x^3)^2 + x = x^6 - 16x^3 + x + 64 = \text{a square, say} = (x^3 + 8)^2$$

This gives $32x^3 = x$ or $32x^2 = 1$ which gives an irrational result. However, if 32 were a square, this would be rational. This 32 comes from 4 times 8 and so we need to substitute 8 with a number that when multiplied by 4 gives a square. This could be say $4^3 = 64$.

Greek Book IV Problem 18

To find two numbers such that the cube of the first added to the second gives a cube and the square of the second added to the first gives a square.

Greek Book IV Problem 18

To find two numbers such that the cube of the first added to the second gives a cube and the square of the second added to the first gives a square.
So assume x and $64 - x^3$ are the numbers. Therefore,

$$(64 - x^3)^2 + x = x^6 - 128x^3 + 4096 + x = \text{a square, say} = (x^3 + 64)^2$$

whence $256x^3 = x$ and $x = 1/16$. Hence, the numbers are $1/16$ and $64 - x^3 = 262143/4096$.

References

- Burton, D. (2011). The History of Mathematics : An introduction (Seventh ed.). New York: McGraw-Hill.
- Heath, T. (1921) A History of Greek Mathematics Volume II From Aristarchus to Diophantus. Oxford: Oxford University Press.
- Heath, T. (1910) Diophantus of Alexandria. Cambridge: Cambridge University Press. (Public Domain - see https://archive.org/details/diophantusofalex00heatiala)
- Herrin, Judith (2013). Margins and Metropolis: Authority across the Byzantine Empire. Princeton University Press.
- MacLeod, R. (2004). The Library of Alexandria Centre of Learning in the Ancient World (New pbk. ed.). London ; New York : New York.

References

- Pollard, J. and Reid, H. (2007) The Rise and Fall of Alexandria: Birthplace of the Modern World. New York:Penguin Group.
- Sesiano, J. (1982) Books IV to VII of Diophantus' Arithmetica In the Arabic Translation Attributed to Questa Ibn Luqa . New York: Springer-Verlag
- Tannery, P. (1893) Diophanti Alexandrini Opera omnia: cum graecis commentarii. Teubner (written in Latin archived here: https://archive.org/details/diophantialexan03plangoog)

References

- http://www.ancient.eu/timeline/Alexander_the_Great/
- https://www.britannica.com/place/Alexandria-Egypt
- http://www.encyclopedia.com/people/science-and-technology/mathematics-biographies/diophantus-alexandria
- Schappacher, N. www-irma.u-strasbg.fr/~schappa/NSch/Publications_files/1998cBis_Dioph.pdf
- Slides from CO 680 from Steve Furino