Epitaph of Diophantos of Alexandria (possibly 3rd century CE?):

This tomb holds Diophantos. Ah, how great a marvel! The tomb tells scientifically the measure of his life. God granted to him to be a boy for the sixth part of his life, and adding a twelfth part to this, his cheeks were clothed with down; he lit the light of wedlock after a seventh part, and five years after his marriage, he was granted a son. Alas! late-born wretched child; after attaining the measure of half his father's life, chill Fate took him. After consoling his grief with the science of numbers for four years, he ended his life. (*Greek Anthology*, 126)

From: **Book I** of the *Arithmetica* of Diophantos of Alexandria

(Not strictly literal) translation from the Greek by JL

Most honored Dionysius, knowing that you are eager to learn to [set up and] solve problems concerning numbers, I tried starting from the foundations that are the basis of these things to lay down the nature and the power of numbers.

This thing might seem more difficult since it is not yet familiar, for the souls of beginners do not hope to succeed, but it will be easy for you because of your enthusiasm and my exposition of the material; for desire comes to knowledge quickly when it receives teaching.

But besides these things you know that all numbers are compounded from some number of units, and their production has no limit. There happen to be among them:

- *squares*, which are formed by multiplying some number by itself, and this number is called the side of the square;
- *cubes*, which are formed from squares by multiplying by their sides;
- *power-powers*, which are formed by multiplying a square by itself;
- *power-cubes*, which are formed by from squares by multipying by the cube with the same side;
- *cubo-cubes*, which are formed by multiplying a cube by itself.

It turns out that most arithmetical problems are woven by adding or subtracting or multiplying or taking ratios of these with each other or with the sides. As you proceed along the path that will be shown to you, they are solved.

Each of these numbers has been accepted to be an element of the theory of arithmetic using an abbreviation.

- The square numbers are called powers and the sign of these is the Δ [capital "delta"] having an Υ [capital "upsilon"] superscript: Δ^{Υ} – "power." [JL: the Greek word is *dunamis*]
- The symbol for a cube is K with the Υ superscript: K^{Υ} – "cube." [JL: the Greek word is *kubos*]

- The symbol for a square multiplied by itself is two capital deltas with the Υ superscript: $\Delta^{\Upsilon}\Delta$ – "power-power."
- The symbol for a square multiplied by the cube of its side is ΔK with the Υ superscript: ΔK^{Υ} – "power-cube."
- The symbol for a cube multiplied by itself is the double K with superscript Υ: $K^{\Upsilon}K$ – "cubo-cube."
- The symbol for a number having none of these types, but having an indeterminate number of units in itself is ς.
- There is another constant part of definite numbers, the unit, and its symbol is M with superscript o: M^o – unit [JL: the Greek word is *monos*].

Just as the parts of numbers are named after the numbers[1], so the parts of the numbers just named will be given names derived from those numbers as follows:

from the number—the numbered part
from the power—the powered part
from the cube—the cubed part
from the power-power—the power-powered part
from the power-cube—the power-cubed part
from the cubo-cube—the cubo-cubed part

Each of these will have, in addition to the corresponding symbol of the number, the sign χ distinguishing its species [or type].

Now that I have set out for you the name of each of the numbers, I will go on to give their multplications. These will be almost clear from the names:

A number multiplied by a number makes a power [i.e. a square]
A number multiplied by [its] power makes a cube
A number multiplied by [its] cube makes a power-power
A number multiplied by [its] power-power makes a power-cube
A number multiplied by [its] power-cube makes a cubo-cube
A power multiplied by a power makes a power-power
A power multiplied by a cube makes a power-cube
A power multipled by a power-power makes a cubo-cube
A cube multplied by a cube makes a cubo-cube.

A number multiplied multiplied by its part makes a unit.

Since the unit does not change and stands forever, any species multiplied by it will have the same species.

When the parts having the same name are multiplied, they will make parts having the same name as the numbers. For instance, a numbered part multiplied by:

[1] JL: What is happening here is that Diophantos is giving names for the reciprocals of these different classes of numbers. For instance the reciprocal number 5 is the 1/5th part, the reciprocal of a square x^2 is a square part $1/x^2$ and so forth.

a numbered part makes a powered part
[its] powered part makes a cubed part
[its] cubed part makes a power-powered part
[its] power-powered part makes a power-cubed part
[its] power-cubed part makes a cubo-cubed part

That is, it will come out as the names suggest.

A numbered part multiplied

by a power makes a number
by a cube makes a power
by a power-power makes a cube
by a power-cube makes a power-power
by a cubo-cube makes a power-cube

A powered part multiplied:

by a number makes a numbered part
by a cube makes a number
by a power-power makes a power
by a power-cube makes a cube
by a cubo-cube makes a power-power

A cubed part [multiplied]:

by a number makes a powered part
by a power makes a numbered part
by a power-power makes a number
by a power-cube makes a power
by a cubo-cube makes a cube

A power-powered part [multiplied]:

by a number makes a cubed part
by a power makes powered part
by a cube makes a numbered part
by a power-cube makes a number
by a cubo-cube makes a power

A power-cubed part [multiplied]

by a number makes a power-powered part
by a power makes a cubed part
by a cube makes a powered part

by a power-power makes a numbered part
by a cubo-cube makes a number

A cubo-cubed part [multiplied]

by a number makes a power-cubed part
by a power makes a power-powered part
by a cube makes a cubed part
by a power-power makes a powered part
by a power-cube makes a numbered part

A lack times a lack is a presence, a lack times a presence is a lack, and the symbol for a lack is Λ [JL: from the Greek word *leipsis*].

Now that you have been apprised of the multiplications, the divisions of the species that have been set forth are clear. As a beginner in this business, it will be well to practice with addition and subtraction and multiplication with the species, and how you might add species, both present and lacking, with other species (which may themselves be present or lacking).

After these things, if it happens in some problem that some species are equal to the same species, but they are not of the same number, it will be necessary to subtract similar things from each of the two parts until one species becomes equal to one species. If somehow in either of the two parts or in both some lacking species are present, it will be necessary to add the lacking species in both parts, until the species of the two parts become present, and again to subtract similar things from similar things, until one species is left behind in each of the two parts.

Let this be practiced on what is set down in the propositions, if possible, until one species is left equal to one species. Later we will also show you how problems where two species are left equal to one are solved.

Now let us be on the way to the propositions, since we have gathered together much material on the species. They are many in number and great in bulk, and because of this they are established slowly for those who study them. Some of them are difficult to remember, so I decided to split them up where possible, and above all to begin with those that act as elements and proceed from the simpler to the more complex. In this way they will be accessible to beginners and their training will be more memorable, when their study in thirteen books has been completed.

Proposition 1. To divide the proposed number into two numbers with a given difference.

Let the given number be 100 and the difference be 40. To find the numbers. Let the lesser number be set out $\varsigma 1$. Then the larger will be $\varsigma 1 M^o 40$. Both together will be $\varsigma 2 M^o 40$. Therefore $M^o 100$ is equal to $\varsigma 2 M^o 40$. And from similar things take away similar things. I take away M^o40 from the M^o100 [and the $\varsigma2M^o40$], and the remaining $\varsigma2$ are equal to M^o60. Therefore each ς is M^o30. To what was set down: The lesser number will be M^o30 while the greater will be M^o70 and the demonstration is clear.

Proposition 2. It is necessary to divide the proposed number into to numbers in a given ratio.

Let it be proposed to divide the number 60 into two numbers in 3^{pl} [i.e. triple] ratio. Let the lesser number be set out $\varsigma1$. The the greater will be $\varsigma3$ and the greater is three times the lesser. The remaining requirement is that the two numbers [together] be equal to M^o60. But the two together are $\varsigma4$. So $\varsigma4$ is equal to M^o60, and ς equals M^o15. Then the smaller number is M^o15 and the larger is M^o45.

Proposition 3. To divide the proposed number into two numbers in a given ratio and a given difference.

Let it be proposed to divide the number 80 into two numbers such that the greater number is 3^{pl} the lesser and still exceeds by M^o4. Let the lesser number be set out $\varsigma1$. Then the greater is $\varsigma3$ and M^o4. The remaining thing I wish is that the two numbers together are M^o80. But the two together are $\varsigma4M^o4$. Therefore $\varsigma4M^o4$ and M^o80 are equal. And I take away similar things from similar things. It remains M^o76 is equal to $\varsigma4$ and ς will be M^o19. To what was set down: the lesser number will be M^o19 and the greater will be M^o61 [when the M^o4 which I took away from the M^o80 are added. For I took them away to find out how many M^o each number will be, and later I add the M^o4 to the larger number, after knowing how many are in each.]

Proposition 4. To find two numbers in a given ratio so that their difference is also given.

Let it be proposed that the larger number be 5^{pl} the smaller, and to make their difference M^o20. Let the lesser number be set out $\varsigma1$. Then the larger will be $\varsigma5$. The remaining thing I wish is that $\varsigma5$ exceed $\varsigma1$ by M^o20. But their difference is $\varsigma4$ and this equals M^o20. Therefore the smaller number is M^o5 and the larger is M^o25. And the larger continues to be 5^{pl} the smaller and the difference is M^o20.

Proposition 5. To divide the proposed number into two numbers so that of each of the numbers obtained, the given non-identical parts added together equal a given number.

It is clearly necessary for the given number to be between the two numbers that come about if the given non-identical parts of the proposed number are made.

Let it be proposed to divide 100 into two numbers so that of the first number the 3rd part and of the second number the 5th part taken together are M^o30. Let the 5th part of the second number be $\varsigma1$; the second number itself is then $\varsigma5$. Then the 3rd part of the first number is will be $M^o30\Lambda\varsigma1$, and the first number itself will be $M^o90\Lambda\varsigma3$. The remaining thing I wish is for the two numbers together to equal M^o100. But the two numbers together are $M^o 90\varsigma 2$; and these are equal to $M^o 100$. And from similar things similar things. Therefore $M^o 10$ will equal $\varsigma 2$ and ς will be $M^o 5$.

To what was set down. I set out the 5th part of the second number $\varsigma 1$. This equals $M^o 5$, and therefore the second number itself is $M^o 25$. The 3rd part of the first is $M^o 30 \Lambda \varsigma 1$, which is $M^o 25$, so the first number itself is $M^o 75$. And the 3rd part of the first number and the 5th part of the second number remain $M^o 30$ [together they make the proposed number].

Proposition 6. To divide the proposed number into two numbers such that the given part of the first exceeds the given part of the other by a given number.

It is clearly necessary that the given number is smaller than the number that comes about if the given part of the number proposed from the start in which the excess exists is taken.

Let it be proposed to divide 100 into two numbers such that the 4th part of the first exceeds the 6th part of the second by $M^o 20$.

I set out the 6th part of the second, $\varsigma 1$; the second number itself will be $\varsigma 6$. Then the 4th part of the first will be $\varsigma 1 M^o 20$, and therefore the first number itself will be $\varsigma 4 M^o 80$. The remaining thing I wish is that the two numbers added together give $M^o 100$. But the two numbers added together make $\varsigma 10 M^o 80$ and these are equal to $M^o 100$. From similar things similar things. What remains is $\varsigma 10$ is equal to $M^o 20$ and the $\varsigma 1$ becomes 2.

To what was set down. I set out the the 6th part of the second number $\varsigma 1$; it will be $M^o 2$ and therefore the number itself will be $M^o 12$. The 4th part of the first is $\varsigma 1 M^o 20$, so it is $M^o 22$, and therefore the first number itself is $M^o 88$. And the 4th part of the first number continues to exceed the 6th part of the second by $M^o 20$ and the two numbers together make the proposed number.

From: **Book II** of the *Arithmetica*

Proposition 8. To divide the proposed square into two square numbers.

Let it be proposed to divide the number 16 into two square numbers. Let the first number be set out $\Delta^{\Upsilon} 1$. Therefore the other number will be $M^o 16 \Lambda \Delta^{\Upsilon} 1$. It will therefore be necessary for $M^o 16 \Lambda \Delta^{\Upsilon}$ to be equal to a square. I form the square from however many ς's, Λ as many M^o as is the side of $M^o 16$, let it be $\varsigma 2 \Lambda M^o 4$. Then the square itself will be $\Delta^{\Upsilon} 4 M^o 16 \Lambda \varsigma 16$. These are equal to $M^o 16 \Lambda \Delta^{\Upsilon} 1$. Let the lack be added to both, and from similar things similar things.

Therefore $\Delta^{\Upsilon} 5$ are equal to $\varsigma 16$ and the ς becomes the 5th part of $16 M^o$.

The one number will be $256^{\backslash 25}$ [JL: This what our existing manuscripts write for the 25th part of 256, or $\frac{256}{25}$] and the other number will be $144^{\backslash 25}$ [JL: That is, $\frac{144}{25}$.] ...

Comments:

1. This is one of the few times when Diophantos uses rational numbers instead of integers in the solution of one of his problems.
2. John of Chortasmenos (1370 - 1437 CE) wrote the following marginal remark to this proposition "Thy soul, Diophantos, be with Satan because of the difficulty of your theorems."
3. In 1621 CE, Pierre de Fermat wrote in his margin at this point: "If an integer n is greater than 2, then $a^n + b^n = c^n$ has no solutions in nonzero integers a, b, and c. I have a truly marvelous proof of this proposition which the margin is too narrow to contain." This celebrated claim, which came to be known as *Fermat's Last Theorem*, was finally proved in the mid-1990's by Andrew Wiles and Richard Taylor using the theory of elliptic curves(!)