

**La place de la démarche algorithmique dans le projet de Diophante de développer  
« l'invention » dans les problèmes arithmétiques**

Jean Christianidis (Univ. of Athens), Alain Bernard (UPEC and Centre A. Koyré)

Symposium ALGO: Pratiques algorithmiques dans les mathématiques pré-modernes,  
Lille 13 oct.2011

**HANDOUT**

**Part I**

*Arithmetica* 14.25-16.7 Tannery

From now on, we shall follow the way along the propositions (*epi tas protaseis chôrsômen hodon*), having at our disposal much collected matter on the species themselves. Since <the things involved in the collected matter> are many in number and large in size, <and since> for this reason they are mastered only slowly by those who acquire them and <since> there are in them things that are difficult to memorize, I thought it worth to divide what in them is susceptible <of being divided>, and moreover to arrange those being at the beginning, by way of elements, from the most simple to the most complex, as it seems convenient to do. In this way, indeed, their route might become easier to follow for the beginners and their introduction will be memorized. As for their complete treatment, it will be done in thirteen books.

Part II / Diophantus *Arithmetica*, problem I.12

1.	Τὸν ἐπιταχθέντα ἀριθμὸν διελεῖν εἰς δύο ἀριθμοὺς δῖς, ὅπως ὁ εἷς τῶν ἐκ τῆς πρώτης διαιρέσεως πρὸς ἓνα τῶν ἐκ τῆς δευτέρας διαιρέσεως λόγον ἔχη δεδομένον, ὁ δὲ λοιπὸς τῶν ἐκ τῆς δευτέρας διαιρέσεως πρὸς τὸν λοιπὸν τὸν ἐκ τῆς πρώτης διαιρέσεως λόγον ἔχη δεδομένον.	To divide a prescribed number into two numbers twice, so that one of the <numbers obtained> from the first division should have a given ratio to one of the <numbers obtained> from the second division, and the remaining <number> of the second division should have a given ratio to the remaining <number> of the first division.	STATEMENT(S)
2.	Ἐπιτετάχθω δὴ τὸν ρ διελεῖν εἰς δύο ἀριθμοὺς δῖς, ὅπως ὁ μείζων τῶν ἐκ τῆς α <sup>ης</sup> διαιρέσεως τοῦ ἐλάσσονος τῶν ἐκ τῆς β <sup>ας</sup> διαιρέσεως ἦ β <sup>πλ.</sup> , ὁ δὲ μείζων τῶν ἐκ τῆς β <sup>ας</sup> διαιρέσεως τοῦ ἐλάσσονος τῶν ἐκ τῆς α <sup>ης</sup> διαιρέσεως ἦ γ <sup>πλ.</sup> .	Let it be prescribed again to divide the 100 into two numbers twice, so that the greatest <number obtained> from the first division should be double the least <number> of the second division, and the greatest <number> of the second division should be triple the least <number> of the first division.	
3.	Τετάχθω ὁ ἐλάσσων ὁ ἐκ τῆς β <sup>ας</sup> διαιρέσεως $s \bar{a}$ ,	Let the least of the second division be set ( <i>tetachtô</i> ) 1 <i>arithmos</i> .	POSITIONS = CORE OF THE SOLUTION
4.	ὁ ἄρα μείζων τῶν ἐκ τῆς α <sup>ης</sup> διαιρέσεως ἔσται $s \bar{\beta}$ .	The greatest <among the numbers obtained> from the first division, therefore, will be 2 <i>arithmoi</i> ,	
5.	ὁ ἐλάσσων ἄρα τῶν ἐκ τῆς α <sup>ης</sup> διαιρέσεως ἔσται $\dot{M} \bar{\rho} \wedge s \bar{\beta}$ .	and, consequently, the least from the first division <will be> 100 units wanting 2 <i>arithmoi</i> ;	
6.	καὶ ἐπεὶ ἐστὶν αὐτοῦ τριπλασίων ὁ μείζων τῶν ἐκ τῆς β <sup>ας</sup> διαιρέσεως, ἔσται $\dot{M} \bar{\tau} \wedge s \bar{\epsilon}$ .	and since the greatest from the second division is the triple of the latter, this will be 300 units wanting 6 <i>arithmoi</i> .	
7.	λοιπὸν ἐστὶ καὶ τοὺς τῆς β <sup>ας</sup> διαιρέσεως συντεθέντας ποιεῖν $\dot{M} \bar{\rho}$ .	There remains that the <numbers> of the second division, composed with each other, should make 100 units;	
8.	ἀλλὰ συντεθέντες ποιοῦσι $\dot{M} \bar{\tau} \wedge s \bar{\epsilon}$ .	but, when they are <indeed> put together, they make 300 units wanting 5 <i>arithmoi</i> .	
9.	ταῦτα ἴσα $\dot{M} \bar{\rho}$ ,	The latter are equal to 100 units,	
10.	καὶ γίνεται ὁ $s \bar{\mu}$ .	and the <i>arithmos</i> becomes 40 units.	EQ + EQ SOLVING
11.	ἐπὶ τὰς ὑποστάσεις. ἔταξα τὸν μείζονα τῶν ἐκ τῆς α <sup>ης</sup> διαιρέσεως $s \bar{\beta}$ , ἔσται $\dot{M} \bar{\pi}$ .	<Let us come> to the positions ( <i>epi tas hypostaseis</i> ). I have set ( <i>etaxa</i> ) the greatest of the <numbers out> of the first division 2 <i>arithmoi</i> , this will be 80 units;	TO THE POSITIONS
12.	τὸν δὲ ἐλάσσονα <τῶν ἐκ> τῆς αὐτῆς διαιρέσεως $\dot{M} \bar{\rho} \wedge s \bar{\beta}$ , ἔσται $\dot{M} \bar{\pi}$ .	<I have set> the least of the same division 100 units wanting 2 <i>arithmoi</i> , this will be 20 units;	
13.	τὸν δὲ μείζονα τὸν ἐκ τῆς β <sup>ας</sup> διαιρέσεως $\dot{M} \bar{\tau} \wedge s \bar{\epsilon}$ , ἔσται $M \bar{\xi}$ .	<I have set> the greatest of the second division 300 units wanting 6 <i>arithmoi</i> , this will be 60 units;	

14.	τὸν δὲ ἐλάσσονα τὸν ἐκ τῆς β <sup>α</sup> διαίρεσεως $\mathfrak{S} \bar{a}$ , ἔσται $M \bar{\mu}$ .	<I have set> the least of the second division 1 <i>arithmos</i> , this will be 40 units.	
15.	καὶ φανερὰ ἡ ἀπόδειξις.	And the proof is clear.	PROOF

### Our ‘symbolism’ for the schematic analysis of Diophantus’s problem:

The abbreviations we use are partly inspired by the ones used by Paul Ver Eecke in the comments accompanying his French translation of the *Arithmetica* (Diophante 1959). However, they are completed here by some specific signs for several crucial notions or procedures that are discussed for the first time in the present paper. Note, however, that this system of ‘transcription’ has intrinsic limits that become obvious in the case of operations (see below).

- Indeterminate numbers, which are either sought numbers or squares-to-be-obtained appearing in the statements of problems, are symbolized by capital letters. Thus,  $X, Y, X^2, Y^3$  are used for sought numbers. The squares to be obtained are sometimes abbreviated by a special symbol  $\square$
- The terms of the “arithmetical theory” are symbolized by lower case letters like  $x, x^2, x^3$ , etc. Thus, the unknown “*arithmos*” is symbolized by  $x$ .
- The signs for operations, like  $+$ ,  $-$ , etc. do not have the same meaning when used to connect the above symbols:
  - When they connect, capital letters, like  $X + Y$ , they denote the result of a prescribed addition between terms within the statement.
  - When they connect lower case letters, like  $1x^2 + 5x - 3$ , they denote a collection of species that are of different types. For a thorough discussion of this interpretation of such “expressions”, that are unlike modern ‘polynomials’

Paradoxically, then, these signs never denote the operations that are expressed in the Greek text, which are kept distinct from their outcomes. In particular, the sign  $-$ , when used for terms of the “arithmetical theory”, denotes a wanting term (cf. *leipsis*).

- The sign  $:=$  is used to introduce a position as a result.  
Examples:  $X := 1x, Y^2 := 2x^2, X + Y := 2x$ , etc.
- The sign  $=$  is used to denote finally obtained equations.  
Examples:  $5x + 2 = 3 - 1x, 1x + 1 = 4, 1x^2 - 1 = 2x + 3, 1x = 2$ , etc.
- The sign  $\Rightarrow$  is used to denote the prescriptive aspect of the prescription of a problem: it might be read “has to be” or “has to make”.  
Examples:  $X^2 + Y^2 \Rightarrow 16, Y + 12 \Rightarrow \square(V^2), XY + Gvn \Rightarrow \square(U^2)$ .
- The sign  $\rightarrow$  is used to denote the outcome of a procedure. Accordingly, this sign is used only in the simulators. Example:  $X^2 / x^2 + Y / (2x + 1) \rightarrow sq$ . The sign “/” indicates the double meaning of the algorithm, that is, as corresponding to a prescription of a problem (in which case the capital letters are taken into account), or as expressed within the “arithmetical theory” (in which case the lower case letters are taken into account).

### Part III

#### The method of simulation:

#### A method of invention in which procedural aspects are central

#### III.1) One first examples of simulation

##### a) problem II.20 (*Arithm.* 114.10-22)

1	To find two numbers, so that the square on each of the two, added to the other, makes a square. <sup>1</sup>	STAT.
2	Let the first <number> be set '1 <i>arithmos</i> ' ( $1x$ ), the second '1 unit <and> 2 <i>arithmoi</i> ' ( $2x + 1$ ), so that <i>the square on the first &lt;number&gt;, adding to itself the second, might produce a square.</i>	POSITIONS
3	There remains that the square on the second, adding to itself the first, <should> make a square.	
4	But the square on the second, adding to itself the first, makes 4 <i>dunameis</i> , 5 <i>arithmoi</i> and one unit ( $4x^2+5x+1$ ).	
5	And the latter <should be> equal to a square.	
6	I form ( <i>plassô</i> ) the square from two <i>arithmoi</i> wanting two units ( $2x-2$ ). The <square> itself makes 4 <i>dunameis</i> , 4 units wanting 8 <i>arithmoi</i> .	
7	And the < <i>arithmos</i> > gives 3 13 <sup>teens</sup> .	EQ
8	And the first will be 3 13 <sup>teens</sup> , the second 19 13 <sup>teens</sup> , and they make the problem.	NBS

##### b) Schematic presentation

Statement:  $? X, ? Y: X^2 + Y \Rightarrow \square(U^2) (E_1), Y^2 + X \Rightarrow \square(V^2) (E_2).$

The positions  $X := 1x$  and  $Y := 2x + 1$  are introduced on the basis of a justification, namely the italicized procedure, which is formulated in a sufficiently general manner so as to make possible the two following interpretations:

- It can be read as representing one of the two prescriptions, say the  $(E_1): X^2 + Y \Rightarrow \square$ .
- But it can also be related to the algorithm  $x^2 + (2x + 1) \rightarrow (x + 1)^2$ , which is entirely expressible in the terms of the "arithmetical theory" and corresponds to a tacit knowledge concerning the possible derivation of an expression ( $x^2$  added to  $2x + 1$ ) into another, namely  $(x + 1)^2$ .

Symbolic representation of the simulator:  $X^2 / x^2 + Y / (2x + 1) \rightarrow sq.$

The simulation, in this case, yields the two first positions:

<sup>1</sup>  $? X, ? Y: X^2 + Y \Rightarrow \square(U^2) (E_1), Y^2 + X \Rightarrow \square(V^2) (E_2).$

P #	Positions	Method	Heuristic explanation
1	$X := 1x$	simulation	simulator
2	$Y := 2x + 1$		$X^2 / x^2 + Y / (2x + 1) \rightarrow sq.$
3	$Y^2 + X := 4x^2 + 5x + 1$	rw-d	<i>loipon esti</i> + E <sub>2</sub>
4	$V := 2x - 2$	<i>plassô</i>	
5	$V^2 := 4x^2 + 4 - 8x$		
Implicit equation = $4x^2 + 5x + 1 = 4x^2 + 4 - 8x$ , hence $x = \sqrt[3]{13}$			

### c) Simulation and simulator: two definitions

#### 1) “Method of simulation”

We call “**simulation**” the method of invention by which one or more prescriptions might be ‘solved’ through *the explicit statement of a procedure that can be interpreted in two ways*, one related to the prescription, the other related to a corresponding procedure framed in the terms of the “arithmetical theory”.

#### 2) “Simulator”

We call “**simulator**” such an explicit procedure, from which several positions are set as starting points of the treatment of a problem. The simulator might be stated directly as a heuristic explanation for the positions, before or after taking them, or can itself be justified by an intermediary reasoning.

### d) remark

In problem II.20 the simulator was a procedure (by adding a number to a square we produce a square) and not an algorithm in the strict sense of the term. In contrast, in the following example the simulator is a true algorithm.

### III.2) Problem II.26

#### a) The problem

? X, ? Y:  $XY + X \Rightarrow \square(U^2)$  (E<sub>1</sub>),  $XY + Y \Rightarrow \square(V^2)$  (E<sub>2</sub>),  $U + V \Rightarrow 6$  (E<sub>3</sub>).

1	To find two numbers, so that their product, added to either, makes a square, and the sides on the obtained squares added together make a given number.	STAT
2	Let in be prescribed to make the <number> 6.	
3	Since, as soon as <i>there are two numbers, the greater of which is four times the lesser minus one unit, their product adding to itself the lesser makes a square</i> , I posit the lesser 1 <i>arithmon</i> (1x), the greater 4 <i>arithmous</i> wanting 1 unit (4x – 1) and it comes, similarly, that <i>their product adding to itself the lesser makes a square</i> .	POSITIONS
4	It remains that the <product>of them adding to itself the greater, that is, 4 <i>arithmous</i> wanting 1 unit (4x – 1), to make a square, the side of which is 6 units wanting the 2 <i>arithmous</i> (2x) of the side of the lesser,	
5	so that, according to the problem, the sides of the two, when taken together make 6 units.	
6	But the <product> of them adding to itself the greater makes 4 <i>dynameis</i> <and> 3 <i>arithmous</i> wanting 1 unit ( $4x^2 + 3x - 1$ ),	
7	while the <produced> from 6 units wanting 2 <i>arithmous</i> (6 – 2x), <makes> 4 <i>dynameis</i> <and> 36 units wanting 24 <i>arithmous</i> ( $4x^2 + 36 - 24x$ ).	
8	These are equal to each other.	
9	And the <i>arithmos</i> (x) becomes 37/27.	EQ
10	To the positions: I have set the lesser 1 <i>arithmon</i> , it will be 37	T.P
11	and the greater 4 <i>arithmous</i> wanting 1 unit, it will be 121.	
12	And the proposition holds.	

#### b) The method of simulation in this example:

To find two numbers, so that their product, added to either, makes a square, and the sides on the obtained squares added together make a given number (6 in the instance).

The first positions are obtained through the following justification:

Since, as soon as *there are two numbers, the greater of which is four times the lesser minus one unit, their product adding to itself the lesser makes a square*, I posit the lesser ‘1 *arithmon*’ (1x), the greater ‘4 *arithmous* wanting 1 unit’ (4x – 1) and it comes, similarly, that *their product adding to itself the lesser makes a square*.

As in the previous case, there is here a procedure (formulated in the first italicized sentence). In this case, the procedure is an algorithm and makes again possible the two following interpretations:

- (a) As one of the prescriptions  $XY + X \Rightarrow \square$ , once the “lesser” and “greater” are identified with each of the sought numbers.
- (b) As the algorithm  $x \times (4x - 1) + x \rightarrow (2x)^2$ , again expressible in the terms of the “arithmetical theory” and to which the reformulation strongly alludes. Later on, the text makes clear that  $2x$  is the side of the obtained square. (*Arithm.* 122.17).

In abbreviation, this double meaning can be written thus:  $X/x \times Y/(4x - 1) + X/x \rightarrow sq.$

### c) Schematic analysis of the problem

P #	Positions	Method	Heuristic explanation
1	$X := 1x$	simulation	simulator $X/x \times Y/(4x - 1) + X/x \rightarrow sq.$
2	$Y := 4x - 1$		
3	$U := 2x$		
4	$V := 6 - 2x$	rw-i	<i>loipon esti</i> + $E_2 + E_3 + P_3$
5	$XY + Y := 4x^2 + 3x - 1$	rw-d	$P_1, P_2, E_2$
6	$V^2 := 4x^2 + 36 - 24x$	rw-d	$P_4$

**Problem II.25**

To find two numbers so that the square on their sum, wanting either number, makes a square.

In our symbolism the problem is written:  $? X, ? Y: (X + Y)^2 - X \Rightarrow \square, (X + Y)^2 - Y \Rightarrow \square.$

Simulator and positions found by simulation:

“I first take some square, from which, by removing some <well-chosen> numbers, I leave out a square. Let <the number> be the <number> 16. *The latter, when it leaves out 12 units, becomes a square, and again when 7 units, it becomes a square.* Hence, I posit them again *en-dynamei*, so that the one is ‘12 *dynameis*’ ( $12x^2$ ), the other ‘7 *dynameis*’ ( $7x^2$ ) and the <square> on the two, ‘16 *dynameis*’ ( $16x^2$ ), and it remains that *the <square> on the two, wanting each of them, makes a square.*” (Arithm. 120.14–20)

Here a kind of generic procedure, which gives the rationale for the two simulators chosen, is given: “one square wanting one or the other number makes another square.” 16 being chosen for the first square, the two simulators deduced from this idea are  $16 - 12 \rightarrow sq.$  and  $16 - 7 \rightarrow sq.$  and are then restated “*en-dynamei*”, that is, as  $16x^2 - 12x^2 \rightarrow sq.$  and  $16x^2 - 7x^2 \rightarrow sq.$  More precisely, the last formulation makes a kind of synthesis of the various restatements:  $(X + Y)^2 / 16x^2 - X$  or  $Y / 12x^2$  or  $7x^2 \rightarrow sq.$

P #	Positions	Method	Heuristic explanation
1	$X := 12x^2$	Simulation	Generic simulator: $sq. - nb1 \text{ or } nb2 \rightarrow sq.$ Two resulting simulators: $(X + Y)^2 / 16 - X$ or $Y / 12$ or $7 \rightarrow sq.$ Reformulation ‘ <i>en-dynamei</i> ’: $(X + Y)^2 / 16x^2 - X$ or $Y / 12x^2$ or $7x^2 \rightarrow sq.$
2	$Y := 7x^2$		
3	$(X + Y)^2 := 16x^2$		