“ALGORITHMIC MATHEMATICS” AND “DIALECTIC MATHEMATICS”: The “Yin” and “Yang” in Mathematics Education

Man-Keung SIU
Department of Mathematics
University of Hong Kong
Hong Kong SAR, China
email: mathsiu@hkucc.hku.hk

ABSTRACT

Peter Henrici coined the term “algorithmic mathematics” and “dialectic mathematics” in a 1973 talk. I will borrow these two terms and attempt to synthesize the two aspects from a pedagogical viewpoint with illustrative examples gleaned from mathematical developments in Eastern and Western cultures throughout history. Some examples from my teaching experience in the classroom will also be given.

1 Introduction

At the 1973 Joint AMS-MAA (American Mathematical Society – Mathematical Association of America) Conference on the Influence of Computing on Mathematical Research and Education Peter HENRICI of Eidgenössische Technische Hochschule coined the terms "algorithmic mathematics" and "dialectic mathematics" and discussed the desirable equilibrium of these two polarities [8; see also 4, Chapter 4]. In this talk I will borrow these two terms and attempt to synthesize the two aspects from a pedagogical viewpoint with illustrative examples gleaned from mathematical developments in Eastern and Western cultures throughout history. This paper is to be looked upon as a preliminary version of the text of my talk, which will surely suffer from the lack of the much needed reflection which usually arises *after* the talk and the much desired stimulation which is brought about by the audience *during* the talk.

Maybe at the outset I should beseech readers to bear with a more liberal usage of the word "algorithm" in this talk, viz any well-defined sequence of operations to be performed in solving a problem, *not* necessarily involving branching upon decision or looping with iteration. In particular, this talk does *not* aim at probing the difference and similarity between the way of thinking of a mathematician and a computer scientist. (The latter question certainly deserves attention. Interested readers may wish to consult the text of a 1979 talk by Donald KNUTH [9].) Hopefully, the meaning I attach to the terms "algorithmic mathematics" and "dialectic mathematics" will become clearer as we proceed. Let me quote several excerpts from the aforementioned paper of Henrici to convey a general flavour before we start on some examples:

> "*Dialectic mathematics* is a rigorously logical science, where statements are either true or false, and where objects with specified properties either do or do not exist. *Algorithmic mathematics* is a tool for solving problems. Here we are concerned not only with the existence of a mathematical object, but also with the credentials of its existence. *Dialectic* mathematics is an intellectual game played according to rules about which there is a high degree of consensus. The rules of the game of *algorithmic* mathematics may vary according to the urgency of the problem on hand. ⋯ *Dialectic* mathematics invites contemplation. *Algorithmic* mathematics invites action. *Dialectic* mathematics generates insight. *Algorithmic* mathematics generates results." [8]

2 Examples of "algorithmic mathematics" and "dialectic mathematics"

My first example is a very ancient artifact dating from the 18th century B.C. (now catalogued as the Yale Babylonian Collection 7289), a clay tablet on which was inscribed a square and its two diagonals with numbers (in cuneiform expressed in the sexagesimal system) 30 on one side and 1.4142129... and 42.426388... on one diagonal (see Figure 1).

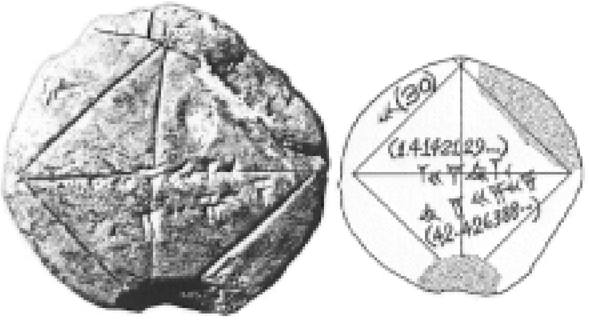

Figure 1

There is no mistaking its meaning, viz the calculation of the square root of 2 and hence the length of the diagonal of a square with side of length 30. The historians of mathematics Otto NEUGEBAUER and Abraham SACHS believe that the ancient Babylonians worked out the square root of 2 by a rather natural algorithm based on the following principle. Suppose x is a guess which is too small (respectively too large), then $2/x$ will be a guess which is too large (respectively too small). Hence, their average $\frac{1}{2}(x + 2/x)$ is a better guess. We can phrase this procedure as a piece of "algorithmic mathematics" in solving the equation $X^2 - 2 = 0$:

Set $x_1 = 1$ and $x_{n+1} = \dfrac{1}{2}(x_n + 2/x_n)$ for $n \geq 1$.
Stop when x_n achieves a specified degree of accuracy .

It is instructive to draw a picture (see Figure 2) to see what is happening. The picture embodies a piece of "dialectic mathematics" which justifies the procedure:

ξ is a root of $X = f(X)$ and ξ is in $I = [a, b]$.
Let f and f' be continuous on I and $|f'(x)| \leq K < 1$
for all x in I. If x_1 is in I and $x_{n+1} = f(x_n)$ for $n \geq 1$,
then $\lim_{n\to\infty} x_n = \xi$.

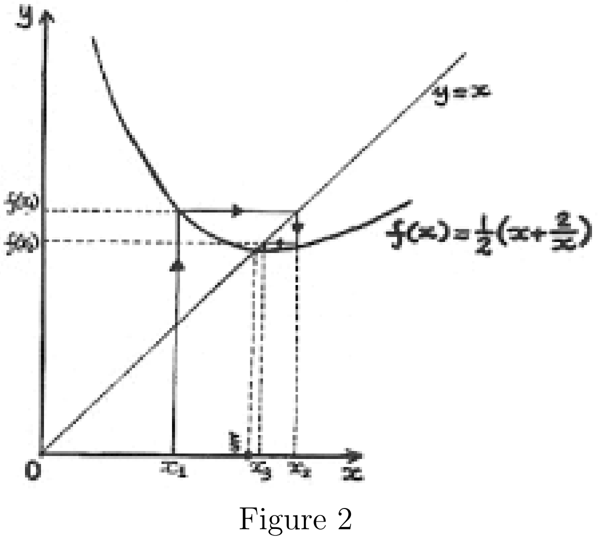

Figure 2

"Algorithmic mathematics" abounds in the ancient mathematical literature. Let us continue to focus on the extraction of square root. In the Chinese mathematical classics *Jiuzhang Suanshu* [*Nine Chapters On the Mathematical Art*] compiled between 100B.C. and 100A.D. there is this Problem 12 in Chapter 4:

> "Now given an area 55225 [square] *bu*. Tell: what is the side of the square?
> ... The Rule of Extracting the Square Root: Lay down the given area as *shi*. Borrow a counting rod to determine the digit place. Set it under the unit place of the *shi*. Advance [to the left] every two digit places as one step. Estimate the first digit of the root. ..." (translation in [3])

The algorithm is what I learnt in my primary school days. It yields in this case the digit 2, then 3, then 5 making up the answer $\sqrt{55225} = 235$. Commentaries by LIU Hiu in the mid 3rd century gave a geometric explanation (see Figure 3) in which integers $a \in \{0, 100, 200, \ldots, 900\}$, $b \in \{0, 10, 20, \ldots, 90\}$, $c \in \{0, 1, 2, \ldots, 9\}$ are found such that $(a + b + c)^2 = 55225$.

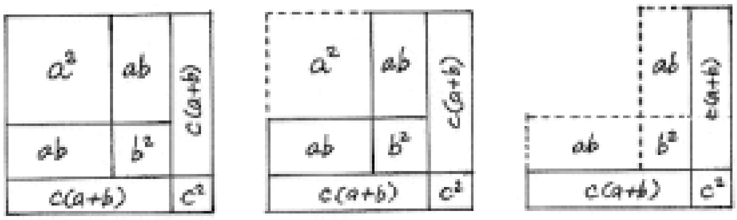

Figure 3

A suitable modification of the algorithm for extracting square root gives rise to an algorithm for solving a quadratic equation. One typical example is Problem 20 in Chapter 9 of *Jiuzhang Suanshu*:

> "Now given a square city of unknown side, with gates opening in the middle. 20 *bu* from the north gate there is a tree, which is visible when one goes 14 *bu* from the south gate and then 1775 *bu* westward. Tell: what is the length of each side?" (translation in [3])

Letting x be the length of each side, we see that the equation in question is $X^2 + 34X = 71000$. A slight modification of the picture in Figure 3 (see Figure 4) will yield a modified algorithm.

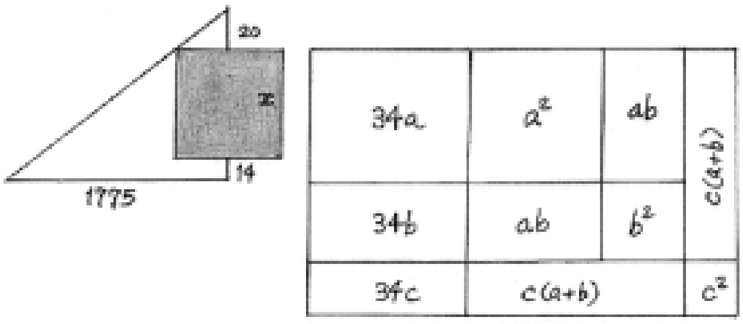

Figure 4

The same type of quadratic equations was studied by the Islamic mathematician Muhammad ibn Mūsā AL-KHWARIZMI in his famous treatise *Al-kitāb al-muhtasar fǐ* *hisab al-jabr wa-l-muqābala* [*The Condensed Book On the Calculation of Restoration And Reduction*] around 825A.D. The algorithm exhibits a different flavour from the Chinese method in that a closed formula is given. Expressed in modern day language, the formula for a root x of $X^2+bX=c$ is $x=\sqrt{(b/2)^2+c}-(b/2)$. Just as in the Chinese literature, the "algorithmic mathematics" is accompanied by "dialectic mathematics" in the form of a geometric argument (see Figure 5).

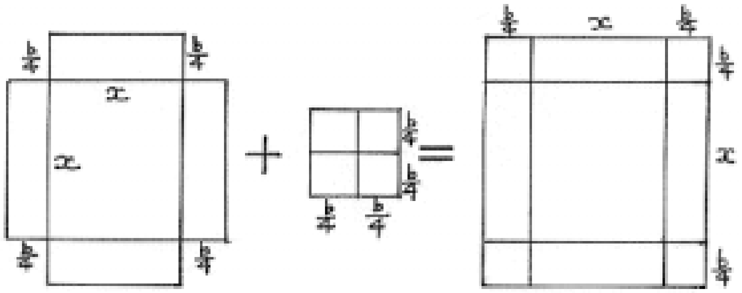

Figure 5

The author concluded by saying, "We have now explained these things concisely by geometry in order that what is necessary for an understanding of this branch of study might be made easier. The things which with some difficulty are conceived by the eye of the mind are made clear by geometric figures."

3 Intertwining of "algorithmic mathematics" and "dialectic mathematics"

Let us come back to the equation $X^2-2=0$. On the algorithmic side we have exhibited a constructive process through the iteration $x_{n+1}=\frac{1}{2}(x_n+2/x_n)$ which enables us to get a solution within a demanded accuracy. On the dialectic side we can guarantee the existence of a solution based on the Intermediate Value Theorem applied to the continuous function $f(x)=x^2-2$ on the closed interval $[1,2]$. The two strands intertwine to produce further results in different areas of mathematics, be they computational results in numerical analysis or theoretic results in algebra, analysis or geometry. At the same time the problem is generalized to algebraic equations of higher degree. On the algorithmic side there is the work of QIN Jiushao who solved equations up to the tenth degree in his 1247 treatise, which is equivalent to the algorithm devised by William George HORNER in 1819. On the dialectic side there is the Fundamental Theorem of Algebra and the search of a closed formula for the roots, the latter problem leading to group theory and field theory in abstract algebra. In recent decades, there has been much research on the constructive aspect of the Fundamental Theorem of Algebra, which is a swing back to the algorithmic side. A classic example to illustrate this back-and-forth movement between "algorithmic mathematics" and "dialectic mathematics" is the work of Paul GORDAN and David HILBERT in the theory of invariants at the end of the 19th century. Gordan was hailed as the "King of the Invariants" and in 1868 established the existence of a finite basis for the binary forms through hard and long calculations covering page after page. The work was so laborious already for the binary forms that people could not push forth the argument for forms of higher degree. Hilbert came along in 1888 to give an elegant short existence proof of a finite basis for forms of any degree. It is frequently reported that Gordan commented, upon learning of the proof by Hilbert, “This is not mathematics. This is theology.” What is less frequently mentioned is that Hilbert worked hard to find a constructive proof of his theorem on basis. He succeeded in 1892, finding a constructive proof through knowledge of the existence proof. Upon learning of this constructive proof, Gordan was reported to say, “I have convinced myself that theology also has its merits.” [12, Chapter V]

Thus we see that it is not necessary and is actually harmful to the development of mathematics to separate strictly “algorithmic mathematics” and “dialectic mathematics”. Traditionally it is held that Western mathematics, developed from that of the ancient Greeks, is dialectic, while Eastern mathematics, developed from that of the ancient Egyptians, Babylonians, Chinese and Indians, is algorithmic. As a statement in broad strokes this thesis has an element of truth in it, but under more refined examination it is an over-simplification. Let me illustrate with a second example. This example may sound familiar to readers, viz the Chinese Remainder Theorem. The source of the result, and thence its name, is a problem in *Sunzi Suanjing* [*Master Sun’s Mathematical Manual*] compiled in the 4th century that reads:

> “Now there are an unknown number of things. If we count by threes, there is a remainder 2; if we count by fives, there is a remainder 3; if we count by sevens, there is a remainder 2. Find the number of things.” (translation in [10])

To solve this problem, which can be written in modern terminology as a system of simultaneous linear congruence equations

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 7\ ,$$

the text offers three magic numbers 70, 21, 15 which are combined in a proper way to yield the least positive solution

$$2 \times 70 + 3 \times 21 + 2 \times 15 - 105 \times 2 = 23\ .$$

In his treatise *Suanfa Tongzong* [*Systematic Treatise on Arithmetic*] of 1592 CHENG Dawei even embellished this solution as a poem which reads:

“ ’Tis rare to find one man
Of seventy out of three,
There are twenty one branches
On five plum blossom trees.
When seven disciples reunite
It is in the middle of the month,
Discarding one hundred and five
You have the problem done.”

It is interesting to note (but I am no qualified historian of mathematics to trace the transmission of knowledge) that the same problem with its solution also appears in *Liber Abaci* of 1202 by Leonardo of Pisa, better known as FIBONNACI. It reads:

> “Let a contrived number be divided by 3, also by 5, also by 7; and ask each time what remains from each division. For each unity that remains from the division by 3, retain 70; for each unity that remains from the division by 5, retain 21; and for each unity that

> remains from the division by 7, retain 15. And as much as the number surpasses 105, subtract from it 105; and what remains to you is the contrived number." [4, p.188]

In ancient China the problem was handed down from generation to generation, gradually attaining a glamour which was attached to events as disparate as a legendary enumeration of the size of his army by the great general HAN Xin in the late 3rd century B.C. to a parlour trick of guessing the number of a collection of objects. (The story about Han Xin may explain a common confusion some people make in identifying the author of *Sunji Suanjing* with another Sun Ji who flourished seven centuries earlier and who was famous for his treatise on military art.) This much is a familiar story told and re-told. We will turn to look at the problem from an angle not as commonly adopted by popular accounts.

The first time I myself encountered the name of the Chinese Remainder Theorem (CRT) explicitly mentioned was when I, as a student, read Chapter V of *Commutative Algebra* by Oscar ZARISKI and Pierre SAMUEL [14]. The name is given to Theorem 17 about a property of a Dedekind domain, with a footnote that reads:

> "A rule for the solution of simultaneous linear congruences, essentially equivalent with Theorem 17 in the case of the ring J of integers, was found by Chinese calendar makers between the fourth and the seventh centuries A.D. It was used for finding the common periods to several cycles of astronomical phenomena."

In many textbooks on abstract algebra the CRT is phrased in the ring of integers $\mathbb{Z}$ as an isomorphism between the quotient ring $\mathbb{Z}/M_1 \ldots M_n\mathbb{Z}$ and the product $\mathbb{Z}/M_1\mathbb{Z} \times \cdots \times \mathbb{Z}/M_n\mathbb{Z}$ where M_i, M_j are relatively prime integers for distinct i, j. A more general version in the context of a commutative ring with unity R guarantees an isomorphism between $R/I_1 \cap \cdots \cap I_n$ and $R/I_1 \times \cdots \times R/I_n$ where $I_1, \ldots, I_n$ are ideals with $I_i + I_j = R$ for distinct i, j. Readers will readily provide their own "dialectic" proof of the CRT.

For many years I have been curious as to how the abstract CRT develops from the concrete problem in *Sunzi Suanjing*. One mostly cited (but not quite accurate) account appears in Volume II of *History of the Theory of Numbers* by Leonard Eugene DICKSON which says:

> "Sun-Tsŭ, in a Chinese work Suan-ching (arithmetic), about the first century A.D., gave in the form of an obscure verse a rule called t'ai-yen (great generalization) to determine a number having the remainders 2, 3, 2, when divided by 3, 5, 7, respectively. ..." [5, Chapter II]

This account probably originated from a series of articles published in the Shanghai newspaper *North-China Herald* titled "Jottings on the science of the Chinese" written by the British missionary Alexander WYLIE of the London Missionary Society. Wylie was one of the most prominent pioneers in the study of Chinese Science after Antoine GAUBIL of the first half of the 18th century and Edouard BIOT of the first half of the 19th century. In No. 116 (October 1852) of the *North-China Herald* he wrote:

> "The general principles of the *Ta-yen* are probably given in their simplest form, in the above rudimentary problem of Sun Tsze;

> Subsequent authors enlarging on the idea, applied it with much effect to that complex system of cycles and epicycles which form such a prominent feature in the middle-age astronomy of the Chinese. The reputed originator of this theory as applied to astronomy is the priest Yih Hing who had scarely finished the rough draft of his work *Ta-yen leih sháo*, when he died A.D. 717. But it is in the "Nine Sections of the art of numbers" by Tsin Keu chaou that we have the most full and explicit details on this subject. ..."

The account of Wylie was subsequently translated into German by K.L. BIERNATZKI in 1856, elaborated by L. MATTHIESSEN in 1874/76, who pointed out that the Chinese result is same as that expounded by Carl Friedrich GAUSS in Section II of his *Disquisitiones Arithmeticae* of 1801 [6]. (Kurt MAHLER clarified this mistaken point in a short paper published in *Mathematische Nachrichten* in 1958 [11].)

The author of the 1247 treatise *Shushu Jiuzhang* [*Mathematical Treatise in Nine Sections*] referred to in Wylie's account was one of the most famous Chinese mathematicians of the 13th century by the name of QIN Jiushao (Tsin Keu chaou). From the first two problems in Book I we can discern the source of the problem as well as the naming of the technique he introduced, viz "Da Yan (Great Extension) art of searching for unity". Problem 1 states:

> "In the *Yi Jing* [*Book of Changes*] it is said, "The Great Extension number is 50, and the Use number is 49." Again it is said, "It is divided into 2 [parts], to represent the spheres; 1 is suspended to represent the 3 powers; they are drawn out by 4, to represent the 4 seasons; three changes complete a symbol, and eighteen changes perfect the diagrams." What is the rule for the Extension and what are the several numbers?" (translation in Wylie's article)

This is a problem about the art of fortune telling by combination of blades of shi grass. It provides an exercise about residue classes of congruence. Problem 2 states:

> "Let the solar year be equal to $365\frac{1}{4}$ days, the moon's revolution, $29\frac{499}{940}$ days, and the Jia Zi, 60 days. Suppose in the year A.D. 1246, the 53rd day of the Jia Zi is the Winter solstice or 1st day of the Solar year; and the 1st day of the Jia Zi is the 9th day of the month. Required the time between two conjunctions of the commencement of these three cycles; also, the time that has already elapsed, and how much as yet to run." (translation in Wylie's article)

This is a problem about the reckoning of calendar where the number of days was counted from a beginning point called the Shang Yuan, that being the coinciding moment of the winter solstice, the first day of the lunar month and also the first day of the cycle of sixty.

Let us phrase the "Da Yan art of searching for unity" in modern terminology to illustrate the algorithmic thinking embodied therein. The system of simultaneous congruence equation is

$$x \equiv A_1 \pmod{M_1}, \qquad x \equiv A_2 \pmod{M_2}, \; \ldots\;, \; x \equiv A_n \pmod{M_n}\ .$$

Qin's work includes the general case when $M_1, \dots, M_n$ are not necessarily mutually relatively prime. His method amounts to arranging to have $m_i | M_i$ with $m_1, \dots, m_n$ mutually relatively prime and $LCM(m_1, \dots, m_n) = LCM(M_1, \dots, M_n)$. An equivalent problem is to solve $x \equiv A_i \pmod{m_i}$ for $i \in \{1, \dots, n\}$, which is solvable if and only if $GCD(M_i, M_j)$ divides $A_i - A_j$ for all $i \neq j$. The next step in Qin's work reduces the system (in the case $M_1, \dots, M_n$ are mutually relatively prime) to solving separately a single congruence equation of the form $k_i b_i \equiv 1 \pmod{M_i}$. Finally, in order to solve the single equation $kb \equiv 1 \pmod{m}$ Qin uses reciprocal subtraction, equivalent to the famous euclidean algorithm, to the equation until 1 (unity) is obtained.

Writing out the algorithm in full, we have

$$m = bq_1 + r_1, b = r_1 q_2 + r_2, r_1 = r_2 q_3 + r_3, \text{ etc. with } m > b > r_1 > r_2 > \cdots$$

so that ultimately r_i becomes 1. Set $k_1 = q_1$, then $k_1 b \equiv q_1 b \equiv -r_1$ (all congruences refer to modulo m). Set $k_2 = k_1 q_2 + 1$, then $k_2 b \equiv k_1 q_2 b + b \equiv -r_1 q_2 + b \equiv r_2$. Set $k_3 = k_2 q_3 + k_1$, then $k_3 b \equiv k_2 q_3 b + k_1 b \equiv r_2 q_3 - r_1 \equiv -r_3$. Set $k_4 = k_3 q_4 + k_2$, then $k_4 b \equiv k_3 q_4 b + k_2 b \equiv -r_3 q_4 + r_2 \equiv r_4$, etc. In general, we have $k_i b \equiv (-1)^i r_i \pmod{m}$. This algorithm provides a method for solving $kb \equiv 1 \pmod{m}$ as well as a proof that what is calculated is a solution. The method is to start with $(1, b)$ and change (k_i, r_i) to (k_{i+1}, r_{i+1}), stopping when $r_i = 1$ and i is even. Then k_i is a solution. For example, to solve $14k \equiv 1 \pmod{19}$ we start with $(1, 14)$, which is changed to $(1, 5)$, then to $(3, 4)$, then to $(4, 1)$, then to $(15, 1)$. Hence 15 is a solution. When the calculation is performed by manipulating counting rods on a board as in ancient times, the procedure is rather streamlined. Within this algorithmic thinking we can discern two points of dialectic interest. The first is how one can combine information on each separate component to obtain a global solution. This feature is particularly prominent when the result is formulated in the CTR in abstract algebra. The second is the use of linear combination which affords a tool for other applications such as for curve fitting or the Strong Approximation Theorem in valuation theory.

It is not surprising that the euclidean algorithm is used in Qin's work. The principle was familiar to the ancient Chinese who explained it in Chapter 1 of *Jiuzhang Suanshu* as:

> "Rule for reduction of fractions: If [the denominator and numerator] can be halved, halve them. If not, lay down the denominator and numerator, subtract the smaller number from the greater. Repeat the process to obtain the *dengsu* (greatest common divisor). Reduce them by the *dengsu*." (translation in [3])

It is called the euclidean algorithm in the Western world because it is contained in the first two propositions of Book VII of *Elements* compiled by EUCLID in about 300 B.C. If we read these two propositions we would be struck by its strong algorithmic flavour. Proposition 1 states:

> "Two unequal numbers being set out, and the less being continually subtracted in turn from the greater, if the number which is left never measures the one before it until an unit is left, the original numbers will be prime to one another." (translation in [7])

This is followed by Proposition 2 which says:

> "Given two numbers not prime to one another, to find their greatest common measure." (translation in [7])

A reading of the proofs of these two propositions will offer the reader a more balanced view of the style of the book *Elements*. The kind of mathematics developed in *Elements* is traditionally seen as an archetype of "dialectic mathematics". This more balanced view betrays the over-simplified belief that Eastern-Western mathematics is synonymous with algorithmic-dialectic mathematics. Furthermore, some people even stress above all only the formal and rigorous aspect of "dialectic mathematics". I will now follow the reasoning put forth by S.D. AGASHE [1] to reveal the (somewhat algorithmic) background and motives of the mathematics contained in the first two books of *Elements*. Proposition 14 in Book II addresses the construction of a square equal (in area) to a given rectilinear figure. It seems the problem of interest is to compare two rectilinear figures, whose one-dimensional analogue of comparing two line segments is easy. For two line segments we can put one onto the other and see which one lies completely inside the other (or is equal to the other). Actually this is what Proposition 3 of Book I sets out to do:

> "Given two unequal straight lines, to cut off from the greater a straight line equal to the less." (translation in [7])

To justify this result we have to rely on Postulate 1, Postulate 2 and Postulate 3. Unfortunately, for rectilinear figures the problem is no longer as straightforward, except for the case of two squares when we can reduce the investigation to the sides of each square by putting one onto the other so that one square lies completely inside the other (or is equal to the other). Incidentally we need Postulate 4 to guarantee that. Hence we have found a way to compare two rectilinear figures, viz we try to reduce a rectilinear figure to a square, which is the content of Proposition 14 in Book II:

> "Construct a square equal to a given rectilineal figure." (translation in [7])

Let us first try to reduce a rectangle to a square. A rectangle can be readily converted to an *L*-shaped gnomon which is the difference between two squares. Actually that is the content of Proposition 5 in Book II (see Figure 6).

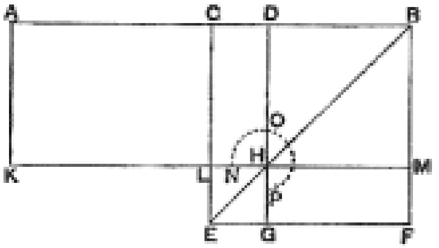

Figure 6

To make the difference of two squares a square we can ask a reversed question about the sum of two square being equal to a square. The latter question is answered by the famous Pythagoras' Theorem which is Proposition 47 in Book I! To complete the picture we must construct a rectangle equal to a rectilinear figure. By decomposing a rectilinear figure into triangles and by contructing a rectangle (or more generally a parallelogram with one angle given) equal to each triangle, the problem will be solved. The construction of a parallelogram (with one angle given) equal to a triangle is the content of Proposition 42, Proposition 44 and Proposition 45 in Book I, whose proofs all rely on Postulate 5 about parallelism. Viewed in this way, the axiomatic approach exemplified in *Elements* gains a richer meaning.

4 Pedagogical viewpoint

I now come to the pedagogical viewpoint. In the first part of my talk I tried to show how the two aspects — "algorithmic mathematics" and "dialectic mathematics" — intertwine with each other. It reminds me of the "yin" and "yang" in Chinese philosophy in which the two aspects complement and supplement each other with one containing some part of the other. (To go even further than that I would even borrow a metaphor probably from the biologist and popular science writer Stephen Jay GOULD: Is a zebra a white animal with black stripes or a black animal with white stripes?) If that is the case, then in the teaching of mathematics we should not just emphasize one at the expense of the other. When we learn something new we need first to get acquainted with the new thing and to acquire sufficient feeling for it. A procedural approach helps us to prepare more solid ground to build up subsequent conceptual understanding. In turn, when we understand the concept better we will be able to handle the algorithm with more facility. In the mathematics education community there has been a long-running debate on procedural vs conceptual knowledge, or process vs object in learning theory, or computer vs no-computer learning environment. In a more general context these are all related to a debate on algorithmic vs dialectic mathematics, which are actually not two opposing forces but can be joined to provide an integrated way of learning and teaching. I will now give five examples on learning and teaching, with the last two having more to do with research. I apologize for the obvious lopsided emphasis on algebra in these five examples. My excuse is that they all have to do with my own classroom experience.

(1) Solving a system of linear equations by reduction to echelon form is clearly algorithmic in nature. (By the way, the algorithm was explicitly recorded and explained in Chapter 8 of *Jiuzhang Suanshu*. The title of the chapter itself is telling — *Fangcheng*, which means literally "the procedure of calculation by a rectangular array".) However, a clear understanding of this working does much to help us understand the more abstract and theoretical part of linear algebra and see why many of the concepts and definitions make sense. I will not therefore regard an exercise in manipulating a system of linear equations as a routine exercise for those who are less apt at coping with abstract theory, but as a preparation for it. Suitably dressed up, even a routine exercise can become a useful lead into interesting and useful theory. As an example, we can ask:

> "Let W_1 be the subspace in $\mathbb{R}^3$ spanned by $(1,1,2)$, $(3,0,-1)$, $(1,-2,-5)$ and let W_2 be the subspace in $\mathbb{R}^3$ spanned by $(4,1,1)$, $(1,4,-1)$, $(2,-7,3)$. Calculate the intersection of W_1 and W_2. Describe the geometry of it."

An ad hoc calculation in this concrete case supported by a clear geometric picture, with

$(4, 1, 1)$ lying on the line of intersection of the two hyperplanes W_1 and W_2, leads to a more theoretical discussion in a general situation.

(2) As a pupil I came across in school algebra many homework problems which ask for writing expressions like $p^3q + pq^3$ or $5p^2 - 3pq + 5q^2$ or $p^4 + q^4$ or ... in terms of a, b, c where p, q are the roots of $aX^2 + bX + c = 0$. Each time I could arrive at an answer, maybe sometimes after long calculation. I used to query why an answer must come up for such so-called "symmetric" expressions. It was only many years later that I came to understand this in the form of the Fundamental Theorem on Symmetric Polynomial. There are different proofs for the result and it can be formulated in a rather general context of polynomials over a commutative ring with unity. But I still find it helpful to work out one example in an algorithmic fashion to get a flavour of the dialectic proof. For instance let us try to express the polynomial

$$X_1^3X_2^2 + X_2^3X_3^2 + X_3^3X_1^2 + X_1^2X_2^3 + X_2^2X_3^3 + X_3^2X_1^3$$

in terms of $\sigma_1 = X_1+X_2+X_3$, $\sigma_2 = X_1X_2+X_2X_3+X_3X_1$, $\sigma_3 = X_1X_2X_3$. Naturally we can write the polynomial in X_1, X_2, X_3 as a polynomial in X_3 with coefficients involving X_1, X_2, i.e.

$$f(X_1, X_2, X_3) = (X_1^3X_2^2 + X_1^2X_2^3) + (X_1^3 + X_2^3)X_3^2 + (X_1^2 + X_2^2)X_3^3 \ .$$

Applying our knowledge of polynomials in X_1, X_2 (after so much working in school algebra), we arrive at

$$f(X_1, X_2, X_3) = \tau_1\tau_2^2 + (\tau_1^3 - 3\tau_1\tau_2)X_3^2 + (\tau_1^2 - 2\tau_2)X_3^3$$

where $\tau_1 = X_1 + X_2$, $\tau_2 = X_1X_2$. Now, write $\sigma_1 = \tau_1 + X_3$, $\sigma_2 = \tau_2 + \tau_1X_3$, $\sigma_3 = \tau_2X_3$. From the first two relationships we can express τ_1, τ_2 in terms of σ_1, σ_2 and X_3, i.e. $\tau_1 = \sigma_1 - X_3$, $\tau_2 = \sigma_2 - \sigma_1X_3 + X_3^2$. Substituting τ_2 back to the third relationship we can express $X_3^3 = \sigma_3 - \sigma_2X_3 + \sigma_1X_3^2$. Hence we can express the coefficients $\tau_1\tau_2^2$, $\tau_1^3 - 3\tau_1\tau_2$, $\tau_1^2 - 2\tau_2$ in terms of $\sigma_1, \sigma_2, \sigma_3$ and X_3 up to the second power. Substituting back to $f(X_1, X_2, X_3)$ we obtain, after some rather tedious (but worthwhile!) work,

$$f(X_1, X_2, X_3) = \sigma_1\sigma_2^2 - 2\sigma_1^2\sigma_3 - \sigma_2\sigma_3 \ .$$

Note that suddenly all terms involving X_3 vanish and that is the answer we want! Coincidence in mathematics is rare. If there is any coincidence, it usually begs for an explanation. The explanation we seek in this case will lead us to one proof of the Fundamental Theorem on Symmetric Polynomial.

(3) The simplest type of extension field discussed in a basic course on abstract algebra is the adjunction of a single element algebraic over the ground field, say $\mathbb{Q}$. The element α, say in $\mathbb{C}$, is said to be algebraic over $\mathbb{Q}$ if α is the zero of some polynomial with coefficients in $\mathbb{Q}$. The dialectic aspect involves the "finiteness" of the extension field $\mathbb{Q}(\alpha)$ viewed as a finite-dimensional vector space over $\mathbb{Q}$. It is helpful to go through some algorithmic calculation to experience the "finiteness". For instance, take $\alpha = \sqrt{2}$. It is easy to see that a typical element in $\mathbb{Q}(\alpha)$ (by knowing what $\mathbb{Q}(\alpha)$ stands for) is of the form $(a + b\alpha)/(c + d\alpha)$ where a, b, c, d are in $\mathbb{Q}$, because any term involving a higher power of α can be ground down to a linear combination (over $\mathbb{Q}$) of 1 and α.

The procedure on conjugation learnt in school allows us to revert the denominator as part of the numerator, i.e.

$$\begin{aligned} 1/(c+d\alpha) &= (c-d\alpha)/(c+d\alpha)(c-d\alpha) = (c-d\alpha)/(c^2-2d^2) \\ &= [(c/(c^2-2d^2)] + [(-d)/(c^2-2d^2)]\alpha \ . \end{aligned}$$

Hence, a typical element in $\mathbb{Q}(\alpha)$ is of the form $a + b\alpha$ where a, b are in $\mathbb{Q}$. It is more instructive to follow with a slightly more complicated example such as $\alpha = \sqrt{1+\sqrt{3}}$. It is not much harder to see that we can confine attention to linear combinations of $1, \alpha, \alpha^2, \alpha^3$, but this time it is much more messy to revert the denominator as part of the numerator. This will motivate a more elegant dialectic proof modelled after the algorithmic calculation for $\alpha = \sqrt{2}$. Another useful piece of knowledge about algebraic elements is: If a and b (say in $\mathbb{C}$) are algebraic over $\mathbb{Q}$, then $a+b$ is algebraic over $\mathbb{Q}$. The dialectic aspect involves the notion of "finiteness" by viewing $\mathbb{Q}(a,b)$ as a finite-dimensional vector space over $\mathbb{Q}$. Going through an algorithmic calculation may help to consolidate understanding. For instance, take $\sqrt{2}$, which is algebraic over $\mathbb{Q}$ as a zero of X^2-2, and take $\sqrt[3]{3}$, which is algebraic over $\mathbb{Q}$ as a zero of $X_3^3 - 3$. Try to find a polynomial with coefficients in $\mathbb{Q}$ such that $\sqrt{2}+\sqrt[3]{3}$ is a zero of it. We can follow an algorithm which expresses $X^2-2 = (X-\sqrt{2})(X+\sqrt{2})$ and $(X^3-3) = (X-\alpha)(X-\alpha\omega)(X-\alpha\omega^2)$ where $\alpha(\in \mathbb{R})$ is such that $\alpha^3 = 3$ and $\omega = \frac{1}{2}(\sqrt{3}i - 1)$, then consider the polynomial

$$g(X) = (X-\sqrt{2}-\alpha)(X+\sqrt{2}-\alpha)(X-\sqrt{2}-\alpha\omega)(X+\sqrt{2}-\alpha\omega)(X-\sqrt{2}-\alpha\omega^2)(X+\sqrt{2}-\alpha\omega^2)$$

which reduces after some calculation to $X^6 + 6X^4 - 6X^3 + 12X^2 - 36X + 1$ (noting that $\alpha^3 = 3$ and $1 + \omega + \omega^2 = 0$). It is certainly not incidental that ultimately no coefficient involves $\sqrt{2}$ or α or ω ! Further enquiry will suggest a constructive proof of the general result by making use of symmetric polynomials.

(4) To begin with a simple example, let z be a (complex) root other than 1 of the equation $X^5 - 1 = 0$, so $z^4 + z^3 + z^2 + z + 1 = 0$, or $(z^1 + z^4) + (z^2 + z^3) = 0$. Write $\eta_0 = z^1 + z^4$ and $\eta_1 = z^2 + z^3$ and note that $\eta_0 + \eta_1 = -1$ and $\eta_0\eta_1 = \eta_0 + \eta_1 = -1$. Hence, η_0, η_1 are roots of $Y^2 + Y - 1 = 0$, say

$$\eta_0 = \frac{-1+\sqrt{5}}{2} \ , \ \eta_1 = \frac{-1-\sqrt{5}}{2} \ .$$

From $\eta_0 = z + \frac{1}{z}$ we obtain $z^2 - \eta_0 z + 1 = 0$ so that one value for z is $z = \frac{1}{2}(\eta_0 + \sqrt{\eta_0^2 - 4}) = \frac{1}{4}[-1 + \sqrt{5} + \sqrt{-10-2\sqrt{5}}]$. This calculation is the basic idea Carl Friederich GAUSS applied to solve the equation $X^N - 1 = 0$ where N is a prime number. (I have a slight suspicion that Gauss was inspired by the work of Alexandre-Théophile VANDERMONDE who solved that equation in a brilliant 1774 paper titled "Memoire sur la résolution des équations" [13, Chapter 11 and Chapter 12].) The calculation will go through in general if at each stage we can break up the sum of powers of z into two halves, which is the case when N is of the form $2^{2^s} + 1$, i.e. N is a Fermat prime. This is the theory of cyclotomy developed by GAUSS in Section VII of his *Disquisitiones Arithmeticae* of 1801 in connection with his celebrated discovery in 1796 of the constructibility of a regular seventeen-sided polygon by straight-edge and compasses [6].

We now go tangentially off the work of Gauss but take with us one crucial point: express $\eta_0\eta_1$ in the form $a\eta_0 + b\eta_1 + c$ for some integers a, b, c. Let p be an odd prime of the form $2f + 1$ and g is a primitive root of p. Let $C_0 = \{g^{2s} | s \in \{0, 1, 2, \ldots, f - 1\}\}$ and $C_1 = \{g^{2s+1} | s \in \{0, 1, 2, \ldots, f - 1\}\}$, then $\{1, 2, \ldots, p-1\}$ is decomposed into the disjoint union $C_0 \cup C_1$. We call C_0, C_1 cyclotomic classes and $(i, j) = |(C_i+1) \cap C_j|$ (with $i, j \in \{0, 1\}$) cyclotomic numbers. If $\eta_0 = \sum_{t \in C_0} z^t$ and $\eta_1 = \sum_{t \in C_1} z^t$, then it turns out that $\eta_0 + \eta_1 = -1$ and $\eta_0\eta_1 = (1, 0)\eta_0 + (1, 1)\eta_1 + c$ where c is the number of 0 in $C_0 + C_1$ (repetition counted). More generally, let p be a prime number and $q = p^\alpha = ef+1$ and g is a generator of the multiplicative group of the finite field $GF(q)$, which is decomposed into a disjoint union $C_0 \cup C_1 \cup \cdots \cup C_{e-1}$ where $C_i = \{g^{es+i} | S \in \{0, 1, 2, \ldots, f - 1\}\}$ (cyclotomic class). We call $(i, j) = |(C_i+1) \cap C_j|$ (with $i, j \in \{0, 1, \ldots, e-1\}$) cyclotomic numbers. The fascinating property which comes out of the calculation is that, when and only when $(i, 0) = (f - 1)/e$ for all $i \in \{0, 1, \ldots, e - 1\}$, then C_0 is a difference set in $GF(q)$, i.e. each nonzero element in $GF(q)$ is the difference $x - y$ of the same number of pairs of elements (x, y) in $C_0 \times C_0$. For instance, this is true for $q = 11$ so that $C_0 = \{1, 3, 4, 5, 9\}$, the set of quadratic residues modulo 11, is a difference set. If you look at all the differences (modulo 11) $x - y$ of pairs (x, y) of numbers in C_0, you will find each nonzero number appearing exactly twice. Research on difference sets is a nice mixture of "algorithmic mathematics" and "dialectic mathematics".

(5) The last example is a personal anecdote about a piece of research work. Let me first describe the problem. Let F be the finite field with $q = p^s$ elements, i.e. $F = GF(q)$. A function $f : F \to \mathbb{C}$ is called a nontrivial multiplicative character of F if $f(0) = 0$, $f(1) = 1$ but $f \not\equiv 1$ on $F^* = F \setminus \{0\}$, and $f(b_1b_2) = f(b_1)f(b_2)$ for all b_1, b_2 in F. In this case, it is well-know that

$$\sum_{b \in F} f(b)\overline{f(b+a)} = \begin{cases} q - 1 & \text{if } a = 0\ ; \\ -1 & \text{if } a \neq 0\ . \end{cases} \qquad (\#)$$

Harvey COHN asks whether the converse is true: If $f : F \to \mathbb{C}$ is such that $f(0) = 0$, $f(1) = 1$, $|f(a)| = 1$ for all a in F^* and (#) holds, must f be a nontrivial multiplicative character of F? In the summer of 1996 I could settle the real case (so that $f(a)$ is either 1 or -1 for nonzero a) with an affirmative answer when F is a prime field. That much is "dialectic mathematics". I failed to extend the argument to the case when F is not necessarily a prime field. Hence the work was put aside until my interest was resurrected in the spring of 1999 when a young colleague, Stephen CHOI, gave a seminar on the same problem arising in a different context, attacked by a different approach. Naturally we joined forces to look at the general case. We noted that (#) involves only the addition in F but not the multiplication in F. If we compose a specific injective multiplicative character $\chi : F \to \mathbb{C}$ of F with an additive bijection $\varphi : F \to F$, then $f = \chi \circ \varphi$ satisfies (#) since χ satisfies (#). It remains to see if there exists any additive bijection φ which is not multiplicative. I turned to "algorithmic mathematics" by actually doing the calculation using a representation of F as the quotient ring of $GF(p)[X]$ modulo the ideal generated by an irreducible polynomial of degree s. One day upon re-checking the calculation of some concrete cases, I found an error, which I corrected. But in either case — the original incorrect version and the correct version — (#) was satisfied. To my dismay more errors in the calculation were detected, but each time, with correction or no correction, (#) was still satisfied. That made me become aware that more often than not, φ is not multiplicative. Finally we could prove this and give a negative answer to the problem in the case of non-prime fields [2].

5 Epilogue

To conclude I would like to share with readers a Zen saying from the Tang monk Qingyuan Weixin:

> "Before I had studied Zen for thirty years, I saw mountains as mountains, and waters as waters. When I arrived at a more intimate knowledge, I come to the point where I saw the mountains are not mountains, and waters are not waters. But now that I have got its very substance I am at rest. For it is just that I see mountains once again as mountains, and waters once again as waters."

REFERENCES

[1] S.D. Agashe, The axiomatic method: Its origin and purpose, *Journal of the Indian Council of Philosophical Research*, 6(3)(1989), 109-118.

[2] K.K. Choi, M.K. Siu, Counter-examples to a problem of Cohn on classifying characters, *J. Number Theory*, 84 (2000), 40-48.

[3] J.N. Crossley, A.W.C. Lun, K.S. Shen, *The Nine Chapters On the Mathematical Art: Companion and Commentary*, Oxford University Press, Oxford, 1999.

[4] P.J. Davis, R. Hersh, *The Mathematical Experience*, Birkhäuser, Boston-Basel-Stuttgart, 1980.

[5] L.E. Dickson, *History of the Theory of Numbers, Volume II*, Chelsea Publishing Company, New York, 1920.

[6] C.F. Gauss, *Disquisitiones Arithmeticae* (translation by A.A. Clarke), Yale University Press, New Haven, 1966.

[7] T.L. Heath, *The Thirteen Books of the Elements*, 2nd edition, Cambridge University Press, Cambridge, 1925; reprinted by Dover, New York, 1956.

[8] P. Henrici, Computational complex analysis, *Proc. Symp. Appl. Math.*, 20(1974), 79-86.

[9] D.E. Knuth, Algorithms in modern mathematics and computer science, in *Algorithms In Modern Mathematics and Computer Science*, (eds.) A.P. Ershon, D.E. Knuth, Springer-Verlag, New York-Heidelberg, 1981, 82-99.

[10] L.Y. Lam, T.S. Ang, *Fleeting Footsteps: Tracing the Conception of Arithmetic and Algebra in Ancient China*, World Scientific, Singapore-New Jersey-London-Hong Kong, 1992.

[11] K. Mahler, On the Chinese Remainder Theorem, *Mathematische Nachrichten*, 18(1958), 120-122.

[12] C. Reid, *Hilbert*, Springer-Verlag, New York-Heidelberg, 1970.

[13] J.P. Tignol, *Lécons sur la théorie des équations*, Institut de Mathématique Pure et Appliquée, Université Catholique de Louvain, Louvain-la-Neuve, 1980.

[14] O. Zariski, P. Samuel, *Commutative Algebra, Volume I*, Van Nostrand, Princeton, 1958.