SOME REMARKS ON THE THEOREM ABOUT THE INFINITY OF PRIME NUMBERS

Ercole Castagnola*, Roberto Tortora**

**Nucleo di Ricerca Didattica, Università Federico II, Naples, Italy*

***Dipartimento di Matematica e Applicazioni, Università Federico II, Naples, Italy*

Abstract. *The famous Euclid's theorem on the infinity of prime numbers represents a typical case of difficulties for students. In this work we present some reflections and proposals to contrast such difficulties, focused on: a) the problem of proofs by contradiction – in this case viewed as inessential – also in relation with the dychotomy potential/actual infinite; b) a comparison between the current proof and the original Euclid's one, especially for its potential influence on the building of algebraic language; c) the opportunity of privileging students' exploratory activities as necessary steps toward the construction of the proof, and the chances that a wise use of technologies offer to this exploration.*

INTRODUCTION AND THEORETICAL FRAME

It is widely recognized that students encounter several difficulties in understanding and producing mathematical proofs. The problem is somewhat specific in Geometry, where the role of pictures can be seen as a guide to reasoning. But a large part of theorems in Geometry appear as self-evident, so that a proof hardly seems necessary, while in a few cases proofs are difficult, with the result that students often resigns themselves to learn by hearth without any awareness of the arguments. On the contrary, in Arithmetics some meaningful properties can be selected, at the same time simple and non-trivial, therefore very suitable for introducing students to proofs. This is the case of Euclid's famous theorem on the infinity of prime numbers.

In this paper we want to stress some particular features of this theorem, from historical, epistemological and didactical points of view. In particular we want: a) to analyze the influence of a comparison between the original proof and two modern versions of it, on the development of students' linguistic competences (the use of algebraic symbols); b) to show how the difficulties of students in understanding a proof by contradiction, can, in a sense, be neglected, since it is neither strictly necessary nor effective to proceed in this case in an indirect way; c) to stress the role of technologies in assisting the heuristic stage as a necessary step before the proof, both for motivation and for a (partially) autonomous construction of the proof itself.

Many authors have variously emphasized the importance of using history (in particular, original sources) in Mathematics Education (Fauvel & Van Maanen, 2000), (Katz, 2000), (Furinghetti & Radford, 2002), (Castagnola, 2002a). It is not a case that in the last years many texts and materials have been specifically devoted to teachers: for instance, (Berlinghoff & Gouvêa, 2004), with a lot of references, and (Katz & Michalowicz, 2005); or websites like (1), a real mine of historical information; or *Convergence*, an online magazine, (website (4)), where mathematics, history and teaching interact. The introduction of a historical dimension reaches many goals: it humanizes the image of mathematics and helps in modifying the current view of mathematics as made of continuous progresses, showing a lot of sudden turning-points, wrong paths and blind alleys, which gives meaning to otherwise boring students' efforts; and it offers materials to develop intuition, particularly when presented using modern symbols, verbal expressions and cultural tools, instead than, according to Recapitulation Principles, those employed by ancient authors.

A different problem concerns students' difficulties in using algebraic language for abstracting and generalizing (Radford, 2000). Such difficulties are still more evident when a proof is involved (Mariotti, 1998), in particular a proof by contradiction.

Calculators, in particular the graphic-symbolic ones, are widely recognized as precious tools in school practice (Castagnola, 2002b). First of all, they free both teachers and students from the risk of "getting lost" in cumbersome calculations, allowing to turn attention to problems, at the same time more meaningful from a mathematical point of view and closer to the complexity of real world (Kaput, 2002), (Paola, 2006). Moreover, technological tools, bearing an "embodied intelligence", can be seen as powerful means to facilitate objectification and generalization of mathematical concepts (Radford, 2003), and to overcome some students' rigidities ("the prime numbers are only 2, 3, 5" or "the *really existing* numbers are only small integers"). Finally, in Mathematics Education a combined use of history and technology has already taken into account (Castagnola, 2004).

THE THEOREM ON THE INFINITY OF PRIME NUMBERS

The theorem on the infinity of prime numbers is one of the most famous and of the most "beautiful" in the history of mathematics. Several proofs have been produced (see for instance the website (3)), but the best known, modelled on Euclid's original proof, is surely the most easily understood, a striking example of simplicity and elegance. In spite of that, this proof appears much more obscure for students than we could think at first sight. A deep and careful analysis of the proof and of its didactical implications is presented in (Polya, 1973). After that, many authors have focused their attention on the difficulties involved in the contradiction argument employed in the proof, e.g. (Reid & Dobbin, 1998). Other authors have underlined the logical subtleties, all but easy to be understood, involved in such kind of reasoning (Antonini, 2003), (Antonini & Mariotti, 2006); or the necessity to enter an "imaginary" world, where the usual rules of logic can be put in doubt (Leron, 1985). (For more references, see the quoted papers). In particular, Leron notes how the "distance" between the assumption *a contrario* and the conclusion causes the total loss of all the constructions performed in the intermediate steps, erroneously perceived as meaningless.

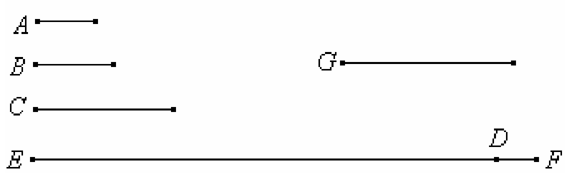
We believe that this kind of difficulties constitute a very serious problem. But since, in the specific case of our theorem, reasoning by contradiction does not seem to us anyhow necessary for the proof, we don't enter here into this subject, which surely deserves further attention, as we intend to do elsewhere. Instead, we prefer to devote our attention to other aspects. In particular, we believe that a big difficulty is connected with the idea of infinity, another one with the use of algebraic notations. Moreover, we think that comparing the actual proof with the original Euclid's version can help students to overcome such difficulties. Another decisive help comes from technological tools, today easily available in classwork.

We want to begin comparing three versions of the proof: the original Euclid's one (Proposition 20, book IX of *Elements*), as reported in (Heath, 1956); the "modern" (1925) version of the same author; and that used today in mathematics texts.

I. Euclid's version.

"PROPOSITION 20. ***Prime numbers are more than any assigned multitude of prime numbers.***

Let *A, B, C* be the assigned prime numbers; I say that there are more prime numbers than *A, B, C.* For let the least number measured by *A, B, C* be taken, and let it be *DE*; let the unit *DF* be added to *DE.* Then *EF* is either prime or not.



First, let it be prime; then the prime numbers *A, B, C, EF* have been found which are more than *A, B, C*.

Next, let EF not be prime; therefore it is measured by some prime number [VII. 31]. Let it be measured by the prime number G. I say that G is not the same with any of the numbers A, B, C. For, if possible, let it be so. Now A, B, C measure DE; therefore G also will measure DE. But it also measure EF. Therefore G, being a number, will measure the remainder, the unit DF: which is absurd. Therefore G is not the same with any one of the numbers A, B, C. And by hypothesis it is prime.

Therefore the prime numbers A, B, C, G have been found which are more than the assigned multitude of A, B, C. Q.E.D." (Heath, 1956, v. 2, p. 412)

II. Heath's version

"The number of prime numbers is infinite.

Let *a, b, c, … k* be any prime numbers. Take the product *abc···k* and add unity. Then (*abc···k* + 1) is either a prime number or not a prime number.

(1) If it *is*, we have added another prime number to those given.

(2) If it is *not*, it must be measured by some prime number [VII. 31], say *p*. Now *p* cannot be identical with any of the prime numbers *a, b, c, … k*. For, if it is, it will divide

> *abc*···*k*. Therefore, since it divides (*abc*···*k* + 1) also, it will measure the difference, or unity: which is impossible.

Therefore in any case we have obtained one fresh prime number. And the process can be carried on to any extent". (Heath, 1956, v. 2, p. 413)

III. A typical today version

There exist infinitely many prime numbers.

Let us suppose that all the prime numbers are the following: $p_1, p_2, \ldots, p_n$. The purpose is to prove that there is a prime number not included in this list. For that, consider the natural number $M = p_1 \cdot p_2 \cdots p_n + 1$ and examine the two alternatives:

Case 1. If M is prime, then it is certainly a "new" prime not included in the previous list, because it is greater than each number $p_1, p_2, \ldots, p_n$.

Case 2. If M is composite, then it has a prime divisor q. We say that q does not belong to the initial list of prime numbers. In fact, if $q = p_k$ for some k, then q would divide both M and $p_1 \cdot p_2 \cdots p_n$ and therefore also their difference $M - p_1 \cdot p_2 \cdots p_n = 1$. But the prime number q cannot be a divisor of 1. This *contradiction* implies that q is different from every p_k and hence it is the new prime we were looking for.

TWO EPISTEMOLOGICAL QUESTIONS

It is very interesting to compare the three proofs. The substance of reasoning is evidently the same, but many meaningful differences leap before our eyes, concerning the meaning of the concepts involved, the "sense" of infinity, the language employed, and so on. (Many interesting comments on Euclid's "style" are reported in the historical website (2)). As an example, Euclid's notion of prime number is different from the nowadays accepted one: "*A **prime number** is that is measured by a unit alone*." (Definition 11, Book VII). Thus, Euclid, like the overwhelming majority of our students, does not consider among the possible divisors of a number the number itself (a divisor must be smaller than the number that it divides). This allows an interesting discussion on the evolution of mathematical definitions (see, for this, (Paola, 2000), (Zaslavsky & Shir, 2005)).

Of course, a detailed analysis of all the differencies between the proofs would bring us very far. Here we want to focus our attention on two particular points: the roles of the reasoning by contradiction and of infinity in the proof of the theorem, and the evolution of algebraic linguistic tools used to denote numerical variables.

The roles of the proof by contradiction and of infinity

By comparing the different proofs, but also their statements, we can note that Euclid doesn't mention directly the *infinity* of prime numbers. His conception of infinity is *potential*: whatever collection of prime numbers we start with, there is always another prime number not included in it (and the proof shows in what way "to build it"); i.e. prime numbers are always *more* than any established quantity of them.

It is clearly a way of perceiving the infinity more familiar to students; in fact, it corresponds to the very early way of understanding natural numbers as an infinite collection, in accordance with the fact that for every natural number *n*, big as it can be, there is a bigger one: the *successor* of *n*. In our opinion this is the only way of conceiving the infinity at the beginning of secondary school. Well, if we state the theorem as Euclid did, then we realize that the proof is direct and even "constructive"; and that nothing prevents us to conclude the proof saying: "Therefore the prime numbers are infinitely many".

The need for the proof by contradiction, whose length – the length of permanence in the "absurd" world – can however be reduced (Leron, 1985), rises on the contrary from the fact that the subtle, and very awkward for students, concept of actual infinity is employed, whose definition is, among other things, given by negation: a set is infinite if it is *not* equinumerous to any initial segment {1, 2, …., *n*} of the set *N* of natural numbers[1]. To deny such a property we need a double negation: we suppose, by contradiction, that the prime numbers are finitely many, therefore it is not true that doesn't exist an *n* for which they can be put in a one-to-one correspondence with the set {1, 2, …., *n*}; therefore such an *n* exists and this allows to represent the prime numbers as $p_1, p_2, \ldots, p_n$. Then the proof goes on till the conclusion. It is quite evident that such a way to present the result makes it uselessly involved, by bringing logical and linguistic subtleties in the foreground, and hiding the substance and the constructiveness of the main argument.

On the development of algebraic notations

Let us compare the ways by which the first prime numbers are denoted in the three proofs. In Euclid's proof 3 prime numbers are considered, denoted by the 3 first letters of the alphabet. The proof is than carried out in a way that suggests that if, instead of 3, we had used any number, the result should have been the same. A particular case is treated, but "we see" that it has a general value. The use of the number 3 in Euclid (by the way, it would be amusing to ask why the choice turns just to 3, but this is another talk) is similar to the use and the drawing of a "generic" triangle to argue about any triangle, a question on which many authors have discussed, from Kant onwards, see for instance (Lolli, 2005). This way of proceeding is surely a little "bug", if we see it with the eyes of modern rigour (it is likely that Euclid were aware of this, but he had not at his disposal a more rigorous linguistic tool), but it is also the way we proceed very often also today in mathematical communication, evidently because the greater concreteness of the particular case yields greater effectiveness. Moreover, it stimulates the ability to integrate intuition and reasoning and to control and keep distinct what is specific from what is general.

[1] Not to speak of the deep theoretical problems underlying the definition of an infinite set: as it is well known, the definition is not unique, and the Dedekind's one (a set is infinite if it is equipotent to a proper subset), is equivalent to the first one only if we accept the axiom of choice. The questions involved are by far too challenging for students.

In Heath's version the first prime numbers are denoted by a, b, c, … k, the first letters of the alphabet. The "analogy" between the alphabetical ordering and the order of natural numbers is still kept, but the trick of the dots allows to directly treat the case of any number. Also this linguistic solution can be criticized: after all, k is the 11^{th} letter of the (English) alphabet, but it indicates, on the contrary, any position in the alphabet (evidently 11 seems a big enough number to assume this role). But such a criticism is expression of an excessive pedantry, since in this case (as, and perhaps better, than in Euclid's version) no misunderstanding is possible: as a matter of fact, this type of notation is everyday systematically used without any trouble.

The notation in the third version of the proof is completely different. The first prime numbers are represented by p_1, p_2, …, p_n, where indexes and dots are used to give an account of the indefinite amount of involved elements. There is no doubt about the superiority of this notation, the result of a long evolution and of more and more urgent demands of rigour in the history of mathematics. But we do raise some doubts on the opportunity of using this notation at school, or at least we wonder if it is correct to propose this sophisticated form of language with too much confidence and without the necessary care and graduality. Probably it could help to introduce previously the *list* (an ordered set of elements), an important data structure of computer science, widely used in many scientifical contexts, for instance in statistics.

Coming to students' behaviour, we know that they tend to see in the use of letters only a shortened way to describe some property. For instance they interpret without any difficulty an expression like $A = ½·b·h$ as the formula for the area of a triangle. It is more difficult for them to use an expression containing letters as a tool for abstraction and generalization (Radford, 2000).

In fact, students feel the modern notation in the proof of our theorem too involved, and in general prefer Euclid's proof. This can be observed whenever the proof is proposed by the teacher, and, if they choose by themselves the symbols to represent the situation, almost no one uses a notation similar to the modern one, while Euclid's or Heath's notations appear often. Moreover, we have not to forget that doesn't exist any formula with n as a variable to represent the n^{th} prime number, contrarily to what happens for simpler sequences. For instance it is less difficult (but by no means trivial) to accept the symbol $2k–1$ to represent the general odd number: the reason is that the sequence 1, 3, 5, …, of odd numbers is easily recognised to be generated by natural numbers, by subtracting a unit from the double of each of them, so the symbol $2k–1$ looks exactly as the expression of such a procedure.

We can resume our discussion saying that the proof "with indexes" doesn't convey anything more then the classic one. By this, we are not saying that indexes shouldn't be used (they are useful and sometimes necessary, for example for lists), but only that we must carefully arrive to this point and do not overlap the effort of a proof to that of a too subtle and not strictly necessary use of linguistic tools.

THE ROLE OF TECHNOLOGY IN THE EXPLORATORY PROCESS

According to a constructivistic point of view, we believe that a mathematical result can come in a class only after an exploratory process. In our case, as in other ones, this approach enhances motivation and understanding of the statement of the theorem and of its proof; and, as we will see, it offers also the possibility to touch other topics, to formulate conjectures, to discover properties. But, in order to be able to carry the exploration far enough, technology turns out to be an essential instrument. In this section we illustrate the main lines of a widely experimented didactical path inspired to the above principles. In the classwork the exploratory activity is always intertwined with readings from original sources, and is performed by individual work and collective discussions.

A first activity consists of trying to understand how prime numbers are arranged among natural numbers. For instance, we can build a table collecting the number of primes in each century from 1 to 1000, like the following one (Burton, 2005, p. 383):

Interval	1 - 100	101 - 200	201 - 300	301 - 400	401 - 500	501 - 600	601 - 700	701 - 800	801 - 900	901 - 1000
Number of primes	25	21	16	16	17	14	16	14	15	14

By inspection of this table (and, if necessary, of larger ones, to be found on catalogues or on websites like (3)), we note that prime numbers, though irregularly, tend to become rarer and rarer. It is known (and can be shown to students) that for any number n, it is possible to find a sequence of n consecutive natural numbers which are all composite: for instance, the n numbers $(n+1)!-(n+1)$, $(n+1)!-n$, …, $(n+1)!-3$, $(n+1)!-2$. Moreover, since programs of symbolic calculation like DERIVE and MAPLE contain, in their library of functions, the function $\pi(x)$ that tells how many primes are less than or equal to x, it is possible to graph $\pi(x)$ using bigger and bigger values of x: the graph seems to become more and more "horizontal".

So, the observation of both tables and graphics highlights a phenomenon for which there are two possibilities: either prime numbers somewhere disappear from the sequence of natural numbers, and hence they are finitely many, or for every prime p it is possible to find a greater one, and hence they are infinitely many[2]. The theorem we are considering justify itself as the answer to this dilemma.

Now the problem naturally arises: how a number like $p_1 \cdot p_2 \cdots p_n+1$ came into Euclid's mind? This gives the opportunity of opening a discussion on the question: "If a finite number of primes are given, how can I build another prime not already in

---

[2] Perhaps we can take here the opportunity of speaking about asymptotes in a non-conventional way. Or, if we are working with young students, it is possible (or even suitable) to riconsider the topic some years later, proposing to them to approximate the function $\pi(x)$ with a function $f(x)$ regular enough, namely with continuous first and second derivatives. Students should conclude that the first derivative has to be non-negative and the second one negative, without ruling out the possibility that $f(x)$ becomes definitively constant. By the way, we know that the function $\pi(x)$ is asymptotic to the function $g(x) = x/\ln(x)$, and that $g'(x) > 0$ for $x > e$ and $g''(x) < 0$ for $x > e^2$.

the list?” So, the construction in Euclid’s proof can again be preceded by an exploration. There are many available procedures: for instance, we can carry on the following one. Let’s start from the prime number 2 and build the number $a_1 = 2+1 = 3$, which is prime. In the second step build $a_2 = 2\cdot3+1 = 7$, prime. From 2, 3 and 7, obtain $a_3 = 2\cdot3\cdot7+1 = 43$, prime. At the next step we get: $a_4 = 2\cdot3\cdot7\cdot43+1 = 1807 = 13\cdot139$. Both 13 and 139 are “new” primes; we could use both, but taking only the smaller, we obtain: $a_5 = 2\cdot3\cdot7\cdot43\cdot13+1 = 23479 = 53\cdot443$. And so on…

Otherwise we can follow the more “known” path: $b_1 = 2+1 = 3$, which is prime; $b_2 = 2\cdot3+1 = 7$, prime; $b_3 = 2\cdot3\cdot5+1 = 31$; $b_4 = 2\cdot3\cdot5\cdot7+1 = 211$; $b_5 = 2\cdot3\cdot5\cdot7\cdot11+1 = 2311$, all prime numbers; $b_6 = 2\cdot3\cdot5\cdot7\cdot11\cdot13+1 = 30031 = 59\cdot509$. And so on.[3]

This process actually gives more and more new prime numbers. We can use a symbolic calculator (here we are using *TI-89 Titanium*) to overcome the lenghtness and difficulties of calculations but also to distinguish between the two possible cases for b_i, since the command `factor` allows to easily establish if a given number is prime or composite (see Figure 1). When the calculation is not assisted by a powerful tool, it is quite sure that only the first case is noticed, since the first composite value of $p_1\cdot p_2\cdots p_n+1$ is too big. On the contrary, by the aid of a calculator, the exploration can go on without difficulties, to reach for instance the case shown in Figure 2. In our opinion, this is a simple and meaningful example, to see how a calculator can be a really useful tool in helping students to understand and build a meaning.

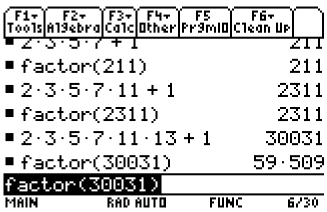


Figure 1

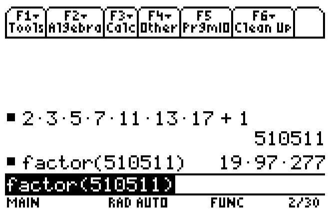


Figure 2

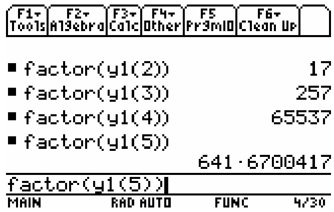


Figure 3

It is important to stress that the observation of a finite number of cases can never replace a proof, but it allows only to do some *conjecture*, to be confirmed or disproved. History tells us how that behaviour can be misleading: it is enough to recall the well known example of Fermat who in 1640 enunciated the conjecture “All the numbers $F_n = 2^{2^n}+1$ are prime” (n any natural number). Let’s still use a symbolic calculator to examine the conjecture. We insert in *Editor* (where functions can be defined) the function y1(x) = 2^(2^x)+1. Using the command `factor`, we discover

[3] The numbers b_i are interesting in themselves. As observed, the first five of them are all prime numbers, whereas b_6, b_7, b_8 are not. In (Burton, 2005) many interesting facts are reported: for instance till today (2005) only 19 primes have been identified in the sequence (the largest, discovered in 2000, that is $p_1\cdot p_2\cdot\ldots\cdot42209 + 1$, has 18241 digits), while all the other b_i’s for $p \leq 120000$ are composite. And nobody knows whether there are finitely or infinitely many primes of the form b_i. Well, knowing about simple problems still unsolved is always a fascinating stimulation for students.

that the conjecture is actually false, showing (see Figure 3) that F_5 is not prime, but is the product of two primes: $F_5 = 2^{32}+1 = 641 \cdot 6700417$[4].

CONCLUSIVE REMARKS AND FURTHER DEVELOPMENTS

In the previous section we have suggested a possible classroom path for the proof of the theorem. One of the two authors has experimented for years in his classes such a path, with different developments and deepenings, according to class contexts and circumstances. We think that the whole experience gives evidence to the goodness of the suggested approach, whereas no specific didactical situation or students' work does it adequately. This is the reason why, – but also due to space limits of this work, – we don't give detailed reports or comments on specific events.

In our opinion two problems would deserve further deepening. The first one concerns proofs by contradiction. Following the opinions of some logicians (Lolli, 2005), we guess that many theorems in school curricula, usually proven by this technique, can also be proven in a direct way, slightly modifying, if necessary, their statements. Then the problem would turn into a linguistic one, namely to show how any implication can be expressed in an equivalent way by its contrapositive. We intend to come back to this problem in a forthcoming work.

The second problem concerns infinity, and its two facets as potential or actual infinity. Obviously, on this topic all has already been said from a conceptual point of view. But we think that the discussion is still open on how and when and why the notion of infinity occurs in school in its two forms. The theorem of prime numbers is an important moment, but it isn't the only one and we think that any possible deepening of this problem would be interesting. We will take care also of this question in the next future.

References

Antonini, S.: 2003, *Dimostrare per assurdo: analisi cognitive in una prospettiva didattica*, Doctoral thesis, Dipartimento di Matematica, Pisa University.

Antonini, S. and Mariotti, M.A.: 2006, 'Reasoning in an absurd world: difficulties with proof by contradiction', in *Proc. of the 30th PME Conference*, Prague, 2, 2-65.

Berlinghoff, W.B. and Gouvêa, Q.: 2004, *Math through the Ages, A Gentle History for Teachers & Others*, The Math. Association of America, Washington, D.C.

Burton, D.M.: 2005, *Elementary Number Theory*, McGraw Hill, Singapore.

Castagnola, E.: 2002a, 'Learning to teach algebra: an Italian experience with reference to history', *Proc. of the II Intern. Conf. on the Teaching of Math.*, Heronissos, Greece.

---

[4] Leonhard Euler (1707-1783) found the result in 1739, of course without technological tools. His method can be read for instance in (Dunham, 1992) or in (Øre, 1988). Here we have another example of an open problem: today it is conjectured that all the numbers $2^{2^n}+1$ are composite for $n \geq 5$, that is there are only 4 Fermat primes. This conjecture has been verified till $n = 30$ (Burton, 2005).

Castagnola, E.: 2002b, ‘The functionality of CABRI and DERIVE in a graphic calculator’, *Proc. of the Intern. Conf. “The Humanistic Renaissance in Math. Education”*, Palermo, 80-86.

Castagnola, E.: 2004, ‘From Euclid to Descartes, to … Cabri. Using history and technology to explore mathematics’, *Proc. of HPM 2004*, Uppsala, 167-174.

Dunham, W.: 1990, *Journey through Genius: The Great Theorems of Mathematics*, John Wiley & Sons, USA.

Fauvel, J. and Van Maanen, J. (eds): 2000, *History in mathematics education*. ICMI Study, Kluwer, Dordrecht.

Furinghetti, F. and Radford, L.: 2002, ‘Historical Conceptual Developments and the Teaching of Mathematics: from Phylogenesis and Ontogenesis Theory to Classroom Practice’, in L. English (ed.), *Handbook of International Research in Mathematics Education*, L. Erlbraum Associates, Mahwah, NJ, 631-654.

Heath, T.L.: 1956, *The Thirteen Books of Euclid’s Elements*, Dover, New York [reprint of the II edition, Cambridge University Press, 1925, London].

Kaput, J.: 2002, ‘Implications of the Shift from Isolated, Expensive Technology to Connected, Inexpensive, Divers and Ubiquitous Technologies’, in F. Hitts (ed.) *Representations and Mathematics Visualization*, Mexico, 80-109.

Katz, V. (ed.): 2000, *Using history to teach mathematics. An International perspective*, The Mathematical Association of America, Washington, D.C.

Katz, V. and Michalowicz, K.D.: 2005, *Historical Modules for the Teaching & Learning of Mathematics*, CD-rom, The Math. Ass. of America, Washington, D.C.

Leron, U.: 1985, ‘A direct approach to indirect proofs’, *Educ. Studies in Math.* 16, 321-325.

Lolli, G.: 2005, *QED. Fenomenologia della dimostrazione*, Bollati Boringhieri, Torino.

Mariotti, M.A.: 1998, ‘Introduzione alla dimostrazione all’inizio della scuola secondaria superiore’, *L’insegnamento della Matematica e delle Scienze Integrate* 21B-3, 209-252.

Øre, O.: 1988, *Number Theory and Its History*, Dover, New York.

Paola, D.: 2000, ‘Le definizioni: dalla parte degli studenti’, *L’insegnamento della Matematica e delle Scienze Integrate* 23A-B, 6, 562-600.

Paola, D.: 2006, ‘Nuove tecnologie e studio delle grandezze che variano’, *L’insegnamento della Matematica e delle Scienze Integrate* 29A-B, 4, 347-356.

Polya, G.: 1973[2], *How to solve it*, Princeton University Press, Princeton, NJ.

Radford, L.: 2000, ‘Signs and meanings in students emergent algebraic thinking: a semiotic analysis’, *Educational Studies in Mathematics* 42, 237-268.

Radford, L.: 2003, ‘Gestures, Speech, and Sprouting of Signs: A Semiotic-Cultural Approach to Students’ Types of Generalization’, *Mathematical Thinking and Learning* 5(1), 37-70.

Reid, D. and Dobbin, J.: 1998, ‘Why is proof by contradiction difficult?’, in *Proceedings of the 22th PME Conference*, Stellenbosch, South Africa, v. 4, 41-48.

Zaslavsky, O. and Shir, K.: 2005, ‘Students’ Conceptions of a Mathematical Definition’, *Journal for Research in Mathematics Education*, 36:4, 317-346.

Websites

(1) http://aleph0.clarku.edu/~djoyce/java/elements/toc.html

(2) http://www-groups.dcs.st-andrews.ac.uk/~history

(3) http://www.utm.edu/research/primes/

(4) http://convergence.mathdl.org