MATHEMATICS IN ANCIENT GREECE
FROM THE 6th TO THE 4th CENTURY BCE
FROM PYTHAGORAS TO EUCLID

History of mathematics, Bologna, October 2013

Part III

Proof of incommensurability and *Reductio ad absurdum*

I. Summary of the precedent lessons.

The study of Greek mathematics from the middle of the 6th century to the beginning of the 5th BCE, has led us to two characters differentiating it from other mathematics.

- Firstly on one hand the importance given by early Greek mathematics to geometry even concerning arithmetical questions and on the other hand the rigor used in demonstrations[1].
- The use of a form of proof called 'by the impossible' or 'by the absurd' or '*reductio ad impossibile*' or else '*reductio ad absurdum*'.

But we also saw these two characters are not of the same importance. The emphasis on geometry could be a mark of this mathematics, but it was certainly not a breaking point with the others. It is all the more conclusive if, as many scholars claim, it is true some of the principal results had been known long before elsewhere. The point is not so much if this is true or false, but its very possibility shows there is continuity between all these mathematics. And the same remark can be made concerning the rigor of the demonstrations.

On the contrary, the second point appears to have been entirely ignored outside of these mathematics and more generally outside the ancient Greek thought. It was not only a new tool giving new and spectacular mathematical results, but a new method of reasoning. It appeared so important to the Greeks themselves that this new kind of reasoning is found permeating the whole Greek thought. To the point where it is difficult for us, the moderns, to be sure if its origins are to be found in mathematics (though we saw it was probably the case) or elsewhere as for instance in philosophy[2].

It does not mean both characters are disjointed. Indeed, it is the very importance given to geometry instead of numbers and computations which leaded to this new form of thought. And inversely, this new way of thinking demanded absolutely rigorous proofs for mathematical statements.

[1] Cf. M. Caveing, *La figure et le nombre*, p. 144-149.
[2] For such point of view cf. for instance A. Szabo, *The Beginnings of Greek Mathematics* or W. Knorr, *The Evolution of Euclidean Elements*, p. 298.

Now we need to solve some mystery. Why and when did this method so useful to the mathematicians appear? And following their lead, why did thinkers of other fields decide to adopt this new method? It is the subject of this lesson.

II. Geometry and origins of incommensurability.

The oldest texts we have in relation with this question are of Plato and Aristotle. The second author is especially important in the search of the origins since he uses the incommensurability as a model of some form of syllogisms.

One of the difficulties is the brevity of these texts which moreover are not very explicit. Fortunately, as noted by many mathematicians and historians of mathematics, it is possible to reconstruct mathematical proofs from very thin hints.

In *Prior Analytics*, Aristotle writes:

'*It is clear then that the ostensive syllogisms are effected by means of the aforesaid figures; these considerations will show that* reductiones ad impossibile *also are effected in the same way. For all who effect an* argument per impossibile *infer syllogistically what is false* ('ψεῦδος')*, and prove the original conclusion hypothetically when something impossible results from the assumption of its contradictory; e.g. that the diagonal (…) is incommensurate (…)*[3]*, because odd numbers are equal to evens if it is supposed to be commensurate. One infers syllogistically that odd numbers come out equal to evens, and one proves hypothetically the incommensurability of the diagonal, since a falsehood results through contradicting this. For this we found to be reasoning* per impossibile ('διὰ τὸ ἀδυνάτου')*, viz. proving something impossible* ('ἀδύνατον') *by means of an hypothesis conceded at the beginning.*' (I, 23, 41a21-32, transl. A. Jenkinson).

i) The first indication we find here concerns the proof which convinced the mathematicians of the incommensurability of the diagonal: a demonstration by '*reductio ad absurdum*'.

ii) The second one is a little more problematic because Aristotle (as usual) is extremely brief. He did not give explicitly the mathematical figure whose diagonal is incommensurable. Since the Greek term he uses is 'διάμετρος', it could be any polygon or even a circle.
It is nevertheless reasonable to think he omits to go into the details because he was speaking of the simplest case, the square, the meaning being obviously: the diagonal is not commensurable [with its side].
Nevertheless, some historians and mathematicians think the first case of incommensurability was not discovered in the square but in the pentagon. It is all the more a tempting hypothesis because the pentagon and the pentagram are Pythagorean symbols and the Pythagoreans were the ones who obtained the first proof of the existence of incommensurable magnitudes[4].

[3] The translator writes here '… e.g. that the diagonal **of the square** is incommensurate **with the side**'. But though we agree with his interpretation, Aristotle does not specify either the figure (the square) or the other part of the figure to take as ratio of the diagonal (the side). So we put dots instead of the words emphasized in the quotation.
[4] Though this point is hotly debated among modern scholars.

III. Irrationality and pentagon.

The demonstration uses the following diagram:

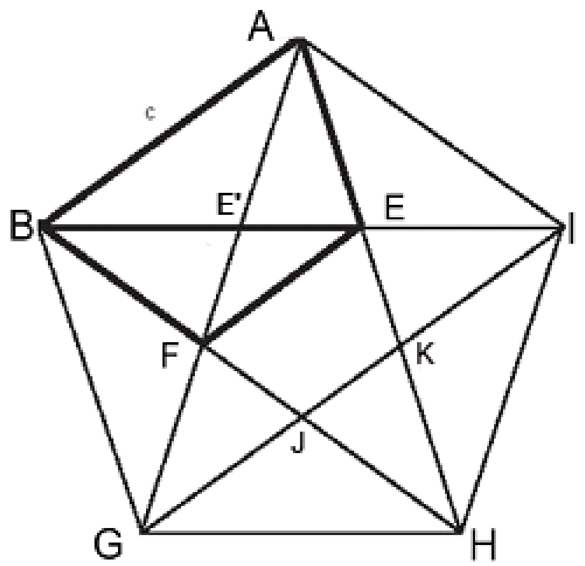


Figure 1

Let *d* denote the length of the diagonal *AG* and *c* the side *AB*.
We will also note *E'* the intersection of *BI* with *AG*, and *c' = E'E, d' = FE*.
Let us suppose the ratio *d/c* to be rational.
We can then find a unit such that *d* and *c* are both integers.

a) The pentagon is a regular figure inscribed in a circle, so that all the arcs on the circle cut by the summits of the pentagons are equal thus also all the angles at the summit:
angle (*BAG*) = angle (*GAH*) = angle (*HAI*) = angle (*AIB*) =…
Let us note α their common value.

a') Since five of them intercept the whole circle (for instance *BAG*, *GAH*, *HAI*, *BGA* and *AHI*), we have:
$5\alpha = 2$ right-angles (= 180°).

b) Since angle (*AE'B*) = *2* right-angles - $2\alpha = 3\alpha$ (from a')) = angle (*AEI*) = angle (*IKH*) = angle (*HJG*) = angle (*GFB*), the polygon
***EKJFE'* is a regular pentagon.**

c) Since from b), *FE' = E'E*, the triangle *FE'E* is isosceles and angle (*FE'E*) = angle (*BE'A*) = 3α (again from b)), so we get angle (*BEF*) = ½ (*2* right-angles - $3\alpha) = \alpha$ = angle (*IBA*) (from a)) = angle (*BIG*) (again from a)), we obtain:
***AB, EF* and *IG* are parallel**.

c') Since from a) angle (*BIG*) = α = angle (*IGH*), we have:
_BI_ and _GH_ are parallel.

d) The triangle *ABE* is isosceles:
Since from a), angle (*BAE*) = 2α and angle (*ABE*) = α, we get:
angle (*AEB*) = *2* right-angles - $3\alpha = 2\alpha$ (from a'))
and the triangle **_ABE_ is isosceles**.
In particular we have:
BE = AB := c.

e) Since *AB* = *AI* and (from a)) angle (*BAE'*) = angle (*ABE'*) = angle (*EAI*) = angle (*AIE*), the triangles **_AE'B_ and _AEI_ are isosceles and equal**.
In particular we get:
BE' = EI.

f) Since *d := BI = BE + EI = BE' + E'I = 2BE - E'E* (from e)) = *2AB –E'E* (from d)) *:= 2c – c'* we get:
c' = 2c - d (1)
Moreover since *E'E* is a (strict) part of *BE = AB,* we get
c' < c (2)
And from the third equality we obtain also: *EI = d - BE* i.e.
EI = d - c (3)

g) Since (from c)): *FE* and *AB* are parallel, we have:
angle (*EFA*) = angle (*BAF*) = α = angle (*GAH*)
and the triangle *AEF* is isosceles, so that ***d' := FE = AE***.

h) Since (from e)) the triangle *AEI* is isosceles, *d' = AE = EI* = (from (3)) *d-c*,
so that :
d' = d-c (4)
and in particular ***d' < d*** (5).

From (1), (2), (4) and (5) we have:

c' = 2c - d < c and ***d' = d-c < d*** (*).

Now there is a new regular (convex) pentagon *EKJFE'* and pentagram in the center of the first one, of side *c'* and diagonal *d'*. From the above results (valid for any pentagon) applied to the new one, we get:
c'' = 2c' - d' < c' and *d'' = d' - c' < d'* (*')
where c'' and d'' are respectively the side and the diagonal of the pentagon inscribed in *EKJFE'* (cf. figure 2 below). And this process can be repeated indefinitely (cf. figure 2):

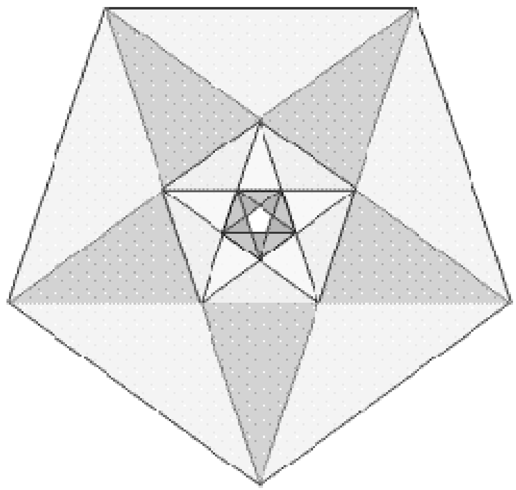


Figure 2

> In particular we obtain an infinite sequence *c, c', c'',* ... (and also *d, d', d'',...*) of strictly decreasing positive integers. But this is impossible[5], and we can conclude the hypothesis is false i.e. ***c* and *d* are not commensurable**.

This result is based on the use of infinite series nowhere found inside Greek mathematics which tends to avoid the use of the infinity (and the paradoxes connected to it). Moreover all the ancient texts, as well as the later commentators of Aristotle, connect irrationality with the diagonal of the square.
Moreover it is not sure such a long demonstration would have convinced both mathematicians and non-mathematicians of the certitude of the existence they never heard of before. It certainly does not agree to the immediate obviousness of the conclusion as implied by the above text of Aristotle. And anyway if we would accept this form of demonstration, we will see when we will study the '*anthyphairesis*' a simpler form of this proof would give the incommensurality of the diagonal in a simpler figure than the pentagon, the square (cf. infra, IV.iii.5).
Last but certainly not least, the proof has nothing to do with the question of the even/odd, and so it is impossible to be the demonstration Aristotle is speaking of.

We can then conclude: when Aristotle speaks of the 'incommensurability of the diagonal' he means its incommensurability to the side of the square[6].

We have already considered the question of the diagonal of a square when we studied Pythagoras' theorem and Plato's testimony in *Meno*. In this text the diagonal of a square was shown to produce a square of surface double of the original square, which means in modern terms the ratio of the diagonal to the side is equal to the square root of *2*.
Thus, the modern translation of the Greek incommensurability of its ratio to the side means the irrationality of $\sqrt{2}$, i.e. Aristotle writes about the proof by '*reductio ad absurdum*' of the irrationality of $\sqrt{2}$.

---

[5] This differentiates integers from continuous magnitudes, since there exist such infinite strictly decreasing sequences of magnitudes, as for instance the sequence obtained by continuously dividing any given magnitude by *2*.
[6] In accordance with the translation given in §2 (cf. supra, note 3).

IV. The usual proofs of the incommensurability of the diagonal (proposition X.117 in the *Elements* and '*anthyphairesis*').

There are many ways to prove the irrationality of $\sqrt{2}$. The difficulty is to find one coherent with the textual testimonies and the mathematical knowledge of this time. In complete opposition of the main purpose in mathematics, which is the largest generalization, we need here a proof giving exactly the result but nothing more.

From Aristotle's text we can already say the result of irrationality we are looking for concerns exclusively the square root of *2*. Moreover, Plato's *Theaetetus* (see annex 1) shows the proof shall be different from the one used to prove the irrationality of the square roots of other integers, like *3, 5, …* .

So the proof must verify two essential conditions:

- to be absolutely convincing or in Proclus' terms to compel 'assent by the irrefutable arguments of science' and
- to be impossible to be easily generalized to all integers, especially *3* and *5*.

Among the many possible pretenders to be the first demonstration of the irrationality of $\sqrt{2}$ there are essentially two, with their many variations, which are accepted by the historians of mathematics because they are supposed to be in accordance to the above conditions.

i) The standard proof found in the *Elements*.

This proof is found at the end of the book X of Euclid's Elements. It is the one of the proposition numbered 117 and, since it has nothing to do at this place, it is considered almost unanimously as inauthentic, even by the ones who consider it is the proof Aristotle had in mind in the *Analytics*.

They argue, it is an old one Euclid or his editors decided to add since it was historically so important, as a testimony of the origins of the irrationality, certainly the most important theory of early Greek geometry. There are many variants of this proof, but they all share the same characters we will study here.
One of the reasons this proof was so successful is certainly connected to the fact it is the proof we, moderns, would give nowadays. Let us consider it in details.

Let us denote by z the square root of 2 (*i.e.* $z^2 = 2$), then:

Hypothesis. We suppose z to be rational, so that:
there exist two integers p and q such that $z = p/q$.

We can moreover suppose p and q to be relatively prime. We will deduce a contradiction and in agreement with the '*reductio ad absurdum*', we will obtain the irrationality of z.

Result 1: p is even.

From $z^2 = 2$ and $z = p/q$ we get: $2 = (p/q)^2 = p^2/q^2$ and then: $2q^2 = p^2$,
so p^2 and thus p is even, since the square of an even (respectively an odd) number is even (respectively odd).

Result 2: q is odd.

p and q are relatively prime, then they can not be both even, thus: q is odd.

Consequence:

From result 1, p is even i.e. $p = 2r$ where r is an integer. Thus we have:
$2\,q^2 = p^2 = (2r)^2 = 4r^2$, so $q^2 = 2r^2$ is even,
and as above in the demonstration of Result 1 we get:
q is even.

But from result 2, the integer q is odd. Thus q is both even and odd which is impossible. Consequently, the hypothesis is false and z is not rational, thus the diagonal is not commensurable with the side of the square.

This proof uses implicitly the partition of the (positive) integers into two parts, the odd and the even, the fundamental division of the integers in Greek mathematics as shown for instance in Plato's books[7].

[7] Cf. *Charmides* 166a, *Euthydemus*. 290c, *Gorgias* 451b, *Hippias major* 367a, *Ion*, 537e, *Phaedo* 104a-b, *Phaedrus* 274c, *Statesman* 259e, *Protagoras* 357a, *Republic* 510c, 522e, *Theaetus* 198, …

ii) The inconstancies of the standard proof.

We will not detail the problems, since essentially it is in contradiction with both necessary conditions listed at the beginning of this chapter:

1. The demonstration supposes the theory of relatively prime numbers, which is inconsistent with the texts. As a matter of fact, switching *2* by any prime numbers *p*, the proof of the proposition X. 117 of the *Elements* would give the irrationality of the square root of *p*. This contradicts both Aristotle's *Analytics* which concerns exclusively the square root of *2*, and Plato's *Theateteus*, where only the numbers *3, 5, …* are treated, excluding *2*.

2. The demonstration is also inconsistent with the conclusion of the proof as reported by Aristotle. According to the text, the proof by '*reductio ad absurdum*' leads to the absolutely impossible vanishing of the odd numbers in the even ones[8] conclusion even for non-mathematicians, explaining its use by Aristotle as a model of '*reductio ad absurdum*'.

   On the other hand, the conclusion of the proof of the proposition X.117 is the existence of a number both odd and even[9]. It is of course an impossibility but entirely different from the one pointed by Aristotle, the totality of the odd numbers becoming the even numbers[10].

---

[8] And according to Greek symbolism, it would mean the disappearing of the males into the females.

[9] As a matter of fact, the real (impossible) conclusion is the existence of a couple of integers which are both relatively prime with each other and not relatively prime, which is, if possible, even more impossible, but also even more remote from Aristotle's conclusion.

[10] Symbolically it is much weaker since it means the existence of hermaphrodites well-known by the ancient Greeks in biology and a kind of a commonplace in their literature. The term 'hermaphrodite' comes indeed from the Greek name of the two-sexed child of Hermes and Aphrodite.

iii) Another proof: the proof by '*anthypairesis*'.

Since the standard proof which was almost universally adopted at the end of the 19th century shows so blatant discrepancies with the textual testimonies, another one was proposed by a Danish mathematician Hieronymus Zeuthen at the beginning of the 20th century.
It is based on the so-called '*anthyphairesis*', transliteration of the Greek term 'ἀνθυφαίρεσις', formed from 'ὑφαίρεω' ('subtract') et 'αντι' whose meaning here is 'answer', 'alternating' so that 'ἀνθυφαίρεσις' may be translated by 'alternated subtraction'.

It is a generalization to magnitudes of the so-called Euclid's algorithm used to determine what is called 'common measure' by ancient Greek mathematicians ('κοινὸν μέτρον') and 'Greatest Common Divisor' of two integers by modern ones.

1. Euclid's algorithm.

Both the term (verb or name) of the family '*anthyphairesis*' and the method appear firstly in the propositions 1 and 2 of the book VII of the *Elements*.

Proposition 1. *Two unequal numbers (being) laid down, and the lesser being continually subtracted, in turn, from the greater, if the remainder never measures the (number) preceding it, until a unit remains, then the original numbers will be prime to one another.*

Proposition 2. *To find the greatest common measure of two given numbers (which are) not prime to one another.*

In the proposition 2, Euclid proves that the method consisting of 'ἀνθυφαιρουμένου'i.e. the application of the '*anthyphairesis*' to two non-relatively prime integers, will finally give the GCD of these numbers. And the same method applied to two relatively prime numbers will give at the end the unity.

Explanation. In the proposition 1, let m and n be 2 integer with $m > n$. Let p_1 be the greatest integer such that $m > p_1 n$, so that we can write:
$m = p_1 n + q_1$ with $q_1 < n$ (1).
If n is not a divisor of m, then q_1 is an integer (i.e. non null) and since $q_1 < n$, there exists a greatest integer p_2 such that $n > p_2 q_1$. So we can write:
$n = p_2 q_1 + q_2$ and $q_2 < q_1$ (2).
We can now proceed alike with q_2 and q_1 and so on, till either one of the q_h divides q_{h-1} or is equal to 1.

According to the proposition 1, if after some iterations, for some k we obtain q_k equals to 1, then m and n are relatively prime.
According to proposition 2 if after some iterations, for some k we obtain $q_{k+1} \neq 1$ is a divisor of q_k, then m and n are not relatively prime and their GCD is equal to q_{k+1}.

There is no other possibility: since the sequence $q_1, q_2, q_3, \ldots$ is strictly decreasing, it is necessarily finite.

So after a finite number of applications of 'alternate subtractions', depending of the numbers *m* and *n*, the process will necessarily end, and the last term of the series will be either *1* (then these numbers are relatively prime) or another number different from *1* (and then it is the GCD of these numbers).

The first proposition is easy to prove: let *r* be a common divisor of the integers *m* and *n*. Then from (1) it is a divisor of q_1, so from (2) it is a divisor of q_2, and so on, it will divide any q_h. So if the last number q_k of this sequence is equal to 1, there is no common divisor of *m* and *n* so that they are relatively prime.
To prove the second proposition, if *m* and *n* are not prime, as we saw above, any common divisor of *m* and *n* will divide all the q_h, so all the q_h are multiples of their GCD. Inversely if q_{k+1} divide q_k it will also divide q_{k-1} (because of the identity (k+1)), and so on, it will divide all the q_h. Thus, from the identities (2) and (1) it will also divide *n* and *m*, thus it is a divisor of both *m* an *n*, and since it is also divided by their GCD, it is equal to it.

Exemples.

1. Let us take $m = 7$ and $n = 3$. We can subtract twice *3* from *7* and we obtain as rest *1*, so *3* and *7* are relatively prime numbers (proposition VII.1)
2. Let now take $m = 12$ and $n = 8$. We can subtract once *8* from *12* and we get *4* as rest i.e. $12 = 8 + 4$. Since *4* is a divisor of *8*, it is the GCD of *12* and *8*.

Exercise 1. Let *m, n* be two integers. For any integer *h*

a) What is the relation between GCD (*hm, hn*) and GCD (*m, n*)?
b) What is the relation between the sequences of q_k obtained in computing GCD (*m,n*) and GCD (*hm,hn*)?
c) What is the relation between the sequences of p_k obtained in computing GCD (*m,n*) and GCD (*hm,hn*)?

Remark. The exercise proves though the sequence of q_k depends of the representation of the ratio of *m/n* (or in modern terms of the representation of the rational *m/n*), the sequence of p_k does not.

2. Generalized '*anthyphairesis*'.

The existence of a GCD is a property of integers, but the method of '*anthyphairesis*' can be extended to any couple of magnitudes.

Let a and b be such magnitudes, p_1 the greatest **integer** such that $m > p_1 n$. We can write:
$a = p_1 b + q_1$ with $q_1 < n$ (1).
If b does not divide a, q_1 is a magnitude (i.e. non null) and since $q_1 < n$, there exists a greatest integer p_2 such that $n > p_2 q_1$, and we can write:
$b = p_2 q_1 + q_2$ with $q_2 < q_1$ (2).
We can now proceed alike with q_2 and q_1 and so on.

This algorithm is given in the two first propositions of the book X of the *Elements*.
There is nevertheless a huge difference between the case of integers and the general case.
While in the first case (for integers) the algorithm is always finite, for arbitrary magnitudes this is no more true.
As a matter of fact, the propositions 1 to 3 give the following equivalence:
Two magnitudes are commensurable if and only if the '*anthyphairesis*' is finite.
It is then possible to use it to determine if two magnitudes are commensurable or incommensurable[11].

[11] At least according to the modern mathematicians, since we do not find any hint of such a possibility in the Antiquity.

3. Generalized '*anthyphairesis*' and continued fractions.

Since we have few mathematical texts before and even long after Euclid, and moreover they did not detail the methods used to obtain results, especially the ones concerning computations, it is not easy to determine how the mathematicians of the Antiquity made their computations. Anyway, even if there were probably other methods, the '*anthyphairesis*' was an extremely powerful and convenient way to obtain approximation by fractions or ratios. Moreover according several later commentators including Proclus, it was already used by the old Pythagoreans.
And in a careful study of some approximations given without any explanation by later authors (Archimedes, Archytas, …) Jean Itard showed by comparing several methods of approximations, including some certainly not known in this time, the only reasonable method giving these results was the one by *anthyphairesis*[12].
This method was such a common tool for the mathematicians of the 3rd century BCE, they did not bother to indicate its use, so it was certainly well-known much earlier.
As we will see, this method is closely related to what is called in modern mathematics 'continuous fractions'[13].

The generalized '*anthyphairesis*'.
-
Let a and b be two magnitudes with $a > b$. If b divides a we stop here. Otherwise let p be the greatest **integer** such that
$a > p\, b$. Thus we can write:
$a = p\, b + q_1$ where q_1 is a **magnitude** such that $q_1 < b$ (1)
and evidently $a > pb$ or $a/b > p$ (1').

If q_1 divides b we stop here. Otherwise let p_1 be the greatest integer such that $b > p_1\, q_1$.
Then we have:
$b = p_1\, q_1 + q_2$ where q_2 is a **magnitude** such that $q_2 < q_1$ (2).

From (1) we have:
$a/b = p + q_1/b$ (3)
and from (2):
$b/q_1 = p_1 + q_2/q_1$ thus

$q_1/b = 1/(p_1 + q_2/q_1)$ (4).

Using the equality (4) in (3), we get:

$$a/b = p + 1/(p_1 + q_2/q_1) = p + \cfrac{1}{p_1 + \cfrac{q_2}{q_1}} \qquad (5)$$

[12] Jean Itard, *Les livres arithmétiques d'Euclide*.
[13] To be precise, we need to assume in the rest of the chapter some natural properties on the sets of homogenous magnitudes. For instance, there is a total order relation noted < (or >); the addition is an internal operation such that if x and y are two homogeneous magnitudes, we have $x < y$ if and only if there exists another magnitude z such that $y = x + z$, and z is noted $y - x$.

with $q_2 < q_1 < b$ and evidently: $a/b < p + \frac{1}{p_1}$ (5’)

and we can continue. For instance, the next step will be:
If q_2 divides q_1 we stop here. Otherwise since $q_2 < q_1$, there exists an integer p_2 and a **magnitude** q_3 with $q_3 < q_2$ such that:
$q_1 = p_2 q_2 + q_3$
and dividing by q_2 we obtain:
$q_1/q_2 = p_2 + q_3/q_2$ thus

$$q_2/q_1 = 1/(p_2 + q_3/q_2) \qquad (6)$$

and replacing q_2/q_1 in (5) by the second term of the equality (6), we get:

$$a/b = p + \cfrac{1}{p_1 + \cfrac{1}{p_2 + \cfrac{q_3}{q_2}}} \qquad (7)$$

with $q_3 < q_2 < q_1 < b$, and $a/b > p + \cfrac{1}{p_1 + \cfrac{1}{p_2}}$ (7’)

and so on.
Thus, we obtain for a/b a sequence of fractions of the form:

$$a/b = p + \cfrac{1}{p_1 + \cfrac{1}{p_2 + \cfrac{1}{p_3 + \ldots}}}$$

where $p, p_1, p_2, p_3, \ldots$ form a sequence of (**non necessarily decreasing**) **integers** and $q_1, q_2, q_3, \ldots$ a sequence of **strictly decreasing magnitudes**.

The fractions $\boldsymbol{P_k}$:

$\boldsymbol{P_0} = p,$

$\boldsymbol{P_1} = p + \frac{1}{p_1},$

$\boldsymbol{P_2} = p + \cfrac{1}{p_1 + \cfrac{1}{p_2}},$

$\boldsymbol{P_3} = p + \cfrac{1}{p_1 + \cfrac{1}{p_2 + \cfrac{1}{p_3}}},$

…
(where all the $p, p_1, p_2, \ldots$ are integers) are called in modern terms ‘continuous’ or ‘continued’ fractions.

Exercise 2. Let a, b be two magnitudes. For any integer h

a) What is the relation between the sequences of q_k obtained in computing the ‘anthyphairesis’ of (a,b) and the ‘anthyphairesis’ (ha,hb)?
b) What is the relation between the sequences of p_k obtained in computing ‘anthyphairesis’ of (a,b) and the ‘anthyphairesis’ (ha,hb)?
c) What can you conclude for the sequence $\boldsymbol{P_k}$ with respect to the ratio of two homogeneous magnitudes?

4. **Generalized '*anthyphairesis*' and approximations.**

The 'continuous fractions' $\boldsymbol{P_0}, \boldsymbol{P_1}, \boldsymbol{P_2}, \ldots$ give a sequence of approximations of the ratio *a/b* by ratios of integers with the following properties:

a) They are more and more complicated
b) The $q_1, q_2, q_3, \ldots$ form a sequence of strictly decreasing magnitudes, and according to proposition X.1 we would say, in modern terms, the 'continuous fractions' $\boldsymbol{P_0}, \boldsymbol{P_1}, \boldsymbol{P_2}, \ldots$ converge to *a/b*.
c) According to (1'), (5'), (7'), these fractions alternates in the following sense: for any integer k we have :
$\boldsymbol{P_{2k}} < a/b < \boldsymbol{P_{2k+1}}$

Examples.

1) Maybe sometimes you wondered how the fraction *22/7* was found as an approximation of π. As a matter of fact Archimedes gave it as an upper-bound for π[14]. But in any case, it is easy to get it using the '*anthyphairesis*' when we know 3,14 is an approximation of π.
So let us put $a = 314$ and $b = 100$. According to the '*anthyphairesis*', we write:
$314 = 3 \times 100 + 14$ (1)
and as the first approximation we get:
$\pi \approx 314/100 \approx 3.$

Then we write:
$100 = 7 \times 14 + 2$ or $100/14 = 7 + 2/100$ (2)
i.e. $14/100 = 1/(7 + 1/50)$,
and we get:
$\pi \approx 314/100 = 3 + 14/100 = 3 + 1/(7 + 1/50) \approx 3 + 1/7 = 22/7.$

2) Let us use this method to approximate $\sqrt{2}$.
We will apply it to the ratio $\sqrt{2}/1$ i.e. $a = \sqrt{2}, b = 1$:

First step.
$\sqrt{2} = 1 + (\sqrt{2} - 1)$ (1)
and we get:
$p = 1, q_1 := (\sqrt{2} - 1)$
with the first approximation:
$\sqrt{2} \approx \boldsymbol{P_0} = 1.$

Second step.
We have:
$1/3 < q_1 = \sqrt{2} - 1 < 1/2$ (since $(4/3)^2 = 16/9 < 2 < (3/2)^2 = 9/4$), so we get:
$b = 1 = 2(\sqrt{2} - 1) + (3 - 2\sqrt{2})$ so that
$p_1 = 2, q_1 = \sqrt{2} - 1, q_2 := 3 - 2\sqrt{2}$
and

[14] Cf. Achimedes, *Measurement of the circle.*

$$a/b = \sqrt{2} = 1+\cfrac{1}{2+\cfrac{3-2\sqrt{2}}{\sqrt{2}-1}}.$$

Since $(3 - 2\sqrt{2})/(\sqrt{2} - 1) = (3 - 2\sqrt{2})(\sqrt{2} + 1)/(\sqrt{2} - 1)(\sqrt{2} + 1) = (3\sqrt{2} + 3 - 4 - 2\sqrt{2})/1 = \sqrt{2} - 1$, we obtain:

$\sqrt{2} = 1 + 1/(2 + (\sqrt{2} - 1))$ (2)

and we get the approximation:

$\sqrt{2} \approx \boldsymbol{P_1} = 1+1/2 = 3/2 = 1,5$.

Third step.

We have:

$2(3 - 2\sqrt{2}) < q_1 = \sqrt{2} - 1 \Leftrightarrow 6 - 4\sqrt{2} < \sqrt{2} - 1 \Leftrightarrow 7 < 5\sqrt{2} \Leftrightarrow 49 < 50$

and

$q_1 = \sqrt{2} - 1 < 3(3 - 2\sqrt{2}) \Leftrightarrow 7\sqrt{2} < 10 \Leftrightarrow 98 < 100$.

So we get:

$q_1 = \sqrt{2} - 1 = 2q_2 + q_3 = 2(3 - 2\sqrt{2}) + (5\sqrt{2} - 7)$

so that

$p = 1, p_1 = 2, p_2 := 2, q_2 = 3 - 2\sqrt{2}, q_3 := 5\sqrt{2} - 7$,

and

$$a/b = \sqrt{2} = p+\cfrac{1}{p_1+\cfrac{1}{p_2+\cfrac{q_3}{q_2}}} = 1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{5\sqrt{2}-7}{3-2\sqrt{2}}}}$$

and we get the approximation:

$\sqrt{2} \approx \boldsymbol{P_2} = 1+1/(2 + 1/2)) = 1+1/(5/2) = 1 + 2/5 = 7/5 = 1,4$.

More generally we have here a pattern and all the $\boldsymbol{P_k}$ are of the form:

$$\boldsymbol{P_k} = 1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}\cdots}}}$$

So at the fourth step we get: $\sqrt{2} \approx \boldsymbol{P_3} = 17/12 \approx 1,417$

and at the fifth step: $\sqrt{2} \approx \boldsymbol{P_4} = 41/29 \approx 1,4139$[15].

[15] Do the same for $\sqrt{3}$.

5. Generalized '*anthyphairesis*' for the pentagon and for the square.

The main mathematical argument in favour of the study of the pentagon as leading to the existence of incommensurable magnitudes, is the '*anthypheraisis*' process is easily translated geometrically on this figure. Under the hypothesis the 'diagonal' of the pentagon is commensurable to its side, the infinite sequence of pentagons and pentagrams included into each other implies the existence of a strictly decreasing sequence of (positive) integers, which is impossible (cf. §3 above).
But even this argument is not convincing since we have the same phenomenon for the square, and the computations are much simpler.

Firstly for any integer (and even any magnitude) a and b with $a > b$, we have:
$(a+b)^2 + (a-b)^2 = 2a^2 + 2b^2$ (1)
which is immediate consequence of two results of early Greek mathematics, and in any case required to prove Pythagoras' theorem:
$(a+b)^2 = a^2 + 2ab + n^2$ and $(a-b)^2 = a^2 – 2ab + b^2$.

Let us now suppose there exists two integers p and q such that the square root of 2 is equal to the ratio of p and q i.e. $\sqrt{2} = p/q$. Then we have:
$2q^2 = p^2$ (2)
with necessarily $2q > p > q$ (2').

If we note a and b the integers defined by: $a = q$ et $b = p-q$, from (1) we get:
$(a+b)^2 + (a-b)^2 = p^2 + (2q-p)^2 = 2a^2 + 2b^2 = 2q^2 + 2(b-q)^2$ and we get:
$p^2 + (2q-p)^2 = 2q^2 + 2(b-q)^2$.

From (2), the last equality gives:
$p^2 + (2q-p)^2 = p^2 + 2(b-q)^2$ thus:
$(2q-p)^2 = 2(b-q)^2$ so that:
$2 = (2q-p)^2/(b-q)^2$ (3).

Let us note p' and q' the integers: $p' = 2q-p$ and $q' = p-q$ (which makes sense since from (2'): $2q > p > q$).

From (3) we get:
$2 q'^2 = p'^2$ (4)
which implies $2q' > p' > q'$ (4')
and (from the inequalities (2')) we get:
$p' < p$ and $q' < q$ (4'').

So we obtain two new integers $p' < p$ and $q' < q$ such that $\sqrt{2}$ is equal to the ratio of p' and q'. Since we can iterate the above process with p' and q', and so on, we get an infinite sequence of strictly decreasing (positive) integers, which is impossible.

We can see this on the following drawing which gives a geometric construction more in accordance with ancient Greek geometers' proofs[16]:

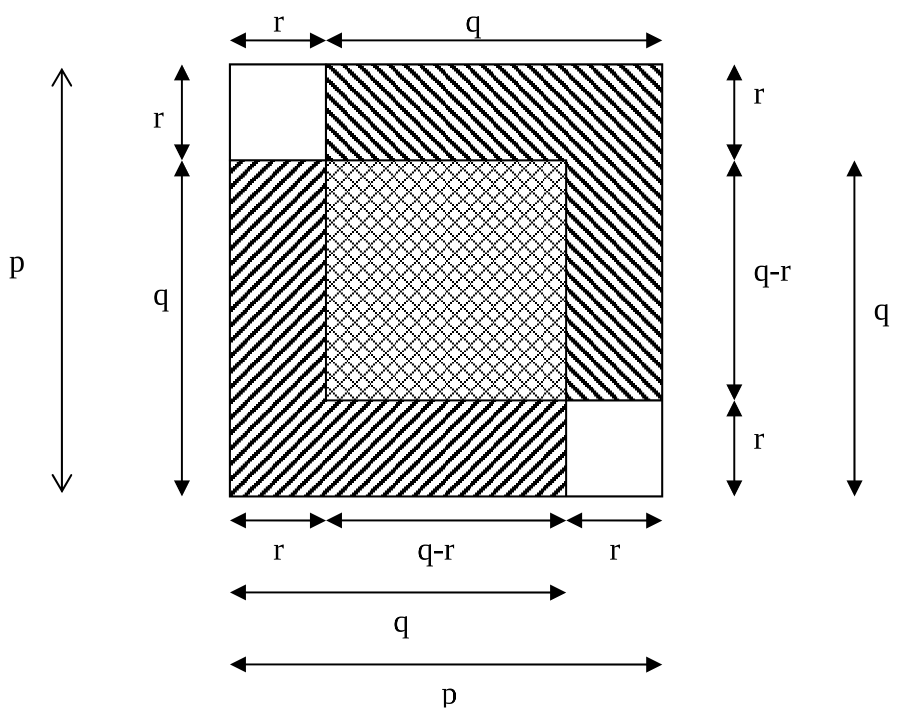


Figure 3

The big square of side p has an area p^2. It is composed on one hand by 2 small squares of side $r = p\text{-}q$ and on the other hand by two square of sides q minus their intersection i.e. the square of side at the center $(q\text{-}r)$ since it is counted twice. Thus we have:
$p^2 = 2r^2 + 2q^2 - (q\text{-}r)^2$.
Since $p^2 = 2q^2$, we get:
$2r^2 = (q\text{-}r)^2$
and thus:
$2 = (q\text{-}r)^2/ r^2$,
with evidently: $q\text{-}r < p$ et $r < q$.
Then if we note: $p' = q\text{-}r$ and $q' = r$, we get two integers p' and q' such that:
$p'^2 = 2q'^2$ i.e. avec $p' < p$ et $q' < q$.

We can then iterate, this time with the squares of side respectively p' and q', and we get a infinite strictly decreasing sequence of squares of sides the integers $p, p', \ldots$ (and also $q, q', \ldots$), which is impossible.
Thus, even from the point of view of the '*anthyphairesis*', the proof of the incommensurability is easier for a square than for a pentagon, and mathematically there is no advantage to use the second instead of the first one.

[16] It does not mean such a proof was ever given in Greek geometry (cf. next paragraph).

6. Generalized ‘*anthyphairesis*’ and irrationality.

The proof for the origin of the irrationality i.e. of the incommensurability of the diagonal to the side of the square is usually considered as the demonstration of the proposition X.117 in Euclid’s *Elements*. Unfortunately, as we saw, it presents many inconsistencies with the textual testimonies. So scholars have searched for others, and many think to have found it with the method of ‘generalized *anthypairesis*’ since:

a) It is a very ancient mathematical tool.
b) It is found in 3 propositions of the *Elements*, propositions X.1, X.2, X.3 (but nowhere else, and never used in this manner) from which it is easy to deduce the equivalence: the algorithm of the ‘generalized *anthypairesis*’ for two magnitudes is finite (i.e. the sequence of approximations P_h is finite) if and only if these magnitudes are commensurable (for instance $\sqrt{2}$ is irrational would be equivalent to the sequence of P_k is infinite).
c) It does not use the theory of relative prime numbers which was certainly elaborated much later.

Therefore it seems to solve all the problems of the first construction.
As a matter of fact, this solution has even more difficulties, and wishing to avoid Charybdis, we run on Scylla.

- Firstly it has nothing to do with the conclusion given in Aristotle’s texts which state the conclusion of the ‘*reductio ad absurdum*’ is the impossibility the odd numbers are equal to the even numbers.
- Secondly, like the standard proof, it is in contradiction with the so-called ‘mathematical part’ of Plato’s *Theaetetus* (and other ancient texts) which shows the proof for the irrationality of the square root of *2* has to be different from the one of the square roots of other integers, for instance *3* or *5*. The ‘generalized *anthypairesis*’ method can be applied indifferently to the square root of any integer, especially *3* or *5*.
- Thirdly it uses an infinite algorithm whereas this kind of computations appears nowhere in Greek mathematics, even much later, even in the *Elements,* even where it would have been natural to use it.
- To prove the sequence of approximations P_k is certainly not easy. Many mathematicians found some tricks to simplify the process, but they are of course done in modern symbolism and algebraically. The geometric interpretation according to Greek mathematics is possible, but trickier and certainly less evident, especially at a time when the very existence of irrational magnitudes was unknown, *a fortiori* when the very existence of such infinite approximating sequences was unknown.
- It is certainly not evident and convincing enough to be used as a model for the ‘*reductio ad absurdum*’ in Aristotle’s classification of syllogisms or to lead the mathematicians used to graphic proofs, even less the philosophers, to adopt a new method of reasoning.

So concerning the study of the origins of the irrationality it seems we are at an impasse: we have no hint to understand how the ancient Greek mathematicians came to the **certitude** of the existence of irrational magnitudes.

V. A proof consistent with the texts.

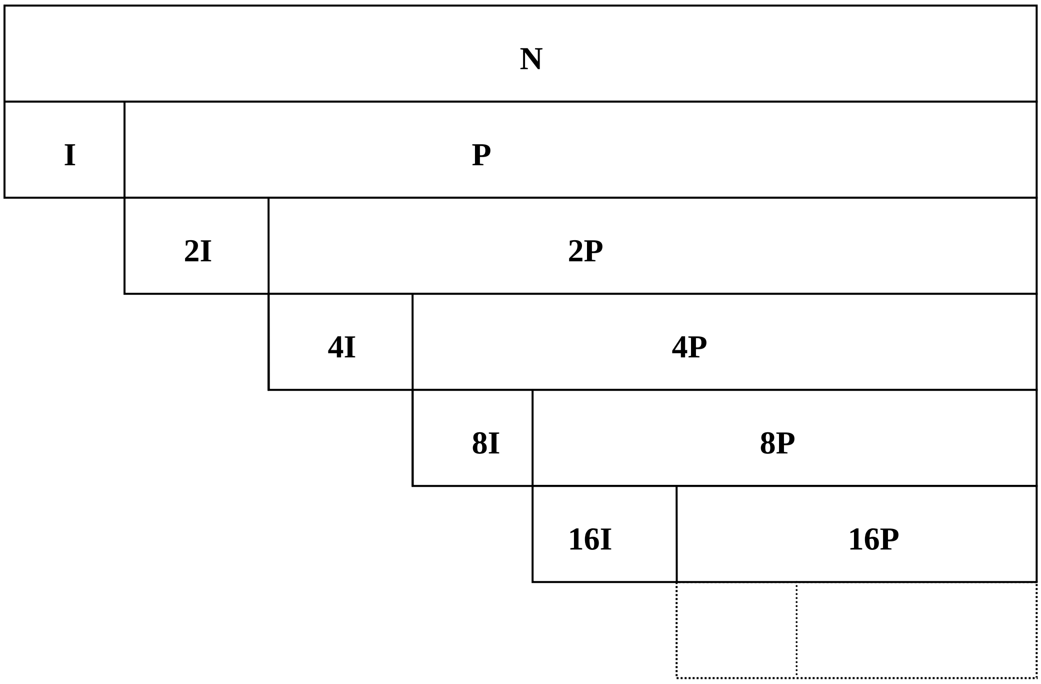
We will now present a proof with the following properties:

1. It uses extremely ancient mathematics, probably known by the ancient Babylonians and certainly the Egyptians.
2. It is in accordance with the ancient Greek texts we have on this subject.
3. It does not use the representation of ratios as ratio of two relatively prime integers (the proposition 22 of book VII of Euclid's *Element*).
4. Contrary to the usual proofs, it does not suppose previously any result proved by a '*reductio ad absurdum*'.
5. It does not have any evident generalization to all integers in particular for *3* and *5*, as requested by Plato's *Theaetetus*.
6. It gives a coherent interpretation of the so-called 'mathematical part' of Plato's Theaetus which subject is precisely the incommensurability.

i) The decomposition odd/even.

As we saw previously, the decomposition of the integers into odd and even is the fundamental property of arithmetic in ancient Greece. But the use of *2* and the division of numbers by *2* as many times as possible (in modern terms by power of *2*), is extremely old, and it is the base of the multiplication, at least of one form of multiplication, in ancient Egypt.

We have also several testimonies about the use by Pythagoreans of tables of powers of *2*, for instance a table given by Nichomachus which has the following form:



It gives a decomposition of even integers as a sequence of the form:
$2(2n+1), 4(2n+1), 8(2n+1), 16(2n+1), \dots$[17]

The integers which are pure powers of *2* being are called even/even (contrary to the meaning in Plato and Euclid). There are also many texts in the oldest Greek works which shows the use of the sequence of the power of *2* was a well-known tool in early Greek mathematics (and even in Egyptian mathematics).
In modern terms its meaning is the following: Any even integer can be written uniquely as a product of a power of *2* with an odd integer i.e. for any integer n there exists two unique integers k and u such that: $n = 2^k u$, where u is odd. For convenience, we will admit the case of the odd numbers by including the case $k = 0$, which is of course an anachronism. But it allows us to shorten the proof, since otherwise we would have to consider separately the case of even and odd integers.

[17] From this decomposition it is very easy to show an extremely counter-intuitive result: there are as many 'rationals' as integers. Could you explain how to do this and what consequences it implies regarding the relation of the Ancients with the infinite?

ii) An essential property of the decomposition odd/even.

The decomposition of any integer n as product of the form $2^k u$ (u odd), has an easy interpretation, evident for instance if we consider the multiplication as the Egyptians did: k is equal to the maximal number of times the integer n can be divided by 2. It is another way to see the uniqueness of k and u.

We have then immediately:

Property of addivity of powers. Let $n = 2^k u$ and $m = 2^l v$ (u and v odd); their product nm verifies: $mn = 2^{k+l} uv$.

Remark. In particular for $n = 2^k u$, we have:
$2n = 2^{k+1} u$, and if n is a (perfect) square, k is necessarily even.

Both results are immediate consequence of the property of the additivity of powers.

iii) The incommensurability of the diagonal to the side of the square.

As we saw, in modern terms, it means the irrationality of the square root of *2*. Using the previous decomposition odd/even we will now give a proof of it.

The beginning is the same as in the standard proof by a '*reductio ad absurdum*'.
Let us suppose $\sqrt{2}$ is rational, we want to obtain a contradiction consistent with Aristotle's testimony.
So let p and q be two integers with $\sqrt{2} = p/q$. As usual, we obtain $2 = p^2/q^2$ and then
$2\, q^2 = p^2$ (1).

From here the demonstration diverges from the standard one, since we do **not assume *p* and *q* relatively prime**.

Let us write p and q using the decomposition odd/even:
There exist four integers k, l, u, v such that:
$p = 2^k\, u,\ q = 2^l\, v$ with u and v odd.

From the property of additivity of powers we have:
$p^2 = 2^{2k}\, u^2$ *and* $q^2 = 2^{2l}\, v^2$.

Replacing in (1) we obtain:
$2\, q^2 = 2\,(2^{2l}\, v^2) = p^2 = 2^{2k}\, u^2$
and from the property of additivity of powers, we get:
$2^{2l+1}\, v^2 = 2^{2k}\, u^2$ (2).

But the decomposition odd/even is unique so we have:
$2l+1 = 2k$ *or* $1 = 2k - 2l$.
The difference of two even numbers is even, so that we get finally:
the unity is even.

Now by definition, an odd number is the sum of an even number and the unity. Since the sum of two even numbers is even, we get that any odd number is an even number, which is exactly the conclusion of Aristotle in the texts of the Analytics.
And it is easy to see this proof verifies all the six conditions listed at the beginning of this chapter iv).

iv) A consequence for the square root of even numbers.

As requested by the condition 5 there is no possible generalization to all the integers. Nevertheless there is an important consequence concerning even numbers.

Let m be an even number of the form:
$m := 2^h w$ with w odd.

Exactly as in the previous proof, by a '*reductio ad absurdum*', if there exists
$p = 2^k u, q = 2^l v$ with u and v odd such that:
$\sqrt{m} = p/q$ i.e. $mq^2 = p^2$,
we obtain the following equality:
$2^h w (2^l v)^2 = (2^k u)^2$
and from the additivity of the powers, we get:

$$2^h w\, 2^{2l} v^2 = 2^{h+2l} w v^2 = 2^{2k} u^2 \qquad (*)$$

and by uniqueness of the decomposition odd/even, we have:

$$h+2l = 2k \qquad (**)$$

So we obtain:

- If h is odd, then this time we have the equality between an odd number and an even number (which is different from the previous conclusion where we got the unity was equal to an even number[18]). Therefore the hypothesis is false and the square root of m is not rational.

- If $h := 2i$ is even, we can not conclude. But, by uniqueness we have both equalities: $h+2l := 2i + 2l = 2k$ (from (**)) and from (*) we get $w v^2 = u^2$ i.e.
  $\sqrt{w} = u/v$ (***)
  where all the integers are odd.

Since $m := 2^h w$, we have: $\sqrt{m} = 2^i \sqrt{w}$
so that the rationality (or the irrationality) of the square root of m is equivalent to the rationality (or irrationality) of the square root of w which in turn is equivalent to (***) i.e. the existence (or not) of 2 **odd** integers u and v such that the square root of w is equal to the ratio of u and v[19].

Thus the problem of the rationality (or irrationality) of the square root of integers is reduced to the question to know for any odd number n when there exists two odd integers whose ratio is equal to the square root of n.

---

[18] Which may explain why future proofs confused the conclusions.
[19] Why is it different from the condition 'the square root of *w* is rational'?

Examples.
The square roots of *2, 6, 8, 10* are irrational; the square root of 4 is rational; the square root of $12 = 4 \times 3 = 2^2 \times 3$ is rational or irrational depending of the rationality or irrationality of the square root of *3*.

Remark. This method can be generalized to cubic roots of integers[20].
As above we obtain the cubic root of any number $n := 2^h w$ where w is odd is irrational if h is not a multiple of *3*.
So for even numbers, the question is once again reduced to the case of odd numbers[21].
For instance the cubic roots of *2, 4, 6* are irrational; the one of *8* is rational; the ones of *10, 12, 14, 16, 18, 20, 22* are irrational; the cubic root of $24 = 8 \times 3 = 2^3 \times 3$ depends of the rationality or the irrationality of the cubic root of *3*.

[20] This is important with respect to the ‘mathematical part’ of Plato’s *Theaetetus* we will consider in the next chapter.
[21] Why?