Università degli studi di Camerino

School of Advanced Studies

DOCTORAL COURSE

IN

MATHEMATICS AND COMPUTER SCIENCE

XXXV cycle

Mathematical Logic in High School: Hints and Proposals

PhD Student

Antonio Fontana

Supervisor

Prof. Carlo Toffalori

Contents

Introduction

In school, students learn how to reason and argue, and logic is the art of reasoning. Aristotle, who first developed it, held it to be so, i.e., the foundation of all science. But one certainly cannot impose on girls and boys an institutional course in logic as a prerequisite to all other knowledge. Not even in high school, when the maturation process of the students allows the teacher some more abstraction. In truth, in the *Archive of Public Education - Cultural, Educational and Professional Profile of High Schools* [129], it is stated that the logical-argumentative area assumes a central role, because it contributes to the formation of a citizen who "*supports her/his own convictions, bringing adequate examples and counterexamples and using concatenations of statements; accepts to change her/his opinion by recognising the logical consequences of a correct argumentation*". But education in logic must be done prudently, in the right formative ways.

Some would argue that the practice of mathematics, often based on reasoning, in particular the model of Euclidean geometry, is in itself a cue to progressively insinuate logical mechanisms. Unfortunately, in recent times, however, Euclidean geometry seems to be a subject in disgrace, often neglected or forgotten. Instead, there are those who emphasise, in mathematics, the importance of intuition, discovery, experience and error, contrasting it with the excessive rigour of too many proofs. The purpose of this thesis is to propose various ideas that, within the fundamental programmes of high school, specifically of Italian Liceo Classico and Liceo Scientifico, attempt to insinuate logic and accustom the students to logic in a way that we hope is light, clear and pleasant. We therefore do not propose a systematic treatment. We prefer to recall basic logic and then to give scattered ideas rather than a structured and definitive theory. But, as mentioned, we are confident that these hints can best prepare students of high school for logic.
Indeed we address ourselves primarily to teachers and we believe that their knowl-

edge of logic is useful and indeed necessary. But through them we also wish to address students.

The thesis is organised as follows.

The first chapter introduces and discusses the whole topic and explains why in our opinion logic is important in high schools. We also discuss how and when to propose it to students.
The next two chapters introduce basic logic to teachers and students. The second illustrates the simplest logic, the Boolean one, recapitulating its essential points and emphasising in particular the use of connectives. The third deals with first-order logic, which we may consider the most classical of logics. Here we highlight in particular the function of quantifiers.
The following chapters propose several topics, belonging to logic or related to logic, that seem very intriguing and could be considered in high school.
First, in chapter four, we treat Aristotelian syllogistics, which, even in recent times, frequently appears in various access tests. We will present some amusing introductions to it, such as those of Lewis Carroll [25] or Pagnan-Rosolini [86].
Chapter five is dedicated to proofs without words. Relying on various examples from geometry, number theory and combinatorial calculus, it illustrates how reasoning can sometimes be successfully expressed and developed through the images and intuitions they suggest. In this chapter, we also discuss the logic of images proposed by Leonardo in the *Codex Atlanticus* [73] to address and solve geometric questions often linked to the Pythagorean theorem.
The sixth chapter is dedicated to what Henri Poincaré called the "mathematical reasoning" par excellence, namely the principle of induction. This law governs natural numbers and is often used as a powerful demonstrative tool in various exercises. However, students seldom learn it and above all understand it properly. Drawing on the history of the principle of induction, from its primitive intuitions to its formalisation by Peano and Dedekind, we attempt to approach it in what we hope will be a pleasant and appealing way, also offering a wide range of examples.
Logical paradoxes are another logical theme that is impossible to forget: mental games that not only disorientate but also intrigue and amuse, which are the heart of the seventh chapter.
To the classical logics considered at the beginning of the thesis, based on two truth

values, yes or no, we then contrast multi-valued and fuzzy logics, which are better suited to analysing situations of uncertainty. We link them, in chapter eight, to the Rényi-Ulam game, which searches for truth in contexts in which the information received may be lying and deceptive.

The final chapter takes up a basic topic of high school mathematics: equations. Diophantine games show us how they can be an opportunity for challenge and fun, as well as suggesting intriguing insights into fundamental themes of modern mathematics: not only number theory and algebra, but also game theory and the theory of computability and computational complexity.

For a general and in-depth overview of mathematical logic, we refer to [10] and [114]. For the theory of computability and computational complexity we refer the reader to [37] and [83], for number theory to [60].

Chapter 1

Why Mathematical logic?

1.1 Some history of logic

There are at least three routes leading to Logic. Two are classical, thousands of years old. The third is relatively more recent. First, there is the path of dialectics, which studies the laws of reasoning in order to enable to use and abuse them in public debates with opponents. Then there is the way of paradoxes (which can be traced back to the sixth century BC). Reasoning sometimes leads to unpredictable conclusions that clash with common experience, or even to antinomies, real puzzles with no apparent way out. In such cases, analysis of reasoning can identify and isolate errors, or confirm embarrassments. Finally, the third, and most recent, way opens up the use of mathematical methods in logic, with its repertoire of arguments and demonstrations. "Mathematical" logic, born essentially in the nineteenth century, can today be considered a branch of modern mathematics.

One of the most important figures in this multi-millennial history, which for the West leads from Greek civilisation to the present day, is Plato, who was the first to identify certain key laws of logic, in particular the principle of non-contradiction, according to which one cannot affirm everything and the opposite of everything, i.e. confirm and deny a proposition at the same time, as the Sophists or the dialecticians did. He stated it in some way in *Book IV* of his famous dialogue *Republic*. Plato can also be traced back to the first intuition of the set theory that he called the theory of ideas, which was the first attempt to understand why a set of objects could be both one and many at the same time. It is not by chance that some of the definitions with which Cantor tried to determine the concept of a set make explicit reference to Plato, for example to his dialogue *Philebus* [96]. However, the greatest logician of antiquity, and in many ways the father of logic as a science, or at least as the basis of all science, was Aristotle, who mainly studied the reasoning scheme called syllogism. A syllogism consists of an ordered triple of propositions in which we find what in modern terms are called quantifiers: all, some, none. Aristotle affirmed the principle of non-contradiction, accompanying it with the principle of the excluded middle, or excluded third (tertium non datur). As we saw before, the former states that for no proposition A both A and its contrary can be affirmed simultaneously. The latter adds that, in any case, exactly one of the two alternatives applies, A or not A, and there are no intermediate possibilities.

A complementary analysis to Aristotle's was carried out by the Stoics, who were interested in a "lower" level of analysis, that of connectives: negation, conjunction, disjunction and implication. In the school of the Stoics, the name of Chrysippus is fundamental, who in a huge series of works (about 700) defined precisely the connectives and also studied the laws of reasoning of propositional logic, in particular *modus ponens* and *modus tollens*. Among other things, Chrysippus also provided an important contribution to mathematics, because he considered the one as a number. Greek logic is thus based on these three cornerstones: Plato, Aristotle and Chrysippus.

After the decline of the classical school, there was a period of disinterest for many centuries, also due to the dark ages of the Middle Ages. But after the year 1000, logic had its second youth, a rebirth that began with Peter Abelard and St Anselm. Of course, the problems and the atmosphere were of a completely different nature from those of the Greek world: there were no longer dialectical discussions in public squares and questions of a religious nature were mainly addressed. The idea of Scholasticism was to arrive at a definition of divinity in logical terms and at one or more demonstrations of the existence of God, obtained as if they were real theorems of mathematics. This study, by the very way it was structured, required great dialectical and logical skill. Anselm of Aosta proposed the ontological proof of God's existence, while Abelard was interested in the question of universals and thus of those general concepts that can be predicated of several individuals.

But to their names can be added that of William of Ockam, perhaps the greatest exponent of medieval logic. Thomas Aquinas set out five arguments to prove the existence of God. Peter of Spain (Petrus Hispanus), who was also pope, fixed the syllogistic. He seems to have suggested the nomenclature and consequent classification of syllogisms, still in use today, based on the vowels A, E, I, O (taken from AdfIrmo and nEgO) and somehow linked to quantifiers. In extreme synthesis: A =

all, E = none, I = some, O = not all.
Scholasticism was a rather long period, about three and a half centuries, and it also allowed the rediscovery of those issues that had been on the agenda in the Greek period, thanks to the recovery and study of the original texts. We refer in particular to the works of Aristotle, which returned to Europe after having been preserved and handed down by the Arabs, but also to the logic of the Stoics, which had been removed and completely forgotten and which the Scholastics had to reinvent, rediscover and study again.
After this second youth, there was a new interlude of oblivion for logic, due partly to the decline of interest and much to the degree of extreme sophistication that Scholasticism had reached towards the end of the 14th century: the arguments had become too complicated to be developed effectively within natural language.
New impulses came with Leibnitz a few centuries later, in the second half of the 1600s. They followed the revolutions that had taken place in the meantime in other fields and in particular in mathematics and algebra. The studies of Viète and Descartes had shown the need for a formal language in this field, which translated the solution of equations into abstract formulas. Leibnitz thought that logic too could be studied with abstract mathematical methods, translating it into calculations and equations, whose solution could settle any discussion on objective bases. As a mathematician, Leibnitz wanted to be able to mechanise the reasoning: after transcribing the data of the question, even the most common ones, into the appropriate language, he wanted to decide on their solution on the basis of appropriate computations. It is in this sense that his famous exhortation "Calculemus!" should be read.
Leibnitz's utopia began to be realised only with the third youth of logic, whose beginning can be officially established in 1847, and whose conclusion can perhaps be fixed in 1936.
The first step, in 1847, was Boole's discovery that the propositional logic of the Stoics could be based on its own particular algebra. In the case of propositions with two truth values, true or false, the latter can be represented by the numbers 1, 0 respectively and the truth of new propositions, formed with the connectives of conjunction, disjunction and negation, correspond respectively to the operations of multiplication, addition modulo 2 and subtraction from 1. New rules replaced the classical algebraic rules: for example, repeating a proposition, i.e. joining it with itself, does not alter its evaluation, whether true or false; like saying that the multiplication operation (if restricted to 0 and 1) is idempotent. In this way both the

principle of non-contradiction and the principle of the excluded third are accepted. Boole's algebra provided an early model of the calculus ratiocinator that Leibnitz had envisioned, and showed how logical deduction could be treated as a branch of mathematics.

After Boole, logic never stopped growing. In the decades that followed, Boole's model also became the basis for the design and operation of electronic circuits and was used by computers to interpret and execute program instructions.

It was with Frege, the German philosopher, logician and mathematician of the late 1800s and early 1900s, that modern logic began to receive a precise axiomatic framework. This is why he is considered the father of modern mathematical logic.

His very ambitious project (logicism) was indeed to prove that all mathematics could be based on logic. During the 19th century, the German mathematician Karlo Weierstrass (1815-1897) had achieved the so-called arithmetisation of analysis and thus highlighted the role of natural numbers in the mathematical structure. For this reason he was called the "father of modern analysis". Frege then set out in search of a logical system that would be the foundation of arithmetic and, through it, of the other parts of mathematics. First he found an abstract language, inspired in some way by Chinese ideography, with which to represent mathematical objects. Thus was born the *Begriffsschrift*, the first example of an artificial formal language with a set of rules to establish which sequences of symbols are acceptable and which are not.

But Frege also managed to reconcile and extend both Aristotelian and Stoic propositional logic, emphasising the use of quantifiers and relations to construct the so-called logic of predicates. He introduced the concept of a formal system. He provided logical axioms of reasoning, to guide deductive calculus, and was also interested in the concept of truth. In this way, he made an immense advance over previous logics, including Boolean logic.

A complete and convincing definition of truth came (at least for first-order logic) only in 1935 with Tarski. More or less contemporary was Gentzen's proposal of an appropriate system of axioms/rules of deduction for the syntax of logical calculus: the so-called *Natural Deduction*, which actually avoids the use of axioms and emphasizes the role of rules - 15 in his case for first-order logic, 11 for propositional logic.

There are also other equivalent systems of proof which reverse the axiom/rule relationship, giving more emphasis to the former. Moreover, Hilbert had already paid great attention to the concept of proof, together with formalism, in the previous

years.
In his project to base the whole of mathematics on logic, Frege could also rely on the concept of set, which in the late nineteenth century was developed by Georg Cantor to allow a rigorous mathematical approach to the study of infinity. Frege believed that a foundation of sets could support arithmetic and thus, as mentioned, all mathematics. He then introduced the concept of natural number in purely logical terms, thanks to set theory. He then turned to find appropriate foundations for this theory.
The Fregean system for sets had six logical principles but, of these, the two basic ones were extensionality and comprehension. They can be formulated in a language with individual variables for sets and with predicates for membership ($\in$) and, of course, equality ($=$).
The principle of extensionality states that two sets are equal if and only if they have the same elements; therefore sets are to be understood only by their elements, and not by the description by which they are introduced.
The principle of comprehension states that given every property $P(x)$ defines a set, that is the set of elements that satisfy it. Note, however, the delicate role that the concept of property plays in the statement - intuitive, and therefore to be fully formalised.
But, in June 1902, a letter arrived to Frege from the young philosopher Bertrand Russell that challenged the logicist program. In particular, Russell noted antinomies within it, i.e. propositions that look correct, but instead leads to contradictions.
Russell's letter made particular reference to the principle of comprehension and pointed out its inconsistency. For if $P(x)$ represents the property $x \notin x$, i.e. that x does not belong to itself, then by the principle of comprehension one can define the set of all x that do not belong to themselves, i.e. $M = \{x : x \notin x\}$. But then about M one easily arrives at the contradiction

$$M \in M \longleftrightarrow M \notin M$$

which is equivalent to

$$(M \in M) \wedge \neg(M \in M).$$

In this consists Russell's paradox, which shows that not every property determines a set, and that not every collection of elements can be considered a set.
The contradictions that emerged from Russell's studies at the beginning of the

twentieth century touched and to some extent undermined the ambition to provide mathematics of the time with the appropriate foundations; they led to multiple and opposing reactions among scholars. In fact, in contrast to those who, like Frege, were shocked and discouraged, there were those, like David Hilbert, who felt that Russell's incident reaffirmed the importance of a serious, rigorous and well-founded axiomatic method, immune to doubts and contradictions.
Hilbert was a German mathematician, one of the most eminent and influential of the nineteenth and twentieth centuries, professor in the prestigious University of Göttingen. He was particularly interested in algebraic number theory. One of his greatest merits, in addition to providing modern physics with the appropriate mathematical foundations, was to reorganise the foundations of geometry in the late 19th century. But Hilbert also made significant contributions to the philosophy of mathematics and logic.
He welcomed Cantor's work on infinity and celebrated it with enthusiastic expressions.
To defend Cantor from his numerous detractors, and to demonstrate that infinity is an admissible theme in mathematics as well, Hilbert developed his own general conception of mathematics, seen as a collection of hypothetical-deductive systems concerning arithmetic, or analysis, or plane geometry, etc., including infinity, fully free in their development, except for the respect of two fundamental rules:

- consistency, i.e. the absence of contradictions, the certainty that the proofs arising from that system will never produce absurd and irreconcilable results;
- completeness, i.e. the capacity to exclude any ambiguity, to prove or disprove any proposition that arises within the system, to prove in any case the proposition itself or its negation.

Thus, for Hilbert, "good" mathematics is a repertoire of formal systems, each with its axioms, rules and theorems, and each consistent and complete. In 1928 Hilbert raised two problems within Frege's first-order logic. First, completeness, specifically the proof that this logic could prove by its rules of deduction all and only those formulas which, seen from the outside, are accepted as valid. The second question was the *Entscheidungsproblem*, or decision problem, and called for a method which, given a formula of first-order logic, would determine in a finite number of well-defined and effective steps whether or not it was provable.
Hilbert was also a representative of the reductionist approach. At the Second International Congress of Mathematics in Paris in 1900, he gave a speech of historic

significance [62], proposing a list of 23 open problems, which he considered to be the challenge for mathematicians of the coming century. The nature of these problems was varied and uneven: some were very specific and technically well delineated, others were too general or too vague to admit an incontrovertible answer. Still others, Problems 1, 2 and 10 (Continuum Hypothesis, Consistency of Arithmetic and Solving Diophantine Equations) have solutions that perhaps were unexpected to Hilbert: they are also important because of their close connection with the foundations of the Computability Theory, and thus with a formal framing of the foundations of Computer Science.

Hilbert's attempt at a complete foundation of mathematics was destined to fail: it was in fact in 1930 that Gödel with his incompleteness theorems demonstrated how a non-contradictory formal system, which includes at least arithmetic, cannot prove its own consistency within its axioms.

The first incompleteness theorem states that in any formal system with the above properties, propositions can be constructed that the system cannot decide: it can neither prove nor reject them on the basis of its axioms and rules of deduction.

The second incompleteness theorem states that no formal system that includes elementary number theory and is free of contradictions can (under appropriate additional assumptions) self-certify its consistency, i.e. prove it internally as its own theorem.

It was only after Gödel's breakthrough, in 1936, that Church and Turing found a solution to Hilbert's second problem, that was just the *Entscheidungsproblem*. By both resorting to the techniques first used by Gödel in his incompleteness theorem for arithmetic, Church and Turing independently established that the decision problem is unsolvable. As a result, they proved what is now called the undecidability of first-order logic.

1936 was therefore a year of innovation, not least because it was in the course of his article [116] on the *Entscheidungsproblem* that Alan Turing

- defined computability in terms of Turing machines (TMs),
- formulated the halting problem for TMs and basically proved its insolubility,
- connected the halting and decision problems.

Before concluding this paragraph, we would like to underline once again how the study and the progress of logic have allowed the development of modern computer science together with its languages and programs: Leibniz's dream of a universal logic, the fundamental works of Turing and Church, and the problems that in the famous list of 23 mathematical questions proposed by Hilbert in 1900 occupy the places 2 and 10, but also 1, have led scientific thought towards the conquest of an explicit concept of "computability", which preceded by some years the realisation of the first modern computers.

1.2 Mathematics: intuition or rigour?

The debate on the role of intuition and rigour in mathematics education and research is still very lively, but it has very ancient roots. In some sense, the issue can be traced back to classical Greece and Euclid, for the geometry of the *Elements* [44] was considered and even revered for centuries as a model of immaculate rigour. Euclid, however, developed it on the basis of intuition, or in any case of perceptible experience, taking care to provide explicit and accurate constructions of the geometric objects he dealt with. Moreover, in the *Elements*, the rigour is not always impeccable and the very first construction itself (that of an equilateral triangle with an assigned side) contains a logical fallacy, albeit venial.
To tell the truth, the need for rigour, although intrinsically present in Euclid's work, did not fully emerge in mathematics until later, at the end of the nineteenth century. In earlier periods of history, mathematics focused above all on solving problems prompted by the physical analysis of the world. The 1800s, on the other hand, were called "the century of rigour", and indeed in that period mathematics addressed the question of the relationship between intuition and experience and developed various theories in this respect.
Felix Klein was one of the first to investigate what was meant by *geometric intuition*. He was convinced that such intuition was something essentially imprecise: for him the axiom was nothing more than the search for a precise statement in an imprecise intuitive construction. Axioms, therefore, only secured a logical substratum on which to base purely intuitive observations. It is therefore clear that Klein was opposed to strictly axiomatic approaches. Regarding the true nature of geometric intuition, he distinguished between naive and refined intuition. The intimate reason for this distinction lies in the fact that the former is totally lacking in rigour while the latter is not a true intuition, since it originates from the logical development of perfectly rigorous axioms. Naive intuition is that which makes it possible to conceive of a completely abstract mathematical entity by making it concrete, so that the re-

sulting definitions are only rigorous in approximation. Klein rejects this intuition that can be derived directly from the senses in favour of the refined intuition that is obtained through a profound conceptual reworking of sensory data.
In this way, the basic question of whether mathematics should rely on intuition or rigour, on experience or logic, on images or thoughts, is posed in a deeper form. For example, in the case of geometry: can the research activity of *homo mathematicus* (be it invention or discovery) be based only on names, signs or symbols, or must he necessarily have recourse to drawings, figures, mental representations, schemes or diagrams?
At the end of the nineteenth century, mathematics, within and outside of geometry, began to present itself as an eminently abstract and formalised discipline. In this perspective, Euclid's axiomatic method, already discussed in the previous paragraph, was revised and perfected, and articulated in a ternary scheme that seemed to create a sort of theoretical *perpetuum mobile*: axioms, definitions, theorems.
A theorem is nothing more than the last step in a finite chain of syntactically correct propositions derived from axioms using «inference rules» accepted as valid by the scientific community. This is the formalist conception of mathematics, the formulation of which is due to Hilbert, who theorised it as a way out of the so-called "crisis of the foundations", as previously mentioned, in often polemical opposition with mathematicians such as Luitzen Brouwer and Henri Poincaré.
In the formalist conception there is hardly any place for images. In his *Grundlagen der Geometrie* of 1899 [63], for example, Hilbert settled Euclidean geometry definitively with an axiomatization that eliminated all intuitive and visual suggestions associated with terms such as point, line and plane.
In 1918, in an essay entitled *Axiomatic Thinking* [64], he expressed his conviction:
"*I believe: everything that can be the object of scientific thought, as soon as it is ripe for the formation of a theory, falls under the axiomatic method and through it under mathematics.*"
In a letter to Frege, Hilbert defends his approach as follows:
"*If this is mathematics, a science of abstract words, naked and «as bare as a ghost to whom one would like to lend a sheet», its practitioners would seem to be hopelessly condemned to wander in an obscure labyrinth of purely syntactic concepts, a dense network of hidden structures. Why, then, do we continue to draw triangles and circumferences on blackboards? Why do both research articles and textbook pages teem with figures, diagrams, schemes and drawings? Why do mathematicians, in their reasoning, not limit themselves to rattling off syllogisms or performing calculation*

after calculation, but strive to visualise problems by resorting to images of all kinds? Images that may be vague, confused, indistinct, or even unrepresentable, or even unintelligible, but which nonetheless play an essential and not merely accessory role in research work and the learning process."

Poincaré, who was a mathematician as famous as Hilbert, and who certainly shared Hilbert's love of mathematics and research, took a completely different view; both believed in a "*science for science's sake*", so beautiful in itself. They then exchanged expressions of mutual esteem (in truth, more on Hilbert's part, who was also younger). On the previous subject, however, the visions of the two tended to diverge.

Poincaré devoted very beautiful and compelling autobiographical pages to intuition and he did not avoid heavy criticisms of Hilbert's aristocratic geometry. A famous example can be read in his treatise *Science and Method* [100], blaming the abstract way in which the German mathematician approached certain fundamental objects such as points, lines and planes, that is, as simple "*things*":

"*What on earth these things are*", Poincaré then comments, "*we not only ignore, but we should not even try to find out. We have no need of it, and even those who have never seen points, lines or planes could do geometry no less well than we can*".

The criticism continues: "*It is understood that in order to prove a theorem it is not necessary, nor even useful, to know what it means. The geometer could very well be replaced by Stanley Jevons's "logical piano*" - a machine of that era, nowadays we could say a computer. And again: "*or if you prefer, you could devise a machine in which you introduce axioms at one end and collect theorems at the other end, like the legendary Chicago machine in which pigs enter alive to come out at the end transformed into ham and sausages. Like such machines, the mathematician has no need to understand what he is doing*".

In short, Poincaré showed his impatience towards too many logical impositions. Let's read another passage from *Science and Method* [100]:

"*For my part, I see nothing in logistics that hinders invention. It certainly does not help to be more concise, quite the contrary; and if it takes 27 equations to prove that 1 is a number, how many will it take to prove a real theorem? [...] It may be safer, but it certainly doesn't go any faster. No, you don't give us wings, you make us walk with dandies.*"

Henri Poincaré therefore preferred intuition to abstraction and rigour. For him, intuition is the instrument of mathematical invention and plays a crucial role: it allows one to choose which route to take in the search for scientific truth, to direct subsequent logical developments. In fact, Poincaré stated: "*logic, which can only give certainty, is the instrument of demonstration; intuition, the instrument of invention*". To use a Kantian expression: "*logic without intuition is empty and intuition without logic is blind*".

Poincaré did not fail to recognise, albeit reluctantly, the limits of pure intuition which, when operating alone, cannot guarantee "*rigour or even certainty*" and often generate misleading convictions. In *Science and Hypothesis* (1902) [101], Poincaré anticipated Brouwer's intuitionism, rejecting, among other things, the principle of the excluded third, to which Hilbert accepted.

Returning to Hilbert, however, it is right to emphasise that in his view rigour is not the "enemy of simplicity", on the contrary, it helps and orients in the most rapid and direct solutions. Rigour is not synonymous with rigidity. It is, rather, essentiality, sobriety, austerity and should not be confused with obtuseness, the pretence of absoluteness and closure, "*it does not hold back like the dandies, on the contrary, it helps to fly*" (remember Poincaré's phrase in [100]).

The "intuition or rigour" antithesis obviously also affects the issue of teaching and learning and is still hotly debated today.

Nowadays, the question becomes: how to educate to reasoning? With regular and insistent exercise, as in the past, or, as it is now preferred, with play, workshops, discovery and the creative cooperation of students with teachers or professors?

Mathematical rigour, and particularly rigorous mathematical language, can seem a bitter enemy of communication: it is well known that non-mathematicians are frightened even to see a formula in a text. Among mathematics teachers, there is a widespread idea that, even in teaching in primary school, a rigorous treatment of mathematics should always be demanded; this demand often takes the form of an exaggerated formalism or an antiquated and obsolete use of the language in which mathematics is expressed. These teachers may believe that they have on their side an authoritative figure, Giuseppe Peano, who indeed wrote: "*the teaching of mathematics must be rigorous at every school level; if a demonstration is done, it must be rigorous; if it cannot be done because of the age or immaturity of the student, then it should not be done*".

Actually, the first to "transgress" this sort of "didactic axiom" was Peano himself. A genius of many interests, when he was asked to write notes on mathematical exercises, especially arithmetic, for elementary school children, he had to realise, probably "playing" as he used to do with children, that there is rigour and rigour. In his famous and amusing booklet *Giochi di aritmetica e problemi interessanti* [90]

he is engaged in a successful work of mathematical divulgation precisely because he feels the futility of resorting to mathematical "rigour" in exchange for a greater understanding and usability of the subject. Finally, Peano himself stated:
"*Mathematical rigour is very simple. It consists in asserting all things that are true, and in not asserting things that we know are not true. It does not lie in affirming all possible truths.*"
In addition to Peano, other Italian mathematicians have dedicated pages of their writings to the debate between intuition and rigour, including Francesco Severi and Federigo Enriques. Their reflections can be defined as mathematical in their dryness and measure, but are witty, lively and colourful in their form. Their studies concern the didactic sphere, i.e. education to rationality. Both recommend the right balance of logic and intuition, and suggest to privilege the latter and to be very cautious in the use of the former.
Severi's reflection [108] advises against the excessive use of logic in the teaching of mathematics, which, if used in exaggerated doses, risks provoking, as he himself states, "*indigestion of the brain*", which is "*forced to ingest food that is too heavy*". On the contrary, "*for the education of the intellect, intuition must first be developed*", which is a "*creative faculty*" and a "*synthesis of sensations, observations and experiences".*
Severi argues that, at least in the first years of schools, teaching should be "*exclusively intuitive*" and abolish all formal definitions and all chains of logical deductions. The imperative is to focus on ideas and not on rigour.
As for mathematical intuition, he recalls Poincaré in certain passages, especially when he speaks of the sudden illumination that sheds "*the brightest light*" on a concept that had previously appeared "*obscure and abstruse*".
On the same subject, that of teaching, concerns similar to Severi's are expressed by another great Italian mathematician of the early 20th century, Federigo Enriques [42].
He believes that, in education, intuition and logic are not "*distinct faculties of intelligence*", but "*inseparable aspects of the same active process*". He then distinguished "*a logic in small and a logic in large*", that is, "*the refined analysis of the process of exact thought and, on the other hand, the study of the organic connections of the system, that is, the macroscopic view of science*". But, he feared, in the concerns of our mathematical educators, the former would prevail over the latter.
At the end of this brief account of an age-old debate on the relationship between intuition and rigour, it seems that the prevailing suggestion is to reconcile the two

extremes, in order to obtain for both the right use in teaching and research, without ever exceeding in one or the other direction.

1.3 National indications for high schools

The history of logic, its recent confluence within mathematics, as well as the debate on the role of intuition and rigour in the teaching and learning of mathematics, suggest to consider an appropriate logical education for both students and future teachers: not only for a technical knowledge of formulas and syllogisms, but for an education in rationality and mathematical thinking.
Over the years, in fact, the role that mathematical logic plays in real life and in cultural education has been highlighted: in the birth and development of computer science for the architecture of calculations, programmes and algorithms; in the search for mathematical and philosophical truth, but also in overcoming the classic opposition between true and false towards the elaboration of a logic of probability and uncertainty; in the study of the delicate relationship between mathematical language and common language, between abstract deduction and normal common sense.
It is, however, a fact that logic is never explicitly mentioned either in the *Indicazioni Nazionali* (Italian National Indications) [128] of Mathematics for *Licei Scientifici* or in those for *Licei Classici*.
In the general outlines and competences of both, we read:
"*... the student will know the elementary concepts and methods of mathematics, both internal to the discipline itself and relevant to the description and prediction of phenomena, particularly of the physical world. They will be able to place the various mathematical theories studied in the historical context in which they developed and understand their conceptual meaning.*
The student will have acquired a historical-critical view of the relationships between the main themes of mathematical thought and the philosophical, scientific and technological context.
In particular, he/she will have acquired the sense and the scope of the three main moments that characterize the formation of mathematical thought: mathematics in Greek civilization, the infinitesimal calculus that was born with the scientific revolution of the seventeenth century and that led to the mathematization of the physical world, the turning point that started from the Enlightenment rationalism and that led to the formation of modern mathematics and to a new process of mathematization

that invested new fields (technology, social sciences, economics, biology) and that changed the face of scientific knowledge".

For the individual classical high school, it is then recommended to devote *"special attention [...] to the relations between mathematical thought and philosophical thought"*.

Ultimately, it seems that logic is only hinted at between the lines: those who seek it may find it, while others probably do not.

Some content of logic, if anything, can be found in the chapter on Philosophy, where it is written that "*thanks to the study of the various authors and the direct reading of their texts, the student will be able to orient himself on the following fundamental problems: ontology, ethics and the question of happiness, philosophy's relationship with religious traditions, the problem of knowledge,* ***logical problems****, the relationship between philosophy and other forms of knowledge, especially science, the sense of beauty, freedom and power in political thought, the latter node being linked to the development of skills related to Citizenship and Constitution*".

Now, given that the indications emphasise the importance of *interdisciplinarity* as a connection between the various sciences and the various cultural expressions, logic being relevant to both Philosophy and Mathematics, it can be considered, at least implicitly, an integral part not only of the former but also of the latter.

In the same vein, one might perhaps venture that the *National Indications* mean logic as "pervasive" and take its learning for granted, as the result of the study of various disciplines, including mathematics and philosophy. But in this way they risk making it invisible to the learner and lead the teacher to undervalue it. And yet, as already mentioned, the need to reason and argue is perfectly relevant.

In any case, the *National Indications* themselves require, as already noted, the development of students' communication and argumentation skills:

"*In particular, mathematics (...) contributes to developing the ability to communicate and discuss, to argue correctly, to understand the views and arguments of others.*"

It is therefore wished the formation of an active and aware citizenship, in which each person is willing to listen attentively and critically to the other and to compare opinions in a solid and objective way.

Education in argumentation can be an antidote to the proliferation of false or uncontrolled information.

It is therefore no coincidence that the Directions insist on this.

In the *Archive of Public Education - Cultural, educational and professional profile of*

Licei - Annex A [129] it is stated: "*Liceal culture allows to deepen and develop knowledge and skills, to mature competences and acquire tools in the five areas of study common to all Liceal courses, and one of these is precisely the logical-argumentative area*". It is therefore reiterated that the latter assumes a central role, precisely because it contributes to the formation of a citizen who "*supports her/his own convictions, giving appropriate examples and counterexamples and using concatenations of statements; accepts to change her/his opinion by recognising the logical consequences of a correct argumentation*" ([128], p. 60).
So the previous recommendation, while leaving aside specific mathematical themes, is repeated in its generality.
Logic is called upon to constitute a fundamental element of a students overall education: it gets students used to abstracting the appropriate theoretical "model" from contingent situations and provides the indispensable tools for understanding the world.
The related competences that pupils must acquire at the end of their high school education are therefore described as follows (in the National Indications for High Schools):

- Knowing how to support one's own thesis and how to listen to and critically evaluate the **arguments** of others.
- To acquire the habit of **reasoning** with logical rigour, **to identify problems** and to identify possible **solutions**.
- To be able to read and **critically** interpret the contents of different forms of communication.

The study of logic is therefore naturally also part of the baggage of a mathematics teacher who wants to offer her/his subject and wants to stimulate her/his pupils in every possible way, encouraging them to reason. The school is no longer a place where notions are administered, but a creative laboratory, a workshop of ideas and projects, with the explicit aim of educating rationality. With this in mind, it is essential that the teacher, not only of mathematics, has a thorough knowledge of the historical and epistemological aspects of her/his discipline, but also (especially in mathematics) a familiarity with logic.
Mathematics at school cannot be reduced to theorems and applications alone, but also to history, to didactic forms matured over the centuries, including logic, to formal rules of reasoning as well as the question of foundations. Teachers who have

not been able to deal with these issues during their degree course will certainly be able to go into them in greater depth in post-graduate and refresher courses. In this respect, the National Indications, despite their limitations, represent an important stage of renewal in an Italian school that has been tied to the Gentile Reform model for too long.

Specifically, a large part of high school has been completely renewed in its curricular structure, methodology and content since the early 1990s, while another considerable part, however, is still unable to break away from the Gentile Reform approach and its traditional views and methods.

This is also the case of Licei, which have courses that date back to the Gentile Reform (traditional addresses) and at the same time, since the early 1990s, have launched experimental courses, such as Piani di Studio Brocca, the Piano Nazionale Informatica (PNI), more recently the Piano Lauree Scientifiche and, most recently, the Licei Matematici project.

The latter could be a good place to introduce students to elements of logic in a pleasant, humorous and non-professorial way.

At the same time, other types of schools, such as Technical and Professional Institutes, have also been experimenting with curricula (including the introduction of a transversal logic curriculum which selects and explores in depth only certain points of the standard curriculum) of increasing interest. Today, these institutes have relatively new curricula.

A final reflection concerns Liceo Classico and all the reformed Licei and their relationship with the university, as indicated in the general lines of the Physics objectives, where they require teachers to "*promote collaboration between educational institutions and universities, research bodies, science museums and the world of work, especially for the benefit of students in the last two years*".

In recent years, in particular, the experience of the Piano Nazionale Lauree Scientifiche (PLS) has established points of contact and ensured collaboration between pupils and teachers at all levels to support the development and spread of a mathematical culture among students, old and new teachers, more generally in the whole modern society. The PLS can also be an opportunity to approach logic in an enjoyable and engaging way.

1.4 Educational experiences

Our report has highlighted the value of reasoning as an indispensable condition for learning, and the inevitable relationship between understanding, knowledge, skills and behaviour.

Understanding is closely linked to reasoning about what is being learnt, whence the need to develop students' ability to reason in a declarative manner, which is considered a critical element by all teachers and acknowledged as a serious deficiency by the results of the OECD-PISA (Programme for International Student Assessment) survey [130], promoted to measure the skills of 15-year-olds in school. The general aim of PISA is to ascertain whether, and to what extent, young people leaving compulsory school have acquired certain skills considered essential for playing a conscious and active role in society and for continuing "lifelong learning".

PISA not only takes into account students' school curricula and knowledge, but also examines their ability to reflect on the same knowledge and experiences by applying them to real-life situations. To indicate this set of knowledge and skills, the term "literacy" was used as the process of acquiring a domain tool that goes beyond the school concept of curriculum mastery. In particular, three areas of literacy have been identified as indispensable in a lifelong learning perspective:

- *reading literacy*, meaning the ability to use and interpret written text by reflecting on it;
- *mathematical literacy*, meaning the functional use of mathematical knowledge in various contexts;
- *scientific literacy*, as the ability to use scientific knowledge and to draw data-based conclusions to understand and make decisions about the natural world.

These three areas of assessment are complemented by that of some transversal competences, such as *problem solving*, understood as an individual's ability to put in place cognitive processes to face and solve real and interdisciplinary situations in which the areas of competence are not within the single domains of mathematics, science or reading.

Among the various strategies put in place to address the causes of the problematic outcomes of the PISA survey is the Education to Rationality, Argumentation and Logic Project [131], carried out within IRRE Liguria from 1999 to 2006, with the scientific partnership of the Faculty of Mathematical, Physical and Natural Sciences of the University of Genoa and the Italian Association of Logic and its Applications (AILA).

The interdisciplinary character of the project gave birth to a research and training group and produced a wide range of activities for the development of education to rationality in the second and in the third years of secondary school, organising multidisciplinary and transversal teaching modules.

The transversality of the approach is expressed by the fact that proposals are formulated to improve or change the curricula of philosophy, physics, computer science, Italian, Latin and mathematics in function of an education to rationality adapted to today's socio-cultural reality. The hinge of the proposal is the need to recover the declarative, argumentative and demonstrative aspect of all the competences and, in equal measure, to prepare young people for the cognitive management of a multiple rationality typical of modern society.

Without familiarity with argumentation, one does not know how to demonstrate; in particular, without the linguistic competence presupposed by the ability to argue, one is not even able to understand the demonstrations set out by a text or by the teacher.

Arguing helps the teacher to understand and interpret the pupils mistakes and strengthens their knowledge of more specific aspects of content, which would otherwise be quickly forgotten. Getting students used to giving definitions is therefore fundamental to language education at all ages: a person who knows how to argue and who knows how to evaluate the arguments of others is a *stronger*, less helpless person. The first definitions are found in Primary School, where defining basically means describing and where, consequently, they are often overabundant (e.g. a triangle is called equilateral when its three sides are equal and when its three angles are equal). Also in Secondary School, it is important that a student succeeds in describing a figure or a situation in appropriate terms and with a certain linguistic precision; it is not reasonable, on the other hand, for the teacher to pretend to always be demanding; there are situations in which, especially in High School, it may be appropriate to replace rigorous definitions with intuitive explanations (for example when one speaks of an *infinite set* or of a *function*).

In the field of arguments that take logic into account, in a first approach free arguments are advisable, meaning arguments that, although taking logic into account, support relevant parts of the discourse with expressive resources of language that are independent of logic. In a more restrictive approach, we have arguments that respect the style of a proof, as scientifically meant: the language chosen is the one most

suited to the disciplinary context and the addressees, the inferences proposed are valid according to classical logic and formal fallacies (i.e. hidden errors in reasoning) are not admitted. This twofold approach should avoid a too drastical distinction and transfer from free to rigorous arguments in a somewhat continuous way.
To further confirm the importance of argumentation as a central competence for the growth of the individual (also underlined by the new National Indications which place its development among the fundamental goals of mathematics education) we cite Claudio Bernardi's contribution to the book [119].
It starts from the premise that arguing is a transversal competence, which is linked to others, including linguistic ones. This correlation causes various difficulties, amplified by the fact that mathematical language has its own peculiarities. Bernardi focuses his attention on the difference between the language of logic in mathematics education and the natural everyday language, which is free of too many symbolisms. Indeed in natural language, in our case Italian, there are words from everyday life that are also used in mathematical language, but without the same meaning. This gives rise to ambiguities that can generate misunderstandings and uncertainties in a student for whom the meaning of everyday language obviously prevails over that of mathematics. Moreover, while mathematical rigour demands precision, clarity and unambiguousness, in everyday life we often use words with more than one meaning. Take the term *logic* itself. Coming from the ancient Greek, it is full of meanings: word, tale, discussion, reasoning.
On the other hand, for today's students, the ability to express themselves in appropriate language and to reason correctly and logically is basic and is almost always linked to their ability to understand and develop mathematics.
The use of specific, less ambiguous language is therefore indispensable. It is therefore necessary to promote, in the appropriate forms and within the appropriate limits, education in logical language: symbolic, precise, less expressive than natural language, but with the advantages listed above.
Here are some examples of the inaccuracies and errors of a logical nature that are found in the structure of sentences that recur frequently in everyday communication. We draw them from the already mentioned Bernardi's work [119].

- First of all, let us consider the language of advertising: a given cream makes the face 75% brighter, or a given shampoo makes the hair 58% softer. It is difficult to believe that these numbers have a real exact scientific content but the impression of people listening to the advertising is that the company producing the cream or shampoo has done precise research on the subject.

- On a packet of biscuits one reads *produced with wholemeal flour* (or with oat wheat, etc.). If you read the list of ingredients, which is required by law to appear on the packaging, you sometimes get a surprise: the biscuits do indeed contain wholemeal or oat flour, but also normal wheat flour. Therefore the initial sentence is not false, but can easily be interpreted as "made *only* with wholemeal flour".

Education to rationality and the ability to argue has been the specific theme of various conferences, including recent ones: in Genoa in 2007, in Salerno in 2008, in Verona in 2009, again in Salerno in 2010, in Sestri Levante in 2016 and in Turin in 2019. The meeting in Sestri Levante was dedicated to the memory of Paolo Gentilini, who for years dealt with the topics described here with passion and depth. The book [138], which follows on from the conference in Sestri Levante, 9-11 June 2016, and was edited in 2019 by Francesca Morselli, Giuseppe Rosolini and Carlo Toffalori, contains testimonies and contributions from various experts and offers many points for reflection on the value of argumentation, which is reaffirmed as a fundamental skill for pupils and teachers alike.
In conclusion, to underline the value of the ability to understand and formulate arguments (*critical thinking* as the Anglo-Saxons say) and its strong ethical and, of course, cognitive value, let me quote Norberto Bobbio (an Italian philosopher, jurist, historian and senator for life of the second half of the 20th century):
"*The theory of argumentation is the study of the good reasons with which men speak and discuss choices that imply reference to values when they have given up imposing them by violence or wrenching them by psychological coercion, that is to say, by oppression and indoctrination*" (in the preface to [94]).

1.5 Access tests, and more besides

Biology, chemistry, physics, mathematics ... But is it also necessary to study logic for a test?
As well as being the first step in competition procedures and sometimes the only one for selecting competitors, the test is now also used for university admission, not only to mathematics and computer science and other exact science degree courses, but also to medicine, social sciences, architecture and others.

Among the most frequent and sometimes most important questions are undoubtedly the questions on logic (in addition to those on general culture). Although not all competitors agree with this method of selection, in competition procedures it is the one preferred, because it is considered objective in the evaluation of candidates. It is therefore used in the most important public competitions, for example in the tests organised by RIPAM, the public administration requalification programme managed by Formez PA - the service centre that operates on a national level and answers to the Department of Public Administration of the Presidency of the Italian Council of Ministers. But quizzes also appear in health competitions, in tests for access to military careers and, as already mentioned, for university admission.
In general, questions are commonly referred to as logic or logical reasoning questions because they do not depend on the cultural level of the subject to whom they are administered and assess only mental flexibility and reasoning ability. In the classification of questions, logic corresponds to different types of questions. A first standard classification distinguishes between:

- verbal logic questions,
- critical reasoning questions,
- questions of mathematical logic,
- questions on abstract reasoning and spatial reasoning, attention and accuracy.

Verbal logic questions assess the candidate's verbal aptitude by testing her or his linguistic competence, control of language and vocabulary. These questions, which require a linguistic solving strategy, take a variety of forms but they are mainly based on relationships and associations between words, identification of antonyms, synonyms, anagrams, etc. Other verbal content questions, known as verbal-critical reasoning questions, require understanding and interpreting the meaning of a text, drawing conclusions from it or excluding implications from it.
Critical reasoning questions test the ability to think logically and deductively, i.e. (again) to understand an argumentative text, to grasp its salient features, to deduce implications and draw conclusions and to recognise causal links between elements (critical thinking). Selection tests frequently ask questions concerning simple deductions, syllogisms, necessary and sufficient conditions, negations and logical-verbal problems in which logically necessary conclusions can be drawn from certain premises. Problem-solving strategies for such questions focus on careful linguistic

analysis, although logical-mathematical rules often facilitate resolution.
Mathematical logic questions assess reasoning ability, mental calculation skills and mathematical and logical intuition. These quizzes often require simple mental calculation skills: basic mathematical knowledge and the ability to apply it directly and immediately are sufficient to solve them. Selection tests consisting of mathematical logic questions must be faced without the use of calculators. Quick calculation is therefore one of the basic prerequisites for these tests. This ability, if not innate, cannot even be taught and is the result of years of practice. It may be enhanced by learning methods to speed up computations, the so-called tricks.
The area of logical-mathematical tests includes:

- questions of numerical logic or numerical reasoning in which the logical connection between the numbers and/or letters in the series must be identified;
- numerical logic questions in graphical-geometric configurations, in which the numbers or letters of a series are presented in various graphical forms;
- questions of interpretation of graphs and tables (in the latter case the questions are said to deal with the critical numerical reasoning), which assess the ability to process and extrapolate numerical information from the data presented in these diagrams;
- questions requiring the application of calculation formulas: the most frequent examples of this category are those quizzes in which one is asked to predict an outcome through the expression of probability judgments or quizzes on space, speed and time, which do not require particular solving strategies but, in general, knowledge of the fundamental relations between these three quantities;
- mathematical problems focusing only on the calculation of values, where the question is posed in the form of a mathematical text and the solution requires the application of various formulas;
- logical-mathematical problems that can be solved using some elementary mathematical tool, i.e. with addition, multiplication, the use of first degree equations or systems of equations, as well as a minimum of logical reasoning to understand the problem;
- logical-mathematical problems centred on problem solving, in which mathematical calculation plays a secondary role to understanding the solving strategy.

A particular category of mathematical logic questions belongs to the area of numerical-deductive reasoning questions concerning complicated numerical series: these are generally administered by RIPAM.
Abstract reasoning questions are non-verbal measures of cognitive abilities that detect whether and to what extent a subject is able to perform simple or complex reasoning when faced with stimulus material, which may consist of geometric figures, drawings of different shapes, different spatial orientation, different constituent elements or other features that differentiate the various components.

Let us propose four examples of logic quizzes with their solutions: the last two have been proposed in admission tests to the Faculty of Medicine. We take them from the collection of logic tests edited by Davide Bondoni [132] at the beginning of 2020.

1. Of a group of people it is known that «all males are minors». It can be deduced that certainly, in the group:
A) all females are of age,
B) all underage persons are males,
C) all underage persons are females,
D) all females are minors,
E) all persons of legal age can only be females.

Solution. Some knowledge of first-order logic, which will be treated later in the thesis, may be useful here. But even proceeding at an informal level, one can observe how the initial statement "*every male is a minor*" (within the considered group) is also expressed, by switching to the negations, as "*every adult is female*" (thus assuming "*adult*" and "*female*" as negations of "*minor*" and "*male*" respectively). This leads to answer E).

2. If TAP means (single) digits divisible by 5, TUP means (single) digits divisible by 3 and TOP means (single) digits divisible by 2, then by which script can the number 92 be expressed?
A) TOP TAP,
B) TUP TOP,
C) TUP TAP,
D) TUP TUP,

E) TOP TUP.

Solution. The right answer is B), i.e. TUP TOP because 9 is divisible by 3 and not by 2 and 5, while 2 is divisible by 2 and not by 3 and 5. After that, it should be noted, regardless of the exercise, that on the basis of the assumptions made other numbers such as 34 and 32 would be TUP TOP.

3. (Medical test 2012) Mario is the second son of a couple with two children, and his wife is an only child. One of Mario's son's grandparents has a daughter named Francesca, who is two years younger than Mario. Given these premises, who is Francesca?
A) Mario's wife.
B) Mario's sister.
C) An aunt of Mario.
D) A daughter of Mario.
E) Mario's mother.

Solution. Mario is married to a woman who is an only child and is the second son of a couple with two children. One of the grandparents of Mario's son, i.e. one of the parents of Mario or his wife, has a daughter named Francesca. Then Francesca can either be Mario's wife or his sister; she cannot be his sister since she is younger than Mario and Mario is the second son. Therefore, she is his wife. Answer A) is therefore the right one.

4. (Medical test 2018) «Every time I get out of bed I feel dizzy». If the previous statement is FALSE, which of the following is certainly true?
A) At least once I got out of bed without feeling dizzy.
B) When I get out of bed, I never feel dizzy.
C) Every morning I feel dizzy.
D) At least once I have got out of bed and felt very dizzy.
E) When I do not get out of bed, I do not feel dizzy.

Solution. Again, the answer would benefit from knowledge of a minimum of propositional logic and first-order logic. Using intuition, however, one arrives at the negation "there is at least one time when I get out of bed and do not feel dizzy", which is answer A).

Apart from the admission quizzes, however, one can agree with what we have already repeated several times, namely that logic can be a prerequisite also for degree courses other than those that are declaredly scientific, such as mathematics and computer science. For example in economics. Let us cite in this regard the text [53], which involves logic in the above-mentioned field. In economics, politics and social life, logic serves both to formalise the context and to suggest a rigorous approach to the problem of making the most appropriate choices.
In this connection, let us recall Arrow's *impossibility theorem*, which deals with the problem of identifying the most equitable and representative system of government. The relevant theory was developed by Kenneth Arrow (US economist, winner of the Nobel Prize for Economics in 1972) and described in *Social Choices and Individual Values* [8]. It singles out and formulates, in precise mathematical language, a series of conditions that seem inescapable in any good democracy: «universality», «non-imposition», «non-dictatorship», «monotonicity» and «independence from irrelevant alternatives». We limit ourselves to this list of them, without going into too much detail. Let us simply add, for example, some words about the third assumption, «non-dictatorship», which excludes that in politics to decide is the title of only one person – an obvious and unavoidable premise.
Anyway Arrow's theorem excludes that such a system exists, and that all these reasonable assumptions can live together. As if to say that perfect democracy does not exist.
In this and other works, Arrow contributed significantly to the evolution of political economy during the 20th century in the direction of greater mathematical rigour; his is one of the first approaches to the social sciences through mathematical formalism. To understand Arrow's logical predisposition and his recourse to mathematical methods and approaches, one can retrieve an interview he gave on one of his annual trips to Italy to the newspaper *Repubblica*. It is entitled "*The Arrow Earthquake*". As well as explaining his passion for mathematics and statistics and their connection with economics, he recounts his youthful encounter with the great Polish logician Alfred Tarski, whose logic course he took in New York in the early 1940s, and the influence those studies had on his theorem.
"*Even today*", reads the interview, "*I don't see how you can discuss choices, social or individual, without using the concepts of the theory of relations*": this is what the economist said.

Chapter 2

Logic at School

2.1 What is logic?

In the previous chapter, we briefly described logic, its history and the reasons for proposing it to teachers and also to high school students. The time has then come to briefly recall the basic elements of logic. Ideally, we address here primarily teachers who are unfamiliar with it but also, why not?, students.

Some ideas for introducing logic and allowing an initial, soft and possibly playful encounter with students come from the works of Raymond Smullyan, starting with the famous *What is the name of this book?* [109] (in Italian *Qual è il titolo di questo libro?*) and continuing with the other books of the same tenor that followed it. Smullyan was a mathematician and philosopher of science of the last century, with a variety of other interests - writer, then pianist and magician. His approach to logic in the books mentioned above is amusing, but far from trivial and indeed, beyond appearance, profound. In [109], in particular, he imagines an ideal and surreal island whose inhabitants are divided into two categories:

- gentlemen who always tell the truth,
- villains who always tell lies.

There is no other way to tell them apart. A traveller arrives on this island and, meeting its inhabitants A, B, C,..., tries to tell whether they are gentlemen or villains.

Example 1. Suppose A says: *"I am a gentleman".* What can be inferred about

A? Is he a gentleman or a villain?

Let us discuss the two possible cases:

- A is a gentleman: then he would tell the truth and, in the present case, claim to be a gentleman.
- A is a villain: then he would always tell lies and, in this case, claim to be the opposite of what he is, thus again a gentleman.

The conclusion is that A claims to be a gentleman in any case, so this statement reveals nothing definite about his nature.

Example 2. Let us now admit that A states instead: *"I am a villain".* The question is the same: What is A?

Let us again discuss the two new possible cases:

- A is a gentleman: then he would tell the truth and therefore could not claim to be a villain.
- A is a villain: then he would always tell lies and could not admit to being what he is, i.e. a villain.

Thus the proposed situation is impossible: A does not exist or, if you prefer, the villain is the one who imagined the story. Note that the example reproduces exactly on the island of Smullyan the so-called *"paradox of the liar"*, or of Epimenides, one of the most famous labyrinths of ancient logic: *he who says «I am lying» is lying if and only if he is telling the truth.*

Example 3. Imagine now that you meet two inhabitants of the island, A and B, and A says: *"at least one of us is a villain".* What are A and B, gentlemen or villains?

It is worth reflecting for a moment on A's statement, that is basically saying: *"either A is a villain, or B is (but possibly both)".* Let us underline in particular the key role played in A's statement by the conjunction **"or"**. Its intervention makes it possible for A's sentence to be considered true when one of the two eventualities proposed, namely *"A is a villain", "B is a villain",* is correct. On the contrary, the sentence is false if neither of its two statements is true, i.e. if both A and B are gentlemen.

To illustrate the situation even better, we can rely on other examples, borrowed from the times of the coronavirus: a communication such as *"tomorrow masks will be distributed free of charge to women* ***or*** *the elderly"* applies to those who are women (also young), or elderly (also men), possibly to women who are also elderly, and excludes men who are also young.

But back to the island of Smullyan. This time the two possible cases for A are:

- A is a gentleman: then he tells the truth and therefore, in this case, since he is not a villain, he says that B is.
- A is a villain: then he would have to tell a lie while, by confessing that between A and B there is at least one villain, he ends up telling the truth.

This second eventuality is therefore impracticable. The first remains. Thus A is a gentleman and B is a villain.

Example 4. Finally suppose that A declares *"I am a villain and B is not".* What are A and B?

The example looks similar to the previous example, in which the sentence also opens with *"A is a villain"* but then continues with ***"or"***. This time, however, the sentence continues with the conjunction ***"and"***: A's sentence joins two statements and is therefore true if and only if both are true, false if and only if one of them is false. As if to say, going back to the masks: the notice that *"tomorrow morning they will be distributed to elderly women"* (i.e. women who are also elderly) applies only to the latter, and excludes those who are male (even if elderly), or young (even if female). But let us come to Smullyan. The two new possible cases for A are now as follows.

- A is a gentleman: but this is impossible, because in such a case the first half of his statement and, consequently, the statement as a whole are false.
- So A is a villain, and is lying. In other words, at least one half of his statement must be false; the first half can no longer be false, because this time A is a villain, and therefore the second half must be false. In other words, B is also a villain.

The conclusion is that A and B are villains.

Apart from the Smullyan Island scenario, the previous examples introduce some general considerations, which may justify subsequent developments.

- First of all, we are faced, albeit for fun, with the need to check the truth of certain statements.
- The four examples have shown us how a case-by-case analysis – by *brute force,* as we say in computer science today – can be useful in the absence of more brilliant strategies. Better get used to considering it. And (let us quote Robert Musil from his essay *The Mathematical Man*[1]) *"mathematics can be defined as a marvellous spiritual apparatus made for thinking in advance of all possible cases".*
- The statements we encountered in the third and fourth examples are structured by joining (... and...), disjoining (... or...), negating (not...) more elementary propositions P, Q, ... In particular, the statement *"A is a villain"* can be considered as the negation, of the other *"A is a gentleman"*.

However it is worth noting the difference, also with regard to the use of *"and", "or", "not",* between the mathematical and logical language, which tends to be rigorous, precise, at the limit fussy, and the common language, which is certainly more open to a variety of nuances. This distinction does not only concern words, but also the concepts they are intended to express.

Let us comment this point and start with *"not".* It is not always easy to establish and apply the criteria with which to deny a given statement. Even a lucid thinker, as Voltaire certainly was, can be surprisingly unaware of this, as the following episode testifies.

Blaise Pascal had observed in his work [87], that if a proposition seems incomprehensible to us, but its negation turns out to be false, then the proposition can be accepted without any problem – a statement in favour of demonstrations by contradiction.

[1] This can be found on pages 39-43 of [81].

But Voltaire, in the 25th and last of his *Philosophical Letters* [121], which is generally dedicated to a punctilious and often exaggerated criticism of Pascal's theses, also dwells on the previous observation and points out that sometimes opposites can be equally false, and cites in this regard the case of the two statements *"an ox flies south with wings", "an ox flies north without wings".* Yet today it is easy to see that the latter is not at all the negation of the former, which in detail says *"there is an ox that flies, and it does so heading south, and it does so with wings",* and thus is negated by claiming that any ox either does not fly, or if it does fly it does not do so heading south, or if it does fly south it does not do so with wings. This second statement is true, for the simple reason that no ox flies. Voltaire was probably unaware of the logical rules of negation – De Morgan's laws – which we shall soon see and which, although known since antiquity, were revived mainly in the nineteenth century.

Let us turn to the ambiguities of *"and"* and *"or"*. Their use in common language is more casual and less precise. Consider for example the following statements, apparently similar and both subject to the conjunction *"and"*:

- *«Charles* ***and*** *Camilla are English»,*
- *«Charles* ***and*** *Camilla are married».*

In the first sentence, however, it is asserted that Charles is an Englishman and Camilla also an Englishwoman, one independently of the other, because the relation *"to be English"* is 1-ary and, even in front of the registry office, one is English on her or his own. The second sentence can instead be interpreted (at least in the most common sense) as the statement that Charles and Camilla are husband and wife. The relation *"to be married"* is in fact binary and one marries in two – unless one interprets the previous assertion as *"Charles is married and Camilla is married",* each on his or her own. But such a situation existed even before they divorced their previous spouses and formed a family together.
Note that situations of this kind also occur in mathematics. Consider for example

- *«3 and 7 are prime»* (in the sense that 3 is a prime number and 7 is a prime number),

- *«3 and 7 are coprime»* (in the sense that their greatest common divisor is 1, a binary relation).

Sometimes *"and"* and *"or"* are confused with each other in usage. For example, one sometimes hears sentences such as *«I like reading detective books and science fiction books»,* with a somewhat natural use of *"and",* but from a logical point of view *"or"* would be more appropriate.
Similar situations can also be observed in algebra.

- One may hear, or even read in books, *«The solutions of the equation* $x^2-3x+2=0$ *are* $x=1$ *and* $x=2$*»* (although it would be more correct to use *"or"*).

- On the contrary, the sentence *«the inequality* $x^2-3x+2\neq 0$ *is valid for* $x\neq 1$ *and* $x\neq 2$*»* (which, by the way, is equivalent to the previous one, turning the two extremes to the negative) makes appropriate use of *"and"*.

There are also different nuances concerning the meaning of the conjunction *"or"*. They were well distinguished, for example, in Latin, but have sometimes been lost in modern languages.

- The Latin "vel" corresponds to sentences like (in Covid times) *«masks will be distributed to women or the elderly»* (in this case, to have the mask, it will be the women, or the elderly, possibly elderly women, but men and young people will be excluded).

- The Latin "aut" has a different meaning, as exemplified by *«either you eat the soup or you jump out of the window»* (of the two options, one excludes the other, but this time eating and jumping makes no sense, while neither eating nor jumping is clearly forbidden).

- Moreover there is the pure incompatibility, evidenced by certain labels on bottles of alcoholic beverages: *«either drink or drive»* (this time drinking and driving are not allowed, but abstaining from both, i.e. neither drinking nor driving, respects the indication).

After warning against these dangers of conjunction, disjunction and negation, let us hazard a strict definition of "logic", based also on our experience on Smullyan Island. In order to introduce it let us underline the following facts.

- First of all, the sentences we considered are formal statements about the inhabitants of the island and their nature, sometimes simple like *"A is a gentleman"*, sometimes more elaborate, when *"and", "or", "not"* intervene.
- There is a visitor aiming to understand the truth about the nature of the people he meets.
- He does so according to certain rules, namely the premise that villains always lie, but gentlemen never do.

Abstractly, we can assume a logic to be a tern as follows.

- First of all, there is an ***alphabet*** consisting of the symbols that one wants to use, and the ***formulas*** that are made up of them, as suitable words of that alphabet, i.e. finite ordered strings of its symbols.
- Then there are ***valuations,*** that decide the truth of these formulas.
- They do so on the basis of pre-established criteria, according to a relationship of ***truth*** between formulas and valuations.

It is then desirable that this relation of truth be accompanied by a notion of ***provability*** of formulas, whereby, for example, a formula is accepted as true by any valuation if and only if it is provable, i.e. there is an proof that supports it.

To provide in detail such a definition is by no means simple. But to illustrate it, let us provide a simple example, that is Boolean logic. We have already outlined its history in the first chapter. It is time to describe it carefully.

2.2 Boolean logic

As we have just seen, the sentences stated during the meetings on the Smullyan Island have proposed

- simpler statements, P, Q, R and so on (such as *"A is a gentleman"*)
- which are then possibly combined to construct more complicated ones thanks to the use of the so-called *connectives "not", "and", "or"*.

In detail:

- the negation *"not"*, which we indicate in the abstract with $\neg$, from every single statement F produces "*not* F", $\neg F$;
- the conjunction *"and"*, denoted by $\wedge$, starts from every ordered pair of statements F and G and produces "F *and* G", $F \wedge G$;
- the disjunction *"or"*, $\vee$, moves from any ordered pair of statements F and G and produces "F *or* G", $F \vee G$.

Of course $\wedge$ and $\vee$ can be applied to statements that are already complicated in themselves, in order to generate, for example, $P \wedge (Q \wedge R)$ or $P \vee (Q \vee R)$ – the conjunction or disjunction of 3 or more formulas, which we have already encountered in the case of Voltaire's oxen. In these cases the use of *parentheses* should be envisaged in order to establish some precedence.

It seems right to ask whether the connectives allowed up to now, i.e. $\neg$, $\wedge$, $\vee$ are sufficient, or whether it is necessary to add others. In fact there is one that is sometimes met in common language and often in mathematical language, when theses and hypotheses are used and expressions such as *"if F then G"* are formulated. An example: *"if it rains I'll take an umbrella"*.
Modern computer science also includes *"if... then..."* in the instructions of its programs.
Let us then admit a new connective, namely the implication *"if... then..."*, usually denoted $\rightarrow$, which is able to constitute from two statements F and G a new one "if F then G", $F \rightarrow G$.
But be careful to distinguish the various components of the proposition thus generated:

- F is the *premise*, or the *hypothesis*,
- G is the *conclusion* or *thesis*,

- $F \to G$ is the actual *implication*.

The position of F and G is important, in contrast to $F \wedge G$ and $F \vee G$. In the latter cases, it seems irrelevant which of F and G is first and which second, the meaning does not change.
On the other hand, it is not the same thing to say *"if it rains I take the umbrella"* and *"if I take the umbrella it rains"*: in the first case we speak of a natural action, in the second of an almost magical power.

Here is another example, suggested by arithmetic. Let's talk about Mersenne primes. Let us recall that, for every integer $n > 1$, the n-th Mersenne number has the form $2^n - 1$. So the succession of Mersenne numbers consists, at least initially, of:

- $2^2 - 1 = 3$, which is prime number (as well as the exponent 2 is a prime number),
- $2^3 - 1 = 7$, still a prime number (and also the exponent 3 is a prime number),
- $2^4 - 1 = 15$, a composite number (and now the exponent 4 is also composite),
- $2^5 - 1 = 31$, this time a prime number (and the exponent 5 is also prime),
- $2^6 - 1 = 63$, a composite number (corresponding to a composite exponent 6),
- $2^7 - 1 = 127$, a prime number (and the exponent 7 is prime),
- but $2^{11} - 1 = 2047 = 23 \cdot 89$ is composite even though the exponent 11 is prime.

In fact, let $n > 1$ be an integer.

- It is true that *«if $2^n - 1$ is a prime number, so is n»*. As if to say that *«if n is a composite number also $2^n - 1$ is composite»*. Suppose in fact $n = a \cdot b$ with a, b integers, $1 < a, b < n$. Then $2^n - 1 = 2^{a \cdot b} - 1 = (2^a)^b - 1^b = (2^a - 1) \cdot \ldots$, where $1 < 2^a - 1 < 2^n - 1$ because $1 < a < n$.
- On the other hand, it is false that *«if N is a prime number also $2^N - 1$ is a prime number»* (the statement that swaps hypothesis and thesis). This is witnessed, for example, by $N = 11$, which is a prime number unlike $2^{11} - 1$.

Therefore let us (at least momentarily) agree that the ***alphabet*** of Boolean logic consists of

- propositional variables P, Q, R, … (for elementary statements like *“t’s raining”*),
- the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$,
- the parentheses (,).

We then define the ***formulas*** of Boolean logic as follows:

- propositional variables are formulas;
- if F and G are formulas, so are (with the possible use of parentheses) $\neg F$, $F \wedge G$, $F \vee G$, $F \rightarrow G$;
- it is not possible to construct other formulas than those just listed.

However, it is permissible to form formulas such as $((P \wedge \neg Q) \vee R) \rightarrow \neg P$.

Let us now establish who and how establishes the truth of a formula.

It seems reasonable to admit that the opinion on variables P, Q, R, … is completely free. Whether it rains or not is established day by day and place by place, it may be that today it is sunny in Naples and it is raining in Camerino.
But when one moves on to more complicated statements like $\neg F$, $F \wedge G$, $F \vee G$ and $F \rightarrow G$, the opinion is manifestly bounded by the opinion one has previously formed about F and G. In fact, it seems evident that:

- if we believe F, we cannot simultaneously accept $\neg F$ (if it is raining, we cannot say that it is not raining);
- we cannot believe $F \wedge G$, i.e. admit both F and G, if we do not preliminarily and separately accept both F and G (masks reserved for old women are only distributed to women who are old);
- we cannot believe in $F \vee G$, i.e. admit at least one of P and Q, if we do not preliminarily accept either F or G (to receive masks reserved for women or old people, one must be a woman or an old person);

- the discussion of $F \to G$ requires more care and will be taken up later.

Consequently we define in abstract ***valuation*** a function v that assigns to each propositional variable P the value 1 or 0 (meaning *"true" or "false", "yes" or "no"* respectively).

Two formulas F and G are said to be *logically equivalent*, or, simply, *equivalent*, if for every valuation v, $v(F) = v(G)$.

Common sense rules then suggest how to extend v to all formulas. Assuming we already know, for F and G formulas, $v(F)$ and $v(G)$, we put

- $v(\neg F) = 1 - v(F) = \begin{cases} 1 & \text{if } v(F) = 0, \\ 0 & \text{if } v(F) = 1, \end{cases}$
- $v(F \wedge G) = v(F) \cdot v(G) = \begin{cases} 1 & \text{if } v(F) = v(G) = 1, \\ 0 & \text{if } v(F) = 0 \text{ or } v(G) = 0, \end{cases}$
- $v(F \vee G) = v(F) + v(G) - v(F) \cdot v(G) = \begin{cases} 1 & \text{if } v(F) = 1 \text{ or } v(G) = 1, \\ 0 & \text{if } v(F) = v(G) = 0, \end{cases}$
- $v(F \to G) = \begin{cases} 1 & \text{if } v(F) = 0 \text{ or } v(F) = v(G) = 1, \\ 0 & \text{if } v(F) = 1 \text{ and } v(G) = 0. \end{cases}$

It should be noted that, at least in the first three cases, the rules stated correspond to elementary operations on 0, 1 (subtraction from 1, product, sum minus product respectively). This was Boole's intuition. In this extended setting, it is understood that a formula F is **true** for a valuation v if $v(F) = 1$, and **false** otherwise.
These are thus the conventions of Boolean logic: not absolute laws or dogmas, but options justified by the arguments we have tried to propose (the "common sense") and which we will continue to propose in the most controversial case of the implication. Alternative options and related logics are certainly possible, though perhaps less convincing.
One way to fix and clarify the above rules in a very expressive form is to resort to tables (***"truth tables"***) organised as follows. One is prepared for each of the four connectives:

- in the column on the left, or in the columns on the left, we list line by line the possible truth values, 1 or 0, of the starting statements (only F in the case of negation, F and G for conjunction, disjunction and implication);
- in correspondence to each of the listed cases, the truth value of the new statement, the one constructed with the use of the connective, is indicated in the final column.

The connective $\neg$

F	$\neg F$
1	0
0	1

The connective $\wedge$

F	G	$F \wedge G$
1	1	1
1	0	0
0	1	0
0	0	0

The connective $\vee$

F	G	$F \vee G$
1	1	1
1	0	1
0	1	1
0	0	0

The connective $\rightarrow$

F	G	$F \rightarrow G$
1	1	1
1	0	0
0	1	1
0	0	1

Here are few comments on this last table, and thus on the truth values of an implication.

- It is quite reasonable to agree that, if F and G are taken to be true, then $F \to G$ can also be taken to be true (*line 1*). Indeed, the alternative would be to consider false an implication whose hypothesis and thesis are assumed to be true (an option that is certainly less convincing).
- Moreover, it is evident that, if F is considered true and G false, then also $F \to G$ must be false (*line 2*); in fact a correct implication, starting from a true premise, cannot lead to a false consequence.

Thus the two cases in which F is true (*the first two lines*) are settled. There remains, however, the problem of establishing which truth value to assign to $F \to G$ when F is false (*the last two lines*). The rule that Boolean logic establishes in this regard is the following:

an implication that moves from a false premise is true.

In other words, from a false hypothesis one can deduce anything one wants, and the corresponding implication is correct. It is advisable to repeat this and keep it in mind:
the only case in which the implication $F \to G$ receives the value 0 is the one in which F is 1 (it is true) and G is 0 (it is false).
In all other situations, in particular in the two lines where F has value 0, $F \to G$ receives value 1.
Note also that, for a valuation v such that $v(F) = 1$ and $v(G) = 0$, $v(F \to G) = 0$ and $v(G \to F) = 1$. Therefore $F \to G$ and $G \to F$ are not equivalent.
The convention adopted for false F is debatable and anything but intuitive, and may generate some understandable doubts. Not for nothing it has been discussed since ancient times. Callimachus, a librarian in Alexandria in the 5th century BC, is credited with an epigram *"Even the crows on the roofs caw about the nature of the conditional"*, which testifies to the passion with which the subject was treated in his times [20]. Even today, the rule is summarised by the Latin expression ***«ex falso quod libet»*** (from a false premise it is correct to deduce what one likes).

Let us try to offer some examples in support of this point of view.

Example 1. The implication *"if 2 + 2 is 5, then 2 + 3 is 6"* starts from a false premise, because 2 + 2 is not 5, and leads to an equally false consequence, because 2 + 3 is not 6. It is however correct, because if we accept that 2 + 2 is 5, then 2 + 3, which comes immediately after 2 + 2, can only be 6. On the other hand, the implication *"if 2 + 2 is 5, then 2 + 2 is greater than 3"* starts from the same false premise as before, but this time it produces a true consequence, because 2 + 2 is greater than 3; on the other hand it is in itself correct, because 5 is greater than 3.

Example 2. Let us tell an anecdote about Bertrand Russell, whom we already know as a logician, philosopher of mathematics and influential thinker of the 20th century, in whose civic life he actively participated, asserting very liberal views on morals and highly criticizing Catholic Church, Christianity and more generally all religions (he was a declared atheist). It is said that during a lecture in which he explained the rule *«ex falso quod libet»*, he received some objections. A listener, unconvinced and mindful of his religious views, tried to tickle him: *"But then, if 2 + 2 is 5, could you prove to me that you are the pope?"*
Russell replied imperturbably: *"Let us assume that 2 + 2 is 5. Subtracting 2 from both sides, we get that 2 equals 3. Subtracting 1 again, we deduce that 2 is equal to 1. Now the pope and I are 2. But if 2 is equal to 1, then we are 1: therefore I am the pope"*. An unquestionable demonstration of the implication that from the false premise of 2 + 2 leads to the equally unlikely identification of Russell with the pope.

Example 3. Henri Poincaré was not a fan of logic and logicians, to whom he reserved heated and often humorous criticism in his writings. Poincarè, however, subscribed to the rule «ex falso quod libet». In his eyes, it is supported by the experience that professors and students sometimes have during a mathematics task, when an initial error alters all the subsequent steps but can sometimes lead, perhaps because of other subsequent errors, to the correct solution. In such cases, the teacher is obliged to assign a negative mark, but it is not easy to respond to the boys' protests ("the result is right, so I did well"). Here, however, is Poincaré's comment, which can be read in his book *Science and Method: "Russell comes to the conclusion that any false proposition implies all other propositions, whether true or false. [...] It is enough to have corrected a bad mathematics paper to realise at once that Russell is perfectly right. The candidate often has to go to a great deal of trouble to deduce the first equation, which is false: but once he has deduced this, it becomes easy* *for him to accumulate the most amazing results, some of which may even be correct".*

Wason's test. This experiment was devised by Peter Wason [124], a cognitive psychologist, who in 1966 subjected 128 university students to it in order to examine their reasoning skills. We use it as a starting point for further exercises on the principle *«ex falso quod libet»*.
Let us suppose that we are given a pack of cards, showing a letter on one side and a number on the other, according to the following principle: **the back of a vowel is an even number**. The following four cards are presented:

D A 4 9

We are asked how many and which cards need to be turned over to confirm the hypothesis in bold.
(**Hint**: as we have repeatedly pointed out, only a card with a vowel and an odd number can disprove the conjecture "vowel → even". Thus, cards A and 9 should be checked, not others. The former might have an odd remainder, the latter a back with a vowel).

Let us now deal with the same problem when the initial conjecture is that, conversely, **the back of an even number is a vowel**, i.e. "even → vowel". Suppose we have in front of us

A K 2 7

The question is the same as before: how many and which cards need to be turned over to confirm the conjecture.

(**Hint**: as before, a card with an even number and a consonant may disprove the conjecture, so it is sufficient to turn over the cards K and 2).

It may be interesting to add some details about the outcome of Wason's original test:

«You are shown a set of four cards placed on a table, each of which has a number on one side and a colored patch on the other side. The visible faces of the cards show 3, 8, red and brown. Which card(s) must you turn over in order to test the truth of the proposition that if a card shows an even number on one face, then its opposite face is red? »

So the principle to be respected is this time “even → red” and to disprove it you need a card with an even letter and a brown colour. In this case the two cards with 8 and brown must be checked on the other side.
In Wason’s study, less than 10 % of the subjects found the correct solution.

2.3 More on truth tables

On the basis of the laws regarding connectives, a truth table can be calculated for every possible formula. The following examples explain how, but at the same time introduce and try to clarify other remarkable aspects of Boolean logic.

Let us first clarify the context. So, imagine a formula constructed from the variables P,Q,R, ..., for instance of the form

- $\neg P$
- or $\neg(P \wedge Q)$
- or $((P \wedge \neg Q) \ \vee R) \rightarrow \neg\ P$.

Or, more generally, imagine to have formulas F,G,H, ... (not just variables) and to build a new one such as

- $\neg F$
- or $\neg(F \wedge G)$
- or $((F \wedge \neg G) \ \vee H) \rightarrow \neg\ H$.

In both cases, one lists the possible values that a valuation assigns to the starting formulas, so to the variables P,Q,R, ... or more generally F,G,H, ... and then, by the truth table, one deduces the value of the resulting formula.

The first difficulty is to actually list all the possible cases. One would wish a procedure that providing them automatically. Here is a possible strategy.

- In the case of a single variable, or a single starting formula, there are only two possible cases 1, 0, which are listed in the column alternating 1 and 0.

- For two variables, or two starting formulas, the possible cases become $4 = 2^2$ (two values for the first formula and, independently, two values for the second), in full (1, 1), (1, 0), (0, 1), (0, 0), that can be listed mechanically by alternating 1 and 0 in blocks of two bits in the first column (1, 1, 0, 0) and of a unique bit in the second (1, 0, 1, 0).

- For three variables, or three starting formulas, the possible cases are $8 = 2^3$ and correspond to the ordered triads of 0 and 1. They are obtained by alternating 1 and 0 in the first column in blocks of four bits (1, 1, 1, 1, 0, 0, 0, 0), in the second in blocks of two (1, 1, 0, 0, 1, 1, 0, 0) and in the third in blocks of one (1, 0, 1, 0, 1, 0, 1, 0).

The procedure is easily extended to the case of several variables, or several starting formulas. The following examples also serve to illustrate it in specific cases. However, they are devoted more generally to show how the tables calculate the truth values of a given formula.

Examples. Let us begin by examining the possible variants of the conjunction "or". The one expressed by the connective $\vee$ corresponds to "vel" and we have already seen the table representing it.

The connective corresponding to the incompatibility condition in *«either drink or drive»* is called Sheffer's and denoted by $|$. For F, G formulas, $F|G$ stands for $\neg(F \wedge G)$. Its truth table is then as follows:

F	G	$F \wedge G$	$F\|G$
1	1	1	**0**
1	0	0	**1**
0	1	0	**1**
0	0	0	**1**

Instead *"aut"* produces from F and G the formula $(F \vee G) \wedge \neg(F \wedge G)$. The corresponding table is then

F	G	$F \vee G$	$F \wedge G$	$\neg(F \wedge G)$	$(F \vee G) \wedge \neg(F \wedge G)$
1	1	1	1	0	**0**
1	0	1	0	1	**1**
0	1	1	0	1	**1**
0	0	0	0	1	**0**

Another example (frequently used in mathematics): "if and only if". It often happens that mathematical statements include the expression "if and only if ", which may appear redundant. But we have already observed how, for F, G formulas, $F \to G$ and $G \to F$ have different meanings and are not equivalent. This is confirmed by a comparison of the respective columns in the truth tables, which we find below. Well: $F \leftrightarrow G$ (F "if and only if" G) means exactly the conjunction $(F \to G) \wedge (G \to F)$. The truth table of this formula is as follows.

F	G	$F \to G$	$G \to F$	$(F \to G) \wedge (G \to F)$
1	1	1	1	**1**
1	0	0	1	**0**
0	1	1	0	**0**
0	0	1	1	**1**

A further possible support to the truth table of $\to$. It can be intuitively agreed that

$$F \to G \text{ is equivalent to } \neg F \vee G.$$

The first formula can in fact be interpreted, at least intuitively, as "either $\neg F$ or (if therefore F holds), then G". Let us compare the truth tables of these two formulas. We obtain respectively

F	G	$F \to G$
1	1	**1**
1	0	**0**
0	1	**1**
0	0	**1**

F	G	$\neg F$	$\neg F \vee G$
1	1	0	**1**
1	0	0	**0**
0	1	1	**1**
0	0	1	**1**

In this way the logical equivalence, for every possible choice of F and G, of the formulas $\neg F \vee G$ and $F \to G$ is confirmed. Comparing their tables, we find that they share the same truth values for each possible valuation, i.e. the same column, and therefore they are equivalent, in the sense that they admit the same meaning.

De Morgan's laws of negation. Augustus De Morgan was a 19th century English logician, a contemporary of Boole, but the laws ascribed to him were in fact already centuries old. They govern the negation of a formula.

- First of all we have that every formula F is logically equivalent to its double negation $\neg\neg F$, in the sense that it has the same column in the truth table. So we can say that, at least in Boolean logic, double negation affirms (but note how common language is, again, more nuanced: for example, an answer like "I am not unavailable" is less condescending than "I am available").

F	$\neg F$	$\neg\neg F$
1	0	**1**
0	1	**0**

- Next, the negation of a conjunction is the disjunction of negations, and the negation of a disjunction is the conjunction of negations. In other words, for each choice of formulae F and G, $\neg(F \wedge G)$ is logically equivalent to $\neg F \vee \neg G$, and $\neg(F \vee G)$ to $\neg F \wedge \neg G$. Returning to the example of the masks, we can observe how, if we restrict their distribution to those who are female and elderly (a conjunction of conditions), then we prohibit it for those who are not female or elderly (the disjunction of negations). Or, if one limits distribution to those who are women or elderly (the disjunction of conjunctions), one denies it to those who are not women and not elderly, and therefore to young men (the conjunction of negations). Truth tables confirm also these De Morgan's laws. In both cases we observe the same column of values, both for $\neg(F \wedge G)$ and $\neg F \vee \neg G$ and for $\neg(F \vee G)$ and $\neg F \wedge \neg G$.

F	G	$F \wedge G$	$\neg(F \wedge G)$	$\neg F$	$\neg G$	$\neg F \vee \neg G$
1	1	1	**0**	0	0	**0**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
0	0	0	**1**	1	1	**1**

F	G	$F \vee G$	$\neg(F \vee G)$	$\neg F$	$\neg G$	$\neg F \wedge \neg G$
1	1	1	**0**	0	0	**0**
1	0	1	**0**	0	1	**0**
0	1	1	**0**	1	0	**0**
0	0	0	**1**	1	1	**1**

2.4 Connectives

The connectives in the alphabet of Boolean logic have been introduced quite freely, on the basis of a few examples. It is then fair to ask

- are they sufficient? Or do we need more?
- And, if the answer to the first of the above questions is yes, are all the connectives already adopted necessary?

To the second question we can answer no: we have already seen that, according to the truth tables, for each choice of formulas F,G,

- $F \to G$ is equivalent to $\neg F \vee G$ (i.e. it has the same meaning for each valuation),
- (De Morgan's laws) $F \vee G$ is equivalent to $\neg(\neg F \wedge \neg G)$ and $F \wedge G$ to $\neg(\neg F \vee \neg G)$.

So, if we wanted, $\neg$, $\wedge$ or $\neg$, $\vee$ would be enough, because the other connectives selected so far can be recovered from them. However, in order to clarify the second question, and more generally to settle the whole problem well, we must establish what is meant by a connective.
Intuitively, a connective (e.g. $\wedge$) is a construction which, starting from certain formulas (F,G in our case), defines a new formula ($F \wedge G$, precisely). On the other hand, what is important about the new formula is not so much its representation ($F \wedge G$ could also be written $F \star G$ or as one prefers), as the meaning that is given to it, and therefore when it is considered true, in relation of course to the truth values assigned to the formulas that define it.
Thus, in the specific case of $\wedge$, for each valuation v,

$$v(F \wedge G) = 1 \text{ if and only if } v(F) = v(G) = 1.$$

In this sense $\wedge$ is naturally identified with the function f of $\{0,1\}^2 in \{0,1\}$ such that

$$f((0,0)) = f((0,1)) = f((1,0)) = 0, \quad f((1,1)) = 1.$$

In the case of negation $\neg$, for each valuation v,

$$v(F) = 1 \text{ if and only if } v(\neg F) = 0.$$

In this sense $\neg$ is naturally identified with the function f of $\{0,1\}$ in $\{0,1\}$ such that

$$f(0) = 0 \ , \ f(1) = 1.$$

These considerations suggest the following:

Definition. Let n be a positive integer. An n-ary connective is a function of $\{0,1\}^n$ in $\{0,1\}$.

The following is an immediate consequence.

Remark. For each positive integer n, there exist 2^{2^n} n-ary connectives (in particular $16 = 2^{2^2}$ binary connectives and $4 = 2^{2^1}$ 1-ary connectives). In fact, there are as many functions from a set with 2^n elements, such as $\{0,1\}^n$, in a set with 2 elements, such as $\{0,1\}$.

So the possible connectives are much more than the 4 we agreed to use. However, it should be noted that, for example, Sheffer's connective $|$ (one of the 16 binary connectives) can still be introduced by relying on the 4 starting ones. In fact $F|G$ stands for $\neg(F \wedge G)$. Note that in this sense $|$ is naturally identified with the function f of $\{0,1\}^2 in \{0,1\}$ such that

$$f((0,0)) = f((0,1)) = f((1,0)) = 1, \quad f((1,1)) = 0.$$

This function is obtained by composition from those corresponding to the connectives $\neg$ and $\wedge$. Sheffer's connective $|$, although formally new, can nevertheless be obtained by combining the starting connectives, and is therefore not indispensable. More generally, let F be a formula of Boolean logic (as we mean it so far), and suppose that the propositional variables occurring in F are among $p_0, \dots, p_{n-1}$. Then F defines the following n -ary connective f_F^n: for each choice of $x_0, \dots, x_{n-1} \in \{0,1\}$,

$$f_F^n(x_0, \dots, x_{n-1}) = v(F)$$

where v is a valuation such that $v(p_i) = x_i$ for every $i < n$. Therefore f_F^n determines a connective which, basically, from n given formulas builds a new one, whose truth values are derived from those of $p_0, \dots, p_{n-1}$ according to the definition just given. The new formula is then obtained from the n given formulas in the same way as F is constructed from $p_0, \dots, p_{n-1}$. So this new connective is generated (like Sheffer's) from the connectives we initially fixed $\neg$, $\wedge$, $\vee$ and $\rightarrow$ or, if we want, from the first three, or even the first two. We claim that in this way we obtain all possible connectives, i.e. all 2^{2^n} n-ary connectives for every positive integer n. As if to say that the connectives $\neg$, $\wedge$, $\vee$ and $\rightarrow$ are more than enough. The proof is, at least in the initial idea, very simple: we count the distinct n-ary connectives generated by $\neg$, $\wedge$ and $\vee$ and, with the help of combinatorial calculus, we see that they are at least 2^{2^n}, thus exhausting all possible cases.

Theorem. *Let n be a positive integer and g an n-ary connective. Then there exists a formula F with propositional variables among $p_0, \ldots, p_{n-1}$ such $f_F^n = g$. Furthermore, F can be chosen as a disjunction of conjunctions of propositional variables or negations of propositional variables.*

Proof.
If g is the null function, it suffices to choose $F = p_0 \wedge \neg p_0$; in fact for each evaluation v, $v(F) = 0$, so that if $\bar{x} = (x_0, \ldots, x_{n-1}) \in \{0,1\}^n$,

$$f_F^n(\bar{x}) = 0 = g(\bar{x}).$$

So in this case $f_F^n = g$. There remain $2^{2^n} - 1$ non-zero n-ary connectives, so we have to determine $2^{2^n} - 1$ formulas F of the type promised in the statement of the theorem, such that the connectives f_F^n are all satisfiable (i.e. have some non-zero valuation) and pairwise non-equivalent (i.e. with distinct valuations).
Consider the set A of the formulas $p_0^{\varepsilon_0} \wedge \ldots \wedge p_{n-1}^{\varepsilon_{n-1}}$ where $\varepsilon_0, \ldots, \varepsilon_{n-1} \in \{+1, -1\}$ and $p_j^{+1} = p_j$, $p_j^{-1} = \neg p_j$ for every integer j with $0 \leq j \leq n-1$.
We have $|A| = 2^n$. Let D be the set of all possible disjunctions of a finite and non-empty set of formulas of A. It results that $|D| = |\wp(A) - \{\phi\}| = 2^{2^n} - 1$.
Let then $F \in D$ and let $H : p_0^{\varepsilon_0} \wedge \ldots \wedge p_{n-1}^{\varepsilon_{n-1}}$ be a formula of A occurring in the disjunction of F.
If v is a valuation such that $v\left(p_j^{\varepsilon_j}\right) = 1$ for every integer j with $0 \leq j \leq n-1$, then $v(H) = 1$, so $v(F) = 1$. Therefore F is satisfiable. It remains to prove that if F and G are two distinct formulas in D, then F and G are not equivalent, in the sense that they differ by at least one valuation. In fact, there exists a formula $H \in A$ that occurs in F and not in G (or vice versa). Let $H : p_0^{\varepsilon_0} \wedge \ldots \wedge p_{n-1}^{\varepsilon_{n-1}}$, as already seen if we set $v\left(p_j^{\varepsilon_j}\right) = 1$ for every integer j such that $0 \leq j \leq n-1$, then $v(F) = 1$.
But for every $(\eta_0, \ldots, \eta_{n-1}) \in \{+1, -1\}^n$ with $(\eta_0, \ldots, \eta_{n-1}) \neq (\varepsilon_0, \ldots, \varepsilon_{n-1})$ there exists a non-negative integer $j < n$ such that $v\left(p_j^{\eta_j}\right) = 0$, so that $v(p_0^{\eta_0} \wedge \ldots \wedge p_{n-1}^{\eta_{n-1}}) = 0$. It follows that $v(G) = 0$.
In particular, F and G are not logically equivalent. □

Some exercises (taken mainly from competition quizzes).

1. *"It is wrong to deny that it is false that the picture was not painted by Cimabue"* is tantamount to stating:
a) The picture was not painted by Cimabue.
b) The picture was painted by an unknown painter.
c) The painting was painted by Cimabue.
d) Cimabue was not a painter.

2. A secretary position requires women with previous work experience. Therefore, the following are excluded:
a) All and only men with previous work experience.
b) All and only men with no previous work experience.
c) Women only, but those with previous work experience.
d) Men or women with no previous work experience.

3. The negation of $a = b = 0$ is
a) $a = b$ and b is different from 0,
b) a is different from b and both are different from 0,
c) a is different from 0 or b is different from 0,
d) a is different from b and b is different from 0.

Answers

1. The correct answer is c). Let us not be disoriented by the many negations in the original sentence. Let us count them: there are four, one after the other. But a fourfold negation $\neg\neg\neg\neg$ affirms.

2. The correct answer is d). In fact, the negation of the condition *"to be a woman with previous work experience"*, which is a conjunction, becomes the disjunction of negations, *"not to be a woman or not to have previous work experience" therefore "to be a man or without previous work experience"*.

3. The correct answer is c). In fact a=b=0 is equivalent to the conjunction of $a = 0$ and $b = 0$. Its negation is equivalent to the disjunction of negations, thus

$a \neq 0$ or $b \neq 0$.

2.5 The problem of satisfiability

We say that a formula F is

- *valid* if for any valuation v we have $v(F) = 1$,
- *not valid* otherwise, if therefore for some valuation v we have $v(F) = 0$.

Furthermore we say that F is

- *satisfiable* if there exists a valuation v for which $v(F) = 1$,
- *unsatisfiable* otherwise, if therefore for any valuation v we have $v(F) = 0$.

Consequently, F is satisfiable if and only if there exists a valuation v for which $v(\neg F) = 0$, i.e. if and only if $\neg F$ is not valid. Turning to negations, F is unsatisfiable if and only if $\neg F$ is valid.

We would now like a (possibly efficient) algorithm to decide whether a given formula F is valid or not, or satisfiable or not. The previous remark enables us to focus on the second question.

SAT satisfiability problem. Determine a procedure that, for each formula F, decides whether F is satisfiable or not.

The acronym SAT is derived from the English word *satisfiability.*

We already know an algorithm as required: the truth tables. In fact, a formula F is satisfiable if and only if its column in its truth table (with respect to the propositional variables in it) contains at least one 1. For example, the formula $F = ((P \wedge \neg Q) \vee R) \to \neg P$ in the three propositional variables P, Q and R has the following truth table, and consequently is satisfiable, because it is accepted by the valuations corresponding to the second row and the last four rows.

P	Q	R	$\neg Q$	$P \wedge \neg Q$	$(P \wedge \neg Q) \vee R$	$\neg P$	$\neg F \vee G$
1	1	1	0	0	1	0	**0**
1	1	0	0	0	0	0	**1**
1	0	1	1	1	1	0	**0**
1	0	0	1	1	1	0	**0**
0	1	1	0	0	1	1	**1**
0	1	0	0	0	0	1	**1**
0	0	1	1	0	1	1	**1**
0	0	0	1	0	0	1	**1**

However, we easily realise the practical difficulty of implementing the method. Already 3 variables require $8 = 2^3$ rows (as many as the possible ordered triads of $0, 1$, that is, as many as the possible ordered triads of values that a valuation assigns to P, Q, R). In general, for the same reason, n propositional variables require 2^n rows: too many, because the number of these rows grows exponentially with respect to the number of variables. For example, with $n = 64$ propositional variables, the number of rows required is 2^{64}, which is a number larger than ten billion billion.
The truth table algorithm therefore takes too much space, and also too much time. Even assuming that each row of a table is explored in 1 second, we can assume 2^n seconds to complete the column of truth values of a formula at least in the worst cases. For example, with $n = 64$ it would take more than ten billion billion seconds or about six hundred billion years.
It is true that if the formula to be checked is satisfiable and the 1 that confirms it occurs in the first line, there is no need to develop the subsequent lines. But this 1 could also intervene at the end of the procedure, in the last line. Moreover, when the formula is not satisfiable, then one has to fill in all the 2^n rows of its column to check in each of them the value 0.

One can then ask whether there is a "fast" way to solve the problem.
In modern computational complexity theory – a branch that connects mathematics and theoretical computer science – the acronym P is used to denote the class of problems (which can be formalised with natural numbers) that are fast to solve. Here P stands for *polynomial.*
In fact it is assumed that a procedure works in fast time if and only if it performs computations of length that is bounded with respect to the length of the input by

a polynomial function $n \to n^k$ (for some positive integer k as exponent).
Recall that the exponential function $n \to 2^n$ asymptotically outperforms any polynomial function $n \to n^k$ because

$$\lim_{n \to +\infty} \frac{2^n}{n^k} = +\infty,$$

in other words the exponential function grows to $+\infty$ faster as n increases. At this point our question can be reformulated by saying: does SAT belong to P?
Certainly not for the truth table algorithm, as we have observed. But in fact no algorithms are presently known that deal with SAT in at most polynomial time. We note, however, that if a formula F is satisfiable (i.e., if there is at least one row with 1 in the column of F, i.e., if there is an valuation that assigns F the value 1), then it suffices that that row or that valuation is suggested (a piece of information that is quick to provide) to check it and find (quickly) the desired value 1.
Problems that are in the same condition constitute the so-called class NP. We do not pause to explain the reason behind the letter N (for non-deterministic. But let us underline that NP-problems are those for which a positive answer can be verified quickly on the basis of a suggestion quick to be obtained. We might say, in crude terms, that NP-problems are those that are quick to solve with a little help. On the basis of this intuitive characterisation and the comparison with that of P one easily deduce $P \subseteq NP$. Whether the two classes coincide or not, is one of the deepest and most complicated questions in theoretical computer science and modern mathematics, included in 2000 among the 7 so-called millennium problems (the main open questions in mathematics today). It is in fact related to network security protocols.
Obviously, if $P = NP$, then SAT belongs to P. On the other hand in NP there are many other problems, combinatorial, algebraic and so on. But a theorem of Cook in 1970 states that if there is a fast algorithm for SAT, then $P = NP$. All problems in NP reduce in fast time to SAT, so that a fast algorithm for SAT generates a fast algorithm for each of them (combined with the reduction algorithm). Thus SAT, apparently just an elementary topic of Bolean logic, is the cornerstone of the whole $P = NP$ problem and shares its relevance and its difficulty.

2.6 Natural deduction

Let F be a formula, $\mathcal{G}$ a set of formulas (which we assume for simplicity to be finite). In Boolean logic we say that F is a *logical consequence* of $\mathcal{G}$ and we write $\mathcal{G} \models F$ if

every valuation that satisfies all the formulas of $\mathcal{G}$ also satisfies F.
Establishing this requires at least in principle a systematic check of all evaluations and a comparison between the values they assign to the formulas of $\mathcal{G}$ and to F. This can be done (at least for finite $\mathcal{G}$) with truth tables. For example, we saw earlier in this way that $F \to G$ e $\neg F \vee G$ are the logical consequences of each other for every choice of formulas F and G.
But generally in mathematics, and also in common life, one follows a completely different approach to persuade oneself that F follows from $\mathcal{G}$: one "proves" F from $\mathcal{G}$, i.e. one starts from the formulas of $\mathcal{G}$ as *"hypotheses"* and tries to develop a reasoning that leads to F as *"thesis"*.
This reasoning consists of a finite sequence of formulas (i.e. statements) $F_0, F_1, \ldots, F_m$ ending with $F_m = F$ and in which, for each $i \leq m, F_i$

- is in $\mathcal{G}$ (i.e. it is a hypothesis),
- or it is an *"axiom"* (it is so self-evident that no doubt arises),
- or it is obtained from previous formulas $F_0, \ldots, F_{i-1}$ by some convincing *"rule of deduction"*.

The following question then arises: is it possible to work out in propositional logic "axioms" and "rules of deduction" in such a way that

- for each $\mathcal{G}$, do the formulas which are proved by $\mathcal{G}$ with their help in the way just described **coincide** with those which are a logical consequence of $\mathcal{G}$?
- in particular, for $\mathcal{G} = \emptyset$, do the formulas which are proved in the way described without hypotheses **coincide** with those which are true for each valuation, i.e. valid?

The answer is positive. There are various systems of axioms and rules of deduction that validate it.

The simplest and most accessible is called ***natural deduction***: it consists of

- no axioms,
- 11 rules of deduction.

It is able to demonstrate all and only "logical" truth, in the sense that, for any $\mathcal{G}$, the formulas obtained by natural deduction from $\mathcal{G}$ are exactly the logical consequences of $\mathcal{G}$. This is the content of a fundamental result of logic, which has the name of *Theorem of Completeness* (in this case, of natural deduction in Boolean logic). Let us add that these ideas can be attributed to the German mathematicians David Hilbert (for the concept of proof) and Gerhard Gentzen (for natural deduction).

Let us move on to present natural deduction in more detail, with its 11 deduction rules of deduction. The attribute of naturalness refers precisely to the absence of axioms (which could be regarded as dogmas or forcings).

The first three deduction rules propose obvious prescriptions, also suggested by common sense.

Rule 1. It is allowed (and indeed recommended) to use hypotheses (i.e. the formulas of $\mathcal{G}$) in a deduction.

Comment. The rule seems evident.

Rule 2. It is allowed to discuss various possible alternative cases separately, using in each of them the general conclusions obtained previously.

Comment. We have applied this suggestion implicitly since the first examples on Smullyan Island. It is clear that the results obtained in a single case cannot be generalised (e.g., the conclusions obtained when interlocutor A is assumed to be a gentleman cannot be applied when interlocutor A is assumed to be a villan). But the analysis of a particular case nevertheless helps to clarify the general picture.

Rule 3. It is right to make use of the reasonings already carried out.

Comment. In other words, if we have already deduced from certain premises that *"A is a gentleman"*, we can use this result for further developments every time we start from those same premises, without repeating how and why.

Eight rules remain. There is a very simple way to remember them. In fact, they correspond to the four connectives $\neg$, $\wedge$, $\vee$ and $\rightarrow$, two for each connective: specifically, one explains how to introduce it, one how to eliminate it. Case by case it is easy to understand in which sense the connective is introduced or eliminated. In the statement of the various rules we indicate in the abstract with F, G, H, ... single formulas.

Rule 4 (Elimination of $\wedge$). From $F \wedge G$ we can deduce F (as well as G).

Comment. If we assume F and G at the same time, then we believe each of them in particular.

Rule 5 (Introduction of $\wedge$). From F and G (together) we can deduce $F \wedge G$.

Comment. Again, the principle seems obvious, and any comment is superfluous.

Rule 6 (Elimination of $\vee$). From $F \vee G$ and $\neg F$ we can deduce G.

Comment. If we know that we have open at least one of two possible ways out, F or G, but we see that the first is unfeasible, then we can rely on the second.

Rule 7 (Introduction of $\vee$). From F (as well as from G) we can deduce $F \vee G$.

Comment. This is a principle we have already encountered: if F is valid, we can deduce a fortiori the validity of the alternative between F and any other option.

Rule 8 (Elimination of $\neg$). If by exploring the particular case $\neg F$ we arrive at a contradiction, then we can deduce in general F.

Comment. We refer to rule 2. If the case of $\neg F$ turns out to be unacceptable, then we can assume F. At the beginning of this chapter, in the examples on Smullyan Island, we have already experienced a similar reasoning: if a case turns out to be inconsistent, we can accept its opposite (Voltaire permitting).

Rule 9 (Introduction of $\neg$). If by exploring the particular case F we arrive at a contradiction, then we can deduce in general $\neg F$.

Comment. Same situation as in the previous rule, only the role of $\neg$ changes.

Rule 10 (Elimination of $\rightarrow$). From F and from $F \rightarrow G$ we can deduce G.

Comment. This is a famous rule, known since antiquity as *modus ponens.* In more modern times it has been called cut *elimination.* We will deal with it shortly later.

Rule 11 (Introduction of $\rightarrow$). If by examining the particular case F we can deduce G, then we can state in general $F \rightarrow G$.

Comment. This is a simple and easy principle, still based on rule 2.

Let us consider now, as promised, the rule of natural deduction that is perhaps the most famous and delicate: ***modus ponens.*** Let us recall that it states that, for F,G formulas,

from F and $F \rightarrow G$ one can deduce G.

Example 1. We should be very careful in applying it appropriately without confusing the roles of the premise F and the conclusion G in the implication $F \rightarrow G$. The rule does not say that

from G and from $F \rightarrow G$ one can deduce F.

Otherwise, from the premises

- I take the umbrella (G),
- if it rains I'll take my umbrella ($F \rightarrow G$)

we would come to the conclusion

- it rains (F).

Instead, it is correct to deduce G (I take the umbrella) from F (it rains) and $F \rightarrow G$.

Example 2. It is correct, on the basis of modus ponens, from

- I don't take the umbrella ($\neg G$),
- if it rains I'll take my umbrella ($F \rightarrow G$)

deducing

- it doesn't rain ($\neg F$).

That is, the following principle (which is called ***modus tollens***) applies:

from $F \to G$ *and from* $\neg G$ *one can to deduce* $\neg F$

(but not vice versa).

To recapitulate:

- *(modus ponens)* from F and from $F \to G$ it is right to deduce G,
- *(modus tollens)* from $F \to G$ and from $\neg G$ it is right to deduce $\neg F$,
- there are no rules that apply to $F \to G$ and G to deduce F, and to $F \to G$ and $\neg F$ to deduce $\neg G$.

Example 3. The following case can be found somewhere on the internet. The premises are:

- forks have 4 teeth,
- my grandfather has 4 teeth.

We wonder whether it is correct to deduce that

- my grandfather is a fork.

Evidently not. For $F =$ *being a fork* and $G =$ *having four teeth*, from $F \to G$ and from G it is not possible to deduce F.

Three more exercises: the logical adventures of Sherlock Holmes

1. Sherlock Holmes and Dr Watson are trapped: their deadly enemy, Professor Moriarty, has lured them in a locked room, closed on all sides. The professor's voice reaches them from outside: *"There are two pitfalls in this room: the first opens the floor and makes you fall into a pool of sharks, the second releases a poisonous gas from the ceiling. But I want to leave you the pleasure of choice. The first thing Holmes tells me, if it's a lie, I'll throw you to the sharks and if it's the truth, I'll*

poison you with gas".
How do Holmes and Watson save themselves?

(**Hint**: think back to the paradox of the liar, the answer that guarantees salvation is *"now we will be thrown to the sharks"*).

2. Holmes and Dr Watson are at Baskerville Castle. In the ancient hall of arms the suspects in the murder of the old owner of the castle are gathered: his wife, the butler, the maid and the mathematics professor. Holmes knows that:

- the guilty always lies,
- the innocent never lies,
- there was an accomplice to the crime, and the latter can tell the truth or lie, depending on the moment.

The butler reveals: *"I am colour blind".*
The lady comments: *"Too bad! Red is a colour of the rainbow".*
The butler protests: *"And in any case, I am not the accomplice".*
The maths teacher also proclaims: *"I am innocent".*
The maid admits: *"Yes, I am the guilty one".*
Who is the guilty party? Who is his or her accomplice? Is the butler really colour blind?
(**A few hints:** as the second example on Smullyan Island has already illustrated, a guilty person who always lies and an innocent person who always tells the truth cannot claim to be the guilty one. It follows that the maid is neither guilty nor innocent, so she is the accomplice and, when she accuses herself, she lies. Then the butler is telling the truth when he excludes being the accomplice, so he is innocent (and colour-blind). Similarly, the lady is innocent because her statement about the rainbow is correct. Conclusion: the murderer is, of course, the mathematics professor).

3. Sherlock Holmes has to unmask the murderer of the lord of Baskerville. The suspects are: the butler, the lady of the castle, the mathematics professor and the doctor. Holmes knows that one and only one of them is lying. The four declare the following.

The butler: *"It wasn't me!"*
The lady: *"It was the doctor."*
The professor: *"It was the lady."*
The doctor: *"The professor is lying."*

Who is the liar? And who is the murderer?

(Hint: you can try first to discuss which of the four is lying.

- Not the butler, because otherwise the doctor does too (claiming that the professor lies too), and only one is a liar.
- Not the lady, for the same reason.
- Not the doctor, otherwise the lady and the professor are telling the truth and contradicting themselves.

The remaining possibility is that the professor is the liar, in which case the doctor is telling the truth when he denounces him, the lady is not guilty, and the butler is also reliable when he claims not to be the murderer. Finally, the lady is also telling the truth, so the doctor is guilty.
A different approach could identify the murderer first and then the liar).

Chapter 3

First-order logic

3.1 Introduction

Boolean logic has obvious limitations in fineness and expressiveness, as the following examples show.

Example 1. Let us consider the world of Genoese football, which we recall as divided between two opposing fans, supporting respectively the teams of Genoa and Sampdoria (listed in alphabetical order). Statements such as *"every Genoese is Genoan", "some Genoese are Genoan" or "the chief of the Genoa police is Sampdorian"* clearly have different meanings. And yet Boolean logic formalizes them in the same way, by resorting to a propositional variable P - unless in the first case a very long conjunction is risked, extended to all the single statements *"A is Genoan"* as A varies among the citizens of Genoa, each represented by an appropriate propositional variable. Ditto in the second case, which requires a similar disjunction.

Example 2. Let us turn to arithmetic and the statement *"every prime number is greater than 1".* The context is different, but Boolean logic formalizes this statement again with a propositional variable P. This time, however, the alternative of a conjunction asserting for each specific prime number that it is greater than 1 makes little sense, because prime numbers are infinitely many. Note then that the statement *"2 is prime"*, which is simpler than the previous one, is also formalized in the same way, by means of a single propositional variable.

A more powerful logic is therefore to be sought, one that is able to distinguish in some way:

- the different complexity of the two statements in example 2,
- the different context of the two examples.

The first requirement is satisfied by allowing the use of *quantifiers*:

- $\forall\, x$ for *"for every x"*,
- $\exists\, x$ for *"there exists x"*.

which operate on variables x of elements (the Genoese, or the natural numbers).

To satisfy the second requirement, appropriate symbols may be allowed on a case-by-case basis:

- symbols of 1-ary relations G, S respectively for *being Genoan, being Sampdorian* in example 1,
- the usual symbols $+, -, \cdot, =, \geq$ of arithmetic in example 2.

The idea is to allow formulas such as $G(x)$ to mean that x is Genoan, or

$$x \geq 2 \wedge \forall u \forall w (x = u \cdot w \rightarrow x = u \vee x = w)$$

to define prime numbers. The logic derived from this is called *first-order logic* (there are other, higher-order logic, which we will not go into here). In order to introduce it correctly, we proceed according to the scheme already followed for Boolean logic, defining in order the ***alphabet*** and the ***formulas***, then the ***valuations*** and finally the ***truth*** relation.

3.2 Alphabet, Formulas, Structures, Truth

Let us begin by introducing the alphabet of first-order logic. In addition to the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$ and the parentheses $($, $)$ it consists of:

- individual variables x, y, z, $\ldots$
- quantifiers $\forall, \exists$

and an infinite number of

- symbols for operations of any number of places f,g, ...
- symbols for relations of any number of places R,S, ...
- symbols for privileged elements (constants) c,d, ...

Among the symbols of this second set we choose those that make up the ***language*** we intend to use: $\left\{ G,S \right\}$ for Genoese, $\left\{+,\cdot,=,\geq,0,1\right\}$ for natural numbers. So a language is a set of operation, relation and constant symbols.

Let us turn to the formulas of first-order logic. In order to obtain those of a given language L we first construct the ***terms*** of L:

- the individual variables x,y,z, ...,
- the constants c,d, ... in L,
- for $t_1,\ldots,t_n$ terms of L and f an operation symbol with n places in L, $f(t_1,\ldots,t_n)$,
- nothing else.

In the case of Genoese, the terms are reduced to individual variables. In the case of numbers they also include $0,1$ and then $x+y$, $x+1$, $x\cdot y$, $y\cdot(x+1)$, $1+1$, ... (by the way: we abbreviate for simplicity $1+1$ with $2,(1+1)+1$ with 3, etc.).

The ***formulas*** of L consist of the following:

(i) the so-called ***atomic formulas***, of the form $R(t_1,\ldots,t_n)$ for R a relation symbol with n places of L and $t_1,\ldots,t_n$ terms of L,

(ii) negations, conjunctions, disjunctions and implications of formulas of L,

(iii) for F formula of L and x individual variable, $\forall\ x\ F$ and $\exists\ x\ F$,

(iv) nothing else.

In the case of the Genoese,

(i) $G(x)$ or $S(x)$,

(ii) $(G(x) \to \neg\, S(x))$, ...

(iii) $\forall\, x\ (G(x) \vee S(x))$, $\exists\, x\ G(x)$, ...

In the case of the numbers,

(i) $x+2=y$, $x-1 \geq z$, ...

(ii) $x+2=y \wedge x+1 \geq z$, ...

(iii) $\forall\, x\ \exists\, y\ \exists\, z\ \ (x+2=y \wedge x+1 \geq z)$, ...

Next let us introduce the valuations of first-order logic. For each language L they are mainly constituted by the ***structures*** in which we first fix the context - a non-empty set U:

- the set of Genoese,
- the set of natural numbers

and then in this context an interpretation is given for all the symbols of L

- an n-ary operation on U for each n-ary operation symbol placed in L,
- an n-ary relation on U for each n-ary relation symbol in L,
- an element of U for every constant in U.

It is then understood that the variables of individuals concern ***elements*** of U.

For example

- between the Genoese G,S are interpreted respectively in the sets of Genoans and Sampdorians,
- among numbers the various symbols $+, \cdot, =, \geq, 0, 1$ are interpreted in the obvious way.

However, there can be quite different structures for the same language, for example, in the case of Genoese,
(a) $U =$ set of natural numbers, with G, S interpreted as the sets of odd and even numbers,
(b) $U =$ again the set of natural numbers, with G, S interpreted this time as the sets of even and prime numbers respectively.

Finally, the concept of ***truth***: in the context of first-order logic, it is rigorously defined by following intuition somehow. It was formulated (together with the previous steps) by the Polish logician Alfred Tarski in 1933 in [112] (firstly published in Polish and then translated in German and English).

For example, in the language of the Genoese the formula $\exists\ x\ (\neg G(x) \wedge \neg S(x))$ is

- true among the Genoese, among whom presumably there are fans of teams other than Genoa and Sampdoria, or people who are wisely uninterested in football,
- false in (a), because among the natural numbers there is none that is neither even nor odd,
- again true in (b), because among the natural numbers there are some that are neither even nor prime, e.g. 15.

Instead $\forall\ x\ (G(x) \to \neg S(x))$ is

- true among the Genoese, among whom presumably no Genoan is also a Sampdorian,
- true in (a), where no even is odd,
- false in (b), because 2 is even and prime.

Remark 1. The two quantifiers $\forall$ and $\exists$ play different and almost antithetical roles:

- one thing is to state $\forall\ x\ G(x)$, which within the first structure means *"in Genoa everybody is a Genoan"*,

- another thing is to state $\exists\ x\ G(x)$, which within the first structure means *"in Genoa there are some Genoans"*

Remark 2. Here is a little story that illustrates the dangers of confusing the two quantifiers $\forall$ and $\exists$. An engineer, a mathematician and a logician are in the compartment of a train travelling through the Scottish countryside to Edinburgh. From the window the travellers observe a grazing cow with a black and white coat.

- In Scotland cows are black and white, - says the engineer.
- No, - objects the mathematician, - we can only say that in Scotland there is a cow with a black and white coat.
- No, - the logician corrects them both, - in Scotland there is a cow whose coat is black and white on at least one side.

Beyond the nitpicking, the three statements are clearly different, and only the last one is really correct. In fact, the engineer states that *"every Scottish cow has either a black or a white coat"*, thus involving the quantifier $\forall$ - but he does so incorrectly, because the example of the one cow observed from the train does not entitle him to generalise. So the mathematician is much more precise when he replaces $\forall$ with $\exists$ to claim that *"there is a Scottish cow that has a black or white coat"*. The logician then refines the argument by noting that the cow only showed one side, and could have a different coat on the other side.

Remark 3. We must also pay much attention to the order in which the quantifiers $\forall$ and $\exists$ follow each other in a discourse. Often, permuting them may alter the meaning of a sentence. Let us consider, for example, the case of fathers and sons. Let us then choose a language with a binary relation symbol $P(y, x)$ that is interpreted in the model constituted by the universe of human beings in the paternity relation: *"to be father of"*. So $P(y, x)$ stands for *"y is father of x"*. Let us then compare the two statements that follow and that are obtained from each other by exchanging the quantifiers of the premise.

- $\forall\ x\ \exists\ y\ P(y, x)$ tells us that every human being has a father (and it fits),
- $\exists\ y\ \forall\ x\ P(y, x)$, on the other hand, that there is a common father for all: a disturbing statement, unless one refers to a heavenly Father with a capital F.

Remark 4. Precise rules clarify how quantifiers behave when they are subject to a negation.

- The opposite of *"they are all Genoans"* is that *"there is someone who is not"*,
- the opposite of *"there are some Sampdorians"* is that *"no one is"* (like saying that *"they are all non-Genoans"*).

In general, for each formula F,

- the negation of $\forall\ x\ F$ is $\exists\ x\ \neg\ F$,
- the negation of $\exists\ x\ F$ is $\forall\ x\ \neg\ F$.

(**Hint**: compare with De Morgan's laws for conjunction and disjunction).

The above examples underline how even for quantifiers mathematical logic turns out to be much more schematic than common language: it adopts in fact a single symbol $\forall$ *"for every"* to translate what is usually expressed by resorting to a great variety of nuances, everybody, anyone, everyone etc., and in the same way a single symbol $\exists$ *"exists" for somebody, at least one ...*

Many proverbs deriving from popular wisdom, besides reiterating the latter observation, provide excellent examples of the use of quantifiers, in particular of $\forall$ in first-order logic. We list some of them, which we then discuss individually.

(a) *"A barking dog doesn't bite"*.

(b) *"He who never tries never succeeds"*.

(c) *"You snooze, you lose"*.

(d) *"He who does not drink in company is a thief or a spy"*.

(e) *"He who is the cause of his own evil, let him weep for himself"*.

Discussion

(a) To put it in a more involuted way, better corresponding to the setting of logic: *"For every dog, if it barks, then it does not bite"*. For an even more formal translation within first-order logic, we rely on a language with two 1-ary relation symbols Ba and Bi for *"barking"* and *"biting"* respectively. The proverb is then expressed in the form of the utterance $\forall\ x\ (Ba(x) \to \neg Bi(x))$. The negation is: *"there is a dog that barks and bites"*, $\exists\ x\ (Ba(x) \wedge Bi(x))$.

(b) This time it is asserted: *"for each person, if he does not try then he does not succeed"*. The structure is analogous to before. We still need two symbols of 1-ary relations T, S for *"to try"*, *"to succeed"* respectively. The proverb is expressed by the statement $\forall\ x\ (\neg T(x) \to \neg S(x))$. The negation is: *"there is one who does not try and succeed"*, $\exists\ x\ (\neg T(x) \wedge S(x))$.

(c) In this case the proverb can be stated (in a form analogous to the two previous cases) as *"for each person, if he sleeps then he catches no fish"*. Thus, using the 1-ary relation symbols S, CF for *"sleeping"* and *"catching fish"* respectively, the statement is expressed by the statement $\forall\ x\ (S(x) \to \neg CF(x))$. The negation is: *"there is one who sleeps and catches fish"*, $\exists\ x\ (S(x) \wedge CF(x))$.

(d) This proverb is more articulated: *"for each person, if he does not drink in company (a negation), then he is either a thief or a spy (a disjunction)"*. By using 1-air relation symbols D, T, S for *"drinking in company"*, *"being a thief"*, *"being a spy"* respectively we get $\forall\ x\ (\neg D(x) \to (T(x) \vee S(x))$. The negation is *"there is someone who does not drink in company and is neither a thief nor a spy"*, $\exists\ x\ (\neg D(x) \wedge \neg T(x) \wedge \neg S(x))$.

(e) We return to the structure of the first examples: *"for each person, if that person is the cause of his illness, let him weep for himself"*. So using the 1-ary relation symbols C,W for *"to be the cause of one's own illness"* and *"to weep for oneself"* respectively, the statement is expressed by the statement $\forall\ x\ (C(x) \to W(x))$. The negation is: *"there is one who is the cause of his own illness and does not mourn himself"*, $\exists\ x\ (C(x) \wedge \neg W(x))$.

Let us consider the example just concluded. In the formula $C(x) \wedge \neg W(x)$ the variable x does not appear under the scope of a quantifier, $\forall\ x$ or $\exists\ x$, which concerns it: it is then said to be **free**, or rather to have a free occurrence.
Its condition obviously changes if we consider $\exists\ x\ (C(x) \wedge \neg W(x))$. In this case we say that x is **bounded**.
A **sentence** is a formula that has no free occurrences of variables: this is the case, for example, of $\exists\ x\ (C(x) \wedge \neg W(x))$. It is then convenient to write a formula F in the form $F(x_0, x_1, \ldots, x_n)$ when one wants to underline that the variables that

appear in it free at least once are among $x_0, x_1, \ldots, x_n$.

Some exercises

1. Let us consider yet another proverb: «*Beer drinkers live one hundred years*» (to be understood: «*live **at least** one hundred years*»).
In order to prove that it is **wrong**, and therefore to deny it, we need to find someone who:
(a) did not drink beer but died before turning 100,
(b) drank beer but died before reaching 100 years of age,
(c) did not drink beer and is already 100 years old,
(d) drank beer and is already 100 years old.

2. Assume it is true that «*he who catches the flu has a fever*». It can then be deduced that:
(a) if Peter does not have the flu then he does not have a fever,
(b) if Peter does not have a fever, then he does not have the flu,
(c) everyone who has a fever has the flu,
(d) none of those who have a fever have the flu.

(In both cases, the correct answer is (b)).

3. «*Every time I get out of bed I feel dizzy*»: Assume this statement to be false. Which of the following is then certainly true?
(a) At least once I got out of bed without feeling dizzy.
(b) When I get out of bed, I never feel dizzy.
(c) Every morning I feel dizzy.
(d) When I do not get out of bed, I do not feel dizzy.
(e) At least once I got out of bed and felt dizzy.

(This time the correct answer is (a)).

3.3 Completeness Theorem and Natural Deduction

Also in first-order logic we introduce two operators that connect sets $\mathcal{G}$ of sentences of a language L and single sentences F of L

one $\models$ of ***logical consequence***,

one $\vdash$ of ***provability***.

The former is defined by placing $\mathcal{G} \models F$ (F is a ***logical consequence*** of $\mathcal{G}$) if and only if every structure that satisfies all the statements of $\mathcal{G}$ also satisfies F, thus proceeding formally as in propositional logic. The same happens for the second. We agree in fact $\mathcal{G} \vdash F$ (F is ***provable*** by $\mathcal{G}$) if and only if there is a proof of F by $\mathcal{G}$, that is an ordered finite sequence $F_0, F_1, \ldots, F_n$ of sentences of L (with n natural number) such that

- F_n is F,
- for each $i \leq n$, F_i is in $\mathcal{G}$, or it is an "axiom", or it is obtained from previous sentences (among $F_1, F_2, \ldots, F_{i-1}$) by a "deduction rule".

The key point is, again, how to define axioms and deduction rules in such a way that the two operators $\models$ and $\vdash$ coincide.
The ***completeness theorem*** proved by Gödel in 1930 ensures that this can be done: one can actually determine a system of axioms and deduction rules such that, for each choice of a language L, a set $\mathcal{G}$ of sentences of L and a sentence F of L,

$$\mathcal{G} \models F \text{ if and only if } \mathcal{G} \vdash F.$$

A possible choice for this system is still the ***natural deduction***, which extends that of the propositional case, still avoiding any axiom and adding four rules of introduction and elimination of the quantifiers $\forall$ and $\exists$. Indeed these procedures are much more subtle and intricate than those on connectives. Let us try to outline them anyway.

(1) Elimination of $\forall$

The basic idea, seemingly obvious but naive, is as follows: if v is a variable and $\alpha(v)$ is a formula (which really contains v as a free variable), then from $\forall\, v\ \alpha(v)$ we deduce that α is satisfied by every element that goes to interpret v.

Useful notation: for t a term of the language L, $\alpha(t)$ denotes the formula that is obtained from α by replacing v by t in each of its free occurrences.

Example. Let $\alpha(v)$ be the formula $\exists\ w\ \neg\ (v = w)$. Then

- if t is a constant c of L, then $\alpha(c)$ is $\exists\ w\ \neg\ (c = w)$,
- if t is the same variable v, then $\alpha(v)$ remains $\exists\ w\ \neg\ (v = w)$, i.e. α,
- if t is the variable w, then $\alpha(w)$ is $\exists\ w\ \neg\ (w = w)$,
- if t is a variable u other than v,w, then $\alpha(u)$ is $\exists\ w\ \neg\ (u = w)$,
- if t is $F(u)$ for F 1-air operation symbol of L, then $\alpha(F(u))$ is $\exists\ w\ \neg\ (F(u) = w)$.

This first rough version of the $\forall$ elimination rule could then be expressed as follows: for each formula $\alpha(v)$ of L,

$$\frac{\forall v \alpha(v)}{\alpha(t)}$$

But such a rule is not always correct.

Example. Let $\alpha(v)$ be the formula $\exists\ w\ \neg(v = w)$, so that $\forall\ v\ \alpha(v)$ becomes $\forall\ v\ \exists\ w\ \neg(v = w)$. Note that this last statement is true in any structure of the language L that contains at least 2 elements. On the other hand:

- if t is a constant c of L, then $\alpha(c)$ i.e. $\exists\ w\ \neg\ (c = w)$ remains true in every structure of L that contains at least 2 elements, i.e. at least one in addition to the interpretation of c;
- if t is a variable u different from w, then $\alpha(u)$, i.e. $\exists\ w\ \neg\ (u = w)$, remains true in every structure of L that admits at least 2 elements, independently from the valuation of u;
- but if t coincides precisely with w then $\alpha(w)$ becomes $\exists\ w\ \neg\ (w = w)$, and is evidently false in any structure, so it cannot be reasonably deduced in any way from $\forall\ v\ \alpha(v)$.

The defect in the last example: the variable v appears in α under the influence of a quantifier $\exists\ w$ that applies to the variable w that will then replace it.

If t is a term of L, we then say that the variable v is free for t in a formula α if v does not appear in α under the influence of a quantifier $\forall$ or $\exists$ that applies to variables occurring in t.

We note that, in the absence of quantifiers $\forall\ v$ or $\exists\ v$ inside α (not out as in $\forall\ v\ \alpha(v)$) v is certainly free for itself in α.
On the basis of the previous definition we can finally propose the correct version of the rule (1): for each formula α of a language L and for each term t of L,

$$\frac{\forall v \alpha(v)}{\alpha(t)}$$

provided that v is free for t in α.

Note in fact that, in the previous example, v is not free for w in α.

(2) Introduction of $\exists$

The rough idea is the same as before, but adapted to the new context: it seems reasonable that, in the presence of an element that explicitly satisfies $\alpha(v)$, one can deduce $\exists\ v\ \alpha(v)$.
Specifically, it seems that, for each formula $\alpha(v)$ of a language L and for each term t of L, we can establish the rule of deduction

$$\frac{\alpha(t)}{\exists v\ \alpha(v)}$$

Again, however, a clarification is necessary - actually the same as in (1).

Example. Let $\alpha(v)$ be the formula $\forall\ w\ (v = w)$. Then $\exists\ v\ \alpha(v)$ i.e. $\exists\ v\ \forall\ w\ (v = w)$ is true in all structures of the language L that contain exactly one element. However, let us replace v by the term w. We obtain as $\alpha(w)$ the formula $\forall\ w\ (w = w)$, which is obviously true in every structure of L. Consequently, we cannot expect $\alpha(w)$ (true in every structure) to imply $\exists\ v\ \forall\ w\ (v = w)$ (true only in structures of cardinality 1). It can be noted, however, that in this case, as before, v is not free for w in $\alpha(v)$. This is therefore the condition that must be excluded.
In fact the correct rule is: for every formula $\alpha(v)$ of a language L and for every term t of L,

$$\frac{\alpha(t)}{\exists v \alpha(v)}$$

provided that v is free for t in α.

Then there are the last two rules

- **elimination** of $\exists$,
- **introduction** of $\forall$

which, however, require even more subtle precautions. We omit the details.

3.4 The satisfiability problem

As in Boolean logic, so in first-order logic we meet the ***satisfiability problem***. We say that a sentence F of a language L is satisfiable if it is true in some structure of L (which is then called a ***model*** of F).

Satisfiability problem for a language L. Determine an algorithm to decide, for each sentence F of L, whether F is satisfiable or not.

As in the propositional case, so we see that such an algorithm, if it exists, makes it easy to obtain procedures for deciding, for F, F' sentences of L and $\mathcal{G}$ finite sets of sentences of L:

- whether F is ***valid*** (i.e. true in every structure) or not;
- whether F is a ***consequence*** of $\mathcal{G}$ ($\mathcal{G} \models F$) or not.

Then the following fundamental theorem applies (but we do not have time to dwell on it for too long).

Compactness theorem. Let $\mathcal{G}$ be a set of statements of L, F an utterance of L. Then $\mathcal{G} \models F$ if and only if there exists a finite subset $\mathcal{G}_0$ of $\mathcal{G}$ such that $\mathcal{G}_0 \models F$.

Note, however, that the same property for the operator $\vdash$ of provability (equivalent to the operator $\models$ of logical consequence because of the completeness theorem) becomes trivial: for $\mathcal{G}$ a set of utterances of L and F a sentence of L, it is clear that $\mathcal{G} \vdash F$ if and only if there exists a finite subset $\mathcal{G}_0$ of $\mathcal{G}$ such that $\mathcal{G}_0 \vdash F$. In fact, every proof of F by $\mathcal{G}$ is, by its very definition, a finite sequence of sentences.

But let us return to a possible algorithm for the satisfiability problem. We quickly present a possible approach, articulated in three steps.

The first step reduces the sentence F under consideration to the so-called universal form.

Definition. A sentence F of L is said to be ***universal*** if and only if F is of the form

$$\forall v_0 \dots \forall v_n \ \alpha(v_0, \dots, v_n)$$

where $\alpha(v_0, \dots, v_n)$ is a formula without quantifiers in the (free!) variables $v_0, \dots, v_n$ (so it is obtained from atomic formulas with the only use of connectives, and has an architecture analogous to that of propositional formulas, except that the atomic formulas replace the propositional variables).

An appropriate procedure then translates a generic statement F into one (in a possibly wider language) that

- is satisfiable if and only if F is,
- is in universal form.

The second step tries to further reduce the problem from universal sentences to sentences without quantifiers.
In this respect it is not restrictive to assume that L contains at least one constant, which otherwise is added, as the satisfiability or unsatisfiability of sentences is obviously preserved.

Definition. Let $\alpha(v_0, \dots, v_n)$ be a quantifier-free formula, such as the one obtained at the end of the first step. We call an **instance of substitution** of α every statement $\alpha(t_0, \dots, t_n)$ with $t_0, \dots, t_n$ constants of L or, more generally, terms of L without variables.

There is then the

Herbrand Theorem. A universal statement $\forall v_0 \dots \forall v_n \ \alpha(v_0, \dots, v_n)$ is satisfiable if and only if every finite conjunction of substitution instances of $\alpha(v_0, \ldots, v_n)$ is satisfiable.

We note that each of these substitution instances (as well as a finite conjunction of them) is an sentence without quantifiers.

But the reduction guaranteed by Herbrand's theorem is not always feasible.

If in fact the language L contains only a finite number of constants and no operation symbols, then it admits only a finite number of variable-free terms and consequently allows to construct only a finite number of substitution instances of $\alpha(v_0, \ldots, v_n)$, so that the universal statement $\forall v_0 \ldots \forall v_n \ \alpha(v_0, \ldots, v_n)$ is satisfiable if and only if the (finite!) conjunction of these instances is.

But otherwise, when L has an infinity of constants or even just one operation symbol (conditions that generate an infinity of variable-free terms), then it also admits an infinity of substitution instances (and consequently an infinity of conjunctions). Therefore the satisfiability check of a single universal sentence $\forall v_0 \ldots \forall v_n \ \alpha(v_0, \ldots, v_n)$ reduces to that of infinitely many sentences without quantifiers, and so cannot be done in practice, except in the negative case. In fact $\forall v_0 \ldots \forall v_n \ \alpha(v_0, \ldots, v_n)$ is unsatisfiable if and only if there exists a finite conjunction of substitution instances that is unsatisfiable: so a unique conjunction (but the problem is to find it).

The third step (in cases where the second is successful) deals with sentences without quantifiers - a context which, as already pointed out, recalls that of propositional logic, except that the old propositional variables are replaced by the new atomic formulas. Appropriate algorithms adapt those of the propositional case and apply to this extended domain: a theorem by J. A. Robinson explains how to proceed.

The difficulties of the second step remain. In fact, as a consequence of Gödel's incompleteness theorems we have that, for a language L with two binary operation symbols $+, \times$, the problem of satisfiability does not admit any possible algorithm.

Chapter 4

Syllogisms

4.1 Introduction

Syllogistics was invented by Aristotle, thus dating back to the 4*th* century BC. It was later deepened by medieval logicians. In many respects it is now outdated, being largely included in first-order logic.

However, it is still relevant today, as it often appears in competition quizzes. It is therefore worth mentioning the basics.

Essentially, a syllogism consists of a series of propositions. In its simplest form, it leads to the deduction of one conclusion from two premises, thus involving three statements.

Moreover, the very etymology of the word *"syllogism"* reveals its literal meaning, which is *"concatenation of reasonings"*, derived from the combination of the words σύν, with, and λογισμός, calculation.

For Aristotle, the syllogism was one of the main tools with which to exercise and develop the logical faculty of reasoning. The theory of the syllogism he developed can be found in his two works *On Interpretation* [4] and *Prior Analytics* [5].

Let us begin by describing the propositions that make up a syllogism as premises or conclusions. Those considered by Aristotle are distinguished between:

- iuniversal or particular, the former expressed by the quantifier "every" or "for all" and the latter by "some" or "there is";
- affirmative or negative.

Combined, they give rise to four main patterns:

- A. *universal affirmative* (e.g. "all professors are boring");
- I. *particular affirmative* ("some professors are boring");
- E. *universal negative* ("no professor is boring");
- O. *particular negative* ("some professors are not boring").

The use of the letters A, I, E, O to distinguish the four models comes after Aristotle and goes back to the medieval logicians: the vowels A and I derive from the Latin "affirmo" while E and O from "nego".

It can be observed that the four different schemes share a common structure that identifies:

- a subject ("the professors", all or some);
- an affirmed or negated verb ("they are" or "they are not");
- a complement ("boring").

In [4] we read: *"...it is necessary to establish what is noun and what is verb, what is negation, affirmation, judgement and discourse"*.

Let us observe that A expresses exactly the negation of O and E that of I: in fact to exclude that all or some professors are boring is equivalent to admitting that at least one is not or that none is. For this reason these propositions, A and O, I and E, are called "contradictory" two by two.
On the other hand, A and E are called "contrary" because they represent the antithetical poles ("all/no-one") of the same proposition; similarly, I and O are called "subcontrary", corresponding to the two options "someone is" and "someone is not". But be careful to distinguish "contrary" and "subcontrary" from "contradictory". Finally, I and O are called "subordinate" to A and E respectively, because they somehow weaken them, going from "all yes" to "some yes" in the case of A and I, and from "all no" to "some no" in the case of E and O.

Medieval logicians also devised a graphic representation to schematise the Aristotelian configuration of the syllogism: the logical square (or Aristotle's square).

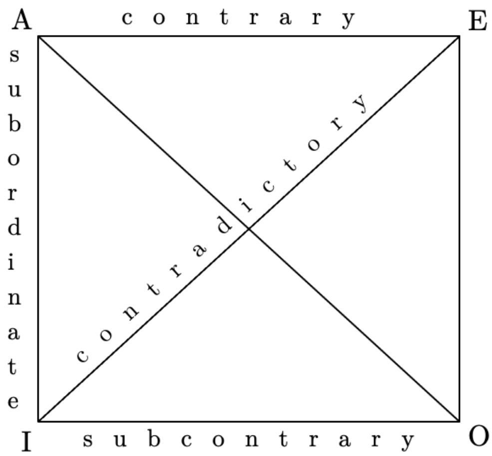


Figure 4.1

A classic example of a syllogism is as follows: from the premises

- all thieves are guilty,
- all guilty people go to jail,

one arrives at the conclusion

- all thieves go to jail.

Three different categories (or terms) are recognised, namely

- the guilty ones who appear only in the premises,
- then the thieves, and finally those who go to jail (both appearing once in the introduction and once in the conclusion).

This structuring applies in general.Thus all syllogisms are assumed to involve precisely three terms denoted S, M and P and named as follows:

- P is *the major term*;
- S is *the minor term*;
- M is *the middle term*.

The middle term is required to appear in the premises, once together with P (*major premise*) and once together with S (*minor premise*).

The conclusion of the syllogism will be "S is (or is not) P" in the four variants A, I, E, O seen earlier.
In the previous example, M corresponds to the guilty, S to the thieves, P to those who go to jail.
In general, depending on the position of M in the two premises, we distinguish four figures of syllogism:
1) "M is P", "S is M";
2) "P is M", "S is M";
3) "M is P", "M is S";
4) "P is M", "M is S".
Since there are 4 figures of a syllogism and 4 possible forms A, I, E, O of both the premises and the conclusion, the total number of distinct modes (models) of syllogisms is $4 \times 4 \times 4 \times 4 = 4^4 = 256$.
However, it is shown that most of these modes are fallacious, i.e. they lead to wrong conclusions. For example, a syllogism of the form

- all murderers are colour-blind;
- the professor is not colour-blind;

therefore

- the professor is the murderer

is wrong and not acceptable.
Its structure corresponds to the previous description, in particular the middle term M coincides with the class of the colour-blind, S with that of the professor alone, P with that of the murderers. And yet, the reasoning clearly does not add up.

4.2 How to recognise valid syllogisms

It is therefore necessary to identify among the 256 models of syllogism the valid ones, which turn out to be "only" 24. Medieval logicians devised mnemonic rules to distinguish fallacious modes from valid ones. These rules can be found as a sort of joke in a poem attributed to Peter of Spain, who was a 13th century Portoguese philosopher, physician and sage, who also became pope under the name of John XXI, and earned Dante's praise in Canto XII of *Paradise* [2]. The above-mentioned rhyme (found in the work *Summulae Logicales* [95]) recalls the 24 valid syllogisms thanks to as many key words such as Barbara, Barbari, Darii and Ferison. The vowels of the words describe in order the form (A, I, E, O) of the major premise, the minor premise and the conclusion respectively. Let us describe some of these valid patterns.

Barbara is a syllogism of the first figure, so the middle term is first in the major premise and second in the minor premise. The three A vowels of the syllogism Barbara indicate that the three propositions composing the syllogism are all universal affirmative. The example already proposed about thieves, but also the following, falls into this scheme:

- all chimpanzees are apes;
- all apes are nice;

therefore:

- all chimpanzees are nice.

In this case, the middle term corresponds to apes, the lower term to chimpanzees and the higher term to those who are nice.
Barbari, on the other hand, has the same figure as Barbara but changes the vowel of the conclusion, i.e. “i”, so the conclusion is particular affirmative. The following example falls into this pattern:

- all chimpanzees are apes;
- all apes are nice;

therefore:

- there is a chimpanzee that is nice.

Although the premises are the same as Barbara’s, in this case the conclusion has been weakened as it is subordinate.

Darii is also a syllogism of the first figure but only the major premise remains universal affirmative A while the minor premise and the conclusion are particular affirmatives I. Consider for example:

- all chimpanzees are nice;

- there are some Juventus fans even among chimpanzees;

therefore:

- there are some Juventus fans who are nice.

Finally, Ferison belongs to the class of the third figure, so the middle term appears in the first place in both premises. Of these, the major one is universal negative E, the minor one is particular affirmative I while the conclusion is particular negative O. The following syllogism falls into this pattern:

- no cannibals are vegetarians;
- some cannibals are murderers;

ergo:

- there are murderers who are not vegetarians.

The validity or fallacy of a syllogism depends only on its mode and not on the terms in it. So whether it speaks of thieves or monkeys, the Barbara model, for example, retains its validity as such, indepentently of the terms that comprise it.

In order to guarantee the validity of a good syllogism it is also appropriate, if not necessary, to assume that the terms constituting it are not empty. Consider the following further example of the Barbari scheme, this time pertaining to the world of crime:

- all ghosts are murderers;
- all murderers go to jail;

Therefore:

- there are ghosts who go to jail.

The conclusion “there are ghosts that go to jail” evidently presupposes that ghosts exist.
This is assumed in every syllogism. Such an assumption is called an *Aristotelian axiom.*

As already pointed out, modern logic has evolved a great deal since the time of Aristotle (from Boolean logic to first-order logic), so it is not surprising that syllogisms present some inadequacies when compared to these new horizons.

The use of the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$ of propositional logic and the quantifiers followed by a variable x, $\forall\, x$ and $\exists\, x$, of first-order logic ensures a more agile and immediate notation.
Thus, a syllogism like the previous Ferison example, with the further introduction of the three symbols C, V, A to denote cannibals, vegetarians and murderers respectively, translates into:

- $\forall\, x\ (C(x) \rightarrow \neg\, V(x))$ “no cannibal is a vegetarian”;
- $\exists\, x\ (C(x) \wedge A(x))$ “there are murderous cannibals”;

therefore

- $\exists\, x\ (A(x) \wedge \neg\, V(x))$ “there are murderers who are not vegetarians”.

The syllogistic lends itself to other perplexities.

- The conclusion of the previous example Darii leads to consider the intersection of the two categories of chimpanzees and Juventus fans, i.e. the class of chimpanzees who are also Juventus fans. But this resulting category does not seem to be represented in reality, unlike the two that determine it as an intersection.
- The syllogistic approach applies to 1-ary relations (such as “being a chimpanzee” or “being a thief”). But common language and mathematics also use binary or even more complicated relations. In mathematics, a relation of equivalence, or order, is binary, i.e. it involves two objects and not just one. The British logician Augustus De Morgan proposed a famous example in common language. Consider the simple reasoning: “all horses are animals; therefore all horse heads are animal heads”. In it the relation “being the head of” does not concern a single object but a pair. So the deduction, although elementary, escapes any syllogistic scheme.
- There are some very famous examples of statements that are considered syllogisms even if, to be nitpicky, they do not exactly correspond to the relevant

prescriptions; among them there is also the one (attributed to Aristotle himself) that "all men are mortal; Socrates is a man; therefore Socrates is mortal". In order for the reasoning to be correct, it is necessary to think of Socrates as a category formed only by Socrates himself and thus to state "all Socrateses are mortal". Note that the same consideration applies to the other example, given earlier, about the colour-blind professor.

4.3 Diagrams and graphs

In the centuries following the Middle Ages, other more intuitive and accessible algorithms were devised to recognise correct syllogisms. Among them is the method proposed by Euler in his *Letters to a German Princess* [47] of 1761 (letters 102 to 108). Basically, it consists of what today are called **Euler-Venn diagrams** and are often taught in primary and secondary schools. Their name derives from the fact that they were also drawn by John Venn in 1880. In reality, it seems that they were used also by Leibniz and probably others before him. The basic idea is to interpret each property, i.e. each term of a syllogism, as the set of elements satisfying it and to represent them respectively as:

- a kind of enclosure surrounded by a closed curved line;
- the collection of points that lie within it.

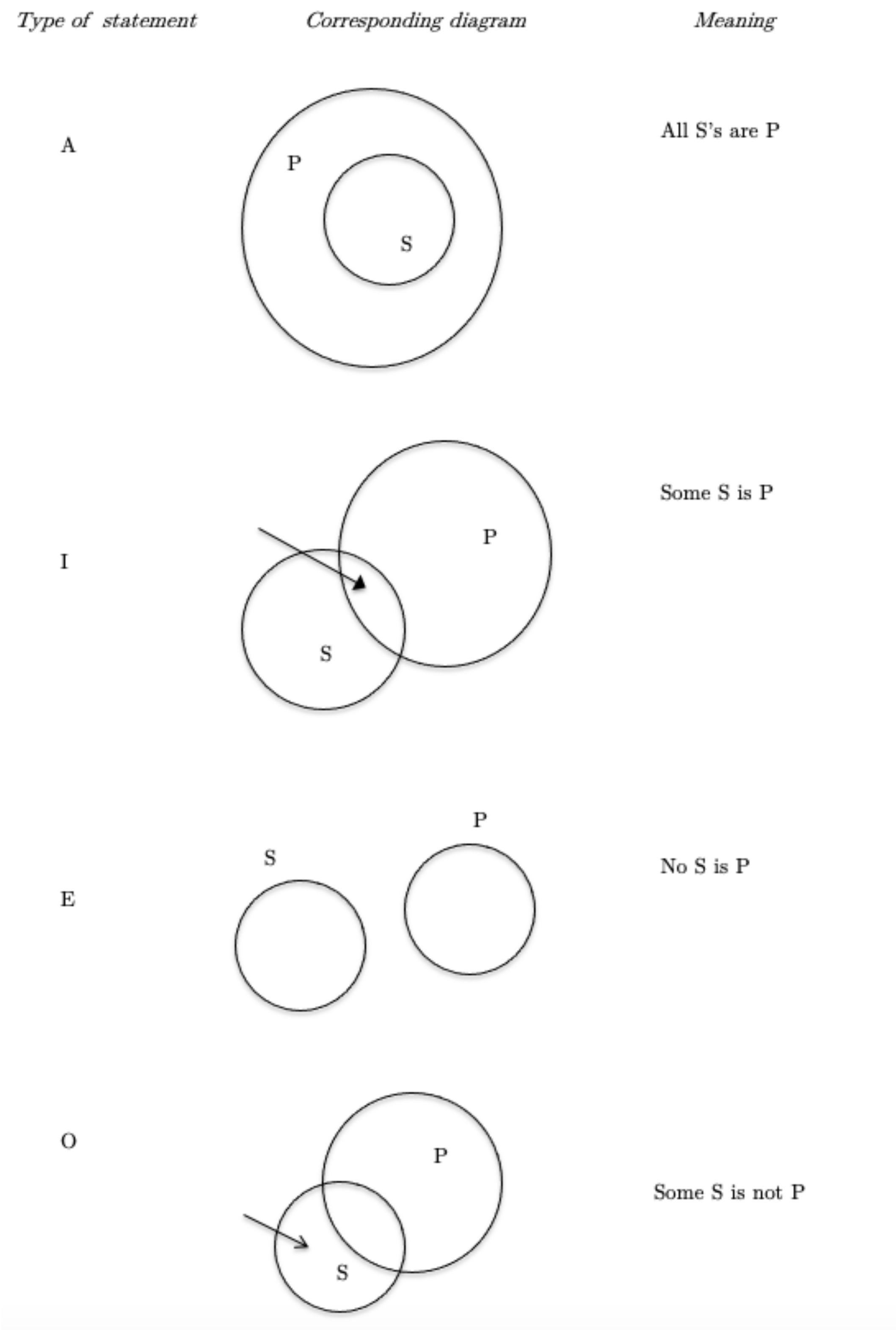


Figure 4.2

In this way, the four types of statements in the Aristotelian quadrilateral correspond to the same number of diagrams. The diagrams of A and E transpose the concept of inclusion and disjunction between sets. Those of I and O differ only for the position of the arrow in the previous figure: the aim of I is in fact to underline the existence of common elements for the two premises S and P, that of O, instead, is to underline the presence of elements in S outside P.

We can reinterpret some syllogisms among those analysed to test the visual power of the Euler-Venn diagrams. Let us start from that Barbara, for which "all chimpanzees are monkeys; all monkeys are nice; therefore all chimpanzees are nice".

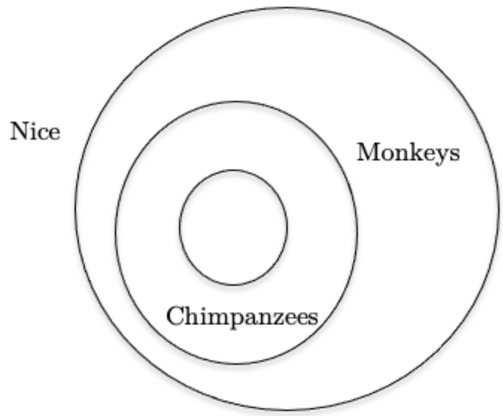


Figure 4.3

The same diagram describes the Barbari syllogism (as can be trivially verified). On the other hand, from Darii one deduces, from the premises that all chimpanzees are nice and there are chimpanzees who are fans of Juventus, the existence of nice fans of Juventus.

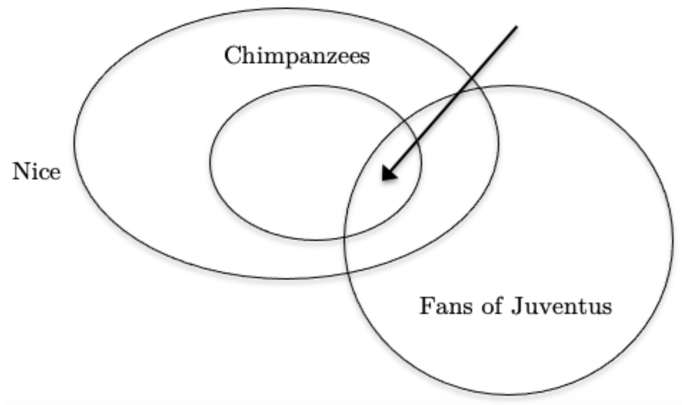


Figure 4.4

As for Ferison's case (in which, if no cannibal is a vegetarian but some cannibal is a murderer, then there is some murderer who is not a vegetarian) the diagram describing it is as follows:

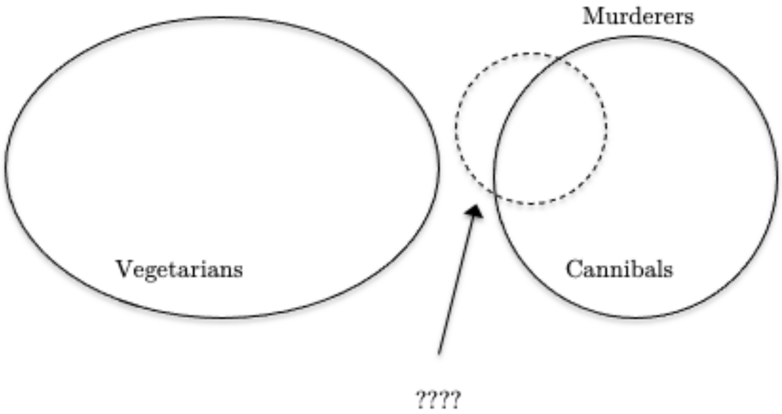


Figure 4.5

Note that this diagram fails to clarify whether the area of the murderers intersects that of the vegetarians. A dotted line has been used to underline this. A playful and light-hearted alternative to the Euler-Venn method is that proposed by Lewis Carroll in his two works *The Game of Logic* [23] and *Symbolic Logic* [24]. In general, all of Carroll's books, even those less "serious" than those already mentioned, are full of word games and logical tricks. Many of these are inevitably lost in the Italian translation because a joke that works in English, once translated into Italian, does not necessarily retain its subtext.

Consider also the paradoxical "syllogism" in chapter 4 of *Through the Looking Glass* [26]: *"...if it was so, it might be; and if it were so, it would be; but as it isn't, it ain't. That's logic".* Another very famous but less surreal example is suggested by *Alice in Wonderland*, Chapter 6 [25]:

- every cat that grins is Cheshire;
- all the cats Alice has met are grinning;

therefore

- all cats Alice has met are Cheshire.

In Carroll's vision, syllogisms are seen as a sort of board game, with a board consisting of a square panel divided into $2^3 = 8$ portions related to the 3 terms S, M and P, that are determined by 3 filters that screen the light in three different ways: one blue, one striped and one grey, as shown in the figure.

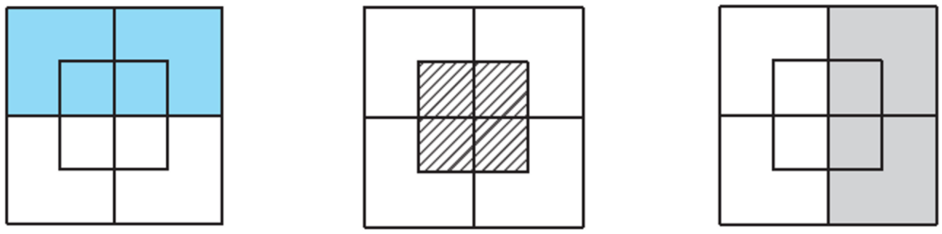


Figure 4.6

However, each filter only screens part of the light, so when the light is screen simultaneously by two filters, e.g. blue and grey, 4 distinct zones are determined (left image); whereas with all three filters together, 8 zones in total are singled out (right image).

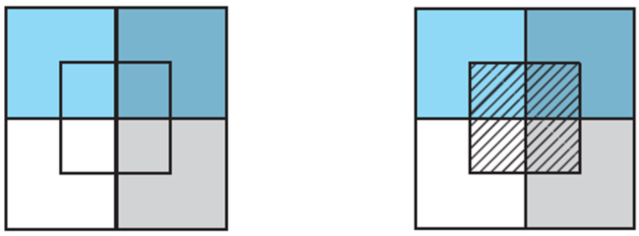


Figure 4.7

The eight different zones are characterized by the presence and absence of each filter and can be summarised in the following table:

	no	yes	no	no	yes	no	yes	yes
	no	no	yes	no	yes	yes	no	yes
	no	no	no	yes	no	yes	yes	yes

Table 4.1

Now let us try to analyse the syllogism involving Alice and cats by imagining that each filter on the board represents one of the characteristics of the cats in Wonderland: grey for the grinning cats, blue for the Cheshires and striped for the cats Alice met. Suppose that the whole square identifies all the cats in Wonderland.
The major premise is that "every cat that grins is a Cheshire". It only involves the blue and grey filters, so the square remains divided into only four zones. Moreover there is no cat in Wonderland that has the grey feature but not the blue as the previous premise is universal affirmative. To transcribe this information onto the square, we delete the area of these cats (grey but not blue) in Wonderland.

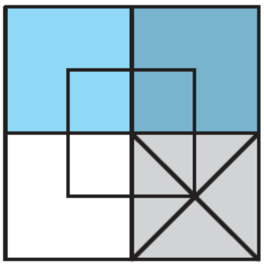


Figure 4.8

The minor premise on the other hand states that "all the cats Alice has met grin".
After inserting the striped filter and removing the blue one, we move on to trace the information that the premise contains: now that part of the square representing the striped cats that are not grey must be deleted.

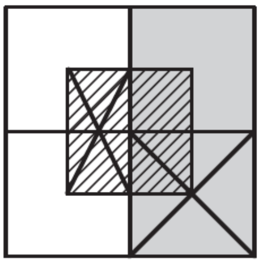


Figure 4.9

At this point the blue filter is inserted again and the grey is removed to see if there is any information linking the two characteristics blue and striped.

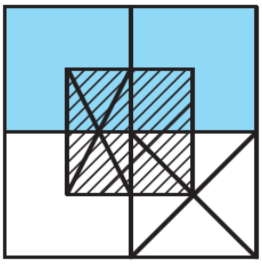


Figure 4.10

The only illuminated and not obliterated area is screened by both the blue and striped filters, leading to the conclusion "all the cats Alice has met are Cheshire".

There are other more complex situations that can be analysed with this method; take an example inspired by [23]:

- no sweet cake is inedible;
- some fresh cakes are inedible;

therefore

- some fresh cakes are not sweet.

In this case the blue filter corresponds to inedible cakes, the grey filter to sweet cakes and finally the striped filter to fresh cakes. Unlike the previous case, the minor premise is not universal but particular. If the major premise determines an entire area to be deleted, the minor premise indicates that a certain area is occupied by at least "an individual" and this area is obviously the one illuminated by the striped and blue filters. To indicate this, a dot is inserted in the aforementioned zone, paying attention to the fact that part of the zone in which we insert it cannot be occupied.

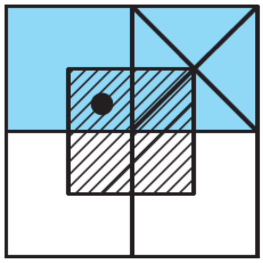
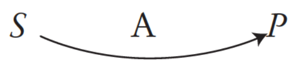


Figure 4.11

The conclusion can be seen by removing the blue filter and inserting the grey one, i.e. "some fresh cakes are not sweet".

Another easy and witty method for solving syllogisms is the one devised by Ruggero Pagnan and Pino Rosolini in [86]: the four forms A, E, I, O are represented by four oriented graphs.

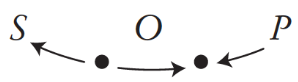
- universal affirmative A.



- particular affirmative I.

- universal negative E.

- particular negative O.

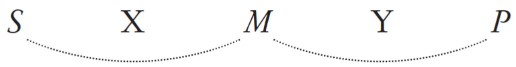


The steps of the algorithm for solving syllogisms are as follows:

1) determine the types of the major and minor premises and translate them into the language of graphs

where X and Y are two of the possible graphs listed above;

2) the graphs are rewritten by superimposing the mean term M;



3) if the arrows passing through the information common to the two premises have the same direction, they are joined to form a single arrow;

4) if possible, read the statement that corresponds to the graph obtained.

For example take the syllogism from Alice and the Cats in Wonderland:

- every cat that grins is Cheshire;
- every cat Alice has met grins;

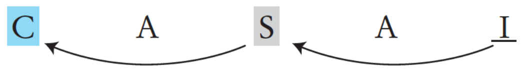
therefore

- all cats Alice has met are Cheshire.

By denoting by the initial letter each involved characteristic and applying the algorithm, we obtain:

1) each S is C and each I is S;

2) the corresponding graphs are;



3) the arrows that pass through S go in the same direction and we obtain

4) the degree corresponds to the statement "every I is C".

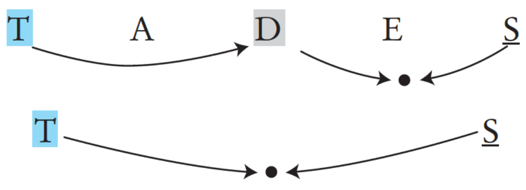
Other more complex examples are given by the following syllogisms.

1) Consider the syllogism

- cakes are sweet;
- pies are not sweet;

therefore

- pies are not cakes.

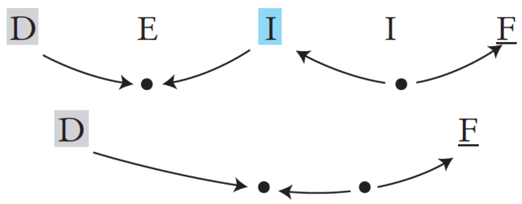


2) Let us deal with:

- no sweet cake is inedible;
- some fresh cakes are inedible;

therefore

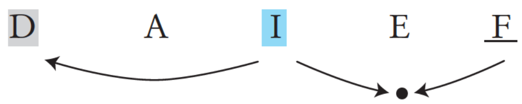
- some fresh cakes are not sweet.



3) Finally

- inedible cakes are sweet;
- no fresh cakes are sour;

therefore ...



In case 3) the method fails because the graph obtained does not fall into the expected types. In fact step 3 did not produce any arrows.

4.4 First-order monadic logic

The part of first-order logic that considers only 1-ary relations and thus includes syllogistics is called "monadic". We have already dealt with one statement that is overseen by this type of logic, that of the cannibals and vegetarians of the Ferison model:

$$(\forall x \ (C(x) \to \neg V(x)) \land \exists x \ (C(x) \land A(x))) \to \exists x \ (A(x) \land \neg V(x)),$$

in which quantifiers, variables of individuals, and symbols for 1-ary relations were used to rewrite the syllogism "no cannibals are vegetarians; some cannibals are murderers; ergo, there are murderers who are not vegetarians".

Monadic logic, however, transcends syllogisms because it deals with cases in which the intervening 1-ary relations are not just 3, for S, M and P, but extend to arbitrary values. For example, it considers extended sequences of syllogisms - those that are called sorites (or polysyllogisms).

Actually, the term *sorites*, coined in the 4*th* century AD by the Roman rhetorician Gaius Marius Victorinus, traditionally refers to two different questions. Etimologically it derives from the Greek σωρός, i.e. *"heap"*. It thus attests the large number of propositions that form a polysyllogism – the topic we are interested in. But it also recalls a famous paradox that dates back to the 4th century BC and is attributed to the philosopher Eubulides of Miletus. We will tell it later.
Anyway, just to avoid any misunderstanding, let us underline that a sorites is not contradictory per se, even if, as in the case of syllogisms, it may sometimes be fallacious. The point is, again, to distinguish right from wrong polysyllogisms.

When the number of original propositions of a sorites far exceeds that of a classical syllogism, it becomes much more difficult to organise them in order to direct them to the conclusion. Carroll was also interested in this problem, and in [23], [24] and [25] proposed some explanatory examples.
The first is taken from the dialogue between the protagonist and the Cheshire Cat in the sixth chapter of [25]. In response to the child's worried reaction to the prospect of meeting two madmen like the Hatter and the March Hare, the Cat declares that he and Alice are mad too, and goes on to explain why. To prove his own madness, he states that no dog is mad. Then he goes on to say that a dog growles when it is angry and wags its tail when it is pleased, whereas he, on the contrary, growles when he is pleased and wags his tail when he is angry: therefore he is mad.
This argument is obviously incorrect, and provides an example of fallacious sorites. It develops in fact from the 3 premises of the Cat:

- no dog is mad;
- all dogs growl when they are angry and wag their tails when they are pleased;
- I growl when I am pleased and wag my tail when I am angry;

to deduce

- I am mad.

But to arrive at this conclusion he would need, if anything, as a first premise "who is not a dog is mad", instead of "who is a dog is not mad".

A further example, taken from the second part of [24], which was never published,

takes up a classic argument attributed to the Stoics and which in turn repurposes the famous antinomy of the liar. In ancient Egypt, on the banks of the Nile, a crocodile kidnaps a child. The mother begs him to return it safe and sound. The mother and the crocodile agree on the following: the woman must predict whether or not the crocodile will devour the child; if she guesses right, the child will be returned to her, and if she fails, it will be devoured.
The mother then guesses that the child will be devoured. It remains to be seen what the crocodile will do, about which it is stated that he will be true to his word. On the other hand,

- if the woman tells the truth, then the crocodile renders her the child and thus makes her tell a falsehood;
- on the other hand, if the woman speaks falsely, the crocodile devours the baby and thus attests that she is telling the truth.

Carroll examines the situation and points out, precisely, how the problem is misplaced.

From these two examples, it is clear that the general and abstract problem of solving a sorites, i.e. understanding whether it is true or false, is not at all trivial when the number of its premises begins to increase. Obviously, exploring one by one the possible concatenations of deductions in order to find a correct one that confirms the reasoning is not the right way to go, nor would it make sense to try to guess a correct one, if it exists. Nor does it make sense to resort again to aids such as Peter of Spain's poems, Euler-Venn's diagrams or Pagnan-Rosolini's graphs. As we said, a sorites can include an enormous number - therefore a heap - of statements, among which it is difficult to orient oneself.

And here it is the case that, taking a cue also from the embarrassments of the crocodile tale, we recall the above-mentioned paradox of Eubulides.
One considers a heap of sand: a single grain of sand is not enough to make it up, because one grain is not a heap, and neither are two, or three, or four, or one hundred grains. But at a certain point the heap begins to be a heap, and so the question is: when does this happen? Eubulides' argument confirms how delicate and insidious the concept of truth is and what risks are run by rigidly limiting it to only two antagonistic alternatives, heap yes or heap no, as is done in classical logic, neglecting

intermediate nuances.
Returning to polysyllogisms, the question posed by the philosopher from Miletus could raise a similar problem, about the maximal number of statements in a polysyllogism that still allow to manage and master it, and to exclude any possible failure. Indeed it seems necessary to develop a sort of rapid calculation of syllogisms and polysyllogisms, and thus to provide a repertoire of algorithms, no matter how refined, but solid and effective, to resolve the question.

In this perspective it can be very useful to see sorites and syllogisms within first-order logic. We have already seen with an example how all these arguments can be translated into a sentence of this logic, which uses only symbols for 1-ary relations. An algorithm for the satisfiability problem could check the validity of these sentences. On the other hand we know that this algorithm does not exist for the whole first-order logic, or at least for some of its languages (for example, that with two binary operation symbols). But now we are only interested in monadic first-order logic, which restricts its languages to 1-ary relations. This narrower scope might allow the development of specific algorithms.
Let us recall that in the case of syllogisms there are three relations involved, but in sorites this number could be extended to an arbitrary value N with the corresponding 1-ary relation symbols, say $R_1, \ldots, R_N$. We would then like a procedure capable of establishing, for each sentence E that can be written with 1-ary relation symbols, whether E is valid or fallacious. As we know, it is equivalent to deciding for every E whether it is satisfiable or not. The example of cannibals and vegetarians we have already dealt with, slightly changed according to the notation we have just established, uses three symbols of 1-way relations R_1, R_2, R_3, and writes:

$$(\forall x\ \ (R_1(x) \to \neg\ R_2(x)) \wedge \exists x\ \ (R_1(x) \wedge R_3(x))) \to \exists x\ \ (R_3(x) \wedge \neg\ R_2(x)).$$

However, our algorithm should apply to every E and therefore to every N. We should then recall that the validity of E is independent of the meaning that one intends to assign to $R_1, \ldots, R_N$ and therefore of their interpretation (as already seen for classical syllogisms), but refers only to the way in which these symbols are combined. Thus E is to be understood as valid if all interpretations confirm it, and fallacious if at least one contradicts it.

Logical research reached an important milestone when, in 1915, German mathematician Leopold Löwenheim proved in an important theorem that first-order monadic

logic is decidable: in other words, the sought-after algorithm exists.
The reason is as follows. Let us assume that the sentence E contains precisely N symbols of 1-ary relations, then let Q be its quantifier rank (a number that somehow notices the presence of the occurrences of the quantifiers $\exists$ and $\forall$ within E). It is then shown that E is valid if confirmed by all its interpretations in finite universes of at most $Q \times 2^N$ elements, while it is fallacious if denied by at least one of them. This significantly improves our setting, passing from arbitrary universes to some of finite and limited cardinality.
In the specific case of polysyllogisms, the threshold can even be lowered to 2^N elements. Then the following decision algorithm applies: given a sentence E of first-order monadic logic,

- N and possibly Q are determined;
- all the interpretations $R_1, \ldots, R_N$ are listed in universes of dimension at most $Q \times 2^N$ or even 2^N if one considers the restricted scope of the sorites;
- it is observed that these universes, unless isomorphisms, are at most finitely many and can be completely classified;
- one checks for each of them whether E is satisfied or not;
- If the answer is always yes, one concludes that E is valid, while if it is sometimes no, then E is fallacious.

Not that this gets around all difficulties. In fact the number of these universes to be checked, despite being finite, can be very big in practice.
For example, in the case of syllogisms, there are three 1-ary relations present and therefore $N = 3$ and consequently, if we neglect Q, we have universes with $8 = 2^3$ elements to examine. But cataloguing the ways in which three 1-ary relations, i.e. three subsets, are arranged in a world of 8 objects is a combinatorial problem which is not easy, and almost more complicated than counting the 256 syllogistic ways.
Obviously, as N increases, things get even worse, both because of the exponential trend of 2^N and because of the successive steps of the algorithm. These difficulties are confirmed by the scientific investigation of that branch of modern theoretical computer science that goes by the name of computational complexity. It turns out in fact that each algorithm for the satisfiability of monadic first-order logic, not

only the one identified by Löwenheim but also any alternative procedure, comes to employ working times exponential with respect to the length of E, that is, to the number of symbols that appear in it and therefore, in a broad sense, to the number N of the relations that intervene in it.

It might be possible to weaken the initial demands, by fixing in advance a maximum number N_0 of relations for which the algorithm is to be used. In such hypotheses the situation certainly improves, but not so much as to allow us to successfully tackle the problem of satisfiability for first-order monadic logic. In the most obstinate cases, the best solving procedures are likely to take even longer to solve the problem than the already long time taken by the logic of connectives.

Chapter 5

Mathematics through images

5.1 Proofs without words: an introduction

Two possible logical formalisations of mathematical reasoning have already been given, the Boolean and the first-order. In each of them, an abstract concept of proof, inspired by Hilbert, has been introduced and discussed. A proof is viewed as a finite ordered sequence of formulas, which evolves according to precise rules of deduction. A theorem is then the last step of a proof, i.e. the last formula of the sequence.

This vision, useful in theory, and moreover anticipating the ideas of computation and programme in modern theoretical computer science, is however fatally limited. It is difficult to reduce a proof to a mere combinatorial calculation of successive formulas, and a theorem to its final stage. There are beautiful and fascinating theorems, as well as other more grey and dull theorems. Similarly, the same theorem may admit brilliant, concise and elegant proofs as well as slow, dry, uninformative proofs.

A current in the philosophy of mathematics, the so-called mathematical Platonism, believes that a theorem somehow pre-exists in a world of ideas and that the human mind can only rediscover it. The same can be said of a proof. This vision is clearly linked to Plato and his conception of mathematics. For example, in *Book VII* of his dialogue *Republic* [97], the philosopher writes that *"[...] geometry is the science of what always is, and not of what at one moment is generated and at another moment perishes"*. Logicians such as Frege, Cantor, Russell and Gödel can be considered Platonists, albeit with a variety of nuances.

Of course, someone prefers the opposite view, namely that mathematics, with its theorems and relative proofs, is the fruit of the human mind, that generates and elaborates it, inspired by the world around us, by the study of nature and the universe, by the other less exact sciences.

Anyhow, whatever way mathematics is conceived, as the discovery of eternal ideas or the autonomous construction of the intellect guided by the analysis of reality, mathematics cannot be reduced to aseptic calculations, but lives also as emotion and lightning.

Reasoning and intuition thus seem to coexist in mathematical research. But it is legitimate to ask what role sensations, particularly visual ones, can play in all this. Are mathematics and images antithetical?

In Plato the former is the antechamber to the fullness of knowledge of the world and of oneself, while the latter is only the first step of this process. On the other hand, Plato appreciates art, and in particular painting, only when it avoids any emotion and contributes to the formation of the soul. Therefore a contrast emerges in Plato's thought between these two poles, mathematics and image, and consequently between mathematics and art, at least if we understand the latter as the creation of images – in the broadest sense.

Today, on the contrary, the image seems to play a predominant role in education, nor can it be denied that mental activity also relies on imaginative thought and that its models are also rooted in the concreteness of perceptual processes.

If we accept the idea that "perceiving" is actually "thinking", or at least contributes to it in a decisive way, we can assume that our brain is already in its perceptive phase a sort of biological simulator capable of predicting behaviour, drawing on memory and formulating hypotheses: perceiving an object is to imagine the actions implied by its use, and it is also to abstract, select particular traits and ignore others.

The relationship and the fracture between the abstract of cognitive capacities dear to mathematicians and the concrete of the senses that inspire the creation of images were considered in the last century with a very modern spirit by the German psychologist of perception and art, Rudolph Arnheim (1904-2007). However, his analysis did not stop at the specific field of the arts, but extended to all fields of knowledge.

According to Arnheim, in didactic practice learning towards perceptual abstraction should be guided by means of appropriate illustrations, trying to maintain a rich concrete context: *"in the perception of form lies the germ of the formation of concepts"*, as we read in his 1969 work *Visual Thinking* [7].

In an attempt to guide the student to perceptual abstractions, simplified constructs are used, summarising reality. Often, however, such a scientific concretisation fatally ends up providing, almost by definition, only a modified and reduced case, which fails to give even a glimmer of the situation itself and risks being a false facilitation. The phenomenon is taken out of context, as if it were an independent event, and exhibited *"against an empty background that eliminates the granular and noisy part of the concrete situation"*. But, on the contrary, according to Arnheim, science education works best if it embraces the whole process from direct, empirical perception to formalised constructions, and if it ensures a continuous exchange between them. George Polya (1887-1985), a Hungarian mathematician, who is considered a precursor, if not the father, of the conception of mathematics known as quasi-empiricism, also contributed to analysing even more directly and with extreme finesse the combination of the concrete and the abstract in mathematics. For him, mathematical reasoning is *"secure, beyond dispute"*, but not a guarantee. In his fundamental work *Mathematics of Plausible Reasoning* [102], he writes:

"Mathematics is regarded as a demonstrative science. Yet this is only one of its aspects. [...] You have to guess a mathematical theorem before you prove it; you have to guess the idea of the proof before you carry through the details. You have to combine observations and follow analogies; you have to try and try again. The result of the mathematician's creative work is demonstrative reasoning, a proof; but the proof is discovered by plausible reasoning, by guessing".

But there is more: according to the new empiricism and Polya, mathematics has developed and continues to develop throughout history, in the same way as the other natural sciences and in particular the physical sciences, without escaping a kind of "observational reporting", albeit transformed into calculations, hence mental experiments and approximations.

An example in which physical and sensory instruments intervene to support mathematical results is that of geometric figure drawing, which is carried out in the first years of school, for example (real) constructions with ruler and compasses. It is in this context that the concept of "proof without words" was born, proposed by the American mathematician Roger B. Nelsen in his book of the same title in 1993 [82]. These are proposals for proofs, even outside geometry, which are reduced to the name of the theorem or the algebraic formula to be proved, and then to one or more related figures, to very few textual indications and to the request to construct the entire argument from these indications. They, as the introduction to Nelsen's text states, *"are pictures or diagrams that help the observer see why a particular statement may be true, and also to see how one might begin to go about proving it true"*. The proofs without words are thus a kind of visual thinking, or rather visual education in thinking, an introduction to logic through images, and thus constitute a source from which to draw extensively for teaching. They provide an opportunity to encourage reflection and comparisons between different types of demonstrations of the same result, so that students become accustomed to not being tied to a single demonstrative procedure, but to discover connections between different parts of mathematics. In addition, they make it possible:

- to underline how the use of the language of figures is useful for discovering and clarifying the logical path of certain demonstrative procedures;
- to consolidate the ability to formalise and express in a rigorous language the intuitions obtained from geometric analysis;
- to check how the students have internalised and are able to use the knowledge they have already acquired in new problem situations.

Although the term was coined recently (the first proofs without words appeared in *Mathematics Magazine* during 1975 and then ten years later in *The College Mathematics Journal*, both published by the Mathematical Association of America), the first proofs involving only a figure constructed with a ruler and compasses date back to ancient Greece and Pythagoras himself (c. 600 BC) but also Euclid (c. 300 BC) in his *Elements*. Other testimonies from the ancient world date back to imperial China and are contained in the millenary text *Zhou Bi Suan Jing* (200 BC) [133] and finally to the Indian mathematician and astronomer Bhaskara (c. 200 AD), as we will see in later examples.
Their relevance is sealed by the interest they have always aroused in teachers, who appreciate their pedagogical intent to replace the classical (and sometimes pedantic) *"textbook proofs"*.
Let us propose an example of this kind of proof, planning to analyse it later from the point of view of proofs without words. Consider the theorem according to which the sum of the first n natural numbers (the n-th triangular number) is $T_n = \frac{n(n+1)}{2}$.
A well-known proof applies the principle of mathematical induction to n.

- The basic step concerns $n = 0$ and observes that $T_0 = 0 = \frac{0 \cdot 1}{2} = 0$.

- Let us then assume the thesis to be true for some n, so that $T_n = \frac{n(n+1)}{2}$, and prove it for $n+1$. In fact

$$\begin{aligned} T_{n+1} = T_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \\ = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)[(n+1)+1]}{2} = \\ = \frac{(n+1)(n+2)}{2} \end{aligned}$$

as claimed.

Far more direct, persuasive and intuitive is, as we shall see, the wordless approach. It is therefore time to give a few examples to highlight its power and effectiveness. We will focus on 3 main arguments, also external to geometry, among the many that are already considered in Nelsen's books, and then in the literature that followed them:

1) the Pythagorean theorem and the Pythagorean triples;
2) the combinatorial calculus;
3) sums of convergent series.

5.2 The Pythagorean theorem and the Pythagorean terns

As a first example, let us consider one of the milestones of mathematics, one of its most famous theorems, with a lot of alternative demonstrations: Pythagoras' theorem, according to which "in a right triangle, the square constructed on the hypotenuse is equivalent to the sum of the squares constructed on the catheti". If therefore a, b, c denote respectively the lengths of the two catheti and the hypotenuse, the equality $a^2 + b^2 = c^2$ is valid.
Pythagoras' theorem also admits several proofs without words. In this sense we may also partly view the one Euclid proposes in proposition 47 of the first book of *Elements* [44]. Let us recall it.
We refer to the following figure. In it we recognise the starting point of the theorem, i.e. the right triangle ABC with hypotenuse AB and catheti AC and BC, and the squares constructed on the three segments $ABED$, $ACGF$, $BCMK$ respectively.

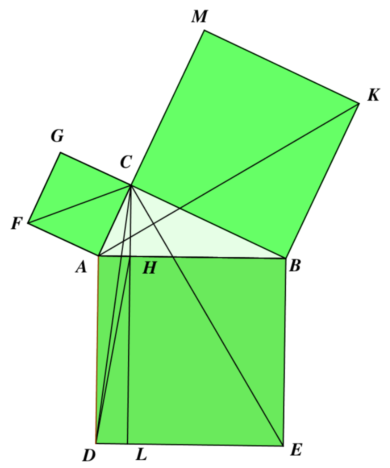


Figure 5.1

Let CL be the segment fromt C parallel to AD, so orthogonal to AB. The triangles FAB and CAD are congruent because of the first criterion of congruence of triangles: they have in fact $AB = AD$ because they are sides of the same square $ABDE$; moreover $AF = AC$, because they are sides of the same square $ACGF$; finally the angles $F\hat{A}B$ and $C\hat{A}D$ have the same amplitude because they are the sum of a right angle and of a common angle that is $C\hat{A}B$.
Furthermore, the triangles CAD and AHD have the same base AD and the same height AH, and are therefore equivalent. Thus they both have, CAD and AHD, half the area of the rectangle $ADLH$. On the other hand, the triangles FAB and FAC also have the same base AF and the same height AC, so they are equivalent, and both have an area equal to half that of the square $ACGF$.
The rectangle $ADLH$ is therefore equivalent to the square $ACGF$.
Similarly, the rectangle $BELH$ is equivalent to the square $BKMC$.
So, in the end, the square $ABED$ on the hypotenuse AB, which is the sum of the rectangles $ADLH$ and $BELH$, is equivalent to the sum of the squares $ACGF$ and $BCMK$ on AC and BC.

A more properly "proof without words" is the one that can be deduced from the above-mentioned Chinese text *Zhou Bi Suan Jing* [133], dating back to 200 B.C. It makes use of the following figure:

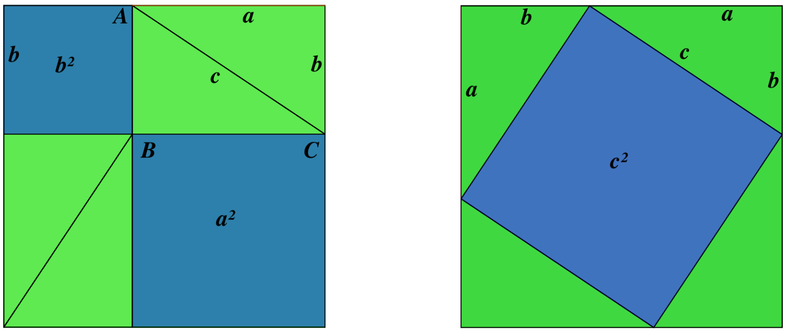


Figure 5.2

We recognise the right-angled triangle ABC of catheti a, b and hypotenuse c. The square whose side is the sum of the catheti, therefore measuring $a+b$, can be decomposed in two ways:

- on the left as the sum of the two squares constructed on the catheti and in the 4 triangles equal to the initial one,
- on the right as the sum of the square constructed on the hypotenuse and again of four triangles equal to the original one.

Both on the left and on the right, the right-angled triangles are coloured in green, and the rest of the figure in light blue. By comparing these parts in light blue, the thesis is easily obtained.

Indeed certain non-marginal properties need to be checked for correctness, namely that the 4 triangles on the left and right are all equal to each other (and to the starting triangle), and that the quadrilateral on the right is really a square, in particular it has 4 right angles. But all of this can be easily verified, and indeed may provide the cue to invite students to complete the demonstration in these details.

A proof two millennia later, but similar in some respects, was obtained by the British astronomer George B. Airy (1801-1892) [135]. It is accompanied and explained by the following verses:

I am, as you can see,
a^2+b^2-ab.
When two triangles on me stand,

square of hypothenuse is plann'd
but if I stand on them instead
the square of both sides are read.

The proof is based on the following figure:

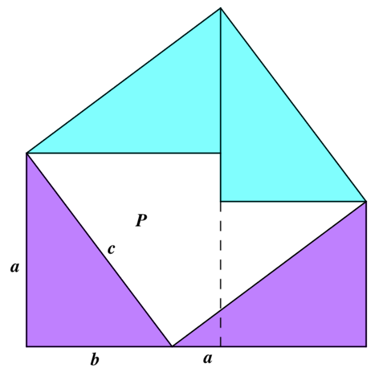


Figure 5.3

The right-angled triangle referred to is the purple one at the bottom left, which is however equal to the other purple right-angled triangle at the right, and to the two light blue right-angled triangles at the top. The part in white and light blue corresponds to the square constructed on the hypotenuse, the part in white and purple to the sum of the squares constructed on the catheti. The purple and light blue parts are obviously equal, since they are made up of two of the four original right-angled triangles. The white part then measures $a^2 + b^2 - ab$, which is the quantity mentioned in the poem.

Another proof without words of the theorem is provided by the 20th US President James A. Garfield (1831-1881) [54]. In it, no squares appear, but a right-angled trapezoid, together with two copies of the right triangle under consideration. The lengths of the catheti and hypotenuse are denoted here by x, y, z. The triangles are in light green, ABC and CED respectively, while the trapezoid also adds the white part to them, thus coinciding with $ABED$.

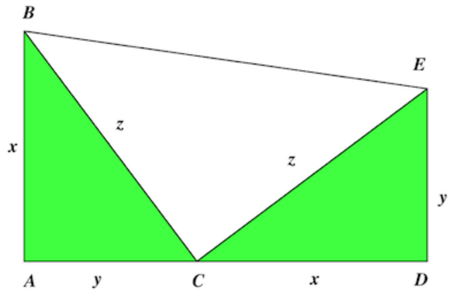


Figure 5.4

Note that the white triangle at the centre of the figure is right in C and is also isosceles, since the two side angles are complementary, in fact they correspond to the acute angles of the right triangle.
The trapezoid $ABED$ has height $x+y$ and bases x and y respectively, so area $S = \frac{(x+y)(x+y)}{2} = \frac{(x^2+y^2)}{2} + xy$. But the same area is obtained as the sum of those of the three right triangles, two with catheti x and y, the other one with two equal catheti of measure z, so it is: $S = \frac{xy}{2} + \frac{xy}{2} + \frac{z^2}{2} = xy + \frac{z^2}{2}$ Comparing the two expressions we obtain the thesis of the theorem.

A further proof, less recent than the previous ones, is attributed to the Arab mathematician Thabit Ibn Qurra (826-901) [135], known in the Western world as Thebizius; it relies on the following figure:

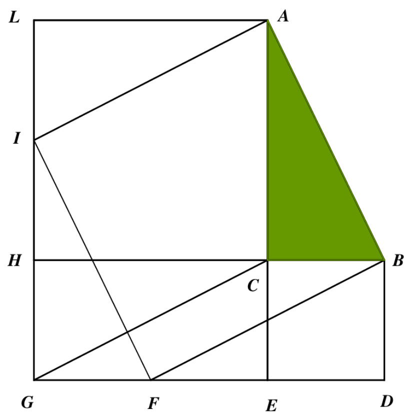


Figure 5.5

The right triangle under consideration is the one in green ABC. One can recognise quite well both the squares constructed on the catheti, respectively $ACHL$ and $CBED$, and the square constructed on the hypotenuse, namely $ABFI$. In order to

complete the overall polygon $ABDGL$ we need:
- in the first case, in addition to the squares on the catheti, the rectangle CHGE (which is composed of two triangles equal to the initial triangle, CGH and CGE),
- in the second case, the two rectangle triangles IGF and CBD, which are again both equal to the starting triangle.

About a millennium later, in 1873, Henry Perigal (1801-1898) [137], a stockbroker with a passion for mathematics, proposed another brilliant proof of the theorem, based on the following figure:

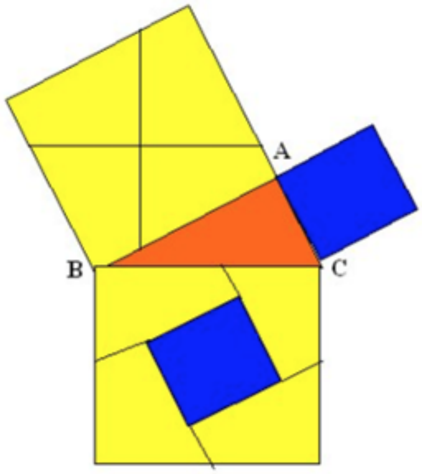


Figure 5.6

The right triangle is the orange one ABC, and the squares on the catheti AC and AB are one in blue and the other in yellow. The latter is divided by two lines passing through its centre (i.e. the point where the diagonals meet) and orthogonal to each other, one perpendicular and one parallel to the hypotenuse BC.
The square on BC is divided into five parts, corresponding to the blue square and the four parts of the yellow square. In doing so, Perigal demonstrated the equivalence of the sum of the two yellow and blue squares with the one constructed on the hypotenuse.

The last proposed version is due to the Prussian mathematician Georg F. von Templehoff (1737-1807) [113], who developed it in 1769 on the basis of the following figure:

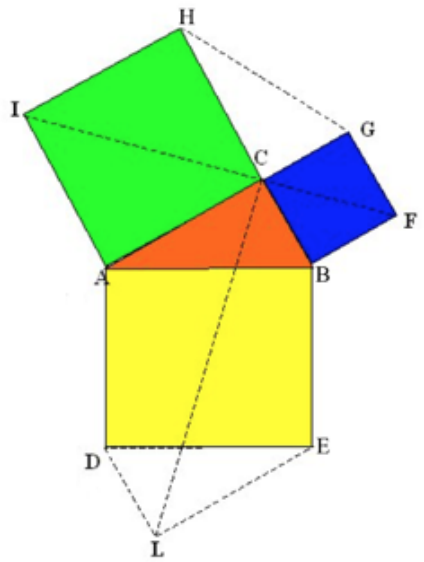


Figure 5.7

The right triangle is the orange one ABC, the squares to be compared (on the catheti AC and CB and on the hypotenuse AB respectively) are the green one $ACHI$, the blue one $BCGF$ and the yellow one $ABED$. To the latter we add the right triangle EDL, which is equivalent to the initial triangle. G and H are then joined, obtaining a right triangle CHG, which is still equivalent to the original one. It is proved that the quadrilaterals $FGHI$, $ABFI$, $ADLC$ and $BCLE$ are equivalent. The hexagon $ABFGHI$ is therefore equivalent to the hexagon $ADLEBC$. But if we remove from the two hexagons the common triangle ABC and the equal triangles CGH and DLE, the remaining parts, namely the sum of the squares of the catheti and the square of the hypotenuse, are equivalent, whence the thesis of the theorem.

Closely related to the Pythagorean theorem is the concept of the Pythagorean triple. This is an ordered triple of positive integers (a, b, c) that constitute the measures of the two catheti and the hypotenuse of a right triangle, and therefore satisfy the Pythagorean equation $a^2 + b^2 = c^2$. Of course the roles of a, b can be interchanged. However, we can fix, for example, $a < b$.
The equation in question is homogeneous of the second degree, so if a triple (a, b, c) satisfies it, so does every triple (ka, kb, kc) for every positive integer k. For example, the Pythagorean triple $(3, 4, 5)$ generates $(6, 8, 10), (9, 12, 15), (12, 16, 20)$ etc. in this way. A Pythagorean triple (a, b, c) whose components a, b, c are coprime (and there-

fore pairwise coprime) is called primitive. An example is $(3,4,5)$. Each Pythagorean triple is obtained from a primitive, which is found by dividing the 3 components by their greatest common divisor. The Pythagorean triple is then obtained from the primitive thus generated by multiplying its components by that greatest common divisor.

The problem arises of classifying all Pythagorean triples, and therefore all primitive Pythagorean triples. A proof without words of the infinity of these primitive Pythagorean triples was proposed in 1987 by Charles Vanden Eynden in his text *Elementary Number Theory* [49]:

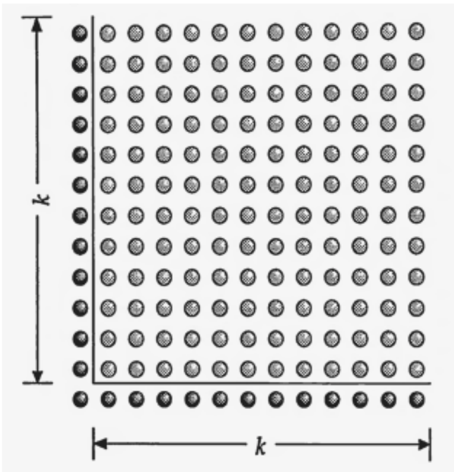


Figure 5.8

Let us consider any positive integer that is an odd square, and thus expressible as both h^2 and $2k+1$, for h and k appropriate positive integers. Then $k^2+h^2 = k^2+(2k+1) = (k+1)^2$ and we obtain a Pythagorean triple $(h,k,k+1)$ which is certainly primitive because $k, k+1$ are coprime. The preceding figure illustrates the construction: the inner square contains k^2 dots, the outer one $(k+1)^2$, the difference is given by the $k+k+1 = 2k+1$ dots on the edges. If their number is also a square, a primitive Pythagorean triple is determined. For example, from $9 = 3^2 = 2 \cdot 4+1$, then for $h = 3$ and $k = 4$, we obtain the primitive triple $(3,4,5)$.

Euclid proposes a more extensive and powerful method for generating arbitrary Pythagorean triples. He does so in Lemma 1 to Proposition 29 of the tenth book of *Elements* [44]. Translated into modern terms, his strategy consists of taking two positive integers $m > n$ and calculate:

$$\begin{cases} a = m^2 - n^2 & \text{(the difference of the squares)} \\ b = 2mn & \text{(the double product)} \\ c = m^2 + n^2 & \text{(the sum of squares).} \end{cases}$$

For example, for $m = 2$ and $n = 1$ we obtain by this way again $(3,4,5)$. But not every Pythagorean triple can be obtained in this way: not for example $(9,12,15)$ because it is easy to see that 15 cannot be represented as the sum of two squares. But all the primitive triples can be obtained in this way, provided that we take m,n coprime and with opposite parity. We will deepen this topic later, in Chapter 9.
The verification that a triple as before is Pythagorean can be done with an algebraic calculation that is neither difficult nor fascinating:

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 + n^4 - 4m^2n^2 + 2m^2n^2 = m^4 + n^4 + 2m^2n^2 = (m^2 + n^2)^2.$$

But one may prefer the following (vaguely without words) argument, devised in 1994 by David Houston [66]. We refer to the right triangle of catheti m and n, and hence of (possibly irrational) hypotenuse $\sqrt{m^2+n^2}$. Let θ be the acute angle opposite the cathetus of measure n.

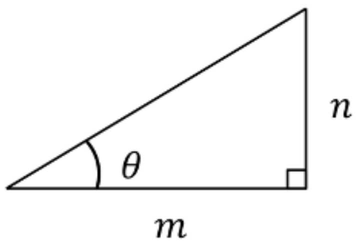


Figure 5.9

The trigonometric functions of θ are given by:

$$\begin{cases} cos\theta = \frac{m}{\sqrt{m^2+n^2}} \\ sin\theta = \frac{n}{\sqrt{m^2+n^2}} \end{cases}.$$

Turning to the double angle 2θ and using the trigonometric formulas of duplication we have

$$\begin{cases} \cos(2\theta) = (cos\theta)^2 - (sin\theta)^2 = \frac{m^2-n^2}{m^2+n^2} \\ \sin(2\theta) = 2sin\theta \cdot cos\theta = \frac{2mn}{m^2+n^2} \end{cases}.$$

Thus we have a right triangle whose catheti are $cos(2\theta), sin(2\theta)$ and hypotenuse 1. Multiplying by m^2+n^2 we obtain the given Pythagorean triple

$$(a,b,c) = \left(m^2-n^2, 2mn, m^2+n^2\right).$$

5.3 Applications to combinatorics

Several famous properties of natural numbers, and hence various laws of arithmetic, can be demonstrated without words. The basic idea is to represent every unity as a point, and thus every natural number n as n points, suitably arranged.

This also leads to the law (already considered and proved by induction) that the sum of the first n natural numbers is given by $T_n = \frac{n(n+1)}{2}$, so $1+2+\ldots+(n-1)+\ n = \frac{n(n+1)}{2}$.

This is the rule that the young Gauss would have derived at the age of 9. Carl Friedrich Gauss (Braunschweig 1777-Göttingen 1855) was one of the greatest mathematicians who ever lived. His contributions to science ranged from analysis to number theory, from statistics to differential geometry. According to his 1862 biography, *Memoir of Gauss* [123], by his colleague Wolfgang von Waltershausen (1809-1876), when Gauss was still a very young pupil, his teacher set him and his class the task of calculating the sum of the first 100 numbers, to try to keep the pupils, especially the more restless ones, occupied for a while. But Gauss solved the exercise in a few minutes, observing that the numbers in question, from 1 to 100, are divided (first to last, second to last but one, etc.) into 50 pairs with the constant sum $101 = 1+100 = 2+99 = 3+98$, etc. Thus the result is $50 \cdot 101$, i.e. $\frac{100\cdot 101}{2}$. Thus, in abstract mathematical symbols, we derive the formula already mentioned:

$$T_n = \sum_{i=1}^{n} i = 1+2+\ldots+n = \frac{n(n+1)}{2} \ .$$

A first proof without words of the law in question dates back to ancient Greece and is as follows:

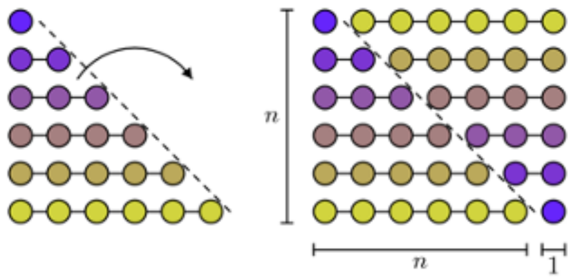


Figure 5.10

On the left the sum $1+2+\cdots+n$ is represented through the distribution of addends in n rows. On the right the sum is doubled, resulting in a rectangular distribution of points over n rows and $n+1$ columns. This results in $n(n+1)$ points. In conclusion $1+2+\ldots+n = \frac{n(n+1)}{2}$.
A second proof without words of the same property makes use of more sophisticated and recent tools, namely combinatorial calculus. Let us recall that, for $n > k$ positive integers, the binomial coefficient $\binom{n}{k}$ represents the number of possible ways in which it is possible to arrange the n elements (in this case points) in "slots", i.e. sets, of k elements.
Furthermore

$$\binom{n}{k} = \frac{n!}{(n+k)! \cdot k!} .$$

Let us now consider the figure: The addends of our sum are represented by n rows,

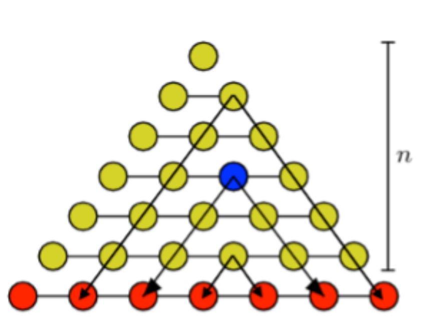


Figure 5.11

which in general form an equilateral triangle.
We add an additional red line, corresponding to $n+1$. Each unit of the addends from 1 to n (the "dot" in blue) is perfectly determined by a pair of dots in the red line, those that are reached by proceeding diagonally to the right or left. So the

dots in the first n rows are just $\binom{n+1}{2}$ and the sum is

$$\binom{n+1}{2} = \frac{(n+1)!}{(n+1-2)! \cdot 2!} = \frac{(n+1) \cdot n \cdot (n-1)!}{(n-1)! \cdot 2} = \frac{n(n+1)}{2}.$$

Another famous sum of arithmetic is that of the first n odd numbers, which coincides with the square of n, that is:

$$\sum_{i=0}^{n-1} (2i+1) = 1+3+5+\ldots+(2n-1) = n^2.$$

The equality is proved without words by the following figure. On the left is represented the sum of the odd numbers from 1 to $(2n-1)$, each on a single line (of n total lines). On the right, the same points that were previously in the rows fill a square of side n: they are therefore n^2.

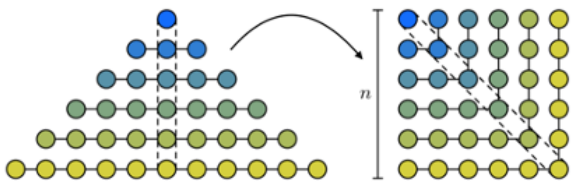


Figure 5.12

The sums $1+2+\cdots+n$ when n ranges over positive integers are called *triangular numbers* (as we already said, precisely because they can be represented as a triangle, in the way described above). Then $T_n = 1+2+\ldots+n$. Two laws that govern the sequence of T_n explaining recursively how each of its even or odd terms is derived from the preceding ones are the following:

a) $3T_n + T_{n-1} = T_{2n}$;

b) $3T_n + T_{n+1} = T_{2n+1}$.

Here is a proof without words of both.

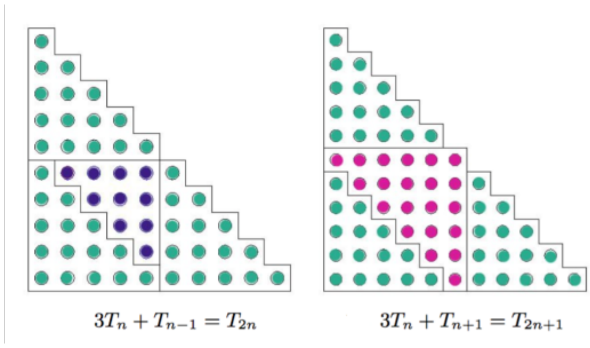


Figure 5.13

Triangular numbers are indispensable for the understanding of a fundamental result of number theory, the *Nicomachus theorem*, which owes its name to the ancient Greek mathematician Nicomachus of Jerash (ca. 60 - ca. 120), who was also the originator of the previous proof on the sum of the first n odd numbers. The theorem states that "the sum of the cubes of the first n natural numbers is equal to the square of the n-th triangular number", that is:

$$\sum_{i=1}^{n} i^3 = T_n^2 = \left(\sum_{i=1}^{n} i\right)^2 \quad \text{thus} \quad 1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2 .$$

This proof becomes evident if we consider the following figure:

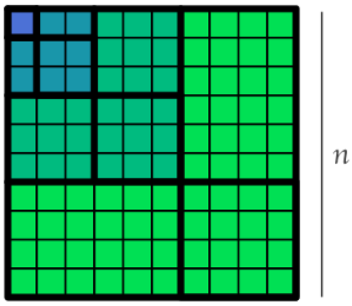


Figure 5.14

The differently coloured areas (dark blue, light blue, dark green, light green) that fill the square of side n (in the specific case 10) correspond to a number of squares that is given by the successive cubes $1, 8, 27, 64$. But along the edge, for example vertically, there are $1, 2, 3, 4$, the sum of which is precisely the triangular number $10 = T_n = 1 + 2 + 3 + 4$. So the same square is filled with $100 = 10^2$ squares.

Another famous arithmetic sequence is the Fibonacci sequence, proposed by the Pisan mathematician Leonardo Fibonacci (c. 1770-1242) in his *Liber Abaci* [134]. Its terms F_n are defined again by recurrence, with respect to a positive integer n, in the following way:

$$\begin{cases} F_1 = 1 \\ F_2 = 1 \\ F_n = F_{n-1} + F_{n-2} \ , \ \forall n \geq 3. \end{cases}$$

Thus we obtain the sequence 1, 1, 2, 3, 5, 8, 13, 21, 34,... . Fibonacci's number theory has been extensively studied. There are various laws, some surprising, that link them. Among them is the rule that states that the sum of the squares of the first n Fibonacci numbers is equal to the product of the last of them and the one immediately following it:

$$\sum_{i=1}^{n} F_i^2 = F_n \cdot F_{n+1} \quad .$$

This can be demonstrated numerically, by induction. Or one can consider the following figure, which represents the squares of the Fibonacci numbers 1, 1, 4, 9, 25, 64, 169, ... according to the definition of the numbers themselves. The rectangle that is progressively formed has the sides F_n (in this case 13) and F_{n+1} (i.e. 21). This leads to the following figure, which proves the equality mentioned above:

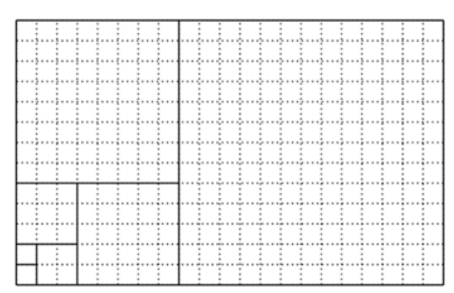


Figure 5.15

Another identity about Fibonacci numbers is the following, valid for any integer $n > 2$:

$$F_{n+1}^2 = 4F_n^2 - 4F_{n-2} \cdot F_{n-1} - 3F_{n-2}^2.$$

Here is a proof without words of it.

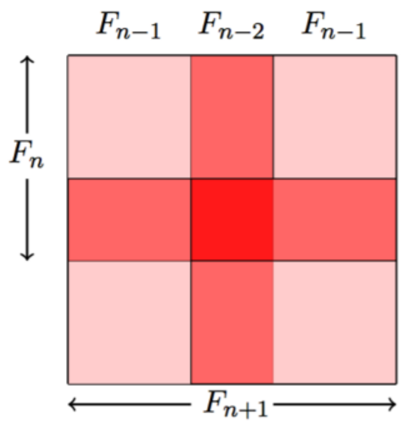


Figure 5.16

The large square in the figure has side F_{n+1}, so $F_n + F_{n-1}$. But in turn F_n is expressed as $F_{n-2} + F_{n-1}$. Thus the big square is made up of

- 4 small squares in pale pink, of side F_{n-1},
- the central square in red, of side F_{n-2},
- 4 rectangles in brighter pink, of sides F_{n-1} *and* F_{n-2}.

It can also be seen as the sum of 4 squares of side F_n from which, however, must be subtracted

- the 4 bright pink rectangles,
- 3 times the central red square (which in the above sum occurs 4 times).

Thus we arrive at the identity stated above for every integer $n > 2$:

$$F_{n+1}^2 = 4F_n^2 - 4F_{n-2} \cdot F_{n-1} - 3F_{n-2}^2.$$

5.4 Sums of convergent series

Mathematics, but also physics with the study of phenomena, is often faced with additions of an (e.g. countable) infinity of addends. One might expect that, if the addends are all positive, the sum is also infinite. But one realises that, surprisingly,

this sum sometimes has a finite value.
Let us consider, for example, the case of the so-called geometric series of ratio 1/2, i.e.

$$\sum_{n=1}^{\infty}\left(\frac{1}{2}\right)^n=\sum_{n=1}^{\infty}\frac{1}{2^n}=\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\dots$$

This is connected with the first of Zeno's paradoxes, the one, called "of the dichotomy", in which, having to travel a certain distance (let's say of length 1), one has to reach first half, then half of the remaining half, and so on. But the sum of the lengths of the infinite number of stages to be reached in this way (hence the result of the previous addition) is finite, and indeed equal to 1.
A demonstration without words can start from a square of side 1 and therefore also area 1. Let us divide it in half, as in the figure:

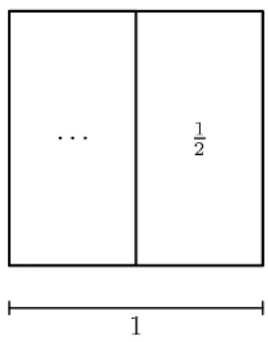


Figure 5.17

Each half will then have area 1/2 but can be divided in half. The procedure can be repeated indefinitely, as shown below:

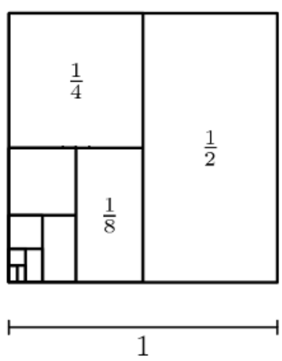


Figure 5.18

The sum of all these areas cannot exceed 1, since they are all contained in the starting square. In addition, each portion of the square will be involved sooner or later, so that we can conclude

$$\sum_{n=1}^{\infty}\left(\frac{1}{2}\right)^{n}=1 \ .$$

This proof was proposed in 1981 by the American mathematician Warren Page [85].

The fact that a geometric series of positive ratio r

$$\sum_{n=1}^{\infty} r^{n}$$

converges, i.e. has a finite sum, is true not only for $r = 1/2$ but also for any $r < 1$. Here is a wordless proof for $r = 1/3$, then for

$$\sum_{n=1}^{\infty}\left(\frac{1}{3}\right)^{n}=\sum_{n=1}^{\infty}\frac{1}{3^{n}}=\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+\frac{1}{81}+\dots$$

The figure referred to is:

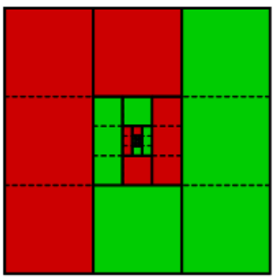


Figure 5.19

In detail
- again, consider a square of side 1 and so area 1;
- first divide it into 3 parts (corresponding to the 3 vertical stripes in the figure);
- colour the left strip (one third of the square) and the upper square of the central strip red, and the right strip and the lower square in the central strip green;
- repeat the colouring in the central square (one third of the central strip), but reversing the order of the colours;
- iterate the procedure.

It is clear that in the end the part coloured in red is half the square. But it is also made up of the sum of a third of the square, then a third of a third (i.e. a ninth), and so on. In conclusion:

$$\sum_{n=1}^{\infty}\left(\frac{1}{3}\right)^n = \frac{1}{2}\ .$$

Let us now turn to the geometric series of ratio $r = 1/4$, thus to:

$$\sum_{n=1}^{\infty}\left(\frac{1}{4}\right)^n = \sum_{n=1}^{\infty}\frac{1}{4^n} = \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \frac{1}{256} + \dots$$

One can proceed in a completely analogous way to the two previous examples starting from a square of side and area 1, as proposed by the American mathematician Sunday A. Ajose [1], namely:

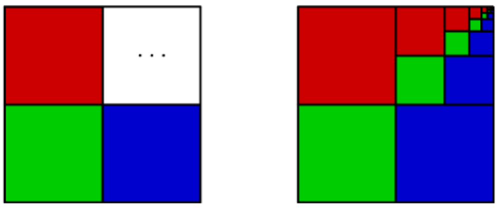


Figure 5.20

It can be seen that the total sum (corresponding to the green portion of the square) is 1/3 (the third part of the square, together with the other two red and blue parts). Or alternatively, consider an equilateral triangle of area 1 and proceed as follows:

- divide it into 4 equilateral pairwise congruent triangles;
- colour with different colours (red, green and blue) only 3 triangles and thus three

quarters of the starting triangle;
- divide the one triangle left blank into four more equilateral triangles;
- repeat the colouring in a similar manner;
- iterate the procedure.

It is clear that in the end the coloured parts are the third part of the starting triangle. But it is also made up of the sum of a quarter of the triangle, then a quarter of a quarter (i.e. a sixteenth) and so on. In conclusion:

$$\sum_{n=1}^{\infty}\left(\frac{1}{4}\right)^n=\frac{1}{3}$$

All this is illustrated by the following pictures:

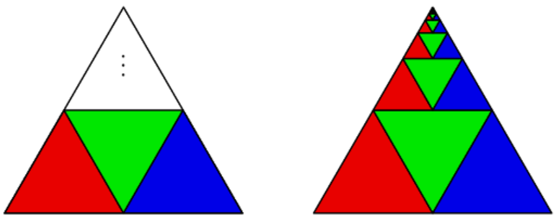


Figure 5.21

There is a law that generalises the 3 previous examples, valid for every ratio r with $0<r<1$. It states that the relevant series always converges to the sum that follows:

$$\sum_{n=0}^{\infty} r^n=\frac{1}{1-r}\ .$$

Warning: this time we start from $n=0$, so the series considered in the previous examples must be premised with an addend $r^0=1$, so that their results (increased by 1) become respectively $2, \frac{3}{2}, \frac{4}{3}$.
To show this more general result "without words", we start by drawing all the segments of length $r^0=1$, r^1, r^2, and so on, as in the next figure. On the segment $r^0=1$ we construct a square of side $r^0=1$. Draw a segment from the upper left vertex amnd this square and the right endpoint of the n-th segment of length r^n, again as in the figure below. conceived by the English mathematician John H. Webb and proposed in 1987 [125]. Suppose now n goes to $+\infty$.

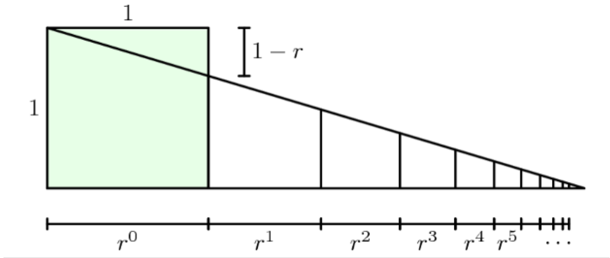


Figure 5.22

The diagonal segment determines two similar right triangles: the former is the one at the top with catheti 1 and $1-r$; the latter is the one at the bottom with catheti 1 and $\sum_{n=0}^{\infty} r^n$ (assuming that the geometric series converges). Then the following proportion holds:

$$(1-r) : 1 = 1 : \sum_{n=0}^{\infty} r^n$$

from which it follows that $\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}$.

Let us consider an analogous series,

$$\sum_{n=1}^{\infty} nr^n$$

It can also be written through a double summation:

$$\sum_{n=1}^{\infty} nr^n = \sum_{n=1}^{\infty} \sum_{i=n}^{\infty} r^i$$

Its convergence for $0 < r < 1$ is deduced from that of the previous series:

$$\sum_{n=1}^{\infty} \sum_{i=n}^{\infty} r^i = \sum_{n=1}^{\infty} r^n \cdot \frac{1}{1-r} = \frac{1}{1-r} \left(\sum_{n=0}^{\infty} r^n - 1 \right) = \frac{r}{(r-1)^2} \ .$$

A visualisation of this result, and a proof without words of it, is provided by the following figure, devised by the US mathematician Stuart Swain in 1984 and called “Gabriel’s staircase”. The reference is probably to the French architect Ange-Jacques Gabriel and a wing of the Palace of Versailles that he designed. The addend corresponding to $n = 0$ is also considered, but its role is completely irrelevant, because its value is $0 \cdot r^0$, i.e. 0.

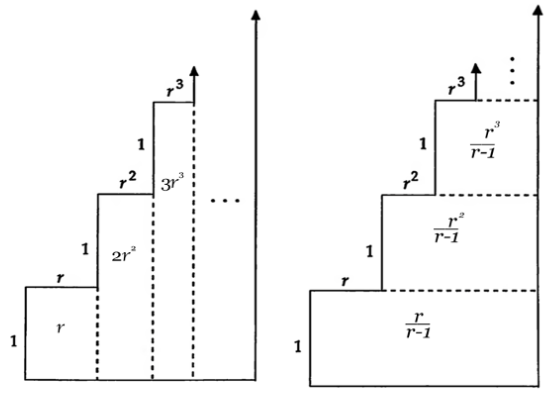


Figure 5.23

Let us comment on this proof without words. On the left we see the surface composed of the sum of rectangles of base r^n (always smaller for $0 < r < 1$) and height n, therefore of area nr^n. The total area of this figure is therefore given by the sum of the series under examination. But the same surface can be subdivided as on the right, into "horizontal" rectangles with the same height, and with base that:

- at the bottom is $r + r^2 + r^3 + \ \dots$ so $\frac{1}{1-r} - 1 = \frac{1-(1-r)}{1-r} = \frac{r}{1-r}$;

- followed in the same way by $\frac{r^2}{1-r}, \frac{r^3}{1-r}, \dots$ etc.

The area is then obtained as $\frac{r+r^2+r^3+\dots}{1-r} = \frac{r}{(1-r)^2}$, as indicated.

5.5 Logic and geometry in Leonardo da Vinci's imaginary

Leonardo da Vinci (1452-1519) also anticipated proofs without words in some sense. His approach to mathematics is in fact mainly visual, geometric and intuitive, and yet it succeeds in being effective and convincing, even from a didactic perspective. We find it developed in many of the figures (and their captions) in one of his most famous written works, *Codex Atlanticus (Atlantic Codex)* [73].
The first person to notice and emphasise in Leonardo these characteristics of a thought that is based and evolves on a logic of images was the French poet Paul

Valéry (1871-1945). Valéry, not unfamiliar with mathematical knowledge, dedicated an essay to the subject in 1894 entitled *Introduction to Leonardo da Vinci's method* [118]. In it he states, speaking of Leonardo:

"analogy is precisely the faculty of varying images, of combining them, of making the part of one coexist with the part of the other, and of discovering, voluntarily or involuntarily, the relations of their structures. This makes the intellect, which is their place, indescribable. There, words lose their virtue. They are formed, they leap before his eyes; it is he who describes the words to us. [...] For it is from there that amazing decisions, perspectives, dazzling intuitions, exact judgements, illuminations, and even stupidities, spring forth. [...] As I stated above, the phenomena of mental image production are very little studied. I remain firm in my conviction of their importance. I maintain, in fact, that certain laws, peculiar to these phenomena, are essential and, moreover, endowed with an extraordinary generality; and that the variations of the images, the restrictions imposed on these variations, the spontaneous productions of image-response or of complementary images, make it possible to reach worlds as absolutely distinct as those of dreams, states of ecstasy, and deduction by analogy".

Let us therefore delve into this lesser-known dimension of Leonardo's work, both because it exemplifies the potential of an approach to mathematics based on geometric intuition, and because it is rich in ideas and suggestions for good mathematics teaching.

In the *Codex Atlanticus*, Leonardo describes his project, presenting it as a sort of game, but demonstrating that he was well aware of the classic problem of squaring curved figures (i.e. constructing an equivalent square, perhaps with the tools of the rule and compasses).

We read in fact in folio 272 versus of a *"ludo geometrico"* (geometric game) *"in which the process of squaring surfaces of curved sides is given infinitely many times"*. And immediately afterwards: *"[...] The square is the end of all the labour of geometric surfaces. Every surface awaits its quadrature", which is "the end of geometric science"*.

Leonardo drew curvilinear or mixtilinear figures within a circle, colouring them or deleting them – thus highlighting them to underline his interest.

A caption indicates the procedure needed to obtain an equivalent square. The

pages of the *Codex Atlanticus* illustrate in a very comprehensible way the arguments Leonardo used to square his figures. At the base there are procedures for the duplication of geometric figures or, more generally, for constructing multiple figures with respect to one considered at the outset, all based on the Pythagorean theorem. Leonardo's intelligence was evidently struck by this theorem, whose intellectual beauty he probably admired, but also its fertility, i.e. its ability to combine meanings and images to generate new meanings and images. In this way, apparently difficult problems find an immediate solution.
Let us illustrate this by starting with perhaps the simplest and best known case: that of the duplication of an assigned square, i.e. the construction of a square with an area twice its own.

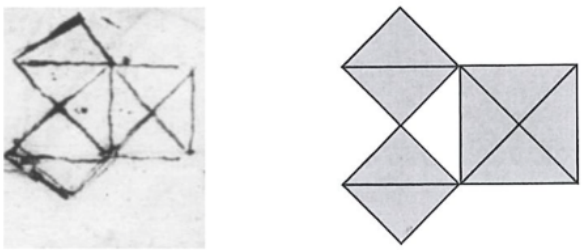


Figure 5.24

The drawings in the *Codex* deal with this problem, which is a simple application of Pythagoras' theorem to the case of the isosceles right triangle and is also the subject of a famous scene in Plato's dialogue *Meno* [98]. From the figure drawn by Leonardo, it is easy to understand that the square constructed on the hypotenuse contains four whole copies of the original triangle, which is contained twice in each of the two squares constructed on the catheti. There are no calculations or formulas, but the message is nevertheless very clear.
From the preceding drawing, another geometric property of great interest is also derived: if one wants to obtain an area twice that of an assigned square, one need only construct the square whose side is the diagonal of that square (regardless of the size of the side of the starting square).

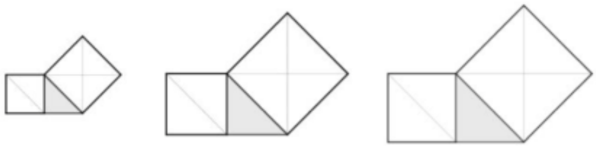


Figure 5.25

Leonardo then asks himself how to obtain a square that is any multiple of the original square. By using the previous construction, he manages to construct squares of triple area, quadruple area and so on. Each time, it is sufficient for him to consider a right triangle whose catheti measure respectively as

- the side of the initial square (say 1),
- the side of the square just constructed (therefore of area n).

Then the square on the hypotenuse of this rectangle triangle will have area $n+1$. In this way Leonardo obtains beautiful spirals that convey a sense of dynamism and at the same time aesthetic beauty thanks to the various aspects of regularity they possess (the search for regularity in a world with mostly irregularities was also a theme dear to Leonardo who was fascinated and almost obsessed by the golden ratio and its visual applications). In this setting, his drawing recalls an illustrious classical precedent, namely *Theodore's spiral*, on the right in the figure below.

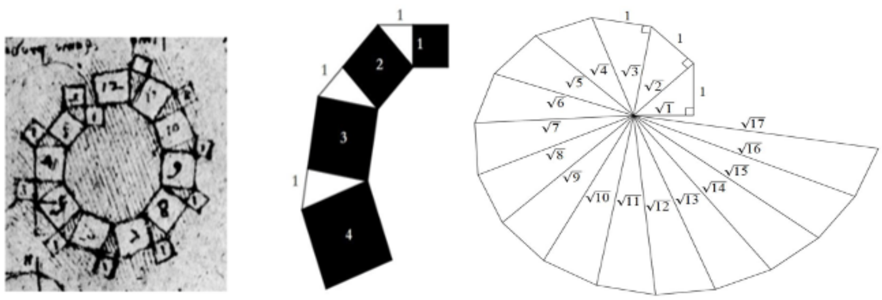


Figure 5.26

Examination of the *Code* also reveals a desire to determine a system for duplicating, in addition to squares, other figures such as circles or parts thereof. For these purposes it was evidently decisive for Leonardo to use a variant of Pythagoras' theorem valid for circles inscribed with squares constructed on the sides of a right triangle: in this case the diameters of the three circles are respectively equal to the sides of the squares.

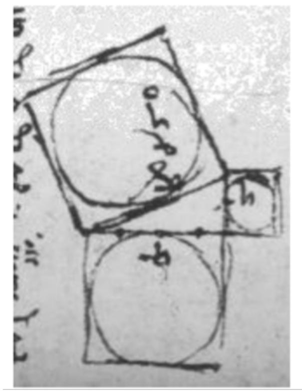


Figure 5.27

The circle whose diameter is the hypotenuse of a right triangle increases its area as the area of any one of the two circles constructed on the cathetus increases. It can also be seen that, similarly to what happens with squares, when the triangle becomes isosceles, the circle whose diameter is the hypotenuse is twice as large as the one whose diameter is one of the two catheti.

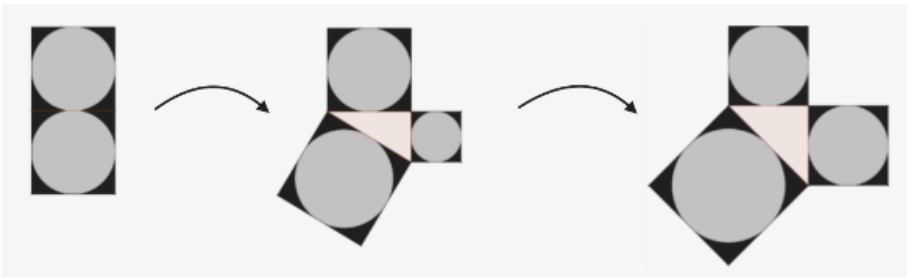


Figure 5.28

A simple reasoning confirms the property. We know in fact that the square constructed on the hypotenuse has double area than the one constructed on a cathetus. On the other hand, the area of the respective circles is obtained by halving the diameter, that is the side of the square, so that the area is divided by 4, and then multiplying by π. This is true for the hypotenuse as well as for any of the catheti. Thus the relation between the areas of the circles (one twice as large as the other) is preserved. In the following figure i, c denote the hypotenuse and the cathetus, respectively, and R, r the radii of the corresponding circles (equal respectively to half of i, c).

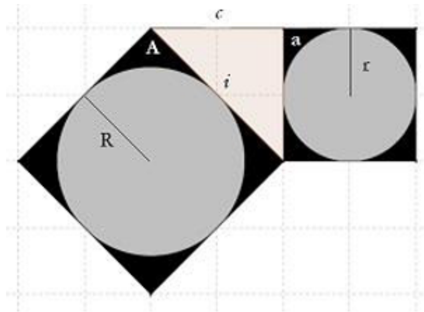


Figure 5.29

If the construction is iterated, it is possible to obtain, analogously to what happens with squares, a circle whose area is any multiple of that of the starting circle.

Something analogous still holds when we consider mixtilinear surfaces, for examples parts of circles: it is possible to construct others similar to them that have an area multiple of the original one. If in fact, observing the preceding figure, one subtracts the circle of greater area from the square in which it is inscribed and analogously for the circle of smaller area, one will see that the area of the mistilinear figure thus obtained in the first case is double that corresponding to the second. The mistilinear figures thus obtained are called interstices, and are represented by the letters A, a in the following figure.
The same obviously applies to the circular segments indicated in the figure by the letters B, b. Leonardo called them *portions*.

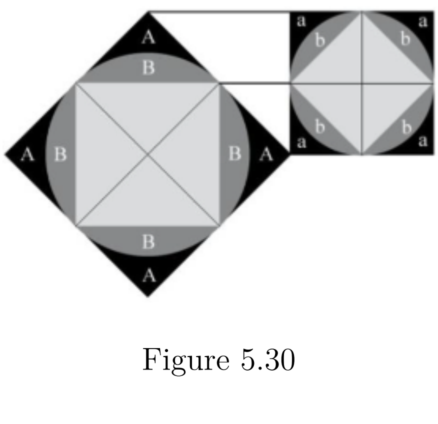


Figure 5.30

We also obtain results analogous to the Pythagorean theorem, but applied to interstices and portions.

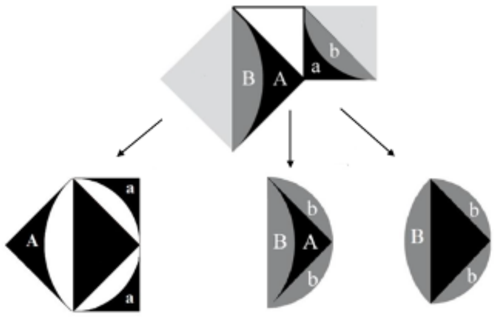


Figure 5.31

And again: by iterating the procedure, it is possible to construct spirals that have, at each step, interstices and portions of double the area of the figures obtained at the previous step.

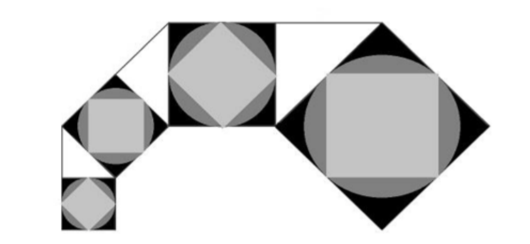


Figure 5.32

Thus, considering any square, the area of each of its interstices is double the area of an interstice belonging to the preceding square, and so on backwards. The same relation applies to portions and can be represented by the following graphic succession of "sums":

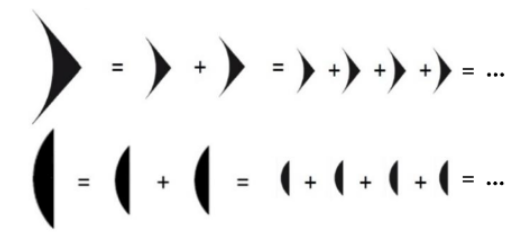


Figure 5.33

The relationship between similar figures inspired Leonardo to create many of the drawings found in the *Codex*. In particular, there is a mixtilinear figure that appears almost obsessively in the manuscript, the *lunula*. This was one of the first figures that could be squared with a ruler and compasses, constructing the side of a square with the same area. The result is attributed to Hippocrates of Chios (ca. 470-410 BC), a follower of Pythagoras.

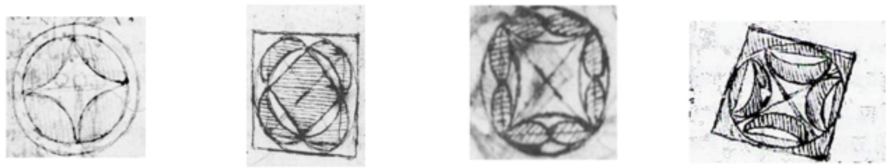


Figure 5.34

Let us first recall the context. Two secant circumferences are given, as in the following figure:

- the first (on the right) has centre P and radius $PR = PQ$,
- the second (left) has centre O and radius $OR = OQ$.

Therefore the points of incidence are R and Q.

The curvilinear surface that is obtained as the difference between the two circumferences consists of two parts, which are called lunulae.
To square, for example, the left one, let us consider the isosceles triangle PQR, which is rectangular, with P vertex of the right angle, because it is inscribed in the right semicircumference of the second circumference, that is the smallest in the figure. Then

- the right semicircle of the smallest circle is composed of the lunula and then of the circular segment of the greater circle denoted by B;
- the left semicircle, which has the same area, is composed of the triangle PQR and the two circular segments denoted b.

From Pythagoras' theorem for circular segments, we deduce that the two ones corresponding to b have together the same area as those of B. Moving on to the differences, we see that the lunula has the same area as the isosceles right triangle PQR and, through it, can be squared.

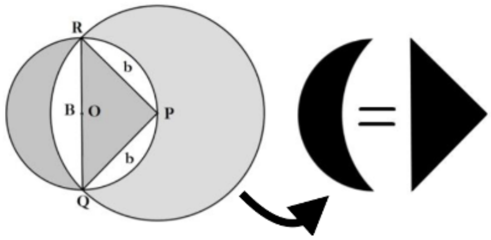


Figure 5.35

The equivalences highlighted by Leonardo's figures have a pedagogical value that can be defined as great. Consider the one we have just seen between the lunula and the triangle. This is a very simple example to understand but at the same time extremely formative in relation to the perceptual difficulties typically encountered in learning plane geometry.

In addition to all this, once again applying qualitative but rigorous arguments, it is even possible to make a comparison between the perimeters of the lunula and the diameter. It is enough to remember that the shortest path between two points is the rectilinear one to understand that the perimeter of the triangle will be surely smaller than the perimeter of the lunula. In fact RQ, as the chord of the greater circle, is smaller than the corresponding arc from R to Q. In the same way, with reference to the smaller circle, the chords $PQ = PR$ are smaller than the corresponding arc, that is of a quarter of the circumference, so that their sum is smaller than the semicircle from R to Q.

Examples of this kind help at least to reduce if not to eliminate the confusion that arises between the concepts of equality, equivalence and isoperimetry.

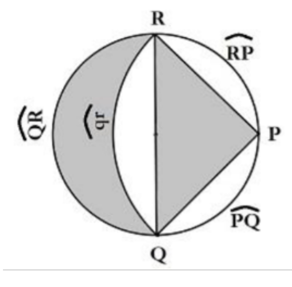


Figure 5.36

Leonardo himself illustrates the geometric transformations he performs in order to highlight the equivalences sought in the captions beneath the figures in the *Codex*. Exploring the meaning of these phrases provides interesting didactic ideas aimed at bringing to light the relationship between geometric design and logical deduction. Promoting these intuitive solutions makes it possible to solve problems that would otherwise require a considerable number of calculations difficult to manage.

Chapter 6

History and education of mathematical induction

6.1 Introduction

In the previous chapter we outlined a beautiful and elegant way to perform proofs of mathematical statements, without spending words or number, but just observing images that explain themselves. But often the mathematical reasoning relies on more articulated and rigorous tools, as in the case of the induction principle, already exemplified at the end of Section 5.1. The induction principle is powerful, sophisticated and sometimes brilliant, but not always easy for students to understand and apply. Proofs using it do require words, and even heavy calculations. But its foundation is still the son of intuition.

In fact, the idea that natural numbers follow one another from 1 (or 0, if you prefer) by adding each time 1 to the previous number, is relatively simple to conceive. It is another matter, however, to formalize this intuition in the principle of induction and especially to recognize it as the very foundation of natural numbers, as such a powerful tool for demonstrations concerning them. This did not happen until between 1888 and 1889, thanks to Dedekind and Peano. Nevertheless, pretty much consistent, and progressively more and more refined anticipations of it have been detected since antiquity.

The intent of this chapter is to review some of these foreshadowings, which on the one hand significantly intersect the history of science, philosophy and even litera-

ture, and on the other hand inspire exercises on induction itself, simple enough to propose in classrooms. We believe that these references can facilitate the understanding of the principle among students. Indeed the Italian Indicazioni Nazionali ([128], pp. 241 and 337) also underline its importance.
First let us recall here the assertion of the principle of mathematical induction. For simplicity, in this chapter we mean as natural numbers the numbers $1, 2, 3, \ldots, 0$ excluded - thus the positive integers. In this context the principle is formulated as follows:

a set of natural numbers which:

- contains 1,
- for any natural number n, if it includes n it also includes its successor $n+1$,

contains all natural numbers.

The principle of induction is then useful for introducing new concepts about natural numbers. We limit ourselves to the simple example of the factorial. For an arbitrary natural number N, N factorial, denoted $N!$, can be presented as the product of all natural numbers $\leq N$, therefore

$$N! = N \cdot (N-1) \cdot \ldots \cdot 2 \cdot 1.$$

But another way of defining it is to specify

- its value for $N = 1$,
- how to get the value for $N = n+1$ from that for $N = n$, for any n.

Then one puts:

- 1!=1,
- for each natural number n, $(n+1)! = n! \cdot (n+1)$ (in fact the product of the first $n+1$ natural numbers is obtained by multiplying that of the first n by the new factor $n+1$).

Therefore $2! = 1! \cdot 2 = 2$, $3! = 2! \cdot 3 = 6$, $4! = 3! \cdot 4 = 24$, $5! = 4! \cdot 5 = 120$ and so on.
The induction principle assures us that in this way the totality of natural numbers N is involved. Moreover on its basis one proves that there exists a unique function

defined by the previous conditions. We speak then, in this case and in all analogous ones, of ***definition by induction***. In the case of the factorial this approach sounds more elaborate than the former, but less vague, since it avoids the ellipsis, and, above all, more effective in the progressive computation of the factorial values.

The principle of induction is also very useful for proving statements about natural numbers. In fact, assume to have to prove a certain property for the totality of these numbers. It is enough:

(i) to obtain it first for $n = 1$,

(ii) then deduce it from a generic n to the next $n+1$.

In this way the property is transmitted from 1 to 2, from 2 to 3, from 3 to 4 and so on. Such a procedure is called ***proof by induction***. We will see several examples of this in the chapter. It does not exhaust the possible strategies to solve questions concerning natural numbers, because mathematics is open to the imagination; however, it proves to be an incisive and efficient tool. In it we distinguish two distinct moments: the *basic step* (i) and then the *inductive step* (ii). Both compose it, and both are indispensable for its success, even the basic one: if we did not know that the property holds for 1, we could not, with the sole use of (ii), extend it to 2, 3, etc.
The structure of a proof by induction is suitable for possible variations, depending on the case. For example, if one wants to prove a property of natural numbers greater than 1, one proves it for $n = 2$ (the basic step) and then transfers it from n to $n+1$ for every $n > 1$ (the inductive step). One may also prefer, in the inductive step, to move from $n-1$ to n rather than from n to $n+1$. Unfortunately these operations, if carried out too casually, can cause some bewilderment in the students.
In fact, there are many objective difficulties that students encounter in understanding the logical subtleties of the principle of induction, definitions by induction and proofs by induction, and which have already been extensively analyzed in the literature on mathematics education. Among these factors that disorient or lead to error, let us mention in the very statement of the principle

- the intrigue of "if" and "for each" overlapping in it ([50], [120], [16], [33]),
- the use of abstract variables,

and in proofs

- the apparent indeterminacy, already mentioned, with which the inductive step is formulated, sometimes from n to $n+1$ and sometimes from $n-1$ to n (are the two procedures equivalent?),
- the similar mutability of the basic step of the procedure, which is sometimes 1, sometimes, depending on the property to be proved, becomes 0, or 2, if not a more generic n_0 [43],
- an underestimation of this basic step, often and wrongly considered a pure formality [11], and the consequent incorrect identification between the proof by induction and its inductive step, which instead is one of its components.

The list does not end here, but we will discuss further reasons for confusion later.

One can trust, however, that the historical account of the ways through which the principle has gradually matured over the centuries, sometimes naive and imperfect, often lucid and ingenious, will simplify their understanding and instill in students the perception that mathematical laws, induction and not only, are never aprioristic and predetermined, but emerge and become clearer with time and reflection.

The precise and refined statement of the principle, its very naming (induction) and the rigorous formulation of the initial intuition are improved only with time, just as the awareness of its power develops as a reliable method of mathematical demonstration. Regardind the understanding of its key role in the definition of natural numbers, it emerges, as already mentioned, only in the late nineteenth century with Dedekind and Peano. A slow, almost millennial progress. Knowing it can only increase confidence with the principle and understanding of its many nuances.

This historical approach is not entirely new. We find traces of it, for example, within [41]. Here, however, we seek to pursue it systematically, addressing it to high schools teachers and, through them, to students: the hope is to inspire workshops, term papers and other activities on this sensitive topic. The most suitable year for the conduct of such initiatives seems to us to be the last one, when one can assume in students a greater maturity, a better predisposition to an overall view, the possession of a broader and more balanced knowledge of philosophy, history, and literature.

The plan of the chapter is, then, easy to sketch: from the perspective just described we investigate insights of mathematical induction, in order, in Plato, Euclid, Dante, Maurolico, Pascal, Wallis and Jacob Bernoulli, Euler, Gershon, Gauss, Bossut and Lalande, De Morgan, the Grassmanns and Peirce and, finally, Dedekind and Peano. We then take a similar but shorter route regarding the method of infinite descent, which is connected to induction. This time we go from the Pythagoreans again to Euclid, then to Campanus of Novara and finally to Fermat. After that, we briefly discuss the connection between the two principles, induction and infinite descent. Before we begin our exposition, we point out two classic, brief and clear references on the history of mathematical induction: [17] and [19], both of which can be found on the net.

6.2 Plato, and a first easy case

An early, simple trace of induction mathematics is discerned in a passage from [99]. The overall argument is as abstract as ever, as it examines and compares the concepts of "one" and "multiple". But within the dialogue, the main interlocutor, that is, the philosopher Parmenides, proposes the case of a series of objects contiguous, such as the squares arranged side by side in Figure 6.1. The purpose is to count their sides of contact.

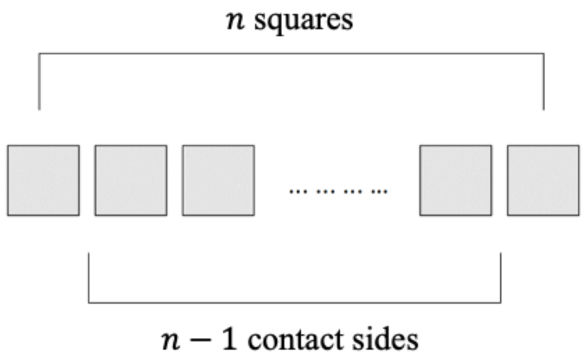


Figure 6.1

Let us then follow Parmenides' argument, according to [99], [136] (we follow here the latter reference).

- *Two things, then, at the least are necessary to make contact possible?*
- *They are.*

- *And if to the two a third be added in due order, the number of terms will be three, and the contacts two?*
- *Yes.*
- *And every additional term makes one additional contact, whence it follows that the contacts are one less in number than the terms*; ***the first two terms exceeded the number of contacts by one, and the whole number of terms exceeds the whole number of contacts by one in like manner; and for every one which is afterwards added to the number of terms, one contact is added to the contacts***.
- *True.*
- *Whatever is the whole number of things, the contacts will be always one less.*
- *True.*
- *But* ***if there be only one, and not two, there will be no contact***.

So, with today's eyes, we could say that Parmenides proves by induction that n squares imply $n-1$ contact sides. The basic step $n=1$ is treated in the punchline, the inductive one from n to $n+1$ in the previous passage, highlighted in boldface. Rearranging the details should be a simple exercise.

6.3 Euclid and prime numbers

Some commentators also detect some germ of induction in Euclid's famous proof of the infinity of primes: proposition 20 of the ninth book of [44]. Euclid lived a few decades after Plato. The proposition in question is rightly considered a milestone in the history of mathematical thought. As such, we feel it is fair to mention it to students. The way Euclid enunciates it is as follows:

Prime numbers are more than any assigned multiplicity of primes.

We could then rephrase it this way, without alterating its spirit too much:

For every positive integer n, there exist at least n prime number.

Euclid's argument can then been easily readjusted in terms of a proof by induction. The *base case*: if $n=1$, we need only to observe that there exists at least one prime number, say 2.

The *inductive step*: let us assume the statement true for some positive integer n and prove it for $n+1$. Suppose then that we have n distinct prime numbers, we must construct at least one new one. Let $p_1, p_2, \ldots, p_n$ be these primes, multiply them and add 1, obtaining $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Clearly $Q > 1$, so Q possesses at least one prime factor q. This q cannot coincide with any of $p_1, p_2, \ldots, p_n$, otherwise it divides their product and consequently the difference between Q and this product, i.e. 1, which is impossible. So q is the new prime sought.

In truth, Euclid in [44], while using in substance the previous argument, limits it only to the case of 3 prime numbers, thus to $n = 3$. Whether this already foreshadows the procedure of induction is a highly debatable question, to which we shall return. However, it may be useful to propose a few examples, perhaps precisely in the case $n = 3$, to illustrate that procedure.

- Applied to $2, 3, 5$ it yields $2 \cdot 3 \cdot 5 + 1 = 31$, which is prime.
- Applied to $3, 5, 7$ it yields $3 \cdot 5 \cdot 7 + 1 = 106$, which is not prime, but it decomposes into prime factors as $106 = 2 \cdot 53$ and admits as divisors the prime numbers $2, 53$ which are different from the starting ones.
- Applied to $2, 7, 11$ it yields $2 \cdot 7 \cdot 11 + 1 = 155$, which is not prime but decomposes into prime factors as $155 = 5 \cdot 31$ and admits as divisors the prime numbers $5, 31$ which are different from the starting ones.

6.4 A literary interlude: Dante

A hint, actually somewhat faint, of the principle of induction is also attributed to Dante Alighieri in the *Divine Comedy*, in relation to verses 55-57 of Canto XV of *Paradise* [2]:

Tu credi che a me tuo pensier mei
da quel ch'è primo, sì come raia
da l'un, se si conosce, il cinque e 'l sei.

Here is a translation in English:

Thou thinkest that to me thy thought doth pass
From Him who is the first, as from the unit,
If that be known, ray out the five and six.

The encounter between Dante and his ancestor Cacciaguida is recounted there. The latter, being among the blessed in Paradise, has the power to read the thoughts of others without the need to hear them. In fact, he can contemplate them in God, in whom they are perpetually present and from whom they are reflected. Similarly, Dante writes, relying on an arithmetical simile, all numbers, 5 and 6 in particular, are generated by 1. His verses thus manifest that intuition mentioned at the beginning of the note, about how natural numbers succeed each other starting from 1. The mathematical property intervenes, however, only as a poetic tool, without any didactic pretension: Dante does not intend to teach anything, but relies on this comparison to explain himself. Moreover, elsewhere in the Poem, Dante also employs mathematics as allegory. Anyway it cannot fail to strike one that even in the reading of the *Comedy* (which Italian students meet extensively in their high school years) one perceives some trace of induction.

6.5 Maurolico and odd numbers

Francesco Maurolico was a Sicilian mathematician and lived from 1494 to 1575. In his treatise *Arithmeticorum libri duo* of 1557 [78] he says that he wants to pursue new paths for the study of mathematics. Among them there is precisely the principle of induction. One of its applications, presented in [78], concerns the connection between odd numbers and squares - already noted in ancient times by Nicomachus of Jerash. Maurolico first observes:

Every square added with the odd number that follows produces the next square [proposition 13].

In modern notation: for every natural number n, the following holds

$$n^2 + (2n+1) = (n+1)^2.$$

This is precisely the property that progressive differences between two consecutive squares correspond to odd numbers: in detail

$$1^2 - 0^2 = 1 - 0 = 1, \quad 2^2 - 1^2 = 4 - 1 = 3, \quad 3^2 - 2^2 = 9 - 4 = 5,$$

$$4^2 - 3^2 = 16 - 9 = 7,\ 5^2 - 4^2 = 25 - 16 = 9,\ 6^2 - 5^2 = 36 - 25 = 11$$

and so on. Thanks to this, Maurolico deduces that:

From the sum of the odd numbers taken successively in order from unity, square numbers are constructed from unity, corresponding to the same odd numbers [proposition 15*].*

To put it again in today's way, for each natural number n it holds

$$1+3+\ldots+(2n-1) = \; n^2 :$$

the sum of the first n odd numbers coincides with the square of n, as is still confirmed by the examples: $1=1$, $1+3=4, 1+3+5=9$, $1+3+5+7=11$ and so on. This is the same result proved by Figure 5.12 in Section 5.3 without words involving triangular numbers. Here is how Maurolico deduces this statement from the previous one, using induction and not any figure.

In fact, by the previous proposition [the 13], to begin, the unit with the following odd makes the following square, that is, 4*. And the same* 4*, the second square, with the third odd, that is,* 5*, makes the third square, that is,* 9*. Likewise* 9*, the third square, with the fourth odd, that is,* 7*, makes the fourth square, that is,* 16*.* ***And so to infinity****, we prove the objective by repeating the use of proposition* 13.

So Maurolico examines odd numbers up to 7 and squares up to 16, and there he stops. However, the final expression «And so to infinity» («Et sic deinceps in infinitum» in the original Latin text) foreshadows subsequent behavior and insinuates applications that go well beyond 7 and 16. A rigorous mathematician of our times would prefer more general, abstract and conclusive arguments. However, the germ of the idea is very present.

The topic can certainly be proposed to students, perhaps with a form similar to Plato's one.

6.6 Pascal and the arithmetic triangle

Blaise Pascal was not only a mathematician and physicist, but also, in his own way, a computer engineer (inventor and promoter of the calculating machine named in his honour Pascalina), and moreover a philosopher, mystic and writer. In his *Traité du triangle arithmétique* of 1657, he describes the construction that in Italy is called Tartaglia's triangle, but in France is attributed to him (Pascal's treatise on the arithmetic triangle can be found, in the original French language, in [88]). It is therefore referred to as Pascal's triangle. However, to avoid any controversy over its presumed paternity, we shall call it the arithmetic triangle. Here it is in its most familiar version (Figure 6.2).

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1

Figure 6.2

The image that Pascal proposes in his treatise is essentially the same, except that the lines in the previous diagram become the diagonals running from left to right and from bottom to top (Figure 6.3).

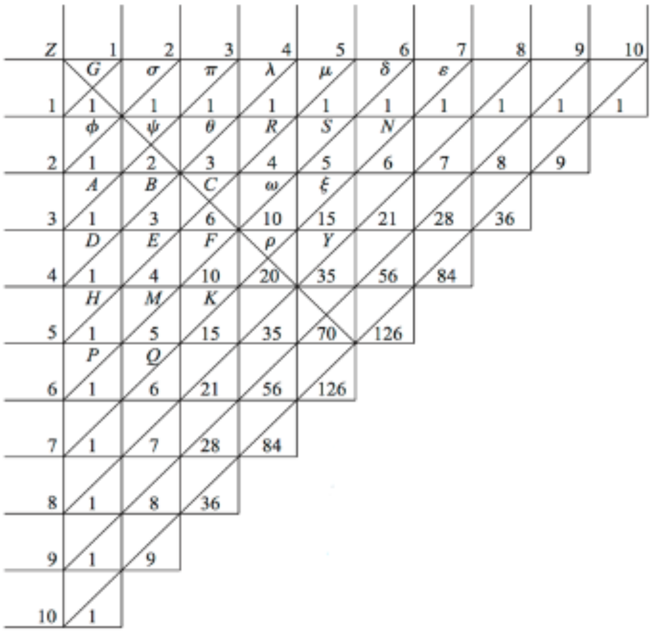


Figure 6.3

Pascal then lists various propositions (he calls them "consequences") about the elements of this triangle. The twelfth, translated into modern terms and referring to Figure 6.2, thus not Pascal's one, states: within the arithmetic triangle

> the ratio between two consecutive elements that meet going from left to right along a line

equals

> that which exists between the order numbers of the diagonal from the right in which the first element stands and that coming from the left in which the second element stands.

This is a difficult statement to read and understand, but we will try to explain it with a few examples.

- If we consider the elements $6, 4$ of the fifth line, we can note that the first one is in the third diagonal from the right, the second one in the second diagonal from the left, and in fact the proportion $6\colon 4 = 3\colon 2$ applies.
- Similarly, if we take the elements $20, 15$ of the seventh line, we can note that the first one is in the fourth diagonal from the right, the second in the third from the left, and in effect we have $20\colon 15 = 4\colon 3$.

Pascal asserts that this law applies in all generality. However, what is important for us is not the combinatorial result he wants to achieve (worthy of attention, but perhaps too difficult for high school students), but the way he organises his proof. Here is what he says on the subject - we adapt his original text slightly to Figure 6.2 to make it easier to read.

> *Although this proposition* [the property that is to be proved] *has an infinity of cases, a very short demonstration of it will be given, assuming two lemmas.*

> *The first one, which is self-evident: that this proportion is found in the second line* [whose elements are $1, 1$ and are respectively in the first diagonal from the right and the first diagonal from the left, so that the proportion to be satisfied is $1 : 1 = 1 : 1$, which is trivially true].

The second one, that if this proportion is found in any line, it is necessarily found in the following line. From which we see that it is necessarily in all the lines; for it is in the second line for the first lemma; and then for the second it is in the third line, then in the fourth, and infinitely.

So, we would say today, Pascal fully describes the structure of a proof by induction, both the basic and the inductive steps, to apply it to the lines of the triangle in Figure 6.2, starting with the latter as the initial case.
Let us add that, with regard to this strategy of induction, Pascal makes no mention whatsoever in his treatise of Francesco Maurolico, who preceded him by more than a century. However, he shows elsewhere that he is familiar with his work [78] - we shall see later why - so much so that he mentions it in the famous letter he sends under the pseudonym of Dettonville to his mathematician colleague Pierre de Carcavi, the main subject being the cycloid [89].

6.7 John Wallis and pyramidal numbers

One of the first exercises proposed to students in order to accustom them to the use of induction concerns the value of the sum of the first n natural numbers, $1+2+\ldots+n=T_n$, as n varies, hence the so-called n-th triangular number (already encountered in Section 5.3). The famous case of $n=100$, for which we obtain

$$1+2+\ldots+100=5050\ ,$$

as announced at the beginning of Section 5.3, is the result that Gauss (is said to have) arrived at in a few minutes at the age of nine. We also saw that the conclusion extends to every possible n, in the form:

$$1+2+\ldots+n=\frac{n\cdot(n+1)}{2}\ .$$

In Section 5.3 we proposed the Gauss demonstration as an example of proof without words. In Section 5.1 we gave the proof by induction, indeed less direct and brilliant, and more laborious. Anyway it is advisable to present and compare the two methods in classroom, also to lead students to reflect on the variety of possible solution approaches to mathematical problems. We will return to this topic in the section on Poincaré. Here we can add that Gauss's strategy was probably already known to the ancient Greeks and had also been employed by Maurolico in proposition 7 of the first book of [78]. The Sicilian mathematician formulated the result in this way:

each natural number n, multiplied by the next, gives as a product twice the corresponding triangular number.

In modern terms, $n\cdot(n+1) = 2\cdot(1+2+\ldots+n)$. Maurolico, instead of $n = 100$, had examined the easier case $n = 4$, for which $4\cdot 5 = 20$ and $1+2+3+4 = 10$. He had observed that by successively adding the four addends $1,2,3,4$ with themselves, but in the opposite order, i.e. with $4,3,2,1$ respectively, the common sum $5 = 1+4 = 2+3 = 3+2 = 4+1$ was obtained four times, so that the overall sum was $20 = 4\cdot 5$.
It is precisely this proposition of Maurolico that Pascal mentions in his letter to Carcavi, enunciating it and then attributing its demonstration to the Italian mathematician [89], p. 16.

Let us now consider a similar question: to calculate for each positive integer n the sum of the first n squares, i.e. the so-called n-th *pyramidal number*. Another classical application of induction, more challenging than the previous one, proves that

$$1^2+2^2+\ldots+n^2 = \frac{n\cdot(n+1)\cdot(2n+1)}{6} = \frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6} \qquad (*).$$

Thus the sum of the first 100 squares is $\frac{100\cdot 101\cdot 201}{6} = 50\cdot 101\cdot 67 = 338350$. If this example seems too complicated, here are a couple of simpler ones.

- For $n = 3$, $1^2+2^2+3^2 = 1+4+9 = 14$ and in fact $\frac{3\cdot 4\cdot 7}{6} = 14$.
- For $n = 4, 1^2+2^2+3^2+4^2 = 1+4+9+16 = 30$ and in fact $\frac{4\cdot 5\cdot 9}{6} = 30$.

However one may reasonably wonder how these example can lead to devise the general law $(*)$, which is certainly more elaborate and less intuitive than the previous one on triangular numbers.
The question about pyramidal numbers was considered by the English mathematician John Wallis (1616-1703) in proposition XIX of his 1656 treatise *Arithmetica Infinitorum* [122], p. 15. To be precise, Wallis compared the sum of the first n squares with the product $n^2(n+1)$, trying to evaluate their ratio

$$\frac{1^2+2^2+\ldots+n^2}{n^2\ (n+1)}\ .$$

Observe how for triangular numbers a similar comparison between the sum $1+2+\ldots+n$ and the product $n(n+1)$ leads to the constant ratio $\frac{1+2+\ldots+n}{n(n+1)} = \frac{1}{2}$.

Wallis explicitly calculated the above fraction for values of n from 1 to 6. If with a little patience we perform the same computations, we obtain respectively:

- for $n = 1$, $\frac{1}{1\cdot 2} = \frac{1}{2} = \frac{3}{6} = \frac{3}{6} = \frac{2}{6} + \frac{1}{6} = \frac{1}{3} + \frac{1}{6} = \frac{1}{3} + \frac{1}{6\cdot 1}$,
- for $n = 2$, $\frac{1+4}{4\cdot 2} = \frac{5}{12} = \frac{4}{12} + \frac{1}{12} = \frac{1}{3} + \frac{1}{12} = \frac{1}{3} + \frac{1}{6\cdot 2}$,
- for $n = 3$, $\frac{1+4+9}{9\cdot 4} = \frac{14}{36} = \frac{7}{18} = \frac{6}{18} + \frac{1}{18} = \frac{1}{3} + \frac{1}{18} = \frac{1}{3} + \frac{1}{6\cdot 3}$,
- for $n = 4$, $\frac{1+4+9+16}{16\cdot 5} = \frac{30}{30} = \frac{3}{8} = \frac{9}{24} = \frac{8}{24} + \frac{1}{24} = \frac{1}{3} + \frac{1}{24} = \frac{1}{3} + \frac{1}{6\cdot 4}$,
- for $n = 5$, $\frac{1+4+9+16+25}{25\cdot 6} = \frac{55}{25\cdot 6} = \frac{11}{5\cdot 6} = \frac{11}{30} = \frac{10}{30} + \frac{1}{30} = \frac{1}{3} + \frac{1}{30} = \frac{1}{3} + \frac{1}{6\cdot 5}$,
- for $n = 6$, $\frac{1+4+9+25+36}{36\cdot 7} = \frac{91}{36\cdot 7} = \frac{13}{36} = \frac{12}{36} + \frac{1}{36} = \frac{1}{3} + \frac{1}{36} = \frac{1}{3} + \frac{1}{6\cdot 6}$.

Wallis found that, at least in these first six cases, the ratio is greater than $\frac{1}{3}$ but gets closer and closer to it, because the difference corresponds to $\frac{1}{6n}$. From this examination he thought he could deduce, as indeed he did, that as n increases, the difference tends to 0 and so the ratio tends to $\frac{1}{3}$.
He might even have conjectured that, for every positive integer n,

$$\frac{1^2 + 2^2 + \ldots + n^2}{n^2\ (n+1)} = \frac{1}{3} + \frac{1}{6n} \ ,$$

or

$$1^2 + 2^2 + \ldots + n^2 = \frac{n^2\,(n+1)}{3} + \frac{n\,(n+1)}{6} \ ,$$

an identity which corresponds perfectly to (*): in fact it is easy to see that

$$\frac{n^2\,(n+1)}{3} + \frac{n\,(n+1)}{6} = \frac{2n^2\,(n+1) + n\,(n+1)}{6} = \\ = \frac{(n+1)(2n^2+n)}{6} = \frac{n(n+1)(2n+1)}{6} \ .$$

But Wallis's story interests us not so much for these calculations (avoidable in the classroom), but for another reason. «*Fiat investigatio per modum inductionis*», he writes at the beginning of his exposition. On this occasion, therefore, he explicitly uses the term *induction*. However, one may ask: is it reasonable to stop, as he does, at the first six natural numbers in order to deduce a property valid for every natural? Is his procedure the same one we have called "proof by induction"? Or isn't it rather a generalization suggested by a few examples, by some insistent basic steps, but without a serious inductive step and therefore somewhat rash? It is true that after proposing his six examples, Wallis adds «*et sic deinceps*», i.e. «and so on». But it is not easy to see how his calculations generalise *in infinitum*. Euclid also stops at case 3, and Maurolico at the value 4, of which 16 is the square. But their reasoning suggests how to proceed in general. The computations of Wallis, no.

His approach thus appears unjustified at least in our eyes, and in truth not only in ours: he received various criticisms on these grounds from great mathematicians of his time and shortly thereafter, including those of Jacob Bernoulli (1655-1705), who disapproved of him both in a 1686 note in the *Acta Eruditorum* and in his work (published posthumously in 1713) *Ars Conjectandi*. Both can be found on archive.org: the page to refer to is, in the former case, 282 in volume 1 of the 1744 edition of the works [12] and in the latter, page 95 of the original 1713 edition [13].

Bernoulli reproached Wallis for having limited his investigation to checking a few examples, without developing it with generality and rigour, proving for each n the transition from n to $n+1$.
As for the other question raised - are there alternative proofs of the identity $(*)$, more brilliant and convincing, as is the case with triangular numbers? - the answer is yes. We cite in this respect the wordless proof independently devised by Martin Gardner and Dan Kalman and referred to in [82] at page 78: certainly more elaborate than the triangular numbers, but effective and ingenious.

Let us add that the law $(*)$ was already known to the ancient Greeks. Archimedes enunciates it and then adopts it in his treatise *On conoids and spheroids* (lemma at proposition 2, p. $107-109$ in [3]); the argument he follows in his proof, however, does not seem to contain a trace of induction.

6.8 Euler

To underline the naivety of Wallis' approach, we turn to Leonhard Euler (1707-1783), one of the greatest mathematicians in history. We consider in particular a short letter addressed to a Bernoulli and numbered $E461$ in the index of Eulerian works edited by the Swedish mathematician Gustav Eneström [47]. Who the addressee Bernoulli is, the text does not make clear, but he can probably be identified with Johann

III, grandson of the first and more famous Johann. The letter presumably dates from 1772. In the final lines, Euler points out the singular case of the polynomial x^2-x+41, emphasising that, for every integer n from 1 to 40, the corresponding value n^2-n+41 is prime. For example

- $1^2-1+41=41$ is prime,
- $2^2-2+41=43$ is prime,
- $3^2-3+41=47$ is prime,

and so on, until $40^2-40+41=1601$.

Students can check the intermediate values with the help of a calculator. However, we anticipate the answer: the numbers that are obtained, all of them prime, are in the order $41,43,47,53,61,71,83,97,\ 113,131,151,173,197,223,251,281,313,347,383,$ $421,461,503,547,593,641,691,743,797,853,911,971,1033,1097,1163,1231,1301,1373,$ $1447,1523,1601$.

However, are these 40 affirmative examples (a far larger sample than the 6 considered by Wallis) sufficient to conclude that for every natural number n, n^2-n+41 is prime? Certainly not, because at the very next step we encounter

$$41^2-41+41=41^2$$

which is obviously a composite number. Remember that verifying an even large number of examples, is completely different from finding a general proof valid for every n : 40 is a relatively large threshold, certainly greater than 6, but natural numbers are infinitely many.

Let us add three curiosities about Euler's observation.

1. First, there are other primes of the form n^2-n+41 for values of $n>41$, e.g. already $43^2-43+41=1847$.

2. One may ask what happens if one inserts another positive integer N instead of 41 : to what extent does the sequence of values of the polynomial x^2-x+N, when x varies between the natural numbers, consist of only prime numbers? The question can be posed to the students for their consideration.

We note however that for $x = 1$ we have $1^2 - 1 + N = N$, from which we deduce that we must restrict the analysis to $N = 1$ or N prime, otherwise the initial value of the sequence is already composite.
Furthermore, for $N = 1$ the next values obtained are 1,3,4,... and thus already at the third step include composite numbers.
Let us assume then that N is prime. We observe that, as for 41, for $x = N$ we obtain

$$N^2 - N + N = N^2$$

which is evidently composite. It then remains to consider the intermediate values from 1 up to $N - 1$. The prime numbers N for which, in the same way as for 41, all values of $n^2 - n + N$ for $1 \leq n < N$ are primes are called *lucky Euler primes*. However, there are very few of them, just six, namely $2, 3, 5, 11, 17$ and 41 : a result that is by no means simple to prove.

3. Some people attribute to Euler the examination of the polynomial $x^2 + x + 41$ instead of $x^2 - x + 41$, which thus differs in the sign of x. Concerning this new polynomial, we observe that, this time, for $0 \leq n < 40$ we obtain prime values of $n^2 + n + 41$, while

$$40^2 + 40 + 41 = 40 \cdot (40 + 1) + 41 = 40 \cdot 41 + 41 = 41 \cdot 41 = 41^2$$

is composite. Actually, the example is essentially the same as the previous one, because the second polynomial can be obtained from the first by changing the variable from x to $x + 1$: in detail

$$(x+1)^2 - (x+1) + 41 = x^2 + 2x + 1 - x - 1 + 41 = x^2 + x + 41.$$

Thus, the two polynomials assume the same images, except that the value of the indeterminate x in the second case is decreased by 1.

6.9 Levi ben Gershon, cubes and permutations

Let us go back in time, to Dante's epoch to be precise. Levi ben Gershon - also known by his Graecised name Gersonides - lived at that time from 1288 to 1344, worked in southern France, was a major exponent of medieval Jewish thought, a philosopher, theologian, astronomer and also mathematician.
His treatise *Maasei Hoshev* is dated 1321, the same year as Dante's death. The title

comes from the *Bible*, Exodus, 26, 1, specifically from the passage in which God instructs Moses on how to build his sanctuary, recommending an «artist's work»: such is the translation of *Maasei Hoshev* according to the Jerusalem Bible, but the expression can also be rendered in a more mathematical way, as «*the art of the calculator*».

The book consists of 68 propositions and then the discussion of various problems. The contribution to the history of mathematical induction is conspicuous, as the article [104] points out. Gershon calls the procedure "*growing step by step*". He uses it to solve some questions, including the following two, which again could reasonably be proposed as exercises to nowadays students. However, they seem less elementary than many dealt with so far, which is why they have been postponed to now. They are respectively: the sum of cubes and the number of permutations.

We have already considered triangular numbers (the sums of the first natural numbers) and pyramidal numbers (the sums of their squares). The next step is to deal with sums of cubes. The following identity, valid for every natural number n applies to them (generally known as Nicomachus theorem, as pointed out in Section 5.3, whose proof without words is proposed in Figure 5.14, such as those presented on pages 84-89 of [82]; this time they seem more elaborate and less intuitive, only because of the greater difficulty of the situation to be faced):

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2 \qquad (**) \ .$$

Therefore the sum in question coincides with the square of the n-th triangular number, and thus also with $\frac{n^2 \cdot (n+1)^2}{4}$.

Proposition 41 of *Maasei Hoshev* considers precisely this argument. It focuses on the square of the sum of the first n natural numbers. It proves that, for $n > 1$, the difference between this square and the previous one, relating to the sum of the first $n-1$ numbers, is equal to the cube of n. Thus in modern notation

$$(1 + 2 + \ldots + (n-1) + n)^2 - (1 + 2 + \ldots + (n-1))^2 = n^3.$$

For example

- $(1+2)^2 - 1^2 = 9 - 1 = 8 = 2^3$,
- $(1+2+3)^2 - (1+2)^2 = 36 - 9 = 27 = 3^3$,
- $(1+2+3+4)^2 - (1+2+3)^2 = 100 - 36 = 64 = 4^3$,

- $(1+2+3+4+5)^2-(1+2+3+4)^2=225-100=125=5^3$

and so on.

From this, Gershon deduces that the square of the sum of the first n natural numbers coincides precisely with the sum of their cubes, as we already know:

$$(1+2+\ldots+n)^2=1^3+2^3+\ldots+n^3$$

for every positive integer n. In fact, the square in question differs by n^3 from the one relating to $n-1$, which in turn differs by $(n-1)^3$ from the previous one, and so on, up to the base case $n=1$, for which $1^2=1=1^3$ obviously applies. It is therefore sufficient to add member by member the equalities obtained above on the individual cubes, from 1 up to n.

This is therefore the same reasoning as Maurolico's one for the sum of the first n odd numbers. In fact, Maurolico also deals with the question of cubes in propositions 57 and 58 of [78]. It should be noted, however, that Gershon limits his "proof by induction" to $n=5$, thus making use of precisely the equalities explicitly given above as an example. On the other hand, his procedure is clearly generalisable and well outlined. In the case of 5, one can easily check that:

$$(1+2+3+4+5)^2=15^2=125=1+8+27+64+125=1^3+2^3+3^3+4^3+5^3.$$

Let us add that an inductive approach to the proof of identity $(**)$ was pursued, before Gershon, by the Persian mathematician Al-Karaji (953-1029), who deduced it for $n=10$. Gershon's treatment, however, seems more mature and conscious.

The other classic question considered by Gershon concerns combinatorial calculus, and specifically the number of possible permutations on n objects, for integer $n>1$. In his proposition 63, he proves that by increasing the number of objects by 1, thus from n to $n+1$, the number of permutations is obtained by multiplying the previous value by $n+1$. In other words, if for every integer $n>1$ we denote by P_n the number of permutations on n objects, then we have for every such n:

$$P_{n+1}=(n+1)\cdot P_n.$$

Starting from this consideration and from the easy observation that the permutations on 2 objects are 2, i.e. $P_2=2$, Gershon deduces that, for each $n>1$, the number of permutations on n objects is given by the product of all integers from n up to 1, that is, $n!$; thus

$$P_n = n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 \qquad (***).$$

In detail, Gershon firstly observes that $P_2 = 2 = 2!$, from which he then deduces that $P_3 = 3 \cdot P_2 = 3 \cdot 2! = 3!$, and so on for higher values of n. Actually, he stops at $n = 5$ also this time, but it is clear that the procedure extends to the higher integers "*ad infinitum*".

Moving on to today's students: the proposal of a few initial examples, which also clarify the non-trivial concept of permutation, can inspire them with the general law, which, following Gershon's approach, they can prove by induction.

However, even in this case it will be useful to compare this possible strategy with the following one, which avoids the use of induction. It can be seen (perhaps starting from small values of $n = 2, 3, \ldots$) that every permutation of n objects remains perfectly determined

- by the value it associates with the first, and which it can choose in n distinct ways,
- then by the value it associates with the second and which can choose in $n-1$ distinct ways, those remaining after the choice of the first,
- then again by the value it associates with the third and which it chooses in $n-2$ distinct ways, those remaining after the choice of the first two,

and so on, until the image associated with the last object, which will obligatorily coincide with the only one left available.

Thus, there are altogether $n!$ possibilities of choice, and consequently as many permutations.

6.10 Gauss

We have already recounted Gauss' feat as a schoolboy on triangular numbers. A few years later, in 1796, he obtained the proof of one of his most famous theorems, a property of prime numbers (to be precise, of pairs of distinct odd prime numbers) that is called *law of quadratic reciprocity*: too complicated to be referred to here. Let us simply say that Gauss himself celebrated it as the «*gem of higher arithmetic*». He showed it when he was still very young: when, after months of work, he completed his first proof, he was not yet nineteen years old, in fact he noted that he had completed it on the 8th April of that year 1796, while he would have celebrated his birthday on the 30th of the same month. From then and 1818 he obtained 5 more different proofs of the same law, and 2 more were found after his death and appear in his posthumous writings.

The law of quadratic reciprocity is set out and discussed in full in section 4 of the famous treatise *Disquisitiones Arithmeticae*, which Gauss composed in 1801 [55]. It is stated in article (as if said paragraph) 131 of this work, after which the following articles present the above proof, which uses precisely a method of induction. In fact, Gauss first face and positively solves the "simplest" cases, those involving the smallest odd primes, and then goes on to write in article 136 more or less like this: let us assume that the law is not valid in general, then it would be valid for pairs of primes less than or equal to a certain positive integer n, and no longer for pairs of primes less than or equal to $n+1$. Gauss then continues his argument, deducing a contradiction from these premises. He thus proves how the law is transmitted, in the sense just described, from n to $n+1$.

Impossible to go into detail here, as already mentioned. In any case, the fact that such an illustrious mathematician used the method of induction in one of his most celebrated theorems undoubtedly impressed his colleagues, increasing their interest in that principle.

6.11 Bossut, Lalande and the powers of a binomial

However, we read in [19] that even at the beginning of the 19th century, the term "*induction*" was used in the mathematical sphere in a vague and undefined way, meaning both the more naive way in which Wallis understood it and the more mature way of Bernoulli. To confirm this ambiguity, we cite the names of Charles Bossut (1730-1814) and Joseph Jérôme Lalande (1732-1807), who were respectively a mathematician and abbot, and an astronomer and freemason, and both cooperated in Diderot and D'Alembert's encyclopaedic project. Among the entries in the *Encyclopédie méthodique* [40] there is one dedicated to induction, on page 207 of the second volume. Bossut and Lalande are said to have compiled it. In their commentary, however, they restrict themselves to one example, although famous: the binomial theorem, i.e. the formula that expresses the powers of a binomial $(x+a)^m$ (with m being a positive integer) as the sum of monomials in the decreasing powers of x and increasing powers of a. For example:

$$(x+a)^1 = x+a,$$

$$(x+a)^2 = x^2+2ax+a^2,$$

$$(x+a)^3 = x^3+3ax^2+3a^2x+a^3,$$

and so on. Already for these initial exponents $m = 1,2,3$ it can be observed how the coefficients on the right correspond to the first, second and third rows of the arithmetic triangle in Figure 6.2. The binomial theorem confirms this impression for each exponent m. The proof can be obtained by induction on m - in the way we understand induction today, i.e. by checking the initial exponent 1 and then going from a generic m to the next $m+1$ for each m. All this at the cost of some somewhat intricate combinatorial calculations, which we would not recommend for the students we are addressing. However, we are interested in the way the *Encyclopédie* describes induction, which is still far from the modern view. Here is in fact what we read about it:

whoever, without knowing the exact and general way of proving this formula, would nevertheless conclude it by having verified it for $m = 1,2,3$ etc., would judge by induction. Therefore, one must not use this method unless there is no more exact one, *but even in this case one must use it only with great circumspection; for sometimes one might arrive at false conclusions.*

Therefore induction is still conceived in the way of Wallis and criticised in the way of Bernoulli.

6.12 De Morgan and Ruffini's theorem

The one who finally managed to describe the connotations of induction, as we understand it nowadays, was, a few decades later, Augustus De Morgan. He even collaborated in an encyclopaedia, the *Penny Cyclopaedia*, a kind of popular dictionary, comparable to today's Wikipedia. For it he compiled 106 entries, including one concerning induction itself, which can be found on pages 465-466 of volume XIV, published in 1838 [138].
De Morgan explains the principle of induction in terms that are familiar to us. He states: suppose we have a property of natural numbers and we succeed in proving that if it holds for three consecutive of them $n, n+1, n+2$, then it also holds for the next $n+3$; well, under this hypothesis, that property

- if holds for $1,2,3$, it transfers to 4,
- from $2,3,4$ it then transfers to 5,
- from $3,4,5$ it transfers again to 6

and so on «*ad infinitum*», so that it holds for every number.

It will be objected that the argument, referring to triads rather than to single natural numbers, is fatally complicated. But, the adaptation to a single n is soon done: it is sufficient to prove that the property is preserved by going from an arbitrary n to $n+1$.
Whether the premises are three or one, De Morgan emphasises the benefit of this. In the simplest case of 1-ary properties, there is no need to prove an infinity of deductions, from 1 to 2, 2 to 3, and so on, but it suffices to show a single condition from n to $n+1$ for every n, then combine it with the proof of the base case $n = 1$.
Returning to the entry in the *Penny Cyclopaedia*: De Morgan is the first to clearly name this procedure *induction*, and not its more or less ambiguous variants. To be

precise, he first calls it «*successive induction*» but then, at the end of his script, «*mathematical induction*».
De Morgan proposes two examples of it. The first is the same as Maurolico's one. The second concerns the divisibility of polynomials and therefore, in some way, their decomposition into irreducible factors. It is in fact a matter of proving that

for each positive integer n and for each parameter a,
$x^n - a^n$ is divisible by $x - a$.

The question can be reasonably proposed to students as an exercise in the use of induction, but also for better familiarisation with polynomials, Ruffini's theorem, etc. De Morgan already provides the answer, pointing out that for every positive integer n (in particular > 1)

$$x^n - a^n = x^n - a^{n-1}x + a^{n-1}x - a^n = x\left(x^{n-1} - a^{n-1}\right) + a^{n-1}(x-a)$$

so that $x^n - a^n$ is divisible by $x - a$ if and only if $x^{n-1} - a^{n-1}$ is also divisible by $x - a$. The previous consideration can then be applied: the required property, that $x^n - a^n$ is divisible by $x - a$, is trivially true for the exponent $n = 1$ and from this it then transfers to $n = 2, n = 3$, «*ad infinitum*».
If anything, it can be noted that De Morgan sets the inductive step from $n - 1$ to n and not from n to $n + 1$. But it should be apparent by now that the difference is not relevant: he could have similarly concluded that $x^{n+1} - a^{n+1}$ is divisible by $x - a$ if and only if $x^n - a^n$ is.

6.13 The Grassmans, Peirce et al.

It was towards the end of the 19th century that a general need began to be felt to provide mathematics and its main concepts with a clear and rigorous physiognomy and firm foundations. The need then matures to define exactly what numbers are, from naturals to integers, to rationals, to reals and beyond. Often the goal is achieved by defining a new class of numbers with reference to another. Thus the integers are formally introduced as "differences" of natural numbers, the rationals as "fractions" of integers, the reals as "sections" of rationals. But the natural numbers are the fundamental ones, the first that come to mind and that we learn as children, "the only ones created by God" - as Kronecker would have said. To introduce them, it is necessary either

- to define them with reference to other concepts even more general than numbers, for example to sets, or
- to axiomatize them as is done in geometry when dealing with a point, a straight line or a plane.

In this context, the principle of induction finally acquires a definite form and reveals its crucial role.
Various mathematicians contribute to this reflection. We quote here among others

- the two Grassmann brothers, German, first and foremost Hermann (1809-1877) but also Robert (1815-1901), less famous;
- or Charles Sanders Peirce (1839-1914), an American logician and mathematician.

By Hermann Grassmann we remember the 1861 textbook of arithmetic, *Lehrbuck der Arithmetik* [58], by Peirce the 1881 article *On the logic of numbers* [92].
In these references, in particular in the second one, and in others by the Grassmanns, the definition of the operations of addition and multiplication of natural numbers is proposed precisely in terms of recursion: for each pair of positive integers m, n, we define the sum of m with n

- first for $n = 1$
- and then for $n+1$ from that for n,

and the same is done for the product. The basic idea is

- in the case of addition, to add 1 to m as many times as n,
- in that of multiplication, to add m to itself as many times as n.

Induction allows this intuition to be formalised in the best possible way. For addition

$$\begin{cases} m+1 = \text{ the least greater element of } m, \quad \text{i.e. its successor,} \\ m+(n+1) = \text{ successor of } m+n \ , \end{cases}$$

while for multiplication we rely on the addition just defined and establish

$$\begin{cases} m \cdot 1 = m, \\ m \cdot (n+1) = m \cdot n + m. \end{cases}$$

To understand: a sum such as $5+3=8$ is obtained by adding 1 to $5+2=7$, which in turn is obtained by adding 1 to $5+1=6$, which is finally obtained by adding 1 to 5. Similarly, a product such as $5\cdot 3=15$ is obtained by adding 5 to $5\cdot 2=10$, which in turn is obtained by adding 5 to $5\cdot 1=5$. These procedures are not certainly the most efficient for calculating the two operations. They, however, provide an adequate definition - the same one that we will later find in Peano.
Again, with the help of the principle of induction, various elementary properties of addition and multiplication are then proved.
A curiosity: Peirce's 1881 article includes, in the final lines, the famous syllogism about Texans - people who, according to the western epic, do not hesitate to carry a revolver and use it. Peirce's argument is then as follows:

- every Texan kills a Texan,
- no one is killed by more than one person,
- therefore, every Texan is killed by a Texan.

The conclusion is valid assuming that Texans are a finite number. It does not involve the principle of induction, but lends itself to some discussion with students as a non-trivial exercise in logic.

6.14 Peano and Dedekind

Let us turn to 1889, the year in which the book by the Italian mathematician Giuseppe Peano (1858-1932) *Arithmetices principia, nova methodo exposita*, or *The Principles of Arithmetic Proposed by a New Method* [91], appeared. Written in Latin, it pursues and achieves the aims of rigour, clarity and simplicity that inspired its author. It presents the famous axiomatisation of natural numbers that we commonly adopt today. It is based on three basic concepts: the one (1), successor and equality. The axioms proposed on the opening page are in fact nine, but of these there are four, from the second to the fifth included, that concern the relation of equality, of which they postulate in particular the reflexive, symmetric and transitive properties: thus it constitutes a relation of equivalence. But the ones that interest us are the others, that is, the first and the last four, which state that:

- 1 is a natural number,

- the successor $n \to n+1$ is a function that constructs new natural numbers from natural numbers

and later that

- two natural numbers with equal successors are equal,
- 1 is not the successor of any natural number
- and finally, the principle of induction, expressed in the way we know it: a set of natural numbers that contains 1 and is preserved under successor includes all natural numbers.

The principle of induction is thus taken as the fundamental axiom for determining natural numbers. Indeed, it can be shown that, with reference to the basic concepts of 1 and successor and in conjunction with Peano's other postulates, it defines them "up to isomorphism": a technical expression which, translated in rough terms, means this, that a mathematical structure that obeys these axioms is nothing more than a superficial repainting of the natural numbers, of which it retains in essence the exact same architecture.

Peano's approach was prepared and largely anticipated not only by the Grassmanns and Peirce, but also and above all by the German mathematician Richard Dedekind (1831-1916). In his 1888 short essay *Was sind und was sollen die Zahlen?*, in English *What are numbers and what are they for*? [36], even Dedekind introduces natural numbers, but he seems more interested in defining them rather than axiomatising them, and in proving rather than postulating the principle of induction - unlike Peano. His approach then serves to implicitly prove the property mentioned above, i.e. that the conditions stated by Peano characterise the natural numbers "up to isomorphism".
The comparison between Peano and Dedekind can be an opportunity to insinuate the role of axioms in mathematics in the classroom.

6.15 Poincaré, chess and physics

The history of the advent of mathematical induction could be concluded here, with Peano and 1889. However, we would like to add something about Henri Poincaré. He dedicates very beautiful pages to induction in his most famous essay [101]. We

find them in Chapter 1, especially paragraphs IV to VI included.
Poincaré actually prefers the term recurrence, *récurrence* in French, to *induction*. However, he describes the procedure of a proof by induction in the way that is now familiar to us, albeit starting from $n-1$ to n:
«*A theorem is first established for* $n = 1$*; then it is proved that, if it is true for* $n-1$*, it is also true for* n*, and it is concluded that it is true for all the integers*» (here integer means what in this chapter is called natural number).
Poincaré then reiterates the main characteristic of induction: replacing an infinite sequence of syllogisms with a single proposition. Thus, instead of proving a theorem about natural numbers

- first for 1,
- then for 2, transferring it from 1 to 2,
- then for 3, transferring it from 2 to 3,

and so on for infinite steps that it is impossible to go through in reality; one verifies it again for the *base case* 1 and then prove the *inductive step* from $n-1$ to n. Poincaré then praises recurrence as «*the mathematical reasoning par excellence*», capable of going from the finite to the infinite.

He takes the cue from this to emphasise the difference between mathematics and the game of chess, to which it is often compared. In fact, he notes how a chess player can combine at most four or five moves in advance, and still foresee a finite number of them; the mathematician, on the other hand, goes further thanks to induction, because the gaze of his mind becomes so sharp that it embraces an infinite number.
Poincaré also distinguishes mathematical induction from the other induction procedure, which is applied in physics and the natural sciences. Same name, but distinctly different meanings. In the second case, the idea of a universal law underlying these phenomena arises from the observation of reality and the observation of events that are repeated or preserved there. This law, based on belief in a general order of things, is accepted because it is suggested by a myriad of examples - a myriad, but still a finite quantity. For example, Newton induces from the apple falling on his head and from similar experiences the law of universal gravitation.
In the same way, one might remark, Wallis deduces the formula for the sum of cubes from the examination of a few particular cases. But, Poincaré observes, in the field of arithmetic, the exploration of a finite number of examples is not sufficient to

produce a valid proof for the whole infinity of integers (far more than a myriad). Mathematical induction does not stop at an investigation of a few values, but goes beyond them, because it is based not on an examination of nature, but on the capacities of the mind - and thanks to them it «*necessarily imposes itself*».
Unfortunately, this dual meaning of the word *induction*, the mathematical one and, shall we say, the physical one, can be a reason for further uncertainty and misunderstanding among students: a reason to pause with them to clarify and distinguish the two concepts.

The comparison with the inductive procedure of physics is, moreover, an opportunity to resume and deepen the discourse already insinuated when speaking of the identities relating to triangular numbers ($*$), sums of cubes ($**$) and permutations ($***$). In these cases, we gave proofs based on the principle of induction as well as other arguments that disregard it and sometimes prove to be more illuminating. Indeed mathematical induction constitutes, as Poincaré reiterates, a formidable demonstrative tool, but only after the property to be proved has already been intuited in another way. At that point it can exert all its proven power. But when one has to discover that property, to glimpse it even vaguely, then induction does not help.
Gila Hanna distinguishes in her classic article [59] between mathematical proofs that explain and illuminate and mathematical proofs that merely prove. The method of induction, although subtle and effective, seems to correspond more to the second identikit. This characteristic is reiterated in [11]. Even [61] warns against the risk that the induction procedure, even when perfectly acquired and well mastered, is reduced to a recipe for mechanically solving problems without understanding them. From this point of view, a preliminary approach à la Wallis, i.e. the analysis of a few initial cases, may be useful to instil a first impression, a working hypothesis. This is recommended by [33] and [41]. The same is true for the proof of the inductive step, for which [9] suggests to start again from the proofs of the simplest cases, from 1 to 2, from 2 to 3 etc., in order to extend it with greater awareness from a generic n to $n+1$ - as Maurolico, Gershon and others did.

6.16 An appendix: the method of infinite descent

Poincaré [101] states that in reasoning by induction, or *récurrence* as it may be, a single statement succeeds in concentrating infinite syllogisms, which derive «*cascading*» from it. This expression «*cascading*» recalls a law of natural numbers that goes hand in hand with induction: the so-called *principle of the minimum*, which is the basis of the method named, precisely, the *infinite cascade*, or Fermat's *infinite descent*.

Let us recall that the principle of the minimum, referring to the usual relation of order of the natural numbers, states in that context that:

every non-empty set of natural numbers admits a minimum

i.e. a first element. As a result, no strictly infinite descending sequence can exist among natural numbers, which would constitute a non-empty set with no minimum. We call this prohibition the *principle of infinite descent.*

The statement thus expresses, like induction, an intuitive property of natural numbers that is easy to perceive. It was clarified and perfected by Pierre de Fermat in the 17th century. It admits, however, like induction, illustrious precursors. We present some of them. A simple and clear, but much more extensive treatment can be found in [139].

We will clarify the connection of this principle of the minimum with that of induction at the end of the chapter.

6.17 The Pythagoreans and the square root of 2

Let us go back in time, to the beginning of the history of mathematics. Among the most disruptive discoveries of the Pythagoreans is that of mutually incommensurable quantities, i.e., speaking in modern arithmetic terms, irrational real numbers: a sensitive subject for high school mathematics. The most famous example of incommensurable segments relates to the side and diagonal of a square, that is the cathetus and hypotenuse of an isosceles right triangle corresponding to half a square. Various arguments prove them to be so. One, generally attributed to the Pythagoreans, is as follows.

Let us start with the square $ABCD$ in Figure 6.4. Let us assume that side AB and diagonal AC are commensurable. Then there are two positive integers l, d that represent their measure with respect to an appropriate common subsegment, which

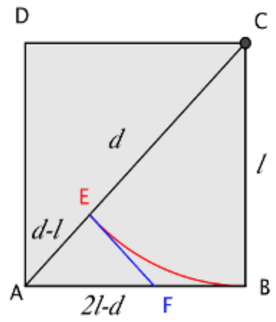


Figure 6.4

then enters exactly l times AB and d times AC.

Clearly $l < d < 2l$, because the side AB is less than the diagonal AC, which in turn is less than the sum of the two sides AB and BC. Then $2l-d, d-l$ are still positive integers. Let us put for simplicity $l' = d - l$.

We now draw the circle of centre C and radius CB and denote by E the point where it intersects the diagonal AC. For E we draw the perpendicular to AC, which is also the tangent to the circle at E. Let F be the point at which it intersects the side AB. Since the angle AEF is right and the angle EAF is half of a right angle, the triangle AEB is still half of a square. The side of this square is AE and the diagonal is AF. Furthermore, AE has the same length as EF, and both equal FB, because EF and FB represent the tangents to the circle exiting from point F. Let us observe now that:

- the measure of AE with respect to the initial sub-segment is evidently $d-l = l'$,
- that of AF (the difference between AB and FB) is $l - l' = l - (d-l) = 2l - d$.

Therefore AE and AF are also commensurable, having measures $l' < 2l - d$ with respect to the fixed sub-segment. Furthermore $l' < l$ because $d < 2l$. The starting situation is transmitted from the square of side AB to the square of side AE, which is smaller but still of integer length.

The process can be repeated, each time generating smaller and smaller natural numbers and ultimately a strictly decreasing infinite succession of natural numbers, $l > l' > \cdots$, which is impossible.

In arithmetical terms, it has been proved that the ratio of the lengths of the diagonal and side of a square, i.e. $\sqrt{2}$, is not a rational number, i.e. it is not a fraction of (positive) integers.

Similar constructions also prove the irrationality of the golden number $\frac{1+\sqrt{5}}{2}$, as

the ratio between the lengths of the diagonal and the side of a regular pentagon - segments that are also incommensurable.
Returning to the square: the previous proof, based on the method of infinite descent, can be reformulated in purely algebraic terms to prove that $\sqrt{2}$ is an irrational number, as follows. Let us assume by contradiction that $\sqrt{2}$ is rational, then

$$\sqrt{2} = \frac{d}{l}$$

with d, l positive integers. Then l is a positive integer for which $\sqrt{2}\,l$, equalling d, is still a positive integer.

Consider again $l' = d - l = l\sqrt{2} - l = l\left(\sqrt{2} - 1\right)$. It is still an integer. Furthermore

- $0 < l' < l$ because $1 < \sqrt{2} < 2$ and therefore $0 < \sqrt{2} - 1 < 1$;
- its product with $\sqrt{2}, l'\sqrt{2}$ coincides with $l\left(2 - \sqrt{2}\right) = 2l - l\sqrt{2} = 2l - d$ and is itself an integer, positive because $2 > \sqrt{2}$.

We have therefore found a positive integer $l' < l$ that has the same property as l, in the sense that its product with $\sqrt{2}$ is still a positive integer. The procedure can be iterated, generating smaller and smaller positive integers, but with the same behaviour, thus contradicting the impossibility of producing a strictly decreasing infinite subsequence of naturals.

6.18 Euclid again

The procedure of successive reduction to “smaller” cases that we have seen for the square root of 2 was called by Aristotle *antanairesis* and applied by Euclid in his famous algorithm for calculating the greatest common divisor, still widely used today for its acknowledged efficiency. Euclid expounds it in his own way, identifying natural numbers with measures of segments, in propositions 1 and 2 of Book VII of the [44] - the first that he dedicates to arithmetic. The antanairesis or, if we prefer, the method of infinite descent appears in particular in proposition 1. Adapted in modern terms it proceeds as follows. Given two positive integers $m > n$,

- one divides m by n obtaining the remainder $r < n$. If this remainder is 0, then n divides m and the greatest common divisor is precisely n.

- Otherwise, one divides n by r, obtaining the remainder $r' < r$.
- The procedure is iterated but must be interrupted after a finite number of steps, when the remainder becomes 0.

The last non-zero remainder is the greatest common divisor of the last two numbers involved, but it is also the greatest common divisor sought for m and n. In fact, it is easy to observe that the common divisors of m,n are the same as those of n,r as well as of r,r', up to the last pair considered.
An example: the greatest common divisor of 72 and 15 is 3 because

- 72 divided by 15 gives quotient 2 and remainder 12;
- 15 divided by 12 gives quotient 1 and remainder 3;
- 12 divided by 3 gives quotient 4 and remainder 0.

So, the last non-zero remainder is 3.

In truth, the reference to the method of infinite descent is not so explicit in Euclid's original text, which, moreover, ends his discourse after reaching the third remainder. However, proposition 31 of the same Book VII of [44] is also often cited as even more convincing evidence of its use. Expressed in modern terms, it states:

every composite number admits a prime factor.

Here is its proof according to Euclid, still slightly adapted to today's terminology. Let n be a composite number, then n has at least one non-trivial factor n', i.e. such that $1 < n' < n$. If this is prime, we are fine; if it is composite, the reasoning on n applies to it again. But this process must stop within a finite number of steps producing a prime number, otherwise it violates the principle of infinite descent.

6.19 Campanus of Novara

Johannes Campanus of Novara (1220-1296) was a mathematician, astronomer and astrologer, as well as chaplain to three popes, including Boniface VIII. He is regarded as one of the greatest mathematicians of his time. He translated from Arabic and commented on Euclid's *Elements*: 15 volumes later printed in Venice in 1482 [45]. Book VII opens with some of his statements on natural numbers (on pp. 105-106).

Among the postulates concerning them is «*no number can be diminished to infinity*», which is precisely the principle of infinite descent.

6.20 Fermat and the Last Theorem

We finally arrive at Pierre de Fermat (1607-1665), French, magistrate by profession, mathematician (brilliant) for pleasure. He studied the theory of natural numbers in depth but left no articles or essays on the subject. However, his son Samuel collected the annotations he wrote in the margins of a copy of the treatise *Arithmetica* by the ancient Alexandrian mathematician Diophanthus [39]. His Observation 45 provides evidence for the following statement:

the area of a right-angled triangle whose sides have integer numbers for lengths cannot be a square of an integer.

For example

1. the area of the right-angled triangle whose sides have for lengths the natural numbers of the Pythagorean tern $3, 4, 5$ measures 6, which is not a square;
2. similarly, the area of the right-angled triangle whose sides have for lengths the natural numbers of the other Pythagorean tern $5, 12, 13$ measures 30, which is not a square.

The result was used by Fermat to show the $n = 4$ case of his famous and enigmatic *Last Theorem*, i.e. to exclude the existence of (non-zero!) natural numbers a, b, c for which $a^4 + b^4 = c^4$ (thus of triples that for exponent 4 correspond to those that for $n = 2$ are called Pythagorean triples). To prove this premise on areas, Fermat elaborates and then applies precisely the procedure of infinite descent, on which other famous successive proofs of the *Last Theorem* for exponent 4 are based.
Fermat considers this method of his susceptible to extraordinary developments in number theory. He notes on the edge of Diophantine's page that he has found a proof of the corresponding principle, but that the margin on which he is writing his commentary is too small to contain the details - just as with his other more famous observation on the Last Theorem.

Elsewhere in his writings Fermat reiterates that he has obtained this proof of the principle of infinite descent, and describes the procedure in the following terms: if we have a certain property of the natural numbers to prove, and suppose towards a contradiction that it admits of a counterexample, and then prove that this first counterexample yields a second smaller one, and this in turn a third still smaller one, and so on ad infinitum, then it can be deduced that no counterexample exists and ultimately that all natural numbers satisfy that property.

6.21 Induction and infinite descent

Let us conclude by briefly examining, as promised, the relationship between the two principles of induction and of the minimum. Both manifest, as we have said, properties that are easy to recognise among natural numbers. Therefore, both of them can be considered in some sense the flip side of the coin with respect to the other: in fact, induction traverses the positive integers upwards starting from 1 and continuing to infinity, whereas the cascade method traverses them downwards, and after a finite number of steps must stop.
However, the two statements are not equivalent to each other: the principle of induction implies that of the minimum, but not vice versa. Let us see why. The relevant considerations can perhaps be proposed to students and discussed with them. Let us first prove:

the principle of the minimum is a consequence of the principle of induction.

Let S be a set of naturals with no minimum. We want to prove that S is empty. Let us form the set X of the natural numbers n for which none among $1, 2, \dots, n-1, n$ stands in S. Then:

- 1 stands in X, otherwise 1 stands in S and so, since there are no natural numbers < 1, it is the minimum of S;
- if a natural number n is in $X, n+1$ is also in X. Otherwise, since none of $1, \dots, n$ stands in S (since n is in X), it follows that $n+1$ stands in S, and indeed is the minimum of S.

By the principle of induction X coincides with the set of all the naturals. Therefore S is empty.

However, the principle of the minimum is more general than the principle of induction, because it continues to hold in worlds other than (or, rather, not isomorphic

to) that of the naturals with 1 and successor.
Consider, for example, instead of ℕ with 1 and the successor function, a structure in which the underlying set consists of two copies of ℕ, one red and one green, with no common elements. The overall 1 is the red 1, while the overall successor function acts as its red and green correspondents respectively on the copy of the same colour. The resulting order relation extends the red and green ones, assuming in addition that the red elements precede the green ones. Figure 6.5 illustrates the structure built in this way (with the order from left to right):

Figure 6.5

The minimum principle is satisfied, because it is so in both its red and green parts: a non-empty subset of this universe

- or contains only green elements, and therefore has its own green minimum,
- or also contains red elements, and therefore has its own red minimum (the minimum of the red elements, which precede all the greens).

On the other hand, the principle of induction, which would apply individually in the red and green worlds, no longer works in general: for example, the set X of red elements

- contains the red 1 (which is the overall minimum),
- is preserved for the successor function (which sends red elements into red elements),

but excludes all green elements, and thus does not exhaust the whole set.

This concludes the example. If wished, one could add that, assuming the Zermelo well order theorem, any set can be well ordered, thus endowed with a ordering relation that satisfies the principle of the minimum - but not necessarily induction. However, in all honesty, these developments in set theory, and the hints they imply about the axiom of choice, seem to us entirely premature in a high school classroom.

In any case, we refer to [75] for a popular treatment of them.

To sum up: the principles of induction and of the minimum represent properties of the natural numbers that matured progressively and, we might say, simultaneously, but independently, at least until both were precisely stated. At that point, the problem of their relationship arose with all likelihood, which however led to some divergence of opinion. There were those who considered them equivalent, with some reasons that are difficult to argue against: see the fine and detailed analysis by [84]. But in the end, it must be recognised that the connection between the two principles is the one we have described above. We can recall, though, that the principle of the minimum is equivalent to the principle of *complete induction* which, in the context of totally ordered sets $(A, \leq)$, is stated as follows:

a property of $(A, \leq)$ that, for every element x of A, if it is satisfied by every element $y < x$ of A is also transmitted to x, consequently holds for all elements of A.

The minimum principle, expressed in the same context, becomes

every non-empty subset of $(A, \leq)$ admits minimum,

and implies that of complete induction, and vice versa. Proving this is not difficult but, again, seems too abstract as an exercise for high school students.

Chapter 7

Paradoxes

7.1 Introduction

Etymologically, the word "paradox" is derived from the Greek παρά (*"parà"*, over, against) and δόξα (*"doxa"*, opinion). In fact, following the definition given in 1988 by the English philosopher Mark Sainsbury in his book *Paradoxes* [107], a paradox can be defined as *"an apparently unacceptable conclusion derived by apparently acceptable reasoning from apparently acceptable premises"*.

A paradox, therefore, is a proposition, a result, which by its content or the way it is expressed, appears contrary to current opinion and predictions, and is therefore surprising and incredible.

Paradox, thus, recalls the concept of contradiction – but in its case inescapable, at least apparently inexplicable. There is, however, a real theory of paradoxes, which tries to classify them. One can for instance distinguish among:

1) *logical or negative* paradoxes that break down points of view that have not been explored in depth enough, and lead to rethinking them,

2) *rhetorical or null* paradoxes, which are real exercises in subtle reasoning, aimed at proving everything and the opposite of everything,

3) *ontological or positive* paradoxes, such as proofs by contradiction which, by showing how certain premises lead to absurds, prove the validity of the opposite point of

view.

There is also a history of paradoxes, which has gone through at least three periods of great interest: in the Greek period, in the Middle Ages and at the turn of the 19*th* and the 20*th* century. The different names by which paradoxes were called in the three periods reflect the different attitudes towards them. For the Greeks they were paralogisms, literally "beyond logic"; for the medievals *insolubilia*, or "insoluble problems"; for modern people antinomies, "against the rules" or, indeed, just paradoxes, that is "beyond common opinion". There is, thus, a progressive change of perspective: from pure and simple errors in reasoning, paradoxes were first revalued as inexplicable dilemmas, and then regarded as indications of common-sense problems, beyond the dimension of a simple intellectual pastime.

The attitude of those who study and cultivate them also varies and goes from the tragic to the humorous, from the sympathetic to the reluctant. Aristotle held them in high regard, trying to suggest almost convincing and useful solutions. Before him, Zeno put them at the basis of a particular conception of knowledge and reality.

But paradoxes are not limited to the philosophical sphere, and they also appear in literature: Pirandello built his literary works on whirlwinds of almost paradoxical situations and beyond; Beckett used paradox to create absurd, impossible situations, capable of well representing a human condition devoid of meaning and references.

Turning to art, Dalì and Magritte painted a surreal world in their works, celebrating a dreamlike and paradoxical vision of reality.

Even in physics, Schrödinger and Einstein relied on paradox in the theory of relativity; Olbers, with his paradox of the *"dark night"* (according to which *"how is it possible that the sky is dark at night despite the infinity of stars in it?"*) was able to undermine an entire cosmological system.

Finally, Russell and others used these dilemmas to test the emerging set theory and to contribute to the clarification of its foundations. To this topic, we will devote the next paragraphs, the third one in particular.

How to overcome a paradox? The strategies for succeeding in it depend on the nature of the paradox. For example, when faced with a positive paradox, the most reasonable reaction is to acknowledge it. Otherwise, one tries to challenge either its premises or the thread of its reasoning. Logic certainly helps.

However, we would like to emphasise how paradoxes, or at least some of them, can be presented to secondary school students, both because they amaze and sometimes amuse, and because they lead to reflections on the nature and history of science. Let us highlight the initiatives that have been taking place in recent years in this regard and mention the internet site https://sites.google.com/view/pensareperparadossi .

7.2 Zeno's paradoxes

The most known paradoxes are probably those developed by Zeno of Elea, a Greek philosopher who lived in the fifth century BC. His teacher Parmenides theorised that reality was uncreated and indestructible, unchanging and indivisible, and therefore also immobile. He expounded his convictions in a poem *On Nature* [30], declaring that *"whatever is, is (being), and cannot ever not be; whatever is not (nonbeing), is not, and cannot ever be"*. Zeno composed his four most famous paradoxes (the dichotomy, Achilles and the tortoise, the arrow and the stadium, respectively) in support of these theses, thus also contesting the mere possibility of movement. To present the paradoxes we draw on Aristotle's *Physics* [6], historically among the first ones to mention them (but not the first to mention Zeno, who already appears among the characters in Plato's dialogue *Parmenides* [99]). We focus here on the first two paradoxes, which are also the most famous.

1) The paradox of the dichotomy or of the motion. Aristotle says: *"Zeno's arguments about motion, which cause so much trouble to those who try to answer them, are four in number. The first asserts the non-existence of motion on the ground that which is in motion must arrive at the half-way stage before it arrives at the goal"*. To put it in full: a runner who wants to reach a finishing line from the starting point must first reach the halfway point, and before that the halfway point of the halfway point, and so on. Ultimately, he does not even move. A different version, which can also be deduced from Aristotle's words, assumes in some sense the opposite perspective and points out that the runner, moving towards the goal, must arrive at halfway, and then at half of the remaining half (3/4 of the total),

followed by 7/8, so that, in conclusion, he never reaches the end.
2) The paradox of Achilles (and the tortoise): *"The second is the so-called Achilles, and it amounts to this, that in a race the quickest runner can never overtake the slowest, since the pursuer must first reach the point whence the pursued started, so that the slower must always hold a lead".* Note that Aristotle speaks of Achilles but not of the tortoise. For the record, the animal seems to appear in the version of the paradox given by Simplicius, written many centuries after Aristotle.

There have been many attempts since antiquity to explain these and other paradoxes. Aristotle refutes Zeno by introducing in some way the theme of continuity, and implicitly also that of infinitesimals. We know how the ancient philosopher distinguished between potential and actual infinity. To be clear: a segment can stretch indefinitely without ever widening to an infinite straight line; it can increase in power but is forbidden to reach the dimension of an actual, concrete infinity.
According to Aristotle, however, time and space flow in the manner of the dimensionless points of a segment, with continuity, and do not split up schematically as Zeno would like. Or, rather, they can do so as many times as one wishes, but not to arrive at an infinite division into portions of finite length.

A version of the paradox, which introduces its most recurrent mathematical explanation, is presented by the Argentine writer Borges in his famous essay *The Perpetual Race of Achilles and the Tortoise*, dating from 1932 [15]:

"Achilles, symbol of speed, has to catch up with the tortoise, symbol of slowness. Achilles runs ten times faster than the tortoise and so gives him a ten-meter advantage. Achilles runs those ten meters, the tortoise runs one; Achilles runs that meter, the tortoise runs a decimeter; Achilles runs that decimeter, the tortoise runs a centimeter; Achilles runs that centimeter, the tortoise runs a millimeter; Achilles the millimeter, the tortoise a tenth of the millimeter, and ad infinitum, so that Achilles can run forever without catching up".

Following the reading of the Borges text, we finally arrive at the mathematical explanation of the paradox already announced:

"Achilles' speed need only be set at a second per meter to determine the time needed: $10 + 1 + \frac{1}{10} + \frac{1}{100} + \frac{1}{1000} + \frac{1}{10000} + \ \ldots$ *The limit of the sum of this infinite geometric*

progression is twelve (more exactly eleven and one-fifth; more exactly eleven times three twenty fifths), but it is never reached. That is, the hero's course will be infinite and he will run forever, but he will give up before twelve meters, and his eternity will not see the end of twelve seconds. That methodical dissolution, that boundless descent into more and more minute precipices, is not really hostile to the problem; it is just to imagine it in the right way".

As we shall see, the result does not exactly coincide with 12, as Borges seems to affirm, that approximates it only by excess. But, beyond these details, the possibility of a finite sum, 12 or less than 12, for an addition of infinite terms, all positive, may certainly strike those less familiar with mathematics. Even more surprising, on reflection, is the idea of being able to dominate an infinite sum. However, we have already discussed this in Chapter 5 on proofs without words, in particular in Paragraph 4. Let us recall that for every real number r with $0 < r < 1$ we have that the sum of the infinite powers of r with natural exponent is finite,

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r} \ .$$

Applying this general result to the case $r = 1/10$ we obtain

$$\sum_{n=0}^{\infty} \frac{1}{10^n} = \frac{1}{1-\frac{1}{10}} = \frac{10}{9} \ .$$

This will be the space covered by the tortoise after these infinite displacements. That of Achilles will be instead, in the same way, $10 + 10/9 = 100/9$. The difference is just the initial distance between them, that is 10. So, we could say, when the tortoise has run 10/9 of a metre, Achilles reaches it. In fact, the rejoining happens after a time of 10/9 of a second if we assume that Achilles runs at the constant speed of 1 metre per second, and the turtle runs 1 decimetre per second.
For $r = 1/2$ (the case we have already examined in Chapter 5) we then have a similar explanation for the dichotomy paradox. In fact

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = 1 \ .$$

The endless stages that the runner covers, each time half of the previous one, allow him to complete the path. Strictly speaking, however, if we interpret Aristotle's account in the other possible sense, i.e., if we think that the runner, in order to arrive at the finishing line, must reach halfway, and before that half of the half, and then half of the half of the half, and so on, then not the distance covered, but the distance to be covered increases progressively to 1. We are therefore led to the conclusion that the runner does not even move: he stands still because he stands still, which is somewhat what Zeno states.

Archimedes is credited with the awareness that a series of this kind can have a finite sum, precisely only for $0 < r < 1$; however, it was only in the nineteenth century, with Gauss and then especially with Augustin-Louis Cauchy (1789-1857) and Karl Weierstrass (1815-1897), that the theory of numerical series took on its own form and consistency. The sum of infinite addends is then understood as the limit, if it exists, finite or infinite, of the succession of partial sums. Consequently, in the case of the geometric series, the preceding results can be confirmed and clarified in the following way (which specifies in theory what has already been anticipated by the proofs without words in Chapter 5). We start from the equality, valid for any r and for any n, easy to verify:

$$(1-r)\cdot\left(1+r+r^2+\ldots+r^n\right) = 1+r+r^2+r^3+\ldots+r^n-r-r^2-r^3-\ldots-r^n-r^{n+1}$$

$$= 1-r^{n+1} \ .$$

Whereby the $n-th$ partial sum for $r \neq 1$ takes the expression:

$$1+r+r^2+\ldots+r^n = \frac{1-r^{n+1}}{1-r} \ .$$

Now, for $|r| < 1$ (possibly for negative r), as n increases, the power r^{n+1} tends to 0 and so the series converges to the finite value $\frac{1}{1-r}$.
Instead, for $r \geq 1$, the series "diverges" and has sum $+\infty$. According to Cauchy's theory, then, for $r \leq -1$ the series has no limit, and the sum remains undefined.

Indeed, as Borges again points out, Zeno's paradoxes evoke and call on the fascinating and insidious theme of infinity. Let us quote two famous passages from the Argentinean writer:

- the first, again from [15], describes infinity as a *"worrisome word (and then a concept) we have engendered fearlessly and that, once it besets our thinking, explodes and annihilates it"*;
- the second, taken from *Metempsychosis of the Tortoise* (1984) mentions *"a concept that corrupts and makes others mad"*, and makes it clear that it is not

the Evil *"whose limited empire is ethics"*, but *"infinity"*. We did not find any translation of this essay in English. The original text in Spanish Avatares de la toruga can be found in [14], Discusión, p. 254.

Another mathematical explanation of Zeno's paradoxes is discussed by Bertrand Russell in *Mathematics and the Metaphysicians* (1901), one of the essays in *Mysticism and Logic* [106]. He points out how the philosopher from Elea insinuates the *"three most abstract problems of motion"*: not only infinity, but also, in order, infinitesimals and continuity. It is then observed that time and space are not the discrete succession of disjointed intervals, but flow with continuity, as Aristotle believed. A segment, however small, is not a point. It is enough to visually compare

- a segment
- and a finite or numerable succession of its points, which then divide it into separate intervals,

to see the difference between the fluidity of one and the fragmentation of the other. Segments and seconds can be measured by natural numbers and calculations relating to them, but to formalise points and instants we need real analysis with its instruments, hence the differential calculus. Space and time are continua of points or instants, not discrete and fragmented sequences. Russell then celebrates the role of Karl Weierstrass (with Dedekind and Cantor) in the rigorous introduction of the real numbers and the consequent clarification of the concept of continuity. To Weierstrass we owe, as already mentioned, the development among the reals of a rigorous and convincing approach to infinitesimal calculus. The axiom of continuity, conceived by Dedekind and Cantor, accredits the real numbers as the appropriate abscissae for the points of a segment or for the instants of a time interval.
Russell then mentions in his essay Georg Cantor and the birth due to him of the mathematics of infinity, in which the classical Euclidean principle that "the whole is greater than its parts" falls away. Often in fact, at infinity, the whole has as many elements as one of its parts, adding or removing a point no longer makes a difference. This is not the case in the finite worlds, where, if we add or subtract 1 to 4 elements, we obtain 5 and 3 respectively, and there is no longer any way of establishing a 1-1 correspondence between the resulting sets and the original one. At infinity the matter changes.
If, going back to Zeno's second paradox, we denote by 0 and 1 respectively the initial positions of Achilles and the tortoise and then by 2, 3, 4, ... the subsequent ones

(so that the hero and the animal arrive simultaneously at 1 and 2, then at 2 and 3, and so on), then at each stage of the run-up, the tortoise is ahead. For the reunion to occur, Achilles would have to count on an extra step. But in Cantor's theory the culmination (i.e., the infinite cardinality $\aleph_0$ of the set of naturals) of the two sequences:

- those $0, 1, 2, \ldots$ of natural numbers,
- the other one $1, 2, 3, \ldots$ of their subsequent,

is the same: $\aleph_0 + 1 = \aleph_0$, as if to say that the two sets are in 1-1 correspondence with each other precisely by means of the function that to each natural n associates $n+1$.

The same happens in the scenario of that continuum where, according to Russell, the chase actually takes place. Times and spaces of the chase are now viewed as intervals of real numbers: for example, that $]0,1[$ between 0 and 1 excluded. Here then is how to establish a 1-1 correspondence with $]0,1]$, 1 included. We fix in $]0,1[$ a sequence, for example the one strictly decreasing and convergent to 0 formed by powers of $\frac{1}{2}$, so:

$$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots, \frac{1}{2^n}, \ldots$$

with n varying between positive integers (we exclude $\frac{1}{2^0} = 1$ because it is outside the starting interval). We then define a function f of $]0,1]$ in $]0,1[$ by posing:

- $f(1) = \frac{1}{2}$, $f\left(\frac{1}{2}\right) = \frac{1}{4}$, $f(\frac{1}{4}) = \frac{1}{8}$ and in general $f(2^n) = \frac{1}{2^{n+1}}$ for each n,
- $f(x) = x$ for every other x of $]0,1]$, so for x other than 1 and outside the sequence.

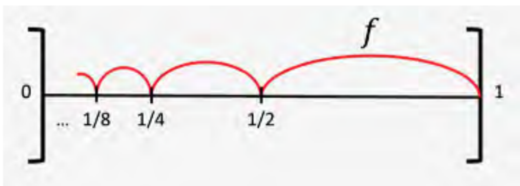


Figure 7.1

It is easy to check that f is the required bijection.

Furthermore, the argument somehow echoes the paradox of the dichotomy, with the successive steps that, by means of f, 1 takes in order to get closer to 0; or, as already mentioned, that of Achilles' run-up, which at each step reaches $f(n)$, the $n-th$ position of the tortoise, which in the meantime has run away in $f(n+1)$. Ultimately, and in extreme synthesis, according to Russell the paradoxes are solved by noting with Cantor that for two infinite sets their "equinumerosity" does not prevent the fact that one is larger than the other.

Coming back to logic, a famous transposition of the Achilles and the tortoise argument was proposed by Lewis Carroll. We know that he was a surreal spirit, an imaginative and fantastic creator of stories and logic puzzles. It is not surprising then that he turned his attention also to the subject of Zeno. This time, however, the path to be taken is a syllogism: the starting point is its premise and the unattainable end point its conclusion. Carroll's story, entitled *What the Tortoise Said to Achilles*, dates back to 1895, i.e., to the last years of its author's life, and was published in *Mind* (the most important British philosophical magazine) [27]. The author imagines that Achilles and the tortoise, having abandoned their inconclusive chase, begin to discuss the first proposition of Euclid's *Elements* [44], namely the construction of an equilateral triangle with an assigned side AB. Let us briefly recall how it is obtained:

- draw the circumferences with radius AB and centre in A and B respectively;
- consider one of the points of intersection (which we call C);
- note that AC is the radius of the first circumference, and is therefore equal to AB, and that BC is the radius of the second circumference, and is therefore still equal to AB;
- conclude that AC and BC, since they are both equal to AB, are equal to each other.

Carroll imagines Achilles and the tortoise debating the last syllogism:

a) two things equal to a third are equal to each other;
b) the two segments AC and BC are equal to AB;
z) the two segments AC and BC are equal to each other.

The tortoise accepts premises a) and b), but denies that they alone justify conclusion z). It notes the need to interpose a further assumption c):

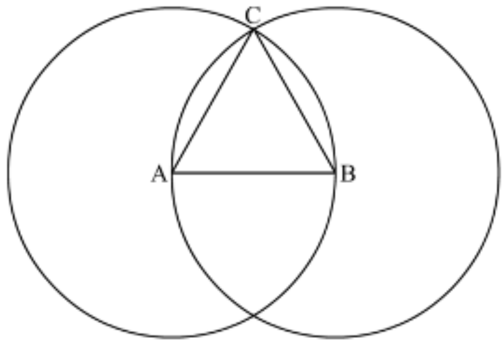


Figure 7.2

a) two things equal to a third are equal to each other;
b) the two segments AC and BC are equal to AB;
c) if a) and b) are valid, z) is valid;
z) the two segments AC and BC are equal to each other.

Achilles agrees. But at this point the turtle declares that it accepts the validity of a), b) and c), but not of z), and induces Achilles to a further interpolation:

d) if a), b) and c), are valid, z) is valid.

The game continues without end. Indeed, *"some months afterwards [...] Achilles was still seated on the back of the much-enduring Tortoise, and was writing in his note-book, which appeared to be nearly full"*: this is the epilogue of the story.

From the point of view of logical reasoning, Carroll's argument highlights the importance of previously agreeing, in the use of syllogisms and more generally in deductive calculus, on specific rules that oversee and direct demonstrations, rather like the programming of modern computers. In this specific case, the one that leads from a) and b) to z) without further ado. But beyond the theoretical details, the story, and the adaptation of Zeno's paradox to the logical mechanisms of the mind, testify to the happy creativity of its author.

Recently, Zeno's paradoxes have even affected computer science: a non-trivial application, and indeed an intriguing one that stimulates reflection on history, powers and limits of computers. We recall that the birth of computers is generally related to Alan Turing and his 1936 article [116], where the modern concepts of:

- program (the Turing machine),
- software, i.e. repertoire of programmes (the universal Turing machine)

take shape. Among the reasons that motivated Turing in his research were Gödel's incompleteness theorems and the ascertained impossibility for the human mind to completely supervise the natural numbers and their usual operations of addition and multiplication. The question then arose: what can, or cannot, be calculated in $\mathbb{N}$? And what does it mean to calculate? The answer was given by the concept of Turing machine and then by the Church-Turing thesis, already discussed in Chapter 1, which accredited Turing machine as the adequate answer to the previous questions. That is, one argued that a problem involving natural numbers, or which can be reduced to natural numbers by encoding their data, admits an algorithm of solution if and only if there is a Turing machine that provides the intent, and therefore, in the absence of such a machine, it remains devoid of any answering procedure. On this basis, one finds problems on the natural numbers that Turing machines cannot solve and that therefore escape any solution.
A further embarrassment arises, even in favourable cases, about the duration of computations, i.e., the efficiency of a programme. Sometimes the calculations of a Turing machine, even if in theory they guarantee a good result, i.e., an answer, in practice are too long, beyond any foreseeable limit of reasonable expectation. This arouses the desire for more powerful machines, both in terms of the field in which they operate and the time at which they work. New horizons are then spreading in computer science, or it is hoped that they will spread, capable of meeting these needs: the so-called hyper-computation, which in recent years has inspired the enthusiasm of some and the uncompromising criticism of others.
Among the hyper-computational models there is also a so-called *Zeno's machine*, which can certainly be presented to the students, if only as a curiosity.
This question was suggested by a great mathematician of the $20th$ century, Hermann Weyl (1885-1955), who in 1927 [126] wondered whether, from a physical or rather kinematic point of view, the idea of an automaton performing calculations of infinite length in a finite amount of time was plausible, and even feasible. A Zeno machine, to be precise, which might take up to half an hour to perform its first step, but then speeds up, reducing the internal working time each time by half: thus, the second

step takes a quarter of an hour, the third seven and a half minutes, and in general the *n-th* step the 2^n-*th* portion of an hour. In this way even complex conjectures would be solved in 60 minutes. It is true, in fact, that the natural numbers are infinite, but the *n-th* between them would be checked in the interval 2^n, and we know that:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots+\frac{1}{2^n}+\ldots=1\ .$$

Let us conclude by observing that, despite the various mathematical explanations, the paradoxes still seem to arouse lively interest today and maintain their philosophical and existential relevance, perhaps because they are figures of the human parable, which is itself unfinished, unfulfilled and indecipherable. The literary quotations concerning them are innumerable, even in modern times. We have already mentioned Borges. We could add, among the writers whose work recalls Zeno and his paradoxes almost explicitly, Kafka first of all, for one of his most famous novels, *The Castle* [69], or for the short stories *Before the Law* [70] (which later merged into the other masterpiece *The Trial* [71]) and *An Imperial Message* [72] - Borges even maintains that *"Achilles is among the first Kafkaesque characters in literature"*. Or, limiting ourselves to Italian literature, we could think of Italo Calvino and the "deductive" stories of the *Cosmicomiche* [21], brought together in *Ti con zero* [22], or Dino Buzzati (1906-1972) and his short story *I sette messaggeri* [18].

7.3 Paradoxes of truth

According to some, what is nowadays commonly referred to as paradox originated with Epimenides of Crete (6th century BC). He was the first to enunciate the so-called paradox of the liar, which is reputed to be historically the first example of this kind of puzzle and is consequently also called Epimenides' paradox. The intrigue concerns the sentence *"All Cretans are liars"*. If it is Epinomides himself, who is a Cretan, who states it, then it also refers to him, and is therefore a lie. Even Saint Paul testifies to the paradox in his letter to Titus: he reformulates it by speaking of the Cretans, *"eternal liars"*, *"as one of their own prophets admitted"* - here Epimenides himself is alluded to and it is concluded that *"his testimony is true"*. It is not clear whether in this way Paul shows that he has not understood the underlying contradiction, or whether he is exercising some kind of irony.

In fact, in the form in which it is stated by Epimenides the paradox leaves some way out: what does it mean to "be a liar"? To lie always, or most of the time? In the second sense, Epimenides may be a liar by habit, like all his countrymen, but as honest as he admits it.

A more incisive and convincing version of the paradox, which puts him beyond these doubts, is attributed to Eubulides of Miletus, a Greek philosopher of the second half of the 4th century BC. In this new formulation, one imagines that someone says *"I am lying"*, and one recognises that such a person is lying if and only if he is telling the truth.

The liar's paradox has inspired a wealth of philosophical, literary and even mathematical adaptations. A famous judicial version can be found in the *Noctes Atticae* [56] by the Latin writer Aulus Gellius (125-180). It tells of the lawsuit brought by the Greek philosopher Protagoras, *"the sharpest of the sophists"*, against his disciple Euathlus on the following grounds.

Euathlus had enrolled in Protagoras' school to learn the art of law, agreeing to pay his fee in two halves, one at the beginning of his studies and the other on completion, when he would defend his first case and win it. But Euathlus lingered in his studies without completing his "training".

So, his teacher, annoyed at the lack of income, decided to take him to court. He felt that this way, whatever the judges' verdict, Euathlus would have to compensate him in any case:

- because of the judgement, if it had been in favour of Protagoras,
- but, if not, precisely because he would have successfully defended his first case.

The young Euathlus retorted that he had no obligation to the master, regardless of the outcome of the case:

- if winner, because supported by the court,
- if defeated, because the clause with the master would have lapsed.

Aulus Gellius tells that the judges, unfamiliar with too many logical subtleties, decided to postpone the case to a distant date, so that Euathlus had nothing to pay and in essence won the case.

Many centuries after Aulus Gellius, the paradox can be found in a passage from *Jacques the Fatalist and his Master* [38], written in 1775 by Denis Diderot (1713-1784). It deals with the protagonist Jacques who decides to visit an acquaintance, a certain Gousse, who is in prison. He finds him calm and serene and asks him the reasons for his imprisonment. But Gousse replies in a surreal way: he has denounced himself (over women's issues) and won the case, then lost it and was consequently imprisoned.

An even more explicit reference to the paradox of the liar can be found in the pages of Cervantes' *Don Quixote* [28], specifically in the second part of Chapter 52, where the author tells of a colossal hoax played on Sancho Panza, who is made to believe that he has been appointed governor of an island, named Barattaria. In this new guise, he is presented with the following case. On the island there is a bridge and on that bridge a court and a gallow. Whoever crosses the bridge is obliged to explain the reason to the judges: if he tells the truth, he is let through, but if he tells a lie, he is immediately hanged. But a passer-by has arrived on the bridge and has declared that he wants to cross in order to be hanged. At this point the judges do not know what to do:

(a) if they hang him, they recognise that he has told the truth and therefore cannot execute him;
(b) if they let him pass freely, they recognise that he has told a lie and therefore must put him to death.

Sancho at first advises solomonically (or rather, with an explicit reminiscence of Solomon and his famous verdict on the child disputed by two supposed mothers) to divide the traveller in half, freeing one and hanging the other; but then he proposes a more tolerant and wise sentence, that is, to send the traveller free in his entirety, since in controversial cases it is always better to be lenient (*in dubio pro reo*).

A similar dilemma is encountered in *The Lady, or the Tiger?* [111], a late 19th century tale by American writer Frank Stockton, which tells of a semi-barbaric king who administers justice in a very bizarre way: anyone suspected of a serious crime is ushered into an amphitheatre, where two closed doors await him, behind which are hidden a ferocious tiger and a beautiful woman. Depending on which door he chooses to open, the suspect will find himself either mauled by the tiger as he is found guilty, or married to the woman, and thus rewarded as he is found innocent. In that kingdom, however, it happens that the king's beloved daughter takes to flirting with a young courtier, that the king learns of the affair, dislikes it and consequently condemns the unfaithful subject to place himself before the bloodiest tiger or the most charming girl known to man. The princess, however, knows in advance which door hides the beast and which the woman, and so a glance of understanding from the tribune to the arena would be enough to save her lover. But the woman knows that she will lose him in any case: either because he is attacked by the tiger or because he is married to her rival, so she decides to keep silent. The young man then unsuspectingly opens a door, but the tale ends without revealing which one.

A famous mathematical variant of this argument is the already mentioned paradox that Russell proposed in a 1902 letter to Gottlob Frege. We have already mentioned this in the first chapter. The paradox concerns the then nascent set theory, to which Frege had given an initial attempt at axiomatization, relying in particular on *the axiom of comprehension* according to which each "property" defines a set, that of the elements that satisfy it. An assertion that seems easy to accept and agree with yet turns out to be extremely insidious. Russell in fact referred it to the following property of sets X:

$$\text{“}X \text{ does not belong to } X\text{”}, \text{“}X \notin X\text{”}.$$

Using the principle of comprehension, Russell formed the set U of sets X that satisfy that property, i.e., do not belong to themselves. Then he asked whether that set U belongs to itself or not. He concluded:

$$U \in U \text{ if and only if } U \notin U,$$

which is evidently a contradictory and unacceptable statement.

A lighter arrangement of the paradox, aimed at those not too familiar with set abstractions, was proposed, or at least picked up, by Russell himself in 1918. It is called the barber's paradox. It supposes that in a village there is only one *"barber"*, who is to be understood as the one who shaves all the men who do not shave themselves. It specifies that he himself is a carefully shaved man. It asks who shaves the barber. It concludes that the barber shaves himself if and only if he does not shave himself.

A new formulation of the liar's paradox was provided in 1913 by the British logician Philip Jourdain. In it he imagines a card, in which on one side is written the proposition: *"The sentence on the other side of this card is true"* and on the other side: *"The sentence on the other side of this card is false"*. Thus, the two statements refer to each other and contradict each other endlessly.

A further variation on the theme is the one theorised by the German philosophers and logicians Grelling and Nelson in 1908, concerning adjectives unable to define themselves. In the English language, there are some adjectives that describe themselves as they are: "short" is short, "pentasyllabic" (i.e., composed of five syllables) is pentasyllabic, "English" is english. Others, however, do not possess the same characteristic: for example, "long" is not long, "eptasyllabic" (i.e. composed of seven syllables) is not eptasyllabic, "red" is not red and so on. We call *"heterological"* an adjective that does not describe itself. Thus:

(a) *"short", "pentasyllabic", "English"* are not heterological,
(b) *"long", "eptasyllabic", "red"* are.

The question: is *"heterological"* heterological or not?
The answer: "heterological" describes itself if and only if it does not ... it is heterological if and only if it is not.

Another version of the liar's paradox, developed by Ferdinand Gonseth in 1936, assumes the existence of a huge, potentially endless, library. A clerk who wants to put things in order draws up catalogues of all the books in the library, subdividing them according to every possible criterion of distinction. So, he writes catalogues of all the books, of those written in English, of those dealing with logic, and so on. But the catalogues thus composed are so numerous that the clerk finds himself compelled to write the catalogues of the catalogues too, again organising them according to every possible heading. He completes then:

(a) a catalogue of all catalogues (which therefore cites itself);
(b) or the catalogue of catalogues of books of literature (which does not cite itself because it is not a catalogue of books of literature).

Among the various criteria for distinguishing among catalogues is whether or not a catalogue cites itself. Let us consider the catalogue that performs this second task, i.e. lists the catalogues that are not cited. To the question of whether or not this catalogue should be cited within it, the answer is: the catalogue is cited if and only if it is not cited.

How to overcome the paradox of the liar, and all these variants? Let us avoid considering them simply in the rhetorical or the null sense, i.e., as exhibitions of logical subtlety for its own sake.
In some cases, as in Russell's antinomy, we can interpret them in a positive sense: in the specific case, we acknowledge that Frege's approach to sets is ill-founded and needs to be revised, avoiding the principle of comprehension, and we look for new axiomatic perspectives. The concept of sets is delicate and needs to be approached with care.
Barber's version is slightly different, unless we intend to overcome it by rejecting its premises. But we can perhaps grasp the ambiguity of the situation, and take note that the alternative "shave yourself ", "get shaved by the barber" is not so absolute.
The paradox of Epimenides (at least in the version where the protagonist says "I am lying") and the other variants of Jourdain, Grelling-Nelson and Gonseth are another matter.
However, an attempt explanation was proposed in 1933 by Tarski in [112]. The Polish mathematician observed that, when speaking of language, one must distinguish between two levels: the language itself, with its statements, and the metalanguage that discusses it (and in any case expresses itself through language).
According to this subdivision, the liar is certainly free to tell a falsehood, employing normal language. But when he goes on to affirm *"I am lying"*, then he encroaches on metalanguage, that is, he judges the truth or falsity of his assertion. According to Tarski, it is precisely from this ambiguity that the paradox of the liar arises, with the variants listed above.
As for the distinction between language and metalanguage, Tarski illustrates it with a famous example. In it he observes how the statement "snow is white" is true if and only if the snow is white. On one hand we have a formal proposition with its terms "snow" and "whiteness". On the other hand we have their interpretation in nature, i.e., the snow (as an atmospheric phenomenon) and the white (as a colour). If the abstract words "snow" and "whiteness" are understood as snow falling from the sky and as the colour white, then the statement is true. But if by "snow" is meant the sea, and by "white" the colour red, then the statement is false, because the sea is not red. In the paradox of the liar, however, the two dimensions are confused and superimposed.

7.4 Paradoxes of the heap

Also attributed to Eubulides is the well-known *sorites paradox* (from the Greek σωρός (*"sorós"*) meaning "heap"), which can be expressed as follows. A heap of sand is given. If we remove a grain from it, we will still have a heap. We then remove another grain: it is still a heap. If we remove another grain, and then another grain, the pile will become smaller and smaller, until there is only one grain of sand left, which is no longer a heap. But at what step in the process does the heap cease to be a heap?

Or viceversa, by gradually adding to the remaining grain the others previously removed, at what step of the process does the heap become a heap again?

Because of the principle of induction, one could say: never.

Theorem 6.1. No collection of grains of sand is a heap.

Proof. The following statements are universally accepted as valid:

(a) a collection of only one grain is not a heap;

(b) if a collection of grains is not a heap, it does not become one by adding another grain.

From (a) and (b) the thesis follows, precisely because of the principle of induction.

A similar paradox is that of the *"bald man"*, according to which no man is bald, or all men are bald. In fact, a man with a lot of hair is certainly not bald, nor does he become bald if a hair falls out. But if he keeps losing hair, he becomes bald. But when does the transition take place?

Otherwise, let's consider a man without hair. It is not enough to transplant just one to remove his baldness. In general, a bald man does not cease to be bald because he acquires an extra hair. Is the difference between bald and non-bald a single hair?

Again disrupting the principle of induction, we deduce:

Theorem 6.2. All men are bald.

Proof. It is sufficient to observe that:

(a) a man without hair is bald,

(b) if men with n hairs are bald, so are those with $n+1$.

From the principle of induction: men of any number of hairs are bald.

In truth, the transition from baldness to abundance of hair occurs gradually, and cannot be resolved in a manichean alternative, yes or no. The quality of being bald or not cannot be measured in this way by the quantity of hair, by setting a precise threshold for which one passes from one condition to another. Idem for the heap. The approach of classical logic, with the alternative true or false, is not very subtle. This subject will be discussed in more detail in the next chapter.

Speaking of induction, another one of its apparent consequence (this time, however, not paradoxical, but erroneous and subtly misleading) is the one that deduces that all apples are red (or similar statements).
Let us recall it. Since there is at least one red apple, it is sufficient to show that the apples of any finite set have all the same colour. We proceed by induction on the number n of apples in this set. If $n=1$, the thesis is obvious. Let us assume it is true for n and let us prove it for $n+1$. Let's consider $n+1$ apples: removing the first one we obtain n, that therefore, for the inductive hypothesis, have all the same colour; removing the last one we obtain again n, still all of the same colour. So, all the $n+1$ apples have the same colour.
The error, or if you prefer the cheat, is that the previous reasoning does not work when there are 2 apples (i.e., $n=1$ and $n+1=2$). In fact, in this case, when one is removed, the other retains its colour, without being forced to share the colour of the removed one. For this to work, there must be at least a third apple, which remains whether we remove the first or the last.

7.5 Other logical paradoxes

Let us now return to the truth value of an implication, then to the evaluation of the connective "if... then" and to the rule expressed by the Latin locution *ex falso quod libet*.
We have already commented on it. It does not represent a paradox itself, but it is certainly far from being intuitive and easy to share. Here we would like to underline some consequences that are just as surprising, but not unacceptable - they need at most some patient explanation.

Among these, one of the most compelling is certainly that recounted by Raymond Smullyan in [109]: the *drinker's* paradox, or to use the author's words, *the drinking principle.*

Here is how Smullyan proposes it: *"A man was at a bar. He suddenly slammed down his fist and said, «Gimme a drink, and give everyone else a drink, cause when I drink, everybody drinks!» So, drinks were happily passed around the house. Some time later, the man said, «Gimme another drink, and give everyone else another drink, cause when I take another drink, everyone takes another drink!» So, second drinks were happily passed around the house. Soon after, the man slammed some money on the counter and said, «And when I pay, everybody pays!»".*

The assertion to be discussed is then the following: *in every pub there is a customer x such that, if he drinks, then everyone else drinks.*
The assertion is certainly astonishing, yet it is true. The argument proceeds by distinguishing two cases:

- either everyone drinks, and then any customer is fine as x;
- or there is someone who does not drink, but then one can take this very patron as x. In fact, in doing so, the proposition *"if x drinks everyone drinks"* has a false antecedent and thus since *ex falso quod libet* is true.

Smullyan then goes on to relate two other variants of the paradox: a more dramatic one claims the existence on earth of a woman who, if she becomes sterile, condemns the entire human race to extinction. The other is instead a “dual” version of the drinker principle and states that there is at least one person who drinks if someone drinks.

The reasoning behind them proceeds in the same way as for the drinker. In the first case, either all women become sterile, and so each among them satisfies the claim; or not all become sterile, and so one who remains fertile attests to the claim.

In the other case, either there is at least one person who drinks or there is not. If there is none, i.e., no one drinks, then anyone can make the assertion true: since it is false that anyone drinks, it follows from *ex falso quod libet* that if anyone drinks, then the chosen person drinks. On the other hand, if there are some who drinks, let us choose one among them and call him x. The conditional sentence *“if someone drinks, x drinks”* has both the antecedent and the consequent true, so by the truth rules of implication it is true.
Curry’s paradox concerns a further bizarre consequence of the truth rules of implication, that raises some further minimal doubts about them. Haskell Curry was a twentieth century logician who described his argument in a 1942 article (*The Inconsistency of Certain Formal Logics* [32]). His is a further variant of the ancient paradox of the liar. In this case we consider the sentence *“if this statement is true, then Russell is the Pope”*, but if you wish, the resulting statement can be replaced by any other extravagance.
Here is the proof: let us assume that the statement in italics, i.e., the implication, is false; for this reason, the antecedent statement, i.e., the implication itself, must be true and the consequent statement false, so that we should recognise that Russell is not the Pope. But this is a contradiction: the implication cannot be true because it is false. So, we must reject the original assumption by assuming that the implication is true. Now there are two possible cases, the antecedent statement is false, or it is true. The first case does not exist, because the antecedent statement is the implication itself, which we are assuming to be true. The second case exists because of the hypothesis we are assuming and necessarily leads to the conclusion that the consequent statement is true, that is, Russell is the Pope.
In order to understand such a surreal deduction, it is worth noting that the sentence *“if this statement is true, then . . . ”* is self-referential, that is, it speaks of itself by confusing the subject it deals with and the reflection on the subject itself. It is this ambiguity that allows the kind of sleight of hand (based on the difference between

language and metalanguage) we have illustrated.

Another rule of the implication is that it remains true when the hypotheses are strengthened: in other words, if the implication $F \rightarrow G$ holds, then, whatever H is, the implication $(H \wedge F) \rightarrow G$ also holds.

A check of the truth tables is sufficient to confirm this:

F	G	H	$F \rightarrow G$	$H \wedge F$	$(H \wedge F) \rightarrow G$
1	1	1	1	1	1
1	1	0	1	0	1
1	0	1	0	1	0
1	0	0	0	0	1
0	1	1	1	0	1
0	1	0	1	0	1
0	0	1	1	0	1
0	0	0	1	0	1

Notice how, in the rows where the column of $F \rightarrow G$ contains the truth value 1, so does $(H \wedge F) \rightarrow G$ (which then adds a 1 also in the fourth row, corresponding to the 0 of $F \rightarrow G$).

But let us consider the clearly true statement *"if I jump off the roof of a skyscraper, then I kill myself"* and take as H *"I put on a parachute"*. We get the implication *"if I put on a parachute and jump off the roof of a skyscraper, then I will kill myself"*, whose truth is no longer so obvious, if the parachute works and opens at the right moment.
Otherwise, appropriately contextualised, an atmospheric prediction such as *"if it rains, then it doesn't rain hard"* can be considered reasonable; but passing to the negations of antecedent and consequent, and in full respect of the laws of logic, it leads to the statement *"if it rains hard, then it doesn't rain"* which, in the same context that ensures the reasonableness of the first implication, can very likely turn out to be false.
In order to explain the last two "paradoxes", one can observe how the multiform causal connections that link antecedent and consequent in everyday speech sometimes escape mathematical modelling, which is too rigid and incapable of grasping

all their nuances.

7.6 More about bald men

As already mentioned, a fuzzy approach provides a more convincing explanation of paradoxes such as those of the heap or the bald man. We find it for example in [57]. We expose it in the case of the bald man. We denote, for every natural number n, with $B(n)$ the proposition "every man with n hair is bald". In classical logic we accept the following propositions as true, therefore with a Boolean truth value of 1:

- $B(0)$,
- $B(n) \to B(n+1)$ for every natural n.

The induction principle then leads us to the paradoxical conclusion

$$B(n) \text{ for every } n,$$

therefore that all men are bald regardless of how much hair they have, even if one believes that the maximum number of hairs on the head is $140,000$ and consequently it is difficult to claim $B(140,000)$, that is, that a man with $140,000$ hairs is bald. Anyway

- from $B(0)$, $B(0) \to B(1)$ we can deduce by modus ponens $B(1)$, which therefore has truth value 1 (in fact a valuation assigns to the conjunction of $B(0)$ and $B(0) \to B(1)$ the product $1 \cdot 1 = 1$, which is transmitted a fortiori to the consequence $B(1)$),
- from $B(1)$, $B(1) \to B(2)$ we deduce by modus ponens $B(2)$, which therefore has truth value 1 (in fact a valuation assigns to the conjunction of $B(1)$ and $B(1) \to B(2)$ the product $1 \cdot 1 = 1$, which is transmitted a fortiori to consequence $B(2)$),

  etc. etc.

But now let's assume from the fuzzy point of view that

- $B(0)$ has truth value 1 (how can you doubt it?),
- but $B(n) \to B(n+1)$ has, for each n, a truth value just below 1, say $1-\epsilon$ with real positive ϵ small at will, for example truth value $99/100 = 1 - 1/100$.

Proceeding as above, this time we have:

- the conjunction of $B(0)$ and $B(0) \to B(1)$ has the truth value corresponding to the product $1 \cdot 99/100 = 99/100$, which then is the least possible truth value of $B(1)$,
- the conjunction of $B(1)$ and $B(1) \to B(2)$ has a truth value $\geq (99/100)^2$, which is transmitted a fortiori to consequence $B(2)$,

etcetera etcetera, so that for every n the truth value of $B(n)$ is $\geq (99/100)^n$, which becomes smaller and smaller and indeed tends to 0 when n increases and goes to infinity. In particular, $B(140,000)$ has a truth value $\geq (99/100)^{140,000}$, which is very close to 0.

Chapter 8

Logic in uncertainty situations

8.1 The game of Rényi – Ulam

Every day, we are protagonists of situations that want us to make choices such as "on/off", "yes/no", "true/false", or "in/out", to the point where we sometimes apply this secular logical antithesis even to non-properly technological domains, for which there are more than two possible answers.
Nowadays, we also witness the temptation and often the practice of fake news. In these cases, the alternative is no longer "yes/no", but "yes/no/maybe", with many possible gradations of "maybe", depending on the reliability of the speaker.
From these observations, the need for a logical approach arises, in which the truth values are not just two, true or false, but include intermediate levels. We need, therefore, the development of a logic of uncertainty.
On the other hand, this term "uncertainty" also takes on different meanings depending on the context in which it is used, and it extends far beyond logic, involving information technology, philosophy, psychology, legal argumentation, medical diagnosis, not to mention mathematics itself.

Here we present and analyze some simple models of uncertainty situations. We believe that they can be proposed without problems to high school students, to stimulate their curiosity and their attention on some notable aspects:
1) firstly the fact that not always the cases of ordinary life can be approached, examined and decided according to classical logic and its only two values of truth (*"yes"* or *"no"*) and that on the contrary they often require a less rigid and more varied treatment;

2) but also the development of a logic and an algebra that take these needs into account, appropriately adapting the classical model.

As a starting example, consider a guy who is sometimes liar. Suppose he is playing with a friend, who has been asked to guess the value of a number that the liar imagined. The interlocutor is allowed to ask him questions, to which he answers, sometimes lying. Let us also suppose that only *"yes/no"* questions are allowed in the game. So one can ask if the number is 112, but not the value of the number.

Or, to make the situation even more exciting, let us place it in a courtroom, when what has to be guessed is not properly a number, but the culprit. Suppose that the first character is a witness, and the one who interrogates him is the defense attorney, for example Mickey Haller, the "Lincoln lawyer", the character in various Michael Connelly detective stories [29]. Indeed the number to guess might could correspond to who, among many possible suspects (say N suspects), is the real culprit. Therefore the defense attorney, in order to prove the innocence of his client, has to induce the main prosecution witness, who is answering his questioning and knows the real murderer, to finally point him out to the court without a shadow of a doubt. But this interlocutor could be recalcitrant, or even in bad faith, and so answers monosyllabically, saying only *yes* or *no*, and could sometimes lie. Finally, Haller should formulate as few questions as possible, so as not to prolong the interrogation too much and annoy the judge.
If we want to translate this setting in mathematical terms, we can identify the suspects with the first N positive integers, and hence the space of the possible hypotheses with the set $\Omega = \{1, 2, ..., N\}$: the murderer will then correspond to an element $x \epsilon \Omega$.
Expressed in this numerical way, the situation that arises in both these examples is the one formulated by the Polish mathematician Stanisław Ulam in the following terms in his book *Adventures of a Mathematician* in 1976 [117]:

"Someone thinks of a number between one and one million (which is just less than 2^{20}*). Another person is allowed to ask up to twenty questions, to each of which the first person is supposed to answer only yes or no".*

In our case, as said, the questioner is Haller, the answerer the witness. In truth, the value of one million is unrealistic and excessive when referring to murder suspects. Anyway it is reasonable to fix a maximal number of questions that the latter person, i.e., the lawyer, can ask the former to force him to unmask the guilty party. In the Ulam scenary, 20 questions are enough when $N = 1000000$, because N equals just less than 2^{20}. Indeed $log_2 1000000$ is approximately 19.9. Let us explain why 20 questions with answer "yes/no" are then sufficient to find the mysterious value x when each answer is right and there is no lie. In fact, Haller could use the following strategy:

- ask the witness whether the number x is between one and five hundred thousand, to reduce the cardinality of the search space by half i.e., from just below 2^{20} to just below 2^{19},
- then continue in the same way, halving each time the solution interval, passing question after question from 2^{19} possible options to less, that is 2^{18}, from 2^{17} to 2^{16} and so on,
- until we arrive with the twentieth question below $2^1 = 2$ possibilities, i.e., at 1. At that point the true x will be revealed.

Indeed Mickey Haller could even avoid specifying the values 2^{19}, 2^{18} and so on, asking the witness each time directly, whether x is in the first or second half of the previous interval, to allow the witness an answer between *yes* and *no*. Once dropped from 2^{20} to 1, however, Haller will be able to identify x unambiguously, as long as the witness' answers are still honest. Under this hypothesis, 20 *yes*-or-*no* questions are enough to guess a number between 1 and 2^{20}, and consequently between 1 and one million.

From an abstract point of view, with reference to an initial space Ω of cardinality N (which is power of 2), corresponding as said to the positive integers from 1 to N, we can associate to each natural number t (up to the first one that exceeds the logarithm in base 2 of N), and in substance to the questions up to t, the set X_t of the positive integers selected in Ω after the relative answers. In detail we put:

- first of all, $X_0 = \Omega$;
- for each t, we subdivide X_t into two subsets of equal cardinality X and $X_t - X$, we ask whether $x \in X$ or not and we put X_{t+1} equal to the first or the second of the two sets depending on whether the answer is *yes* or *no*.

At the end of the procedure, x is the only element in the intersection of the various X_t.

But now let us suppose that, as Ulam himself imagines in his book, the questioner sometimes lies, for example once or twice. Ulam then asks, *"how many questions would one need to get the right answer"*?

In fact, this variant, which admits the possibility of lying answers, was considered before Ulam, and in a slightly different way, by the Hungarian mathematician Alfréd Rényi in 1961, in *On a problem of information theory* [105]. Thus, it is now commonly called the Ulam-Rényi game (with lies).

Rényi assumed a certain percentage e of false answers, which he attributed only to the malice of the interlocutor, but also to the possibility that the latter did not understand the question or was unaware of some fact, or to the "noise" that can be generated in the transmission channels, thus to unintentional errors in the transmission of data (for example from a shuttle or a satellite in flight to the space base on earth). For this reason, the terms "errors" and "lies" are used synonymously in Rényi's text. Instead Ulam hypothesized a maximum number e of lies that, in the case of Haller, the witness can pronounce: up to e, but not more than e. Therefore the case we have just examined is $e = 0$, that is, no lie.

Let us now consider the simplest case with lies, that of a single lie, thus $e = 1$. Haller can initially follow the same strategy as for $e = 0$ and then, in order to find the number x between 1 and N, formulate the same questions as before, so as many questions as before, corresponding to the logarithm to base 2 of N.

This time, however, the value of x that is eventually derived could be right or wrong, depending on whether or not the witness told the lie at hand.

Haller then adds a further question, asking whether the answers so far received are true or not. We distinguish four cases:

- If the answer is *yes* and the answer is truthful, then the x-value shown above is the correct one.

- If the answer is *yes* and it is false, then it represents the only admissible lie, i.e., the first lie, so that, again, the previous answers are correct and the value of x obtained is the correct one.

Ultimately, a *yes* answer means that the output obtained is right. However the same cannot be said for a *no* answer.

- If the answer is *no* and it is a lie, then there have been no previous lies and the value of x is correct, but Haller cannot know if this is really the case.
- On the other hand, if the answer is *no* and it is truthful, then it reveals a previous lie and thus raises the problem of finding it among the approximately $log_2 N$ claimed, to change it and reinterpret all the subsequent statements of the witness. In this case, the arising situation is the same as the initial one, i.e. the search for a mysterious number, referring no longer to x among N possible values, but to the position of the lie among (approximately) $log_2 N$ eventualities, with the advantage that, since the available lie has already been told, Haller is certain that his witness from now on will answer truthfully.

On the other hand, the lawyer could repeat the final question twice in succession: a double *yes* or a double *no* necessarily coincide with the truth; a *yes* and a *no*, regardless of their order, include a lie and thus ensure the correctness of the previous testimony.

We have to acknowledge that this analysis of the case $e = 1$ is rather laborious and makes us fear major complications as e increases. Anyway, fix any arbitrary maximum threshold e of lies. Now suppose to repeat the first question until receiving $e+1$ equal answers, i.e., all *yes* or all *no*. As the maximal number of lies is e, $e+1$ agreeing answers provide the correct information.
Nevertheless, the maximum number of repetitions of the question which guarantees this goal in the worst situations is $2e+1$, in the case where the first $2e$ answers are divided exactly in half: e for the *yes* ones and e for the *no* ones, so that the following answer will decide whether or not the testimony is true. The most favorable case is when the first $e+1$ answers all agree. However, whether these answers reach the number $2e+1$ or are reduced to "only" $e+1$, the repetitions to be formulated are obviously too many. Indeed the procedure will have to be renewed at the subsequent questions, albeit with reference to the number of lies left available after those already used.

To underline the ineffectiveness of this method from a computational point of view, let us return to the simple but extremely instructive case of a single lie. We have seen that in this circumstance Haller is allowed to know the truth only with some complication, at least when the first supplementary question is answered as *no*.

If one wants to minimize the execution time and the number of necessary questions, one must resort to very complex and sophisticated tools, which are based on some ideas of the American mathematician Elwyn Berlekamp, known precisely for his work on information and combinatorial game theories.
As shown in the 2002 text *Searching Games with Errors* by Andrzej Pelc [93], in the case where $e = 1$, the minimum size of the winning strategy, i.e., the minimum number of k questions needed to win the game, is given by the following minimization conditions that are obtained from Berlekamp's results:

- $min\{k: \ N(k+1) \leq 2^k\}$ if the number N is even;
- $min\{k: \ N(k+1) + (k-1) \leq 2^k\}$ if the number N is odd.

In the case where $N = 1000000 \sim 2^{20}$ the value one finds, generically and regardless of the type of question (as long as the answer is of the type *yes/no* and admitting 1 lie or error), up to an integer approximation, is 25.
In case Haller asks questions that have a specific character, e.g., comparative or bisection type questions about the search space (such as "is it smaller than...?" or "is it located in this half?") we expect a similar result to the previous one, but a higher threshold due to the tighter constraints. In fact, the estimate we get this time is $log_2 N + log_2 log_2 N + 1$ for a generic N, and thus approximately 26 for $N = 1000000 \sim 2^{20}$.

The subtle difference between the two numerical values obtained makes us realize how much the type of questions asked to the interlocutor can influence the course of the game.
Pelc himself, in his aforementioned work, underlines the blurred but palpable distinction between two different approaches to the game that translate into two different strategies of the organization of questions: the *adaptive* one whereby each question is modulated on the basis of the answers to the previous questions, or the one whereby questions are not necessarily linked to each other and belong to a pre-established list. Obviously, the first approach is the one that best suits a courtroom where a cross-examination, such as the one that sees Mickey Haller as a protagonist, is taking place and requires a good spirit of improvisation and versatility; the second tactic is the one used in the previous speculations on numbers (a strategy adopted a priori) in a situation that is not very applicable to everyday scenes. The adaptive approach allows some reduction on the minimum number of questions to be asked

only when the number of "suspects", i.e., N, is greater than or equal to 21 (for the adaptive there is then a minimum of 8 questions, which becomes 9 in the other situation). The difference between the two approaches becomes more pronounced when the number of errors and lies starts to increase. Indeed, one realizes that:

- exact estimates (as in the case of $e = 1$) can be obtained also for $e = 2$ and $e = 3$, which set the minimum number of questions, when N is one million, at 29 and 33 respectively;
- equally exact values can be found when N is a power of 2 and $e = 3$;
- the more general case with e and N being completely arbitrary still seems to be far from a solution.

As one might expect, the situation becomes more and more complicated as e increases, quickly becoming unmanageable when the questions asked no longer involve only two answers of the type *yes* or *no*.

In addition to the "computational" aspects, certain connections with logic are also of great interest in the Rényi-Ulam game. The possibility of lying means that two possible answers which are the negation of each other do not necessarily lead to an unacceptable state of incoherence, on the contrary can provide some information: for example, they ensure that the stock of lies has been reduced by one unit. This means that if the witness answers the same question first affirmatively and immediately later negatively (or vice versa), Haller will have progressed in his search for the real murderer, though. Moreover, in order to discover the true answer to the question, he will simply have to repeat it a third time (in the case of a single lie).
Translated into mathematical terms, in order to discover the logical truth value of a proposition, it is useful and not superfluous for it to be confirmed twice. Also in logic, at least in this area, the principle "repetita iuvant" (i.e., "repeating does good") applies.
Joining a proposition with itself strengthens it, in contrast to classical logic, where a proposition of the type $A \wedge A$ has the same truth value as the single A. In the logic underlying the Ulam game this is no longer guaranteed.

Moreover in the logic of the Rényi-Ulam game, the principle of the excluded third, according to which of each statement A either its positive version, i.e., A, or its negation, i.e., $\neg A$, is true, but never both simultaneously, no longer applies. Enunciating A and $\neg A$ in succession, or vice versa, does not produce any paradoxical situation since the interlocutor to whom the questions are directed is allowed to lie a certain number of times. Moreover, the player, i.e., Haller in our case, regardless of the value of e, is not so much interested in finding out whether every single answer given by the witness is reliable or not as in asking him the questions in such a way as to induce him to spend his lies as soon as possible.

From this perspective, each answer, whether affirmative or negative, contains the same precious information content.

It is then evident that in Ulam and Rényi's game the truth values of an assertion cannot be restricted to just two, i.e., 1 or 0, as in classical logic, but must be extended to 3, i.e. {*yes, no, maybe*}, or $\{1, 0, \frac{1}{2}\}$ in the case of a single lie, and to an even wider spectrum of values if the number of lies should increase.

Therefore, it becomes necessary to abandon classical logics and resort to new logics called *many-valued*, i.e., open to more truth values. These will be the subject of the next section.

8.2 Many-valued logics

The roots of many-valued logic can be traced back to Aristotle. In Chapter IX of *De Interpretatione* [4] Aristotle considers the timely sentence *"Tomorrow a naval battle will take place"*, which cannot be evaluated from the point of view of truth or falsity. The sentence belongs to a broad category of propositions that make predictions about the future, referring to future events that are unnecessary or not actually determined. The Greek philosopher thus suggests the existence of a "third" logical state for propositions.

The one who started to develop many-valued logics in a new, original and independent way was the Polish logician and philosopher Jan Łukasiewicz in 1920. He first focused on the idea of an additional third truth value, signifying "possible", "indeterminate", admitting later extensions to logics with four or five values and claiming that, at least in principle, there is no obstacle to develop infinite-valued logics.

The British mathematician and popularizer Ian Stewart describes the novelty of this point of view in the article *A partly true story* [110], in a joking and surreal tale, in which he imagines a revived Epimenides conversing with Łukasiewicz himself. Here are some lines from it. It is Epimenides himself who narrates in the first person.

«Instead of just two truth values, 1 for a true statement and 0 for a false one," Łukasiewicz said, "I am prepared to consider half-truths with truth value 0.5 or near-falsehoods with value 0.1 – in general, any number between 0 and 1».
«Why would anyone want to do that? » I asked, bemused.
Łukasiewicz smiled. «Suppose I said that the club president looks like
Charlie Chaplin. Do you think that's true?»
«Of course not!»
«Not even his feet?»
«Well, I guess they do rather...»
«So it's not completely false, either.»
«Well, he does look a bit like Chaplin. »
Łukasiewicz leaned toward me. He had very penetrating eyes.
«How much like him? »
«Around 15 percent, I'd say. »
«Good, then my statement "the club president looks like Charlie Chaplin" is 15 percent true. It has a truth value of 0.15 in fuzzy logic.»
«That's playing with words. It doesn't mean anything.»
Łukasiewicz grasped my arm.
«Oh, but it does. It helps to resolve paradoxes.»

As the story goes on, Łukasiewicz explains to Epimenides how logics less categorical than the classical one make it possible to overcome even the paradox of the liar. The argument is discussed in the case of a sheet of paper such that on one side is written that the statement on the opposite side is true, and on the other one that the statement on the opposite side is false. Łukasiewicz observes that it is sufficient to imagine an additional truth value 1/2 and to assign it to each of the two statements on the paper in order to overcome any embarrassment: in fact, by doing so, each of the two statements will be considered neither true nor false.

Many-valued logics (usually referred to as MVL) differ from classic logics precisely because they no longer have just two, but a greater number, if not an infinity of truth values. The spectrum of these values is thus broader than the traditional 1 and 0. These latter remain, meaning respectively "true" and "false", or rather "absolutely true" or "absolutely false" (since intermediate possibilities will also appear), but other options are added.

The assignment of these truth values should again follow precise rules, starting from the evaluation of the simplest formulas. For example, it must respect the principle that, if one component of a formula is replaced by another one with the same truth value, the evaluation of the overall formula also remains unchanged. Even many-valued logics, like classic logics, rely on the connectives $\wedge, \vee, \neg$ and $\rightarrow$, suitably adapted and integrated. However, it must be stressed that, already in the case of 3 truth values, i.e., 0, 1, and $\frac{1}{2}$, the total number of n-ary connectives (for a positive integer n) gets greater as n increases, if compared to classic logic. In fact, an n-ary connective must be understood as a function of $\left\{0,\ 1, \frac{1}{2}\right\}^n in\ \left\{0,\ 1, \frac{1}{2}\right\}$. Consequently, the n-ary connectives increase in total from 2^{2^n} to 3^{3^n}. In particular:

- 1-ary connectives become $3^{3^1} = 27$ instead of $2^{2^1} = 4$,
- binary connectives become $3^{3^2} = 19683$ instead of $2^{2^2} = 16$.

Moreover, when we expand the truth values of a proposition, we will obviously have to revise their assignment.
The trivalent logic L_3 constructed by Łukasiewicz represents a first example and model. The following tables illustrate how negation and implication are evaluated in L_3. They refer to arbitrary formulas F and G.

1) The connective $\neg$

F	$\neg F$
1	0
0	1
1/2	1/2

2) The connective $\rightarrow$

F	G	$F \to G$
1	1	1
1	0	0
0	1	1
0	0	1
1/2	1/2	1
1/2	0	1/2
1/2	1	1
1	1/2	1/2
0	1/2	1

The other connectives of disjunction and conjunction are introduced through the following definitions:

- $F \vee G = (F \to B) \to B$,
- $F \wedge G = \neg(\neg F \vee \neg B)$.

The tables concerning them are the following ones.

3) The connective $\vee$

F	G	$F \vee G$
1	1	1
1	0	1
0	1	1
0	0	0
1/2	1/2	1/2
1/2	0	1/2
1/2	1	1
1	1/2	1
0	1/2	1/2

4) The connective $\wedge$

F	G	$F \wedge G$
1	1	1
1	0	0
0	1	0
0	0	0
1/2	1/2	1/2
1/2	0	0
1/2	1	1/2
1	1/2	1/2
0	1/2	0

In particular in L_3 "false implies possible" is held to be true (see the last line of the table of $\rightarrow$), in full respect of the principle *"ex falso quodlibet"*. There are, however, 3-valued logics that move in another direction. For example, in the weak 3-valued logic K_3^I of Stephen Kleene (a 20th century American logician) "false implies possible" is declared possible because of the uncertainty that the eventuality "possible" entails, as we read in [76].
As already mentioned, for each $m > 2$ one introduces to the Łukasiewicz mode a logic L_m with m truth values, i.e. $0, \frac{1}{m-1}, \frac{2}{m-1}, \ldots, \frac{m-2}{m-1}, 1$: in particular the three aforementioned values 0, $\frac{1}{2}$, 1 for $m = 3$, or 0, $\frac{1}{3}$, $\frac{2}{3}$, 1 for $m = 4$ and so on.
In 1993 Daniele Mundici, in his article *The logic of Ulam's game with lies* [80], proved that the most adequate logic for Rényi and Ulam's game with e lies is exactly that of Łukasiewicz L_{e+2} with $e+2$ truth values 0, $\frac{1}{e+1}$, $\frac{2}{e+1}, \ldots, \frac{e}{e+1}, 1$.
Nowadays, the landscape of many-valued logics is very wide. In fact, they can be applied not only to Ulam's game with lies, but also to various situations of uncertainty in everyday life.

The 1970*s* were marked by an interest in *fuzzy* sets and logics. This new approach to the notion of uncertainty is suggested by certain applications to computer science. It was initiated by Lofti A. Zadeh, a US-born Soviet mathematician and engineer from the University of California, Berkeley, known for his contributions in the field of systems theory and automatic controls. He worked between 1972 and 1979, taking up for *fuzzy* set theory certain insights that can be traced back to Descartes, Russell and Einstein.

Zadeh himself illustrates his ideas in the following quote from *Fuzzy logic, neural networks and soft computing*, a 1994 article [127]: *"The term fuzzy logic is currently used in two different senses. In a narrow sense, fuzzy logic is a logical system that aims at a formalization of approximate reasoning. As such, it is rooted in multivalued logic. [...] In a broad sense, fuzzy logic is almost synonymous with fuzzy set theory ... a theory of classes with unsharp boundaries. [...] What is important to recognize is that ... today the growing tendency is to use the term fuzzy logic in its broad sense"*.

Thus the premises are the same as in Aristotle and Łukasiewicz. Let us propose them again, imagining the case of a gentleman, let's call him Horace, who lays petunia seedlings in a flowerbed in his garden, without bothering to bury and fertilize them and thus ensuring that they survive. So, can we say that Horace *"planted"* petunias? It is difficult to admit that, if we compare his actions to those of a qualified gardener. It becomes easier, if we compare his behavior to someone who throws petunias straight into the bin. An example that leads even Zadeh to consider intermediate truth values between "absolutely true" and "absolutely false", which he calls "degrees of truth".

But it is in deductive calculus that *fuzzy* logic shows itself to be original and different. In fact, in many-valued logics as in classical ones, the "inferential" apparatus, i.e., the system of rules that oversee deductions, moves from certain formulas (the hypotheses) to deduce others (the theses or consequences). In general, the truth value of the hypotheses determines that of the consequences.

Instead, in *fuzzy* logic one starts from a *fuzzy* set of hypotheses to produce a *nuanced* set of formulas that can be deduced from it. In other words, in *fuzzy* logic, both being hypotheses and being deducible from given hypotheses are vague concepts. Thus, both the premises and the conclusion have an "indistinct" degree of truth, which can vary over a spectrum of predetermined values.

This brings us to *fuzzy* sets and how to interpret the concept of membership.

In classical set theory, specifically in the ZF system of Zermelo and Fraenkel, there is an axiom, called separation axiom, which allows to carve out within a set S the subset of elements $x \in S$ that verify a given "property" P.

Nevertheless, in the fuzzy domain this consideration cannot remain so strict. In the set of petunias there are *fuzzy* properties, such as those of being planted, which change their meaning depending on whether a professional gardener, Horace, or someone who throws them in the rubbish takes care of them. Otherwise, referring to the arguments of the previous chapter, in the set of all men there are *nuanced* properties such as “young”, “big”, “tall”, “bald”, of which it is not easy to fix the boundaries. Is it possible to apply the axiom of separation also to these properties? In other words: do expressions such as “the set of young men”, “the set of big men”, “the set of tall men”, “the set of bald men” make sense? When does a man start to be young, or big, or tall, or bald? Let’s focus on the first case: it is clear that a 10 years old boy is young, but an old 90 years old man isn’t anymore. But when does the end of youth and the beginning of old age officially take place?

In the *fuzzy* approach the various properties (being young, or big, or tall, or bald) are understood vaguely and can only occur with a fuzzy degree of truth (which, in the case of youth, is 1 or nearly for the 10-year-old, 0 or nearly for older people, more indistinct in the intermediate ages).

Moreover, this is how it is in common language, which is fluid and devoid of excessively rigid oppositions. The *fuzzy* approach is particularly favoured in the legal sphere and also in the medical sphere, where it is difficult to provide a clear-cut characterization of conditions such as “sick”, “healthy”, “prediabetic”, “osteopenia”, and so on.

The fuzzy point of view has also produced technological devices in areas where qualitative evaluation elements are ill-suited to the use of binary logic. The modern theory of automatic controls, which originally dealt with well-defined problems with as precise information as possible with excellent results, has recently opened to different perspectives and more complex non-linear control techniques, for example when

- the system is not precisely known,
- there are considerable parametric variations,
- the multiplicity of objectives to be achieved makes decision-making difficult.

One of the most interesting prerogatives of *fuzzy* logic, recently explored, is precisely the possibility of converting elements of human experience into numerical algorithms; the result is automatic or semi-automatic procedures with artificial experience.

Chapter 9

Diophantine games and the theory of computability

9.1 Playing with equations

Algebra is generally regarded as the branch of mathematics dealing with equations. Its own name seems to confirm this; in fact, it derives from the Arabic "al-jabr", a word that appears in the title of a work dating back to the IX century A.D., by the Persian mathematician Mohammed ibn-Musa al-Khwarizmi, dedicated precisely to equations. Indeed, "al-jabr" means "reduction" and refers to the procedure that moves negative terms in an equation from one member to another by changing their sign.

Nowadays algebra, although inspired by equations, has progressively become the abstract science of structures. Moreover the mere solution of equations is generally considered as a useless and boring exercise, anything but a game. Nevertheless, a simple example may convince otherwise.

Let's imagine two players, A and B, facing each other in a battlefield consisting of an equation with integer coefficients, such as $x_1 + y_1 + x_2 = y_2^2$. The indeterminates x_1, x_2 are those of A, while the others y_1, y_2 are those of B. The game between the two is played as follows

- first A chooses a natural value for x_1, for example $X_1 = 3$, so that the equation becomes $3 + y_1 + x_2 = y_2^2$;

- then B chooses a natural value for y_1, such as $Y_1 = 6$, so that the equation becomes $9 + x_2 = y_2^2$;
- A chooses for x_2 the value $X_2 = 1$, so that the equation becomes $10 = y_2^2$;
- at this point B has no way of answering with any natural value Y_2 for y_2 that satisfies $10 = Y_2^2$ because 10 is not a square.

It is then agreed that A is the winner, as well as in all cases where the choice of indeterminates does not satisfy the equation. Otherwise, the winner is B.
Actually, A always has a winning strategy in this game, because with the choice of the value of x_2 he can always obtain that the sum $x_1 + y_1 + x_2$ is not a square. In fact, there are arbitrarily large natural numbers that are not squares.

Every equation with integer coefficients in an even number $2n$ of indeterminates generates to a similar game, where the two players alternately replace the unknowns $x_1, y_1, \ldots, x_n, y_n$ with natural numbers. If the equation is eventually satisfied, B wins. Otherwise, A does.

These games are then linked to a delicate and fascinating subject in mathematics, namely Diophantine equations, i.e., equations with integer coefficients where integer or even natural solutions are searched. The adjective "Diophantine" is a tribute to the III century A.D. Alexandrian mathematician Diophantus, who studied these topics. We already met him in Section 6.20. It is well known that Diophantine equations, despite their simple appearance, are very tricky. Let us therefore devote the next two paragraphs to reminding of their dangers and highlighting their surprising links with logic.

9.2 Diophantine equations

The restriction on the solutions of Diophantine equations, to be found in the range of integers or even naturals, seems to simplify their search. But on the contrary, this restriction often proves to be a complication. Here is a historically famous example that illustrates the pitfalls.

The problem of the cattle farmer (Euler, *Elements of Algebra* [48], Part II, Chapter 1, Question 6) A farmer lays out the sum of 1770 crowns in purchasing horses and oxen; he pays 31 crowns for each horse, and 21 crowns for each ox. How many horses and oxen did he buy?

The initial impression is that the solution is easy to find. In fact, let x, y denote respectively the number of oxen and horses bought. Then we obtain the following equation with integer coefficients:

$$31x\ +\ 21y\ =\ 1770.$$

This has two unknowns and one can express the first as a function of the second, for example y from x as

$$y = \frac{-31x\ +\ 1770}{21}.$$

It is in fact convenient to isolate here, for reasons that we shall see, the unknown with the smallest coefficient in absolute value, which is 21 of y, but of course there is no prohibition to prefer x instead.
Nevertheless, the hope of a quick solution is only illusory. One just has to reflect for a moment to realize that if, for example, $x = 0$ (that is, if the farmer does not buy any ox) then we obtain $y = 1770/21 = 590/7$: a rational value but not an integer one, because in $\mathbb{N}$ the division of 590 by 7 is not exact and gives the quotient 84 and the remainder 2 (the quotient and the remainder of 1770 with respect to 21 are consequently 84 and 6). Well, 590/7 would be the number of horses bought. But to such a conclusion it is easy to object that horses are bought in full, and not in sevenths or twenty-firsts.
Furthermore, it could happen that, for positive integer values of x, the other indeterminate y takes on negative integer values, which is similarly absurd in Euler's problem. However, this eventuality can be quickly remedied by imposing the condition $31x\ \leq\ 1770$ on the solutions.
Clearly it is much less easy to find integer solutions in the infinity of rational ones. Nevertheless, Euler devised a quick and brilliant procedure.
First, we have to note that our equation certainly admits integer solutions because the greatest common divisor of the coefficients of the indeterminates, $GCD(21, 31) = 1$, divides the constant term 1770.
In fact, by Bézout's identity, this greatest common divisor is represented as a linear combination of 21 and 31 with integer coefficients and, as a divisor of 1770, transfers this property to it. Indeed, the Bézout identity approach and ultimately the Euclidean successive division algorithm provide an alternative procedure for finding

these integer solutions. But let us focus on Euler's method and, reassured on this preliminary point (the existence of integer solutions), let us proceed, deriving from the previous expression of y and the division in $\mathbb{N}$ of 1770 and 31 by 21 (precisely, $1770 = 84 \cdot 21 + 6$ and $31 = 1 \cdot 21 + 10$),

$$y = -x + 84 + \frac{-10x+6}{21}.$$

Let us denote by t the algebraic fraction $(-10x+6)/21$. We thus obtain the integer equation

$$21t + 10x = 6,$$

which is simpler than the previous equation because the coefficient with the smallest absolute value is reduced from 21 to 10. Furthermore, the original indeterminates x, y can be expressed in a parametric form with respect to t, firstly x as $(-21t + 6)/10$ and consequently y, again as a linear function of t with rational coefficients.
Repeat this procedure until, each time the representations of x, y being simplified by the new parameter, the same x, y are expressed as linear functions with integer coefficients (and not only rational ones) of this parameter. Thus, each integer value of the parameter produces two integer values for the indeterminates. It is easily checked whether these values respect the conditions $x \geq 0$ and $31x \leq 1770$. It turns out that the natural solutions of (x, y), net of the negative solutions to be excluded for each of the unknowns, are only three, namely $(9,\ 71), (30,\ 40)$ and $(51,\ 9)$.

In general, if we consider polynomials with integer coefficients looking for integer roots (we refer to polynomials of any degree, and in any number of indeterminates), the situation that arises is extremely varied. In fact, the answers are sometimes affirmative and sometimes negative, confirming or excluding solutions in $\mathbb{Z}$, often because of a sign that changes, or a coefficient that increases or decreases by 1.
For instance

$$2x+4=0, \quad x^2-1=0, \quad x^2+y^2-1, \ \ldots$$
$$2x+5=0, \quad x^2-2=0, \quad x^2+y^2+1, \ \ldots$$

are all equations with integer coefficients, with almost intangible differences between them, at least if compared column by column; however, in the first row they also have integer solutions, respectively -2, ± 1, $(\pm 1,\ 0)$ and $(0,\ \pm 1)$ while in the second they do not.

There are many examples, at least as famous as that of the Euler farmer, of equations that

- admit integer coefficients (possibly negative),
- but lack integer roots.

Indeed, in this way we encounter polynomials with integer coefficients whose roots are

- rational and not integer, such as $3/2$ for $2x-3$,
- or real and irrational, such as the golden number $\phi, \sqrt{2}, \sqrt[3]{2}$ for x^2-x-1, x^2-2, x^3-2 respectively,
- or even imaginary such as i for x^2+1.

Let us now propose other famous examples of Diophantine equations - just a few among many possible ones.

The Bombelli equation. Singular is the case of

$$x^3-15x-4,$$

a polynomial usually associated with the name Rafael Bombelli, an Italian mathematician of the Renaissance. It is not difficult to see that this polynomial admits the integer root 4 (which is among the integer divisors of the constant term -4): $4^3-15\cdot 4-4=0$.
Nevertheless, whoever, being aware of the solution formulas of the third-degree equations in one unknown (those that Bombelli and his Italian colleagues of the same epoch determined), proceeded to apply them, would find himself in front of a surprise, namely the necessity to obtain, at a certain point of the calculation, the square root of -121, that is $11i$ if i exists, and nothing apparently sensible otherwise.
However, if we accept the first option, the i that appears then vanishes and finally gives way to the 4 that we are looking for, together with two other irrational solutions.

The Pythagorean equation and Pythagorean triples. Another important Diophantine equation that has marked the history of mathematics is the homogeneous second-degree equation (with integer coefficients) of the Pythagorean Theorem

$x^2+y^2=z^2$. It admits so-called *trivial* integer solutions (those for which one of a and b is 0, and the other equals c).
But, as said in Chapter 5, there are also solutions (a,b,c) with a,b,c positive integers (therefore non-trivial): *the Pythagorean triples*, such as (3, 4, 5) or (5, 12, 13). In this case a,b,c are the measures of the catheti and hypotenuse of a right-angled triangle (as can be seen from Figure 5.9). From an algebraic point of view, other integer solutions such as $(\pm 3, \pm 4, \pm 5)$ and $(\pm 5, \pm 12, \pm 13)$ can be added, which lose their geometric meaning.
There are also solutions that go beyond the integers (as in the case, already implicitly considered above, in which $x=y=1, z=\cdots ?$).
The "recipe" proposed by Euclid (*Elements*, Book X, Lemma 1 at Proposition 29 in [44]) and already sketched in Chapter 5, gives us almost all the Pythagorean triples. Indeed, in Euclid's original text, arithmetic is somewhat confused with geometry, the positive integers become segments and are thus identified with their measurements, in fact we used this feature to translate it into a proof without words (Section 5.2). Nevertheless, adapted in a modern key, i.e., in algebraic rather than geometric terms, the recipe suggests taking, as we know, two positive integers $u>v$ and then constructing

$$a=u^2-v^2, \quad b=2uv, \quad c=u^2+v^2.$$

It is easy to verify that (a,b,c) is a Pythagorean triple. However, some Pythagorean triples escape this construction. As already underlined, this is the case with $(9,12,15)$, since 15 cannot be expressed as the sum of two squares.
Call *primitive* any Pythagorean triple whose components are coprime, as for (3, 4, 5) and (5, 12, 13) but not for (9, 12, 15). In the millennia after Euclid, the work of various mathematicians, in particular Kronecker, made it clear that

- all primitive Pythagorean triples (a,b,c) are obtained by Euclid's recipe, i.e., as $a=u^2-v^2$, $b=2uv$, $c=u^2+v^2$ starting from two positive integers $u>v$ **prime to each other and of opposite parity**
- each non-primitive Pythagorean triple is obtained from a primitive one by multiplying its components by their greatest common divisor (e.g., $(9,\ 12,\ 15) = (3\cdot 3,\ 3\cdot 4,\ 3\cdot 5)$).

Fermat's Last Theorem. An immediate generalization of the Pythagorean equation to a polynomial of integer degree $n>2$ leads to the Diophantine equations

$x^n + y^n = z^n$. These are the subject of the so-called Fermat's Last Theorem, in memory of the French mathematician Pierre de Fermat who first enunciated but did not prove it. We already introduced it in Section 6.20. According to its statement there are no non-trivial integer solutions (thus triples composed of integers all non-zero) to the previous equation when the exponent n is greater than 2. In the margins of a copy of Diophantus' *Arithmetica* [39], in correspondence to problem VIII of Book II (*"splitting a given square into the sum of two squares"*), which thus referred to Pythagorean triples, Fermat himself noted: *«I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.»*
The mystery remained until 1994, when Andrew Wiles (1953 - ...) provided the first complete proof of the theorem, based on sophisticated mathematical tools such as elliptic curves, modular forms and so on, unthinkable in Fermat's time.

The Hardy-Ramanujan number. Which positive integers can be expressed in more than one way as the sum of two cubes? In other words, does the Diophantine equation $x^3 + y^3 = z^3 + t^3$ admit positive integer solutions for which we have $\{x, y\} \neq \{z, t\}$? The minimum integer that is expressed in two distinct ways as the sum of two cubes of positive integers is 1729. In fact:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

This number and its double representation are famous because they are linked to the following anecdote from Ramanujan's life story told by Hardy: we take it from D.R. Hofstadter's book, *Gödel, Escher, Bach: an Eternal Golden Braid*, 1979 [65].

«I remember once going to see him [Ramanujan] when he was lying ill at Putney. I had ridden in taxi-cab N. 1729, and remarked that the number seemed to me rather a dull one, and that I hoped was not an unfavorable omen. "No, Hardy," he replied, "it is a very interesting number; it is the smallest number expressible as a sum of two cubes in two different ways". »

Catalan's conjecture. Diophantine equations are also connected to the famous conjecture proposed in 1844 by the French mathematician Eugène Catalan (later proved in 2002 by the Romanian mathematician Preda Mihăilescu), according to which the only two "pure" powers of non-zero natural numbers whose difference is 1 are $3^2 = 9$ (a square) and $2^3 = 8$ (a cube). Positive integer solutions are therefore sought for the equation

$$x^2 - y^3 = 1 \ ,$$

or more generally

$$x^n - y^m = 1,$$

with n, m integer exponents greater than 1. The only possible combination is that for which $x = m = 3$ and $y = n = 2$.

Pell's equations. Finally, let us consider Diophantine equations of the form

$$x^2 - dy^2 = 0 \ ,$$

with d a positive integer. Euler linked them by mistake to the name of the mathematician John Pell (1611-1685), after which they are named. We note that they all have the trivial integer solutions $x = \pm 1$ and $y = 0$.
As far as non-trivial solutions are concerned, we distinguish two cases:

- for d a perfect square there is no way to express 1 as the difference of two non-zero squares, $1 = x^2 - \left(\sqrt{d}\, y\right)^2$, so there are no non-trivial solutions;
- the case where d is not a perfect square is the only really interesting one; a broad and sophisticated theory intervenes to classify the non-trivial solutions.

9.3 H10 and DPRM

In the face of such a variety of complicated examples, it is not surprising that, among the famous 23 problems that David Hilbert proposed to the mathematical community in 1900, one finds, precisely at place number 10, the one of recognizing with an appropriate algorithm polynomials with integer coefficients that also have integer, or even natural roots. Here is the way Hilbert himself state it (English translation).

H10, Hilbert's Tenth Problem. *Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.*

Incidentally: neither the degree nor the number of indeterminates of the polynomials under investigation receive any bound. In fact, if one narrows the setting of the investigation appropriately, algorithms that fulfil this requirement can sometimes be found. Let us present three examples, at least two of which recur routinely in the teaching of high-school mathematics.

The case of degree 1. Let us first focus on equations of degree 1 in an arbitrary number of unknowns, thus of the form

$$a_1x_1+\ldots+a_nx_n=b$$

with n positive integer, $a_1,\ldots,a_n$,b integers and $a_1,\ldots,a_n$ not all 0. As we have already anticipated when discussing Euler's farmer problem, this equation $a_1x_1+\ldots+a_nx_n=b$ admits integer solutions $z_1,\ldots,z_n$ if and only if the greatest common divisor d of $a_1,\ldots,a_n$ divides b.

Here is the proof.

First suppose that the equation has an integer solution $(z_1,\ldots,z_n)$, so $a_1z_1+\ldots+a_nz_n=b$. Let d be the greatest common divisor of the coefficients $a_1,\ldots,a_n$. Then for each $i=1,..,n$ there exists an integer b_i for which $a_i=db_i$. It follows that $b=db_1z_1+\ldots+db_nz_n=d(b_1z_1+\ldots+b_nz_n)$ is divisible by d.
Conversely, we know from Bézout's identity that the greatest common divisor d of $a_1,\ldots,a_n$ is expressed as their linear combination with integer coefficients $d=a_1u_1+\ldots+a_nu_n$, where indeed the integers $u_1,\ldots,u_n$ are calculated explicitly with the Euclidean algorithm of successive divisions. If d divides b, i.e., $b=dq$ by some integer q, we deduce $b=a_1qu_1+\ldots+a_nqu_n$.

The case of a single indeterminate. Let us now consider equations of arbitrary degree, but with only one indeterminate x, thus expressible in normal form as

$$a_0+a_1\cdot x+a_2\cdot x^2+\ldots+a_n\cdot x^n=0$$

with n positive integer, $a_0,a_1,\ldots,a_n$ integers, $a_n\neq 0$.
We proceed as usual in the search for integer solutions. It is clear that if $a_0=0$, then the equation possesses the 0 solution in $\mathbb{Z}$. Therefore, we can assume that a_0 is different from 0. It is then well known that integer solutions, if they exist, are to be found in the finite framework constituted by the divisors of a_0. In fact, if z is an integer solution of the given equation, it turns out that $z(a_1+a_2z+\ldots+a_n\cdot z^{n-1})=-a_0$, i.e. precisely that z is a divisor of a_0.

Consequently, in the worst-case scenario, it is sufficient to perform a systematic brute force check, extended to these values, in order to identify among them those that eventually solve the equation. It is in this way that, for example, one arrives at the root 4 of the Bombelli equation.

An equation of degree 2 in two indeterminates. Finally, let us deal with the case of an equation of degree 2 in two indeterminates x, y of the form

$$a \cdot x^2 + b \cdot y = c$$

where this time we assume that a, b, c are positive integer and we look for natural values (i.e., non-negative integers) for x and y. Then, we have

$$0 \leq x \leq a \cdot x^2 \leq c, \quad 0 \leq y \leq b \cdot y \leq c.$$

It follows that the area in which to search for solutions is finite, included between 0 and c, consequently it can be explored again by brute force methods, aimed at checking every possible value of x, y between 0 and c.

Let us come back to H10. Note then that an algorithm capable of deciding the presence of integer roots generates one to detect the existence of natural roots. It is sufficient to apply Lagrange's classical theorem of 1770, according to which in $\mathbb{Z}$, the natural numbers (i.e., non-negative integers) coincide exactly with the sums of four squares. Thus, a polynomial equation such as that in Euler's problem $31x + 21y = 1770$ admits for x, y solutions in $\mathbb{N}$ (thus expressible as sums of 4 squares) if and only if in $\mathbb{Z}$ the following polynomial equation in $2 \cdot 4 = 8$ variables, easily obtainable from the previous one, has solutions,

$$31\left(t_1^2 + t_2^2 + t_3^2 + t_4^2\right) + 21\left(z_1^2 + z_2^2 + z_3^2 + z_4^2\right) = 1770.$$

Hilbert's problem disregards, as mentioned, limitations on the degree and number of indeterminates and the resulting facilities and requires a completely general algorithm.

However, the answer to Hilbert's tenth problem, obtained in 1970 by Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matijasevic, is unexpected ([77], [34] and [35]): in fact, instead of providing the algorithm sought, it excludes its existence.

Theorem (Davis-Putnam-Robinson-Matijasevic DPRM). *There exists no* *algorithm capable of distinguishing, for every integer coefficient polynomial, whether it admits integer roots or not.*

This conclusion derives from the developments in mathematics that took place between 1900 and 1970, and in particular from the revolution that occurred in 1936, when Turing proposed his computational model, as already illustrated in Chapter 1. Let us briefly explain the link with polynomials.
As seen in Chapter 1, a statement such as *"there is an algorithm"* (to solve a certain problem on natural or integers) is objectively vague. Even more so is its negation *"there is no algorithm"* for that given purpose. In fact, if in the positive case an algorithm can be produced to prove its existence, in the negative version no such constructive argument can help. The concept of an "algorithm" is only intuitive. Well, Turing's intention was precisely to give a mathematically rigorous content to these assertions, as briefly summarized in Chapter 1, via the notion of "Turing machine". Since this concept can be well defined in mathematical terms, the question of whether or not an algorithm exists also takes on its own consistency and clarity. By *"problem"* we mean here a question such as the following: given a subset W of $\mathbb{N}$, decide the membership of W of a generic $n \in \mathbb{N}$, i.e., establish whether n is in W or not.
Then this set W is said to be:

- *decidable* if there exists an algorithm, i.e., there exists a Turing machine, which separates the elements inside W from those outside,
- *semidecidable* if there exists an algorithm, i.e., there exists a Turing machine, which at least lists the elements of W (without necessarily recognizing those outside).

The concept of semidecidability is thus weaker than decidability. In fact it is shown that W is decidable if and only if it is semidecidable together with its complementary $\mathbb{N} - W$ (the so-called *Post theorem*): in fact there is an algorithm that knows how to distinguish the elements inside and outside W if and only if one has actual lists of both the elements of W and those of the complementary - scrolling through them one can easily establish, case by case, whether the input n considered is in W or not.

Above all, one discovers sets W of naturals that are

- semidecidable but not decidable (so they admit algorithms that list their elements, but not procedures that distinguish their elements from others),

- or even not semi-decidable.

The theorem of Davis, Putnam, Robinson and Matijasevic connects these abstract theorems to the world of integer coefficient polynomials and thus transfers the cases of undecidability from subsets of $\mathbb{N}$ to the solutions of integer coefficient equations and specifically to the Hilbert tenth problem. The correlation is established at the key point of its proof, where the semi-decidable subsets W of $\mathbb{N}$ are characterised as the Diophantine ones: those for which there exists a polynomial $q_W(x, y_1, \ldots, y_n)$ with integer coefficients such that, for every natural number N, N belongs to W if and only if, by intervening in that polynomial as a parameter instead of x, it allows natural solutions for the equation $q_W(N, y_1, \ldots, y_n) = 0$.

Thus we discover even in H10 how the study of equations significantly intersects the history of scientific thought, in particular the essence of the concept of algorithm. Through it algebra and logic, are also connected to the genesis of modern computer science and point out its unexpected limitations, i.e., the existence of cases, singular but not circumscribed, in which the desired algorithm does not exist.

9.4 Diophantine games

Let us return to Diophantine games. As already underlined, the initial example of this chapter can be extended to any polynomial equation $p(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$ with integer coefficients, in an arbitrary number of indeterminates, which we assume to be $2n$ and indicate by $x_1, \ldots, x_n, y_1, \ldots, y_n$ (we will recall the reason for this apparent restriction in a moment).

The relative game always involves two players A and B, who proceed as follows: within $\mathbb{N}$

- A chooses a value X_1 for x_1,
- B opposes him a value Y_1 for y_1,
- A selects X_2 for x_2,
- B opposes him a value Y_2 for y_2,

and so on, until X_n, Y_n for x_n, y_n respectively.

If at the end of this procedure $p(X_1, \dots, X_n, Y_1, \dots, Y_n) = 0$, then B wins. Otherwise, for $p(X_1, \dots, X_n, Y_1, \dots, Y_n) \neq 0$, A wins.

Warning: in the polynomial $p(x_1, \dots, x_n, y_1, \dots, y_n)$ some of the indeterminates $x_1, \dots, x_n, y_1, \dots, y_n$ may only appear in figure and not in substance. As if to say that the involved player renounces the corresponding move. In this way the assumption made, of an even number $2n$ of indeterminates, becomes legitimate.

Diophantine games were proposed by James Jones in 1982 [67]. They are clearly inspired by the solution of H10 and related issues, but they are also linked to the important contribution to game theory made by Michael Rabin in 1957 [103].

Here are other examples of Diophantine games.

Example 1. Let us again consider Euler's farmer problem and describe the corresponding Diophantine game, based on the equation $31x_1 + 21y_1 = 1770$. In it:

- A chooses a natural value X_1,
- B answers a natural value Y_1.

In the end, B wins if and only if $31X_1 + 21Y_1 = 1770$. From our previous discussion, it is easy to deduce that A possesses a winning strategy, all he (or she) needs to do is to avoid choosing 9, 30 and 51 as x_1, at which point B will have no way to successfully reply.

Example 2. Let us now return to Catalan's conjecture. We write the corresponding equation in the form

$$(x_1 + 1)^2 - (y_1 + 1)^3 = 1$$

so that when x_1, y_1 take on natural values, $x_1 + 1, y_1 + 1$ become positive integers. The game between the players A and B now develops as follows:

- first A chooses a value for x_1 among the natural numbers,
- then B contrasts it with a value for y_1 also in $\mathbb{N}$.

If in this way the equation is solved, B wins. Otherwise A wins.
Recalling the solution of the conjecture, it is easy to deduce that the latter has an easy winning strategy, i.e., to choose for x any value other than 2. At that point B will have no way of answering him guaranteeing equality.
The game could be extended to all cases in which the exponents 2, 3 are replaced by an arbitrary ordered pair of values $n, m > 1$. But Mihăilescu's theorem continues to guarantee a winning strategy for A. Indeed, if $(n,m) \neq (2,\ 3)$, then there is no need of precautions: for equations containing powers other than a square and a cube, there is no admissible solution in $\mathbb{N}$.

It is time to clarify what is meant by a winning strategy for A or B.
We avoid too many details here and rely on informal definitions.

Assume then that one has a ***winning strategy for B***, if one can find

- Y_1 as a function of X_1,
- Y_2 as a function of $X_1,\ X_2$,
  ...
- Y_n as a function of $X_1,\ \ldots, X_n$,

such that $p(X_1, \ldots, X_n, Y_1, \ldots, Y_n) = 0$.

On the other hand, there is a ***winning strategy for A*** if it is possible to find

- X_1,
- X_2 as a function of Y_1,
  ...
- X_n as a function of $Y_1,\ \ldots, Y_{n-1}$,

such that $p(X_1, \ldots, X_n, Y_1, \ldots, Y_n) \neq 0$ for each choice of Y_n.

Here are other examples that illustrate this concept about more or less elementary questions of arithmetic.

Example 3. Consider the game of the equation $x_1 = y_1^2 + y_2^2 + y_3^2 + y_4^2$. Actually,

x_2, x_3, x_4 are missing, i.e. they are "fictitious": the indeterminates are evidently only 5, i.e. $x_1, y_1,\ y_2,\ y_3,\ y_4$.
But it is convenient for us to pretend that they are 8 and also include $x_2, x_3,\ x_4$. As if to say that, in the relative game, A gives up his second, third and fourth moves, leaving the initiative to B in those cases.
This time it is B who has a winning strategy: each natural number X_1 can be expressed in $\mathbb{N}$ as the sum of 4 squares, by virtue of the aforementioned Lagrange theorem.

The outcome would have been different if the squares had been 2 (the number 3 cannot be expressed as the sum of 2 squares), or 3 (the number 7 cannot be expressed as the sum of 3 squares).

Example 4. Let us now consider the equation $x_1 = 2y_1$, i.e., $x_1 - 2y_1 = 0$. Note that in this case A has a winning strategy: all he (or she) has to do is to choose X_1 odd, after which B has no way of telling him any Y_1 that would make the equation true. The arithmetical meaning drawn from this game is that not every natural number possesses its half.

Example 5. Let's take $2x_1 = y_1$, i.e., $2x_1 - y_1 = 0$. This time B has a winning strategy, he (or she) only needs to choose $Y_1 = 2X_1$. We rely here on the obvious observation that every natural has its double.

Example 6. Two possible variants of the previous examples are derived for square roots and squares, i.e., for the equations $x_1 = y_1^2$ and $x_1^2 = y_1$, i.e., $x_1 - y_1^2 = 0$ and $x_1^2 - y_1 = 0$. In the first case, A has a winning strategy, because not every natural is a square; in the second case, the strategy is for B, because every natural has a square.

Example 7. An example on Pythagorean triples. Consider the equation $(2x_1+3)^2 + y_1^2 = y_2^2$, thus a variant of the Pythagorean equation.
We observe that the values of $2x_1 + 3$ when x_1 ranges over natural numbers correspond to odd integers > 1.
This time, it is B who has a winning strategy. Recall Euclid's characterization of the Pythagorean triples, and note that

$$2X_1 + 3 = (X_1+2)^2 - (X_1+1)^2.$$

Then, B only needs to choose

$$Y_1 = 2 \cdot (X_1 + 2) \cdot (X_1 + 1), \quad Y_2 = (X_1 + 2)^2 + (X_1 + 1)^2.$$

Example 8. Finally, consider the case of $x_1y_1 + x_2y_2 = 1$. Here the winning strategy is for A: (s)he only needs to choose X_1, X_2 that are not coprime e.g., $X_1 = 2, X_2 = 4$, so 1 cannot be expressed in the desired form. In particular, there is no way to express 1, which is odd, as $2Y_1 + 4Y_2$, which is still even.

9.5 Links with game theory

According to the conventions of game theory, Diophantine games are finite games (i.e., with a limited number of moves) between 2 players, with perfect information and victory or defeat outcome, and with no random moves. A famous theorem of Zermelo and von Neumann then applies and ensures that in each of them exactly one of the two opponents has a winning strategy.

In truth, in the specific case of Diophantine games, this general property is derived in a direct and very simple way thanks to logic. It is in fact the principle of the excluded third that guarantees, for every polynomial with integer coefficients $p(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$ (with n a positive integer), that exactly one of the following two statements is true among the naturals:

- either the statement
  $\exists x_1 \forall y_1 \exists x_2 \forall y_2 \ldots \exists x_n \forall y_n \; p(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) \neq 0$,
  in which case A admits a winning strategy,
- or its negation
  $\forall x_1 \exists y_1 \forall x_2 \exists y_2 \ldots \forall x_n \exists y_n \; p(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n) = 0$ and then it is B who possesses it.

Therefore in this setting the Zermelo-von Neumann theorem gets almost trivial.
But at this point another question arises in a natural way, i.e. to establish case by case, that is, i.e., polynomial by polynomial, who is the lucky player between A and B, the one with a winning strategy. We will discuss this subject in the following paragraphs.

We conclude this by emphasizing how Diophantine games also provide an opportunity to introduce the highly topical subject of game theory and its fascinating applications to economics.

9.6 Links with computability theory

The connection with H10 links Diophantine games also to computability theory, with some surprising results. Let us explore this topic here. A result by Jones, which characterizes the semidecidable subsets of $\mathbb{N}$ in terms of equations, or rather diophantine inequalities, is useful to us.

Theorem 1. (Jones, [67]). For every semidecidable subset W of $\mathbb{N}$ there exists a polynomial $p_W(x, x_{1,} y_1, x_2, y_2)$ with integer coefficients and 5 indeterminates such that, for every natural number N, N belongs to W if and only if in $\mathbb{N}$ it is true that $\exists x_{1,} \forall y_1 \exists x_2 \forall y_2 \; p_W(N, x_{1,} y_1, x_2, y_2) \neq 0$

Passing to Diophantine games, the same condition can be formulated as follows. Note that, for each natural number N, the polynomial $p_W(x, x_1, x_2, y_1, y_2)$ generates one in 4 variables, $p_W(N, x_1, x_2, y_1, y_2)$, in which N substitutes the first indeterminate x as a parameter. Therefore N belongs to W if and only if, in the game related to $p_W(N, x_1, x_2, y_1, y_2)$, the player A has a winning strategy.

Corollary. For every semidecidable subset W of $\mathbb{N}$ there exists a polynomial $p_W(x, x_{1,} y_1, x_2, y_2)$ with integer coefficients and 5 indeterminates such that, for every natural number N, N belongs to W if and only if A has a winning strategy in the Diophantine game of $p_W(N, x_1, x_2, y_1, y_2)$.

This connection to calculability theory causes unpredictable consequences for Diophantine games.
First of all, there is no general algorithm that can decide, for each game, i.e., for each polynomial with integer coefficients, who of A and B has a winning strategy. Furthermore, the result holds even in the restricted domain of polynomials in 4 indeterminates, as in Jones' article [67].

Theorem 2. There is no algorithm that decides, for each integer coefficient polynomial in 4 indeterminates x_1, x_2, y_1, y_2, who of A and B has a winning strategy in the corresponding diophantine game.

Proof. Consider a semidecidable but undecidable subset W of $\mathbb{N}$. Since W is semidecidable, Theorem 1 associates to it a polynomial $p_W(x, x_1, y_1, x_2, y_2)$ with integer coefficients and 5 indeterminates such that a generic natural number N lies in W if and only if A has a winning strategy in the diophantine game of the polynomial in 4 indeterminates $p_W(N, x_1, y_1, x_2, y_2)$.
But since W is undecidable, no algorithm can decide who of A and B has a winning strategy in games involving the polynomials $p_W(N, x_1, y_1, x_2, y_2)$ as N varies, least of all in the more general context of all integer coefficient polynomials in 4 indeterminates. $\dashv$

On the other hand, even when a winning strategy exists for A or B, we cannot be content with knowing its existence in the abstract. We would like it explained in detail, effective, algorithmic, *computable*, and then use it. Well, this concept of a *computable winning strategy* constitutes the main argument of Rabin's 1957 work *"Effective computability of winning strategies"* to which we therefore refer for a rigorous treatment. We limit ourselves here once again to an informal definition.

Following Rabin, we say that one has a ***computable winning strategy for B***, if one can give explicit algorithms that provide

- Y_1 as a function of X_1,
- Y_2 as a function of $X_1,\ X_2$,

  ...
- Y_n as a function of $X_1,\ \ldots, X_n$

such that $p(X_1, \ldots, X_n, Y_1, \ldots, Y_n) = 0$.

Similarly, one has a ***computable winning strategy for A*** if one can give explicit algorithms that provide

- X_1,
- X_2 as a function of Y_1,

  ...

- X_n as a function of $Y_1, \ldots, Y_{n-1}$

such that $p(X_1,\ldots,X_n,Y_1,\ldots,Y_n) \neq 0$ for each choice of Y_n.

That being said, further puzzles arise in this respect among Diophantine games.

Theorem 3. There exists a polynomial with integer coefficients and 6 indeterminates such that in its Diophantine game B has a winning strategy, but no computable one.

The proof adapts a result of Rabin in game theory, itself based on the existence of *simple sets* - a concept elaborated by Post in the theory of computability. These are sets S of naturals such that:

- S is semidecidable,
- the complementary $\mathbb{N}-S$ is infinite, but without infinite semidecidable subsets.

We are not discussing the relevance of the notion within computability. It is enough for us to know that these sets exist.

Proof. Let S be a simple, in particular semidecidable, set of natural numbers. Then let p_s be the polynomial in 5 indeterminates that is associated with it by Theorem 1. This time we adapt it to construct a polynomial in 6 indeterminates

$$p(x_1,y_1,x_2,y_2,x_3,y_3) = p_s(x_1+y_1,x_2,y_2,x_3,y_3).$$

Thus, a winning strategy for player B in the game of p requires to oppose to each natural X_1 chosen by A a natural Y_1 such that B still has a winning strategy for the continuation of the game, i.e., that of $p(X_1,Y_1,x_2,y_2,x_3,y_3) = p_s(X_1+Y_1,x_2,y_2,x_3,y_3)$, and thus a Y_1 such that $X_1+Y_1 \notin S$.

Since $\mathbb{N} - S$ is infinite, this computable winning strategy for B is possible: whatever X_1 A proposes, B takes out of S a natural number $M \geq X_1$ and then chooses $Y_1 = M - X_1$, so that $X_1+Y_1 = M \notin S$.

On the other hand, a computable winning strategy for B would effectively oppose to each natural X_1 a natural number Y_1 so that $X_1+Y_1 \notin S$ and thus, as X_1 increases, would algorithmically generate within $\mathbb{N} - S$ an infinite and semidecidable set, the one composed precisely of the sums $X_1 + Y_1$: a conclusion that contradicts the hypothesis that S is simple. $\dashv$

9.7 Links with computational complexity theory

We deal here with another seemingly innocent curiosity about equations, that could be reasonably proposed to high school students, but connects Diophantine games to a capital topic of modern computing. To introduce it, let us return to the particular cases of H10 on $\mathbb{Z}$ for which we have provided a solution algorithm. We refer first of all to equations of degree 1

$$a_1x_1 + \ldots + a_nx_n = b$$

for which we know there is an integer solution if and only if the greatest common divisor d of $a_1, \ldots, a_n$ divides b. As we know, the Euclidean algorithm answers this condition, and does that running in times that modern computational complexity theory recognises as short, to be precise quadratic, i.e. of second degree, with respect to the *length* of the "initial data" $a_1, \ldots, a_n$. In conclusion, the algorithm not only exists, but is executed quite effectively.
Let us now turn, again on $\mathbb{Z}$, to equations in one indeterminate

$$a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_n \cdot x^n = 0$$

with $a_n \neq 0$ and, in the interesting cases, $a_0 \neq 0$ as well. We have seen how the possible integer solutions are in the set of divisors of a_0. However, this time the search for these divisors, although elementary in principle, proves to be tricky in practice. There are no known procedures that always complete it quickly. Indeed, the best algorithms known today for retrieving the divisors of an integer take in the worst cases prohibitively long (*exponential*, to use the appropriate technical term) before providing their output. However, nothing prohibits, and nothing ensures, that for our problem faster procedures will be discovered in some future time.
Indeed, in 1999, Cucker, Koiran and Smale [31] provided an algorithm checking in a short time the existence of integer solutions for Diophantine equations in 1 indeterminate.
Finally, let us consider the third case of equations with degree 2 and two unknowns

$$a \cdot x^2 + b \cdot y = c$$

with a, b, c positive integers, for which we wish to decide the existence of roots X, Y that are non-negative, and consequently less than or equal to c. We have already seen how the finite range determined in this way again permits a brute force approach, aimed at considering all ordered pairs of integers (X, Y) with $0 \leq X, Y \leq c$ and checking for each of them whether $a \cdot X^2 + b \cdot Y = 0$ or not until the first possible positive answer. However, the cases to be explored in the worst-case scenario, when the solution is not there or is late in appearing, are $(c+1)^2$, i.e., an exponential quantity with respect to the length of c in base 10 or 2 (which coincides roughly with its logarithm in that base). As many, therefore too many, checks may be required.

The question of measuring the efficiency of an algorithm, or rather of identifying those problems that admit an efficient solving algorithm, constitutes that area of modern theoretical computer science already mentioned, and called *computational complexity*.

We have already seen in Chapter 2 that, when efficiency is evaluated with the parameter *time*, thus relating, for a given program, the duration of its computations to the length of the corresponding inputs, we assume the slogan

fast = at most polynomial.

In other words, one considers as fast a program that performs its calculations in times that are governed by a polynomial function with respect to the length of the input, and one consequently brands as slow an algorithm that instead takes, at least asymptotically, as this length varies, times that are more than polynomial, in particular exponential. Related to this issue is the $P = NP$ problem, already discussed in Chapter 2.

What is the connection with our equations $a \cdot x^2 + b \cdot y = c$? We have just underlined the difficulty of finding in a fast way its roots. On the other hand, it is easy to agree that if we can rely on a bit of help, i.e., if solutions X, Y for x, y exist between 0 and c and someone suggests them to us, then it is quick for us to check them, because all we have to do is to calculate $a \cdot X^2 + b \cdot Y$ and verify that it results in c. The time cost of all this, which is very accessible, is that of three multiplications, one addition and the checking of an equality. Observe alto that these possible solutions X, Y have a length limited by that of the coefficient c and are therefore fast to present. The conclusion is that the problem of equations certainly lies in NP.

As to whether it belongs to P, however, this remains to be clarified for the reasons already stated. Therefore, the question on $a \cdot x^2 + b \cdot y = c$ may viewed a very special case of the much more general question whether P and NP coincide. But the two problems are in fact equivalent. In other words

- if, by examining the question on the equations, one proves that it lies outside P, then, evidently, one is entitled to infer that $P \neq NP$,
- if, however, and herein lies the surprising part of the argument, one proves that the problem on the equations lies in P, then one can deduce that P and NP are equal.

So, the problem manifests the same characteristics as SAT: it lies in NP, and is in P if and only if $P = NP$. It is then said to be *NP-complete* (like SAT): to put it in intuitive terms, finding a fast algorithm that solves it is equivalent to proving that $P = NP$.

The problem of finding the divisors of a non-zero integer, related to the question of finding the integer roots of a polynomial in one indeterminate, is also in NP. In fact, checking a particular submultiple, once one knows it, boils down to performing the relevant division and verifying that it is exact, i.e., gives 0 as remainder. If, however, no non-trivial submultiple exist and can be suggested to us, the difficulties increase. As already mentioned, there is no evidence that the divisor question is in P, even if some people conjecture "yes". However, it is not believed that it is *NP*-complete, and thus capable, like the question on equations of degree 2, of deciding for itself whether $P = NP$ is valid or not.
Also Diophantine games have their links to computational complexity, as said. To begin with, there is a theorem by Tung (in his 1987 paper, *Computational complexities of diophantine equations with parameters* [115], affirming the *NP*-completeness of the problem of deciding whether or not A admits a winning strategy in a Diophantine game with polynomials in 2 indeterminates.

Theorem 4. (Tung). The problem of deciding whether player A has a winning strategy in a Diophantine game for polynomials of two indeterminates is *NP*-complete.

So, in this case the input is a Diophantine polynomial and one would like to know whether or not A admits a winning strategy in the corresponding game. Well, this question is *NP*-complete, so solving it quickly is equivalent to affirmatively solving $P = NP$.

It then becomes natural to introduce the concept of a fast computable winning strategy. Informally, we can say that one has a ***fast computable winning strategy for B***, if one can exhibit explicit algorithms that give, in time at most polynomial in the length of the input,

- Y_1 as a function of X_1,
- Y_2 as a function of $X_1,\ X_2$,
  ...
- Y_n as a function of $X_1,\ \ldots, X_n$

such that $p(X_1,\ldots,X_n,Y_1,\ldots,Y_n) = 0$.

Instead, one has a ***fast computable winning strategy for A***, if one can exhibit explicit algorithms that give, in time at most polynomial in the length of the input,

- X_1 (i.e., no time limit),
- X_2 as a function of Y_1,
  ...
- X_n as a function of $Y_1,\ \ldots, Y_{n-1}$

such that $p(X_1,\ldots,X_n,Y_1,\ldots,Y_n) \neq 0$ for each choice of Y_n.

The following theorem, again due to Jones (in the article [67]), holds.

Theorem 5. There exists a polynomial with integer coefficients and 4 indeterminates such that in its Diophantine game B has a computable winning strategy, but no fast computable winning strategy.

9.8 The algebra of games

Diophantine games are preserved by conjunction and disjunction, i.e. they naturally extend from single equations to systems (i.e. conjunctions) of several equations, as well as to their disjunctions.
Consider in fact the following variants of the original game: instead of an equation $p(x_1, \dots, x_n, y_1, \dots, y_n) = 0$ with integer coefficients, we consider either

- a system of several equations (their conjunction), or
- their disjunction.

Recall that, among integers,

- finitely many numbers are all equal to 0 if and only if the sum of their squares is so,
- one of finitely many factors is equal to 0 if and only if their product is.

Note that the second property remains valid over any integral domain, while the first extends to, for example, $\mathbb{Q}$ and $\mathbb{R}$ but not to $\mathbb{C}$.

In any case, if $p_1, \dots, p_h$ are polynomials with integer coefficients,
(a) satisfying among the integers the system of equations $p_1 = 0, \dots, p_h = 0$ is equivalent to satisfying the single equation $p_1^2 + \dots + p_h^2 = 0$,
(b) satisfying among the integers a disjunction of equations $p_1 = 0$ or $\dots$ or $p_h = 0$ is equivalent to satisfying the single equation $p_1 \cdot \dots \cdot p_h = 0$.

We deduce that:

- there is a winning strategy for A or B in game (a) if and only if there is the strategy for the Diophantine game of the polynomial $p_1^2 + \dots + p_h^2$;
- there is a winning strategy for A or B in game (b) if and only if there is the strategy for the Diophantine game of the polynomial $p_1 \cdot \dots \cdot p_h$.

9.9 Links with number theory

Many of the famous results or open problems of number theory (in particular on prime numbers) can be translated into Diophantine games, where in the first case brilliant strategies apply and in the second case one has to admit the provisional absence of known strategies.

A simple premise. Let $n, m \in \mathbb{N}$, then:

- $n \geq m$ if and only if B has a winning strategy for the equation $n = y + m$, i.e., $n - (y + m) = 0$;
- consequently $n > m$, i.e., $n \geq m + 1$, if and only if B has a winning strategy for the equation $n = y + m + 1$, i.e., $n - (y + m + 1) = 0$.

The following is easy to deduce:
Lemma. A natural number $N > 1$ is prime if and only if B has a winning strategy for the Diophantine game of the equation

$$(N - (y_2 + x_1 x_2 + 1)) \cdot (x_1 x_2 - (y_3 + n + 1)) \cdot (x_1 - 1) \cdot (x_2 - 1) = 0.$$

Proof. For the sake of simplicity, we denote the polynomial just introduced by $P_r(N,\ x_1,\ x_2,\ y_2, y_3)$. In it, at the moment, $N > 1$ represents only a parameter and not a given indeterminate.
In the corresponding Diophantine game, the first to move is A with X_1, X_2, after which B returns $Y_2,\ Y_3$. According to the above considerations, fixed $X_1,\ X_2 \in \mathbb{N}$, there exist $Y_2,\ Y_3$ so that $P_r(N,\ X_1,\ X_2,\ Y_2, Y_3) = 0$ if and only if either

- $N - (Y_2 + X_1 X_2 + 1) = 0$ for some Y_2 i.e., $N > X_1 X_2$, or
- $X_1 X_2 - (Y_3 + n + 1) = 0$ for some Y_3, i.e., $N < X_1 X_2$ (so, at least so far, $N \neq X_1 X_2$), or
- if $N = X_1 X_2$, then $X_1 = 1$ or $X_2 = 1$, i.e., the decomposition of N is trivial.

But this obviously amounts (remembering the assumption that $N > 1$) to stating precisely that N is prime. In this case, and only in this case, B has a winning strategy. $\dashv$

Let us now deal with the problems of arithmetic that have been predicted.

Example 1. The *infinity of primes* (a celebrated result of Euclid's *Elements*) is equivalent to the existence of a winning strategy for B in the Diophantine game of the polynomial

$$(y_1 - (x_1 + y_2))^2 + (y_1 - (y_3 + 2))^2 + (P_r(y_1, x_4, x_5, y_5, y_6))^2 = 0,$$

i.e., of the system composed of the equations

$$y_1 = x_1 + y_2, \qquad y_1 = y_3 + 2, \quad P_r(y_1, x_4, x_5, y_5, y_6) = 0.$$

Equivalently $y_1 \geq x_1$, $y_1 \geq 2$ and therefore y_1 is prime (in the third equation y_1 is regarded as an indeterminate). The reason is soon explained: since there are infinitely many primes, whatever natural number X_1 proposed by A, B can find a prime $Y_1 \geq X_1$.
On the other hand, if prime numbers constituted a finite set only, and M was its maximum, A would only need to choose $X_1 > M$ to deprive B of any possibility of successful replication.

Example 2. The conjecture about the existence of infinite pairs of *twin primes* (two prime numbers that differ by 2, such as 3 and 5, or 17 and 19) is equivalent to the existence of a winning strategy for B in the diophantine game of the polynomial

$$(y_1 - (x_1 + y_2))^2 + (y_1 - (y_3 + 2)^2 + (Pr(y_1, x_4, x_5, y_5, y_6))^2$$

$$+ (Pr(y_1, +2, x_7, x_8, y_8, y_9))^2 = 0,$$

i.e., the possibility of guaranteeing the conditions $y_1 \geq x_1$, $y_1 \geq 2$, whence obviously $y_1 + 2 \geq x_1$, $y_1 + 2 \geq 2$, and y_1, $y_1 + 2$ primes. The details are analogous to the previous example.

Example 3. Goldbach's conjecture (that every even number > 2 is the sum of two primes) is equivalent to the existence of a winning strategy for B in the diophantine game of the equation that corresponds to the system formed by $2(x_1 + 2) - (y_2 + y_3) = 0$ and the equations that, when annihilating, ensure that y_2 and y_3 are primes (in particular greater than 1).

In fact, assume the conjecture to be valid. At the beginning of the game A proposes a generic even number > 2, which can be represented in the form $2(X_1 + 2)$ for the appropriate $X_1 \in \mathbb{N}$. Let us admit that B opposes the decomposition of this number into the sum of two primes Y_2, Y_3: then all the above polynomials, and thus the sum of their squares, get value 0 (due to the appropriate choice of variables appearing

after x_1, y_2 and y_3 in the game, in accordance with its rules).
Conversely, suppose the conjecture is false. Then it is A who has a winning strategy. It is sufficient for him to choose a counterexample $2(X_1+2)$ inexpressible as the sum of two primes.
Whatever the values Y_2 and Y_3 that B opposes, at least one of the two is not prime, so that the polynomial that would attest its primality cannot equal 0 (again due to an appropriate choice of further variables, according to the rules of the game).

Example 4. It is still an open question in arithmetic whether prime numbers of the form m^2+1 (i.e., successors of squares, such as 5, 17, 37, 101 etc.) are an infinity or not. Indeed, the problem is the last in a list of four (the first two being the previous two examples respectively), proposed in 1912 by the German mathematician Edmund Landau during the *International Congress of Mathematicians*.
Let us consider the polynomial

$$(y_1+x_2)^2+1=(y_2+2)(y_3+2)$$

and the related Diophantine game. Note that:

- if there are infinitely many primes of the above form, and thus arbitrarily large primes of that form, then it is A who admits a winning strategy (whatever Y_1 B proposes, A adds X_2 to it so that $(Y_1+X_2)^2+1$ is prime; then there is no way for B to decompose it into the product of two integers $Y_2+2, Y_3+2>1$);
- on the other hand, if the primes of the form under consideration are finitely many, and M is their maximum, then the situation is reversed and it is B who has a winning procedure ((s)he only has to choose $Y_1 \geq \sqrt{M}$, after which, whatever A's answer X_2, $(Y_1+X_2)^2+1>Y_1^2 \geq M$ is composite, and B can provide two factors Y_2+2, Y_3+2).

Thus, it is confirmed that exactly one between A and B possesses a winning strategy, and moreover we know what this possible strategy consists of. But to find out who is the lucky player, one must resolve an age-old question about the primes.

In conclusion, we want again emphasize how Diophantine games, besides suggesting how to play with equations, introduce challenging topics in a light-hearted manner. They can be a pleasant interlude in mathematics courses, especially in scientific high schools, but not only. Arithmetic is sometimes neglected in the curricula of these schools, but it was always and is still considered the "queen of mathematics"; so it deserves more attention. Moreover, thanks to Diophantine games, new horizons of (economic) game theory and theoretical computer science can be opened or at least insinuated. In all this, logic intervenes, both for the game theory part and, thanks to DPRM, for the most surprising and paradoxical aspects.

Conclusion

Let us draw a brief picture of the work done in this thesis. Its nodal axis has been "logic", exhibited and recommended as a reasoning technique, in all its aspects of strength and internal coherence.

Thus we do believe that logic should be taught at school to all students, from the first school levels to high school, in order to let them develop the logical-argumentative and analytical thinking skills and learn how to reason and to face and solve problematic situations. Naturally, all this should be done gradually, with prudence and creativity, and in any case favouring the dimension of intuition and amazement over the coldness of excessive rigor.

In our thesis we focus mainly on mathematical logic. In many ways, in fact, logic has become a fundamental part of mathematics, albeit with fruitful interactions with computer science, language and much more.

We have tried to highlight in a particular way various ideas of logic that can intrigue students because they are linked to the history of thought, or because they are capable of inspiring games of intelligence. For various reasons this is the common denominator of proofs without words, syllogisms, mathematical induction, paradoxes, Pinocchio's logic (= logic with lies), and Diophantine games.

Finally let us recall some papers this thesis is originating, on Diophantine games [51] and induction [52], respectively.

Bibliography

[1] S. A. Ajose, R. B. Nelsen, *Proof without Words: Geometric Series*, Mathematics Magazine, 67(3) (1994), p. 230.

[2] D. Alighieri, *La Divina Commedia*, Forma Edizioni (2021).

[3] Archimede, *Works*, ed. T. L. Heath, Cambridge University Press (1897), https://archive.org/details/worksofarchimede00arch/mode/2up.

[4] Aristotle, *De interpretatione*, Clarendon Press (1997).

[5] Aristotle, *Prior analytics*, Hackett Publishing Company (1989).

[6] Aristotle, *Physics*, Hackett Publishing Company (2018).

[7] R. Arnheim, *Visual thinking*, University of California Press (2004).

[8] K. J. Arrow, *Social choice and individual values*, Yale University Press (2012).

[9] S. Avital, S. Libeskind, *Mathematical Induction in the classroom. Didactical and mathematical issues*, Educational Studies in Mathematics, 9 (1978), pp. 429-438.

[10] J. Barwise (ed.), *Handbook of Mathematical Logic*, North Holland (1977).

[11] P. R. Baxandall et al. (eds.), *Proof in mathematics*, Institute of Education (1978).

[12] J. Bernoulli, *Opera* (1747), https://archive.org/details/jacobibernoulli00conggoog.

[13] J. Bernoulli, *Ars conjectandi* (1713), https://archive.org/details/jacobibernoulli00bern.

[14] J. L. Borges, *Obras completas*, Emecé Editores (1974). Includes: *Discusión*, pp. 173-286, see also: https://archive.org/details/BorgesObrasCompletasBorges/Borges-Obras-Completas-Borges/page/n11/mode/2up.

[15] J. L. Borges, *Selected non-fictions*, Viking (1999). Includes: *The perpetual race of Achilles and the Tortoise*, pp. 43-47.

[16] C. Brumfield, *A note on mathematical induction*, Mathematics Teacher 67, 7 (1974), pp. 616-618.

[17] W. H. Bussey, *The Origin of Mathematical Induction*, American Mathematical Monthly, 24 (1917), pp. 199-207.

[18] D. Buzzati, *I sette messaggeri*, Mondadori (2018).

[19] F. Cajori, *Origin of the name "Mathematical Induction"*, American Mathematical Monthly, 25 (1918), pp. 197-201.

[20] Callimachus, *Works*, Kessinger (2010).

[21] I. Calvino, *Le cosmicomiche*, Mondadori (2016).

[22] I. Calvino, *Ti con zero*, Mondadori (2019).

[23] L. Carroll, *The Game of Logic*, CreateSpace Independent Publishing Platform (2018).

[24] L. Carroll, *Symbolic Logic*, CreateSpace Independent Publishing Platform (2016).

[25] L. Carroll, *Alice in Wonderland*, Gallimard Edition (2014).

[26] L. Carroll, *Through the Looking Glass*, SeaWolf Press (2019).

[27] L. Carroll, *What the tortoise said to Achilles*, Mind, IV(14), (1895), pp. 278-280.

[28] M. de Cervantes, *Don Quixote*, Penguin Classics (2003).

[29] M. Connelly, *The Lincoln Lawyer*, Little, Brown and Company (2005).

[30] A. H. Coxon, *The Fragments of Parmenides: A Critical Text with Introduction and Translations, the Ancient Testimonia and a Commentary*, Las Vegas Parmenides Publishing (2009).

[31] F. Cucker, P. Koiran, S. Smale, *A Polynomial Time Algorithm for Diophantine Equations in One Variable*, J. Symbolic Computation 27 (1999), pp. 21-29.

[32] H. B. Curry, *The Inconsistency of Certain Formal Logics*, The Journal of Symbolic Logic, Vol. 7, N° 3 (1942), pp. 115-117.

[33] A. Cusi, N. Malara, *Improving Awareness about the Meaning of the Principle of Mathematical Induction*, in: O. Figueras et al. (editors), *Proceedings of the 32nd Conference of the International Group for the Psychology of Mathematics Education* (2008), pp. 393-399.

[34] M. Davis, Y. V. Matijasevic, J. Robinson, *Hilbert's Tenth Problem: Diophantine Equations: Positive Aspects of a Negative Solution*, in: F. E. Browder (ed.), *Mathematical Developments Arising from Hilbert Problems*, Proceedings of Symposia in Pure Mathematics XXVIII.2, American Mathematical Society (1976), pp. 323–378.

[35] M. Davis, *Hilbert's Tenth Problem is Unsolvable*, American Mathematical Monthly, Vol. 80 (1973), pp. 233–269.

[36] R. Dedekind, *Was sind und was sollen die Zahlen?*, Braunschweig (1888).

[37] K. J. Devlin, *The Millennium Problems: The Seven Greatest Unsolved Mathematical Puzzles Of Our Time*, Basic Books (2011).

[38] D. Diderot, *Jacques the Fatalist and His Master*, Penguin Classics (1986).

[39] Diophantus, *Arithmeticorum libri sex*, with the comment of C. G. Bachet and annotations by P. Fermat (1670), https://www.maa.org/press/periodicals/convergence/mathematical-treasure-bachets-arithmetic-of-diophantus.

[40] J. B. Le Rond d'Alembert et al., *Encyclopédie méthodique, ou par order de matières*, Panckoucke (1784-85), https://archive.org/details/mathematiques158alem.

[41] P. Di Martino, *Matematica sperimentale vs matematica relazionale. Il caso del principio di induzione*, L'insegnamento della matematica e delle scienze integrate, 41 B(1) (2018), pp. 30-52.

[42] F. Enriques, *Insegnamento dinamico*, Periodico di Matematiche 4, 1 (1921), 6-16; new edition Centro Studi Enriques, Agorà, La Spezia (2003).

[43] P. Ernest, *Mathematical Induction: a pedagogical discussion*, Educational Studies in Mathematics, 15 (1984), pp. 173-179.

[44] Euclid, *The Thirteen Books of the Elements*, Dover Publications (2012).

[45] Euclid, *Preclarissimus liber elementorum Euclidis perspicacissimi*, with the comment of Campanus of Novara, Venezia (1482), https://searchworks.stanford.edu/view/2177452.

[46] L. Euler, *Extrait d'une lettre de M. Euler le Père à M. Bernoulli, concernante la Mèmoire imprimé parmi ceux du 1771* (1772), https://archive.org/details/euler-e461/page/n1/mode/2up.

[47] L. Euler, *Letters to a German princess*, IOP Concise Physics (2019).

[48] L. Euler, *Elements of Algebra*, Springer (1972).

[49] C. V. Eynden, *Elementary Number Theory*, Waveland Pr Inc (2006).

[50] E. Fishbein, I. Engel, *Psychological Difficulties in Understanding the Principle of Mathematical Induction*, in G. Vergnaud et al. (eds.), Proceedings of the 13th Conference of the International Group for the Psychology of Mathematics Education, Vol. 1 (1989), pp. 276-282.

[51] A. Fontana, C. Toffalori, *Giocare con le equazioni*, L'insegnamento della matematica e delle scienze integrate, 45 (2022), pp. 139-168 (1st part) and 357-379 (2nd part).

[52] A. Fontana, C. Toffalori, A. Veredice, *L'induzione matematica tra storia e didattica*, Nuova Secondaria, to appear.

[53] M. Giaquinta, H. Hosni, *Teoria della scelta sociale e teorema fondamentale dell'economia del benessere. Razionalità, coerenza, efficienza ed equità*, Scuola Normale di Pisa (2015).

[54] J. A. Garfield, *Pons Asinorum*, New-England Journal of Education, Vol. 3, No.14, (1876), p. 161.

[55] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer (1986).

[56] A. Gellius, *Noctes Atticae*, Nabu Press (2010).

[57] J. A. Goguen, *The logic of inexact concepts*, Synthese 19 (1969), pp. 325-373.

[58] H. Grassmann, *Lehrbuch der Arithmetik* (1861), https://archive.org/details/lehrbuchderarit00grasgoog.

[59] G. Hanna, *Proofs that prove and proofs that explain*, in G: Vergnaud et al. (eds.), *Proceedings of the Thirteenth International Conference on the Psychology of Mathematics Education*, Vol. 2 (1989), pp. 45-51.

[60] G. H. Hardy, *An Introduction to the Theory of Numbers*, Oxford University Press (2008).

[61] G. Harel, *The Development of Mathematical Induction as a Proof Scheme: A Model for DNR-Based Instruction*, in S. Campbell and R. Zazkis (eds.), *Learning and Teaching Number Theory: Research in Cognition and Instruction* (2001), pp. 185-22.

[62] D. Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. 8 (1902), pp. 437-479, see also https://www.ams.org/journals/bull/1902-08-10/S0002-9904-1902-00923-3.

[63] D. Hilbert, *Foundations of Geometry*, https://math.berkeley.edu/ ~wodzicki/160/Hilbert.pdf .

[64] D. Hilbert, *Axiomatic Thinking*, Philosophia Mathematica s1-7 (1970), pp. 1-12.

[65] D. R. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid*, Basic Books (1999).

[66] D. Houston, *Proof without Words: Pythagorean Triples via Double Angle Formulas*, Mathematics Magazine, 67(3) (1994), p. 187.

[67] J. P. Jones, *Some undecidable determined games*, International Journal of Game Theory, 11 (1982), pp. 63-70.

[68] J. P. Jones, *Three universal representations of recursively enumerable sets*, The Journal of Symbolic Logic, 43 (1978), pp. 335-351.

[69] F. Kafka, *The Castle*, Schocken Books (1998).

[70] F. Kafka, *Before the Law*, BoD E-Short (2015).

[71] F. Kafka, *The Trial*, Schocken (1999).

[72] F. Kafka, *An Imperial Message*, Paperless (2017).

[73] Leonardo da Vinci, *Il Codice Atlantico*, Giunti Editore (2000).

[74] S. Leonesi, C. Toffalori, *Logica a processo. Da Aristotele a Perry Mason*, Franco Angeli (2016).

[75] S. Leonesi, C. Toffalori, *Matematica, miracoli e paradossi. Storie di cardinali da Cantor a Gödel*, Mondadori (2007).

[76] G. Malinowski, *Many-Valued Logics*, Oxford University Press (1993).

[77] Y. V. Matijasevic, *Hilbert's Tenth Problem*, MIT Press, Cambridge, Massachusetts (1993).

[78] F. Maurolico, *Arithmeticorum libri duo* (1575), http://mathematica.sns.it/opere/65/.

[79] F. Morselli, G. Rosolini, C. Toffalori (eds.), *Educare alla razionalità. Tra logica e didattica della matematica*, Unione Matematica Italiana (2019).

[80] D. Mundici, *The logic of Ulam's games with lies*, in C. Bicchieri & M. Dalla Chiara (eds.), *Knowledge, Belief, and Strategic Interaction*, Cambridge University Press (1992).

[81] R. Musil, *Precision and Soul: Essays and Addresses*, University of Chicago Press, (1995).

[82] R. B. Nelsen, *Proofs Without Words*, MAA (2009).

[83] P. Odifreddi, *Classical Recursion Theory*, North Holland (1988 and 1999).

[84] L. D. Öhman, *Are Induction and Well-Ordering Equivalent?*, The Mathematical Intelligencer, 41 (2019), pp. 33-40.

[85] W. Page, *Proof Without Words: Geometric Sums*, Mathematics Magazine, 54(4) (1981), p. 201.

[86] R. Pagnan, G. Rosolini, *Il gioco della logica di Lewis Carroll e i sillogismi*, Mondadori Education, Archimede 2 (2010), pp. 82-90.

[87] B. Pascal, *De l'esprit géométrique: Ecrits sur la Grâce et autres textes*, Flammarion (1999).

[88] B. Pascal, *Traité du triangle arithmetique* (1665), http://cudl.lib.cam.ac.uk/view/PR-CCB-00013-00024/3.

[89] B. Pascal, *Lettres de A. Dettonville à Monsieur de Carcavy* (1658-1659), https://gallica.bnf.fr/ark:/12148/btv1b8626200n.image.

[90] G. Peano, *Giochi di aritmetica e problemi interessanti*, Edizioni Clichy (2017).

[91] G. Peano, *Arithmetices principia, nova methodo exposita* (1889), https://archive.org/details/arithmeticespri00peangoog/mode/2up.

[92] C. Peirce, *On the logic of numbers*, American Journal of Mathematics, 4 (1881), pp. 85-95.

[93] A. Pelc, *Searching games with errors-fifty years of coping with liars*, Theoretical Computer Science, 270 (2002), pp. 71-109.

[94] C. Perelman, L. Olbrechts-Tyteca, *Trattato dell'argomentazione*, Einaudi (1996).

[95] Peter of Spain, *Language in dispute*, Benjamin (1990).

[96] Plato, *Philebus*, Cambridge University Press (2010).

[97] Plato, *Republic*, Penguin Classics (2007).

[98] Plato, *Meno*, Geoffrey Steadman (2017).

[99] Plato, *Parmenides*, Aeterna Press (2015).

[100] J. H. Poincaré, *Science and method*, Alpha Editions (2019).

[101] J. H. Poincaré, *Science and hypothesis*, Bloomsbury Academic (2017).

[102] G. Polya, *Mathematics and Plausible Reasoning, Volume 1: Induction and Analogy in Mathematics*, Princeton University Press (1990).

[103] M. O. Rabin, *Effective computability of winning strategies*, in M. Dresher (ed.), *Contributions to the theory of games*, Annals of Mathematical Studies 39 (1957), pp.147-157.

[104] N. L. Rabinovitch, *Rabbi Levi ben Gershon and the Origins of Mathematical Induction*, Archive History Exact Science, 6 (1970), pp. 237-248.

[105] A. Rényi, *On a problem in information theory*, Magyar Tud. Akad. Mat. Kutató Int. Közl. 6 (1961), pp. 505–516.

[106] B. Russell, *Mysticism and logic and other essays*, New Publisher (2021).

[107] R. M. Sainsbury, *Paradoxes*, Cambridge University Press (1995).

[108] F. Severi, *La matematica*, Energie Nove II, 9, Torino (1919), see also E. Vesentini, *Un contributo di Francesco Severi alle riviste di Pietro Gobetti*, Archimede 48 (1996), pp. 115-121.

[109] R. Smullyan, *What is the name of this book?*, Prentice Hall (1978).

[110] I. Stewart, *A partly True Story*, Scientific American, Vol. 268, No. 2 (1993), pp. 110-112.

[111] F. R. Stockton, *The lady, or the tiger?*, Leopold Classic Library (2015).

[112] A. Tarski, *The concept of truth in the languages of the deductive sciences*, in: *Logic, Semanctics, Metamathematics: Papers from 1923 to 1938*, ed. by J. Corcoran, Hackett (1983).

[113] G. F. von Tempelhof, *Geometrie Für Soldaten Und Die Esnicht Sind*, Wentworth Press (2018).

[114] C. Toffalori, P. Cintioli, *Logica matematica*, McGraw-Hill (2000).

[115] S. P. Tung, *Computational complexities of diophantine equations with parameters*, Journal of Algorithms 8 (1987), pp. 324-336.

[116] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. 42 (1937), pp. 230-265.

[117] S. M. Ulam, *Adventures of a Mathematician*, University of California Press (1991).

[118] P. Valéry, *Introduction à la méthode de Léonard de Vinci*, Homme et Littérature (2021).

[119] V. Villani, C. Bernardi, R. Porcaro, S. Zoccante, *Non solo calcoli*, Springer (2013).

[120] V. Villani, *Cominciamo da zero. Domande, risposte e commenti per saperne di più sui perché della Matematica*, Pitagora (2003).

[121] Voltaire, *Philosophical letters, or, Letters regarding the English nation*, Hackett (2007).

[122] J. Wallis, *Arithmetica Infinitorum* (1656), https://archive.org/details/ArithmeticaInfinitorum.

[123] W. von Waltershausen, *Gauss zum Gedächtniss*, HardPress (2018).

[124] P. Wason, *Reasoning*, in B. Foss (ed.), *New Horizons in Psychology*, Penguin (1996), pp. 135-151.

[125] J. H. Webb, *Proof without Words*, Mathematics Magazine, 60(3) (1987), p. 177.

[126] H. Weyl, *Philosophy of Mathematics and Natural Science*, Princeton University Press (2009).

[127] L. A. Zadeh, *Fuzzy Logic, Neural Networks, and Soft Computing*, in *Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems*, World Scientific (1996), pp. 775-782.

[128] https://www.indire.it/lucabas/lkmw_file/licei2010/indicazioni_nuovo_impaginato/_decreto_indicazioni_nazionali.pdf

[129] https://archivio.pubblica.istruzione.it/riforma_superiori/nuovesuperiori/doc/Allegato_A_definitivo_02012010.pdf

[130] https://www.oecd.org/pisa/

[131] http://www.irre.liguria.it/progetti/educazione_alla_razionalita/

[132] https://mat.unicam.it/sites/mat.unicam.it/files/bondoni%20200304.pdf

[133] https://ctext.org/zhou-bi-suan-jing

[134] https://www.progettofibonacci.it/liber_abaci.html

[135] http://web.math.unifi.it/archimede/archimede_NEW_inglese/pitagora/exh_pitagora/scheda3.html

[136] http://classics.mit.edu/Plato/parmenides.html

[137] https://mathshistory.st-andrews.ac.uk/Extras/Perigal_maths_astro/

[138] https://archive.org/details/pennycyclopaedi18unkngoog/page/464/mode/2up?view=theater

[139] https://www.cut-the-knot.org/WhatIs/WhatIsInfiniteDescent.shtml

Words of Thanks

In these few lines, I would like to thank the people who made this thesis possible and who accompanied me during this beautiful adventure. Firstly, I would like to give heartfelt thanks to Prof. Carlo Toffalori, who gave me the passion for mathematical logic and guided me with his experience in the most delicate moments of the realization of the thesis. I would also like to thank all the people who represented for me in these years a source of comfort and affection, that is my wife Giovanna, my son Andrea and my daughter Carmela.