DEDUCTION AND INDUCTION

Leong Yu Kiang
Department of Mathematics
National University of Singapore

It is generally known that mathematics is deductive in nature in contrast to the inductive nature of science as exemplified by, for instance, physics. That is to say, a mathematician draws a specific conclusion from a set of general premisses (or axioms and postulates) while a physicist draws a general conclusion from a set of premisses based on experimental observations. What is perhaps not so widely known is that in mathematics there is an inductive process which operates on two levels. On the first level, it is somewhat similar to experimentation in which calculations are made and special cases studied in the hope of discovering or gathering sufficient evidence for a general pattern. On the other (higher) level, it is a rigorous process of reasoning which establishes the truth of a general conclusion adduced to usually by particular cases or sometimes by inspired guess work (more respectfully referred to as intuition). The processes of induction and deduction represent two divergent paths of reasoning. The purpose of this article is not to delve into the precise meaning of these two processes nor to discover their logical connections. Rather, we shall give concrete examples to illustrate, if not to illuminate upon, the nature of these important thought processes.

Before stepping into mathematical water, let us skim over it by narrating two stories. The first is a much-repeated story (or a variant thereof) which brings out in a striking way the rigour of mathematical thought. Once, a party comprising an astronomer, a physicist and a mathematician landed on an unexplored island. Grazing on the lush pasture, not far from where they landed, were three sheep which had their sides towards the learned men. The astronomer, who saw that the sides of these sheep were black, remarked, "The sheep on this island are all black." The physicist, who saw what the astronomer saw, said, "The three sheep over there are black." The mathematician, however, said, "The sides of those sheep facing me are black."

The second story is really a quotation from the book [6, p. 11] by George Polya, the well-known American mathematician and mathematics educator, and caricatures different views of inductive thinking:

> "Look at this mathematician," said the logician. "He observes that the first ninety-nine numbers are less than hundred and infers hence, by what he calls induction, that all numbers are less than a hundred."
>
> "A physicist believes," said the mathematician, "that 60 is divisible by all numbers. He observes that 60 is divisible by 1, 2, 3, 4, 5 and 6. He examines a few more cases, as 10, 20, and 30, taken at random as he says. Since 60 is divisible also by these, he considers the experimental evidence sufficient."
>
> "Yes, but look at the engineers," said the physicist. "An engineer suspected that all odd numbers are prime numbers. At any rate, 1 can be considered as a prime number, he argued. Then there come 3, 5, and 7, all indubitably primes. Then there comes 9; an awkward case, it does not seem

to be a prime number. Yet 11 and 13 are certainly primes. 'Coming back to 9,' he said, 'I conclude that 9 must be an experimental error.'"

The basic and simplest deduction in mathematics is the so-called syllogism of Aristotelian logic, which may be summed up in the following classical example:

All men are mortal.
Socrates is a man.
Therefore Socrates is mortal.

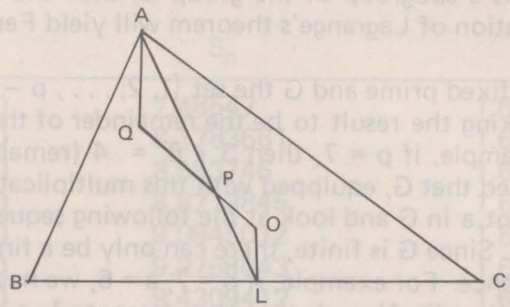
In euclidean geometry every triangle has an angle sum of 180 degrees. So does an equilateral triangle, and hence, its angles being equal, each angle must be equal to 60 degrees. However, it is not the result of measurements accummulated since antiquity that led Euclid to the conclusion that all triangles must have the same angle sum of 180 degrees but the result of logical deduction from a prescribed set of axioms or postulates whose truth is assumed (on the grounds of being "self-evident") and whose choice is undoubtedly based on empirical experience. Such a choice is now known to be arbitrary, there being no such thing as a "correct" choice. We could equally well live, mathematically speaking, in a world where every triangle has an angle sum greater than 180 degrees. In such a system (often called Riemanniam geometry), any two lines will invariably meet in a "real" point and this system will be as "consistent" as an euclidean one. At the other extreme, we could also choose to "live" in a system in which there are infinitely many lines through a given point and "parallel" to a given line — the so-called hyperbolic geometry. The question as to whether the "real" world we live in is euclidean or non-euclidean cannot be determined by purely physical measurements. Even if we could construct astronomically large triangles, there will still be the problem of an acceptable tolerance of errors in measurement. Modern physics seems to favour a non-euclidean model of the universe perhaps more on grounds of conceptual simplicity.

Deductive reasoning is essentially linear. The complexity of a proof of a major theorem is often accentuated by the need to obtain numerous minor or auxiliary results which are traditionally called lemmas, corollaries or propositions and which could be technically complicated in formulation, content and proof. Upon the truth of the multitude of such statements is thus built the edifice of the theorem — in much the same way as the summit of a pyramid. Sometimes a foundation stone of the pyramid may be found to be weak and untenable. Yet the summit need not collapse and it often happens that the weak stone could be replaced by a solid one.

While an important theorem is often difficult to prove, mathematicians never tire in their search for a proof that is simpler than known proofs. To discover a new theorem is to discover one facet of Truth, but to discover a simpler proof of an established theorem is to catch a glimpse of Beauty. A simple proof is often called an elegant proof. The attainment of simplicity is often the hallmark of a successful theory. Such simplicity is reflected in the following proof of a theorem due to the prolific Swiss mathematician Leonhard Euler (1707 — 1783) [2, p. 141].

Theorem. In any triangle, the centre of the circumscribed circle, the point of intersection of the medians and the point of intersection of the altitudes lie (in this order) on a straight line in such a way that the altitude intersection is twice as far from the median intersection as the circumscribed centre is.

Proof. Let L be the mid-point of BC, O the centre of the circumscribed circle and P the point of intersection of the medians. It is well-known that AP = 2PL. Extend OP to Q where PQ = 2OP. Hence AP/PL = PQ/OP, and since $A\hat{P}Q = O\hat{P}L$, the triangles APQ, OPL are similar. Thus $P\hat{A}Q = P\hat{L}O$ and AQ is parallel to OL. In other words, Q lies on the altitude through A. By considering the mid-point of AC, we can similarly argue that Q lies on the altitude through B. Therefore Q is the altitude intersection.



When one looks for examples of mathematical gems which stand out for its sublime beauty, one invariably turns to number theory. Perhaps the most famous example is the celebrated theorem of Pierre Fermat (1601 – 1665) which asserts that if p is any prime and a any integer not divisible by p, then p divides $a^{p-1} - 1$. In terms of the modern congruence notation, this becomes

$$a^{p-1} \equiv 1 \pmod{p},$$

in which the notation "$x \equiv y \pmod{n}$" means that n divides $x - y$. The rationale for introducing this seemingly extraneous notation is that it permits us to perform operations similar to the ordinary arithmetical ones. In particular, we have:

(1) If $x \equiv y \pmod{n}$, $u \equiv v \pmod{n}$, then $x + u \equiv y + v \pmod{n}$ and $xu \equiv yv \pmod{n}$.

(2) If $mx \equiv my \pmod{n}$ and m is relatively prime to n, then $x \equiv y \pmod{n}$.

A simple proof of Fermat's theorem involves some of these properties. First we note that the $(p - 1)$ integers $a.1, a.2, a.3, \ldots, a.(p-1)$ cannot be divisible by p and so must have non-zero remainders when divided by p. In other words, for each $1 \leqslant i \leqslant p-1$, $a.i \equiv r_i \pmod{p}$, where $1 \leqslant r_i \leqslant p-1$. Moreover, the $(p-1)$ integers $r_1, \ldots, r_{p-1}$ are different. For $r_i = r_j$ would imply that $ai \equiv aj \pmod{p}$, and so by property (2), $i \equiv j \pmod{p}$. This is possible only if $i = j$ since $0 \leqslant |i - j| < p - 1$. Therefore $r_1 r_2 \ldots r_{p-1} = 1.2 \ldots (p-1) = (p-1)!$ after a suitable re-arrangement. Using property (1), we then have $a^{p-1}.(p-1)! \equiv (p-1)! \pmod{p}$, and since p does not divide $(p-1)!$, property (2) gives $a^{p-1} \equiv 1 \pmod{p}$.

As it often turns out, many results in elementary number theory occurs as corollaries of theorems in a deeper and more general theory in modern mathematics. The preceding classical result of Fermat, for instance, crops up naturally within the framework of group theory. The axioms of this theory were formulated at the beginning of this century though the notion and properties of groups had been studied and exploited as early as 1830 for finite permutation groups in connection with the search for a "formula" for the solutions of a polynomial equation. Without going into the details (see [4]), we will attempt to indicate how Fermat's theorem arises in group theory. Let us just say that a group G is a non-empty set of elements satisfying certain given axioms and that a subgroup of G is a (non-empty) subset H of G such that the elements of H also satisfy the same axioms. If G is finite, the number of elements of G is called the "order" of G. A basic result, called Lagrange's theorem, is that if H is a subgroup of the group G, then the order of H divides the order of G. An application of Lagrange's theorem will yield Fermat's theorem.

First, let p be a fixed prime and G the set $\{1, 2, \ldots, p-1\}$ and we "multiply" two elements in G taking the result to be the remainder of the ordinary product on division by p. For example, if $p = 7$, then $3 * 6 = 4$ (remainder of 18 on division by 7). It can be checked that G, equipped with this multiplication, becomes a group. Next, take any element a in G and look at the following sequence of elements of G: $1, a, a*a, a*a*a, \ldots$. Since G is finite, there can only be a finite number of distinct elements in this sequence. For example, if $p = 7$, $a = 6$, we have $1, 6, 1, 6, 1, 6, \ldots$. Thus there is an integer n ($\geqslant 1$) such that the elements $1, a, a*a, \ldots, \underbrace{a*a*\ldots*a}_{n-1}$ are distinct (call the set of such elements H) and such that $\underbrace{a*a*\ldots*a}_{n} = 1$. Then H is a subgroup of G and the order of H is n. In particular, if $a = 1$, then $H = \{1\}$. From Lagrange's theorem, we know that $p - 1 = mn$ for some positive integer m. Now $\underbrace{a*a*\ldots*a}_{p-1} = \underbrace{b*b*\ldots*b}_{m}$ where we write $b = \underbrace{a*\ldots*a}_{n}$. However, $b = 1$, and hence $\underbrace{a*a*\ldots*a}_{p-1} = 1$, which is equivalent to the statement $a^{p-1} \equiv 1 \pmod p$.

A negative result is equally important in mathematics. Since the advent of non-euclidean geometry, mathematicians have become accustomed to and often expect negative answers to outstanding problems. The work of Evariste Galois (1811 – 1832) on the impossibility of solving the general polynomial equation of degree greater than 4 by radicals (that is, by the usual algebraic operations) led to a whole new theory in modern algebraic number theory which is still breaking new ground in mathematics. And recently, the negative answer to Hilbert's Tenth Problem (see [1]) is a culmination of fundamental work in logic whose tentacles are now beginning to be felt in diverse branches of mathematics and even in physics and statistics.

Associated with negative results is a process of mathematical reasoning called "proof by contradiction." However, this process by no means yields negative results only (see [5]). We will use this reasoning to show that there does not exist any square matrix A with real entries and of odd order satisfying the matrix equation $A^2 + I = 0$, where I and O are the corresponding identity and zero matrices respectively. Suppose such an nxn matrix A exists. Then $A^2 = -I$, and by the properties of determinants, $(\det A)^2 = \det(A^2) = \det(-I) = (-1)^n = -1$. This contradicts the fact that $(\det A)^2 \geqslant 0$, det A being a real number. It follows that there is no such A. To appreciate the simplicity and economy of this argument, one has only to try to prove it directly even in the case when $n = 3$. Of course, the argument will not work when n is even because $(\det A)^2 = 1$ will not give rise to any contradiction. In fact, if we take $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ then indeed, $A^2 + I = \dot{0}$.

Let us perform some calculations on the series $S_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ and $T_n = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2}$. With the aid of a calculator, we obtain the following table:

n	S_n	T_n
1000	7.48547	1.6439343
2000	8.1783661	1.6444337
3000	8.583746	1.6446001
4000	8.8713845	1.6446832
5000	9.0945012	1.6447329
6000	9.2768043	1.644766
7000	9.4309412	1.6447896
8000	9.5644618	1.6448072
9000	9.6822361	1.6448209
10000	9.7875892	1.6448317

We observe that both S_n and T_n increase as n increases, and it appears that the latter increases "more slowly" than the former. If we compute further, we become convinced that T_n converges to a certain number; but we could not be certain whether the increase in S_n might not "eventually slow down sufficiently" to converge. Taxing the limits of a computer will not prove any suspicion conclusively, but a little mathematics will. We consider

$$\begin{aligned} S_{2^n} &= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \ldots + \frac{1}{8}\right) + \ldots + \left(\frac{1}{2^{n-1}+1} + \ldots + \frac{1}{2^n}\right) \\ &\geqslant 1 + \frac{1}{2} + 2\cdot\frac{1}{4} + 4\cdot\frac{1}{8} + \ldots + 2^{n-1}\cdot\frac{1}{2^n}. \\ &= 1 + \frac{1}{2}n. \end{aligned}$$

A fortiori, S_n increases indefinitely. On the other hand,

$$\begin{aligned} T_n &< 1 + \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \ldots + \left(\frac{1}{n-1} - \frac{1}{n}\right) \\ &= 2 - \frac{1}{n},\ n < 1, \end{aligned}$$

in view of the fact that $\frac{1}{r^2} < \frac{1}{r(r-1)} = \frac{1}{r-1} - \frac{1}{r}$. Hence $T_n < 2$ for all integral values of n. More mathematics could be used to show that T_n converges to $\pi^2/6 \approx 1.6449$.

Empirical evidence cannot be a substitute for a mathematical proof but it can indicate or strengthen a preferred view. To illustrate the pitfalls of drawing a hasty conclusion from empirical evidence, let us calculate the values of the polynomial $f(n) = n^2 - 79n + 1601$. With the aid of a table of primes, we quickly see that $f(1)$, $f(2), \ldots, f(79)$ are all primes. It would be tempting to conclude that $f(n)$ is prime for any integer n ($\geqslant 1$). However, one more calculation would shatter this hope: $f(80) = 1681 = 41^2$.

Famous mathematicians alike have fallen into such pitfalls. For instance, Fermat conjectured that the numbers $F_n = 2^{2^n} + 1$ are prime for every positive integer n, possibly on the basis that $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, which are prime. This was proved false by Euler, who showed that $F_5 = 641 \times 6700417$. These numbers F_n are called Fermat's numbers, an account of which could be found in [3].

Euler, one of the most prolific mathematicians of all time, is reputed to have made many discoveries by the inductive process. He was a great calculator and his work on number theory (and partitions of numbers, in particular) contains results arrived at by inductive calculations. An interesting example of how he collected numerical evidence to support a certain formula is given in an English translation [6, pp. 91–98] of the original French paper. This formula concerns an interesting recurrence relation for the number $\sigma(n)$ which is defined to be sum of all the positive divisors of the positive integer n. For example, the divisors of 12 are 1, 2, 3, 4, 6 and 12, and so $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$. The formula is given by

$$\begin{aligned}\sigma(n) &= \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7)\\ &\quad + \sigma(n-12) + \sigma(n-15) - \sigma(n-22) - \sigma(n-26)\\ &\quad + \sigma(n-35) + \sigma(n-40) - \sigma(n-51) - \sigma(n-57)\\ &\quad + \sigma(n-70) + \sigma(n-77) - \sigma(n-92) - \sigma(n-100)\\ &\quad + \cdots,\end{aligned}$$

where the integers 1, 2, 5, 7, 12, 15, . . . are governed by the relation

Number	1	2	5	7	12	15	22	26	35	40	51	. . .
Difference	$\underline{1}$	3	$\underline{2}$	5	$\underline{3}$	7	$\underline{4}$	9	$\underline{5}$	11	. . .	

Euler obtained this formula by a formal application of infinitesimal calculus to infinite series without worrying about convergence of series. He was aware of the need to justify such a method since he went to great lengths to collect the numerical evidence.

To come down to a lower plane, consider the expression

$$f(n) = \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{n^2}\right).$$

Let us ask whether this can be simplified to give a "nice" expression. First we compute sufficiently many terms and then try to pick out any apparent pattern:

n	2	3	4	5	6	7	8	9	10	11
f(n)	$\frac{3}{4}$	$\frac{2}{3}$	$\frac{5}{8}$	$\frac{3}{5}$	$\frac{7}{12}$	$\frac{4}{7}$	$\frac{9}{16}$	$\frac{5}{9}$	$\frac{11}{20}$	$\frac{6}{11}$

If we look at even values of n, we note that the numerators of f(n) appear as a sequence

$$3,\ 5,\ 7,\ 9,\ 11,\ \ldots$$

and the denominators as another sequence

$$4,\ 8,\ 12,\ 16,\ 20,\ \ldots$$

This suggests that $f(2m) = (2m + 1)/(4m)$, $m = 1, 2, \ldots$. For odd values of n, the numerators and denominators are given by the sequences

$$2,\ 3,\ 4,\ 5,\ 6,\ \ldots$$
$$3,\ 5,\ 7,\ 9,\ 11,\ \ldots$$

This again suggests that $f(2m + 1) = (m + 1)/(2m + 1)$, $m = 1, 2, \ldots$. It appears that f(n) is given by two different formulae, but it soon becomes apparent that f(n) could be given by one formula:

$$f(n) = (n+1)/(2n),\ n = 2, 3, 4, \ldots$$

This seems to work for any specific value of n that we substitute. Yet how do we prove that it will work for all $n \geqslant 2$? Fortunately, there is a method, known as mathematical induction, which establishes a correct inductive guess on a sound basis.

In its most elementary application, mathematical induction is used to demonstrate the truth of a mathematical statement concerning the positive or natural integers. For instance,

$$\text{“}\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n},\ n = 2, 3, 4, \ldots\text{”}$$

is such a statement, and so is

“$2^{2^n} + 1$ is a prime for any positive integer n”.

The second statement is, of course, false. Now, instead of considering the first statement as one single statement in the variable n, we could also consider it to be a collection of statements, one statement corresponding to each value of n, and we number these statements by the positive integers: P(1), P(2), . . . , P(k) . . . , where

$$P(1) = \text{“}\ 1 - \frac{1}{4} = \frac{2+1}{2 \times 2}\ \text{”},$$

$$P(2) = \text{“}\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) = \frac{3+1}{2 \times 3}\text{”},$$

$$\vdots$$

$$P(k) = \text{“}\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) \cdots \left(1 - \frac{1}{(k+1)^2}\right) = \frac{k+2}{2(k+1)}\text{”},$$

$$\vdots$$

Mathematical induction establishes the truth of P(n) for all $n \geqslant 1$ in two steps.

Step 1. Check the truth of P(1). This is immediate.

Step 2. Assuming the truth of P(k) for any given positive integer k, show that the next statement P(k + 1) is also true. Now, since P(k) is true, we have

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\ldots\left(1-\frac{1}{(k+1)^2}\right) = \frac{k+2}{2(k+2)}.$$

Multiplying by $1 - \dfrac{1}{(k+2)^2}$ gives

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\ldots\left(1-\frac{1}{(k+2)^2}\right) = \frac{k+2}{2(k+1)} \cdot \frac{(k+1)(k+3)}{(k+2)^2}$$

$$= \frac{k+3}{2(k+2)}$$

This is just the statement P(k + 1), which is then true if P(k) is true. The principle of mathematical induction will assert that P(n) is true for all n = 1, 2, ...

A correct execution of Step 2 is important in order to get a correct conclusion. To appreciate this, we give a "proof" by mathematical induction of the statement P(n):

"Any n numbers are equal."

(Or, in Polya's colourful language, "Any n girls have eyes of the same colour.")

Step 1. P(1) is clearly (vacuously) true.

Step 2. Suppose that P(k) is true. Now, given any (k + 1) numbers, $a_1, a_2, \ldots, a_{k+1}$ say, we wish to show that $a_1 = a_2 = \ldots = a_{k+1}$. First, consider the k numbers $a_1, a_2, \ldots, a_k$. By the truth of P(k), they must be all equal, i.e. $a_1 = a_2 = \ldots = a_k$. On the other hand, the same argument on the k numbers $a_2, a_3, \ldots, a_k, a_{k+1}$ also shows that $a_2 = a_3 = \ldots = a_k = a_{k+1}$. Hence $a_1 = a_2 = \ldots = a_k = a_{k+1}$. Hence P(k + 1) is also true.

What has gone wrong? If we examine Step 2 carefully, we will see that we have implicitly assumed that the numbers $a_1, a_2, \ldots, a_k$ have members in common with the numbers $a_2, a_3, \ldots, a_k$: namely, $a_2, \ldots, a_k$. This is valid if $k \geqslant 3$. But what happens if k = 2? While a_1 is equal to itself and a_2 is equal to itself, there is no way of deducing that $a_1 = a_2$. So Step 2 cannot be successfully carried out from P(1) to P(2). Any gap in the chain of inductive argument renders the conclusion unproved. There is an interesting account of various aspects of induction in [6].

Though mathematical induction is a standard and powerful tool, it cannot always be applied to settle innocuous-looking conjectures in number theory whose truth has been verified up till the limits of computation. We have only to mention the famous conjecture which Goldbach mentioned in a letter to Euler in 1742:

"Any even integer greater than 4 is the sum of two odd primes." For instance, 24 = 7 + 17, 100 = 29 + 71, 4000 = 11 + 3989. Up to now, no counter-example has been found. But the conjecture remains unproved. Among some of the results related to this conjecture is a theorem of Vinogradov that all odd integers from a certain point onwards are sums of three odd primes, and the theorem of van der Corput and Estermann that "almost all" even numbers are sums of two primes. More recently, Chen Jing-ren proved that any even integer is a sum of an odd prime and a product of at most two odd primes. What appears to be easily verified empirically seems to defy all efforts to derive it logically from accepted premises. Mathematics abounds in empirically supported but yet unproved conjectures. It makes one wonder whether there are certain facets of Truth which could only be glimpsed at through inductive discoveries.

References

[1] C.T. Chong, "Hilbert's Tenth Problem", Mathematical Medley 9 (1981), 39 – 42.

[2] Heinrich Dorrie, "100 great problems of elementary mathematics: Their history and solution", translated by David Antin, Dover Publications, New York, 1965.

[3] G.H. Hardy and E.M. Wright, "An introduction to the theory of numbers", Fourth Edition, Oxford University Press, London, 1959.

[4] I.N. Herstein, "Topics in algebra", Second Edition, John Wiley, New York, Santa Barabara, London, Sydney, Toronto, 1975.

[5] Y.K. Leong, "Reduction ad absurdum (proof by contradiction)", Mathematical Medley 8 (1980), 12 – 16.

[6] G. Polya, "Induction and analogy in mathematics", Volume I (Of mathematics and plausible reasoning), Oxford University Press, London, 1954.