A conceptual proposal on the *undecidability* of the distribution law of prime numbers and theoretical consequences

Gianfranco Minati*

In music and in mathematics there is the same perfume of eternity

**Abstract**†

Within the conceptual framework of number theory, we consider prime numbers and the classic still unsolved problem to find a complete law of their distribution. We ask ourselves if such persisting difficulties could be understood as due to theoretical incompatibilities. We consider the problem in the conceptual framework of computational theory. This article is a contribution to the philosophy of mathematics proposing different possible understandings of the supposed *theoretical* unavailability and indemonstrability of the existence of a law of distribution of prime numbers. Tentatively, we conceptually consider demonstrability as computability, in our case the conceptual availability of an algorithm able to compute the general properties of the presumed primes’ distribution law *without computing such distribution*. The link between the conceptual availability of a distribution law of primes and decidability is given by considering how to decide if a number is prime without computing. The supposed distribution law should allow for any given prime knowing the next prime without factorial computing. *Factorial properties of numbers, such as their property of primality, require their factorisation (or equivalent, e.g., the sieves), i.e., effective computing. However, we have factorisation techniques available, but there are no (non-quantum) known algorithms which can effectively factor arbitrary large integers. Then factorisation is undecidable. We consider the theoretical unavailability of a distribution law for factorial properties, as being prime, equivalent to its non-computability, undecidability.*

---

* Italian Systems Society, Milan, Italy; gianfranco.minati.it.
† Received on November 15th, 2019. Accepted on December 17th, 2019. Published on December 30th, 2019. doi: 10.23755/rm.v37i0.480. ISSN: 1592-7415. eISSN: 2282-8214.
©Gianfranco Minati. This paper is published under the CC-BY licence agreement.
The availability and demonstrability of a hypothetical law of distribution of primes are inconsistent with its undecidability. The perspective is to transform this conjecture into a theorem.

**Keywords**: algorithm; computation; decidability; incompleteness; indemonstrability; law of distribution; prime numbers; symbolic; undecidability.

**2010 AMS subject classification**: 11N05; 00A30; 11A51.

# 1 Introduction

Number theory is an antique and fascinating discipline. Number theory considers endless properties of numbers such as perfect numbers, golden ratios, and Fibonacci numbers.

An endless list of approaches, problems, properties, and results added one to the other over time deal with prime numbers and the possibility to find a suitable law of their distribution.

With regards to prime numbers, mathematicians introduced several conjectures, and not definitive, proven partial results.

To name a few, we recall properties and results relating to prime number generation such as the *Fundamental theorem of Arithmetic* (by Gauss in the 1801), the Goldbach's conjecture (approximately 1742), the classic sieve of Eratosthenes (275–194 B.C.), the sieve of Sundaram (approximately 1934), the sieve of Atkin (approximately 2003), and the Mersenne prime (1536) - of the form \( M_n = 2^n - 1 \) - for pseudorandom number generators, all used for applications such as cryptography.

Throughout history, several important mathematicians have tentatively contributed to the identification of the asymptotic law of distribution of prime numbers and its proof. We just mention Legendre (approximately 1808), Dirichlet (approximately 1837), Gauss (approximately in 1849 reported the connection between prime numbers and logarithms), Riemann (in 1859) wrote his very famous article (Riemann, 1859), Euler's theorem (approximately 1763) as a generalisation of Fermat's little theorem, Chebyshev (approximately 1850), and Yitang Zhang’s contributions to the twin-prime conjecture (approximately 2013).

However, since providing a complete review of the literature is beyond the scope of this article, we leave it to the reader to familiarize themselves with the literature on this subject.

*The contribution to the philosophy of mathematics of the present article is to propose different possible understandings of the unavailability and
A conceptual proposal on the undecidability of the distribution law of prime numbers and theoretical consequences

indemonstrability of the existence of the law of distribution of prime numbers. Further research is expected to allow suitable formalisations.

In Section 2 we consider generic indemonstrability as a fact of incompleteness and platonic consistency of knowledge. This is further explored in Section 4, in a constructivist understanding, where we propose indemonstrability to prevent inevitably implicit inconsistencies because a paradigm shift is required instead.

In Section 3 we propose to consider demonstrability as having symbolic nature and as decidability. Indemonstrability cannot be demonstrated and it can be intended as a fact of incompleteness, case of undecidability. The link between the conceptual availability of a distribution law of primes and decidability is given by considering how to decide if a number is prime without computing. The supposed distribution law should allow for any given prime knowing what the next prime with without computing such sequences.

However, factorial properties of numbers, such as their property of being prime, require their factorisation (or equivalent, e.g., the sieves), i.e., effective computing.

Because of that it is not possible to know in advance the properties of the factorisation, in the same way as it is not possible to solve the alt of a Turing Machine (TM) - the halting problem consists on determining if an arbitrary computer program and its input will finish running or continue to run forever (such as being in loop). A general algorithm to solve the halting problem for all possible program-input couples cannot exist-, it is not possible to know the result of the processing of a Neural Network without performing the entire processing, and to know the patterns generated by a Cellular Automata without performing the entire processing.

In Section 4, regarding the research relating to a Prime’s Distribution Law (PDL), we present, for the general reader, a short, partial overview of the situation as it currently consists mainly of a list of conjectures. Such conjectures have been not falsified but, rather, computationally confirmed by considering numerically large cases.

In Section 5 we tentatively conceptually consider demonstrability as computability, i.e., in our case the conceptual existence of an algorithm able to compute the general properties of the presumed primes’ distribution law without computing such distribution. We tentatively consider generic indemonstrability, unavailability as undecidability of the law of distribution and the probabilistic nature of the Prime Number Theorem (PNT) as an aspect of its undecidability. We consider then the usability of such undecidability, in the historical conceptual framework of the very effective usability of imaginary numbers. We ask ourselves if the non-demonstrability of existence of the PDL and its non-discovery can be intended as a prototype of the non-distribution and of possible different non-equivalent non-distributions. Besides, such non-demonstrability
of existence and the persisting non-availability of the PDL may be considered as a prototype of the generic non-demonstrability, of theoretical incompleteness, and theoretical incomprehensibility.

We conclude by mentioning how from the issues considered above it is possible to use such incompleteness in order to introduce paradigm shifts and non-equivalent, mutually irreducible, incommensurable approaches.

2 Indemonstrability as a fact of consistency

We consider here a kind of platonic consistency of the knowledge, as theoretical incompleteness [1, 2] which manifests when dealing with incomplete problems or indemonstrability of incomplete or wrong theses. In a constructivist understanding it is a kind of experiment having no reaction as a result, stating that the experiment is inadmissible, inconsistent, wrong.

As a classic example, consider the unsuccessful attempts to demonstrate the fifth postulate in Euclidian geometry. The history of the attempts to demonstrate the fifth postulate reveals how the conclusion was obtained by appealing to a new proposition that was equivalent to the fifth postulate itself.

The Italian mathematician Eugenio Beltrami discovered the Giovanni Girolamo Saccheri's article *Euclides ab omni naevo vindicatus* (*Euclid Freed of Every Flaw*), published in 1733 in which he tried to prove the Euclid's postulate of parallel lines. By using a similar approach, Beltrami, among others, inadvertently introduced a paradigm shift towards the non-Euclidean geometries by reasoning per reductio ad absurdum, i.e., as a result of the impossibility of proving the absurdity of the negation of the fifth postulate [3, 4].

An example of a relationship between theoretical incompleteness and indemonstrability is given by the two celebrated Gödel's syntactic incompleteness theorems [5].

The meaning of the first theorem states that within any mathematical theory, having at least the power of arithmetic, there exists a formula that, neither the formula nor its negation is syntactically provable. In other words, it is possible to construct a formally correct proposition that, however, cannot be proven or disproved. This is logically equivalent to the construction of a logical formula that denies its provability.

The meaning of the second theorem is that no coherent system is able to demonstrate its own syntactic coherence. The two theorems can be intended to prove the inexhaustibility in principle of pure mathematics [6-8]. "In other words, infinite-state logical theories when sufficiently complex are necessarily incomplete. Whether this result implies a sort of incompleteness of other kinds of theories (for instance, those of physics) is still an open question [9, p. 7]."
A conceptual proposal on the undecidability of the distribution law of prime numbers and theoretical consequences

As for incompleteness in physics, it is closely related to the *uncertainty principles*. It relates to the well-known uncertainty principle, first introduced by Werner Heisenberg [10]. Furthermore, there is the *principle of complementarity* introduced by Neils Bohr [11] stating that the corpuscular and undulatory aspects of a physical phenomenon cannot be observed simultaneously.

This is the case of the measurement of *homologous components* such as position and momentum.

From now on we consider a tentative relationship among some generic concepts such as indemonstrability, incompleteness and undecidability:
- theoretical incompleteness and indemonstrability; indemonstrability as a fact of incompleteness;
- demonstrability of incompleteness;
- the other issue is that of indemonstrability and (as?) undecidability.

### 3 Indemonstrability and undecidability

A problem is considered as “undecidable” when there is no algorithm that produces the corresponding solution in a finite time for each instance of the input data. A typical example is the *classic halting problem* for the Turing Machine [12]. The set of decidable problems is incomplete. In this regard, Turing himself introduced an issue of ‘completion’ by inserting the concept of Oracle [13], representing another logic, possibly incommensurable, that, however, combines, interferes, superimposes, and acts on that in use. All this in the framework of a general theory of truth, e.g., Tarskian semantics, see, for instance [1].

However, even in case of availability of effective computational algorithms, the finite precision or finite memory (in case for symbolic manipulation) implies theoretical incompleteness [14-16].

Moreover, another example is given by the non-explicit, non-symbolic computation, for instance, of Artificial Neural Networks (ANNs), see, for example [17, 18].

The computational processing is represented and performed in a non-analytical, non-symbolic way through weighted connections and levels. If we look instant per instant at the calculation performed, it is incomprehensible and we have to wait for the final result. This also applies to other computational processes such as Cellular Automata. The computation acquires properties not formally prescribed like learning [19, 20].

Particular classes of ANNs, such as those with non-Turing computable weights, and Recurrent-ANNs [21, 22] show a non-Turing behaviour for which the principles of hypercomputation [23-25] and naturally-inspired computation [26] apply.
Indemonstrability cannot be symbolically demonstrated and is intended to be a fact of incompleteness, case of undecidability. Furthermore, it is possible to conceptually consider symbolic demonstrability as having logical equivalences with decidability.

4 Prime numbers

Please download the latex template and see the .pdf file to see how to format editing definitions, theorems, corollaries.

At this point we may ask ourselves how to interpret the non-comprehension, the non-availability of the PDL, which is used in areas such as cryptography [27]? As incompleteness of the theory of numbers, undecidability, and indemonstrability [28]?

The problem has been frequented by mathematicians for centuries, with important, but not definitive results.

At this point we may consider two questions:
- In a constructivist understanding, can we intend such barrier to prevent an inevitably, implicitly inconsistent demonstration because a paradigm shift is required instead?
- In a platonic understanding, can we intend such a barrier to protect from an inevitably wrong demonstration contrasting with the general consistency and requiring different entry points?

4.1 A brief summary of the current situation

Attention to prime numbers first focused on the question whether they were infinite or not, and then turned to the understanding how they are distributed within natural numbers. It dates back to the 3rd century BC and to the Euclid’s first proof that infinitely many primes exist (see the Elements, Book IX, Proposition 20), see the Polignac’s conjecture below. In modern times Euler gave an alternative proof of this result by using, for the first time, concepts coming from infinitesimal mathematical analysis. Gauss understood the still fundamental key to the understanding of a crucial characteristic of the prime numbers: their density.

Riemann introduced his conjecture, listed below, which concerns the distribution of the zeros of a particular complex function, known as the zeta function, which has a very close connection with the distribution of primes. In particular, the distribution of the zeros of the zeta function is linked to the possibility of accurately counting the prime numbers.

In what follows, we propose a very short overview on the very large world of attempts to deal with the still unsolved problem of finding a PDL. This world
includes mainly conjectures and few theorems. We give approximate reference
dates for the convenience of the general reader.

4.2 An overview

The overview [29-31] includes the following subjects.

1) Goldbach’s conjecture 1742: every even integer greater than 2 can be expressed as the sum of two primes.

2) Cramér’s conjecture, 1936: it gives an asymptotic estimate for the size of gaps between consecutive prime numbers

\[ \limsup_{n \to \infty} \frac{p_{n+1} - p_n}{(\ln p_n)^2} = 1, \]

where:
- \( p_n \) denotes the \( n \)th prime;
- \( \ln \) is the natural logarithm.

This is based on a probabilistic model assuming that the probability that a natural number \( x \) is prime is \( 1/\ln x \), from which it can be shown that the conjecture is true with probability 1. In other words, if the prime numbers follow a "random" distribution, it is very likely that the conjecture is true. In short, the Cramér’s Conjecture states that the difference between two consecutive prime numbers always remains less than the square of the natural logarithm of the smaller of the first two.

This conjecture implies the following:

3) Opperman’s conjecture, approximately 1882: the conjecture states that, for every integer \( x > 1 \), there is at least one prime number between \( x(x - 1) \) and \( x^2 \).

This conjecture in turn implies the next conjecture:

4) Legendre’s (1752 – 1833) conjecture: it states that there exists at least one prime number between \( n^2 \) and \( (n + 1)^2 \) for all natural numbers.

The previous conjectures are all more restrictive than the Bertrand Postulate (which has been proven and is now a theorem):

5) Bertrand Postulate, approximately 1845: in its less restrictive formulation it states that for every \( n > 1 \) there is always at least one prime \( p \) such that \( n < p < 2n \).

6) Polignac’s Twin prime conjecture (approximately 1846 and previously considered by Euclid): it states that there are infinitely many twin primes, or pairs of primes that differ by 2. As numbers get larger, primes become less frequent and twin primes become rarer as well. In this regard in 1919 Brun’s Theorem showed that the sum of the reciprocals of the twin primes converges to a sum, now known as Brun’s constant. In 2010, the value of Brun’s constant was approximately \( 1.902160583209 \pm \)
based on all twin primes less than $2 \times 10^{16}$. Conversely, the sum of the reciprocals of all primes diverges to infinity [32].

7) Riemann Hypothesis, 1859: it deals with the distribution of the zeros of a particular complex function, now called "Riemann zeta function", which has a very close connection with the distribution of primes. In particular, the distribution of its zeros is linked to the possibility of accurately counting the prime numbers. The Riemann Hypothesis can be described geometrically by saying that the zeros of the Riemann zeta function are confined to two lines in the complex plane [33, 34].

8) The Prime Number Theorem (PNT) describes the asymptotic distribution of prime numbers: it states a general view of how primes are distributed among positive integers and also states that the primes become less common as they become larger. Let $\pi(x)$ be the prime-counting function that gives the number of primes less than or equal to $x$, for any real number $x$. The PNT then states that $x / \log x$ is a good approximation to $\pi(x)$, that is $\pi(x) \sim x \log x$. This notation means only that the quotient limit of the two functions $\pi(x)$ and $x / \ln (x)$ for $x$ which tends to infinity is 1, but not that the limit of the difference of the two functions, as $x$ tends to infinity, is 0. This means that for large enough $N$, the probability that a random integer not greater than $N$ is prime is very close to $1 / \log(N)$. The PNT is based on several previous and subsequent, increasingly specifying contributions, such as Legendre’s conjecture stating that $\pi(a)$ is approximated by the function $a / (A \log a + B)$, where $A$ and $B$ are unspecified constants; Gauss studied the problem; Dirichlet introduced a logarithmic integral $\text{li}(x)$ as approximating function; the connection between the prime number theorem and the Riemann zeta function is very deep and allowed by the Euler product.

The plausibility of such conjectures and approaches is supported by a large number of computational simulations which did not lead to falsifying cases.

5 Indemonstrability as undecidability of the distribution?

The main conclusions of the study may be presented in a short Conclusions section, which may stand alone or form a subsection of a Discussion or Results.

We are tentatively proposing to consider here the incomplete, probabilistic or approximate nature of PNT not as much as a limit to be solved by more appropriated approaches, but as an unavoidable theoretical aspect, price to be paid for consistency within the theory of computation rather than within number
theory itself. We consider here that number theory and its properties and theorems may be not incompatible with the availability of regularities in the distribution of prime numbers, while such availability can be considered incompatible with other properties and theories, such as general forms of theoretical, structural incompleteness, such as the halting problem for the Turing Machine in theory of computation.

We consider here, reasoning in proof by contradiction, that the computability of such distribution is possible.

5.1 Demonstrability as computability

The question relates to the conceptual availability of an algorithm able to compute general properties of the primes’ distribution.

Such properties are supposed to allow to know for any number the properties of the following sequence of prime numbers without computing each item of such sequences.

We just mention that the case of the knowledge of properties of a function, e.g., continuity, differentiability, minimum and maximum points, asymptotes, is different. Properties of a function are known from its formal definition and not from the knowledge of the properties of the distribution of all the values assumed in its domain of validity, i.e., law of distribution.

We may know the analytical properties of an exponential function without computing its values in any points on the abscissa axis.

The same holds for sequences of numbers such as the Fibonacci sequence defined as $F_n = F_{n-1} + F_{n-2}$, with $F_1 = F_2 = 1$ (two successive Fibonacci numbers are relatively prime).

How do we decide if a number is prime without computing?

When considering a number, we may take into account, for instance, some of its properties 1) will not require its factorisation –we consider here the case of factorization of an integer. We do not consider here the cases related to polynomial factorization and rings- or 2) will consider its factorisation.

As stated by the fundamental theorem of arithmetic every integer $> 1$ either is prime itself or is the product of prime numbers. This product is unique regardless of the order of the factors. The first explicit proof of the theorem of arithmetic, namely that the set of integer numbers has a unique factorization, is due to Carl Friederich Gauss, who inserted it in the Disquisitiones Arithmeticae, published in 1798, but already introduced by Euclid.

Examples of properties of the first kind (not requiring factorisation) are generic properties such as considering if a number is greater or less than another, the number of its digits, and if it is even or odd. Similarly, properties of values of a function are known from its formal definition and do not require the
effective computation of values. *Positions within the sequence of natural numbers correspond to properties.*

Examples of properties of the second kind (requiring the factorisation of the number) relate the identification of the number as given by the exponentiation of a base and prime numbers.

In the first case, it is possible to detect a property *without computing and factorise.*

However, *factorial properties of numbers,* as their factorial breakdown, exponential factor values and their being prime, i.e., non-decomposability, require their factorisation (or equivalent, e.g., the sieves), i.e., effective computing.

Properties of a distribution law, e.g., the graph of a function, its continuity, regularity, domains, and values of its derivatives, allow to know subsequent values moving along the graph without computing each value corresponding to the punctual abscissas.

In the case of factorisations, each of them must be computed since not made available by any property of a distribution law.

In the second case, factorisation is then *necessary.*

For instance, each value of the function \( f = x^n \) is available on its graph. Rather, each factorisation of an integer (factorisation is different from "combinatorial calculus" when factors are known) is in principle unknown and must be computed case by case, being not available from sequences or any graph.

In the first case, we have available the complete *computational procedure,* i.e., an algorithm.

In the second case, we have *factorisation techniques* available, but there are no known algorithms (can integer factorization be solved in polynomial time on a non-quantum computer [35]?) which can *effectively* factor arbitrary large integers, see, for instance, [36] and [37].

The adjective *effectively* refers to the definition of TM for which the *algorithm* should produce the solution in a *finite* time for each instance of the input data [12]. This also refers to *tractable* problems that can be solved by algorithms in *polynomial time,* i.e., for a problem of size \( n \), the time or number of steps needed to find the solution is a polynomial function of \( n \). Conversely, algorithms for solving *intractable* problems require times that are exponential functions of the problem size \( n \).

*Then factorisation is undecidable.*

Furthermore, we mention that sieves, such as the Eratosthenes, Legendre (it is an extension of Eratosthenes’ idea), Brun, Selberg, and Turán sieves [38], have an *exponential time complexity* with regard to input size, making them pseudo-polynomial algorithms.

*We consider the theoretical unavailability of a distribution law for factorial properties, as being prime, equivalent to its non-computability, undecidability.*
A conceptual proposal on the undecidability of the distribution law of prime numbers and theoretical consequences

The availability and demonstrability of a hypothetical PDL are inconsistent with its undecidability.

In the second case, factorisation is then necessary. Because of that it is not possible to know in advance the properties of the factorisations, in the same way as it is not possible to solve the alt of a TM (see the Introduction), it is not possible to know the result of the processing of a Neural Network without performing the entire processing, and to know the patterns generated by a Cellular Automata without performing the entire processing. Positions within the sequence of natural numbers do not correspond to the distributed property of being prime number.

In light of that, we tentatively propose the speculative conjecture that the complete knowledge of the PDL, that allows the availability of a rule, is not possible since it would disprove the Alt Problem for a TM. We conclude that the PDL is undecidable. We may conclude the indemonstrability of the Riemann Hypothesis (Millennium Problem), the Riemann hypothesis is undecidable in arithmetic.

Conceptual non-availability of an algorithm defines all undecidable problems as correspondent to the Alt Problem for a Turing Machine.

The probabilistic nature of PNT should be considered an aspect of its undecidability.

This will theoretically provide reassurance about the usage of prime numbers for a large variety of applications such as cryptography and pseudorandom number generation.

5.2 Using the indemonstrability

A theoretical incompletable list of non-equivalent models and approaches are necessary to deal with the endless acquisitions and modality of acquisition of properties in complexity and emergent phenomena. This is the case for uncertainty principles and theoretical incompleteness such as that of mathematics, of the Turing machines, and of the so-called Logical Openness in the Dynamic Usage of Models -DYSAM [39, pp. 64-88], based on established approaches in the literature, such as Ensemble learning [40, 41] and Evolutionary Game Theory [42, 43]. Other cases relate to the undecidability and irreducibility of emergence [17, 44], the usage of the non-computable and unknowable imaginary numbers, however very effective and used, and the non-symbolic computation of ANN and CA.

The non-demonstrability of the PDL primes’ distribution law is well used in cryptography in the same way as some pharmaceutical products are used for their side-effects.
This relates to the usage of the *theoretically incomprehensible* [45] which is suitable for introducing paradigm-shifts and non-equivalent, incommensurable, mutually irreducible approaches.

Can the non-demonstrability of the primes’ distribution law become the prototype of the non-distribution(s) having some possible different levels of equivalence; the prototype of the non-demonstrability, of theoretical incompleteness, and of theoretical incomprehensibility?

**Conclusions**

We shortly considered the research about primes in mathematics and the theoretical, still elusive, results looking for a PDL.

We considered as these endless difficulties may be interpreted as logical consistency, since the availability of such distribution law could be theoretically incompatible with other consolidated theories and properties.

This is the case for the theoretical incompleteness of mathematics, the Turing machines, and of the so-called Logical Openness in the use of Dynamic Usage of Models (DYSAM).

We considered the conceptual incompatibility of the availability of a PDL and the Alt Problem for a TM, i.e., implying that the PDL is undecidable.

*The link between the conceptual availability of a PDL and decidability* is given by considering how to decide if a number is prime without its computation. The supposed PDL should allow to know the sequence of primes without their computation, but considering only their sequential positions which coincide, however, with the numbers in question.

*However, factorial properties of numbers, such as their primality, require their factorisation (or equivalent, e.g., the sieves), i.e., effective computing.*

Because of that it is not possible to know in advance the properties of the factorisation, in the same way as it is not possible to solve the alt of a TM, it is not possible to know the result of the processing of a Neural Network without performing the entire processing, and to know the patterns generated by a Cellular Automata without performing the entire processing. *Positions within the sequence of natural numbers do not correspond to the distributed property of a prime number.*

We may conclude that the availability and demonstrability of a hypothetical PDL are inconsistent with its undecidability.

The perspective is to transform this conjecture into a theorem.

Furthermore, we considered the unavailability of a PDL as corresponding, representing incompleteness in mathematics and physics. However, such incompleteness can be used, e.g., for cryptography, imaginary numbers, and
A conceptual proposal on the undecidability of the distribution law of prime numbers and theoretical consequences

non-symbolic computation, in order to introduce paradigm-shifts and non-equivalent, mutually irreducible approaches.

References


A conceptual proposal on the undecidability of the distribution law of prime numbers and theoretical consequences

Notes in Computer Science; Springer: Cham, Switzerland, Volume 8553, pp. 379–392, 2014.


