

# Uncomputable Numbers

**Douglas S. Robertson**

Cooperative Institute for Research in Environmental Sciences  
University of Colorado  
Boulder, CO 80309

We have seen that the sequence of digits in numbers such as  $\pi$ , although they are an infinite string of random-looking digits, actually contain a only very small quantity of compressed information. The question immediately arises, are there numbers (strings of digits) that do not contain (cannot be compressed into) a finite quantity of compressed information? When the question is phrased this way, in terms of quantitative information requirements, the answer is fairly obvious. But when the problem was first posed in the 1930's mathematicians did not have access to the formalism of Greg Chaitin's Algorithmic Information Theory, and the problem was not only much more difficult, but the correct answer was not at all obvious. In fact, the correct answer appeared to many to be not just wrong, but absurd.

As with so much of the computer revolution, this surprising discovery sprang from the fertile intellect of Alan Turing. Turing's work was based on that of David Hilbert and Kurt Gödel, which in turn was based on the invention of set theory and transfinite algebras by Georg Cantor. One of Turing's profound insights led him to ask the startling question: Is there a number that cannot be expressed by any mathematical formula at all? He called this an "uncomputable" number, and he realized that the question is equivalent to asking whether there is a number that cannot be calculated by a computer program [see Turing, 1936].

Turing's question seems at first to be paradoxical, even nonsensical. How could there be such a thing as an uncomputable number? It would be beyond mathematics, in the sense that mathematics itself would not be powerful enough to express such a number.

The key to understanding the significance of Turing's question lies in an understanding of the similar crisis that was touched off by the discovery of irrational numbers by the Pythagoreans in about 500 B.C. The Pythagoreans knew about the positive integers, of course, (1, 2, 3, . . .) and they knew how to add, subtract, multiply and divide integers, although, lacking place-value notation for numbers, their techniques for multiplication and especially division were incredibly tedious and clumsy. Awkward as they were, the Pythagorean's techniques were good enough to allow them to handle the arithmetic of the rational numbers as well as integers (a rational number or fraction is defined as a ratio of two integers, *i.e.*,  $3/5$ ,  $10/3$ , etc.) And the Pythagoreans knew a great deal about the properties of integers and rational numbers. They knew about prime numbers, for example, and Euclid was to prove that the number of primes is infinite. (A description of Euclid's proof is given in Appendix 1.) Further, they knew that the rationals are dense. In other words, given any two distinct rational numbers, no matter how close they are in magnitude, there is an infinite number of rational numbers between them. The argument is straightforward: the mean

or midpoint between any two rational numbers is rational. And the midpoint between one of the numbers and the original midpoint is rational, etc. (See the discussion in Courant and Robbins, 1996, pp. 57-58.)

If there is an infinite number of rational numbers contained in any interval, no matter how small that interval is, then that would seem, naively, to be enough numbers. Why on Earth would anyone ever need any more than that? And yet the Pythagoreans were able to prove that  $\sqrt{2}$  is not a rational number, that there are no integers  $a$  and  $b$ , whose ratio gives  $\sqrt{2}$ . A modern version of the proof is given in Appendix 2. According to some accounts this discovery so frightened the Pythagoreans that the mathematician who discovered irrational numbers, Hippasus, was taken out in a ship and thrown overboard [Dunham, 1990, pp. 9-10]. Today they might simply cut off his research grant. But the historical records are a bit vague: Rather than discovering irrational numbers, Hippasus' crime may have been merely to reveal their existence to non-members of the secretive Pythagorean sect.

The discovery of irrational numbers gave the first clue that arithmetic was vastly more complicated and more mysterious than it appeared. For the Pythagoreans, an irrational number was something that could not be expressed within the mathematics that they knew. They had no idea how to perform arithmetic with such numbers or even how to write them down. They simply could not understand how irrational numbers could exist. The uncomputable numbers present similar philosophical difficulties for modern mathematics, but at a far deeper level.

In the eighteenth century, the Swiss mathematician Leonhard Euler noticed that the existence of irrational numbers raised some very profound questions. The rational numbers can be defined as the numbers that satisfy linear equations with integer coefficients. In other words, if  $a$  and  $b$  are integers, then the linear equation:

$$ax + b = 0 \tag{1}$$

defines a rational number,  $x$ , and all rational numbers can be expressed in this form. Since the existence of irrational numbers proves the existence of numbers that cannot be expressed with linear equations, Euler wondered if perhaps there exist numbers that cannot be expressed with an equation of any order. In other words, Euler asked if there is a number  $x$  that cannot be expressed as the solution to a polynomial of any order, an equation of the form:

$$a + bx + cx^2 + dx^3 + ex^4 + \dots = 0 \tag{2}$$

in which all of the coefficients ( $a, b, c, \dots$ ) are integers. Euler called such a number a transcendental number. After more than a century of work, Hermite was able to prove that  $e$  (the base of natural logarithms, 2.71828 . . .) was a transcendental number, and Lindemann later showed that  $\pi$  was also transcendental [Stewart, 1996, p 66].

Therefore Alan Turing knew that there that there were numbers that could not be expressed by linear equations, and numbers that could not be expressed by polynomial equations of any order. He then asked whether there exists a number that cannot be expressed by any mathematical

expression at all, a number whose value could not be calculated by any finite sequence of logical operations, and called such a number an “uncomputable number.” This is a natural generalization of Euler’s question, and yet it is far more profound. The irrational numbers demonstrate the existence of limits on the power of linear equations. The transcendental numbers demonstrate the existence of limits on the power of polynomial expressions. Turing’s question suggests the existence of limits on the power of mathematics itself. Turing was able to prove the surprising result that the uncomputable numbers do exist. Perhaps even more surprising, essentially *all* numbers turn out to be uncomputable. The computable numbers, including all of the numbers that are actually used in any mathematical calculation (such as 2, 19,  $\pi$ , and  $\sqrt{2}$ ) are the genuine oddballs in the real number system.

This demonstration that nearly all real numbers are beyond the power of mathematics itself is an insight as deep and troubling for us as the existence of irrational numbers was for the Pythagoreans. As we noted, rational numbers contained all of the numbers that the Pythagoreans knew how to express and manipulate. To them the irrational numbers were somehow not numbers. Yet from our vantage point today, we can see a long history of this type of discovery, the successive inventions of new kinds of numbers that could not be manipulated or even expressed using the rules that worked perfectly well for all of the numbers that were known previously.

The first such discovery was the rationals themselves. The first use of rational numbers is lost in the mists of history. In Egypt, at the time of the Rhind Papyrus (about 1700 BC) scribes are already handling rational numbers (See Newman, 1956). Yet the rationals do not behave the same way that integers do: to manipulate rationals you need a new algebra. In modern notation, the algebra of rational numbers uses rules that look something like this [*cf.* Courant and Robbins, 1996, pp. 52-54]:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad (3)$$

Which in fact is exactly the way that the integers behave (just set  $b = d = 1$ ) although the arithmetic of integers is not usually expressed in this fashion. This is typical of the invention of new types of numbers. New rules are developed that work perfectly well for both the old numbers and the new ones. The new rules replace the old rules, which only apply to the older types of numbers.

Similarly, the irrational numbers cannot be handled with the rules used to calculate the rational numbers. To deal rigorously with irrationals you need new notations and mathematical techniques including such things as non-terminating decimal fractions and infinite series, which can handle both rational and irrational numbers [Courant and Robbins, 1996, pp. 58-72].

But even before the difficulties with irrational numbers were sorted out, mathematicians encountered another type of number that did not behave according to the rules that were known previously. The development of negative numbers created a similar crisis. As Stewart noted [1996, p. 155]:

In the mid-1600's Antoine Arnauld argued that the proposition  $-1 : 1 = 1 : -1$  must be nonsense: 'How can a smaller be to a greater as a greater is to a smaller.' . . . In 1712 we find Leibniz agreeing that Arnauld had a point.

It turns out, as we might have expected, that there is no real problem here. What is needed is a new algebra, a new set of rules for handling numbers. The new rules look something like [Courant and Robbins, 1996, pp. 54-55]:

$$(-a)(-b) = ab \tag{4}$$

But mathematicians had no sooner begun to develop the algebra of negative numbers when another new type of number began to appear in their calculations: square roots of negative numbers. And again the cry was heard: These things are not numbers. They do not follow the rules that we use to represent and to manipulate numbers. And once again the cure was the same: New rules were needed, new algebras that could handle these numbers correctly. A sample of the new rules looks something like [Courant and Robbins, 1996, pp 88-92]:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \tag{5}$$

Again notice that, just as before, the new rules apply perfectly well to the old numbers (this time set  $b = d = 0$ ).

Now we come to the crux of the problem with uncomputable numbers. At first blush they might seem to be just the next step in this sequence, a new type of number that present mathematics cannot cope with, but that some brilliant new discovery will allow us handle with ease and alacrity. But this is not the case. Today, thanks to the work of Cantor, Gödel, and Turing, we know far more about the limitations of mathematics itself than any earlier generation of mathematicians did. And it is clear that the problem with uncomputable numbers lies in those fundamental limitations of mathematics itself, rather than with any inadequacy of our current methods and techniques.

A full understanding of uncomputable numbers is deeply bound up with fundamental questions concerning the nature of infinity. Mathematicians over the centuries have argued that infinity cannot exist, that it is not a number. Why? Because infinity does not obey the same rules that other numbers do.

Does this sound familiar? By now it should. And it does not mean that infinity does not exist, nor that it is not a number. In fact, infinity is a lot of numbers. As we shall see, there is more structure among the infinite (or transfinite) numbers than there is within the more conventional finite numbers. But the transfinite numbers need a new algebra, a different set of rules, just as the irrational numbers and the imaginary numbers had needed new sets of rules in the past. The transfinite numbers actually proved to be somewhat more tractable than the uncomputable numbers, which are ordinary, finite real numbers. This should not be too surprising: after all, transfinite numbers were discovered first, before the turn of the twentieth century, in fact.

The development of the algebra of transfinite numbers was largely the creation of one man: Georg Cantor. Cantor devised at least five major ideas, each of them so brilliant and original, so simple, elegant, and powerful, that each one alone would have been sufficient to be the crowning event in the career of a great mathematician. The first of Cantor's major ideas was the basic realization that infinities were not absurd or impossible, but were actually numbers that needed only a new algebra to unlock their mysteries.

Intellectuals as far back as Galileo had argued that infinite numbers were absurd because, for example, every positive integer can be multiplied by itself to produce a perfect square, and every perfect square has an integer square root. Therefore there are exactly as many perfect squares as integers, although the perfect squares constitute only a small part (a "proper subset") of the set of integers. This violates a fundamental mathematical principle that goes back at least as far as Euclid's Common Notion number 5: the whole is greater than the part.

Cantor developed the fundamental insight that this Euclidean principle applies only to finite numbers. Further, he realized that the property of having parts that are equal to the whole is the defining property of infinite numbers. It is the single attribute that is possessed by all infinite numbers, and by no finite number. This is another of Cantor's original ideas.

The next idea of Cantor's is hinted at in Galileo's argument. Cantor realized that in order to deal with the question of what it means to say that one transfinite number is different from another, he first had to deal with the question of what it means to say that a pair of transfinite numbers are equal to one another. To settle this problem he developed the notion of a set, which is simply a definable collection of objects or elements. A set may contain a finite or an infinite number of objects. The question Cantor then had to resolve is: Under what conditions can we say that two sets contain the same number of elements? If the sets each contain a finite number of elements, there is no difficulty: We simply count the elements in each set. But if the sets each contain an infinite number of elements then we need a more powerful idea than counting. It is not practical to count the elements of an infinite set; it takes just too much time.

Cantor's new idea was the following definition: two sets of objects are said to contain the same number of elements if those elements can be put in one-to-one correspondence; *i.e.*, if every element in one set can be matched up with exactly one element in the other set, with no elements in either set left out of the matching. This essential idea is easier to understand than it is to state. To take a simple example, suppose you are feeding lunch to a small army. Just as everyone is seated, you suddenly realize that you do now know whether you have the correct number of forks. And it would take hours to count both people and forks. But you do not need to count. You simply ask everyone to pick up a fork. You then ask if there is anyone who does not have a fork. If everyone has a fork, you then ask whether there are there any forks left on any of the tables. If there are no forks left, then you know that you have exactly the right number of forks, even though you do not know how many forks or people there are. You have demonstrated a one-to-one correspondence between people and forks, and that is all you need to know.

This idea, of one-to-one correspondence, is brilliant in its simplicity, elegance and stunning power. Cantor realized that it is powerful enough to count infinite numbers. It is the basis of the algebra of the transfinite numbers. The idea is so simple that it may seem odd to spend so much time on it, but it is so powerful and so critically important that it must be clearly understood.

The idea of one-to-one correspondence is closely related to counting, which is simply a process of putting objects in one-to-one correspondence with positive integers. But it is much more powerful than counting because you do not actually have to do all the work. You can simply describe the correspondence rigorously. For example, in Galileo's argument, the set of positive integers can be put in one-to-one correspondence with the set of perfect squares. No one would argue that any integer or perfect square has been left out or forgotten from the correspondence. Did we forget that 28472 is matched with 810654784? No, we did not forget it. It is right there on the list. Yet we were able to construct this entire matching convincingly in a very short amount of time, a few seconds even, far less time than would be needed to count all of the squares.

Now at last mathematicians were in possession of a tool that is powerful enough to investigate the nature and properties of the transfinite numbers. And in the hands of a genius this simple tool revealed the most surprising results.

Cantor began examining the sets that could be put in one-to-one correspondence with the positive integers. They are called "countable" or "denumerable" sets, for the obvious reason. Infinite sets of positive numbers such as even numbers, squares, cubes, or primes, were trivially countable. More surprisingly, Cantor found that the rational numbers are countable. It began to look as if every infinite set were countable.

We now come to the most surprising result of Cantor's remarkable career. He next showed that the real numbers (rationals plus irrationals) are not countable. In other words, there is an infinity that is larger than the number of positive integers. The proof is so simple that it is easy to describe in a few minutes. Indeed there are many accounts of it in the popular literature, dating back at least to Hahn [1956] and Gamow [1961]. The critical proof begins by assuming that the real numbers are countable, and then uses this assumption to derive a very simple contradiction, thereby showing that they are not countable. The proof is sketched in Appendix 3.

This discovery, that there are at least two infinite numbers that are unequal, would have been enough by itself to place Cantor in the first rank of mathematicians. But he did more. With another proof that is only slightly more complicated than the one cited above, he showed that there are more infinite numbers. There are lots of them.

To sketch out how this proof works, we need to define some terminology and describe some of the theory of sets. A "subset" of a set is defined as a set that is made up of elements selected from the original set. The subset may contain all of the elements of the original set, or it may contain no elements at all. (The set with no elements is called the null set or the empty set. This set, by definition, is a subset of every set). A "proper subset" is defined as a subset that is not empty nor does it contain all of the elements of the original set.

Now if the original set has  $n$  elements, then there are  $2^n$  possible subsets. The proof of this is straightforward: there are two possibilities for the first element in the set (in or out of the subset), two more for the second element, two for the third, etc., so the total number of possibilities is  $2 \times 2 \times 2 \dots = 2^n$ . Similarly, there are  $2^n - 2$  proper subsets (all of the original subsets minus the empty set and the entire set).

The essence of Cantor's new proof involves showing that the elements of a set cannot be placed in one-to-one correspondence with all of the subsets of that set. For a set with a finite number of elements the proof is trivial because  $2^n$  is larger than  $n$  for all finite  $n$ . But for a transfinite number of elements we have to make the argument with more care. The proof is sketched in Appendix 4.

Since the number of subsets of a set must be larger than the number of elements in the set, each transfinite number can be used to generate a larger number by calculating the number of subsets of a set with that number of elements. Cantor called the first transfinite number (the infinity of the counting numbers)  $\aleph_0$ . We could then list an infinite sequence of transfinite numbers:

$$\begin{aligned} \aleph_1 &= 2^{\aleph_0} \\ \aleph_2 &= 2^{\aleph_1} \\ \aleph_3 &= 2^{\aleph_2} \\ &\vdots \\ &\vdots \\ &\vdots \end{aligned}$$

An excellent and readable discussion of the details of Cantor's proofs can be found in Dunham [1990, pp 245-280].

Cantor then asked one more question that finally defeated even his genius. The question that he was unable to answer is: Does this list contain all of the transfinite numbers? Or have we missed any? Cantor was able to show that there is no transfinite that is smaller than  $\aleph_0$ . But he then asked whether there is any transfinite number between  $\aleph_0$  and  $2^{\aleph_0}$ . He believed that there was no such number, but he was unable to prove it. We now know that he failed to prove this conjecture because it is false. There are numbers between  $\aleph_0$  and  $2^{\aleph_0}$ , although, in an odd twist, you can ignore them and still have a consistent mathematics, just as you can develop a consistent mathematics of the integers while ignoring the existence of all of the numbers that lie between any two consecutive integers.

And there is yet another set of transfinite numbers that Cantor missed. In an uncanny echo of Euler's and Turing's questions, mathematicians asked whether there are infinite numbers that cannot be expressed in this fashion. And again the answer is yes: There is a set of transfinities that are too large to be expressed in terms of other transfinities. They are now known as the "inaccessible infinities." The inaccessible infinities turn out to be important in Lebesgue measure theory [Stewart, 1996, p 69].

Is this the end of the story? Do we finally have a complete understanding of numbers, and of what constitutes a number? Of course we do not. The process never terminates. Just when we think that we understand numbers, they surprise us once again. Even today, mathematicians are exploring the properties of another new type of number, the “non-standard” or “hyperreal” numbers, that hold the potential of revolutionizing the calculus and vastly simplifying it, according to the proponents of the idea. The hyperreal numbers were developed to allow a rigorous definition of infinitesimal numbers [Stewart, 1996, pp. 80-88].

We now return to the question that began this discussion, the existence of uncomputable numbers. Using Cantor’s algebra of transfinite numbers, it is straightforward to show that the computable numbers form a countable set. The argument is fairly simple: any computer program can be expressed as a sequence of binary digits. And the number of possible sequences of binary digits is just the number of counting numbers,  $\aleph_0$ . And the number of output values, compressible or incompressible, from each program is at most  $\aleph_0$ . So the maximum number of possible computable numbers is  $\aleph_0 \times \aleph_0$ . But in his famous proof that the rational numbers are countable Cantor had shown that  $\aleph_0 \times \aleph_0$  is just  $\aleph_0$ , a countable infinity. So the computable numbers form a countable set. And Cantor had shown that the set of real numbers (including the irrationals) contains a larger infinity than this. Therefore, as we said, nearly all numbers are uncomputable. There are simply too many real numbers, and there are not enough formulas (computer programs or sequences of mathematical operations) to cover all of them, even if each formula is able to express a lot of computable numbers.

What does an uncomputable number look like? It is hard to describe explicitly because the description cannot be done in terms of mathematics. Yet it is not difficult to give an operational definition for the construction of an uncomputable number. You simply toss a coin or roll some dice or use any other genuinely random process to determine each digit of the number. When you have done this an infinite number of times, you will have (with a probability of one) generated an uncomputable number. This may help to clarify the idea that uncomputable numbers comprise nearly all numbers: it simply means that if you select a number at random, its digits are very likely to be random. In point of fact, it is not necessary that every digit of an uncomputable number be determined randomly. It is only necessary to have an infinite number of such digits. An uncomputable number could consist of all zeros, for example, except for every millionth or billionth digit, which is determined randomly.

Another useful way to think about uncomputable numbers uses the concept of conservation of information. Since an uncomputable number contains an infinite number of randomly determined digits, it contains an infinite amount of compressed information. And an infinite amount of compressed information cannot be compressed into any finite computer program. That would violate Greg Chaitin’s theorem that information is conserved under logical operations. Therefore no finite computer program can generate an uncomputable number. This is fundamentally what “uncomputable” means. But a computer program is just a string of logical operations, and logical operations are what defines mathematics. Therefore no sequence of mathematical operations can produce an uncomputable number.

Also recall from the discussion of compressibility of information Chaitin's theorem that states that most long bitstrings cannot be compressed. As the length of the string approaches infinity, the fraction that *can* be compressed (the ratio of computable numbers to uncomputable numbers) approaches zero, because the computable numbers form a countable set and the real numbers do not.

Therefore, even though our ability to define and manipulate new types of numbers will go on forever, there will always remain the vast ocean of uncomputable numbers forever beyond our reach. They are as remote and inaccessible as the final digits of  $\pi$ .

The discovery of uncomputable numbers demonstrates the existence of limits on the capabilities of computers, which are in fact limits on mathematics itself. No computer program can calculate the value of an uncomputable number. Nearly all numbers are therefore beyond the power of both computers and mathematics. The concept of "number" is too powerful for mathematics to handle. Only the computable numbers lie within the capabilities of mathematics. Few more startling and unexpected discoveries have ever been made in mathematics. And it may be hard to imagine that even stranger discoveries await us in mathematics. But there is no reason to think that the process will end, or that the next discovery will be less strange than the last. As J.B.S. Haldane succinctly put it, the world is not only stranger than we imagine, it is stranger than we can imagine. This is yet another of the stunning changes in fundamental philosophical outlook or viewpoint that have accompanied the dawn of a new level of civilization, as described in Robertson (1998).

#### References:

- Courant, R., and H. Robbins, *What is Mathematics*, Oxford University Press, Oxford, 1996.
- Dunham, W., *Journey Through Genius: The Great Theorems of Mathematics*, Wiley, New York, 1990.
- Gamow, G., *One, Two, Three, . . . Infinity*, Viking Press, New York, 1961.
- Newman J.R., The Rhind Papyrus, in *The World of Mathematics*, J.R. Newman (ed.), vol 3, pp 170-179, Simon and Schuster, New York, 1956.
- Hahn, H., Infinity, in *The World of Mathematics*, J.R. Newman (ed.), vol 3, pp 1593-1618, Simon and Schuster, New York, 1956.
- Kline, M. *Mathematics -- The Loss of Certainty*, Oxford U. Press, Oxford, 1980.
- Robertson, D.S., *The New Renaissance: Computers and the Next Level of Civilization*, Oxford University Press, Oxford, UK, 1998; ISBN-10: 0195121899; ISBN-13: 978-0195121896.
- Stewart, I., *From Here to Infinity*, Oxford U. Press, New York, 1996.
- Turing, A.M., On Computable Numbers, with an Application to the Entscheidungsproblem, in *Proceedings of the London Mathematical Society*. 2 **42**: 230–65. 1936–37.  
[doi:10.1112/plms/s2-42.1.230](https://doi.org/10.1112/plms/s2-42.1.230)
-

**Appendix 1:** Euclid's proof that the number of prime numbers is not finite.

Euclid's proof is given here because it is intrinsically interesting, historically interesting, and because it is related to the remaining arguments here. Its historical interest is that it is one of the earliest proofs in number theory to survive. It is relevant because it has the identical form as the other three proofs contained here. In order to prove that something does not exist, you first assume that it does exist (assume the converse), and then use this assumption to derive a contradiction.

Following the discussion in Courant and Robbins [1996, pp. 22-23], to prove that the number of prime numbers is not finite, we first assume that there is only a finite number,  $n$ , of them. If  $n$  is finite, then in principle we could construct a complete list of all of the primes  $P_1, P_2, P_3, P_4, \dots, P_n$  using an algorithm like the sieve of Eratosthenes [see Courant and Robbins, 1996, p 25]. But we can then use this list to generate new prime numbers that are not on the list. To do this we multiply together all of the primes on our (complete) list and add 1, to generate the number  $A$ .

$$A = P_1 \times P_2 \times P_3 \times P_4 \dots \times P_n + 1$$

The critical fact about  $A$  is that when you divide it by any of the prime numbers on list of primes you get a remainder of 1. Thus  $A$  is not divisible by any of those prime numbers. Now if  $A$  is prime then the proof is completed, because you have shown that there is a prime that is not on the list, which was complete under the assumption that the number of primes is finite. However, if  $A$  is not prime you are no better off, because  $A$  must then be divisible by at least two primes and you already know that it is not divisible by any of the primes on your list. Therefore, again, there must exist prime numbers that are not on your list.

This is the essential contradiction that Euclid found: If you assume that the number of prime numbers is finite, then you can list them all and then use that list to generate prime numbers that are not contained on the list. Thus any finite list must be incomplete and the complete list of primes cannot be finite. The structure of this proof is strikingly similar to Cantor's proof in Appendix 3.

---

**Appendix 2:** Proof that  $\sqrt{2}$  is not a rational number.

Unfortunately, we do not know the exact form of the proof derived by the Pythagoreans. No text of the original proof survives. What follows here is a modern proof, but it is one that is probably similar to the arguments made by the Pythagoreans. It does not use any concepts that would have been unfamiliar to them, and it is consonant with Aristotle's comment that the proof involved showing that a number must be both odd and even at the same time [Kline, 1980, pp. 104-105].

To prove that  $\sqrt{2}$  is not rational, we once again begin by assuming the converse, that it is rational. In other words, we assume that there exist two integers  $a$  and  $b$  such that:

$$\sqrt{2} = a/b \tag{1}$$

or

$$\sqrt{2} b = a \tag{2}$$

Without loss of generality, we can assume that the fraction in equation 1 is reduced, in other words that  $a$  and  $b$  contain no common factor. This is critical to the proof. (If  $a$  and  $b$  do contain a common factor, we can always remove it by reducing the fraction to its lowest terms and then proceed with the argument.) Now since we are dealing with exclusively positive numbers there are no problems introduced by squaring both sides of equation 2:

$$2 b^2 = a^2 \tag{3}$$

And immediately we are in trouble, because no perfect square is twice the size of another perfect square. To see why this is so, let us complete the proof. We need to realize that the square of an even number is even, and the square of an odd number is odd (the proof of this will be left for the interested reader). Now  $a^2$  must be an even number, because of the factor of 2 on the left-hand side of this equation. Therefore  $a$  must be an even number. We can then write:

$$a = 2 c \tag{4}$$

where  $c$  the integer that is half of  $a$ . But substituting (4) into (3) gives:

$$2 b^2 = (2 c)^2 \tag{5}$$

or

$$b^2 = 2 c^2 \tag{6}$$

But by the same argument this equation implies that  $b$  is an even number. Therefore both  $a$  and  $b$  must be even numbers, and this contradicts our original assumption that  $a$  and  $b$  have no common factor.

There is another way to approach the problem that may be a little simpler and clearer, but it makes use of the fact that any integer can be written as a product of prime numbers in exactly one way, which had not been proved in Pythagoras' day but was proved in Euclid (proposition IX.14). The key to this proof lies in the fact that the prime factors of a perfect square always occur an even number of times (because each is repeated in the process of squaring--the details are left for the interested reader). Thus if you examine the prime factors of the numbers on each side of equation 3, you find that there must be an even number of 2's on the right side, but an odd number on the left (because of the extra 2). And this is impossible because the prime factorization of a number is unique. This is an example of proof by parity check, or a check on oddness and evenness.

**Appendix 3:** Cantor's proof that the real numbers (rationals plus irrationals) are not countable.

Cantor's proof is startlingly similar to Euclid's proof in Appendix 1. Euclid assumed that he could construct a complete and finite list of prime numbers, and then used the list to generate a prime number that is not on the list. Here we will assume that we have a complete and countable list of the real numbers, and use the list to generate a real number that is not on the list.

Cantor's proof therefore begins as before by assuming the converse, that the real numbers are countable. And for convenience we will restrict ourselves to the real numbers between 0 and 1. (If they are not countable, then the entire set is not countable either.) If these real numbers are countable then they can be placed in one-to-one correspondence with the positive integers. The correspondence would have to look something like this, with the integers on the left and real numbers on the right:

1	. <b>1</b> 9644288109756658 . . .
2	.0 <b>3</b> 486104543266486 . . .
3	.09 <b>6</b> 28292540917152 . . .
4	.160 <b>9</b> 4330572703651 . . .
5	.2749 <b>5</b> 673518857526 . . .
6	.49463 <b>9</b> 52247371909 . . .
7	.940513 <b>2</b> 0005681276 . . .
8	.1224953 <b>4</b> 301465490 . . .
9	.44181598 <b>1</b> 36297743 . . .
10	.609631859 <b>5</b> 0244591 . . .
.	.
.	.
.	.

Every integer appears on the left hand side of the list. And if this list exhibits a one-to-one correspondence between the integers and the real numbers, as assumed, then every real number (between zero and one) must appear somewhere on the right-hand side.

We know what the left-hand side of the list looks like. And although we don't know what the right-hand side looks like, we can use it anyway to derive the desired contradiction. Whatever real numbers appear on the right-hand side, we can always construct a real number whose successive digits consist of the first digit from the first number on the list, the second digit from the second, and so forth, selecting the digits along the diagonal of the list. These digits are printed in bold type in the sample list above. (This is why the proof is referred to as Cantor's "diagonal proof.") In the case of this particular list, the number would look like:

.1369592415 . . .

Next we construct a new real number by adding .11111111 . . . to this number, neglecting the operation of carrying, i.e.,  $9+1=0$ . The resulting number is:

.2470603526 . . .

Cantor then asked the deadly question: Where does this new number occur in our list? If the list contains all real numbers then this number must be there somewhere. But it is not the first number on the list, because it is different from that number in the first digit. It is not the second number because it is different from that number in the second digit. Similarly, it is not the third on the list, or the fourth, or the fifth, or . . .; it is simply not anywhere on the list, which we assumed was complete. And this argument holds no matter how the numbers are arranged on the right-hand side of the list. This is the contradiction that Cantor discovered, and it completes the proof.

There are a few more technicalities that Cantor had to deal with. He used a more rigorous method of generating the number that is not on the list, for example. But this is the essence of the proof: no matter how you try to set up a one-to-one correspondence between the positive integers and the real numbers, there is always at least one real number that is not on the list. We can *always* construct such a number. In fact, we can always construct lots of them. Thus there is no one-to-one correspondence between the positive integers and the real numbers. These two infinite numbers (the number of integers and the number of real numbers) are not equal, because the necessary one-to-one correspondence does not exist.

**Appendix 4:** Cantor’s proof that the elements of a set cannot be placed in one-to-one correspondence with the subsets of that set:

Cantor’s proof begins the same way as all of the proofs here: It assumes that the subsets of a set can be placed in one-to-one correspondence with the elements of a set, and it then uses this assumption to derive a contradiction, thereby showing that at least one subset is always missing from the matchup.

The argument from this point on is more subtle and requires a little more effort than in the diagonal proof (Appendix 3). Basically, Cantor notes that when you match each element of a set with some subset of that set there are two possible types of matching. In the first type, the matched element is a member of the subset that it is matched with; in the second type, the element is not a member of its matched subset. All of the matchings must be of one type or the other. If the elements in the set are labeled a, b, c . . . (continuing with an infinite alphabet) then the matching might look something like this:

a - {a,c,d}  
 b - {b}  
 c - {b,c,d,p,q,z}  
 d - {b,c,d}  
 .  
 .  
 .  
 -----  
 p - {b,e,q,z}

q - {a}  
r - {x,y,z}  
s - {c,d,e,f,g,h,i}  
.  
.  
.

Where the brackets denote a subset and the dashed line separates the two types of matchings. The key to the argument is that the elements on the left side that are below the dashed line constitute a subset of the original set {p,q,r,s . . .}. Again, Cantor asks the deadly question: Where does this subset appear on the right-hand side of the list? In fact, it cannot be found anywhere on the right-hand side of the list. It cannot be above the dashed line, because each of the subsets there contains the element that it is matched with, none of which is contained in the critical subset. Similarly, it cannot be below the dashed line, because each of those subsets does not contain the corresponding element on the left-hand-side, all of which are in the critical subset. Therefore, no matter how you try to match the elements of a set with the subsets of the same set, you can always construct at least one subset that is missing from the matchup.

---

The above text is adapted from Robertson, 1998, pp. 71-92.