THE PRIME NUMBER THEOREM AND THE RIEMANN HYPOTHESIS

A marriage of calculus and arithmetic

BERNARD RUSSO
University of California, Irvine

MARINA HIGH SCHOOL
JUNE 7, 2011

Biographical Sketch—Bernard Russo

Graduate Study in Mathematics
UCLA 1961-1965

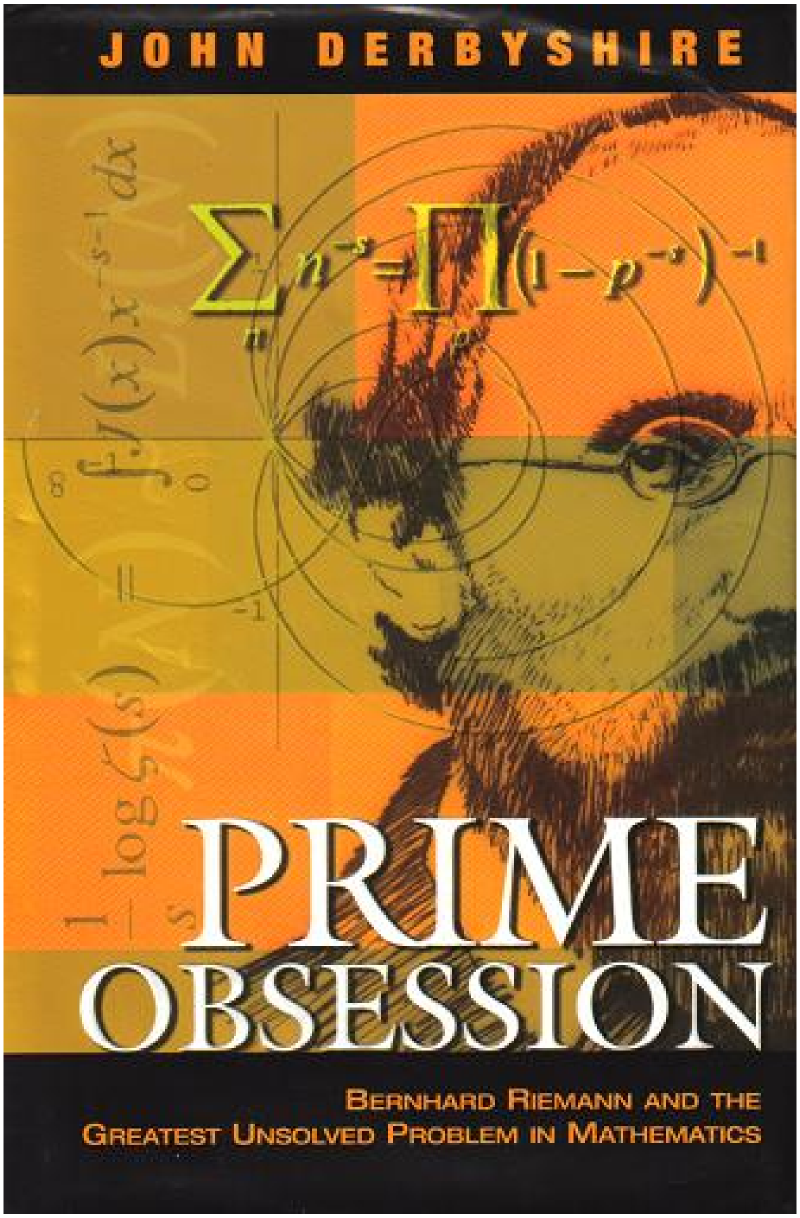
Professor of Mathematics
UCI 1965-2005

Professor Emeritus of Mathematics
UCI 2005-present

Associate Secretary
American Mathematical Society 1998-2002

Chairman
Department of Mathematics UCI 2001-2004

“book report”
“PRIME OBSESSION”


JOHN DERBYSHIRE
$\sum_n n^{-s} = \prod_p (1-p^{-s})^{-1}$
$\frac{1}{s}\log\zeta(s) = \int_0^\infty J(x)x^{-s-1}\,dx$
PRIME OBSESSION
BERNHARD RIEMANN AND THE GREATEST UNSOLVED PROBLEM IN MATHEMATICS

JOHN DERBYSHIRE

2003

Prologue

- Is there a general rule or formula for how many primes there are less than a given quantity, *that will spare us the trouble of counting them*? (The Prime Number Theorem PNT, proved in 1896, does this approximately; the Riemann Hypothesis RH, still unproven, does this exactly.)

- The Riemann Hypothesis is now the great white whale of mathematical research. The entire twentieth century was bracketed by mathematicians' preoccupation with it.

Unlike the

Four-Color Theorem,
or
Fermat's Last Theorem,
the
Riemann Hypothesis

is not easy to state in terms a nonmathematician can easily grasp.

The four-color problem was stated in 1852 and solved in 1976;

Fermat's Last 'Theorem' was stated in 1637 and solved in 1994;

the Riemann Hypothesis was stated in 1859 and remains unsolved to this day.

Divergence of the harmonic series

$1 + 1/2 + 1/3 + 1/4 + \cdots = \infty$

Proof: (Nicole d'Oresme 1323–1382).

$$\begin{aligned} 1/3 + 1/4 &> 1/2 \\ 1/5 + 1/6 + 1/7 + 1/8 &> 1/2 \\ 1/9 + 1/10 + \cdots + 1/16 &> 1/2 \\ \ldots \end{aligned}$$

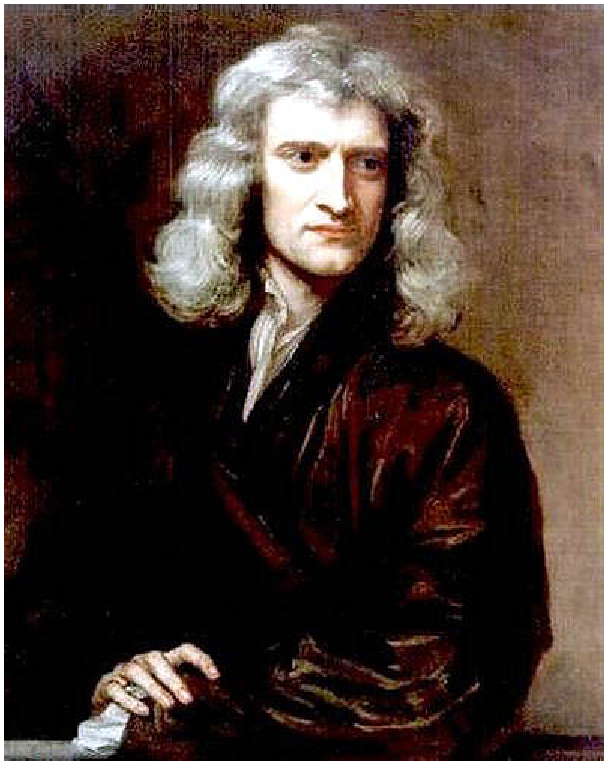
("You can't beat going to the original sources.")

The traditional division of mathematics into subdisciplines:

Arithmetic (whole numbers)
Geometry (figures)
Algebra (abstract symbols)
Analysis (limits).

The first and last combine to form *analytic number theory*. There are others (and how!)

Analysis dates from the invention of calculus by Newton and Leibnitz in the 1670s.



Arithmetic, by contrast with analysis, is widely taken to be the easiest, most accessible branch of math. Be careful though—it is rather easy to state problems that are ferociously difficult to prove (e.g., Goldbach conjecture, Fermat's Last 'Theorem').

MATHEMATICS SUBJECT CLASSIFICATION

(AMERICAN MATHEMATICAL SOCIETY)

00-XX General
01-XX History and biography
03-XX Mathematical logic and foundations
05-XX Combinatorics
06-XX Lattices, ordered algebraic structures
08-XX General algebraic systems
11-XX **NUMBER THEORY**
12-XX Field theory and polynomials
13-XX Commutative algebra
14-XX Algebraic geometry
15-XX Linear algebra; matrix theory
16-XX Associative rings and algebras
17-XX Nonassociative rings and algebras
18-XX Category theory; homological algebra
19-XX K-theory
20-XX Group theory and generalizations
22-XX Topological groups, Lie groups
26-XX Real functions
28-XX Measure and integration
30-XX **COMPLEX FUNCTION THEORY**

31-XX Potential theory
32-XX Several complex variables
33-XX Special functions
34-XX Ordinary differential equations
35-XX Partial differential equations
37-XX Dynamical systems, ergodic theory
39-XX Difference and functional equations
40-XX Sequences, series, summability
41-XX Approximations and expansions
42-XX Harmonic analysis on Euclidean spaces
43-XX Abstract harmonic analysis
44-XX Integral transforms
45-XX Integral equations
46-XX Functional analysis
47-XX Operator theory
49-XX Calculus of variations, optimal control
51-XX Geometry
52-XX Convex and discrete geometry
53-XX Differential geometry
54-XX General topology
55-XX Algebraic topology
57-XX Manifolds and cell complexes
58-XX Global analysis, analysis on manifolds

60-XX Probability theory
62-XX Statistics
65-XX Numerical analysis
68-XX Computer science
70-XX Mechanics of particles and systems
74-XX Mechanics of deformable solids
76-XX Fluid mechanics
78-XX Optics, electromagnetic theory
80-XX Classical thermodynamics, heat
81-XX Quantum theory
82-XX Statistical mechanics, matter
83-XX Relativity and gravitational theory
85-XX Astronomy and astrophysics
86-XX Geophysics
90-XX Operations research
91-XX Game theory, economics
92-XX Biology and other natural sciences
93-XX Systems theory; control
94-XX Information and communication
97-XX Mathematics education

The Prime Number Theorem

- Is there a biggest prime? NO (300BCE). (**see THEOREMS 4 and 7 in Appendix 1**)
- Whole numbers are to primes what molecules are to atoms (Fundamental Theorem of Arithmetic) Atoms run out before you get to 100; the primes go on forever. (**see THEOREMS 1 and 2 in Appendix 1**).
- Do the primes eventually thin out. Can we find a rule, a law, to describe the thinning-out? There are

  25 primes between 1 and 100
  17 between 401 and 500
  14 between 901 and 1000
  4 between 999,901 and 1,000,000.
  (**see THEOREMS 5 and 8 in Appendix 1**)
- The Prime Counting Function. The number of primes up to a given quantity x is denoted by $\pi(x)$ (x need not be a whole number).

- The Prime Number Theorem states roughly that: $\pi(N)$ behaves very much like $N/\log N$. (This is the ‘natural logarithm’, to base $e = 2.718\cdots$, not to base 10.)
  (**see THEOREM 6 in Appendix 1**)

- PNT was conjectured by Gauss at the end of the 18th century, and proved by two mathematicians (independently and simultaneously) at the end of the 19th century, using tools developed by Riemann in the middle of the 19th century.

- If the Riemann Hypothesis is true, it would lead to an *exact* formulation of PNT, instead of one that is always off by several percent.

On the Shoulders of Giants

- The greatest mathematician who ever lived was the first person to whom the truth contained in the PNT occurred—Carl Friedrich Gauss (1777-1855).

(age 10) $1 + 2 + \cdots + 100 = ?$

(age 15) Beginning in 1792, at the age of 15, Gauss had amused himself by tallying all the primes in blocks of 1,000 numbers at a time, continuing up into the high hundreds of thousands.

- The other first rank mathematical genius born in the 18th century—Leonhard Euler (1707-1783)—solved the "Basel problem" and discovered the "Golden Key."

- There is also the ‘Russian connection’: Peter the great established an Academy in St. Petersburg in 1682 and imported Euler from Switzerland to run it—Russia had just come out of a dark period of its development

Riemann's Zeta Function

The Basel problem opens the door to the zeta* function, which is the mathematical object the Riemann Hypothesis is concerned with.
The Basel problem (posed in 1689) is: What is the *exact* value of

$$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}\cdots?$$

*Not to be confused with the Catherine Zeta-Jones function

The answer (Euler 1735): $\pi^2/6$.

He also showed that

$$1 + \frac{1}{16} + \frac{1}{81} + \frac{1}{256} \cdots = \pi^4/90$$

$$1 + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} \cdots = \pi^6/945$$

and so forth.

In summary, Euler found the exact value of $1+\frac{1}{2^N}+\frac{1}{3^N}+\frac{1}{4^N}\cdots$ for every even $N = 2, 4, 6, \ldots$.

However, to this day, no one knows the exact value of this series for any odd value of N, $N = 3, 5, 7, \ldots$.

Are they irrational? **(see Appendix 2 for some facts about irrational numbers)**

Replace the exponent $N = 2$ in the Basel problem by any (for the moment *real*) number s to get the **zeta function**

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

The series defining the zeta function converges as long as $s > 1$ (s need not necessarily be a whole number) but it diverges for $s = 1$. It appears that the zeta function also diverges for any $s < 1$ (since the terms are bigger than the corresponding terms for $s = 1$) and it behaves like $1/(s-1)$ for $s > 1$.

Thus, the domain of the zeta function is the set of all (real) numbers greater than 1. Right?

WRONG!

WHAT IS EULER'S "GOLDEN KEY"?

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} \cdots$$

$$(1 - \frac{1}{2^s})\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} \cdots$$

$$(1 - \frac{1}{3^s})(1 - \frac{1}{2^s})\zeta(s) =$$

$$= 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{2^s} \cdots + \frac{1}{25^s} + \cdots\cdots$$

This leads to $\prod_p (1 - \frac{1}{p^s})\zeta(s) = 1$ and the golden key: $\sum_n n^{-s} = \prod_p (1 - p^{-s})^{-1}$

The golden key is the initial link between analysis (zeta function)) and arithmetic (primes). Hence it could be viewed as the "engagement" of analysis with arithmetic.

Bernhard Riemann's legacy

In Riemann's doctoral dissertation, the "Riemann integral" occurs, now taught as a fundamental concept in calculus courses.

His habilitation lecture (second doctoral degree) was on the foundations of geometry. The ideas contained in this paper were so advanced that it was decades before they became fully accepted, and 60 years before they found their natural physical application, as the mathematical framework for Einstein's General Theory of Relativity.

Domain Stretching

The Riemann Hypothesis states: **All non-trivial zeros of the zeta function have real part one-half**.

What is a zero of a function? What are the zeros of the zeta function? When are they non-trivial. After we answer these questions we'll move on to "real part one-half."

A "zero" of a function is a number a such that the function has the value zero at a. In other words, if you graph the function, its zeros are the numbers on the x-axis at which the graph of the function crosses the x-axis. A good example is the function $\sin x$, which has zeros at $x = 0, \pi, -\pi, 2\pi, -2\pi, \ldots$

An infinite series might define only part of a function; in mathematical terms, an infinite series may define a function over only part of that function's domain. The rest of the function might be lurking away somewhere, waiting to be discovered by some trick.

EXAMPLE 1: $S(x) = 1 + x + x^2 + x^3 + \cdots$, which converges for $-1 < x < 1$ and equals $1/(1-x)$ for those values of x. Since $1/(1-x)$ makes sense for all numbers except $x = 1$, this shows that the domain of $S(x)$ is larger than $-1 < x < 1$.

EXAMPLE 2: The Gamma function and the factorial symbol. If you define $H(x) = \int_0^\infty e^{-t}t^{x-1}\,dt$, then one has $H(2) = 1$, $H(3) = 2$, $H(4) = 6$, $H(5) = 24, \ldots$, in fact for every positive integer m, $H(m) = (m-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (m-2)(m-1)$.

Back to the zeta function

In addition to arguments greater than 1, the zeta function has values for all arguments less than 1. This extension of the zeta function is done in two steps: first to all arguments between 0 and 1 (by changing signs in the series), and then to all negative arguments (by using a deep formula in Riemann's famous 1859 paper).

The extended zeta function has the value zero at every negative even number. These are the trivial "zeros" of the zeta function.

STEP 1: Define the “eta” function”:

$\eta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} \cdots$

This converges whenever $s > 0$.

It is easy to see that for $s > 1$,

$$\zeta(s) = \frac{\eta(s)}{1 - \frac{1}{2^{s-1}}}$$

Therefore, $\zeta(s)$ extends to the positive real axis.

STEP 2: From Riemann's 1859 paper, for every $s > 0$ (except for $s = 1$)

$$\zeta(1-s) = 2^{1-s}\pi^{-1}\sin(\tfrac{1-s}{2}\pi)(s-1)!\zeta(s)$$

For example $\zeta(-15)$ can be calculated from $\zeta(16)$

This extends $\zeta(s)$ to all values of $s < 0$ and moreover shows that if $m = 1, 2, \ldots$

$$\zeta(-2m) = 0$$

Thus $\zeta(s)$ is defined for all real number except for $s = 0, 1$ and the negative even integers

$$-2, -4, -6, -8, \ldots$$

are what are called the "trivial zeros" of the zeta function.

- If the Riemann Hypothesis were true, it would reveal a deep secret about prime numbers which has no foreseeable practical consequences that could change the world. In particular, PNT would follow as a consequence. However, RH is much stronger than PNT, and the latter was proved using weaker tools.

- There were several significant landmarks between Riemann's paper in 1859 and the proof of PNT (in 1896). The main significance of Riemann's paper for the proof of the PNT is that it provided the deep insights into analytic number theory that showed the way to a proof.

- If the PNT was the great white whale of number theory in the 19th century, RH was to take its place in the 20th, and moreover was to cast its fascination not only on number theorists, but on mathematicians of all kinds, and even on physicists and philosophers.

- There is also the neat coincidence of the PNT being first thought of at the end of one century (Gauss, 1792), then being proved at the end of the next (Hadamard and de la Vallée Poussin, 1896).

- The attention of mathematicians turned to RH, which occupied them for the following century—which came to its end without any proof being arrived at.

- By the later 19th century the world of mathematics had passed out of the era when really great strides could be made by a single mind working alone. Mathematics had become a collegial enterprise in which the work of even the most brilliant scholars was built upon, and nourished by, that of living colleagues.
- One recognition of this fact was the establishment of periodic International Congresses of Mathematicians, with PNT among the highlights of the first meeting in 1897 in Zürich. There was a second Congress in Paris in 1900.

- The Paris Congress will forever be linked with the name of David Hilbert, a German mathematician working at Göttingen, the university of Gauss, Dirichlet, and Riemann, for his address on the mathematical challenges of the new century, RH being the most prominent among them.
- Each problem came from some key field of mathematics at the time. If they were to be solved, their solution would advance that field in new and promising directions.

Nine Zulu Queens Ruled China

- We know what the trivial zeros of the zeta function are. What are the non-trivial zeros? For this we need to know about complex numbers.

- Mathematicians think of numbers as a set of nested Russian dolls. The inhabitants of each Russian doll are honorary inhabitants of the next one out.

- In $\mathbf{N}$ you can't subtract; in $\mathbf{Z}$ you can't divide; in $\mathbf{Q}$ you can't take limits; in $\mathbf{R}$ you can't take the square root of a negative number. With the complex numbers $\mathbf{C}$, nothing is impossible. You can even raise a number to a complex power.

- Therefore, in the zeta function, the variable s may now be a complex number, and the Riemann hypothesis now makes sense: it asserts that the non-trivial zeros of the zeta function all lie on the vertical line whose horizontal coordinate is equal to 1/2.
- We shall need a complex plane extension process to determine the precise domain of this complex valued zeta function.

Hilbert's Eighth Problem

- Since 1896 it was known, with mathematical certainty, that, yes indeed, $\pi(N)$ could be approximated arbitrary closely by $N/\log N$. Everyone's attention now focused on the nature of the approximation—What is the error term?

- Riemann did not prove the PNT, but he strongly suggested it was true, and even suggested an expression for the error term. That expression involved all the non-trivial zeros of the zeta function.

- One of the questions left in this talk is: what exactly is the relation between the zeros of the zeta function and the prime number theorem. This is answered in Derbyshire's book.

SUMMARY OF WHAT WE LEARNED

There is a mathematical expression that predicts roughly how many prime numbers there are smaller that any number you care to name. You know also that this prediction, by Gauss, is not entirely accurate, and that the amount by which it is wrong is the subject of another mathematical expression, devised by the German mathematician Bernhard Riemann. With Gauss's estimate, proved independently by two other mathematicians in 1896, and Riemann's correction, conjectured but not yet proved by anyone, we know much more about how the prime numbers are distributed. At the heart of Riemann's correction factor, and essential to understanding how it is related to prime numbers, is Riemann's zeta function, and in particular, a series of numbers which are known as the Riemann zeros.

APPENDIX 1—PRIME NUMBERS

THEOREM 1—FUNDAMENTAL THEOREM OF ARITHMETIC (PART I—EXISTENCE)

Every positive integer (other than 1) is either a prime or a product of primes.

PROOF:

Let Let $n \geq 2$ be an any integer. If n is a prime, there is nothing to prove. If n is not a prime it has a divisor different from itself and from 1. If m is the smallest such divisor, then m must be a prime. Let's call it p_1 and write $n = p_1 n_1$ for some integer n_1 with $n_1 < n$. Repeat this argument starting with n_1. Either n_1 is a prime, in which case we are done, or it has a prime factor p_2 and there is an integer $n_2 < n_1$ with $n_1 = p_2 n_2$. We now have $n = p_1 p_2 n_2$. Continuing this process we obtain a sequence of primes $p_1, \ldots, p_k$, and a sequence of integers $n_k < n_{k-1} < \cdots < n_1 < n$, with $n = p_1 p_2 \cdots p_k n_k$. Since $1 < n_k < n_{k-1} < \cdots < n_1 < n$, at some point, n_k must be a prime. This completes the proof.

THEOREM 2—FUNDAMENTAL THEOREM OF ARITHMETIC (PART II-UNIQUENESS)

Every positive integer is a product of primes in only one way.

PROOF:

If there were numbers with two distinct prime factorizations, let n be the smallest such number. If P is any prime number, then P cannot appear in both factorizations of n—if it did, then n/P, which is smaller than n would have two distinct factorizations. So we have $n = p_1 p_2 \cdots p_k = q_1, q_2 \cdots q_m$ where no prime p_j is the same as any of the primes q_i. We may assume that p_1 is the smallest p_j and q_1 is the smallest q_i. Since n is composite, $p_1^2 \leq n$ and $q_1^2 \leq n$. Since $p_1 \neq q_1$, we must have $p_1 q_1 < n$. Set $N = n - p_1 q_1$. Now note that N has a unique factorization since it is smaller than n, and N is divisible by p_1 and q_1. Since N has a unique factorization, it is also divisible by $p_1 q_1$. But we also can write $n = N + p_1q_1$ so that n is also divisible by p_1q_1. This is the same as saying that q_1 divides n/p_1. But $n/p_1 = p_2 \cdots p_k$ is less than n and so it has a unique prime factorization and it follows that q_1 must be one of $p_2, \ldots, p_k$. This is a contradiction, completing the proof.

THEOREM 3

If a prime divides a product of two numbers, then it must divide one of the numbers (PROOF NOT GIVEN)

THEOREM 4

There is no largest prime number.

PROOF:

Let p be any prime and consider the number Q which is one more than the product of all primes up to p: $Q = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p + 1$. Then Q is not divisible by any of the primes up to p, so it is either a prime itself, or it is divisible by a prime, larger than p, In either case, there is a prime larger than the given p. The theorem is proved.

THEOREM 5

There are blocks of arbitrary length of composite numbers.

PROOF:

As in the proof of THEOREM 4, let p be any prime and note that ALL numbers $2, 3, 4, \ldots, p-1, p$ are divisible by at least one prime up to p. Now define Q to be the product of all primes up to p: $Q = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p$ (we don't add one this time). Then the following $p-1$ numbers are all composite, proving the theorem: $Q+2, Q+3, Q+4, \ldots, Q+p$.

THEOREM 6 (PNT)

$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$ (NO PROOF GIVEN)

THEOREM 7

$\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges (NO PROOF GIVEN)

THEOREM 8

There is a prime number between n and $2n$ for every $n = 1, 2, \ldots$ (NO PROOF GIVEN)

APPENDIX 2—IRRATIONAL NUMBERS

THEOREM 9

$\sqrt{2}$ is irrational

PROOF:

Suppose that $\sqrt{2} = a/b$ where a/b is a fraction in lowest terms. Since $2b^2 = a^2$, it follows that a^2 is even, and hence a is even, say $a = 2c$. Then 2b$^2 = (2c)^2 = 4c^2$ so that $b^2 = 2c^2$ is even, and so is b. This contradicts the fact that a/b was in lowest terms, and proves the theorem.

THEOREM 10

$\sqrt{N}$ is irrational unless N is a perfect square (NO PROOF GIVEN)

THEOREM 11

$N^{1/m}$ is irrational unless $N = a^m$ for some integer a (NO PROOF GIVEN)

THEOREM 12

If $x^m + c_1 x^{m-1} + \cdots + c_m = 0$ and $c_1, c_2, \ldots, c_m$ are integers then x is irrational, unless it is an integer. (NO PROOF GIVEN)

THEOREM 13

$\log_{10} 2$ is irrational

PROOF:

Let us suppose that $\log_{10} 2 = a/b$. This is the same as $10^{a/b} = 2$, equivalently, $10^a = 2^b$, or $2^a 5^a = 2^b$. By the uniqueness in the fundamental theorem of arithmetic (Theorem 2), we must have, in particular, $a = 0$, which is a contradiction since $\log_{10} 2 \neq 0$, This proves the theorem.

THEOREM 14

$\log_n m$ is irrational if one of m and n has a prime factor which the other lacks.

(NO PROOF GIVEN)

THEOREM 15

e is irrational

PROOF:

Suppose that e were rational, say $e = a/b$. Let k be any integer $\geq b$. Define the number t to be

$$t = k!\left(e - 1 - \frac{1}{1!} - \frac{1}{2!} - \cdots - \frac{1}{k!}\right)$$

Thus

$$t = k!\left(\frac{a}{b} - 1 - \frac{1}{1!} - \frac{1}{2!} - \cdots - \frac{1}{k!}\right)$$

and so it is clear that t is a positive integer. But if you use the series for the number e, you find that $t < 1$, which is a contradiction. We have

$$\begin{aligned} t &= k!\left(\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \cdots\right) \\ &= \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \cdots \\ &< \frac{1}{k+1} + \frac{1}{(k+1)^2} + \cdots \\ &= \frac{1}{k+1}\left(1 + \frac{1}{k+1} + \frac{1}{(k+1)^2} + \cdots\right) \\ &= \frac{1}{k+1}\left(\frac{1}{1 - \frac{1}{k+1}}\right) = \frac{1}{k} < 1, \end{aligned}$$

as was stated. Thus e is irrational.