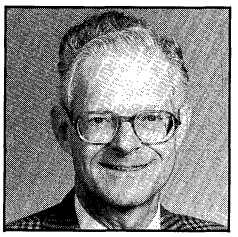
# Prime Number Records

*Paulo Ribenboim*



**Paulo Ribenboim** received his B.S. from the University of Brazil and his Ph.D. from the University of Sao Paulo. Professor Emeritus of Mathematics at Queen's University, Ontario, he is widely known as a lively lecturer on algebra and number theory and has held academic positions in 11 countries. Recent appointments include the University of Paris, the Mathematics Institute at the University of Munich, and the Mathematical Sciences Research Institute at Berkeley. He enjoys travel, classical music, the arts, and fine food.

The theory of prime numbers can be roughly divided into four main inquiries: How many prime numbers are there? How can one produce them? How can one recognize them? How are the primes distributed among the natural numbers? In answering these questions, calculations arise that can be carried out only for numbers up to a certain size. This article records the biggest sizes reached so far—the prime number records.

All the world loves records. They fascinate us and set our imaginations soaring. The famous *Guinness Books of Records*, which has appeared in surprisingly many editions, contains many noteworthy and interesting occurrences and facts. Did you know, for example, that the longest uninterrupted bicycle trip was made by Carlos Vieira of Leiria, Portugal? During the period June 8–16, 1983, he pedalled for 191 hours nonstop, covering a distance of 2407 km. Or did you know that the largest stone ever removed from a human being weighed 6.29 kg? The patient was an 80-year-old woman in London, in 1952. And nearer our usual lines of interest: Hideaki Tomoyoki, born in Yokohama in 1932, quoted 40,000 digits of $\pi$ from memory, a heroic exploit that required 17 hours and 20 minutes, with pauses totalling 4 hours. Leafing through the *Guinness Book*, one finds very few scientific records, however, and even fewer records about numbers.

Not long ago I wrote *The Book of Prime Number Records* [**3**], in which I discuss the feats of mathematicians in this domain so neglected by Guinness. How this book originated is a story worth telling. Approached by my university to give a colloquium lecture for undergraduate students, I sought a topic that would be not only understandable but interesting. I came up with the idea of speaking about *prime number records*, since the theme of records is already popular with students in connection with sports. The interest of the students so exceeded my expectations that I resolved to write a monograph based on this lecture. In the process I learned of so many new facts and records that the brief text I had planned kept on expanding. Thanks to colleagues who supplied me with many helpful references, I was at last able to complete this work.

I must confess that when preparing the lecture I did not know a lot (indeed I knew very little!) about the theorems for primes and prime number records. For me all these facts, although quite interesting, were not tied together. They seemed to be just isolated theorems about prime numbers, and it was not clear how they

could be woven into a connected theory. But when one wishes to write a book, the first task is to shape the subject matter into a coherent whole.

The scientific method may be considered as a two-step process: first, observation and experiment—*analysis*; then formulation of the rules, theorems, and orderly relationships of the facts—*synthesis*. Stated in these terms, my task was thus to present a synthesis of the known observations about prime numbers, with an emphasis on the records achieved. Any originality of my work undoubtedly lies in the systematic investigation of the interplay between theory and calculation. This undertaking needs no justification if one keeps in mind what role the prime numbers have in the theory of numbers. After all, the fundamental theorem of elementary number theory says that every natural number $N > 1$ can be expressed in a unique way (except for the order of the factors) as a product of primes. Prime numbers are thus the foundation stones on which the structure of arithmetic is raised.

Now, how did I go about organizing the theory of prime numbers? I began by posing four direct, unambiguous questions:

1. How many prime numbers are there?
2. How can one generate primes?
3. How can one know if a given number is prime?
4. Where are the primes located?

As we shall see, out of these four questions the theory of prime numbers naturally unfolds.

## How Many Primes Are There?

As is well known, Euclid in his *Elements* proved that there are infinitely many primes, proceeding as follows: Assume that there are only finitely many primes. Let $p$ be the largest prime number and $P$ be the product of all primes less than or equal to $p$; then consider the number $P$ plus 1:

$$P + 1 = \left( \prod_{q \leq p} q \right) + 1.$$

Two cases are possible: either (a) $P + 1$ is prime, or (b) $P + 1$ is not prime. But if (a) is true, $P + 1$ would be a prime number larger than $p$. And if (b) holds, none of the primes $q \leq p$ is a prime factor of $P + 1$, so the prime factors of $P + 1$ are all larger than $p$. In both cases the assumption that there is a largest prime $p$ leads to a contradiction. This shows that there must be an infinite number of primes.

From this indirect proof one cannot deduce a method for generating prime numbers, but it prompts a question: Are there infinitely many primes $p$ such that the corresponding number $P + 1$ is also prime? Many mathematicians have devoted calculations to this question.

**Record.** $p = 13649$ *is the largest known prime for which* $P + 1$ *is also prime*; *here*, $P + 1$ *has* 5862 *decimal digits. This was found by H. Dubner in* 1987.

There are many other proofs of the existence of infinitely many primes; each reveals another interesting aspect of the set of all prime numbers. Euler showed

that the sum of the reciprocals of the prime numbers is divergent:

$$\sum \frac{1}{p} = \infty.$$

From this we again see that there cannot be only finitely many primes. Euler's proof can be found in many elementary books on number theory or real analysis, such as [**1**], and permits an interesting deduction. For any $\varepsilon > 0$, no matter how small, we know

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}} < \infty.$$

Hence the prime numbers are closer together, or are less sparsely scattered along the number line, than are numbers of the form $n^{1+\varepsilon}$. For example, the primes lie closer together than the squares $n^2$, for which Euler showed

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Another simple and elegant proof that infinitely many primes exist was given by Pólya. It clearly suffices to find an infinite sequence $F_0, F_1, F_2, F_3, \ldots$ of pairwise relatively prime natural numbers (i.e., no two having a common divisor greater than 1); since each $F_n$ has at least one prime factor, then there are infinitely many primes. It is easy to prove that the sequence of Fermat numbers $F_n = 2^{2^n} + 1$ has this property. Clearly neither $F_n$ nor $F_{n+k}$ $(k > 0)$ is divisible by 2; and if $p$ is an odd prime factor of $F_n$, then $2^{2^n} \equiv -1 \pmod{p}$, so that $2^{2^{n+k}} = (2^{2^n})^{2^k} \equiv 1 \pmod{p}$. Thus $F_{n+k} \equiv 2 \pmod{p}$, and since $p > 2$, it follows that $p$ does not divide $F_{n+k}$. I will devote further attention to the Fermat numbers after the next section.

### Generating Prime Numbers

The problem is to find a "good" function $f$: $\mathbf{N} \to \{\textit{prime numbers}\}$. This function should be as easy to calculate as possible and, above all, should be representable by previously well-known functions. One may place additional conditions on this function, for example:

*Condition (a).* $f(n)$ equals the $n$th prime number (in the natural order); this amounts to a "formula" for the $n$th prime number.

*Condition (b).* For $m \neq n$, $f(m) \neq f(n)$; this amounts to a function that generates distinct primes, but not necessarily all the primes.

One can also seek a function $f$ defined on $\mathbf{N}$ with integer values (but not necessarily positive values) that fulfills

*Condition (c).* The set of prime numbers coincides with the set of positive values of the function. This is a far looser requirement and one that can be fulfilled in unexpected ways, as we shall later see.

To begin, let's discuss formulas for prime numbers. There are plenty of them! In fact many of us in younger days sought—often with success—a formula for the $n$th prime number. Unfortunately, all these formulas have one thing in common: They express the $n$th prime number through functions of the preceding primes that are difficult to compute. Consequently these formulas are useless for deriving properties of the prime numbers. Nevertheless, I will give as an illustration one such formula, found in 1971. I do so in honor of its discoverer, J. M. Gandhi, a mathematician who died far too young, who also worked on Fermat's Last Theorem.[1]

To simplify the statement of the formula, I will introduce the Möbius function $\mu$: $\mathbf{N} \to \mathbf{Z}$, given by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n \text{ is square-free and a product of } r \text{ distinct prime factors} \\ 0 & \text{otherwise.} \end{cases}$$

Now if $p_1, p_2, p_3, \ldots$ is the sequence of prime numbers in increasing order, set $P_{n-1} = p_1 p_2 \ldots p_{n-1}$; then Gandhi's formula is

$$p_n = \left[ 1 - \log_2 \left( -\frac{1}{2} + \sum_{d \mid P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right].$$

Here $\log_2$ indicates the logarithm in base 2 and $[x]$ denotes, as usual, the largest integer less than or equal to the real number $x$. One can see how difficult it is to calculate $p_n$ using Gandhi's formula!

Now we sketch the construction of a function that generates prime numbers. E. M. Wright and G. H. Hardy in their famous book [**1**] showed that if $\omega = 1.9287800\ldots$ and if

$$f(n) = \left[ 2^{2^{\cdot^{\cdot^{2^{\omega}}}}} \right] \qquad \text{(with } n \text{ twos)}$$

then $f(n)$ is prime for all $n \geq 1$. Thus $f(1) = 3$, $f(2) = 13$, and $f(3) = 16381$, but $f(4)$ is rather hard to calculate and has almost 5000 decimal places. However, as the exact value of $\omega$ depends on knowledge of the prime numbers, this formula is ultimately uninteresting.

Do any truly simple functions generate prime numbers? There are no such polynomial functions because of the following negative result:

**Result.** For every $f \in \mathbf{Z}[X_1, \ldots, X_m]$ there are infinitely many $m$-tuples of integers $(n_1, \ldots, n_m)$ for which $|f(n_1, \ldots, n_m)|$ is a composite number.

Other similar negative results are plentiful.

Well, then, are there polynomials in just *one* indeterminate for which many consecutive values are primes? More precisely: Let $q$ be a prime number. Find a polynomial of degree 1, in fact a polynomial of the form $f_q(X) = dX + q$, whose values at the numbers $0, 1, \ldots, q-1$ are all prime. Then $f_q$ generates a sequence of $q$ prime numbers in arithmetic progression with difference $d$ and initial value $q$.

---

[1] J. M. Gandhi, born in 1933, died on January 23, 1982, after an apparently harmless operation.

For small values of $q$ finding $f_q$ is easy:

| $q$ | $d$ | Values at $0, 1, \ldots, q-1$ | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 1 | 2 | 3 | | | | |
| 3 | 2 | 3 | 5 | 7 | | | |
| 5 | 6 | 5 | 11 | 17 | 23 | 29 | |
| 7 | 150 | 7 | 157 | 307 | ... | ... | 907 |

However, we do not know how to prove that this is possible for every prime number $q$.

**Records.** *In* 1986, *G. Löh gave the smallest values of d for two primes*:

$$\text{For } q = 11, \quad d = 1\,536\,160\,080.$$

$$\text{For } q = 13, \quad d = 9\,918\,821\,194\,590.$$

One can also examine the related problem: to search for the longest sequences of primes in arithmetic progression.

**Record.** *The longest known sequence of primes in arithmetic progression consists of* 22 *terms in the sequence with first term* $a = 11\,410\,337\,850\,553$ *and difference* $d = 4\,609\,098\,694\,200$ (*work coordinated by P. Pritchard*, 1993).

Euler discovered quadratic polynomials for which many values are primes. He observed that if $q$ is the prime 2, 3, 5, 11, 17, or 41, then the values $f_q(0), f_q(1), \ldots, f_q(q-2)$ of the polynomial $f_q(X) = X^2 + X + q$ are prime. (Evidently $f_q(q-1) = q^2$ is not prime, so this sequence of consecutive prime values is the best one can hope for.) For $q = 41$ this gives 40 prime numbers: $41, 43, 47, 53, \ldots, 1447, 1523, 1601$.

The next question is obvious: Can one find primes $q > 41$ for which the first $q-1$ values of Euler's quadratic are all prime? If infinitely many such primes $q$ exist, we could generate arbitrarily long sequences of primes! However, the following theorems say this is not to be:

**Theorem.** *Let q be a prime number. The integers* $f_q(0), f_q(1), \ldots, f_q(q-2)$ *are all primes if and only if the imaginary quadratic field* $\mathbf{Q}(\sqrt{1-4q})$ *has class number* 1 (*G. Rabinovitch*, 1912).

(A quadratic field $K$ has class number 1 if every algebraic integer in $K$ can be expressed as a product of primes in $K$, and if any two such representations differ only by a unit, i.e., an algebraic integer that is a divisor in 1 in $K$.)

**Theorem.** *Let q be a prime number. An imaginary quadratic field* $\mathbf{Q}(\sqrt{1-4q})$ *has class number* 1 *if and only if* $4q - 1 = 7$, 11, 19, 43, 67, *or* 163, *that is*, $q = 2$, 3, 5, 11, 17, *or* 41.

The imaginary quadratic fields of class number 1 were determined in 1966 by A. Baker and H. M. Stark, independently and free of the doubt that clung to Heegner's earlier work in 1952.

Thus the following unbeatable record has been attained:

**Record.** *$q = 41$ is the largest prime number for which the values $f_q(0), f_q(1), \ldots, f_q(q-2)$ of the polynomial $f_q(X) = X^2 + X + q$ are all primes.*

It is worth mentioning that in the solution of this quite harmless-looking problem a rather sophisticated theory was required. Details are given in another article [**2**].

We now turn to some polynomials whose positive values coincide with the set of prime numbers. The astonishing fact that such polynomials exist was discovered in 1971 by Yu. V. Matijasevič in connection with the tenth Hilbert problem. Here are the records, which depend on the number of unknowns $n$ and the degree $d$ of the polynomial:

**Records.**

| $n$ | $d$ | *Year* | |
|---|---|---|---|
| 21 | 21 | 1971 | *Yu. V. Matijasevič (not explicit)* |
| 26 | 25 | 1976 | *J. P. Jones, D. Sato, H. Wada, and D. Wiens* |
| 42 | 5 | 1976 | *Jones et al. (not explicit): Lowest d* |
| 10 | $\sim 1.6 \times 10^{48}$ | 1978 | *Yu. V. Matijasevič (not explicit): Lowest n* |

It is not known whether the minimum values for $n$ and $d$ are 10 and 5, respectively.

## Recognizing Prime Numbers

Given a natural number $N$, is it possible to determine with a finite number of calculations whether $N$ is a prime? Yes! It suffices to divide $N$ by every prime number $d$ for which $d^2 < N$. If the remainder is nonzero every time, then $N$ is prime. The trouble with this method is that a large $N$ requires a large number of calculations. The problem, therefore, is to find an algorithm $A$ where the number of computations is bounded by a function $f_A$ of the number of digits of $N$, so $f_A(N)$ does not grow too fast with $N$. For example, $f_A(N)$ should be a polynomial function of the number of binary digits of $N$, which is $1 + [\log_2(N)]$. Essentially, this number is proportional to the natural logarithm $\log N$, since $\log_2(N) = \log N / \log 2$.

This problem remains open—we do not know whether such a polynomial algorithm exists. On the one hand, we cannot prove the impossibility of its existence; on the other hand, no such algorithm has yet been found. Efforts in this direction have produced several primality-testing algorithms. According to the point of view, they may be classified as follows:

Algorithms for arbitrary numbers
Algorithms for numbers of special form

Algorithms that are fully justified by theorems
Algorithms that are based on conjectures

Deterministic algorithms
Probabilistic algorithms

To clarify these notions I offer some examples.

One algorithm applicable to arbitrary numbers is that of G. L. Miller (1976), the complexity of which can be estimated only with the help of the generalized Riemann conjecture. Assuming this conjecture, for Miller's algorithm the estimate $f_A(N) \leq C(\log N)^5$ is valid, where $C$ is a positive constant. Thus this is an algorithm whose polynomial growth rate remains uncertain. By contrast, the algorithm of L. M. Adleman, C. Pomerance, and R. S. Rumely (1983) possesses a completely assured complexity estimate, and the number of computation operations as a function of the number of binary digits of $N$ is bounded by $(\log N)^{C \log\log\log N}$ where $C$ is a constant. The complexity is therefore in practice not far from polynomial, and this algorithm can be applied to an arbitrary integer $N$.

Both of these algorithms are deterministic, unlike those I shall now describe. First, I must introduce the so-called pseudoprime numbers. Let $a > 1$ be an integer. For every prime $p$ that does not divide $a$, Fermat's Little Theorem says $a^{p-1} \equiv 1 \pmod{p}$. But it is quite possible for a number $N > 1$ with $a^{N-1} \equiv 1 \pmod{N}$ to be composite—in which case we say $N$ is *pseudoprime for the base a*. For example, 341 is the smallest pseudoprime for the base 2. Every base $a$ has infinitely many pseudoprimes. Some among them satisfy an additional congruence condition and are called *strong pseudoprimes for the base a*; they too are infinite in number.

An algorithm is called a *probabilistic prime number test* if its application to a number $N$ leads either to the conclusion that $N$ is composite or to the conclusion that with high probability $N$ is a prime number. Tests of this type include those of R. Baillie and S. S. Wagstaff (1980) and M. O. Rabin (1980). In these tests one examines certain "witnesses." Let $k > 1$ (for example, $k = 30$) and let $a_1 = 2$, $a_2 = 3, \ldots, a_k$ be primes that will serve as witnesses. Should a witness fail to satisfy the condition $a_j^{N-1} \equiv 1 \pmod{N}$, then $N$ is surely composite. If for every witness $a_j$ the preceding congruence holds (that is, if $N$ is pseudoprime for the base $a_j$ for $j = 1, 2, \ldots, k$) then $N$ is with high probability a prime number. Rabin's test is similar, using more restrictive congruences, which lead to better probabilities. This test leads to the conclusion that $N$ either is certainly composite or with probability $1 - (1/4^k)$ is prime. For $k = 30$, then, the test gives a false result only once out of every $10^{18}$ values of $N$. These probabilistic tests are clearly very easy to apply.

Now we turn to prime number tests applicable to numbers of the form $N \pm 1$, where many if not all of the prime factors of $N$ are known. The tests for $N + 1$ depend on a weak converse, due to Pepin, of Fermat's Little Theorem, while those for $N - 1$ use the Lucas sequence.

In 1877 Pepin showed that the Fermat numbers $F_n = 2^{2^n} + 1$ are prime if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. The search for primes among the Fermat numbers $F_n$ has produced several records.

**Record.** *The largest Fermat number known to be prime is* $F_4 = 65537$.

**Record.** $F_{11}$ *is the largest Fermat number all of whose prime factors have been determined* (*R. P. Brent and F. Morain*, 1988).

**Record.** $F_{23471}$ *is the largest Fermat number known to be composite; it has the factor* $5 \times 2^{23473} + 1$ (*W. Keller*, 1984).

**Record.** $F_{22}$ *is the smallest Fermat number not yet proven prime or composite.*

For the Mersenne numbers, $M_q = 2^q - 1$, with $q$ a prime, one applies the Lucas test (1878): Let $S_0 = 4$, $S_{k+1} = S_k^2 - 2$, for $k \geq 0$. Then $M_q$ is prime if and only if $M_q$ is a divisor of $S_{q-2}$. This test makes it possible to discover very large primes.

**Record.** *To date*, 33 *Mersenne primes are known. The largest Mersenne prime now known is* $M_q$ *for* $q = 859433$, *a number whose decimal expression has* 258,716 *digits. It was found with a Cray computer by D. Slowinski, in* 1993.

The next smaller Mersenne primes are $M_q$ for $q = 756839$, $q = 216091$, and $q = 132049$ (all by Slowinski). Such large numbers could not be tested for primality were it not for their special form.

**Record.** *The largest known composite Mersenne number is* $M_q$ *for* $q = 39051 \times 2^{6001} - 1$ (*W. Keller*, 1987).

For many years—from 1876, when E. Lucas proved $M_{127}$ prime, until 1989—the title "largest prime number" was always held by a Mersenne prime. That became true again in 1992, but in the three intervening years another champion reigned:

**Record.** *The largest prime known today that is not a Mersenne prime is* $391581 \times 2^{216193} - 1$. *For this discovery we are indebted to six mathematicians; in reverse alphabetical order* (*and why not*?) *they are S. Zarantonello, J. Smith, G. Smith, B. Parady, L. C. Noll, and J. Brown.*

## The Distribution of the Prime Numbers

At this point we know the following:

1. There are infinitely many prime numbers.
2. There is no reasonably simple formula for the prime numbers.
3. One can determine whether a given number is prime if it is not too large.

What can one say about the way the primes are distributed among the natural numbers? Earlier I gave a hint in connection with Euler's proof of the existence of infinitely many primes: The primes are closer together than are, for example, the squares. A quite simple way to discuss the distribution of the primes is to count the number of primes less than a given number. For every real $x > 0$, set $\pi(x) = |\{\text{prime numbers } p | p \leq x\}|$. Thus $\pi$ is the function that counts the prime numbers. To have a good idea of the behavior of $\pi$ we can compare it with simpler functions. This approach leads to results of an asymptotic nature.

When only 15 years old, C. F. Gauss conjectured from his studies of prime number tables that

$$\pi(x) \sim \frac{x}{\log x}.$$

That is, the limit of the quotient

$$\frac{\pi(x)}{x/\log x}$$

as $x \to \infty$ exists and equals 1. An equivalent formulation is

$$\pi(x) \sim \int_1^x \frac{dt}{\log t}.$$

The function on the right is called the logarithmic integral and is denoted *Li*. Gauss's assertion was proved in 1896 by J. Hadamard and C. de la Vallée Poussin; previously P. L. Chebyshev had shown that the limiting value, if it exists, must be 1.

This theorem belongs among the most significant results in the theory of prime numbers, for which reason it is customarily referred to as the *Prime Number Theorem*. However, this theorem obviously says nothing about the exact value of $\pi(x)$. For that purpose we have the famous formula that D. F. E. Meissel found in 1871, expressing the exact value of $\pi(x)$ in terms of $\pi(y)$ for all $y \le x^{2/3}$ and prime numbers $p \le x^{1/2}$.

**Record.** *The largest integer N for which* $\pi(N)$ *has been exactly calculated is* $N = 10^{17}$ *(by M. Deleglise, 1992). The value is* $\pi(10^{17}) = 2\,625\,557\,157\,654\,233$.

The differences

$$\left|\pi(x) - \frac{x}{\log x}\right| \quad \text{and} \quad |\pi(x) - Li(x)|$$

do not remain bounded as $x \to \infty$. Evaluating these error terms as exactly as possible is enormously important in applications of the Prime Number Theorem. On the basis of tables it was first conjectured, and then proved (J. B. Rosser and L. Schoenfeld, 1962), that for all $x \ge 17$, $x/\log x \le \pi(x)$. This is interesting because, by contrast, the difference $Li(x) - \pi(x)$ changes sign infinitely many times, as J. E. Littlewood (1914) showed. In 1933, S. Skewes showed that the difference $Li(x) - \pi(x)$ is negative for some $x_0$ with $x_0 \le e^{e^{e^{7.7}}}$. As a matter of fact, this change in sign occurs much earlier:

**Record.** *The smallest* $x_0$ *for which* $Li(x) - \pi(x)$ *is negative must be less than* $6.69 \times 10^{370}$ *(H. J. J. te Riele, 1986).*

The most important function for studying the distribution of primes is the Riemann *zeta function*: For every complex number $s$ with $\mathrm{Re}(s) > 1$, the series $\sum_{n=1}^{\infty} 1/n^s$ is absolutely convergent; it is also uniformly convergent in every half-plane $\{s | \mathrm{Re}(s) > 1 + \varepsilon\}$ for any $\varepsilon > 0$. The function $\zeta$ thus defined can be extended by analytic continuation to a meromorphic function defined in the entire complex plane, with only one pole. The pole is at the point $s = 1$, has order 1, and the residue there is 1. It was the study of the properties of this function that ultimately made the proof of the Prime Number Theorem possible. The function $\zeta$ has zeros at $-2, -4, -6, \ldots$, as one can easily show with the help of the functional equation satisfied by $\zeta$. All other zeros of $\zeta$ are complex numbers $\sigma + it$ ($t$ real) with $0 < \sigma < 1$.

The so far unproved *Riemann hypothesis* says: The nontrivial zeros of the Riemann zeta function are located on the *critical line* $\frac{1}{2} + it$ ($t$ real). Without going into the details, I will just observe that many theorems about the distribution of primes can be proved with the assumption of the Riemann hypothesis. It is therefore of fundamental importance to determine the nontrivial zeros of $\zeta$. By

symmetry considerations, it suffices to determine the zeros with $t > 0$, which can be listed in a sequence $\sigma_n + it_n$, where $t_n \le t_{n+1}$ and in case $t_n = t_{n+1}$ we require that $\sigma_n < \sigma_{n+1}$. (It must first be shown that there are at most a finite number of zeros of $\zeta$ for each value of $t$.)

**Record.** *For* $n \le 1\,500\,000\,001$ *all the zeros* $\sigma_n + it_n$ *of the Riemann zeta function are located on the critical line; that is,* $\sigma_n = \frac{1}{2}$. *These calculations were carried out in* 1986 *by J. van de Lune, H. J. J. te Riele, and D. T. Winter.*

**Record.** *In* 1974, *N. Levinson showed that at least one third of the zeros of the Riemann zeta function are on the critical line, and in* 1989 *J. B. Conrey improved this result, replacing* 1/3 *by* 2/5.

The foregoing considerations are based on the asymptotic behavior of the function $\pi$ and on the function $\zeta$, which is very useful for estimating the error terms. One can say that they deal with the estimation of $\pi$ "at infinity." Next we turn to the *local* behavior if $\pi$—estimating the gaps between the prime numbers. Here the fundamental question is: Knowing the $n$th prime $p_n$, where will one find the following prime $p_{n+1}$? Thus, one is concerned with the sequence of differences $d_n = p_{n+1} - p_n$. It is easy to see that $\limsup d_n = \infty$, that is, arbitrarily long blocks of consecutive composite numbers exist. Here is one: For any $N$, the $N$ consecutive numbers

$$(N+1)!+2, (N+1)!+3, \ldots, (N+1)!+(N+1)$$

are composite. It has amused some mathematicians to find the largest blocks of consecutive composite numbers between fairly small primes—the widest gaps between such primes.

**Record.** *The largest gap between prime numbers that has been effectively calculated consists of the* 863 *composite numbers following the prime* $P = 6\,505\,941\,701\,960\,039$ (*unpublished; communicated to the author in* 1993, *by S. Weintraub*).

The question about wide gaps between not too large primes can be made more precise. Let us look at the sequence $d_n/p_n$ of relative gaps. As early as 1845 J. Bertrand postulated from a study of tables that a prime always lies between $p_n$ and $2p_n$, for every $n \ge 1$. It was Chebyshev who first proved this result, which can be written in the form $p_{n+1} < 2p_n$ or, better, $d_n/p_n < 1$. This result, while amusing, is much weaker than what can be deduced by using the Prime Number Theorem:

$$\lim_{n\to\infty} \frac{d_n}{p_n} = 0$$

The theory of gaps between prime numbers has led to the following conjecture: For every $\varepsilon > 0$ the inequality $p_{n+1} < p_n + p_n^{1/2+\varepsilon}$ holds for all sufficiently large $n$.

**Record.** *The latest entry in a long line, the current record was the work of C. J. Mozzochi in* 1986: $p_{n+1} < p_n + p_n^{1/2+11/20-1/384}$.

What about the limit inferior of the difference sequence $d_n$? Two prime numbers $p$ and $p'$ ($p < p'$) are said to be *twin primes* if $p' - p = 2$. We still do not know if there are infinitely many twin primes, i.e., if $\liminf d_n = 2$. The question is

delicate. In 1919 V. Brun showed that the sum over all pairs of twin primes

$$\sum \left( \frac{1}{p} + \frac{1}{p+2} \right) = B < \infty.$$

It follows that if there are infinitely many twin primes, which one expects to be the case, then they are thinly dispersed. In 1976, Brun's constant was calculated by R. P. Brent: $B = 1.90216054$.

**Record.** *The largest known pair of twin primes is* $1\,706\,595 \times 2^{11235} \pm 1$. *The pair was discovered in* 1990 *by B. K. Parady, J. F. Smith, and S. Zarantonello of the "six from Amdahl," the same group currently holding the record for the largest non-Mersenne prime.*

## Conclusion

Lest this presentation grow too long, I have had to pass over many fascinating questions, such as the behavior of primes in arithmetic progression, to say nothing of the Goldbach conjecture. Fortunately these and many other facts have been both recorded and amply explained in a book [**4**] that is just waiting to be read! I will close with two curiosities to work into your repertoire.

A *repunit* is an integer of the form $R_n = 111\ldots1$, with $n$ decimal digits equal to 1. We do not know if there are infinitely many prime repunits, but we do have the following record.

**Record.** *H. C. Williams and H. Dubner showed in* 1986 *that* $R_{1031}$ *is a prime number.*

Only four other repunits that are primes are known: $R_2$, $R_{19}$, $R_{23}$, and $R_{317}$.

I offer one final noteworthy record—but if you want to know why and how it was found, you must ask H. Dubner, who announced it in 1988.

**Record.** *The largest known prime number whose digits are also all prime is*

$$7532 \times \frac{10^{1104} - 1}{10^4 - 1} + 1.$$

The observation and study of the prime numbers is a fruitful as well as diverting activity. Mathematicians derive much enjoyment from it, and that alone is worth the labor. In time, one comes to consider the prime numbers as friends—friends who bring us problems!

*Acknowledgment.* Translated from the German by Bart Braden and Ellen Curtin.

## References

1. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, 1960.
2. P. Ribenboim, Euler's famous prime generating polynomial and the class number of imaginary quadratic fields, *L'Enseignement Mathématique* 34 (1988) 23–42.
3. P. Ribenboim, *The Book of Prime Number Records*, 2nd ed., Springer, New York, 1989.
4. P. Ribenboim, *The Little Book of Big Primes*, Springer, New York, 1991.