BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 21, Number 2, October 1989
©1989 American Mathematical Society
0273-0979/89 $1.00 + $.25 per page

The book of prime number records, by Paulo Ribenboim. Springer-Verlag, New York, Berlin, Heidelberg, 1988, xxiii + 476 pp., $49.80. ISBN 0-387-96573-4

Do people ever ask you, "What is the largest known prime?" or "For how many zeros of the zeta function is the Riemann Hypothesis known to hold?" Now at last there is a book which answers many questions of this type.

Guinness published the *Book of World Records* to settle arguments. Ribenboim has written a similar book to settle arguments about prime numbers. The world would be very civilized indeed if a brawl in a pub began with a dispute about how many twin primes are known. Some of the records which are reported are the results of computer searches and some of them are statements of theorems which approach best possible results.

Euclid's proof that there are infinitely many primes is well known to most mathematicians: If there were only finitely many primes, list all of them, multiply them together and add 1. The resulting number is not divisible by any prime on the list. However, either it is prime or it has a prime factor not on the list. In either case, there exists a prime not on the list which was supposed to contain all primes.

Some students misunderstand this proof and believe that it says that if you multiply together all the primes up to some point, and add 1, the result must be prime. Write $p\#$ for the product of all primes $\leq p$. Then $p\#+1$ is indeed prime for $p = 2, 3, 5, 7$ and 11, which fosters the students' misconception. However, $13\#+1$ is not prime. Is $p\#+1$ ever prime again? Yes, it is prime also for $p = 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549$ and 13649. The last five examples were discovered by Dubner [4] in 1987. The record largest known p for which $p\#+1$ is prime is $p = 13649$.

Write $\pi(x)$ for the number of primes up to x. A simple approximation for $\pi(x)$ is $\pi(x) \approx x/\log x$. A closer approximation is $\pi(x) \approx \mathrm{Li}(x) = \int_0^x dt/\log t$. What is the largest x for which $\pi(x)$ has been computed exactly? The record is $\pi(4 \times 10^{16}) = 1{,}075{,}292{,}778{,}753{,}150$, computed by Lagarias, Miller and Odlyzko [6] in 1985. They used a supercomputer, of course, but it did not generate each of these primes. They used an inclusion-exclusion technique based on a formula devised by Meissel in 1871 (and improved by several researchers since then). It is interesting to note that they chose the algorithm which is asymptotically *second* fastest. (The overhead of the algorithm which is ultimately fastest makes it slower than the second best one for numbers which are small enough to perform the calculation at all.)

The distribution of prime numbers is closely connected to the location of the zeros of the Riemann zeta function. This function of a complex variable has infinitely many zeros with real part between 0 and 1. If all of these zeros had real part equal to 1/2, as Riemann conjectured in his famous Riemann Hypothesis, then $\mathrm{Li}(x)$ would be a very good approximation to $\pi(x)$, as we would have $\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log x)$. Various mathematicians have determined that the first few zeros of the zeta function all lie on the line $\mathrm{Re}(s) = 1/2$. The record is held by van de Lune, te Riele and Winter [**9**] who in 1986 verified the Riemann Hypothesis for the first 1,500,000,001 zeros.

What is the longest table of prime numbers ever made? The longest table ever published is that of D. N. Lehmer [**7**], which lists the primes up to 10,017,000. In the middle of the nineteenth century, Kulik prepared a table of factors of all numbers (other than multiples of 2, 3, and 5) up to 100,330,200. The primes up to this limit can be found easily in this table. However, there is only one copy of it (in the Vienna Academy of Sciences), one volume (out of 8) is missing, and the table contains too many errors to be worth publishing. In 1959, Baker and Gruenberger published a microcard table of the first six million primes—those up to 104,395,289. Now that we have computers, no more extensive tables are likely to be published because it is quite easy to generate a table of primes in a computer memory by the Sieve of Eratosthenes. Then the computer can perform the desired examination of the table and print a summary of the result. What then is the largest x so that all primes up to x have ever been formed and studied in a computer memory? Young and Potler [**10**] have computed all primes up to 7.2635×10^{13} and studied the gaps between consecutive primes. Their record-making calculations are still continuing now.

It is easy to exhibit large gaps between consecutive primes: A block of N consecutive composite numbers begins with $(N+1)! + 2$. Hence it is no big deal to find a long block of composite numbers unless it is the *first* occurrence of a block of that length. The prime gaps have been tabulated by Young and Potler [**10**] for primes up to 7.2635×10^{13}. The largest gap they found was 778 (i.e., 777 composites) which follows the prime 42,842,283,925,351. Naturally, they did not find examples of every gap up to 778. The smallest missing gap size is 676.

While Euclid knew that there are infinitely many primes, even today we do not know whether there are infinitely many pairs p, $p+2$ of twin primes. Therefore, it is worthwhile to count the small twin primes and to seek large ones. The largest x for which we know exactly how many twin primes there are below x is 10^{11}: In 1976 Brent counted 224,376,048 primes $p \leq 10^{11}$ for which $p+2$ is also prime. Noting that this number is approximately the population of the United States, Shanks [**8**, second edition, p. 219] proposed giving each American one pair of prime twins. Numerical evidence and a heuristic argument suggest that the number of pairs of twin primes up to x is asymptotically $cx/\log^2 x$, where c is an explicitly given constant.

About a dozen pairs of twin primes are known in which the numbers have more than 1000 digits. Most of these were discovered by Dubner, Keller and Atkin and Rickert. The three largest known pairs are $663777\times 2^{7650}\pm 1$, $571305\times 2^{7701}\pm 1$ and $1706595\times 2^{11235}\pm 1$. These were discovered in 1989 by a team of six coworkers headed by Bodo Parady. The numbers in the pairs have 2309, 2324 and 3389 digits, respectively. The fact that it is comparatively easy to find such large twin prime pairs supports the conjecture that there are infinitely many of them.

It is not trivial to prove that a number with more than 1000 digits is prime. The special form $k2^n \pm 1$ of the large prime pairs is chosen to facilitate these proofs. If N is a large prime, then it is almost always easy to prove that N is prime provided that one knows the prime factorization of either $N - 1$ or $N + 1$. A theorem like this one is used for the proof:

THEOREM 1 (PROTH, POCKINGTON, LEHMER, SELFRIDGE). *If N is odd and if for each prime q dividing $N - 1$ there exists an a for which $a^{N-1} \equiv 1 \pmod{N}$, but $a^{(N-1)/q} \not\equiv 1 \pmod{N}$, then N is prime.*

The a's are found by trial and error. Usually it is easy to find them among the small quadratic nonresidues of N. There is a similar theorem for the case of $N+1$ factored completely. See [2] for references to theorems of this type. For the special case of Mersenne numbers $M_p = 2^p - 1$ there is an even more efficient test:

THEOREM 2 (LUCAS, LEHMER). *If p is odd, then M_p is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$, where $S_1 = 4$ and $S_{j+1} = S_j^2 - 2$ for $j \geq 1$.*

The three largest known Mersenne primes are M_p for $p = 110503$, 132049 and 216091. Colquitt and Welsh discovered 110503 after Slowinski found the other two. The 65050-digit number M_{216091} is presently the largest known prime. The search for new Mersenne primes is continuing. As of June, 1989, all p up to about 145,000 have been tested. This shows that M_{132049} is the thirtieth Mersenne prime in order of size.

The even perfect numbers are $2^{p-1}M_p$ for those p for which M_p is prime. No odd perfect numbers are known and it is likely that there are none. Many theorems give improbable properties of hypothetical odd perfect numbers. The record lower bound on the size of an odd perfect number is due to Brent and Cohen [1] who showed that any such number must exceed 10^{150}. Exactly thirty-one perfect numbers are known, one for each Mersenne prime.

The iterated use of Theorem 1 is an efficient method for generating large random primes for use in cryptography. To construct a secret 100-digit prime, say, for the Rivest-Shamir-Adleman public-key cryptosystem, you might proceed as follows: Begin with a 10-digit number N_1 which you know is prime. (It doesn't have to be secret.) Try various random 10-digit numbers k_1 until some $N_2 = 2k_1N_1 + 1$ satisfies $2^{N_2-1} \equiv 1 \pmod{N_2}$. (Satisfying the latter congruence shows that N_2 is probably prime.) Try to prove that N_2 is prime via Theorem 1. (If you fail, try more values of k_1.) Now repeat the process with 1 added to the subscripts. After nine iterations you arrive at a 100-digit prime N_{10} which no one has ever seen before.

There are two ways that primes may be in arithmetic progressions: They may lie in a given (infinite) arithmetic progression or they may form the entire (finite) progression. Dirichlet proved that if the first term a and common difference $d > 1$ of an arithmetic progression are relatively prime, then the arithmetic progression contains infinitely many primes. When a and $d > 1$ are relatively prime, define $p(d, a)$ to be the smallest prime in the arithmetic progression $\{a + kd; k \geq 0\}$. The question of how large $p(d, a)$ can be is a very difficult one. There are not enough primes for it to be much smaller than $\phi(d) \log d$ always, where $\phi(d)$ is the number of a relatively prime to d with $1 \leq a < d$. In the other direction, Elliott and Halberstam [**5**] have shown that for all $\varepsilon > 0$ and for all $d > 1$ not belonging to a thin (density 0) sequence, we have $p(d, a) < \phi(d)(\log d)^{1+\varepsilon}$ for almost all a relatively prime to d with $1 \leq a < d$. To avoid a trivial difficulty, we usually restrict a to lie between 1 and d. Define $p(d)$ to be the greatest $p(d, a)$ for $1 \leq a < d$ with a relatively prime to d. Linnik's theorem asserts that there is a constant $L > 1$ such that $p(d) < d^L$ for all sufficiently large d. Various authors have proved a succession of smaller values for L. Chen [**3**] proved in 1979 that $L = 17$ will do. This is the record for results in published papers. Chen and Liu have claimed that $L = 13.5$ will do, but their paper has not appeared yet. It has been conjectured that $L = 2$ or even that $p(d) < d \log^2 d$, but we are far from proving any inequality that good.

Even less is known about primes which form an arithmetic progression. In 1939, van der Corput proved that there are infinitely many three-term arithmetic progressions of primes. However, we still do not know whether there are infinitely many arithmetic progressions consisting of four primes. Computer searches have uncovered many arithmetic progressions consisting of a small number of primes. The record is a progression of 19 primes discovered by Pritchard in 1985. The first term is 8,297,644,387 and the common difference is 4,180,566,390.

Some large primes are interesting because they divide numbers of simple form such as $b^n \pm 1$ or Fibonacci numbers u_n for small b and n. (See [**2**], for example.) To factor a large integer is a difficult problem. Let me mention the record factorizations for the two fastest known algorithms. The running time for Pomerance's quadratic sieve method depends on the size of the number factored and not on the nature of the prime factors of the number. It is appropriate to use the size of the number factored to measure the success of this method. The record is the factorization of the 106-digit divisor of $2^{353} + 1$ done in April, 1989, by A. K. Lenstra, M. Manasse and several dozen other researchers who ran the program on thousands of computers for several months. H. W. Lenstra, Jr.'s elliptic curve factorization method tends to find small prime factors more quickly than larger ones. The size of the prime factor discovered is the appropriate measure of its success. Only about a dozen factors having more than 30 digits have been discovered in the four years the method has been in use. The greatest of these is the 38-digit prime factor of the Fibonacci number u_{467} (which has 98 digits) discovered in May, 1989, by Silverman. By the way, the record Fibonacci prime is u_{2971}, discovered by Williams.

Ribenboim's book is informative and easy to read. One can begin reading almost anywhere. It is even chattier than a book review in this *Bulletin*. The book is accessible to nonexperts. It is not just a list of records. Much background material is included, too. Many simple proofs are given. It is an excellent source of ideas for a lecture to a mathematics club or high school.

My main criticism of it is the poor quality of typesetting. It is far inferior to the TEX to which I have become accustomed. The 101-pp. bibliography has a verbose three-column format. One column holds the year of the publication and another gives the author. The title and the other information occupies the third column.

The book is so popular that the first edition sold out completely in only one year. A second edition will appear soon. Many of the records have been broken; these will be updated in the new edition. (Some records in this review will be superseded before it appears in print.) A few typographical errors will be corrected as well, but, alas, the book will not be retypeset.

References

1. R. P. Brent and G. L. Cohen, *A new lower bound for odd perfect numbers*, Math. Comp. **53** (1989).

2. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$, up to high powers*, Contemporary Math., vol. 22, Amer. Math. Soc., Providence, R.I., 1983; second edition 1988.

3. J. R. Chen, *On the least prime in an arithmetical progression and theorems concerning the zeros of Dirichet's L-function*. II, Sci. Sinica **22** (1979), 859–889.

4. H. Dubner, *Factorial and primorial primes*, J. Recr. Math. **19** (1987), 197–203.

5. P. D. T. A. Elliott and H. Halberstam, *The least prime in an arithmetic progression*, Studies in Pure Mathematics (R. Rado, ed.) Academic Press, London, 1971, pp. 59–61.

6. J. C. Lagarias, V. S. Miller and A. M. Odlyzko, *Computing $\pi(x)$: the Meissel-Lehmer method*, Math. Comp. **44** (1985), 537–560.

7. D. N. Lehmer, *List of prime numbers from* 1 *to* 10,006,721, reprinted by Hafner, New York, 1956.

8. D. Shanks, *Solved and unsolved problems in number theory*, Spartan, Washington, 1962; second edition by Chelsea, New York, 1978; third edition by Chelsea, Bronx, 1985.

9. J. van de Lune, H. J. J. te Riele and D. T. Winter, *On the zeros of the Riemann zeta function in the critical strip*. IV, Math. Comp. **47** (1986), 667–681.

10. J. Young and A. Potler, *First occurrence prime gaps*, Math. Comp. **52** (1989), 221–224.

S. S. Wagstaff, Jr.
Purdue University

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 21, Number 2, October 1989
©1989 American Mathematical Society
0273-0979/89 $1.00 + $.25 per page

Limit theorems for stochastic processes, by J. Jacod and A. N. Shiryaev. Grundlehren der Mathematischen Wissenschaften, vol. 288, Springer-Verlag, Berlin, Heidelberg, New York, 1987, xvii + 600 pp., $98.00. ISBN 3-540-17882-1

1. Introduction. Two important threads in the fabric of stochastic processes come together in this monograph: semimartingales and convergence