Testing for Primes Gets Easier

New test reduces time to determine if a 100-digit number is prime from a century to a few hours

A computer scientist and two mathematicians have discovered a surprising new way to decide whether numbers are prime, meaning they have no divisors other than themselves and 1. This is one of the oldest problems in mathematics. In the view of many number theorists, a method so rapid as the one proposed should have been impossible to find.

Since the time of the ancient Greeks, mathematicians have known that there are infinitely many prime numbers and for centuries mathematicians have known that primes are distributed among the whole numbers in an irregular manner. They also realized that it is infeasible to test for large primes by trying out all smaller numbers that could possibly be factors. In the 17th century, the French number theorist Marin Mersenne wrote despairingly that "To tell if a given number of 15 or 20 digits is a prime, all time would not suffice for the test." But testing for primes has always been deemed important as a benchmark of progress in number theory. In 1801, the German mathematician Carl Gauss wrote, "The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated."

The significance of the new test for primes is mainly aesthetic, not practical. Large prime numbers are used in fast Fourier transforms and in generating random numbers but existing, slower methods of finding primes suffice for these purposes.

The principal author of the result is Leonard Adleman, a computer scientist with a joint appointment at the University of Southern California and the Massachusetts Institute of Technology. Adleman explains that he first became intrigued by the problem of finding an efficient way to determine whether numbers are prime about 5 years ago. He worked on the problem sporadically until about 1 year ago, when he thought he had an answer. In collaboration with Robert Rumely, a number theorist visiting at MIT, he spent the past year developing a method that looked extremely rapid. Carl Pomerance, a number theorist at the University of Georgia, then proved it was so. With this new method, it is possible to decide whether a 100-digit number is a prime in a few hours of computer time. In contrast, such a problem would have required a century of computer time with the best available methods to date.

The reason all previous tests were so slow is that the number of computational steps they require is an exponential function of the size of the number to be tested; they are so-called exponential time algorithms. For testing large numbers, the computations are excessive. What was wanted was a test that requires a number of computational steps that is only a polynomical function of the size of the number to be tested—a polynomial time algorithm.

The difference between an exponential and polynomial function can be dramatic. For example, if the number of computational steps to solve a problem is the typical polynomical function, x^3, the computations take 1/5 second of computer time when x is 60. If, however, the number of steps is the exponential function 3^x, the computations take centuries of computer time when x is 60. Adleman, Rumely, and Pomerance did not quite achieve the goal of finding a test for primes that requires only polynomial time but they came within a hairsbreadth of it.

Adleman explains their test for primes as an outgrowth of a probabilistic test devised several years ago by Robert Solovay of the University of California at Berkeley and Volkur Strassen of the University of Zurich and then independently discovered by Michael Rabin of the Hebrew University in Jerusalem (*Science*, 4 June 1976). The test, said Rabin at that time, can determine "for all practical purposes" whether a number is a prime. But many mathematicians were troubled by its probabilistic nature and refused to accept it. Peter Weinberger of Bell Laboratories in Murray Hill, New Jersey, for example, asked what it means to be a prime for "all practical purposes." Either a number is or it is not a prime.

In explaining the probabilistic test, Adleman makes an analogy with dice. Solovay and Strassen showed, he says, that a number n can be thought of as a die with n facets. Each facet can be red or white. If n is a prime, all facets are red. If n is not a prime, at least half the facets are white. One way to decide whether n is a prime is to look at all the facets, but this requires an inordinate number of computations when n is large. An alternative is to look at a certain number of them, say 100 facets, chosen at random. Then, if all are red, "you know that either n is a prime or you are very unlucky," Adleman explains.

What Adleman and Rumely did is to broadly generalize the mathematical notion of a red or white facet. This allows them to judiciously choose which facets to look at in order to see if n is a prime. Adleman explains that with each number facet that he checks, he learns something about n. As he checks more and more facets, he puts more and more constraints on the structure of n until, finally, he learns that, if all the facets are red, either n is a prime or n must be divisible by at least one of a short list of numbers. He then tries those numbers. If none divide n, it is a prime.

In order to decide how fast this new method is, Adleman next developed a heuristic argument that the algorithm could decide if a number n is a prime in fewer than $\log n^{(\log \log \log n)^2}$ steps. When Pomerance saw a preprint of his paper, he realized that he could prove exactly how many steps are required by generalizing a result of Karl Pracher published in 1955. Using this result, he proved that the number of computational steps required is about $\log n^{(\log \log \log n)^2}$, which is very very close to being a polynomial. The function $\log \log \log n$ is nearly a constant and if it were a constant the method would require only a polynomial number of steps.

Ronald Graham of Bell Laboratories in Murray Hill suspects that eventually it will be proved that testing for primes has a polynomial time algorithm. He explains that in the past, when researchers got within $\log \log \log n$ of showing some-

0036-8075/80/0926-1503$00.50/0

thing was a constant, it was eventually proved to be so. For example, a decade ago researchers were looking for efficient ways to find the median of a sequence of n numbers. At first a method was found that required $n \log \log n$ steps. This was succeeded by a method requiring $n \log \log \log n$ steps. Finally, a method was found that required a constant times n steps.

The new way of testing for primes also is intriguing to mathematicians because of the relation prime testing bears to the harder and more practical problem of factoring. Factoring and testing for primes are twin problems, says Pomerance, although it is not clear how to go from the first to the second. "To me, it [the new prime testing algorithm] gives evidence that it may be possible to find a polynomial time algorithm for factoring," says Graham.

If such a factoring algorithm could be discovered, it would have important implications for cryptography. A code which was developed by Adleman together with Ronald Rivest and Adi Shamir of MIT and which has attracted widespread interest is based on the problem of factoring a very large number. If factoring were somehow made easy, the code would be insecure. Adleman points out that the close relation between testing for primes and factoring illustrates that the difference between what is basic theoretical research and what is research that is directly applicable to cryptography can be quite small.

—GINA BARI KOLATA

Plug Pulled on Chemistry Computer Center

After an unusually brief trial, NSF and DOE decide to phase out chemists' first try at big science, the National Resource for Computation in Chemistry

The National Science Foundation (NSF) and the Department of Energy (DOE), joint sponsors of the National Resource for Computation in Chemistry (NRCC), have decided to terminate the not yet 3-year-old organization. The agencies have requested the Lawrence Berkeley Laboratory, home of the NRCC, to prepare a plan for phasing out the computational chemistry center by 30 September 1981. Although a compromise that would permit some NRCC activities to be continued has been proposed, agency officials say that doubts about the need for an NRCC coupled with tight budgets make it certain that the phase-out will occur as scheduled.

The NRCC was established to be a place where computational chemists could do things not possible in their own laboratories, such as solving problems requiring the use of a state-of-the-art supercomputer and developing and standardizing new software for community-wide use. Headed by William Lester, a quantum chemist on leave from IBM, and governed by a 12-person policy board comprising chemists of varied specialties, the NRCC has been a division of the Lawrence Berkeley Laboratory (LBL) since its birth in October 1977.* The organization has an annual budget of about $1.75 million.

When the NSF and DOE set up the NRCC, the agencies made its continued existence contingent on a favorable review after a 3-year trial period. Earlier this year, the agencies selected a ten-person review committee to evaluate the NRCC and make recommendations as to its future.† Under the chairmanship of William Goddard of the California Institute of Technology, the review committee this April reported serious shortcomings in the NRCC, but nonetheless recommended its continuation as an experiment for two additional years. According to Goddard, it was "too early to terminate the NRCC." To remedy the shortcomings, the committee also recommended some major changes in the organization that would eliminate all of the NRCC's professional staff and reduce its budget to just over $500,000 per year (excluding overhead).

Specifically, the review committee said that the NRCC should no longer fund grants for either internal or external computing time, should abandon its in-house software development activities, should leave all software distribution to the Quantum Chemistry Program Exchange at Indiana University, and should not buy its own central computer. On the positive side, the review committee said the NRCC should continue a series of highly successful workshops it has been holding and should establish an external postdoctoral program to replace in-house software development.

Perhaps in a gamble aimed at preserving a whole loaf rather than just a half, the LBL director, David Shirley, told NSF's Chemistry Advisory Committee that the skeleton NRCC that would remain if the review committee's recommendations were accepted would have little intellectual content and would not be appropriate for a scientific research laboratory. Shirley sketched out what he considered to be a minimum acceptable NRCC, one that would be comparable in staffing and scientific content to that existing now.

By the end of July, the two agencies had made up their minds. According to James Kane, Director of Basic Energy Sciences at DOE, the agencies construed the review committee's report as "a strong recommendation that the NRCC was not worth continuing as it was set up." Agency officials told *Science* that their already negative reading of the report and a unanimous recommendation by the NSF Chemistry Advisory Committee to close the NRCC combined with Shirley's position left them no choice but to terminate the experiment.

Shirley, Lester, and the NRCC policy board have since come up with a compromise proposal and have secured the blessings of Goddard's review committee, but Richard Nicholson, Director of NSF's Chemistry Division, and Elliot

*The NRCC policy board members are: Bruce Berne, Columbia University; Charles Bender, Lawrence Livermore Laboratory; Mary Good, Louisiana State University; William Guillory, University of Utah; James Ibers (chairman), Northwestern University; Carroll Johnson, Oak Ridge National Laboratory; Martin Karplus, Harvard University; Herbert Keller, California Institute of Technology (resigned in 1979); William Miller, University of California at Berkeley; John Pople, Carnegie-Mellon University; Anessur Rahman, Argonne National Laboratory; and Kenneth Wiberg, Yale University.

†Members of the review committee are: Allen Bard, University of Texas at Austin; John Brauman, Stanford University; William Busing, Oak Ridge National Laboratory; Marshall Fixman, Colorado State University; Willis Flygare, University of Illinois; William Goddard (chairman), California Institute of Technology; Dudley Herschbach, Harvard University; Daniel Kivelson, University of California at Los Angeles; Howard Simmons, DuPont; and John Tully, Bell Laboratories.

0036-8075/80/0926-1504$00.50/0