New Test Finds "Certified" Primes in Record Time

A new way to test for primes numbers is the first to use modern mathematics for this old problem and can quickly prove that a number is or is not a prime

Two computer scientists have found a new way to determine whether large numbers are prime—an old problem that is of practical as well as theoretical importance. The method differs from others that preceded it because it uses modern mathematics and because it can quickly provide a rigorous proof that a number is, in fact, a prime.

Primes—numbers such as 3 and 5 that have no factors other than themselves and 1—are the elementary particles of number theory. Every number that is not itself a prime can be constructed by multiplying primes together. Since the time of the ancient Greeks, mathematicians have known that there are infinitely many primes and that they are unevenly distributed among the whole numbers. But it has not been clear how to quickly decide if a large number is a prime.

Large prime numbers are used in fast Fourier transforms, in cryptography, and in generating random numbers, so there is a real demand for good ways to find these numbers. The goal of computer scientists is to find a method that takes only "polynomial time," meaning that it should be quick to run on a computer and one that determines, without ambiguity, whether a number is a prime. These are features of the new method, which was developed by Shafi Goldwasser and Joseph Kilian of the Massachusetts Institute of Technology. But the method is not yet ideal—there may be a few numbers that it cannot prove are primes and it is not yet quite fast enough to compete with previous methods. For these reasons the method is as yet of mostly theoretical interest.

In the past decade, mathematicians have devised a variety of methods to test for primes, but each has its drawbacks. In the mid-1970's, Michael Rabin of Harvard University and the Hebrew University in Jerusalem and, independently, Robert Solovay of the University of California at Berkeley and Volker Strassen of the University of Zurich discovered a probabilistic way of testing for primes. The test is fast and easy, but its probabilistic nature troubled some researchers. If you test a number and the answer comes out that it is not a prime, the answer is absolutely correct. But if the test says a number is a prime, there is always some small degree of uncertainty in its decision. The test cannot be used to prove, in a mathematically rigorous fashion, that a number is a prime.

"These probabilistic algorithms are essentially a random search for a proof that the number is not prime. If, after searching for a polynomial number of steps, such proof is not found, the algorithm gives up and says 'probably prime.' Thus, failure to prove that a number is not prime provides circumstantial evidence that the number is in fact prime," Goldwasser explains.

At about the same time as these probabilistic methods were introduced, Gary Miller of the University of Southern California discovered a test for primes that is not probabilistic, runs in polynomial time, and is always correct when it says a number is not prime. But whether it is correct when it says a number is prime depends on whether a well-known conjecture in complex analysis, the Extended Riemann Hypothesis, is true. If the conjecture is false, many numbers that Miller's algorithm says are primes will turn out not to be primes after all. Quite a few mathematicians believe this hypothesis is true, but, despite extensive work on the problem, the hypothesis has not been proved yet.

The program provides what Goldwasser calls "a short certificate of primality."

What was needed was a way to get arounc the probabilistic nature of the first twc methods without relying on the Extendec Riemann Hypothesis. In 1980, three mathematicians did just that, although their method, too, has its drawbacks. In 1980, Leonard Adleman of the University of Southern California and Robert Rumley and Carl Pomerance of the University of Georgia found a method that is deterministic—it always gives the correct answer—and that is quite rapid. "It is routinely used for numbers up to 200 digits in length," says Andrew Odlyzko of AT&T Bell Laboratories, "and it is fairly easy to extend to larger numbers."

But this method was not quite a polynomial time one, although it was very nearly so. At first, computer scientists suspected that it would soon be modified to be polynomial time. Yet, says Goldwasser, "5 years have passed and no one has improved the method. I think a substantially different idea is needed to make it go faster."

The new method devised by Goldwasser and Kilian is a probabilistic algorithm that is always correct and that almost always runs in polynomial time. However, it is not yet fast enough to be of clear practical importance. Like the original probabilistic methods, it is correct when it tells you that a composite number is truly not a prime. But, unlike those methods, it is also correct when it tells you that a number is a prime. The program provides what Goldwasser calls "a short certificate of primality," which is a proof that can easily be verified that a number is indeed a prime. This means that the test can be used to generate "certified primes," which are needed for some of the new cryptography schemes. However, there may be a very small proportion of primes for which the test fails. In these cases, "failure" means that the algorithm runs as slowly as the one devised by Adleman, Pomerance, and Rumley. This is where the probability comes in—there is a very small chance that a number that you are trying to test may be one of these.

But there may actually be no primes for which the algorithm fails. It is just that the possibility of such primes cannot yet be ruled out. If anyone could find a prime that makes the method fail, says Hendrik Lenstra of the Mathematical Sciences Research Institute in Berkeley, California, that finding "would be mathematically exciting." It would imply that another conjecture in number theory, one that describes the distribution of primes, is incorrect.

In order to be sure that Goldwasser and Kilian's algorithm never fails and that, in fact, there is no group of numbers for which the method takes as long as the other algorithm, number theorists would have to know more than they know now about the distribution of prime numbers. The idea is to look in any interval from a number x to x

+ $(x)^{1/2}$. "You want enough primes in that interval so that you can find one quickly," says Goldwasser.

A conjecture that number theorists say is probably true is that as numbers grow large, the biggest gap between two primes is bounded by the logarithm of the larger prime. If this conjecture could be proved, then Goldwasser and Kilian's method would always work. The probability of finding a number for which it fails would be zero. Yet, says Lenstra, the conjecture is "fairly strong and it has been around for years. Although it is a reasonable conjecture, I am not sure I will live to see it proved."

Goldwasser and Kilian's method is of particular interest to mathematicians for two theoretical reasons. One is that the method allows mathematicians to recognize, for the first time, members of an infinite set of primes by using a polynomial time algorithm. This set contains nearly all the primes.

The second interesting aspect of the method is that it uses elliptic curves in its proof. This sort of modern mathematics was first used in complexity theory—the search for the fastest possible computer algorithms—by Lenstra. Early this year, Lenstra devised a new way to factor numbers based on elliptic curves. Goldwasser, hearing of this result, was inspired to use elliptic curves for the related problem of testing for primes. "Elliptic curves turn out to be a very useful tool," she says. She and Kilian made use of a method recently developed by Rene Schoof of the Mathematical Sciences Research Institute in Berkeley to determine the order of a group of points on an elliptic curve. This allows them to quickly try different groups of points on a curve in their attempts to find a group whose order is of the form useful in a test for primes.

The computation of the order of a group of points on an elliptic curve, however, is what slows down the new method. "The main problem is making Schoof's algorithm practical," says Lenstra. Still, Odlyzko is optimistic. It is entirely possible that that part of the algorithm might be speeded up. "It will take a lot more work, but they may be able to make their algorithm practical," he remarks.

Odlyzko also speculates that the test might in fact be universally applicable. "There is some hope that you can prove the test will work on all primes," he says. But for now, the new method is of mathematical interest because it is a polynomial time method which is always correct and because, as Ronald Rivest of MIT puts it, "it applies the very modern method of elliptic curves to the very old problem of testing for primes." ■ **Gina Kolata**

Polynesians' Litter Gives Clues to Islands' History

The natural history of many of the Pacific Islands, once thought to be virtually pristine, turns out to have been significantly distorted by recent human activity

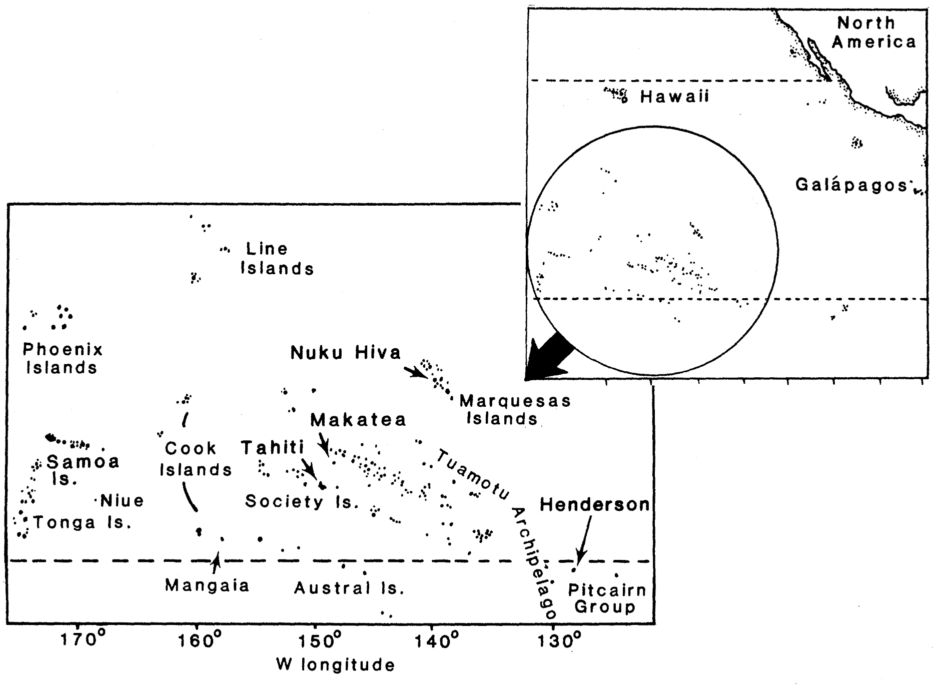
Many of the far-flung islands of the South Pacific have experienced only fleeting human contact, in some cases just a century or so of Polynesian habitation between 800 and 500 years ago. For this reason the islands have often been assumed to be still in, or at least very close to, a natural state. For instance, Henderson Island, a remote outpost of the Pitcairn group, has been described as "one of the few islands of its size in the warmer parts of the world still little affected by human activity," according to one recent observer.

It turns out, however, that the Polynesian presence, albeit brief, had a devastating effect on the natural history of Henderson. The same is almost certainly true for all other islands of the Pacific.

Two ornithologists, David Steadman, of the New York State Museum, and Storrs Olson, of the National Museum of Natural History, Washington, discovered this state of affairs when they recently examined the contents of archeological material recovered a decade ago from a cave and five shelters located along the north shore of the island. This glimpse of the record reveals that at least one third of the species of land birds that once lived there no longer do so.

From the limited amount of information available so far on some of the other remote Pacific islands, it seems that the pattern evident on Henderson is typical: human habitation caused significant local extinctions. For instance, the much more complete fossil studies on the Hawaiian islands show that in historic times there were more than twice as many bird species as there are now.

The implications of these results are several. For instance, an overall survey of the modern distribution of bird species (and presumably of other organisms, too) throughout the area is both impoverished and distorted compared with the true, natural state. Theoretical inferences about the composition and dynamics of natural ecosystems are therefore likely to be, at best, incomplete. From a practical point of view, this historical perspective of species distribu-


North America
Hawaii
Galápagos
Line Islands
Phoenix Islands
Nuku Hiva
Marquesas Islands
Makatea
Samoa Is.
Cook Islands
Tahiti
Tuamotu Archipelago
Niue
Society Is.
Henderson
Tonga Is.
Mangaia
Austral Is.
Pitcairn Group
170°
160°
150°
140°
130°
W longitude