Mathematics

High-speed tests for primes

from Ian Stewart

PRIME numbers have exercized the imagination and ingenuity of mathematicians since at least the time of Euclid. The recent upsurge of interest in public-key encryption[1] has added a practical, indeed military, dimension to two venerable questions: first, given a number, is it prime or composite, and second, if it is composite, what are its factors?

In principle, there exist specific procedures, or algorithms, that can solve both problems: if the number is n, try all possible divisors up to $\sqrt{n}$. In practice, these are hopelessly inefficient, taking perhaps a million years to test a 40-digit number on a fast computer. Better though less direct methods exist, and until recently the best techniques might solve the first question for an 80-digit number and the second for a 40-digit number in an acceptable time. This reflects a general (but conjectural) view that the second problem is substantially harder than the first.

The efficiency of an algorithm is usually gauged by estimating how rapidly the computational time grows as the number of digits k of the number n increases. If this time is always smaller than Ck^r for some constant C and a fixed power k^r of k, then the algorithm is said to run in polynomial time. Trial-and-error division runs in exponential time $C2^k$, which (as Thomas Malthus vividly insisted when $r=1$) grows infinitely faster in the long run.

For a truly practical algorithm the value of the constant C is also important. For instance, an algorithm that required exactly one billion years, for any n, would run in polynomial (indeed constant) time. But in less artificial cases, a polynomial-time algorithm is usually efficient and practicable, whereas an exponential-time algorithm is not.

Whether the problem of deciding whether a number is prime or composite can be solved in polynomial time remains in doubt. (It is widely believed that the factors of a composite number cannot be found in polynomial time, but this has never been proved.) The current status of this problem is a catalogue of useful near-misses.

The basis of most modern primality tests is Fermat's 'Little' Theorem: if p is prime and a is not divisible by p, then $a^{p-1}-1$ is divisible by p. This can be used to prove a number composite, without exhibiting any factors. For example, when $p=4$ and $a=2$, one must evaluate $2^4-1=15$. This is not divisible by 4, so 4 cannot be prime. By applying this test for a suitable number of randomly chosen numbers a, it is possible to obtain a probabilistic algorithm for primality that runs in polynomial time. 'Probabilistic' means that the procedure terminates within the time limit with a probability near 1, and if it does terminate, will prove or disprove primality.

Unfortunately, some composite numbers satisfy the Fermat Theorem for all a, 'by accident'. They are called Carmichael numbers, and an example is the number 561 = 3.11.17. Refining the Fermat Test eliminates some, but not all, of these: the numbers remaining are called strong pseudoprimes to the base a.

A composite number cannot be a strong pseudoprime to every base; so the proper selection of bases might lead to an efficient algorithm for primality. In 1976. G. Miller[2] showed that the choice of bases can be made so as to yield an algorithm that runs in polynomial time — but only by assuming the validity of the 'Extended Riemann Hypothesis', one of the most famous and difficult unsolved conjectures in mathematics.

In 1980 L. Adleman and R. Rumely announced a 'nearly' polynomial-time algorithm, which has recently been published[3]. It involves more general strong pseudoprimality tests, using bases a that are of the form

$$a_0 + a_1\zeta + \ldots + a_{m-1}\zeta^{m-1}$$

where ζ is a complex mth root of unity. These cyclotomic integers were introduced by Ernst Kummer in about 1843 in an attack on another famous conjecture, Fermat's Last Theorem (the equation $x^p + y^p = z^p$ has no integer solutions for $p>3$) and led to the modern theory of algebraic numbers. By exploiting some deep theorems from algebraic number theory, such as the 'Higher Reciprocity Laws', Adleman and Rumely were led to conjecture a running-time for their algorithm of the form

$$_kC \log\log k$$

intermediate between polynomial and exponential time. Using additional number-theoretic results, Carl Pomerance and Andrew Odlyzko proved this conjecture. The algorithm, at least in an improved form, is computer-practical: estimates suggest that 200-digit numbers may eventually be tested for primality in a few minutes on a fast computer.

Number Theory is usually thought (by outsiders) to be one of the purest and least applicable areas of mathematics. The work of Adleman, Rumely, Pomerance, Odlyzko and others suggests that a major revision of this view may be in order. And it is likely than many other questions about the efficiency of algorithms will also require number-theoretic methods of analysis. □

Ian Stewart is in the Mathematics Institute of the University of Warwick, Coventry CV4 7AL.

1. Rivest, R., Shamir, A. & Adleman, L. *Commun. ACM* **21**, 120 (1978).
2. Miller, G.L. *J. Comput. Systems Sci.* **13**, 300 (1976).
3. Adelman, L.M., Pomerance, C. & Rumely, R.S. *Ann. Math.* **117**, 173 (1983).

Astronomy

Quasars: searching out the smallest and nearest

from Martin Elvis

MUCH of the immediate excitement in astronomy comes from finding the biggest, the most luminous or the most distant of the various kinds of object. Particular satisfaction for those who search out extremes is provided by quasars, for they can be seen out to redshifts of 3.5 — equivalent to looking back about 80 per cent of the age of the Universe. When it comes to studying the details of quasars' physical structure, and thus to understanding how they work, there is a problem, however. The smallest dimension that can be directly resolved using current technology at a redshift of 3 is about 15 pc (10^{19} cm). This is remarkably small but, unfortunately, it is still not small enough. Variability in quasars and other active galaxies is seen on time scales of a few days[1], implying that the radiating region must be at least a few light-days across — about 10^{16} cm.

To study quasar structure in detail, we have to change our perspective and look for much nearer, but weaker, examples. In the past two years, several of the nearest galaxies have been found to contain miniature examples of quasars in their nuclei. Now radio observations[2] have begun to examine these miniature quasars at just this scale. In the first miniature quasar examined, an elongated structure aligned with the minor axis of the galaxy was found. This suggests that the tiny central quasar 'knows' the orientation of the much larger galaxy.

Norbert Bartel of MIT and his collaborators at Haystack Observatory, JPL and the Max-Planck-Institut in Bonn used very long-baseline interferometry (VLBI) to achieve this result. It is the first time that structure has been seen in an active nucleus (the term used for low-luminosity quasars) close to the scale of the intense radiation

Martin Elvis is in the Smithsonian Astrophysical Observatory, Cambridge, Massachusetts 02138.

0028-0836/83/160661-02$01.00