Number theory

Geometry finds factors faster

Ian Stewart

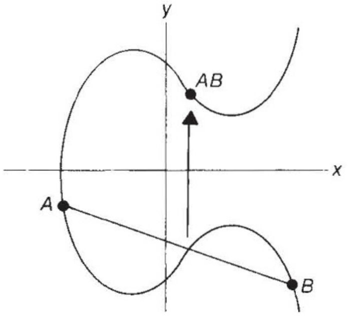
EVERY whole number can, in theory, be resolved into prime factors. In practice the process may take longer than the lifetime of the Universe. The obvious method, trial division by all primes up to the square root, is hopelessly inefficient. Its execution time grows so rapidly that improvements of a factor of, say, 100 in computer speeds will add only a few digits to the size of numbers that can be dealt with. To factorize an arbitrary 250-digit number — that is, one without special features that make it easy to factorize — is currently out of the question.

On the other hand, nobody has ever proved that prime factorization really must be as hard as it seems to be. Efficient and effective methods have not been ruled out. A new method, devised by Hendrik Lenstra of the University of Amsterdam and based on deep ideas from algebraic geometry and number theory, points to a new direction for attack (*Factoring Integers with Elliptic Curves,* Mathematical Sciences Research Institute preprint, Berkeley, 1986). The problem is of practical importance because of its relation to public-key cryptosystems — methods, hoped to be 'unbreakable', for putting messages into code. If a fast-factor algorithm exists, some of these methods will be breakable. The problem also has intrinsic mathematical interest as one of the most basic questions in number theory.

The objective is an algorithm: a prescribed procedure, involving no guesswork, and guaranteed either to produce a factor or to show that the number is prime. The efficiency of an algorithm is measured by the way its worst-case 'running time' grows with the number n of digits of the number being factorized. The running time is usually defined as the number of arithmetical operations ($+,\times$ and so on) involved, and only a relatively crude estimate is sought. A 'good' algorithm runs in polynomial time, growing no faster than some fixed power of n; a bad one runs in exponential time, growing as the nth power of some constant.

For an n-digit number of size roughly 10^n, trial division requires about $10^{n/2}$ trials. Even at one arithmetic operation per trial (which is far too low an estimate) this has exponential growth, hence is inefficient. In contrast, the euclidean algorithm for finding the least common multiple (l.c.m.) of two n-digit numbers takes about $5n$ steps. So this runs in polynomial time and is highly efficient.

To illustrate the alternatives to trial division, I will describe Pollard's $p-1$ method (see Riesel, H. *Prime Numbers and Computer Methods for Factorization,* Birkhäuser, Boston, 1985). This method starts with a number N and looks for prime factors p such that $p-1$ has only 'small' prime divisors. It is based on a number-theoretic fact: if $p-1$ divides a number Q and p does not divide Q then p divides a^Q-1 for any a not divisible by p. Then the l.c.m. of N and a^Q-1 is divisible by p, and this can be found rapidly by the euclidean algorithm. In practical implementations a standard series of Qs is defined and stored in the computer: for example, Q = l.c.m.$(1,2,\ldots,r)$ for $r = 1,2,3,\ldots$ up to some predetermined limit. As an example, the method has been used to find the factor p=2670091735108484737 of $3^{136}+1$. Although p is large, $p-1$ has the factorization $2^7.3^2.7^2.17^2.19.569.631.23993$, and the primes involved there are all small.



The group law on an elliptic curve. Given two points A and B, form the line joining them. This cuts the curve in a third point. Reflect that point in the horizontal (y) axis to get the point AB, which is the 'product' of the original points A and B.

The key to Lenstra's method is to view Pollard's algorithm in more abstract terms. Suppose that p is a prime. If any two of the set of numbers $1,2,\ldots,p-1$ are multiplied together modulo p (that is, the remainder is taken on dividing the product by p) then another number in that set is obtained. The set is said to form a group under multiplication modulo p. Pollard's method can be seen as exploiting the structure of this group. Lenstra's method is obtained from Pollard's by replacing the group by a more subtle one: the group of points on an elliptic curve.

Elliptic curves have been studied by number-theorists for about a century; not for applications to prime factorization, but because of their intrinsic mathematical beauty and interest. They are curves defined by an equation of the form $y^2 = x^3+ax+b$, for constants a and b. Associated with any such curve is a geometric multiplication law. Given any two points A and B on the curve, draw the line between them (see figure). Because the curve has an equation of degree 3 this line meets the curve at a third point. Multiply the y-coordinate of this third point by -1: because of the term y^2 in the equation, the result is still a point on the curve. Call it the 'product' AB of the first two points. The surprise is that this product obeys sensible algebraic laws: the points on the curve form a group.

In Lenstra's algorithm the coordinates x and y are taken to be integers modulo N, where N is the number to be factorized. If a single elliptic curve is used the method is much like Pollard's. However, the number $p-1$ that occurs in Pollard's method is replaced by the number $p-t$ where t depends on the choice of elliptic curve. Different curves give different ts, so there is a whole range of possible numbers $p-t$. As long as just one of these has small divisors, the method will find a factor.

The algorithm therefore starts by choosing some elliptic curve and seeking a factor by a generalized version of Pollard's method. If this fails, it does something that is not available in the original Pollard method: it tries another elliptic curve. Provided there is a reasonably dense set of numbers near p that are a product of small primes, the method will find a factor rapidly. The precise running time is rather complicated, and its proof depends on a plausible but unproved conjecture on this density. Other known methods have a similar conjectured running time, but they lack one important feature of Lenstra's method: the running time depends on the size of the prime factors of N.

Until very recently nobody had expected there to be any connection between elliptic curves and prime factorization. Only with hindsight is the connection clear. Although Lenstra's method may seem complicated, it is a natural generalization of Pollard's method. Perhaps even more efficient primality tests lurk unsuspected among the discoveries of number theorists. If so, some deep and abstract mathematics will take on a new, practical guise. Computer scientists working on algorithms for factorization would be well advised to brush up on their number theory. □

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

Erratum

IN the article 'Melting and the surface' by Robert Cahn (*Nature* **323**, 668; 1986) a sentence in the sixth paragraph was omitted. The second half of the paragraph should have read: "The melting temperature of argon at atmospheric pressure is 84 K, but allowing for the pressure in the bubbles (estimated from the measured anomalously small lattice parameter of the argon) it should be about 250 K. In fact, the diffraction pattern of solid argon is detectable up to 730 K, that is, a metastable superheating of 480 K!"