Making Factoring Faster

A new method will significantly cut factoring times for most numbers, and will also put a split in the factoring community

The Dutch mathematician Hendrik Lenstra recently announced his discovery of a new factoring method that has surprised and delighted the mathematical community by its simplicity and cleverness. The method promises to greatly speed up the factoring of many numbers and connects two seemingly unrelated fields of mathematics.

Mathematicians have tried to factor large numbers since the time of the ancient Greeks. It is a process akin to breaking down a molecule into atoms; only in the case of factoring, the molecule is a large number and the atoms are the primes which, multiplied together, give the number as their product. The brute force way of factoring would be to divide the number by each prime less than its square root. Those primes that divided evenly would be the factors. But this method is far too inefficient when the number to be factored is large. The 58-digit number $2^{193} - 1$, for example, would take 50 billion years to factor in this way, even if the factoring were done by a computer that performed a billion divisions a second. But a group of researchers at Sandia Laboratories headed by Gus Simmons factored that number in half an hour with their more indirect methods, and Lenstra's method promises to cut the time further still.

But Lenstra's method is limited. It is very fast for numbers whose prime factors are of different sizes. For numbers whose prime factors are approximately equal in size, however, the new algorithm is only about as fast as the best existing methods.

Because of this limitation, Lenstra's method is expected to alter the sociology of the factoring community, splitting the pure from the applied factorers. Until recently, nearly all factorers were pure. Most mathematicians who were interested in factoring were motivated simply because the numbers are there, because factoring is a challenge. They built up lists of "wanted" and "most wanted" numbers, which were numbers that had resisted the best efforts of mathematicians who tried to factor them. As they got better at factoring, they gradually knocked off one number after another from their list. These mathematicians, says Carl Pomerance of the University of Georgia in Athens, are "like stamp collectors who try to fill in missing gaps in their collections."

In contrast to these mathematicians, there is now a group that factors because factoring is related to cryptography. Several cryptographic schemes developed in the past decade depend for their security on the fact that factoring is hard. Because of these codes, the National Security Agency is supporting factoring research and has even hired at least one academic factoring expert, Marvin Wunderlich, to work full time on factoring with a parallel processing computer. Simmons' group is also concentrating on factoring at the request of the Defense Department.

Factoring in order to break one of the new codes, however, is a very particular type of factoring. To break these codes, it is necessary to factor a large number. But these large numbers are purposely cooked up; they are not, in a sense, naturally occurring numbers that would be expected to have both small and large primes as factors. Instead, they are composed of two prime factors of approximately equal size, which means that Lenstra's method will be no better than the methods already at hand. For that reason, says Pomerance, "Lenstra's algorithm will put a split in the factoring community."

> Lenstra's method represents "the first time 20th-century mathematics has been used for factoring."

But independent of its immediate practical consequences, mathematicians agree that the algorithm itself is, as Andrew Odlyzko of AT&T Bell Laboratories puts it, "very exciting." In addition, says A. Oliver Atkin of the University of Illinois at Chicago, Lenstra's method represents "the first time twentieth century mathematics has been used for factoring. The ideas for the other factoring methods are basically due to Gauss [the well-known 18th-century mathematician]. With Lenstra's algorithm, there is really quite deep and potent modern mathematics being used, which I think is quite significant."

Lenstra uses mathematical objects, called elliptic curves, to elicit information about a number's factors by working solely with the number to be factored. The idea is that since the number is a product of its factors, you implicitly are working with the factors when you work with the number. This is not an entirely new idea. In fact, a factoring scheme devised by the English mathematician J. Pollard, called the Pollard rho method, does the same sort of thing, only using quadratic functions rather than elliptic curves. But elliptic curves, says Simmons, "are a more powerful mathematical tool than quadratic functions and that's the reason for Lenstra's increased efficiency."

To mathematicians, the scheme seems beautiful in its simplicity and so clear that, says Odlyzko, "It's surprising that someone hasn't thought of it before." After all, Odlyzko notes, thousands of mathematicians are experts on algebraic curves.

But now that the door has been opened, it is possible that mathematicians may find other sorts of functions useful for factoring. "It's a neat notion," says Simmons. "Undoubtedly, there are many other classes of functions that can be exploited. The thing I believe Lenstra has done is to make people aware that other functions can be used. Before this, no one ever thought of using functions other than quadratics."

Still, although Lenstra's method makes at least some factoring much easier, mathematicians are left with the question of whether factoring is intrinsically a hard problem or whether there is some as yet undiscovered method that will make it easy. Even with the new algorithm, Pomerance remarks, "the big breakthrough in factoring hasn't come yet. The point is that until someone either proves or comes up with a convincing reason why factoring has to be hard, you have to wonder. Maybe 10 years from now, people won't be talking about factoring because it will be easy to do."—GINA KOLATA