A curving path toward faster factoring

The mathematical grapevine is buzzing with reports of a newly invented method for factoring large numbers. At the center of this excitement is a one-page summary sent out last month by Dutch mathematician Hendrik W. Lenstra Jr. of the University of Amsterdam. Lenstra's new factoring algorithm, in certain cases, may turn out to be faster than any of the general-purpose factoring methods now in use.

"It's a really beautiful idea," says Andrew M. Odlyzko of AT&T Bell Laboratories in Murray Hill, N.J., who was one of the first to hear of Lenstra's achievement. "Like most great ideas, it's extremely simple. For people with the right mathematical background, it takes literally two minutes to describe."

News of Lenstra's work has spread quickly. Several mathematicians are already writing computer programs to implement the method while others are tinkering with its steps or probing its implications.

"It's extremely straightforward to program," says Duncan A. Buell of Louisiana State University in Baton Rouge. Buell wrote his version of the Lenstra algorithm in the computer language C, requiring only about 250 lines for his program.

The key new feature in Lenstra's method is the use of elliptic curves: equations of the form $y^2 = x^3 + ax + b$, where values for a and b are chosen randomly. Lenstra started learning about these curves a year ago. Combined with his long-standing interest in primality testing (determining whether a number is evenly divisible only by one and itself [SN: 3/6/82, p. 158]) and in factorization of integers (finding which prime numbers when multiplied together produce a given composite number), the result was a new factoring algorithm.

"There was an element of coincidence in the convergence of these ideas," says Odlyzko. "Things somehow came together and clicked."

Lenstra's method works best when the number to be factored turns out to be the product of three or more prime numbers or the product of two primes that are far apart in value. This makes Lenstra's method attractive for factoring numbers drawn from a table of "most-wanted factorizations"—a list of particularly difficult numbers to factor (SN: 1/14/84, p. 20). These numbers come up in number theory and other types of mathematics research.

"If two factors differ greatly in size, then Lenstra's new algorithm can buy a great improvement in running time," says Gustavus J. Simmons of the Sandia National Laboratories in Albuquerque, N.M. Simmons heads the Sandia group that presently holds the record for factoring the longest "hard" number — 71 decimal digits—using a general-purpose factoring method (SN: 3/17/84, p. 171).

How big the improvement will be depends on how well Lenstra's algorithm runs when it is written out for a computer. "You have to test these things," says Hugh C. Williams of the University of Manitoba in Winnipeg. "It's one thing to say theoretically what it should do and quite another matter to discover, when you put it on a machine, just how fast it actually goes. But it deserves to be looked at."

So far, Lenstra's algorithm doesn't threaten the security of cryptosystems that depend on the difficulty of factoring numbers. These schemes often involve the product of two primes, but the primes can be chosen so that they are relatively close together in value (SN: 11/24/84, p. 330). For factoring such composite numbers, Lenstra's algorithm appears to be no better than the "quadratic sieve" method, invented by Carl Pomerance of the University of Georgia in Athens and currently the fastest general-purpose factoring method.

"But it's a brand new idea," says Pomerance. "Maybe we'll find some variation of it that will make it competitive with the things that we have now or even make it much better." He adds, "With new algorithms coming along, it's hard to count on the security of cryptosystems. Who's to say that someone can't come up with a new idea that's going to work fantastically?"

—I. Peterson

Migma: An approach to neutron-free fusion

Nuclear fusion, according to its proponents, will be the ultimate cheap-fuel energy source, an answer to the world's energy problems—if they can make it work. Although significant progress has been made in recent years, development has been much slower than the first proponents of fusion hoped when they began 40 years ago.

About 12 years ago, at a meeting of the American Physical Society, physicist Bogdan Maglich presented an unorthodox method of approaching fusion. At the time, other physicists were quite skeptical. Now, in the Feb. 25 Physical Review Letters, Maglich and co-workers report a significant achievement in what they call "aneutronic fusion—"a word so new it is not yet in any dictionary." Other physicists are still somewhat reserved.

In principle, "conventional" magnetic fusion experiments involve the formation of a plasma (consisting of atomic nuclei and electrons) by ionizing a gas. This plasma is then confined by a suitably shaped magnetic field and heated to a temperature at which significant numbers of fusions occur. In practice, magnetic fields do not confine very well. Instabilities in the plasma's behavior tend to build up until they enable the plasma to break out of confinement. So the race is to hold the plasma at least long enough for a useful number of fusions to occur.

In conventional experiments the plasma is heated so that the nuclei gain enough energy to overcome the electrical repulsion between them and so are able to fuse. In Maglich's scheme, which he calls a migma (from the Greek word for mixture), the nuclei gain energy not by heating but by being accelerated in a linear accelerator. In the current experiment, deuterons — the nuclei of deuterium, an isotope of hydrogen—come out of the accelerator with 0.7 million electron-volts energy, the equivalent of heating to 7 billion kelvins. They also have a directed motion rather than the random motions of a thermally energized plasma. Therefore, a magnetic field can be set up in the migma cell, as they call the vessel they use, that forces the nuclei into self-intersecting orbits that form a kind of rosette around the center of the field. Orbits of this kind provide many opportunities for nuclei to encounter each other and fuse.

The confinement time in this experiment, 20 seconds, was less than the 60 seconds of the DCX-1 device, a conventional experiment chosen for comparison. But the triple product of energy, confinement time and density—the three critical parameters—is 10 to 20 times that of DCX-1, and none of the typical instabilities formed.

The word "aneutronic" comes from the reaction they ultimately hope to use, in which hydrogen and lithium fuse to helium with two protons left over. The easiest reaction (and the goal of most conventional experiments) is deuterium and tritium yield helium plus a leftover neutron. The neutron is a penetrating and potentially damaging particle. The protons from the lithium reaction, being electrically charged, are easy to capture and not damaging. Energy is harvested from these leftover particles and that, too, is easier with charged particles.

According to James Nering of United Sciences, Inc., in Princeton, N.J., the organization Maglich and co-workers formed to do these migma experiments, the present experiment used deuterons because they make measuring and following the action easier.

In 1973, when Maglich first presented the idea, the physics community reacted so skeptically that he could not get funds from the Department of Energy, which funds most of the U.S. fusion program. He did, however, obtain $20 million in private funds from sources in Japan, Switzerland, Saudi Arabia and the United States. Now, according to an announcement by United Sciences, money is included in the Defense Appropriations Bill for fiscal year 1985 for a study of migma's space applications.

—D.E. Thomsen