Cracking the 100-digit factoring barrier

After 26 days of computation, the final digits fell into place last week. By piecing together the output from dozens of computers in the United States, Australia and the Netherlands, a team of computer scientists and mathematicians successfully split a particularly tough 100-digit number into its two prime-number factors, a 41-digit number and a 60-digit number.

"This represents the 4-minute mile of factoring," says mathematician Ronald L. Graham of AT&T Bell Laboratories in Murray Hill, N.J. Only four years ago, the best anyone could do using a general-purpose factoring scheme was to break a "hard" 71-digit number (one with no small factors) into its prime-number components (SN: 1/14/84, p.20). Factoring a 100-digit number seemed beyond reach – at least until the beginning of the next decade.

The present achievement also highlights the potential vulnerability of cryptographic security systems based on the assumption that factoring large numbers is difficult. "Most people 10 years ago thought that 100 decimal digits would be safe for a long time," Graham says.

In principle, factoring is straightforward. Simply divide the number to be factored by smaller numbers, looking for those that leave no remainder. However, this procedure consumes tremendous amounts of computer time. Even on the fastest available computers, using such a method to factor a 100-digit number having no small factors would take longer than the age of the universe.

For large numbers, more indirect factoring methods must be used. One popular strategy is known as the "quadratic sieve," invented in 1981 by Carl Pomerance of the University of Georgia in Athens. The idea behind the quadratic sieve is to concentrate on the simpler task of factoring a large collection of specially selected small numbers, each of which is considerably smaller than the number to be factored. The information from those smaller problems can then be pieced together to factor the original number.

To accomplish the 100-digit factorization, Arjen K. Lenstra of the University of Chicago and Mark S. Manasse of the Digital Equipment Corp. (DEC) Systems Research Center in Palo Alto, Calif., used a form of the quadratic-sieve method allowing different computers to work independently on small pieces of the problem. They developed a program capable of running on a variety of computers, from supercomputers to multiprocessor workstations, and got the help of about a dozen collaborators in the United States and elsewhere. The program was designed to run whenever local computers happened to be idle, filling in computer time that would otherwise be wasted. The results were funneled by electronic mail to DEC for the final computation.

The 100-digit number chosen for the record-breaking effort came from a specially compiled list of "wanted" factorizations. The number is the 100-digit remainder after dividing $11^{104}+1$ by the numbers 2, 17 and 6,304,673.

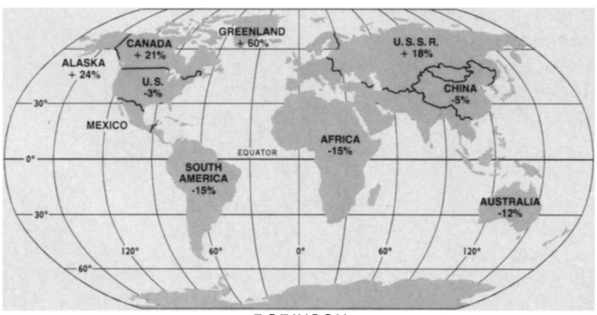
The researchers are now gathering the necessary data to factor a 102-digit number, which could take about a month. With the participation of several thousand computers, it may be possible to factor a 120-digit number, says Manasse.

Pomerance favors an approach that depends less on large networks of expensive computers and more on low-cost, custom-built machines for factoring large numbers. He and a colleague are building a $25,000 machine that should be able to handle 100-digit numbers (SN: 1/23/88, p.62). Meanwhile, another colleague, W.R. (Red) Alford, is using 100 personal computers – the simplest available – to factor a 95-digit number. Collecting the data for the final step took about four months.

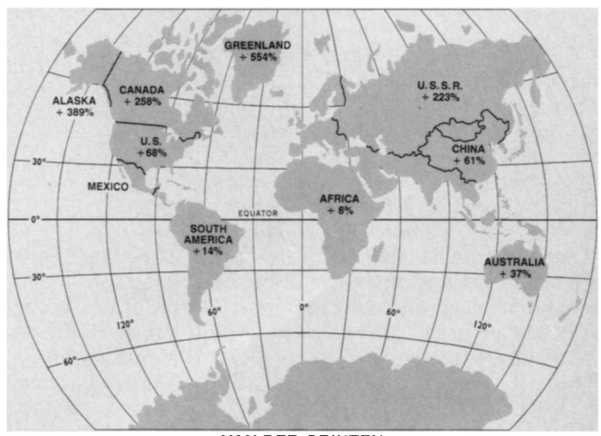
"With a million [personal computers], you could factor a 145-digit number within a reasonable amount of time," Pomerance says. Even a 200-digit number would be accessible, if someone were willing to spend the money and could build enough factoring machines.

Factoring has been moving ahead a lot faster than people had thought possible, says Gustavus J. Simmons of the Sandia National Laboratories in Albuquerque, N.M. In 1978, factoring was thought to be so difficult that government experts were willing to base the security of an extremely sensitive nuclear facility on the difficulty of factoring a 103-digit number. Now such a number can be factored in roughly twice the time it took Lenstra and Manasse to factor a 100-digit number. Says Simmons, "That's a very dramatic indication of what's happened over those 10 years." – *I. Peterson*

The world according to National Geographic



ROBINSON



VAN DER GRINTEN

National Geographic Society

The National Geographic Society has traded in its time-worn world map for one that portrays the Earth more realistically. The society's new official map (left), developed by a geographer from the University of Wisconsin-Madison, more closely approximates the globe than does any other flat, continuous map of the world, says John B. Garver Jr., chief cartographer for the society in Washington, D.C.

Arthur H. Robinson, creator of the newly adopted map, says trying to depict the world precisely in two dimensions – peeling the "skin" off the globe and forcing it to lie flat – proves mathematically impossible. But the Robinson map eliminates most of the high-latitude distortion of the Van der Grinten projection (right), which National Geographic first selected for its world map in 1922. The distortion percentages shown above indicate how close to true size the Earth's land areas appear on each map.