RSA-129 and Its Factors

1143816257578888676692357799761466120102182967212423625625618429357 \
0693524573389783059712356395870505898907514759929002687954354 1
=
3490529510847650949147849619903898133417764638493387843990820577
X
32769132993266709549961988190834461413177642967992942539798288533

Bellcore's MasPar supercomputer to arrive at the factors: two primes of 65 and 64 digits.

In explaining the significance of the Bellcore feat, Rivest says that "assessing the difficulty of factoring these large numbers has become very important for the security of the national information infrastructure." Or as Lenstra puts it, "If we can do it, someone else can do it." The factoring of RSA-129 does not, however, mean the RSA code is obsolete. Even now, Rivest says, few users rely on numbers as small as RSA-129. "They're using numbers which are considerably larger, and this accomplishment will encourage them to use numbers larger yet." Numbers as long as 200 digits are predicted to be 7000 times more difficult to factor, and a 400-digit number may be 300 billion times more difficult.

But as in an arms race, no escalation is likely to go unmatched for long. At the same press conference where Lenstra and company announced the defeat of RSA-129, he promised a "surprise" for the next factoring feat. He hinted at a new, faster algorithm—and perhaps a test involving a number with quite a few more digits than 129.

–Gary Taubes

NUCLEAR RESEARCH

Physicists Find a Double Dose of Magic

DARMSTADT—Magic seems to abound at Germany's heavy-ion accelerator laboratory, GSI. Researchers there are the acknowledged masters of the black art of creating new heavy elements by smashing smaller nuclei together—they are credited with discovering the three heaviest elements currently known—and they also bring a magic touch to other regions of the periodic table. So much was evident last week, when GSI scientists announced that they had created the isotope tin-100, a so-called "doubly magic" nucleus that had been predicted by theories of nuclear structure but never before found.

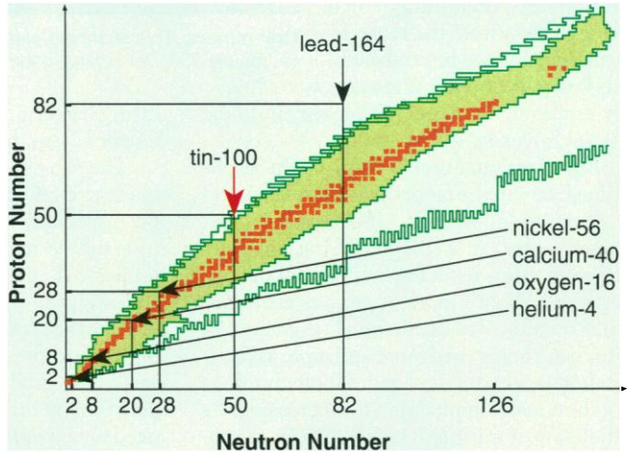
Nuclear physicists are acclaiming the achievement, which other laboratories had also been pursuing. "There was talk 15 years ago about trying to make tin-100 nuclei, but at that time many people thought it would be impossible to do," says Brad Sherrill of the National Superconducting Cyclotron Laboratory at Michigan State University (MSU). Tin-100, which has equal numbers of protons and neutrons, lies far from the range of stable elements; in stable nuclei of this size, a large majority of neutrons ordinarily counteracts the electromagnetic repulsion of the charged protons, which would otherwise break the nucleus apart. But physicists eager to test nuclear theories had a strong incentive to try to make tin-100. According to current theories, the isotope's complement of protons and neutrons constitute "magic numbers," which should make it—relatively speaking—far more stable than nuclei with slightly different numbers. By making and studying the isotope, physicists could test the theories' predictions.

Indeed, the GSI team, led by Jörg Friese from Munich's Technical University and Gottfried Münzenberg from GSI, now estimates that compared to nearby isotopes, which have lifetimes in the range of less than a millisecond, tin-100 is a virtual Methuselah, surviving for several seconds. More detailed studies of the new isotope, says Sherrill, should help researchers test fine points of the current nuclear theory, which holds that protons and neutrons occupy a series of spherical "shells." When a nucleus contains full shells of protons or neutrons (2, 8, 20, 28, 50, or 82 of them, for example), it gains extra stability and is said to have a magic number. Doubly magic nuclei have magic numbers of both protons and neutrons.

Doubly magic nuclei serve as prime testing grounds for this picture because of their simplicity. As soon as a nucleus has more than a few protons and neutrons, the equations governing its structure ordinarily become impossibly complicated, and it becomes very difficult for theorists to predict its properties accurately. Full shells of protons and neutrons simplify the equations. Tin-100, however, has an added advantage: equal numbers of protons and neutrons, a symmetry that improves the situation even further. "A doubly magic nucleus like tin-100 is a nice simple system," says Sherrill. So far, physicists have studied four other doubly magic nuclei with equal numbers of protons and neutrons, but all are smaller than tin-100. The new member of this select group will help researchers prove the validity of the theory for larger nuclei.

But such studies will have to wait until the GSI group can scale up production of the isotope. The team made tin-100 by smashing xenon-124 ions against a target of beryllium, then analyzing the charge and mass of the debris in search of the isotope. Despite the relatively long half-life of tin-100 nuclei, they are very hard to make because of the delicate balance of forces: After such a violent collision, the chance that the nuclear debris will settle into neat spherical shells before electromagnetic repulsion breaks it apart is slim. In fact, the GSI team had to bombard the target with 1.7×10^{13} xenon ions to produce just seven tin-100 nuclei.

The other groups also pursuing the isotope are further behind. The disappointment may be particularly sharp for a group at the French heavy-ion accelerator GANIL at Caen. They have produced various tin isotopes including tin-101, and they finished another run on the very day the Darmstadt team announced its findings. Says group leader Marek Lewitowicz: "From the data we gathered, we have a 90% chance of also identifying tin-100 at GANIL."



Isotope table. Doubly magic nuclei with equal protons and neutrons.

The race that has just ended at Darmstadt may be the last of its kind. The next doubly magic nucleus with equal protons and neutrons would be lead-164, which is so far outside the range of stable nuclei that even a double dose of magic will not preserve it. "No one suspects that that nucleus will be possible," says Sherrill.

–Michael Simm and Daniel Clery

Michael Simm is a science writer in Bonn.