Major-league sieving for faster factoring

Factoring a large number to determine its prime-number components typically takes a long time – so much time on even the fastest available computers that an important method of encrypting digital information can count on the difficulty of factoring for maintaining security. However, factoring techniques have improved sufficiently in recent years to bring numbers of more than 100 digits easily within range.

Last week, a team of researchers using a relatively new method known as the number field sieve succeeded in factoring a 116-digit number. This sets a record for the largest number yet factored by the general version of the technique.

More important, this factorization required less computer time than comparable 116-digit factorizations using a rival technique known as the quadratic sieve, says Arjen K. Lenstra of Bell Communications Research (Bellcore) in Morristown, N.J. Over the last few years, the quadratic sieve has been the favored technique for cracking large composite numbers (SN: 5/7/94, p.292).

Lenstra worked with Bruce Dodson of Lehigh University in Bethlehem, Pa., and Peter L. Montgomery of the Centrum voor Wiskunde en Informatica (CWI) in Amsterdam, the Netherlands, to set the new record.

Invented in 1988 by John M. Pollard of Reading, England, the number field sieve looked promising from the beginning, especially for factoring numbers of a special form. But it wasn't clear how practical and efficient the method would be for factoring large numbers in general.

In 1990, Lenstra and a colleague used the method to factor a 155-digit Fermat number, $2^m + 1$, where $m = 2^9$ (SN: 6/23/90, p.389). Meanwhile, mathematicians developed a version of the number field sieve that can be used for factoring any composite number.

Last month, researchers at Oregon State University in Corvallis, Reed College in Portland, Ore., and CWI used improved versions of the number field sieve to factor a 162-digit "special" number and a 105-digit "general" number.

Lenstra and his colleagues topped the 105-digit record. They required a month of computer time, using about 100 workstations at Lehigh for the initial steps and a MasPar MP-1 computer at Bellcore for the final stage, to complete the factorization.

Along the way, the researchers discovered a curious, unexpected speedup in certain steps. They can now take advantage of this behavior to achieve even faster factoring. "We've been working on it for years," Lenstra says. "Now it's becoming practical." – *I. Peterson*

Babies' brains charge up to speech sounds

In the first study of its kind, scientists have charted electrical activity in infants' brains and linked the pulses to a baby's ability to recognize simple syllables. The ebb and flow of cerebral currents suggests that babies discern a change from one syllable to another in less than one-half second, assert psychologists Ghislaine Dehaene-Lambertz and Stanislas Dehaene at the University of Oregon in Eugene.

Separate electrical bursts, which reflect steps taken by the brain to make sense of the sound just heard, appear in infants by age 2 months, the researchers report in the July 28 NATURE.

Prior investigations have found that 2-month-old babies distinguish speech sounds employed in many languages, an ability that dwindles as youngsters learn a native tongue (SN: 2/8/92, p.91).

The Oregon investigators – who are also affiliated with the National Center for Scientific Research in Paris – placed a net holding 58 electrodes embedded in wet sponges around the heads of 16 infants, all between 2 and 3 months old. While wearing this gear, youngsters heard a series of four identical syllables (either "ba" or "ga"), followed on some trials by the same syllable and on others by the alternative syllable.

For each child, the researchers calculated overall brain electrical activity across an average of 51 trials.

An initial electrical increase in the brain's temporal lobe peaked about one-fifth of a second after the first presentation of a syllable. Subsequent sounds in a series generated similar, weaker rises in temporal activity. The researchers speculate that these peaks reflect processing of basic acoustic information.

A second discharge peaked one-fifth of a second after the first and also declined following the initial syllable presentation. However, that electrical burst returned to its original level when a different syllable concluded a trial, suggesting that the second peak resulted from brain processes devoted specifically to speech sounds, the scientists assert.

Finally, about one-half second after a second peak sparked by a new syllable, frontal lobe electrical activity dropped markedly. Brain areas that detect unexpected visual and acoustic information probably generated this temporary slump, the psychologists argue.

The first two electrical peaks reached slightly higher levels on the left side of the brain, but the strong left-hemisphere advantage for language typical of most adults did not emerge. – *B. Bower*

Fish dishes may catch on among smokers

Dining on fish on a regular basis may serve smokers well, researchers suggest.

A study of 4,928 former smokers and 4,032 smokers, all age 45 to 64, indicates that the more fish the volunteers ate, the lower their likelihood of having lung disease. Dark-meat fish, such as salmon and bluefish, have the highest concentrations of the protective n-3 polyunsaturated fatty acids, scientists report in the July 28 NEW ENGLAND JOURNAL OF MEDICINE.

Compared to participants who reported rarely eating fish, the volunteers who ate seafood most often – about four times a week – had half the incidence of chronic obstructive pulmonary disease (COPD), says coauthor Eyal Shahar of the University of Minnesota School of Public Health in Minneapolis. The 1,000 volunteers with COPD had at least one of the following conditions: chronic bronchitis, emphysema, or reduced lung function, as measured by a spirometer.

Although the study does not prove that eating fish protected the smokers, it makes a good case for more research on the relationship between fish consumption and COPD, says Shahar. In epidemiological research, he notes, "it's almost surprising to find such a strong correlation as we have."

Gary W. Hunninghake of the University of Iowa College of Medicine in Iowa City agrees. He describes the findings as "highly suggestive" of an association between how much fish smokers eat and their risk of COPD.

However, the investigators detected no such correlation for the 1,674 black volunteers. "We are uncertain why," they write, but they suggest that there may have been insufficient data on blacks to find an association.

Other research boosts the argument that fish may help protect against the damage cigarette smoking inflicts, says Shahar. For instance, scientists know that smoking can lead to the chronic inflammation of the lungs that characterizes COPD, and studies have shown that large doses of n-3 fatty acids interfere with the body's inflammatory response.

Nonsmokers who suffer from occasional bouts of bronchitis need not rush to the fishmonger because of this study, Shahar says. In fact, the findings have "no implication for nonsmokers," he contends, adding that their bronchitis differs significantly from that of smokers.

Nor do these findings let fish-loving smokers off the hook. "I don't want this [research] to cause people to say, 'Yea! I can smoke and eat fish.' This is my worst nightmare," says Shahar, whose father died of smoking-related lung cancer.

– *T. Adler*