Biomedicine

Breast cancer allayed by mastectomy

Preventive mastectomies protect against breast cancer in many women with a high inherited risk of getting the disease, a 33-year study shows.

A study of 214 women at high risk of breast cancer who had undergone preventive mastectomies at the Mayo Clinic in Rochester, Minn., showed that only three women—1.4 percent—subsequently developed breast cancer. Two died. The operations were performed between 1960 and 1993.

Among 403 sisters of members of this group who didn't undergo mastectomy, 156—nearly 39 percent—had breast cancer at some point. Of these patients, 90 died from the cancer. The study was published in the Jan. 14 NEW ENGLAND JOURNAL OF MEDICINE.

The researchers evaluated a woman's risk of breast cancer by looking at the incidence of breast and ovarian malignancies among her close and distant relatives.

The study provides data that women at risk can use to make a decision about surgery, says study coauthor Lynn C. Hartmann, a medical oncologist at Mayo. "It's my sense as a clinician that high-risk women are quite well informed and may have already made a decision [about surgery] before I see them," she says. However, "at first, women tend to overestimate their risk."

Traditional preventive mastectomy, called subcutaneous mastectomy, removes breast tissue but retains the nipples. Mayo surgeons used that technique in all the surgeries in the study. An alternative today, called total mastectomy, couples removal of more breast tissue with better breast reconstruction, Hartmann says. "Most people would do a total mastectomy today, if they were going this direction," she says.

Women in at-risk families now have genetic testing with which to ascertain their risk, she adds, an advantage most of the women in this test didn't have. —*N.S.*

AZT shows no ill effects on babies

About 5 years ago, pregnant women infected with HIV began getting the drug AZT to limit transmission of the AIDS virus to their fetuses. This practice continues today, although doctors augment AZT with other drugs to suppress the virus.

The current drug combination limits to about 5 percent the frequency of HIV transmission to infants. But because tests in animals show that AZT exposure might cause cancer, researchers have worried that AZT might harm the children.

A new study in babies up to age 4 suggests that it doesn't. Scientists at the National Institute of Allergy and Infectious Diseases (NIAID) in Bethesda, Md., compared 122 HIV-negative babies who had been exposed to AZT both in the womb and during their first 6 weeks after birth with 112 healthy babies never exposed to AZT. They found no significant differences between the groups in physical growth, mental function, immune-system development, or heart function. Further tests showed no cancer in either group, and among children who received eye examinations, there was little difference, the researchers report in the Jan. 13 JOURNAL OF THE AMERICAN MEDICAL ASSOCIATION.

The scientists collected their data from dozens of pediatric clinics across the United States.

"It provides some reassurance to these women," says study coauthor Mary Culnane, a nurse and medical officer at NIAID. The findings offer "new and important information" for women who have to make a choice about using AZT, she says.

The infants were part of a study of HIV-infected mothers conducted prior to 1995, in which some received AZT and some received an inert substance, or placebo. When AZT's potent anti-HIV effects were realized, the placebo portion of the study was stopped and all participating mothers received AZT afterward. The infants examined in the new study were born HIV-free despite their mothers' infections. —*N.S.*

Mathematics

The scarcity of cluster primes

The distribution of primes—whole numbers evenly divisible only by themselves and 1—has long intrigued mathematicians. More than 2,000 years ago, Euclid proved there are infinitely many primes. Nonetheless, primes gradually become scarcer as the numbers get larger.

To gain insights into the somewhat irregular distribution of prime numbers, mathematicians have studied a variety of subsets of all primes. The so-called twin primes, for example, consist of pairs of consecutive prime numbers that differ by 2, such as 41 and 43. Whether there are infinitely many twin primes remains one of the major unsolved questions in number theory.

Cluster primes define another puzzling subset. For a prime number p to qualify as a cluster prime, every even number less than $p - 2$ must be the difference of two primes, both of which are less than or equal to p. For example, 11 is a cluster prime because each of the even numbers 2, 4, 6, and 8 can be written as a difference between two of the primes 2, 3, 5, 7, or 11. The first 23 primes greater than 2 are all cluster primes. The smallest noncluster prime is 97. In effect, the definition of a cluster prime encompasses a particular type of grouping among primes that mathematicians have found worthwhile investigating.

Mathematicians have observed that cluster primes become increasingly rare as primes get larger. New computations reveal that by the time the numbers reach 10 trillion, noncluster primes outnumber cluster primes by a ratio of about 325 to 1. In the January AMERICAN MATHEMATICAL MONTHLY, Richard Brecksmith and John L. Selfridge of Northern Illinois University in DeKalb and the late Paul Erdös report results suggesting that cluster primes are less numerous than twin primes. However, "we have no way of proving that either of these two collections is infinite," the mathematicians remark. —*I.P.*

Cracking a prime cryptosystem

Invented more than 20 years ago, the so-called RSA cryptosystem is widely used to provide privacy for electronic mail, ensure authenticity of digital data, and handle credit-card payments on the Internet. The system's security hinges on the observation that factoring numbers into their prime-number components becomes impractical for sufficiently large numbers.

No one has yet discovered an efficient recipe for factoring large numbers, and many mathematicians and computer scientists believe that no such method exists (SN: 5/7/94, p. 292). In the RSA scheme, the numbers involved typically have 309 decimal digits (1,024 bits).

The RSA cryptosystem has other potential vulnerabilities, however, and researchers have expended considerable effort to expose such weaknesses (SN: 10/3/98, p. 217). "At the moment, it appears that proper implementations [of RSA] can be trusted to provide security in the digital world," computer scientist Dan Boneh of Stanford University concludes in the February NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY.

One important, open question concerns whether cracking the RSA cryptosystem is, in fact, as hard as factoring. The specific mathematical procedure used for encrypting and decrypting data might contain a loophole that a malicious eavesdropper could exploit to intercept and decrypt a message without having to factor a large number.

Boneh and Ramarathnam Venkatesan of the Microsoft Corp. in Redmond, Wash., have recently uncovered mathematical evidence that, in certain cases, using techniques rooted in algebra to break the RSA cryptosystem may indeed be easier than factoring. Nonetheless, the result "does not point to any weakness of the system," the researchers contend. Though breaking may be easier than factoring, the time required to break the cryptosystem is still likely to be so long that the operation is impractical. —*I.P.*