All their suggestive properties indicate that primes are not randomly scattered among the integers, yet prime numbers, in their maddening perversity, defy all attempts aimed at putting them precisely in their places. To try to prove many conjectures about prime numbers, mathematicians therefore often must devise sneaky strategems to get at their prey indirectly. They fence in the unruly conjecture, first staking out a wide swath of territory before gradually closing in on it. The pursuers then draw the net tighter, taking in corners and cutting down boundaries while scrupulously checking for loopholes. Finally, if all goes well, the conjecture is trapped.

One such attempt is the continuing work on the Goldbach conjecture, which views prime numbers as the building blocks of other numbers. The Prussian mathematician Christian Goldbach suggested the idea in a letter to Euler in 1742. His claim, expressed in modern terms, is that every even number greater than 4 is the sum of two odd primes (that is, primes other than 2). The number 32, for instance, is the sum of 13 and 19. This proposition is now known as the "strong" Goldbach conjecture. The "weak" Goldbach conjecture holds that every odd number greater than 7 can be expressed as the sum of three odd primes. In both cases, the same prime number may be used more than once in a single sum.

Excerpts from Peterson, I. (1988). *The Mathematical Tourist*. New York, NY. W. H. Freeman and Company.

Various guesses about prime numbers, perhaps even the strong Goldbach conjecture, may truly turn out to be undecidable. Few mathematical fields other than number theory have so high a proportion of widely believed but unproved propositions. This doesn't mean that the conjectures are all likely to be false, but it implies that for some conjectures, an airtight case might not exist, despite the steady accumulation of persuasive evidence in its favor. Mathematical proofs require more than just overwhelming evidence.

Even so, the quest isn't hopeless. Near misses and proofs that confirm special cases or parts of conjectures hint that eventually techniques may be developed to handle the problems—although it could take centuries. That is far different from saying that a conjecture can never be proved, for a single breakthrough could put such suppositions as the number of twin primes suddenly within reach. Meanwhile, with the use of computers, specific knowledge about prime numbers is growing steadily, although considering the centuries of effort put in by numerous mathematicians, the theory of prime numbers still seems meager.

47

Success in the search for mammoth primes, which hide among composite numbers, requires a lot of patience, luck, and fortitude and takes some strategic planning using a few tools from number theory. The quarry are huge numbers such as $2^{44,497} - 1$. The question is whether this 13,395-digit mammoth, just one of an endless supply of candidates, is prime or composite.

Of course, big-prime hunters could stalk their game simply by writing out the number N and dividing into it, one by one, all the integers, starting with 2. If no integers divide into the target number evenly, N must be a prime. Going any further than the square root of N during the search is pointless because factors are always found in pairs. If N has a factor larger than the square root of N, then the factor's partner must be smaller. Using only odd numbers after division by 2 is another possible shortcut.

In the case of mammoth primes, however, the trial-division method proves to be hopelessly time-consuming. A computer able to carry out a billion trial divisions every second would take considerably longer than the current age of the universe to finish the job. Trial division works best for relatively small numbers, although even a 100-digit number is beyond reach unless it happens to have a small factor or a special structure.

The real trouble with trial division is that it provides more information than is required by the question of whether a number is prime. The method not only supplies the answer but also gives the factors of any number that happens to be composite. The idea, then, is to find techniques that pinpoint primality without at the same time finding factors. If a given number has no small factors, such techniques for testing primality are bound to be speedier than trial division and its variants.

48

A decade or so ago, an interest in factoring was the mark of an eccentric. Only a handful of number theorists cared to wrestle with lengthy strings of digits. This small, obscure group of mathematicians worked quietly, prying open large composite numbers to unlock their prime secrets. They reveled in the pure delight of calculation and in the pleasure of devising elegant algorithms to do their work. Like many ardent hunters, they even kept a list of "wanted" and "most wanted" targets *(see Figure 2.5)*.

Those mathematicians are still around, but they have been joined by a crowd of computer scientists and applied mathematicians eager to test their skills. Armed with advanced algorithms, sophisticated computers, and specialized calculating machines, the newcomers are rapidly changing the formerly sedate and sheltered world of factoring. In just a few years, successful factorizations of "hard" numbers have jumped from numbers with 50 decimal digits to those with more than 80. Now, the list of "most wanted" factorizations must be updated regularly.

Factoring is of considerable interest because the security of several important cryptographic systems depends on the difficulty of factoring numbers with 100 or more digits. Without doubt, compared with testing for primality, factoring is hard. It takes a day or so of supercomputer time to break an 80-digit number that happens to have no small factors. It would take only a few seconds, if that, to tell whether the number is a prime. Much current research is aimed at providing as sharp an estimate as possible of how hard factoring really is.

Excerpts from Peterson, I. (1988). *The Mathematical Tourist*. New York, NY. W. H. Freeman and Company.