an Article from SCIENTIFIC AMERICAN

DECEMBER, 1982 VOL. 247, NO. 6

The Search for Prime Numbers

Until recently the testing of a 100-digit number to determine whether it is prime or composite could have taken a century even with a large computer. Now it can be done in a minute

by Carl Pomerance

The prime numbers are the multiplicative building blocks of the number system. If a number is prime, there are no smaller natural numbers that can be multiplied to yield it as their product. The prime number 11, for example, cannot be broken down into smaller factors; only 1×11 is equal to 11. If a number is composite, on the other hand, it can be expressed as the product of two or more prime factors. The composite number 12 is equal to $2 \times 2 \times 3$. Every whole number larger than 1 is either a prime or the product of a unique set of primes. This fact, which was known to the ancient Greeks, is so central to the system of natural numbers that it is called the fundamental theorem of arithmetic.

How can one determine whether a number is prime or composite? The most straightforward way is to divide the number to be tested by the integers in sequence: 2, 3, 4 and so on. If any of the divisions comes out even (that is, leaves no remainder), the test number is composite and the divisor and the quotient are factors of the number. If all the integers up to the test number are tried and none of the divisions comes out even, the number is prime. Actually it is not necessary to continue up to the test number; the procedure can be stopped as soon as the trial divisor exceeds the square root of the test number. The reason is that factors are always found in pairs; if a number has a factor larger than the square root, it must also have one smaller.

Stopping the trial division at the square root can greatly speed up a test for primality, and there are other short cuts, such as deleting all the even trial divisors after 2. Nevertheless, the trial-division algorithm is utterly incapable of testing the largest primes known. Consider the 13,395-digit number $2^{44,497} - 1$, which was proved to be prime in 1979 by Harry L. Nelson and David Slowinski of the Lawrence Livermore Laboratory. If a computer were to carry out trial divisions at the rate of a million divisions per second, and if it were to stop once it reached the square root of the number, it would need $10^{6,684}$ years to finish the task.

The trouble with the trial-division method is that it does far more than is required: trial division not only decides whether a number is prime or composite but also gives factors of any composite number. Although there are methods of factoring that do not depend on trial division, none of them can factor an arbitrary number having a "mere" 100 digits in any reasonable time, even with a large computer. It turns out, however, that it is possible to determine whether or not a number is prime without necessarily finding any factors in case the number is composite. If the number has no small factors, such methods are almost invariably more efficient than the methods that give the factors. In the past two years a method has been developed that enables a computer to determine the primality of an arbitrary 100-digit number in about 40 seconds of running time.

The problem of testing for primality and the superficially related problem of factoring are classic problems in the theory of numbers, the branch of mathematics that deals with the properties of whole numbers. Number theory is rich in problems that are tantalizingly simple to state but notoriously difficult to solve. Number-theory problems having to do with primality have been a source of fascination to mathematicians at least since Euclid.

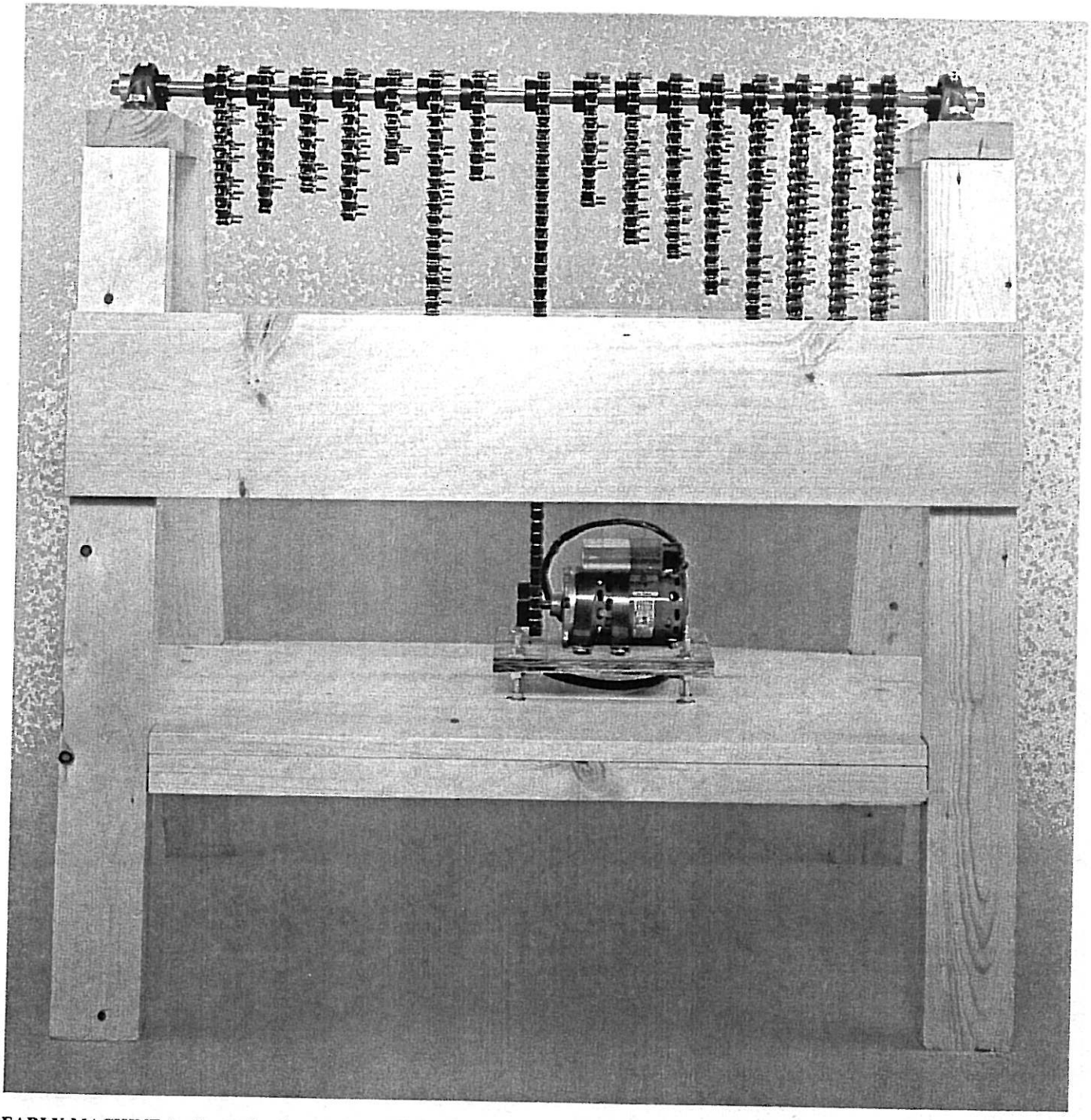
For example, there appear to be infinitely many prime twins, which are pairs of primes such as 17 and 19 that differ by 2, but the conjecture has not been proved. It is almost certainly true that there is always at least one prime between the squares of consecutive integers, but the statement also stands unproved. Christian Goldbach conjectured in 1742 that every even number after 2 is the sum of two primes; 32, for instance, is the sum of 13 and 19. Goldbach's conjecture too has resisted all attempts at proof, although in 1937 the Russian mathematician I. M. Vinogradov showed that all "large enough" odd numbers can be expressed as the sum of three primes. Vinogradov was not, however, able to state explicitly what is meant by the term "large enough."

A corollary of Vinogradov's theorem is that all large enough even numbers can be expressed as a sum of four primes; according to the theorem, it is always possible to represent the odd number that is three less than any large enough even number as a sum of three primes. The even number is then the sum of the three primes and the prime number 3. In 1966 the Chinese mathematician Chen Jing-run showed that all large enough even numbers can be expressed as the sum of a prime number and a number that is either prime or the product of two primes. Such approximations to Goldbach's conjecture are deep results in the sense that their proofs call for advanced mathematical analysis and are quite difficult.

There are also many statements about primes that can be proved by elementary methods, and many of the proofs are delightfully ingenious. For example, it was known by Euclid that the number of primes is infinite. The argument is indirect: it is assumed that the number of primes is finite, in which case there must be some largest prime, and from the assumption a contradiction is derived. Suppose the largest prime is p. Then consider the number N, defined as the product of all the prime numbers from 2 to p. The number $N + 1$ must be either prime or composite. $N + 1$ is greater than p, and so according to the original assumption it must be composite; otherwise it would be a prime larger than p. Since $N + 1$ is composite, the fundamental theorem of arithmetic implies that it has prime factors. Because of the way $N + 1$ was constructed, however, it leaves the remainder 1 when it is divided by any prime from 2 to p. Its prime factors (if it has any) must therefore be larger than p. Again the assumption that there is some largest prime leads to a contradiction, and so there can be no upper limit on the set of primes.

In a similar spirit it is easy to prove that consecutive primes can be as far apart as one might want. Consider the sequence of numbers $n! + 2$, $n! + 3$, $n! + 4, \ldots, n! + n$, where $n!$ (read n factorial) is the product of all the whole numbers from 1 to n. Note that $n! + 2$ is evenly divisible by 2, $n! + 3$ is evenly divisible by 3 and so on; finally, $n! + n$ is evenly divisible by n. Hence all $n - 1$ numbers in the sequence are composite. The sequence can be made as long as one likes simply by picking a large enough number n.

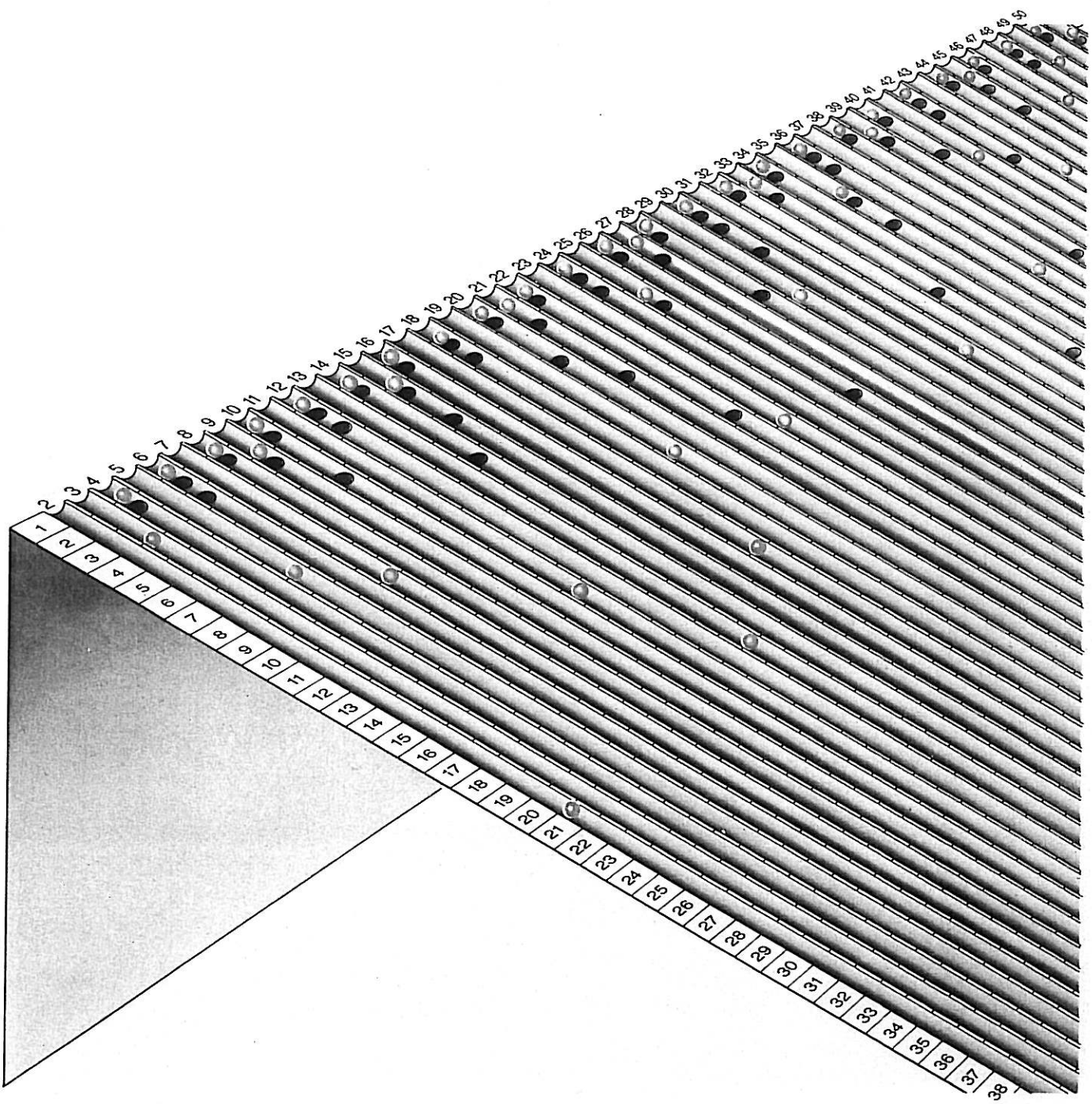
Many mathematicians have regarded number theory as "the queen of mathematics," partly for the intricate beauty of its proofs but also because there has long been the feeling that its study is a form of pure contemplation, unburdened by the potential for practical consequences. Since 1977, however, the development of number theory has also been stimulated by the recognition that



EARLY MACHINE for the exploration of the number system was built in 1926 by D. H. Lehmer of the University of California at Berkeley. Constructed out of a sawhorse, bicycle chains and other readily available materials, the machine was a special-purpose computer that could be programmed to search rapidly for numbers having the special form necessary for solving certain problems in number theory. Primality testing, that is, the classification of a number as being either prime or composite, is one of the most important of these problems. (A prime is a number evenly divisible only by itself and 1; if a number has other divisors, it is composite.) The conditions that must be met by a numerical solution to a problem could be programmed on Lehmer's machine by inserting bolts into certain links of the bicycle chains. When the chains were turned by a motor, the machine would run until all the bolts were lined up; the motor was then automatically turned off. The number corresponding to the configuration of the chains at the stopping point would satisfy the conditions programmed. Lehmer built several faster versions of the machine, but the 1926 version has since been destroyed. The machine in the photograph is one now being built by Roberto Canepa of Carnegie-Mellon University at the Computer Museum in Marlboro, Mass.

it could have an important application to cryptography, the study of secure communication. In that year Ronald L. Rivest of the Massachusetts Institute of Technology, Adi Shamir of the Weizmann Institute of Science and Leonard M. Adleman of the University of Southern California pointed out that a public-key cryptographic system could be based on the difficulty of factoring a large composite number that is the product of, say, two 100-digit primes.

In a public-key system the means of encoding the message can be made public knowledge without jeopardizing the security of the code. The Rivest-Shamir-Adleman code is based on the relative ease of determining that two large numbers are prime and then multiplying them, compared with the great practical difficulty of factoring their product without prior knowledge of how it was constructed. If the 200-digit product of two 100-digit primes were made pub-



PRIME-NUMBER SIEVE, attributed to the ancient Greek scholar Eratosthenes, was one of the first methods invented for distinguishing primes from composites among the numbers up to some predetermined limit. The sieve is represented in the illustration by an inclined plane in which holes have been made; the numbers to be tested for primality are represented by balls that roll down grooves in the plane. The holes are made according to a fixed procedure. First, holes in the second row are made at every second groove except the groove designated 2. Thus all the even-numbered balls except the ball in groove 2 fall through the holes. Next the lowest-numbered groove without a hole is found, namely the third groove. Holes are then made in the third row at every third groove except the groove designated 3. The procedure is continued by making holes in every fifth groove in the fifth row, every seventh groove in the seventh row and so on, stopping after the row whose number is less than or equal to the square root of the largest number to be tested. The balls that do not fall through a hole correspond to prime numbers. For example, all 25 primes smaller than 100 can be determined by collecting all the balls from 2 to 100 that roll past the seventh row of holes. (There are no primes greater than 7 that are less than or equal to the square root of 100.)

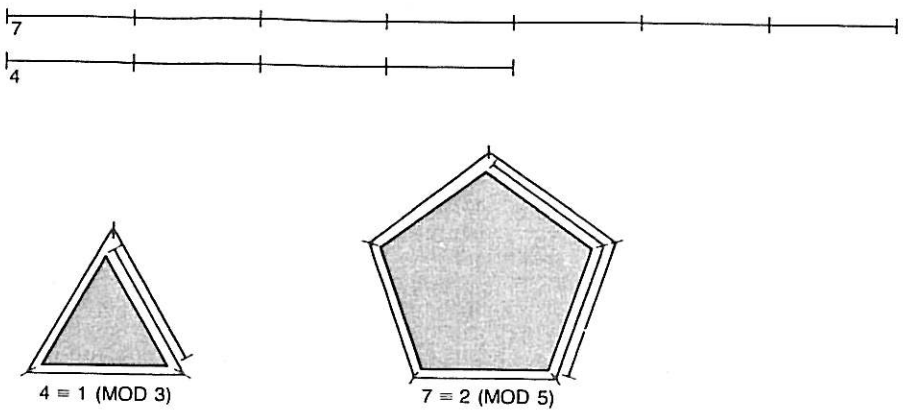
lic, anyone could encode a message by employing the 200-digit number. Only knowledge of the two prime factors, however, would make it possible to decode the message. There are public-key cryptographic systems that do not depend on factoring, but the security of the Rivest-Shamir-Adleman system rests on the intractability of the factoring problem, and its operation rests on the assumption that the 100-digit factors of the key number are indeed prime. Efficient primality tests that do not depend on factoring are therefore of great value to the cryptographic system [see "The Mathematics of Public-Key Cryptography," by Martin E. Hellman; SCIENTIFIC AMERICAN, August, 1979].

All known methods of testing primality that do not depend on factoring trace their lineage to a theorem first stated by Pierre de Fermat in a letter to his friend Bernard Frénicle de Bessy on October 18, 1640. The theorem, usually called Fermat's little theorem, states that if n is a prime number and b is any whole number, then $b^n - b$ is a multiple of n. For example, if n is equal to 7 and b is equal to 2, the theorem correctly states that $2^7 - 2$, or 126, is a multiple of 7.

For primality testing the importance of the theorem is the logically equivalent statement that if $b^n - b$ is not a multiple of n, then n is a composite number. When n is equal to 4 and b is equal to 3, the expression $3^4 - 3$ is equal to 78, which leaves a nonzero remainder (namely 2) when it is divided by 4. Hence the little theorem makes it possible to conclude, in a somewhat roundabout way, that 4 is not a prime.

Although the little theorem is a fundamental and powerful result, it has several elementary proofs, one of which I shall give below. The theorem makes it possible to state properties of numbers that are so large they cannot even be written in decimal form. From the fact that $2^{44,497} - 1$ is prime, for example, the theorem states that the number 3 raised to the power $2^{44,497} - 1$, minus 3, is evenly divisible by $2^{44,497} - 1$. The result of the exponentiation is a number so unimaginably huge that it could never be written in decimal form; furthermore, the process of division that would give the quotient explicitly could not possibly be done by any physically conceivable computer.

To get to such distant outposts of the number system one can use the arithmetic wheel, invented by Carl Friedrich Gauss. He formulated modular arithmetic, in which the absolute size of a number is irrelevant and all that matters is the size of the last turn of the arithmetic wheel employed to reach the number. The number n is expressed as the remainder after n is divided by some number m called its modulus; the remainder is written n modulo m, or n (mod m). The number m plays the role of the size of the wheel, the number n represents the absolute size of the number and the remainder n (mod m) represents the size of the last partial turn of the wheel needed to reach n.



MODULAR ARITHMETIC is a system of calculation with important applications in primality testing. In modular arithmetic the only thing that matters about any number n is the remainder when n is divided by some modulus m. The absolute size of the number n is disregarded. The most familiar example of modular arithmetic is the common system of telling time, in which the hours are designated by their values modulo 12. The triple-bar sign is read "is congruent to"; the numbers on each side of the sign have the same remainder when they are divided by the modulus. For example, the expression $4 \equiv 1$ (mod 3) means that 4 and 1 leave the same remainder when they are divided by 3, namely 1. The remainder is often called the residue.

In modular arithmetic many of the laws of ordinary arithmetic have close analogues. In particular it is possible to add and multiply in modular arithmetic as long as the results are expressed as congruences; all numbers that leave the same remainder with respect to a given modulus are said to be congruent with respect to that modulus. The remainder after division of a number by the modulus is often called the residue of the number with respect to the modulus.

In ordinary arithmetic 6 plus 7 is equal to 13, a result that is readily reproduced in arithmetic with a modulus of, say, 5. It turns out that 6 (mod 5) + 7 (mod 5) is congruent to 1 + 2, or in other words 3, and that 13 (mod 5) is also congruent to 3. Similarly, 4×5 is equal to 20, whereas in arithmetic modulo 3 the multiplication is done as 4 (mod 3) $\times$ 5 (mod 3), which is congruent to 1×2. The product is therefore 2, and 20 (mod 3) is also congruent to 2.

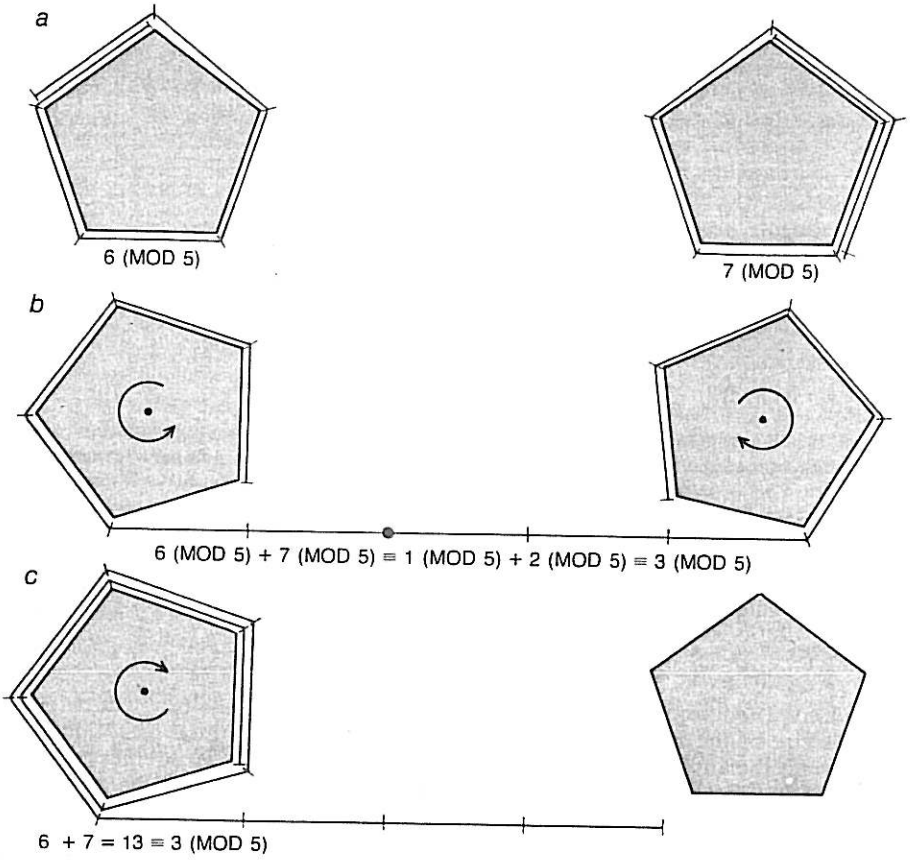
In Gauss's notation Fermat's little theorem states that if n is prime, then $b^n - b$ is congruent to 0 (mod n), or in other words $b^n - b$ is a multiple of n. The advantage of Gauss's notation is that the rules of modular arithmetic make it possible to calculate the value of $b^n - b$ modulo n without having to divide $b^n - b$ by n. For a number such as $2^7 - 2$ the advantages of Gauss's system do not seem to be significant because direct division is easy. To find the remainder when a number such as $3^{1,037} - 3$ is divided by 1,037, however, modular arithmetic becomes almost indispensable.

The essence of the problem is to find the value of $3^{1,037}$ (mod 1,037). In modular arithmetic it is not necessary to calculate the value of the enormous number $3^{1,037}$. All one need do is to repeatedly apply the fact that in modular arithmetic the residue of the square of a number is congruent to the square of the residue of the number.

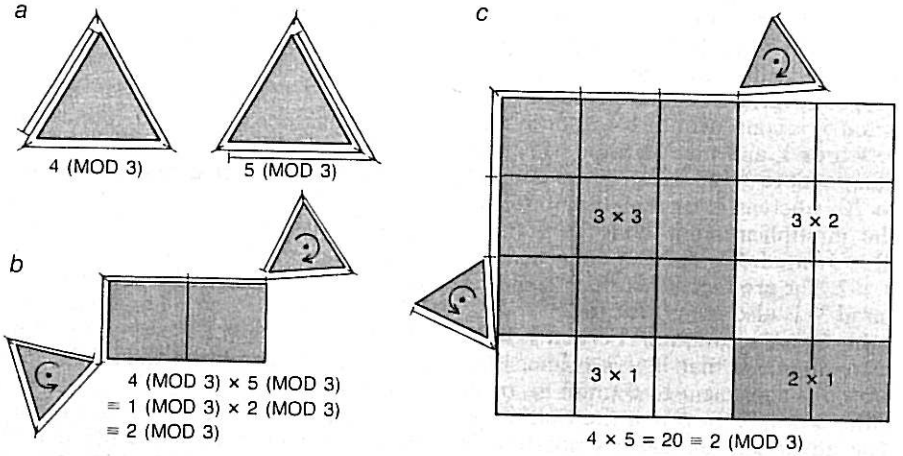
For example, once 3^8 (mod 1,037) is calculated, 3^{16} (mod 1,037) can be obtained by squaring the residue of 3^8 and finding the residue of this number modulo 1,037. In this way one can find the residues modulo 1,037 of 3, 3^2, 3^4, 3^8 and so on up to $3^{1,024}$. The number $3^{1,037}$ is equal to $3^{(1,024+8+4+1)}$, which in turn is equal to $3^{1,024} \times 3^8 \times 3^4 \times 3$ by the law of exponents; hence $3^{1,037}$ (mod 1,037) is congruent to $3^{1,024}$ (mod 1,037) $\times$ 3^8 (mod 1,037) $\times$ 3^4 (mod 1,037) $\times$ 3 (mod 1,037). When all the calculations are done, it is found that $3^{1,037}$ is congruent to 845 (mod 1,037), and so $3^{1,037} - 3$ is congruent to 842 (mod 1,037) [*see illustration on page 141*]. On the basis of Fermat's little theorem, therefore, 1,037 must be composite, since the remainder on dividing $3^{1,037} - 3$ by 1,037 does not equal zero. The procedure gives scarcely any clue that might be employed to find the factors of 1,037.

It is amusing to carry out the procedure with a programmable calculator. To avoid round-off errors the value of n should be limited to numbers with at most half of the number of digits displayed by the calculator. With a large computer the calculation can be done rapidly even if the input number has thousands of digits. Thus enormous numbers can often be identified by the Fermat test as being composite.

The proof of Fermat's little theorem follows from a simple consequence of



ADDITION IN MODULAR ARITHMETIC is carried out much as it is in ordinary arithmetic. The residue of each number with respect to the given modulus is determined and the residues are added. If the sum is greater than the modulus, the residue of the sum is found. In the example shown here the total length of two strings, one of length 6 and the other of length 7, is found modulo 5. In arithmetic modulo 5 the number of full turns a string takes around a pentagon is disregarded and only the length of the string that remains after the last full turn is considered relevant. Thus to modulo 5, 6 is congruent to 1 and 7 is congruent to 2 (*a*). When the residues of string are unwound and spliced, the total length of the two residues is 3 (*b*). When all the string is wrapped around one pentagon, the length of string that remains after all the full turns are taken is 3, and so the ordinary sum of 6 and 7 is congruent to 3 modulo 5 (*c*). In general the sum of the residues of two numbers is congruent to the residue of their ordinary sum.



MULTIPLICATION IN MODULAR ARITHMETIC is also done in a way similar to its analogue in ordinary arithmetic. In the example given 4 and 5 are multiplied modulo 3; they are represented as strings wrapped around a triangle. The residue of each number is the length of the string that remains after all full turns of the string around the triangle have been taken (*a*). The residue of 4 modulo 3 is 1 and the residue of 5 modulo 3 is 2. The product of the two residues is the area of the rectangle having sides equal to the length of each residue; in other words, 1 times 2 equals 2 (*b*). The product of 4 and 5, on the other hand, is the area of the rectangle having sides of length 4 and 5. The residue of the product (*c*) is obtained by disregarding the area of any smaller rectangle whose sides are equal to the length of string required for a whole number of turns around the triangle (*gray regions*). The area of the remaining rectangle (*colored region*) is the residue of the product of 4 and 5 modulo 3. Thus the general rule is that the product of the residues of two numbers is congruent to the residue of their ordinary product.

the fundamental theorem of arithmetic: If a prime number evenly divides the product of several numbers, then it evenly divides at least one of the numbers. For example, 4×9 or 36, is evenly divisible by the prime number 3, and of course one of the factors (namely 9) is also evenly divisible by 3. The statement is not true for a composite number: 4×9 is evenly divisible by 6, but neither 4 nor 9 is evenly divisible by 6.

To prove Fermat's result that $b^n - b$ is a multiple of n when n is prime, note that $b^n - b$ is equal to $b \times (b^{n-1} - 1)$. Hence if b itself is a multiple of n, so is $b^n - b$. The theorem thus remains to be proved only for the case in which b is not a multiple of n; the proof proceeds on this assumption.

The basic idea is that if the numbers b, $2b$, $3b$ and so on up to $(n-1)b$ are multiplied together, their product can be rearranged as $b^{n-1}(n-1)!$. On the other hand, it follows from the fundamental theorem of arithmetic that the residues modulo n of b, $2b$, $3b$ and so on up to $(n-1)b$ are the numbers 1, 2, 3 and so on up to $n-1$, possibly in some mixed-up order. Some elementary algebra then allows the conclusion that $(b^{n-1} - 1)(n-1)!$ is a multiple of n. Because the prime number n does not evenly divide any of the numbers from 1 to $n-1$, whereas n does evenly divide the product $(b^{n-1} - 1)(n-1)!$, another application of the fundamental theorem of arithmetic implies that n evenly divides $b^{n-1} - 1$. Since $b^{n-1} - 1$ is a factor of $b^n - b$, the theorem follows.

It might appear that Fermat's little theorem completely solves the problem of primality testing, in that it seems to provide a quick way of distinguishing a prime number from a composite one. Unfortunately there is a logical flaw in this conclusion. If for some number b the number $b^n - b$ gives a nonzero remainder when it is divided by n, then n is certainly composite. Suppose, however, $b^n - b$ is a multiple of n. Does it follow that n must be prime?

Several examples suggest the answer is yes: $2^2 - 2$ is a multiple of 2, $2^3 - 2$ is a multiple of 3 and $2^5 - 2$ is a multiple of 5, and the numbers 2, 3 and 5 are all primes. Some 2,500 years ago Chinese mathematicians discovered the pattern and asserted that if $2^n - 2$ is a multiple of n, then n must be prime. Gottfried Wilhelm Leibniz, who made a study of the binary patterns in the *I Ching*, believed the result as well. In 1819, however, the French mathematician Pierre Frédéric Sarrus pointed out that $2^{341} - 2$ is a multiple of 341, even though 341 is a composite number, the product of 11 and 31. Since Sarrus's work many other counterexamples involving many different values of the base b have been found: $3^{91} - 3$ is a multiple of the composite number 91

and $4^{15} - 4$ is a multiple of the composite number 15. All these statements can be verified with a small calculator by applying modular arithmetic in the way I have already described.

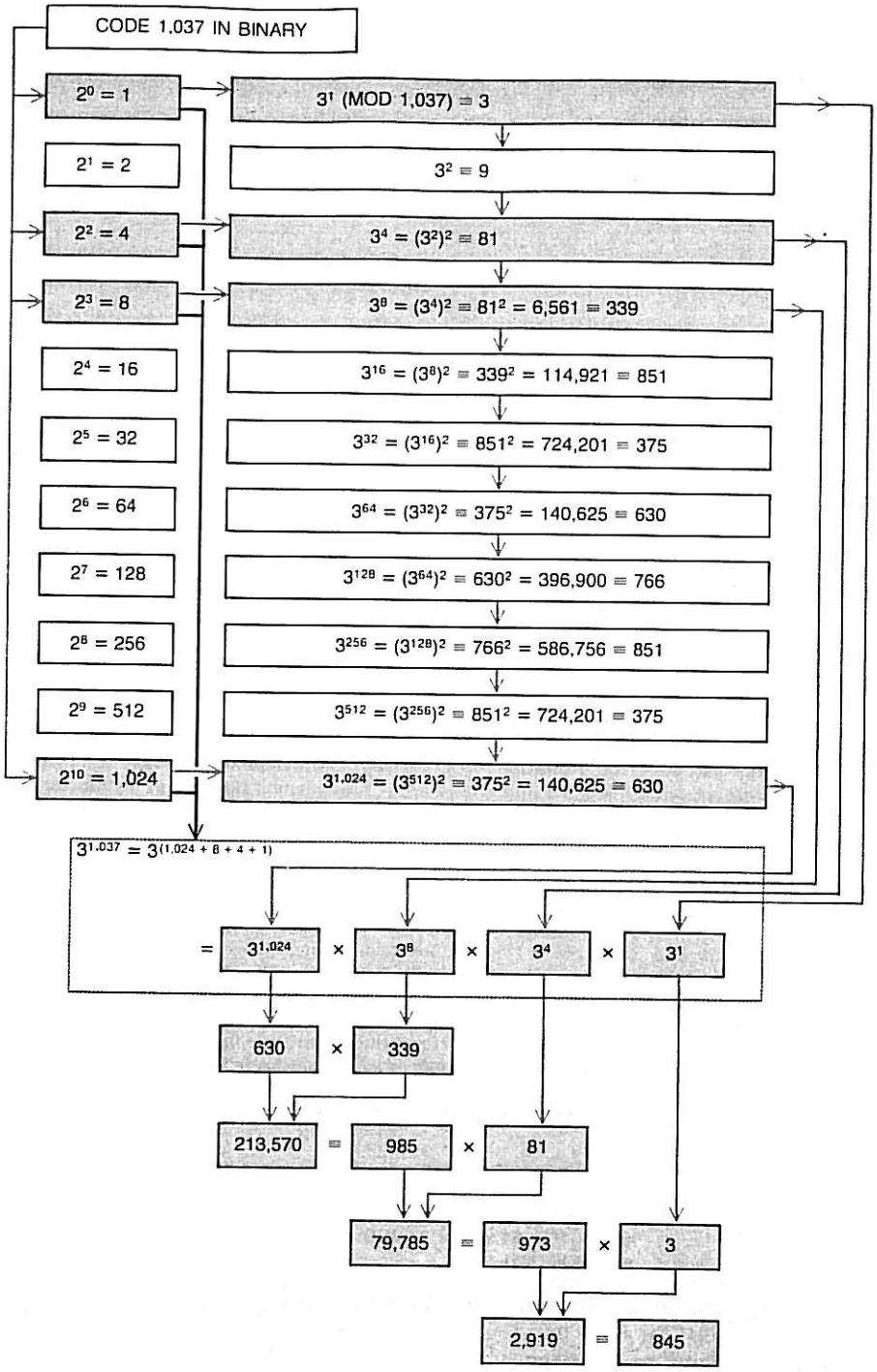
A number that fails to show up as a composite number by Fermat's test with a given value of b yet happens to be composite is called a pseudoprime to the base b. The number 341 is a pseudoprime to the base 2, whereas 91 is a pseudoprime to the base 3 and 15 is a pseudoprime to the base 4. It turns out that for every base b there are infinitely many pseudoprimes. There are even composite numbers, such as 561 (the product of 3, 11 and 17) and 1,729 (the product of 7, 13 and 19) that are pseudoprimes to every base b. Numbers of this kind are called Carmichael numbers, after the American mathematician R. D. Carmichael, who discovered their properties in 1909.

The existence of Carmichael numbers puts an end to any hope that the Fermat test, at least as it was originally formulated, can separate all the primes from the composites. Nevertheless, Carmichael numbers are exceedingly rare, and even the pseudoprimes to a single base b are rare when they are compared with the primes. Jan Bohman of the University of Lund has shown that there are exactly 882,206,716 primes smaller than 20 billion. John L. Selfridge of the journal *Mathematical Reviews* and Samuel S. Wagstaff, Jr., of the University of Georgia have calculated that there are only 19,865 pseudoprimes to the base 2 that are smaller than 20 billion. If the Fermat test were carried out to the base 2 for all the numbers smaller than 20 billion, the error rate would be only about one in a million.

The scarcity of pseudoprimes to the base 2 among all the numbers smaller than 20 billion suggests that any number that passes the Fermat test to base 2 is likely to be prime. Moreover, if the number is a composite that passes the Fermat test to base 2, it may not be able to pass the Fermat test to base 3. One would like to assert that by applying the Fermat test to base 3, one could significantly reduce the probability that a composite number that has passed the base-2 test is still posing as a prime. Because the tests may not be independent ones, however, the Fermat test to base 3 might not rule out many composites that had not already been eliminated by the base-2 test.

Recently a variation of the Fermat test that meets the requirement that tests to different bases be independent was developed by D. H. Lehmer of the University of California at Berkeley and independently by Robert M. Solovay of the California Institute of Technology and Volker Strassen of the Swiss Federal Institute of Technology. The test has the feature that if the test number n is composite, it will be recognized as composite for at least half of the values of the base b between 1 and n. Thus by randomly choosing, say, 100 different bases and applying the Lehmer-Solovay-Strassen test to each one, the probability that some random composite number n will pass all 100 tests is less than or equal to one in 2^{100}, or about one in 10^{30}.

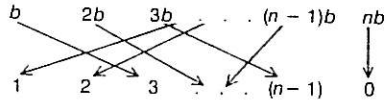
Solovay and Strassen said that their test constitutes a "Monte Carlo primality test." (A number of probabilistic methods in mathematics and physics have been named for the city noted for



APPLICATION OF MODULAR ARITHMETIC circumvents calculations that would be exceedingly time-consuming and prone to error if they were done in ordinary arithmetic. The flow chart demonstrates how the remainder can be found when the number $3^{1,037}$ is divided by 1,037, without ever calculating the value of $3^{1,037}$. The method depends on the fact that the residue of the square of a number is equal to the square of its residue to a given modulus. By repeatedly squaring the residue of a power of 3 and taking the residue of the result one can find in sequence the residues modulo 1,037 of 3, 3^2, 3^4, 3^8, 3^{16} and so on up to $3^{1,024}$. Because $3^{1,037}$ is equal to $3^{1,024} \times 3^8 \times 3^4 \times 3$, the remainder when $3^{1,037}$ is divided by 1,037 is equal to the residue of the product of the residues $3^{1,024} \pmod{1,037} \times 3^8 \pmod{1,037} \times 3^4 \pmod{1,037} \times 3 \pmod{1,037}$. The entire procedure can be done with a programmable calculator.

CONSIDER THE NUMBERS b, $2b$, $3b$, ..., $(n-1)b$, nb

FINDING THE RESIDUES OF THE NUMBERS MODULO n SETS UP A CORRESPONDENCE IN WHICH THE REMAINDERS ARE A PERMUTATION OF THE COEFFICIENTS OF b.



HENCE $b \times 2b \times \ldots \times (n-1)\,b \pmod n \equiv 1 \times 2 \times \ldots \times (n-1) \pmod n$.

THEREFORE $|b \times 2b \times \ldots \times (n-1)b| - |1 \times 2 \times \ldots \times (n-1)| \equiv 0 \pmod n$.

BUT $b \times 2b \times \ldots \times (n-1)b = b^{n-1}(n-1)!$ AND $1 \times 2 \times \ldots \times (n-1) = (n-1)!$.

HENCE $|b \times 2b \times \ldots \times (n-1)b| - |1 \times 2 \times \ldots \times (n-1)| =$

$|b^{n-1}(n-1)!| - |(n-1)!| = (b^{n-1}-1)(n-1)! \equiv 0 \pmod n$.

THEREFORE $(b^{n-1}-1)(n-1)!$ IS A MULTIPLE OF n, WHICH IS SUFFICIENT TO PROVE FERMAT'S THEOREM.

PROOF OF FERMAT'S "LITTLE THEOREM" follows from the application of the fundamental theorem of arithmetic and from the rules of multiplication in modular arithmetic. Fermat's little theorem states that if n is a prime number and b is any whole number, $b^n - b$ is a multiple of n. For the case in which b is a multiple of n, the conclusion of the theorem follows at once: because $b^n - b$ is equal to $b(b^{n-1}-1)$, b is a factor of $b^n - b$ and so $b^n - b$ is a multiple of n. For the case in which b is not a multiple of n it is sufficient to show that $b^{n-1}-1$ is a multiple of n. A corollary to the fundamental theorem of arithmetic states that if a prime number evenly divides the product of several numbers, it also evenly divides one of the numbers. Thus because n does not evenly divide any of the numbers from 1 to $n-1$, n does not evenly divide their product $(n-1)!$ either. Hence if it can be proved that $(b^{n-1}-1)(n-1)!$ is evenly divisible by n, then it follows that $b^{n-1}-1$ and $b^n - b$ are also evenly divisible by n. Consider the numbers b, $2b$, $3b$ and so on up to nb. No two of the numbers, say ib and jb, can give the same remainder when they are divided by n. If they could, then $ib - jb$, which is equal to $(i-j)b$, would be a multiple of n, because subtraction would cause the two remainders to cancel. Since b is not a multiple of n, the fundamental theorem of arithmetic implies that $i - j$ is a multiple of n. The number n, however, cannot evenly divide any numbers of the form $i - j$, where i and j are chosen from the sequence of numbers from 1 to n. Thus the supposition that ib and jb give the same remainder when they are divided by n leads to a contradiction. Because the remainder when n divides nb is 0 and because division by n only gives remainders from 0 to $n-1$, the numbers b, $2b$, ..., $(n-1)b$ must give all the remainders from 1 to $n-1$, in some order, when they are divided by n. The diagram shows that dividing the numbers b, $2b$, ..., $(n-1)b$ by n and then taking the remainder amounts to setting up a correspondence between the numbers b, $2b$, ..., $(n-1)b$ and the numbers 1, 2, ..., $(n-1)$ in some order. Since the residues of the numbers in each set are the same except for order, the residue of the product $b \times 2b \times \ldots \times (n-1)b$ is equal to the residue of the product $1 \times 2 \times \ldots \times (n-1)$. Subtracting one product from the other causes the residues to cancel, and so the difference of the two products is a multiple of n. The algebraic manipulations show that the difference of the two products is equal to $(b^{n-1}-1)(n-1)!$, and so this expression is evenly divisible by n. Fermat's little theorem is thereby proved for all whole numbers b.

341 PSEUDOPRIME TO BASE 2

$2^{341} = 2^{256} \times 2^{64} \times 2^{16} \times 2^4 \times 2$

$\equiv 64 \times 16 \times 64 \times 16 \times 2 \pmod{341}$

$\equiv 2 \pmod{341}$

HENCE $2^{341} - 2 \equiv 0 \pmod{341}$

THEREFORE 341 PASSES THE FERMAT TEST TO BASE 2

BUT $341 = 11 \times 31$

561 PSEUDOPRIME TO ANY BASE

$2^{561} = 2^{512} \times 2^{32} \times 2^{16} \times 2$

$\equiv 103 \times 103 \times 460 \times 2 \pmod{561}$

$\equiv 2 \pmod{561}$

HENCE $2^{561} - 2 \equiv 0 \pmod{561}$

THEREFORE 561 PASSES THE FERMAT TEST TO BASE 2

BUT $561 = 3 \times 11 \times 17$

$3^{561} = 3^{512} \times 3^{32} \times 3^{16} \times 3$

$\equiv 273 \times 273 \times 69 \times 3 \pmod{561}$

$\equiv 3 \pmod{561}$

HENCE $3^{561} \times 3 \equiv 0 \pmod{561}$

THEREFORE 561 PASSES THE FERMAT TEST TO BASE 3

PSEUDOPRIME is a number that passes the test for primality derived from Fermat's little theorem for some base b but is nonetheless a composite number. Thus a pseudoprime to the base b is a composite number n that divides $b^n - b$ evenly. The French mathematician Pierre Frédéric Sarrus was the first to point out that 341, which is the product of 11 and 31, is a pseudoprime to the base 2. The verification that $2^{341} - 2$ is evenly divisible by 341 is done here in modular arithmetic in a way similar to the procedure in the illustration on the preceding page. Some numbers, called Carmichael numbers after the American mathematician R. D. Carmichael, are pseudoprimes to any base b. The number 561, which is the product of 3, 11 and 17, is the smallest Carmichael number; here it is shown to be a pseudoprime to the bases 2 and 3.

its games of chance.) In a practical sense the description seems accurate; it would appear, for example, that in the cryptographic application the operation of a code is not handicapped by a vanishingly small chance that the numbers on which it is based are not prime after all. It has also been argued, however, on what I regard as shaky philosophical grounds, that because every ordinary mathematical proof is subject to correction and human error, one ought to accept a strong probabilistic verification of primality as being a mathematical proof of primality.

There is indeed reason to believe the probability is considerably greater than one in 10^{30} that arguments accepted as mathematical proofs are in error. The history of mathematics bears witness to numerous examples of "proof" that later turned out to be misleading or erroneous. There is, however, a qualitative difference between probabilistic verification and mathematical proof that is important to mathematicians. A proof is a deductive argument, in which each step follows logically from the preceding steps. The proof carries such weight not only because the conclusion can be seen to be valid but also because a valid conclusion must follow from the force of the argument. What the idea of a Monte Carlo primality test does suggest, I think, is that the concept of proof and the concept of certainty are quite different from each other.

In 1876 the French mathematician Édouard A. Lucas gave an ironclad primality test for any number n. Suppose there is a number b for which b^{n-1} is congruent to 1 modulo n but for which $b^{(n-1)/p}$ is not congruent to 1 modulo n for each prime factor p of $n-1$. Then Lucas proved that n must be prime.

For example, suppose the number n to be tested is 257; then $n-1$ is equal to 256, or 2^8, so that every prime factor p of $n-1$ is equal to 2. In order to prove that n is prime one must find a number b such that b^{256} is congruent to 1 modulo 257 but $b^{256/2}$ is not congruent to 1 modulo 257. Although there is no indication given by the Lucas test of how to find the special number b, many such numbers satisfy the conditions of the theorem for any prime number n; a random search will almost always be successful. When b is equal to 3, for example, 3^{256} is congruent to 1 modulo 257, but $3^{256/2}$ is congruent to 256 modulo 257. Hence 257 is prime. Although the Lucas test too is a Monte Carlo test, in the sense that the number b must be selected at random, it delivers a rigorous proof of primality once the number b is found.

There is one aspect of the Lucas test that limits it to numbers having a special form. Unless every prime factor p of the number $n-1$ can be found, the test cannot be applied. Of course, if n is suspected to be prime, it is an odd number, and

THE NEW CHEVROLET CAVALIER. ITS NEW HIGH COMPRESSION FUEL-INJECTED ENGINE WILL MAKE IT GO QUICKER. SO WILL ITS NEW LOWER PRICE.

Chevrolet is utilizing advanced state-of-the-art front-wheel-drive technology in the new Cavalier. With its new high-torque, electronically fuel-injected 2.0 Liter engine and new lower price,* it's going to give imports competition they haven't seen before.

Cavalier's front-wheel-drive response and available new 5-speed transmission are designed to offer you a new level of driving pleasure.

The new 2.0 Liter Cavalier. Powered by Chevrolet's determination to put Cavalier on top. And priced to keep it there.

See and drive the new fuel-injected Cavalier Sedan, Coupe or Wagon. From America's sales leader. With all that Cavalier offers today, if you haven't seen your Chevy dealer, you're not ready to buy.

Front-wheel-drive Cavalier Sedan

Let's get it together . . . buckle up.

GM

*Based on a comparison of Manufacturer's Suggested Retail Prices for 1982 and 1983 Cavalier models. Levels of equipment vary. Some Chevrolets are equipped with engines produced by other GM divisions, subsidiaries, or affiliated companies worldwide. See your dealer for details.

USA-1 IS TAKING CHARGE

Chevrolet

CAVALIER · CELEBRITY · CHEVETTE · CAMARO · CITATION · MALIBU · MONTE CARLO · CAPRICE · CORVETTE

so $n-1$ is divisible by 2. Such a head start is seldom enough; the Lucas test is not generally feasible unless $n-1$ factors easily, as it did in my example.

If all the prime factors of $n+1$ can be found more readily than those of $n-1$, another test (also first proposed by Lucas) can determine the primality of the number n. Lehmer improved on the test in 1930, and for the numbers to which it can be applied the Lucas-Lehmer test can be run extremely fast on a large computer. The test has demonstrated the primality of the largest primes known, numbers of the form 2^p-1, where p itself is a prime number. Such numbers are called Mersenne numbers, after the 17th-century French mathematician Marin Mersenne, who once gave a list of prime numbers p for which he believed 2^p-1 is prime. It is evident that if n is a Mersenne number, all the prime factors of $n+1$ are known at once: they are all equal to 2.

In 1975 John Brillhart of the University of Arizona, Lehmer and Selfridge showed how to construct a primality test for a number n if only some of the prime factors of $n-1$ or $n+1$ are known. Hugh C. Williams of the University of Manitoba has raised this kind of testing to a fine art: partial factorizations of n^2+1, n^2-n+1 or n^2+n+1 are now sufficient for testing the primality of n. If none of the numbers factors easily, however, the tests bog down. Although many 100-digit numbers can be tested by such methods, it has been estimated that the testing of certain stubborn 100-digit primes would have required a century of computer time. Thus what has been needed is a test for primality that does not depend on the special form of the number being tested.

In 1980 Adleman and Robert S. Rumely of the University of Georgia developed a test that has radically altered the efficiency of testing the primality of large numbers having no special form. The test as it was originally formulated was probably capable of testing the primality of any number having from 50 to 100 digits in four to 12 hours with a large computer. Henri Cohen of the University of Bordeaux and Hendrik W. Lenstra, Jr., of the University of Amsterdam have since improved the test in several significant ways so that it can now run about 1,000 times faster: a 100-digit number can be tested in about 40 seconds with the Control Data Corporation–Cyber 170–750 computer.

How does the Adleman-Rumely test achieve such efficiency? Its details require a technical understanding of algebraic number theory, but in its essence the test is quite similar to the one devised by Fermat. Two auxiliary numbers, called the initial number I and the Euclidean number E, are constructed. The number I is a product of several primes, such as $2\times3\times5\times7$, or 210. The number E is called the Euclidean number because its definition is reminiscent of Euclid's proof that there are infinitely many primes. E is the product of all the primes p, q, r and so on, such that the numbers $p-1$, $q-1$, $r-1$ and so on are all factors of I. The number 70, for example, is a factor of 210, and because 70 is one less than the prime number 71, 71 is defined as a factor of the Euclidean number E. The factors of 210 that are exactly one less than a prime number are 1, 2, 6, 10, 30, 42, 70 and 210 itself. Hence E is the product of the

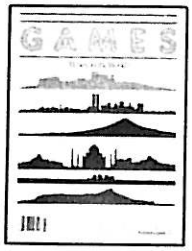
THE MERSENNE PRIMES TO $2^{62,982}$

VALUE OF p FOR WHICH 2^p-1 IS PRIME	2^p-1	WHEN PROVED PRIME	BY WHOM	MACHINE USED
2	3	ANTIQUITY	MENTIONED IN EUCLID'S ELEMENTS	
3	7			
5	31			
7	127			
13	8,191	1461	MENTIONED IN CODEX LAT. MONAC. 14908	
17	131,071	1588	PIETRO ANTONIO CATALDI	
19	524,287			
31	2,147,483,647	1772	LEONHARD EULER	
61	19 DIGITS	1883	I. M. PERVOUCHINE	
89	27 DIGITS	1911	R. E. POWERS	
107	33 DIGITS	1914	R. E. POWERS, E. FAUQUEMBERGE	
127	39 DIGITS	1876 – 1914	ÉDOUARD LUCAS, E. FAUQUEMBERGE	
521	157 DIGITS	1952	RAPHAEL M. ROBINSON	SWAC
607	183 DIGITS			
1,279	386 DIGITS			
2,203	664 DIGITS			
2,281	687 DIGITS			
3,217	969 DIGITS	1957	HANS RIESEL	BESK
4,253	1,281 DIGITS	1961	ALEXANDER HURWITZ	IBM-7090
4,423	1,332 DIGITS			
9,689	2,917 DIGITS	1963	DONALD B. GILLIES	ILLIAC-II
9,941	2,993 DIGITS			
11,213	3,376 DIGITS			
19,937	6,002 DIGITS	1971	BRYANT TUCKERMAN	IBM 360/91
21,701	6,533 DIGITS	1978	LAURA NICKEL, CURT NOLL	CDC-CYBER-174
23,209	6,987 DIGITS	1979	CURT NOLL	CDC-CYBER-174
44,497	13,395 DIGITS	1979	HARRY L. NELSON, DAVID SLOWINSKI	CRAY-1

MERSENNE PRIME is a prime number that is one less than a power of 2; the numbers of this form are named for the French mathematician Marin Mersenne. Such primes have been of interest since antiquity because, as was shown by Euclid, if the number 2^p-1 is prime, the number $2^{p-1}(2^p-1)$ is perfect, that is, equal to the sum of all its factors except itself. If 2^p-1 is prime, then p too is prime, but the converse does not necessarily hold. It is not known whether there are infinitely many Mersenne primes, nor is it known whether there are infinitely many Mersenne composites, but both statements are probably true. In recent years the growth of the table of known Mersenne primes has paralleled the growth of computing power. According to David Slowinski of the Lawrence Livermore Laboratory, showing that $2^{8,191}-1$ is not a prime took 100 hours with the ILLIAC-I computer, 5.2 hours with the IBM System 7090, some 49 minutes with the ILLIAC-II, 3.1 minutes with the IBM System 360/91 and 10 seconds with the CRAY-1. Slowinski and Harry L. Nelson, also of Lawrence Livermore, have examined the Mersenne numbers for all values of p up to 50,000 without identifying any primes larger than $2^{44,497}-1$. Recently Guy M. Haworth, Steven M. Holmes, David J. Hunt, Thomas W. Lake and Stewart F. Reddaway of International Computing Limited have been continuing the search with the help of the ICL-DAP, a supercomputer having 4,096 processors that operate in parallel. They have now searched for Mersenne primes for values of p up to 62,982 without finding any new Mersenne primes.

HERE, AT LAST, AMERICA!

A magazine that hasn't a clue as to who will become president in 1984...that doesn't have the foggiest notion whether there's life in outer space...that won't help you lose weight, improve your golf game, and positively will not keep you up-to-date on what's happening in the world of business and finance!



BUT...if you turn to the Crossword Puzzle before you read the news columns...if your pulse races at the challenge of an intricate maze or brainteaser...if you can't resist exciting word games, number games, logic games, cryptograms...and if you want to keep up-to-date on the latest games around...

We may just be made for each other!

GAMES is the magazine for people who like to think—and have fun at the same time!

GAMES is the magazine you *play*, not just read. GAMES will *involve you* on every page. *Intrigue you. Puzzle you.* It will hold your interest like no other magazine ever has.

Whether you've only a few minutes to unwind during the day...a couple of hours to kill on a train, plane...or simply want to dig in for a relaxing evening of challenging fun at home...GAMES is your ticket to a good time!

In every fascinating issue, you'll find PENCILWISE...a special section devoted to ingenious cryptic crosswords, acrostics, word searches, unusual mazes and more.

You'll also find THE WORLD'S MOST ORNERY CROSSWORD...with two sets of clues (one hard, one easy. Take your pick!)

And that's not all! Every month, you'll enjoy the most unusual and clever trivia quizzes, logic puzzles, word and number games, and brainteasers of all kinds.

So if you're looking for a challenging, creative, totally different way to fill your leisure time, *any time*...treat yourself to GAMES!

To subscribe to GAMES, just send a check or money order to GAMES Magazine, P.O. Box 10147, Des Moines, Iowa 50340. You'll receive one year (12 issues) for only $14.97. For foreign and Canadian orders, add $2.00. Allow 4-8 weeks for delivery of your first issue.

GAMES' GUARANTEE OF SATISFACTION: Subscribe to GAMES now, and if you're ever not satisfied—for any reason—just tell us, and you'll receive a complete refund on all unmailed copies.

Subscribe to GAMES today! Mail the coupon below.

YES! Send me 1 year (12 issues) of **GAMES** Magazine for only $14.97.

☐ Payment enclosed
☐ Bill me later

For Canadian and foreign orders, add $2.00 per subscription.

Allow 4-8 weeks for delivery of first issue.

Offer effective through Feb. 28, 1983

JSAD6

Name _____

Address _____

City _____

State _____ Zip _____

Mail to: GAMES Magazine
P.O. Box 10147
Des Moines, IA 50340

prime numbers 2, 3, 7, 11, 31, 43, 71 and 211, or 9,225,988,926. The number E must be constructed so that it is larger than the square root of the number n being tested for primality; in my example, with the initial number 210, the Adleman-Rumely method would work as long as n is no larger than about 10^{19}. The running time for the computer is proportional to a power of the number I, and so I should also be chosen to be as small as possible.

There is a kind of dynamic tension between the numbers E and I. For the test to be valid E must be large; for the test to be fast I must be small. Moreover, since E depends on I, the auxiliary numbers cannot be chosen independently of each other. The number 210 is a good example of a choice for I because it is a relatively small number with many factors that are one less than a prime. To prove that the Adleman-Rumely test is always fast it was necessary to verify that suitable numbers E and I can always be found and to give an estimate of their size.

By coincidence, work on the question had already been done. In 1955 Karl Prachar of the Agricultural University of Vienna showed that there are infinitely many integers having a large number of factors that are one less than a prime. To apply Prachar's result to the original Adleman-Rumely test it was necessary to show that the numbers I could be constructed so that they are "square-free," that is, not divisible by any square of an integer larger than 1. Cohen and Lenstra have recently shown that in their variation of the test the square-free condition can be dropped. It was also possible to strengthen Prachar's result by employing later findings made by Patrick X. Gallagher of Columbia University and Enrico Bombieri of the Institute for Advanced Study. Andrew M. Odlyzko of Bell Laboratories and I analyzed the construction of the numbers that can appear as I in the new primality test.

After the numbers I and E have been constructed certain tests analogous to the Fermat test are done for each pair of primes p and q in which p, the first member of the pair, is a factor of E and q, the second member of the pair, is a factor of $p - 1$. The test is not carried out for whole numbers but rather for numbers called algebraic integers that correspond to p and q. An algebraic integer is a complex number that is the root of a polynomial whose coefficients are integers and whose leading coefficient is 1. For example, $\sqrt{2}$, i (the imaginary square root of -1) and $(-1 + i\sqrt{3})/2$ are all algebraic integers because they are roots of the algebraic equations $x^2 - 2 = 0$, $x^2 + 1 = 0$ and $x^3 - 1 = 0$.

If n, the number being tested for primality, fails the test corresponding to one of the pairs of primes p and q, then n is recognized to be composite. If n passes all the tests, it is still not certain to be prime, but the number of possible factors remaining to be checked is small. Adleman and Rumely have shown that any composite number n passing all tests of the Fermat type must have prime factors in a set with exactly I elements. Lenstra has shown that the numbers in the set are equal to the residues of the powers n, n^2, n^3 and so on up to n^I, modulo E. By trial division, if any of the numbers in the set other than 1 or n divides n without remainder, n is composite; otherwise n must be prime. Although the last step makes the Adleman-Rumely method appear to be a factoring method, I must stress that the conclusion of the last step is valid only if n has passed all previous tests of the Fermat type. Most and perhaps all composite numbers will fail at least one of the Fermat-type tests and so need not have a factor that can be found by the trial division of the last step.

The speed and completely general applicability of the new primality tests have opened the way to the theoretical investigation of numbers previously inaccessible even to the fastest computers. Suppose, however, arbitrary numbers

SIZE OF NUMBER

PRIMALITY TEST	20 DIGITS	50 DIGITS	100 DIGITS	200 DIGITS	1,000 DIGITS
TRIAL DIVISION	2 HOURS	10^{11} YEARS	10^{36} YEARS	10^{86} YEARS	10^{486} YEARS
LUCAS, BRILLHART-LEHMER-SELFRIDGE, WILLIAMS	5 SECONDS	10 HOURS	100 YEARS	10^{9} YEARS	10^{44} YEARS
ADLEMAN-RUMELY, COHEN-LENSTRA	10 SECONDS	15 SECONDS	40 SECONDS	10 MINUTES	1 WEEK

TIME REQUIRED to test an arbitrary number for primality varies widely according to the kind of primality test. Here it is assumed that the tests are run with a fast computer; in particular, for the method of trial division it is assumed that the computer does a million divisions per second regardless of the size of the number being tested. The running times given for the family of tests similar to the one invented by the French mathematician Édouard A. Lucas represent worst cases; prime numbers of special form can often be tested much faster. Most of the times listed are estimates, but entries shaded in color reflect experience with a computer. In practice all three kinds of test can be combined into one test that runs slightly faster than the third test.

having many more than 100 digits are subjected to the tests. How quickly can one expect the tests to deliver primality judgments for such numbers? This question and similar ones have become theoretically important for a branch of computer science called complexity theory. According to a currently accepted definition in complexity theory, a primality test is computationally slow unless it can be carried out in what is called polynomial time. That is, the test is regarded as being slow unless the time it takes to test a number n is less than a fixed power k of the number of digits in n. I shall designate the number of digits in n by the symbol $d(n)$; notice that $d(n)$ itself is a number, and so one can write the number of digits in $d(n)$ as $d(d(n))$.

It turns out that according to the definition provided by complexity theory, the Adleman-Rumely and Cohen-Lenstra tests are computationally slow. Their running time is bounded by $d(n)$ raised to the power $d(d(d(n)))$ times some constant c. The expression $d(d(d(n)))$ is the number of digits in the number of digits in the number of digits in the number n; no matter what the constant c is, the product of c and the expression will eventually exceed the constant k and become indefinitely large as n grows, and so the bound on the running time is not a polynomial one.

Nevertheless, for relatively "small" numbers the criterion provided by complexity theory can be misleading because the expression $d(d(d(n)))$ drifts toward infinity at an extremely leisurely rate. For example, even for a number n as large as $10^{1,000}$, $d(d(d(n)))$ is only equal to 1. The first number n for which the expression is equal to 2 is $10^{999,999,999}$. In other words, for all numbers less than $10^{999,999,999}$ the running time for the new primality tests is bounded by the power c of $d(n)$. Thus although the new tests do not run in polynomial time, they "nearly" do.

Now that primality testing can be done quickly for moderately large numbers attention may shift to the companion problem of factoring. Progress in factoring would of course have immediate implications for cryptographic systems based on factoring. The developments in primality testing have no direct bearing on the problem of factoring; on the other hand, no one has ever proved that factoring is intractable. There is no guarantee that someone will not invent a revolutionary method of factoring tomorrow. Therefore a decision on the long-term security of the public-key systems that are based on the difficulty of factoring calls for a subjective judgment of whether or not there will be any major advances in factoring. The recent developments in primality testing serve to emphasize the potential vulnerability of any such code to a theoretical breakthrough.