DISCOVERY

with Neville de Mestre

Prime numbers

The word "prime" comes from the Latin word "primus" meaning "first" or "most important." Hence we have prime minister, prime mover, prime suspect and prime number. A prime number (or prime, for short) is defined as any natural number which has just two factors, itself and 1.

The number 1 is not included in the set of primes because of an agreement by mathematicians concerning a simpler definition of primes. This definition is:

> A prime number is a natural number which has exactly two factors.

Prime numbers are important as the building blocks for the set of all natural numbers, because prime factorisation is an important and useful property of all natural numbers.

Although the earliest prime numbers are listed in many mathematical reference books, your students can discover them by using the method known as the Sieve of Eratosthenes, named after the Greek geographer and astronomer who lived from c. 276–194 BC. Eratosthenes was also famous for being the first to scientifically calculate the Earth's circumference, which he did correctly to within 80 km.

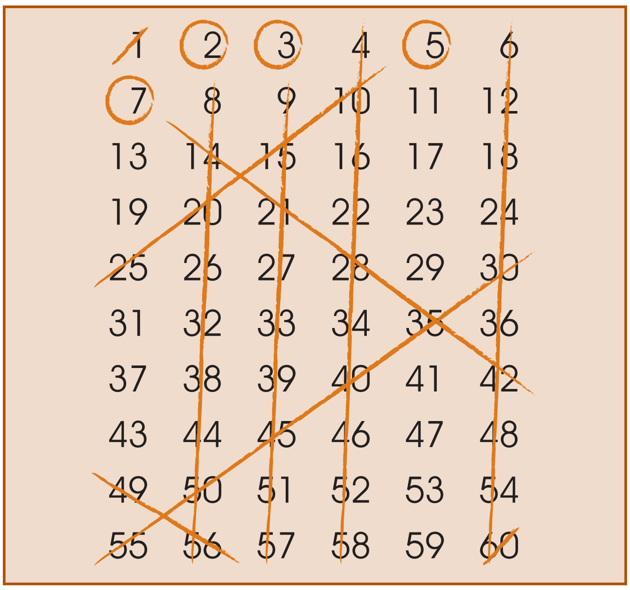

Figure 1. The Sieve of Eratosthenes.

To illustrate his method for obtaining the primes, write down all the natural numbers in rows of six, finishing wherever you like. Here we will stop at 60, but your students might like to go further.

Cancel the number 1 since it is not prime by definition. Circle the first (and only even) prime 2, and cross out all the even numbers because they have more than two factors (at least 1, 2 and themselves). This means that the rest of column two, and all of columns four and six are eliminated.

Circle the next available number 3 as the next prime number. Eliminate all higher numbers which have 3 as a factor. This eliminates all columns three and six (the latter having already been eliminated). Note that at this stage the remaining columns (one and five) contain all the primes greater than 3, but all the numbers in these two columns are not prime. So in the process of using the Sieve we have discovered a very simple rule:

> All prime numbers greater than 3 have the form $6N\pm1$, where N is some natural number.

Continuing with the Sieve method we see that the next available number is 5, so we circle it. We cross out all multiples of 5 using a series of parallel diagonal lines.

We continue with this for the next available number 7 crossing out by diagonal lines in the opposite direction (see Figure 1). Eventually you will be left with the prime numbers less than 60, namely:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.

A discerning eye might notice that we have already obtained the primes in our Sieve by just completing the diagonals based on the prime number 7. Why is this so?

Well, if a natural number greater than 1 is not prime it is called *composite*. Composite numbers have at least two factors which are not itself or 1. Consider 39, which has factors 1, 3, 13, 39. Now 3 and 13 are intermediate factors which are not 39 or 1, and so 39 is not a prime number. Hence if we wanted to see whether or not 39 is prime without using the Sieve we could just divide 39 successively by the natural numbers 2, 3, 4, 5, etc. up to 38 to see if any division produced a zero remainder. We would find that dividing by 3 gave a zero remainder, and so quickly we know that 39 is not prime. Note that division by 13 also produces a zero remainder, but division by 3 has already done the job for us. Therefore, when a number is composite, division by the smaller of the intermediate factors is enough of a test.

Let us try a similar approach with 37. We would divide it successively by 2, 3, 4, up to 36 and find a remainder each time. So we would conclude that 37 is prime. But we would not have to do all these tedious divisions, because we know that just division by 2 sorts out all the even numbers, and so division by 4, 6, 8, … 34, 36 is unnecessary. How far would we have to go dividing by prime numbers to see if 37 is prime or not. Dividing by 2, 3 and 5 successively does not leave a remainder of zero. The next prime is 7, but 7 × 7 = 49 which is greater than 37. If 7 was an intermediate factor of 37 there would have to be another intermediate factor less than 7 — but we have checked them already. So 37 is prime. Essentially we have discovered a simple test for a prime:

> To see if any natural number N is prime or not, divide it by all the prime numbers less than or equal to $\sqrt{N}$ to see if there are any zero remainders. If none, then N is prime.

Figure 1 had all the natural numbers up to 60, so the test only requires us to divide by all the prime numbers less than or equal to $\sqrt{60} \cong 7.8$ in value. These primes are 2, 3, 5 and 7 respectively, and so using the Sieve up to and including 7 was enough.

Ask your students to check whether or not 221 is a prime number? Also ask them to suggest other numbers to try.

Prime numbers are useful for security purposes with codes. Euclid proved that there are an infinite number of prime numbers, so organisations such as banks and governments know that there are plenty of large prime numbers out there to play with. Multiplying two of these large primes together gives a composite number that is difficult to determine its factors if you did not do the original multiplication. The CIA in the United States is supposedly offering US$10 000 for any new prime discovered with more than 100 digits. Finding one takes months of computer time and, when you find one, it may already be known. You can ask your students to look up large primes on the Internet to see comments about the largest prime discovered so far.

Since all prime numbers greater than 3 have the form $6N \pm 1$, it follows that there should be many prime numbers whose difference is 2. These are called twin primes and from the Sieve we can see that the twin primes less than 60 are (3,5) (5,7) (11,13) (17,19) (29,31) and (41,43). An unsolved problem of mathematics is whether or not there are an infinite number of twin primes. Ask your students to find all the twin primes less than 200.

Many people have tried to find a formula for prime numbers, but so far without success. Some of these attempts include $N^2 + N + 11$ (does not hold for $N = 10$ or 11), $N^2 + N + 41$ (does not hold for $N = 40$ or 41), $N^2 - 79N + 1601$ (which gives a prime for all N from 1 to 80, but not for $N = 81$), and

$$2^{2^N} + 1$$

(which holds for $N = 1, 2, 3, 4$ but not 5). It took a long while for someone to show that the factors of $2^{32} + 1$ are 641 and 6 700 417.

Finally here are three problems for your students to think about.

Problem 1

In a popular 2003 novel, "The Curious Incident Of The Dog In The Night-Time," author Mark Haddon numbered his chapters in ascending order of prime numbers. If there are 51 chapters in the book, what is the number of the final chapter?

Problem 2

A teacher said that the product of her age, the age of her dog and the number of her house is 18 067. How old is she?

Problem 3

Take any prime number greater than or equal to 5, square it, add 13, and divide the answer by 12. The remainder is always 2. Why?

Happy discoveries!