OF PRIME INTEREST

As you know, a prime number is any positive integer, other than 1, which has exactly two distinct factors (itself and 1). Thus the set of primes starts 2, 3, 5, 7, 11, . . . , The integers which have more than two distinct factors are called composite numbers. These composite numbers can always be factored until they are expressed as a product of prime numbers, and for each number there is only one such product of primes. These facts are known to Mathematicians as the Fundamental Theorem of Arithmetic.

e.g. $36 = 12 \times 3 = 4 \times 3 \times 3 = 2 \times 2 \times 3 \times 3$ or $36 = 6 \times 6 = 2 \times 3 \times 2 \times 3$ or $36 = 4 \times 9 = 2 \times 2 \times 3 \times 3$

In each case, 36 is factored as the product of two 2's and two 3's (the order of factors is of course unimportant). This expression of an integer as a product of prime factors is of considerable use as the following examples show:

1. 1,764 is a perfect square because
$1{,}764 = 2 \times 2 \times 3 \times 3 \times 7 \times 7$
$= (2 \times 3 \times 7) \times (2 \times 3 \times 7)$
$= 42^2$

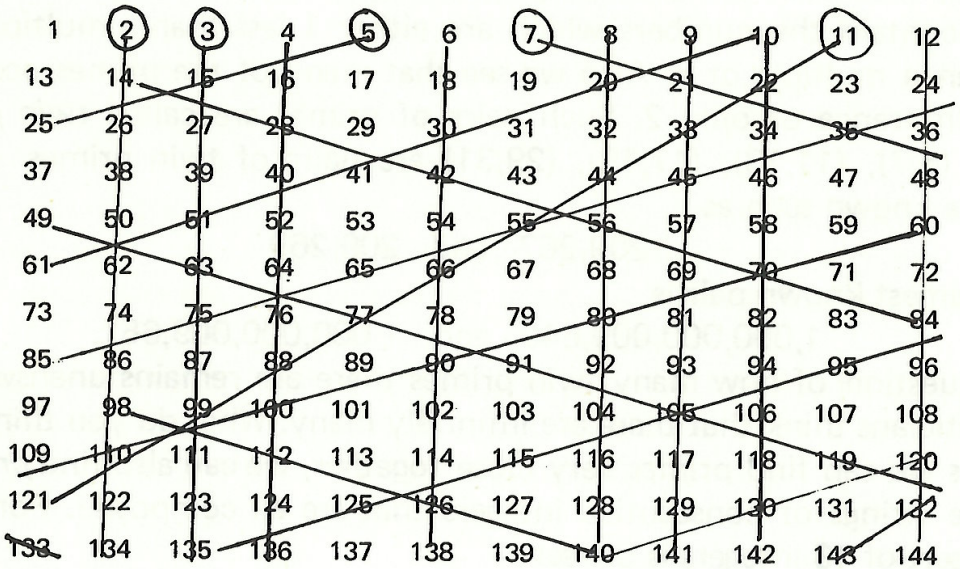
2. 1,764 is divisible by 147 because
$147 = 3 \times 7^2$
and $1{,}764 = 2^2 \times 3^2 \times 7^2$
$= (3 \times 7^2) \times 2^2 \times 3$
$= 147 \times 12.$

3. To find the highest common factor of 441 and 294, write $441 = 3^2 \times 7^2$ and $294 = 2 \times 3 \times 7^2$.
So the highest common factor is 3×7^2 (why?)
$= 147.$

4. To find the lowest common multiple of 441 and 294, write $441 = 3^2 \times 7^2$ and $294 = 2 \times 3 \times 7^2$.
So the lowest common multiple $= 2 \times 3^2 \times 7^2$ (why?)
$= 882.$

If you cannot find a list of prime numbers then you could make your own list, by checking each number to see if it is prime or not. However Eratosthenes of Cyrene (250 BC) found an easier method when he developed a sieve for prime

numbers. To use his sieve, write down a subset of positive integers from 2 upwards in order (you may go as far as you like). Then circle the 2 and cross out all other multiples of 2. The next number in the remaining set is 3. Circle the 3 and proceed to cross out all other multiples of 3. Continue this process of crossing out the composite numbers until you cross out the multiples of the highest prime whose square is a member of the set you are working with. Then the untouched members will be the primes in that see (see table).



A table of primes (Note the straight lines)

Mathematicians have been aware of prime numbers for a very long time, but there still remain many unanswered questions even today. For years, mathematicians have puzzled over the pattern of prime numbers in the integers and we will look at three problems related to this elusive pattern.

1. How many primes are there?

We can see that if the above table were to be extended, more lines of multiples would be deleted. Will the number of these lines increase enough to cross out *every* number after a certain point in the set of integers? In other words, is there a largest prime number?

Euclid (300 BC) supplied us with the answer. He argued that if there were a largest prime number (let us call it p), then the number n, where

$$n = (2 \times 3 \times 5 \times 7 \times \ldots p) + 1$$

could not be factored into primes. We see that 2 does not divide n because there would be a remainder of 1 if we tried to divide n by 2. Similarly, any other prime

up to and including p could not be a factor of n because there would again be a remainder of 1 when we tried to divide n by that prime. But as n is an integer it must have a prime factorization and so p cannot possibly be the largest prime. This shows that the set of primes is infinite.

2. How often do the primes occur?

If we return to our table, we can notice some interesting features in the pattern of primes. You will see that all primes after 3 occur in four columns. These columns contain the numbers which are either 1 less than a multiple of 6 or 1 more than a multiple of 6. Also we see that many of the primes occur in pairs, with a difference of only 2. Such pairs of primes are called *twin primes.* For example (5,7), (11,13), (17,19), (29,31) are pairs of twin primes. Larger twin primes are known such as

209,267 and 209,269

and the largest known pair is

1,000,000,009,649 and 1,000,000,009,651.

The question of how many twin primes there are remains unanswered. Many mathematicians think that there are infinitely many. What do you think?

Just as we can find primes very close together, we can also find *prime deserts.* These are strings of consecutive integers that are all composite. For example, a prime desert of 13 integers is the set

{114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126}.

In fact, it is possible to find prime deserts containing as many integers as you wish. See if you can prove this using problem 3 as a hint.

3. Is there a formula for prime numbers?

One approach that has been used to find a pattern of the prime numbers is to search for a formula f(x) that will generate prime numbers each time the pronumeral x is replaced by an integer. About 300 BC, Euclid tried the formula

$$p = x^2 + x + 17$$

and found that p was a prime when x was replaced by 0,1,2,3, . . . 15 but when x = 16,

$$p = 16^2 + 16 + 17 = 16(16 + 1) + 17 = 17 \times 17$$

which alas is not prime. The formula

$$p = x^2 + x + 41$$

was also found to generate primes when x was replaced by 0,1,2, . . . 39 but replacing x by 40 causes a composite result. It is not hard to see that any such formula of this type is doomed to failure as a prime generator since there is always an obvious replacement for x which will give a composite number. For $p = x^2 + x + 17$ the obvious replacement is of course

$x = 17$ for then we see that

$$p = 17^2 + 17 + 17 = 17(17 + 1 + 1)$$
$$= 17 \times 19 \text{ (composite).}$$

When the constant in the formula is a 1 the replacement that gives a composite result is not so obvious, but it can still be found.

Fermat (1601–1675), a very famous French mathematician, thought that

$$F(n) = 2^{2^n} + 1$$

would be a prime generator. He found that

$$F(0) = 2^{2^0} + 1 = 2^1 + 1 = 3,$$

$F(1) = 5$, $F(2) = 17$, $F(3) = 257$ and $F(4) = 65{,}537$ were primes.

However it did not take Euler, a Swiss mathematician of the time, long to show that $F(5) = 641 \times 6{,}700{,}417$. In fact no other Fermat numbers are known to be prime, although over 30 have been checked (see Vol. 7 No. 1).

Another French mathematician of the same time, Marin Mersenne, gave the formula $2^p - 1$ (where p is a prime) which he claimed would be prime for certain values of p. These primes are called Mersenne primes. It is interesting that it was not until 1903 that $2^{67} - 1$ was found to be a composite number when an American Professor named Cole discovered that

$$2^{67} - 1 = 193{,}707{,}721 \times 761{,}838{,}257{,}287.$$

He said that it took him "every Sunday for three years" to discover this. Is it any wonder? [For more facts about Mersenne numbers, see Vol. 7 No. 2 – Ed.].

Although the search for a formula has proved fruitless, it has provided us with examples of very large prime numbers. For example the largest known prime number is $2^{19937} - 1$, which would take 6,002 digits to write out in full! Maybe you might like to try for a larger one?

Problems

1. In the sieve of Eratosthenes, why can we stop at the highest prime whose square is a member of the chosen set?
2. Why do all the composite numbers in the table lie on straight lines?
3. The integers $1 \times 2 \times 3 \ldots \times 10 \times 11 + 2$, $1 \times 2 \times 3 \ldots \times 10 \times 11 + 3, \ldots 1 \times 2 \times 3 \ldots \times 10 \times 11 + 11$ are all composite. Why? Find a prime desert with at least 100 integers in it.
4. Find the first prime p for which $2^p - 1$ is not a prime.

K. Wilkins