PERFECT NUMBERS

John Cosgrave
(Carysfort)

A natural number m is said to be perfect if the sum of all the divisors of m equals 2m. Thus, 6 and 28 are perfect, because 1,2,3 and 6 are the factors of 6; 1,2,4,7,14 and 28 are those of 28 and 1+2+3+6 = 12 = 2 x 6.

$$1+2+4+7+14+28 = 56 = 2 \times 28.$$

One could say that m is perfect if the sum of all the factors of m, less than m, equals m. Thus

$$1+2+3 = 6$$

and $1+2+4+7+14 = 28$.

Anyone who did the calculations required to find which integers m, with $m \leqslant 1000$ (say), were perfect, would find only three examples, namely 6,28 and 496. These numbers have the following "prime factorization"

$$6 = 2^1 \times 3^1$$

$$28 = 2^2 \times 7^1$$

$$496 = 2^4 \times 31^1$$

3,7,31 are the only proper odd factors of 6,28 and 496 respectively, and they are also primes - not only that, for it is also striking that they are each one less than a power of 2, and also these powers of two are in each case one more than the corresponding power of 2 occurring in the prime decompositions of 6,28 and 496 (namely $2^1, 2^2, 2^3$) so one is led to guess that:

Theorem 1 If the number (2^n-1) is prime, then the number $2^{n-1}(2^n-1)$ is perfect.

Proof Let $p = (2^n-1)$ and suppose p is prime. Then the factors of $2^{n-1}.p$ are as follows:

$$1,2,2^2,\ldots,2^{n-1} \quad \text{(their sum is } (2^n-1))$$

and $p,2p,2^2p,\ldots,2^{n-1}p$ (their sum is $(2^n-1)p$).

Thus the sum of all the factors of $2^{n-1}.(2^n-1)$ is:

$$(2^n-1) + (2^n-1)p, \quad \text{i.e.} \quad (2^n-1)(1+p). \quad \text{This equals } (2^n-1)2^n,$$

which is $2.(2^{n-1}.p)$. So $2^{n-1}(2^n-1)$ is perfect.

Now it could be that 2^4 p is perfect for some prime p other than 31. Lets see what p would have to be like. Suppose 2^4p was perfect, then since the factors of 2^4p are: $1,2,2^2,2^3,2^4$ (whose sum is 31), and $p,2p,2^2p,2^3p,2^4p$ (whose sum is 31p), it would follow that

$$31 + 31p = 2 \times (2^4p) = 32p.$$

$$\text{i.e.} \quad 31 + 31p = 32p$$

$$\text{i.e.} \quad 31 = 32p - 31p = p.$$

so p would have to equal 31 after all!

You are now ready for

Theorem 2 If the integer $2^{n-1}.p$ is perfect, where p is an odd prime, then $p = (2^n-1)$.

Proof The factors of $2^{n-1}.p$ are:

$1, 2, 2^2, \ldots, 2^{n-1}$ (whose sum is (2^n-1))

and $p, 2p, 2^2p, \ldots, 2p^{n-1}$ (whose sum is $(2^n-1)p$),

and it would follow that:

$$(2^n-1) + (2^n-1)p = 2 \times (2^{n-1}p) = 2^n p.$$

$$\text{i.e.} \quad (2^n-1) + (2^n-1)p = 2^n p.$$

$$\text{i.e.} \quad (2^n-1) = 2^n p - (2^n-1)p = p.$$

$$\text{So we have} \quad (2^n-1) = p.$$

Theorem 1 and 2 were known to Euclid and tell us that the only even perfect numbers of the form $2^{n-1}p$ are those for which $p = (2^n-1)$. These perfect numbers are said to be of Euclid type. The theorem of Euler (18th century) states that the only even perfect numbers are those of Euclid type (so there are none of the form, say, $2^4p^2q^3$, where p, q are odd primes).

What we now wish to ask is this, when is the number (2^n-1) a prime number. These numbers are called the Mersenne numbers $(M_n, M_n = (2^n-1))$ after the 17th century French mathematician Mersenne, (see for example, Volume One of Dicksons Theory of Numbers).

M_2, M_3, M_5 and M_7 (i.e. 3,7,31 and 127) are prime, M_4, M_6, M_8, M_9 and M_{10} are composite. It is easy to show that if n is composite then M_n is composite. It was once (wrongly) thought that if n is prime then M_n is prime and this is seen to be false for the next case after M_7 for $M_{11} = (2^n-1) = 2047 = 23 \times 89$.

Theorem 3 If n is composite so also is M_n.

Proof Since n is composite, then $n = a \times b$ for some integers a and b with $a, b \geq 2$. Now $M_n = (2^n-1) = (2^{ab}-1)$

$$= (2^a-1)(2^{a(b-1)}+\ldots+2^b+1).$$

Now $a \geq 2 \Rightarrow (2^a-1) \geq (2^2-1) = 3$,

and $b \geq 2 \Rightarrow (2^{a(b-1)}+\ldots+2^b+1) \geq (\text{——} +2^2+1) = 5$.

Thus M_n is the product of two integers (2^4-1) and $(2^{a(b-1)}+\ldots+2^b+1)$ neither of which is 1, and so M_n is composite.

So we are now interested in the numbers $M_2, M_3, M_5, M_7, M_{11}, M_{13}, M_{17}, M_{19}, M_{23}, M_{29}, M_{31}, \ldots$ i.e. the Mersenne numbers with prime suffix. M_2, M_3, M_5 and M_7 were known to be prime by A.D.100, Regius (1536) noted that M_{11} is composite. Cataldi (1603) showed that M_{13}, M_{17} and M_{19} are primes (by checking for prime divisors a la Eratosthenes), but erred in claiming that so also are M_{23} and M_{29} and M_{37} (why did he not say anything about M_{31}?). These last three were put right by Fermat (1640) who showed that $(2^{23}-1)$ is divisible by 47, and that $(2^{37}-1)$ is divisible by 223; and Euler (1732) who showed that $(2^{29}-1)$ is divisible by 1103.

In 1644, Mersenne claimed that the first eleven perfect numbers are given by $2^{p-1}(2^p-1)$ for $p = 2,3,5,7,13,17,19,31,67,127,257$; but he erred at least in including 67 and excluding 61,89 and 107. Laczo (1867) proved that $(2^{67}-1)$ is composite (without actually exhibiting a factorization). Cole (1903) gave an explicit factorization of M_{67} which was

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

Euler (1750) showed that $(2^{31}-1)$ is prime;

Lucas (1876) showed that $(2^{127}-1)$ is prime;

Pervouchini (1883) showed that $(2^{61}-1)$ is prime;

Powers (1911) showed that $(2^{89}-1)$ is prime;

Powers (1914) showed that $(2^{107}-1)$ is prime.

So all the Mersenne primes (in order) up to M_{127} are:

$$M_{2,3,5,7,13,17,19,31,61,89,107,127}.$$

$$M_{127} = 170,141,183,460,469,231,731,687,303,715,884,105,727.$$

D. Lehiner (1951-52) showed that $(2^{521}-1)$, $(2^{607}-1)$, $(2^{1279}-1)$, $(2^{2203}-1)$ and $(2^{2281}-1)$ are primes. Riesel (1958) showed that $(2^{3217}-1)$ is prime. Harwitz (1960?) showed that $(2^{4253}-1)$ and $(2^{4423}-1)$ are primes. Gollies (1964) showed that $(2^{9689}-1)$, $(2^{9941}-1)$ and $(2^{112,3}-1)$ are primes. Tuckermann (1971) showed that $(2^{19937}-1)$ is prime. Lastly, the 25th Mersenne prime was discovered on the 30 October 1978 by two 18 year old students (at the California State University), Laura Nickel and Kurt Noll:

$$M_{21,701} = (2^{21,701}-1) \text{ is prime,}$$

and so,

$$2^{21,700}(2^{21,701}-1) \text{ is the 25th even perfect number.}$$

<u>Theorem</u> (Euler): Let p be an odd prime, then any prime factor of $M_p(=(2^p-1))$ must be of the form $(2np+1)$ for some integer n. This, together with the observation that if a number N is composite it has a prime factor $\leq\sqrt{N}$, enabled Euler to verify the primality of Mp for small values of p. To take an example: to check if $(2^{13}-1)$ is prime, $(2^{13}-1) = 8191$. According to Euler, any prime factor of $(2^{13}-1)$ must be of the form $(2n.13)+1$, i.e. of the form $(26n+1)$. According to Eratosthenes we need only search for prime divisors up to 8191, which is between 90 and 91. Now when

Now when $n=1$, $26n+1 = 27$ is not prime;
$n=2$, $26n+1 = 53$ is prime;
$n=3$, $26n+1 = 79$ is prime;
$n\geq 4$, $26n+1 \geq 105 > 91$; so no need to check.

Now it only remains to check if 53 or 79 divide 8191. If neither does, we know 8191 is prime. You should check to see.

The Euler test involves so much calculation for large p as to make his test of no practical value. The following test (the only one used - the only other one, in fact) is the one which has been used since 1876.

<u>Lucas-Lehmer Theorem</u>: Let p = 3,5,7,11,13,17,19,... (odd prime). Define the sequence $\{a_n\}$ as follows:

$$a_1 = 14, \quad a_2 = a_1^2-2, \quad a_3 = a_2^2-2 \text{ etc.}$$

Then (i) if M_p divides a_{p-2}, M_p is prime.
(ii) if M_p does not divide a_{p-2}, M_p is composite.

<u>Examples</u> <u>When p=3</u>. $M_p = 2^3-1 = 7$. $a_{p-2} = a_{3-2} = a_1 = 14$ and here M_p divides a_{p-2}, and M_p (i.e. 7) is prime.

<u>When p=5</u>. $M_p = (2^5-1) = 31$. $a_{p-2} = a_{5-2} = a_3$. Now $a_1 = 14$. $a_2 = 14^2-2 = 196-2 = 194$. $a_3 = 194^2-2 = 37636-2 = 37634$, therefore M_5 divides a_3, and 31 divides 37634, therefore M_5 is prime.

Shorter Solution (using congruences)

$a_1 = 14$, $a_2 = 14^2 - 1 = 196-2 = 194$.

Now $a_2 = 194 \equiv 8 \pmod{31}$ (since $\underline{194} = (6.31)+8$)

Therefore $a_2 \equiv 8^2 \pmod{31}$

$a_2^2 - 2 \equiv 8^2 - 2 \equiv 64-2 \equiv 62 \equiv 0 \pmod{31}$

$a_3 \equiv 0 \pmod{31}$. Therefore M_5 divides a_3, and M_5 is prime.

SECONDARY SCHOOL MATHEMATICS

T.J. Laffey

There has been quite an amount of discussion for some time now on the content of mathematics courses in secondary schools. Many people feel that there has been a general decline in the level of computational skill and ability to solve problems in students who leave school. Various attempts are being made to identify the reasons for this and to find remedies. Among the reasons suggested are the following:-

(1) The "New Math",

(2) Over-emphasis on teaching "concepts" and a feeling that as long as the "concepts" are O.K., the answer doesn't matter,

(3) The more abstract presentation of material, particularly geometry, with the result that the students are not taught to relate mathematics to commonsense and experience,

(4) An unwillingness on the part of teachers and pupils to spend large amounts of time going through, perhaps somewhat dull and repetitive routines, in order that students get to know these techniques thoroughly.

At present, there is a great deal of debate going on throughout the world on the value of the so-called New Math. (i.e. sets, relations