2.5. Fermat's and Mersenne's numbers. The first four Fermat numbers are prime, and Fermat conjectured that all were prime. Euler, however, found in 1732 that

$$F_5 = 2^{2^5} + 1 = 641.6700417$$

is composite. For

$$641 = 5^4 + 2^4 = 5.2^7 + 1$$

divides each of $5^4 . 2^{28}+2^{32}$ and $5^4.2^{28} - 1$ and so divides their difference F_5.

In 1880 Landry proved that

$$F_6 = 2^{2^6} + 1 = 274177.67280421310721.$$

More recent writers have proved that F_n is composite for

$$7 \leqslant n \leqslant 16, n = 18, 19, 21, 23, 36, 38, 39, 55, 63, 73$$

and many larger values of n. No factor is known for F_{14}, but in all the other cases proved to be composite a factor is known.

No prime F_n has been found beyond F_4, so that Fermat's conjecture has not proved a very happy one. It is perhaps more probable that the number of primes F_n is finite.† If this is so, then the number of primes 2^n+1 is finite, since it is easy to prove

THEOREM 17. *If $a \geqslant 2$ and $a^n + 1$ is prime, then a is even and $n = 2^m$.*

For if a is odd then $a^n + 1$ is even; and if n has an odd factor k and $n = kl$, then $a^n + 1$ is divisible by

$$\frac{a^{kl} + 1}{a^l + 1} = a^{(k-1)l} - a^{(k-2)l} + \cdots + 1.$$

† This is what is suggested by considerations of probability. Assuming Theorem 7, one might argue roughly as follows. The probability that a number n is prime is at most

$$\frac{A}{\log n},$$

and therefore the total expectation of Fermat primes is at most

$$A\sum\left\{\frac{1}{\log(2^{2^n}+1)}\right\} < A\sum 2^{-n} < A.$$

This argument (apart from its general lack of precision) assumes that there are no special reasons why a Fermat number should be likely to be prime, while Theorems 16 and 17 suggest that there are some.

It is interesting to compare the fate of Fermat's conjecture with that of another famous conjecture, concerning primes of the form $2^n - 1$. We begin with another trivial theorem of much the same type as Theorem 17.

THEOREM 18. *If $n > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime.*

For if $a > 2$, then $a - 1 | a^n - 1$; and if $a = 2$ and $n = kl$, then we have $2^k - 1 | 2^n - 1$.

The problem of the primality of $a^n - 1$ is thus reduced to that of the primality of $2^p - 1$. It was asserted by Mersenne in 1644 that $M_p = 2^p - 1$ is prime for

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257,$$

and composite for the other 44 values of p less than 257. The first mistake in Mersenne's statement was found about 1886,† when Pervusin and Seelhoff discovered that M_{61} is prime. Subsequently four further mistakes were found in Mersenne's statement and it need no longer be taken seriously. In 1876 Lucas found a method for testing whether M_p is prime and used it to prove M_{127} prime. This remained the largest known prime until 1951, when, using different methods, Ferrier found a larger prime (using only a desk calculating machine) and Miller and Wheeler (using the EDSAC 1 electronic computer at Cambridge) found several large primes, of which the largest was

$$180M_{127}^2 + 1,$$

which is larger than Ferrier's. But Lucas's test is particularly suitable for use on a binary digital computer and it has subsequently been applied by a succession of investigators (Lehmer and Robinson, Hurwitz and Selfridge, Riesel, Gillies, Tuckerman and finally Nickel and Noll). As a result it is now known that M_p is prime for

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107,$$
$$127, 521, 607, 1279, 2203, 2281, 3217,$$
$$4253, 4423, 9689, 9941, 11213, 19937, 21701,$$

and composite for all other $p < 21700$. The largest known prime is thus M_{21701}, a number of 6533 digits.‡

† Euler stated in 1732 that M_{41} and M_{47} are prime, but this was a mistake.

‡ See the end of chapter notes.

But, by Theorem 62,

$$\frac{\phi(n)}{\phi(N)} = \frac{n}{N} \prod_{p|n, p\nmid N} \left(1 - \frac{1}{p}\right) = a \prod_{p|n, p\nmid N} \left(1 - \frac{1}{p}\right)$$

and Theorem 272 follows at once.

When $m = 1$, we have $c_n(1) = \mu(n)$, that is

$$\mu(n) = \sum_{\substack{1 \leqslant h \leqslant n \\ (h,n)=1}} e\left(\frac{h}{n}\right). \tag{16.6.4}$$

16.7. The functions $d(n)$ and $\sigma_k(n)$. The function $d(n)$ is the number of divisors of n, including 1 and n, while $\sigma_k(n)$ is the sum of the kth powers of the divisors of n. Thus

$$\sigma_k(n) = \sum_{d|n} d^k, \quad d(n) = \sum_{d|n} 1,$$

and $d(n) = \sigma_0(n)$. We write $\sigma(n)$ for $\sigma_1(n)$, the sum of the divisors of n.

If

$$n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l},$$

then the divisors of n are the numbers

$$p_1^{b_1} p_2^{b_2} \dots p_l^{b_l},$$

where

$$0 \leqslant b_1 \leqslant a_1, \quad 0 \leqslant b_2 \leqslant a_2, \quad \dots, \quad 0 \leqslant b_l \leqslant a_l.$$

There are

$$(a_1 + 1)(a_2 + 1) \dots (a_l + 1)$$

of these numbers. Hence

THEOREM 273:

$$d(n) = \prod_{i=1}^{l} (a_i + 1).$$

More generally, if $k > 0$,

$$\sigma_k(n) = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \dots \sum_{b_l=0}^{a_l} p_1^{b_1 k} p_2^{b_2 k} \dots p_l^{b_l k}$$

$$= \prod_{i=1}^{l} \left(1 + p_i^k + p_i^{2k} + \dots + p_i^{a_i k}\right).$$

Hence

THEOREM 274:

$$\sigma_k(n) = \prod_{i=1}^{l} \left(\frac{p_i^{(a_i+1)k} - 1}{p_i^k - 1}\right).$$

In particular,

THEOREM 275:

$$\sigma(n) = \prod_{i=1}^{l} \left(\frac{p_i^{a_i+1} - 1}{p_i - 1}\right).$$

16.8. Perfect numbers. *A perfect* number is a number n such that $\sigma(n) = 2n$. In other words a number is perfect if it is the sum of its divisors other than itself. Since $1 + 2 + 3 = 6$, and

$$1 + 2 + 4 + 7 + 14 = 28,$$

6 and 28 are perfect numbers.

The only general class of perfect numbers known occurs in Euclid.

THEOREM 276. *If $2^{n+1} - 1$ is prime, then $2^n(2^{n+1} - 1)$ is perfect.*

Write $2^{n+1} - 1 = p, N = 2^n p$. Then, by Theorem 275,

$$\sigma(N) = (2^{n+1} - 1)(p + 1) = 2^{n+1}(2^{n+1} - 1) = 2N,$$

so that N is perfect.

Theorem 276 shows that to every Mersenne prime there corresponds a perfect number. On the other hand, if $N = 2^n p$ is perfect, we have

$$\sigma(N) = (2^{n+1} - 1)(p + 1) = 2^{n+1} p$$

and so

$$p = 2^{n+1} - 1.$$

Hence there is a Mersenne prime corresponding to any perfect number of the form $2^n p$. But we can prove more than this.

THEOREM 277. *Any even perfect number is a Euclid number, that is to say of the form* $2^n(2^{n+1} - 1)$, *where* $2^{n+1} - 1$ *is prime.*

We can write any such number in the form $N = 2^n b$, where $n > 0$ and b is odd. By Theorem 275, $\sigma(n)$ is multiplicative, and therefore

$$\sigma(N) = \sigma(2^n)\sigma(b) = (2^{n+1} - 1)\sigma(b).$$

Since N is perfect,

$$\sigma(N) = 2N = 2^{n+1} b;$$

and so

$$\frac{b}{\sigma(b)} = \frac{2^{n+1} - 1}{2^{n+1}}.$$

The fraction on the right-hand side is in its lowest terms, and therefore

$$b = (2^{n+1} - 1)c, \quad \sigma(b) = 2^{n+1} c,$$

where c is an integer.

If $c > 1$, b has at least the divisors $b, c, 1$, so that

$$\sigma(b) \geqslant b + c + 1 = 2^{n+1} c + 1 > 2^{n+1} c = \sigma(b),$$

a contradiction. Hence $c = 1$, $N = 2^n(2^{n+1} - 1)$, and

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

But, if $2^{n+1} - 1$ is not prime, it has divisors other than itself and 1, and

$$\sigma(2^{n+1} - 1) > 2^{n+1}.$$

Hence $2^{n+1} - 1$ is prime, and the theorem is proved.

The Euclid numbers corresponding to the Mersenne primes are the only perfect numbers known. It seems probable that there are no odd perfect numbers, but this has not been proved. The most that is known in this direction is that any odd perfect number must be greater than 10^{200}, that it must have at least 8 different prime factors and that its largest prime factor must be greater than 100110.†

16.9. The function $r(n)$. We define $r(n)$ as the number of representations of n in the form

$$n = A^2 + B^2,$$

where A and B are rational integers. We count representations as distinct even when they differ only 'trivially', i.e. in respect of the sign or order of A and B. Thus

$$0 = 0^2 + 0^2, \quad r(0) = 1;$$

$$1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2, \quad r(1) = 4;$$

$$5 = (\pm 2)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 2)^2, \quad r(5) = 8.$$

We know already (§ 15.1) that $r(n) = 8$ when n is a prime $4m + 1$; the representation is unique apart from its eight trivial variations. On the other hand, $r(n) = 0$ when n is of the form $4m + 3$.

We define $\chi(n)$, for $n > 0$, by

$$\chi(n) = 0 \ (2 \mid n), \quad \chi(n) = (-1)^{\frac{1}{2}(n-1)} \ (2 \nmid n).$$

Thus $\chi(n)$ assumes the values $1, 0, -1, 0, 1, \ldots$ for $n = 1, 2, 3, \ldots$. Since

$$\tfrac{1}{2}(nn' - 1) - \tfrac{1}{2}(n - 1) - \tfrac{1}{2}(n' - 1) = \tfrac{1}{2}(n - 1)(n' - 1) \equiv 0 \pmod 2$$

When n and n' are odd, $\chi(n)$ satisfies

$$\chi(nn') = \chi(n)\chi(n')$$

for all n and n'. In particular $\chi(n)$ is multiplicative in the sense of § 5.5.

It is plain that, if we write

$$\delta(n) = \sum_{d \mid n} \chi(d), \tag{16.9.1}$$

then

$$\delta(n) = d_1(n) - d_3(n), \tag{16.9.2}$$

† See end of chapter notes.