Chapter 3
Primes

As we go to larger and larger integers, primes become rarer and rarer. Is there a largest prime after which all whole numbers are composite? This sounds counterintuitive and, in fact, it isn't true, as Euclid demonstrated a long time ago. Actually, he did it without demonstrating any primes – he just showed that assuming a finite number of primes leads to a neat contradiction.

Primes are found by sieves, not by formulas, the classical sieve having been designed by Eratosthenes in classic Greece. (Formulas that pretend to give only primes are really shams.) Primality testing has advanced to a stage where the primality or compositeness of 100-digit numbers can now be ascertained by computer in less than a minute, without actually giving any of the factors [3.1]. Factoring, on which the security of certain kinds of cryptographic systems depends (Chaps. 10–15), is still very difficult at this writing.

The largest primes known are of a special form called *Mersenne* primes because they don't hide their compositeness too well and, indeed, some were discovered by high-school students. The largest Mersenne prime known (in mid-1983) has 25,962 digits! Mersenne primes lead to even *perfect numbers* and to prime "repunits", meaning repeated units, i. e., numbers consisting exclusively of 1's in any given base system. (The Mersenne primes are repunits in the binary number system.)

Of special interest are the *Fermat primes* of which, in spite of Fermat's expectations, only 5 are known, the largest one being 65537. Each Fermat prime allows the construction of a regular polygon by using only straightedge and compass – Gauss's great discovery made just before he turned nineteen.

3.1 How Many Primes are There?

Again we turn to Euclid, who proved that there are infinitely many primes by giving one of the most succinct indirect proofs of all of mathematics:

Suppose that the number of primes is finite. Then there is a largest prime p_r. Multiply all primes and add 1:

$$N = p_1 p_2 \ldots p_r + 1 .$$

M. Schroeder, *Number Theory in Science and Communication*, 5th ed.,
DOI 10.1007/978-3-540-85298-8_3, © Springer-Verlag Berlin Heidelberg 2009

Now N is larger than p_r and thus cannot be a prime because p_r was assumed to be the largest prime. Thus N must have a prime divisor. But it cannot be any of the *known* primes because by construction of N, all known primes divide $N-1$ and therefore leave the remainder 1 when dividing N. In other words, none of the known primes divides N. Thus, there is a prime larger than p_r – a contradiction! We must therefore conclude that there is no largest prime, i. e., that there are infinitely many.

In actual fact, the above construction *often* (but not always) does give a prime. For example:

$$\begin{aligned}
&2+1=3\\
&2\cdot 3+1=7\\
&2\cdot 3\cdot 5+1=31\\
&2\cdot 3\cdot 5\cdot 7+1=211\\
&2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311,
\end{aligned}$$

all of which are prime. *But*

$$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=30031=59\cdot 509.$$

Suppose we set $P_1 = 2$ and call P_{n+1} the largest prime factor of $P_1P_2\ldots P_n+1$. Is the sequence P_n monotonically increasing? No! Both P_9 and P_{10} have 16 decimal digits but P_{10} equals only about $0.3\,P_9$.

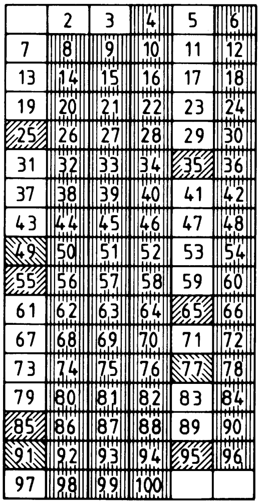
3.2 The Sieve of Eratosthenes

Like gold nuggets, primes are mostly found by sieves – the first one having been designed in ancient Greece by Eratosthenes of Kyrene around 200 B.C. Eratosthenes's sieve idea is charmingly simple.

To find the primes below 100, say, write down the integers from 1 to 100 in order. Then, after 2, cross out every second one $(4,6,8\ldots)$, in other words all the even numbers, because they are divisible by 2 and therefore not prime (except 2 itself). Then, after 3, cross out every third number that is still standing $(9,15,21\ldots)$ because these numbers are divisible by 3 and therefore also not prime. Repeat the crossing out process for every fifth number after 5 and every seventh number after 7. The remaining numbers (except 1, which is not considered a prime) are the 25 primes below 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,
53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Roughly speaking, to find the primes below a given integer N, we only have to use sieving primes smaller than $\sqrt{N}$. (This rule would tell us that by sieving with 2, 3, 5 and 7 we will find all primes below $11^2 = 121$, while actually we have found 4 more primes.)



	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100		

Fig. 3.1 The sieve of Eratosthenes (modulo 6)

In applying Eratosthenes's sieve method there is an additional trick that simplifies matters considerably: we write the integers in six columns starting with 1 (Fig. 3.1). Then only the first and the fifth columns (no pun) contain primes because all numbers in the second, fourth, and sixth columns are divisible by 2, and those in the third column are divisible by 3.

To eliminate the numbers divisible by 5 and 7 as well, a few 45° diagonals have to be drawn, as shown in Fig. 3.1.

Things become a little more complicated if we include the next two primes, 11 and 13, in our sieve because the numbers divisible by 11 and 13 follow "knight's-move" patterns as known from chess. But then we have already eliminated all composite numbers below $17 \cdot 19 = 323$. In other words, we have caught the 66 primes up to 317 in our 6-prime sieve.

Sieving may connote a child playing in a sandbox or a gold digger looking for a prime metal, but sieving in number theory is a very respectable occupation and sometimes the only method of finding an elusive prime or unmasking a composite as such. Of course, the sieving algorithms employed today are becoming increasingly sophisticated. We will hear more about the search for primes, especially the urgently needed very large ones, in subsequent chapters.

3.3 A Chinese Theorem in Error

The ancient Chinese had a test for primality. The test said that n is prime iff[1] n divides $2^n - 2$:

$$n|(2^n - 2). \tag{3.1}$$

[1] Here and in the rest of this book, "iff" means *if and only if.* Further, x "divides" y means that x divides y *without leaving a remainder.* As a formula this is written with a vertical bar: $x|y$.

As we shall prove later, (3.1) is indeed true if n is an odd prime (by Fermat's theorem). Of course, for $n = 2$, (3.1) is trivially true.

Example: for $n = 5$, $2^n - 2 = 30$, which is indeed divisible by 5.

Conversely, for odd $n < 341$, if n is *not* prime n does *not* divide $2^n - 2$.

Example: for $n = 15$, $2^n - 2 = 32{,}766$, which is *not* divisible by 15.

Fortunately (for their self-esteem!), the ancient Chinese never tried $n = 341$, which is composite: $341 = 11 \cdot 31$ and yet 341 divides $2^{341} - 2$ without remainder. This might be a bit hard to check by abacus, but the test is within reach of many a programmable pocket calculator. Of course, the calculation does not give the quotient $(2^{341} - 2)/341$, a number 101 digits long, but rather the remainder, which is 0, thereby falsely asserting that $341 = 11 \cdot 31$ is prime.

The rules for calculating high powers efficiently will be given later, together with a "fast" calculator program.

3.4 A Formula for Primes

In 1947, *Mills* [3.2] showed that there is a constant A, such that $\lfloor A^{3^n} \rfloor$ is[2] prime for every n. Here we have a formula that, although it does not generate each and every prime, could be used to generate arbitrarily large primes – for which the sieve methods are less suited.

For anyone who has an appreciation of what a precious thing a prime is, this seems impossible. And indeed, there is trickery at play here, albeit cleverly hidden trickery: determination of the constant A presupposes prior knowledge of the primes! This trickery is explained in the excellent little book by *Nagell* [3.3], but it *is* a bit tricky, and we will illustrate the point by another, not quite so surreptitious, trick. Consider the real constant

$$B = 0.203000500000007000000000000000110\ldots. \qquad (3.2)$$

Upon multiplying by 10 and taking the integer part, one obtains 2 – the first prime. Dropping the integer part, multiplying by 100, and taking the integer part then gives 3 – the second prime. In general, after the nth prime has been extracted from B, multiplying by 10^{2^n} and taking the integer part yields the $(n+1)$th prime. Thus, we have specified a (recursive) algorithm[3] for specifying not only primes but *all* the primes, and in proper order at that!

[2] The so-called "Gauss bracket" or "floor function" $\lfloor x \rfloor$ is defined as the largest integer not exceeding x. Thus, $\lfloor 4.9 \rfloor = 4$; but $\lfloor 5.0 \rfloor = 5$. The Gauss bracket (for $x \geq 0$) corresponds to the instruction "take integer part", often designated by INT in computer programs.

[3] Can the reader specify a nonrecursive algorithm, i. e., one that gives the nth prime directly, without calculating all prior ones?

Of course, here the trick is patently transparent: we have simply “seeded” the primes, one after another, into the constant B, interspersing enough 0’s so that they do not “run into” each other. In other words, the constant B does not yield any primes that are not already known. (How many 0’s between seeded primes are required to guarantee that adjacent primes do not overlap in B? If 0’s are considered expensive because they make B very long, that question is not easy to answer and, in fact, requires a little “higher” number theory.)

Apart from (3.2) and Mill’s formula, there have been many other prescriptions for generating primes or even “all” primes. Most of these recipes are just complicated sieves in various disguises, one of the few really elegant ones being Conway’s Prime Producing Machine (cf. R. K. Guy, Math. Mag. *56*, 26–33 (1983)). Other attempts, making use of Wilson’s theorem (Sect. 8.2), are hilarious at best and distinguished by total impracticality. All this (non)sense is reviewed by U. Dudley in a delightful article (“Formulas for Primes”, Math. Mag. *56*, 17–22 (1983)).

One of the most astounding algorithms for producing primes, in fact seemingly all of them and in perfect order, is the *Perrin sequence*. This sequence is defined by the recursion $A(n+1) = A(n-1) + A(n-2)$, with the initial condition $A(0) = 3$, $A(1) = 0$, and $A(2) = 2$ (cf. I. Stewart, Sci. Am. *247*, 6, 102–103 (June 1996)). Lucas has proved that whenever n is prime n divides $A(n)$. But the converse also seemed to be true: if n divides $A(n)$, n is prime. But alas, a first counterexample was found for $n = 271441 = 521^2$.

3.5 Mersenne Primes

A *Mersenne number* is a number $M_p = 2^p - 1$, where p is *prime*. If M_p itself is prime, then it is called a *Mersenne prime*. Note that numbers of the form $2^n - 1$, where n is composite, can never be prime because, for $n = pq$,

$$2^n - 1 = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + \ldots + 1), \tag{3.3}$$

However, not all primes p yield Mersenne primes, the first exception being $p = 11$, because $2^{11} - 1 = 2047 = 23 \cdot 89$. Still, there is a fairly simple primality test for numbers of the form $2^p - 1$, the so-called Lucas Test: $2^p - 1$ is prime *iff* (note the double f, meaning *if and only if*) M_p divides S_p $(p > 2)$, where S_n is defined by the recursion

$$S_n = S_{n-1}^2 - 2, \tag{3.4}$$

starting with $S_2 = 4$.

Thus, for example, S_{11} is given by the 10th number in the sequence

$$4,\ 14,\ 194,\ 37634, \ldots,$$

which is not divisible by $M_{11} = 2047$. Thus, M_{11} is composite.

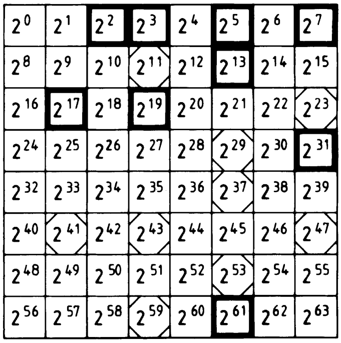


Fig. 3.2 Mersenne primes on a checkerboard

While this test does not reveal any factors, there is another test that *can* give a factor for M_p with $p = 4k + 3$: for $q = 2p + 1$ prime, $q|M_p$ *iff* $p \equiv 3 \bmod 4$.

Example: $p = 11 = 4 \cdot 2 + 3$; $M_{11} = 2047$ is not divisible by $(p-1)/2 = 5$ and is therefore divisible by $2p + 1 = 23$. Check: $2047 = 23 \cdot 89$. Check! Similarly, 47 is discovered as a factor of $M_{23} = 8388607$, etc.

Figure 3.2 shows the first 9 Mersenne primes arranged on a checkerboard. On January 17, 1968, the largest known prime was the Mersenne prime $2^{11213} - 1$, an event that was celebrated with a postmark (Fig. 3.3) from Urbana, Illinois (at no profit to the U.S. Post Office, considering the zero value of the stamp).

In the meantime, much larger Mersenne primes have been found. The record on November 18, 1978, stood at $2^{21701} - 1$, a prime with 6533 decimal digits found by two California high-school students, Laura Nickel and Curt Noll, using 440 hours on a large computer. The next Mersenne prime is $2^{23209} - 1$. By early 1982 the largest known prime was $2^{4497} - 1$, having 13395 digits [3.4].

More recently, another Mersenne prime was discovered by D. Slowinski, the 28th known specimen: $2^{86243} - 1$. Assuming that there are no other Mersenne primes between it and $M(27) = 2^{44497} - 1$, then $2^{86243} - 1$ is, in fact, $M(28)$.

Are there more Mersenne primes beyond $2^{86243} - 1$? The answer is almost certainly *yes*. Curiously, we can even say roughly how large the next Mersenne prime is: 10^{38000} – give or take a dozen thousand orders of magnitude. How can we make such a seemingly outrageous statement?

Fermat and Euler proved that all factors of M_p must be of the form $2kp + 1$ and simultaneously of the form $8m \pm 1$. Thus, *potential* factors of M_p are spaced on average $4p$ apart. Assuming that, subject to this constraint, the number of factors of a Mersenne number is governed by a Poisson process, Gillies [3.5] conjectured that of all the primes in the "octave" interval $(x, 2x)$, on average approximately 2

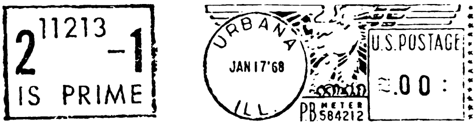


Fig. 3.3 The largest known Mersenne prime on Januar 17, 1968

give Mersenne primes. More precisely, the density of primes near p giving rise to Mersenne primes $M_p = 2^p - 1$ would be asymptotic to

$$\frac{2}{p \ln 2}.$$

In a recent paper S. S. Wagstaff, Jr. ("Divisors of Mersenne primes", Math. Comp. *40*, 385–397 (1983)), following an argument by H. W. Lenstra, Jr., suggested that the expected number of primes p in an octave interval is $e^\gamma = 1.78\ldots$. Thus, the correct asymptotic density would be

$$\frac{e^\gamma}{p \ln 2}.$$

Comparing this with the general prime density for primes near p, $1/\ln p$, we see that of

$$\frac{p}{e^\gamma \log_2 p}$$

primes, one prime on average leads to a Mersenne prime. For $p \approx 100000$, this means that roughly every 3000th prime gives a Mersenne prime. (The appearance of the factor e^γ is a consequence of Merten's theorem, see Sect. 12.1, and its relevance to prime sieving.)

The distribution of primes p that generate Mersenne primes is expressed even more simply if we consider the density of $\log_2 p$: it is constant and should equal e^γ. Since $\log_2 p$ very nearly equals $\log_2(\log_2 M_p)$, these statements are equivalent to the following: if $\log_2(\log_2 M(n))$ is plotted as a function of n, we can approximate the empirical "data" by a straight line with a slope of about $1/e^\gamma = 0.56$. In fact, for the 27 smallest Mersenne primes $(2 \leq p \leq 44497)$ the average slope is 0.57, remarkably close to $1/e^\gamma$. The correlation coefficient between $\log_2(\log_2 M(n))$ and n in this range exceeds 0.95.

Figure 3.4 shows $\log_2(\log_2 M(n))$ versus n for 28 known Mersenne primes (assuming $n = 28$ for $p = 86243$). The great regularity is nothing short of astounding.

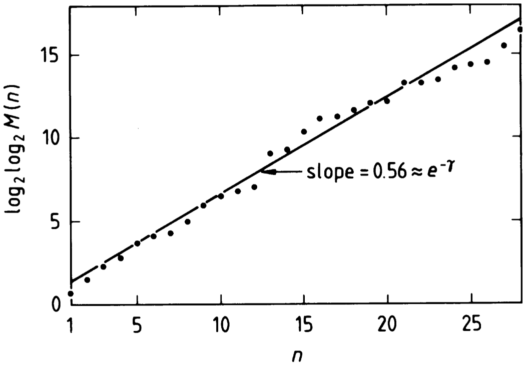


Fig. 3.4 $\log_2(\log_2 M(n))$ versus n

As a Poisson process, the cumulative distribution P of the *intervals* between successive values of $\log_2(\log_2 M(n))$ should go according to the exponential law:

$$P = 1 - \mathrm{e}^{-d/\overline{d}}$$

with $\overline{d} = 1/\mathrm{e}^{\gamma}$. This function is plotted in Fig. 3.5 together with the empirical evidence (in interval ranges of 0.2). Here again, the correspondence with the theoretical result expected from a Poisson process is very good. Specifically, the mean interval (0.57) is close to the standard deviation (0.51) and (beyond the information contained in Fig. 3.5) successive intervals are nearly uncorrelated (correlation coefficient $= -0.17$).

Using 0.56 as the average increment of $\log_2(\log_2 M(n))$ with n, we expect the next Mersenne prime above $2^{86243} - 1$ in the "neighbourhood" of $2^{130000} \approx 10^{38000}$. Of course, to find a prime in this vast "haystack" that gives a Mersenne prime is no small order.

More accurately, we can say that the *probability* of finding the next Mersenne prime either below or above 10^{34000} is about 0.5, and the probability that it exceeds 10^{65000} is less than 10 %. But where is it, *exactly* – not with an uncertainty of thousands of orders of magnitude? Even the fastest number crunchers available today, using the most efficient search algorithms, will have a hey (hay?) day.

Unfortunately, the Mersenne primes are very thinly seeded. Thus, if one is looking for a 50-digit prime among the Mersenne primes, one is out of luck: $2^{127} - 1$ has 39 digits and the *next* Mersenne prime, $2^{521} - 1$, has 157 digits – an awesome gap!

Does a Mersenne prime M_p always yield another Mersenne prime by the formula

$$2^{M_p} - 1\ ?$$

This had been widely conjectured, but a counterexample is now known: the prime $p = 13$ gives a Mersenne prime $M_{13} = 8191$, but $2^{8191} - 1$ is composite. Too bad! The nearest Mersenne primes, $2^{4423} - 1$ and $2^{9689} - 1$, have 1332 and 2917 decimal digits, respectively – leaving another great void.

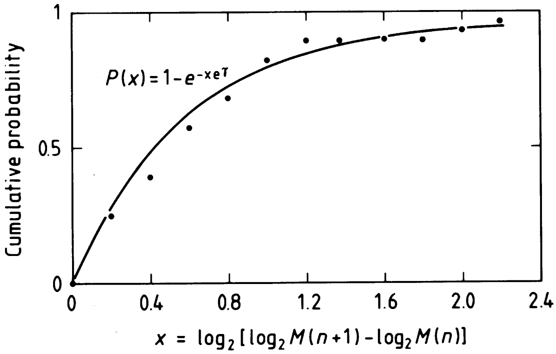


Fig. 3.5 Interval statistics

3.6 Repunits

Expressed as binary numbers, all numbers of the form $2^n - 1$ consist exclusively of 1's, namely exactly n 1's. For example $M_4 = 2^4 - 1 = 15$, or 1111 in binary. Similarly, for any a, $(a^n - 1)/(a - 1)$ expressed in base a consists of precisely n 1's and no other digits. Such numbers are called "repunits", and apart from those to the base 2, those to base 10 have been the most widely studied. For a repunit to be prime, n must be prime, but as with the Mersenne numbers, that is not sufficient.

Examples: $(10^5 - 1)/9 = 11111 = 41 \cdot 271$ and $(10^7 - 1)/9 = 1111111 = 239 \cdot 4649$.

More examples for which $(10^9 - 1)/9$ is composite can be created by finding primes $q > 3$ such that $\operatorname{ord}_q 10 = p$ (see Chap. 14 for the definition of ord). In fact, q then divides $(10^p - 1)/9$.

Which prime exponents p give repunit primes and whether there are infinitely many are two of the many unsolved problems of number theory. With some luck $(10^{317} - 1)/9$ was proved prime, but not until most 50 years after $(10^{23} - 1)/9$ was found to be prime. Primality testing of large numbers is not easy and *factoring* is even more difficult! In fact, the factoring of $(10^{71} - 1)/9$ (into two primes with 30 and 41 digits, respectively) had to wait for 1984 machines and algorithms.

3.7 Perfect Numbers

Each Mersenne prime has a companion *perfect number* $P = M_p 2^{p-1}$. A perfect number is a number for which the sum of all divisors (not including P itself) equals P. Thus, for example, $M_2 = 2^2 - 1 = 3$ leads to the perfect number $P = 6$; and indeed, the sum of the divisors of 6: $1 + 2 + 3$ equals 6 itself.

The next Mersenne prime, M_3, equals $2^3 - 1 = 7$ and the corresponding perfect number is 28. Check: $1 + 2 + 4 + 7 + 14 = 28$. Check!

It is easy to see why this is so. Since M_p is by definition prime, the only divisors of the perfect number $P = M_p 2^{p-1}$ are

$$1, 2, \ldots, 2^{p-1}, M_p, 2M_p, \ldots, 2^{p-1} M_p,$$

and their sum equals

$$\sum = 1 + 2 + \ldots + 2^{p-1} + M_p(1 + 2 + \ldots + 2^{p-1}), \quad \text{or} \tag{3.5}$$

$$\sum = (1 + M_p)(2^p - 1) = 2^p M_p = 2P. \tag{3.6}$$

(The factor 2 appears here because we included, in the sum, P itself as a divisor of P.) The remarkable fact that *all even* perfect numbers are of the form $M_p 2^{p-1}$, where M_p is a Mersenne prime, was first *proved* by Leonhard Euler (1707–1783), the great Swiss mathematician (and not just that!) from Basel who worked for most of his life in St. Petersburg, the then new capital of all the Russias.

Because 37 Mersenne primes are known, at the time of this writing, there are exactly 37 known perfect numbers, all of them even, and the largest one having 909526 decimal places. No odd perfect numbers are known and, tantalizingly, it is not known whether there are any such. As of 1971, no odd perfect number had been found among all the numbers up to 10^{36}. P. Hagis, Jr., showed recently that an odd perfect number not divisible by 3 has at least eleven prime factors (Math. Comp. *40*, 399–404 (1983)).

Apart from perfect numbers, there are pseudoperfect numbers (Sect. 5.9) and *amicable* numbers. Amicable numbers come in pairs. The sum of divisors of one amicable number equals its mate and vice versa. The smallest amicable pair is 220 and 284. Another pair is 17296 and 18416. In a sense, perfect numbers are "self-amicable".

In a further generalization, certain number sequences are called *sociable*. In these, each number equals the sum of the divisors of the preceding number, and the first number equals the sum of divisors of the last number. One such five-member sociable group is 14288, 15472, 14536, 14264, 12496. There is a sociable chain of length 28 whose smallest member is 14316.

A frequently used concept in number theory is the sum of some function f taken over all divisors of a number n, *including* n itself. This is usually shown by the following notation:

$$\sum_{d|n} f(d).$$

Using this notation, our statement about perfect numbers P reads

$$\sum_{d|p} d = 2P, \tag{3.7}$$

the factor 2 appearing here because by definition P itself is a divisor of itself and therefore is included in the sum.

There was a time when the present author was much impressed by the fact that the sum of *reciprocal* divisors of P is *always* 2:

$$\sum_{d|p} \frac{1}{d} = 2! \tag{3.8}$$

(Here, for once, the exclamation mark does not do any harm because 2! – read "two factorial" – still equals 2.) However, (3.8) is a "trivial" consequence of (3.7) because, in a sum over all divisors d of a given number n, the divisor d may be replaced by n/d. This reverses the *order* of the terms in such a sum, but does not affect its value:

$$\sum_{d|n} f(d) = \sum_{d|n} f(n/d). \tag{3.9}$$

Indeed, for $n = 6$ and $f(d) = d$,

$$1+2+3+6 = 6+3+2+1. \tag{3.10}$$

Applying (3.8) to (3.6), we have

$$2P = \sum_{d|P} d = \sum_{d|P} \frac{P}{d}, \tag{3.11}$$

confirming (3.8). Check: $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 2$. Check!

It is remarkable that the sum of the reciprocal divisors of a perfect number always equals 2, no matter how large it is. This implies that perfect numbers cannot have too many small divisors, as we already know.

3.8 Fermat Primes

Besides the Mersenne primes $2^p - 1$, which lead to perfect numbers, and of which only 37 are presently known, there is another kind of prime family with even fewer known members: the Fermat primes. Only 5 such primes are currently known.

$$F_n = 2^{2^n} + 1 \quad \text{for} \quad n = 0,\ 1,\ 2,\ 3,\ 4. \tag{3.12}$$

They are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$.

Incidentally, for $2^m + 1$ to be prime, m must be a power of 2. In fact, for any $a^m + 1$ to be prime, a must be even and $m = 2^n$.

All numbers of the form $2^{2^n} + 1$, whether prime or composite, are called Fermat numbers. They obey the simple (and obvious) recursion

$$F_{n+1} = (F_n - 1)^2 + 1, \quad \text{or} \tag{3.13}$$

$$F_{n+1} - 2 = F_n(F_n - 2), \tag{3.14}$$

which leads to the interesting product

$$F_{n+1} - 2 = F_0 F_1 \ldots F_{n-1}. \tag{3.15}$$

In other words, $F_n - 2$ is divisible by all lower Fermat numbers:

$$F_{n-k} \mid (F_n - 2), \qquad 1 < k \leq n. \tag{3.16}$$

With (3.16) it is easy to prove that all Fermat numbers are coprime to each other, and the reader may wish to show this.

Fermat thought that all Fermat numbers F_n were prime, but Euler showed that $F_5 = 4294967297 = 641 \cdot 6700417$, which can easily be confirmed with a good pocket calculator.

The fact that F_6 and F_7 are also composite is a little harder to show because F_6 has 20 decimal digits and F_7 has 39. Nevertheless, *complete* factorizations of F_6, F_7 and, since 1981, F_8 are now known. Further, it is now known that F_{11}, F_{12} and F_{13}

are composite, and *some* of their factors are known. Another Fermat number known to be composite is F_{73}, which has more than 10^{21} digits! For special primality tests for Fermat numbers, see *Hardy* and *Wright* [3.6].

At present the smallest, and so far most enduring mystery is presented by F_{20}: its primality status remains unknown. However, the latest progress in primality testing, reported by Walter Sullivan in The New York Times in February 1982 and in [3.1], might yet reveal other Fermat primes, although the next candidate, F_{20}, has 315653 digits. One helpful clue which has been utilized in the past is that, if F_n is composite, then it is divisible by $k \cdot 2^{n+2} + 1$ for some k. In fact, Euler knew this, and that is how he discovered the factor $641 = 5 \cdot 2^7 + 1$ in F_5.

In this manner the compositeness of some *very* large Fermat numbers has been established. For example, $5 \cdot 2^{3313} + 1$ is a factor of F_{3310}. By the way, F_{3310} has more than 10^{990} *digits* – not to be confused with the comparatively miniscule number 10^{990}.

3.9 Gauss and the Impossible Heptagon

In March 1796, the Fermat primes suddenly took on a new and overwhelming significance. A precocious teenager from the German ducal town of Brunswick had just discovered that the circle could be divided into 17 equal parts by purely "geometric means", i. e., by straightedge and compass – something that had eluded professional mathematicians and amateurs alike for over two millennia. In fact, nobody had even suspected that such a feat could be possible. After the cases of 2, 3, 4, 5 and 6 had been solved by the ancient Greeks, "everybody" had been working on the "next" case: the regular heptagon (7-gon). But the Brunswick youth proved that that was impossible and that the only regular n-gons that could be constructed were those derivable from the Fermat primes.

The young person, of course, was none other than Carl Friedrich Gauss [3.7], who was himself so impressed by his feat of unlocking a door that had been closed for 2000 years that he decided to become a mathematician rather than a philologist, to which fate his excellence in the classical languages seemed to have "condemned" him.[4]

[4] His love of books and languages never left Gauss for the rest of his life. At the age of 62 he learned yet another foreign language – Russian – and began to read Pushkin in the original. Gauss selected the University of Göttingen rather than his "state" university, Helmstedt, for his studies, mainly because of Göttingen's open library policy. Even in his first semester at Göttingen, Gauss spent much time in the university library, which was well stocked and where he had access to the writings of Newton and Euler and many others of his predecessors. Much of what Gauss read there he had already derived himself, but he still felt that reading was essential – in stark contrast to other scientific geniuses, notably Einstein, who was convinced he could create most of the correct physics from within himself and who is supposed to have said, in jest, that if nature was not the way he felt it ought to be, he pitied the Creator for not seeing the point ("Da könnt' mir halt der liebe Gott leid tun, die Theorie stimmt doch." [3.8]).

We shall return to the important subject of dividing the circle, or *cyclotomy* by its learned name, in several other contexts later in this book. Let it only be said here that for the circle to be divisible into n parts, n must be the product of *different* Fermat primes or 1 and a nonnegative power of 2. Thus, regular polygons of $n = 2,3,4,5,6,8,10,12,15,16,17,20,24,30,\ldots$ sides can be geometrically constructed, while $n = 7,9,11,13,14,18,19,21,22,23,25,\ldots$ are *impossible* to construct in this manner. Here the "impossible" part of Gauss's assertion is as significant as his positive statement.