CHAPTER X

MERSENNE NUMBERS AND FERMAT NUMBERS

§ 1. Some properties of Mersenne numbers. Mersenne numbers $M_n = 2^n - 1$ have already been discussed; cf. Chapter IV, § 5. Theorem 5 of Chapter V may be expressed by saying that in order that an even number should be a perfect number it is necessary and sufficient that it should be of the form $2^{n-1}M_n$, where n is a natural number and M_n is a Mersenne prime number. This is why Mersenne numbers which are prime are of particular interest; moreover, the greatest prime numbers that are known are Mersenne numbers.

As we learned in Chapter IV, § 5, if a Mersenne number M_n is prime, number n is also prime; the converse, however, is not necessarily true (for example $M_{11} = 23 \cdot 89$).

It is easy to prove that a natural number m is a Mersenne number if and only if $m+1$ has no odd prime divisor. As noticed by Golomb [1], this provides a method of finding all Mersenne numbers, the method being similar to the sieve of Eratosthenes.

We now prove a theorem which, in a number of cases, enables us to decide whether a Mersenne number is composite or not.

THEOREM 1. *If q is a prime of the form $8k+7$, then $q \mid M_{(q-1)/2}$.*

Proof. In virtue of a formula of Chapter IX, since q is a prime, we have $\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \pmod q$. If q is a prime of the form $8k+7$, then, by property IV of Legendre's symbol (cf. Chapter IX, § 1), we have $\left(\frac{2}{q}\right) = 1$. Consequently, $2^{(q-1)/2} \equiv 1 \pmod q$, whence $q \mid 2^{(q-1)/2} - 1$, as required.

An easy induction shows that $2^{4k+3} > 8(k+1)$. In fact, $2^7 > 8 \cdot 2$, and, if $2^{4k+3} > 8(k+1)$, then $2^{4(k+1)+3} > 2^4 \cdot 8(k+1) > 8(k+2)$. Therefore, if $q = 8k+7 > 7$, then $2^{(q-1)/2} - 1 > 8k+7 = q$, which proves that *if q is a prime of the form $8k+7 > 7$, then the number $M_{(q-1)/2}$ is composite — it is divisible by q.* Hence the following

COROLLARY. *If n is a prime > 3 of the form $4k+3$ and if number $q = 2n+1$ is a prime, then number M_n is composite; for, it is divisible by q.*

In particular, this is the way to establish that the following Mersenne numbers are composite, a prime divisor of any of them being also found: $23 \mid M_{11}$, $47 \mid M_{23}$, $167 \mid M_{83}$, $263 \mid M_{131}$, $359 \mid M_{179}$, $383 \mid M_{191}$, $479 \mid M_{239}$, $503 \mid M_{251}$, $719 \mid M_{359}$, $839 \mid M_{419}$, $863 \mid M_{431}$, $887 \mid M_{443}$, $983 \mid M_{491}$, $1319 \mid M_{659}$, $1367 \mid M_{683}$, $1439 \mid M_{719}$, $1487 \mid M_{743}$, $1823 \mid M_{911}$, $2039 \mid M_{1019}$.

It follows from the conjecture H (Chapter III, § 8) that there exist infinitely many prime numbers p of the form $4k+3$ for which $q = 2p+1$ is a prime. Thus, by the corollary, we see that the conjecture H implies the existence of infinitely many primes p such that the numbers M_p are composite (cf. Schinzel and Sierpiński [3], p. 198, C_9).

As regards theorem 1, we note that an argument analogous to the one used in its proof shows that, *if q is a prime of the form $8k+1$, then $q \mid M_{(q-1)/2}$*. Here, however, the number $(q-1)/2 = 4k$ cannot be a prime. For example, we have $17 \mid M_8$, $41 \mid M_{20}$, $89 \mid M_{44}$, $97 \mid M_{48}$.

We do not know any composite Mersenne number which has a prime index and which is not a product of different primes. Neither are we able to prove that there exist infinitely many square-free Mersenne numbers.

E. Gabard [1], [2] proved that each of the numbers M_{151} and M_{183} is a product of five different prime numbers.

THEOREM 2. *If n is a natural number > 1, then M_n cannot be the m-th power of a natural number, m being a natural number > 1* (cf. Gerono [1]).

Proof. Suppose that $2^n - 1 = k^m$, where k and $m > 1$ are natural numbers. Since $n > 1$, number k is odd. If m were even, then k^m would be of the form $8t+1$, whence $k^m + 1 = 2(4t+1)$. But, since $n > 1$, $k^m + 1 = 2^n$ is divisible by 4, which is a contradiction. Consequently m is odd and $2^n = k^m + 1 = (k+1)(k^{m-1} - k^{m-2} + \ldots - k + 1)$, the second of the factors being an algebraic sum of an odd number of odd summands, is an odd number, whence, in virtue of the fact that it is a divisor of 2^n, it is equal to 1. Therefore $2^n = k+1$, and so $m = 1$, contrary to the assumption. This proves theorem 2.

Theorem 2 implies that there are no Mersenne numbers that are squares except $M_1 = 1^2$. On the other hand, there exist Mersenne numbers which are triangular numbers. However, there are only four of them $M_1 = t_1$, $M_2 = t_2$, $M_4 = t_5$, $M_{12} = t_{90}$ (cf. Browkin and Schinzel [1] and also Ramanujan [1], Nagell [4], [11], Skolem, Chowla and Lewis [1], Chowla, Dunton and Lewis [1], Mordell [8], Shapiro and Slotnicki [1]).

It is easy to prove that for $|x| < \frac{1}{2}$ the following equality holds:

$$\frac{1}{(1-x)(1-2x)} = M_1 + M_2 x + M_3 x^2 + \ldots$$

EXERCISES. **1.** Prove that every odd natural number is a divisor of infinitely many Mersenne numbers.

Proof. If m is an odd natural number, then, by the theorem of Euler, for any natural number k we have $m \mid M_{k\varphi(m)}$.

2. Find the least Mersenne number that is divisible by the square of a natural number > 1.

Answer. It is the number $M_6 = 2^6-1 = 63 = 3^2\cdot 7$, because $M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15 = 3\cdot 5$ and $M_5 = 31$.

3. Find the least Mersenne number which has an odd index and which is divisible by the square of a natural number > 1.

Answer. It is the number $M_{21} = 7^2\cdot 127\cdot 337$ because $M_7 = 127$, $M_9 = 7\cdot 73$, $M_{11} = 23\cdot 89$, $M_{13} = 8191$, $M_{15} = 7\cdot 31\cdot 151$, $M_{17} = 131071$, $M_{19} = 524287$.

Remark. The next Mersenne number after M_{21} which has odd index and is divisible by the square of a natural number > 1 is the number M_{63}; the next number with the same property is M_{105}. They are both divisible by 7^2 because $M_{21} \mid M_{63}$ and $M_{21} \mid M_{105}$.

4. Prove that if a and n are natural numbers greater than 1, then, if a^n-1 is a prime, it is a Mersenne number.

Proof. In the case where $a > 2$, we have $a-1 \mid a^n-1$, so, in view of $n > 1$, $1 < a-1 < a^n-1$, which shows that number a^n-1 cannot be a prime. Thus we see that the assumption that a^n-1 is a prime implies that $a < 2$, whence $a = 2$ (because $1-1$ is not a prime). Consequently, $a^n-1 = M_n$.

5. Prove that, if m is an arbitrary natural number, s the number of digits of n in the scale of ten, then there exists a Mersenne number M_n whose first s digits are equal to the s digits of m, respectively.

The proof follows immediately from an analogous property of the numbers 2^n (cf. Sierpiński [11], theorem 2).

6. Prove that for any natural number s the last s digits of the numbers M_n $(n = 1, 2, \ldots)$ form an infinite periodic sequence, the period being formed of $4\cdot 5^{s-1}$ terms.

The proof follows from theorem 1, p. 246, of my paper referred to above.

Many theorems on divisors of numbers M_n have been collected by E. Storchi in paper [1].

§ 2. Theorem of E. Lucas and D. H. Lehmer.

THEOREM 3 [1]. *A number M_p, p being an odd prime, is prime if and only if it is a divisor of the $(p-1)$-th term of the sequence $s_1, s_2, \ldots$, where* $s_1 = 4$, $s_k = s_{k-1}^2-2$, $k = 1, 2, \ldots$

Proof. Let $a = 1+\sqrt{3}$, $b = 1-\sqrt{3}$. We have $a+b = 2$, $ab = -2$, $a-b = 2\sqrt{3}$. We define sequences u_n, v_n $(n = 1, 2, \ldots)$ of natural numbers by

$$u_n = \frac{a^n-b^n}{a-b}, \qquad v_n = a^n+b^n.$$

[1] Lehmer [4] (cf. also Kraïtchik [1], p. 141, and Trost [3]).

These formulae imply that for any $n = 1, 2, \ldots$ we have

$$u_n = \binom{n}{1} + \binom{n}{3}\cdot 3 + \binom{n}{5}\cdot 3^2 + \ldots, \qquad v_n = 2\left(1 + \binom{n}{2}\cdot 3 + \binom{n}{4}\cdot 3^2 + \ldots\right).$$

Hence for any natural k, l we have

$$2u_{k+l} = u_k v_l + v_k u_l, \tag{1}$$

$$(-2)^{l+1} u_{k+l} = u_l v_k - u_k v_l \quad \text{for} \quad k > l, \tag{2}$$

$$u_{2k} = u_k v_k, \tag{3}$$

$$v_{2k} = v_k^2 + (-2)^{k+1}, \tag{4}$$

$$v_k^2 - 12u_k^2 = (-2)^{k+2}, \tag{5}$$

$$2v_{k+l} = v_k v_l + 12u_k u_l. \tag{6}$$

For an odd prime q we denote by $\omega(q)$ the least natural number n such that $q \mid u_n$ (provided it exists).

We now prove three following lemmas.

LEMMA 1. *An odd prime q divides u_n, n being a natural number, if and only if $\omega(q) \mid n$.*

Proof of lemma 1. Let q be a given odd prime number. We denote by S the set of natural numbers n such that $q \mid u_n$. By (1) and (2), if two numbers, k and l, belong to the set S, then number $k+l$ is also a number of the set S, moreover, if $k > l$, then $k-l$ belongs to S. Thus we see that the set S has following property: the sum and the difference (provided it is positive) of any two numbers of the set S belong to S. Let d be the least natural number that belongs to S. From the above-mentioned property of the set S, we infer by a simple induction that numbers kd, $k = 1, 2, \ldots$, are in the set S. On the other hand, suppose that a natural number n belongs to S and that n divided by d leaves a positive remainder r. Then $n = td+r$, where t is an integer $\geqslant 0$, and $r < d$. The case $t = 0$ is clearly impossible, since r, being less than d, cannot be equal to n and thus cannot belong to the set S because of the definition of d. Consequently, t is a natural number and thus td belongs to S, whence, by the property of S, number $r = n-td$, as the difference of two numbers of the set S with $n > td$, must belong to S; this, however, contradicts the definition of d. From this we conclude that $r = 0$, which means that the set S is just the set of positive multiples of a number that belongs to it. Therefore if a number n belongs to S, then $\omega(q) \mid n$ and *vice versa*. This proves lemma 1.

LEMMA 2. *If q is a prime > 3, then*

$$q \mid u_q - 3^{(q-1)/2} \tag{7}$$

and

$$q \mid v_q - 2. \tag{8}$$

Proof of lemma 2. In order to prove (7) we write

$$u_q = \frac{1}{2\sqrt{3}}[(1+\sqrt{3})^q-(1-\sqrt{3})^q] = \sum_{k=0}^{(q-1)/2}\binom{q}{2k+1}3^k.$$

In the sum of the right-hand side the binomial coefficients are all divisible by the prime q, except for the last, which is equal to 1; hence formula (7) follows.

In order to prove (8) we write

$$v_q = (1+\sqrt{3})^q+(1-\sqrt{3})^q = 2\sum_{k=0}^{(q-1)/2}\binom{q}{2k}3^k.$$

In this sum all the binomial coefficients, apart from the first one, are divisible by q; hence formula (8) follows.

LEMMA 3. *If for a prime $q>3$ the number $\omega(q)$ exists, then $\omega(q)\leqslant q+1$.*

Proof of lemma 3. Since $u_1=2$, $v_1=2$, by (1) and (2) with $k=q$, $l=1$, we find $2u_{q+1}=2u_q+v_q$ and $-4u_{q-1}=2u_q-v_q$, whence $-8u_{q+1}u_{q-1}=4u_q^2-v_q^2$. But, in virtue of lemma 2, we have $q\mid u_q^2-3^{q-1}$ and $q\mid v_q^2-4$. Since q is a prime >3, by the theorem of Fermat we obtain $q\mid 3^{q-1}-1$. Therefore we have $q\mid u_q^2-1$ and so $q\mid 4u_q^2-v_q^2$. Consequently $q\mid 8u_{q+1}u_{q-1}$, which, by $q>3$, implies that either $q\mid u_{q+1}$ or $q\mid u_{q-1}$. In the former case, in virtue of lemma 1 we obtain $\omega(q)\leqslant q+1$, in the latter we have $\omega(q)\leqslant q-1$. Thus, in any case, $\omega(q)\leqslant q+1$, which shows the validity of lemma 3.

We now turn to the proof of sufficiency of the condition of theorem 3. Suppose that p is an odd prime and let $M_p\mid s_{p-1}$. Then

$$M_p\mid 2^{2^{p-2}}s_{p-1}. \tag{9}$$

We have $2s_1=v_2$. For a natural number n suppose that $2^{2^{n-1}}s_n=v_{2^n}$, this being true for $n=1$. Since $s_{n+1}=s_n^2-2$, we then have $2^{2^n}s_{n+1}=(2^{2^{n-1}}s_n)^2-2^{2^{n}+1}=v_{2^n}^2-2^{2^n+1}$. But, in virtue of (4) with $k=2^n$, we have $v_{2^{n+1}}=v_{2^n}^2-2^{2^n+1}$. Thus $2^{2^n}s_{n+1}=v_{2^{n+1}}$. The formula $2^{2^{n-1}}s_n=v_{2^n}$ is thus proved by induction. Hence, for $n=p-1$ we have

$$2^{2^{p-1}}s_{p-1}=v_{2^{p-1}}. \tag{10}$$

By (10), from (9) we obtain

$$M_p\mid v_{2^{p-1}}, \tag{11}$$

whence, by (3) with $k=2^{p-1}$,

$$M_p\mid u_{2^p}. \tag{12}$$

Now let q denote an arbitrary prime divisor of M_p. Since, in view of the fact that p is odd, number $M_p=2^p-1$ is not divisible by 3, we have $q>3$. The relation $q\mid M_p$ and formula (12) give $q\mid u_{2^p}$, and consequently, by lemma 1, we have $\omega(q)\mid 2^p$. On the other hand, $\omega(q)$ does not divide 2^{p-1} because, if it did, we would have, by lemma 1, $q\mid u_{2^{p-1}}$, whence, by (5) with $k=2^{p-1}$, q would be a divisor of a power of the number 2 which is impossible since q is a prime >3. Hence $\omega(q)=2^p$. In virtue of lemma 3, we then have $2^p\leqslant q+1$, whence $M_p\leqslant q$, which, in virtue of the relation $q\mid M_p$, proves that $M_p=q$, which means that M_p is a prime.

The sufficiency of the condition of theorem 3 is thus proved. In order to prove the necessity we prove the following

LEMMA 4. *If p is a prime of the form $12k+7$, then $p\mid 3^{(p-1)/2}+1$.*

Proof of lemma 4. Let p be a prime of the form $12k+7$, where k is an integer $\geqslant 1$. Then $p>3$ and, by property I of Legendre's symbol (cf. Chapter IX, § 1), we find $\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$. By property V of Legendre's symbol we have $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right)=-1$, whence $\left(\frac{3}{p}\right)=-1$. Consequently $3^{(p-1)/2}\equiv -1\pmod p$, whence $p\mid 3^{(p-1)/2}+1$, as asserted.

We now turn to the proof of the necessity of the condition of theorem 3. Suppose that p is a prime >2 and that the number $q=M_p$ is also a prime. Since $p>2$, we have $8\mid 2^p=q+1$. Hence $q=8t+7$, where t is an integer $\geqslant 0$. We have $q-1=2^p-2=2(2^{p-1}-1)$. Since $p-1$ is even, i.e. $p-1=2s$, where s is a natural number, we have $2^{p-1}-1=(3+1)^s-1=3u$, where u is an integer. Hence $3\mid 2^{p-1}-1\mid q-1=8t+6$, whence $3\mid t$, i.e. $t=3k$, where k is an integer. Therefore $q=8t+7=24k+7$.

By (4), with $k=2^{p-1}$, we have

$$v_{2^p}=v_{2^{p-1}}^2-4\cdot 2^{2^{p-1}-1}. \tag{13}$$

But since $q=24k+7=8\cdot 3k+7$, by theorem 1 we find $q\mid M_{(q-1)/2}$, i.e. $q\mid M_{2^{p-1}-1}=2^{2^{p-1}-1}-1$, whence, by (13),

$$q\mid v_{2^p}-v_{2^{p-1}}^2+4. \tag{14}$$

But, by (6) with $k=q$, $l=1$, and since $q+1=2^p$, we have

$$2v_{2^p}=v_qv_1+12u_qu_1=2v_q+12u_q.$$

Consequently,

$$v_{2^p}=v_q+6u_q=(v_q-2)+6(u_q+1)-4. \tag{15}$$

Since $q = 24k+7$, we may apply lemma 4 to number q; so $q \mid 3^{(q-1)/2}+1$, and hence, by (7), $q \mid u_q+1$ and, by (8), $q \mid v_q-2$. Thus, by formula (15), $q \mid v_{2^p}+4$, whence, by (14), $q \mid v^2_{2^{p-1}}$. This, in view of (10), $q = M_p$ being odd, shows that $M_p \mid s_{p-1}$, and this completes the proof of the necessity of the condition.

Theorem 3 is thus proved.

It is easy to prove that theorem 3 is equivalent to the following theorem of Lucas:

THEOREM 3[a]. *A number M_p, where p is an odd prime, is a prime if and only if number M_p is a divisor of the $(p-1)$-th term of the sequence $t_1, t_2, \ldots$, where $t_1 = 2$, $t_{k+1} = 2t_k^2-1$ for $k = 1, 2, \ldots$*

The proof of equivalence follows immediately from the fact that the sequence s_k $(k = 1, 2, \ldots)$ turns into the sequence t_k $(k = 1, 2, \ldots)$ if s_k is replaced by $2t_k$. Thus, since M_p is odd, the relations $M_p \mid s_{p-1}$ and $M_p \mid t_{p-1}$ are equivalent.

A proof of theorem 3[a] based on the theory of trigonometric functions of complex variable was given by T. Bang [1].

§ 3. How the greatest of the known prime numbers have been found. Theorem 3 cannot be easily applied in investigation of Mersenne numbers whose indices are greater than, say, ten. The reason is that the terms of the sequence s_k $(k = 1, 2, \ldots)$ increase very rapidly with k. By induction, it follows from the definition of the sequence $(s_1 = 4,\ s_k = s^2_{k-1}-2,\ k = 2, 3, \ldots)$ that $s_k \geqslant 10^{2^{k-2}}+4$ for any $k = 2, 3, \ldots$ Consequently $s_{10} > 10^{2^8} = 10^{256}$, which shows that the tenth term s_{10} has more than 250 digits. Number s_{100} cannot even be written as a decimal as it has more than 10^{27} digits.

Therefore, in order to apply theorem 3 while investigating whether a given number M_p (p being a prime > 2) is a prime or not, we proceed as follows.

For any integer t we denote by $\bar{t}$ the remainder left by t divided by M_p. Thus for any integer t we have $M_p \mid t-\bar{t}$. Now we define a sequence r_k $(k = 1, 2, \ldots)$ by

$$r_1 = 4, \qquad r_{k+1} = \overline{r_k^2-2} \quad \text{for} \quad k = 1, 2, \ldots \tag{16}$$

and we prove by induction that

$$M_p \mid s_k - r_k \quad \text{for} \quad k = 1, 2, \ldots \tag{17}$$

We see that (17) is valid for $k = 1$. Suppose that it is true for a natural number k. Then, *a fortiori*, $M_p \mid s_k^2-r_k^2$, whence $M_p \mid s_k^2-2-(r_k^2-2)$. Since $s_k^2-2 = s_{k+1}$, and, in view of $M_p \mid t-\bar{t}$ with $t = r_k^2-2$, and by (16), $M_p \mid r_k^2-2-r_{k+1}$, we obtain $M_p \mid s_{k+1}-r_{k+1}$. Formula (17) is thus proved by induction on $k = 1, 2, \ldots$

By (17), formula $M_p \mid s_{p-1}$ is equivalent to the formula $M_p \mid r_{p-1}$. By (16) in order to calculate r_{p-1} one has to calculate $p-2$ squares of the numbers which are the remainders obtained by dividing by M_p, these having clearly no more digits than number M_p, and to calculate the remainders left by these squares minus 2 divided by M_p. The electronic computers that exist nowadays are able to carry out the calculation described above for primes p up to about ten thousand.

It has been discovered in this way that number M_{101} is composite since it is not a divisor of the corresponding number r_{101}. We do not know any prime divisor of this number, though we do know that M_{101} is the product of two different primes. As announced by J. Brillhart and G. D. Johnson [1], p. 365, number $2^{101}-1$ has no prime divisors less than 2^{35}. Hence it follows that number M_{101} cannot be a product of three or more prime divisors (different or not) because if it could and if p were the least of those prime factors, we would have $p^3 < 2^{101}$ which would give $p < 2^{34}$. On the other hand, as we have already mentioned, M_{101} is not a prime and, by theorem 2, it is not the square of a prime number either. Therefore M_{101} can only be the product of two different primes.

A situation similar to the one described above arises for M_{137}. We know that M_{137} is the product of two different prime numbers, but we do not know either of them.

Until the year 1950 the greatest known prime number was M_{127}, which has 39 digits. It was investigated by E. Lucas in 1876 and in 1914 E. Fauquemberge proved it to be a prime. In January 1952 by the use of electronic computers SWAC the numbers M_{521} and M_{607} were proved to be prime. The former has 157 digits, the latter 183 digits. In the same year, in June, the number M_{1279} was proved to be a prime; it has 376 digits. In September, 1952, the same was proved about the numbers M_{2203} and M_{2281} the former having 664 digits, and the latter 687 digits (1).

The next known prime number in the order of magnitude is number M_{3217}; it has 969 digits.

The primes M_{9689}, M_{9941} and M_{11213} which are now the largest known primes were discovered by using the ILLIAC II at the Digital Computer, Laboratory of the University of Illinois. The M_{11213} has 3381 digits. The computing time was 2 hours 15 minutes (D. B. Gilles [1]).

Thus twenty three prime Mersenne numbers M_n are known, namely for $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4219, 4423, 9689, 9941, 11213$

(1) More details on these large prime numbers are to be found in papers of H. S. Uhler [2], [3].

For primes $p \leqslant 100$ the factorizations of numbers 2^p-1 are known. For example, number M_{97} is the product of two primes, the smaller being 11447 (cf. Brillhart and Johnson [1], Brillhart [1]). We do not know any prime factor of any of the numbers M_p, $p = 101$, 137, 139, 149, 199, 227, 257, although we know that they are composite.

There was a conjecture that if a Mersenne number M_n is a prime, then number M_{M_n} is also a prime. This is true for the first four Mersenne prime numbers, but for the fifth, i.e. for $M_{13} = 8191$, the conjecture was disproved by D. J. Wheeler in 1953. Number $M_{M_{13}} = 2^{8191}-1$ (which has 2466 digits) turned out to be composite (cf. Robinson [1], p. 844). This fact was shown by an application of the theorem of Lucas and Lehmer; the calculation involved was done by an electronic computer and required 100 hours. None of the prime divisor of this number is known. However, in 1957 it was proved that, though number M_{17} is a prime, number $M_{M_{17}}$ is composite. It is divisible by $1768(2^{17}-1)+1$. Similarly, though number M_{19} is prime, the number $M_{M_{19}}$ is composite, divisible by $120(2^{19}-1)+1$. In this connection there is another conjecture (still undecided): the sequence $q_0, q_1, q_2, \ldots$, where $q_0 = 2$, $q_{n+1} = 2^{q_n}-1$, $n = 0, 1, 2, \ldots$, contains only prime numbers. This has been verified for q_n with $n \leqslant 4$; number q_5, however, as it is easy to verify, has more than 10^{37} digits, and so it cannot even be written as a decimal. Moreover, since the prime divisor of number q_5 are of the form $2kq_4+1 > 2q_4$, number q_5 has no prime divisors that have less than 39 digits. Therefore, at the present time at least, it is impossible to decide whether number q_5 is prime or not.

§ 4. Prime divisors of Fermat numbers. The Fermat numbers $F_n = 2^{2^n}+1$ ($n = 0, 1, 2, \ldots$) may be considered as a particular case of the numbers of the form a^n+1, where a is a natural number >1. Suppose that a number a^m+1, where m is a natural number >1, is a prime. If m has an odd divisor $k>1$, then $n = kl$, whence $a^l+1 \mid (a^l)^k+1 = a^m+1$ and, since $k>1$, the number a^m+1 is composite. Consequently, if a^m+1, where m is a natural number >1, is a prime, then number m must be a power of number 2, i.e. $m = 2^n$, where n is a natural number. In particular, if 2^m+1, where m is a natural number, is a prime, then it must be a Fermat number.

Hence it follows that in order that a natural number s be a prime Fermat number, it is necessary and sufficient that s be a prime >2 and $s-1$ have no odd prime divisors. This indicates a method of finding all the Fermat numbers that are prime. The method is a double application of Eratosthenes' sieve. (Compare an analogous method of finding Mersenne numbers, § 1.)

THEOREM 4. *If a is an even integer, n a natural number and p a prime such that $p \mid a^{2^n}+1$, then $p = 2^{n+1}k+1$, where k is a natural number.*

Proof. Since $p \mid a^{2^n}+1$, we have $p \mid a^{2^{n+1}}-1$; $p \mid a^{2^n}-1$ is impossible, because, if $p \mid 2$, so $p = 2$, which is a contradiction since $p \mid a^{2^n}+1$ implies $(p, a) = 1$, and a is even. Let δ denote the exponent to which a belongs $\bmod p$. Since $p \mid a^{2^{n+1}}-1$, by theorem 9 of Chapter VI we have $\delta \mid 2^{n+1}$, the relation $\delta = 2^n$ being impossible, because $p \mid a^{2^n}-1$ does not hold. From this we infer that $\delta = 2^{n+1}$ and, since by the theorem of Fermat $p \mid a^{p-1}-1$, we obtain $\delta \mid p-1$, that is $2^{n+1} \mid p-1$, whence $p = 2^{n+1}k+1$, where k is a natural number, as was to be proved.

THEOREM 5. *Any divisor >1 of number F_n, where n is an integer >1, is of the form $2^{n+2}k+1$, where k is a natural number.*

Proof. As follows from the proof of theorem 4 (with $a = 2$), if p is a prime and $p \mid F_n$, then number 2 belongs to the exponent $2^{n+1} \bmod p$. On the other hand, theorem 4 implies that p is of the form $2^{n+1}t+1$, where t is a natural number. Consequently, if $n>1$, it is of the form $8k+1$, whence, as we learned in § 1, the relation $p \mid M_{(p-1)/2}$, i.e. $p \mid 2^{(p-1)/2}-1$, holds. But, since 2 belongs to the exponent $2^{n+1} \bmod p$, we must have $2^{n+1} \mid (p-1)/2$, and so $2^{n+2} \mid p-1$, whence $p = 2^{n+2}k+1$, where k is a natural number.

Thus we see that any prime divisor of number F_n ($n>1$) is of the form $2^{n+2}k+1$. Moreover, since any divisor >1 of number F_n is the product of prime divisors of F_n, then it must also be of the above form (because the product of two numbers of the form $mk+1$ is also of this form). Theorem 5 is thus proved.

Theorem 5 is used in investigations whether a given Fermat number is prime or not. For example, the prime divisors of number F_4 are, by theorem 5, of the form $2^6k+1 = 64k+1$. In order to verify whether number F_4 is prime one has to divide it by primes of this form which are not greater than $\sqrt{F_4}$, i.e. less than 2^8. The only number which satisfies the above conditions is number 193; therefore, since $F_4 = 65537$ is not divisible by 193, it is prime.

We now turn to number F_5. By theorem 5, any prime divisor of it must be of the form $2^7k+1 = 128k+1$. Substituting $k = 1, 2, 3, 4, 5$ we obtain prime numbers for $k = 2$ and $k = 5$ only. They are numbers 257 and 641, respectively. Dividing number $F_5 = 2^{32}+1$ by these two numbers, we see that it is divisible by the second of them. Consequently, F_5 is composite. As regards the proof that $641 \mid F_5$, an easy elementary proof which does not involve any explicit dividing is at hand. In fact,

we have $641 = 5^4+2^4 \mid 5^4\cdot 2^{28}+2^{32}$ and $641 = 5\cdot 2^7+1 \mid 5^2\cdot 2^{14}-1 \mid 5^4\cdot 2^{28}-1$, whence 641 is a divisor of the difference of the numbers $5^4\cdot 2^{28}+2^{32}$ and $5^4\cdot 2^{28}-1$, i.e. of the number $2^{32}+1 = F_5$.

We have $F_5 = 641\cdot 6700417$. Since $\sqrt{6700417} < 2600$ and the prime divisors of 6700417 (as divisors of F_5) are of the form $128k+1$, where $k = 5, 6, \ldots$, we see that in order to verify whether 6700417 is prime or not it is sufficient to divide the number by $128k+1$ with $5 \leqslant k \leqslant 20$. This, however, yields a positive remainder for any such k. Thus we see that 6700417 is a prime. The fact that F_5 is the product of two different primes was discovered by Euler in 1732.

The prime divisors of number F_6 must be of the form $256k+1$. Here the first prime divisor is obtained for $k = 1071$ and is 274177. Therefore number F_6 is composite, which was found by Landry in 1880. It can be proved that F_6 is, like F_5, the product of two primes.

The method of finding a prime divisor of a number F_n among the numbers of the form $2^{n+2}k+1$ is successful only in the case where the requierd prime divisor is small enough. In the opposite case, even by substituting very many natural numbers successively for k, we may not obtain any prime divisor of F_n. This is the case of the numbers F_7 and F_8, the former having 39 digits, the latter 78 digits. We do not know any prime divisor of any of these two numbers; neither do we know a decomposition of any of them into a product of two numbers greater than 1. However, as was proved by J. C. Morehead in 1905, F_7 is composite, and in 1909 J. C. Morehead and A. E. Western proved that also F_8 is composite. Their proof is based on theorem 6, see § 5 below.

Number F_9 is composite. As was found by Western in 1903 the number $2^{11}k+1$, where $k = 2^5\cdot 37$, is a prime divisor of F_9.

The question whether F_{10} is composite or not has been answered quite recently. In 1963 J. L. Selfridge with the aid of the electronic computer SWAC verified that F_{10} is composite, it is divisible by $2^{12}\cdot 11131+1$.

The same problem for the subsequent two numbers was much easier to solve. In 1899 Cunningham found two prime divisors of number F_{11}; they are $2^{13}\cdot 39+1$ and $2^{13}\cdot 119+1$. For F_{12} three different prime divisors have been found: the divisor $2^{14}\cdot 7+1$ was found by Pervouchin and Lucas in 1877, the divisors $2^{16}\cdot 397+1$ and $2^{16}\cdot 973+1$ were found by Western in 1903.

Numbers F_{13} and F_{14} were proved to be composite by J. L. Selfridge and A. Hurwitz [1], but no prime factor of them has been found. Number F_{15} was established to be composite in 1925 by Kraïtchik. He found that $2^{21}\cdot 573+1$ is its prime divisor.

F_{16} was found to be composite in 1953 by Selfridge. By the use of the electronic computer SWAC he found that $2^{19}\cdot 1575+1$ is its prime factor. The importance of this result lies in the fact that it disproves the conjecture that all the terms of the sequence

$$2+1,\quad 2^2+1,\quad 2^{2^2}+1,\quad 2^{2^{2^2}}+1,\quad 2^{2^{2^{2^2}}}+1,\quad \ldots$$

are prime numbers. In fact, number F_{16} (which has 19729 digits) is the fifth term of the sequence.

Number F_{17} is the least Fermat number about which we do not know whether it is prime or not. Number F_{18} is composite. In 1903 Western found that $2^{20}\cdot 13+1$ is its prime divisor. Also number F_{19} is composite. In 1962 Riesel found that $33629\cdot 2^{21}+1$ is its prime divisor.

We do not know whether the numbers F_{20}, F_{22} are prime or not. In 1878 Pervouchin found that the number F_{23} is composite, he showed that $2^{25}\cdot 5+1$ is its prime divisor. At present 46 composite Fermat numbers are known. They are the numbers F_n with $n = 5$, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945. The greatest known composite Fermat number is F_{1945}. It has a prime divisor $2^{1947}\cdot 5+1$ (cf. Robinson [2]). The number of the digits of F_{1945} is greater than 10^{582}, so we are unable even to write it down. In § 6 it is explained how we can show that number F_{1945} is divisible by number $2^{1947}\cdot 5+1$, 587 digits.

We are unable to prove that there exist infinitely many composite Fermat numbers, or to prove that there is at least one Fermat number $> F_4$ that is prime. The fact that there are many Fermat numbers $> F_4$ which are known to be composite and that there is no such prime Fermat number, has been a source of the conjecture that all the Fermat numbers $> F_4$ are composite.

By theorem 5, prime divisors of Fermat numbers are of the form $k\cdot 2^m+1$, where k, m are natural numbers; it has been investigated, therefore, which numbers of this form are prime.

If $k = 1$, the numbers 2^m+1 are prime if and only if they are Fermat numbers. Consequently, we know only five such numbers, for $m = 1, 2, 4, 8, 16$. The least number of this form about which we do not know whether it is prime is the number $2^{2^{17}}+1$. In consequence of what we have said above, there are only four numbers of the form $2\cdot 2^m+1$ which are known to be prime. They are for $m = 1$, 3, 7, 15. However, we know 19 primes of the form $3\cdot 2^m+1$. They are obtained for $m = 1$, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276, 353, 408, 438, 534. There are only three known prime numbers of the form $4\cdot 2^m+1$, where $m = 1, 2, \ldots$ They are obtained for $m = 2$, 6, 14. There are 12 known primes of the form $5\cdot 2^m+1$ (where $m = 1, 2, \ldots$), for $m = 1$, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947. For any natural number

$k \leqslant 100$ we know at least one natural number m such that number $k \cdot 2^m + 1$ is prime. (It is known that for $k = 47$ numbers $k \cdot 2^m + 1$ are composite for any $m < 583$, cf. Robinson [2] and Selfridge [1]). On the other hand it can be proved that there exist infinitely many natural numbers k such that $k \cdot 2^m + 1$ is composite for $m = 1, 2, \ldots$; see exercise 3, below.

For $n = 39$ and $n = 207$ we have $3 \cdot 2^{n+2} + 1 \mid F_n$. For any of the numbers $n = 5, 23, 73, 125, 1945$, we have $5 \cdot 2^{n+2} + 1 \mid F_n$ and also $5 \cdot 2^{39} + 1 \mid F_{36}$. If for a number of the form $k \cdot 2^m + 1$ we put $k = m = n$, we obtain a *Cullen number* $C_n = n \cdot 2^n + 1$ (cf. Beeger [2]). A. J. C. Cunningham and H. J. Woodall [1] proved that any of the Cullen numbers C_n with $1 < n < 141$ is composite and has a small prime divisor. However, it has been proved that number C_{141} is prime (Robinson [2]).

EXERCISES. **1.** Prove that if m is a natural number $\neq 3$, then number $2^m + 1$ is not a power of a natural number, the exponent being greater than 1.

Proof. At first we prove that if m is a natural number $\neq 3$, then number $2^m + 1$ is not the square of a natural number. In fact, if $2^m + 1$ were equal to n^2, where n is a natural number, then, clearly, n would be odd and greater than 1; moreover, it would be greater than 3, because $n = 3$ gives $m = 3$, contrary to the assumption. Therefore $2^m = n^2 - 1 = (n-1)(n+1)$, whence $n - 1 = 2^k$, $n + 1 = 2^{m-k}$, where k would be a natural number contained between 1 and m, $k < m - k$. Hence $2^{m-k} - 2^k = 2$, which, in view of the fact that $k > 1$, is impossible. Now suppose that $m \neq 3$ and $2^m + 1 = n^s$, where s is a natural number > 1. Since $2^m + 1$ is not a square, s must be odd. Consequently, $2^m = n^s - 1 = (n-1)(n^{s-1} + n^{s-2} + \ldots + n + 1)$, which is impossible because the second factor, being a sum of odd numbers, is an odd number > 1. The proof is thus completed.

2. Prove that for Fermat numbers $m = 2^{2^n} + 1$ $(n = 0, 1, 2, \ldots)$ the relation $m \mid 2^m - 2$ holds.

Proof. For any integer $n \geqslant 0$ we have $n + 1 \mid 2^n$, whence $2^{n+1} \mid 2^{2^n}$ and consequently $2^{2^{n+1}} - 1 \mid 2^{2^n} - 1$, and, since $m = 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1$, we obtain $m \mid 2^{2^n} - 1$, whence, *a fortiori*, $m \mid 2^m - 2$.

Remark. Hence it follows that composite Fermat numbers are pseudoprime (Chapter V, § 7).

It can be proved that if for a natural number k number $m = 2^k + 1$ satisfies the relation $m \mid 2^m - 2$, then m is a Fermat number (Jakóbczyk [1], p. 122, theorem X).

3. Prove that there exist infinitely many natural numbers k such that for any of them number $k \cdot 2^n + 1$ is composite for any natural number n.

Proof. As we have already learned, numbers F_m are prime for $m = 0, 1, 2, 3, 4$; moreover, number F_5 is the product of two prime numbers, 641 and p, where $p > F_4$. By the Chinese remainder theorem, there exist infinitely many natural numbers k that satisfy the two congruences

$$k \equiv 1 \pmod{(2^{32} - 1)641} \quad \text{and} \quad k \equiv -1 \pmod{p}. \tag{18}$$

We are going to prove that if k is any such number and if in addition, it is greater than p, then all the numbers $k \cdot 2^n + 1$, $n = 1, 2, \ldots$, are composite.

At first suppose that $n = 2^s(2t+1)$, where s is one of the numbers $0, 1, 2, 3, 4$ and t is an arbitrary integer $\geqslant 0$. In virtue of (18), we have $k \cdot 2^n + 1 \equiv 2^{2^s(2t+1)} + 1 \pmod{2^{32} - 1}$ and, since $F_s \mid 2^{32} - 1$ and $F_s \mid 2^{2^s(2t+1)} + 1$, we infer that number $k \cdot 2^n + 1$ is divisible by F_s at the same time being greater than $p > F_s$, it is composite.

Now let $n = 2^5(2t+1)$, where $t = 0, 1, 2, \ldots$ In virtue of (18), we have $k \cdot 2^n + 1 \equiv 2^{2^5(2t+1)} + 1 \pmod{641}$ and, since $641 \mid 2^{2^5} + 1 \mid 2^{2^5(2t+1)} + 1$, we infer that number $k \cdot 2^n + 1$ is divisible by 641. But it is greater than 641, and so it is composite.

It remains to consider the case where n is divisible by 2^6, i.e. where $n = 2^6 t$ for $t = 1, 2, \ldots$ In virtue of formulae (18), we have $k \cdot 2^n + 1 \equiv -2^{2^6 t} + 1 \pmod{p}$. But $p \mid 2^{2^5} + 1 \mid 2^{2^6} - 1 \mid 2^{2^6 t} - 1$, whence we infer that number $k \cdot 2^n + 1$ is divisible by p and greater than p, and so it is composite.

We have thus proved that number $k \cdot 2^n + 1$ is composite for any $n = 1, 2, \ldots$ (cf. Sierpiński [27]).

2. Find all the primes of the form $n^n + 1$, where n is a natural number, that have no more than 300000 digits.

Solution. There are only three primes that satisfy this condition. They are: $1^1 + 1 = 2$, $2^2 + 1 = 5$, $4^4 + 1 = 257$. In fact, if a number $n^n + 1$, where n is a natural number, is a prime, then, clearly, n cannot have any odd divisor > 1, and so it must be of the form $n = 2^k$, where k is a natural number. But then $n^n + 1 = 2^{2^k} + 1$, whence we infer that k cannot have any odd divisor > 1, and so $k = 2^s$, where s is an integer $\geqslant 0$. Hence it follows that $n^n + 1 = F_{2^s + s}$. Thus, for $s = 0$ we obtain number $F_1 = 5$, for $s = 1$ number $F_3 = 257$, for $s = 2$ and $s = 3$ numbers F_6 and F_{11}, which are composite; for $s = 4$ we obtain the number $F_{20} > 2^{2^{20}} > 2^{10^6}$, but this has more than 300000 digits (Sierpiński [19]).

5. Find all the primes of the form $n^{n^n} + 1$ that have not more than a milliard miliards of digits.

Solution. There are only two such numbers: $1^{1^1} + 1 = 2$, $2^{2^2} + 1 = 17$. The proof is similar to that used in the preceding exercise. We prove first that if $n > 2$ and number $n^{n^n} + 1$ is a prime, then $n = 2^{2^s}$, where s is a natural number. Therefore $n^{n^n} + 1 = F_{2^{2^s} + 2^s + s}$. For $s = 1$ we obtain the number F_9 which is composite, for $s = 2$ we obtain number F_{66} which has more than 10^{18} digits. It follows that, if it is true that there are no prime numbers of the form $n^{n^n} + 1$ with $n > 2$, then there exist infinitely many composite Fermat numbers.

6. Prove that among the numbers $2^{2^n} + 3$, $n = 1, 2, \ldots$, there are infinitely many composite ones.

Proof. We are going to show that all the numbers $2^{2^{2k+1}} + 3$, where $k = 1, 2, \ldots$, are composite. In fact, as we know, for natural numbers k we have $2^{2k} = 3l + 1$, where l is a natural number. Hence $2^{2^{2k+1}} + 3 = 2^{6l+2} + 3 = 4(2^3)^{2l} + 3 \equiv 4 + 3 \equiv 0 \pmod 7$. But, since for any natural number k number $2^{2^{2k+1}} + 3$ is > 7, it is composite. The problem whether among the numbers $2^{2^n} + 3$ there exist infinitely many primes remains open.

7. Prove that any of the numbers $2^{2^n} + 5$, $n = 1, 2, \ldots$, is composite.

The proof follows from the fact that all these numbers are divisible by 3.

§ 5. A necessary and sufficient condition for a Fermat number to be a prime.

THEOREM 5. *In order that a Fermat number F_n, where n is a natural number, be a prime, it is necessary and sufficient that $F_n \mid 3^{(F_n - 1)/2} + 1$.*

Proof. Let n denote a natural number. Suppose that $F_n \mid 3^{(F_n-1)/2}+1$. Then F_n cannot be divisible by 3. Let p be any prime divisor of F_n different from 3. Let δ be the exponent to which 3 belongs mod p. Since $p \mid 3^{F_n-1}-1$, we must have $\delta \mid F_n-1 = 2^{2^n}$. If δ were $< 2^{2^n}$, then $\delta = 2^k$, where k is a non-negative integer $< 2^n$. Consequently, $2^k \mid 2^{2^n-1} = (F_n-1)/2$, so $\delta \mid (F_n-1)/2$ and therefore, since $p \mid 3^\delta-1$, $p \mid 3^{(F_n-1)/2}-1$ and so, by $p \mid F_n$, we would have $p \mid 3^{(F_n-1)/2}+1$, whence $p \mid 2$, so $p = 2$, which is impossible because $p \mid F_n$ and F_n is odd. Therefore $\delta = 2^{2^n}$. But, as we know, $\delta \mid p-1$, whence $p = 2^{2^n}k+1$, where k is a natural number, whence $p \geqslant 2^{2^n}+1 = F_n$ and, since $p \mid F_n$, we see that $F_n = p$, which proves that F_n is a prime. The condition is thus proved to be sufficient.

In order to show that the condition is necessary we prove the following

LEMMA. *If p is a prime of the form $12k+5$, then $p \mid 3^{(p-1)/2}+1$.*

Proof of the lemma. If p is a prime and $p = 12k+5$, then, by the properties of Legendre's symbol, $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$, whence, by property V of Legendre's symbol, $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$. Consequently $\left(\frac{3}{p}\right) = -1$, and so $3^{(p-1)/2} \equiv -1 \pmod p$, which gives $p \mid 3^{(p-1)/2}+1$, as required.

Now let n be a natural number. Number $F_n = 2^{2^n}+1$ is of the form $12k+5$ because for any natural number n we have $2^n = 2m$, and, as it is easy to verify (by simple induction for example) that $4^m \equiv 4 \pmod{12}$ for any $m = 1, 2, \ldots$ Consequently $F_n = 4^m+1 \equiv 5 \pmod{12}$, i.e. $F_n = 12k+5$ and, if F_n is a prime, then, by the lemma, $F_n \mid 3^{(F_n-1)/2}+1$.

Thus we see that the condition of theorem 5 is sufficient.

Theorem 5 is thus proved. It implies that if F_n is a prime, then number 3 is a primitive root of number F_n. (The proof is obtained simply by noting that the number 3 belongs to the exponent $F_n-1 \bmod F_n$, which actually follows from the proof of theorem 5.)

The useful procedure for applying theorem 5 in order to decide whether a Fermat number F_n is prime or not is as follows. We denote by $\bar{t}$ the remainder left by F_n divided by an integer t and set

$$r_1 = 3, \quad r_{k+1} = \overline{r_k^2}, \quad k = 1, 2, \ldots$$

By an easy induction we verify that $F_n \mid 3^{2^{k-1}}-r_k$ holds for any $k = 1, 2, \ldots$. Hence, for $k = 2^n$, we find $F_n \mid 3^{(F_n-1)/2}-r_{2^n}$. From this we infer that number $3^{(F_n-1)/2}+1$ is congruent to $r_{2^n}+1 \bmod F_n$.

This is the very method by which numbers F_7, F_8, F_{13} and F_{14} have been proved to be composite.

The number F_7 has 39 digits, so in order to find the number $r_{2^7}+1 = r_{128}+1$, necessary for applying the procedure described above, some hundred and thirty squares of natural numbers, each having less than 39 digits, had to be calculated. Moreover, each of these squares had to be divided by number F_7 (which has 39 digits). Nowadays the calculation described above is not difficult to perform owing to the use of electronic computers, but in the year 1905, i.e. when Morehead obtained this result, the task was very tedious, although it could be performed.

A similar method was applied to F_8, F_{13} and F_{14} in order to find that they are also composite numbers. The method described above gives no information about the prime divisors of the number under consideration; neither it gives any decomposition of the number into a product of two factors greater than 1. This is why we do not know any such decomposition of the numbers F_7, F_8, F_{13} and F_{14}.

The next Fermat number, whose character is unknown, namely F_{17}, has more that 30000 digits; the calculations involved in the procedure described above, and used to show that numbers F_7, F_8, F_{13} and F_{14} are composite involve in this case some ten thousand divisions of numbers that have well over ten thousand digits, each by a number that has over 30000 digits.

EXERCISE. Find the least prime divisor of number $12^{2^{15}}+1$.

Solution. By theorem 4, each prime divisor p of number $12^{2^{15}}+1$ is of the form $12^{2^{16}}k+1$, where k is a natural number. Consequently, $p > 2^{16}+1 = F_4$. Since F_4 is a prime, by theorem 5 we have $F_4 \mid 3^{2^{15}}+1$. Hence $3^{2^{15}} \equiv -1 \pmod{F_4}$. But, in virtue of the theorem of Fermat, $2^{2^{16}} = 2^{F_4-1} \equiv 1 \pmod{F_4}$, whence $4^{2^{15}} \equiv 1 \pmod{F_4}$. Therefore $12^{2^{15}} = 3^{2^{15}} \cdot 4^{2^{15}} \equiv -1 \pmod{F_4}$, so $F_4 \mid 12^{2^{15}}+1$. Thus we see that number F_4 is the least prime divisor of number $12^{2^{15}}+1$, the latter being $> F_4$ and thus composite. We do not know whether there are infinitely many composite numbers among the numbers $12^{2^n}+1$, where $n = 1, 2, \ldots$, or whether there are infinitely many primes among them.

§ 6. How the fact that number $2^{2^{1945}}+1$ is divisible by $5 \cdot 2^{1947}+1$ was discovered. By theorem 5, any prime divisor of number F_{1945} is to be found among numbers $2^{1947}k+1$, where k are natural numbers. For $k = 1$, number $2^{1947}+1$ is divisible by 3, and so it is composite. For $k = 2$, we obtain number $2^{1948}+1 = (2^4)^{487}+1$, which is divisible by 2^4+1; so again it is a composite number. For $k = 3$ we obtain $2^{1947} \cdot 3+1$, which is divisible by 5 (because $2^4 \equiv 1 \pmod 5$), whence $2^{1947} \cdot 3+1 = (2^4)^{486} \cdot 2^3 \cdot 3+1 \equiv 2^3 \cdot 3+1 \equiv 0 \pmod 5$), and so it is composite. For $k = 4$, we obtain number $2^{1949}+1$, which is divisible by 3, and so it is composite again. Thus in order to find a prime divisor of number F_{1945} we arrive at the stage where we have to divide it by number $m = 2^{1947} \cdot 5+1$, which has 587 digits. Since, as it is easy to calculate,

number F_{1945} has more than 10^{582} digits, it is quite impossible even to write it down, let alone to divide it by m. But our aim is not to divide F_{1945} by m but to establish whether F_{1945} is divisible by m or not. The method by means of which we can do it is as follows.

We denote by $\bar{t}$ the remainder left by an integer t divided by m. It follows from the definition of $\bar{t}$ that for any integer t we have $m \mid t-\bar{t}$. We define the sequence r_k $(k=1,2,\ldots)$ by the conditions

$$r_1 = 2^2, \quad r_{k+1} = \overline{r_k^2}, \quad k = 1, 2, \ldots \tag{19}$$

We are going to prove by induction that

$$m \mid 2^{2^k} - r_k \quad \text{for any} \quad k = 1, 2, \ldots \tag{20}$$

Formula (20) is clearly true for $k=1$ because $2^{2^1}-r_1 = 0$. Suppose that it is true for a natural number k. By (20), we have $m \mid 2^{2^{k+1}} - \overline{r_k^2}$, whence, in view of $m \mid t-\bar{t}$ for $t = r_k^2$, we obtain $m \mid r_k^2 - \overline{r_k^2}$. This gives $m \mid 2^{2^{k+1}} - \overline{r_k^2}$ and so, by (19), $m \mid 2^{2^{k+1}} - r_{k+1}$. Thus formula (20) is proved by induction. For $k = 1945$ it gives

$$m \mid F_{1945} - r_{1945} - 1,$$

whence it follows that number F_{1945} is congruent to $r_{1945}+1 \pmod m$. Consequently, in order to establish whether F_{1945} is divisible by m, it is sufficient to find whether $r_{1945}+1$ is divisible by m.

Let us see what calculations are involved in calculating number r_{1945}. It follows from (19) that the numbers $r_1, r_2, \ldots$ are the remainders obtained by dividing by m, so any of them is less than m, whence it has not more than 587 digits. Thus, it follows from (19) that in order to obtain number r_{1945} one has to calculate the squares of 1944 natural numbers, each having not more than 587 digits, and to divide these squares (i.e. numbers that have no more than 1175 digits) by number m, which has 587 digits.

Present day electronic computers have proved capable of carrying out these calculations. In this way number F_{1945} has been shown to be divisible by number $m = 2^{1947}\cdot 5+1 < F_{1945}$ and so it is a composite number. The investigations of numbers $2^{1947}k+1$ for $k = 1, 2, 3, 4$, presented above together with theorem 5, show that m is the least natural divisor >1 of the number F_{1945}, and so m is a prime.

In a similar way the least prime divisors of all the other known composite Fermat numbers except the numbers F_7, F_8, F_{13}, and F_{14} have been found.

CHAPTER XI

REPRESENTATIONS OF NATURAL NUMBERS AS SUMS OF NON-NEGATIVE kth POWERS

§ 1. Sums of two squares.

THEOREM 1. *A natural number n is the sum of two squares of integers if and only if the factorization of n into prime factors does not contain any prime of the form $4k+3$ that has an odd exponent.*

LEMMA. *If an odd prime p divides the sum of the squares of two relatively prime integers, then it must be of the form $4k+1$.*

Proof of the lemma. Let a, b be two relatively prime integers and p an odd prime such that $p \mid a^2+b^2$. Then $a^2 \equiv -b^2 \pmod p$; this, raised to the $(p-1)/2$-th power gives $a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} \pmod p$. But, since $(a, b) = 1$, the numbers a, b are not divisible by p, whence, by the theorem of Fermat, $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$; consequently, $(-1)^{(p-1)/2} \equiv 1 \pmod p$, which by $p > 2$, gives $(-1)^{(p-1)/2} = 1$ and proves that $(p-1)/2$ is even. Therefore p must be of the form $4k+1$.

Proof of the theorem. Suppose that a number n can be represented as the sum of the squares of two integers,

$$n = a^2+b^2. \tag{1}$$

Let

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s} \tag{2}$$

be the factorization of n into prime factors. Finally, let p be a prime divisor of the form $4k+3$ of the number n. Write $d = (a, b)$, $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$. In virtue of (1), $d^2 \mid n$, and so $n = d^2 n_1$, where n_1 is a natural number. Suppose that the exponent on p in factorization (2) is odd. Then, since $n = d^2 n_1$, we must have $p \mid n_1 = a_1^2 + b_1^2$, which contradicts the lemma. Thus we have proved that the condition of the theorem is necessary.

In order to prove that it is sufficient we note that without any loss of generality we may assume that n is greater than 1, since for the number 1 we have $1 = 1^2+0^2$. Suppose that (2) is the factorization of n into prime factors. Let m be the greatest natural number whose square