

## NON-EXISTENCE OF ODD PERFECT NUMBERS OF THE FORM

$$3^{2\beta} \cdot p^\alpha \cdot s_1^{2\beta_1} s_2^{2\beta_2} s_3^{2\beta_3}$$

BY G. CUTHBERT WEBBER

Euler's result [2; 514], [3; 14–15] that any odd perfect number  $n$  has the form  $n = p^\alpha q_1^{2\gamma_1} q_2^{2\gamma_2} \cdots q_t^{2\gamma_t}$ , where  $p, q_1, \dots, q_t$  are primes and  $p \equiv 1 \equiv \alpha \pmod{4}$ , was extended by Sylvester [8], if  $q_1 = 3$ , in which case he proved that  $t \geq 4$ . In that paper Sylvester stated that  $t = 4$  is impossible; this statement is proved in the present paper.

The following notations are used:  $a \mid b$  and  $a \nmid b$  mean  $a$  divides  $b$  and  $a$  does not divide  $b$ , respectively;  $a \rightarrow b \pmod{m}$  means  $a$  belongs to  $b \pmod{m}$ .

**Auxiliary lemmas.** Lemmas 1 and 2 are due to Brauer [1].

**LEMMA 1.** *Let  $q$  be a positive prime. The Diophantine equation  $q^2 + q + 1 = y^m$  has no solution for  $m > 1$ .*

**LEMMA 2.** *Let  $r$  and  $s$  be different positive integers and  $p$  be a prime. The system of simultaneous Diophantine equations  $x^2 + x + 1 = 3p^r$ ,  $y^2 + y + 1 = 3p^s$ , has no solutions in positive integers  $x, y$ .*

The word different can be stricken from the above lemma since  $x^2 + x + 1 = y^2 + y + 1$  implies  $x + y = -1$  unless  $x = y$ .

We set  $f_i(x) = x^{i-1} + \cdots + x + 1$  and refer to it as a cyclotomic sum. If  $j$  is a prime  $p$ , then  $f_p(x)$  is the  $p$ -th cyclotomic polynomial. It is well known that the prime divisors of  $f_\nu(x)$  are  $p$  and primes of form  $pz + 1$ , but  $p^2$  is never a divisor.

Results concerning factors of  $f_i(x)$  are contained in

**LEMMA 3.** *If  $m, q$  and  $s$  are integers,  $t$  a prime, then*

I.  *$m \mid s$  implies  $f_m(x) \mid f_s(x)$ .*

II. *If  $q \equiv 1 \pmod{t}$ , then  $f_s(q) \equiv 0 \pmod{t}$  if and only if  $t \mid s$ .*

III. *If  $q \rightarrow k > 1 \pmod{t}$ , then  $f_s(q) \equiv 0 \pmod{t}$  if and only if  $k \mid s$ .*

*Proof.* The proofs of I and II are obvious from the form  $f_i(x) = (x^i - 1) \cdot (x - 1)^{-1}$ . In III,  $q^k - 1 \equiv 0 \pmod{t}$ ,  $f_k(q) \equiv 0 \pmod{t}$ , so that  $k \mid s$  implies  $f_s(q) \equiv 0 \pmod{t}$  by I. For the converse let  $s = ky + z$ ,  $0 \leq z < k$ . If  $z > 1$ ,  $f_s(q) = f_{ky}(q) + q^{ky} + q^{ky+1} + \cdots + q^{ky+z-1} \equiv 0 + 1 + q + \cdots + q^{z-1} \pmod{t}$ . Hence,  $f_s(q) \equiv 0 \pmod{t}$  implies  $f_z(q) \equiv 0 \pmod{t}$  which is impossible with  $z < k$ . Accordingly,  $z = 0$  so that  $k \mid s$ .

Received March 3, 1948; in revised form, June 25, 1951. Presented to the American Mathematical Society, October 25, 1947. While this paper was in the hands of the Editor a paper by Ullrich Kühnel [5] appeared containing the same result.