THEOREM II. *Let $C_1P_1 + \cdots + C_sP_s$ be identically zero, where the P_i are distinct power products each of degree $d>0$ in a nonzero F and its derivatives. Then each C_i is in the perfect ideal generated by F.*

NEW YORK CITY

ON THE NON-EXISTENCE OF ODD PERFECT NUMBERS OF FORM $p^{\alpha}q_1^2q_2^2 \cdots q_{t-1}^2q_t^4$

ALFRED BRAUER[1]

One of the oldest unsolved mathematical problems is the following one: Are there odd perfect numbers?[2] If such a number n exists, it must have the form

$$n = p^{\alpha} q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_t^{2\beta_t}$$

where $p, q_1, q_2, \cdots, q_t$ are primes and $p \equiv \alpha \equiv 1 \pmod 4$. This has been proved by Euler.[3] Sylvester[4] obtained estimates for t, in particular $t \geqq 4$, and $t \geqq 7$ if $n \not\equiv 0 \pmod 3$. Recently, it was shown by R. Steuerwald[5] that the case $\beta_1 = \beta_2 = \cdots = \beta_t = 1$ is impossible, and by H. J. Kanold[6] that the same is true for $\beta_1 = \beta_2 = \cdots = \beta_t = 2$. Moreover Kanold proved that n is not perfect if the greatest common divisor d of $2\beta_1+1, 2\beta_2+1, \cdots, 2\beta_t+1$ is divisible by 9, 15, 21, or 33, and some similar results. All these results deal with the case $d>1$.

In the following, it will be proved that no odd perfect number n of form $p^{\alpha}q_1^2q_2^2 \cdots q_{t-1}^2q_t^4$ exists. Here we have $d=1$. For the proof I use

Presented to the Society, April 24, 1943; received by the editors March 1, 1943.

[1] The relation of the results of this paper to another paper by H. J. Kanold, *Verschärfung einer notwendigen Bedingung für die Existenz einer ungeraden vollkommenen Zahl*, J. Reine Angew. Math. vol. 184 (1942) pp. 116–124, will be considered in an addendum to be published in the December Bulletin.

[2] For the history of the problem see Dickson, *History of the theory of numbers*, vol. 1, 1919, pp. 1–33.

[3] *Commentationes arithmeticae collectae*, vol. 2, *Tractatus de numerorum doctrina* 1849, p. 514; *Opera postuma*, vol. 1, 1862, pp. 14–15.

[4] *Sur l'impossibilité de l'existence d'un nombre parfait impair qui ne contient pas au moins* 5 *diviseurs premiers distincts*, C. R. Acad. Sci. Paris vol. 106 (1888) pp. 522–526; *Collected mathematical papers*, vol. 4, 1912, pp. 611–614. *Sur une classe spéciale des diviseurs de la somme d'une série géométrique*, C. R. Acad. Sci. Paris vol. 106 (1888) pp. 446–450; *Collected mathematical papers*, vol. 4, 1912, pp. 607–610.

[5] *Verschärfung einer notwendigen Bedingung für die Existenz einer ungeraden vollkommenen Zahl*, Sitzungsberichte der mathematisch-naturwissenschaftlichen Abteilung der Bayerischen Akademie der Wissenschaften zu München, 1937, pp. 68–72.

[6] *Untersuchungen über ungerade vollkommene Zahlen*, J. Reine Angew. Math. vol. 183 (1941) pp. 98–109.

theorems of T. Nagell on Diophantine equations. With the same method similar results may be obtained.

LEMMA 1. *Let q be a positive prime. The Diophantine equation*

$$q^2 + q + 1 = y^m$$

has no solution for $m > 1$.

PROOF. T. Nagell[7] has proved the following theorem: *If $m > 1$ is not a power of 3, then the Diophantine equation $x^2+x+1=y^m$ has no solutions in integers x, y with $y \neq \pm 1$.* In order to obtain all the solutions of

$$x^2 + x + 1 = y^3, \tag{1}$$

it is sufficient to solve the cubic Diophantine equation

$$a^3 - 3ab^2 + b^3 = 1 \tag{2}$$

and to set

$$x = a^3 - 3a^2b + b^3 - 1 \quad \text{and} \quad x = -a^3 + 3a^2b - b^3. \tag{3}$$

It follows from the Theorem of Thue-Siegel that (2) has only a finite number of solutions. Nagell gives the solutions

$$a=1,\ b=0;\quad a=0,\ b=1;\quad a=b=-1;\quad a=2,\ b=-1;\quad a=1,\ b=3. \tag{4}$$

But it is unknown whether there are other solutions in integers a, b. Since the discriminant of (2) is positive, we can not apply the general theorems of Delaunay and Nagell for cubic Diophantine equations. It follows from (3) and (4) that (1) has at least the following solutions: $x=0$, $y=1$; $x=-1$, $y=1$; $x=18$, $y=7$; $x=-19$, $y=7$.

By Nagell's theorem we have only to consider the case $m=3^k$ for the proof of our lemma. But we do not need the complete solution of (1); it is sufficient to prove that this equation has no solution where $x=q$ is a positive prime.

For $q=3$ we have $q^2+q+1=13$. This is no cube. If $q \equiv 1 \pmod 3$, then

$$q^2 + q + 1 \equiv 0 \pmod 3, \tag{5}$$

but

$$q^2 + q + 1 \not\equiv 0 \pmod{3^2} \tag{6}$$

[7] *Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$*, Norsk Matematisk Forenings, Skrifter (1) no. 2 (1921). Cf. *L'analyse indéterminée de degré supérieure*, Mémorial des Sciences Mathématiques, vol. 39 (1929), p. 58.

since it is well known that the prime divisors of the pth cyclotomic polynomial $f_p(x)$, where p is a prime, are the primes of form $ph+1$ and p itself; but $f_p(x)$ is not divisible by p^2 for any integer x. It follows from (5) and (6) that q^2+q+1 is not a cube for $q\equiv 1 \pmod 3$.

Now, let q be a prime of form $3h+2$. Since $y^2+y+1<y^3$ for $y\geqq 2$, it follows from $q^2+q+1=y^3$ that $q>y$. Moreover we have $q(q+1)=(y-1)(y^2+y+1)$. Since q is a prime and greater than y, it follows that $y-1$ is relatively prime to q. Hence q is a divisor of y^2+y+1. This gives a contradiction because y^2+y+1 has no prime divisor of form $3h+2$.

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.*

PROOF. Nagell[8] has proved that the Diophantine equation $x^2+x+1=3z^k$ $(k>2)$ has no solution with $z>1$. Hence we have only to consider the case $r=1$, $s=2$. Then we have

$$x^2+x+1=3p, \qquad y^2+y+1=3p^2. \tag{7}$$

If these equations have a solution in positive integers, then it follows from (7) that

$$0<x<p<y<2p \tag{8}$$

and, on the other hand, that

$$(2x+1)^2 \equiv -3 \equiv (2y+1)^2 \pmod p,$$
$$2x+1 \equiv \pm(2y+1) \pmod p$$

since p is a prime, hence either

$$x \equiv y \pmod p \tag{9}$$

or

$$x \equiv -y-1 \pmod p. \tag{10}$$

In the first case, it follows from (8) and (9) that

$$y = p + x \tag{11}$$

and in the second case, from (8) and (10) that

$$y = 2p - x - 1. \tag{12}$$

On the other hand, it follows from (7) that $p\neq 3$ and that $x\equiv y\equiv 1$

[8] Loc. cit.

(mod 3). This contradicts (11) and (12).

Now we are able to prove our theorem.

THEOREM. *An odd number of form* $n=p^\alpha q_1^2q_2^2 \cdots q_{t-1}^2q_t^4$ *is not perfect.*

PROOF. We change the notation and write n in the following form

$$n = p^\alpha q_1^2 q_2^2 \cdots q_k^2 r_1^2 r_2^2 \cdots r_l^2 s^4 \qquad (k \geqq 0, l \geqq 0)$$

where the primes q_κ are congruent to 1 (mod 3) and where the primes r_λ are incongruent to 1 (mod 3). Let us assume that n is perfect, then we have

$$2n = \sigma(n) = \sigma(p^\alpha)\sigma(q_1^2)\sigma(q_2^2) \cdots \sigma(q_k^2)\sigma(r_1^2)\sigma(r_2^2) \cdots \sigma(r_l^2)\sigma(s^4),$$

where $\sigma(n)$ denotes the sum of the divisors of n. It follows that

$$\begin{aligned} 2n &= 2p^\alpha q_1^2 q_2^2 \cdots q_k^2 r_1^2 r_2^2 \cdots r_l^2 s^4 \\ &= \sigma(p^\alpha)\prod_{\kappa=1}^{k}(1+q_\kappa+q_\kappa^2)\prod_{\lambda=1}^{l}\{(1+r_\lambda+r_\lambda^2)\}(1+s+s^2+s^3+s^4). \end{aligned} \tag{13}$$

Each factor $1+q_\kappa+q_\kappa^2$ is divisible by 3, but not by 9; each factor $1+r_\lambda+r_\lambda^2$ is not divisible by 3. All the other prime divisors of

$$\prod_{\kappa=1}^{k}(1+q_\kappa+q_\kappa^2)\prod_{\lambda=1}^{l}(1+r_\lambda+r_\lambda^2)$$

have the form $3h+1$. We have now to distinguish between some cases.

I. $n \not\equiv 0$ (mod 3). Here we have $k=0$. Since n is not divisible by 3, it follows from Sylvester's theorem mentioned above that n must contain at least 8 different primes; hence $l \geqq 6$. Moreover we obtain from (13) that $\prod_{\lambda=1}^{l}(1+r_\lambda+r_\lambda^2)$ is a divisor of $p^\alpha s^4$. It may happen that one of the l factors of this product equals p, but each of the $l-1$ remaining factors cannot be a power of p by Lemma 1. Hence each of these $l-1$ factors must be divisible by s, and their product must be divisible by s^5. This gives a contradiction.

II. $n \equiv 0$ (mod 3), $n \not\equiv 0$ (mod 27). Here $k \leqq 2$. One of the primes r_λ, say r_1, equals 3 since $p=3$ is not possible. It follows that n is divisible exactly by 3^2, and hence by $\sigma(3^2)=13$, because of (13). Therefore we have either $13=p$, $13=q_1$, or $13=s$.

IIa. $p=13$. Since $\alpha+1$ is even, $\sigma(p^\alpha)=(p^{\alpha+1}-1)/(p-1)$ is divisible by $p+1$. Hence n must be divisible by 7, and it follows that either one of the primes q_κ, say $q_1=7$, or $s=7$.

II$a\alpha$. $q_1=7$. n must be divisible by $\sigma(q_1^2)=57$, therefore by 19, and we have either $q_2=19$ or $s=19$.

II$a\alpha$1. $q_2=19$. n is divisible by $\sigma(q_2^2)=381$, hence by 127. Since $127\equiv 1 \pmod 3$ and $k\leqq 2$, we have $127=s$. Thus

$$n = 13^{\alpha}\cdot 3^2\cdot 7^2\cdot 19^2\cdot 127^4 r_2^2 r_3^2 \cdots r_l^2,$$

$$(14)\qquad \begin{aligned} 1 = \frac{\sigma(n)}{2n} &= \frac{\sigma(13^{\alpha})\cdot 13\cdot 57\cdot 381\cdot\sigma(127^4)\sigma(r_2^2)\cdots\sigma(r_l^2)}{2\cdot 13^{\alpha}\cdot 9\cdot 49\cdot 361\cdot 127^4\cdot r_2^2\cdots r_l^2} \\ &= \frac{\{(1/14)\cdot\sigma(13^{\alpha})\}\sigma(127^4)\sigma(r_2^2)\cdots\sigma(r_l^2)}{13^{\alpha-1}\cdot 7\cdot 19\cdot 127^3\cdot r_2^2\cdots r_l^2}.\end{aligned}$$

Since the prime divisors of $\sigma(127^4)$ have the form $5h+1$, they are different from 7, 13, 19, and 127. It follows now from (14) that they are of form $3h+2$, hence of form $15h+11$. Since

$$\sigma(127^4) \equiv 1+7+4+13+1 \equiv 11 \pmod{15},$$

the number of prime divisors of $\sigma(127^4)$ must be odd if n should be perfect.

Let us first assume that $\sigma(127^4)$ is a prime. Then we have $\sigma(127^4) = r_\lambda$,

$$(15)\qquad \begin{aligned}\sigma(r_\lambda^2) = 1 + r_\lambda + r_\lambda^2 = 1 + 1 + 127 + 127^2 + 127^3 + 127^4 \\ + (1 + 127 + 127^2 + 127^3 + 127^4)^2.\end{aligned}$$

Setting $\sigma(r_\lambda^2)=A$ it follows from (14) that A can have only the prime divisors 7, 13, 19, and 127. But, by (15),

$$A \not\equiv 0 \pmod 7,\qquad A\not\equiv 0 \pmod{19},\qquad A\not\equiv 0 \pmod{127}.$$

Since $A>13$, it follows that A is a power of 13. This contradicts Lemma 1.

Let us assume now that $\sigma(127^4)$ is composite. Since the number of its prime divisors would be odd, there would be at least 3 factors r_λ, and at least one of them, say r_2, must be less than $\{\sigma(127^4)\}^{1/3}$. But

$$\{\sigma(127^4)\}^{1/3} < \{127^3(127+1+.01)\}^{1/3} < 641,$$

therefore r_2 would be one of the following primes of form $15h+11$: 11, 41, 71, 101, 131, 191, 251, 281, 311, 401, 431, 461, 491, 521. Since $\sigma(r_2^2)\neq 7$, 13, 19, 127, it must be divisible by at least two of these primes, by Lemma 1. But $f(x)=1+x+x^2\equiv 0 \pmod 7$ for $x\equiv 2$, 4; $f(x)\equiv 0 \pmod{13}$ for $x\equiv 3$, 9; $f(x)\equiv 0 \pmod{19}$ for $x\equiv 7$, 11. Hence it is easy to see that $\sigma(r_2^2)$ is relatively prime to $7\cdot 13\cdot 19$ for $r_2=41$, 71, 101, 131, 251, 281, 461, 491, 521. For $r_2=401$ and 431 we have $(\sigma(r_2^2), 13\cdot 19)=1$ and $\sigma(r_2^2)\not\equiv 0 \pmod{127}$. For the remaining primes 11 and 191 we have $\sigma(127^4)\not\equiv 0 \pmod{11}$ and $\sigma(127^4)\not\equiv 0 \pmod{191}$. This is impossible since r_2 was a divisor of $\sigma(127^4)$.

II$a\alpha$2. $s=19$. Since $\sigma(19^4)$ is divisible by 151, we have $q_2=151$, and since $\sigma(151^2)=22953=3\cdot 7\cdot 1093$, we have $q_3=1093$. This contradicts $k\leqq 2$.

II$a\beta$. $s=7$. Since $\sigma(7^4)=2801$ is a prime and since $\sigma(2801^2)=37\cdot 43\cdot 4933$, it follows that $q_1=37$, $q_2=43$, $q_3=4933$. This is impossible.

IIb. $q_1=13$. Since $\sigma(q_1^2)=3\cdot 61$, we have either p, q_2 or $s=61$.

II$b\alpha$. $p=61$. Here n is divisible by $(p+1)/2$, hence either $q_2=31$ or $s=31$.

II$b\alpha$1. $q_2=31$. Since $\sigma(q_2^2)=3\cdot 331$ and $k\leqq 2$, we have $s=331$. Therefore n is divisible by $\sigma(331^4)$, hence by 5, and n has the form

$$n = 61^\alpha\cdot 3^2\cdot 13^2\cdot 31^2\cdot 5^2\cdot 331^4\cdot M^2. \tag{16}$$

Since $\sigma(p^\alpha)/p^\alpha \geqq (p^\alpha+p^{\alpha-1})/p^\alpha=(p+1)/p$, it follows from (16) that

$$\sigma(n)/2n > (62\cdot 13\cdot 183\cdot 993\cdot 31)/(2\cdot 61\cdot 9\cdot 13^2\cdot 31^2\cdot 25) = 331/325 > 1.$$

This is impossible.

II$b\alpha$2. $s=31$. $\sigma(31^4)\equiv 0 \pmod{11}$ and $\sigma(11^2)=7\cdot 19$. Hence $q_2=7$ and $q_3=19$. This contradicts $k\leqq 2$.

II$b\beta$. $q_2=61$. Since $\sigma(61^2)=3\cdot 13\cdot 97$, we have either $p=97$ or $s=97$. If $p=97$, then n is divisible by $(p+1)/2=7^2$, therefore $s=7$ since $q_1=13$, $q_2=61$, and $k\leqq 2$. But it was proved in II$a\beta$ that $s=7$ is impossible. For $s=97$ the proof is the same as in II$b\alpha$2 since $97\equiv 31 \pmod{11}$.

II$b\gamma$. $s=61$. $\sigma(61^4)$ is divisible by 5 and by 131. Therefore $r_2=131$, and either $p=5$ or $r_3=5$. If $p=5$, then $\sigma(p^\alpha)$ contains the factor $p+1=6$. Thus $\sigma(n)$ can contain only one other factor 3, hence $k=1$. Since $\sigma(131^2)\not\equiv 0 \pmod{13}$ and $\sigma(131^2)\not\equiv 0 \pmod{61}$, it is necessary that $\sigma(131^2)$ and n contain another prime factor of form $3h+1$. This is impossible. If $r_3=5$, then n is divisible by $\sigma(5^2)=31$, hence $q_2=31$, $q_3=331$. This contradicts $k\leqq 2$.

IIc. $s=13$. Since $\sigma(13^4)=30941$ is a prime, we have either $p=30941$ or $r_2=30941$. But $p=30941$ is impossible because n must be divisible by $(p+1)/2$ and $30941\equiv -1 \pmod{27}$. Hence $n\equiv 0 \pmod{27}$; this contradicts $k\leqq 2$. Therefore $r_2=30941$, and n is divisible by $\sigma(30941^2)$.

Let us first assume that $\sigma(30941^2)$ is a prime, then $\sigma(30941^2)=q_1$ since $\sigma(30941^2)\equiv 3 \pmod 4$. Now $\sigma(q_1^2)\equiv 0 \pmod{151}$, therefore

$q_2=151$, and n is divisible by $\sigma(151^2)$, hence by 7. This contradicts $k\leqq 2$.

Let us now assume that $\sigma(30941^2)$ is composite. It is easy to see that all the prime factors of $\sigma(30941^2)$ are greater than 151. Since these prime factors are congruent to 1 (mod 3), it follows that either $q_1>150$ and $q_2>150$, or $q_1>150$ and $p>150$.

In the first case we have $k=2$ and hence $p\not\equiv 2$ (mod 3), therefore $p\equiv 1$ (mod 12). Since $(p+1)/2$ is a divisor of n and since 19 cannot be a divisor of n, the case $p=37$ is impossible. It follows that $p>60$.

In the latter case we have $q_2>60$ if $k=2$, because otherwise $\sigma(q_2^2)$ is divisible by one of the primes 19, 127, 331, 7, or 631; this is impossible since these primes are not divisors of $\sigma(30941^2)$. Hence, if $k=2$, two of the primes q_1, q_2, p are greater than 150 and the third is greater than 60. The product

$$P=\prod_{\kappa=1}^{2}\sigma(q_\kappa^2)\prod_{\lambda=1}^{l}\sigma(r_\lambda^2)$$

must be a divisor of $9p^\alpha q_1^2q_2^2s^4$. Each factor $\sigma(q_\kappa^2)$ is divisible by 3. But only one of them may have the form $3p^t$ by Lemma 2. Therefore at least one of the 8 prime factors of $q_1^2q_2^2s^4$ is a divisor of $\sigma(q_1^2)\sigma(q_2^2)$; hence only 7 of these factors may be divisors of the product $\sigma(r_1^2)\sigma(r_2^2)\cdots\sigma(r_l^2)$. It may happen that one of these l factors equals p; each of the others is not a power of p, by Lemma 1, and contains, therefore, at least one of the remaining 7 prime factors of $q_1^2q_2^2s^4$. It follows that $l\leqq 8$.

We have $r_1=3$; $r_2=30941$. The primes r_λ are different from 5, 11, 23, 47, 53, 83, since $q_1>60$ and $q_2>60$. Therefore $r_3\geqq 17$, $r_4\geqq 29$, $r_5\geqq 41$, $r_6\geqq 59$, $r_7\geqq 71$, $r_8\geqq 89$ and

$$\frac{\sigma(n)}{2n}<\frac{\sigma(151^2)\cdot 151\cdot 61\cdot 13\cdot 30941\cdot\sigma(17^2)\cdot\sigma(29^2)\cdot 41\cdot 59\cdot 71\cdot 89\cdot 30941}{2\cdot 151^2\cdot 150\cdot 60\cdot 9\cdot 13^4\cdot 17^2\cdot 29^2\cdot 40\cdot 58\cdot 70\cdot 88\cdot 30940}<1.$$

This is not possible. For $k=1$, it follows similarly that $l\leqq 7$, and the proof is the same.

III. $s=3$. Here we have $k\leqq 4$. Since n must be divisible by $\sigma(3^4)=121$, it follows successively that n is divisible by 7, 19, 127, 5419, and 31. These five primes are congruent to 1 (mod 3) and congruent to 3 (mod 4). Hence $k\geqq 5$; this is impossible. Herewith our theorem is proved for each case.

UNIVERSITY OF NORTH CAROLINA