Proof of a conjecture of Kummer.

By PETER DÉNES in Budapest.

§ 1. Introduction.

E. KUMMER [1] stated without proof the following

Theorem. *If n is a non-negative rational integer, p an odd prime, $\zeta = e^{2\pi i/p}$, $\Omega(\zeta)$ the field of the p^{th} roots of unity over the rational number field, φ, φ_1 are integers, prime to p, in $\Omega(\zeta)$ satisfying the congruence*

$$(1) \qquad \varphi \equiv \varphi_1 \pmod{p^{n+1}},$$

and if k is a rational integer, with $(p-1) \nmid k$, then

$$D_{kp^n} \log \varphi(e^v) \equiv D_{kp^n} \log \varphi_1(e^v) \pmod{p^{n+1}},$$

where the symbol $D_m \log \varphi(e^v)$ denotes the value of the m^{th} derivative of $\log \varphi(e^v)$ with respect to v at $v = 0$. $\varphi(e^v)$ results by setting e^v instead of ζ in $\varphi(\zeta)$, and e is the Naperian base.

H. S. VANDIVER [2] ascertained that KUMMER has not published any proof of the above theorem and proved it first [3] in the special case $\varphi = \varphi_1$, $\varphi(1) = \varphi_1(1)$, $n = 1$; then in a later paper [4] in the case $\varphi = \varphi_1$, $\varphi(1) \equiv \varphi_1(1) \pmod{p^{n+1}}$. In 1939 Vandiver has mentioned that J. V. USPENSKY has proved KUMMER's above conjecture with the only restriction $\varphi = \varphi_1$, but this paper was not yet published [5].

In this paper I give the complete proof of the above theorem (see § 3). Prof. VANDIVER informed me in a letter of August 31, 1951, when I communicated him my proof that the paper of USPENSKY has not been published because of his death and is not intended to be published in the near future. I am giving therefore firstly in § 2 a proof for the result of USPENSKY, i. e. for the case $\varphi = \varphi_1$ of the theorem, which certainly differs from USPENSKY's proof who attained his result by correcting the methods of KUMMER. On the other hand, the proof given in § 2 (see Lemma G) uses methods perfectly different from KUMMER's ones.

§ 2. Lemmas.

We are beginning with the proof of some lemmas.

Lemma A. *If k and m are rational integers, and $0 < k < m$, then*

$$D_k (1-e^v)^m = 0.$$

The proof follows immediately from

$$\frac{d^k (1-e^v)^m}{dv^k} = (-1)^k m(m-1)\cdots(m-k+1)(1-e^v)^{m-k} \cdot e^{kv}.$$

Lemma B. *If $F(e^v)$ is a polynom of e^v the coefficients of which are rational integers and $F_0 \neq 0$ denotes its value at $v=0$, then for $k>0$*

$$D_k \log F(e^v) = \sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} D_k \left(\frac{F(e^v)-F_0}{F_0} \right)^i.$$

Proof. We remark that if $|F(e^v)-F_0| < |F_0|$, then

$$\log F(e^v) = \log F_0 + \sum_{i=1}^{\infty} \frac{(-1)^{i-1}}{i} \left(\frac{F(e^v)-F_0}{F_0} \right)^i.$$

Now, in

$$F(e^v) = \sum_{g=0}^{t} a_g e^{gv}$$

the coefficients $a_0, \ldots, a_t$ are rational integers. We transform this polynom:

$$F(e^v) = \sum_{j=0}^{t} b_j (1-e^v)^j$$

where $b_0, \ldots, b_t$ are also rational integers, namely

$$b_j = (1-1)^j \sum_{g=j}^{t} \binom{g}{j} a_g.$$

Thus we have

$$F(e^v) - F_0 = \sum_{j=1}^{t} b_j (1-e^v)^j,$$

as $F_0 = b_0$. Hence

$$D_k \left[\frac{F(e^v)-F_0}{F_0} \right]^i = \frac{1}{F_0^i} \cdot D_k \sum_{j=i}^{it} B_j (1-e^v)^j,$$

where $B_i, \ldots, B_{it}$ are rational integers. By Lemma A we see that for $i > k$

$$D_k \left(\frac{F(e^v)-F_0}{F_0} \right)^i = 0.$$

Since $\log F_0$ is a constant, we have the proof of Lemma B.

Lemma C. *If f_0 is a rational integer such that $f_0 \equiv F_0 \pmod{p}$, and $p \nmid f_0$, then for positive integers k, u*

$$D_k \log F(e^v) \equiv \sum_{i=1}^{w} (-1)^{i-1} \frac{1}{i} D_k \left[\frac{F(e^v)-f_0}{f_0} \right]^i \qquad (\bmod p^u)$$

holds, where w is a suitable positive integer.

Proof. By hypothesis we have

$$F_0 - f_0 = Mp$$

where M is a rational integer. Thus

$$F(e^v) - f_0 = Mp + \sum_{j=1}^{t} b_j (1 - e^v)^j,$$

and hence

$$\frac{1}{i} \cdot D_k \left[\frac{F(e^v) - f_0}{f_0} \right]^i = \frac{1}{i \cdot f_0^i} D_k \sum_{g=0}^{i} \sum_{j=i-g}^{(i-g)t} C_{gj} \cdot p^g (1 - e^v)^j,$$

where the C's are rational integers. The members on the right-hand side in which the second index j of C is greater than k disappear according to Lemma A. The remaining members, for $j \leqq k$, are multiplied by the g^{th} power of p. From the inequalities

$$k \geqq j \geqq i - g$$

we get

$$g_{\min} = i - k.$$

We set now $i = i^* p^r$ with $p \nmid i^*$. We see, by $p \nmid f_0$, that the remaining members are divisible by p^{g-r} and so Lemma C is true if

$$g - r > u,$$

i. e., — as the most inadvantageous case is $g = g_{\min}$ — if

$$i^* p^r > k + u + r.$$

As $p \geqq 3$, the inequality $p^z > k + u + z$ has for any value of $k + u$ a minimal solution $z = z_0$. Now putting

$$w = p^{z_0},$$

the members with $i \geqq w$ on the right-hand side of

$$D_k \log F(e^v) = D_k \log f_0 + \sum_{i=1}^{\infty} \frac{(-1)^{i-1}}{i} D_k \left(\frac{F(e^v) - f_0}{f_0} \right)^i$$

are all divisible by p^u which completes the proof.

Lemma D. *If k is a positive intenger, with $(p-1) \nmid k$, $n \geqq 0$ a rational integer, $h(e^v)$ a polynom of e^v*

$$h(e^v) = \sum_{i=0}^{t} f_i \cdot e^{iv} \tag{2}$$

with rational integers $f_0, \ldots, f_t$, and

$$g(e^v) = \sum_{i=0}^{p-1} e^{iv}, \tag{3}$$

then

$$D_{kp^n} h(e^v) \cdot g(e^v) \equiv 0 \pmod{p^{n+1}}. \tag{4}$$

Proof. If i is a non-negative rational integer, then we get

$$D_{kp^n} e^{iv} \cdot g(e^v) = i^{kp^n} + (i+1)^{kp^n} + \cdots + (i+p-1)^{kp^n},$$

and $i, i+1, \ldots, i+p-1$ represent a complete system of residues mod p. If r is a primitive root mod p and w a member of this system, prime to p, then

$$w \equiv r^z \pmod{p}$$

and

$$w^{kp^n} \equiv r^{zkp^n} \pmod{p^{n+1}},$$

where the number z takes all the values $1, 2, \ldots, p-1$. Hence, as $kp^n \geqq n+1$, we have

$$D_{kp^n} e^{iv} \cdot g(e^v) \equiv \frac{r^{(p-1)kp^n} - 1}{r^{kp^n} - 1} \pmod{p^{n+1}},$$

where $(r^{kp^n} - 1)$ is prime to p, as $(p-1) \not| \, k$ and

$$r^{(p-1)kp^n} \equiv 1 \pmod{p^{n+1}}.$$

Consequently

$$D_{kp^n} e^{iv} \cdot g(e^v) \equiv 0 \pmod{p^{n+1}}. \tag{5}$$

From (2) and (5) follows (4) immediately.

Lemma E. *If $q > 0, s > 0, n \geqq 0$ are rational integers and $h(e^v)$ is defined by* (2), *then*

$$D_{q(p-1)p^n} h(e^v) \cdot g^s(e^v) \equiv 0 \pmod{p^z}, \tag{6}$$

where $z = \min\ [(s-1), (n+1)]$.

Proof. We put

$$\{g(e^v)\}^s = \sum_{i=0}^{s(p-1)} a_{s,i} \cdot e^{iv},$$

where $a_{s,0}, \ldots, a_{s,s(p-1)}$ are rational integers and

$$A_{s,i} = \sum_{j=0}^{\left[\frac{(p-1)s+p-i}{p}\right]} a_{s,i+jp} \qquad (i = 0, 1, \ldots, p-1),$$

where $[x]$ denotes the largest integer $\leqq x$. Then

$$A_{s,i} = p^{s-1} \qquad (i = 0, 1, \ldots, p-1). \tag{7}$$

(7) can be verified by induction. Assuming that it is true for $s-1$ instead of s, we get from

$$\{g(e^v)\}^s = \{g(e^v)\}^{s-1} \cdot (1 + e^v + \cdots + e^{(p-1)v}),$$

$$A_{s,i} = A_{s-1,i} + A_{s-1,i+1} + \cdots + A_{s-1,p-1} + A_{s-1,0} + \cdots + A_{s-1,i-1} = p \cdot p^{s-2} = p^{s-1}.$$

As (7) is true also for $s = 1$, we have the proof of (7). Moreover we have

$$D_{q(p-1)p^n} e^{jv} \cdot g^s(e^v) = \sum_{i=0}^{s(p-1)} a_{s,i} \cdot (i+j)^{q(p-1)p^n}. \tag{8}$$

If $(i+j)$ is divisible by p, then $(i+j)^{q(p-1)p^n} \equiv 0 \pmod{p^z}$, because of

$q(p-1)p^n > n+1 \geqq z$; consequently, if we regard (8) as a congruence modulo p^z, all members fall out which are divisible by p. If, on the other hand, $p \nmid (i+j)$, then

$$(i+j)^{q(p-1)p^n} \equiv 1 \pmod{p^{n+1}},$$

or, as $z \leqq n+1$,

$$(i+j)^{q(p-1)p^n} \equiv 1 \pmod{p^z}.$$

Thus, we get by (8)

$$D_{q(p-1)p^n} e^{j v} \cdot g^s(e^v) \equiv \sum_{i=0}^{s(p-1)} a_{s,i} \equiv (p-1)p^{s-1} \pmod{p^z},$$

and as $s-1 \geqq z$, finally

$$D_{q(p-1)p^n} e^{j v} \cdot g^s(e^v) \equiv 0 \pmod{p^z}$$

which completes, by (2), the proof.

Lemma F. *If* $c>0$, $k>0$, $m \geqq 0, n \geqq 0$ *are rational integers, with* $k < p-1$, *and* $h(e^v)$ *is defined by* (2), *then*

$$D_{kp^n} h(e^v) \cdot g^{cp^m}(e^v) \equiv 0 \pmod{p^{m+n+1}}. \tag{9}$$

Proof. First we assume $p>3$ and $m \geqq 1$, or, if $p=3$, either $c>1$, or $m>1$. (Thus, the cases $m=0$, resp. $p=3$ and $cm=1$ are excluded for the present.) According to the law of differentiation of a product we have

$$D_{kp^n} h(e^v) \cdot g^{cp^m}(e^v) = \sum_{i=0}^{kp^n} \binom{kp^n}{i} \cdot D_i h(e^v) \cdot g^{c(p-2)p^{m-1}}(e^v) \cdot D_{kp^n-i}\, g^{2cp^{m-1}}(e^v). \tag{10}$$

We assume that Lemma F is true for $m-1$ instead of m. In (10), the number i should be divisible by the j^{th} power of p:

$$i = qp^j \qquad (p \nmid q, 0 \leqq j \leqq n).$$

Therefore by $k<p$ the binomial coefficient $\binom{kp^n}{qp^j}$ is divisible by the $(n-j)^{th}$ power of p:

$$\binom{kp^n}{qp^j} \equiv 0 \qquad \pmod{p^{n-j}}. \tag{11}$$

If neither i, nor $(kp^n - i)$ is divisible by $p-1$, then we have, according to our assumption that Lemma F holds for $m-1$ instead of m,

$$D_{qp^j} h(e^v) \cdot g^{c(p-2)p^{m-1}}(e^v) \equiv 0 \qquad \pmod{p^{m+j}}$$

and

$$D_{kp^n-qp^j}\, g^{2cp^{m-1}}(e^v) \equiv 0 \qquad \pmod{p^{m+j}}$$

from which follows by $m>0$:

$$(n-j)+(m+j)+(m+j) \geqq n+m+1. \tag{12}$$

If for example i is divisible by $(p-1)$, then Lemma E can be used. If $p>3$, then $c(p-2)p^{m-1} \geqq 2$, as $c>0$ and $m>0$; therefore $z \geqq 1$. If $p=3$ and $mc>1$, then again $z \geqq 1$, because of $c \cdot 3^{m-1} \geqq 2$. Hence

$$D_{qp^j} h(e^v) \cdot g^{c(p-2)p^{m-1}}(e^v) \equiv 0 \quad \pmod{p}, \quad \text{if} \quad (p-1) \mid q.$$

Thus we have also in this case

(13) $$(n-j)+(j+m)+1=n+m+1,$$

and the same equation holds if (kp^n-i) is divisible by $(p-1)$, because of $2cp^{m-1}\geqq 2$. Both numbers i and kp^n-i cannot be divisible at the same time by $(p-1)$, as $0<k<p-1$. (12) and (13) give the exponent of the power of p, by which the members on the right-hand side of (10) are divisible by our assumptions.

Now in the case $p=3$, $mc=1$ we have

$$D_{3^n k}e^{uv}\cdot g^3(e^v)=u^{3^n k}+3(u+1)^{3^n k}+6(u+2)^{3^n k}+7(u+3)^{3^n k}+$$
$$+6(u+4)^{3^n k}+3(u+5)^{3^n k}+(u+6)^{3^n k}$$

which can be transformed as a congruence modulo 3^{n+2}:

$$\begin{aligned}D_{3^n k}e^{uv}\cdot g^3(e^v)&\equiv\\ &\equiv\{u^{3^n k}+7u^{3^n k}+7\cdot 3\cdot 3^n k\cdot u^{3^n k-1}+u^{3^n k}+6\cdot 3^n ku^{3^n k-1}\}+\\ &+\{3(u+1)^{3^n k}+6(u+1)^{3^n k}+6\cdot 3\cdot 3^n k(u+1)^{3^n k-1}\}+\\ &+\{6(u+2)^{3^n k}+3(u+2)^{3^n k}+3\cdot 3\cdot 3^n k(u+2)^{3^n k-1}\}\equiv\\ &\equiv 9u^{3^n k}+9(u+1)^{3^n k}+9(u+2)^{3^n k}\equiv 0 \qquad (\operatorname{mod} 3^{n+2}).\end{aligned}$$

This proves, by (2), the validity of Lemma F in the case $p=3$, $m=1$, $c=1$.

Hence, Lemma F is proved by the assumptions that $m>0$ and that it is true for $m-1$ instead of m; to complete the induction, we must verify it for the case $m=0$:

$$D_{kp^n}h(e^v)\cdot g^c(e^v)\equiv 0 \qquad (\operatorname{mod} p^{n+1}).$$

This follows, however, immediately from Lemma D, by setting in (4) instead of $h(e^v)$ the polynom $h(e^v)\{g(e^v)\}^{c-1}$.

Lemma G. *If n is a non-negative rational integer, k a positive integer, $(p-1)\nmid k$, φ is an integer, prime to p, in $\Omega(\zeta)$, and φ_1 is another form of φ, then*

$$D_{kp^n}\log\varphi(e^v)\equiv D_{kp^n}\log\varphi_1(e^v) \qquad (\operatorname{mod} p^{n+1}).$$

Proof. If φ is prime to p, also $\varphi(1)$ is prime to p; hence Lemma B implies that $D_{kp^n}\log\varphi(e^v)$ is a rational number the denominator of which is prime to p. Consequently, it is congruent modulo p^{n+1} with a rational integer.

First we assume $k<p-1$. The two forms of φ satisfy a relation

$$\varphi_1(\zeta)=\varphi(\zeta)+\psi(\zeta)\cdot g(\zeta)$$

where $\psi(\zeta)$ is an integer in $\Omega(\zeta)$ and

$$g(\zeta)=1+\zeta+\cdots+\zeta^{p-1}.$$

From this follows

(14) $$\varphi_1(e^v)=\varphi(e^v)+\psi(e^v)\cdot g(e^v)$$

and

(15) $$\varphi_1(1)\equiv\varphi(1) \qquad (\operatorname{mod} p).$$

According to Lemma C, we have, putting $\varphi(1)=\varphi_0$,

$$D_{kp^n}\log\varphi(e^v)\equiv\sum_{i=1}^{w}(-1)^{i-1}\cdot\frac{1}{i}\cdot D_{kp^n}\left[\frac{\varphi(e^v)-\varphi_0}{\varphi_0}\right]^i \pmod{p^{n+1}}$$

and, by (14), (15),

$$D_{kp^n}\log\varphi_1(e^v)\equiv\sum_{i=1}^{w}(-1)^{i-1}\cdot\frac{1}{i}\cdot D_{kp^n}\left[\frac{\varphi(e^v)-\varphi_0+\psi(e^v)g(e^v)}{\varphi_0}\right]^i \pmod{p^{n+1}}$$

where w is a suitable natural number (in accordance with Lemma C).

Denoting by $\chi_{ji}(e^v)$ the following polynom of e^v

$$\chi_{ji}(e^v)=[\varphi(e^v)-\varphi_0]^{i-j}\,[\psi(e^v)]^j \qquad (j=1,2,\ldots,i),$$

we get

$$(16)\qquad D_{kp^n}\log\varphi_1(e^v)-D_{kp^n}\log\varphi(e^v)\equiv$$
$$\equiv\sum_{i=1}^{w}\sum_{j=1}^{i}(-1)^{i-1}\cdot\frac{1}{i}\binom{i}{j}D_{kp^n}\chi_{ji}(e^v)\cdot g^j(e^v) \pmod{p^{n+1}}.$$

The terms of the sum in (16) have, by

$$\frac{1}{i}\binom{i}{j}=\frac{1}{j}\binom{i-1}{j-1},$$

the following form

$$(17)\qquad (-1)^{i-1}\cdot\frac{1}{j}\binom{i-1}{j-1}D_{kp^n}\chi_{ji}(e^v)\cdot g^j(e^v).$$

Supposing that j is divisible exactly by the a^{th} power of p, (17) is divisible owing to Lemma F by p^b with

$$b=-a+(n+a+1)=n+1.$$

Hence, all terms on the right-hand side of (16) are divisible by p^{n+1}. Thus we have the proof of Lemma G for $k<p-1$.

Turning to the general case, consider a polynom

$$\xi(e^v)=x_0+x_1e^v+\cdots+x_ue^{uv}$$

of e^v where $x_0,\ldots,x_u$ are rational integers. If j is a non-negative integer, the congruence

$$(18)\qquad D_{kp^n}\xi(e^v)\equiv D_{[k+j(p-1)]p^n}\xi(e^v) \pmod{p^{n+1}}$$

follows easily from the evident relation

$$x_i^{kp^n}\equiv x_i^{[k+j(p-1)]p^n} \pmod{p^{n+1}}.$$

From (18) we infer that (17) is divisible by p^{n+1} also for $k>p-1$, $(p-1)\nmid k$. This completes the proof of Lemma G.

§ 3. Proof of the theorem.

Making use of Lemma G we can prove the validity of the conjecture of KUMMER.

The integer φ of the field $\Omega(\zeta)$ has the form

$$\varphi = d_0 + d_1\zeta + \cdots + d_t\zeta^t$$

where $t, d_0, \ldots, d_t$ are rational integers. If $t \leqq p-2$, φ is given in its normal form and in this case we apply a star to distinguish it from any other form:

$$\varphi^* = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}. \tag{19}$$

Here $a_0, \ldots, a_{p-2}$ denote rational integers.

Another integer φ_1 of $\Omega(\zeta)$ has also a normal form:

$$\varphi_1^* = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} \tag{20}$$

with rational integers $b_0, \ldots, b_{p-2}$. If the congruence (1) is true we have

$$\varphi_1^* - \varphi^* \equiv (b_0 - a_0) + (b_1 - a_1)\zeta + \cdots + (b_{p-2} - a_{p-2})\zeta^{p-2} \equiv 0 \pmod{p^{n+1}}$$

and, by setting $\lambda = 1 - \zeta$, we can write

$$\varphi_1^* - \varphi^* \equiv c_0 + c_1\lambda + c_2\lambda^2 + \cdots + c_{p-2}\lambda^{p-2} \equiv 0 \qquad \pmod{p^{n+1}} \tag{21}$$

where $c_0, \ldots, c_{p-2}$ are rational integers. We show that in (21) $c_0, \ldots, c_{p-2}$ are all divisible by p^{n+1}. In fact, applying (21) as a congruence modulo the principal ideal (λ), we obtain that c_0 is divisible by (λ) and, as c_0 is a rational integer, it is divisible by p. Similarly modulo $(\lambda)^2$ we find that c_1 is divisible by p, and so on, up to c_{p-2}. Now, dividing the integers $c_0, \ldots, c_{p-2}$ by p and regarding (21) as a congruence modulo p^n, we can repeat the applied method and find that the c's are divisible by p^2. This process can be repeated $(n+1)$-times, and finally we obtain

$$c_0 \equiv \cdots \equiv c_{p-2} \equiv 0 \qquad \pmod{p^{n+1}}.$$

Thus we get by

$$a_k - b_k = (-1)^k \sum_{i=k}^{p-2} \binom{i}{k} \cdot c_i \qquad (k = 0, 1, \ldots, p-2),$$

$$a_k \equiv b_k \pmod{p^{n+1}} \qquad (k = 0, 1, \ldots, p-2).$$

Hence we have

$$\varphi_1^*(e^v) = \varphi^*(e^v) + p_{n+1} \cdot h(e^v), \tag{22}$$

where $h(e^v)$ is a polynom of e^v of a degree $\leqq p-2$ with rational integer coefficients.

Taking the first derivative of $[\log \varphi_1^*(e^v) - \log \varphi^*(e^v)]$ with rescept to v, we get by (22)

$$\frac{d \log \varphi_1^*(e^v)}{dv} - \frac{d \log \varphi^*(e^v)}{dv} = \frac{\frac{d\varphi_1^*}{dv}}{\varphi_1^*} - \frac{\frac{d\varphi^*}{dv}}{\varphi^*} = p^{n+1} \frac{\varphi^*(e^v)\frac{dh(e^v)}{dv} - h(e^v)\frac{d\varphi^*(e^v)}{dv}}{\{\varphi^*(e^v)\}^2 + p^{n+1}\varphi^*(e^v)h(e^v)}$$

and, continuing the differentiation, the m^{th} derivative is

$$\text{(23)} \quad \frac{d^m \log \varphi_1^*(e^v)}{dv^m} - \frac{d^m \log \varphi^*(e^v)}{dv^m} = p^{n+1} \frac{H(e^v)}{[\{\varphi^*(e^v)\}^2 + p^{n+1}\varphi^*(e^v)h(e^v)]^m}$$

where $H(e^v)$ is a polynom of e^v with rational integer coefficients. Setting $v=0$ in (23), the denominator on the right-hand side is prime to p, as φ is prime to p. Hence

$$\text{(24)} \qquad D_m \log \varphi_1^*(e^v) \equiv D_m \log \varphi^*(e^v) \pmod{p^{n+1}}$$

for any rational integer $m > 0$. (24) yields, by Lemma G, the proof of the theorem.

Bibliography.

[1] E. Kummer: Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen für den Fall, daß die Klassenzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes. *Abhandlungen d. k. Akad. d. Wiss. Berlin* (1857), pp. 41—74. (See p. 54.)

[2] H. S. Vandiver: On Kummer's memoir of 1857 concerning Fermat's last theorem. *Proceedings Nat. Acad. Sci.,* U. S. A. **6** (1920), pp. 266—269. (See p. 269.)

[3] H. S. Vandiver: On Kummer's memoir of 1857 concerning Fermat's last theorem. *Bull. Amer. Math. Soc.,* **28** (1922), pp. 400—407.

[4] H. S. Vandiver: On power characters of singular integers in a properly irregular cyclotomic field. *Trans. Amer. Math. Soc.,* **32** (1930), pp. 391—408.

[5] H. S. Vandiver: On the composition of the group of ideal classes in a properly irregular cyclotomic field. *Monatshefte f. Math. u. Physik,* **48** (1939), pp. 369—380. (See cit. 12.)

(Received March 1, 1952.)