ON FERMAT'S LAST THEOREM (THIRTEENTH PAPER)

BY

TARO MORISHIMA

1. **Introduction.** In the present paper we shall investigate Case I of Fermat's last theorem.

Kummer(1) showed that if l is an odd prime and $x^l+y^l+z^l=0$ is satisfied in rational integers prime to each other and to l, then

$$B_n\left[\frac{d^{l-2n}\log(x+e^v y)}{dv^{l-2n}}\right]_{v=0} \equiv 0 \pmod{l},$$

where $B_1=1/6$, $B_2=1/30$, and so on, are the numbers of Bernoulli, and $n=1, 2, 3, \cdots, (l-3)/2$. Mirimanoff(2) proved that these criteria may be replaced by

$$B_n f_{l-2n}(t) \equiv 0 \pmod{l}, \qquad n = 1, 2, 3, \cdots, (l-3)/2,$$

where

$$-t = x/y,\ y/x,\ x/z,\ z/x,\ y/z,\ z/y,$$

and

$$f_n(t) = \sum_{r=0}^{l-1} r^{n-1}t^r.$$

He also derived the criteria

$$f_{l-n}(t)f_n(t) \equiv 0 \pmod{l},$$
$$f_{l-1}(t) \equiv 0 \pmod{l}, \qquad n = 2, 3, \cdots, (l-1)/2.$$

The writer(3) extended the above results and proved the following theorems:

THEOREM A(3). *If l is an odd prime and*

$$\alpha^l + \beta^l + \gamma^l = 0 \tag{1}$$

is satisfied in integers α, β, γ belonging to the cyclotomic field $k(\zeta)$ prime to $1-\zeta$, where ζ is a primitive lth root of unity, $\zeta=e^{2\pi i/l}$, then we have

Received by the editors April 27, 1950.

(1) E. Kummer, Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin (1857).

(2) D. Mirimanoff, Journal für die Mathematik vol. 128 (1905) pp. 45–68.

(3) T. Morishima, Jap. J. Math. vol. 11 (1935) pp. 241–252, Theorem 3.

(2) $$b_n f_{l-n}(t) \equiv 0 \pmod{l},$$

for $n=1, 2, 3, \cdots, l-2$ *and*

(3) $$-t \equiv a/b,\ b/a,\ a/c,\ c/a,\ b/c,\ c/b \pmod{l},$$

where $b_0=1$, $b_1=-1/2$, $b_{2n}=(-1)^{n-1}B_n$, $b_{2n+1}=0$, *and* a, b, c *are rational integers and*

$$\alpha \equiv a,\ \beta \equiv b,\ \gamma \equiv c \pmod{1-\zeta}.$$

THEOREM B(4). *If* (1) *is satisfied in integers in* $k(\zeta)$ *prime to* $1-\zeta$, *then we have*

$$f_{l-n}(t)f_n(t) \equiv 0 \pmod{l}$$

for $n=1, 2, \cdots, l-1$, *the other symbols being defined as in Theorem* A.

Theorem B is equivalent to Theorem A, that is, Theorem B follows from (2) and conversely(5).

In the following §§4 and 5 we shall find results which are obtained from the above theorems.

2. **Extension of Vandiver's theorem**(6). Let l be an odd prime and let $\alpha=\alpha(\zeta)$ be an integer or fraction in the cyclotomic field $k(\zeta)$ prime to $1-\zeta$, ζ being a primitive lth root of unity. For brevity set

$$[\log \alpha]^{(n)} = \left[\frac{d^n \log \alpha(e^v)}{dv^n}\right]_{v=0}, \quad [\alpha]^{(n)} = \left[\frac{d^n\alpha(e^v)}{dv^n}\right]_{v=0}.$$

Set also $\beta/\alpha=\delta$, where α, β are integers in $k(\zeta)$ prime to $1-\zeta$, then

(4) $$[\log(\alpha+\zeta^s\beta)]^{(m)} = [\log \alpha]^{(m)} + [\log(1+\zeta^s\delta)]^{(m)}$$

and

$$\begin{aligned}
[\log(1+\zeta^s\delta)]^{(m)} &= \left[\frac{(\zeta^s\delta)'}{1+\zeta^s\delta}\right]^{(m-1)} \\
&= \left[(\zeta^s\delta)'\sum_{r=0}^{l-1}(-1)^r(\zeta^s\delta)^r\right]^{(m-1)} - \left[(\zeta^s\delta)'\frac{(\zeta^s\delta)^l}{1+\zeta^s\delta}\right]^{(m-1)} \\
&\equiv \left[\sum_{r=0}^{l-1}(-1)^r\frac{1}{r+1}((\zeta^s\delta)^{r+1})'\right]^{(m-1)} - \left[\frac{(\zeta^s\delta)'}{1+\zeta^s\delta}\right]^{(m-1)}\delta_0^l \\
&\equiv \sum_{r=0}^{l-1}(-1)^r\frac{1}{r+1}\left[(\zeta^s\delta)^{r+1}\right]^{(m)} - [\log(1+\zeta^s\delta)]^{(m)}\delta_0^l
\end{aligned}$$

$$\pmod{l},$$

(4) T. Morishima, loc. cit. p. 252. For $k=1$, Theorem 7 reduces to Theorem B.

(5) D. Mirimanoff, loc. cit.

(6) H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A. vol. 11 (1925) pp. 292–298.

where $s=1, 2, \cdots, l-1$; $2 \leqq m \leqq l-2$;

$$((\zeta^s\delta)^{r+1})' = \frac{d(e^{sv}\delta(e^v))^{r+1}}{dv} \qquad (r = 0, 1, 2, \cdots, l-1),$$

$$\delta_0 = [\delta(e^v)]_{v=0} = \delta(1),$$

and $\alpha+\beta$ is prime to $1-\zeta$. Hence

$$\text{(5)} \qquad \begin{aligned} [\log(1+\zeta^s\delta)]^{(m)} &\equiv \frac{1}{1+\delta_0}\sum_{r=0}^{l-1}(-1)^r\frac{1}{r+1}[(\zeta^s\delta)^{r+1}]^{(m)} \\ &\equiv \frac{1}{1+\delta_0}\sum_{r=0}^{l-1}\frac{(-1)^r}{r+1}\sum_{n=0}^{m}C_{m,n}[\zeta^{(r+1)s}]^{(m-n)}[\delta^{r+1}]^{(n)} \\ &\equiv \sum_{n=0}^{m}a_{m,n}s^{m-n} \pmod{l}, \end{aligned}$$

where

$$a_{m,n} = \frac{1}{1+\delta_0}C_{m,n}\sum_{r=0}^{l-1}(-1)^r(r+1)^{m-n-1}[\delta^{r+1}]^{(n)} \qquad (n = 1, 2, \cdots, m)$$

and

$$\text{(6)} \qquad \begin{aligned} a_{m,0} &= \frac{-1}{1+\delta_0}\sum_{r=1}^{l}r^{m-1}(-\delta_0)^r \\ &\equiv \frac{-1}{1+\delta_0}f_m(-\delta_0) \pmod{l}. \end{aligned}$$

Now, using (4) and (5), we have

$$\begin{aligned} [\log\{(\alpha+\zeta^s\beta)(\alpha+\zeta\beta)^{l-1}\}]^{(m)} &\equiv [\log(\alpha+\zeta^s\beta)]^{(m)} - [\log(\alpha+\zeta\beta)]^{(m)} \\ &\equiv [\log(1+\zeta^s\delta)]^{(m)} - [\log(1+\zeta\delta)]^{(m)} \\ &\equiv \sum_{n=0}^{m}(s^{m-n}-1)a_{m,n} \pmod{l}, \end{aligned}$$

whence, if

$$\text{(7)} \qquad [\log\{(\alpha+\zeta^s\beta)(\alpha+\zeta\beta)^{l-1}\}]^{(m)} \equiv 0 \pmod{l}$$

for $s=2, 3, \cdots, l-1$, then

$$\sum_{n=0}^{m-1}(s^{m-n}-1)a_{m,n} \equiv 0 \pmod{l} \qquad (s = 2, 3, \cdots, l-1),$$

where $2 \leqq m \leqq l-2$. Hence we obtain

$$\text{(8)} \qquad a_{m,n} \equiv 0 \pmod{l}$$

for $n=0, 1, \cdots, m-1$, since the determinant

$$\begin{vmatrix} 2-1 & 2^2-1 & \cdots & 2^m-1 \\ 3-1 & 3^2-1 & \cdots & 3^m-1 \\ \cdot\cdot\cdot & \cdot\cdot\cdot & \cdot\cdot\cdot & \cdot\cdot\cdot \\ (m+1)-1 & (m+1)^2-1 & \cdots & (m+1)^m-1 \end{vmatrix} \not\equiv 0 \pmod{l}.$$

From (6), (7), and (8) we have the following lemma:

LEMMA 1. *If l is an odd prime and, for $s=2, \cdots, l-1$, (7) is possible in integers α, β in $k(\zeta)$ prime to $1-\zeta$, then we have*

$$f_m(-\delta_0) \equiv 0 \pmod{l},$$

where

$$\delta_0 = \frac{\beta(1)}{\alpha(1)},$$

$$\alpha \equiv \alpha(1), \qquad \beta \equiv \beta(1) \pmod{1-\zeta},$$

$$1+\delta_0 \equiv \frac{\alpha+\beta}{\alpha} \not\equiv 0 \pmod{1-\zeta},$$

and $\alpha(1)$, $\beta(1)$ are rational integers.

We now consider the relation

$$\alpha^l + \beta^l + \gamma^l = 0,$$

where l is an odd prime and α, β, γ are integers in $k(\zeta)$ prime to $1-\zeta$. From this relation we obtain

$$\prod_{s=0}^{l-1} (\alpha + \zeta^s\beta) = -\gamma^l,$$

which gives

$$(\alpha + \zeta^s\beta) = \mathfrak{d}\mathfrak{a}_s^l \qquad (s = 0, 1, 2, \cdots, l-1),$$

where $\mathfrak{d}$ is the greatest common ideal divisor of α, β and $\mathfrak{a}_0, \mathfrak{a}_1, \cdots, \mathfrak{a}_{l-1}$ are ideals in $k(\zeta)$. Hence we have

$$(9) \qquad (\alpha + \zeta^s\beta)(\alpha + \zeta\beta)^{l-1} = \mathfrak{d}^l\mathfrak{a}_s^l\mathfrak{a}_1^{l(l-1)} \qquad (s = 1, 2, \cdots, l-1).$$

We now employ the law of reciprocity(7) between two integers ω_s^{l-1}, θ_r^{l-1} in $k(\zeta)$, where

(7) H. Hasse, Jber. Deutschen Math. Verein. vol. 6 (1930) p. 110.

$$\omega_s = (\alpha + \zeta^s\beta)(\alpha + \zeta\beta)^{l-1}, \quad \theta_r = \theta(\zeta^r), \tag{10}$$

and the principal ideal (θ_r) is the lth power of an ideal in $k(\zeta)$ which is prime to ω_s and $1-\zeta$. Then we may write, using (9),

$$1 = \left(\frac{\omega_s}{\theta_r}\right)\left(\frac{\theta_r}{\omega_s}\right)^{l-1} = \zeta^L,$$

where

$$L = \sum_{n=2}^{l-2} (-1)^n [\log \omega_s^{l-1}]^{(n)} [\log \{\theta(\zeta^r)\}^{l-1}]^{(l-n)}.$$

Hence we have

$$L \equiv \sum_{n=2}^{l-2} (-1)^n r^{l-n} [\log \omega_s]^{(n)} [\log \theta(\zeta)]^{(l-n)} \equiv 0 \pmod{l}$$

for $r=1, 2, \cdots, l-3$, $s=1, 2, \cdots, l-1$, whence

$$[\log \omega_s]^{(n)} [\log \theta(\zeta)]^{(l-n)} \equiv 0 \pmod{l} \tag{11}$$
$$(n = 2, 3, \cdots, l-2;\ s = 1, 2, \cdots, l-1),$$

since the determinant $|r^{l-n}|$ is prime to l. Now, if

$$[\log \theta(\zeta)]^{(l-n)} \equiv 0 \pmod{l},$$

then we take

$$f_n(t) [\log \theta(\zeta)]^{(l-n)} \equiv 0 \pmod{l} \tag{12}$$

instead of

$$[\log \omega_s]^{(n)} [\log \theta(\zeta)]^{(l-n)} \equiv 0 \pmod{l},$$

where

$$t = -b/a,$$
$$\alpha \equiv a, \qquad \beta \equiv b \pmod{1-\zeta}$$

and a, b are rational integers. If

$$[\log \theta(\zeta)]^{(l-n)} \not\equiv 0 \pmod{l},$$

then we obtain from (11)

$$[\log \omega_s]^{(n)} \equiv 0 \pmod{l} \qquad (s = 1, 2, \cdots, l-1)$$

which gives, using Lemma 1 and (10),

$$f_n(t) \equiv 0 \pmod{l},$$

whence

$$f_n(t)[\log \theta(\zeta)]^{(l-n)} \equiv 0 \pmod{l}, \tag{13}$$

where

$$t = -b/a,$$

$$\alpha \equiv a, \qquad \beta \equiv b \pmod{1-\zeta}$$

and a, b are rational integers.

In the same way (12) and (13) are satisfied by

$$-t = a/b,\ a/c,\ c/a,\ b/c,\ c/b,$$

where

$$\alpha \equiv a, \qquad \beta \equiv b, \qquad \gamma \equiv c \pmod{1-\zeta}$$

and a, b, c are rational integers.

From the relation

$$\alpha^l + \beta^l + \gamma^l = 0$$

we also obtain

$$a^l + b^l + c^l \equiv 0 \pmod{(1-\zeta)^l},$$

whence

$$a^l + b^l + c^l \equiv 0 \pmod{l^2},$$

$$a + b + c \equiv 0 \pmod{l}.$$

Hence

$$(a+b)^l \equiv -c^l \equiv a^l + b^l \pmod{l^2}$$

which gives

$$(1-t)^l \equiv 1 - t^l \pmod{l^2},$$

where $-t=a/b,\ b/a$. From this relation we have easily

$$\sum_{r=1}^{l-1} r^{l-2} t^r \equiv 0 \pmod{l}. \tag{14}$$

In the same way (14) is satisfied by $-t=a/c,\ c/a,\ b/c,\ c/b$.

Hence from (12), (13), and (14) we have

THEOREM 1. *If l is an odd prime and*

$$\alpha^l + \beta^l + \gamma^l = 0$$

is satisfied in integers α, β, γ in the cyclotomic field $k(\zeta)$ prime to $1-\zeta$ and $\theta(\zeta^r)$ is an integer which is the lth power of an ideal in $k(\zeta)$ prime to α, β, γ, *and* $1-\zeta$, *where* $r=1, 2, \cdots, l-3$, *then we have*

$$f_n(t)\left[\log \theta(\zeta)\right]^{(l-n)} \equiv 0 \pmod{l} \qquad (n = 2, 3, \cdots, l-1)$$

for $-t=a/b, b/a, a/c, c/a, b/c, c/b$, *where*

$$f_n(t) = \sum_{r=0}^{l-1} r^{n-1}t^r,$$

$$\left[\log \theta(\zeta)\right]^{(m)} = \left[\frac{d^m \log \theta(e^v)}{dv^m}\right]_{v=0},$$

$$\alpha \equiv a, \qquad \beta \equiv b, \qquad \gamma \equiv c \pmod{1-\zeta}$$

and a, b, c *are rational integers.*

The above demonstration of Theorem 1 is analogous to that of Theorem A, and also, using the above method, we can obtain Theorem A by taking the unit

$$\left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2}$$

instead of $\theta(\zeta)$, where r is a primitive root of l. In particular, if α, β, γ are rational integers x, y, z respectively, Theorem 1 gives Vandiver's theorem(8).

3. **Irregular ideal classes in the cyclotomic field.** Let l be an odd prime and let the number of ideal classes in the cyclotomic field $k(\zeta)$ be $h=l^r q$ with $(l, q)=1$.

Consider the group of classes of all the ideals in the field of the form $\mathfrak{a}^q$ where $\mathfrak{a}$ is an ideal in $k(\zeta)$. This gives a group of order l^r and is called the irregular class group of $k(\zeta)$.

Pollaczek(9) gave the following results:

LEMMA 2(9). *There exists in* $k(\zeta)$ *a system of fundamental units* η_i *which have the property*

$$\eta_i^{s-r^{2i}} = \xi_i^l, \qquad i = 1, 2, \cdots, (l-3)/2,$$

where ξ_i *is a unit in* $k(\zeta)$ *and* s *stands for the substitution* $(\zeta:\zeta^r)$, r *being a primitive root of* l.

LEMMA 3(10). *In* $k(\zeta)$ *we may select a basis, which we shall call a normal basis, for the irregular class group*

$$C_1, C_2, \cdots, C_t$$

such that

(8) H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A. vol. 11 (1925) pp. 292–298.
(9) F. Pollaczek, Math. Zeit. vol. 21 (1924).
(10) F. Pollaczek, loc. cit.; T. Morishima, Jap. J. Math. vol. 10 (1933) p. 105.

$$C_i^{s-c_i} = 1, \qquad i = 1, 2, \cdots, t,$$

where the c's are positive rational integers, s being the substitution $(\zeta:\zeta^r)$.

We now designate by

$$(15) \qquad Q_1, Q_2, \cdots$$

the C's mentioned in Lemma 3 such that the corresponding c's are quadratic residues, modulo l, and by

$$(16) \qquad N_1, N_2, \cdots$$

the C's mentioned in Lemma 3 in which the c's are quadratic nonresidues. We also designate by

$$\mathfrak{p}_1, \mathfrak{p}_2, \cdots$$

the ideals of classes N in (16) such that

$$\mathfrak{p}_i^{l^{m_i}} = (\rho_i), \qquad \rho_i^{s-c_i} = \omega_i^{l^{m_i}}, \qquad i = 1, 2, \cdots,$$

where $c_i = r^{(2i+1)l^{m_i-1}}$, l^{m_i} is the order of $\mathfrak{p}_i$ and ρ_i, ω_i are integers in $k(\zeta)$, and by

$$\mathfrak{q}_1, \mathfrak{q}_2, \cdots$$

the ideals of classes Q in (15) such that

$$\mathfrak{q}_i^{l^{n_i}} = (\tilde{\rho}_i), \qquad \tilde{\rho}_i^{s-\tilde{c}_i} = \tilde{\omega}_i^{l^{n_i}}, \qquad i = 1, 2, \cdots,$$

where $\tilde{c}_i = r^{(l-1-2i)l^{n_i-1}}$, l^{n_i} is the order of $\mathfrak{q}_i$, and $\tilde{\rho}_i$, $\tilde{\omega}_i$ are integers in $k(\zeta)$. The integer ρ_i satisfying the above conditions we shall call *the integer defined by the ideal* $\mathfrak{p}_i$.

With this notation we have the following lemma.

LEMMA 4(11). *If among the elements of a normal basis of the irregular class group of* $k(\zeta)$ *there exists for a certain quadratic non-residue j exactly* z_j *classes*

$$(17) \qquad N_{u_1}, N_{u_2}, \cdots$$

such that

$$N_{u_i}^{s-b_{u_i}} = 1$$

and $b_{u_i} \equiv j \pmod{l}$, *then there are in the same class group* z_j or $z_j - 1$ *basis classes*

$$Q_{v_1}, Q_{v_2}, \cdots$$

where

$$Q_{v_i}^{s-a_{v_i}} = 1$$

(11) F. Pollaczek, loc. cit.; T. Morishima, Jap. J. Math. vol. 10 (1933); T. Morishima, Jap. J. Math. vol. 11 (1935) p. 238.

and $a_{v_i} \equiv r/j \pmod{l}$, *r being a primitive root of l. In particular, if the second case holds, among the integers* ρ_i *defined by the ideals* $\mathfrak{p}_i$ *of the classes N in* (17) *there exists one and only one integer which is not primary and conversely; and also in this case the unit* η_i, *where* $i=(1/2)\mathrm{ind}(r/j)$, *is a singular primary unit having the property stated in Lemma* 2.

Now by a result in a previous paper of the writer's we have the following lemma.

LEMMA 5([12]). *If l is an odd prime and* (1) *is satisfied in integers in* $k(\zeta)$ *prime to* $1-\zeta$, *then it is impossible that for all values*

$$-t = a/b,\ b/a,\ a/c,\ c/a,\ b/c,\ c/b,$$

$$f_n(t) \equiv 0 \pmod{l},$$

where $n=3, 5, 7, 9, 11, 13$, *the other symbols being defined as in Theorem* 1.

From Lemma 1 and Lemma 5 we obtain the following lemma.

LEMMA 6. *If l is an odd prime and* (1) *is possible in integers in* $k(\zeta)$ *prime to* $1-\zeta$, *then, for at least one of* $m=2, 3, \cdots, l-1$, *at least one of* $[\log\{(\alpha+\zeta^m\beta)(\alpha+\zeta\beta)^{l-1}\}]^{(n)}$, $[\log\{(\beta+\zeta^m\gamma)(\beta+\zeta\gamma)^{l-1}\}]^{(n)}$, $[\log\{(\gamma+\zeta^m\alpha)\cdot(\gamma+\zeta\alpha)^{l-1}\}]^{(n)}$, *say* $[\log\{(\alpha+\zeta^m\beta)(\alpha+\zeta\beta)^{l-1}\}]^{(n)}$, *is not divisible by l, where* $n=3, 5, 7, 9, 11, 13$.

Now for $n=3, 5, 7, 9, 11, 13$ if in $k(\zeta)$ none of ideal classes N in (16) is such that

$$N_n^{s-c_n} = 1, \qquad c_n \equiv r^n \pmod{l},$$

or if all integers ρ_i defined by the ideals $\mathfrak{p}_i$ of the classes N in (16) are primary, then we have

$$\{(\alpha+\zeta^m\beta)(\alpha+\zeta\beta)^{l-1}\}^{qf(s)} = \theta\omega^l,$$

where q is the factor of the class number h of $k(\zeta)$ such that $h=l^\tau q$, $(l, q)=1$, θ is a primary number or 1, ω is an integer in $k(\zeta)$ and $f(s)$ is the symbolic power

$$(18) \qquad (s-r)(s-r^2)(s-r^3)\cdots(s-r^{l-2})/(s-r^n),$$

s standing for the substitution $(\zeta:\zeta^r)$, r being a primitive root of l. From this we obtain

$$f(r^n)[\log\{(\alpha+\zeta^m\beta)(\alpha+\zeta\beta)^{l-1}\}]^{(n)} \equiv 0 \pmod{l},$$

whence, using (18), we have

$$[\log\{(\alpha+\zeta^m\beta)(\alpha+\zeta\beta)^{l-1}\}]^{(n)} \equiv 0 \pmod{l}$$

which is contrary to Lemma 6.

([12]) T. Morishima, Jap. J. Math. vol. 11 (1935) p. 246.

From this result and Lemma 4 we have the following theorem.

THEOREM 2. *If l is an odd prime and*

$$\alpha^l + \beta^l + \gamma^l = 0$$

is satisfied in integers α, β, γ in $k(\zeta)$ prime to $1-\zeta$, then for each $n=3, 5, 7, 9, 11, 13$ there exists at least one class N_n in $k(\zeta)$ such that

$$N_n^{s-c_n} = 1, \qquad c_n \equiv r^n \pmod{l}, \tag{19}$$

and in each case $n=3, 5, 7, 9, 11, 13$ one and only one of the integers ρ_n defined by the ideals $\mathfrak{p}_n$ of the classes N_n in (19) is not primary and the unit η_i is primary, where $i=(l-n)/2$ and η_i is the unit having the property stated in Lemma 4, the other symbols being defined as above.

Now if (1) is satisfied in integers in $k(\zeta)$ prime to $1-\zeta$ and for all of $n=l-2, l-4, \cdots, l-2[(l-1)/4]$

$$f_n(t) \equiv 0 \pmod{l},$$

where $[(l-1)/4]$ is the greatest integer in $(l-1)/4$, the other symbols being defined as in Theorem A, then we have

$$f_{l-2n}(t)f_{2n+1}(t) \equiv 0 \pmod{l}$$

for $n=1, 2, \cdots, (l-3)/2$. We also have easily

$$f_l(t) = \sum_{r=0}^{l-1} r^{l-1}t^r = \sum_{r=1}^{l-1} t^r \equiv 0 \pmod{l}.$$

Hence we obtain

$$\sum_{n=1}^{(l-3)/2} f_{l-2n}(t)f_{2n+1}(t) + 2f_l(t)\sum_{r=1}^{l-1} t^r \equiv \sum_{n=0}^{(l-1)/2} \sum_{s=1}^{l-1}\sum_{r=1}^{l-1} r^{l-2n-1}s^{2n}t^rt^s \equiv 0 \pmod{l},$$

whence

$$\sum_{r,s} \frac{r^{l+1} - s^{l+1}}{r^2 - s^2} t^rt^s + \frac{l+1}{2}\sum_{r=1}^{l-1} r^{l-1}t^{2r} + \frac{l+1}{2}\sum_{r=1}^{l-1} r^{l-1}t^l \equiv 0 \pmod{l},$$

where $\sum_{r,s}$ indicates summation over all the values $r=1, 2, \cdots, l-1$, $s=1, 2, \cdots, l-1$ except the values which satisfy

$$r^2 \equiv s^2 \pmod{l}.$$

From this relation we obtain

$$\sum_{r=1}^{l-1}\sum_{s=1}^{l-1} t^rt^s + \frac{l-1}{2}\sum_{r=1}^{l-1} t^{2r} + \frac{l-1}{2}(l-1)t \equiv 0 \pmod{l};$$

if $t\equiv -1 \pmod{l}$, we can take $t\equiv 2 \pmod{l}$ instead of $t\equiv -1 \pmod{l}$ since $a+b+c\equiv 0 \pmod{l}$, whence for $l>3$

$$t \equiv 0 \pmod{l},$$

which is contrary to the assumption. Hence we have the following:

THEOREM 3. *If $l>3$ is prime and* (1) *is satisfied in integers in $k(\zeta)$ prime to $1-\zeta$, then for at least one of $n=l-2, l-4, \cdots, l-2[(l-1)/4]$*

$$f_n(t) \not\equiv 0 \pmod{l},$$

where the symbols are defined as in Theorem A *and $t\not\equiv -1 \pmod{l}$.*

From Lemma 1 and Theorem 3 we obtain

$$[\log \{(\alpha + \zeta^m\beta)(\alpha + \zeta\beta)^{l-1}\}]^{(n)} \not\equiv 0 \pmod{l} \tag{20}$$

for at least one of $n=l-2, l-4, \cdots, l-2[(l-1)/4]$, where m is one of 2, 3, $\cdots$, $l-1$.

Hence by a demonstration which is analogous to that of Theorem 2 we have, using (20), the following theorem.

THEOREM 4. *If $l>3$ is a prime and* (1) *is possible in integers in $k(\zeta)$ prime to $1-\zeta$, then for at least one of $n=l-2, l-4, \cdots, l-2[(l-1)/4]$ there exists a class N_n in $k(\zeta)$ such that*

$$N_n^{s-c_n} = 1, \qquad c_n \equiv r^n \pmod{l}$$

and the integer ρ_n defined by the ideal $\mathfrak{p}_n$ of N_n is not primary, and the unit $\eta_{(l-n)/2}$ is primary, where the symbols are defined as in Theorem 2.

Now by Theorem 2 and Theorem 4 for at least seven values of n the integer ρ_n defined by the ideal $\mathfrak{p}_n$ of the class N_n in (16) is not primary, since we may assume[13] that $l-2[(l-1)/4]>13$, that is, $l>23$. Hence, if among the elements of a normal basis of the irregular class group of $k(\zeta)$ there exist e_1 classes N defined as in (16) and e_2 classes Q defined as in (15), then by Lemma 4

$$e_1 - e_2 \geqq 7,$$

whence we have the following theorem.

THEOREM 5. *Let the elements of a normal basis of the irregular class group of the cyclotomic field $k(\zeta)$ be*

$$N_1, N_2, \cdots, N_{e_1},$$
$$Q_1, Q_2, \cdots, Q_{e_2},$$

where the N's are defined as in (16) *and the Q's are defined as in* (15). *If e_1-e_2*

[13] T. Morishima, Jap. J. Math. vol. 11 (1935) p. 246, Theorem 4.

<7, *then*

$$\alpha^l + \beta^l + \gamma^l = 0$$

is impossible in integers α, β, γ *in* $k(\zeta)$ *prime to* $1-\zeta$, l *being an odd prime.*

4. **Bernoulli numbers.** Assume that the B's are the Bernoulli numbers ($B_1=1/6$, $B_2=1/30$, etc.), and l is an odd prime and none of the first half in the set $B_1, B_2, \cdots, B_{(l-3)/2}$ is divisible by l, that is,

$$B_1 \not\equiv 0,\ B_2 \not\equiv 0,\ \cdots,\ B_s \not\equiv 0 \pmod{l}, \tag{21}$$

where $s=[(l-1)/4]$. If (1) is satisfied in integers belonging to the cyclotomic field $k(\zeta)$ prime to $1-\zeta$, then we obtain from (2) and (21)

$$f_{l-2}(t) \equiv 0,\ f_{l-4}(t) \equiv 0,\ \cdots,\ f_{l-2s}(t) \equiv 0 \pmod{l},$$

where $s=[(l-1)/4]$. This is contrary to Theorem 3. Hence we have the following theorem.

THEOREM 6. *If* l *is an odd prime and none of the first half in the set of the Bernoulli numbers* $B_1, B_2, \cdots, B_{(l-3)/2}$ *is divisible by* l, *that is,*

$$B_1 \not\equiv 0,\ B_2 \not\equiv 0,\ \cdots,\ B_s \not\equiv 0 \pmod{l},$$

where $s=[(l-1)/4]$, *then*

$$\alpha^l + \beta^l + \gamma^l = 0$$

is never satisfied in integers α, β, γ *belonging to the cyclotomic field* $k(\zeta)$ *prime to* $1-\zeta$, *where* ζ *is a primitive* l*th root of unity.*

From this theorem we easily obtain the following:

THEOREM 6′. *If* l *is an odd prime and the equation*

$$\alpha^l + \beta^l + \gamma^l = 0$$

is satisfied by integers in $k(\zeta)$ *prime to* $1-\zeta$, *then at least one of the Bernoulli numbers in the set*

$$B_1, B_2, \cdots, B_s$$

is divisible by l, *where* s *is* $(l-1)/4$ *or* $(l-3)/4$ *according as* $l\equiv 1 \pmod 4$ *or* $l\equiv 3 \pmod 4$, *the other symbols being defined as in Theorem* 6.

Now by a result in a previous paper of the writer's we have the following lemma.

LEMMA 7([14]). *If the equation* (1) *is solvable for* α, β, γ *integers in the cyclotomic field* $k(\zeta)$ *prime to* $1-\zeta$, *then*

([14]) T. Morishima, Jap. J. Math. vol. 11 (1935) p. 246.

$$B_{(l-2n-1)/2} \equiv 0 \pmod{l}$$

for $n=1, 2, 3, 4, 5, 6$, *where the symbols are defined as in Theorem* 6.

Hence from Theorem 6′ and Lemma 7 we obtain, since we may assume[14] that $l>23$, the following theorem.

THEOREM 7. *If the equation* (1) *is solvable for* α, β, γ *integers in the cyclotomic field* $k(\zeta)$ *prime to* $1-\zeta$, *then at least seven of the Bernoulli numbers in the set*

$$B_1, B_2, \cdots, B_{(l-3)/2}$$

are divisible by l.

5. **The first factor of the cyclotomic class number.** Let h be the class number of the cyclotomic field $k(\zeta)$ defined by a primitive lth root of unity, l being an odd prime.

It is known that $h=h_1h_2$ where h_1 is called the first factor of the class number and h_2 is called the second factor of the class number and the latter is equal to the class number of the real subfield $k(\zeta+\zeta^{-1})$ of $k(\zeta)$ of degree $(l-1)/2$.

In a previous paper[15] the writer proved that if the equation $\alpha^l+\beta^l+\gamma^l=0$ is satisfied in integers α, β, γ belonging to the real subfield $k(\zeta+\zeta^{-1})$ of $k(\zeta)$ prime to $1-\zeta$, where l is an odd prime, then the first factor h_1 of the class number of $k(\zeta)$ is divisible by l^{12}. In the present section we shall extend this result and prove that if (1) is possible in integers in the field $k(\zeta+\zeta^{-1})$ prime to $1-\zeta$, then

$$h_1 \equiv 0 \pmod{l^{13}}.$$

Now from a result in a previous paper of the writer's we obtain the following theorem.

THEOREM C[16]. *If* l *is an odd prime and the equation* (1) *is satisfied in integers* α, β, γ *belonging to the field* $k(\zeta+\zeta^{-1})$ *prime to* $1-\zeta$, *then*

$$E_m = \eta_m^{\,l}$$

$$(m = (l-3)/2, (l-5)/2, (l-7)/2, (l-9)/2, (l-11)/2, (l-13)/2)$$

and

$$B_i \equiv 0 \pmod{l^2},$$

$$i = \frac{(l-2n)l^\tau + 1}{2}, \qquad \tau \geqq 1; n = 2, 3, 4, 5, 6, 7,$$

where

(15) T. Morishima, Jap. J. Math. vol. 11 (1935) p. 251, Theorem 6.
(16) T. Morishima, Jap. J. Math. vol. 11 (1935) p. 251, Theorem 5.

$$E_m = \epsilon^{f(s)} \text{ (symbolic power)},$$

$$\epsilon = \left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2},$$

$$f(s) = \sum_{i=0}^{(l-3)/2} r^{l-2im-1} s^i,$$

r is a primitive root of l and s is the substitution $(\zeta:\zeta^r)$.

By Vandiver's result[17] we also have

$$\frac{n^r - 1}{l} \sum_{a=1}^{l-1} a^r = \sum_{a=1}^{l-1} \sum_{s=1}^{r} a^r C_{r,s} \left(\frac{d_a}{a}\right)^s l^{s-1}, \tag{22}$$

where

$$d_a \equiv - a/l \pmod{n},$$

$$0 \leqq d_a < n, \ (n, l) = 1,$$

whence for $r = (l-2m)l^c + 1$, $c > 0$,

$$\frac{n^r - 1}{l} \sum_{a=1}^{l-1} a^r \equiv r \sum_{a=1}^{l-1} d_a a^{r-1} \pmod{l^2}.$$

On the other hand it is known that

$$\frac{1}{l} \sum_{a=1}^{l-1} a^r \equiv b_r \pmod{l^2}, \tag{23}$$

where $b_1 = -1/2$, $b_{2r} = (-1)^{r-1} B_r$ (Bernoulli numbers), $b_{2r+1} = 0$, and $l > 3$. Hence

$$\frac{n^r - 1}{r} b_r \equiv \sum_{a=1}^{l-1} d_a a^{r-1} \pmod{l^2}.$$

For $c = 1$ and 13, this yields

$$\begin{aligned} \frac{n^{(l-2m)l+1} - 1}{(l-2m)l+1} b_{(l-2m)l+1} &\equiv \sum_{a=1}^{l-1} d_a a^{(l-2m)l} \pmod{l^2}, \\ \frac{n^{(l-2m)l^{13}+1} - 1}{(l-2m)l^{13}+1} b_{(l-2m)l^{13}+1} &\equiv \sum_{a=1}^{l-1} d_a a^{(l-2m)l^{13}} \pmod{l^2}, \end{aligned} \tag{24}$$

whence

$$\frac{n^{(l-2m)l+1} - 1}{(l-2m)l+1} b_{(l-2m)l+1} \equiv \frac{n^{(l-2m)l^{13}+1} - 1}{(l-2m)l^{13}+1} b_{(l-2m)l^{13}+1} \pmod{l^2}.$$

---

(17) H. S. Vandiver, Ann. of Math. (2) vol. 18, p. 112, (7a).

From this relation and Theorem C we have for $m=2, 3, 4, 5, 6, 7$

$$b_{(l-2m)l^{13}+1} \equiv 0 \pmod{l^2}. \tag{25}$$

We also have from (22) and (23)

$$\frac{n^{l-2m+1}-1}{l-2m+1} b_{l-2m+1} \equiv \sum_{a=1}^{l-1} d_a a^{l-2m} \pmod{l}.$$

From this relation and (24) we obtain

$$\frac{n^{l-2m+1}-1}{l-2m+1} b_{l-2m+1} \equiv \frac{n^{(l-2m)l^{13}+1}-1}{(l-2m)l^{13}+1} b_{(l-2m)l^{13}+1} \pmod{l},$$

which gives, using Theorem 6′,

$$b_{(l-2m)l^{13}+1} \equiv 0 \pmod{l}, \tag{26}$$

where $2 \leqq l-2m+1 \leqq 2[(l-1)/4]$, $[(l-1)/4]$ being the greatest integer in $(l-1)/4$.

From Vandiver's result[18] concerning the first factor h_1 of the class number of $k(\zeta)$ we also have

$$h_1 \equiv \frac{l \prod_s b_{sl^{13}+1}}{2^{(l-3)/2}} \pmod{l^{13}}, \tag{27}$$

where $s=1, 3, \cdots, l-2$.

Hence we obtain from (25), (26), and (27)

$$h_1 \equiv 0 \pmod{l^{13}},$$

whence we have the following theorem.

THEOREM 8. *If l is an odd prime and*

$$\alpha^l + \beta^l + \gamma^l = 0$$

is possible in integers α, β, γ in the real subfield $k(\zeta+\zeta^{-1})$ of $k(\zeta)$ prime to $1-\zeta$, then the first factor of the class number of $k(\zeta)$ is divisible by l^{13}.

TOKYO COLLEGE OF SCIENCE,
TOKYO, JAPAN.

(18) H. S. Vandiver, Bull. Amer. Math. Soc. vol. 25 (1918) p. 460, (8).