if $D > D_1(\varepsilon)$. It follows from Burgess's inequality [1] that if $D > D_2(\varepsilon)$, then

$$\Big|\sum_{n=N+1}^{N+H}\chi(n)\Big| \leqslant \frac{1}{4}\varepsilon H$$

for $H > D^{(1+\varepsilon)/4}$. Thus, by partial summation, we get

$$\sum_{n>D^{(1+\varepsilon)/4}}\frac{\chi(n)}{n} = \sum_{D^{(1+\varepsilon)/4}<n\leqslant D}\frac{\chi(n)}{n}+\sum_{D<n}\frac{\chi(n)}{n} \leqslant \frac{1}{4}\varepsilon\log D+1. \tag{4}$$

Taking

$$D_0(\varepsilon) = \max\{D_1(\varepsilon), D_2(\varepsilon)\},$$

our assertion follows immediately from (3) and (4).

References

[1] D. A. Burgess, *On character sums and L-series II*, Proc. London Math. Soc. 13 (1963), 524–536.

[2] — *Estimating* $L_\chi(1)$, Norske Vid. Selsk. Forh. (Trondheim) 39 (1966), 101–108.

[3] S. Chowla, *Bounds for the fundamental unit of a real quadratic field*, ibid. 37 (1964), 85–87.

[4] J. Pintz, *Elementary methods in the theory of L-functions VII. Upper bound for* $L(1, \chi)$, Acta Arith. 32 (1977), 397–406.

[5] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachrichten, 1918, 21–29.

[6] P. J. Stephens, *Optimizing the size of* $L(1, \chi)$, Proc. London Math. Soc. 24 (1972), 1–14.

DEPARTMENT OF MATHEMATICS
TOYO UNIVERSITY
Kawagoe-Shi, Saitama 350
Japan

Received on 6.9.1988
and in revised form on 10.11.1988 (1865)

ACTA ARITHMETICA
LV (1990)

On the Kummer–Mirimanoff congruences

by

TAKASHI AGOH (Chiba)

1. Introduction. Let p be an odd prime, $\boldsymbol{Z}$ the ring of integers, $\boldsymbol{Z}_p$ the ring of all rational numbers which are p-integral, B_m the mth Bernoulli number defined by

$$v/(e^v-1) = \sum_{k=0}^{\infty}(B_k/k!)v^k$$

and $\varphi_n(v)$ the Mirimanoff polynomial, i.e.,

$$\varphi_n(v) = \sum_{i=1}^{p-1} i^{n-1}v^i \qquad (n\in\boldsymbol{Z}).$$

We denote by $[f(v)]_0^{(m)}$ the value of $d^m\{f(v)\}/dv^m$ at $v=0$ for the m-times differentiable function $f(v)$ of v.

In 1857 Kummer [7] showed that if ν and ϱ are units in $\boldsymbol{Z}_p$ such that $\nu^p+\varrho^p-1=0$, then the following congruences hold for $t=\nu, \varrho$:

$$(K_0) \qquad [U_t(v)]_0^{(p-2)} \equiv 0 \pmod p,$$

$$(K_m) \qquad B_{2m}[U_t(v)]_0^{(p-1-2m)} \equiv 0 \pmod p, \quad m = 1, 2, \ldots, g,$$

where $U_t(v) = 1/(1-te^v)$ and $g=(p-3)/2$.

In [5] Hasse gives the proof of this result by using the reciprocity law for the power residue symbol (see also the proof of Inkeri [6]).

Here we should note that $[U_t(v)]_0^{(i)}$ may be replaced by $\varphi_{i+1}(t)$ if $i\geqslant 1$ and $t\not\equiv 0, 1 \pmod p$ (see Lemma 4 in § 2). Thus, in the above congruences we shall treat $[U_t(v)]_0^{(i)}$ and $\varphi_{i+1}(t)$ without distinction.

On the other hand, Mirimanoff [10] made the full observation for the above result and proved that the congruences (K_m), $m=0, 1, \ldots, g$, hold for $t=t'$ with $t'\not\equiv 0, 1 \pmod p$ if and only if the following congruences hold for $t=t'$:

$$(M_0) \qquad \varphi_{p-1}(t) \equiv 0 \pmod p,$$

$$(M_m) \qquad \varphi_{m+1}(t)\,\varphi_{p-1-m}(t) \equiv 0 \pmod p, \quad m = 1, 2, \ldots, g.$$

The congruences (K_m) and $(M_m)(m = 0, 1, \ldots, g)$ are the so-called *Kummer-Mirimanoff congruences*. A basic relation between $B_j\varphi_{p-j}(t)$ and $\varphi_i(t)\varphi_{p-i}(t)$ may be given by the following congruence (see the proof of Theorem 5 in § 3):

$$\frac{1+t}{2}\varphi_{p-1}(t)+\frac{1-t}{m+1}\sum_{j=2}^{p-2-m}\binom{p-1-m}{j}B_j\varphi_{p-j}(t)$$

$$\equiv -\sum_{i=2}^{m+1}\binom{m}{i-1}\varphi_i(t)\varphi_{p-i}(t) \pmod p,$$

where $t \not\equiv 0, 1 \pmod p$ and m is any integer with $1 \leqslant m \leqslant p-4$.

The main purpose of this paper is to derive some congruences which have the same solutions as those of the Kummer–Mirimanoff congruences. Furthermore, by using these congruences we shall study the first case of Fermat's last theorem. Here, we note that some kinds of congruences stated in this paper are already known, however all of them are obtained by different ways.

2. Some preliminaries. We shall give some lemmas related to the Bernoulli numbers and Mirimanoff polynomials.

LEMMA 1. *Let* $S_m(p) = 1^m+2^m+\ \ldots\ +(p-1)^m$ *for* $m\in\boldsymbol{Z}$. *Then* $S_m(p) \equiv 0 \pmod p$ *if* $(p-1)\nmid m$, *and* $S_m(p) \equiv p-1 \pmod p$ *if* $(p-1)|m$.

Proof. Let r be a primitive root of p. If $rk \equiv \bar{k} \pmod p$, $0 < \bar{k} \leqslant p-1$, for $k = 1, 2, \ldots, p-1$, then $\{\bar{1}, \bar{2}, \ldots, \overline{p-1}\} = \{1, 2, \ldots, p-1\}$, hence $r^m S_m(p) \equiv S_m(p) \pmod p$. If $(p-1)\nmid m$, then $r^m \not\equiv 1 \pmod p$, which gives $S_m(p) \equiv 0 \pmod p$. The assertion for the case $(p-1)|m$ is trivial. ∎

The theorem of von Staudt–Clausen completely describes the denominators of non-zero Bernoulli numbers. That is, if $m \geqslant 1$, then

$$B_{2m} = c_{2m} - \sum_{(p-1)|2m}(1/p),$$

where c_{2m} is some integer and the sum is taken over all primes p such that $(p-1)|2m$.

As a consequence of this, we see that

LEMMA 2. *Let* $m \geqslant 1$. *If* $(p-1)\nmid 2m$, *then* $B_{2m}\in\boldsymbol{Z}_p$. *If* $(p-1)|2m$, *then* $pB_{2m}\in\boldsymbol{Z}_p$, *more precisely* $pB_{2m} \equiv -1 \pmod p$.

LEMMA 3. *Let* $m \geqslant 1$ *and* $p-1 \geqslant k \geqslant 1$. *If* $(p-1)\nmid m$, *then*

$$(m+1)\sum_{i=k}^{p-1} i^m \equiv -\sum_{j=1}^{m+1}\binom{m+1}{j}k^j B_{m+1-j} \pmod p.$$

Proof. Consider the identity

$$v\sum_{i=k}^{p-1} e^{iv} = (e^{pv}-e^{kv})B(v),$$

where $B(v) = v/(e^v-1)$. Here we have

$$\left[v\sum_{i=k}^{p-1} e^{iv}\right]_0^{(m+1)} = (m+1)\sum_{i=k}^{p-1} i^m$$

and

$$[(e^{pv}-e^{kv})B(v)]_0^{(m+1)} = \sum_{j=1}^{m+1}\binom{m+1}{j}(p^j-k^j)B_{m+1-j}.$$

If $(p-1)\nmid m$, then $pB_m \equiv 0 \pmod p$. So the lemma follows. ∎

LEMMA 4. *Let* $t \not\equiv 0, 1 \pmod p$. *Then*

$$(1-t)[U_t(v)]_0^{(m)} = 1 \qquad \text{if } m = 0,$$

$$\equiv \varphi_{m+1}(t) \pmod p \qquad \text{if } m \geqslant 1.$$

Proof. The case $m = 0$ is trivial. Let $N_{k,t}(v) = \sum_{j=k}^{p-1}(te^v)^j$ $(0 \leqslant k \leqslant p-1)$. Since $\{1-(te^v)^p\}U_t(v) = N_{0,t}(v)$ and $[N_{0,t}(v)]_0^{(m)} = \varphi_{m+1}(t)$ for $m \geqslant 1$, the lemma follows. ∎

By this lemma we know that if $t \not\equiv 0, 1 \pmod p$, then we may replace $[U_t(v)]_0^{(i)}$ by $\varphi_{i+1}(t)$ in the congruences (K_m) $(m = 0, 1, \ldots, g)$.

On the other hand, if we set $\lambda_m(t) = (1-t)^{m+1}[U_t(v)]_0^{(m)}$, then, by direct calculation (cf. Agoh [1], Mirimanoff [10])

$$\lambda_m(t) = \sum_{k=1}^{m} b_k^m t^k(1-t)^{m-k} = t\sum_{k=1}^{m} b_k^m(t-1)^{m-k} = \sum_{k=1}^{m} c_k^m t^k,$$

where

$$b_k^m = \sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^m \quad \text{and} \quad c_k^m = \sum_{i=0}^{k}(-1)^i\binom{m+1}{i}(k-i)^m.$$

From these expressions of $\lambda_m(t)$ we see that $\lambda_m(t) = t^{m+1}\lambda_m(1/t)$. Hence, it may be permitted to replace t by $1/t$ in the congruences (K_m) and (M_m).

LEMMA 5. *Let* $\varphi_{k,m+1}(v) = \sum_{j=k}^{p-1} j^m v^j$ $(1 \leqslant k \leqslant p-1,\ m\in\boldsymbol{Z})$. *If* $t \not\equiv 0, 1 \pmod p$ *and* $m \geqslant 1$, *then*

$$\varphi_{k,m+1}(t) \equiv \frac{1}{1-t}\left\{\sum_{i=1}^{m}\binom{m}{i}\varphi_{i+1}(t)\,k^{m-i}t^k + k^m t^k - t\varphi_{m+1}(t)\right\} \pmod p.$$

Proof. For brevity, set $U_t^{(m)} = [U_t(v)]_0^{(m)}$. Since

$$N_{k,t}(v) = U_t(v)(te^v)^k - U_t(v)(te^v)^p,$$

using Lemma 4 we have

$$\varphi_{k,m+1}(t) = [N_{k,t}(v)]_0^{(m)} \equiv t^k \sum_{i=0}^{m} \binom{m}{i} U_t^{(i)} k^{m-i} - t^p U_t^{(m)}$$

$$\equiv \frac{t^k}{1-t}\left\{\sum_{i=1}^{m}\binom{m}{i}\varphi_{i+1}(t)k^{m-i} + k^m\right\} - \frac{t}{1-t}\varphi_{m+1}(t) \pmod p,$$

which shows that the lemma holds. ∎

3. Some results related to the Kummer–Mirimanoff congruences. In the following we assume that p is an odd prime with $p \geqslant 5$. Let S and T be two sets of some congruences with indeterminate t. Then the symbol "$S \Rightarrow T$" means that if $t = t'$ with $t' \not\equiv 0, 1 \pmod p$ is a solution of the system of congruences in S, then $t = t'$ is also a solution of the system of congruences in T.

Let $K = \{(K_i)|\ i = 0, 1, \ldots, g\}$ and $M = \{(M_i)|\ i = 0, 1, \ldots, g\}$. First we shall prove

THEOREM 1. (1) *For all* $i = 1, 2, \ldots, g$,

$$K\backslash\{(K_i)\} \Rightarrow \{(K_i)\}, \quad M\backslash\{(M_i)\} \Rightarrow \{(M_i)\}.$$

(2) *If* $t \not\equiv -1 \pmod p$, *then*

$$K\backslash\{(K_0)\} \Rightarrow \{(K_0)\}, \quad M\backslash\{(M_0)\} \Rightarrow \{(M_0)\}.$$

Proof. Consider the identity

$$B(v)U_t(v) = \frac{1}{1-t}B(v) + \frac{t}{1-t}vU_t(v).$$

Since $[B(v)]_0^{(m)} = B_m$, using Lemma 4 it may be deduced that

$$(1-t)[B(v)U_t(v)]_0^{(p-1)} - [B(v)+tvU_t(v)]_0^{(p-1)}$$

$$\equiv (1-t)\sum_{i=0}^{p-1}\binom{p-1}{i}B_i U_t^{(p-1-i)} - \{B_{p-1} + (p-1)tU_t^{(p-2)}\}$$

$$\equiv \left\{\sum_{i=0}^{p-2}\binom{p-1}{i}B_i\varphi_{p-i}(t) + B_{p-1}\right\} - \left\{B_{p-1} + (p-1)\frac{t}{1-t}\varphi_{p-1}(t)\right\}$$

$$\equiv 0 \pmod p.$$

Here $\binom{p-1}{i} \equiv (-1)^i \pmod p$, $B_{2i+1} = 0$ for $i \geqslant 1$ and $\varphi_p(t) \equiv 0 \pmod p$, so we obtain

$$\frac{1+t}{2(1-t)}\varphi_{p-1}(t) + \sum_{i=1}^{g} B_{2i}\varphi_{p-2i}(t) \equiv 0 \pmod p. \tag{3.1}$$

On the other hand, we have the identity

$$\{U_t(v)\}^2 = U_t(v) + \frac{d}{dv}\{U_t(v)\}.$$

It follows from Lemma 4 that

$$(1-t)^2[\{U_t(v)\}^2]_0^{(p-2)} - (1-t)^2\left[U_t(v) + \frac{d}{dv}U_t(v)\right]_0^{(p-2)}$$

$$\equiv (1-t)^2\sum_{i=0}^{p-2}\binom{p-2}{i}U_t^{(i)}U_t^{(p-2-i)} - (1-t)^2\{U_t^{(p-2)} + U_t^{(p-1)}\}$$

$$\equiv \sum_{i=1}^{p-3}\binom{p-2}{i}\varphi_{i+1}(t)\varphi_{p-1-i}(t) + 2\varphi_{p-1}(t) - (1-t)\{\varphi_{p-1}(t) + \varphi_p(t)\}$$

$$\equiv 0 \pmod p.$$

Noting that

$$\binom{p-2}{i} + \binom{p-2}{p-2-i} \equiv 2(-1)^i(i+1) \pmod p,$$

we can deduce

$$(1+t)\varphi_{p-1}(t) + 2\sum_{i=1}^{g}(-1)^i(i+1)\varphi_{i+1}(t)\varphi_{p-1-i}(t) \equiv 0 \pmod p. \tag{3.2}$$

From (3.1) and (3.2) the results clearly follow. ∎

Let k and m be integers such that $1 \leqslant k \leqslant p-1$ and $m \leqslant p-3$. We now consider the following identity:

$$\alpha_{k,m,t}(v) = \beta_{k,m,t}(v) + \gamma_{m,t}(v), \tag{3.3}$$

where

$$\alpha_{k,m,t}(v) = \{B(v)e^v\}\{\varphi_{m+1}(te^{kv})\},$$

$$\beta_{k,m,t}(v) = v\sum_{i=1}^{p-1}\Big(\sum_{j=0}^{ik} e^{jv}\Big)i^m t^i$$

and

$$\gamma_{m,t}(v) = \varphi_{m+1}(t)B(v).$$

Let $B_i' = B_i$ for $i \neq 1$ and $B_1' = -B_1$. Since

$$[B(v)e^v]_0^{(i)} = B_i' \quad \text{and} \quad [\varphi_{m+1}(te^{kv})]_0^{(i)} = k^i\varphi_{m+1+i}(t),$$

we may write

$$[\alpha_{k,m,t}(v)]_0^{(p-1-m)} = \sum_{i=0}^{p-1-m}\binom{p-1-m}{i}B_i'\{k^{p-1-m-i}\varphi_{p-i}(t)\}.$$

Also we have

$$[\beta_{k,m,t}(v)]_0^{(p-1-m)} = (p-1-m)\sum_{i=1}^{p-1} i^m S_{p-2-m}(ik+1)t^i$$

and

$$[\gamma_{m,t}(v)]_0^{(p-1-m)} = B_{p-1-m}\varphi_{m+1}(t).$$

Noting that $B'_{p-1-m} = B_{p-1-m}$ if $m \neq p-2$, we deduce from (3.3) that

$$(3.4)\quad k^{p-1-m}\varphi_p(t) + \sum_{i=1}^{p-2-m}\binom{p-1-m}{i}k^{p-1-m-i}\{B'_i\varphi_{p-i}(t)\} = (p-1-m)\sum_{i=1}^{p-1} i^m S_{p-2-m}(ik+1)t^i.$$

Here, consider the congruences

$$(A_{k,m})\qquad \sum_{i=1}^{p-1} i^m S_{p-2-m}(ik+1)t^i \equiv 0 \pmod p,$$

where $1 \leqslant k \leqslant p-1$ and $m \leqslant p-3$. And set

$$K(a) = \{(K_i)|\ i = 0, 1, \ldots, a\}, \quad 0 \leqslant a \leqslant g,$$

$$X_m(b) = \{(A_{k,m})|\ k = 1, 2, \ldots, b\}, \quad 1 \leqslant b \leqslant p-2$$

and

$$Y_k(c) = \{(A_{k,m})|\ m = p-3-c,\ p-2-c, \ldots, p-3\}, \quad 0 \leqslant c \leqslant g.$$

Then we can state the following

THEOREM 2. (1) *If* $0 \leqslant a \leqslant g$, *then* $K(a) \Leftrightarrow X_{p-3-2a}(2a+1)$. *In particular,*

$$K \Leftrightarrow X_0(p-2).$$

(2) *If* $1 \leqslant k \leqslant p-1$ *and* $0 \leqslant a \leqslant g$, *then* $K(a) \Leftrightarrow Y_k(2a)$. *In particular,*

$$K \Leftrightarrow Y_k(p-3).$$

Proof. By taking $m = p-3$ in (3.4), we have

$$(3.5)\qquad k\varphi_{p-1}(t) \equiv 2\sum_{i=1}^{p-1} i^{p-3} S_1(ik+1)t^i \pmod p.$$

Also, if $0 \leqslant m \leqslant p-4$, then

$$(3.6)\quad (p-1-m)k^{p-2-m}\varphi_{p-1}(t) + 2\sum_{i=2}^{p-2-m}\binom{p-1-m}{i}k^{p-1-m-i}\{B_i\varphi_{p-i}(t)\} \equiv 2(p-1-m)\sum_{i=1}^{p-1} i^m S_{p-2-m}(ik+1)t^i \pmod p.$$

From (3.5) and (3.6) the assertion $K(a) \Rightarrow X_{p-3-2a}(2a+1)$ is obvious. Conversely, assume the congruences in $X_{p-3-2a}(2a+1)$. If $D = (a_{ij})$ is a matrix of order $2a+1$ with $a_{ij} = i^j$ $(1 \leqslant i, j \leqslant 2a+1)$, then $\det D \not\equiv 0 \pmod p$. Since $p \nmid \binom{2a+2}{i}$, we have $X_{p-3-2a}(2a+1) \Rightarrow K(a)$. The second assertion in (1) is nothing but a special case for $a = g$. On the other hand, the statement (2) immediately follows from the congruences (3.5) and (3.6) with $m = p-4, p-5, \ldots, p-3-2a$. ∎

By observing the case $m \leqslant -1$ in (3.4), we can also derive the similar results to Theorem 2. Especially, we shall treat here the case $m = -1$.

Let $q_p(r)$ be the Fermat quotient with base $r \geqslant 2$, i.e., $q_p(r) = (r^{p-1}-1)/p$. Consider the system of congruences

$$(G_0)\qquad \sum_{i=2}^{p-1} q_p(i)t^i \equiv 0 \pmod p,$$

$$(G_m)\qquad \sum_{i=1}^{p-1}\frac{1}{i}\left[\frac{i(m+1)}{p}\right]t^i \equiv 0 \pmod p, \quad m = 1, 2, \ldots, p-2,$$

where $[x]$ means the greatest integer in a real number x.

Letting $G = \{(G_i)|\ i = 0, 1, \ldots, p-2\}$, we shall prove

THEOREM 3. $K \Leftrightarrow G$.

Proof. Let $1 \leqslant k \leqslant p-1$ and take $m = -1$ in (3.4):

$$(3.7)\qquad k^p\varphi_p(t) + \sum_{i=1}^{p-1}\binom{p}{i}k^{p-i}\{B'_i\varphi_{p-i}(t)\} = p\sum_{i=1}^{p-1}\frac{1}{i}S_{p-1}(ik+1)t^i.$$

Here

$$B'_{p-2} = 0, \quad \varphi_1(t) \equiv \varphi_p(t) \equiv 0 \pmod p, \quad pB'_{p-1} \equiv -1 \pmod p, \quad k^{p-1} \equiv 1 \pmod p$$

and

$$\binom{p}{i} \equiv \{(-1)^{i-1}/i\}p \pmod{p^2} \quad \text{for } i = 2, 3, \ldots, p-3,$$

so we have

$$k^p\varphi_p(t) + \sum_{i=1}^{p-1}\binom{p}{i}k^{p-i}\{B'_i\varphi_{p-i}(t)\}$$

$$= k^p\varphi_p(t) + pk^{p-1}B'_1\varphi_{p-1}(t) + \sum_{i=2}^{p-3}\binom{p}{i}k^{p-i}\{B_i\varphi_{p-i}(t)\} + pkB_{p-1}\varphi_1(t)$$

$$\equiv pk\sum_{r=2}^{p-1} q_p(r)t^r + pk^{p-1}B'_1\varphi_{p-1}(t) + p\sum_{i=2}^{p-3}\frac{(-1)^{i-1}}{i}k^{p-i}\{B_i\varphi_{p-i}(t)\} \pmod{p^2}.$$

Also, the number of elements in the set $\{1, 2, \ldots, ik\}$ which are divisible by p is $[ik/p]$, hence

$$S_{p-1}(ik+1) \equiv ik - \left[\frac{ik}{p}\right] \pmod p.$$

This gives

$$p\sum_{i=1}^{p-1}\frac{1}{i}S_{p-1}(ik+1)t^i \equiv p\left\{\sum_{i=1}^{p-1}\frac{1}{i}\left\{ik-\left[\frac{ik}{p}\right]\right\}t^i\right\}$$
$$\equiv pk\,\varphi_1(t)-p\sum_{i=1}^{p-1}\frac{1}{i}\left[\frac{ik}{p}\right]t^i \equiv -p\sum_{i=1}^{p-1}\frac{1}{i}\left[\frac{ik}{p}\right]t^i \pmod{p^2}.$$

Consequently, we have, from (3.7)

$$(3.8)\qquad -\tfrac{1}{2}k^{p-1}\varphi_{p-1}(t)+\sum_{i=2}^{p-3}\frac{(-1)^i}{i}k^{p-i}\{B_i\varphi_{p-i}(t)\}$$
$$\equiv k\sum_{r=2}^{p-1}q_p(r)t^r+\sum_{i=1}^{p-1}\frac{1}{i}\left[\frac{ik}{p}\right]t^i \pmod{p}.$$

If we assume the congruences (K_i) $(i=0,1,\ldots,g)$, then

$$k\sum_{i=2}^{p-1}q_p(i)t^i+\sum_{i=1}^{p-1}\frac{1}{i}\left[\frac{ik}{p}\right]t^i \equiv 0 \pmod{p}.$$

Since $\sum_{i=1}^{p-1}(1/i)[i/p]\,t^i=0$, we have (G_0), which gives (G_m) $(m=1,2,\ldots,p-2)$. Conversely, assume the congruences in G. Then it follows from (3.8) that

$$-\tfrac{1}{2}k^{p-3}\varphi_{p-1}(t)+\sum_{i=2}^{p-3}\frac{(-1)^i}{i}k^{p-2-i}\{B_i\varphi_{p-i}(t)\}\equiv 0 \pmod{p}.$$

By the same reason as stated in the proof of (1) of Theorem 2, we can derive the congruences in K. This completes the proof of the theorem. ∎

The congruence (G_{p-2}) is equivalent to (K_0) and (M_0). In fact, since

$$(1/i)[i(p-1)/p]=(i-1)/i \quad \text{for } i=2,3,\ldots,p-1,$$

(G_{p-2}) becomes

$$\sum_{i=2}^{p-1}\frac{i-1}{i}t^i \equiv \varphi_1(t)-\varphi_{p-1}(t)\equiv -\varphi_{p-1}(t)\equiv 0 \pmod{p}.$$

We can rewrite the coefficients of congruences in G using the Fermat quotients. Let $1\leqslant i,\ k\leqslant p-1$. Then there exist unique positive integers $c_i(k)$ and $d_i(k)$ such that $ki=c_i(k)p+d_i(k)$ and $1\leqslant d_i(k)\leqslant p-1$. Consider the congruences

$$(G'_m)\qquad \sum_{i=1}^{p-1}q_p(d_i(m+1))\,t^i\equiv 0 \pmod{p},\qquad m=0,1,\ldots,p-2,$$

and put $G'=\{(G'_i)|\ i=0,1,\ldots,p-2\}$. Then we have

THEOREM 4. $G\Leftrightarrow G'$.

Proof. Since $c_i(k)=[ki/p]$, it follows that

$$(ki)^{p-1}-d_i(k)^{p-1}\equiv -(ki)^{p-2}\left[\frac{ki}{p}\right]p \pmod{p^2}.$$

Noting that $k^{p-1}\varphi_p(t)\equiv\varphi_p(t) \pmod{p^2}$, we have

$$\sum_{i=1}^{p-1}\{(ki)^{p-1}-d_i(k)^{p-1}\}t^i\equiv\varphi_p(t)-\sum_{i=1}^{p-1}d_i(k)^{p-1}t^i$$
$$\equiv\sum_{i=1}^{p-1}(i^{p-1}-1)t^i+\sum_{i=1}^{p-1}(1-d_i(k)^{p-1})t^i \pmod{p^2}.$$

Hence

$$k\Big\{\sum_{i=1}^{p-1}q_p(i)t^i-\sum_{i=1}^{p-1}q_p(d_i(k))t^i\Big\}\equiv-\sum_{i=1}^{p-1}\frac{1}{i}\left[\frac{ki}{p}\right]t^i \pmod{p}.$$

Since $q_p(i)=q_p(d_i(1))$, we may rewrite the congruences of G as those of G'. ∎

We report here that the congruences in the above systems G and G' were introduced in a paper of Fueter (see (VI) and (VII) in [2]). To obtain them he used a clever method in the theory of cyclotomic field defined by a primitive pth root of unity. However, we derived them by quite different ways.

As stated in Section 1, the following theorem has been proved by Mirimanoff [10] (see also Ribenboim [11], p. 139–148). We shall give here a simpler and direct proof using (3.4).

THEOREM 5. $K\Leftrightarrow M$.

Proof. Let $1\leqslant m\leqslant p-4$ and take $k=1$ in (3.4):

$$(3.9)\qquad \varphi_p(t)+\sum_{i=1}^{p-2-m}\binom{p-1-m}{i}B'_i\varphi_{p-i}(t)=(p-1-m)\sum_{i=1}^{p-1}i^mS_{p-2-m}(i+1)t^i.$$

Since $p-1-m\geqslant 3$, by Lemmas 1 and 5

$$(p-1-m)\sum_{i=1}^{p-1}i^mS_{p-2-m}(i+1)t^i\equiv(p-1-m)\sum_{j=1}^{p-1}j^{p-2-m}\varphi_{j,m+1}(t)$$
$$\equiv\frac{p-1-m}{1-t}\sum_{j=1}^{p-1}j^{p-2-m}\left\{\sum_{i=1}^{m}\binom{m}{i}\varphi_{i+1}(t)\,j^{m-i}t^j+j^mt^j-t\varphi_{m+1}(t)\right\}$$
$$\equiv\frac{p-1-m}{1-t}\left\{\sum_{i=1}^{m}\binom{m}{i}\varphi_{i+1}(t)\,\varphi_{p-1-i}(t)+\varphi_{p-1}(t)-S_{p-2-m}(p)\,t\varphi_{m+1}(t)\right\}$$
$$\equiv\frac{p-1-m}{1-t}\sum_{i=1}^{m}\binom{m}{i}\varphi_{i+1}(t)\,\varphi_{p-1-i}(t)+\frac{p-1-m}{1-t}\varphi_{p-1}(t) \pmod{p}.$$

Hence, from (3.9)

$$(3.10)\quad (m+1)\frac{1+t}{2(1-t)}\varphi_{p-1}(t)+\sum_{j=2}^{p-2-m}\binom{p-1-m}{j}B_j\varphi_{p-j}(t)$$
$$\equiv -\frac{m+1}{1-t}\sum_{i=1}^{m}\binom{m}{i}\varphi_{i+1}(t)\,\varphi_{p-1-i}(t)\pmod p.$$

If we assume the congruences in K, then, by taking successively $m=1, 2, \ldots, g$ in (3.10) we can deduce $\varphi_{i+1}(t)\,\varphi_{p-1-i}(t)\equiv 0 \pmod p$, $i=1, 2, \ldots, g$. Conversely, assume the congruences in M. Then, by taking $m=p-4, p-6, \ldots, 1$ successively we have $B_j\varphi_{p-j}(t)\equiv 0 \pmod p$, $j=2, 4, \ldots, p-3$. This completes the proof of the theorem. ∎

Incidentally, we see from (2) of Theorem 1 that if $t\not\equiv -1 \pmod p$, then

$$K\setminus\{(K_0)\}\Leftrightarrow M\setminus\{(M_0)\}.$$

Let $2\leqslant k\leqslant p-1$ and $|m|\leqslant p-2$. We observe the identity

$$(3.11)\qquad \delta_{k,m,t}(v)=\varepsilon_{k,m,t}(v)+\eta_{k,m,t}(v),$$

where

$$\delta_{k,m,t}(v)=\varphi_{m+1}(te^{kv})\{-te^{v}\,U_t(v)\},$$
$$\varepsilon_{k,m,t}(v)=\sum_{i=0}^{p-1}\Big(\sum_{j=i}^{p-1}j^m e^{ij(k-1)+iv}\Big)t^i,$$
$$\eta_{k,m,t}(v)=-\varphi_{m+1}(e^{(k-1)v})\,U_t(v).$$

By taking $m=p-2$ in (3.11) and substituting $v=0$ we have

$$-\frac{t}{1-t}\varphi_{p-1}(t)=\sum_{i=0}^{p-1}\Big(\sum_{j=i}^{p-1}j^{p-2}\Big)t^i-\frac{1}{1-t}S_{p-2}(p),$$

which gives, by Lemma 1,

$$(3.12)\qquad \frac{t}{1-t}\varphi_{p-1}(t)\equiv -\sum_{i=1}^{p-1}\Big(\sum_{j=i}^{p-1}j^{p-2}\Big)t^i\pmod p.$$

If $-(p-2)\leqslant m\leqslant p-3$, then

$$[\delta_{k,m,t}(v)]_0^{(p-2-m)}$$
$$=k^{p-2-m}\varphi_{p-1}(t)(1-U_t^{(0)})-\sum_{i=0}^{p-3-m}\binom{p-2-m}{i}k^i\varphi_{m+1+i}(t)\,U_t^{(p-2-m-i)}$$
$$\equiv -\frac{1}{1-t}\left\{k^{p-2-m}\varphi_{p-1}(t)t+\sum_{i=0}^{p-3-m}\binom{p-2-m}{i}k^i\varphi_{m+1+i}(t)\,\varphi_{p-1-m-i}(t)\right\}\pmod p,$$

$$[\varepsilon_{k,m,t}(v)]_0^{(p-2-m)}=(k-1)^{p-2-m}S_{p-2}(p)+\sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}j^m\{j(k-1)+i\}^{p-2-m}\Big\}t^i$$

and

$$[\eta_{k,m,t}(v)]_0^{(p-2-m)}=-\sum_{i=0}^{p-2-m}\binom{p-2-m}{i}(k-1)^i\,S_{m+i}(p)\,U_t^{(p-2-m-i)}.$$

Here $S_{m+i}(p)\equiv 0 \pmod p$ unless $m+i\equiv 0 \pmod{p-1}$. Thus

$$[\eta_{k,m,t}(v)]_0^{(p-2-m)}$$
$$\equiv\begin{cases}0 \pmod p & \text{if } 1\leqslant m\leqslant p-3,\\ \binom{p-2-m}{-m}(k-1)^{-m}\dfrac{1}{1-t}\varphi_{p-1}(t)\pmod p & \text{if } -(p-2)\leqslant m\leqslant 0.\end{cases}$$

From (3.11) we obtain: if $1\leqslant m\leqslant p-3$, then

$$(3.13)\quad k^{p-2-m}\frac{t}{1-t}\varphi_{p-1}(t)+\frac{1}{1-t}\sum_{i=0}^{p-3-m}\binom{p-2-m}{i}k^i\varphi_{m+1+i}(t)\varphi_{p-1-m-i}(t)$$
$$\equiv -\sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}j^m\{j(k-1)+i\}^{p-2-m}\Big\}t^i\pmod p.$$

Also, if $-(p-2)\leqslant m\leqslant 0$, then

$$(3.14)\quad \left\{k^{p-2-m}t+\binom{p-2-m}{-m}(k-1)^{-m}\right\}\frac{1}{1-t}\varphi_{p-1}(t)$$
$$+\frac{1}{1-t}\sum_{i=0}^{p-3-m}\binom{p-2-m}{i}k^i\varphi_{m+1+i}(t)\varphi_{p-1-m-i}(t)$$
$$\equiv -\sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}j^m\{j(k-1)+i\}^{p-2-m}\Big\}t^i\pmod p.$$

Consider the congruences

$$(T_{k,m})\qquad \sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}j^m\{j(k-1)+i\}^{p-2-m}\Big\}t^i\equiv 0\pmod p,$$

where $2\leqslant k\leqslant p-1$ and $|m|\leqslant p-2$. Here, note that if $m=p-2$, then the congruence $(T_{k,m})$ does not depend on k.

Letting

$$M(a)=\{(M_i)|\ i=0, 1, \ldots, a\},\quad 0\leqslant a\leqslant g,$$
$$P_m(b)=\{(T_{k,m})|\ k=2, 3, \ldots, b\},\quad 2\leqslant b\leqslant p-1,$$
$$Q_k(c)=\{(T_{k,m})|\ m=p-2-c,\ p-1-c, \ldots, p-2\},\quad 0\leqslant c\leqslant g,$$

we may state the following theorem:

THEOREM 6. (1) *If* $0 \leqslant a \leqslant g$, *then* $M(a) \Leftrightarrow P_{p-2-a}(a+2)$. *In particular,*

$$M \Leftrightarrow P_{(p-1)/2}((p+1)/2).$$

(2) *If* $2 \leqslant k \leqslant p-1$ *and* $0 \leqslant a \leqslant g$, *then* $M(a) \Leftrightarrow Q_k(a)$. *In particular,*

$$M \Leftrightarrow Q_k((p-3)/2).$$

Proof. Observe the congruences (3.12) if $a = 0$, and (3.13) with $m = p-2-a$ if $1 \leqslant a \leqslant g$. Since $p \nmid \binom{a}{i}$, by the same reason as stated in the proof of (1) of Theorem 2 we can prove the first statement. On the other hand, from (3.12) we know that $M(0) \Leftrightarrow Q_k(0)$. Next, take successively $m = p-3$, $p-4, \ldots, p-2-a$ in (3.13), where $1 \leqslant a \leqslant g$. Then we know that the assertion in (1) for integers a with $1 \leqslant a \leqslant g$ clearly follows. On the other hand, since $p \nmid \binom{j}{i}$ $(0 \leqslant i < j \leqslant a)$, we may deduce the second statement. ∎

For the case $-(p-2) \leqslant m \leqslant 0$ we can give the similar results to Theorem 6 by using (3.14). However, we shall discuss here only the case $m = -1$ and derive the equivalent system to Le Lidec's ([8], [9]). We do not enter into details, but it is easily seen that the congruences in the system L of the next theorem are essentially the same as Granville's variants ([3], Theorem L3-(g), p. 80) for the Le Lidec congruences. We emphasize that these congruences can be obtained by observing a special case of (3.14) for $m = -1$.

Let $2 \leqslant k \leqslant p-1$ and $g(k)$ be an integer such that $(k-1)g(k) \equiv -1 \pmod p$. Also, let $\alpha_m(k)$ be an integer such that $mg(k) \equiv \alpha_m(k) \pmod p$ and $1 \leqslant \alpha_m(k) \leqslant p-1$ for each $m = 1, 2, \ldots, p-1$. We set

$$\beta_m(k) = \begin{cases} 1/\alpha_m(k) & \text{if } \alpha_m(k) > m, \\ 0 & \text{if } \alpha_m(k) < m. \end{cases}$$

Here, the case $\alpha_m(k) = m$ does not occur because $p \nmid k$.

Consider the system of congruences

$$(L_0) \qquad \varphi_{p-1}(t) \equiv 0 \pmod p,$$

$$(L_n) \qquad \sum_{i=1}^{p-1} \beta_i(n+1)\, t^i \equiv 0 \pmod p, \quad n = 1, 2, \ldots, p-2.$$

Letting $L = \{(L_i) |\ i = 0, 1, 2, \ldots, p-2\}$, we shall prove the following theorem:

THEOREM 7. $M \Leftrightarrow L$.

Proof. Set $m = -1$ in (3.14). Noting that $\binom{p-1}{i} \equiv (-1)^i \pmod p$ and $\varphi_1(t) \equiv \varphi_p(t) \equiv 0 \pmod p$, we have

$$(3.15) \qquad \{t+(1-k)\}\frac{1}{1-t}\varphi_{p-1}(t) + \frac{1}{1-t}\sum_{i=2}^{p-2}(-1)^i k^i \varphi_i(t)\varphi_{p-i}(t) \equiv -\sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}\frac{1}{j}\{j(k-1)+i\}^{p-1}\Big\} t^i \pmod p.$$

Suppose that $j(k-1)+i \equiv 0 \pmod p$. Since $(k-1, p) = 1$, there exists an integer $g(k) > 0$ such that $(k-1)g(k) \equiv -1 \pmod p$. Hence $ig(k) \equiv j \pmod p$. Conversely, if $ig(k) \equiv j \pmod p$, then $j(k-1)+i \equiv i\{(k-1)g(k)+1\} \equiv 0 \pmod p$. So, using Lemma 3 and (3.1) we have

$$\begin{aligned}
&\sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}\frac{1}{j}\{j(k-1)+i\}^{p-1}\Big\} t^i \\
&\quad\equiv \sum_{i=1}^{p-1}\Big\{\sum_{j=i}^{p-1}\frac{1}{j}\Big\} t^i - \sum_{i=1}^{p-1}\beta_i(k)\, t^i \\
&\quad\equiv \sum_{i=1}^{p-1}\Big\{\sum_{r=1}^{p-1}\binom{p-1}{r} B_{p-1-r}\, i^r\Big\} t^i - \sum_{i=1}^{p-1}\beta_i(k)\, t^i \\
&\quad\equiv \Big\{\sum_{r=2}^{p-3}\binom{p-1}{r} B_{p-1-r}\,\varphi_{r+1}(t) + \binom{p-1}{p-2} B_1\,\varphi_{p-1}(t)\Big\} - \sum_{i=1}^{p-1}\beta_i(k)\, t^i \\
&\quad\equiv -\frac{t}{1-t}\varphi_{p-1}(t) - \sum_{i=1}^{p-1}\beta_i(k)\, t^i \pmod p,
\end{aligned}$$

because $B_{p-2}\,\varphi_2(t) = 0$ and $B_0\,\varphi_p(t) \equiv 0 \pmod p$. Consequently, it follows from (3.15) that

$$\sum_{i=2}^{p-2}(-1)^i k^i \varphi_i(t)\varphi_{p-i}(t) + (1-k)\varphi_{p-1}(t) \equiv (1-t)\sum_{i=1}^{p-1}\beta_i(k)\, t^i \pmod p.$$

By this congruence we see that the theorem holds. ∎

We shall give some notes on the congruences in the system L.

For $m = 1, 2, \ldots, p-1$, it follows that $\alpha_m(k) > m$ if and only if $\alpha_{p-m}(k) < p-m$. Therefore, in the congruence (L_{k-1}) $(k \neq 1)$ one of terms $\beta_m(k)\, t^m$ and $\beta_{p-m}(k)\, t^{p-m}$ $(1 \leqslant m \leqslant (p-1)/2)$ inevitably vanishes.

Let k and k' be integers such that $2 \leqslant k, k' \leqslant p-1$ and $kk' \equiv 1 \pmod p$. We have $(1-k)\alpha_m(k) \equiv m \pmod p$ and similarly for k', which give $\alpha_m(k)+\alpha_m(k') \equiv m \pmod p$ for $m = 1, 2, \ldots, p-1$. If $\alpha_m(k) < m$, then $\alpha_m(k') = m-\alpha_m(k) < m$. Also if $\alpha_m(k) > m$, then $\alpha_m(k') = p+m-\alpha_m(k) > m$. On the other hand, if $\alpha_m(k) > m$, then $\beta_m(k) \equiv (1-k)(1/m) \pmod p$, hence (L_{k-1}) $(k \neq 1)$ is equivalent to the congruence of the form

$$\sum_{i=1}^{(p-1)/2}\frac{1}{a_i(k)}\, t^{a_i(k)} \equiv 0 \pmod p,$$

where $a_i(k) \in \{1, 2, \ldots, p-1\}$ and $a_i(k) \neq a_j(k)$ if $i \neq j$. Consequently, we see that if $kk' \equiv 1 \pmod p$, then (L_{k-1}) is equivalent to $(L_{k'-1})$. For a given k, the integer k' such that $kk' \equiv 1 \pmod p$ is uniquely determined. Also $k^2 \equiv 1 \pmod p$ if and only if $k = p-1$. Therefore, the system L contains at most $(p+1)/2$ $(= 1+(p-3)/2+1)$ independent congruences.

4. The first case of Fermat's last theorem. We can directly use all of results stated above as criteria for the first case of Fermat's last theorem.

Suppose that the equation

$$x^p + y^p + z^p = 0, \quad p \nmid xyz, \tag{4.1}$$

holds for integers x, y and z prime to each other. If $t' = -y/x$, then from the assumption we have $t' \not\equiv 0, 1 \pmod p$, so $t = t'$ is a solution of the systems K, M, $X_0(p-2)$, $Y_k(p-3)$, G, G', $P_{(p-1)/2}((p+1)/2)$, $Q_k((p-3)/2)$ and L. Also we may state that, by symmetry, all of elements t' in the set

$$W = \left\{-\frac{y}{x}, -\frac{x}{y}, -\frac{z}{y}, -\frac{y}{z}, -\frac{x}{z}, -\frac{z}{x}\right\}$$

are solutions of these systems. If $t' = -y/x$, then the elements of W are congruent modulo p to those of the set

$$H = \left\{t', \frac{1}{t'}, 1-t', \frac{1}{1-t'}, \frac{t'-1}{t'}, \frac{t'}{t'-1} \bmod p\right\},$$

since $x+y+z \equiv 0 \pmod p$.

If $t' \equiv -1 \pmod p$, then we may take $t' \in H$ with $t' \equiv 2, 1/2 \pmod p$ instead of $t' \equiv -1 \pmod p$. So, by Theorem 1 it can be confirmed that there exists an element t' of H such that $t = t'$ is necessarily a solution of (K_0) (or (M_0)) if only $t = t'$ is a solution of (K_m) (or (M_m)) for $m = 1, 2, \ldots, g$. We add that if $t' \equiv -1 \pmod p$, then the systems K and M are of no interest as criteria of (4.1). In fact, if $t' = -y/x \equiv -1 \pmod p$, then $x^p \equiv y^p \pmod{p^2}$, hence $q_p(2) \equiv 0 \pmod p$. Therefore, by Lemma 2 $\varphi_{p-1}(-1) \equiv 2q_p(2)(pB_{p-1}) \equiv -2q_p(2) \equiv 0 \pmod p$, and also $\varphi_m(-1) \equiv \{2(1-2^m)/m\}B_m \equiv 0 \pmod p$ for odd integers m with $3 \leqslant m \leqslant p-2$. So the congruences in the systems K and M clearly hold for $t = t'$ such that $t' \equiv -1 \pmod p$.

By making use of Theorems 3 and 7 we shall prove the following theorem:

THEOREM 8. *If the equation* (4.1) *is satisfied in integers x, y and z prime to each other, then $t = t' \in W$ is a solution of the following congruences*:

$$(1) \quad \sum_{i=97}^{p-1} q_p(i)t^i \equiv 0 \pmod p.$$

$$(2) \quad \sum_{0<i<p/2} \frac{1}{i}t^i \equiv 0 \pmod p.$$

$$(3) \quad \sum_{p/4<i<p/3} \frac{1}{i}t^i - \sum_{2p/3<i<3p/4} \frac{1}{i}t^i \equiv 0 \pmod p.$$

$$(4) \quad \sum_{\substack{0<i<p \\ i:\text{odd}}} \frac{1}{i}t^i \equiv 0 \pmod p.$$

$$(5) \quad \sum_{\substack{p/3<i<p/2 \\ i:\text{odd}}} \frac{1}{i}t^i - \sum_{\substack{p/2<i<2p/3 \\ i:\text{even}}} \frac{1}{i}t^i \equiv 0 \pmod p.$$

Proof. Since $p \nmid xyz$, we may assume here $t' \not\equiv 0, 1 \pmod p$.

(1) Granville and Monagan [4] showed that if the equation (4.1) holds, then $q_p(r) \equiv 0 \pmod p$ for all integers r with $2 \leqslant r < 97$. So we know from (G_0) that (1) holds for $t = t'$.

(2) By (M_0) and (G_1) the congruence (2) clearly follows. We can also deduce (2) directly from (L_1), since $g(2) \equiv -1 \pmod p$ and $\alpha_m(2) = p-m > m$ for $m = 1, 2, \ldots, (p-1)/2$.

(3) By (G_2) and (G_4) we have

$$\sum_{p/4<i<p/2} \frac{1}{i}t^i - \sum_{p/2<i<3p/4} \frac{1}{i}t^i \equiv 0 \pmod p.$$

Also, by (G_2) and (G_3)

$$\sum_{p/3<i<p/2} \frac{1}{i}t^i - \sum_{p/2<i<2p/3} \frac{1}{i}t^i \equiv 0 \pmod p.$$

From these congruences we obtain (3).

(4) Consider the congruence (L_{p-2}). We have $g(p-1) \equiv (p+1)/2 \pmod p$, so $\alpha_m(p-1) = (p+m)/2 > m$ if m is odd, and $\alpha_m(p-1) = m/2 < m$ if m is even. Hence

$$\sum_{\substack{0<i<p \\ i:\text{odd}}} \frac{2}{p+i}t^i \equiv 0 \pmod p,$$

which yields the congruence (4). Incidentally, we may further add the congruence $\varphi_{p-1}(-t) \equiv 0 \pmod p$, since the left hand side of (4) is equal to $(1/2)\{\varphi_{p-1}(t) - \varphi_{p-1}(-t)\}$.

(5) We observe here the congruence (L_2). Since $g(3) \equiv (p-1)/2 \pmod p$, we see that if m is odd, then $\alpha_m(3) = (p-m)/2$, so $\alpha_m(3) > m$ if and only if $p/3 > m$. Also, if m is even, then $\alpha_m(3) = (2p-m)/2$, hence $\alpha_m(3) > m$ if and only if $2p/3 > m$. Thus the congruence (L_2) may be written as follows:

$$\sum_{\substack{0<i<p/3 \\ i:\text{odd}}} \frac{2}{p-i}t^i + \sum_{\substack{0<i<2p/3 \\ i:\text{even}}} \frac{2}{2p-i}t^i \equiv 0 \pmod p.$$

Using this and (2) the result follows immediately.

This completes the proof of the theorem. ∎

References

[1] T. Agoh, *On the first case of Fermat's last theorem*, J. Reine Angew. Math. 319 (1980), 21–28.

[2] R. Fueter, *Kummers Kriterium zum letzen Theorem von Fermat*, Math. Ann. 85 (1922), 11–20.

[3] A. J. Granville, *Diophantine equations with varying exponents with special reference to Fermat's last theorem*, Ph. D. Thesis, Queen's Univ., Kingston, 1987, 207 pp.

[4] A. J. Granville and M. B. Monagan, *The first case of Fermat's last theorem is true for all prime exponents up to* 714,591,416,091,389, Trans. Amer. Math. Soc. 306 (1988), 329–359.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II*, Jahresber. Deutsch. Math.-Verein., 1930, 204 pp. Reprinted by Physica-Verlag, Würzburg 1965.

[6] K. Inkeri, *Some extensions of criteria concerning singular integers in cyclotomic fields*, Ann. Acad. Sci. Fenn. Ser. AI, 49 (1948), 3–15.

[7] E. E. Kummer, *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Abhandl. Königl. Akad. Wiss. Berlin, 1857, 41–74.

[8] P. Le Lidec, *Sur une forme nouvelle des congruences de Kummer–Mirimanoff*, C. R. Acad. Sci. Paris, Sér. A, 265 (1967), 89–90.

[9] — *Nouvelle forme des congruences de Kummer–Mirimanoff pour le premier cas du théorème de Fermat*, Bull. Soc. Math. France 97 (1969), 321–328.

[10] D. Mirimanoff, *L'équation indéterminée* $x^l + y^l + z^l = 0$ *et le critérium de Kummer*, J. Reine Angew. Math. 128 (1905), 45–68.

[11] P. Ribenboim, 13 *lectures on Fermat's last theorem*, Springer, New York–Heidelberg–Berlin 1979.

DEPARTMENT OF MATHEMATICS
SCIENCE UNIVERSITY OF TOKYO
Noda, Chiba 278, Japan

Received on 6.9.1988
and in revised form on 16.1.1989 (1866)

ACTA ARITHMETICA
LV (1990)

CM-fields and exponents of their ideal class groups

by

KUNIAKI HORIE (Yamaguchi) and MITSUKO HORIE (Fukuoka)

By an *algebraic number field*, we shall mean a finite algebraic extension over the rational number field $\boldsymbol{Q}$. All such fields will be supposed to lie in the complex number field $\boldsymbol{C}$. Let j denote the complex conjugation of $\boldsymbol{C}$. An algebraic number field k is called a *j-field* when k is invariant as a whole under j, i.e., $k^j = k$ and when $\sigma j = j\sigma$ on k for all isomorphisms σ of k into $\boldsymbol{C}$. Then a j-field is either a totally real algebraic number field or a CM-field, namely, a totally imaginary quadratic extension over a totally real algebraic number field.

Let l be a fixed prime number. For any algebraic number field F, let C_F denote the ideal class group of F, A_F the Sylow l-subgroup of C_F, h_F the class number of F, and s_F the order of A_F. The exponent of each finite group G will be denoted by $\exp G$. In the present paper, we shall first prove the following

THEOREM 1. *Let k be a j-field; let r, m, and n be natural numbers. Then only a finite number of CM-fields K have the following two properties:*

(i) $h_K/s_K \leqslant m$ *and* $\exp A_K \leqslant l^r$,

(ii) *there exists a sequence* $k = k_0 \subset k_1 \subset \ldots \subset k_n = K$ *of j-fields such that for each* $\nu \in \{1, 2, \ldots, n\}$, $k_\nu = k_{\nu-1}$ *or* $k_\nu/k_{\nu-1}$ *is a cyclic extension of degree l.*

Now, for each (multiplicative) abelian group $\mathfrak{M}$ on which j acts, we put

$$\mathfrak{M}^- = \{\mu \in \mathfrak{M} \mid \mu^j = \mu^{-1}\}.$$

For any j-field F, we let

$$h_F^- = h_F/h_{F^+},$$

where F^+ denotes the maximal real subfield of F; h_F^- is known to be an integer. Furthermore, as j acts on A_F in the obvious manner, we can define

$$s_F^- = |A_F^-|.$$

In the case $l > 2$, this becomes the highest power of l dividing h_F^- and we can prove the following result which is more precise than Theorem 1.