374. *Il quadricentenario di Keplero*, Archimede, 1972, pp. 1–15.
375. *Ueber Galoische Geometrien*, in Geometrie, Wissenschaftliche Buchgesellschaft Darmstad, 1972, pp. 100–117.
376. *Inequalities concerning symmetric or almost-symmetric functions*, Tensor N.S 24 (1972), pp. 273–287.
377. *Riflessi vicini e lontani del pensiero e dell'opera di Federigo Enriques*, Atti e Conv. Internaz. Geometria, Milano 1971, 1975, pp. 11–25.
378. *On algebraic varieties as intersections of primals in a projective or affine space*, Atti Conv. Internaz. Geometria, Milano 1971, 1975, pp. 35–53.
379. *Some arithmetical problems on the use of the balance*, Rend. Acc. Naz. Lincei, (8), 54 (1973), pp. 1–12.
380. *Strutture matematiche e realtà fisica*, Nuova Antologia, N. 2072 (1973), pp. 472–480.
381. *Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois*, Ann. di Mat., (8), 96 (1973), pp. 289–337.
382. *Generalizzazione di un procedimento di Levi-Civita atto a costruire soluzioni particolari di sistemi differenziali*, Rend. Acc. Naz. Lincei, (8), 55_2 (1973), pp. 1–5.
383. *Il carteggio marconiano presso l'Accademia dei Lincei*, Nuova Antologia, N. 2079 (1974), pp. 306–321.
384. *Sur les correspondences involutoires régulières dans les ensembles finis*, C. R. Ac. Sc. Paris 279 (1974), pp. 309–311.
385. *Prefazione*, al Seminario sulla Evoluzione Biologica, Centro Linceo Interdisciplinare, 7 (1975), pp. 5–6.
386. *Le Accademie Scientifiche*, Nuova Antologia, N. 2091 (1975), pp. 319–322.
387. *Introduzione al Convegno copernicano*, Atti del Convegno su: Copernico e la cosmologia moderna, Lincei Quad. 216. (1975), pp. 7–11.
388. *Sugli insiemi finiti di punti di uno spazio grafico*, Rend. di Mat., (6), 8 (1975), pp. 37–63.
389. *Archimede e la scienza moderna*, Archimede 2 (1975), pp. 5–15.
390. *Su di un presunto controesempio per l'ipotesi dei quattro colori*, Rend. Acc. Naz. Lincei, (8), 59 (1975), novembre, pp. 1–2.
391. *Severi Francesco*, Dictionary of Scientific Biography, 12 (1975), pp. 330–332.
392. *L'opera di Tullio Levi-Civita*, Atti dei Convegni Lincei 8 (1975), pp. 9–29.
393. *Lucien Godeaux*, Boll. Un. Mat. Ital., (4), 11 (1975), pp. 639–644.
394. *Un approccio al problema dei quattro colori*, Rend. Accad. Naz. dei Quaranta, (5), 1–2 (1975), pp. 60.
395. *Incidence structures and Galois geometries, with special regard to regular involutive correspondences, arcs, caps, segments and conics*, Teorie combinatorie, Atti dei Convegni Lincei, 17 (Roma, 1973), Vol. I, 1976, pp. 331–369.
396. *Invarianti proiettivi integrali inerenti a certe coppie o terne di curve chiuse*, Rend. Acc. Naz. Lincei, (8), 61 (1976), pp. 420–427.
397. (con G. Korchmaros) *Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica*, Rend. Acc. Naz. Lincei, (8), 62 (1977), pp. 1–7.
398. *Sulle potenze di una matrice quadrata d'ordine $n \geqslant 2$*, Abh. Math. Sem. Univ. Hamburg 47 (1978), pp. 71–78.

ACTA ARITHMETICA
XLV (1984)

On Fermat's last theorem

by

TAKASHI AZUHATA (Tokyo)

1. Introduction. In this paper we will consider the following equation:

$$X^{p^n}+Y^{p^n}+Z^{p^m}=0, \tag{1}$$

where p is an odd prime number and n, m are natural numbers. Assume that there exist relatively prime integers x, y, z satisfying (1) in the case $m = n$. Then the following theorem holds.

THEOREM. *Under the above assumption, if r is an integer satisfying one of the following conditions:*

(i) $r|x$, $p\nmid x$,

(ii) $r|x-y$, $p\nmid x^2-y^2$,

(iii) $r|x^2-yz$, $p\nmid xy+yz+zx$,

(iv) $r|x^2+yz$, $p\nmid x(y-z)(x^2+yz)$,

then the following congruence holds:

$$r^{p-1} \equiv 1 \pmod{p^{n+1}}. \tag{2}$$

This result was shown by Furtwängler [1], McDonnell [4], Moriya [5] and Inkeri [2], [3] (see Ribenboim [6], Lec. IX). We will show that (2) also holds for mod p^{2n}.

2. Preliminaries. We denote by

$\boldsymbol{Q}$ the field of rational numbers,

$\boldsymbol{Z}$ the ring of rational integers,

ζ a primitive p^n-th root of unity,

$K = \boldsymbol{Q}(\zeta)$ the cyclotomic field generated by ζ,

$A = \boldsymbol{Z}[\zeta]$ the ring of integers of K,

g a primitive root mod p^n, if $n = 1$, let $g^{p-1} \not\equiv 1 \pmod{p^2}$,

$s = (\zeta\colon \zeta^g)$ a substitution generating $\mathrm{Gal}(K/\boldsymbol{Q})$,

$A\alpha$ the principal ideal in K generated by $\alpha \in A$.

Let $v = 2v' = p^{n-1}(p-1)$ and $\lambda = 1-\zeta$, then $A\lambda$ is the prime ideal in K such that $Ap = A\lambda^v$. For $k \in \boldsymbol{Z}$, let g_k be the unique integer such that

$g_k \equiv g^k \pmod{p^n}$ and $1 \leqslant g_k \leqslant p^n-1$. If $k<0$, this stands for the least positive solution of the congruence equation $Xg^{-k} \equiv 1 \pmod{p^n}$. Put

$$f(X) = \sum_{i=0}^{\nu-1} h_{-i} X^i \quad \text{with} \quad h_{-i} = \frac{1}{p^n}(gg_{-i} - g_{-i+1}).$$

Then $f(X) \in \mathbf{Z}[X]$ and

$$f(g) = \sum_{i=0}^{\nu-1} \frac{1}{p^n}(g^{i+1}g_{-i} - g^i g_{-i+1}) = \frac{1}{p^n}(g^\nu g_{-\nu+1} - g_1)$$

$$= \frac{g_1}{p^n}(g^\nu - 1) \not\equiv 0 \pmod{p},$$

since $g^\nu \not\equiv 1 \pmod{p^{n+1}}$. The following lemma is a well-known result which was also used in [3] (see, for example, Washington [7], § 6.2).

LEMMA 1. *For any ideal* $\mathfrak{A}$ *in* K, $\mathfrak{A}^{f(s)}$ *is a principal ideal, where we employ the symbolic power.*

LEMMA 2. *Let* $\mathfrak{Q}$ *be a prime ideal of* K. *If* $N_{K/Q}(\mathfrak{Q})-1$ *is divisible by* p^{n+1}, *then the degree of* $\mathfrak{Q}$ *is a divisor of* $p-1$.

Proof. Let f be the degree of $\mathfrak{Q}$. Then f is the least positive integer satisfying the congruence $q^f \equiv 1 \pmod{p^n}$, where q is the rational prime number divisible by $\mathfrak{Q}$. If f is divisible by p, putting $f = pf'$, we have $q^{f'} \equiv 1 \pmod{p^n}$ from $q^f \equiv 1 \pmod{p^{n+1}}$. This contradicts the definition of f. So f is not divisible by p. On the other hand, f is a divisor of $p^{n-1}(p-1)$. Hence we get our assertion.

3. Theorems. Now we may extend the above theorem as follows.

THEOREM 1. *If the equation* (1) *holds for integers* x, y, z, *with* $(x, y, z) = 1$, *then we have* $r^{p-1} \equiv 1 \pmod{p^{m+n}}$ *for a rational integer* r *satisfying the condition* (i) *or* (ii). *If in particular* $m = n$, *we also have* $r^{p-1} \equiv 1 \pmod{p^{2n}}$ *for* r *satisfying the condition* (iii) *or* (iv):

(i) $r|x$, $p\nmid x$,

(ii) $r|x^2-y^2$, $p\nmid x^2-y^2$,

(iii) $r|x^2-yz$, $p\nmid xy+yz+zx$,

(iv) $r|x^2+yz$, $p\nmid x(y-z)(x^2+yz)$.

We first prove the following

THEOREM 2. *Assume that there exist* $\alpha, \beta, \gamma \in A$ *satisfying* (1) *for* $m \leqslant n$ *with* $(\lambda, \alpha, \beta, \gamma) = 1$, *and assume that* $\lambda^3|\alpha+\beta$ *if* $\lambda|\gamma$. *If* r *is a rational integer with* $(r, \alpha, \beta, \gamma) = 1$ *satisfying one of the conditions* (v), (vi), (vii), *then we have*

$$r^{p-1} \equiv 1 \pmod{p^{m+n}}. \tag{3}$$

Further assume that $m = n$ *and that if one of the integers* α, β, γ *is divisible by* λ, *then the sum of the other two of them is divisible by* λ^3. *Then we also have*

$$r^{p-1} \equiv 1 \pmod{p^{2m}} \tag{4}$$

for a rational integer r *satisfying the condition* (viii) *or* (ix):

(v) $r|\alpha$, $\lambda\nmid\alpha$,

(vi) $r|\alpha-\beta$, $\lambda\nmid\alpha^2-\beta^2$,

(vii) $r|\alpha+\beta$, $\lambda\nmid\alpha^2-\beta^2$,

(viii) $r|\alpha^2-\beta\gamma$, $\lambda\nmid\alpha\beta+\beta\gamma+\gamma\alpha$,

(ix) $r|\alpha^2+\beta\gamma$, $\lambda\nmid\alpha(\beta-\gamma)(\alpha^2+\beta\gamma)$ *when* $p \geqslant 5$.

To prove this theorem, we need the following lemmas.

LEMMA 3. *Under the same assumption as in the first half of Theorem 2, we have*

(x) *if* $\lambda\nmid\gamma$, *then* $\left((\alpha+\zeta^k\beta)^{p^m-1}(\alpha+\zeta^{2k}\beta)\right)^{f(s)} = \zeta^{ck}\xi_k^{p^m}$,

(xi) *if* $\lambda|\gamma$, *then* $\left((\alpha+\zeta^k\beta)^{p^m-1}(\alpha+\zeta^{2k}\beta)\right)^{f(s)} = \zeta^{dk}(1+\zeta^k)^{f(s)}\omega_k^{p^m}$,

where $(k, p) = 1$, $\xi_k, \omega_k \in A$, $c \equiv \dfrac{\beta(1)}{\alpha(1)+\beta(1)} f(g)$, $d \equiv 0 \pmod{p}$ *with* $\alpha(X)$, $\beta(X) \in \mathbf{Z}[X]$ *such that* $\alpha = \alpha(\zeta)$, $\beta = \beta(\zeta)$.

Proof. We only prove the case $k = 1$. The other cases are shown similarly. It follows from (1) that

$$\prod_{i=0}^{p^n-1} (\alpha+\zeta^i\beta) = (-\gamma)^{p^m}. \tag{5}$$

First we assume that $\lambda\nmid\gamma$. If there exists prime ideal $\mathfrak{P}$ in K such that $\mathfrak{P}|A(\alpha+\zeta^i\beta)$ and $\mathfrak{P}|A(\alpha+\zeta^j\beta)$ $(0 \leqslant i < j < p^n)$, then $\mathfrak{P}|A\lambda\alpha$ and $\mathfrak{P}|A\lambda\beta$. So we see that $\mathfrak{P}|A\alpha$, $\mathfrak{P}|A\beta$ from $\mathfrak{P}|A\gamma$ and $\lambda\nmid\gamma$. Thus we may write $A(\alpha+\zeta^i\beta) = \mathfrak{A}\mathfrak{C}_i$ with ideals $\mathfrak{A} = (A\alpha, A\beta)$ and $\mathfrak{C}_i$ in K, where $\mathfrak{C}_i$ are pair-wise relatively prime. Since $\mathfrak{A}^{p^n}\prod_{i=0}^{p^n-1}\mathfrak{C}_i = (A\gamma)^{p^m}$ from (5) and $m \leqslant n$, we get $A(\alpha+\zeta^i\beta) = \mathfrak{A}\mathfrak{B}_i^{p^m}$ with ideals $\mathfrak{B}_i$ in K such that $\mathfrak{B}_i^{p^m} = \mathfrak{C}_i$. It follows from Lemma 1 that $\mathfrak{A}^{f(s)} = A\mu$, $\mathfrak{B}_i^{f(s)} = A\tau_i$ with $\mu, \tau_i \in A$. Hence we have

$$\left((\alpha+\zeta\beta)^{p^m-1}(\alpha+\zeta^2\beta)\right)^{f(s)} = \varepsilon(\mu\tau_1^{p^m-1}\tau_2)^{p^m}, \tag{6}$$

where ε is a unit of K. We notice that $s^{\nu'}$ is a complex conjugate and $f(s) \times (1+s^{\nu'}) = (g-1)(1+s+s^2+\ldots+s^{\nu-1})$. Let $N_{K/Q}(\mathfrak{A}) = \mathbf{Z}a$, $N_{K/Q}(\mathfrak{B}_i) = \mathbf{Z}b_i$ where $\mathbf{Z}a$, $\mathbf{Z}b_i$ are ideals in $\mathbf{Z}$ generated by $a, b_i \in \mathbf{Z}$ respectively. Then, multiplying (6) by its complex conjugate, we obtain

$$(\pm ab_1^{p^m-1}b_2)^{p^m(g-1)} = \varepsilon\bar{\varepsilon}\left(\mu\bar{\mu}(\tau_1\bar{\tau}_1)^{p^m-1}\tau_2\bar{\tau}_2\right)^{p^m}.$$

Hence we see that $\varepsilon\bar{\varepsilon} = \eta^{p^m}$ with a unit η in K. Putting $\varepsilon = \zeta^c\delta$ with a real unit δ, we get $\varepsilon\bar{\varepsilon} = \delta^2 = \eta^{p^m}$. Therefore we have $\delta = (\delta^i\eta^j)^{p^m}$ with $i, j \in \mathbf{Z}$ such that $p^m i+2j=1$. Hence we may write

$$\left((\alpha+\zeta\beta)^{p^m-1}(\alpha+\zeta^2\beta)\right)^{f(s)}=\zeta^c\xi_1^{p^m}$$

with $\xi_1=\delta^i\eta^j\mu\tau_1^{p^m-1}\tau_2$.

Now we estimate the value of c modulo p. Let $\xi_1=F(\zeta)$ with $F(X)\in Z[X]$. The polynomial

$$\prod_{i=0}^{v-1}\left(\left(\alpha(X^{g^i})+X^{g^i}\beta(X^{g^i})\right)^{p^m-1}\left(\alpha(X^{g^i})+X^{2g^i}\beta(X^{g^i})\right)\right)^{h-i}-X^cF(X)^{p^m}$$

vanishes at $X=\zeta$. So we may write

$$\prod_{i=0}^{v-1}\left(\left(\alpha(X^{g^i})+X^{g^i}\beta(X^{g^i})\right)^{p^m-1}\left(\alpha(X^{g^i})+X^{2g^i}\beta(X^{g^i})\right)\right)^{h-i}$$
$$=X^cF(X)^{p^m}+\Phi(X)M(X),$$

where $\Phi(X)=1+X^{p^{n-1}}+\ldots+X^{p^{n-1}(p-1)}$, $M(X)\in Z[X]$. Putting $X=e^v$ and taking the logarithms of both sides, we have

$$\sum_{i=0}^{v-1}h_{-i}(p^m-1)\log\left(\alpha(e^{g^iv})+e^{g^iv}\beta(e^{g^iv})\right)+\sum_{i=0}^{v-1}h_{-i}\log\left(\alpha(e^{g^iv})+e^{2g^iv}\beta(e^{g^iv})\right)$$
$$=cv+p^m\log F(e^v)+\log\left(1+G(e^v)\right),$$

where

$$G(e^v)=\frac{\Phi(e^v)M(e^v)}{e^{cv}F(e^v)^{p^m}}.$$

On taking derivative and putting $v=0$, it follows from $G'(1)\equiv 0 \pmod p$ that

$$\frac{\beta(1)}{\alpha(1)+\beta(1)}f(g)\equiv c \pmod p.$$

Next we consider the case $\lambda|\gamma$. By the same argument as above, we have $A(\alpha+\zeta^i\beta)=A\lambda^{e_i}\mathfrak{A}\mathfrak{B}_i^{p^m}$, where $\mathfrak{A}=(A\alpha, A\beta)$ and $\mathfrak{B}_i$ are ideals in K prime to $A\lambda$, and $e_i\geqslant 1$. If $(i,p)=1$, then we see that $e_i=1$ since $\lambda^3|\alpha+\beta$, $\alpha+\zeta^i\beta\equiv\alpha+\beta \pmod{A\lambda}$ and $\alpha+\zeta^i\beta\not\equiv\alpha+\beta \pmod{A\lambda^2}$. Putting $\alpha+\beta=(1-\zeta)\alpha_1=(1-\zeta^2)\alpha_2$, we get

$$\frac{\alpha+\zeta\beta}{1-\zeta}=\frac{\alpha+\beta}{1-\zeta}-\beta=\alpha_1-\beta,\qquad \frac{\alpha+\zeta^2\beta}{1-\zeta^2}=\frac{\alpha+\beta}{1-\zeta^2}-\beta=\alpha_2-\beta.$$

It follows from

$$A(\alpha_1-\beta)=\mathfrak{A}\mathfrak{B}_1^{p^m},\qquad A(\alpha_2-\beta)=\mathfrak{A}\mathfrak{B}_2^{p^m},$$

that

$$\left((\alpha_1-\beta)^{p^m-1}(\alpha_2-\beta)\right)^{f(s)}=\zeta^d\tau^{p^m} \tag{7}$$

with $\tau\in A$. Since $\lambda^2|\alpha_1$, $\lambda^2|\alpha_2$, we see that $\alpha_1(1)\equiv\alpha_1'(1)\equiv\alpha_2(1)\equiv\alpha_2'(1)\equiv 0 \pmod p$, where $\alpha_1(X), \alpha_2(X)\in Z[X]$ such that $\alpha_1=\alpha_1(\zeta)$, $\alpha_2=\alpha_2(\zeta)$. So we have

$$d\equiv(p^m-1)\frac{\alpha_1'(1)-\beta'(1)}{\alpha_1(1)-\beta(1)}f(g)+\frac{\alpha_2'(1)-\beta'(1)}{\alpha_2(1)-\beta(1)}f(g)\equiv 0 \pmod p.$$

Multiplying (7) by $\left((1-\zeta)^{p^m-1}(1-\zeta^2)\right)^{f(s)}$, we get

$$\left((\alpha+\zeta\beta)^{p^m-1}(\alpha+\zeta^2\beta)\right)^{f(s)}=\zeta^d(1+\zeta)^{f(s)}\omega_1^{p^m}$$

with $\omega_1=\tau(1-\zeta)^{f(s)}$. This completes the proof.

Lemma 4. *Let q be a rational prime number with $q\neq p$. Assume that the following congruence holds:*

$$\zeta^a\equiv\tau\xi^{p^m} \pmod{Aq}, \tag{8}$$

where $a\in Z$, $(a,p)=1$, $\tau,\ \xi\in A$, $(q,\tau\xi)=1$ and τ is real. Then we have

$$q^{p-1}\equiv 1 \pmod{p^{m+n}}. \tag{9}$$

Proof. Let $\mathfrak{Q}$ be a prime ideal in K dividing Aq. Assuming that $\tau=1$, we see that

$$\xi^{p^{m+n-1}}\equiv\zeta^{ap^{n-1}}\not\equiv 1,\qquad \xi^{p^{m+n}}\equiv 1 \pmod{\mathfrak{Q}}.$$

Hence we have (9) from $p^{m+n}|N_{K/Q}(\mathfrak{Q})-1$ and by Lemma 2. In the case $\tau\neq 1$, raising to the power $1-s^{v'}$ on the both sides of (8), we obtain

$$\zeta^{2a}\equiv(\xi\bar{\xi}^{-1})^{p^m} \pmod{Aq}.$$

Hence (9) holds as shown above.

Lemma 5. *Under the same assumption as in Theorem 2, we have:*
(xii) *if r satisfies* (v), *then* $(r,\beta\gamma)=1$,
(xiii) *if r satisfies* (viii) *or* (ix), *then* $(r,\alpha\beta\gamma)=1$,
(xiv) *if r satisfies* (vi) *or* (vii), *then* $(r,\alpha\beta)=(r,\alpha+\zeta^i\beta)=1$ $(1\leqslant i<p^n)$.

Proof. We denote by $\mathfrak{Q}$ a prime ideal in K dividing Ar.

(xii) If $r|\alpha$ and $(r,\beta\gamma)\neq 1$, then we have $r\equiv\alpha\equiv\beta\equiv\gamma\equiv 0 \pmod{\mathfrak{Q}}$ for some $\mathfrak{Q}$ from $\alpha^{p^n}+\beta^{p^n}+\gamma^{p^m}=0$. This contradicts to $(r,\alpha,\beta,\gamma)=1$.

(xiii) If $r|\alpha^2+\beta\gamma$ or $r|\alpha^2-\beta\gamma$ and $(r,\alpha\beta\gamma)\neq 1$, then we also get $r\equiv\alpha\equiv\beta\equiv\gamma\equiv 0 \pmod{\mathfrak{Q}}$ for some $\mathfrak{Q}$, which is a contradiction.

(xiv) In the same way as above, it is impossible that $r|\alpha+\beta$ or $r|\alpha-\beta$ and $(r,\alpha\beta)\neq 1$. If $r|\alpha+\beta$ or $r|\alpha-\beta$ and $(r,\alpha+\zeta^i\beta)\neq 1$ with $1\leqslant i<p^n$, then we get $(1-\zeta^i)\beta\equiv 0$ or $(1+\zeta^i)\beta\equiv 0 \pmod{\mathfrak{Q}}$ from $\alpha+\beta\equiv\alpha+\zeta^i\beta\equiv 0$ or $\alpha-\beta\equiv\alpha+\zeta^i\beta\equiv 0 \pmod{\mathfrak{Q}}$ for some $\mathfrak{Q}$. Since $\lambda\nmid r$, $(r,\beta)=1$ and $1+\zeta^i$ is a unit, this is a contradiction.

Proof of Theorem 2. We put $\alpha(1) = u$, $\beta(1) = v$ and $\gamma(1) = w$. Notice that $\alpha+\beta+\gamma \equiv 0 \pmod{A\lambda}$ and $u+v+w \equiv 0 \pmod{p}$. We denote by q a prime number dividing r.

(v) Let $r|\alpha$ and $\lambda\nmid\alpha$. If $\lambda\nmid\gamma$, it follows from Lemma 3 that

$$\big((\alpha+\zeta\beta)^{p^m-1}(\alpha+\zeta^2\beta)\big)^{f(s)} \equiv \zeta^a\beta^{p^m f(s)} \equiv \zeta^c\xi_1^{p^m} \pmod{Aq},$$

where $\xi_1 \in A$, $a = (p^m+1)b$, $c \equiv \dfrac{v}{u+v}b \pmod{p}$, $b = f(g)$. Note that $(q, \beta\xi_1) = 1$ by Lemma 5. So we have

$$\zeta^{a-c} \equiv \big((\beta^{f(s)})^{-1}\xi_1\big)^{p^m} \pmod{Aq}.$$

Since $\lambda\nmid\alpha$, we see that

$$a-c \equiv b-\frac{v}{u+v}b \equiv \frac{u}{u+v}b \not\equiv 0 \pmod{p}.$$

Hence we have (3) from Lemma 4. If $\lambda|\gamma$, from Lemma 3,

$$\begin{aligned}\big((\alpha+\zeta^2\beta)^{p^m-1}(\alpha+\zeta^4\beta)\big)^{f(s)} &\equiv \zeta^{2a}\beta^{p^m f(s)}\\ &\equiv \zeta^{2d}(1+\zeta^2)^{f(s)}\omega_2^{p^m} \equiv \zeta^{2d+b}(\zeta^{-1}+\zeta)^{f(s)}\omega_2^{p^m} \pmod{Aq},\end{aligned}$$

where $\omega_2 \in A$, $(q, \beta\omega_2) = 1$, $d \equiv 0 \pmod{p}$. So we see that

$$\zeta^{2a-2d-b} \equiv (\zeta^{-1}+\zeta)^{f(s)}\big((\beta^{f(s)})^{-1}\omega_2\big)^{p^m} \pmod{Aq}.$$

Since $2a-2d-b \not\equiv 0 \pmod{p}$ and $\zeta^{-1}+\zeta$ is real, we have (3) from Lemma 4.

(vi) Assume that $r|\alpha-\beta$ and $\lambda\nmid\alpha^2-\beta^2$. Then $\lambda\nmid\gamma$ from $\lambda\nmid\alpha+\beta$. So, from Lemma 3,

$$\begin{aligned}\big((\alpha+\zeta^2\beta)^{p^m-1}(\alpha+\zeta^4\beta)\big)^{f(s)} &\equiv \big(\alpha^{p^m}(1+\zeta^2)^{p^m-1}(1+\zeta^4)\big)^{f(s)}\\ &\equiv \zeta^a\alpha^{p^m f(s)}\big((\zeta^{-1}+\zeta)^{p^m-1}(\zeta^{-2}+\zeta^2)\big)^{f(s)}\\ &\equiv \zeta^{2c}\xi_2^{p^m} \pmod{Aq}.\end{aligned}$$

It follows from Lemma 5 that $(q, \alpha\xi_2) = 1$. We notice that $\zeta^{-1}+\zeta$ and $\zeta^{-2}+\zeta^2$ are real and that $a-2c \equiv \dfrac{u-v}{u+v}b \not\equiv 0 \pmod{P}$ from $\lambda\nmid\alpha-\beta$. Hence we get (3) from Lemma 4.

(vii) If $r|\alpha+\beta$ and $\lambda\nmid\alpha^2-\beta^2$, in the same way as above, we have

$$\begin{aligned}\big((\alpha+\zeta^2\beta)^{p^m-1}(\alpha+\zeta^4\beta)\big)^{2f(s)} &\equiv \big(\alpha^{p^m}(1-\zeta^2)^{p^m-1}(1-\zeta^4)\big)^{2f(s)}\\ &\equiv \zeta^{2a}\alpha^{2p^m f(s)}\big((\zeta^{-1}-\zeta)^{2p^m-2}(\zeta^{-2}-\zeta^2)^2\big)^{f(s)}\\ &\equiv \zeta^{4c}\xi_2^{2p^m} \pmod{Aq},\end{aligned}$$

where $(q, \alpha\xi_2) = 1$ by Lemma 5. Since $(\zeta^{-1}-\zeta)^2$ and $(\zeta^{-2}-\zeta^2)^2$ are real and $2a-4c \not\equiv 0 \pmod{p}$, we also get (3) from Lemma 4. We may also prove the rest of Theorem 2 similarly.

(viii) Assume that $r|\alpha^2-\beta\gamma$ and $\lambda\nmid\alpha\beta+\beta\gamma+\gamma\alpha$. It follows from the equation $\alpha(\alpha+\zeta^k\beta)-\beta(\gamma+\zeta^k\alpha) = \alpha^2-\beta\gamma$ that

$$\big(\alpha^{p^n}(\alpha+\zeta^k\beta)^{p^n-1}(\alpha+\zeta^{2k}\beta)\big)^{f(s)} \equiv \big(\beta^{p^n}(\gamma+\zeta^k\alpha)^{p^n-1}(\gamma+\zeta^{2k}\alpha)\big)^{f(s)} \pmod{Aq}.$$

From Lemma 3, we have the following congruences according to the three cases: (a) $\lambda\nmid\beta\gamma$ with $k=1$, (b) $\lambda|\beta$ with $k=2$, (c) $\lambda|\gamma$ with $k=2$.

Case (a).

$$\zeta^c(\alpha^{f(s)}\xi_1)^{p^n} \equiv \zeta^{c'}(\beta^{f(s)}\xi_1')^{p^n} \pmod{Aq},$$

where

$$c-c' \equiv \frac{v}{u+v}b-\frac{u}{w+u}b \equiv -\Big(\frac{v}{w}+\frac{u}{w+u}\Big)b \equiv \frac{uv+vw+wu}{vw}b \not\equiv 0 \pmod{p}.$$

Case (b).

$$\begin{aligned}\zeta^{2c}(\alpha^{f(s)}\xi_2)^{p^n} &\equiv \zeta^{2d'}(1+\zeta^2)^{f(s)}(\beta^{f(s)}\omega_2')^{p^n}\\ &\equiv \zeta^{b+2d'}(\zeta^{-1}+\zeta)^{f(s)}(\beta^{f(s)}\omega_2')^{p^n} \pmod{Aq},\end{aligned}$$

where

$$2c-(b+2d') \equiv \frac{2v}{u+v}b-b \equiv -b \not\equiv 0 \pmod{p}.$$

Case (c).

$$\begin{aligned}\zeta^{2d}(1+\zeta^2)^{f(s)}(\alpha^{f(s)}\omega_2)^{p^n} &\equiv \zeta^{b+2d}(\zeta^{-1}+\zeta)^{f(s)}(\alpha^{f(s)}\omega_2)^{p^n}\\ &\equiv \zeta^{2c'}(\beta^{f(s)}\xi_2')^{p^n} \pmod{Aq},\end{aligned}$$

where

$$b+2d-2c' \equiv b-\frac{2u}{w+u}b \equiv -b \not\equiv 0 \pmod{p}.$$

In every case, each term of the congruence modulo Aq is prime to Aq from Lemma 5. Hence we obtain (4) by Lemma 4.

(ix) Let $r|\alpha^2+\beta\gamma$ and $\lambda\nmid\alpha(\beta-\gamma)(\alpha^2+\beta\gamma)$. From the equation $(\alpha+\zeta^k\beta)\times$ $\times(\alpha+\zeta^{-k}\gamma) = \alpha^2+\beta\gamma+\zeta^{-k}\alpha(\gamma+\zeta^{2k}\beta)$, we have

$$\begin{aligned}&\Big(\big((\alpha+\zeta^k\beta)(\alpha+\zeta^{-k}\gamma)\big)^{p^n-1}(\alpha+\zeta^{2k}\beta)(\alpha+\zeta^{-2k}\gamma)\Big)^{f(s)}\\ &\qquad\equiv \zeta^{-bk}\big(\alpha^{p^n}(\gamma+\zeta^{2k}\beta)^{p^n-1}(\gamma+\zeta^{4k}\beta)\big)^{f(s)} \pmod{Aq}.\end{aligned}$$

We get the following congruences from Lemma 3 according to the three cases: (a) $\lambda\nmid\beta\gamma$ with $k=1$, (b) $\lambda|\beta$ with $k=2$, (c) $\lambda|\gamma$ with $k=2$.

Case (a).

$$\zeta^{c+c'}(\xi_1\xi'_{-1})^{p^n} \equiv \zeta^{-b+2c''}(\alpha^{f(s)}\xi''_2)^{p^n} \pmod{Aq},$$

where

$$c+c'+b-2c'' \equiv \frac{v}{u+v}b-\frac{w}{u+w}b+b-\frac{2v}{w+v}b \equiv \left(-\frac{v}{w}+\frac{w}{v}+\frac{w-v}{w+v}\right)b$$
$$\equiv \left(\frac{w^2-v^2}{vw}-\frac{w-v}{u}\right)b \equiv (w-v)\left(\frac{u(v+w)-vw}{uvw}\right)b$$
$$\equiv \frac{(v-w)(u^2+vw)}{uvw}b \not\equiv 0 \pmod{p}.$$

Case (b).

$$\zeta^{2c+2d'}(1+\zeta^2)^{f(s)}(\xi_2\omega'_{-2})^{p^n} \equiv \zeta^{b+2c+2d'}(\zeta^{-1}+\zeta)^{f(s)}(\xi_2\omega'_{-2})^{p^n}$$
$$\equiv \zeta^{-2b+4c''}(\alpha^{f(s)}\xi''_4)^{p^n} \pmod{Aq},$$

where

$$3b+2c+2d'-4c'' \equiv 3b+\frac{2v}{u+v}b-\frac{4v}{w+v}b \equiv 3b \not\equiv 0 \pmod{p}.$$

Case (c).

$$\zeta^{2d+2c'}(1+\zeta^2)^{f(s)}(\omega_2\xi'_{-2})^{p^n} \equiv \zeta^{b+2d+2c'}(\zeta^{-1}+\zeta)^{f(s)}(\omega_2\xi'_{-2})^{p^n}$$
$$\equiv \zeta^{-2b+4c''}(\alpha^{f(s)}\xi''_4)^{p^n} \pmod{Aq},$$

where

$$3b+2d+2c'-4c'' \equiv 3b-\frac{2w}{u+w}b-\frac{4v}{w+v}b \equiv -b \not\equiv 0 \pmod{p}.$$

We note that each term of the congruence modulo Aq in every case is prime to Aq from Lemma 5, and $p \geqslant 5$. Therefore (4) holds by Lemma 4. Note that we need the condition $\lambda \nmid \alpha$ in (ix). In fact, if $\lambda | \alpha$, then we have

$$\zeta^{c+c'}(\xi_1\xi'_{-1})^{p^n} \equiv \zeta^{-b+2d''}(1+\zeta^2)^{f(s)}(\alpha^{f(s)}\omega''_2)^{p^n}$$
$$\equiv \zeta^{2d''}(\zeta^{-1}+\zeta)^{f(s)}(\alpha^{f(s)}\omega''_2)^{p^n} \pmod{Aq}$$

with $k=1$, but $c+c'-2d'' \equiv \frac{v}{u+v}b-\frac{w}{u+w}b \equiv 0 \pmod{p}$. This completes the proof of Theorem 2.

Remark. We use the condition $m \leqslant n$ only to prove Lemma 3. If we further assume that $(\alpha, \beta)=1$, then Lemma 3 is also valid for $m>n$, and so is Theorem 2. For, in that case, if $\lambda \nmid \gamma$, we have $A(\alpha+\zeta^i\beta) = \mathfrak{B}_i^{p^m}$ from (5) since $\alpha+\zeta^i\beta$ are pairwise relatively prime. If $\lambda | \gamma$, we have $A(\alpha+\zeta^i\beta) = A\lambda^{e_i}\mathfrak{B}_i^{p^m}$ by the similar argument.

Proof of Theorem 1. Our assertion follows immediately from Theorem 2 and Remark. The conditions (i), (iii) and (iv) are the same things as (v), (viii) and (ix) respectively. If $q|r|x^2-y^2$ with a prime q, then we have $q|x+y$ or $q|x-y$. So the condition (ii) follows from (vi), (vii). We notice that the first half of Theorem 1 is valid for every m and n as mentioned in Remark since $(x, y)=1$, and that (1) has no solutions in $\boldsymbol{Z}$ if $p=3$.

Corollary 1. *Under the same conditions as in Theorem, the congruence* (2) *also holds for modulo* p^{2n}.

Corollary 2. *If there exist* $x, y, z \in \boldsymbol{Z}$ *satisfying* (1) *with* $(x, y, z)=1$, $p \nmid xyz(x-y)$, *then* $2^{p-1} \equiv 1$, $3^{p-1} \equiv 1 \pmod{p^{m+n}}$ *hold.*

Proof. One of the integers x, y, x^2-y^2 is divisible by 2, and one of them by 3. Hence we get the assertion from Theorem 1.

Corollary 3. *If the equation* (1) *has a solution* $x, y, z \in \boldsymbol{Z}$ *with* $(x, y, z)=1$, $p \nmid xyz$ *when* $m=n$, *then we have* $2^{p-1} \equiv 1$, $3^{p-1} \equiv 1 \pmod{p^{2n}}$.

Proof. One of the integers x, y, z is even. Hence we have $2^{p-1} \equiv 1 \pmod{p^{2n}}$ from Theorem 1. If $3|xyz$, then $3^{p-1} \equiv 1 \pmod{p^{2n}}$ holds from Theorem 1. Assume that $3 \nmid xyz$, then x^2-y^2, y^2-z^2 and z^2-x^2 are divisible by 3 and one of them is not divisible by p, otherwise we have $x \equiv y \equiv z \pmod{p}$ and $3x \equiv 0 \pmod{p}$, which contradicts to the assumption since $p \neq 3$. Hence we have $3^{p-1} \equiv 1 \pmod{p^{2n}}$ from Theorem 1.

Acknowledgement. The author wishes to thank Professor I. Yamaguchi for his kind advice and encouragement.

References

[1] P. Furtwängler, *Letzter Fermatschen Satz und Eisensteins'ches Reziprozitätsgesetz*, Sitzungsber. Akad. d. Wiss. Wien. Abt. IIa, 121 (1912), pp. 589–592.

[2] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser, A, I, 33 (1946), 60 p.

[3] — *Some extensions of criteria concerning singular integers in cyclotomic fields*, Ann. Acad. Sci. Fenn. Ser, A, I, 49 (1948), 15 p.

[4] J. McDonnell, *New criteria associated with Fermat's last theorem*, Bull. Amer. Math. Soc. 36 (1930), pp. 553–558.

[5] M. Moriya, *Über die Fermatsche Vermutung*, J. Reine Angew. Math. 169 (1933), pp. 92–97.

[6] P. Ribenboim, *13 Lectures on Fermat's last theorem*, Springer-Verlag, 1979.

[7] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, 1982.

DEPARTMENT OF MATHEMATICS
SCIENCE UNIVERSITY OF TOKYO
Tokyo, Japan

Received on 14. 12. 1982
and in revised form on 6. 3. 1984 (1333)