Mem. Fac. Educ. Ehime Univ.,Nat. Sci., Vol. 14, No. 1 35～40 (1993)

Fermat's Last Theorem over Algebraic Number Fields

Toshiaki OKAMOTO

Department of Mathematics, Faculty of Education
Ehime University, Matsuyama, 790, Japan
(Received April 13, 1993)

Abstract

If Fermat's equation $\alpha^{\ell}+\beta^{\ell}+\gamma^{\ell}=0$, *g.c.d.*$(\alpha\beta\gamma,\ \ell)=1$ *has solutions, then a criterion is given, where* α, β, γ *are integers of a certain algebraic number field.*

1. Introduction

Following notations will be used :

Let ℓ be a fixed odd prime unmber, $k=\mathbf{Q}(\zeta)$ be the cyclotomic number field defined by $\zeta=\exp(2\pi i/\ell)$, E be an algebraic number field such that its degree is n, g.c.d.$(n,\ \ell)=1$ and its discrimiant is prime to ℓ. Moreover let $K=kE$, $\lambda=1-\zeta$ the prime ideal in k dividing ℓ, and

$$\mathbf{1}_a(M)=\left.\frac{d^a\log M(e^v)}{dv^a}\right|_{v=0}\ (a=1,\ \cdots,\ \ell-2),\ \mathbf{1}_{\ell-1}(M)=\left.\frac{d^{\ell-1}\log M(e^v)}{dv^{\ell-1}}\right|_{v=0}+\frac{M(1)-1}{\ell}$$

Kummer's logarithmic differential quotients of M.

Now, Fermat's cubic over quadratic number fields studied by R. Fueter[3], W. burnside[2], A. Aigner[1] and others. And they established many beautiful theorems.

In this paper we shall investigate general Fermat's equation

(1) $$\alpha^{\ell}+\beta^{\ell}+\gamma^{\ell}=0,\ \text{g.c.d.}(\alpha\beta\gamma,\ \ell)=1,$$

where α, β, γ are integers of K.

2. The case of cyclic number field E

In this section let ℓ be a prime ideal or completely decomposed in E.

The purpose of this section is to prove following theorem which is a generalization of Vandiver's theorem[7].

Theorem 1. *Suppose that there exist numbers ε_i $(i=1, \cdots, n-1)$ of K such that*

(*a*) *principal ideal (ε_i) is ℓ th power of an ideal in K,*

(*b*) $\varepsilon_i \equiv 1 \pmod{\ell}$,

(*c*) $\varepsilon_1^{a_1} \cdots \varepsilon_{n-1}^{a_{n-1}} \equiv 1 \pmod{\ell\lambda}$ *if and only if* $a_i \equiv 0 \pmod{\ell}$ *for all* $i=1, \cdots, n-1$,

(*d*) $N\varepsilon_i \equiv 1 \pmod{\ell\lambda}$, *where N denotes the relative norm with respect to K/k.*

Besides, if Fermat's equation (1) *has solutions, then we have*

$$f_a(t) S_E\{\mathbf{1}_{\ell-a}(M)\} \equiv 0 \pmod{\ell}, \quad a=2, \cdots, \ell-2$$

and

$$f_{\ell-1}(t) \equiv 0 \pmod{\ell},$$

where

$$f_a(t) = \sum_{m=1}^{\ell-1} m^{a-1} t^m,$$

$\alpha \equiv \alpha_0$, $\beta \equiv \beta_0$, $\gamma \equiv \gamma_0 \pmod{\lambda}$ *(α_0, β_0, γ_0 are integers of E), S_E is the absolute trace from E, t denotes a rational integer (We are able to take it so.) such that*

$$-t \equiv \frac{\beta_0}{\alpha_0}, \frac{\alpha_0}{\beta_0}, \frac{\beta_0}{\gamma_0}, \frac{\gamma_0}{\beta_0}, \frac{\alpha_0}{\gamma_0} \text{ or } \frac{\gamma_0}{\alpha_0} \pmod{\ell},$$

and $M \equiv 1 \pmod{\lambda}$ such that the principal ideal (M) is ℓ th power of an ideal in K.

In order to prove theorem 1 we need following lemmas.

Lemma 1. *Let ℓ be a prime ideal in E, and assume that α_i $(i=1, \cdots, m)$ are elements of E, such that the determinant $\det(\alpha_i^{\sigma^j})$ is congruent to 0 modulo ℓ, where $i=1, \cdots, m$, $j=0, \cdots, m-1$ and σ is a generator of the Galois group with respect to extention $E/\mathbf{Q}$. Then $\alpha_1, \cdots, \alpha_m$ are linear dependent over the residue field $\mathbf{Z}/\ell\mathbf{Z}$ ($\mathbf{Z}$ denotes the ring of rational integers.) and the reverse is true.*

Proof. We may assume that g.c.d.$(\alpha_i, \ell) = 1$ $(i=1, \cdots, m)$. We will prove above lemma by induction on m. Let $m=1$ then the above is ovbious. Next assume that above is true for $m-1$. And we put $\alpha_i = \alpha_1 \beta_{i-1}$ $(i=2, \cdots, m)$, then $\det(\beta_i^{\sigma^j}) \equiv 0 \pmod{\ell}$ with $\beta_0 = 1$, so that we have $\det(\gamma_i^{\sigma^j}) \equiv 0 \pmod{\ell}$ $(i=1, \cdots, m-1 : j=0, \cdots, m-2)$, where $\gamma_i = \beta_i^{\sigma} - \beta_i$. Now if $\gamma_i \equiv 0 \pmod{\ell}$, then we have $\alpha_{i+1} \equiv c\alpha_i \pmod{\ell}$ for some rational integer c, or if g.c.d.$(\gamma_i, \ell) = 1$ $(i=1, \cdots, m-1)$, then we have from the hypothesis of induction $\sum_{i=1}^{m-1} c_i \gamma_i \equiv 0 \pmod{\ell}$ with some rational integers c_i $(i=1, \cdots, m-1)$ and some c_i is not congruent to 0 modulo ℓ. This concludes the proof. The revese is obvious.

Following lemma is obvious.

Lemma 2. *Let ℓ be completely decomposed in E, and assume that α_i $(i=1, \cdots, n-1)$ are elements of E, such that the determinant* $\det(\alpha_i^{\sigma^j})$ *is congruent to* 0 *modulo* $\mathfrak{L}$ *and* $S_E(\alpha_i)$ $\equiv 0 \pmod{\ell}$, *where* $i=1, \cdots, n-1, j=0, \cdots, n-2$, σ *is the same meaning as in lemma* 1 *and* $\mathfrak{L}$ *is a prime ideal in E dividing* ℓ. *Then* $\alpha_1, \cdots, \alpha_{n-1}$ *are linear dependent over the residue field* $\mathbf{Z}/\ell\mathbf{Z}$.

Lemma 3. *With the same assumptions as in above theorem we have*

$$\delta^\sigma \equiv \delta \pmod{\lambda}$$

where $\delta=\beta/(\alpha+\beta)$ *and* σ *is the same meaning as in lemma* 1.

Proof. We put $A=(\alpha+\zeta\beta)/(\alpha+\beta)=1-\delta\lambda$, then we have from Hasse[4]

$$S_E\left\{\sum_{a=1}^{\ell-1}(-1)^a \mathbf{1}_a(\varepsilon_i)\,\mathbf{1}_{\ell-a}(A)\right\}\equiv 0 \pmod{\ell},$$

so that

$$S_E\{\alpha_i(1)\delta(1)\}\equiv 0 \pmod{\ell},$$

where $\varepsilon_i=1+\alpha_i\ell$ $(\alpha_i=\alpha_i(\zeta))$. Therefore we have

$$\sum_{j=0}^{n-1}\alpha_i(1)^{\sigma^j}\,\delta(1)^{\sigma^j}\equiv 0 \pmod{\ell}, \quad i=1, \cdots, n-1.$$

Now, if $\sum_{i=1}^{n-1} c_i\,\alpha_i(1)\equiv 0 \pmod{\ell}$, then

$$\varepsilon_1^{c_1}\cdots\varepsilon_{n-1}^{c_{n-1}}\equiv\prod_{i=1}^{n-1}(1+c_i\,\alpha_i\ell)\equiv 1 \pmod{\ell\lambda},$$

where c_i are rational integers. By the condition (c) we have

$$c_1\equiv\cdots\equiv c_{n-1}\equiv 0 \pmod{\ell}.$$

Hence we have from lemma 2, 3

$$\delta^\sigma\equiv\delta \pmod{\lambda}.$$

Next lemma is due to Morishima[6].

Lemma 4. *Suppose that α, β are integers of K and* g.c.d.$(\alpha+\beta, \ell)=1$. *Then we have*

$$\mathbf{1}_a\left(\frac{\alpha+\zeta^i\beta}{\alpha+\beta}\right)\equiv\sum_{\nu=0}^{a} i^\nu x_{a,\nu}(\alpha, \beta) \pmod{\ell},$$

$$(a=1, \cdots, \ell-2;\ i=0, 1, \cdots, \ell-1)$$

where $x_{a,\nu}(\alpha, \beta)$ *is an integer of E and independent of i.*

Moreover if

$$\alpha\equiv\alpha_0,\ \beta\equiv\beta_0 \pmod{\lambda},$$

then we have

$$x_{a,a}(\alpha,\ \beta)\equiv\mathbf{1}_a\left(\frac{\alpha_0+\zeta\beta_0}{\alpha_0+\beta_0}\right)\ (\mathrm{mod.}\ \ell)$$
$$(a=1,\ \cdots,\ \ell-2)$$

where α_0, β_0 *are integers of* E.

Proof. We have

$$\mathbf{1}_a\left(\frac{\alpha+\zeta^i\beta}{\alpha+\beta}\right)=\left[-\sum_{n=1}^{a}\frac{\delta(e^v)^n}{n}(1-e^{iv})^n\right]_{v=0}^{(a)}$$
$$=\left[-\sum_{n=1}^{a}\frac{\delta(e^v)^n}{n}\sum_{r=0}^{n}{}_nC_r(-1)^r e^{irv}\right]_{v=0}^{(a)}$$
$$=\sum_{s=0}^{a}i^s\sum_{n=1}^{a}\sum_{r=0}^{n}{}_nC_r\,{}_aC_s\frac{(-1)^{r+1}r^s}{n}[\delta(e^v)^n]_{v=0}^{(a-s)},$$

where $[f(e^v)]_{v=0}^{(m)}=\left.\dfrac{d^m f(e^v)}{dv^m}\right|_{v=0}$. Hence we have

$$\mathbf{1}_a\left(\frac{\alpha+\zeta^i\beta}{\alpha+\beta}\right)\equiv\sum_{\nu=0}^{a}i^\nu\,x_{a,\nu}(\alpha,\ \beta)\ (\mathrm{mod.}\ \ell).$$

Since

$$\mathbf{1}_a\left(\frac{\alpha_0+\zeta\beta_0}{\alpha_0+\beta_0}\right)\equiv\mathbf{1}_a\ (1-\delta(1)\lambda)$$
$$\equiv\left[-\sum_{n=1}^{a}\frac{\delta(1)^n}{n}(1-e^v)^n\right]_{v=0}^{(a)}$$
$$\equiv\sum_{n=1}^{a}\frac{\delta(1)^n}{n}\sum_{r=0}^{n}{}_nC_r(-1)^{r+1}r^a\ (\mathrm{mod.}\ \ell)$$

we have

$$\mathbf{1}_a\left(\frac{\alpha_0+\zeta\beta_0}{\alpha_0+\beta_0}\right)\equiv x_{a,a}(\alpha,\ \beta)\ (\mathrm{mod.}\ \ell).$$

We now are able to prove theorem 1.

Proof of theorem 1. Let

$$A_i=\frac{\alpha+\zeta^i\beta}{\alpha+\beta}\ (i=0,\ \cdots,\ \ell-1).$$

Then we have from Hasse[4]

$$S_E\left\{\sum_{a=1}^{\ell-1}(-1)^a\,\mathbf{1}_a\ (A_i^{S^j})\mathbf{1}_{\ell-a}(M)\right\}\equiv 0\ (\mathrm{mod.}\ \ell),$$

where $S=(\zeta\rightarrow\zeta^r)$ is the substitution and r is a primitive root of mod. ℓ. And hence

$$\sum_{a=1}^{\ell-1}r^{aj}\,S_E\{(-1)^a\,\mathbf{1}_a(A_i)\mathbf{1}_{\ell-a}(M)\}\equiv 0\ (\mathrm{mod.}\ \ell),$$

accordingly

$$S_E\{\mathbf{1}_a\ (A_i)\mathbf{1}_{\ell-a}(M)\}\equiv 0\ (\mathrm{mod.}\ \ell),\quad a=1,\ \cdots,\ \ell-1.$$

We also have from lemma 4

$$\sum_{\nu=0}^{a} i^{\nu}\ S_E\{x_{a,\nu}(\alpha,\ \beta)\mathbf{1}_{\ell-a}(M)\}\equiv 0\ (\mathrm{mod.}\ \ell)$$
$$(a=1,\ \cdots,\ \ell-2;\ i=0,\ \cdots,\ \ell-1)$$

and hence

$$S_E\{x_{a,\nu}(\alpha,\ \beta)\ \mathbf{1}_{\ell-a}\ (M)\}\equiv 0\ (\mathrm{mod.}\ \ell).$$
$$(a=1,\ \cdots,\ \ell-2;\ \nu=0,\ \cdots,\ a)$$

In particular we have

$$S_E\{x_{a,a}(\alpha,\ \beta)\ \mathbf{1}_{\ell-a}\ (M)\}\equiv 0\ (\mathrm{mod.}\ \ell)$$

and from lemma 4

$$S_E\ \left\{\mathbf{1}_a\left(\frac{\alpha_0+\zeta\beta_0}{\alpha_0+\beta_0}\right)\mathbf{1}_{\ell-a}\ (M)\right\}\ \equiv\ 0\ (\mathrm{mod.}\ \ell).$$

Hence we have from lemma 3 and Hasse[5]

$$f_a(t)S_E\{\mathbf{1}_{\ell-a}\ (M)\}\equiv 0\ (\mathrm{mod.}\ \ell),\quad a=2,\ \cdots,\ \ell-2.$$

Now, we have from Fermat's relation (1)

$$\alpha_0+\beta_0+\gamma_0\equiv 0\ (\mathrm{mod.}\ \ell)$$

and

$$(\alpha_0+\beta_0)^{\ell}\equiv \alpha_0^{\ell}+\beta_0^{\ell}\ (\mathrm{mod.}\ \ell^2).$$

Hence

$$f_{\ell-1}(t)\equiv 0\ (\mathrm{mod.}\ \ell).$$

3. The case of Abelian number field E

In this section with E we denote an absolute Abelian number field such that the invariant of Galois group with respect to $E/\mathbf{Q}$ is $\{n_1,\ \cdots,\ n_r\}$ $(n_{i-1}|n_i,\ i=2,\ \cdots,\ r)$ and $(\varphi(n^{r-1}),\ \ell)=1$, where φ denotes Euler's function.

Lemma 5. *If $E=E_1\cdots E_r$, then let ℓ be a prime ideal or completely decomposed in E_i $(i=1,\ \cdots,\ r)$. And suppose that there exist numbers $\varepsilon(i,\ j_i)$ $(j_i=1,\ \cdots,\ m_i-1)$ in each composite fields kE_i' such that*

(*a*) *the principal ideal $\varepsilon(i,\ j_i)$ is ℓ th power of an ideal in kE_i',*

(*b*) $\varepsilon(i,\ j_i)\equiv 1\ (\mathrm{mod.}\ \ell)$,

(*c*) $\varepsilon(i,\ 1)^{a_1}\cdots\varepsilon(i,\ m)^{a_m}\equiv 1\ (\mathrm{mod.}\ \ell\lambda)$ *(where $m=m_i-1$) if and only if $a_j\equiv 0\ (\mathrm{mod.}\ \ell)$ for all $j=1,\ \cdots,\ m$,*

(*d*) $N_i\varepsilon(i,\ j_i)\equiv 1\ (\mathrm{mod.}\ \ell\lambda)$,

where E_i, E_i', N_i denote the cyclic number field with degree n_i, any subfield with degree m_i of E_i and the relative norm with respect to kE_i'/k, respectively. Besides, if Fermat's equation (1) has solutions, we have

$$\delta^{\sigma}\equiv\delta\ (\mathrm{mod.}\ \ell),$$

where $\delta=\beta/(\alpha+\beta)$ and σ denotes any element of Galois group with respect to $E/\mathbf{Q}$.

Proof. We shall prove the above by induction on degree n. Let $n=1$, 2, then we have the above by lemma 3. Now, assume that lemma 5 is true from 1 to $n-1$. Then we have from Hasse[4] and the hyposeses of induction

$$\sum_{i=0}^{p-1} \delta^{\sigma^i} \equiv c \pmod{\lambda},$$

where p, $\sigma(\neq 1)$, c denote any prime factor of n, any element with order p of Galois group with respect to $E/\mathbf{Q}$ and a rational integer, respectively. Accordingly, if $r=1$, we have from lemma 3 $\delta^{\sigma} \equiv \delta \pmod{\lambda}$, or if $r>1$, then we have

$$p\delta - \sum_{i,j,k=0}^{p-1} \delta^{\sigma^{ik}\tau^{jk}} + \sum_{i,j=0}^{p-1} \sum_{k=1}^{p-1} \delta^{\sigma^{ik}\tau^{jk}} \equiv c \pmod{\lambda}$$

where σ, $\tau(\neq 1)$ denote any independent elements (*i.e.* $\sigma^i\tau^j=1$ if and only if $\sigma^i=\tau^j=1$.) with order p of Galois group with respect to $E/\mathbf{Q}$ and c is a rational integer. Hence we have

$$\delta^{\sigma} \equiv \delta \pmod{\lambda}.$$

By lemma 5 we can prove follwoing theorem.

Theorem 2. *Under the same assumptions as in lemma* 5 *we have the congruences of theorem* 1.

Remark. *If* ℓ *is completely decomposed over Galois number field* E, *then we can prove theorem* 1.

References

[1] A. Aigner, Die kubische Fermatgleichung in quadratischen Körpern, J. reine angew. Math. **195** (1956), 3–17.

[2] W. Burnside, On the rational solutions $X^3+Y^3+Z^3=0$ in quadratic fields, Proc. London Math. Soc. **14** (1915), 1–4.

[3] R. Fueter, Die Diophantische Gleichung $\xi^3+\eta^3+\zeta^3=0$, Sitzungsbericht Heidelberg Akad. d. Wiss. 1913, 25. Abh. 25pp.

[4] H. Hasse, Das allgemeine Reziprozitätsgesetz der ℓ – ten Potenzreste für beliebige, zu ℓ prime Zahlen in gewissen Oberkörpern des Körpers der ℓ – ten Einheitswurzeln, J. reine angew. Math. **154** (1925), 199–214.

[5] H. Hasse, Zahlbericht, Teil II, Physica-Verlag·Würzburg-Wien, 1970.

[6] T. Morishima, Über die Fermatsche Vermutung, XI, Jpn. Math. **11** (1934), 241–252.

[7] H. S. Vandiver, Laws of reciprocity and the first case of Fermat's last theorem, Proc. Nat. Acad. Scie. U.S.A. Vol. **11** (1925), 292–298.