Bull. Fac. Educ. Ehime Univ., Nat. Vol. 21, No. 1 1~6 (2000)

Fermat-like Diophantine Equations

Toshiaki OKAMOTO

Department of Mathematics, Faculty of Education
Ehime University, Matsuyama, 790-8577, Japan
(Received June 1, 2000)

Abstract

We shall give criteria on certain diophantine equations concerning Fermat-like equaiton over algebraic number fields.

Keywords: diophantine equaitons, Fermat.

1 Introduction

The following notations will be used:
Let ℓ be a fixed odd prime number, $\mathbf{Q}$ be the rational number field, $\mathbf{Z}$ be the rational integer ring, $k = \mathbf{Q}(\zeta)$ be the cyclotomic number field defined by $\zeta = \exp(2\pi i/\ell)$, E be an algebraic number field whose discriminant is not divisible by ℓ, S_E be the trace with respect to $E/\mathbf{Q}$. Moreover let $K = kE$, $\lambda = 1 - \zeta$ be the prime ideal in k dividing ℓ,

$$\begin{aligned} \mathrm{l}_a(M) &= \left.\frac{d^a \log M(e^v)}{dv^a}\right|_{v=0}, \quad (a = 1, ..., \ell - 2), \\ \mathrm{l}_{\ell-1}(M) &= \left.\frac{d^{\ell-1} \log M(e^v)}{dv^{\ell-1}}\right|_{v=0} + \frac{M(1)-1}{\ell}, \end{aligned}$$

be Kummer's logarithmic differential quotients of $M = M(\zeta)$
and

$$\left(\frac{M}{N}\right) \text{ be the } \ell\text{-th power residue symbol.}$$

2 A Proposition

In this section we shall give a proposition with respect to next diophantine equations :

$$\alpha^\ell + \beta^\ell + \gamma^\ell = 0, \quad \gcd(\alpha\beta\gamma, \ell) = 1, \tag{1}$$

and

$$\alpha^\ell + \beta^\ell = \kappa\gamma^\ell, \quad \gcd(\alpha\beta\gamma\kappa,\ \ell\ ) = \gcd(\alpha, \beta, \kappa) = 1, \tag{2}$$

where $\alpha,\ \beta,\ \gamma,\ \kappa$ are integers of K. And assume that

$$\pi^{\ell^f - 1} \equiv 1 \pmod{\ell}, \ \pi \text{ is an integer of } K,$$

$$\pi^{\ell^f - 1} = 1 + \alpha'\ell,$$

$$\alpha + \beta \equiv 0 \pmod{\kappa} \text{ for (2).}$$

Next, let

$$A = \frac{\alpha+\zeta^2\beta}{\alpha+\zeta\beta},$$

$$\alpha \equiv \alpha_0,\ \beta \equiv \beta_0,\ \alpha' \equiv \alpha'_0 \pmod{\lambda},$$

where $\alpha_0,\ \beta_0,\ \alpha'_0$ are integers of E.

In the previous paper [6] we described next lemma :

Lemma *Suppose that $\alpha,\ \beta$ are integers of K and $\gcd(\alpha+\beta,\ell)=1$. Then we have*

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

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

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

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

then we have

$$x_{a,a}(\alpha,\beta) \equiv \mathrm{l}_a(\frac{\alpha_0+\zeta\beta_0}{\alpha_0+\beta_0}) \pmod{\ell},$$

$$(\ a=1,\dots,\ell-2\ )$$

where $\alpha_0,\ \beta_0$ are integers of E.

From now on suppose that (1) or (2) holds. Then we have easily next proposition by using H.Hasse ([1], [2]) and the above lemma for the numbers A,π.

Proposition 1 (1) *If $\beta \equiv 0 \pmod{\pi}$ and $\gcd(\pi,\alpha)=1$, then*

$$S_E\left(\alpha'_0\frac{\beta_0}{\alpha_0+\beta_0}\right) \equiv 0 \pmod{\ell}.$$

(2) *If $\alpha-\beta \equiv 0 \pmod{\pi}$ and $\gcd(\pi,\alpha)=1$, then*

$$S_E(\alpha'_0) \equiv 2S_E\left(\alpha'_0\frac{\beta_0}{\alpha_0+\beta_0}\right) \pmod{\ell}.$$

(3) *If $\alpha+\beta \equiv 0 \pmod{\pi}$, $\gcd(\pi,\alpha)=1$ and $\pi \in E$, then*

$$S_E(\alpha'_0) \equiv 2S_E\left(\alpha'_0\frac{\beta_0}{\alpha_0+\beta_0}\right) \pmod{\ell}.$$

Proof. If $\beta \equiv 0 \pmod{\pi}$ and $\gcd(\pi,\alpha+\beta)=1$, then since $A \equiv 1 \pmod{\pi}$ and A is ℓ-th power of an ideal in K we have

$$\left(\frac{A}{\pi}\right)=1 \text{ and } \left(\frac{\pi^{\ell^f-1}}{A}\right)=1.$$

Hence from the reciprocity law we have

$$1=\left(\frac{A}{\pi}\right)=\left(\frac{\pi^{\ell^f-1}}{A}\right)\left(\frac{A}{\pi^{\ell^f-1}}\right)^{-1}.$$

Accordingly

$$S_E(\alpha'_0\mathrm{l}_1(A)) \equiv S_E\left(\alpha'_0\mathrm{l}_1\left(\frac{\alpha+\zeta^2\beta}{\alpha+\beta}\right)-\alpha'_0\mathrm{l}_1\left(\frac{\alpha+\zeta\beta}{\alpha+\beta}\right)\right) \equiv 0 \pmod{\ell},$$

and since

$$\mathrm{l}_1\left(\frac{\alpha+\zeta^2\beta}{\alpha+\beta}\right) \equiv x_{1,0}(\alpha,\beta)+2x_{1,1}(\alpha,\beta) \pmod{\ell},$$
$$\mathrm{l}_1\left(\frac{\alpha+\zeta\beta}{\alpha+\beta}\right) \equiv x_{1,0}(\alpha,\beta)+x_{1,1}(\alpha,\beta) \pmod{\ell},$$

we have

$$S_E\left(\alpha_0'\frac{\beta_0}{\alpha_0+\beta_0}\right)\equiv 0 \pmod{\ell}.$$

When $\pi \mid (\alpha-\beta)$ and $\gcd(\pi,\alpha)=1$, since

$$A\equiv\frac{1+\zeta^2}{1+\zeta}=\varepsilon \pmod{\pi}$$

is a unit we have

$$\left(\frac{A}{\pi}\right)=\left(\frac{\varepsilon}{\pi}\right)=\left(\frac{\varepsilon}{\pi^{\ell^f-1}}\right)^{-1}\left(\frac{\pi^{\ell^f-1}}{\varepsilon}\right)=\zeta^L, L=\frac{1}{2}S_E\left(\alpha_0'\right).$$

On the other hand from

$$\left(\frac{A}{\pi}\right)=\left(\frac{A}{\pi^{\ell^f-1}}\right)^{-1}=\left(\frac{\pi^{\ell^f-1}}{A}\right)\left(\frac{A}{\pi^{\ell^f-1}}\right)^{-1}$$

we have the desired result.

If $\pi \mid (\alpha+\beta)$, $\pi\in E$, $\gcd(\pi,\alpha)=1$, since $A\equiv 1+\zeta=\varepsilon \pmod{\ell}$ is a unit and

$$\delta=2^{-1}\varepsilon=1-\frac{1}{2}\lambda,$$

we have

$$\left(\frac{A}{\pi}\right)=\left(\frac{\varepsilon}{\pi}\right)=\left(\frac{2^{-1}}{\pi}\right)\left(\frac{\varepsilon}{\pi}\right)=\left(\frac{\delta}{\pi}\right)=\left(\frac{\delta}{\pi^{\ell^f-1}}\right)^{-1}$$
$$=\left(\frac{\pi^{\ell^f-1}}{2^{-1}}\right)\left(\frac{\pi^{\ell^f-1}}{\varepsilon}\right)\left(\frac{\delta}{\pi^{\ell^f-1}}\right)^{-1}=\left(\frac{\pi^{\ell^f-1}}{\delta}\right)\left(\frac{\delta}{\pi^{\ell^f-1}}\right)^{-1}=\zeta^L,\ L\equiv\frac{1}{2}S_E\left(\alpha_0'\right) \pmod{\ell}.$$

On the other hand since

$$\left(\frac{A}{\pi}\right)=\left(\frac{A}{\pi^{\ell^f-1}}\right)^{-1}=\left(\frac{\pi^{\ell^f-1}}{A}\right)\left(\frac{A}{\pi^{\ell^f-1}}\right)^{-1}=\zeta^R,\ R\equiv S_E\left(\alpha_0'\frac{\beta_0}{\alpha_0+\beta_0}\right) \pmod{\ell},$$

we have the desired result. □

3 The Equation $x^3+y^3=z^\ell$

In this section we treat the next diophantine equation over the ring $\mathbf{Z}$:

$$x^3+y^3=z^\ell,\ xyz\neq 0,\ \gcd(x,y)=1, \tag{3}$$

where ℓ is a fixed prime number. Mordell [4] showed solutions of the above for $\ell=2$, and when $\ell>3$ Nagell [5] proved that the above has no solutions such that $y=\pm 1$.

We shall consider (3) for $\ell>3$.

In this subject let ρ be a fixed primitive cubic root of unity and $\lambda_0=1-\rho$.

If z is not divisible by 3 and $z\not\equiv 0 \pmod{\ell}$, then we have from (3)

$$x+y=c^\ell,\ x+y\rho=\alpha^\ell,\ \gcd(c\alpha,\ 3\ell)=1$$

where c,α are integers in $\mathbf{Q}$ and $\mathbf{Q}(\rho)$, respectively.
Accordingly we have

$$c^\ell+(\rho^\ell\alpha)^\ell+(\overline{\rho^\ell\alpha})^\ell=0,\ \gcd(c\alpha,3\ell)=1, \tag{4}$$

where $\overline{*}$ denotes the conjugate number of $*$.

In (4) let $\pi = \lambda_0$, and using (2) of proposition 1 we have

Theorem 1 *If* (3) *has solutions such that* $xy \not\equiv 0 \pmod{\ell^2}$, $z \not\equiv 0 \pmod{\ell}$ *and* $3 \not| z$, *then* $3^{\ell-1} \equiv 1 \pmod{\ell^2}$.

4 The Equation $x^4 - y^4 = z^\ell$

In this section we consider the next diophantine equation ove the ring $\mathbf{Z}$:

$$x^4 - y^4 = z^\ell,\ xyz \neq 0,\ \gcd(x, y) = 1, \tag{5}$$

where ℓ is a fixed prime number. Fermat and Euler proved that the above has no solutions for $\ell = 4$. Mordell [4] proved that the above has no solutions for $\ell = 2$.

In this subject let $i = \sqrt{-1}$ and $\lambda_0 = 1 - i$.

If z is odd and $z \not\equiv 0 \pmod{\ell}$, then we have from (5)

$$x - y = c^\ell,\ x + y = d^\ell,\ x + yi = \alpha^\ell,\ \gcd(cd\alpha, 2\ell) = 1,$$

where c, d and α are integers in $\mathbf{Q}$ and $\mathbf{Q}(i)$, respectively. Accordingly we have

$$c^\ell + (di^\ell)^\ell = \lambda_0 (i^\ell \alpha)^\ell,\ \gcd(cd\alpha, 2\ell) = 1. \tag{6}$$

In (6) let $\pi = \lambda_0$, and using (3) of proposition 1 we have

Theorem 2 *If* (5) *has solutions such that* $xy \not\equiv 0 \pmod{\ell^2}$, $z \not\equiv 0 \pmod{\ell}$ *and z is odd, then* $2^{\ell-1} \equiv 1 \pmod{\ell^2}$.

In 1993 H. Darmon[3] proved that

Theorem 3 *Suppose that the Shimura–Taniyama conjecture is true, and let* $\ell > 10$. *Then equation* (5) *has no solution if* $\ell \equiv 1 \pmod 4$, *and has no solution with z even.*

Recently, the above conjecture has been proved.

5 The Equation $y^2 = x^\ell + k$

In this section $E = \mathbf{Q}(\sqrt{k})$ be a quadratic field, where k is a rational integer. Moreover h, φ_E denote the class number of E and Euler's phi function over E, respectively. And we investigate the rational integer solutions of following hyperelliptic equation:

$$y^2 = x^\ell + k,\ \gcd(x, y) = 1, \tag{7}$$

where k is a negative rational integer, $\ell > 1$ be an odd, $\gcd(k, \ell) = 1$, $k \not\equiv 1 \pmod 8$, $\gcd(h, \ell) = 1$ and $\gcd(\varphi_E(2k), \ell) = 1$. Let $k = f^2 c$, $f > 0$, where c is the square free rational integer. Then $E = \mathbf{Q}(\sqrt{c})$.

(7) is called the Mordell equation[4] if $\ell = 3$.

Next theorem is due to Lebesgue(cf.[4], p.301).

Theorem 4 *Diophantine equation*

$$y^2 = x^p - 1,\ x > 1$$

has no solution, where p is an odd prime number.

If (7) has rational integer solutions x and y, then

$$(y + f\sqrt{c})(y - f\sqrt{c}) = x^\ell$$

and $\gcd(y + f\sqrt{c}, y - f\sqrt{c}) = 1$. Hence we have

$$y + f\sqrt{c} = \mathcal{A}^\ell \text{ and } y - f\sqrt{c} = \bar{\mathcal{A}}^\ell,$$

where $\mathcal{A}$ is an ideal of E and $\bar{\mathcal{A}}$ is the conjugate ideal of $\mathcal{A}$. Accordingly, when the class number of E is prime to ℓ we have

$$y + f\sqrt{c} = \alpha^\ell \text{ and } y - f\sqrt{c} = \bar{\alpha}^\ell,$$

where α is an integer of E and $\bar{\alpha}$ is the conjugate number of α. Hence we have

$$\alpha^\ell - \bar{\alpha}^\ell = 2f\sqrt{c}.$$

Next lemma is analogous to Morishima and Miyoshi[7].

Lemma. *$\alpha - \bar{\alpha}$ is divisible by $2f\sqrt{c}$.*

Proof. $(\alpha/\bar{\alpha})^\ell \equiv 1 \pmod{2f\sqrt{c}}$ and from the condition we have $\gcd(\varphi_E(2f\sqrt{c}), \ell) = 1$. Hence we have the lemma. □

We have next propositions:

Proposition 2 *If (7) has rational integer solutions x and y, then we can denote*

$$(a + f\sqrt{c})^\ell - (a - f\sqrt{c})^\ell = \pm 2f\sqrt{c}, \tag{8}$$

where a is a some rational integer.

Proof. From the lemma we have

$$\frac{\alpha - \bar{\alpha}}{2f\sqrt{c}} = \varepsilon,$$

where ε is a unit of E. Moreover $\bar{\varepsilon} = \varepsilon$, i.e. $\varepsilon = \pm 1$. Anyway, we can denote $\alpha = a \pm f\sqrt{c}$. □

From the above proposition we have

Proposition 3 *If the next polynomial with an indeterminante X*

$$F(X) = \left\{ \sum_{s=0}^{(\ell-1)/2} \binom{\ell}{2s+1} k^s X^{\ell-2s-1} \right\} \pm 1 \tag{9}$$

has no factor $X^2 - a^2$, then (7) has no rational integer solutions, where a is a rational integer.

In reverse

Proposition 4 *If (9) has a rational integer solution $X = a$, then*

$$y^2 = (a^2 - k)^\ell + k, \ \gcd(y, a^2 - k) = 1, \ \exists y \in \mathbf{Z}.$$

Proof. Since (8) holds, $(a + f\sqrt{c})^\ell = y \pm f\sqrt{c}$ for some rational integer y and from $F(a) = 0$ we have $\gcd(y, a^2 - k) = 1$. □

Hence we have

Theorem 5 *All solutions of (7) are obtained by $y^2 = (a^2 - k)^\ell + k$, where a is a rational integer solution of $F(X) = 0$.*

If $\ell = 3$, then $F(X) = 3X^2 + k \pm 1$. Hence

Example 1 *Let $\ell = 3$. If $-\frac{k-1}{3}$(when $k \equiv 1 \pmod 3$) or $-\frac{k+1}{3}$(when $k \equiv -1 \pmod 3$) is not square, then (7) has no solution.*

On the other hand, when $-\frac{k-1}{3}$ or $-\frac{k+1}{3}$ is square,

$$y^2 = \left(-\frac{4k-1}{3}\right)^3 + k = -\frac{k-1}{3} \cdot \left(\frac{8k+1}{3}\right)^2$$

or

$$y^2 = \left(-\frac{4k+1}{3}\right)^3 + k = -\frac{k+1}{3} \cdot \left(\frac{8k-1}{3}\right)^2,$$

respectively.

If $\ell = 5$, then $F(X^{\frac{1}{2}}) = 5X^2 + 10kX + k^2 \pm 1$. Hence

Example 2 *Let* $\ell = 5$. (7) *has solutions if and only if* $25k^2 - 5(k^2 \pm 1) = 20k^2 \pm 5 = 25b^2$ *and* $-k + b($*or* $-k - b)$ *is square for some rational integer* b.

By using a computer algebra system *MuPAD Light* we have next proposition.

Proposition 5 *For* $f = 1$, $-11 < c < -1$ *and prime numbers* $3 < \ell < 542$ *as in* (7), *the polynomial* (9) *is irreducible over* $\mathbf{Q}$, *accordingly* (7) *has no rational integer solution.*

References

[1] H. Hasse, Das allgemeine Reziprozitötsgesetz 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.

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

[3] H. Darmon, The equation $x^4 - y^4 = z^p$, C.R. Math. Rep. Acad. Sci. Canada, Vol.**15**,No.**6**(1993), 286 – 290.

[4] L. J. Mordell, Diophantine Equations, Academic Press, London and New York, 1969.

[5] T. Nagell, Des équations indéterminées $x^2+x+1 = y^n$ et $x^2+x+1 = 3y^n$. Norsk. Mat. Forenings Skr. Series I, **2**(1921), 12 – 14.

[6] T. Okamoto, Fermat's Last Theorem over Algebraic Number Fields, Mem. Fac. Educ. Ehime Univ., Nat. Sci., Vol. **14**, No.1(1993), 35-40.

[7] T. Morishima and T. Miyoshi, ON THE DIOPHANTINE EQUATION $x^p + y^p = cz^p$, Proc. Amer. Math. Soc. Vol.**16**, No.4(1965), 833 – 836.