113. On Certain Diophantine Equations in Algebraic Number Fields

By Mutsuo WATABE
Department of Mathematics, Keio University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1982)

1. Diophantine equations of the following type have been discussed by many authors.

Let K be an algebraic number field of some type (e.g. totally real, abelian over $\boldsymbol{Q}$, or "almost real" cf. [3]), α, β given roots of unity, and m a given natural number. Find the solutions of the equation:

(1) $$\xi^m+\alpha=\eta, \quad \xi\in K(\beta+\beta^{-1}), \quad \eta\in U_{K(\beta)},$$

where U_F will mean the group of units of the algebraic number field F. (Cf. [1]–[5]. E.g. it is shown in [3] that when K is almost real, $\alpha=\beta=-1$, $m\geqq 3$, $\xi\in U_K$, then the only possible solutions are given by ξ $=$a root of unity. This covers the results of [2], [5].)

We shall denote in the following the ring of integers of the field F by $\mathcal{O}_F$. p will mean an odd prime, and for any natural number n, ζ_n will mean a primitive n th root of unity.

Remark. From (1) follows immediately $\xi\in\mathcal{O}_{K(\beta+\beta^{-1})}$.

In this note, we prove the following three theorems:

Theorem A. *Suppose K to be totally real and $m=1$ in* (1).

(I) *If $\alpha=\beta=\zeta_4$, then $\xi=0$.*

(II) *If $\alpha=\beta=\zeta_p$, then $\xi=(\zeta_p^{c-1}-\zeta_p)/(1-\zeta_p^c)$ with $c\in\{1,2,\cdots,p-1\}$.*

(III) *If $\alpha=\beta=\zeta_p$, K is moreover non-abelian and of prime degree over $\boldsymbol{Q}$, then $\xi=0$ or 1.*

Remark. To Theorem A may be associated a problem posed by Julia Robinson, cited in [4], asking for possibilities of expressing 1 as the difference of two units in an algebraic number field.

Theorem B. *Suppose K to be totally real, $m\geqq 2$, $\alpha=\beta=1$, $\eta\neq 1$. Then the only possible solutions of* (1) *are given by $\xi=$a root of unity.*

Theorem C. *Suppose $K/\boldsymbol{Q}$ to be abelian, $m=2$, $\alpha=1$ and $\beta=\zeta_{4k}$ where k is an odd natural number $\geqq 3$. Then the only solution of* (1) *is $\xi=0$, $\eta=1$.*

2. *Proof of Theorem A.* Our equation is in this case $\xi+\alpha=\eta$, $\alpha=\beta=\zeta_4$ or ζ_p, $\xi\in K(\alpha+\alpha^{-1})$, $\eta\in U_{K(\alpha)}$. Notice first ξ should be $\in\mathcal{O}_{K(\alpha)}$ as α, $\eta\in\mathcal{O}_{K(\alpha)}$.

(I) Suppose $\xi\neq 0$. As $K(\zeta_4+\zeta_4^{-1})=K$ is totally real, all conjugates ξ' of ξ are real, and $|\xi'\pm\xi_4|>1$, so that $\xi+\zeta_4$ can not be $\in U_{K(\zeta_4)}$.

(II) As $K(\zeta_p+\zeta_p^{-1})$ is totally real, $\xi \in K(\zeta_p+\zeta_p^{-1})$ and $\eta=\xi+\zeta_p \in U_{K(\zeta_p)}$, also the complex conjugate $\bar{\eta}=\xi+\zeta_p^{-1} \in U_{K(\zeta_p)}$, and $\eta\bar{\eta}^{-1} \in U_{K(\zeta_p)} \in \mathcal{O}_{K(\zeta_p)}$. We have $|\eta|=|\bar{\eta}|$, and it is easily seen that all conjugates $\eta\bar{\eta}^{-1}$ have the absolute value 1. Thus $\eta\bar{\eta}^{-1}$ is a root of unity in virtue of Kronecker's theorem. Put $\eta=\bar{\eta}\zeta_n^c$, with $(n, c)=1$. Clearly $\zeta_n^c \neq 1$, and we have also $\zeta_n^c \neq -1$, because this would imply $-\xi=(\zeta_p+\zeta_p^{-1})/2$ which is not an integer. So we have $n \geqq 3$. Put $n=n_0p^\nu$, $(n_0, p)=1$, $\nu \geqq 0$, and examine different cases.

(a) $n_0=1$, $\nu \geqq 2$. Raising the both sides of the equation

$$(\xi+\zeta_p)/(\xi+\zeta_p^{-1})=\zeta_{p^\nu}^c$$

to the p th power and then substracting 1, we see easily $\zeta_{p^{\nu-1}}^c-1 \in p\mathcal{O}_{K(\zeta_p)}$, and so $\zeta_{p^{\nu-1}}-1 \in p\mathcal{O}_{K(\zeta_p)}$ as $(c, p)=1$, which implies $Q(\zeta_{p^{\nu-1}}) \subset K(\zeta_p)$. Using the fact $(p)=(\zeta_{p^{\nu-1}}-1)^{\varphi(p^{\nu-1})}$ as ideal in $Q(\zeta_{p^{\nu-1}})$, we obtain $(\zeta_{p^{\nu-1}}-1)\,\mathcal{O}_{Q(\zeta_{p^{\nu-1}})} = ((\zeta_{p^{\nu-1}}-1)\,\mathcal{O}_{K(\zeta_p)}) \cap Q(\zeta_{p^{\nu-1}}) \subset (p\mathcal{O}_{K(\zeta_p)}) \cap Q(\zeta_{p^{\nu-1}}) = p\mathcal{O}_{Q(\zeta_{p^{\nu-1}})} = ((\zeta_{p^{\nu-1}}-1)\mathcal{O}_{Q(\zeta_{p^{\nu-1}})})^{\varphi(p^{\nu-1})}$.
This shows the impossibility of this case, as $\varphi(p^{\nu-1}) \geqq 2$ for $\nu \geqq 2$.

(b) $n_0 \geqq 2$, $\nu \geqq 1$. Then we should have $(\zeta_p-\zeta_p^{-1})/(\xi+\xi_p^{-1})=\zeta_{n_0p^\nu}^c-1$, $(c, n_0p^\nu)=1$. This is not possible, since $\zeta_{n_0p^\nu}-1$, $\xi+\zeta_p^{-1}$ are units and $\zeta_p-\zeta_p^{-1}$ is not a unit.

(c) $n_0 \geqq 3$, $\nu=0$. Then we get $(\zeta_p-1)\mathcal{O}_{K(\zeta_p)}=(\zeta_{n_0}-1)\mathcal{O}_{K(\zeta_p)}$ as in (b). This is not possible if $n_0=2^{\mu+1}$ or $n_0=q^\mu$ $(\mu \geqq 1)$, where q is an odd prime different from p. If n_0 has distinct prime factors, then $\zeta_{n_0}-1$ is a unit, so that $(\zeta_p-1)\,\mathcal{O}_{K(\zeta_p)}=(\zeta_{n_0}-1)\,\mathcal{O}_{K(\zeta_p)}=\mathcal{O}_{K(\zeta_p)}$, which is also a contradiction.

Thus only the case $n_0=1$, $\nu=1$ remains. Namely $(\xi+\zeta_p)/(\xi+\zeta_p^{-1}) =\zeta_p^c$, $c \in \{1, 2, \cdots, p-1\}$, which yields $\xi=(\zeta_p^{c-1}-\zeta_p)/(1-\zeta_p^c)$ and $\xi \in K(\zeta_p+\zeta_p^{-1})$.

(III) In this case, we have $K \cap Q(\zeta_p)=Q$ for any odd prime p. If $c \geqq 3$ in $\xi=(\zeta_p^{c-1}-\zeta_p)/(1-\zeta_p^c)$, ξ must be a unit in $K \cap Q(\zeta_p)=Q$. Hence $\xi=\pm 1$. However $\xi \neq -1$, because $\zeta_p^c-\zeta_p^{c-1}+\zeta_p-1 \neq 0$. Therefore we obtain $\xi=1$. If $c=2$, then we have $\xi=0$. If $c=1$, then we get $\xi=1$.

Thus the proof of Theorem A is concluded.

3. *Proof of Theorem B.* Without loss of generality, we may assume that m is prime.

(i) Let $m=p$ an odd prime. As $\eta=(\xi+1)(\xi+\zeta_p)\cdots(\xi+\zeta_p^{p-1}) \in U_{K(\zeta_p)}$, $\xi^p \in \mathcal{O}_{K(\zeta_p)}$ and $\xi \in K(\zeta_p+\zeta_p^{-1})$, we have $\xi \in \mathcal{O}_{K(\zeta_p+\zeta_p^{-1})}$ and $\xi+\zeta_p \in U_{K(\zeta_p)}$. Then we have $\xi=(\zeta_p^{c-1}-\zeta_p)/(1-\zeta_p^c)$ with $c \in \{1, 2, \cdots, p-1\}$ in virtue of (II) in Theorem A. If $c=1$, then $\xi=1$, in contradiction with $\eta=\xi^p+1 \in U_{K(\zeta_p)}$. If $c=2$, then $\xi=0$. This also contradicts $\eta \neq 1$. If $c \geqq 3$, then ξ is a unit in totally real algebraic number field $K(\zeta_p+\zeta_p^{-1})$, so we have immediately Theorem B from the cited Grossman's result [3].

(ii) Consider now the case $m=2$. As $\eta=(\xi+\zeta_4)(\xi+\zeta_4^{-1})\in U_{K(\zeta_4)}$, $\xi^2\in\mathcal{O}_{K(\zeta_4)}$ and $\xi\in K=K(\zeta_4+\zeta_4^{-1})$, we have $\xi\in\mathcal{O}_K$ and $\xi+\zeta_4\in U_{K(\zeta_4)}$, so that $\xi=0$ in virtue of (I) in Theorem A. This is a contradiction and the proof is completed.

4. *Proof of Theorem C.* As $\eta=(\xi+\zeta_4)(\xi+\zeta_4^{-1})\in U_{K(\zeta_{4m})}$, $\delta=\xi+\zeta_4$ and its complex conjugate $\bar{\delta}=\xi+\zeta_4^{-1}$ are in $U_{K(\zeta_{4m})}$, so that $\bar{\delta}\delta^{-1}\in U_{K(\zeta_{4m})}\subset\mathcal{O}_{K(\zeta_{4m})}$. Moreover, since $K(\zeta_{4m})$ is contained in some cyclotomic field, $\gamma=\bar{\delta}\delta^{-1}$ is a root of unity by a well known theorem. Then $(\gamma-1)\xi=-\zeta_4(\gamma+1)$. It is clear that $\gamma\neq 1$. Hence $\xi=-(\gamma+1)\zeta_4/(\gamma-1)$. From $\xi+\zeta_4=-2\zeta_4/(\gamma-1)\in U_{K(\zeta_{4m})}$, we have

$$\pm 1=N_{K(\zeta_{4m})}(\xi+\zeta_4)=N_{K(\zeta_{4m})}\left(-\frac{2\zeta_4}{\gamma-1}\right).$$

This yields $\gamma=-1$, since γ is a root of unity. Thus we obtain $\xi=0$, $\eta=1$. The proof is completed.

Acknowledgement. The author is grateful to Profs. S. Iyanaga and H. Wada for reading this paper in manuscript and giving much kind advice for its improvement.

References

[1] P. Chowla: Ph. D. Dissertation. University of Colorado (1961).
[2] V. Ennola: A note on a cyclotomic diophantine equation. Acta Arith., **28**, 157–159 (1975).
[3] E. H. Grossman: On the solution of diophantine equations in units. ibid., **30**, 137–143 (1976).
[4] L. J. Mordell: On a cyclotomic diophantine equation. Journ. de Math., **42**, 205–208 (1963).
[5] M. Newman: Diophantine equation in cyclotomic fields. J. reine angew. Math., **265**, 84–89 (1974).