ACTA ARITHMETICA
LVII (1991)

On unit solutions of the equation $xyz = x+y+z$ in a number field with unit group of rank 1

by

LIANG-CHENG ZHANG and JONATHAN GORDON (Urbana, Ill.)

1. Introduction. The equation

$$xyz = x+y+z = 1$$

has been studied and shown to have no solution in the rational number field $\boldsymbol{Q}$ ([2], [4], [5]). This leads to the study of the equation

$$u_1 u_2 u_3 = u_1+u_2+u_3 \tag{1.1}$$

where u_i, $i = 1, 2, 3$, is a unit in the ring of integers of an algebraic number field K. When K is a quadratic extension of $\boldsymbol{Q}$ the problem has been completely solved [3]. Mollin *et al.* proved that if $K = \boldsymbol{Q}(\sqrt{d})$, where d is a squarefree rational integer, then there exist solutions to (1.1) if and only if $d = -1$, 2 or 5. In this paper we will show, for a real number field K with unit group U_K having rank 1 and containing a fundamental unit $\eta > 3$, (1.1) has no solution. Consequently, we shall prove that (1.1) has no solution in any pure cubic field $\boldsymbol{Q}(\sqrt[3]{m})$ and we shall also give an alternative proof of the theorem of Mollin *et al.* in [3].

2. Results

THEOREM. *Let K be a real number field such that the group of units U_K of the ring of integers of K has rank* 1. *Let η be the fundamental unit which is greater than* 1. *If $\eta > 3$ then there exist no solutions to the equation* (1.1).

Proof. We assume $\eta > 3$. Let $u_i = \pm\eta^{l_i}$, $l_i \in \boldsymbol{Z}$, $i = 1, 2, 3$, be a solution of (1.1) and

$$u = u_1 u_2 u_3 = u_1+u_2+u_3.$$

We may assume $u > 0$, if not look at

$$-u = (-u_1)(-u_2)(-u_3) = (-u_1)+(-u_2)+(-u_3).$$

1980 *Mathematics Subject Classification*: 11D25, 11R27, 11R16.

So at least one $u_i > 0$. We may assume $u_1 > 0$. Then, without loss of generality, we may assume that $l_1 \geqslant l_2 \geqslant l_3$, and consequently $\eta^{l_1} \geqslant \eta^{l_2} \geqslant \eta^{l_3}$. There are only two possibilities, that is, the case

$$\eta^{l_1+l_2+l_3} = \eta^{l_1}+\eta^{l_2}+\eta^{l_3} \tag{2.1}$$

or the case

$$\eta^{l_1+l_2+l_3} = \eta^{l_1}-\eta^{l_2}-\eta^{l_3}. \tag{2.2}$$

We first consider the case (2.1). If $l_2+l_3 \geqslant 1$, then

$$\eta^{l_1+l_2+l_3} = \eta^{l_1}\eta^{l_2+l_3} \geqslant \eta^{l_1}\eta > 3\eta^{l_1} \geqslant \eta^{l_1}+\eta^{l_2}+\eta^{l_3}.$$

If $l_2+l_3 \leqslant 0$, then

$$\eta^{l_1+l_2+l_3} = \eta^{l_1}\eta^{l_2+l_3} \leqslant \eta^{l_1} < \eta^{l_1}+\eta^{l_2}+\eta^{l_3}.$$

So (2.1) is impossible.

Now consider the case (2.2). If $l_2+l_3 \geqslant 0$, then

$$\eta^{l_1+l_2+l_3} = \eta^{l_1}\eta^{l_2+l_3} \geqslant \eta^{l_1} > \eta^{l_1}-\eta^{l_2}-\eta^{l_3}.$$

If $l_2+l_3 < 0$, then

$$\eta^{l_1+l_2+l_3} = \eta^{l_1}\eta^{l_2+l_3} \leqslant \frac{1}{\eta}\eta^{l_1} < \frac{1}{3}\eta^{l_1}.$$

Here we note that $l_1 > l_2$, otherwise if $l_1 \leqslant l_2$ then

$$\eta^{l_1}-\eta^{l_2}-\eta^{l_3} \leqslant -\eta^{l_3} < 0$$

which is impossible. Therefore $l_3 \leqslant l_2 \leqslant l_1-1$ and

$$\eta^{l_3} \leqslant \eta^{l_2} = \eta^{l_1}\eta^{l_2-l_1} \leqslant \eta^{l_1}\eta^{-1} = \frac{1}{\eta}\eta^{l_1} \leqslant \frac{1}{3}\eta^{l_1}. \tag{2.3}$$

Thus

$$\eta^{l_2}+\eta^{l_3} \leqslant \tfrac{2}{3}\eta^{l_1} \quad \text{and} \quad \tfrac{1}{3}\eta^{l_1} \leqslant \eta^{l_1}-\eta^{l_2}-\eta^{l_3}.$$

Therefore, (2.2) is impossible. This completes the proof.

Remarks. 1. Let $K = \mathbf{Q}(\sqrt[3]{m})$ be a pure cubic field, where $m = ab^2$, a, b are positive squarefree integers with $(a, b) = 1$. Since $\mathbf{Q}(\sqrt[3]{ab^2}) = \mathbf{Q}(\sqrt[3]{a^2b})$, we may assume that $a > b$ without loss of generality. It is not hard to see that if the fundamental unit $\eta > 1$ of K, then $\eta > 3$. To see this we use Artin's lower bound ([1], [6])

$$4\eta^3+24 > d_k$$

where d_k is the discriminant of K, and

$$d_k = \begin{cases} 27a^2b^2 & \text{if } ab^2 \not\equiv \pm 1 \pmod 9, \\ 3a^2b^2 & \text{if } ab^2 \equiv \pm 1 \pmod 9). \end{cases}$$

Therefore if $d_k > 132$, then $\eta > 3$. For $ab^2 \not\equiv \pm 1 \pmod 9$, $d_k = 27a^2b^2 > 132$ provided $ab \geqslant 3$. The only exceptional case occurs when $m = 2$ when $\eta = 1+\sqrt[3]{2}+\sqrt[3]{4} > 3$ is the fundamental unit. For $ab^2 \equiv 1 \pmod 9$, $d_k = 3a^2b^2 > 132$ provided $ab \geqslant 7$ which always holds.

2. Let $K = \mathbf{Q}(\sqrt{d})$ where $d > 1$ is a squarefree integer and $d \neq 2, 5$. If $\eta > 1$ is the fundamental unit of K, then $\eta > 3$. This can be seen as follows. Let $\eta = a+b\sqrt{d} > 1$ and $\eta' = a-b\sqrt{d}$. Then

$$\eta\eta' = N(\eta) = \pm 1 \quad \text{and} \quad |\eta'| = 1/\eta < 1.$$

Consequently

$$a = \frac{1}{2}(\eta+\eta') > 0, \quad b = \frac{1}{2\sqrt{d}}(\eta-\eta') > 0.$$

For $d \not\equiv 1 \pmod 4$, $\eta = a+b\sqrt{d} \geqslant 1+\sqrt{6} > 3$ provided $d \geqslant 6$. The only exception then occurs in case $d = 3$, when $\eta = 2+\sqrt{3} \geqslant 3$ is the fundamental unit.

If $d \equiv 1 \pmod 4$, then $d \geqslant 13$ and $a, b \geqslant 1/2$. Since

$$\eta-\eta' = 2b\sqrt{d} \geqslant \sqrt{d} \quad \text{and} \quad \eta+\frac{1}{\eta} \geqslant \eta-\eta' \geqslant \sqrt{d},$$

we have $\eta^2-\sqrt{d}\eta+1 \geqslant 0$. Thus

$$\eta \geqslant \frac{\sqrt{d}+\sqrt{d-4}}{2} \geqslant \frac{\sqrt{13}+\sqrt{9}}{2} > 3.$$

An immediate consequence of the theorem and the first remark is the following corollary.

Corollary 1. *Let $K = \mathbf{Q}(\sqrt[3]{m})$ be a pure cubic field and U_K be the group of units of the ring of integers of K. Then the equation* (1.1) *has no solutions.*

Making use of the theorem and the second remark, we shall prove the Theorem of Mollin *et al.* in [3].

Corollary 2 (Theorem of Mollin *et al.*). *Let $K = \mathbf{Q}(\sqrt{d})$, where d is a squarefree integer. Let U_K denote the group of units in the ring of integers of K. There exist solutions to the equation* (1.1) *if and only if $d = -1$, 2 or 5.*

Proof. For $d > 1$ and $d \neq 2, 5$ there exists no solution to (1.1) by the second remark and the theorem. For $d = 2$, $u_1 = 1+\sqrt{2}$, $u_2 = 1-\sqrt{2}$, $u_3 = -1$ is a solution. For $d = 5$, $u_1 = 2+\sqrt{5}$, $u_2 = (1+\sqrt{5})/2$, $u_3 = 1$ is a solution.

For $d < 0$, $d \neq -1, -3$, $U_K = \{\pm 1\}$ and the equation (1.1) is not solvable. For $d = -1$, $U_K = \{\pm 1, \pm i\}$. It is easy to see that a solution exists: $u_1 = 1$, $u_2 = i$ and $u_3 = -i$. For $d = -3$, $U_K = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, where ζ is a primitive 6th root of unity. We use the simple fact that if $|a_1+a_2+a_3| = 1$, $|a_k| = 1$, $k = 1, 2, 3$ then there exist $1 \leqslant i < j \leqslant 3$ such that $a_i+a_j = 0$. This can be seen by viewing a parallelogram as four vectors with clockwise orientation in which case opposite vectors are additive inverses or in the degenerate case adjacent vectors are additive inverses. We have $1 = |\zeta^{l_1}\zeta^{l_2}\zeta^{l_3}| = |\zeta^{l_1}+\zeta^{l_2}+\zeta^{l_3}|$ and $|\zeta^{l_i}| = 1$, $i = 1, 2, 3$. So we may assume $\zeta^{l_2} = -\zeta^{l_1}$, then

$$\zeta^{l_3} = \zeta^{l_1}+\zeta^{l_2}+\zeta^{l_3} = \zeta^{l_1}\zeta^{l_2}\zeta^{l_3} = -\zeta^{2l_1}\zeta^{l_3}.$$

Consequently, $(\zeta^{l_1})^2 = -1$. Thus $\zeta^{l_1} = \pm i$, which is impossible.

Acknowledgements. The authors wish to thank Bruce C. Berndt for his encouragement and H. Edgar for carefully reading our manuscript.

References

[1] E. Artin, *Theory of Algebraic Numbers*, Göttingen 1959.
[2] J. W. S. Cassels, *On a diophantine equation*, Acta Arith. 6 (1960), 47–52.
[3] R. A. Mollin, C. Small, K. Varadarajan and P. G. Walsh, *On unit solutions of the equation $xyz = x+y+z$ in the ring of integers of a quadratic field*, ibid. 48 (1987), 341–345.
[4] W. Sierpiński, *On some unsolved problems of Arithmetics*, Scripta Math. 25 (1960), 125–136.
[5] — *Remarques sur le travail de M. J. W. S. Cassels "On a diophantine equation"*, Acta Arith. 6 (1961), 469–471.
[6] L. C. Zhang, *On the units of cubic and bicubic fields*, Acta Math. Sinica, New Series, 1 (1985), 22–34.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
1409 West Green Street
Urbana, Illinois 61801
U.S.A.

Received on 27.6.1989 (1949)

ACTA ARITHMETICA
LVII (1991)

Note on a decomposition of integer vectors, II

by

S. CHAŁADUS (Częstochowa) and YU. TETERIN (Leningrad)

The notation of this paper is that of [6]. For m linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \boldsymbol{Z}^k$, $H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)$ denotes the maximum of the absolute values of all minors of order m of the matrix $\begin{pmatrix}\boldsymbol{n}_1\\ \vdots \\ \boldsymbol{n}_m\end{pmatrix}$ and $D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)$ the greatest common divisor of these minors. Furthermore

$$h(\boldsymbol{n}) = H(\boldsymbol{n}) \quad \text{for } \boldsymbol{n} \neq \boldsymbol{0}, \quad h(\boldsymbol{0}) = 0$$

and for $k \geqslant l \geqslant m$, $k > m$

$$c_0(k, l, m) = \sup\inf\left(\frac{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}\right)^{(k-l)/(k-m)} \prod_{i=1}^{l} h(\boldsymbol{p}_i),$$

where the supremum is taken over all sets of linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \boldsymbol{Z}^k$ and the infimum is taken over all sets of linearly independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l \in \boldsymbol{Z}^k$ such that for all $i \leqslant m$

$$\boldsymbol{n}_i = \sum_{j=}^{l} u_{ij}\boldsymbol{p}_j, \quad u_{ij} \in \boldsymbol{Q}; \tag{1}$$

$\| \ \|$ denotes the usual Euclidean norm.

The aim of the paper is to prove the following two theorems.

THEOREM 1. *For all integers k, l, m satisfying $k \geqslant l \geqslant m$, $k > m$ we have*

$$c_0(k, l, m) \leqslant \gamma_{k-m,k-l}^{1/2} \binom{k}{m}^{(k-l)/(2(k-m))}$$

where $\gamma_{k-m,k-l}$ is the Rankin constant (see [4]).

THEOREM 2. *For all integers k, l, m satisfying $k \geqslant l \geqslant m$, $k > m$ and for every H there exist linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \boldsymbol{Z}^k$ such that*

$$\frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)} > H \tag{2}$$