Far East J. Math. Sci. (FJMS) **14**(1) (2004), 1-7

AN EXTENSION OF VULAKH'S THEOREM ON UNITS IN COMPLEX CUBIC FIELDS

KENNETH S. WILLIAMS

(Received January 2, 2004)

Submitted by K. K. Azad

Abstract

Let $f(x) = x^3 - tx^2 - ux - 1 \in \mathbb{Z}[x]$. Conditions are given on t and u which ensure that $f(x)$ has exactly one real root θ which is the fundamental unit (> 1) of the cubic field $\mathbb{Q}(\theta)$.

1. Introduction

Recently Vulakh [2, Theorem 1, p. 1306] has proved the following theorem.

Theorem 1. *Let* $f(x) = x^3 - tx^2 - ux - 1$, *where* t *and* u *are integers such that*

$$\begin{cases} t > u(u+1)/2, & \text{if } u \text{ is odd,} \\ t \geq u(u+2)/2, & \text{if } u \text{ is even.} \end{cases} \tag{1.1}$$

Assume that $f(x)$ *has exactly one real root* θ. *Let* $K = \mathbb{Q}(\theta)$. *Assume that the discriminant of* $f(x)$ *is squarefree. Then* θ *is a fundamental unit of the*

2000 Mathematics Subject Classification: 11R16, 11R27.

Key words and phrases: fundamental unit, real cubic field with two complex embeddings.

Research supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

ring O_K *of the integers of K, that is, every unit of* O_K *is of the form* $\pm\theta^k$ *for some* $k \in \mathbb{Z}$.

We note that if the conditions of Theorem 1 are met, then K is a real cubic field with two complex embeddings. We prove the following extension of Vulakh's theorem. It is always stronger than Vulakh's theorem when $|u| \geq 24$, as well as in some other cases. The proof is elementary.

Theorem 2. *Let* $f(x) = x^3 - tx^2 - ux - 1$, *where* t *and* u *are integers such that*

$$t \geq (u^2 + 18|u| + 12)/4.$$

Then

(i) $f(x)$ *is irreducible in* $\mathbb{Z}[x]$,

(ii) *the discriminant* D *of* $f(x)$ *is negative so that* $f(x)$ *has exactly one real root* θ,

(iii) *if the discriminant of* $f(x)$ *is squarefree, then* θ *is the fundamental unit* > 1 *of the ring* O_K *of integers of the cubic field* $K = \mathbb{Q}(\theta)$.

2. Proof of Theorem 2

First we observe that

$$t \geq \frac{u^2 + 18|u| + 12}{4} \geq \frac{12}{4} = 3 \tag{2.1}$$

and

$$t > \frac{18|u|}{4} \geq |u|. \tag{2.2}$$

Secondly we show that $f(1) \neq 0$. Suppose that $f(1) = 0$. Then $t + u = 0$. By (2.1) $t > 0$ so that $u < 0$ and $|u| = -u = t$, contradicting (2.2). Hence

$$f(1) \neq 0. \tag{2.3}$$

Thirdly we show that $f(-1) \neq 0$. Suppose that $f(-1) = 0$. Then $u = t + 2$. By (2.1) we have $t > 0$ so that $u > 0$ and thus $|u| = u = t + 2 > t$, which contradicts (2.2). Hence

$$f(-1) \neq 0. \tag{2.4}$$

From (2.3) and (2.4) we see that ± 1 are not roots of the cubic $f(x)$ so that $f(x)$ has no linear factors in $\mathbb{Z}[x]$ and thus $f(x)$ is irreducible in $\mathbb{Z}[x]$, proving (i).

Fourthly, we prove that

$$4t^3 - u^2t^2 + 18ut - 4u^3 > 4(1+t)^{\frac{3}{2}}. \tag{2.5}$$

We consider two cases according as $u \geq 0$ or $u < 0$. If $u \geq 0$, then $|u| = u$ and

$$t \geq \frac{u^2 + 18u + 12}{4}.$$

Thus

$$\begin{aligned} &4t^3 - u^2t^2 + 18ut - 4u^3 \\ &\quad = t^2(4t - u^2) + 2u(9t - 2u^2) \\ &\quad \geq t^2(18u + 12) + \frac{u}{2}(u^2 + 162u + 108) \\ &\quad \geq 12t^2 \\ &\quad > 4(1+t)^{\frac{3}{2}}. \end{aligned}$$

If $u < 0$, then $|u| = -u$ and

$$t \geq \frac{u^2 - 18u + 12}{4}.$$

Then, as $u < 0$ and $t \geq 3$, we have

$$\begin{aligned}4t^3 - u^2t^2 + 18ut - 4u^3 &> 4t^3 - u^2t^2 + 18ut^2 - 4u^3\\ &> 4t^3 - u^2t^2 + 18ut^2\\ &= t^2(4t - u^2 + 18u)\\ &\geq 12t^2\\ &> 4(1+t)^{\frac{3}{2}}.\end{aligned}$$

This completes the proof of (2.5).

The discriminant D of $f(x)$ is given by

$$D = -4t^3 + u^2t^2 - 18ut + 4u^3 - 27,$$

see for example [1, p. 139]. By (2.5) we see that

$$-D-27 = 4t^3 - u^2t^2 + 18ut - 4u^3 > 4(1+t)^{\frac{3}{2}} > 0, \tag{2.6}$$

so that

$$D < 0. \tag{2.7}$$

Thus $f(x)$ has exactly one real root θ, proving (ii).

From (2.6) and (2.7) we deduce that

$$|D| > 27 + 4(1+t)^{\frac{3}{2}}, \tag{2.8}$$

so that by (2.1)

$$|D| > 59. \tag{2.9}$$

Next we show that $f(1+t) > 0$. We have (as $t > 0$ and $t > |u|$)

$$\begin{aligned}f(1+t) &= (1+t)^3 - t(1+t)^2 - u(1+t) - 1\\ &= t(2+t) - u(1+t)\\ &> t(1+t) - u(1+t)\end{aligned}$$

$$\geq t(1+t) - |u|(1+t)$$

$$= (t - |u|)(1+t)$$

$$\geq 0,$$

so that

$$f(1+t) > 0. \tag{2.10}$$

Next we determine the sign of $f(1)$. We have

$$f(1) = -t - u \leq |u| - t < 0,$$

by (2.2), so that

$$f(1) < 0. \tag{2.11}$$

As f has exactly one real root θ, we deduce from (2.10) and (2.11) that

$$1 < \theta < 1 + t. \tag{2.12}$$

Now suppose that D is squarefree so that the discriminant $d(K)$ of K is equal to D and thus by (2.9) we have

$$|d(K)| > 59.$$

Let η denote the fundamental unit (> 1) of O_K. Hence, by [1, Theorem 13.6.1, p. 370], we have

$$\eta^3 > \frac{|d(K)| - 27}{4}. \tag{2.13}$$

Then, from (2.8) and (2.12), we deduce

$$\eta^3 > (1+t)^{\frac{3}{2}} > \theta^{\frac{3}{2}}$$

so that

$$\eta^2 > \theta. \tag{2.14}$$

As $\theta(\theta^2 - t\theta - u) = 1$, we deduce that $\theta \mid 1$ in O_K, so that θ is a unit of O_K. Hence, by Dirichlet's unit theorem, we have

$$\theta = \pm\eta^k \tag{2.15}$$

for some $k \in \mathbb{Z}$ [1, Theorems 13.4.2, 13.5.2, pp. 362, 366]. As $\theta > 1$ and $\eta > 1$ we deduce from (2.15) that

$$\theta = \eta^k, \quad k \in \mathbb{N}. \tag{2.16}$$

From (2.14) and (2.16) we obtain

$$1 < \eta^k < \eta^2, \quad k \in \mathbb{N},$$

so that $k = 1$ and $\theta = \eta$. Hence θ is the fundamental unit (> 1) of O_K, proving (iii).

3. An Example

We close with a numerical example to which Theorem 2 applies but Theorem 1 does not.

Example. $f(x) = x^3 - 152x^2 - 17x - 1$.

Here $t = 152$ and $u = 17$. As

$$\frac{u(u+1)}{2} = \frac{(17)(18)}{2} = 153 > t$$

the condition (1.1) is not satisfied and Vulakh's theorem does not apply.

As

$$\frac{u^2 + 18|u| + 12}{4} = \frac{17^2 + (18)(17) + 12}{4} = \frac{289 + 306 + 12}{4}$$

$$= \frac{607}{4} = 151.75 < 152 = t$$

and

$$\operatorname{disc}(x^3 - 152x^2 - 17x - 1) = -7397063$$

being a prime is squarefree, Theorem 2 applies and the unique real root θ of $x^3 - 152x^2 - 17x - 1 = 0$ is the fundamental unit (> 1) of the cubic field $K = \mathbb{Q}(\theta)$, $\theta^3 - 152\theta^2 - 17\theta - 1 = 0$.

References

[1] S. Alaca and K. S. Williams, Introductory Algebraic Number Theory, Cambridge University Press, 2004.

[2] L. Ya. Vulakh, Continued fractions associated with $SL_3(\mathbb{Z})$ and units in complex cubic fields, Canad. J. Math. 54 (2002), 1305-1318.

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics, Carleton University
Ottawa, Ontario, Canada K1S 5B6
e-mail: williams@math.carleton.ca