COLLOQUIUM MATHEMATICUM

VOL. 109 2007 NO. 1

UNITS GENERATING THE RING OF INTEGERS OF COMPLEX CUBIC FIELDS

BY

ROBERT F. TICHY (Graz) and VOLKER ZIEGLER (Wien)

Abstract. All purely cubic fields such that their maximal order is generated by its units are determined.

1. Introduction. In 1954 Zelinsky [15] showed that, if V is a vector space over a division ring D, then every linear transformation can be written as the sum of two automorphisms unless $\dim V = 1$ and D is the field of two elements. Later many authors investigated similar problems for various classes of rings. This gives rise to the following definition (see Goldsmith, Pabst and Scott [6]).

DEFINITION 1. Let R be a ring (with identity). An element r is called *k-good* if $r = e_1 + \cdots + e_k$ with $e_1, \ldots, e_k \in R^*$. If every element of R is *k-good* we also call the ring *k-good*.

The *unit sum number* $u(R)$ is defined as $\min\{k : R \text{ is } k\text{-good}\}$. If the minimum does not exist but the units generate R additively we set $u(R) = \omega$. If the units do not generate R we set $u(R) = \infty$.

For some historical information on this topic and several examples we refer to the recent papers of Ashrafi and Vámos [1], and Vámos [14].

Endomorphism rings have been studied in great detail and also some other classes of rings were investigated from this point of view. Which rings of integers are k-good has been investigated by Ashrafi and Vámos [1]. In particular, they proved that the rings of integers of quadratic fields, complex cubic fields and cyclotomic fields $\mathbb{Q}(\zeta_{2^N})$, with $N \geq 1$, are not k-good for any integer k. Jarden and Narkiewicz [9] proved that every finitely generated integral domain of characteristic zero has unit sum number ω or ∞. In other words, they proved that no ring of integers has finite unit sum number. However, the question which rings of integers are generated by their units

2000 *Mathematics Subject Classification*: 11D25, 11R16.

Key words and phrases: units, complex cubic fields, cubic Diophantine equations.

The authors gratefully acknowledge support from the Austrian Science Fund (FWF) under project Nr. P18079-N12 and S9611.

remains. In the case of quadratic fields Belcher [2] and Ashrafi and Vámos [1] answered independently this question.

Similar questions arose in 1964 when Jacobson [8] asked which number fields K have the property that all algebraic integers of K can be written as sums of distinct units. Let us denote by $\mathcal{U}$ the set of number fields that have this property. Jacobson [8] proved that the number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are members of $\mathcal{U}$. Some years later Śliwa [12] proved that these two fields are the only quadratic fields with this property. Moreover Śliwa showed that no field of the form $\mathbb{Q}(\sqrt[3]{d})$ is in $\mathcal{U}$. Criteria for a number field to lie in $\mathcal{U}$ were given by Belcher [2, 3]. In particular Belcher [3] proved that $K \in \mathcal{U}$ if 2 is the sum of two distinct units and the ring of integers of K is generated by its units. By an application of this criterion Belcher [3] characterized all cubic number fields with negative discriminant that lie in $\mathcal{U}$.

The aim of this paper is to investigate which rings of integers of complex cubic fields, in particular purely cubic fields, are generated by their units.

Theorem 1. *Let $X^3 - BX - C$ be an irreducible polynomial having a complex root, and let α be any root of this polynomial, possibly not complex. Let $\mathcal{O} = \mathbb{Z}[\alpha]$. Then $\mathcal{O}$ is generated by its units if and only if there exists a solution (X, Y) to the Diophantine equation*

$$X^3 + BXY^2 - CY^3 = \pm 1$$

such that there is a unit of $\mathbb{Z}[\alpha]$ of the form $Z + X\alpha + Y\alpha^2$ with Z an integer.

This theorem together with the results of Delaunay [5] and Nagell [10] yields:

Corollary 1. *Let d be a cube-free integer and $K = \mathbb{Q}(\sqrt[3]{d})$ the corresponding purely cubic field. Then the order $\mathbb{Z}[\sqrt[3]{d}]$ is generated by its units, i.e. there exist $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}[\sqrt[3]{d}]^*$ that generate $\mathbb{Z}[\sqrt[3]{d}]$, if and only if $d = a^3 \pm 1$ with $a \in \mathbb{Z}$.*

As our main result we will establish the following theorem.

Theorem 2. *Let d be a cube-free integer and let $\mathcal{O}_d$ be the maximal order of $\mathbb{Q}(\sqrt[3]{d})$. The ring $\mathcal{O}_d$ is generated by its units if and only if d is square-free, $d \not\equiv \pm 1 \bmod 9$ and $d = a^3 \pm 1$ for some integer a or $d = 28$.*

Since in general $\mathbb{Q}(\sqrt[3]{d})$ has no integral power basis the proof of Theorem 2 is far from being straightforward.

2. The quadratic case revisited. The aim of this section is to present the basic ideas for the proofs of our results. For this purpose we start with the quadratic case and give a simple proof of the result due to Ashrafi and Vámos [1, Theorems 7 and 8].

PROPOSITION 1. *Let $d \in \mathbb{Z}$ be square-free. Then $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ is generated by its units if and only if $d = a^2 \pm 1$ for some $a \in \mathbb{Z}$.*

Before we prove Proposition 1 we establish the following helpful lemma.

LEMMA 1. *If ε is a unit of some number field K with $\deg K = d$ and some powers of ε generate the additive group of integers (or some order of K) then so also do $1, \varepsilon, \ldots, \varepsilon^{d-1}$.*

Proof. It is enough to show that the $\mathbb{Z}$-module generated by $1, \varepsilon, \ldots, \varepsilon^{d-1}$ contains ε^k for all $k \in \mathbb{Z}$. This is easy to see since ε is an algebraic integer, and we have $\varepsilon^d = a_0 + a_1\varepsilon + \cdots + a_{d-1}\varepsilon^{d-1}$ with $a_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, d-1$. Now by induction we see that every positive power of ε is a linear combination of $1, \varepsilon, \ldots, \varepsilon^{d-1}$ with integral coefficients. Similarly we can express $\varepsilon^{-1}, \varepsilon^{-2}, \ldots$ as integral linear combinations of $1, \varepsilon, \ldots, \varepsilon^{d-1}$. ■

Proof of Proposition 1. Assume $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^*$ generate $\mathcal{O}$. Then also 1 and ε generate $\mathcal{O}$, where ε is the fundamental unit of $\mathcal{O}$. Therefore we may assume that 1 and ε generate $\mathcal{O}$. Let $\varepsilon = x + y\sqrt{d}$. Then the statement that 1 and ε generate $\mathcal{O}$ is equivalent to $(1, 0)$ and (x, y) generating the lattice $\mathbb{Z}^2$, hence $y = \pm 1$. Since ε is a unit we have $x^2 - dy^2 = \pm 1$ and therefore $x^2 - d = \pm 1$ or $d = \mp 1 + x^2$. This shows one direction.

Now assume $d = a^2 \pm 1$. Every unit $\varepsilon = x + y\sqrt{d} \in \mathcal{O}$ satisfies the equation $x^2 - dy^2 = x^2 - (a^2 \pm 1)y^2 = \pm 1$ with mixed signs. Obviously one solution is $x = a$ and $y = 1$. Since $(1, 0)$ and $(a, 1)$ generate $\mathbb{Z}^2$, also 1 and $\varepsilon = a + \sqrt{d}$ generate $\mathcal{O}$. ■

PROPOSITION 2. *Let $d \in \mathbb{Z}$ be square-free. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is generated by its units if and only if*

$$d = \begin{cases} a^2 \pm 1, & d \not\equiv 1 \bmod 4, \\ a^2 \pm 4, & d \equiv 1 \bmod 4. \end{cases}$$

Proof. Use the same method as above with $\sqrt{d}$ replaced by $(1 + \sqrt{d})/2$ for $d \equiv 1 \bmod 4$. Note that the ring of integers is generated by 1 and $\sqrt{d}$ if $d \not\equiv 1 \bmod 4$, and by 1 and $(1 + \sqrt{d})/2$ otherwise. ■

3. The general cubic case. This section is devoted to the proof of Theorem 1 and Corollary 1.

Proof of Theorem 1. Since $\mathbb{Q}(\alpha)$ has a complex embedding as well as a real one, its unit rank equals 1, and Dirichlet's unit theorem shows that every unit is of the form $\pm\varepsilon^n$, where $n \in \mathbb{Z}$ and ε is the fundamental unit.

If $\varepsilon_1, \varepsilon_2, \varepsilon_3$ generate $\mathbb{Z}[\alpha]$ then so also do $\pm\varepsilon_1, \pm\varepsilon_2, \pm\varepsilon_3$. Thus we may assume $\varepsilon_1 = \varepsilon^{k_1}$, $\varepsilon_2 = \varepsilon^{k_2}$ and $\varepsilon_3 = \varepsilon^{k_3}$ with $k_1, k_2, k_3 \in \mathbb{Z}$. Therefore we may assume by Lemma 1 that $1, \varepsilon, \varepsilon^2$ generate $\mathbb{Z}[\alpha]$.

Write $\varepsilon = a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Z}$. Then a short computation shows that

$$\varepsilon^2 = \overbrace{a^2 + 2bcC}^{\widetilde{a}:=} + (\overbrace{2ab + 2bcB + c^2C}^{\widetilde{b}:=})\alpha + (\overbrace{b^2 + 2ac + c^2B}^{\widetilde{c}:=})\alpha^2.$$

Therefore the vectors $(1, 0, 0)$, (a, b, c) and $(\widetilde{a}, \widetilde{b}, \widetilde{c})$ generate the lattice $\mathbb{Z}^3$, i.e. $\det M = \pm 1$, where

$$M = \begin{pmatrix} 1 & 0 & 0 \\ a & b & c \\ \widetilde{a} & \widetilde{b} & \widetilde{c} \end{pmatrix}.$$

A short computation shows

$$\det M = b\widetilde{c} - \widetilde{b}c = b^3 - bc^2B - c^3C = \pm 1,$$

and ε has the desired form.

The other direction is quite easy. Assume $\varepsilon = a + b\alpha + c\alpha^2$ has the properties described in Theorem 1. Then the vectors $(1, 0, 0), (a, b, c)$ and $(\widetilde{a}, \widetilde{b}, \widetilde{c})$ generate $\mathbb{Z}^3$, where $\varepsilon^2 = \widetilde{a} + \widetilde{b}\alpha + \widetilde{c}\alpha^2$. Hence 1, ε and ε^2 generate $\mathbb{Z}[\alpha]$. ∎

Proof of Corollary 1. We apply Theorem 1 with $B = 0$, $C = d$ and put $\alpha = \sqrt[3]{d}$. Hence $\mathcal{O} = \mathbb{Z}[\alpha]$ is generated by its units if and only if there is a unit $\varepsilon \in \mathcal{O}$ of the form $\varepsilon = a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Z}$ such that

$$b^3 - dc^3 = \pm 1.$$

By a theorem of Delaunay [5] the equation $X^3 - dY^3 = \pm 1$ has at most one solution besides the trivial solution $X = \pm 1$ and $Y = 0$. Moreover, Delaunay showed that for any solution (X, Y) to $X^3 - dY^3 = 1$ the quantity $X + \sqrt[3]{d}\,Y$ is a fundamental unit. Assuming, $b^3 - dc^3 = \pm 1$ we know from the proof of Theorem 1 that the fundamental unit satisfies $\varepsilon = \pm(a + b\sqrt[3]{d} + c\sqrt[3]{d})$. On the other hand, by Delaunay [5], $\varepsilon = \pm(\widetilde{b} + \widetilde{c}\sqrt[3]{d})$, where $(\widetilde{b}, \widetilde{c})$ is the non-trivial solution to $X^3 - dY^3 = 1$. If (b, c) is a non-trivial solution then we get a contradiction, therefore $b = \pm 1$ and $c = 0$. Hence $\varepsilon = a \pm \sqrt[3]{d}$. This yields $a^3 \pm d = \pm 1$ or equivalently $d = a^3 \pm 1$ for some integer a. ∎

4. Purely cubic fields of the first kind. The next two sections are devoted to the proof of Theorem 2.

First, we recall the well known fact (see e.g. [4, Section 6.4.3]) that if $d = ab^2$ with $a, b \in \mathbb{Z}$ square-free and coprime, then $\mathcal{O}_d$ is generated by 1, $\sqrt[3]{ab^2}$ and $\sqrt[3]{a^2b}$ if $d \not\equiv \pm 1 \bmod 9$, and by $\frac{1}{3}(1 + a\sqrt[3]{ab^2} + b\sqrt[3]{a^2b})$, $\sqrt[3]{ab^2}$ and $\sqrt[3]{a^2b}$ otherwise. Because of $\mathbb{Q}(\sqrt[3]{b^2}) = \mathbb{Q}(\sqrt[3]{b})$ we exclude the case $a = 1$.

Next we remark that in the case where d is square-free and $d \not\equiv \pm 1 \bmod 9$, Corollary 1 yields Theorem 2.

Consider now the case $d \not\equiv \pm 1 \bmod 9$ and $b \neq 1$. In view of Lemma 1, we assume that there exists a unit $\varepsilon = X + Y\sqrt[3]{ab^2} + Z\sqrt[3]{a^2b}$ such that $\{1, \varepsilon, \varepsilon^2\}$ generates $\mathcal{O}_d$. Since

$$\varepsilon^2 = X^2 + 2abYZ + (aZ^2 + 2XY)\sqrt[3]{ab^2} + (bY^2 + 2XZ)\sqrt[3]{a^2b}, \tag{1}$$

we have to investigate the equation $\det M = \pm 1$, where

$$M = \begin{pmatrix} 1 & 0 & 0 \\ X & Y & Z \\ X^2 + 2abYZ & aZ^2 + 2XY & bY^2 + 2XZ \end{pmatrix}.$$

Therefore (Y, Z) has to be a solution to the Diophantine equation

$$by^3 - az^3 = \pm 1. \tag{2}$$

It is obvious that together with $\{1, \varepsilon, \varepsilon^2\}$ also $\{1, \varepsilon^{-1}, \varepsilon^{-2}\}$ generates the algebraic integers (see Lemma 1). Since

$$\varepsilon^{-1} = (X^2 - abYZ) + (aZ^2 - XY)\sqrt[3]{ab^2} + (bY^2 - XZ)\sqrt[3]{a^2b},$$

also $(aZ^2 - XY, bY^2 - XZ)$ is a solution to (2). By a theorem of Delaunay [5] and Nagell [10] we know that (2) has at most one solution with $Y \geq 0$. Suppose (Y, Z) is such a solution. Then

$$aZ^2 - XY = \pm Y,$$
$$bY^2 - XZ = \pm Z.$$

Note that the signs for Y and Z must be the same. Eliminating X from these equations yields $bY^3 - aZ^3 = 0$, which is a contradiction. Note that $YZ \neq 0$, since $b \neq 1$ and $a \neq 1$.

5. Purely cubic fields of the second kind. Now the situation is more complicated. Since $ab^2 \equiv \pm 1 \bmod 9$ we have $a \equiv 1 \bmod 3$ and $a \equiv \pm b \bmod 9$. Let $a \equiv eb \bmod 9$ with $e \in \{\pm 1\}$. Then together with $\frac{1}{3}(1 + a\sqrt[3]{ab^2} + b\sqrt[3]{a^2b})$, $\sqrt[3]{ab^2}$, $\sqrt[3]{a^2b}$ also 1, $\sqrt[3]{ab^2}$, $\frac{1}{3}(1 + \sqrt[3]{ab^2} + e\sqrt[3]{a^2b})$ is an integral basis. Therefore we write

$$\varepsilon = \widetilde{X} + \widetilde{Y}\sqrt[3]{ab^2} + \widetilde{Z}\sqrt[3]{a^2b} = \xi + \eta\sqrt[3]{a^2b} + \zeta\,\frac{1 + \sqrt[3]{ab^2} + e\sqrt[3]{a^2b}}{3},$$

hence

$$\widetilde{X} = \xi + \zeta/3, \qquad \widetilde{Y} = \eta + \zeta/3, \qquad \widetilde{Z} = e\zeta/3.$$

Moreover, let $X = 3\widetilde{X}$, $Y = 3\widetilde{Y}$ and $Z = 3\widetilde{Z}$. We can express ε^2 in the new basis:

$$\varepsilon^2 = \overbrace{\left(\xi^2 - eb\eta^2 + \zeta^2\,\frac{e(2ab-b)-1}{9} + 2\eta\zeta\,\frac{e(ab-b)}{3}\right)}^{\widetilde{\xi}:=}$$
$$+\overbrace{\left(-eb\eta^2 + \zeta^2\,\frac{a-eb}{9} + 2\xi\eta + 2\eta\zeta\,\frac{1-eb}{3}\right)}^{\widetilde{\eta}:=}\sqrt[3]{ab^2}$$
$$+\overbrace{\left(3eb\eta^2 + \zeta^2\,\frac{2+eb}{3} + 2\xi\zeta + 2eb\eta\zeta\right)}^{\widetilde{\zeta}:=}\frac{1}{3}\,(1+\sqrt[3]{ab^2}+e\sqrt[3]{a^2b}).$$

Therefore we have to investigate the equation $\det M = \pm 1$, where

$$M := \begin{pmatrix} 1 & 0 & 0 \\ \xi & \eta & \zeta \\ \widetilde{\xi} & \widetilde{\eta} & \widetilde{\zeta} \end{pmatrix}.$$

This yields the equation

$$eb(3\eta+\zeta)^3 - a\zeta^3 = \pm 9,$$

which is equivalent to

$$bY^3 - aZ^3 = e_1 9, \tag{3}$$

where $e_1 \in \{\pm 1\}$. Together with $\{1, \varepsilon, \varepsilon^2\}$ also $\{1, \varepsilon^{-1}, \varepsilon^{-2}\}$ generates $\mathcal{O}_d$. Therefore together with (Y, Z) also $\left(\frac{aZ^2-XY}{3}, \frac{bY^2-XZ}{3}\right) \in \mathbb{Z}\times\mathbb{Z}$ is a solution to the Diophantine equation

$$by^3 - az^3 = \pm 9. \tag{4}$$

Assume $\left(\frac{aZ^2-XY}{3}, \frac{bY^2-XZ}{3}\right)$ satisfies (4) with $e_1'9$ on the right side, where $e_1' \in \{\pm 1\}$. As above we see that the two solutions

$$\pm\left(\frac{aZ^2-XY}{3}, \frac{bY^2-XZ}{3}\right) \quad \text{and} \quad \pm(Y, Z)$$

are distinct since otherwise

$$aZ^2 - XY = \pm 3Y, \qquad bY^2 - XZ = \pm 3Z.$$

These two equations imply $\pm 9 = bY^3 - aZ^3 = 0, \pm 6YZ$ depending on the signs. However, each of these cases is impossible since $X, Y, Z \in \mathbb{Z}$. Note that $3 \mid Z$ and $3 \mid Y$ are each impossible, since then both Y and Z are divisible by 3 and this implies $27 \mid 9$, a contradiction.

On the other hand, a famous result due to Siegel [11] tells us that there is at most one solution to

$$|ax^n - by^n| \le c$$

if

$$|ab|^{n/2-1} \geq \lambda_n c^{2n-2} \quad \text{with} \quad \lambda_n = 4\Big(n \prod_{p|n} p^{1/(p-1)}\Big)^n.$$

In our case this yields $|ab| > 1.356 \cdot 10^{13}$. However, if we use this estimate, too many cases remain to be checked individually. So we have to refine this method.

Now we take into account that ε is a unit. Therefore we find

$$X^3 + ab^2Y^3 + a^2bZ^3 - 3abXYZ = e_2 27, \tag{5}$$

with $e_2 \in \{\pm 1\}$. Assume $a \geq 10$. Since $bY^3 - aZ^3 = \pm 9$ and $Z \neq 0$, we see that Y and Z have the same sign. We may assume that $Y, Z > 0$, and moreover that $|\varepsilon| < 1$. Since

$$\begin{aligned} Y\sqrt[3]{ab^2} + Z\sqrt[3]{a^2b} \geq \sqrt[3]{ab}(\sqrt[3]{a} + \sqrt[3]{b}) > 3\sqrt[3]{ab} > 3 \\ > |3\varepsilon| = |X + Y\sqrt[3]{ab^2} + Z\sqrt[3]{a^2b}|, \end{aligned}$$

we have $X < 0$.

Let us compute the asymptotics of X and Y in terms of Z, and of X and Z in terms of Y. Since we need exact error terms we use the so called L-notation (cf. [7]). This notation allows us to keep track of how large the constants of the usual O-terms get. The L-notation is defined as follows: For two functions $g(t_1, \dots, t_k)$ and $h(|t_1|, \dots, |t_k|)$ and positive numbers $u_1, \dots, u_k$ we write $g(t_1, \dots, t_k) = L_{u_1,\dots,u_k}(h(|t_1|, \dots, |t_k|))$ if $|g(t_1, \dots, t_k)| \leq h(|t_1|, \dots, |t_k|)$ for all $t_1, \dots, t_k$ with absolute value at least $u_1, \dots, u_k$ respectively. Note that all the following computations have been performed with Mathematica® 5.0.1.

First we compute Y in terms of Z:

$$Y = \sqrt[3]{\frac{aZ^3 + e_1 9}{b}} = Z\sqrt[3]{a/b} + \frac{3e_1\sqrt[3]{a/b}}{aZ^2} - \frac{9\sqrt[3]{a/b}}{a^2Z^5} + O(1/Z^6).$$

For further computations we need an L-term instead of an O-term. Let

$$\begin{aligned} Y^+ &= Z\sqrt[3]{a/b} + \frac{3e_1\sqrt[3]{a/b}}{aZ^2} + 11\,\frac{\sqrt[3]{a/b}}{a^2Z^5}, \\ Y^- &= Z\sqrt[3]{a/b} + \frac{3e_1\sqrt[3]{a/b}}{aZ^2} - 11\,\frac{\sqrt[3]{a/b}}{a^2Z^5}. \end{aligned}$$

Computations show

$$\begin{aligned} &-(b(Y^+)^3 - aZ^3 - e_1 9)(b(Y^-)^3 - aZ^3 - e_1 9) \\ &\qquad = (1771561 - 395307\zeta^2 - 263538e_1\zeta^3 - 14520\zeta^4 \\ &\qquad\qquad + 39204e_1\zeta^5 + 38475\zeta^6 + 11610e_1\zeta^7 + 360\zeta^8)/(a^{10}Z^{30}), \end{aligned}$$

where $\zeta = aZ^3$. This quantity is positive if $\zeta > 28.66$, in particular if $a \geq 29$

and $Z \geq 1$. This shows

$$Y(a,b,Z) = Z\sqrt[3]{a/b} + \frac{3e_1\sqrt[3]{a/b}}{aZ^2} + L_{29,1,1}\left(11\,\frac{\sqrt[3]{a/b}}{a^2Z^5}\right). \tag{6}$$

Similarly we obtain

$$Z(a,b,Y) = Y\sqrt[3]{b/a} + \frac{3e_1\sqrt[3]{b/a}}{bY^2} + L_{29,1,1}\left(11\,\frac{\sqrt[3]{b/a}}{b^2Y^5}\right). \tag{7}$$

Now let us compute X. Remember that

$$p_1 := bY^3 - aZ^3 - e_1 9 = 0, \tag{8}$$

$$p_2 := X^3 + ab^2Y^3 + a^2bZ^3 - 3abXYZ - e_2 27 = 0. \tag{9}$$

We compute the Gröbner basis of the ideal generated by p_1 and p_2 with respect to the lexicographic term order such that $X \prec Z \prec Y$. The first component of the Gröbner basis is

$$\begin{aligned} p_3 := {} & 729a^3b^3e_1 - 6561a^2b^2e_2 + 19683abe_1 - 19683e_2 + 243a^2b^2X^3 \\ & - 1458abe_1e_2X^3 + 2187X^3 + 27abe_1X^6 - 81e_2X^6 + X^9 \\ & + 486a^4b^3Z^3 - 2916a^3b^2e_1e_2Z^3 + 4374a^2bZ^3 \\ & - 135a^3b^2e_1X^3Z^3 - 324a^2be_2X^3Z^3 + 6a^2bX^6Z^3 \\ & + 108a^5b^3e_1Z^6 - 324a^4b^2e_2Z^6 - 15a^4b^2X^3Z^6 + 8a^6b^3Z^9. \end{aligned}$$

Since p_3 is a polynomial of degree 3 in X^3, it has either one or three real roots. Because p_3 comes from a Gröbner basis with lexicographic order, the solutions of p_3 for some fixed Z are the same as those of p_2 with (Y,Z) a fixed solution to p_1, with the same Z. Since the constant term is positive (remember $Y, Z \geq 1$ and $a \geq 10$), either all roots of p_2 are negative or only one is negative. The fact that the coefficient of X^2 in p_2 is zero shows that not all three roots can be negative. Therefore we deduce that there is exactly one negative root of p_3 for positive Z. If we compute the asymptotics of the solutions to p_3 in terms of Z we find that one asymptotics has the form

$$-2Z\sqrt[3]{a^2b} + \frac{3 - 3abe_1}{a^{4/3}b^{2/3}Z^2} + \frac{6 + 9abe_1(abe_1 - 1)}{a^{10/3}b^{5/3}Z^5} + O(1/Z^6).$$

Indeed, this is the desired approximation to X. Let us compute

$$-p_3(X^+, Z)p_3(X^-, Z) = \frac{229582512Z^{96}a^{68}b^{36} + \cdots}{Z^{90}a^{60}b^{30}},$$

where the rest of the numerator is a polynomial of lower degree (in each variable) and

$$X^+ = -2Z\sqrt[3]{a^2b} + \frac{3-3abe_1}{a^{4/3}b^{2/3}Z^2} + 2\,\frac{6+9ab(ab+1)}{a^{10/3}b^{5/3}Z^5},$$
$$X^- = -2Z\sqrt[3]{a^2b} + \frac{3-3abe_1}{a^{4/3}b^{2/3}Z^2} - 2\,\frac{6+9ab(ab+1)}{a^{10/3}b^{5/3}Z^5}.$$

Since the numerator is positive for $a \geq 41$, $b \geq 1$ and $Z \geq 1$, we deduce

$$X(a,b,Z) = -2Z\sqrt[3]{a^2b} + \frac{3-3abe_1}{a^{4/3}b^{2/3}Z^2} + L_{41,1,1}\left(2\,\frac{6+9ab(ab+1)}{a^{10/3}b^{5/3}Z^5}\right). \tag{10}$$

Similarly we obtain

$$X(a,b,Y) = -2Y\sqrt[3]{ab^2} + \frac{3+3abe_1}{a^{2/3}b^{4/3}Y^2} + L_{51,1,4}\left(2\,\frac{6+9ab(ab+1)}{a^{5/3}b^{10/3}Y^5}\right). \tag{11}$$

Because of the form of the L-terms we assume from now on $a \geq 51$, $b \geq 1$, $Y \geq 4$ and $Z \geq 1$.

If we substitute (6) and (10) in $(aZ^2 - XY)/3$, and (7) and (11) in $(bY^2 - XZ)/3$, we obtain

$$\begin{aligned} Y' := \frac{aZ^2 - XY}{3} &= aZ^2 + \frac{3e_1}{Z} - \frac{1}{abZ} + \frac{3}{aZ^4} - \frac{3e_1}{a^2bZ^4} \\ &+ L_{51,1,1}\left(\frac{40}{3aZ^4} + \frac{4}{a^3b^2Z^4} + \frac{6}{a^2bZ^4} + \frac{29}{a^2Z^7} + \frac{12}{a^4b^2Z^7} + \frac{29}{a^3bZ^7}\right), \end{aligned} \tag{12}$$

and

$$\begin{aligned} Z' := \frac{bY^2 - XZ}{3} &= bY^2 - \frac{3e_1}{Y} - \frac{1}{abY} + \frac{3}{bY^4} + \frac{3e_1}{ab^2Y^4} \\ &+ L_{51,1,4}\left(\frac{40}{3bY^4} + \frac{4}{a^2b^3Y^4} + \frac{6}{ab^2Y^4} + \frac{29}{b^2Y^7} + \frac{12}{a^2b^4Y^7} + \frac{29}{ab^3Y^7}\right), \end{aligned} \tag{13}$$

respectively. Note that $Z' = bY^2 + R_1$, where R_1 is small if Y, a, b are large. Remember that we assume $Y \geq 4, a \geq 51$ and $b \geq 1$. In the case of (13) we see that $|R_1| < 0.822$. Since Z' is an integer, also R_1 has to be an integer, hence $R_1 = 0$ and $Z' = bY^2$. Similarly, if we assume $Z \geq 4, a \geq 51$ and $b \geq 1$ we obtain $Y' = aZ^2 + R_2$, with $|R_2| < 0.757$. Hence $R_2 = 0$ and $Y' = aZ^2$. If $Z = 2$ then $Y' = aZ^2 + e_1 3/2 + R_3$. From (12) we compute $|R_3| < 0.031$ if $a \geq 51$ and $b \geq 1$. But this implies that Y' is not an integer and we have a contradiction. In the case of $Z = 1$ we find $Y' = a + 3e_1 + R_4$, with $|R_4| < 0.355$ if $a \geq 51$ and $b \geq 1$, hence $Y' = a + 3e_1$. Since (Y', Z') is a solution to (4) and $Y' = a + 3e_1$ and $Z' = bY^2$ we obtain

$$b(a+3e_1)^3 - a(bY^2) - 9e_1' = a^3b + 9a^2be_1 + 27ab + 27be_1 - 9e_1' - ab^3Y^6 = 0 \tag{14}$$

and therefore $b \mid 9$. Since $ab^2 \equiv \pm 1 \bmod 9$ we find $b = 1$. Now (14) has the following form:

$$a^3 + 9a^2e_1 + 27a + 27e_1 - 9e_1' - aY^6 = 0.$$

This yields $a \mid 18$ or $a \mid 36$. Since we assume $a \geq 51$ we have a contradiction.

Now, if we assume $Y \geq 4$, $a \geq 51$ and $b \geq 1$, then we have $Y' = aZ^2$ and $Z' = bY^2$. Moreover, we obtain $ba^3Z^6 - ab^3Y^6 = \pm 9$, hence $ba \mid 9$, which is again a contradiction to $a \geq 51$.

6. Small a**.** We still have to consider the case $a \leq 50$ or $Y \leq 3$. In this section we want to exclude the case $a \leq 50$. Since $ab^2 \equiv \pm 1 \bmod 9$ we have $a \equiv 1 \bmod 3$ and $b \equiv \pm a \bmod 9$. Since we assume that a and b are square-free with $\gcd(a,b) = 1$ and $a > b \geq 1$, there are only finitely many possibilities left for the pair (a,b).

For all possible pairs (a,b) we will solve the Diophantine equation $bY^3 - aZ^3 = \pm 9$ with $Z > 0$. If an equation has more than two solutions, the quantity $d = ab^2$ may satisfy the conditions of Theorem 2. In particular we prove the following lemma.

LEMMA 2. *Let* $0 < b < a \in \mathbb{Z}$, $a \leq 50$, a *and* b *square-free and* $\gcd(a,b) = 1$, *with* $ab^2 \equiv \pm 1 \bmod 9$. *Then* $(a,b) \in \mathcal{P}$, *where*

$$\begin{aligned}\mathcal{P} = \{&(46,37),(46,35),(46,19),(46,17),(46,1),(43,38),(43,34),\\ &(43,29),(43,11),(43,7),(43,2),(37,35),(37,26),(37,17),\\ &(37,10),(37,1),(34,29),(34,11),(34,7),(31,23),(31,22),\\ &(31,14),(31,13),(31,5),(22,13),(22,5),(19,17),(19,10),\\ &(19,1),(13,5),(10,1),(7,2)\}.\end{aligned}$$

Moreover, all solutions $(Y,Z) \in \mathbb{Z} \times \mathbb{Z}$ *to* $by^3 - az^3 = \pm 9$ *with* $Z > 0$ *and* $(a,b) \in \mathcal{P}$ *are listed in Table* 1.

Table 1. Solutions (Y,Z) to $by^3 - az^3 = \pm 9$ with $Z > 0$

a	b	Y	Z	Y	Z
46	37	1	1		
43	34	1	1		
31	22	1	1		
31	5	2	1		
22	13	1	1		
19	10	1	1		
10	1	1	1		
7	2	-1	1	2	1

Proof. The first part of the lemma is clear. The second part is a result of a computation in PARI [13]. In particular we solved all Thue equations of the form

$$Y'^3 - ab^2Z^3 = (bY)^3 - ab^2Z^3 = 9b^2$$

with $(a,b)\in\mathcal{P}$ and only considered solutions (Y',Z) such that $b\,|\,Y'$. Indeed, all solutions have this property. The computation took only a few seconds on a common work station. ∎

Lemma 2 tells us that the only candidate is $d=7\cdot 2^2=28$. From (5) we obtain $e_2=1$ and $X=-1$. Hence $\xi=\eta=0$ and $\zeta=-1$. Therefore $\varepsilon=-\frac{1}{3}(1+\sqrt[3]{28}-\sqrt[3]{98})$ and $\varepsilon^2=-3+\sqrt[3]{28}$. Since $(1,\theta_1:=\sqrt[3]{28},\theta_2:=\frac{1}{3}(1+\sqrt[3]{28}-\sqrt[3]{98}))$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{28}$, we have $\varepsilon=-\theta_2$ and $\varepsilon^2=\theta_1-3$. Moreover, we have

$$\overbrace{\begin{pmatrix} 1 & 0 & 0\\ 0 & 0 & -1\\ -3 & 1 & 0\end{pmatrix}}^{M:=}\begin{pmatrix}1\\ \theta_1\\ \theta_2\end{pmatrix}=\begin{pmatrix}1\\ \varepsilon\\ \varepsilon^2\end{pmatrix}.$$

Since $\det M=1$ also $1,\varepsilon,\varepsilon^2$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{28}$ and therefore $\mathcal{O}_{28}$ is generated by its units.

7. The case $Y=1$. We are left with the case $Y\le 3$. Since $3\nmid Y$ we have to consider the cases $Y=1$ and $Y=2$. By the previous section we may assume $a\ge 51$. First we consider the case $Y=1$. From (3) we get

$$b-aZ^3=\pm 9$$

or $Z^3=(b\mp 9)/a$. Since $a>b$ and $a\ge 51$ we deduce $Z=1$ and $a=b-9$. If we substitute this in (5) we obtain

$$81b+27b^2+2b^3-27e_2-27bX-3b^2X+X^3=0.$$

If we put $X=\xi'+b$ and $\eta=b$ we obtain

$$-27e_2+\xi'^3+81\eta-27\xi'\eta+3\xi'^2\eta=0,$$

hence $3\,|\,\xi'$. If we put $\xi'=3\xi$ we get the Diophantine equation

$$-e_2+\xi^3+3\eta-3\xi\eta+\xi^2\eta=0. \tag{15}$$

If we solve (15) for η we obtain

$$\begin{aligned}\eta&=-\frac{\xi^3-e_2}{\xi^2-3\xi+3}=-\xi-3-\frac{6}{\xi}+\frac{-9+e_2}{\xi^2}+O\left(\frac{1}{\xi^3}\right)\\ &=-\xi-3-L_5\left(\frac{8}{\xi}\right),\end{aligned}$$

i.e. if $\xi\ge 9$ then $\eta=-\xi-3$. But $\eta=-\xi-3$ yields $6\xi=9+e_2$. Since $\xi\in\mathbb{Z}$, this is a contradiction. So we compute η for each ξ with $-8\le\xi\le 8$. In the case of $e_2=1$ we find the solutions $(\xi,\eta)=(1,0),(2,-7),(4,-9)$ and in the case of $e_2=-1$ we find $(\xi,\eta)=(-3,0),(1,-2),(-3,-9)$. Note that $\eta=b>0$. None of these solutions yields a proper b.

8. The case $Y = 2$. Now we discuss the case $Y = 2$, that is, $8b - aZ^3 = \pm 9$ or $Z^3 = (8b \mp 9)/a$. Since $8b \mp 9$ is odd, also Z must be odd. Since $a \geq 51$ we also have $Y \geq Z > 0$, hence $Z = 1$. Therefore $a = 8b + 9e_1$ with $e_1 = \pm 1$. If we put $Y = 2,\ Z = 1$ and $a = 8b + 9e_1$ into (5) we get

$$128b^3 - 27e_2 + 216b^2e_1 + 81b - 48b^2X - 54be_1X + X^3 = 0.$$

If we use the transformation indicated by $X = \xi' + 4b$ and $b = \eta$, we get

$$-27e_2 + \xi'^3 + 81\eta - 54e_1\xi'\eta + 12\xi'^2\eta = 0.$$

Note that $3 \mid \xi'$, hence we put $\xi' = 3\xi$ to obtain

$$-e_2 + \xi^3 + 3\eta - 6e_1\xi\eta + 4\xi^2\eta = 0. \tag{16}$$

We solve (16) for η to obtain

$$\begin{aligned}\eta &= -\frac{\xi^3 - e_2}{4\xi^2 - 6e_1\xi + 3} = -\frac{\xi}{4} - \frac{3e_1}{8} - \frac{3}{8\xi} + \frac{8e_2 - 9e_1}{32\xi^2} + O\left(\frac{1}{\xi^3}\right) \\ &= -\frac{\xi}{4} - \frac{3e_1}{8} + L_6\left(\frac{1}{2\xi}\right) = -\frac{2\xi + 3e_1}{8} + L_6\left(\frac{1}{2\xi}\right).\end{aligned}$$

We see that η cannot be an integer if $\xi \geq 6$. So we compute the quantity η for each ξ with $-6 \leq \xi \leq 6$. We find that the only integral solutions are

$$\begin{aligned}(\xi, \eta) &= (3, 0), (6, -1) && \text{if } e_1 = e_2 = 1, \\ (\xi, \eta) &= (-3, 0), (3, -2) && \text{if } e_1 = -e_2 = 1, \\ (\xi, \eta) &= (3, 0), (-3, 2) && \text{if } e_1 = -e_2 = -1, \\ (\xi, \eta) &= (-3, 0), (-6, 1) && \text{if } e_1 = e_2 = -1.\end{aligned}$$

So we are reduced to $b = 2$ and $e_1 = -1$ or $b = 1$ and $e_1 = -1$. Hence $a = 7$ or $a = -1$. Thus the only proper pair is $(a, b) = (7, 2)$, which has been found above.

Acknowledgement. We are grateful to W. Narkiewicz for drawing our attention to this kind of problem.

REFERENCES

[1] N. Ashrafi and P. Vámos, *On the unit sum number of some rings*, Q. J. Math. 56 (2005), 1–12.

[2] P. Belcher, *Integers expressible as sums of distinct units*, Bull. London Math. Soc. 6 (1974), 66–68.

[3] —, *A test for integers being sums of distinct units applied to cubic fields*, J. London Math. Soc. (2) 12 (1976), 141–148.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[5] B. Delaunay, *Vollständige Lösung der unbestimmten Gleichung* $X^3q + Y^3 = 1$ *in ganzen Zahlen*, Math. Z. 28 (1928), 1–9.

[6] B. Goldsmith, S. Pabst, and A. Scott, *Unit sum numbers of rings and modules*, Q. J. Math. 49 (1998), 331–344.
[7] C. Heuberger, A. Pethő, and R. F. Tichy, *Thomas' family of Thue equations over imaginary quadratic fields*, J. Symbolic Comput. 34 (2002), 437–449.
[8] B. Jacobson, *Sums of distinct divisors and sums of distinct units*, Proc. Amer. Math. Soc. 15 (1964), 179–183.
[9] M. Jarden and W. Narkiewicz, *On sums of units*, Monatsh. Math., to appear.
[10] T. Nagell, *Solution complète de quelques équations cubiques à deux indéterminées*, J. Math. Pures Appl. 4 (1925), 209–270.
[11] C. L. Siegel, *Die Gleichung* $ax^n - by^n = c$, Math. Ann. 114 (1937), 57–68.
[12] J. Śliwa, *Sums of distinct units*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 22 (1974), 11–13.
[13] The PARI Group, Bordeaux, *PARI/GP, version 2.1.5*, 2004; http://pari.math.u-bordeaux.fr/.
[14] P. Vámos, *2-good rings*, Q. J. Math. 56 (2005), 417–430.
[15] D. Zelinsky, *Every linear transformation is a sum of nonsingular ones*, Proc. Amer. Math. Soc. 5 (1954), 627–630.

Institute of Analysis
and Computational Number Theory
Graz University of Technology
Steyrergasse 31
A-8010 Graz, Austria
E-mail: tichy@tugraz.at

Institute of Mathematics
University of Natural Resources
and Applied Life Sciences, Vienna
Gregor-Mendelstr. 31
A-1180 Vienna, Austria
E-mail: ziegler@finanz.math.tugraz.at

Received 30 August 2006;
revised 25 October 2006 (4785)