PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 91, Number 3, July 1984

ON UNITS OF CERTAIN CUBIC FIELDS AND THE DIOPHANTINE EQUATION $x^3 + y^3 + z^3 = 3$

MANNY SCAROWSKY

ABSTRACT. The Diophantine equation $x^3 + y^3 + z^3 = 3$ is replaced by a sequence of parametrized Diophantine equations which can be factored in certain cubic fields. A unit in these fields is readily available. Some results about these fields and the parametrized equations are proved.

1. Introduction. The equation

$$x^3 + y^3 + z^3 = 3 \tag{1}$$

has long been known to have as solutions in integers $(1,1,1)$, $(4,4,-5)$ and its permutations. It is conjectured that there are no more.

It is easy to see that in (1) $x \equiv y \equiv z \equiv 1 \pmod 3$ and two of x, y, z, say x, y, have the same parity. Hence we may write $x = Y - 3a$, $y = Y + 3a$, where a is an integer ≥ 0 and (1) becomes $2Y^3 + 54a^2Y + z^3 = 3$ or, letting $X = 2Y$, $Z = -z$ we have

$$X^3 + 108a^2X - 12 = 4Z^3. \tag{2}$$

Now the cubic on the left in (2) is clearly irreducible (e.g., Eisenstein's Irreducibility Criterion) and is increasing as a function of X. Thus it defines a real cubic field $K = Q(\theta)$, where θ is the real root of the cubic, with exactly one fundamental unit. Since the solutions of (2) with $a = 0$ are known [1, p. 225] and correspond to the known solutions of (1), we see that we may reformulate the conjecture that these are all the solutions of (1) as follows: *For each* $a > 0$,

$$N_{K/Q}(X - \theta) = X^3 + 108a^2X - 12 = 4Z^3$$

has no solutions in integers.

2. Properties of the field $K = Q(\theta)$. We will assume throughout that $a > 0$. Note that the discriminant of $X^3 + 108a^2X - 12$ is $-2^4 3^5(1 + 6^4a^6)$. Also $N(1 - 9a^2\theta) = N(\theta^3/12) = 1$, so that $\eta = 1 - 9a^2\theta$ is a unit of the field K.

THEOREM 1.

(i) *An integral basis for* K *is* $\{1, \theta_1, \theta_2\}$, *where* $\theta_1 = (2^4 \cdot 3^3a^4 + \theta + 6a^2\theta^2)/b, \theta_2 = \theta^2/2$, *and* b^2 *is the largest square dividing* $6^4a^6 + 1$. *The discriminant of* K *is* $D = -2^2 3^5(1 + 6^4a^6)/b^2 = -2^2 3^5 q$, *say, where* q *is square-free.*

(ii) $\eta = 1 - 9a^2\theta$ *is never the cube of a unit in* K, *and* K *is never a pure cubic field (i.e., of the form* $Q(\sqrt[3]{m})$*).*

(iii) *For fixed* b, η *is the fundamental unit or its square with a finite number of possible exceptions. If* $b = 1$, η *is the fundamental unit.*

Received by the editors January 21, 1983.
1980 *Mathematics Subject Classification.* Primary 10B10; Secondary 14G99.

(iv) *In* K, $(2)=\underline{p}^3$, $(3)=\underline{q}^3$, $(q_i)=\underline{p}_i^2\underline{q}_i$ *where* q_i *divides* 6^4a^6+1 *to an odd power and these are the only primes which ramify.*

(v) $\underline{p}$, $\underline{q}$ *are never principal ideals. It follows* $3 \mid h$, *the class-number of* K.

(vi) K *is monogenic iff there exist integers* y, z *such that* $2qy^3-54a^2yz-3bz^3=\pm 1$.

PROOF. (i) It is easy to see that $\theta^2/2$ is an integer in K. Letting $\alpha=A+B\theta+C\theta^2/2$ where $A,B,C\in\{0,1\}$ if $p=2$ and $A,B,C\in\{-1,0,1\}$ if $p=3$, one sees that $N(\alpha/p)\in\mathbf{Z}$ iff $A=B=C=0$. Thus the discriminant of $\mathbf{Z}[1,\theta,\theta^2/2]$ is minimal at the primes 2 and 3. As θ_1 is easily seen to be integral over $\mathbf{Z}$, it follows that $D=-2^23^5(1+6^4a^6)/b^2$, and that the basis is as stated.

(ii) If $\eta=1-9a^2\theta=\theta^3/12$ is a cube in K it follows that $\sqrt[3]{12}\in K$ and hence $K=Q(\sqrt[3]{12})$. As the discriminant of $Q(\sqrt[3]{12})$ is -2^23^5 it follows that $1+6^4a^6=b^2$ or $(6^2a^2)^3+36=(6b)^2$. But the solutions of $x^3+36=y^2$ are known [**10**] (and the solutions of $6x^3+1=y^2$ are easily derived from [**1**, p. 220, Theorem 5, p. 225, Theorem 6]) and are given by $(x,y)=(-2,\pm 3)$, $(0,\pm 6)$, $(4,\pm 10)$, $(12,\pm 42)$ and are not of the required form. The discriminants of pure cubic fields are of the form $-3k^2$ [**2**, p. 79].

(iii) This will be proved in the next section.

(iv) We have $(2)=(6/\theta,2)^3$ and $(3)=(\theta,3)^3$. The ramification of the q_i (and of (3)) follows from [**2**, p. 98] and the calculation of the discriminant.

(v) As $(\theta)=\underline{p}^2\underline{q}$ we need only prove this for $\underline{p}$. Assume $\underline{p}=(\alpha)$; then $\underline{p}^3=(2)=(\alpha^3)$, and so $2=\epsilon^i\alpha^3$, $i=0,1,2$, where ϵ is the fundamental unit of K. Say $\eta=\epsilon^s$, where by (ii) $3\nmid s$. Then $2^s=\eta^i\alpha^{3s}=(1/12)^i(\theta^i\alpha^s)^3$. This implies $K=Q((2^j12^i)^{1/3})$ where $j=1,2$; $i=0,1,2$. By (iii) this is impossible.

(vi) This is a straightforward calculation. Assuming $\alpha=x+y\theta_1+z\theta_2$ we find

$$|D(1,\alpha,\alpha^2)|^{1/2}=|2qy^3-54a^2yz^2-3bz^3|\cdot|D|^{1/2}.$$

This completes the proof.

We now apply these results to

$$N(X-\theta)=4Z^3. \tag{3}$$

THEOREM 2. *Let* h *be the class-number of* K, *and* C_K *its class-group. If* $3 \parallel h$, *or more generally if the* 3*-component of* C_K *is a product of cyclic groups of order* 3, *then* (3) *has no solutions.*

PROOF. First let $b=1$. Then from $N(X-\theta)=4Z^3$ we see easily that $(x-\theta)=\underline{p}^2\underline{a}^3$, where $(2)=\underline{p}^3$ and by (v) of Theorem 1 $\underline{p}$ is nonprincipal. If $3^l \parallel h$, raising both sides of this equation to the power $h/3^l$ gives a contradiciton.

Now assume $b\geq 1$. Let p_i be a prime divisor of 6^4a^6+1 to a power greater than 1, and say that $p_i^{m_i} \parallel Z$, $m_i>0$. Then we easily get

$$(x-\theta)=\underline{p}^2\prod \underline{p}_i\underline{q}_i^{3m_i-1}\prod \underline{p}_{i,1}^{a_i}\underline{p}_{i,2}^{3m_i-a_i}\underline{a}^3$$

where the first product is over (some of) the primes p_i dividing 6^4a^6+1 to an odd power, and $(p_i)=\underline{p}_i^2\underline{q}_i$, and the second product is over (some of) the primes dividing 6^4a^6+1 to an even power that split completely, and $(p_i)=\underline{p}_{i,1}\underline{p}_{i,2}\underline{p}_{i,3}$. For instance if p_i divides 6^4a^6+1 to an even power then either p_i remains prime in K, $(p_i)=p_iq_i$ or $(p_i)=\underline{p}_{i,1}\underline{p}_{i,2}\underline{p}_{i,3}$. If p_i remains prime then $(p_i)\nmid(x-\theta)$. If $(p_i)=\underline{p}_i\underline{q}_i$,

say, $\underline{p}_i^{a_i}\underline{q}_i^{b_i} \mid\mid (x-\theta)$. Then either a_i or $b_i = 0$ and correspondingly either b_i or a_i is a multiple of 3 and the factor can be absorbed in $\underline{a}^3$. If $(p_i) = \underline{p}_{i/1}\underline{p}_{i,2}\underline{p}_{i,3}$ and $\underline{p}_{i,1}^{a_i}\underline{p}_{i,2}^{b_i}\underline{p}_{i,3}^{c_i} \mid\mid (x-\theta)$ we may assume that one of a_i, b_i, c_i is 0. Say $c_i = 0$. Then $p_i^{a_i+b_i} = p_i^{3m_i}$ (upon comparing norms of both sides) and $b_i = 3m_i - a_i$.

A similar argument works for those p_i dividing 6^4a^6+1 to an odd power. Also

$$(x^2+\theta x+108a^2+\theta^2) = \prod \underline{p}_i^{6m_i-1}\underline{q}_i \prod \underline{p}_{i,1}^{3m_i-a_i}\underline{p}_{i,2}^{a_i}\underline{p}_{i,3}^{3m_i}\underline{b}^3$$

(where the products satisfy the same conditions as before). Raising both of these equations to the power $h/3^l = h'$ and noting that $\underline{q}_i^{3m_ih'} \sim \underline{p}_i^{3m_ih'} \sim \underline{a}^{3h'} \sim \underline{b}^{3h'} \sim (1)$ we get

$$(1) \sim \underline{p}^{2h'} \prod \underline{p}_i^{h'}\underline{q}_i^{-h'} \prod \underline{p}_{i,1}^{h'a_i}\underline{p}_{i,2}^{-h'a_i},$$

$$(1) \sim \prod \underline{p}_i^{-h'}\underline{q}_i^{h'} \prod \underline{p}_{i,1}^{-h'a_i}\underline{p}_{i,2}^{h'a_i}.$$

Multiplying these two equations together we get a contradiction.

As another application of Theorem 1, we show

THEOREM 3. *Let $b = 1$ (i.e. 6^4a^6+1 is square-free) and assume the class-number, h, of K, is prime to 2. Then, if a is even, $x^3+108a^2x-12 = y^2$ has no solutions.*[1]

PROOF. Under the given conditions we will prove that solving the equation is equivalent to solving the homogeneous equation

$$-9a^2F^4 - 2EF^3 + 3E^4 = -1$$

which has no solutions (mod 8) if $2 \mid a$.[1] We obtain easily that $(x-\theta) = \underline{a}^2$, and from $(h,2) = 1$ we have that $\underline{a}$ is principal, hence $x-\theta = \eta^i\alpha^2$, $i = 0,-1$, $\alpha \in \theta_K$. (Note that η and $x-\theta$ are > 0.)

Let $\alpha = A+B\theta+C\theta^2/2$, $C \geq 0$. If $i = 0$ we obtain

$$(4^a) \qquad A^2+12BC = x,$$

$$(4^b) \qquad 3C^2+2AB-108a^2BC = -1,$$

$$(4^c) \qquad B^2-27C^2a^2+AC = 0.$$

If a prime p divides C then from (4^c) it divides B which contradicts (4^b). Hence $C = 1$, and from (4^c) $A = 27C^2a^2-B^2$. Putting this in (4^b) gives $-B^3-27a^2B = -2$ which is impossible.

If $i = -1$ we obtain

$$(5^a) \qquad A^2+12BC = x,$$

$$(5^b) \qquad 3C^2+2AB-108a^2BC = -1-9a^2x,$$

$$(5^c) \qquad B^2-27C^2a^2+AC = 9a^2.$$

Multiplying (5^a) by $9a^2$ and adding to (5^b) we obtain

$$(5^d) \qquad 9a^2A^2+3C^2+2AB = -1.$$

[1] This also holds if $a^2 \equiv 1 \pmod 5$ or $a \equiv 0 \pmod{13}$.

Hence $(A, C) = 1$. Multiplying (5^d) by $9a^2$ and adding to (5^c) we obtain

$$(9a^2A + B)^2 + AC = 0.$$

Hence $C = E^2$, $A = -F^2$ and $B = EF + 9a^2F^2$. Putting this in (4^d) we obtain $-9a^2F^4 - 2F^3E + 3E^4 = -1$ as required.

REMARK 1. The tables of complex cubic fields (i.e. real fields with complex conjugates) extend only from $0 > D > -20000$ [3]. Of these, 391 have class-number divisible by 3 and 19 of those have class-number divisible by (in fact equal to) 9. These 19 have cyclic class-group. This suggests that any new solutions of (1) (if they exist) must be distributed very sparsely. Perhaps using the methods of Baker one should solve (2) for specific large values of a, for which the class-group of K has a cyclic component of order 3^m $(m \geq 2)$, as a check on the conjecture.

REMARK 2. The method of transforming $x^3 + y^3 + z^3 = k$ into an equivalent system of parametrized cubic equations seems to work only for $k = 1, 6$. For $k = 6$ the known solutions correspond to $a = 0, 9, 15, 36$ (where one can set $x = X - 6a$, $y = X + 6a$, $a \geq 0$) [4, p. 108]. For $k = 1$ one has infinite sequences of parametrized solutions [1, p. 102, 4–6]. We leave to the reader the properties of the relevant cubic fields. Unfortunately a theorem like Theorem 2 does not seem to follow readily. However the above technique may also be applied to equations of the form $x^3 + y^3 + (28 + 36k)z^3 = 6$, or one may study directly equations of the form $X^3 + 108a^2X - 18 = 9Z^3$, etc. Note also that $8x^4 + y^4 + 8 = z^4$ leads to cubic equations defining fields with known units.

3. The units of K. In this section we prove (iii) of Theorem 1 and make some other comments. Although we could follow the method of [7, 11] it is easier to use the inequality [8, p. 118] $|D| \leq 4u^3 + 24$, where u is any unit of K greater than 1. As $0 < \eta < 1$, we have $0 < \theta < 1/9a^2$. Hence $1/\eta = 1 + 3^5 \cdot 6^2a^6 + 9a^2\theta + 81a^4\theta^2 = 3^5 6^2 a^6 + \delta$, $1 < \delta < 3$. Now assume that η^{-1} is not a square; we have shown that it is not a cube. Hence if $\eta^{-1} = \epsilon^s$ (where ϵ is the fundamental unit) we may assume $s \geq 5$ and so, letting $u = (n^{-1})^{1/s}$ we have

$$\frac{2^2 \cdot 3^5(6^4a^6 + 1)}{b^2} < 4(3^5 \cdot 6^2a^6 + 3)^{3/5} + 24.$$

Thus,

$$b^2 > \frac{3^5 \cdot 6^4a^6}{(3 \cdot 6^{2/5}a^{6/5} + 1)^3 + 6} \geq \frac{3^5 \cdot 6^4a^6}{\{(3 \cdot 6^{2/5} + 1)^3 + 6\}a^{18/5}}$$

and

$$b > 29.15a^{6/5}, \tag{6}$$

if η is not a square. (Thus η is either the fundamental unit or the square of a unit if $b = 1, 5, 17, 25, 37, 41, \ldots$.)

Now we will also show that if η is a square, a is bounded (for fixed b). Assume

$$\eta = 1 - 9a^2\theta = \left(\frac{x + y\theta + z\theta^2}{2b}\right)^2, \qquad z \geq 0, x, y, z \in \mathbf{Z}.$$

Then

$$4b^2 = x^2 + 24yz, \tag{7a}$$

$$(7^b) \qquad -36a^2b^2 = 12z^2 + 2xy - yz \cdot 216a^2,$$

$$(7^c) \qquad -y^2 = 2z(-54a^2z + x).$$

(It is clear that 2 divides x and y, and 3 divides y and z.)

From (7^c) and (7^a) any common factor of z and $-54a^2z + x$ divides $2b$, so we may write $z = AE^2$ and $-54a^2AE^2 + x = BF^2$ where A, F are taken from a finite set $(A > 0)$ $(B \leq 0)$. Putting this in (7^b) we obtain

$$\begin{aligned} -36a^2b^2 &= 12A^2E^4 + [2(BF^2 + 54a^2AE^2) - AE^2 \cdot 216a^2]y \\ &= 12A^2E^4 + y(2BF^2 - 108a^2AE^2). \end{aligned}$$

If $y \leq 0$ then this is clearly impossible. Hence $y > 0$ and (as $z \neq 0$), $z > 0$. Thus from (7^a) there are a finite number of possible values for x, y, z and from (7^c) there are only a finite number of possible values of a. In particular, when one checks the case $b = 1$ (or $b = 5$) one finds all possible values of a are excluded, and hence when $b = 1$ (or $b = 5$) $\eta = 1 - 9a^2\theta$ is the fundamental unit. This proves (iii) of Theorem 1.

Comments. (1) Of course the fields defined by $x^3 + 108a^2x - 12 = 0$ were studied because of their relation to (1). The results go through without change for fields defined by $x^3 + 108ax - 12 = 0$, $a > 0$ (except that in Theorem 3, $4 \mid a$). No doubt similar results can be obtained for $x^3 + 12ax - 12 = 0$, $a > 0$.

(2) This suggests that one study the fields defined by $x^3 + abx + b = 0$, $x^4 + abx^2 + cbx + b = 0$ (which have an obvious unit), when $r = 1$, and that one try to show that this unit is 'usually' a fundamental unit.

(3) It can be shown [**2**, p. 264] that if ϵ is a fundamental unit of K then ϵ, $(\epsilon^2\epsilon')^{1/3}$ is a pair of fundamental units for $K(\sqrt{D})$ (ϵ' is a conjugate of ϵ). Thus by straightforward computations, [**2**, p. 216; **13**, p. 227] one obtains $h(K(\sqrt{D})) = h^2(K) \cdot h(Q(\sqrt{D}))$. By [**14**, p. 361 or **15**] $3 \mid h(Q(\sqrt{D}))$ and hence $27 \mid h(K(\sqrt{D}))$. Also by using the Brauer-Siegel Theorem one sees that as $a \to \infty$ through a sequence such that $6^4a^6 + 1$ is square-free, $\log h(K) \sim 3 \log a$.[2]

(4) We do not know if the fields defined by different a's are distinct. Perhaps some may coincide. For this to be so it would be necessary that the Diophantine equation $6^4a^6 + 1 = b^2q$ has for fixed q, two or more distinct solutions.

(5) Finally, we make a conjecture not related to the above. If $\eta = 1 - 9a^2\theta$ is the fundamental unit of K it follows that all solutions of $x^3 + 108a^2xw^2 - 12w^3 = 1$ are given by

$$x - \theta w = \eta^n = (1 - 9a^2\theta)^n, \qquad n \in \mathbf{Z}.$$

The obvious solutions are given by $n = 0, 1$. One may conjecture that these are the only solutions. It is known that there is at most one more solution [**1**, p. 218].

NOTE ADDED IN PROOF. Using the method of [**9**] the class-number of K was calculated for $a = 1$ and was found to be 12. Thus one may apply Theorem 2 to this case.

REFERENCES

1. L. J. Mordell, *Diophantine equations*, Academic Press, New York, 1969.

[2] Also it may be shown from [**16**] that if r_3 is the 3-rank of K and if r_2 is the 3-rank of $Q(\sqrt{\theta})$ that $r_2 \leq r_3 \leq r_2 + 1$.

2. H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer-Verlag, Berlin and New York, 1978.
3. I. O. Angell, *A table of complex cubic fields*, Bull. London Math. Soc. **5** (1973), 37–38.
4. J. C. P. Miller and M. F. C. Woolett, *Solutions of the Diophantine equation* $x^3 + y^3 + z^3 = k$, J. London Math. Soc. **28** (1955), 101–110.
5. L. J. Mordell, *On an infinity of integer solutions of* $ax^3 + ay^3 + bz^3 = bc^3$, J. London Math. Soc. **28** (1955), 111–113.
6. D. H. Lehmer, *On the Diophantine equation* $x^3 + y^3 + z^3 = 1$, J. London Math. Soc. **28** (1955), 275–280.
7. H. J. Stender, *Über die Grundenheit für spezielle unendlichen Klassen reiner kubischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **33** (1969), 203–215.
8. P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967.
9. D. Shanks, *The simplest cubic fields*, Math. of Comp. **28** (1974), 1137–1152.
10. O. Hemer, *Notes on the Diophantine equation* $y^2 - k = x^3$, Ark. Math. **3** (1954), 67–77.
11. L. Bernstein, *On units and fundamental units*, J. Reine Angew. Math. **257** (1972), 129–145.
12. B. Setzer, *Units in totally complex* S_3 *fields*, J. Number Theory **10** (1978), 244–249.
13. J. W. S. Cassels and A. Frohlich, *Algebraic number theory*, Academic Press, London.
14. H. Lang and R. Schertz, *Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper*, J. Number Theory **8** (1976), 352–365.
15 K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.
16. F. Gerth III, *Ranks of* 3*-class groups of non-Galois cubic fields*, Acta Arith. **30** (1976), 307–322.

Department of Mathematics, Loyola Campus, Condordia University, Montreal, Canada H4B 1R6