Application of Gröbner bases to the resolution of systems of norm equations

Attila Pethö *
Mathematical Institute
Kossuth Lajos University
H-4010 Debrecen, P.O.Box 12
Hungary

November 28, 2009

1 Introduction

Let $\mathbb{K}$ be a cubic extension of the rational number field Q . Denote by $\mathbb{Z}_{\mathbb{K}}$ the ring of integers of $\mathbb{K}$ and by $N_{\mathbb{K}/Q}(\gamma)$ the norm of $\gamma \in \mathbb{K}$. Let $P(x) = x^2 + cx + d \in \mathbb{Z}[x]$ and $a, b, n_1, n_2, n_3, \in \mathbb{Z}$. In this paper we give necessary and sufficient conditions for the existance of cubic number fields $\mathbb{K}$ and elements $\eta \in \mathbb{Z}_{\mathbb{K}}$ such that

$$\left\{ \begin{array}{lcl} N_{\mathbb{K}/Q}(\eta) & = & n_1 \\ N_{\mathbb{K}/Q}(\eta - a) & = & n_2 \\ N_{\mathbb{K}/Q}(\eta - b) & = & n_3 \end{array} \right. \qquad (1)$$

or

$$\left\{ \begin{array}{lcl} N_{\mathbb{K}/Q}(\eta) & = & n_1 \\ N_{\mathbb{K}/Q}(P(\eta)) & = & n_2. \end{array} \right. \qquad (2)$$

If (1) as well as (2) is solvable in the sense described above, our theorems immediately imply methods for determining all solutions.
The problem originates from the theory of elliptic curves over algebraic number fields, and is closely related to the determination of torsion groups as described in Fung et al. [2]. Let

$$E : Y^2 = X^3 + AX + B, \quad (A, B \in \mathbb{K})$$

be an elliptic curve in short Weierstrass form. E has discriminant

$$\delta_0 = 4A^3 + 27B^2$$

and absolute invariant

$$j = 12^3 \frac{4A^3}{\delta_0}$$

(cf.[9]). We consider the abelian group of rational points of E over $\mathbb{K}$

$$E(\mathbb{K}) = \{P = (x, y) \in \mathbb{K}^2 | y^2 = x^3 + Ax + B\} \cup \{0\},$$

where the point at infinity $0 = (\infty, \infty)$ serves as the neutral element of addition. By the Mordell-Weil Theorem (see [9]), this group is finitely generated so that we have

$$E(\mathbb{K}) \simeq E_{Tor}(\mathbb{K}) \oplus \mathbb{Z}^r$$

with the finite torsion group $E_{Tor}(\mathbb{K})$ and the rank $r \in \mathbb{N}_0$ of E over $\mathbb{K}$. Fung at al.[2] determined the torsion groups

$$E_{Tor}(\mathbb{K}) \leq E(\mathbb{K})$$

of all elliptic curves E with integral j-invariant over pure cubic fields $\mathbb{K}$. Using well-known results on elliptic curves, they transformed this problem into that of solving finitely many systems of equations of the form (1) or (2). For the resolution of (1) and (2) they used detailed knowledge of the arithmetic of pure cubic number fields. For example, they used an explicit form of integral bases of these number fields. Similar techniques were used by Wentz [8], who partially determined the torsion groups of elliptic curves E with integral j-invariant over cyclic cubic number fields. We show in this paper that by computing the Gröbner bases of suitably defined ideals in $Q[X, Y, Z]$, it is possible to determine all cubic number fields $\mathbb{K}$ in which (1) as well as (2) has solutions, and we are able to find all solutions without using any knowledge on the arithmetic of $\mathbb{K}$. For the theory of Gröbner bases, we refer to Buchberger [1]. In

a forthcoming paper we shall generalize the results of Fung et al.[2] to arbitrary cubic number fields. All computations were performed by means of the computer algebra system MAPLE on a SUN 4-60 workstation of the Fachbereich 14 - Informatik, Universität des Saarlandes.

2 The resolution of (1)

In this section let $a, b, n_1, n_2, n_3, \in \mathbb{Z}$ such that $a \neq b$ and $ab \neq 0$.
Put

$$m_1 = \frac{n_1(a-b) + bn_2 - an_3}{ab(a-b)},$$

$$m_2 = \frac{n_1(a^2-b^2) + b^2 n_2 - a^2 n_3}{ab(a-b)},$$

and

$$p_3(z) = z^3 - (a+b+m_1)z^2 + (ab+m_2)z - n_1.$$

Using this notation we prove

Theorem 1 *Suppose that there exists a cubic number field $\mathbb{K}$ and an integer $\eta \in \mathbb{Z}_{\mathbb{K}}$ such that (1) is satisfied. Then we have $m_1, m_2 \in \mathbb{Z}$, and η is a zero of $p_3(z)$. Conversely, if $m_1, m_2 \in \mathbb{Z}$ and $p_3(z)$ is irreducible in $Q[z]$, and η is a zero of $p_3(z)$, then up to isomorphism $\mathbb{K} = Q(\eta)$ is the unique cubic number field for which (1) is solvable.*

Proof: Let

$$F = \{f_1 = xyz - n_1, f_2 = (x-a)(y-a)(z-a) - n_2, f_3 = (x-b)(y-b)$$

be a basis of the ideal I in $Q[x, y, z]$. Computing the Gröbner basis G of I, corresponding to the lexical ordering $<$ with $x < y < z$ of the power product, we get

$$G = \{p_1 = ab(a-b)(x+y+z-(a+b+m_1)), p_2(y,z), ab(a-b)p_3(z)\},$$

where

$$deg_y p_2(y,z) = 2.$$

Suppose that there exists a cubic number field $\mathbb{K}$ and $\eta \in \mathbb{Z}_{\mathbb{K}}$ satisfying (1). Denote by $\eta_1, \eta_2, \eta_3 = \eta$ the conjugates of η. Then $f_1(\eta_1, \eta_2, \eta_3) = f_2(\eta_1, \eta_2, \eta_3) = f_3(\eta_1, \eta_2, \eta_3) = 0$, hence all polynominals of I vanish at the point (η_1, η_2, η_3). Thus η is a zero of $ab(a-b)p_3(z)$, hence of $p_3(z)$. As $\eta \in \mathbb{Z}_{\mathbb{K}}$, we have that either $\eta \in \mathbb{Z}$ or $\eta \in \mathbb{Z}_{\mathbb{K}} \backslash \mathbb{Z}$. In the second case we immediately get $p_3(z) \in \mathbb{Z}[x]$ and $m_1, m_2 \in \mathbb{Z}$. If $\eta \in \mathbb{Z}$, then $n_1 = \eta^3, n_2 = (\eta - a)^3$ and

$n_3 = (\eta - b)^3$ and an easy computation shows that

$$m_1 = 3\eta - a - b \in \mathbb{Z}$$

and

$$m_2 = 3\eta^2 - ab \in \mathbb{Z},$$

so that the first assertion is proved.

Assume now that $m_1, m_2 \in \mathbb{Z}$, and $p_3(z)$ is irreducible over $Q[z]$. Let $\eta_1, \eta_2, \eta_3 = \eta$ be the zeros of $p_3(z)$. It follows from the first assertion that a cubic number field $\mathbb{K}$ for which (1) is solvable is isomorphic to one of the fields $Q(\eta_i), i = 1, 2, 3$. We show that $\eta \in Q(\eta)$ is indeed a solution.

As $p_2(y, \eta)$ is a quadratic polynomial over $Q(\eta)[y]$, it has two zeros β, β_1 in C. For the pair (β, η) there exists a unique $\alpha \in C$ such that $p_1(\alpha, \beta, \eta) = 0$. Hence the point (α, β, η) is a zero of the ideal I. Especially, we have $f_1(\alpha, \beta, \eta) = 0$, i.e. α and β solve the following system of equations

$$\begin{array}{lcl} \alpha + \beta & = & a + b + m_1 - \eta \\ \alpha\beta & = & \frac{n_1}{\eta}. \end{array} \tag{3}$$

Observe that the irreducibility of $p_3(z)$ implies that $\eta \neq 0$. On the other hand, the pair (η_1, η_2) satisfies (3) too, hence (α, β) is a permutation of (η_1, η_2). We may assume without loss of generality that $\alpha = \eta_1, \beta = \eta_2$. Thus η is a solution of (1) and the theorem is proved. □

Example 1 *Let $n_1 = n_2 = n_3 = 1$. Then $m_1 = m_2 = 0$ and we get*

$$p_3(z) = z^3 - (a + b)z^2 + abz - 1.$$

If $\eta \in \mathbb{Z}$ is a solution of (1) , then the first equation of (1) implies $\eta = 1$. The second and third equations are solvable for $\eta = 1$ only if $a = b = 0$. Hence, by means of Theorem 1, if $(a, b) \neq (0, 0)$ then (1) is solvable in a cubic number field if and only if $p_3(z)$ is irreducible . And this holds if $b \neq 1$ or $(a, b) \neq (0, 0), (2, 2), (0, -3), (-4, 2), (-2, 4)$.

Remark 1 *If $(a, b) \neq (0, 0)$ as well as $(c, d) \neq (0, 0)$, then the finiteness of the number of solutions of (1) or (2) follows easily from the theory of exceptional units. (see [4], [2]). It is also known that unit equations in two variables are effectively solvable, [3]. But using this general result we were unable to decide for which cubic number fields (1) or (2) is solvable. Even for a given number field $\mathbb{K}$ the resolution of a unit equation turns out to be a hard computational problem (see [5], [7]).*

3 The resolution of (2)

In this section we assume that $P(x) = x^2 + cx + d \in \mathbb{Z}[x]$ is irreducible over $Q[x]$. In the opposite case, let $a, b \in \mathbb{Z}$ be the zeros of $P(x)$. Then we have

$$N_{\mathbb{K}/Q}(P(\eta)) = N_{\mathbb{K}/Q}(\eta - a) N_{\mathbb{K}/Q}(\eta - b) = n_2$$

and we get (1), which was studied in section 2.

In the sequel, let $D = c^2 - 4d$ denote the discriminant of $P(x)$. Note that $d \neq 0$ by the irreducibility of $P(x)$. Our main result is

Theorem 2 . *Suppose that there exists a cubic number field $\mathbb{K}$ and $\eta \in \mathbb{Z}_{\mathbb{K}} \backslash \mathbb{Z}$ satisfying (2). Then there exist $w, v, m_1 \in \mathbb{Z}$ such that*

$$w^2 - D(vd + cd - n_1)^2 = 4dn_2, \tag{4}$$

$$m_1 = d - \frac{c(vd + cd + n_1) + w}{2d}, \tag{5}$$

and η is a zero of the irreducible polynominal

$$p_3(z) = z^3 - vz^2 + m_1 z - n_1.$$

Conversely, assume that there exist integers w, v, m_1 such that (4) and (5) hold and that $p_3(z)$ is irreducible. Denote by η one of the zeros of $p_3(z)$. Then, in the cubic number field $\mathbb{K} = Q(\eta)$, (2) has the solution $\eta \in \mathbb{Z}_{\mathbb{K}}$.

Proof: Let

$$F = \{f_1 = x+y+z-v, f_2 = xyz-n_1, f_3 = P(x)P(y)P(z)+n_2\}$$

be a basis of the ideal I in $Q[x, y, z]$. Computing the Gröbner basis G of I as in the proof of Theorem 1 we get

$$G = \{f_1, p_2(y, z), p_6(z)\},$$

where $p_2(y, z) = n_1dy^2 + \hat{p}_2(y, z)$ with a polynominl $\hat{p}_2(y, z)$ which is linear in y, and

$$\begin{aligned} p_6(z) &= dz^6 - 2vdz^5 + (v^2d - vcd + 2d^2 - c^2d - n_1c)z^4 \\ &+(v^2cd + vc^2d - 2vd^2 + vn_1c - 2n_1d)z^3 \\ &+(v^2d^2 + vcd^2 + vn_1c^2 + d^3 - 3n_1cd + n_1c^3 + (n_1^2 - n_2))z^2 \\ &+(vn_1cd - 2n_1d^2 + n_1c^2d + n_1^2c)z + n_1^2d \in \mathbb{Z}[z]. \end{aligned}$$

Suppose that there exists a cubic number field $\mathbb{K}$ and an $\eta \in \mathbb{Z}_{\mathbb{K}} \backslash \mathbb{Z}$ such that (2) holds. Denote by $\eta_1, \eta_2, \eta_3 = \eta$ the conjugates of η and let

$$p(z) = z^3 - vz^2 + m_1z - n_1 \in \mathbb{Z}[z]$$

be the minimal polynomial of η in $Q(z)$. In order to determine the possible $\eta's$, we have to find restrictions on the integers v and m_1. As $\eta_1 + \eta_2 + \eta_3 = v$, the point (η_1, η_2, η_3) is a zero of the ideal I. Thus η_3 is a common zero of $p_6(z)$ and $p(z)$ in C, and since $p(z)$ is irreducible, $p(z)|p_6(z)$. It is easy to see that

$$\frac{p_6(z)}{p(z)} = dz^3 - dvz^2 + m_2z - n_1d = \hat{p}_3(z),$$

where $m_2 \in \mathbb{Z}$. Comparing coefficients in $p_6(z)$ and $p(z)\hat{p}_3(z)$, we obtain the following system of equations for m_1 and m_2.

$$\begin{aligned} m_1d + m_2 &= -vcd + 2d^2 - c^2d - n_1c \\ m_1m_2 &= v^2d^2 + vcd^2 - 2vdn_1 + vc^2n_1 + d^3 - 3cdn_1 + n_1^2 + n_1c^3 - n_2. \end{aligned} \tag{6}$$

From this system we get a quadratic equation for m_1. Since m_1 must be an integer, the discriminant of this equation is a square of an integer w. Computing the discriminant we get equation (4) for the integers v,w, and equation (5) for m_1. This proves the first assertion. The proof of the second assertion is similar to the one of the second assertion Theorem 1 and is therefore omitted.

Corollary 1 *If $D < 0$, than there exist only finitely many cubic number fields $\mathbb{K}$ for which (2) is solvable.*

Proof: If $D < 0$, then for any given $c, d, n_1 \in \mathbb{Z}$, (4) has only finitely many solutions in $(v, w) \in \mathbb{Z}^2$. Hence, the number of possibilities for m_1 is finite too, and the assertion is proved. □

Corollary 2 *Let $D > 0$ and suppose that D is not a square of an integer. If there exists a cubic number field $\mathbb{K}$ and an $\eta \in \mathbb{Z}_{\mathbb{K}} \backslash \mathbb{Z}$ satisfying (2), than there exist infinitely many distinct cubic number fields $\mathbb{K}_i$ $i = 1, 2, ...$ and elements $\eta_i \in \mathbb{Z}_{\mathbb{K}_i} \backslash \mathbb{Z}$ satisfying (2).*

Proof: By hypothesis, (2) has a non-rational integral solution. Hence, by Theorem 2, there exist $v_o, w_o, m_{1o} \in \mathbb{Z}$ such that (4) and (5) hold.
Let $D = f^2F$ with $f, F \in \mathbb{Z}$ and F square free. Put $\mathbb{L} = Q(\sqrt{F})$ and $O = \mathbb{Z}[f\sqrt{F}]$. Then O is an order in $\mathbb{L}$ and the group of its units with norm 1 has rank 1. Let ϵ be a generator of this group and put

$$\tau_o = w_o + (v_od + cd - n_1)f\sqrt{F}.$$

Then, by the hypothesis

$$N_{\mathbb{L}/Q}(\tau_o) = 4dn_2.$$

For $m \in N_o$, set

$$\hat{w}_m + \hat{v}_m f\sqrt{F} = \tau_o \cdot \epsilon^m = \tau_m \tag{7}$$

with $\hat{w}_m, \hat{v}_m \in \mathbb{Z}$. Then $N_{\mathbb{L}/Q}(\tau_m) = 4dn_2$.

In the sequel denote by ξ' the conjugate of $\xi \in \mathbb{L}$. Then we have from equation (7)

$$\hat{v}_m = \frac{\tau\epsilon^m - \tau'\epsilon'^m}{2f\sqrt{F}}$$

and

$$\hat{w}_m = \frac{\tau\epsilon^m + \tau'\epsilon'^m}{2}.$$

The sequences $\{\hat{v_m}\}_{m=0}^{\infty}$ and $\{\hat{w_m}\}_{m=0}^{\infty}$ both satisfy the recursive relation

$$x_{m+2} = (\epsilon + \epsilon')x_{m+1} - x_m. \tag{8}$$

Hence the sequence $\{\hat{v}_m \quad mod \quad M\}_{m=0}^{\infty}$ is purelly periodic for any $M \in \mathbb{Z}$ (cf.[6]). Let p be the length of period of the sequence $\{\hat{v}_m \quad mod \quad d\}_{m=0}^{\infty}$. Then

$$\hat{v}_{kp} \equiv \hat{v}_o = v_o d + cd - n_1 \quad (mod \quad d).$$

Let $w_k = w_{kp}$ and $v_k = (\hat{v}_{kp} - cd + n_1)/d, (k \geq 0)$, then $v_k \in \mathbb{Z}$, and (7) implies that (w_k, v_k) is a solution of (4) for any $k \geq 0$. Put

$$m_{1,k} = d - \frac{c(v_k d + cd + n_1) + w_k}{2d}$$

Then one can prove in a similar manner that $m_{1,k} \in \mathbb{Z}$ for infinitely many $k \in \mathbb{N}_o$.
Of the polynomials

$$p_{3,k}(z) = z^3 - v_k z^2 + m_{1,k} z - n_1,$$

only finitely many are reducible. By Remark 1, for any fixed number field, (2) has only finitely many solutions. So the number of distinct number fields for which (2) is solvable is infinite. The corollary is proved.

Remark 2 *Using the method of proof of the Lemma in section 7 of [2], it is possible to see that if $D > 0$, then there exist only finitely many cubic number fields with negative discriminant for which (2) is solvable.*

Example 2 *Take $n_1 = \pm 1, n_2 = \pm 5$ and $P(x) = x^2 - 11x - 1$ in (2). Then (4) becomes*

$$w^2 - 125(-v + 11 \pm 1)^2 = \pm 20.$$

Hence $5|w$ and so 25 divides the left hand side but obviously does not divide the right hand side of this equation. Thus (2) is not solvable for those values of the parameters.

Example 3 *Take $n_1 = \pm 1, n_2 = \pm 5^4, P(x) = x^2 - 11x - 1$ in (2). Then (4) becomes*

$$w^2 - 125(-v + 11 - n_1)^2 = \pm 4 \cdot 5^4.$$

Putting $w = 25w_1$ we get

$$w_1^2 - 5(\frac{-v + 11 - n_1}{5})^2 = \pm 4.$$

The solutions of this equation are

$$w_1 = \pm(\alpha^n + \beta^n) \equiv \pm L_n$$

and

$$-v + 11 - n_1 = \pm 5 \cdot \frac{\alpha^n - \beta^n}{\sqrt{5}} = \pm 5F_n,$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Hence $\{F_n\}_{n=o}^{\infty}$ is the Fibonacci sequence, and $\{L_n\}_{n=o}^{\infty}$ is the Lucas sequence.

We have

$$m_1 = -1 - 11 - n_1 + \frac{\pm 55F_n \pm 25L_n}{2}$$

by (5). For any $n \geq 0$ these m_1 's are integers because we have $F_n \equiv L_n$ (mod 2) for any $n \geq 0$. In the following table we listed the coefficients and discriminants of all cubic polynomials that generate cubic number fields with negative discriminants for which (2) is solvable for the above parameters.

coefficients in decreasing order				discrimi		
1	-5	-2	-1	-575	$=$	$-$
1	-15	3	-1	-10800	$=$	$-$
1	-20	-7	-1	-13575	$=$	$-$
1	-75	-17	-1	-65200	$=$	$-$
1	-25	158	-1	-166175	$=$	$-$

References

[1] B. Buchberger, *Ein Algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems,* Aequationes Math.,**4** (1970) 374-383.

[2] G.W. Fung, H. Ströher, H.C. Williams and H.G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over pure cubic fields,* J. Number Theory, **36** (1990) 12-45.

[3] K. Győry, *On the solutions of linear diophantine equations in algebraic integers of bounded norm,* Ann. Univ. Sci. Eötvös , Sect. Math., **22-23** (1979-1980), 225-233.

[4] S. Lang, *"Fundamentals of Diophantine Geometry," Springer-Verlag,* New York/Berlin/Heidelberg/Tokyo, 1983.

[5] A. Pethö, *Computational methods for the resolution of diophantine equations,* in: "Number Theory" Ed.: R.A. Mollin, de Gruyter Verlag, 1988, 479-492.

[6] A. Pethö, *Divisibility properties of linear recursive sequences,* in: "Number Theory" Eds.: K. Győry and G. Halász, Coll. Math. Soc. János Bolyai Vol. **51**., 1990, 899-915.

[7] B.M.M. de Weger, *"Algorithms for Diophantine Equations,"* CWI Tract **65**., 1989.

[8] Ch. Wentz, *"Die Torsionsgruppe elliptischer Kurven mit ganzer j-Invariante über zyklisch kubischen Zahlkörpern,"* Diploma Thesis, Saarbrücken, 1990.

[9] H.G,. Zimmer, *"Zur Arithmetik der elliptischen Kurven,"* Bericht Nr. 271 (1986) der Mathematisch-Statistischen Sektion in der Forschungsgesellschaft Joanneum, A-8010 Graz, Austria, Steyrergasse 17.