Publ. Math. Debrecen
56 / 3-4 (2000), 535–546

On Legendre's equation over number fields

By MICHAEL E. POHST (Berlin)

Dedicated to Kálmán Győry on his 60th birthday

Abstract. In this paper we improve on Siegels's bound for the smallest integral solution of the equation $ax^2 + by^2 + cz^2 = 0$ for given integers a, b, c of an algebraic number field F.

1. Introduction

Throughout this paper F denotes an algebraic number field of degree n over the rational numbers $\mathbb{Q}$. We assume that it is generated by a root ρ of a monic irreducible polynomial

$$f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \quad \in \mathbb{Z}[t]. \tag{1.1}$$

Over the complex numbers $\mathbb{C}$ the polynomial $f(t)$ splits into a product of linear factors

$$f(t) = \prod_{j=1}^{n} \left(t - \rho^{(j)}\right), \tag{1.2}$$

where the *conjugates* $\rho = \rho^{(1)}, \ldots, \rho^{(n)}$ are ordered as usual, i.e. $\rho^{(1)}, \ldots, \rho^{(r_1)} \in \mathbb{R}$ and $\rho^{(r_1+1)}, \ldots, \rho^{(n)} \in \mathbb{C} \setminus \mathbb{R}$ subject to $\rho^{(r_1+j)} = \overline{\rho^{(r_1+r_2+j)}} \quad (1 \le j \le r_2)$. Especially, we have

$$n = r_1 + 2r_2. \tag{1.3}$$

Mathematics Subject Classification: 11D09, 11Y40, 11H55.
Key words and phrases: Legendre's equation.

Any element α of $\mathbb{F}$ can be presented as a linear combination of $1, \rho, \ldots$ $\ldots, \rho^{n-1}$ with rational coefficients. Substituting $\rho^{(j)}$ for ρ in that presentation we obtain the j-th conjugate $\alpha^{(j)}$ of α $(1 \leq j \leq n)$. Arithmetical problems usually require computations with *algebraic integers* contained in $\mathbb{F}$, i.e. those elements of $\mathbb{F}$ whose minimal polynomials have coefficients in $\mathbb{Z}$. They form a ring o_F with a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ (*integral basis* of F), the so-called *maximal order* of F. It is related to a very important invariant of F, the *discriminant* d_F of F, via

$$d_F = \left(\det \left(\left(\omega_i^{(j)} \right)_{1 \leq i,j \leq n} \right) \right)^2. \tag{1.4}$$

In order to make o_F a lattice we equip F with a scalar product in the usual way:

$$\langle\ ,\ \rangle : F \times F \to \mathbb{R}^{\geq 0} : (x, y) \mapsto \langle x, y \rangle = \sum_{j=1}^{n} x^{(j)} \overline{y^{(j)}}. \tag{1.5}$$

Fixing the basis $\omega_1, \ldots, \omega_n$ of o_F then $\langle x, x \rangle$ becomes a positive definite quadratic form with coefficient matrix $A = (\langle \omega_i, \omega_j \rangle)_{1 \leq i,j \leq n}$ and (o_F, A) becomes a lattice. We observe that the entries of that Gram matrix are real algebraic integers which belong to $\mathbb{Z}$ in case all zeros of $f(t)$ are real, i.e. the field F is *totally real*. The determinant of the Gram matrix is just $|d_F|$.

We note that the last considerations remain valid, if we replace o_F by any *order* R of F, i.e. a subring of o_F of finite index $(o_F : R)$ ($\mathbb{Z}$-module index). In that case the discriminant of R, obtained from a $\mathbb{Z}$-basis of R as in (1.4), is denoted by d_R. The Gram matrix of that basis has determinant $|d_R|$.

Considering elements x of F as vectors of all conjugates $(x^{(1)}, \ldots, x^{(n)})$, we have besides the norm from F

$$N(x) = \prod_{j=1}^{n} x^{(j)}$$

also the well known norms from n-dimensional Euclidean space. In the sequel we use the *maximum norm*

$$\|x\|_\infty = \max \left\{ |x^{(j)}| \mid 1 \leq j \leq n \right\}$$

and the *Euclidean norm*

$$\|x\|_2 = \sqrt{\langle x, x\rangle}.$$

In this paper we improve on SIEGEL's bounds [4] for the smallest integral solution of Legendre's equation

$$ax^2 + by^2 + cz^2 = 0 \quad (abc \neq 0) \tag{1.6}$$

over a given algebraic number field F. These better bounds are of importance for the calculation of the solutions and needed in connection with the computation of the solutions of relative quartic index form equations [2]. The result is of theoretical interest also, since it supports the observation made in [3] that the Euclidean norm seems to yield better bounds than the maximum norm for problems in algebraic number fields. Since Siegel uses a different norm than we do, we need to be more precise about the quality of our results. Our new bounds are always better in the sense that the resulting search area for a solution has a much smaller volume.

2. Representation of 0 by ternary quadratic forms

Legendre's equation is a special case of a non-degenerate ternary quadratic form representing zero. A representation of zero is always supposed to be non-trivial, i.e., a solution with at least one non-zero coordinate exists. Let us assume that a non-degenerate ternary quadratic form is given over an integral domain R with quotient field F:

$$Q := Q(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j \quad (a_{ij} \in R,\ a_{ij} = a_{ji}). \tag{2.7}$$

It is obvious that Q represents 0 over R, if and only if it represents 0 over F. But over F we can transform the variables x_1, x_2, x_3 linearly into x, y, z such that Q becomes a sum of three squares. Hence, the representation of 0 needs to be discussed only for these forms.

Because of possibly occuring denominators during a transformation of the variables we shortly discuss the relation between integer solutions of (2.7) and of the diagonalized form $Q = ax^2 + by^2 + cz^2$. At first, let

us assume that $d := a_{11}(a_{11}a_{22} - a_{12}^2) \neq 0$, eventually after reordering the variables. In that case quadratic supplementing of (2.7) yields

$$Q = a_{11}\left(x_1+\frac{a_{12}}{a_{11}}x_2+\frac{a_{13}}{a_{11}}x_3\right)^2 + \frac{a_{11}a_{22}-a_{12}^2}{a_{11}}\left(x_2 + \frac{a_{11}a_{23}-a_{12}a_{13}}{a_{11}a_{22}-a_{12}^2}x_3\right)^2$$
$$+ \frac{(a_{11}a_{22} - a_{12}^2)(a_{11}a_{33} - a_{13}^2) - (a_{11}a_{23} - a_{12}a_{13})^2}{a_{11}(a_{11}a_{22} - a_{12}^2)}x_3^2 = 0.$$

Therefore we just need to multiply Q by d to obtain a sum of three squares with coefficients in R. In the remaining cases we either have
$a_{11} \neq 0$ but $a_{11}a_{22} - a_{12}^2 = a_{11}a_{33} - a_{13}^2 = 0$,
or all diagonal elements vanish.

If the first possibility occurs we substitute (x_1, x_2, x_3) by $(y_1, y_2 + y_3, y_2 - y_3)$. For the other case we assume that $a_{12}a_{13} \neq 0$ (after eventually reordering the variables). Then a substitution of (x_1, x_2, x_3) by $(y_1 + y_2, y_1 - y_2, y_3)$ puts us into a situation already discussed, i.e., the coefficient of y_1^2 does not vanish. Hence, the assumption $Q = ax^2 + by^2 + cz^2$ is justified.

In the case of R being the maximal order of an algebraic number field F the existence of a solution of $Q = 0$ is easily decidable by congruence methods. Let $\mathcal{S}$ be the set of all non-zero prime ideals of R which contain at least one of the coefficients a, b, c. Then a necessary and sufficient condition for Q representing 0 is that

(i) $Q^{(j)}$ represents 0 in $\mathbb{R}$ for $1 \leq j \leq r_1$
and

(ii) Q represents 0 in the completions $R_{\mathbf{p}}$ for all but at most one $\mathbf{p} \in \mathcal{S}$.

This is the theorem of Hasse–Minkowski and usually refered to as the local global principle.

In case R is an arbitrary order, the test for a representation of 0 is also carried out in o_F. We note that in the beginning the quadratic form under consideration must indeed be tested, whether it represents zero. Bounds for a solution are obtained only under the assumption that a solution exists at all.

We shall derive bounds for a small solution of $Q = 0$ by following Siegel's ideas (some of which go back to Thue) but using the Euclidean norm instead of the maximum norm. This not only gives better bounds, but it also simplifies the presentation. For example, a superfluous discussion of 3^n cases can be avoided. We consider (1.6) over an order R of F

$(a, b, c \in R)$. We assume that a solution $(\xi, \eta, \zeta) \in R^3 \setminus \{\mathbf{0}\}$ exists. We note that a representation of zero over R is then tantamount to the n equations

$$a^{(\kappa)}(\xi^{(\kappa)})^2 + b^{(\kappa)}(\eta^{(\kappa)})^2 + c^{(\kappa)}(\zeta^{(\kappa)})^2 = 0 \quad (1 \le \kappa \le n).$$

For an easier understanding of Siegel's method we give a short overview on its important steps.

In Step 1 the existence of elements $u, v, w \in R$ of relatively small norm subject to $u\xi + v\eta + w\zeta = 0$ is shown. Siegel does this by using the maximum norm for the conjugates of u, v, w. He obtains his result from Minkowkski's theorem on linear forms. We instead apply Minkowski's theorem on successive minima using a T_2-norm with suitable weights.

In Step 2 the projective line $ux + vy + wz = 0$ is considered. It intersects the cone $ax^2 + by^2 + cz^2 = 0$ obviously in the point (ξ, η, ζ) and in a second point with coordinates, say, $(X, Y, Z) \in F^3$. For the conjugates of X, Y, Z, respectively for the sum of their absolute values, we get upper bounds from Step 1. Finally, a transition from X, Y, Z to integral coordinates yields the result.

Theorem 2.1 (Siegel). *If the diophantine equation $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ has a non-trivial solution in the number field F, then it also has an integral solution X_1, X_2, X_3 whose conjugates $X_l^{(\kappa)}$ $(1 \le l \le 3,\ 1 \le \kappa \le n)$ satisfy*

$$\left|\frac{X_1^{(\kappa)}}{\sqrt{a_2^{(\kappa)}a_3^{(\kappa)}}}\right| < 6|d_R|^{2/n}, \quad \left|\frac{X_2^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_3^{(\kappa)}}}\right| < 6|d_R|^{2/n}, \quad \left|\frac{X_3^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_2^{(\kappa)}}}\right| < 6|d_R|^{2/n}.$$

The major improvements obtained in this paper are better estimates in Step 1. Also, the bounds in Step 2 are better inasmuch as they describe a search area of smaller volume. They are a whole lot better for totally real fields F, a case which is not treated separately by Siegel but which is extremely important for applications to relative quartic index form equations.

In order to avoid a superfluous discussion of various cases we change our notation slightly. Instead of (1.6) we consider the equations

$$\left(a_1x_1^2 + a_2x_2^2 + a_3x_3^2\right)^{(\kappa)} = 0 \qquad (1 \le \kappa \le n) \tag{2.8}$$

for given $a_1, a_2, a_3 \in R$ subject to $a_1a_2a_3 \neq 0$. We stipulate that there is a solution $(\xi_1, \xi_2, \xi_3) \in R^3 \setminus \{\mathbf{0}\}$. Then $\mathbf{b} := \xi_1R + \xi_2R + \xi_3R$ is a non-zero ideal of R whose norm $N(\mathbf{b})$ will be denoted by B.

3. First estimate

In Step 1 we show the existence of $(u_1, u_2, u_3) \in R^3 \setminus \{\mathbf{0}\}$ with special properties satisfying

$$(u_1\xi_1 + u_2\xi_2 + u_3\xi_3)^{(\kappa)} = 0 \qquad (1 \le \kappa \le n). \tag{3.9}$$

Following Siegel's precedent we introduce several constants which will be useful in defining the needed weights for the T_2-norm. We recall that these weights will guarantee that the conjugates of a lattice point (u_1, u_2, u_3), which will exist according to Minkowski, have nice properties. For $\kappa \in \{1, \dots, n\}$ we choose variables κ_i, κ_j, κ_k with values $\{\kappa_i, \kappa_j, \kappa_k\} = \{1, 2, 3\}$ such that

$$|a_{\kappa_k}^{(\kappa)}|\,|\xi_{\kappa_k}^{(\kappa)}|^2 = \max\left\{|a_1^{(\kappa)}|\,|\xi_1^{(\kappa)}|^2, |a_2^{(\kappa)}|\,|\xi_2^{(\kappa)}|^2, |a_3^{(\kappa)}|\,|\xi_3^{(\kappa)}|^2\right\} =: M_\kappa^2.$$

Hence, we always have $\xi_{\kappa_k}^{(\kappa)} \neq 0$. In case $|\kappa - \tilde{\kappa}| = r_2$ for two conjugates κ, $\tilde{\kappa}$, we must additionally require that the values of κ_l and of $\tilde{\kappa}_l$ coincide for $1 \le l \le 3$. In the sequel we identify the variables κ_l and their values to avoid double indices. For the coordinates of a vector $(x_1, x_2, x_3) \in F^3$ we introduce the following abbreviation which makes the exposition easier to read:

$$x_{\kappa_l} := x_{\kappa_l}^{(\kappa)}. \tag{3.10}$$

We also write

$$A_\kappa^2 := |a_1^{(\kappa)} a_2^{(\kappa)} a_3^{(\kappa)}|.$$

We let λ be a positive real number which will be specified later. Introducing the constants

$$\lambda_\kappa := \frac{\lambda B^{1/n} A_\kappa}{|d_R|^{3/(2n)} M_\kappa |a_{\kappa_i}|}, \quad \mu_\kappa := \frac{\lambda B^{1/n} A_\kappa}{|d_R|^{3/(2n)} M_\kappa |a_{\kappa_j}|}, \qquad \nu_\kappa := \frac{M_\kappa^2}{|a_{\kappa_k}| B^{2/n}} \tag{3.11}$$

we can define

$$\tilde{Q}(u_1, u_2, u_3) := \sum_{\kappa=1}^{n} \left(\lambda_\kappa |u_{\kappa_i}|^2 + \mu_\kappa |u_{\kappa_j}|^2 + \nu_\kappa \left| u_{\kappa_k} + \frac{\xi_{\kappa_i}}{\xi_{\kappa_k}} u_{\kappa_i} + \frac{\xi_{\kappa_j}}{\xi_{\kappa_k}} u_{\kappa_j} \right|^2 \right). \tag{3.12}$$

We represent the u_i $(i = 1, 2, 3)$ by a fixed $\mathbb{Z}$-basis of R. Then $\tilde{Q}(u_1, u_2, u_3)$ becomes a positive definite quadratic form in $3n$ variables. It is not difficult to calculate its determinant analogously to the computation of the determinant of a Gram matrix of a $\mathbb{Z}$-basis of R:

$$\det \tilde{Q} = |d_R|^3 \prod_{\kappa=1}^{n} (\lambda_\kappa \mu_\kappa \nu_\kappa) = \lambda^{2n}. \tag{3.13}$$

Minkowski's theorem on successive minima yields the existence of $(u_1, u_2, u_3) \in R^3 \setminus \{\mathbf{0}\}$ satisfying

$$\tilde{Q}(u_1, u_2, u_3) \le (\gamma_{3n}^{3n} \lambda^{2n})^{1/(3n)} =: \Delta, \tag{3.14}$$

where the constants γ_{3n}^{3n} denote Hermite's constants as usual.

On the other hand, we have

$$\tilde{Q}(u_1, u_2, u_3) \ge \sum_{\kappa=1}^{n} \nu_\kappa \left| u_{\kappa_k} + \frac{\xi_{\kappa_i}}{\xi_{\kappa_k}} u_{\kappa_i} + \frac{\xi_{\kappa_j}}{\xi_{\kappa_k}} u_{\kappa_j} \right|^2 \tag{3.15}$$

$$= \sum_{\kappa=1}^{n} B^{-2/n} |(u_1\xi_1 + u_2\xi_2 + u_3\xi_3)^{(\kappa)}|^2. \tag{3.16}$$

Obviously, the element $\beta := u_1\xi_1 + u_2\xi_2 + u_3\xi_3$ of R is in $\mathbf{b}$. By the inequality between arithmetic and geometric means we obtain

$$\sum_{\kappa=1}^{n} B^{-2/n} |(u_1\xi_1 + u_2\xi_2 + u_3\xi_3)^{(\kappa)}|^2 \ge n \sqrt[n]{(N(\beta)/B)^2}.$$

Hence, we get $|N(\beta)| < B$ and consequently $\beta = 0$, if we stipulate

$$(\tilde{Q}(u_1, u_2, u_3)/n) < 1.$$

Because of Minkowski's theorem the latter can be achieved upon requiring

$$\left(\frac{1}{n} (\gamma_{3n}^{3n} \lambda^{2n})^{1/(3n)} \right) < 1. \tag{3.17}$$

From this we easily deduce the following condition on the constant λ:

$$\lambda < (n/\gamma_{3n})^{3/2}. \tag{3.18}$$

We note that the choice of λ according to (3.18) is tantamount to $\Delta < n$. Hence, we can estimate Δ/λ by n/λ. This will be used later. We note that $\lambda < \frac{1}{\sqrt{2}}$ for $n = 1$, $\lambda < \sqrt[4]{3}$ for $n = 2$, and that an upper limit for λ is $\exp(\log(\pi) + 1 - \log(3))^{3/2} = 4.8$ as n tends to infinity. (For this we use BLICHFELDT's estimate [1]

$$\gamma_{3n}^{3n} < \left(\frac{2}{\pi}\right)^{3n} \Gamma\left(1 + \frac{3n+2}{2}\right)^2$$

for Hermite's constants and Stirling's formula.)

This finishes Step 1.

4. Second estimate

In Step 2 we interchange the role of the triples (u_1, u_2, u_3) and (ξ_1, ξ_2, ξ_3). Following Siegel's precedent we consider the projective line

$$u_1 x_1 + u_2 x_2 + u_3 x_3 = 0. \tag{4.19}$$

According to Step 1 it intersects the cone

$$a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0 \tag{4.20}$$

in the point (ξ_1, ξ_2, ξ_3). Consequently, there is a second intersection point, say with coordinates (X_1, X_2, X_3). Since the coordinates of both points satisfy the preceding two equations, we can eliminate variables and get relations between them:

$$\xi_{\kappa_k} X_{\kappa_k} = a_{\kappa_j} u_{\kappa_i}^2 + a_{\kappa_i} u_{\kappa_j}^2, \tag{4.21}$$

and

$$\xi_{\kappa_j} X_{\kappa_k} + \xi_{\kappa_k} X_{\kappa_j} = -2 a_{\kappa_i} u_{\kappa_j} u_{\kappa_k} \tag{4.22}$$

for $\kappa \in \{1, \ldots, n\}$ and $\{\kappa_i, \kappa_j, \kappa_k\} = \{1, 2, 3\}$. We will use these to get upper bounds on the absolute values of X_{κ_l} ($l \in \{i, j, k\}$). We note that we have $(X_1, X_2, X_3) \in F^3$ because of (4.21).

From (3.11), (3.12) and (3.14) we conclude

$$\Delta \geq \lambda (B |d_R|^{-3/2})^{1/n} \sum_{\kappa=1}^{n} \frac{1}{\sqrt{|a_{\kappa_i} a_{\kappa_j}|} |\xi_{\kappa_k}|} \left(|a_{\kappa_j}| \, |u_{\kappa_i}|^2 + |a_{\kappa_i}| \, |u_{\kappa_j}|^2 \right), \tag{4.23}$$

and by applying (4.21) we obtain

$$\sum_{\kappa=1}^{n} \frac{|X_{\kappa_k}|}{\sqrt{|a_{\kappa_i} a_{\kappa_j}|}} = \sum_{\kappa=1}^{n} \frac{|a_{\kappa_j} u_{\kappa_i}^2 + a_{\kappa_i} u_{\kappa_j}^2|}{\sqrt{|a_{\kappa_i} a_{\kappa_j}|}|\xi_{\kappa_k}|} \leq \frac{\Delta |d_R|^{3/(2n)}}{\lambda B^{1/n}} =: K. \tag{4.24}$$

This is the bound for a weighted sum of the absolute values of X_{κ_k} which we need.

For a short overview on the quality of our results we present the following list of data and add a few explanatory remarks.

n	1	2	3	4	5	10	100	1000	∞
λ	0.71	1.32	1.31	1.71	2.00	2.86	4.41	4.75	4.80
Δ/λ	1.41	1.52	2.28	2.34	2.49	3.50	22.66	210.71	∞

For large n the upper bound in the last estimate is about $\frac{1}{30}$ of the result we could obtain from Siegel's bound. For small n we can even beat Siegel's result on the biggest conjugate X_{κ_k}. For $n = 1, 2$ our result is about one fourth of his, even for $n = 10$ we still obtain a constant of 3.50 compared to his constant 6.

However, we must recall that according to our notation the elements X_{κ_k} need not be conjugates of an element of F inasmuch as κ_k can assume values between one and three. Therefore we must estimate the weighted sum of the absolute values of the conjugates of all three elements X_1, X_2, X_3.

As before we start with the estimate obtained for $\tilde{Q}$. We recall that (4.23), (4.24) imply the inequality

$$K \geq \sum_{\kappa=1}^{n} \frac{1}{\sqrt{|a_{\kappa_i} a_{\kappa_j}|}|\xi_{\kappa_k}|} \left(|a_{\kappa_j}||u_{\kappa_i}|^2 + |a_{\kappa_i}||u_{\kappa_j}|^2 \right). \tag{4.25}$$

Hence, we get a priori

$$\sum_{\kappa=1}^{n} \sqrt{\frac{|a_{\kappa_j}|}{|a_{\kappa_i}|}} \frac{|u_{\kappa_i}|^2}{|\xi_{\kappa_k}|} \leq K, \tag{4.26}$$

$$\sum_{\kappa=1}^{n} \sqrt{\frac{|a_{\kappa_i}|}{|a_{\kappa_j}|}} \frac{|u_{\kappa_j}|^2}{|\xi_{\kappa_k}|} \leq K, \tag{4.27}$$

$$\sum_{\kappa=1}^{n} \frac{2|u_{\kappa_i}||u_{\kappa_j}|}{|\xi_{\kappa_k}|} \le K. \tag{4.28}$$

If we want to estimate X_{κ_i}, X_{κ_j} from above by (4.21), (4.22) we note that because of the choice of the index κ_k we need ξ_{κ_k} to be a multiplier of X_{κ_i}, X_{κ_j}. (Only ξ_{κ_k} is guaranteed to be non-zero.) Hence, we must use (4.22). We obtain with the preceding estimates

$$\sum_{\kappa=1}^{n} \frac{|X_{\kappa_j}|}{\sqrt{|a_{\kappa_i}a_{\kappa_k}|}} = \sum_{\kappa=1}^{n} \frac{1}{\sqrt{|a_{\kappa_i}a_{\kappa_k}|}|\xi_{\kappa_k}|} \left|2a_{\kappa_i}u_{\kappa_j}u_{\kappa_k} + \xi_{\kappa_j}X_{\kappa_k}\right|$$

$$\le \sum_{\kappa=1}^{n} \left(\frac{2}{|\xi_{\kappa_k}|} \sqrt{\frac{|a_{\kappa_i}|}{|a_{\kappa_k}|}} |u_{\kappa_j}| \left| \frac{\xi_{\kappa_i}u_{\kappa_i} + \xi_{\kappa_j}u_{\kappa_j}}{|\xi_{\kappa_k}|} \right| + \frac{\sqrt{|a_{\kappa_j}|}|\xi_{\kappa_j}|}{\sqrt{|a_{\kappa_k}|}|\xi_{\kappa_k}|} \frac{|X_{\kappa_k}|}{\sqrt{|a_{\kappa_i}a_{\kappa_j}|}} \right)$$

$$\le \sum_{\kappa=1}^{n} \left(\frac{2|u_{\kappa_i}||u_{\kappa_j}|}{|\xi_{\kappa_k}|} + 2\sqrt{\frac{|a_{\kappa_i}|}{|a_{\kappa_j}|}} \frac{|u_{\kappa_j}|^2}{|\xi_{\kappa_k}|} + \frac{|X_{\kappa_k}|}{\sqrt{|a_{\kappa_i}a_{\kappa_j}|}} \right) \le 4K.$$

Similarly, we get

$$\sum_{\kappa=1}^{n} \frac{|X_{\kappa_i}|}{\sqrt{|a_{\kappa_j}a_{\kappa_k}|}} \le 4K.$$

Taking into account that because of (4.25) even the sum of the left-hand sides of (4.26) and (4.27) is bounded by K, we obtain the result

$$\sum_{\kappa=1}^{n} \left(\left| \frac{X_1^{(\kappa)}}{\sqrt{a_2^{(\kappa)}a_3^{(\kappa)}}} \right| + \left| \frac{X_2^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_3^{(\kappa)}}} \right| + \left| \frac{X_3^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_2^{(\kappa)}}} \right| \right) \le 7K. \tag{4.29}$$

We must remark, however, that the found solution (X_1, X_2, X_3) of Legendre's equation is not necessarily integral. A look at the equations (4.21) tells us that the X_l $(1 \le l \le 3)$ are contained in the inverse $\mathbf{b}^{-1}$ of the ideal $\mathbf{b}$. For this we need that the ideal $\mathbf{b}$ is invertible in its order R, otherwise these considerations must be transfered to the maximal order.

For any $\tau \in \mathbf{b}$ the elements $\tilde{X}_l = \tau X_l$ are integral (in R). Again, we follow Siegel who applies Minkowski's theorem on linear forms to get the existence of $0 \ne \tau \in \mathbf{b}$ satisfying

$$|\tau^{(\kappa)}| \le |d_R B^2|^{1/(2n)}. \tag{4.30}$$

Multiplying the solution (X_1, X_2, X_3) with this τ we obtain our main result.

Theorem 4.1. *If the diophantine equation $a_1x_1^2+a_2x_2^2+a_3x_3^2=0$ has a non-trivial solution in the number field F, then it also has an integral solution X_1, X_2, X_3 which satisfies*

$$\sum_{\kappa=1}^{n}\left(\left|\frac{X_1^{(\kappa)}}{\sqrt{a_2^{(\kappa)}a_3^{(\kappa)}}}\right|+\left|\frac{X_2^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_3^{(\kappa)}}}\right|+\left|\frac{X_3^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_2^{(\kappa)}}}\right|\right)\le 7\frac{\Delta}{\lambda}|d_R|^{2/n}.$$

Remark. For large n the upper bound in the last estimate is about 0.08 times the result we can derive from Siegel's bounds. However, because of the large factor 7 we cannot beat Siegel's result on the biggest conjugate of any X_l $(1\le l\le 3)$. Hence, the major achievement of the last theorem is that it decreases the volume of the search area drastically. The latter is of course important for actual computations.

5. Totally real number fields

We now consider the special case of F being totally real. Because of $\alpha_1\alpha_2\alpha_3\neq 0$, exactly two of the three coefficients $\alpha_1^{(\kappa)}$, $\alpha_2^{(\kappa)}$, $\alpha_3^{(\kappa)}$ must have the same sign for each conjugate $\kappa\in\{1,\dots,n\}$. Since we chose

$$M_\kappa^2=|a_{\kappa_k}^{(\kappa)}|\,|\xi_{\kappa_k}^{(\kappa)}|^2=\max\{|a_1^{(\kappa)}|\,|\xi_1^{(\kappa)}|^2,|a_2^{(\kappa)}|\,|\xi_2^{(\kappa)}|^2,|a_3^{(\kappa)}||\xi_3^{(\kappa)}|^2\},$$

we must have

$$\operatorname{sign}(a_{\kappa_k}a_{\kappa_i})<0<\operatorname{sign}(a_{\kappa_i}a_{\kappa_j})$$

and therefore

$$\max\{|a_{\kappa_i}|\,|X_{\kappa_i}|^2,|a_{\kappa_j}|\,|X_{\kappa_j}|^2\}\le|a_{\kappa_k}|\,|X_{\kappa_k}|^2. \tag{5.31}$$

Using this the estimates of the preceding section become much sharper, since the poor bounds we got from (4.22) are not needed anymore. With (4.24) and (4.30) we obtain the following result for totally real number fields.

Theorem 5.1. *If the diophantine equation $a_1x_1^2+a_2x_2^2+a_3x_3^2=0$ has a non trivial solution in the totally real number field F, then it also has an integral solution X_1, X_2, X_3 which satisfies*

$$\sum_{\kappa=1}^{n}\left(\left|\frac{X_1^{(\kappa)}}{\sqrt{a_2^{(\kappa)}a_3^{(\kappa)}}}\right|+\left|\frac{X_2^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_3^{(\kappa)}}}\right|+\left|\frac{X_3^{(\kappa)}}{\sqrt{a_1^{(\kappa)}a_2^{(\kappa)}}}\right|\right)\le 3\frac{\Delta}{\lambda}|d_R|^{2/n}.$$

Remark. For large n the upper bound in the last estimate is about 0.03 times the result we can derive from Siegel's bounds. For $n = 1, 2$ we even beat Siegel's result on the biggest conjugate of any X_l $(1 \leq l \leq 3)$. The important improvement is of course the decrease of the volume of the required search area.

References

[1] H. F. Blichfeldt, A new principle in the geometry of numbers, with some applications, *Transactions Amer. Math. Soc.* **15** (1914), 227–235.

[2] I. Gaál and M. Pohst, On the resolution of index form equations in relativ quartic extensions, (*submitted to* J. Number Theory).

[3] M. Pohst, On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields, *J. Number Theory* **14** (1982), 99–117.

[4] C. L. Siegel, Normen algebraischer Zahlen, Gesammelte Werke IV, *Springer Verlag*, 1979, 250–268.

MICHAEL E. POHST
FACHBEREICH 3 MATHEMATIK, MA 8–1
TECHNISCHE UNIVERSITÄT BERLIN
STRASSE DES 17. JUNI 136
10623 BERLIN
GERMANY

(Received February 28, 2000; revised May 5, 2000)