PRACE MATEMATYCZNE II, 1972

KAZIMIERZ SZYMICZEK

The integer solutions of the equation $ax^2+by^2+cz^2=0$ in quadratic fields

In a recent paper [1] L. J. MORDELL has given a theorem on the solvability of the equation

$$ax^2+by^2+c = 0 \tag{1}$$

in integers of a quadratic field. We shall prove here by MORDELL'S method an analogous theorem for the equation

$$ax^2+by^2+cz^2 = 0. \tag{2}$$

This equation is of a particular importance in number theory and so it may be of interest to find some elementary necessary and sufficient conditions for its solvability in quadratic fields.

THEOREM. *Let* a, b, c *be rational integers and* $(a, b)=(b, c)=(c, a)=1$. *Then non-trivial integer solutions of the equation* (2) *exist in a quadratic field* $K = Q(\vartheta)$ *if and only if there exist rational integers* p, q, r, d, d_1 *such that*

(3) $ap^2+bq^2 = d$, $(ap, bq) = d_1$, d *is a divisor of* $abcr^2$ *and* ϑ *satisfies the equation*

$$\vartheta^2 + abk^2/d_1^2 + cr^2/d = 0, \tag{4}$$

where k *is a rational integer such that* $abk^2/d_1^2 + cr^2/d$ *is an integer. If these conditions are satisfied, then*

$$x = p\vartheta + bqk/d_1,\ y = q\vartheta - apk/d_1,\ z = r \tag{5}$$

is a solution of (2).

Proof. As is well-known, every integer a of a quadratic field $K = Q(\sqrt{D})$, where D is a square-free rational integer, is of the form $a = u+v\omega$, where u, v are rational integers and $\omega = (1+\sqrt{D})/2$ or $\sqrt{D}$ according as $D \equiv 1 \pmod 4$ or $D \equiv 2, 3 \pmod 4$, respectively. Because of homogeneity of the equation (2) we can restrict ourselves to the solutions of the form $u + v\sqrt{D}$. Next, if α, β, γ is a solution of (2) and $\bar{\gamma}$ is the conjugate of γ, then $\alpha\bar{\gamma}, \beta\bar{\gamma}, \gamma\bar{\gamma}$ is also a solution of (2) and $\gamma\bar{\gamma}$ is a rational integer.

Thus, the equation (2) has an integer solution in a quadratic field $Q(\sqrt{D})$ if and only if it has a solution of the form

(6) $$x = p\vartheta + p_1,\ y = q\vartheta + q_1,\ z = r_1.$$

where p, q, r_1, p_1, q_1 are rational integers, $(p, q)=1$, $\vartheta = s\sqrt{D}$ for a suitable integer s.

Suppose first that (6) is a solution of (2). On substituting in (2) for x, y, z from (6), we get

(7) $$(ap^2+bq^2)\vartheta^2+2(app_1+bqq_1)\vartheta+ap_1^2+bq_1^2+cr_1^2 = 0.$$

Since $\vartheta = s\sqrt{D}$, we must have

(8) $$app_1+bqq_1 = 0.$$

The solution of (8) for p_1, q_1 can be written as

(9) $$p_1 = bqk/d_1,\ q_1 = -apk/d_1,$$

where k is a rational integer and d_1 is defined by (3).

Now, using (3), we have

$$ap_1^2 + bq_1^2 + cr_1^2 = abdk^2/d_1^2 + cr^2,$$

and (7) can be rewritten as

$$\vartheta^2 + abk^2/d_1^2 + cr^2/d = 0.$$

Since $\vartheta = s\sqrt{D}$ is an algebraic integer, $L = abk^2/d_1^2+cr^2/d$ must be an integer. From $d_1 = (ap, bq)$, $(a, b) = (p, q) = 1$ it follows that $d_1 \mid ab$. Thus $abL = (ab/d_1)^2 k^2+abcr^2/d$ and $(ab/d_1)^2 k^2$ are integers, and this implies that $abcr^2/d$ is an integer. From (6) and (9) we obtain (5) and all conditions of the theorem are proved.

On the other hand, if (3), (4) hold the coefficient in (4) is an integer, then the numbers (5) form an integer solution of the equation (2) in the field $Q(\vartheta)$. This completes the proof.

There is an obvious connection between the solvability of (1) and (2) in integers of a quadratic field K: solvability of (1) is equivalent to the existence of a solution of (2) with $z = 1$. Hence from our theorem we derive at once the following

COROLLARY. *Let a, b, c be rational integers, $(a, b) = (b, c) = (c, a) = 1$. Then integer solutions $x = u+v\sqrt{D}$, $y = u_1+v_1\sqrt{D}$ (u, v, u_1, v_1 — rational integers) of the equation (1) exist in a quadratic field $K = Q(\sqrt{D}) = Q(\vartheta)$ if and only if there exist rational integers p, q, d, d_1 such that $ap^2+bq^2 = d$, $(ap, bq) = d_1$, $d \mid abc$ and*

$$\vartheta^2 + abk^2/d_1^2 + c/d = 0,$$

where k is an integer such that $abk^2/d_1^2 + c/d$ is an integer. If these conditions are satisfied, then

$$x = p\,\vartheta + bqk/d_1, \quad y = q\,\vartheta - apk/d_1$$

is a solution of (1).

This includes the part (A) of MORDELL'S theorem [1].

Finally, we shall show that there are quadratic fields in which the equation (1) has no integer solutions but the corresponding equation (2) has a nontrivial solution .

Consider the equation

$$(10) \qquad 2x^2 + y^2 + 1 = 0.$$

Here $abc = 2$, so $d = 2p^2 + q^2 \mid 2$ and only two possibilities arise: $p = 1$, $q = 0$ and $p = 0$, $q = 1$. In the first case $d = 2$, $d_1 = 2$ and the equation for ϑ takes the form $\vartheta^2+(k^2+1)/2 = 0$, where k is an integer such that $(k^2+1)/2$ is an integer. We have $k = 2l+1$, $(k^2+1)/2 = 2l^2+2l+1$ and $\vartheta^2 + 2l^2 + 2l + 1 = 0$. In the second case $d = d_1 = 1$ and $\vartheta^2 + 2k^2 + 1 = 0$. Hence in both cases ϑ does not belong to $Q(\sqrt{-2})$, i.e. the equation (10) has no integer solutions in $Q(\sqrt{-2})$.

Now for

$$2x^2+y^2+z^2 = 0$$

we have for $p=1$, $q=0$, $d=d_1=2$ as above, and (4) gives $\vartheta^2+(k^2+r^2)/2 = 0$, where k, r are chosen so that $(k^2 + r^2)/2$ is an integer. This is the case when $k = 8$, $r = 6$ and then $\vartheta = 5\sqrt{-2}$; formulae (5) give $x = 5\sqrt{-2}$, $y = 8$, $z = 6$.

Remark. There is a known condition for the solubility of (2) in an algebraic number field F, namely the HASSE'S principle guarantees the existence of a solution in F when solutions exist in all completions of the field F.

Moreover, A. SCHINZEL has kindly informed me that there is a paper by T. SKOLEM on this subject: *Über die Lösung der unbestimmten Gleichung $ax^2+by^2+cz^2 = 0$ in einigen einfachen Rationalitätsbereichen.* Norsk Mat. Tidsskr. 10, 50—54, Oslo 1928.

A second paper concerning the equation (2) is by O. HEMER: *On the solvability of the Diophantine equation $ax^2+by^2+cz^2 = 0$ in imaginary Euclidean quadratic fields*, Arkiv för Mat., 2, 57—82 (1954). Both writers consider the equation (2) with coefficients in a quadratic field K but SKOLEM discusses only the cases when $K = Q(\sqrt{-1})$ and $K = Q(\sqrt{-3})$ and HEMER only when $K = Q(\sqrt{-D})$, $D = 1, 2, 3, 7, 11$.

REFERENCE

[1] L. J. Mordell: *The integer solutions of the equation $ax^2 + by^2 + c = 0$ in quadratic fields.* Bulletin of the London Mathematical Society 1(1969), pp. 43—44.

KAZIMIERZ SZYMICZEK

ROZWIĄZANIA RÓWNANIA $ax^2 + by^2 + cz^2 = 0$ W LICZBACH CAŁKOWITYCH CIAŁA KWADRATOWEGO

Streszczenie

Udowodniono następujące twierdzenie:

Niech a, b, c będą liczbami całkowitymi wymiernymi, $(a,b)=(b,c)=(c,a)=1$. *Równanie*

$$ax^2+by^2+cz^2=0$$

posiada nietrywialne rozwiązanie w liczbach całkowitych ciała kwadratowego $K=Q(\vartheta)$ *wtedy i tylko wtedy, gdy istnieją liczby całkowite wymierne* p, q, r, d, d_1 *takie, że* $ap^2+bq^2=d$, $(ap,bq)=d_1$, d *dzieli* $abcr^2$ *oraz* ϑ *spełnia równanie*

$$\vartheta^2+abk^2/d_1^2+cr^2/d=0,$$

gdzie k jest tak dobraną liczbą całkowitą wymierną, że $abk^2/d_1^2+cr^2/d$ *jest liczbą całkowitą.*

Jeśli warunki te są spełnione, to otrzymujemy następujące rozwiązanie równania: $x = p\vartheta + bqk/d_1, y = q\vartheta — apk/d_1$, $z = r$.

Oddano do Redakcji 4. 4. 1970 r.