BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 61, No. 1, 2013

NUMBER THEORY

A Positive Definite Binary Quadratic Form as a Sum of Five Squares of Linear Forms (Completion of Mordell's Proof)

by

A. SCHINZEL

Summary. The paper completes an incomplete proof given by L. J. Mordell in 1930 of the following theorem: every positive definite classical binary quadratic form is the sum of five squares of linear forms with integral coefficients.

Let $f(X,Y) = aX^2 + 2hXY + bY^2$, where $a \geq 0$, h, b are given integers and $\Delta = ab - h^2 \geq 0$. L. J. Mordell [3] considered the equation

$$f(X,Y) = \sum_{r=1}^{n} (a_r X + b_r Y)^2, \tag{1}$$

where a_r, b_r $(r = 1, \ldots, n)$ are integers. He proved that for $n = 4$ the equation (1) is solvable if and only if $\Delta \neq 4^\rho(8\sigma + 7)$, where $\rho \geq 0$, $\sigma \geq 0$ are integers, i.e. Δ can be expressed as a sum of three integer squares. For $n = 5$ Mordell asserted that (1) is always solvable, but the proof given on pp. 280–282 seems to contain a gap on p. 282. The author says "Suppose next that $\Delta = 4^\rho(8\sigma + 7)$ $(\rho > 0)$. By a theorem of Lipschitz [Matthews, *Theory of Numbers*, pp. 159–62], every properly primitive form of determinant Dp^2 where p is a prime, (and hence of determinant $Dp^{2\alpha}$) can be derived from a properly primitive form of determinant D by a substitution with integer coefficients and determinant p (or p^α in the second case). Hence, it suffices to prove our theorem for the improperly primitive forms of determinant Δ, i.e. those with $(a, 2h, b) = 2$. But then h is even since $\Delta = ab - h^2$, and we

2010 *Mathematics Subject Classification*: Primary 11E25.
Key words and phrases: positive definite binary quadratic form, sums of squares of linear forms.

DOI: 10.4064/ba61-1-3 © Instytut Matematyczny PAN, 2013

can write

$$aX^2 + 2hXY + bY^2 = 2\left[\frac{1}{2}aX^2 + 2\left(\frac{1}{2}h\right)XY + \frac{1}{2}bY^2\right]. \tag{2}$$

The determinant of the form in brackets is $\frac{1}{4}\Delta$. Hence, step by step, we are brought to the case $\rho = 0$. Hence the theorem is proved and $N = 5$ in §1".

Now, if $\rho = 1$ the form in brackets in (2) has determinant $8\sigma + 7$ and by the already proved case of the theorem can be represented as $\sum_{r=1}^{5}(a_rX + b_rY)^2$. However, why should $2\sum_{r=1}^{5}(a_rX + b_rY)^2$ be represented as $\sum_{r=1}^{5}(a'_rX + b'_rY)^2$, a'_r, b'_r integers? This question is not answered in [3].

The following argument fills this gap.

Lemma 1 (Ramanujan). *The form $x^2 + y^2 + z^2 + st^2$ $(1 \le s \le 7)$ represents over $\mathbb{Z}$ all non-negative integers.*

Proof. See [1, Theorem 96, p. 105]. ∎

Lemma 2. *For every positive definite classical binary quadratic form f with determinant $\Delta = 4(8\sigma + 7)$ there exist integers t, u such that*

$$\Delta - f(t, u) \tag{3}$$

is a sum of three squares.

Proof. Let $f = aX^2 + 2hXY + bY^2$. Following Mordell (p. 281) by effecting a linear substitution of determinant unity and writing $-y$ for y if need be, we may suppose that the form f is reduced and that $h \ge 0$, so that

$$b \ge a \ge 2h, \qquad a \le 2\sqrt{\Delta/3}. \tag{4}$$

If $a \le 7$, then by Lemma 1 the equation $\Delta = x^2 + y^2 + z^2 + at^2$ has integer solutions (x, y, z, t), thus the conclusion holds with $u = 0$. If $a \ge 8$, then by (4), $\Delta \ge 48$ and $b \le \frac{4\Delta}{3a} \le \frac{\Delta}{6}$. Since $\Delta \equiv 28 \bmod 32$, we have either $\Delta \ge 92$, or $a = b = 8$ and $h = 2$. In the first case

$$f(1,0) < f(2,0) < \Delta, \qquad f(0,1) < f(0,2) < \Delta,$$

$$\begin{aligned} f(-1,-1) < f(2,-2) &= 4a - 8h + 4b \le 4a + \frac{4\Delta}{a} \\ &= 32 + \frac{\Delta}{2} - (a-8)\left(\frac{\Delta}{2a} - 4\right) \le 32 + \frac{\Delta}{2} < \Delta. \end{aligned}$$

The corresponding inequalities are also true in the second case. Taking $(t, u) = (1, 0), (0, 1), (1, -1)$ and assuming that (3) does not hold we obtain

$$a \equiv 0, 4, 5 \bmod 8; \quad b \equiv 0, 4, 5 \bmod 8; \quad a + b - 2h \equiv 0, 4, 5 \bmod 8. \tag{5}$$

Taking in turn $(t, u) = (2, 0), (0, 2), (2, -2)$ we obtain

$$a \equiv 0, 3, 7 \bmod 8; \quad b \equiv 0, 3, 7 \bmod 8; \quad a + b - 2h \equiv 0, 3, 7 \bmod 8. \tag{6}$$

Comparing (5) with (6) we obtain $a \equiv 0 \bmod 8$, $b \equiv 0 \bmod 8$, $h \equiv 0 \bmod 4$, hence $\Delta = ab - h^2 \equiv 0 \bmod 16$, contrary to $\Delta \equiv 28 \bmod 32$.

Completion of Mordell's proof. Let 4^j be the highest power of 4 dividing (a,h,b). Consider first $j = 0$. If $\Delta \neq 4^\rho(8\sigma+7)$ with $\rho \geq 1$ the assertion has been proved by Mordell. If $\Delta = 4(8\sigma+7)$, then by Lemma 2 there exist integers t,u such that $\Delta - f(t,u)$ is a sum of three squares. Since $\Delta - f(t,u)$ is the determinant of the form $f(X,Y) - (uX - tY)^2$, from Mordell's theorem (for $n = 4$) quoted in the introduction we obtain

$$f(X,Y) = (uX - tY)^2 + \sum_{r=1}^{4}(a_rX + b_rY)^2, \qquad a_r, b_r \in \mathbb{Z}\ (r = 1,\ldots,4).$$

If $\Delta = 4^\rho(8\sigma+7)$, $\rho \geq 2$, let $d = (a,h,b)$. We have $d \not\equiv 0 \bmod 4$, since $j = 0$. The form

$$f_d(X,Y) = \frac{a}{d}X^2 + \frac{2h}{d}XY + \frac{b}{d}Y^2$$

is primitive. It cannot be improperly primitive, since in that case $\operatorname{ord}_2 a > \operatorname{ord}_2 d$, $\operatorname{ord}_2 b > \operatorname{ord}_2 d$ and since $ab - h^2 = \Delta \equiv 0 \bmod 16$, $\operatorname{ord}_2 h > \operatorname{ord}_2 d$. Thus $f_d(X,Y)$ is properly primitive and by the Lipschitz theorem there exist a form f_0 with determinant $\Delta d^{-2}4^{\operatorname{ord}_2 d - \rho}$ and integers $\alpha, \beta, \gamma, \delta$ such that

$$f_d(X,Y) = f_0(\alpha X + \beta Y, \gamma X + \delta Y). \tag{7}$$

The determinant of the form df_0 is $4^{\operatorname{ord}_2 d}(8\sigma+7)$, hence by the already proved part of the theorem, df_0 is a sum of five squares of integral linear forms, and by (7) the same applies to f.

Consider now the general case. Since $4 \nmid (a/4^j, h/4^j, b/4^j)$, by the already proved case of the theorem we have

$$\frac{a}{4^j}X^2 + \frac{2h}{4^j}XY + \frac{b}{4^j}Y^2 = \sum_{r=1}^{5}(a_rX + b_rY)^2, \qquad a_r, b_r \text{ integers } (r = 1,\ldots,5).$$

Therefore,

$$aX^2 + 2hXY + bY^2 = \sum_{r=1}^{5}(2^ja_rX + 2^jb_rY)^2. \ \blacksquare$$

A simpler question, namely whether under the same conditions on a, b and h,

$$aX^2 + 2hXY + bY^2 = \sum_{r=1}^{n}(a_rX + b_rY)^2, \qquad a_r, b_r \text{ rationals } (1 \leq r \leq n), \tag{8}$$

was settled affirmatively for $n = 5$ already by Landau [2]. Here we add the following

Theorem. *If* $n \geq 5$, a, b, h *are rationals*, $a \geq 0$, $\Delta = ab - h^2 \geq 0$ *and rationals* $a_1, \dots, a_n$ *satisfy* $a_1^2 + \dots + a_n^2 = a$, *then there exist rationals* $b_1, \dots, b_n$ *such that* (8) *holds.*

Proof. By performing a linear substitution (see [2]) we reduce the general case to the case $h = 0$. If $a = 0$ we have $a_1 = \dots = a_n = 0$ and we choose rational $b_1, \dots, b_n$ such that $b_1^2 + \dots + b_n^2 = b$. If $b = 0$ we take $b_1 = \dots = b_n = 0$. If $a > 0$ and $b > 0$ we distinguish two cases:

(i) $a_n \neq 0$,
(ii) $a_n = 0$.

In case (i) the quadratic form $f(u_1, \dots, u_n) = bu_n^2 - u_1^2 - \dots - u_{n-1}^2 - (a_1 a_n^{-1} u_1 + \dots + a_{n-1} a_n^{-1} u_{n-1})^2$ is indefinite, since $f(0, \dots, 0, 1) = b > 0$ and $f(1, 0, \dots, 0) = -a_1^2 a_n^{-2} - 1 < 0$. By Meyer's theorem there exist integers $v_1, \dots, v_n$ not all zero such that $f(v_1, \dots, v_n) = 0$. The equality $v_n = 0$ implies $v_i = 0$ $(1 \leq i \leq n)$, thus $v_n \neq 0$ and taking

$$b_i = \frac{v_i}{v_n} \quad (1 \leq i < n), \qquad b_n = -a_1 a_n^{-1} b_1 - \dots - a_{n-1} a_n^{-1} b_{n-1}$$

we obtain (8) with $h = 0$.

In case (ii) there exists $k < n$ such that $a_k \neq 0$ and we perform the transposition (k, n).

Acknowledgments. Thanks are due to J. Browkin for his criticism of an earlier version.

References

[1] L. E. Dickson, *Modern Elementary Theory of Numbers*, Univ. of Chicago Press, 1939.

[2] E. Landau, *Über die Zerlegung definiter Funktionen in Quadrate*, Arch. Math. Physik (3) 7 (1904), 271–277; reprinted in Collected Works, Vol. 2, Thales-Verlag, 1986, 109–115.

[3] L. J. Mordell, *A new Waring's problem with squares of linear forms*, Quart. J. Math. 1 (1930), 276–288.

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: schinzel@impan.pl

Received August 22, 2012 (7899)