On representation of large integers by integral ternary positive definite quadratic forms

B.Z. MOROZ

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26
D–5300 Bonn 3

Federal Republic of Germany

MPI/90-67

Résumé. Recently W. Duke has obtained new estimates for the coefficients of cusp–forms of weight 3/2. This allows, via the work of R. Schulze–Pillot, to obtain an asymptotic formula for the number of representations of a large integer by a positive quadratic form. We give a brief survey of this topic and, in particular, confirm a conjecture of R. Heath–Brown's to the extent that every large integer congruent to 7 modulo 8 can be represented in the form $x^2 + y^2 + 125z^2$.

On representation of large integers by integral ternary positive definite quadratic forms

B.Z. MOROZ

A few years after the famous work of C.L. Siegel's, [14], on representation of integers by a genus of quadratic forms had appeared Yu. V. Linnik, [7], initiated a study of representation of integers by an individual ternary quadratic form. Due to the efforts of many authors (cf., for instance, [8], [9], [1], [12], [16], [6], [3] and references therein), we may now claim a success. Let $f(x) = \frac{1}{2} \sum_{1 \leq i,j \leq 3} a_{ij} x_i x_j$ be a positive definite quadratic form with integral rational coefficients, so that $a_{ij} = a_{ji}$, $a_{ij} \in \mathbf{Z}$, $2|a_{ii}$ for $1 \leq i, j \leq 3$, and let $r_f(n) = \mathrm{card}\,\{u | u \in \mathbf{Z}^3,\ f(u) = n\}$ be the representation number of n by f; let $D = \det(a_{ij})$.

<u>Theorem 1</u>. Suppose that $n \in \mathbf{Z}$, $n \geq 1$ and g.c.d.$(n,2D) = 1$. Then $r_f(n) = r(n,\text{gen } f) + O(n^{1/2-\gamma})$ for $\gamma > 1/28$, where $r(n,\text{gen } f)$ denotes the number of representations of n by the genus of f averaged in accordance with Siegel's prescription, [14]. Moreover, if n is primitively represented by f over the ring of p-adic integers for each rational prime p then $r(n,\text{gen } f) \gg_{f,\varepsilon} n^{1/2-\varepsilon}$ for $\varepsilon > 0$.

<u>Proof</u>. Let N be a positive integer such that $2D|N$ and $8|N$, and let $\varphi \in S_0(3/2,N,\chi)$ with $\chi(d) = \left[\frac{2D}{d}\right]$, suppose furthermore that $\varphi \in \mathfrak{A}^{\perp}$, in notations of [12]. Thus φ is a "good" cusp-form of weight 3/2 (and character χ) which does not come from a θ-series. Therefore an argument due to H. Iwaniec, [6], and W. Duke, [3], supplemented by the considerations going back to G. Shimura, [13], and B.A. Cipra, [2], leads to an estimate for the Fourier coefficients of φ (cf. also [4]), and on writing $\varphi(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}$ we obtain: $a(n) \ll_{\varphi,\gamma} n^{1/2-\gamma}$ as soon as $(n,2D) = 1$ and $\gamma < \frac{1}{28}$. By [12, Korollar 3], it follows then that $r_f(n) = r(n,\text{spn } f) + O(n^{1/2-\gamma})$ for $(n,2D) = 1$ and $\gamma < \frac{1}{28}$, where $r(n,\text{spn } f)$ denotes the representation

number of n averaged over the spinor genus containing f (cf. [12]). On the other hand, by [12, Korollar 2], if $(n,2D) = 1$ then $r(n,\mathrm{spn}\, f) = r(n,\mathrm{gen}\, f)$. Finally the estimate $r(n,\mathrm{gen}\, f) \gg n^{1/2-\epsilon}$ for $\epsilon > 0$ is a consequence of Siegel's work, [14], [15] (cf. also [11, Satz (3.1)]), as soon as n is primitively representable by f over the p-adic integers. This completes the proof.

Remark 1. The condition $(n,2D) = 1$ has been used in the proof twice, to insure the estimate $a(n) \ll n^{1/2-\gamma}$ and to deduce the identity $r(n,\mathrm{spn}\, f) = r(n,\mathrm{gen}\, f)$. The former use of this condition is due to the fact that $\varphi \in S(3/2,N,\chi)$ with $\chi = \left(\frac{2D}{d}\right)$ (see [10] for the details). It is an interesting question to what extent one can weaken the condition $(n,2D) = 1$ in the theorem 1. The work of R. Schulze-Pillot, [12] (cf. also [16] and references therein), is pertinent to this question.

Theorem 2. Let q be a rational prime congruent to 5 modulo 8 and let $f(x) = x_1^2 + x_2^2 + q^3x_3^2$. Then $r_f(n) \gg_{q,\epsilon} n^{1/2-\epsilon}$ for $\epsilon > 0$ and $n \equiv 7 \pmod 8$.

Proof. Let $n = q^{\ell}n_1$, $q \nmid n_1$ and suppose that $n \equiv 7 \pmod 8$. Consider the quadratic form $g(x) = x_1^2 + x_2^2 + q^m x_3^2$, where $m = 3 - \ell$ when $\ell \leq 3$ and $m = 0$ when $\ell \geq 3$; let $n_2 = nq^{m-3}$. Since $n_2 \equiv 3 \pmod 8$ if $\ell \geq 3$ and $n_2 \not\equiv 0 (q)$ when $\ell < 3$ it follows from theorem 1 that $r_g(n_2) \gg n_2^{1/2-\epsilon}$ for $\epsilon > 0$. On writing $x_1^2 + x_2^2 = q^{3-m}(n_2 - q^m y_3^2)$ one notes that to each solution of equations: $n_2 = g(y)$ with $y \in \mathbb{Z}^3$, $q^{3-m} = z_1^2 + z_2^2$ with $z_1 \in \mathbb{Z}$, $z_2 \in \mathbb{Z}$ there corresponds a unique solution of the equation $n = f(x)$ with $x \in \mathbb{Z}^3$. Since $q \equiv 1 \pmod 4$, it follows, in particular, that $r_f(n) \gg n^{1/2-\epsilon}$ for $\epsilon > 0$. This completes the proof.

Remark 2. Theorem 2 confirms a conjecture of D.R. Heath-Brown's, [5,p. 137-138], that every large integer congruent to 7 modulo 8 is represented by the form $x_1^2 + x_2^2 + q^3x_3^2$ when $q \equiv 5 \pmod 8$ and q is a rational prime.

Definition. Let $n \in \mathbb{Z}$. We say that n is square-full if $n > 0$ and $p|n \Rightarrow p^2|n$ for each rational prime p.

Corollary. Every sufficiently large positive integer is a sum of at most three square-full numbers.

Proof. By a classical theorem of Gauß's, each positive integer n is either a sum of three squares or it is of the shape $n = 4^{\ell}(8k + 7)$ with $\ell \in \mathbb{Z}$, $k \in \mathbb{Z}$. In the latter case, however, theorem 2 shows that the integer n is represented, for instance, by the form $x_1^2 + x_2^2 + 125x_3^2$ if k is sufficiently large. Other possibilities are also easily eliminated since the form $x^2 + y^2 + 2z^2$ is easily seen to represent n as soon $n = 4 (\text{mod } 8)$, cf. [5, p. 137]. This completes the proof.

Remark 3. This corollary has been first proved by D.R. Heath-Brown, [5], by a different method; according to [5, p. 137], it answers a question posed by P. Erdös and A. Ivic.

Acknowledgement. It is my pleasant duty to thank Professor W. Duke for a few useful conversations during the conference, relating to his work [3].

Literature cited

[1] W.S. Cassels, Rationale quadratische Formen, Jahresbericht der Deutschen Mathematiker-Vereinigung, 82 (1980), p. 81-93.

[2] B.A. Cipra, On the Niwa-Shintani theta-kernel lifting of modular forms, Nagoya Mathematical Journal, 91 (1983), p. 49-117.

[3] W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, Inventiones Mathematicae, 92 (1988), p. 73-90.

[4] O.M. Fomenko and E.P. Golubeva, Asymptotic distribution of integral points on a two-dimensional sphere, Zapiski LOMI, 160 (1987), p. 54-71.

[5] D.R. Heath-Brown, Ternary quadratic forms and sums of three square-full numbers, Séminaire de Théorie des Nombres, Paris 1986/87 (edited by C. Goldstein), Birkhäuser, 1988, p. 137-163.

[6] H. Iwaniec, Fourier coefficients of modular forms of half-integral weight, Inventiones Mathematicae, 87 (1987), p. 385-401.

[7] Yu. V. Linnik, On representation of large integers by positive definite quadratic forms, Izvestia Akademij Nauk SSSR (seria matematicheskaya), 4 (1940), p. 363-402.

[8] Yu. V. Linnik, Ergodic properties of algebraic fields, Springer-Verlag, 1968.

[9] A.V. Malyshev, Yu. V. Linnik's ergodic method in number theory, Acta Arithmetica, 27 (1975), 555-598.

[10] B.Z. Moroz, Recent progress in analytic arithmetic of positive definite quadratic forms, Max-Planck-Institut für Mathematik, Preprint, 1989.

[11] M. Peters, Darstellungen durch definite ternäre quadratische Formen, Acta Arithmetica , 34 (1977), p. 57-80.

[12] R. Schulze-Pillot, Thetareihen positiv definiter quadratischer Formen, Inventiones Mathematicae, 75 (1984), p. 283-299.

[13] G. Shimura, On modular forms of half-integral weight, Annals of Mathematics, 97 (1973), p. 440-481.

[14] C.L. Siegel, Über die analytische Theorie der quadratischen Formen, Gesammelte Abhandlungen, Bd. I, Springer-Verlag, 1966, p. 326-405.

[15] C.L. Siegel, Über die Klassenzahl quadratischer Zahlkörper, loc. cit., p. 406-409.

[16] Yu. G. Teterin, Representations of integers by spinor genera of translated lattices, Zapiski LOMI, 151 (1986), p. 135-140.

B.Z. Moroz
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 3, Allemagne

Postscript.

This note contains the text of my lecture at the $16^{\underline{th}}$ Journées Arithmétiques (Marseilles, July 1989). Since then a new important paper by W. Duke and R. Schulze–Pillot, [17], has appeared, which allows, in particular, to weaken the condition $(n,2D) = 1$ in the Theorem 1 of this note (cf. also Remark 1). Unfortunately, the auhtors suppress the details of the proof of their crucial Lemma 2, [17, p. 50–51]; following [4], where incidentally the proof of the corresponding assertion is also omitted, we are content with a weaker statement, [10, p. 17–19], that leads to the results described above. Finally we cite here two articles, [18], [19], throwing further light on our subject.

References

[17] W. Duke, R. Schulze–Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, Inventiones mathematicae, 99 (1990), 49–57.

[18] W. Duke, Lattice points on ellipsoids, Séminaire de Théorie de Nombres de Bordeaux le 20 mai 1988, Année 1987–88, Exposé n°37.

[19] O.M. Fomenko, Estimates of the norms of cusp–forms and arithmetic applications, Zapiski LOMI, 168 (1988), p. 158–179.

A list of corrections to [10].

p. 3, line 6: read "stay" instead of "start"

p. 5, line 2 from below and p. 26, last line:

read $|s-3-1/24|$ instead of $s-3-1/24$

p. 20 line 13: read x_3^2 instead of x_3

Postscript.

This note contains the text of my lecture at the $16^{\underline{th}}$ Journées Arithmétiques (Marseilles, July 1989). Since then a new important paper by W. Duke and R. Schulze–Pillot, [17], has appeared, which allows, in particular, to weaken the condition $(n,2D) = 1$ in the Theorem 1 of this note (cf. also Remark 1). Unfortunately, the auhtors suppress the details of the proof of their crucial Lemma 2, [17, p. 50–51]; following [4], where incidentally the proof of the corresponding assertion is also omitted, we are content with a weaker statement, [10, p. 17–19], that leads to the results described above. Finally we cite here two articles, [18], [19], throwing further light on our subject.

References

[17] W. Duke, R. Schulze–Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, Inventiones mathematicae, 99 (1990), 49–57.

[18] W. Duke, Lattice points on ellipsoids, Séminaire de Théorie de Nombres de Bordeaux le 20 mai 1988, Année 1987–88, Exposé n°37.

[19] O.M. Fomenko, Estimates of the norms of cusp–forms and arithmetic applications, Zapiski LOMI, 168 (1988), p. 158–179.

A list of corrections to [10].

p. 3, line 6: read "stay" instead of "start"

p. 5, line 2 from below and p. 26, last line:

read $|s-3-1/24|$ instead of $s-3-1/24$

p. 20 line 13: read x_3^2 instead of x_3