

Astérisque

B. Z. MOROZ

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

Astérisque, tome 209 (1992), p. 275-278

http://www.numdam.org/item?id=AST_1992__209__275_0

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

On the 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 [17] on representation of integers by a genus of quadratic forms had appeared, Yu. V. Linnik [10] initiated a study of representation of integers by an individual ternary quadratic form. Due to the efforts of many authors (cf., for instance, [1], [3], [9], [11], [12], [15], [19], 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 $a_{ij} = a_{ji}$, $a_{ij} \in \mathbb{Z}$, $2 \mid a_{ii}$ for $1 \leq i, j \leq 3$, and let $r_f(n) = \text{card} \{u \mid u \in \mathbb{Z}^3, f(u) = n\}$ be the representation number of n by f ; let $D = \det(a_{ij})$.

THEOREM 1. *Suppose that $n \in \mathbb{Z}$, $n \geq 1$ and $\gcd(n, 2D) = 1$. Then $r_f(n) = r(n, \text{gen } f) + O(n^{\frac{1}{2}-\gamma})$ for $\gamma < \frac{1}{28}$, 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 [17]. Moreover, if n is primitively represented by f over the ring of p -adic integers for each rational prime p then $r(n, \text{gen } f) \gg_{f, \epsilon} n^{\frac{1}{2}-\epsilon}$ for $\epsilon > 0$.*

Proof. Let N be a positive integer such that $2D \mid N$ and $8 \mid N$, and let $\varphi \in S_0(\frac{3}{2}, N, \chi)$ with $\chi(d) = (\frac{2D}{d})$, suppose furthermore that $\varphi \in \mathcal{U}^\perp$, in the notation of [15]. Thus φ is a 'good' cusp-form of weight $\frac{3}{2}$ (and character χ) that does not come from a θ -series. Therefore an argument due to H. Iwaniec [9] and W. Duke [3], supplemented by the considerations going back to G. Shimura [16] and B. A. Cipra [2], leads to an estimate for the

Fourier coefficients of φ (cf. also [7]), and on writing $\varphi(z) = \sum_{n=1}^{\infty} a(n)e^{2\pi inz}$ we obtain: $a(n) \ll_{\varphi, \gamma} n^{\frac{1}{2}-\gamma}$ as soon as $(n, 2D) = 1$ and $\gamma < \frac{1}{28}$. By [15, Korollar 3], it follows then that $r_f(n) = r(n, \text{spn } f) + O(n^{\frac{1}{2}-\gamma})$ 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. [15]). On the other hand, by [15, Korollar 2], if $(n, 2D) = 1$ then $r(n, \text{spn } f) = r(n, \text{gen } f)$. Finally, the estimate $r(n, \text{gen } f) \gg n^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$ is a consequence of Siegel's work [17, 18] (cf. also [14, 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 $(n, 2D) = 1$ in Theorem 1 has been used in the proof twice, to ensure the estimate $a(n) \ll n^{\frac{1}{2}-\gamma}$ and to deduce the identity $r(n, \text{spn } f) = r(n, \text{gen } f)$. The former use of this condition is due to the fact that $\varphi \in S(\frac{3}{2}, N, \chi)$ with $\chi = (\frac{2D}{d})$ (see [13] for the details). It is an interesting question to what extent one can weaken the condition $(n, 2D) = 1$ in Theorem 1. The work of R. Schulze-Pillot [15] (cf. also [19] and references therein) is pertinent to this question.

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

Proof. Let $n = q^\ell n_1$, $q \mid n_1$ 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 $n_2 \not\equiv 0 \pmod{q}$ when $\ell < 3$, it follows from Theorem 1 that $r_g(n_2) \gg n_2^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$. 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 the 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 $r_f(n) \gg n^{\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$. This completes the proof.

REMARK 2. Theorem 2 confirms a conjecture of D. R. Heath-Brown [8, p. 137-138], that every large integer congruent to 7 modulo 8 is represented by the form $x_1^2 + x_2^2 + q^3 x_3^2$ 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 $p \mid n \Rightarrow p^2 \mid n$ 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, 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 as $n \equiv 4 \pmod{8}$, cf. [8, p. 137]. This completes the proof.

REMARK 3. This corollary has been first proved by D. R. Heath-Brown [8], by a different method; according to [8, p. 137], it answers a question posed by P. Erdős and A. Ivić.

REMARK 4. This note contains the text of my lecture at the 16th Journées Arithmétiques (Marseilles, July 1989). Since then a new important paper by W. Duke and R. Schulze-Pillot [5] has appeared, which allows, in particular, to weaken the condition $(n, 2D) = 1$ in Theorem 1 of this note (cf. also Remark 1). Unfortunately, the authors suppress the details of the proof of their crucial Lemma 2 [5, p. 50–51]; following [7], where incidentally the proof of the corresponding assertion is also omitted, we are content with a weaker statement [13, p. 17–19] that leads to the results described above. Finally, we cite here two articles [4], [6], throwing further light on our subject.

ACKNOWLEDGEMENT. It is my pleasant duty to thank Professor W. Duke for a few useful conversations during the conference, relating to his work [3]; I am grateful also to Professor R. Schulze-Pillot for a private communication, allowing me to reconstruct the proof of Lemma 2 in [5] mentioned above.

References

- [1] Cassels, J.W.S.: Rationale quadratische Formen. Jahresbericht der Deutschen Mathematiker-Vereinigung, 82 (1980), 81–93.
- [2] Cipra, B.A.: On the Niwa-Shintani theta-kernel lifting of modular forms. Nagoya Mathematical Journal, 91 (1983), 49–117.
- [3] Duke, W.: Hyperbolic distribution problems and half-integral weight Maass forms. Inventiones Mathematicae, 92 (1988), 73–90.
- [4] Duke, W.: Lattice points on ellipsoids. Séminaire de Théorie des Nombres de Bordeaux, le 20 mai 1988, Année 1987–88, Exposé no. 37.
- [5] Duke, W. & Schulze-Pillot, R.: Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids. Inventiones Mathematicae, 99 (1990), 49–57.
- [6] Fomenko, O.M.: Estimates of the norms of cusp-forms and arithmetic applications. Zapiski LOMI, 168 (1988), 158–179.

- [7] Fomenko, O.M. & Golubeva, E.P.: Asymptotic distribution of integral points on a two-dimensional sphere. *Zapiski LOMI*, 160 (1987), 54–71.
- [8] Heath-Brown, D.R.: Ternary quadratic forms and sums of three square-full numbers; in: *Séminaire de Théorie des Nombres, Paris 1986/87* (edited by C. Goldstein), Birkhäuser, 1988; pp. 137–163.
- [9] Iwaniec, H.: Fourier coefficients of modular forms of half-integral weight. *Inventiones Mathematicae*, 87 (1987), 385–401.
- [10] Linnik, Yu. V.: On the representation of large integers by positive definite quadratic forms. *Izvestiya Akademii Nauk SSSR (ser. mat.)*, 4 (1940), 363–402.
- [11] Linnik, Yu. V.: *Ergodic properties of algebraic fields*. Springer-Verlag, 1968.
- [12] Malyshev, A.V.: Yu. V. Linnik's ergodic method in number theory. *Acta Arithmetica*, 27 (1975), 555–598.
- [13] Moroz, B.Z.: *Recent progress in analytic arithmetic of positive definite quadratic forms*. Max-Planck-Institut für Mathematik, preprint, 1989.
- [14] Peters, M.: *Darstellungen durch definite ternäre quadratische Formen*. *Acta Arithmetica*, 34 (1977), 57–80.
- [15] Schulze-Pillot, R.: *Thetareihen positiv definiter quadratischer Formen*. *Inventiones Mathematicae*, 75 (1984), 283–299.
- [16] Shimura, G.: On modular forms of half-integral weight. *Annals of Mathematics*, 97 (1973), 440–481.
- [17] Siegel, C.L., *Über die analytische Theorie der quadratischen Formen*; in: *Gesammelte Abhandlungen*, Bd. I. Springer-Verlag, 1966; 326–405.
- [18] Siegel, C.L., *Über die Klassenzahl quadratischer Zahlkörper*; in: *Gesammelte Abhandlungen*, Bd. I. Springer-Verlag, 1966; 406–409.
- [19] Teterin, Yu. G.: Representations of integers by spinor genera of translated lattices. *Zapiski LOMI*, 151 (1986), 135–140.

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