La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-07944-4 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

Square-free points on ellipsoids

by

R. C. Baker (Egham)

1. Introduction. A point x of Z^k with non-zero coordinates is said to be *square-free* if

$$\mu^2(|x_1|)\ldots\mu^2(|x_k|) = 1.$$

In this note we give a simple criterion for the presence of square-free points on a given ellipsoidal surface

$$f(x) = n. \tag{1}$$

Here $k \geqslant 4$; f is a positive integral quadratic form; and the integer $n > C_1(f)$.

The result obtained depends on the work of Podsypanin [3], who found that for $\varepsilon > 0$ the surface (1) contains

$$\frac{6^k\pi^{-3k/2}}{(\det f)^{1/2}\Gamma(k/2)} Gn^{(k/2)-1} + O(n^{(k/2)-1-\alpha+\varepsilon}) \tag{2}$$

square-free points, where $\alpha = (k-3)/(4k+4)$. Here G is a 'singular series', defined precisely below. (Constants implied by 'O' and '$\gg$' depend at most on f and ε.)

For every prime power p^r $(r \geqslant 2)$ let $\varrho(p^r, n)$ denote the number of solutions of the congruence

$$f(x) \equiv n \pmod{p^r}$$

in integers $x_1, \ldots, x_k$ not divisible by p^2. Let us write

$$n = \prod_p p^{\omega}, \quad 2^k \det f = \prod_p p^{\theta} \tag{3}$$

where $\omega = \omega(n, p)$, $\theta = \theta(f, p)$.

Theorem. (a) *We have*

$$\varrho(p^r, n) \geqslant p^{(r-2)(k-1)} \quad \textit{whenever} \quad p \nmid 2^{k+1}\det f. \tag{4}$$

(b) *For $n > C_1(f)$, the surface* (1) *contains square-free points if, and only if,*

(5) $$\varrho(p^N, n) > 0 \quad \text{for all } p \mid 2^{k+1}\det f.$$

Here

(6) $$N = N(n, f, p) = \begin{cases} \min(5+\theta, 3+\omega), & p = 2,\\ \max\{\min(3+\theta, 1+\omega), 2\}, & p > 2.\end{cases}$$

The condition in (b) is a refinement of one in [3]. Podsypanin requires $\varrho(p^N, n) > 0$ for all primes p with

$$p \mid 2^{k+1}\prod_S D_S.$$

Here the product is over all nonempty $S \subseteq \{1, \ldots, n\}$, with the notations

$$f(x) = \sum_{1\leqslant i,j\leqslant n} a_{ij}x_i x_j, \qquad 2a_{ij} = 2a_{ji} \in \boldsymbol{Z},\ a_{ii} \in \boldsymbol{Z},$$

$$\det f = \det(a_{ij}),$$

$$D_S = \det\Big(\sum_{i,j\in S} a_{ij}x_i x_j\Big).$$

The factor 2^{k+1} is required in (4), (5) because $\det f$ may be an odd multiple of 2^{-k}. Moreover, even in a simple case such as $f(x) = x_1^2 + \ldots + x_k^2$, $4 \leqslant k \leqslant 6$, there are n with $\varrho(2^5, n) = 0$. See Estermann [2].

It is easy to deduce part (b) of the theorem from part (a). To do so we need two expressions for G from [3], § 7. Firstly,

(7) $$G = \prod_p \Big(1 + (1-p^{-2})^{-k}\sum_{\nu=1}^{\infty} B(p^\nu)\Big).$$

Here

$$B(p^\nu) = \sum_{\substack{h=1\\ p\nmid h}}^{p^\nu}\sum_{\varepsilon_1=0}^{1}\cdots\sum_{\varepsilon_k=0}^{1}\sum_{x_1=1}^{p^\nu}\cdots\sum_{x_k=1}^{p^\nu}\frac{(-1)^{\varepsilon_1+\ldots+\varepsilon_k}}{p^{2\varepsilon_1+\ldots+2\varepsilon_k}} \times e\left(\frac{h\big(f(p^{2\varepsilon_1}x_1, \ldots, p^{2\varepsilon_k}x_k) - n\big)}{p^\nu}\right)$$

with the notation $e(\theta) = e^{2\pi i\theta}$.

Moreover, we have

(8) $$1 + (1-p^{-2})^{-k}\sum_{\nu=1}^{m} B(p^\nu) = p^{-(k-1)m}(1-p^{-2})^{-k}\varrho(p^m, n)$$

for $m \geqslant 2$, with

(9) $$B(p^\nu) = 0 \quad \text{for} \quad \nu > N$$

([3], § 7). Thus the infinite series in (7) can all be 'truncated'.

Deduction of (b) from (a). If there is a square-free point x on the surface (1), then obviously (5) holds. Conversely, suppose that (5) holds. In view of (a) and (8), (9), every factor in the infinite product (7) is $> p^{-(k-1)N}$. Moreover,

$$\prod_{p > C_2(f)}\Big(1 + \sum_{\nu=1}^{N} B(p^\nu)\Big) \geqslant n^{-\varepsilon}$$

([3], § 7). Since $N \leqslant 5+\theta$, from (6), we see that

$$G \geqslant n^{-\varepsilon},$$

which, in view of the asymptotic formula (2), yields square-free points on the surface (1) for $n > C_1(f)$.

2. Proof of (a). Let p be a prime, $p \nmid 2^{k+1}\det f$. We begin by showing that there is a solution x of

(10) $$f(x) \equiv n \pmod p$$

for which

(11) $$\nabla f(x) = \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_k}\right) \text{ has } \geqslant 2 \text{ nonzero components} \pmod p.$$

The number of solutions of (10) is

$$\frac{1}{p}\sum_{h=1}^{p}\sum_{x_1=1}^{p}\cdots\sum_{x_k=1}^{p} e\left(\frac{h(f(x)-n)}{p}\right).$$

By a nonsingular linear transformation of the variables (mod p), as in [3], we can transform this expression to become

$$\frac{1}{p}\sum_{h=1}^{p}\sum_{y_1=1}^{p}\cdots\sum_{y_k=1}^{p} e\left(\frac{h(a_1y_1^2 + \ldots + a_ky_k^2) - hn}{p}\right) \geqslant p^{k-1} - \frac{1}{p}(p-1)p^{k/2}.$$

Here $p \nmid a_1 \ldots a_k$. The lower bound is obtained by separating the term $h = 0$ and using the well-known evaluation of Gauss's sum for $h = 1, \ldots, p-1$.

The number of x (mod p) for which $\nabla f(x)$ has one or fewer nonzero components is obviously $\leqslant kp$. For example,

$$\frac{\partial f}{\partial x_2} \equiv \ldots \equiv \frac{\partial f}{\partial x_k} \equiv 0 \pmod p$$

defines a one-dimensional subspace of $(Z/pZ)^k$, since the linear forms $\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_h}$ have determinant $2^k \det f \not\equiv 0 \pmod p$.

Now we easily see that

$$p^{k-1} - \frac{1}{p}(p-1)\, p^{k/2} > kp.$$

After all,

$$kp + \frac{1}{p}(p-1)\, p^{k/2} < \left(\frac{k}{p}+1\right) p^{k/2} < \frac{2k}{3} p^{k/2},$$

while

$$p^{k-1} \geqslant 3^{(k/2)-1}\, p^{k/2} > (2k/3)\, p^{k/2}$$

for $p \geqslant 3$, $k \geqslant 4$. Thus we may choose and fix an $\boldsymbol{x}$ satisfying (10), (11).

We now construct a vector $\boldsymbol{y} \equiv \boldsymbol{x} \pmod p$ with

(12) $$f(\boldsymbol{y}) \equiv n \pmod{p^2}, \qquad p^2 \nmid y_1, \ldots, p^2 \nmid y_k.$$

Suppose, for instance, that

$$\nabla f(\boldsymbol{x}) = (d_1, \ldots, d_k), \qquad p \nmid d_1 d_2.$$

We take $\boldsymbol{y}$ of the form

(13) $$\boldsymbol{y} = \boldsymbol{x} + p\boldsymbol{z},$$

so that

$$f(\boldsymbol{y}) \equiv f(\boldsymbol{x}) + p\boldsymbol{d}.\boldsymbol{z} \pmod{p^2} \equiv n + bp + p\boldsymbol{d}.\boldsymbol{z} \pmod{p^2}$$

where $f(\boldsymbol{x}) = n + bp$. The conditions (12) now reduce to

(14) $$\boldsymbol{d}.\boldsymbol{z} \equiv -b \pmod p$$

together with k conditions

(15.j) $$x_j + pz_j \not\equiv 0 \pmod{p^2} \qquad (j = 1, \ldots, k).$$

Now (15.j) is vacuous if $x_j \not\equiv 0 \pmod p$. Otherwise, it excludes one value of $z_j \pmod p$. We choose x_j to satisfy (15.j) for $j = 3, 4, \ldots, k$. Now (14) reduces to (say)

(16) $$d_1 z_1 + d_2 z_2 \equiv c \pmod p,$$

with $p \nmid d_1 d_2$. There are $\geqslant p-1 \geqslant 2$ choices of z_2 with (15.2). Each defines a value z_1 with (16), and at least one of these z_1's must satisfy (15.1). So we can indeed satisfy (14) together with (15.1)–(15.k), and $\boldsymbol{y}$ can be constructed as asserted.

The above argument is a variant of Hensel's lemma. We now use this lemma in the conventional form (see e.g. [1], pp. 42–43). Since $\nabla f(\boldsymbol{y}) \not\equiv \boldsymbol{0} \pmod p$ by (11), (13), we can construct p^{k-1} solutions of

$$f(\boldsymbol{w}) \equiv n \pmod{p^3}$$

with $\boldsymbol{w} \equiv \boldsymbol{y} \pmod{p^2}$. Thus

(17) $$\varrho(p^3, n) \geqslant p^{k-1}.$$

We already know from (8), (9) that

(18) $$\varrho(p^r, n) = p^{(r-3)(k-1)} \varrho(p^3, n) \qquad (r \geqslant 3).$$

(Recall that $N \leqslant 3$ in (6) since $p > 2$, $\theta = 0$.) Now (a) follows at once on combining (17) and (18).

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press 1966.

[2] T. Estermann, *Sums of squares of square-free numbers*, Proc. London Math. Soc. (2) 53 (1951), pp. 125–137.

[3] E. V. Podsypanin, *On the representation of the integer by positive quadratic forms with square-free variables*, Acta Arith. 27 (1975), pp. 459–488.

ROYAL HOLLOWAY AND BEDFORD NEW COLLEGE
Egham, Surrey TW20 0EX, England

Received on 7.10.1985 (1549)