Square-free points on ellipsoids

by

R. C. Baker (Egham)

1. Introduction. A point \( x \) of \( \mathbb{Z}^k \) with non-zero coordinates is said to be square-free if

\[
\mu^2(|x_1|) \cdots \mu^2(|x_k|) = 1.
\]

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

\[
f(x) = n.
\]

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

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

\[
\frac{6^k \pi^{3k/2}}{(\det(f))^{1/2}} \frac{G(n^{k/2}) - 1 + O(n^{k/2} - 1 - e)}{\Gamma(k/2)}
\]

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

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

\[
f(x) \equiv n(mod \, p^r)
\]
in integers \( x_1, \ldots, x_k \) not divisible by \( p^2 \). Let us write

\[
n = \prod_p p^{\omega}, \quad 2^k \det f = \prod_p p^\theta
\]

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

THEOREM. (a) We have

\[
\varrho(p^r, n) \gg p^{r-2(\alpha-1)} \quad \text{whenever} \quad p \not\equiv 2^{k+1} \det f.
\]
(b) For $n > C_1(f)$, the surface (1) contains square-free points if, and only if,

$$\varepsilon(p^n, n) > 0 \quad \text{for all } p | 2k+1 \text{ det } f.$$ 

Here

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

The condition in (b) is a refinement of one in [3]. Podsypanin requires $\varepsilon(p^n, n) > 0$ for all primes $p$ with $p | 2k+1 \prod S$.

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

$$f(x) = \sum_{i \leq j \leq \min(n, S)} a_{ij} x_i x_j, \quad 2a_{ij} = 2a_{ji} \in \mathbb{Z}, \quad a_{ii} \in \mathbb{Z},$$

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

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

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

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

Here

$$B(p^v) = \sum_{k=1}^{v} \sum_{a_k \neq 0} \frac{p^{k-1} + \ldots + p^{k-1}}{p^{k-1} x_1 \ldots x_k} \times e\left(\frac{a_1 x_1 + \ldots + a_k x_k - n}{p^v}\right)$$

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

Moreover, we have

$$1 + (1 - p^{-2})^{-k} \sum_{v=1}^{\infty} B(p^v) = p^{-(k+1)n}(1 - p^{-2})^{-k} \varepsilon(p^n, n)$$

for $m \geq 2$, with

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

([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 $\gg p^{-(k-1)n}$. Moreover,

$$\prod_{p \geq \gamma_1(f)} \left(1 + \sum_{v=1}^{\infty} B(p^v)\right) \gg n^{-\varepsilon}$$

([3], § 7). Since $N \leq 5 + \theta$, from (6), we see that $G \gg n^{-1}$.

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, $p \not | 2k+1 \text{ det } f$. We begin by showing that there is a solution $x$ of

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

for which

$$\frac{\partial f}{\partial x_1} = \ldots = \frac{\partial f}{\partial x_k} \text{ has } \geq 2 \text{ nonzero components } \pmod{p},$$

for $f(x)$ has $\geq 2$ nonzero components (mod $p$).

The number of solutions of (10) is

$$\frac{1}{p} \sum_{x_1=1}^{p} \ldots \sum_{x_k=1}^{p} \sum_{y_1=1}^{p} \ldots \sum_{y_k=1}^{p} \left(\frac{h(f(x) - n)}{p}\right).$$

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

$$\frac{1}{p} \sum_{y_1=1}^{p} \ldots \sum_{y_k=1}^{p} \sum_{x_1=1}^{p} \ldots \sum_{x_k=1}^{p} e\left(\frac{h(a_1 y_1^2 + \ldots + a_k y_k^2) - h n}{p}\right) \geq p^{k-1} - \frac{1}{p} (p-1)^n.$$

Here $p \not | a_1 \ldots a_k$. 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 $\frac{\partial f}{\partial x_1} = \ldots = \frac{\partial f}{\partial x_k}$ is $\equiv 0$ (mod $p$)
defines a one-dimensional subspace of \((\mathbb{Z}/p\mathbb{Z})^k\), since the linear forms \(\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_k}\) 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

\[ p^{k-1} \geq 3^{(k/2)-1} p^{k/2} > (2k/3) p^{k/2} \]

for \(p \geq 3, k \geq 4\). Thus we may choose and fix an \(x\) satisfying (10), (11).

We now construct a vector \(y \equiv x \pmod{p}\) with

\[ f(y) \equiv n \pmod{p^3}, \quad p^2 \not\equiv y_1, \ldots, p^2 \not\equiv y_k. \]

Suppose, for instance, that

\[ f(x) = (d_1, \ldots, d_k), \quad p \not\equiv d_1 d_2. \]

We take \(y\) of the form

\[ y = x + px, \]

so that

\[ f(y) \equiv f(x) + px \equiv n + bp + px \pmod{p^3} \]

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

\[ d_j z \equiv -b \pmod{p} \]

together with \(k\) conditions

\[ x_j + pz_j \not\equiv 0 \pmod{p^3} \quad (j = 1, \ldots, k). \]

Now (15) 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) for \(j = 3, 4, \ldots, k\). Now (14) reduces to (say)

\[ d_1 z_1 + d_2 z_2 \equiv c \pmod{p}, \]

with \(p \not\equiv d_1 d_2\). There are \(p-1 \geq 2\) 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 \(y\) 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 \(\overline{f}(y) \not\equiv 0 \pmod{p}\) by (11), (13), we can construct \(p^{k-1}\) solutions of

\[ f(w) \equiv n \pmod{p^3} \quad \text{with} \quad w \equiv y \pmod{p^3}. \]

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

\[ g(p^{\theta}, n) \geq p^{k-1}. \]

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

References


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

Received on 7.10.1985 (1549)