Mh. Math. 99, 45–72 (1985)

Monatshefte für
Mathematik


# Integer Points on Curves and Surfaces [1]

By

**Wolfgang M. Schmidt**, Boulder

*(Received 1 October 1984)*

**Abstract.** Various upper bounds are given for the number of integer points on plane curves, on surfaces and hypersurfaces. We begin with a certain class of convex curves, we treat rather general surfaces in $\mathbb{R}^3$ which include algebraic surfaces with the exception of cylinders, and we go on to hypersurfaces in $\mathbb{R}^n$ with nonvanishing Gaussian curvature.

**1. Introduction.** It is well known (JARNIK [8]) that on a plane convex curve of length $l \geqslant 1$ there are $\ll l^{2/3}$ integer points. This estimate is best possible, and the constant in $\ll$ is absolute. The convex curve may be a closed curve or it may be a curve $y = f(x)$. In particular, if $f(x)$ is twice differentiable in some interval of length at most $N \geqslant 1$, with either $f'' > 0$ or $f'' < 0$ throughout, and if the range of $f$ is contained in an interval of length $N$, then the number $Z$ of integer points on the curve $y = f(x)$ satisfies

$$Z \ll N^{2/3} . \tag{1.1}$$

SWINNERTON-DYER [11] took up the question of what can be said if higher derivatives exist. Let $\mathfrak{C}$ be a fixed curve $y = f(x)$ where $x$ runs through some finite closed interval, where $f'''$ exists and is continuous, and where $f'' > 0$ or $f'' < 0$ throughout. Let $Z_N$ be the number of integer points on the blown up curve $N\mathfrak{C}$, consisting of points $(Nx, Ny)$ with $(x, y)$ on $\mathfrak{C}$. Then according to Swinnerton-Dyer, we have

$$Z_N \leqslant c_1(\mathfrak{C}, \varepsilon) N^{(3/5)+\varepsilon} \tag{1.2}$$

for $N \geqslant 1$ and $\varepsilon > 0$.

[1] Written with partial supports from NSF grant No. MCS-8211461.

Since in this result a fixed curve is blown up, we may ask what can be said of an arbitrary smooth curve contained in a square of side $N$. Now given an arbitrary chain of integer points, one can always construct a curve, differentiable to any prescribed order, which passes through these points. Moreover, if the chain of points forms the vertices of a convex polygon, then the smooth curve can also be made convex, so that one cannot assert more than (1.1). Hence my first plan was to impose a condition on the sign of $f'''$. However, it turns out that the third derivative is dispensible, it being enough that the second derivative is monotonic.

**Theorem 1.** *Let $\mathfrak{C}$ be a curve contained in a square of side $N \geqslant 1$, given by $y = f(x)$ where $f''$ exists and is weakly monotonic, and vanishes for at most one value of $x$. Then for $\varepsilon > 0$, the number $Z$ of integer points on $\mathfrak{C}$ has*

$$Z \leqslant c_2(\varepsilon)\, N^{(3/5)+\varepsilon}\,. \tag{1.3}$$

The essential point is that the constant does not depend on $\mathfrak{C}$. The exponent is the same as in (1.2), and indeed the proof is a variation on the argument of Swinnerton-Dyer. I conjecture that in fact $Z \leqslant c_3 N^{1/2}$, or at least $Z \leqslant c_3(\varepsilon)\, N^{(1/2)+\varepsilon}$ for $\varepsilon > 0$. The example $f(x) = \sqrt{x}$ shows that the exponent 1/2 would be best possible.

Let $\mathfrak{C}$ be an algebraic curve defined by an irreducible polynomial equation $f(x, y) = 0$ of degree $d > 1$. Such a curve consists of at most $c_4(d)$ pieces of the type $y = f(x)$ with monotonic $f''$ and with $f''$ not changing sign, plus at most $c_5(d)$ extra points. By Theorem 1 the number $Z(N)$ of integer points $(x, y)$ on $\mathfrak{C}$ with $|x| \leqslant N$, $|y| \leqslant N$ where $N \geqslant 1$, has

$$Z(N) \leqslant c_6(d, \varepsilon)\, N^{(3/5)+\varepsilon}\,. \tag{1.4}$$

I believe that when $\mathfrak{C}$ is of positive genus, then in fact $Z(N) \leqslant c_7(d, \varepsilon)\, N^{\varepsilon}$. Of course, by Siegel's result, $Z(N) \leqslant c_8(f)$ in this case, but our $c_7$ is supposed to be independent of $f$.

We next will discuss surfaces in $\mathbb{R}^3$. Very roughly speaking, our result is that for reasonably nice surfaces contained in a cube of side $N$, the number $Z$ of integer points on the surface has $Z \ll N^{3/2}$. The precise formulation takes a little effort. When the surface is a *cylinder*, i. e. if it consists of the translates of a curve $\mathfrak{C}$ in a given direction, then it is clear that it could have $N$ times as many integer points as the curve. So, for instance when $\mathfrak{C}$ is a plane convex curve, the cylinder could have as many as $\gg N^{5/3}$ integer points in a cube of side $N$. Hence we have to rule out cylinders.

A surface $\mathscr{S}$ will be called *proper* if it consists of points $(x, y, z)$ with $z = f(\mathbf{x})$ where $\mathbf{x} = (x, y)$ runs through a nonempty open set $\mathfrak{D}$, and if the partial derivatives of $f$ up to the third order exists on $\mathfrak{D}$ and can be extended to continuous functions on the closure $\bar{\mathfrak{D}}$ of $\mathfrak{D}$. A proper surface will be called an *elementary piece* if $\mathfrak{D}$ is of the type $a < x < b$, $\psi_1(x) < y < \psi_2(x)$ with continuous functions $\psi_1, \psi_2$ in $a \leqslant x \leqslant b$, if $f_y$ is weakly monotonic on each of the two curves $y = \psi_1(x)$, $y = \psi_2(x)$ $(a \leqslant x \leqslant b)$, and if $f_{yy} \neq 0$, $W \neq 0$ throughout $\mathfrak{D}$, where

$$W = W(x, y) = \begin{vmatrix} f_{yy} & f_{yx} \\ f_{yyy} & f_{yyx} \end{vmatrix}.$$

A proper surface is part of a paraboloid if $f$ is a quadratic polynomial. Such a paraboloid is either a (parabolic) cylinder or an elliptic or hyperbolic paraboloid.

**Theorem 2.** *Suppose that either $\mathscr{S}$ or $\mathscr{S}(\pi/4)$ or $\mathscr{S}(\pi/2)$ or $\mathscr{S}(3\pi/4)$ is an elementary piece, where $\mathscr{S}(\varphi)$ is obtained from $\mathscr{S}$ by rotation about the z-axis by $\varphi$ degrees, or else that $\mathscr{S}$ is part of an elliptic or hyperbolic paraboloid. Then the number of integer points on $\mathscr{S}$ lying in a cube of side $N \geqslant 1$ is $\ll N^{3/2}$, with an absolute constant in $\ll$.*

This was essentially obtained by the author some twenty years ago [10]. The conclusion remains true when $\mathscr{S}(\varphi)$ is an elementary piece with $\tan\varphi$ rational, but now the constant in $\ll$ depends on $\varphi$. The most severe restriction for an elementary piece is that $W \neq 0$. If $W$ is not identically zero, one can expect that $\mathscr{S}$ is contained in the union of not too many elementary pieces and their boundaries. The question thus arises, what does it mean when $W = 0$ on $\mathfrak{D}$? We will see that it means that $\mathscr{S}$ is a *surface of translation*, i. e. the intersection of $\mathscr{S}$ with each plane $x = c$ is always the same curve, up to a translation which may depend on $c$. So what happens when each of $\mathscr{S}$, $\mathscr{S}(\pi/4)$, $\mathscr{S}(\pi/2)$, $\mathscr{S}(3\pi/4)$ is a surface of translation? In the case when $f$ is analytic, we will see that in this case $\mathscr{S}$ is either part of a cylinder or part of a paraboloid. Note that a proper surface is part of a cylinder when

$$f(\mathbf{x}) = g(L(\mathbf{x})) + M(\mathbf{x}) \tag{1.5}$$

with linear forms $L$, $M$ and with $g$ a function of one variable.

Define $W_\varphi$ in the obvious way with respect to $\mathscr{S}(\varphi)$; its domain is the rotated set $\mathfrak{D}_\varphi$ of $\mathfrak{D}$.

**Theorem 3.** *Let $\mathscr{S}$ be a proper*[2] *surface such that $W_1 = W$, $W_{\pi/4}$, $W_{\pi/2}$, $W_{3\pi/4}$ vanish identically. Then $\mathfrak{D}$ contains a nonempty open subset $\mathfrak{E}$ such that the surface $z = f(\mathbf{x})$ with $\mathbf{x} \in \mathfrak{E}$ is part of a cylinder or part of a paraboloid.*

The conclusion would still obtain with other angles, and perhaps with fewer angles. Combining Theorems 2, 3 we will deduce the following

**Corollary.** *Let $n \geqslant 3$ and let $\mathscr{S} \subseteq \mathbb{R}^n$ be an algebraic hypersurface, defined by an irreducible, non-trivial polynomial equation of degree d. Suppose that $\mathscr{S}$ is not a cylinder, and by this I mean that $\mathscr{S}$ should not consists of the translates of a curve $\mathfrak{C}$ in directions parallel to a given $(n-2)$-dimensional subspace. Then given $N \geqslant 1$, the number $Z(N)$ of integer points on $\mathscr{S}$ in the cube $|x_i| < N$ $(i = 1, \ldots, n)$ satisfies*

$$Z(N) \leqslant c_9(n, d)\, N^{n-(3/2)}\,. \tag{1.6}$$

When the algebraic hypersurface is a cylinder but not a linear manifold, the bound $Z(N) \leqslant c_{10}(n, d, \varepsilon)\, N^{n-(7/5)+\varepsilon}$ follows from (1.4).

In the case of a cone, i. e. a surface defined by a homogeneous irreducible polynomial equation of degree $d \geqslant 2$, HEATH-BROWN [7] recently had occasion to derive the slightly weaker estimate $Z(N) \leqslant c_{11}(n, d, \varepsilon)\, N^{n-(3/2)+\varepsilon}$ from a paper of S. D. COHEN [4]. In contrast to Cohen's work, our proof will use only simple geometric arguments. I conjecture that $Z(N) \leqslant N^{n-2+\varepsilon}$ unless $\mathscr{S}$ is a rational surface. Of course, much better estimates can be expected for "most" algebraic hypersurfaces.

Let $\mathfrak{K}$ be a closed convex body in $\mathbb{R}^n$ where $n > 1$. Suppose that $\mathfrak{K}$ has a finite and positive volume $V$, and surface area $S$. Further suppose that there are $Z$ integer points on the surface of $\mathfrak{K}$, not all contained in a linear manifold of dimension less than $n$. ANDREWS [1, 2] has shown that if $\mathfrak{K}$ is *strictly* convex, then

$$Z \ll S^{n/(n+1)}\,, \tag{1.7}$$

$$Z \ll V^{(n-1)/(n+1)}\,, \tag{1.8}$$

with constants in $\ll$ which depend only on $n$. Since Andrews' proof of (1.8) was difficult, we will present another proof here. Whereas

[2] In our proof, in order to avoid complications, we will suppose that $f$ has fourth order partial derivatives.

Andrews' argument depended on "exterior angles" of polytopes, etc., our argument will use the Geometry of Numbers.

Given $\mathfrak{K}$ as above, let $\mathfrak{Z}$ be the set of extremal points, i. e. points in $\mathfrak{K}$ which are not in the interior of a line segment contained in $\mathfrak{K}$. Then $\mathfrak{Z}$ is just the surface of $\mathfrak{K}$ is strictly convex. In general, $\mathfrak{Z}$ is contained in the surface of $\mathfrak{K}$, and $\mathfrak{K}$ is the convex hull of $\mathfrak{Z}$.

**Theorem 4.** *Let $\mathfrak{K}$, $V$, $S$ be as above, and let $\Lambda$ be a lattice of determinant $\Delta$. Suppose there are $Z$ lattice points in $\mathfrak{Z}$, not all lying in a linear manifold of dimension less than $n$. Then*

$$Z \ll S^{n/(n+1)} \Delta^{-(n-1)/(n+1)}, \tag{1.9}$$

$$Z \ll V^{(n-1)(n+1)} \Delta^{-(n-1)/(n+1)}. \tag{1.10}$$

Andrews formulated his theorems only for strictly convex bodies, but his proofs work for any convex bodies if $Z$ is defined as in our theorem. Thus Andrews showed (1.10) when $\Lambda = \mathbb{Z}^n$, the lattice of integer points. Since any lattice is obtained from $\mathbb{Z}^n$ by a suitable linear transformation, (1.10) follows in general. Furthermore, (1.9) follows from (1.10) by the isoperimetric inequality. Thus Theorem 4 is not really more general than (1.7), (1.8), but the formulation in terms of lattices will be convenient for our proof.

When $n > 2$, it is not clear whether the exponents in (1.9), (1.10) are best possible.

Let $f(x_1, \ldots, x_{n-1})$ be analytic (i. e. expandable into a power series in a suitable neighborhood of each point) in an open domain $\mathfrak{D}$. Let $\mathscr{S}(\mathfrak{A})$ be the surface $z = f(x_1, \ldots, x_{n-1})$ with $(x_1, \ldots, x_{n-1})$ running through some compact subset $\mathfrak{A}$ of $\mathfrak{D}$. Finally, let $Z_N$ be the number of integer points on the blown up surface $N\mathscr{S}(\mathfrak{A})$.

With every point of a differentiable hypersurface in $\mathbb{R}^n$ one associates $n-1$ principal curvatures, which may be positive, negative or zero.

**Theorem 5.** *In addition to all the other properties, suppose that each point of $\mathscr{S}(\mathfrak{A})$ has at least $r$ curvatures which are all positive or all negative. Then for $N \geqslant 1$,*

$$Z_N \leqslant c_{12}(f, \mathfrak{A})\, N^{n-2+2/(r+2)}.$$

Now when $\mathscr{S}(\mathfrak{A})$ has nonvanishing Gaussian curvature, then $r \geqslant [n/2]$ (where [ ] denotes integer parts), whence

$$Z_N \leqslant c_{12}(f, \mathfrak{A})\, N^{n-2+2/([n/2]+2)}. \tag{1.11}$$

Like Swinnerton-Dyer, we have to blow up a fixed manifold. For a convex surface in a cube of side $N$, the surface area $S$ is $\ll N^{n-1}$, and (1.7) gives $Z \ll N^{n-2+2/(n+1)}$. Presumably the same estimate holds for $Z_N$ in the situation of (1.11).

Our proofs of Theorems 1 through 4 will be independent of each other. Theorem 5 will be deduced from Theorem 4.

**2. Swinnerton-Dyer's Lemma.** Consider triples of integer points $(u_1, v_1), (u_2, v_2), (u_3, v_3)$ with positive $u_1, u_2, u_3$. Given such a triple, put

$$\Delta_1 = \begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \quad \Delta_3 = \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix}, \tag{2.1}$$

so that

$$u_2 \Delta_2 = u_1 \Delta_1 + u_3 \Delta_3 . \tag{2.2}$$

Put

$$\Lambda = u_1 (u_1 + u_2) \Delta_1 - u_3 (u_3 + u_2) \Delta_3 . \tag{2.3}$$

**Lemma 1.** *Given $N > 0$, $A \geqslant 1$, $B > 0$, $C > 0$, the number of triples with*

$$u_i \leqslant N \quad (i = 1, 2, 3) , \tag{2.4}$$

$$|v_i| \leqslant A u_i \quad (i = 1, 2, 3) , \tag{2.5}$$

$$0 < \Delta_i \leqslant B \quad (i = 1, 2, 3) , \tag{2.6}$$

*and*

$$|\Lambda| \leqslant C \tag{2.7}$$

*is*

$$\ll N^{\varepsilon} B^{\varepsilon} (A B C + A B^3) , \tag{2.8}$$

*with a constant in $\ll$ depending only on $\varepsilon > 0$.*

This is just an elaboration on Lemma 2 of [11].

*Proof.* At first we keep $\Delta_1, \Delta_2, \Delta_3$ fixed and we estimate the number of triples with these values of $\Delta_1$, $\Delta_2$, $\Delta_3$. By reasons of symmetry we may restrict ourselves to triples with $u_3 \leqslant u_1$. Also, initially we will restrict ourselves to triples with $u_1$ lying in a fixed interval of the type $X \leqslant u_1 < 2X$, and with a given value $d$ of $(u_1, u_3) = \text{g. c. d.}(u_1, u_3)$. Note that $d$ divides $\Delta_2$.

We suppose that a triple $(u_1', v_1')$, $(u_2', v_2')$, $(u_3', v_3')$ with all these properties is given, and we consider all possible triples $(u_1, v_1)$, $(u_2, v_2)$,

$(u_3, v_3)$. If we use (2.2) to eliminate $u_2$ from (2.7), we get

$$|\Delta_1(\Delta_1 + \Delta_2)u_1^2 - \Delta_3(\Delta_3 + \Delta_2)u_3^2| \leqslant \Delta_2 C .$$

Since this is also true for the given triple, we may infer that

$$|\Delta_1(\Delta_1 + \Delta_2)(u_1^2 u_3'^2 - u_1'^2 u_3^2)| \leqslant \Delta_2 C(u_3^2 + u_3'^2) .$$

Moreover, since $u_3 \leqslant u_1$, $u_3' \leqslant u_1'$ and $X \leqslant u_1, u_1' < 2X$, we have $u_3^2 + u_3'^2 \leqslant 2(u_1' u_3 + u_1 u_3')$, whence

$$|u_1 u_3' - u_1' u_3| < 2\Delta_1^{-1} C . \tag{2.9}$$

From the validity of (2.2) for both triples we find that

$$\Delta_1(u_1 u_3' - u_1' u_3) = \Delta_2(u_2 u_3' - u_3 u_2') ,$$

so that $u_1 u_3' - u_1' u_3$ is divisible by $\Delta_2/(\Delta_1, \Delta_2)$. It is similarly divisible by $\Delta_2/(\Delta_3, \Delta_2)$, hence is divisible by $\Delta_2/D$ where

$$D = (\Delta_1, \Delta_2, \Delta_3) .$$

So by (2.9), the number of possible values of $u_1 u_3' - u_l' u_3$ is at most

$$4\Delta_1^{-1}\Delta_2^{-1} DC + 1 . \tag{2.10}$$

When $u_1 u_3' - u_1' u_3$ and $u_1', u_3'$ are given, then the pair $u_1, u_3$ is given up to adding multiples of $d^{-1}u_1'$, $d^{-1}u_3'$ (where $d = (u_1', u_3')$), but since we also want that $d = (u_1, u_3)$, the pair $u_1, u_3$ is given up to adding multiples of $u_1', u_3'$. In view of $X < u_1, u_1' < 2X$, the pair $u_1, u_3$ is in fact uniquely determined. But then $u_2$ is determined by (2.2). Now $v_1, v_2, v_3$ have to be chosen to satisfy (2.1). The only possible freedom for $v_1, v_2, v_3$ consists in adding $\lambda u_1, \lambda u_2, \lambda u_3$ where $\lambda$ is rational. But the denominator of $\lambda$ must divide $(u_1, u_2, u_3)$, hence must divide $D$. Thus there are at most $D$ possibilities for $v_1$ (modulo $u_1$), so that by (2.5) there are altogether $\leqslant (2A + 2)D$ possibilities. In conjunction with (2.10) we get

$$\ll AD(\Delta_1^{-1}\Delta_2^{-1} DC + 1)$$

possible triples. Since the interval $1 \leqslant u_1 \leqslant N$ may be covered by $\ll N^\varepsilon$ intervals of the type $X \leqslant u_1 < 2X$, and since the number of possible divisors $d$ of $\Delta_2$ is $\ll \Delta_2^{\varepsilon/3} \ll B^{\varepsilon/3}$, we see that for given $\Delta_1, \Delta_2, \Delta_3$, the number of possible triples is

$$\ll N^\varepsilon B^{\varepsilon/3} AD(\Delta_1^{-1}\Delta_2^{-1} DC + 1) .$$

We have $\Delta_i = E_i D$ with $0 < E_i \leqslant B D^{-1}$ by (2.6). If for given $D$ we take the sum over $E_1, E_2, E_3$, we obtain

$$\ll N^{\varepsilon} B^{\varepsilon/2} A (B C D^{-1} + B^3 D^{-2}) .$$

Summation over $D \leqslant B$ yields

$$\ll N^{\varepsilon} B^{\varepsilon} (A B C + A B^3) .$$

**3. Theorem 1 under an additional hypothesis.** We first will prove Theorem 1 under the additional assumption that $f'''$ exists and is weakly monotonic throughout.

It clearly will cause no loss of generality if we restrict $x$ to a subinterval $I$ in which, say, $f''' \geqslant 0$, and in which $f'', f'$ are of given sign. Suppose that $f'' > 0, f' > 0$ in $I$. Let

$$I(0) \text{ consist of } x \in I \text{ with } f'(x) \leqslant 1 ,$$

and for natural $\alpha$ let

$$I(\alpha) \text{ consist of } x \in I \text{ with } e^{\alpha - 1} < f'(x) \leqslant e^{\alpha} . \tag{3.1}$$

Then since $f'' > 0$, each $I(\alpha)$ is an interval, possibly empty. $I$ is the union of the intervals $I(\alpha)$ with $\alpha \geqslant 0$. Since the range of $f$, as well as $I$, are contained in intervals of length $\leqslant N$, the length of $I(\alpha)$ satisfies

$$\mu(I((\alpha)) \ll e^{-\alpha} N \quad (\alpha \geqslant 0) . \tag{3.2}$$

In fact the union of the intervals $I(\alpha)$ with $\alpha > \alpha_0$ forms an interval of length $\ll e^{-\alpha_0} N$, and when $\alpha_0 > \log N$, this is $\ll 1$. Since an interval of length $\ll 1$ gives rise to $\ll 1$ integer points, it will suffice to consider the intervals $I(\alpha)$ with $\alpha \ll \log N$.

Next, let $I(\alpha, 0)$ consist of $x \in I(\alpha)$ with $f''(x) \leqslant N^{-1}$. Given natural $\beta$, let $I(\alpha, \beta)$ consist of $x \in I(\alpha)$ with

$$e^{\beta - 1} N^{-1} < f''(x) \leqslant e^{\beta} N^{-1} . \tag{3.3}$$

Then $I(\alpha)$ is the union of the intervals $I(\alpha, \beta)$ with $\beta \geqslant 0$. Denoting the end points of $I(\alpha, \beta)$ by $a \leqslant b$, we have in the case $\beta > 0$ that $f'(b) > f'(a) + (b - a) e^{\beta - 1} N^{-1}$, and therefore $b - a < N e^{\alpha - \beta + 1}$. The last relation is trivially true for $\beta = 0$, so that

$$\mu(I(\alpha, \beta)) \ll e^{\alpha - \beta} N \quad (\alpha \geqslant 0, \beta \geqslant 0) . \tag{3.4}$$

By an argument as above we may restrict ourselves to $\beta \leqslant \alpha + O(\log N) \ll \log N$.

Finally, let $I(\alpha, \beta, 0)$ consist of $x \in I(\alpha, \beta)$ with $f'''(x) \leqslant N^{-2}$, and let $I(\alpha, \beta, \gamma)$ where $\gamma > 0$ consist of $x \in I(\alpha, \beta)$ with

$$e^{\gamma-1} N^{-2} < f'''(x) \leqslant e^{\gamma} N^{-2} . \tag{3.5}$$

Since $f'''$ is monotonic, each $I(\alpha, \beta, \gamma)$ is again an interval—possibly empty. In analogy to (3.4) we find that

$$\mu(I(\alpha, \beta, \gamma)) \ll e^{\beta-\gamma} N \quad (\alpha, \beta, \gamma \geqslant 0) , \tag{3.6}$$

and we may restrict ourselves to $\gamma \ll \log N$.

Combining (3.2), (3.4), (3.6) we have

$$\mu(I(\alpha, \beta, \gamma)) \ll \varphi N \tag{3.7}$$

with

$$\varphi = \varphi(\alpha, \beta, \gamma) = \min(e^{-\alpha}, e^{\alpha-\beta}, e^{\beta-\gamma}) . \tag{3.8}$$

Put

$$\Phi = \varphi N^{2/5}. \tag{3.9}$$

Let $Z(\alpha, \beta, \gamma)$ be the number of integer points on our curve $y = f(x)$ with $x \in I(\alpha, \beta, \gamma)$. Since the number of possibilities for $\alpha, \beta, \gamma$ which we need consider is $\ll (\log N)^3$, it will suffice to show that $Z(\alpha, \beta, \gamma) \ll \ll N^{(3/5)+\varepsilon}$. So let

$$P_1, P_2, \ldots, P_Z \tag{3.10}$$

with $Z = Z(\alpha, \beta, \gamma)$ be the integer points in question, and ordered according to their $x$-coordinates. When $Z \geqslant 4$ and when

$$Q_0 = (x_0, y_0),\ Q_1 = (x_1, y_1),\ Q_2 = (x_2, y_2),\ Q_3 = (x_3, y_3) \tag{3.11}$$

are any four consecutive points among (3.10), consider the triple $(u_1, v_1)$, $(u_2, v_2)$, $(u_3, v_3)$ with $u_i = x_{i=1} - x_i$, $v_i = y_{i+1} - y_i$ $(i = 1, 2, 3)$. We distinguish 4-tuples $Q_0, Q_1, Q_2, Q_3$ of two types, characterized by

$$u_1 + u_2 + u_3 > \Phi \tag{3.12}$$

and

$$u_1 + u_2 + u_3 \leqslant \Phi . \tag{3.13}$$

The number of 4-tuples with (3.12) is clearly

$$\ll \Phi^{-1} \mu(I(\alpha, \beta, \gamma)) \ll N^{3/5}$$

by (3.7), (3.9).

The type (3.13) is more difficult. By the mean value theorem, $v_i/u_i = f'(\xi)$ with $\xi$ in $x_i < \xi < x_{i+1}$. Hence by (3.1), $|v_i| \leqslant e^{\alpha} u_i$, and

(2.5) holds with $A = e^{\alpha}$. By applying the mean value theorem twice one sees (as was explained in [11], formula (9)) that

$$\frac{\Delta_3}{u_1 u_2 (u_1 + u_2)} = \frac{u_1 v_2 - u_2 v_1}{u_1 u_2 (u_1 + u_2)} = \tfrac{1}{2} f''(\eta)$$

where $\eta$ lies in $x_1 < \eta < x_3$. Thus $0 < \Delta_3 < \Phi^3 e^{\beta} N^{-1}$ by (3.3). The same bound holds for $\Delta_1$. It is also true for $\Delta_2$, as seen from formula (11) in [11]. Thus (2.6) holds with $B = \Phi^3 e^{\beta} N^{-1}$. Finally, from formula (10) of [11] we see that $|\Delta| \leqslant \Phi^6 e^{\gamma} N^{-2}$ by (3.5), so that (2.7) holds with $C = \Phi^6 e^{\gamma} N^{-2}$. Substituting this into (2.8) we obtain

$$\begin{aligned} &\ll N^{2\varepsilon} (\Phi^9 e^{\alpha+\beta+\gamma} N^{-3} + \Phi^9 e^{\alpha+3\beta} N^{-3}) \\ &= N^{2\varepsilon} \Phi^9 N^{-3} (e^{\alpha+\beta+\gamma} + e^{\alpha+3\beta}) \\ &= N^{(3/5)+2\varepsilon} \varphi^9 (e^{\alpha+\beta+\gamma} + e^{\alpha+3\beta}) \,. \end{aligned}$$

But $\varphi^9 \leqslant \varphi^6 \leqslant e^{-3\alpha} e^{2(\alpha-\beta)} e^{\beta-\gamma} = e^{-\alpha-\beta-\gamma}$ and $\varphi^9 \leqslant \varphi^7 \leqslant e^{-4\alpha} e^{3(\alpha-\beta)} = e^{-\alpha-3\beta}$. Since $\varepsilon > 0$ was arbitrary, we get $\ll N^{(3/5)+\varepsilon}$ four-tuples (3.11) with (3.13). Thus indeed $Z(\alpha, \beta, \gamma) \ll N^{(3/5)+\varepsilon}$.

**4. Theorem 1 in general.** We may well wonder if this is just an exercise on pathological functions!

We need some facts from calculus. Given $x_0 < x_1$ and given a function $f(x)$ in $x_0 \leqslant x \leqslant x_1$, let $g(x) = ax + b$ be the linear function with $g(x_i) = f(x_i)$ $(i = 0, 1)$. Then

$$a(x_1 - x_0) = f(x_1) - f(x_0) = \int_{x_0}^{x_1} df(x) \,.$$

Next, given $x_0 < x_1 < x_2$, let $\psi(x) = \psi(x_0, x_1, x_2; x)$ be the function in $x_0 \leqslant x \leqslant x_2$ with $\psi(x) = (x - x_0)/(x_1 - x_0)$ in $x_0 \leqslant x \leqslant x_1$, but $\psi(x) = (x_2 - x)/(x_2 - x_1)$ in $x_1 \leqslant x \leqslant x_2$. Given a function $f(x)$ in $x_0 \leqslant x \leqslant x_2$, let $g(x) = ax^2 + bx + c$ be the quadratic polynomial with $g(x_i) = f(x_i)$ $(i = 0, 1, 2)$. Then if $f$ has a derivative $f'$ of bounded variation in $x_0 \leqslant x \leqslant x_2$, we have

$$a(x_2 - x_0) = \int_{x_0}^{x_2} \psi(x)\, df'(x) \,,$$

where the right hand side is a Stieltjes integral. We omit the proof since our real interest lies in formula (4.1) below.

Given $x_0 < x_1 < x_2 < x_3$, we define $\omega(x) = \omega(x_0, x_1, x_2, x_3; x)$ in $x_0 \leqslant x \leqslant x_3$, as follows.

$$\omega(x) = \begin{cases} \dfrac{(x-x_0)^2}{2(x_2-x_0)(x_1-x_0)} \quad \text{in } x_0 \leqslant x_1 \leqslant x_1, \\[2ex] \dfrac{1}{2} - \dfrac{(x-x_1)^2}{2(x_3-x_1)(x_2-x_1)} - \dfrac{(x_2-x)^2}{2(x_2-x_0)(x_2-x_1)} \\ \hfill \text{in } x_1 < x < x_2, \\[2ex] \dfrac{(x_3-x)^2}{2(x_3-x_1)(x_3-x_2)} \quad \text{in } x_2 \leqslant x \leqslant x_3. \end{cases}$$

Then $\omega(x)$ has a continuous derivative, and $\omega$ and its derivative vanish at the end points $x_0, x_3$. It is easily checked that $0 \leqslant \omega(x) < \frac{1}{2}$ and that

$$\int_{x_0}^{x_3} \omega(x)\,dx = \tfrac{1}{6}(x_3 - x_0)\,.$$

**Lemma 2.** *Let $f(x)$ be defined in $x_0 \leqslant x \leqslant x_3$ and have a second derivative $f''$ of finite total variation. Let $g(x) = ax^3 + bx^2 + cx + d$ be such that $g(x_i) = f(x_i)$ $(i = 0, 1, 2, 3)$. Then*

$$a(x_3 - x_0) = \int_{x_0}^{x_3} \omega(x)\,df''(x)\,. \tag{4.1}$$

*Proof.* This is certainly true when $f(x) = g(x)$, because then

$$\int_{x_0}^{x_3} \omega(x)\,df''(x) = \int_{x_0}^{x_3} \omega(x)\,g'''(x)\,dx = 6a\int_{x_0}^{x_3} \omega(x)\,dx = a(x_3 - x_0)\,.$$

Setting $h(x) = f(x) - g(x)$, we see that it will suffice to verify that

$$\int_{x_0}^{x_3} \omega(x)\,dh''(x) = 0$$

for functions $h$ with $h(x_i) = 0$ $(i = 0, 1, 2, 3)$ and with $h''$ of bounded variation. Applying partial integration twice and recalling that $\omega, \omega'$ vanish at the end points, we get

$$\int_{x_0}^{x_3} \omega(x)\,dh''(x) = -\int_{x_0}^{x_3} \omega'(x)\,h''(x)\,dx = \int_{x_0}^{x_3} \omega''(x)\,h'(x)\,dx\,.$$

But since $\omega''$ is constant in each of the subintervals $x_i < x < x_{i+1}$, the last integral is a linear combination of the values $h(x_i)$ $(i = 0, 1, 2, 3)$, hence is zero.

Now in order to prove Theorem 1, we may without loss of generality restrict $x$ to an interval $I$ where $f''$ is weakly monotonic and where $f' > 0, f'' > 0$. We define $I(\alpha)$ and $I(\alpha, \beta)$ as before. We consider the points (3.10) on our curve with $x \in I(\alpha, \beta)$; this time $Z = Z(\alpha, \beta)$. Again we consider the 4-tuples of consecutive points $Q_0, Q_1, Q_2, Q_3$ among (3.10), and we construct triples $(u_1, v_1)$, $(u_2, v_2)$, $(u_3, v_3)$. Again define $\Lambda$ by (2.1), (2.3), and put

$$M = |\Lambda| (u_1 u_2 u_3 (u_1 + u_2)(u_2 + u_3)(u_1 + u_2 + u_3))^{-1} .$$

Now write $\mathfrak{T}(\alpha, \beta, 0)$ for the set of 4-tuples with $M \leqslant N^{-2}$, and $\mathfrak{T}(\alpha, \beta, \gamma)$ where $\gamma > 0$ for the set of four-tuples with

$$e^{\gamma - 1} N^{-2} < M \leqslant e^{\gamma} N^{-2} .$$

Since $M \leqslant \Lambda \ll N^4$, the set $\mathfrak{T}(\alpha, \beta, \gamma)$ is empty unless $\gamma \ll \log N$. It will suffice to show that each $\mathfrak{T}(\alpha, \beta, \gamma)$ has cardinality $\ll N^{(3/5)+\varepsilon}$.

We define $\varphi, \Phi$ by (3.8), (3.9). Four-tuples with (3.13) again satisfy (2.5), (2.6), (2.7) with $A = e^{\alpha}$, $B = \Phi^3 e^{\beta} N^{-1}$, $C = \Phi^6 e^{\gamma} N^{-2}$, and the argument goes through as before. There remain the four-tuples in $\mathfrak{T}(\alpha, \beta, \gamma)$ with (3.12). The cubic polynomial $g(x) = a x^3 + \dots$ with $g(x_i) = f(x_i)$ $(i = 0, 1, 2, 3)$ satisfies (4.1). On the other hand, $a = M$ ([11], formula (10)). Thus for $\gamma > 0$ we have

$$\int_{x_0}^{x_3} \omega(x)\, df''(x) > e^{\gamma - 1} N^{-2} (x_3 - x_0) > e^{\gamma - 1} N^{-2} \Phi .$$

In the last inequality we used that $x_3 - x_0 = u_1 + u_2 + u_3 > \Phi$ by (3.12). Since $0 \leqslant \omega(x) < 1/2$, we may infer that $f''(x_3) - f''(x_0) \gg e^{\gamma} N^{-2} \Phi$. Since $f''$ is monotonic with $|f''(x)| \leqslant e^{\beta} N^{-1}$ in $I(\alpha, \beta)$, the number of 4-tuples in question is $\ll N \Phi^{-1} e^{\beta - \gamma}$.

As in § 3, the number of 4-tuples with (3.12) is bounded by $\ll N \Phi^{-1} e^{-\alpha}$ and by $N \Phi^{-1} e^{\alpha - \beta}$. Hence the cardinality of $\mathfrak{T}(\alpha, \beta, \gamma)$ is $\ll N \Phi^{-1} \varphi = N^{3/5}$. This is true both when $\gamma > 0$ and when $\gamma = 0$.

**5. Proof of Theorem 2.** When $\mathscr{S}$ is an elementary piece, our theorem is essentially Satz 1 of [10]. In the notation of that paper we have $A \leqslant N$, $B \leqslant N$, and Hilfssatz 5 should become $l(\mathfrak{U}_i) \ll N$. We are making slightly weaker hypotheses than in [10] about the partial derivatives on the boundary of $\mathfrak{D}$, but this has little effect on the proof. It may happen that our elementary piece is not itself contained in the cube of side $N$, which might necessitate some further easy modifications of the arguments in [10].

Rotation by $\pi/2$ transforms integer points into integer points. So if $\mathcal{S}(\pi/2)$ is an elementary piece, the same conclusions may be drawn as before. Rotation by $\pi/4$ or $3\pi/4$ transforms the lattice $\mathbb{Z}^2$ of integer points into the union of two translates of $\sqrt{2}\,\mathbb{Z}^2$. It easily follows that the number of integer points in our cube is again $\ll N^{3/2}$ if $\mathcal{S}(\pi/4)$ or $\mathcal{S}(3\pi/4)$ is an elementary piece.

When $\mathcal{S}$ is part of an elliptic or hyperbolic paraboloid, interchange the roles of $x, z$. We obtain a surface which is the union of a bounded number of elementary pieces.

**6. Surfaces with $W = 0$.** Given a curve $z = g(y)$ in the $(y, z)$-plane, it gives rise to surfaces of translation $z = g(y - y_1(x)) + z_1(x)$. The intersection of this surface with the plane $x = c$ is the original curve, translated by $(y_1(c), z_1(c))$. Writing $f(x,y) = g(y - y_1(x)) + z_1(x)$ and assuming suitable differentiability conditions we have $f_y = g'$, $f_{yy} = g''$, $f_{yyy} = g'''$, $f_{yx} = -g''y_1'$, $f_{yyx} = -g'''y_1'$ (with $g'$, $g''$, $g'''$ evaluated at $y - y_1(x)$), whence $W = 0$.

The surfaces $z = a(x)y + b(x)$ whose intersection with any plane $x = c$ is a straight line are in general not surfaces of translation, but $f(x,y) = a(x)y + b(x)$ again has $W = 0$.

Now suppose conversely that $f$ has continuous third order partial derivatives and has $W = 0$ on an open set $\mathfrak{D}$. If $f_{yy} = 0$ on $\mathfrak{D}$ and if, say, $\mathfrak{D}$ is convex, then $f = a(x)y + b(x)$. Suppose then that $f_{yy}$ does not vanish identically on $\mathfrak{D}$, so that in fact $f_{yy} \neq 0$ in some nonempty subset $\mathfrak{D}_1$ of $\mathfrak{D}$. Thus

$$\frac{\partial(x, f_y)}{\partial(x, y)} = f_{yy} \neq 0\,,$$

and the map $(x, y) \mapsto (x, f_y)$ is $1-1$ on a nonempty open subset $\mathfrak{D}_2$ of $\mathfrak{D}_1$. The inverse map has $\partial x/\partial x = 1$, $\partial y/\partial x = -f_{xy}/f_{yy}$, and therefore (as a function of $x, f_y$)

$$\frac{\partial f_{yy}}{\partial x} = f_{yyx} + f_{yyy}(-f_{xy}/f_{yy}) = W/f_{yy} = 0\ .$$

Thus $f_{yy}$ is a function of $f_y$ alone, say

$$f_{yy} = B(f_y)\ . \tag{6.1}$$

Now let $x$ be fixed and set $h = f_y$. Then $dh/dy = f_{yy} = B(h) \neq 0$, hence $dy/dh = B(h)^{-1}$. Thus $y = B_1(h) + y_1$ where $B_1$ is an indefinite integral of $B^{-1}$ and where $y_1$ is a constant. Since $B_1$ is monotonic, we can solve for $h$ to get $f_y = h = B_2(y - y_1)$, where $B_2$ is the inverse function of $B_1$. Finally $f = g(y - y_1) + z_1$ where $g$ is an indefinite integral of $B_2$ and where $z_1$ is another constant. For varying $x$ we have $y_1 = y_1(x)$, $z_1 = z_1(x)$, so that $z = f(x, y)$ is, at least locally, a surface of translation.

**7. Proof of Theorem 3.** Let $J$ be the Jacobian

$$J = \frac{\partial(f_x, f_y)}{\partial(x, y)} = \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix} .$$

We will see that when $J = W = W_{\pi/2} = 0$ on $\mathfrak{D}$, then $z = f(x, y)$ is locally a cylinder. On the other hand when $J$ is not identically 0 on $\mathfrak{D}$ and when $W = W_{\pi/4} = W_{\pi/2} = W_{3\pi/4} = 0$, then $z = f(x, y)$ is locally a paraboloid.

By definition, a Wronskian of functions $p(x, y)$, $q(x, y)$, $r(x, y)$, defined and twice differentiable in an open set, is a function

$$\mathfrak{W} = \mathfrak{W}(x, y) = \begin{vmatrix} D_0 p & D_1 p & D_2 p \\ D_0 q & D_1 q & D_2 q \\ D_0 r & D_1 r & D_2 r \end{vmatrix} ,$$

where $D_i$ is a partial differentiation operator of total order $\leqslant i$. When $p, q, r$ are linearly dependent (over $\mathbb{R}$), then each Wronskian vanishes. Conversely, when $p, q, r$ have continuous second order partial derivatives and when every Wronskian vanishes, then there is a nonempty open set where $p, q, r$ are linearly dependent. (See e. g. [9, Lemma 1], where this is shown for rational functions). Since $D_0$ is the identity operator, we may specify $D_1$, $D_2$ to have positive order. We will apply these facts to $p = f_x$, $q = f_y$, $r = 1$. A typical Wronskian becomes

$$\mathfrak{W}(D_1, D_2) = \begin{vmatrix} D_1 f_x & D_2 f_x \\ D_1 f_y & D_2 f_y \end{vmatrix} = \det(\operatorname{grad} D_1 f, \operatorname{grad} D_2 f) ,$$

where for a function $h$ we set $\operatorname{grad} h = (h_x, h_y)$.

$$\text{Now } J = W = 0 \text{ gives } \mathfrak{W}\left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}\right) = \mathfrak{W}\left(\frac{\partial}{\partial y}, \frac{\partial^2}{\partial y^2}\right) = 0.$$

For points where $\operatorname{grad} f_y \neq \mathbf{0}$, or points which are limits of points with this property, it follows that $\mathfrak{W}\left(\frac{\partial}{\partial x},\frac{\partial^2}{\partial y^2}\right)=0$. But in open sets with $\operatorname{grad} f_y=\mathbf{0}$, we have $f_{yy}=f_{yyy}=0$, hence again $\mathfrak{W}\left(\frac{\partial}{\partial x},\frac{\partial^2}{\partial y^2}\right)=0$. Differentiating the relation $J=0$ with respect to $y$ we obtain $\mathfrak{W}\left(\frac{\partial^2}{\partial x\,\partial y},\frac{\partial}{\partial y}\right)+\mathfrak{W}\left(\frac{\partial}{\partial x},\frac{\partial^2}{\partial y^2}\right)=0$, so that $\mathfrak{W}\left(\frac{\partial^2}{\partial x\,\partial y},\frac{\partial}{\partial y}\right)=0$.

If we make the further assumption that $W_{\pi/2}=0$, we may interchange the roles of $x, y$ and see that every Wronskian vanishes. Thus there is an open subset $\mathfrak{E}$ of $\mathfrak{D}$ where $f_x, f_y, 1$ are linearly dependent. Say $af_x+bf_y+c=0$. When $b=0$, then $f_x=\hat{c}$ (a constant), so that $f=g(y)+\hat{c}x$. Thus the piece of our surface with $(x,y)\in\mathfrak{E}$ belongs to a cylinder. The situation is similar when $a=0$. When $ab\neq 0$, we may write $f(x,y)=h(ax+by,\,bx-ay)$ with a certain function $h=h(u,v)$. Now

$$0=af_x+bf_y+c=a^2h_u+abh_v+b^2h_u-abh_v+c=$$
$$=(a^2+b^2)h_u+c\,.$$

Therefore $h_u=\hat{c}$ (a constant) and $h(u,v)=g(v)+\hat{c}u$, whence $f(x,y)=g(bx-ay)+\hat{c}\cdot(ax+by)$. Thus $z=f(x,y)$ with $(x,y)\in\mathfrak{E}$ is part of a cylinder.

Suppose now that $J$ is not identically zero on $\mathfrak{D}$ and that $W=W_{\pi/4}$ $W_{\pi/2}=W_{3\pi/4}=0$ on $\mathfrak{D}$. In view of $J\not\equiv 0$ there is an open subset of $\mathfrak{E}_1$ of $\mathfrak{D}$ where the map $(x,y)\mapsto(f_x,f_y)$ is $1-1$. The argument given for (6.1) shows that there is a nonempty open subset of $\mathfrak{E}_1$ where $f_{yy}=B(f_y)$. Since also $W_{\pi/2}=W_{\pi/4}=W_{3\pi/4}=0$, we find further that $f_{xx}=A(f_x)$,

$$\begin{aligned} f_{xx}+2f_{xy}+f_{yy}&=C(f_x+f_y)\,,\\ f_{xx}-2f_{xy}+f_{yy}&=D(f_x-f_y)\end{aligned}\tag{7.1}$$

for certain functions $A$, $C$, $D$ and for $(x,y)$ in a certain open subset $\mathfrak{E}_2$ of $\mathfrak{E}_1$. It follows that

$$2A(f_x)+2B(f_y)=C(f_x+f_y)+D(f_x-f_y)\,,$$

so that

$$2A(\xi)+2B(\eta)=C(\xi+\eta)+D(\xi-\eta)\tag{7.2}$$

for $(\xi,\eta)$ in the image $\mathfrak{F}_2$ of $\mathfrak{E}_2$ under $(x,y)\mapsto(f_x,f_y)$. Since $A$, $B$, $C$, $D$ are continuous, it may be deduced from (7.2) that they are quadratic polynomials on every connected part of $\mathfrak{F}_2$. To avoid technicalities, we will suppose here that $f$ has fourth order partial derivatives, so that $A, B, C, D$ are twice differentiable. Taking second order partial derivatives of (7.2) we find that

$$2\,A''(\xi) = C''(\xi + \eta) + D''(\xi - \eta)\,,$$
$$2\,B''(\eta) = C''(\xi + \eta) + D''(\xi - \eta)\,.$$

We infer that $A''(\xi) = B''(\eta)$ for $(\xi, \eta) \in \mathfrak{F}_2$, so that $A''(\xi) = B''(\eta)$ is some constant, call is $2a$. Thus

$$A(\xi) = a\,\xi^2 + 2\,b\,\xi + d, \quad B(\eta) = a\,\eta^2 + 2\,c\,\eta + e\,,$$

say. Substituting this into (7.2) we find that

$$C(\xi + \eta) = a\,(\xi + \eta)^2 + 2\,(b + c)\,(\xi + \eta) + d^*\,,$$
$$D(\xi + \eta) = a\,(\xi - \eta)^2 + 2\,(b - c)\,(\xi - \eta) + e^*\,.$$

From (7.1) we get $4f_{xy} = C(f_x + f_y) - D(f_x - f_y)$. Thus

$$\begin{aligned} f_{xx} &= af_x^2 + 2\,bf_x + d\,,\\ f_{yy} &= af_y^2 + 2\,cf_y + e\,,\\ f_{xy} &= af_xf_y + bf_y + cf_x + (d^* - e^*)/4\,. \end{aligned} \tag{7.3}$$

Suppose at first that $a \neq 0$. Then (7.3) becomes

$$\begin{aligned} f_{xx} &= a(f_x + a_1)^2 + d_1,\\ f_{yy} &= a(f_y + b_1)^2 + e_1,\\ f_{xy} &= a(f_x + a_1)\,(f_y + b_1) + u_1\,, \end{aligned} \tag{7.4}$$

with constants $a_1$, $b_1$, $d_1$, $e_1$, $u_1$. Since $f_{xxy} = f_{xyx}$, we get

$$2\,a\,(f_x + a_1)f_{xy} = a\,(f_x + a_1)f_{xy} + a\,(f_y + b_1)f_{xx},$$
$$(f_x + a_1)f_{xy} = (f_y + b_1)f_{xx}.$$

Substituting from (7.4) and simplifying we obtain

$$(f_x + a_1)\,u_1 = (f_y + b_1)\,d_1\,,$$

whence the identity $(\xi + a_1)\,u_1 = (\eta + b_1)\,d_1$. Therefore $u_1 = d_1 = 0$. Similarly $e_1 = 0$. The formulae (7.4) now yield $J = 0$, contrary to our assumption.

Hence $a = 0$ in (7.3). Noting again that $f_{xxy} = f_{xyx}$, we have $2\,bf_{xy} = bf_{xy} + cf_{xx}$, or $bf_{xy} = cf_{xx}$. Similarly, $f_{yyx} = f_{xyy}$ gives

$cf_{xy} = bf_{yy}$. Since $J \neq 0$ on $\mathfrak{E}_2$, we have $b = c = 0$. It now follows from (7.3) that $f_{xx}, f_{yy}, f_{xy}$ are constants. So for $(x, y) \in \mathfrak{E}_2$ our function $f$ is a quadratic polynomial, and the surface $z = f(x, y)$ with $(x, y) \in \mathfrak{E}_2$ is part of a paraboloid.

**8. Proof of the Corollary.** The constants in this section will depend on $d, n$ only. We begin with the case $n = 3$. The singular points of the surface form an algebraic set of dimension $\leqslant 1$ and of degree $\ll 1$, i. e. defined by equations of degree $\leqslant c(d)$. There are $\ll N$ singular integer points in a cube $\mathfrak{B}(N)$ of side $N \geqslant 1$. The nonsingular points can be covered by a bounded number of pieces, where each piece, possibly after permutation of the variables, is of the form $z = f(x, y)$ with $f$ analytic in some open set $\mathfrak{D} \subseteq \mathbb{R}^2$.

Now when $W = W_{\pi/4} = W_{\pi/2} = W_{3\pi/4} = 0$ on $\mathfrak{D}$, then by Theorem 3, the part of the surface $z = f(x, y)$ with $(x, y)$ in a certain nonempty open subset of $\mathfrak{D}$ belongs to a paraboloid or a cylinder. Since our surface is an irreducible algebraic surface, it is then itself a paraboloid or a cylinder. When it is a paraboloid, the number of its integer points lying in $\mathfrak{B}(N)$ is $\ll N^{3/2}$ by Theorem 2. Cylinders are ruled out by our hypothesis.

Suppose, then, that $W \not\equiv 0$ on $\mathfrak{D}$. (The cases when one of $W_{\pi/4}$, $W_{\pi/2}$, $W_{3\pi/4}$ is not zero on $\mathfrak{D}$ can easily be reduced to this.) Then also $f_{yy} \not\equiv 0$ on $\mathfrak{D}$. Since $W$ and $f_{yy}$ are algebraic functions of bounded degrees, there is a bounded number of open sets $\mathfrak{D}_1, \ldots, \mathfrak{D}_l$ such that $W$ and $f_{yy}$ have no zeros in any of them, and $\bar{\mathfrak{D}} = \bar{\mathfrak{D}}_1 \cup \ldots \cup \bar{\mathfrak{D}}_l$. Each $\mathfrak{D}$ may be chosen to have as its boundary parts of algebraic curves of degree $\ll 1$, and the same is now true of each $\mathfrak{D}_i$. Points in $\mathfrak{D}$ which do not belong to any $\mathfrak{D}_i$ are part of a bounded number of algebraic curves of bounded degrees, and these give rise to $\ll N$ integer points in $\mathfrak{B}(N)$, hence may be ignored. We shall say that $\mathfrak{D}$ is "essentially" the union of $\mathfrak{D}_1, \ldots, \mathfrak{D}_l$. In the same way, since their boundaries belong to algebraic curves of bounded degrees, each $\mathfrak{D}_i \cap \mathfrak{B}(N)$ is essentially the union of a bounded number of proper domains $\mathfrak{D}_{ij}$. If a typical domain $\mathfrak{D}_{ij}$, call it $\mathfrak{E}$ for brevity, is given by $a < x < b$, $\psi_1(x) < y < \psi_2(x)$, let $\mathfrak{E}^*$ be the subdomain $a^* < x < b^*$, $\psi_1^*(x) < y < y_2^*(x)$ with $a^* = a + (b - a)N^{-1}, b^* = b - (b - a)N^{-1}$, $\psi_1^* = \psi_1 + (\psi_2 - \psi_1)N^{-1}$, $\psi_2^* = \psi_2 - (\psi_2 - \psi_1)N^{-1}$. The number of integer points with $(x, y)$ in $\mathfrak{E}$ but not in $\mathfrak{E}^*$ is $\ll N$ and may be ignored. $f$ is analytic in $\mathfrak{E}^*$ and on its boundary. The functions $g_i = f_y(x, \psi_i^*(x))$ $(i = 1, 2)$ are algebraic of degree $\ll 1$ in $a^* \leqslant x \leqslant b^*$. This interval may be broken into a bounded number of subintervals, where $g_1, g_2$ are weakly monotonic. Thus $\mathfrak{E}^*$ is essentially the union of $\ll 1$ domains $\mathfrak{E}_k^*$ such that $f_y$ is monotonic on the "upper" and "lower" boundaries of $\mathfrak{E}_k^*$.

The surface $z = f(x, y)$ with $(x, y) \in \mathfrak{E}_k^*$ is an elementary piece. By Theorem 2 this surface contributes $\ll N^{3/2}$ integer points.

We now turn to the case $n > 3$. Reasoning as for $n = 3$, we may concentrate on a piece of the algebraic surface of the type $x_n = = f(x_1, \ldots, x_{n-1})$ where $f$ is defined and analytic in some open set $\mathfrak{D} \subseteq \mathbb{R}^{n-1}$. Write $(x_1, \ldots, x_{n-1}) = (x, y, \mathbf{x}') = \mathbf{x}$ with $\mathbf{x}' \in \mathbb{R}^{n-3}$ and $\mathbf{x} \in \mathbb{R}^{n-1}$.

Suppose at first that *not* all the Wronskians of $1, f_x, f_y$ vanish identically. Here by Wronskian I mean a *special* Wronskian which is a determinant with rows $(D_i 1, D_i f_x, D_i f_y)$ $(i = 0, 1, 2)$ where $D_i$ is a partial differentiation operator of order $\leqslant i$ involving *only the variables* $x, y$. So the points $\mathbf{x}$ where all these special Wronskians vanish lie in an algebraic set $\mathfrak{A} \subseteq \mathbb{R}^{n-1}$ of dimension $\leqslant n-2$ and of degree $\ll 1$. These points contribute $\ll N^{n-2}$ to $Z(N)$. Hence it will suffice to consider $\mathbf{x}'$ for which the special Wronskians do not vanish identically in $x, y$. For such $\mathbf{x}'$, let $\mathcal{S}(\mathbf{x}')$ be the surface in $\mathbb{R}^3$ consisting of $(x, y, z)$ where $z = f(x, y, \mathbf{x}')$ with $(x, y, \mathbf{x}') \in \mathfrak{D}$. This surface is part of an algebraic surface which is not a cylinder. By the case $n = 3$ it contains $\ll N^{3/2}$ integer points with $|x|, |y|, |z| < N$. Taking the sum over $\mathbf{x}'$ we obtain a total of $\ll N^{n-3} N^{3/2} = N^{n-(3/2)}$ integer points.

We may thus suppose that all the special Wronskians of $1, f_x, f_y$ vanish identically. Thus for given $\mathbf{x}'$, there is a relation of linear dependency

$$a + b f_x + c f_y = 0 \tag{8.1}$$

where $a, b, c$ depend on $\mathbf{x}'$ only and are not all zero. Since a map $(x, y, x_3, \ldots, x_i, \ldots, x_{n-1}) \mapsto (x, y, x_3, \ldots, x_i + y, \ldots, x_{n-1})$ gives a $1-1$ correspondence of integer points, we may further suppose that we still have this property for the functions $f(x, y, x_3, \ldots, x_i + y, \ldots, x_{n-1})$, and still on top of that after a permutation of the variables. We will show that in this case our surface is a cylinder as defined in the Corollary.

It will suffice to verify that at most two of the functions $1, f_{x_1}, \ldots, f_{x_{n-1}}$ are linearly independent over $\mathbb{R}$. We endeavour to show that $1, f_x, f_y$ are linearly dependent, where $x, y$ stand for any of the variables $x_1, \ldots, x_{n-1}$. More precisely, we wish to establish a relation

$$A + Bf_x + Cf_y = 0$$

where, in contrast to (8.1), the coefficients $A, B, C$ should be independent of $\mathbf{x} = (x, y, \mathbf{x}')$. For this it will be enough to see that the *general* Wronskians of $1, f_x, f_y$ vanish, where a general Wronskian is a determinant

$$\begin{vmatrix} D_0 1 & D_1 1 & D_2 1 \\ D_0 f_x & D_1 f_x & D_2 f_x \\ D_0 f_y & D_1 f_y & D_2 f_y \end{vmatrix} = \begin{vmatrix} D_1 f_x & D_2 f_x \\ D_1 f_y & D_2 f_y \end{vmatrix}$$

where $D_0 = I$, $D_1 \neq I$, $D_2 \neq I$ and where $D_1, D_2$ are partial differentiation operators involving *any* of the variables $x_1, \ldots, x_{n-1}$.

When $D_1, D_2$ are both of order 1, such a Wronskian is of the type

$$\begin{vmatrix} f_{xu} & f_{xv} \\ f_{yu} & f_{yv} \end{vmatrix} \tag{8.2}$$

where $u, v$ are among $x_1, \ldots, x_{n-1}$. We know from the vanishing of the special Wronskians that

$$\begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix} = 0\ ,$$

where $x, y$ stand for any of $x_1, \ldots, x_{n-1}$. It follows that when $f_{xx} = 0$, then $f_{xy} = 0$ where $y$ is any of $x_1, \ldots, x_{n-1}$. Replacing $f$ by $f(x, y, x_3, \ldots, v + y, \ldots, x_{n-1})$ where $v = x_i$ we find that

$$\begin{vmatrix} f_{xx} & f_{xy} + f_{xv} \\ f_{xy} + f_{xv} & f_{yy} + 2f_{yv} + f_{vv} \end{vmatrix} =$$

$$= \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{vmatrix} + \begin{vmatrix} f_{xx} & f_{xv} \\ f_{vx} & f_{vv} \end{vmatrix} + 2\begin{vmatrix} f_{xx} & f_{xv} \\ f_{xy} & f_{yv} \end{vmatrix} = 0\ ,$$

so that $\begin{vmatrix} f_{xx} & f_{xv} \\ f_{xy} & f_{yv} \end{vmatrix} = 0.$

A similar relation holds with $u$ in place of $v$. Therefore when $f_{xx} \neq 0$ we see that (8.2) vanishes. But when $f_{xx} = 0$, then $f_{xu} = f_{xv} = 0$, and again (8.2) vanishes.

When $D_1, D_2$ are of respective orders 1, 2, the Wronskian is of the type

$$\begin{vmatrix} f_{xu} & f_{xvw} \\ f_{yu} & f_{yvw} \end{vmatrix} \tag{8.3}$$

where $u, v, w$ are among $x_1, \ldots, x_{n-1}$. We know from the vanishing of the special Wronskians that (8.3) is zero when $u, v, w$ belong to the set $\{x, y\}$. We may therefore suppose that the set

$$S = \{x, y, u, v, w\} \tag{8.4}$$

contains at least three distinct variables. We may further suppose that none of $f_{xx}, \ldots, f_{ww}$ is identically zero, for if, say, $f_{ww} = 0$, then also $f_{vw} = 0$ and (8.3) vanishes. Taking partial derivatives in (8.1) we get

$$bf_{xx} + cf_{xy} = 0, \quad bf_{xy} + cf_{yy} = 0 .$$

Thus neither $b$ nor $c$ is identically zero. The function $f_{xy}/f_{xx} = f_{yy}/f_{xy} = -b/c$ does not depend on $x, y$. Now if $z$ is a variable in $S$ distinct from $x, y$, we see that $f_{yz}/f_{yy} = f_{zz}/f_{yz}$ does not depend on $y, z$, and $f_{zx}/f_{zz} = f_{xx}/f_{zx}$ does not depend on $x, z$. We observe that

$$(f_{xy}/f_{xx})^2 (f_{yz}/f_{yy})^2 (f_{zx}/f_{zz})^2 = (f_{yy}/f_{xx}) (f_{zz}/f_{yy}) (f_{xx}/f_{zz}) = 1 ,$$

and the three factors depend, respectively, on $z, x, y$, and on variables other than $x, y, z$. It follows that actually $f_{xy}/f_{yy}$ does not depend on $x, y$ or $z$. Clearly $f_{xy}/f_{yy}$ does not depend on any variables belonging to $S$. So the quotients $f_{ab}/f_{cd}$ with $a, b, c, d$ in $S$ are independent of the variables of $S$. It follows that $f_{ab} = g^{(a,b)} h$, where $g^{(a,b)}, h$ are functions such that $g^{(a,b)}$ is independent of the variables of $S$. By the vanishing of (8.2),

$$\begin{vmatrix} g^{(x,u)} & g^{(x,v)} \\ g^{(y,u)} & g^{(y,v)} \end{vmatrix} = 0 .$$

We obtain

$$\begin{vmatrix} f_{xu} & f_{xvw} \\ f_{yu} & f_{yvw} \end{vmatrix} = \begin{vmatrix} g^{(x,u)} h & g^{(x,v)} h_w \\ g^{(y,u)} h & g^{(y,v)} h_w \end{vmatrix} = 0 .$$

**9. Proof of Theorem 4.** Whereas (1.7) does not imply (1.8), it turns out that (1.9) does imply (1.10). For by a theorem of Jordan, there is an ellipsoid $\mathfrak{E}$ with $\mathfrak{K} \subseteq \mathfrak{E}$ and $V(\mathfrak{E}) \ll V(\mathfrak{K})$. Let $\tau$ be a linear map of determinant 1 such that $\tau\mathfrak{E}$ is a ball. We have

$$S(\tau\mathfrak{K}) \subseteq S(\tau\mathfrak{E}) \ll V(\tau\mathfrak{E})^{(n-1)/n} \ll V(\tau\mathfrak{K})^{(n-1)/n} .$$

The validity of (1.9) for $\tau\mathfrak{K}$ and $\tau\Lambda$ implies the validity of (1.10) for $\tau\mathfrak{K}$ and $\tau\Lambda$, hence the validity of (1.10) for $\mathfrak{K}$ and $\Lambda$. Thus it will suffice to prove (1.9).

Let $\mathfrak{P}$ be the convex cover of $\mathfrak{Z} \cap \Lambda$. Then $\mathfrak{P}$ is a convex polytope contained in $\mathfrak{K}$. The vertices of $\mathfrak{P}$ are precisely the elements of $\mathfrak{Z} \cap \Lambda$, so that $\mathfrak{P}$ has $Z$ vertices. Since $S(\mathfrak{P}) \leqslant S$, it will suffice to prove (1.9) for polytopes. But at first we will prove that

$$F \ll S^{n/(n+1)} \Delta^{-(n-1)/(n+1)}, \tag{9.1}$$

where $F$ is the number of ($(n-1)$-dimensional) faces of $\mathfrak{P}$.

We may suppose without loss of generality that $\Delta = 1$. Let $\lambda_1 \leqslant \ldots \leqslant \lambda_n$ be the successive minima of $\Lambda$ (with respect to the unit ball), so that according to Minkowski, $1 \ll \lambda_1 \ldots \lambda_n \ll 1$. Let $\mathbf{a}_1, \ldots, \mathbf{a}_n$ be a basis of $\Lambda$ with Euclidean norm $|\mathbf{a}_i| \ll \lambda_i$ $(i = 1, \ldots, n)$. When $n = 2$ and $\mathbf{x} = (x_1, x_2)$, put $\mathbf{x}^* = (x_2, -x_1)$; in particular this defines $\mathbf{a}_1^*, \mathbf{a}_2^*$. When $n > 2$, define $\mathbf{a}_1^*, \ldots, \mathbf{a}_n^*$ by

$$\mathbf{a}_i^* = \mathbf{a}_1 \wedge \ldots \wedge \mathbf{a}_{n-i} \wedge \mathbf{a}_{n-i+2} \wedge \ldots \wedge \mathbf{a}_n,$$

i. e. as an exterior product. Then $\mathbf{a}_1^*, \ldots, \mathbf{a}_n^*$ are linearly independent and (since $\Delta = 1$) they generate the polar lattice $\Lambda^*$. When $\lambda_1^*, \ldots, \lambda_n^*$ are the successive minima of $\Lambda^*$, then according to Mahler (see e. g. [3, § VIII.5]), $1 \ll \lambda_i^* \lambda_{n-i+1} \ll 1$ $(i = 1, \ldots, n)$ and $\lambda_i^* \ll |\mathbf{a}_i^*| \ll \lambda_i^*$. Write $H$ for the hyperplane spanned by $\mathbf{a}_1^*, \ldots, \mathbf{a}_{n-1}^*$. It consists of points $\mathbf{x}$ with inner product $\mathbf{x}\mathbf{a}_1 = 0$.

**Lemma 3.** *The number $z(r)$ of lattice points $\mathbf{x}$ of $\Lambda^*$ with $|\mathbf{x}| \leqslant r$ which do not lie in $H$ satisfies*

$$z(r) \ll r^n .$$

*Proof.* In $H$ there are the $n-1$ linearly independent lattice points $\mathbf{a}_1^*, \ldots, \mathbf{a}_{n-1}^*$ with $|\mathbf{a}_i^*| \ll \lambda_i^*$ $(i = 1, \ldots, n-1)$. Hence every lattice point $\mathbf{x}$ not in $H$ has $|\mathbf{x}| \gg \lambda_n^*$. Therefore $z(r) = 0$ unless $r \gg \lambda_n^*$. In this case, when $1 \leqslant j \leqslant n$ and $\lambda_j^* \leqslant r < \lambda_{j+1}^*$, then $z(r) \ll r^j/(\lambda_1^* \ldots \lambda_j^*)$ (see [5, Lemma 1]), and thus $z(r) \ll r^n/(\lambda_1^* \ldots \lambda_n^*) \ll r^n$.

Given a face $\mathfrak{F}$ of $\mathfrak{P}$, let $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ be vertices of $\mathfrak{F}$ (hence of $\mathfrak{P}$) which do not lie in a linear manifold of dimension less than $n-1$. Then $\mathfrak{F}$ contains the simplex with vertices $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$. Therefore $\mathfrak{F}$ has ($(n-1)$-dimensional) volume $S(\mathfrak{F}) \geqslant S(\mathfrak{S})$, where $\mathfrak{S}$ is the simplex with vertices $\mathbf{0}, \mathbf{x}_1 = \mathbf{v}_1 - \mathbf{v}_0, \ldots, \mathbf{x}_{n-1} = \mathbf{v}_{n-1} - \mathbf{v}_0$. Set $\mathbf{y} = \mathbf{x}_1^*$ when $n = 2$ and $\mathbf{y} = \mathbf{x}_1 \wedge \ldots \wedge \mathbf{x}_{n-1}$ when $n > 2$. Then $S(\mathfrak{S}) =$

$= ((n-1)!)^{-1}|\mathbf{y}|$. Since the $\mathbf{x}_i$ lie in $\Lambda$, the vector $\mathbf{y} = \mathbf{y}(\mathfrak{F})$ lies in $\Lambda^*$. It is perpendicular to the face $\mathfrak{F}$. Not more than two faces of $\mathfrak{P}$ can be parallel to each other, so that at most two faces can lead to the same vector $\mathbf{y}$. In fact, when $\mathbf{v}_0, \ldots, \mathbf{v}_{n-1}$ are ordered properly, different faces $\mathfrak{F}$ will give rise to different vectors $\mathbf{y}(\mathfrak{F})$.

Write $F = A + B$, and let $\mathfrak{F}_1, \ldots, \mathfrak{F}_A$ be the faces of $\mathfrak{P}$ which are not parallel to $\mathbf{a}_1$, but $\mathfrak{G}_1, \ldots, \mathfrak{G}_B$ the faces which are parallel to $\mathbf{a}_1$. Writing $\mathbf{y}_i = \mathbf{y}(\mathfrak{F}_i)$ $(i = 1, \ldots, A)$ we have $\mathbf{y}_i \mathbf{a}_1 \neq 0$, so that $\mathbf{y}_i$ does not lie in $H$. If we order in such a way that $|\mathbf{y}_1| \leqslant \ldots \leqslant |\mathbf{y}_A|$, then $|\mathbf{y}_i| \gg i^{1/n}$ by the Lemma. Thus

$$|\mathbf{y}_1| + \ldots + |\mathbf{y}_A| \gg A^{(n+1)/n} .$$

On the other hand,

$$|\mathbf{y}_1| + \ldots + |\mathbf{y}_A| \ll S(\mathfrak{F}_1) + \ldots + S(\mathfrak{F}_A) \leqslant S ,$$

whence $A \ll S^{n/(n+1)}$.

Let $\Pi$ be the orthogonal projection map into $H$. Then $\Pi\mathfrak{P} = \mathfrak{P}'$ is a polytope in $(n-1)$-dimensional space with $(n-1)$-dimensional volume $V(\mathfrak{P}') < S(\mathfrak{P})$. Each face $\mathfrak{G}_i$ (of $\mathfrak{P}$) projects down to a $((n-2)$-dimensional) face $\mathfrak{G}_i' = \Pi\mathfrak{G}_i$ of $\mathfrak{P}'$. The face $\mathfrak{G}_i'$ is perpendicular to the vector $\mathbf{y}(\mathfrak{G}_i)$ which also lies in $H$. Since the vectors $\mathbf{y}(\mathfrak{G}_i)$ have different directions, the faces $\mathfrak{G}_1', \ldots, \mathfrak{G}_B'$ are distinct. Therefore $\mathfrak{P}'$ has at least $B$ faces.

Let $\Lambda' = \Pi\Lambda$ be the projection of $\Lambda$ on $H$. It is a lattice of determinant $\Delta' = \Delta/|\mathbf{a}_1| = 1/|\mathbf{a}_1| \gg 1$. The vertices of $\mathfrak{P}'$ belong to $\Lambda'$. When $n = 2$, so that $\mathfrak{P}'$ is a line segment, we have $B \leqslant 2$ and $S(\mathfrak{P}) > V(\mathfrak{P}') \geqslant \Delta' \gg 1$, whence $B \ll S^{n/(n+1)}$. When $n > 2$, we invoke the case $n-1$ of (1.10), which follows from the case $n-1$ of (1.9), to get $B \ll V(\mathfrak{P}')^{(n-2)/n} \ll S^{(n-2)/n}$. So when $B \neq 0$, then $S \gg 1$ and $B \ll S^{n/(n+1)}$. This, together with the bound for $A$ already given, establishes (9.1). It remains for us to deduce (1.9) from (9.1).

**10. Faces of arbitrary dimension.** Andrews accomplished this deduction with the following trick. Given an edge of $\mathfrak{P}$ with end points $\mathbf{u}, \mathbf{v}$ (which are then vertices of $\mathfrak{P}$), put $\mathbf{z}_1 = \frac{1}{3}(2\mathbf{u}+\mathbf{v})$, $\mathbf{z}_2 = \frac{1}{3}(\mathbf{u}+2\mathbf{v})$. Let $\mathfrak{P}'$ be the convex cover of all these points $\mathbf{z}$. Then the vertices of $\mathfrak{P}'$ are among these points $\mathbf{z}$, which clearly lie in $\Lambda' = \frac{1}{3}\Lambda$. Furthermore, it may be seen that the number of faces $F(\mathfrak{P}')$ cannot be less than $Z = Z(\mathfrak{P})$. Hence

$$Z \leqslant F(\mathfrak{P}') \ll S^{n/(n+1)}(3^{-n}\Delta)^{-(n-1)/(n+1)},$$

whence (1.9).

In fact we will prove rather more. For $0 \leqslant d \leqslant n-1$, let $F_d$ be the number of $d$-dimensional faces of $\mathfrak{P}$. Then we will prove that

$$F_d \ll S^{n/(n+1)}\Delta^{-(n-1)/(n+1)}. \tag{10.1}$$

In other words, we will prove the following

**Theorem 6.** *Let $\mathfrak{P}$ be a convex polytope in $\mathbb{R}^n$ of positive volume and of surface area $S$, whose vertices belong to a lattice $\Lambda$ of determinant $\Delta$. Then* (10.1) *holds for* $d = 0, 1, \ldots, n-1$.

When $n = 3$, then $F_d \ll F = F_2$ ($d = 0, 1, 2$) for arbitrary polytopes ([6, § 10.3]), but already for $n = 4$ we have in general neither $F_2 \ll F = F_3$ nor $F_1 \ll F$ ([6, § 10.4]). Hence for polytopes in general, (9.1) does not yield (10.1).

We will say that a set $\mathfrak{S}$ of points *spans* a linear manifold $\mathfrak{M}$ if $\mathfrak{M}$ is the smallest linear manifold containing $\mathfrak{S}$. We will say that points $\mathbf{z}_1, \ldots, \mathbf{z}_m$ have affine dimension $d$ if the linear manifold spanned by them has dimension $d$; this happens when the vector space spanned by the differences $\mathbf{z}_i - \mathbf{z}_j$ has dimension $d$.

**Lemma 4.** *Suppose that $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_d$ as well as $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_d$ have affine dimension $d$, but $\mathbf{x}_0, \ldots, \mathbf{x}_d, \mathbf{y}_0, \ldots, \mathbf{y}_d$ have affine dimension $> d$. Put*

$$\hat{\mathbf{x}} = (d+1)^{-1}(\mathbf{x}_0 + \ldots + \mathbf{x}_d), \quad \hat{\mathbf{y}} = (d+1)^{-1}(\mathbf{y}_0 + \ldots + \mathbf{y}_d)$$

*and suppose that $\hat{\mathbf{x}}, \hat{\mathbf{y}}$ lie in the interior of a half space $H$. Then there are elements $\mathbf{v}_0, \ldots, \mathbf{v}_d, \mathbf{v}_{d+1}$ among $\mathbf{x}_0, \ldots, \mathbf{y}_d$ which are of affine dimension $d+1$, and there is a point $\mathbf{z}$ in the interior of $H$, of the type*

$$\mathbf{z} = q^{-1}(a_0\mathbf{v}_0 + \ldots + a_{d+1}\mathbf{v}_{d+1}) \text{ with } q = (d+1)^2 \tag{10.2}$$

*and with natural $a_0, \ldots, a_{d+1}$ having*

$$a_0 + a_1 + \ldots + a_{d+1} = q. \tag{10.3}$$

*Proof.* The hypothesis as well as the conclusion is invariant under translations. Hence we may suppose that the origin lies on the boundary of $H$, so that $H$ may be defined by $L(\mathbf{x}) > 0$ with a linear form $L$. Let $\mathbf{v}_0$ be one among $\mathbf{x}_0, \ldots, \mathbf{x}_d, \mathbf{y}_0, \ldots, \mathbf{y}_d$ for which the value of

$L$ is largest. Since $L(\mathbf{x}_0 + \ldots + \mathbf{x}_d) > 0$, we have $dL(\mathbf{v}_0) + L(\mathbf{x}_i) > 0$, and similarly $dL(\mathbf{v}_0) + L(\mathbf{y}_i) > 0$ $(i = 0, \ldots, d)$. Choose $\mathbf{v}_1, \ldots, \mathbf{v}_{d+1}$ among $\mathbf{x}_0, \ldots, \mathbf{y}_d$ such that $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{d+1}$ have affine dimension $d+1$. Define $\mathbf{z}$ by (10.2) with $a_0 = d(d+1)$, $a_1 = \ldots = a_{d+1} = 1$. Then

$$qL(\mathbf{z}) = d(d+1)L(\mathbf{z}_0) + L(\mathbf{z}_1) + \ldots + L(\mathbf{z}_{d+1}) = \sum_{i=1}^{d+1} (dL(\mathbf{z}_0) + L(\mathbf{z}_i)) > 0 ,$$

so that $\mathbf{z}$ lies in $H$.

Now let $\mathfrak{P}$ be the polytope of Theorem 6. Let $\mathbf{v}_0, \ldots, \mathbf{v}_{d+1}$ be any vertices which together have affine dimension $d+1$. Let $\mathbf{z}$ be any point of the type (10.2), (10.3). We define $\mathfrak{P}'$ as the convex cover of all these points $\mathbf{z}$ over all possible $(d+2)$-tuples $\mathbf{v}_0, \ldots, \mathbf{v}_{d+1}$. Then $\mathfrak{P}'$ is a convex polytope whose vertices are among the points $\mathbf{z}$, and hence they belong to $q^{-1}\Lambda$. Given $\mathbf{v}_0, \ldots, \mathbf{v}_{d+1}$, the points $\mathbf{z}$ with (10.2), (10.3) span the linear manifold containing $\mathbf{v}_0, \ldots, \mathbf{v}_{d+1}$. It follows that $\mathfrak{P}'$ "spans" $\mathbb{R}^n$ and therefore has positive volume. We leave it as an exercise to show that every $d$-dimensional face $\mathfrak{G}_d$ of $\mathfrak{P}$ lies in the complement of $\mathfrak{P}'$. Since $\mathfrak{P}' \subseteq \mathfrak{P}$ we have $S(\mathfrak{P}') \leqslant S$. We know from (9.1) that

$$F(\mathfrak{P}') \ll S(\mathfrak{P}')^{n/(n+1)}(q^{-1}\Delta)^{-(n-1)/(n+1)} \ll S^{n/(n+1)}\Delta^{-(n-1)/(n+1)} .$$

It will therefore be enough to show that

$$F_d(\mathfrak{P}) \leqslant F(\mathfrak{P}') . \tag{10.4}$$

Let $\mathbf{p}$ be a fixed point in the interior of $\mathfrak{P}'$. On every $d$-dimensional face $\mathfrak{G}$ of $\mathfrak{P}$ choose $d+1$ vertices $\mathbf{x}_0, \ldots, \mathbf{x}_d$ of dimension $d$ and let $\hat{\mathbf{x}} = (d+1)^{-1}(\mathbf{x}_0 + \ldots + \mathbf{x}_d)$ be the center of the simplex associated with them. By what we said above, $\hat{\mathbf{x}}$ lies outside $\mathfrak{P}'$. The line segment from $\mathbf{p}$ to $\hat{\mathbf{x}}$ will intersect the boundary of $\mathfrak{P}'$ in some point $\mathbf{x}$. There is at least one $(n-1)$-dimensional face $\mathfrak{F}'$ of $\mathfrak{P}'$ containing $\mathbf{x}$. Make some choice and write $\mathfrak{F}' = \mathfrak{F}'(\mathfrak{G})$. Now (10.4) will follow once we can show that the map $\mathfrak{G} \mapsto \mathfrak{F}'(\mathfrak{G})$ is $1-1$. Suppose to the contrary that $\mathfrak{F}'(\mathfrak{G}_1) = \mathfrak{F}'(\mathfrak{G}_2) = \mathfrak{F}'$, say. This face $\mathfrak{F}'$ determines a hyperplane and two open half spaces $H_1, H_2$. The polytope $\mathfrak{P}'$ lies in and on the boundary of one of them, say $H_1$, and is disjoint from $H_2$. Let $\mathbf{x}_0, \ldots, \mathbf{x}_d$ belong to $\mathfrak{G}_1$ and $\mathbf{y}_0, \ldots, \mathbf{y}_d$ to $\mathfrak{G}_2$ and define $\hat{\mathbf{x}}, \hat{\mathbf{y}}$ in the obvious way. Both $\hat{\mathbf{x}}, \hat{\mathbf{y}}$ lie in $H_2$. By Lemma 4 there are vertices $\mathbf{v}_0, \ldots, \mathbf{v}_{d+1}$ of affine dimension $d+1$, and there is a point $\mathbf{z}$ of the type (10.2), (10.3) in $H_2$. By construction, $\mathbf{z}$ belongs to $\mathfrak{P}'$, so that $\mathfrak{P}'$ has points in common with $H_2$, contradicting what we said a few lines above.

## 11. Proof of Theorem 5.

**Lemma 5.** *Suppose $g(\mathbf{u}) = g(u_1, \ldots, u_r)$ is analytic*[3] *in the ball $|\mathbf{u}| \leqslant R$ where $|\mathbf{u}|$ is the Euclidean norm and where $R > 1$. Suppose that $|g(\mathbf{u})| < A R$ throughout, with fixed $A > 1$, and that*

$$g\left(\tfrac{1}{2}(\mathbf{u}_1 + \mathbf{u}_2)\right) < \tfrac{1}{2}\left(g(\mathbf{u}_1) + g(\mathbf{u}_2)\right) \tag{11.1}$$

*for $\mathbf{u}_1 \neq \mathbf{u}_2$. Given a lattice $\Lambda \subset \mathbb{R}^{r+1}$ of determinant 1, the number of lattice points $(u_1, \ldots, u_r, z) = (\mathbf{u}, z)$ on the surface $z = g(\mathbf{u})$ with $|\mathbf{u}| \leqslant R$ is*

$$\ll_r A R^{r-1+(2/(r+2))}.$$

*Proof.* Let $\mathfrak{K}$ be the convex cover of the surface $z = g(\mathbf{u})$ with $|\mathbf{u}| \leqslant R$. Then $\mathfrak{K}$ is compact and is easily seen by (11.1) to have positive volume $V$. Since $V \ll A R^{r+1}$, Theorem 4 yields

$$Z \ll A^{r/(r+2)} R^{r-1+(2/(r+2))}.$$

It therefore will suffice to check that every point $(\mathbf{u}_0, z_0)$ on the given surface is an extremal point of $\mathfrak{K}$. But if the tangent hyperplane at $(\mathbf{u}_0, z_0)$ has the equation $z = M(\mathbf{u})$, then it is a consequence of (11.1) that $f(\mathbf{u}) > M(\mathbf{u})$ for $\mathbf{u} \neq \mathbf{u}_0$. Hence the surface, and therefore $\mathfrak{K}$, with the exception of $(\mathbf{u}_0, z_0)$ itself, lies all on one side of the hyperplane. Thus $(\mathbf{u}_0, z_0)$ is indeed an extremal point.

A quadratic polynomial is a function $q(\mathbf{u}) = a + L(\mathbf{u}) + Q(\mathbf{u})$ where $a$ is constant, $L$ is a linear form, $Q$ is a quadratic form. Such a polynomial is "positive definite" if $Q$ is. In that case

$$\begin{aligned} &\tfrac{1}{2}\left(q(\mathbf{u}_1) + q(\mathbf{u}_2)\right) - q\left(\tfrac{1}{2}(\mathbf{u}_1 + \mathbf{u}_2)\right) = \\ &= Q\left(\tfrac{1}{2}(\mathbf{u}_1 - \mathbf{u}_2)\right) \geqslant c\,|\mathbf{u}_1 - \mathbf{u}_2|^2 \end{aligned} \tag{11.2}$$

with positive $c$, and hence $q$ satisfies (11.1).

Now let $\mathscr{S}$ be a surface in $\mathbb{R}^n$ given by $z = h(\mathbf{x})$ where $\mathbf{x} = (x_1, \ldots, x_{n-1})$ runs through some domain $\mathfrak{D} \subset \mathbb{R}^{n-1}$. Given a subset $\mathfrak{O} \subseteq \mathfrak{D}$, let $\mathscr{S}(\mathfrak{O})$ be the "subsurface" $z = h(\mathbf{x})$ with $\mathbf{x} \in \mathfrak{O}$. Write $Z_N(h, \mathfrak{O})$ for the number of integer points on the blown up surface $N\mathscr{S}(\mathfrak{O})$, i.e. the surface $z = N h(N^{-1}\mathbf{x})$ with $\mathbf{x} \in N\mathfrak{O}$.

---

[3] By this we mean that $g(\mathbf{u})$ is expandable into a power series in a suitable neighborhood of every point of its domain.

**Lemma 6.** *Suppose* $n = r + s + 1$ *where* $r > 0$, *and write* $h(\mathbf{x}) = h(\mathbf{u}, \mathbf{v})$ *with* $\mathbf{x} = (\mathbf{u}, \mathbf{v}) = (u_1, \ldots, u_r, v_1, \ldots, v_s)$. *Suppose h is analytic at the origin with an expansion*

$$h(\mathbf{u}, \mathbf{v}) = q(\mathbf{u}) + h_1(\mathbf{u}, \mathbf{v}) \tag{11.3}$$

*where q is a positive definite quadratic polynomial in* $\mathbf{u}$, *and where* $h_1$ *consists of terms which are at least of degree* 3 *or which involve* $\mathbf{v}$. *Then there is a neighborhood* $\mathfrak{D}$ *of the origin such that*

$$Z_N(h, \mathfrak{D}) \leqslant c_{13}(h, \mathfrak{D})\, N^{n-2+(2/(r+2))}\,. \tag{11.4}$$

*Proof.* The power series

$$\tfrac{1}{2}(h_1(\mathbf{u}_1, \mathbf{v}) + h_1(\mathbf{u}_2, \mathbf{v})) - h_1(\tfrac{1}{2}(\mathbf{u}_1 + \mathbf{u}_2), \mathbf{v}) \tag{11.5}$$

lies in the ideal generated by $g_{ij} = (u_{1i} - u_{2i})(u_{1j} - u_{2j})$ $(1 \leqslant i, j \leqslant r)$, in fact in the ideal generated by

$$g_{ij}u_{1k},\ g_{ij}u_{2k},\ g_{ij}v_l \quad (1 \leqslant i, j, k \leqslant r,\ 1 \leqslant l \leqslant s)\,.$$

Thus (11.5) is $\ll |\mathbf{u}_1 - \mathbf{u}_2|^2 (|\mathbf{u}_1| + |\mathbf{u}_2| + |\mathbf{v}|)$. As a consequence, we see that when $(\mathbf{u}_1, \mathbf{v})$, $(\mathbf{u}_2, \mathbf{v})$ lie in a sufficiently small neighborhood $\mathfrak{D}$ of the origin, say in $|\mathbf{u}|, |\mathbf{v}| < \varrho$, then the expression (11.5) is of modulus $< \frac{1}{2} c\, |\mathbf{u}_1 - \mathbf{u}_2|^2$. In conjunction with (11.2), (11.3) this shows that for fixed $\mathbf{v}$, the function $h(\mathbf{u}, \mathbf{v})$ has property (11.1). Also the function $g_N = N h(N^{-1}\mathbf{u}, N^{-1}\mathbf{v})$ has this property. We are concerned with integer points $\mathbf{x} = (\mathbf{u}, \mathbf{v}) \in N\mathfrak{D}$. For fixed $\mathbf{v}$, the point $\mathbf{u}$ runs through $|\mathbf{u}| < R$ with $R = N\varrho \ll N$, and $g_N$ has values $|g_N| < A\,R$ with $A \ll 1$. Thus for fixed $\mathbf{v}$, Lemma 5 applies and we get $\ll N^{r-1+(2/(r+2))}$ integer points $(\mathbf{u}, z)$. Taking the sum over $\mathbf{v}$ we get an extra factor $\ll N^s = N^{n-r-1}$. The assertion of the lemma follows.

We now zero in on Theorem 5. For each $\mathbf{x}_0 \in \mathfrak{A}$ we will construct a neighborhood $\mathfrak{U}$ such that

$$Z_N(f, \mathfrak{U}) \leqslant c_{14}(f, \mathfrak{U})\, N^{n-2+(2/(r+2))}\,. \tag{11.6}$$

Since $\mathfrak{A}$, being compact, is covered by a finite number of these neighborhoods, the theorem will follow. We may suppose that $\mathbf{x}_0 = \mathbf{0}$. By our hypothesis on the surface $\mathscr{S}$, the quadratic form of curvature associated with each point is of the type

$$\pm (L_1^2 + \ldots + L_r^2 + c_{r+1} L_{r+1}^2 + \ldots + c_{n-1} L_{n-1}^2) \tag{11.7}$$

with independent linear forms $L_1, \ldots, L_{n-1}$. The coordinates $\mathbf{x}, z$ in $z = f(\mathbf{x})$ are not intrinsic coordinates, but nevertheless the expansion of $f$ at the origin is

$$f = a + L(\mathbf{x}) + F(\mathbf{x}) + f_0, \tag{11.8}$$

where $L$ is a linear form, $F$ is a quadratic form of the type (11.7), and $f_0$ contains terms of degree $> 2$. We may suppose that the $+$ sign holds in (11.7). After a suitable orthogonal change of variables from $\mathbf{x} = (x_1, \ldots, x_{n-1})$ to $(\mathbf{u}', \mathbf{v}') = (u_1', \ldots, u_r', v_1', \ldots, v_s')$ (where $r + s + 1 = n$),

$$F(\mathbf{x}) = a_1 u_1'^2 + \ldots + a_r u_r'^2 + b_1 v_1'^2 + \ldots + b_s v_s'^2 \tag{11.9}$$

with $a_i > 0$ $(i = 1, \ldots, r)$. There is only one problem: this change of variables will change $\mathbb{Z}^{n-1}$ into some other lattice, and hence Lemma 6 will not apply. (Never mind that Lemma 5 holds for any lattice of determinant 1).

Suppose the coordinates $\mathbf{u}', \mathbf{v}'$ belong to the orthonormal basis $\mathbf{k}_1, \ldots, \mathbf{k}_{n-1}$, i.e. suppose that

$$\mathbf{x} = u_1' \mathbf{k}_1 + \ldots + u_r' \mathbf{k}_r + v_1' \mathbf{k}_{r+1} + \ldots + v_s' \mathbf{k}_{r+s} .$$

Given large natural $t$, pick points $\mathbf{l}_1, \ldots, \mathbf{l}_{n-1}$ in $\mathbb{Z}^{n-1}$ with $|\mathbf{l}_i - t\,\mathbf{k}_i| \ll 1$ $(i = 1, \ldots, n-1)$. The points $\mathbf{l}_1, \ldots, \mathbf{l}_{n-1}$ have a determinant of absolute value $T \ll t^{n-1}$. Now write

$$\mathbf{x} = T^{-1}(u_1 \mathbf{l}_1 + \ldots + u_r \mathbf{l}_r + v_1 \mathbf{l}_{r+1} + \ldots + v_s \mathbf{l}_{r+s}) . \tag{11.10}$$

Then $u_i' = T^{-1}(t\,u_i + O(|\mathbf{u}| + |\mathbf{v}|))$, $v_i' = T^{-1}(t\,v_i + O(|\mathbf{u}| + |\mathbf{v}|))$, and (11.9) becomes

$$F(\mathbf{x}) = t^2 T^{-2}(a_1 u_1^2 + \ldots + a_r u_r^2 + b_1 v_1^2 + \ldots + b_s v_s^2) + F_0(\mathbf{u}, \mathbf{v})$$

where $F_0$ has coefficients $\ll t\,T^{-2}$. Thus when $t$ is sufficiently large, $F(\mathbf{x}) = Q(\mathbf{u}) + F_1(\mathbf{u}, \mathbf{v})$ with positive definite $Q$ and with every term of $F_1$ involving $\mathbf{v}$. Substitution into (11.8) gives $f(\mathbf{x}) = h(\mathbf{u}, \mathbf{v})$ with $h$ of the type (11.3) of Lemma 6.

The definition of $T$ and (11.10) show that when $\mathbf{x}$ is an integer point, then so is $(\mathbf{u}, \mathbf{v})$. By Lemma 6 there is a neighborhood $\mathfrak{O}$ of the origin with (11.4). Now the transition $(\mathbf{u}, \mathbf{v}) \mapsto \mathbf{x}$ is effected by a certain linear transformation $\tau$. Setting $\mathfrak{U} = \tau\,\mathfrak{O}$ we have indeed (11.6).

## References

[1] ANDREWS, G. E.: An asymptotic expression for the number of solutions of a general class of diophantine equations. Trans. Amer. Math. Soc. **99**, 272—277 (1961).

[2] ANDREWS, G. E.: A lower bound for the volume of strictly convex bodies with many boundary lattice points. Trans. Amer. Math. Soc. **106**, 270—279 (1963).

[3] CASSELS, J. W. S.: An Introduction to the Geometry of Numbers. Grundlehren 99. Berlin–Heidelberg–New York: Springer. 1959.

[4] COHEN, S. D.: The distribution of Galois groups and Hilbert's irreducibility theorem. Proc. Lond. Math. Soc. (3) **43**, 227—250 (1981).

[5] DAVENPORT, H.: Indefinite quadratic forms in many variables (II). Proc. Lond. Math. Soc. (3) **8**, 109—126 (1958).

[6] GRÜNBAUM, B.: Convex Polytopes. Interscience Publ. 1967.

[7] HEATH-BROWN, D. R.: Cubic forms in ten variables. Proc. Lond. Math. Soc. (3) **47**, 225—257 (1983).

[8] JARNIK, V.: Über die Gitterpunkte auf konvexen Kurven. Math. Z. **24**, 500—518 (1925).

[9] ROTH, K. F.: Rational approximations to algebraic numbers. Mathematika **2**, 1—20 (1955).

[10] SCHMIDT, W. M.: Über Gitterpunkte auf gewissen Flächen. Mh. Math. **68**, 59—74 (1964).

[11] SWINNERTON-DYER, H. P. F.: The number of lattice points on a convex curve. J. Number Theory **6**, 128—135 (1974).

W. M. SCHMIDT
University of Colorado
Department of Mathematics
Campus Box 426
Boulder, CO 80309, U.S.A.