References

[1] A. Baker, *Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms*, Phil. Trans. Royal Soc. London, Series A, 263 (1968), pp. 173–191.
[2] — *II. The Diophantine equation $y^2 = x^3+k$*, Phil. Trans. Royal Soc. London, Series A, 263 (1968), pp. 193–208.
[3] J. W. S. Cassels, *An introduction to the geometry of numbers*, Berlin 1959.
[4] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), pp. 279–305.
[5] K. Mahler, *Zur Approximation algebraischer Zahlen I*, Math. Ann. 107 (19 3), pp. 691–730.
[6] — *Ueber die Approximation P-adischer Zahlen*, Jber. Deutsche Math. Ver., (1934), pp. 250–255.
[7] B. van der Waerden, *Modern Algebra*, New York 1953, revised English edition.
[8] H. Weyl, *Algebraic theory of numbers*, Ann. of Math. Studies 1 (Princeton, 1940).

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
Cambridge, England

Reçu par la Rédaction le 2. 5. 1969

ACTA ARITHMETICA
XVI (1970)

Dirichlet's theorem on diophantine approximation. II

by

H. Davenport † and W. M. Schmidt* (Boulder, Colo.)

1. Introduction. We shall be interested in simultaneous approximation to n real numbers $a_1, \ldots, a_n$. There are two forms of Dirichlet's theorem:

(a) *For any positive integer N there exist integers $x_1, \ldots, x_n, y$ not all zero, satisfying*

$$|a_1x_1+\ldots+a_nx_n+y| < N^{-n}, \quad \max(|x_1|, \ldots, |x_n|) \leqslant N. \tag{1a}$$

(b) *For any positive integer N there exist integers $x_1, \ldots, x_n, y$, not all zero, with*

$$\max(|a_1y-x_1|, \ldots, |a_ny-x_n|) < N^{-1}, \quad |y| \leqslant N^n. \tag{1b}$$

For particular $a_1, \ldots, a_n$ we shall say that (a) can be improved if there exists a $\mu = \mu(a_1, \ldots, a_n) < 1$ such that, for every sufficiently large N, the inequalities (1a) may be replaced by

$$|a_1x_1+\ldots+a_nx_n+y| < \mu N^{-n}, \quad \max(|x_1|, \ldots, |x_n|) < \mu N. \tag{2a}$$

We shall say that (b) can be improved if there exists a $\mu < 1$ such that, for every sufficiently large N, the inequalities (1b) may be replaced by

$$\max(|a_1y-x_1|, \ldots, |a_ny-x_n|) < \mu N^{-1}, \quad |y| < \mu N^n. \tag{2b}$$

One main theorem is as follows.

Theorem 1. *For almost every n-tuple $(a_1, \ldots, a_n)$, neither form (a) nor form (b) of Dirichlet's theorem can be improved.*

In this theorem *almost every* is used in the sense of n-dimensional Lebesgue measure. This theorem was announced in the first paper [2] of this series. Khintchine [4] showed that for almost every $(a_1, \ldots, a_n)$ there exists a $\mu = \mu^*(a_1, \ldots, a_n)$ such that (1a) may not be replaced by (2a), and (1b) may not be replaced by (2b). Thus for almost all $(a_1, \ldots, a_n)$,

* The second author was partially supported by NSF-GP-6515.

no arbitrarily good improvement of Dirichlet's theorem is possible. When $n = 1$, Theorem 1 follows easily from the theory of continued fractions.

As was shown in [2], Dirichlet's theorem may be improved for a single number a_1 (in this case forms (a), (b) are identical) precisely if the partial quotients in the continued fraction of a_1 are bounded. But almost every a_1 has unbounded partial quotients.

We shall give a direct proof of the assertion concerning form (a) of Dirichlet's theorem only. The assertion concerning form (b) follows from the following transference theorem.

THEOREM 2. *For any n-tuple* $(a_1, \ldots, a_n)$, *form* (a) *of Dirichlet's theorem can be improved if and only if form* (b) *can be improved.*

The standard transference theorems, while rather more general, are not sufficiently precise to yield Theorem 2.

2. Deduction of Theorem 1 from a metrical theorem on lattices. Let n be a positive integer and put

$$l = n+1. \tag{3}$$

Points in l-dimensional space will be denoted by $\boldsymbol{a}, \boldsymbol{b}, \ldots$ An n-tuple $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ of such points may be interpreted as a point $\boldsymbol{A}$ of ln-dimensional space. A set of n-tuples $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ will be called *everywhere dense* if the corresponding points $\boldsymbol{A}$ are everywhere dense in ln-dimensional space.

Given real numbers $a_1, \ldots, a_n$ and a positive integer N, we define $\Lambda(a_1, \ldots, a_n; N)$ to be the lattice in l-dimensional space with basis vectors

$$\begin{aligned} \boldsymbol{g}_1 &= (N^{-1}, 0, \ldots, 0, a_1 N^n), \\ \boldsymbol{g}_2 &= (0, N^{-1}, \ldots, 0, a_2 N^n), \\ &\ldots\ldots\ldots\ldots\ldots \\ \boldsymbol{g}_n &= (0, 0, \ldots, N^{-1}, a_n N^n), \\ \boldsymbol{g}_l &= (0, 0, \ldots, 0, N^n). \end{aligned}$$

THEOREM 3. *For almost every* $(a_1, \ldots, a_n)$ *the set of n-tuples* $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ *which are part of a basis* $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n, \boldsymbol{a}_l)$ *of a lattice* $\Lambda(a_1, \ldots, a_n; N)$ *for some N is everywhere dense.*

It may be true that for almost every $(a_1, \ldots, a_n)$ the set of lattices $\Lambda(a_1, \ldots, a_n; N)$ with N running through all integers is everywhere dense in the space of lattices of determinant 1. This would be stronger than Theorem 3, but we are unable to prove it[1]

[1] Added in proof. But see a paper *Diophantine approximation and certain sequences of lattices* by the second author to appear in this journal.

Deduction of Theorem 1. As pointed out above, we shall give a direct proof only of part (a). Suppose Λ is a lattice of determinant 1 in l-dimensional space which has a basis containing the vectors $\boldsymbol{e}_1 = (1, 0, \ldots, 0)$, $\boldsymbol{e}_2 = (0, 1, \ldots, 0), \ldots, \boldsymbol{e}_n = (0, 0, \ldots, 1, 0)$. Then every point $\boldsymbol{p} = (\pi_1, \ldots, \pi_l) \neq \boldsymbol{0}$ of Λ satisfies

$$\max(|\pi_1|, \ldots, |\pi_l|) \geqslant 1.$$

Now suppose that $\mu < 1$. Continuity arguments show the existence of a number $\varepsilon = \varepsilon(\mu) > 0$ such that every point $\boldsymbol{p} = (\pi_1, \ldots, \pi_l) \neq \boldsymbol{0}$ which belongs to a lattice Λ' of determinant 1 which has a basis containing vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ with $|\boldsymbol{a}_i - \boldsymbol{e}_i| < \varepsilon$ $(i = 1, \ldots, n)$ satisfies

$$\max(|\pi_1|, \ldots, |\pi_l|) \geqslant \mu.$$

Assume now that $(a_1, \ldots, a_n)$ is an n-tuple and N_0 is an integer such that the inequalities (2a) have a non-trivial solution for every $N > N_0$. Such a solution $x_1, \ldots, x_n, y$ satisfies

$$\max(|x_1 N^{-1}|, \ldots, |x_n N^{-1}|, |x_1 a_1 N^n + \ldots + x_n a_n N^n + y N^n|) < \mu.$$

The point $(x_1 N^{-1}, \ldots, x_n N^{-1}, x_1 a_1 N^n + \ldots + x_n a_n N^n + y N^n)$ is a point $(\pi_1, \ldots, \pi_l) \neq \boldsymbol{0}$ of the lattice $\Lambda(a_1, \ldots, a_n; N)$ with $\max(|\pi_1|, \ldots, |\pi_l|) < \mu$. Hence by what we said above, there are no n-tuples $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ with $|\boldsymbol{a}_i - \boldsymbol{e}_i| < \varepsilon$ $(i = 1, \ldots, n)$ which are part of a basis of $\Lambda(a_1, \ldots, a_n; N)$. Thus the n-tuples of points $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ which are part of a basis of a lattice $\Lambda(a_1, \ldots, a_n; N)$ for some N are not everywhere dense.

By Theorem 3, this happens for almost no $(a_1, \ldots, a_n)$.

In the course of the proof of Theorem 3 we shall need the following theorem which may be of independent interest.

THEOREM 4. *Suppose* $1 \leqslant m < l$ *and write points of lm-dimensional space as*

$$\boldsymbol{X} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m),$$

where $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ *are in l-dimensional space. Let S be a bounded Jordan measurable set in lm-dimensional space of volume* $V(S)$. *Then as* $t \to \infty$, *the number of integer points* $\boldsymbol{X}$ *in tS such that* $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ *are part of a basis of the integer lattice of l-dimensional space is asymptotically equal to*

$$t^{ml} V(S) \big(\zeta(l)\zeta(l-1)\ldots\zeta(l-m+1)\big)^{-1}. \tag{4}$$

When $m = 1$ the points $\boldsymbol{X}$ reduce to primitive lattice points $\boldsymbol{X} = (\boldsymbol{x}_1)$, and the result is well known.

We shall first prove Theorem 4, then Theorem 3, then Theorem 2. To avoid cumbersome notation, we shall prove Theorems 2, 3, 4 only in the case $l = 3$, which is quite typical.

3. Proof of Theorem 4. Since we restrict ourselves to $l=3$, and since, as pointed out, the case $m=1$ is well known, we may assume that

$$m=2,\ l=3. \tag{5}$$

An integer point $\boldsymbol{x}\neq\mathbf{0}$ can be uniquely written $\boldsymbol{x}=k\boldsymbol{x}^*$ where k is a positive integer and $\boldsymbol{x}^*$ is a primitive integer point. We have

$$\sum_{d|k}\mu(d)=\begin{cases}1 & \text{if } k=1, \text{ hence if } \boldsymbol{x} \text{ is primitive,}\\ 0 & \text{otherwise.}\end{cases}$$

Now $d|k$ holds precisely if $\boldsymbol{x}$ may be written in the form $\boldsymbol{x}=d\boldsymbol{x}'$ with some integer point $\boldsymbol{x}'$. Hence

$$\sum_{d=1}^{\infty}\mu(d)\cdot\left\{\begin{matrix}1 & \text{if there is an } \boldsymbol{x}' \text{ with } \boldsymbol{x}=d\boldsymbol{x}'\\ 0 & \text{otherwise}\end{matrix}\right\}$$

is equal to 1 if $\boldsymbol{x}$ is primitive, and it is zero otherwise.

Now assume $\boldsymbol{x}$ to be primitive and $\boldsymbol{x},\boldsymbol{y}$ to be linearly independent points of 3-dimensional space. The points $a\boldsymbol{x}+b\boldsymbol{y}$ with integer coefficients a, b form a sublattice of the (2-dimensional) lattice of all integer points in the plane spanned by $\boldsymbol{x},\boldsymbol{y}$. Denote the index of this sublattice by r. Then $r=1$ precisely if $\boldsymbol{x},\boldsymbol{y}$ are part of a basis of the integer lattice of 3-dimensional space. Thus

$$\sum_{e|r}\mu(e)=\begin{cases}1 & \text{if } r=1, \text{ hence if } \boldsymbol{x},\boldsymbol{y} \text{ are part of a basis,}\\ 0 & \text{otherwise.}\end{cases}$$

Now $e|r$ precisely if $\boldsymbol{y}=s\boldsymbol{x}+e\boldsymbol{y}'$ for some integer s and some integer point $\boldsymbol{y}'$. We have $s\boldsymbol{x}+e\boldsymbol{y}'=\hat{s}\boldsymbol{x}+e\hat{\boldsymbol{y}}'$ exactly if $(s-\hat{s})\boldsymbol{x}=e(\hat{\boldsymbol{y}}'-\boldsymbol{y}')$, and since $\boldsymbol{x}$ is primitive this is possible precisely if $s\equiv\hat{s}\ (\mathrm{mod}\ e)$. We may therefore restrict ourselves to numbers s in $0\leqslant s<e$. Hence if $\boldsymbol{x}$ is primitive and if $\boldsymbol{x},\boldsymbol{y}$ are linearly independent, then

$$\sum_{e=1}^{\infty}\mu(e)\sum_{s=0}^{e-1}\left\{\begin{matrix}1 & \text{if there is a } \boldsymbol{y}' \text{ with } \boldsymbol{y}=s\boldsymbol{x}+e\boldsymbol{y}'\\ 0 & \text{otherwise}\end{matrix}\right\}$$

is equal to 1 if $\boldsymbol{x},\boldsymbol{y}$ are part of a basis, and it is zero otherwise.

Combining our arguments we see that for independent $\boldsymbol{x},\boldsymbol{y}$,

$$\left(\sum_{d=1}^{\infty}\mu(d)\cdot\left\{\begin{matrix}1 \text{ if } \boldsymbol{x}=d\boldsymbol{x}'\\ 0 \text{ otherwise}\end{matrix}\right\}\right)\left(\sum_{e=1}^{\infty}\mu(e)\sum_{s=0}^{e-1}\left\{\begin{matrix}1 \text{ if } \boldsymbol{y}=s\boldsymbol{x}+e\boldsymbol{y}'\\ 0 \text{ otherwise}\end{matrix}\right\}\right)$$

is 1 if $\boldsymbol{x},\boldsymbol{y}$ are part of a basis, and is zero otherwise.

Since $k=3$, $m=2$, the set S is in 6-dimensional space. Points of this space will be written $(\boldsymbol{x},\boldsymbol{y})$ where $\boldsymbol{x},\boldsymbol{y}$ are in 3-dimensional space. Write $z(tS)$ for the number of points $(\boldsymbol{x},\boldsymbol{y})$ in tS with the property that

$\boldsymbol{x},\boldsymbol{y}$ are part of a basis of the 3-dimensional integer lattice. Let $\chi_t(\boldsymbol{x},\boldsymbol{y})$ be the characteristic function of tS. Then we have

$$z(tS)=\sum_{d=1}^{\infty}\mu(d)\sum_{e=1}^{\infty}\mu(e)\sum_{s=0}^{e-1}\ \sum_{\substack{\boldsymbol{x}'\\ \boldsymbol{x}',\boldsymbol{y}'\,\text{indep.}}}\sum_{\boldsymbol{y}'}\chi_t(d\boldsymbol{x}',\ sd\boldsymbol{x}'+e\boldsymbol{y}'). \tag{6}$$

Put

$$f_t(d,e,s)=\sum_{\substack{\boldsymbol{x}'\\ \boldsymbol{x}',\boldsymbol{y}'\,\text{indep.}}}\sum_{\boldsymbol{y}'}\chi_t(d\boldsymbol{x}',\ sd\boldsymbol{x}'+e\boldsymbol{y}').$$

For given d, e, s it is clear that we have the asymptotic formula

$$f_t(d,e,s)\sim t^6V(S)d^{-3}e^{-3}\quad\text{as}\quad t\to\infty. \tag{7}$$

Since

$$\sum_{d=1}^{\infty}\mu(d)\sum_{e=1}^{\infty}\mu(e)\sum_{s=0}^{e-1}d^{-3}e^{-3}=\Big(\sum_{d=1}^{\infty}\mu(d)d^{-3}\Big)\Big(\sum_{e=1}^{\infty}\mu(e)e^{-2}\Big)=1/\big(\zeta(2)\zeta(3)\big), \tag{8}$$

we have almost completed the proof — but not quite.

4. An auxiliary lemma. If we replace $\sum_{d=1}^{\infty}\sum_{e=1}^{\infty}$ on the left hand side of (8) by $\sum_{d=1}^{M}\sum_{e=1}^{M}$, we obtain a sum which comes arbitrarily close to $1/\big(\zeta(2)\zeta(3)\big)$ as $M\to\infty$. Hence if we replace the summation over d, e on the right hand side of (6) by summation over the finite intervals $1\leqslant d\leqslant M$, $1\leqslant e\leqslant M$, we obtain a sum which comes close to $t^6V(S)/\big(\zeta(2)\zeta(3)\big)$. It remains to give an upper bound for the terms on the right hand side of (6) with $d>M$ or $e>M$. Since

$$\sum_{d=M}^{\infty}\sum_{e=1}^{\infty}d^{-3}e^{-2}\quad\text{and}\quad\sum_{d=1}^{\infty}\sum_{e=M}^{\infty}d^{-3}e^{-2}$$

tend to zero as $M\to\infty$, the following lemma will finish our proof of Theorem 2.

LEMMA 1.

$$f_t(d,e,s)\ll t^6d^{-3}e^{-3}.$$

The constant implied by $\ll$ is independent of d, e, s, t.

Proof of Lemma 1. Since the constant implied by $\ll$ may depend on S, and by homogeneity, we may assume that S is the unit ball:

$$|\boldsymbol{x}|^2+|\boldsymbol{y}|^2=x_1^2+x_2^2+x_3^2+y_1^2+y_2^2+y_3^2\leqslant 1. \tag{9}$$

We now put $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$, $z_3 = (x_3, y_3)$. Then $f_t(d, e, s)$ is bounded by the number of triples of points z_1, z_2, z_3 of 2-dimensional space which span this space and which have each z_i in the ellipse

$$(dx)^2 + (sdx + ey)^2 \leqslant t^2. \tag{10}$$

Thus

$$f_t(d, e, s) \leqslant (g_t(d, e, s))^3, \tag{11}$$

where $g_t(d, e, s)$ is the number of integer points in the ellipse (10). We also note that $f_t(d, e, s) = 0$ if the ellipse (10) contains no two linearly independent points. Hence it will suffice to show that

$$g_t(d, e, s) \leqslant 4 \cdot (\text{area of the ellipse (10)}) = 4\pi t^2 d^{-1} e^{-1}, \tag{12}$$

provided the ellipse contains two linearly independent integer points.

We may replace the ellipse by a circular disc D of equal area if we replace the integer lattice by an arbitrary lattice of determinant 1. Suppose the disc D has radius ϱ. Since two independent lattice points lie in it, there is a fundamental parallelogram Π of the lattice having diameter less than 2ϱ. With every lattice point $\boldsymbol{g}$ in the disc D we associate the translate $\Pi(\boldsymbol{g})$ of Π which has $\boldsymbol{g}$ as its center. These parallelograms $\Pi(\boldsymbol{g})$ are disjoint and they all are contained in the disc D' of radius 2ϱ. Hence their number does not exceed the area of D', which is four times the area of D. This completes the proof of Lemma 1.

5. The method of proof of Theorem 3. We shall restrict ourselves to the case $n = 2$, $l = 3$. Throughout the proof, $\boldsymbol{x}, \boldsymbol{y}, \ldots$ will denote points of 3-dimensional space. We shall write (α, β) instead of (α_1, α_2).

Let $\boldsymbol{c}_1 = (\gamma_{11}, \gamma_{12}, \gamma_{13})$, $\boldsymbol{c}_2 = (\gamma_{21}, \gamma_{22}, \gamma_{23})$ be points with

$$\gamma_{11}\gamma_{22} - \gamma_{12}\gamma_{21} \neq 0. \tag{13}$$

Put

$$\gamma = \max(|\gamma_{11}|, \ldots, |\gamma_{23}|). \tag{14}$$

Let δ be positive and C_j^* $(j = 1, 2)$ the cube consisting of points $\boldsymbol{x} = (x_1, x_2, x_3)$ with

$$|x_1 - \gamma_{j1}| < \delta, \quad |x_2 - \gamma_{j2}| < \delta, \quad |x_3| < \delta. \tag{15}$$

Further let C_j $(j = 1, 2)$ be the cube defined by

$$|x_1 - \gamma_{j1}| < \delta, \quad |x_2 - \gamma_{j2}| < \delta, \quad |x_3 - \gamma_{j3}| < \delta. \tag{16}$$

Write $\mathfrak{C}_j^*$ for the cone of points $\lambda\boldsymbol{x}$ with $\boldsymbol{x} \in C_j^*$.

We shall assume $\delta > 0$ to be so small that

$$6\delta(\gamma + \delta)^2 < 1, \tag{17}$$

$$|\gamma'_{11}\gamma'_{22} - \gamma'_{12}\gamma'_{21}| \geqslant \delta \text{ if } |\gamma_{ij} - \gamma'_{ij}| \leqslant \delta \ (i, j = 1, 2), \tag{18}$$

$$C_j^* \text{ is disjoint from } -C_j^*, \pm 2C_j^*, \pm 3C_j^*, \ldots \ (j = 1, 2), \tag{19a}$$

$$\text{the intersection of } \mathfrak{C}_1^*, \mathfrak{C}_2^* \text{ consists only of } \boldsymbol{0}. \tag{19b}$$

Since 6-dimensional space is separable, since $\boldsymbol{c}_1, \boldsymbol{c}_2$ were subject only to (13) and since $\delta > 0$ is arbitrarily small, the following will suffice to prove Theorem 3.

For almost all (α, β), there exist points $\boldsymbol{a}_1, \boldsymbol{a}_2$ with $\boldsymbol{a}_j \in C_j$ $(j = 1, 2)$ such that $\boldsymbol{a}_1, \boldsymbol{a}_2$ are part of a basis of a lattice $\Lambda(\alpha, \beta; N)$.

Let $\Sigma(N)$ be the set of pairs (α, β) for which $\Lambda(\alpha, \beta; N)$ has a basis $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$ with $\boldsymbol{a}_j \in C_j$ $(j = 1, 2)$. The following proposition implies Theorem 3.

PROPOSITION. *There is an $\varepsilon > 0$ such that for every square Q of the type*

$$|\alpha - \alpha_0| < \eta, \quad |\beta - \beta_0| < \eta \tag{20}$$

and every $N > N_1(Q)$, the intersection of Q with $\Sigma(N)$ has measure

$$\mu(Q \cap \Sigma(N)) \geqslant \varepsilon\mu(Q) = \varepsilon 4\eta^2. \tag{21}$$

6. Analysis of the set $\Sigma(N)$. Recall that the lattice $\Lambda(\alpha, \beta; N)$ has the basis

$$\boldsymbol{g}_1 = (N^{-1}, 0, \alpha N^2), \quad \boldsymbol{g}_2 = (0, N^{-1}, \beta N^2), \quad \boldsymbol{g}_3 = (0, 0, N^2). \tag{22}$$

Any two lattice points $\boldsymbol{a}_1, \boldsymbol{a}_2$ may be written

$$\begin{aligned} \boldsymbol{a}_1 &= q_{11}\boldsymbol{g}_1 + q_{12}\boldsymbol{g}_2 + q_{13}\boldsymbol{g}_3, \\ \boldsymbol{a}_2 &= q_{21}\boldsymbol{g}_1 + q_{22}\boldsymbol{g}_2 + q_{23}\boldsymbol{g}_3, \end{aligned} \tag{23}$$

with integer coefficients q_{ij}. They are part of a basis of $\Lambda(\alpha, \beta; N)$ precisely if the integer points

$$\boldsymbol{q}_1 = (q_{11}, q_{12}, q_{13}), \quad \boldsymbol{q}_2 = (q_{21}, q_{22}, q_{23}) \tag{24}$$

are part of a basis of the integer lattice.

For given integer points $\boldsymbol{q}_1, \boldsymbol{q}_2$, let $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ be the set of pairs (α, β) for which $\boldsymbol{a}_1, \boldsymbol{a}_2$ as given by (22), (23) lie in C_1, C_2, respectively.

LEMMA 2. *Suppose the points $\boldsymbol{q}_1, \boldsymbol{q}_2$ satisfy*

$$|q_{11} - N\gamma_{11}| < N\delta, \quad |q_{12} - N\gamma_{12}| < N\delta, \tag{25}$$

$$|q_{21} - N\gamma_{21}| < N\delta, \quad |q_{22} - N\gamma_{22}| < N\delta. \tag{26}$$

Then $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ *is a parallelogram of area*

(27) $$\mu(E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)) \gg N^{-6}$$

and of diameter

(28) $$\Delta(E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)) \ll N^{-3}.$$

(The constants implied by $\ll$ may depend on c_1, c_2, δ (which remain fixed throughout), but they are independent of Q.)

Proof. Write $\boldsymbol{a}_1 = (\alpha_{11}, \alpha_{12}, \alpha_{13})$, $\boldsymbol{a}_2 = (\alpha_{21}, \alpha_{22}, \alpha_{23})$. By (25) we have

$$|\alpha_{11} - \gamma_{11}| = |q_{11}N^{-1} - \gamma_{11}| < \delta \quad \text{and} \quad |\alpha_{12} - \gamma_{12}| < \delta.$$

The inequality $|\alpha_{13} - \gamma_{13}| < \delta$ is equivalent with

(29) $$|q_{11}\alpha + q_{12}\beta + q_{13} - \gamma_{13}N^{-2}| < \delta N^{-2}.$$

Thus $\boldsymbol{a}_1$ lies in C_1 precisely if (29) is satisfied. Similarly, $\boldsymbol{a}_2$ lies in C_2 precisely if

(30) $$|q_{21}\alpha + q_{22}\beta + q_{23} - \gamma_{23}N^{-2}| < \delta N^{-2}.$$

The set $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ consists of all pairs (α, β) with (29) and (30). This set is a parallelogram of area

$$\delta^2 N^{-4} |q_{11}q_{22} - q_{12}q_{21}|^{-1} \gg N^{-6},$$

since

(31) $$N^2 \ll |q_{11}q_{22} - q_{12}q_{21}| \ll N^2$$

by (18), (25), (26).

Let (α, β) and (α', β') be any two points in this parallelogram. Then

$$|q_{11}(\alpha - \alpha') + q_{12}(\beta - \beta')| < 2\delta N^{-2},$$
$$|q_{21}(\alpha - \alpha') + q_{22}(\beta - \beta')| < 2\delta N^{-2}.$$

Hence

$$|\alpha - \alpha'| < 2\delta N^{-2}(|q_{12}| + |q_{22}|)|q_{11}q_{22} - q_{12}q_{21}|^{-1} \ll N^{-3},$$

and similarly $|\beta - \beta'| \ll N^{-3}$. The lemma follows.

LEMMA 3. *Suppose N is large and suppose the integer points $\boldsymbol{q}_1, \boldsymbol{q}_2$ satisfy* (25), (26) *and*

(32) $$\left|\begin{vmatrix} q_{12} & q_{13} \\ q_{22} & q_{23} \end{vmatrix} \Big/ \begin{vmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{vmatrix} - \alpha_0\right| < \eta/4, \quad \left|\begin{vmatrix} q_{13} & q_{11} \\ q_{23} & q_{21} \end{vmatrix} \Big/ \begin{vmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{vmatrix} - \beta_0\right| < \eta/4.$$

Then $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ *is contained in the square Q defined by* (20).

Proof. By what we said above the parallelogram $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ has center

(33) $$\left(\left(\begin{vmatrix} q_{12} & q_{13} \\ q_{22} & q_{23} \end{vmatrix} - N^{-2}\begin{vmatrix} q_{12} & \gamma_{13} \\ q_{22} & \gamma_{23} \end{vmatrix}\right) \Big/ \begin{vmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{vmatrix}, \left(\begin{vmatrix} q_{13} & q_{11} \\ q_{23} & q_{21} \end{vmatrix} - N^{-2}\begin{vmatrix} \gamma_{13} & q_{11} \\ \gamma_{23} & q_{21} \end{vmatrix}\right) \Big/ \begin{vmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{vmatrix}\right).$$

In view of (25), (26), (31), (32) this center will lie in the square

$$Q': \ |\alpha - \alpha_0| < \eta/2, \ |\beta - \beta_0| < \eta/2$$

i N is large. Since $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ has diameter $\Delta(E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)) \ll N^{-3}$, the whole parallelogram $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ lies in Q if N is large.

7. Parallelograms $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$. Suppose (25) and (26) hold. Let $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ be the parallelogram of points (α, β) which satisfy (29), (30) with γ_{13}, γ_{23} replaced by zero. In view of (33) it is clear that $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ is obtained from $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ by translation by a vector whose length is $O(N^{-3})$.

LEMMA 4. *Suppose $\boldsymbol{q}_1, \boldsymbol{q}_2$ satisfy* (25), (26), *and are part of a basis of the integer lattice. Make the same assumptions on $\boldsymbol{q}_1', \boldsymbol{q}_2'$. Then if $(\boldsymbol{q}_1, \boldsymbol{q}_2) \neq (\boldsymbol{q}_1', \boldsymbol{q}_2')$, the parallelograms $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ and $E^*(N, \boldsymbol{q}_1', \boldsymbol{q}_2')$ are disjoint.*

Proof. Suppose (α, β) lies both in $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ and in $E^*(N, \boldsymbol{q}_1', \boldsymbol{q}_2')$.

First assume that $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_1', \boldsymbol{q}_2'$ span the 3-dimensional space. Without loss of generality we may assume that $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_1'$ are linearly independent. Hence the determinant

(34) $$\begin{vmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{11}' & q_{12}' & q_{13}' \end{vmatrix} = \begin{vmatrix} q_{11} & q_{12} & \alpha q_{11} + \beta q_{12} + q_{13} \\ q_{21} & q_{22} & \alpha q_{21} + \beta q_{22} + q_{23} \\ q_{11}' & q_{12}' & \alpha q_{11}' + \beta q_{12}' + q_{13}' \end{vmatrix}$$

has absolute value at least 1.

On the other hand by (25), (26), the entries in the first two columns have absolute values less than $N(\gamma + \delta)$. The entries in the third column on the right hand side of (34) have absolute values less than δN^{-2} by the inequalities (29), (30) with γ_{13}, γ_{23} replaced by zero. Hence we have

$$1 < 6N^2(\gamma + \delta)^2 \delta N^{-2} = 6(\gamma + \delta)^2 \delta,$$

which contradicts (17).

Next, assume that $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_1', \boldsymbol{q}_2'$ lie in a 2-dimensional subspace. We may assume that $\boldsymbol{q}_1' \neq \boldsymbol{q}_1$. Since $\boldsymbol{q}_1, \boldsymbol{q}_2$ are part of a basis,

(35) $$\boldsymbol{q}_1' = u\boldsymbol{q}_1 + v\boldsymbol{q}_2,$$

where u, v are integers. Since $\boldsymbol{q}_1' \neq \boldsymbol{q}_1$, we have $(u, v) \neq (1, 0)$. Since (α, β) lies in $E^*(N, \boldsymbol{q}_1', \boldsymbol{q}_2')$, the point

$$\boldsymbol{a}_1' = q_{11}'\boldsymbol{g}_1 + q_{12}'\boldsymbol{g}_2 + q_{13}'\boldsymbol{g}_3$$

lies in C_1^*. By (35) we have

$$\boldsymbol{a}_1' = u\boldsymbol{a}_1 + v\boldsymbol{a}_2$$

where $\boldsymbol{a}_1 \in C_1^*$ and $\boldsymbol{a}_2 \in C_2^*$. We have $\boldsymbol{a}_1' - u\boldsymbol{a}_1 \in \mathfrak{C}_1^*$, $v\boldsymbol{a}_2 \in \mathfrak{C}_2^*$, whence $v\boldsymbol{a}_2 = 0$, $\boldsymbol{a}_1' - u\boldsymbol{a}_1 = 0$ by (19b). In fact since $\boldsymbol{a}_1 \in C_1^*$ and $u\boldsymbol{a}_1 \in C_1^*$, we have $u = 1$ by (19a). Since $v\boldsymbol{a}_2 = 0$ implies $v = 0$, we have reached a contradiction.

LEMMA 5. *Suppose N is large. Then a point (α, β) lies in $O(1)$ parallelograms $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ with $\boldsymbol{q}_1, \boldsymbol{q}_2$ part of a basis and satisfying* (25), (26).

Proof. Since $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ has diameter $O(N^{-3})$ by Lemma 2, it will suffice to show that at most $O(1)$ parallelograms $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ have their centers in any given disc of radius N^{-3}. Since $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ is obtained from $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ by a translation by a vector of length $O(N^{-3})$, it will be enough to show that there are $O(1)$ parallelograms $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ with $\boldsymbol{q}_1, \boldsymbol{q}_2$ satisfying our conditions and with their center in any given disc of radius N^{-3}. Since $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ has area $\mu(E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)) \gg N^{-6}$ and diameter $O(N^{-3})$ by Lemma 2, we can inscribe in $E^*(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ a small disc $D(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ of radius $\varrho \gg N^{-3}$. These small discs are disjoint by Lemma 4. Hence at most $O(1)$ of them can lie in a disc of radius N^{-3}.

8. End of the proof of Theorem 3. Let $S(N)$ be the set in 6-dimensional space consisting of all points $(\boldsymbol{q}_1, \boldsymbol{q}_2)$ with real components satisfying (25), (26) and (32). Observe that $S(N) = NS(1)$. The set $S(1)$ has volume $V(S(1)) \gg \eta^2$. Hence if $z(N)$ is the number of integer points $(\boldsymbol{q}_1, \boldsymbol{q}_2)$ in $S(N)$ with $\boldsymbol{q}_1, \boldsymbol{q}_2$ part of a basis, then

$$z(N) \gg N^6\eta^2 \tag{36}$$

by Theorem 4.

By Lemma 3, the set $Q \cap \Sigma(N)$ contains at least $z(N)$ parallelograms $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$, which may however not be disjoint. But by Lemma 5, any given point (α, β) is covered by $O(1)$ of these parallelograms. Since $E(N, \boldsymbol{q}_1, \boldsymbol{q}_2)$ has area $\mu(E) \gg N^{-6}$ by Lemma 2, we find that $Q \cap \Sigma(N)$ has area $\mu(Q \cap \Sigma(N)) \gg \eta^2$.

This proves the proposition of § 5, hence Theorem 3.

9. Proof of Theorem 2. For simplicity we shall assume that $n = 2$, and we shall write α, β instead of α_1, α_2. Suppose that for some particular α, β no improvement of Dirichlet's theorem in the form (a) is valid. Then for any $\mu < 1$, there are infinitely many integers N for which the inequalities (2a) are insoluble in integers x_1, x_2, y, not all zero. Hence there

is an increasing sequence of integers N_ν $(\nu = 1, 2, \ldots)$ with the property that

$$|\alpha x_1 + \beta x_2 + y| < (1 - 2^{-\nu})N_\nu^{-2}, \quad \max(|x_1|, |x_2|) < (1 - 2^{-\nu})N_\nu$$

has no solution in integers $x_1, x_2, y \neq 0, 0, 0$. This implies that

$$\max(N_\nu^{-1}|x_1|, N_\nu^{-1}|x_2|, N_\nu^2|\alpha x_1 + \beta x_2 + y|) \geqslant 1 - 2^{-\nu} \tag{37}$$

for all integers $x_1, x_2, y \neq 0, 0, 0$. Thus every lattice point $(\gamma_1, \gamma_2, \gamma_3) \neq 0$ of the lattice $\Lambda(\alpha, \beta; N_\nu)$ satisfies

$$\max(|\gamma_1|, |\gamma_2|, |\gamma_3|) \geqslant 1 - 2^{-\nu}. \tag{38}$$

Hence by a well known principle of the geometry of numbers (see, e.g. Mahler [5] or see [1], § V. 4), the sequence of lattices $\Lambda_\nu = \Lambda(\alpha, \beta; N_\nu)$ has a convergent subsequence. For convenience we shall suppose that the sequence $\{\Lambda_\nu\}$ itself is convergent to a lattice Λ_0. This lattice Λ_0 has determinant 1. Every lattice point $(\gamma_1, \gamma_2, \gamma_3) \neq 0$ of Λ_0 has

$$\max(|\gamma_1|, |\gamma_2|, |\gamma_3|) \geqslant 1. \tag{39}$$

By a theorem of Hajós (for an account, with references, see § 11 in [4]), the lattice Λ_0 is of a rather special type. The lattice Λ_0 must have a basis of the type

$$(1, 0, 0),\ (\varrho, 1, 0),\ (\sigma, \tau, 1) \tag{40}$$

or of a type obtained from (40) by a permutation of the coordinates.

The lattice $\Lambda_\nu^p = \Lambda_\nu^p(\alpha, \beta; N_\nu)$ with basis vectors

$$\boldsymbol{h}_1 = (N_\nu, 0, 0),$$
$$\boldsymbol{h}_2 = (0, N_\nu, 0),$$
$$\boldsymbol{h}_3 = (-\alpha N_\nu, -\beta N_\nu, N_\nu^{-2})$$

is polar to the lattice Λ_ν. The sequence of lattices $\{\Lambda_\nu^p\}$ is convergent to a lattice Λ_0^p which is polar to Λ_0. Hence Λ_0^p again has a basis of the type (40) or obtained from (40) by a permutation of the coordinates. This implies that every point $(\gamma_1, \gamma_2, \gamma_3) \neq 0$ of Λ_0^p satisfies (39).

Continuity arguments imply the existence of a function $f(\nu)$ which tends to 1 as $\nu \to \infty$, such that every point $(\gamma_1, \gamma_2, \gamma_3) \neq \boldsymbol{0}$ of Λ_ν^p satisfies

$$\max(|\gamma_1|, |\gamma_2|, |\gamma_3|) \geqslant f(\nu).$$

Hence for every integer point $(x_1, x_2, y) \neq (0, 0, 0)$ one has

$$\max(|x_1 + \alpha y|N_\nu, |x_2 + \beta y|N_\nu, |y|N_\nu^{-2}) \geqslant f(\nu).$$

Put differently, the inequalities

$$\max(|\alpha y - x_1|, |\beta y - x_2|) < f(\nu)N_\nu^{-1}, \quad |y| < f(\nu)N_\nu^2$$

have no solution in integers $(x_1, x_2, y) \neq (0, 0, 0)$. Since $f(\nu)$ tends to 1, this shows that form (b) of Dirichlet's theorem cannot be improved for (α, β).

Hence if form (a) cannot be improved, then form (b) cannot be improved. The implication in the opposite direction may be shown in an entirely analogous manner.

References

[1] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer Grundlehren 99 (1959).

[2] H. Davenport and W. M. Schmidt, *Dirichlet's theorem on diophantine approximation*, Rendiconti convegno di Teoria dei numeri, Roma 1968. (To appear).

[3] O. H. Keller, *Geometrie der Zahlen*, Enzyklop. der math. Wiss. I. 2, Heft 11, 1954.

[4] A. Ya. Khintchine, *Systems of regular linear equations and a general problem of Čebyšev* (Russian), Izv. Akad. Nauk SSSR (ser. mat.) 12 (1948), pp. 249–259.

[5] K. Mahler, *On lattice points in n-dimensional star bodies, I. Existence theorems*, Proc. Roy. Soc. Lond. A (187) (1946), pp. 151–187.

TRINITY COLLEGE
Cambridge, England

UNIVERSITY OF COLORADO
Boulder, Colorado

Reçu par la Rédaction le 7. 6. 1969

ACTA ARITHMETICA
XVI (1970)

An effective p-adic analogue of a theorem of Thue III
The diophantine equation $y^2 = x^3+k$

by

J. Coates (Cambridge)

I. Introduction. The purpose of the present note is to apply the work of [5], [6] to the equation $y^2 = x^3+k$, where k is any non-zero integer. Let $p_1, \ldots, p_s$ be $s \geqslant 0$ prime numbers, and let $\mathfrak{k}$ be the largest integer, comprised solely of powers of $p_1, \ldots, p_s$, which divides k. We write P for the maximum of $p_1, \ldots, p_s$; if no primes are specified, we take $P = 2$. Then our principal result is as follows:

Theorem 1. *All solutions of the equation $y^2 = x^3+k$ in integers x, y, with $(x, y, p_1 \ldots p_s) = 1$, satisfy*

$$\max(|x|, |y|) < \exp\{2^{10^7(s+1)^4} P^{10^9(s+1)^3} |k/\mathfrak{k}|^{10^6(s+1)^2}\}.$$

It will be observed that when $s = 0$, that is when no primes $p_1, \ldots, p_s$ are specified, Theorem 1 reduces to a slightly weaker form of the result in Baker's paper [1]. On the other hand, if k is comprised solely of powers of $p_1, \ldots, p_s$ so that $|k/\mathfrak{k}| = 1$, then Theorem 1 implies that all solutions of the equation $y^2 = x^3+k$ in integers x, y, with $(x, y, p_1 \ldots p_s) = 1$, satisfy

$$\max(|x|, |y|) < \exp\{2^{10^7(s+1)^4} P^{10^9(s+1)^3}\}. \tag{1}$$

The interest of this result lies in the fact that the number on the right does not depend on the exponents to which $p_1, \ldots, p_s$ divide k. In particular, it can be used to give the following explicit lower bound for the greatest prime factor of x^3-y^2.

Theorem 2. *If x, y are integers, with $(x, y) = 1$, then the greatest prime factor of x^3-y^2 exceeds*

$$10^{-3}(\log\log X)^{1/4},$$

where $X = \max(|x|, |y|)$.

In order to deduce Theorem 2 from (1), we let $\mathfrak{P}$ be either 1 or the greatest prime factor of x^3-y^2, according as $|x^3-y^2| = 1$ or $|x^3-y^2| > 1$, and we let $p_1, \ldots, p_s$ be the primes not exceeding $\mathfrak{P}$.