

On a Linear Diophantine Equation

By

S. Chaładus and A. Schinzel

(Vorgelegt in der Sitzung der math.-nat. Klasse am 15. Oktober 1998
durch des k. M. Andrzej Schinzel)

In memory of Tadeusz Prucnal

Let for vectors $\mathbf{a} = [a_0, \dots, a_k] \in \mathbb{Z}^{k+1}$, $\mathbf{x} = [x_0, \dots, x_k] \in \mathbb{Z}^{k+1}$,
 $b(\mathbf{a}) = \max_{0 \leq i \leq k} |a_i|$, $r(\mathbf{a}) = \prod_{i=0}^k \max\{1, |a_i|\}$, $\mathbf{ax} = a_0x_0 + \dots + a_kx_k$.

M. Drmota [2] has proved the following theorem.

Let $k \geq 1$ and $\mathbf{a} \in (\mathbb{Z} \setminus \{0\})^{k+1}$. Then there exists a non-zero integral solution \mathbf{x} of the equation $\mathbf{ax} = 0$ with

$$r(\mathbf{x}) \leq k r(\mathbf{a})^{1/k} \quad (1)$$

Drmota has further shown that the exponent $1/k$ is optimal for $k = 1, 2$ and that for every k there are vectors $\mathbf{a} \in (\mathbb{Z} \setminus \{0\})^{k+1}$ with arbitrarily large $r(\mathbf{a})$ such that all non-zero integral solutions \mathbf{x} of $\mathbf{ax} = 0$ satisfy

$$r(\mathbf{x}) \gg r(\mathbf{a})^{1/(k+1)} (\log r(\mathbf{a}))^{-(k+1)}$$

We shall show that the exponent $1/k$ in the inequality (1) is optimal for all k and, in fact, there exist vectors $\mathbf{a} \in (\mathbb{Z} \setminus \{0\})^{k+1}$ with arbitrarily large $r(\mathbf{a})$ such that for all $\mathbf{x} \in \mathbb{Z}^{k+1} \setminus \{0\}$ the equation $\mathbf{ax} = 0$ implies

$$r(\mathbf{x}) \geq C(k) r(\mathbf{a})^{1/k}, \quad C(k) > 0,$$

where however, for $k > 2$ the constant $C(k)$ is ineffective. The case $k = 1$ is trivial and for the case $k = 2$ we give an effective proof, which is simpler and shorter than Drmota's. Note that what we denote by k Drmota denotes by $K - 1$.

Theorem. For every k there exist a positive constant $C(k)$ and vectors $\mathbf{a} \in (\mathbb{Z} \setminus \{0\})^{k+1}$ with arbitrarily large $r(\mathbf{a})$ such that for every $\mathbf{x} \in \mathbb{Z}^{k+1} \setminus \{0\}$ the equation $\mathbf{a}\mathbf{x} = 0$ implies

$$r(\mathbf{x}) \geq C(k)r(\mathbf{a})^{1/k}$$

For $k = 2$ one can take

$$C(2) = 2(\sqrt{2} - 1)^{3/2}$$

The proof is based on three lemmas.

Lemma 1. Assume that $1, \alpha_1, \dots, \alpha_\nu$ are real algebraic and linearly independent over the rationals. Then for every positive $\varepsilon < 1$ there exists a number $c(\varepsilon) > 0$ such that for all $\mathbf{x} \in \mathbb{Z}^{\nu+1}$ we have

$$|x_0 + x_1\alpha_1 + \dots + x_\nu\alpha_\nu|r(\mathbf{x}) \geq c(\varepsilon)b(\mathbf{x})^{1-\varepsilon} \quad (2)$$

Proof: By Theorem 1D of Chapter VI of [2] for every $\delta > 0$ there exists a positive $c_0(\alpha_1, \dots, \alpha_\nu, \delta) \leq 1$ such that for all non-zero integers q_1, \dots, q_ν we have

$$|q_1q_2\dots q_\nu|^{1+\delta}\|\alpha_1q_1 + \dots + \alpha_\nu q_\nu\| > c_0(\alpha_1, \dots, \alpha_\nu, \delta),$$

where $\|x\|$ denotes the distance of x to the nearest integer.

It follows hence on taking

$$c_1(\alpha_1, \dots, \alpha_\nu, \delta) = \min_J c_0(J, \delta) \leq 1, \quad (3)$$

where J runs through all non-empty subsets of $\{\alpha_1, \dots, \alpha_\nu\}$, that for all integers x_1, \dots, x_ν we have either $x_1 = \dots = x_\nu = 0$, or

$$\prod_{i=1}^{\nu} \max\{1, |x_i|\}^{1+\delta} \|\alpha_1x_1 + \dots + \alpha_\nu x_\nu\| > c_1(\alpha_1, \dots, \alpha_\nu, \delta). \quad (4)$$

Now, let us take $\alpha_0 = 1$ and put

$$c(\varepsilon) = \min_{0 \leq j \leq \nu} c_1\left(\frac{\alpha_0}{\alpha_j}, \dots, \frac{\alpha_{j-1}}{\alpha_j}, \frac{\alpha_{j+1}}{\alpha_j}, \dots, \frac{\alpha_\nu}{\alpha_j}, \frac{\varepsilon}{\nu}\right) |\alpha_j|. \quad (5)$$

If $x_0 = \dots = x_\nu = 0$ the inequality (2) is true. Otherwise, let

$$b(\mathbf{x}) = |x_j|. \quad (6)$$

If $x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_\nu$ are all equal to 0, then (2) takes the form

$$|x_j\alpha_j||x_j| \geq c(\varepsilon)|x_j|^{1-\varepsilon},$$

which is true since, by (3) and (5), $|\alpha_j| \geq c(\varepsilon)$.

If $x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_\nu$ are not all equal to 0, then the left-hand side of (2) is not less than

$$P = |\alpha_j x_j| \left\| x_0 \frac{\alpha_0}{\alpha_j} + \dots + x_{j-1} \frac{\alpha_{j-1}}{\alpha_j} + x_{j+1} \frac{\alpha_{j+1}}{\alpha_j} + \dots + x_\nu \frac{\alpha_\nu}{\alpha_j} \right\| \\ \times \prod_{\substack{i=1 \\ i \neq j}}^{\nu} \max\{1, |x_i|\}$$

and by (4) applied with ε/ν instead of δ and $\{\alpha_0/\alpha_j, \dots, \alpha_{j-1}/\alpha_j, \alpha_{j+1}/\alpha_j, \dots, \alpha_\nu/\alpha_j\}$ instead of $\{\alpha_1, \dots, \alpha_\nu\}$, and by (6)

$$P \geq |x_j| c(\varepsilon) \prod_{\substack{i=1 \\ i \neq j}}^{\nu} \max\{1, |x_i|\}^{-\varepsilon/\nu} \geq c(\varepsilon) |x_j|^{1-\varepsilon}$$

Lemma 2. Let $f(x) = x^k + c_1 x^{k-1} + \dots + c_k$ be a minimal polynomial of a Pisot number. The recurring sequence given by the conditions

$$a_i = 0 \quad (0 \leq i < k-1), \quad a_{k-1} = 1, \quad a_{m+k} + c_1 a_{m+k-1} + \dots + c_k a_m = 0 \quad (7)$$

satisfies for a certain $c > 0$ and all sufficiently large n , and all integers x_1, \dots, x_k , the relation

$$\max\{1, |x_1 a_{n+1} + \dots + x_k a_{n+k}|\} \prod_{i=1}^k \max\{1, |x_i|\} \geq c |a_{n+1}|. \quad (8)$$

Proof: Let $\vartheta_1, \vartheta_2, \dots, \vartheta_k$ be all the zeros of f and $\vartheta_1 = \vartheta$ be a Pisot number. Hence

$$\vartheta > 1 > \max\{|\vartheta_2|, \dots, |\vartheta_k|\},$$

thus

$$\max\{|\vartheta_2|, \dots, |\vartheta_k|\} = \vartheta^{-2\varepsilon}, \quad \text{where } \varepsilon > 0.$$

By Lemma 1 applied with $\nu = k-1, \alpha_i = \vartheta^i$ there exists a constant $c(\varepsilon) > 0$ such that for all integers x_1, \dots, x_k

$$|x_1 + x_2 \vartheta + \dots + x_k \vartheta^{k-1}| \prod_{i=1}^k \max\{1, |x_i|\} \geq c(\varepsilon) \left(\max_{1 \leq i \leq k} |x_i| \right)^{1-\varepsilon} \quad (9)$$

We shall show that (8) holds for $c = \frac{1}{2}c(\varepsilon)$. Assuming the contrary we would find infinitely many n such that for some integers x_i not all zero

$$\max\{1, |x_1 a_{n+1} + \dots + x_k a_{n+k}|\} \prod_{i=1}^k \max\{1, |x_i|\} < \frac{1}{2}c(\varepsilon)|a_{n+1}|,$$

hence

$$B = \prod_{i=1}^k \max\{1, |x_i|\} < \frac{1}{2}c(\varepsilon)|a_{n+1}|, \quad (10)$$

$$M = \max_{1 \leq i \leq k} |x_i| < \frac{1}{2}c(\varepsilon)|a_{n+1}| \quad (11)$$

and

$$B \left| x_1 + x_2 \vartheta + \dots + x_k \vartheta^{k-1} + x_2 \left(\frac{a_{n+2}}{a_{n+1}} - \vartheta \right) + \dots + x_k \left(\frac{a_{n+k}}{a_{n+1}} - \vartheta^{k-1} \right) \right| < \frac{1}{2}c(\varepsilon).$$

By (9) it follows that

$$B \left| \sum_{i=2}^k x_i \left(\frac{a_{n+i}}{a_{n+1}} - \vartheta^{i-1} \right) \right| > \frac{1}{2}c(\varepsilon)M^{1-\varepsilon},$$

and by (10),

$$\left| \sum_{i=2}^k x_i (a_{n+i} - \vartheta^{i-1} a_{n+1}) \right| > M^{1-\varepsilon} \quad (12)$$

However, since ϑ_i are all distinct we have from the theory of recurring series

$$a_n = \sum_{i=1}^k \alpha_i \vartheta_i^n$$

and, since $a_0 = \dots = a_{k-2} = 0, a_{k-1} = 1, \alpha \neq 0$. Indeed, otherwise the system of $k-1$ homogeneous equations for $\alpha_2, \dots, \alpha_k$ would give $\alpha_2 = \dots = \alpha_k = 0$, hence $a_{k-1} = 0$, a contradiction. Hence

$$a_n = \alpha_1 \vartheta^n + O(\vartheta^{-2n\varepsilon}) \quad (13)$$

and

$$|a_{n+i} - \vartheta^{i-1} a_{n+1}| \leq C_1 |a_{n+1}|^{-2\varepsilon} (i \leq k)$$

for a suitable constant C_1 .

Thus, the left hand side of (12) does not exceed

$$M(k-1)C_1|a_{n+1}|^{-2\varepsilon}$$

and we obtain

$$(k-1)C_1M^\varepsilon > |a_{n+1}|^{2\varepsilon}$$

which contradicts (11) for n (and hence $|a_{n+1}|$) sufficiently large.

Lemma 3. *Let in the notation of Lemma 2: $k = 2, c_1 < 0, c_2 = -1$, and let $A = \mathbb{Z}^2 \setminus \{[0, 0]\}$. The recurring sequence given by the conditions (7) satisfies for all $n \geq 0$ the equality*

$$\min_{[x_1, x_2] \in A} M_n(x_1, x_2) = \max\{1, |c_1|a_n\}, \quad (14)$$

where

$$M_n(x_1, x_2) = \max\{1, |a_{n+1}x_1 + a_{n+2}x_2|\} \max\{1, |x_1|\} \max\{1, |x_2|\}.$$

Proof First we observe that if $[y_1, y_2] \in \mathbb{Z}^2, y_1y_2 < 0$ and $|y_1| \geq |y_2|$ then

$$\frac{|y_2 - |c_1||y_1||}{|y_2|} \geq |c_1| + 1. \quad (15)$$

Now, we proceed to prove (14) by induction on n . For $n = 0$ we have trivially

$$M_0(x_1, x_2) \geq 1 = M_0(1, 0).$$

Assume that (13) holds for the index n . By (7)

$$a_{n+2}x_1 + a_{n+3}x_2 = a_{n+1}y_1 + a_{n+2}y_2,$$

where $y_1 = x_2, y_2 = x_1 + |c_1|x_2$ and $[x_1, x_2] \in A$ implies $[y_1, y_2] \in A$. If $y_2 = 0$ we get $x_1 = -|c_1|y_1$, hence $y_1 \neq 0$ and

$$M_{n+1}(x_1, x_2) = |c_1|a_{n+1}y_1^2 \geq |c_1|a_{n+1}$$

with the equality attained for $y_1 = 1$, i.e. $x_2 = 1, x_1 = -|c_1|$.

If $y_2 \neq 0$ and $y_1y_2 \geq 0$ or $y_1y_2 < 0$, but $|y_1| < |y_2|$ then

$$M_{n+1}(x_1, x_2) \geq |a_{n+1}y_1 + a_{n+2}y_2| \geq a_{n+2} \geq |c_1|a_{n+1}.$$

If $y_1y_2 < 0$ and $|y_1| \geq |y_2|$ then

$$M_{n+1}(x_1, x_2) = M_n(y_1, y_2) \cdot \frac{|y_2 - |c_1||y_1||}{|y_2|}$$

and, by the inductive assumption and (15),

$$M_{n+1}(x_1, x_2) \geq \max\{1, |c_1|a_n\}(|c_1| + 1) \geq |c_1|a_{n+1}.$$

Proof of the theorem: For every k the set S_k of Pisot numbers of degree k is non-empty (see [1], Theorem 5.2.2). Since S_k has no finite limit points it has the least element ϑ . We take for $f(x)$ in Lemma 2 the minimal polynomial of ϑ and put

$$\mathbf{a} = [1, a_{n+1}, a_{n+2}, \dots, a_{n+k}]$$

where the sequence a_n is determined by the conditions (7). By the formula (13)

$$a_{n+1} = \alpha_1 \vartheta^{n+1} + O(\vartheta^{-2\varepsilon(n+1)})$$

and for n large enough

$$r(\mathbf{a}) = |\alpha_1|^k \vartheta^{k(n+1) + \binom{k}{2}} (1 + O(\vartheta^{-(n+1)(1+2\varepsilon)})),$$

hence

$$|a_{n+1}| \geq C_2 r(\mathbf{a})^{1/k}, \quad C_2 \text{ positive, independent of } n. \quad (16)$$

On the other hand, for every $\mathbf{x} \in \mathbb{Z}^{k+1} \setminus \{\mathbf{0}\}$ the condition $\mathbf{a}\mathbf{x} = 0$ implies

$$x_0 = -a_{n+1}x_1 - \dots - a_{n+k}x_k,$$

hence by (8)

$$r(\mathbf{x}) \geq c|a_{n+1}|. \quad (17)$$

It follows from (16) and (17) that one can take

$$C(k) = cC_2.$$

It remains to consider $k = 2$. Then taking in Lemma 3:

$$c_1 = -2 \text{ and putting}$$

$$\mathbf{a} = [1, a_{n+1}, a_{n+2}],$$

where a_n is determined by the condition (7) we find

$$a_n = \frac{(1 + \sqrt{2})^n - (1 - \sqrt{2})^n}{2\sqrt{2}}$$

and for n odd

$$r(\mathbf{a}) < \frac{(1 + \sqrt{2})^{2n+3}}{8} < (1 + \sqrt{2})^3 a_n^2. \quad (18)$$

On the other hand, for every $\mathbf{x} \in \mathbb{Z}^3 \setminus \{\mathbf{0}\}$ the condition $\mathbf{a}\mathbf{x} = 0$ implies

$$x_0 = -a_{n+1}x_1 - a_{n+2}x_2,$$

hence, by (14),

$$r(\mathbf{x}) \geq 2a_n,$$

and, by (18)

$$r(\mathbf{x}) > 2(\sqrt{2} + 1)^{-3/2} r(\mathbf{a})^{1/2} = 2(\sqrt{2} - 1)^{3/2} r(\mathbf{a})^{1/2}$$

References

- [1] Bertin, M. J., Decomps-Guilloux, A., Grandet-Hugot, M., Pathiaux-Delafose, M., Schreiber, J. P.: *Pisot and Salem Numbers*. Basel: Birkhäuser 1992.
- [2] Drmota, M.: *On linear Diophantine equations and Fibonacci numbers*. J. Number Theory **49**, 315–328 (1993).
- [3] Schmidt, W.: *Diophantine approximation*. Lecture Notes in Mathematics, vol. 785. Berlin Heidelberg, New York: Springer 1980.

Authors' addresses: Prof. Dr. Andrzej Schinzel, Instytut Matematyczny, Polskiej Akademii Nauk, P.O. Box 137, P-00-950 Warszawa, Poland; Dr. S. Chaładus, Michałowski 14 m.8, PL-42200 Częstochowa, Poland.

ZOBODAT - www.zobodat.at

Zoologisch-Botanische Datenbank/Zoological-Botanical Database

Digitale Literatur/Digital Literature

Zeitschrift/Journal: [Sitzungsberichte der Akademie der Wissenschaften
mathematisch-naturwissenschaftliche Klasse](#)

Jahr/Year: 1998

Band/Volume: [207_2](#)

Autor(en)/Author(s): Chaladus S., Schinzel Andrzej

Artikel/Article: [On a Linear Diophantine Equation. 95-101](#)