

ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

A. BALOG

A. PERELLI

Diophantine approximation by square-free numbers

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4^e série, tome 11,
n° 3 (1984), p. 353-359

http://www.numdam.org/item?id=ASNSP_1984_4_11_3_353_0

© Scuola Normale Superiore, Pisa, 1984, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (<http://www.sns.it/it/edizioni/riviste/annaliscienze/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Diophantine Approximation by Square-Free Numbers (*).

A. BALOG - A. PERELLI

Introduction.

This paper is devoted to the proof of the following

THEOREM 1. *Let $\varepsilon > 0$ be any fixed number. Then for every irrational number α there are infinitely many square-free numbers s with*

$$(1) \quad \|\alpha s\| < s^{-1/2+\varepsilon}.$$

The classical way of investigating this kind of problem is to use a Fourier-expansion argument and then some estimates for exponential sums. In the paper [1] the first named author has developed an alternative method, based on character sums estimates, in connection with the problem of the distribution of αp modulo one. Theorem 1 is apparently stronger than the corresponding result one can get by the Fourier-expansion method.

The underlying idea is very simple. Let a/q be a convergent to α , in the sense that

$$(2) \quad \alpha = \frac{a}{q} + \frac{\theta}{q^2}, \quad (a, q) = 1, \quad |\theta| < 1.$$

In fact, for every irrational number α we have infinitely many convergents of the form (2), by the Dirichlet approximation theorem. Let \mathcal{S} be an arbitrary set of integers (in the present application \mathcal{S} will be the set of the square-free numbers) and let $1 < L < q < X < q^2$ be parameters. If there is an $s \in \mathcal{S}$, $s < X$, satisfying one of the congruences

$$(3) \quad as \equiv f \pmod{q}, \quad 1 < f < L$$

(*) The present paper was written when the first named author was a C.N.R. Visiting Professor at the University of Genova.

Pervenuto alla Redazione l'11 Novembre 1983.

then

$$(4) \quad \alpha_s = n + \frac{f}{q} + \frac{\theta_s}{q^2},$$

where n is an integer, so that

$$(5) \quad \|\alpha_s\| < \frac{L}{q} + \frac{X}{q^2}.$$

It is reasonable to choose

$$(6) \quad L = q^\beta, \quad X = Lq = q^{1+\beta}, \quad 0 \leq \beta < 1.$$

From (5) we have

$$(7) \quad \|\alpha_s\| < \frac{2}{q^{1-\beta}} = \frac{2}{X^{(1-\beta)/(1+\beta)}} \leq \frac{2}{s^{(1-\beta)/(1+\beta)}}.$$

It is clear that the smaller β is the better result we get.

In other words, a result of type (1) depends on the average distribution of S in short arithmetical progressions. This problem may be handled by using the orthogonality of characters and mean value theorems for Dirichlet polynomials.

Our result may be expressed in another way. Let $1 \leq B \leq A$ be integers with $(A, B) = 1$. It is well known that the integers

$$(8) \quad Am + Bn$$

cover all the integers when m and n run over all the integers. But when m and n run only over all the positive integers then (8) covers all the numbers $> AB$ and only certain numbers between $A + B$ and AB . We may ask for the order of magnitude of the smallest $s \in S$ of the form (8). As $s = Am + Bn$ implies that

$$(9) \quad s \equiv Bn \pmod{A},$$

a result of the form (3) gives a solution of this problem as well.

One may prove the following

THEOREM 2. *Let $\varepsilon > 0$ be any fixed number. Then for every pair of integers A, B satisfying $1 \leq B \leq A$, $(A, B) = 1$ there is a square-free number s satisfying*

$$(10) \quad s = Am + Bn \leq AB^{1/3+\varepsilon}, \quad m \geq 1, n \geq 1.$$

One may use the present method for other sets S , and it turns out that the method works only for quite dense sets, like primes ([1]) and square-free numbers, but not for thin sets, such as the squares.

For instance, we state here without proof the following

THEOREM 3. *Let $\varepsilon > 0$ be any fixed number and let S be the set of all integers which are sum of two squares. Then for every irrational number α there are infinitely many $s \in S$ with*

$$(11) \quad \|\alpha s\| < s^{-1/2+\varepsilon}$$

and for every pair of integers A, B satisfying $1 < B < A$, $(A, B) = 1$ there is an $s \in S$ such that

$$(12) \quad s = Am + Bn < AB^{1/3+\varepsilon}, \quad m \geq 1, n \geq 1.$$

It is worth noting that in (10) it is sufficient to assume that (A, B) is square-free, and it is also possible to weaken the condition $(A, B) = 1$ in (12).

Finally we note that the result of Heath-Brown [3] concerning the least square-free number in an arithmetic progression implies only $5/13$ in place of $1/2$ in (1).

PROOF OF THEOREM 1. We prove only Theorem 1, Theorem 2 being an easy consequence of our arguments. Theorem 3 may be proved using the same techniques as in Theorem 1.

According to our arguments in the Introduction it is sufficient to prove (3), and this follows from

$$(13) \quad R = \sum_{\substack{f \leq L \\ (f,q)=1}} \sum_{\substack{s \leq X \\ as \equiv f \pmod{q}}} \mu^2(s) > 0$$

where L and X satisfy (6) and β is any number satisfying

$$(14) \quad \beta > \frac{1}{3}.$$

Note that the condition $(f, q) = 1$ in (13) is not necessary but it makes possible some simplifications. The rest of this paper is devoted to proving (13).

Our starting point is the relation

$$(15) \quad \mu^2(s) = \sum_{d^2|s} \mu(d).$$

Let $1 < D_0 < X^{1/2}$ be a parameter. We have

$$(16) \quad R = \sum_{\substack{f \leq L \\ (f,a)=1}} \sum_{\substack{s \leq X \\ as \equiv f \pmod{a}}} \sum_{d^2 | s} \mu(d) \\ = \sum_{\substack{f \leq L \\ (f,a)=1}} \left(\sum_{d \leq D_0} + \sum_{d > D_0} \right) \mu(d) \sum_{\substack{m \leq X/d^2 \\ ad^2m \equiv f \pmod{a}}} 1 = R_1 + R_2,$$

say.

As $(f, q) = 1$ the innermost sum in each of R_1 and R_2 is zero unless $(d, q) = 1$. But when $(a, q) = (d^2, q) = 1$ we have trivially

$$(17) \quad \sum_{\substack{m \leq X/d^2 \\ ad^2m \equiv f \pmod{a}}} 1 = \frac{X}{d^2q} + O(1),$$

so that

$$(18) \quad R_1 = \frac{X}{q} \left(\sum_{\substack{f \leq L \\ (f,a)=1}} 1 \right) \left(\sum_{\substack{d \leq D_0 \\ (d,a)=1}} \frac{\mu(d)}{d^2} \right) + O(LD_0).$$

Using the elementary facts

$$(19) \quad \sum_{\substack{f \leq L \\ (f,a)=1}} 1 = \frac{\varphi(q)}{q} L + O(d(q)),$$

and

$$(20) \quad \sum_{\substack{d \leq D_0 \\ (d,a)=1}} \frac{\mu(d)}{d^2} = \prod_{p|a} (1 - p^{-2}) + O(D_0^{-1})$$

we get

$$(21) \quad R_1 = \frac{6}{\pi^2} \prod_{p|a} (1 + p^{-1})^{-1} \frac{XL}{q} + O\left(LD_0 + \frac{Xd(q)}{q} + \frac{XL}{qD_0}\right).$$

Next we turn to the contribution of R_2 . We have trivially that

$$(22) \quad |R_2| \leq \log X \max R(D, D')$$

where

$$(23) \quad R(D, D') = \sum_{\substack{f \leq L \\ (f,a)=1}} \sum_{\substack{D < d \leq D' \\ (d,a)=1}} \sum_{\substack{m \leq X/d^2 \\ ad^2m \equiv f \pmod{a}}} 1$$

and the max is extended to the pairs D, D' satisfying

$$(24) \quad D_0 \leq D < D' \leq 2D \leq X^{1/2}.$$

By the orthogonality of Dirichlet characters we have

$$(25) \quad R(D, D') = \frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \chi(a) \sum_{f \leq L} \bar{\chi}(f) \sum_{D < d \leq D'} \chi(d^2) \sum_{m \leq X/D^2} \chi(m) \\ \ll \frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \left| \sum_{f \leq L} \chi(f) \sum_{m \leq X/D^2} \chi(m) \right| \left| \sum_{D < d \leq D'} \chi(d^2) \right|.$$

Taking

$$(26) \quad a_n = \sum_{\substack{f \leq L \\ n = fm \\ m \leq X/D^2}} 1 \leq d(n)$$

and using the Cauchy-Schwarz inequality we get

$$(27) \quad R(D, D') \ll \left(\frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \left| \sum_{n \leq XL/D^2} a_n \chi(n) \right|^2 \right)^{1/2} \\ \cdot \left(\frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \left| \sum_{D < d \leq D'} \chi^2(d) \right|^2 \right)^{1/2}.$$

We now use the mean-value theorem for Dirichlet polynomials (see Th. 6.2 of [4]) in the form

$$\frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \left| \sum_{n \leq N} b_n \chi(n) \right|^2 \leq \left(1 + \frac{N}{q} \right) \sum_{n \leq N} |b_n|^2.$$

For the second factor on the right of (26) we note that the equation

$$(28) \quad \chi^2 = \chi_1$$

(where χ_1 is a given character mod q and χ is the variable) has at most q^η solutions, where $\eta > 0$ is arbitrary. This follows at once from the fact that the group of the characters mod q is isomorphic to the group of the reduced residue classes mod q (see for example Th. 7.1 of [2]), and the congruence

$$x^2 \equiv c \pmod{q}$$

has at most

$$2^{v(a)} \ll q^\eta, \quad \eta > 0 \text{ arbitrary,}$$

solutions. Thus we get

$$\begin{aligned}
 (29) \quad R(D, D') &\ll q^{\eta/2} \left(\frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \left| \sum_{n \leq XL/D^2} a_n \chi(n) \right|^2 \right)^{1/2} \\
 &\cdot \left(\frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \left| \sum_{D < d \leq D'} \chi(d) \right|^2 \right)^{1/2} \leq q^\eta \left(\left(1 + \frac{XL}{qD^2} \right) \frac{XL}{D^2} \left(1 + \frac{D}{q} \right) D \right)^{1/2} \\
 &\ll q^\eta \left(\frac{X^{1/2} L^{1/2}}{D^{1/2}} + \frac{XL}{q^{1/2} D^{3/2}} \right)
 \end{aligned}$$

and from (22) we obtain

$$(30) \quad R_2 \ll q^\eta \left(\frac{X^{1/2} L^{1/2}}{D_0^{1/2}} + \frac{LX}{q^{1/2} D_0^{3/2}} \right)$$

for any $\eta > 0$. The optimal choice of D_0 is

$$(31) \quad D_0 = q^{1/3+2\eta},$$

and from (16), (21), (30) and (6) we have

$$\begin{aligned}
 R &= \frac{6}{\pi^2} \prod_{p|q} (1 + p^{-1})^{-1} \frac{LX}{q} + O \left(Lq^{1/3+2\eta} + \frac{LX}{q^{1+\eta}} + \frac{L^{1/2} X^{1/2}}{q^{1/6}} \right) \\
 &= \frac{6}{\pi^2} \prod_{p|q} (1 + p^{-1})^{-1} q^{2\beta} + O(q^{1/3+\beta+2\eta} + q^{2\beta-\eta}).
 \end{aligned}$$

As

$$\prod_{p|q} (1 + p^{-1}) \ll \log \log q$$

we have, for all $\beta > \frac{1}{3}$, that

$$R \sim \frac{6}{\pi^2} \prod_{p|q} (1 + p^{-1})^{-1} q^{2\beta} > 0,$$

which completes the proof.

Added in Proof.

In the meantime, we have been informed by Professor Heath-Brown that he has improved the exponent $-\frac{1}{3}$ in our Theorem 1 to $-\frac{2}{3}$. However, his method does not seem to extend to the more general situations covered by ours.

REFERENCES

- [1] A. BALOG, *A remark on the distribution of $x^p \pmod{one}$* , to appear.
- [2] W. J. ELLISON, *Les Nombres Premiers*, Hermann, Paris, 1975.
- [3] D. R. HEATH-BROWN, *The least square-free number in an arithmetical progression*, *J. reine angew. Math.*, **332** (1982), pp. 204-220.
- [4] H. L. MONTGOMERY, *Topics in Multiplicative Number Theory*, Springer Lecture Notes, n°. 227, 1971.

Mathematical Institute of the
Hungarian Academy of Sciences
Reáltanoda u. 13-15
H-1053 Budapest, Hungary

Istituto di Matematica
Università di Genova
Via L. B. Alberti 4
16132 Genova, Italy