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 4e série, tome 11, nº 3 (1984), p. 353-359

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

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*

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

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

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

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

$$as \equiv f \pmod{q}, \quad 1 \leqslant f \leqslant L \tag{3}$$

(*) 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

$$\alpha s = n + \frac{f}{q} + \frac{\theta s}{q^2}, \tag{4}$$

where n is an integer, so that

$$\|\alpha s\| < \frac{L}{q} + \frac{X}{q^2}. \tag{5}$$

It is reasonable to choose

$$L = q^{\beta}, \qquad X = Lq = q^{1+\beta}, \qquad 0 \leqslant \beta < 1. \tag{6}$$

From (5) we have

$$\|\alpha s\| < \frac{2}{q^{1-\beta}} = \frac{2}{X^{(1-\beta)/(1+\beta)}} \leqslant \frac{2}{s^{(1-\beta)/(1+\beta)}}. \tag{7}$$

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 $1 \leqslant B \leqslant A$ be integers with $(A, B) = 1$. It is well known that the integers

$$Am + Bn \tag{8}$$

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

$$s \equiv Bn \pmod{A}, \tag{9}$$

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 $1 \leqslant B \leqslant A$, $(A, B) = 1$ there is a square-free number s satisfying*

$$s = Am + Bn \leqslant AB^{1/3+\varepsilon}, \qquad m \geqslant 1, \ n \geqslant 1. \tag{10}$$

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*

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

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

$$s = Am + Bn \leqslant AB^{1/3+\varepsilon}, \qquad m \geqslant 1,\ n \geqslant 1\,. \tag{12}$$

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

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

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

$$\beta > \tfrac{1}{3}\,. \tag{14}$$

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

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

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

$$R = \sum_{\substack{f \leqslant L \\ (f,q)=1}} \sum_{\substack{s \leqslant X \\ as \equiv f \pmod q}} \sum_{d^2 | s} \mu(d) \tag{16}$$

$$= \sum_{\substack{f \leqslant L \\ (f,q)=1}} \Big(\sum_{d \leqslant D_0} + \sum_{d > D_0} \Big) \mu(d) \sum_{\substack{m \leqslant X/d^2 \\ ad^2 m \equiv f \pmod q}} 1 = R_1 + R_2 ,$$

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

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

so that

$$R_1 = \frac{X}{q} \Big(\sum_{\substack{f \leqslant L \\ (f,q)=1}} 1 \Big) \Big(\sum_{\substack{d \leqslant D_0 \\ (d,q)=1}} \frac{\mu(d)}{d^2} \Big) + O(LD_0) . \tag{18}$$

Using the elementary facts

$$\sum_{\substack{f \leqslant L \\ (f,q)=1}} 1 = \frac{\varphi(q)}{q} L + O\big(d(q)\big) , \tag{19}$$

and

$$\sum_{\substack{d \leqslant D_0 \\ (d,q)=1}} \frac{\mu(d)}{d^2} = \prod_{p \nmid q} (1 - p^{-2}) + O(D_0^{-1}) \tag{20}$$

we get

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

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

$$|R_2| \leqslant \log X \max R(D, D') \tag{22}$$

where

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

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

$$D_0 \leqslant D < D' \leqslant 2D \leqslant X^{1/2}. \tag{24}$$

By the orthogonality of Dirichlet characters we have

$$\begin{aligned} R(D, D') &= \frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}\, q)} \chi(a) \sum_{f\leqslant L} \bar{\chi}(f) \sum_{D<d\leqslant D'} \chi(d^2) \sum_{m\leqslant X/D^2} \chi(m) \\ &\ll \frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}\, q)} \Big|\sum_{f\leqslant L} \chi(f) \sum_{m\leqslant X/D^2} \chi(m)\Big| \Big|\sum_{D<d\leqslant D'} \chi(d^2)\Big|. \end{aligned} \tag{25}$$

Taking

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

and using the Cauchy-Schwarz inequality we get

$$\begin{aligned} R(D, D') \ll & \left(\frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}\, q)} \Big|\sum_{n\leqslant XL/D^2} a_n \chi(n)\Big|^2\right)^{1/2} \\ & \cdot \left(\frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}\, q)} \Big|\sum_{D<d\leqslant D'} \chi^2(d)\Big|^2\right)^{1/2}. \end{aligned} \tag{27}$$

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

$$\frac{1}{\varphi(q)} \sum_{\chi(\mathrm{mod}\, q)} \Big|\sum_{n\leqslant N} b_n \chi(n)\Big|^2 \leqslant \left(1 + \frac{N}{q}\right) \sum_{n\leqslant N} |b_n|^2.$$

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

$$\chi^2 = \chi_1 \tag{28}$$

(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

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

solutions. Thus we get

$$R(D, D') \ll q^{\eta/2}\left(\frac{1}{\varphi(q)}\sum_{\chi(\text{mod}\, q)}\left|\sum_{n\leq XL/D^2} a_n\chi(n)\right|^2\right)^{1/2} \tag{29}$$

$$\cdot\left(\frac{1}{\varphi(q)}\sum_{\chi(\text{mod}\, q)}\left|\sum_{D<d\leq D'}\chi(d)\right|^2\right)^{1/2} \leq q^{\eta}\left(\left(1+\frac{XL}{qD^2}\right)\frac{XL}{D^2}\left(1+\frac{D}{q}\right)D\right)^{1/2}$$

$$\ll q^{\eta}\left(\frac{X^{1/2}L^{1/2}}{D^{1/2}}+\frac{XL}{q^{1/2}D^{3/2}}\right)$$

and from (22) we obtain

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

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

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

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

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

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 meant-time, we have been informed by Professor Heath-Brown that he has improved the exponent $-\frac{1}{2}$ 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 αp mod. 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