Further we have

$$(4.7)\qquad \sum_{L_1<p\le L_2}\frac{\log p}{p^2}\varrho^k\left(\frac{u_1}{k}\right)=\sum_{Z_1<p\le Z_2}\frac{\log p}{p^2}\varrho^k\left(\frac{u_1}{k}\right)\left(1+O\left(\frac{\log_3 x}{\log_2 x}\right)\right)$$
$$=\int_{Z_1}^{Z_2}\frac{\log z}{z^2}\varrho^k\left(\frac{\log x}{k\log z}\right)d\pi(z)\left(1+O\left(\frac{\log_3 x}{\log_2 x}\right)\right).$$

As for G_2 we have similarly $G_3 \ll (\log_3 x/\log_2 x)G_2$. Combining (4.1)–(4.7) completes the proof of Theorem 2.

References

[1] K. Alladi, *Asymptotic estimates of sums involving the Moebius function*. II, Trans. Amer. Math. Soc. 272 (1982), 87–105.

[2] — *The Turán–Kubilius inequality for integers without large prime factors*, J. Reine Angew. Math. 335 (1982), 180–196.

[3] N. G. de Bruijn, *The asymptotic behaviour of a function occurring in the theory of primes*, J. Indian Math. Soc. (N.S.) 15(1951), 25–32.

[4] P. Erdős, A. Ivić and C. Pomerance, *On sums involving reciprocals of the largest prime factor of an integer*, Glas. Mat. 21(41) (1986), 283–300.

[5] A. Hildebrand, *On the number of positive integers $\le x$ and free of prime factors $>y$*, J. Number Theory 22 (1986), 289–307.

[6] A. Hildebrand and G. Tenenbaum, *On integers free of large prime factors*, Trans. Amer. Math. Soc. 296 (1986), 265–290.

[7] L. K. Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin–Heidelberg–New York 1982.

[8] — *Estimation of an integral* (in Chinese), Sci. Sinica 2 (1951), 393–402.

[9] A. Ivić, *On squarefree numbers with restricted prime factors*, Studia Sci. Math. Hungar. 20 (1985), 189–192.

[10] — *On some estimates involving the number of prime divisors of an integer*, Acta Arith. 49 (1987), 21–33.

[11] T. Z. Xuan, *The average order of d(n) over integers free of large prime factors* (in Chinese), Chin. Ann. Math. Ser. A, to appear.

[12] — *Estimates of certain sums involving reciprocals of the largest prime factor of an integer* (in Chinese), J. Beijing Normal Univ. (N.S.) 1988, No. 1, 11–16.

DEPARTMENT OF MATHEMATICS
BEIJING NORMAL UNIVERSITY
Beijing, China

Received on 4.10.1988
and in revised form on 17.1.1989 (1875)

ACTA ARITHMETICA
LV (1990)

B_2-sequences whose terms are squares

by

J. CILLERUELO (Madrid)

Introduction. A sequence of integers $1 \le a_1 < a_2 < \ldots$ is called a *B_2-sequence* if the sums a_i+a_j are all different. Sidon asked for a B_2- sequence for which a_k increases as slowly as possible. There is a trivial argument which allows us to construct such a B_2-sequence with $a_k \ll k^3$ for all k. For a long time, this bound was the best known one until Ajtai, Komlós and Szemerédi [1] showed, with an ingenious method, the existence of a B_2-sequence such that $a_k/k^3 \to 0$. However, this result is far from Erdős' conjecture on the existence, for each $\varepsilon > 0$, of a B_2-sequence with $a_k \ll k^{2+\varepsilon}$ [3].

In this paper we deal with B_2-sequences of squares, in other words, sequences of integers $1 \le a_1 < a_2 < \ldots$ where the sums $a_i^2+a_j^2$ are all distinct.

Again, there is an easy argument giving us, for each $\varepsilon > 0$, a sequence such that $a_k \ll k^{2+\varepsilon}$ and where the sums $a_i^2+a_j^2$ are all different. Apparently, there is not a simple argument to improve this result.

The purpose of this paper is to remove ε, using a new method developed by Javier Cilleruelo and Antonio Córdoba in [2].

THEOREM. *There exists a sequence $A=\{a_k\}$, $a_k \ll k^2$, such that the sums $a_i^2+a_j^2$ are all different.*

Proof. Consider the sets $I_j=\{a;\ 6^j \le a < 6^j+6^{j/2},\ a\equiv 2 \pmod 6\}$ and $I=\bigcup_{j=1}^{\infty} I_j$. The sequence A will be given by the set I except for a few numbers that we have to eliminate: $A=\bigcup_{j=1}^{\infty} A_j$, $A_j \subset I_j$.

Construction of A_k. Once we have chosen the A_j, $j<k$, we shall pick the members of A_k from among the elements of I_k, with a few exceptions, to avoid $a^2+b^2=c^2+d^2$, with $a, b, c, d \in \bigcup_{j=1}^{k} A_j$.

LEMMA 1. *Let a, b, c, d belong respectively to I_k, I_l, I_j, I_m, where $k \ge j \ge m \ge l$, and suppose $a^2+b^2=c^2+d^2$, $a>c>d>b$. Then we have:*

(i) $k=j$.

(ii) *If $l<m$, $k/2 \le m \le 3k/4$.*

Proof. (i) Since $k \geqslant j \geqslant m \geqslant l$, we have

$$6^{2k} < a^2+b^2 = c^2+d^2 < 2(6^j+6^{j/2})^2 < 8\cdot 6^{2j},$$

so $6^{2(k-j)} < 8$ and this is possible only if $k \leqslant j$.

(ii) By (i) we know that a and d belong to the same I_k. Hence

$$4\cdot 6^k < (a-c)(a+c) = (d-b)(d+b) < (6^m+6^{m/2})2(6^m+6^{m/2})$$
$$= 2(6^m+6^{m/2})^2 < 8\cdot 6^{2m},$$

therefore $6^k < 2\cdot 6^{2m}$ and so $m \geqslant k/2$.

Now, if $l<m$,

$$6^{k/2}2(6^k+6^{k/2}) > (a-c)(a+c) = (d-b)(d+b) > (6^m-(6^l+6^{l/2}))6^m$$

$$\Rightarrow 4\cdot 6^{3k/2} \geqslant (6^m-6^m/3)6^m \Rightarrow 6\cdot 6^{3k/2} > 6^{2m} \Rightarrow m \leqslant 3k/4. \blacksquare$$

LEMMA 2. *Let $n = a^2+b^2 = c^2+d^2$, $n \equiv 0$ (4), $\varphi_1 = \arctan(b/a)$ $\varphi_2 = \arctan(d/c)$. Then there exist a_1, b_1, c_1, d_1 such that $n = (a_1^2+b_1^2)(c_1^2+d_1^2)$ with $\tan((\varphi_1-\varphi_2)/2) = b_1/a_1$ and $\tan((\varphi_1+\varphi_2)/2) = d_1/c_1$.*

Proof. Put

$$\alpha = \frac{(a-c,\, b-d)}{2}, \quad \beta = \frac{a+c}{d-b}\alpha, \quad \gamma = \frac{a-c}{2\alpha}, \quad \delta = \frac{b-d}{2\alpha}.$$

It follows from $a^2+b^2 = c^2+d = n$, $a \equiv b \equiv c \equiv d \equiv 0 \pmod 2$ that

$$\alpha, \beta, \gamma, \delta \in \mathbf{Z}, \quad n = (\alpha^2+\beta^2)(\gamma^2+\delta^2)$$

and

$$\frac{2\alpha\beta}{\alpha^2-\beta^2} = \frac{bc-da}{ac+bd} = \tan(\varphi_1-\varphi_2),$$

$$\frac{2\gamma\delta}{\gamma^2-\delta^2} = \frac{bc+da}{ac-bd} = \tan(\varphi_1+\varphi_2).$$

Hence

$$\tan\frac{\varphi_1-\varphi_2}{2} = \frac{\beta}{\alpha} \quad \text{or} \quad -\frac{\alpha}{\beta},$$

$$\tan\frac{\varphi_1+\varphi_2}{2} = \frac{\delta}{\gamma} \quad \text{or} \quad -\frac{\gamma}{\delta}.$$

Choosing $a_1 = \alpha$, $b_1 = \beta$ or $a_1 = \beta$, $b_1 = -\alpha$ and $c_1 = \gamma$, $d_1 = \delta$ or $c_1 = \delta$, $d_1 = -\gamma$ accordingly we satisfy all the requirements of the Lemma. $\blacksquare$

End of the proof of the Theorem. For l, m fixed, $l \leqslant m$, we count how many integers can be expressed in two different ways as a sum of two squares $n = a^2+b^2 = c^2+d^2$, $a, c \in I_k$ (by Lemma 1(i)), $b \in I_l$, $d \in I_m$.

If $n = a^2+b^2 = c^2+d^2$, $a, c \in I_k$, $b \in I_l$, $d \in I_m$, we can describe the equality with two lattice points (a, b) and (c, d) placed on the same circle. An easy geometric observation gives the following estimate for which we use the notation introduced in Lemma 2:

$$|\tan((\varphi_1-\varphi_2)/2) - \Phi_1| < \tfrac{1}{2}\cdot 6^{m/2-k}, \quad |\tan((\varphi_1+\varphi_2)/2) - \Phi_2| < \tfrac{1}{2}\cdot 6^{m/2-k},$$

where

$$\Phi_1 = \tan\big((\arctan(6^{m-k}) - \arctan(6^{l-k}))/2\big),$$
$$\Phi_2 = \tan\big((\arctan(6^{m-k}) + \arctan(6^{l-k}))/2\big).$$

So, there will be a_1, b_1, c_1, d_1 such that $n = (a_1^2+b_1^2)(c_1^2+d_1^2)$ and

$$(*) \quad \begin{cases} |b_1/a_1 - \Phi_1| < \tfrac{1}{2}\cdot 6^{m/2-k}, \\ |d_1/c_1 - \Phi_2| < \tfrac{1}{2}\cdot 6^{m/2-k}, \\ 6^{2k}+6^{2m} \leqslant (a_1^2+b_1^2)(c_1^2+d_1^2) \leqslant (6^k+6^{k/2})^2 + (3^l+3^{l/2})^2. \end{cases}$$

Next, we count how many a_1, b_1, c_1, d_1 satisfy $(*)$. We have two different cases: $l = m$ and $l < m$.

In the case $l = m$ condition $(*)$ is

$$|b_1/a_1| < \tfrac{1}{2}\cdot 6^{m/2-k}, \quad |d_1/c_1 - 1/6^{k-m}| < \tfrac{1}{2}\cdot 6^{m/2-k},$$
$$6^{2k}+6^{2m} \leqslant (a_1^2+b_1^2)(c_1^2+d_1^2) \leqslant (6^k+6^{k/2})^2 + (6^l+6^{l/2})^2.$$

If $b_1 = 0$, then $\tan((\varphi_1-\varphi_2)/2) = 0$ and $\varphi_1 = \varphi_2$; the lattice points (a, b) and (c, d) are the same.

If $m = k$ and $d_1/c_1 = 1$, then $\varphi_1+\varphi_2 = \pi/2$ and the lattice points (a, b) and (c, d) are symmetric with respect to the diagonal.

Finally, if $m < k$ and $d_1/c_1 = 1/6^{k-m}$, then we must have $(b+d)/(a+c) = 1/6^{k-m}$, but this is impossible because $a+c \equiv 4$ (mod 6).

Then

$$0 < |b_1| < \tfrac{1}{2}a_1 6^{m/2}, \quad 0 < |d_1 3^{k-m} - c_1| < \tfrac{1}{2}c_1 6^{-m/2}.$$

Then

$$|a_1| \geqslant 2\cdot 6^{k-m/2} \quad \text{and} \quad |c_1| \geqslant 2\cdot 6^{m/2}.$$

But

$$|a_1 c_1| \leqslant ((a_1^2+b_1^2)(c_1^2+d_1^2))^{1/2} \leqslant 6^k + O(6^{k/2}),$$

and we get a contradiction for k sufficiently large.

The case $l < m$ will be analysed in several steps:

1st step. For fixed a_1, b_1, d_1 we count how many c_1's can satisfy condition $(*)$ with $c_1 > a_1$. (If $c_1 < a_1$, we should fix c_1, b_1, d_1 and count the a_1's.)

From the last inequality of $(*)$, we have

$$(6^{2k}/(a_1^2+b_1^2)-d_1^2)^{1/2} \leqslant c_1 \leqslant ((6^{2k}+6^{3k/2})/(a_1^2+b_1^2)-d_1^2)^{1/2}.$$

The number of the possible c_1 will be less than $6^{k/2}/a_1 \leqslant 6^{m-k/2}b_1$.

2nd step. For fixed a_1, b_1 we count how many d_1's can satisfy $(*)$:

$$c_1 = d_1/\Phi_2+O(d_1 6^{-3m/2+k}), \qquad a_1 = b_1/\Phi_1+O(b_1 6^{-3m/2+k}),$$

because Φ_1, $\Phi_2 \gg 6^{m-k}$, and so

$$(a_1^2+b_1^2)(c_1^2+d_1^2) = (b_1 d_1)^2(1+1/\Phi_1^2)(1+1/\Phi_2^2)+O((b_1 d_1)^2 6^{4k-9m/2}).$$

Now $b_1 d_1 \ll 6^{m-k}a_1 6^{m-k}c_1 \ll 6^{2m-k}$ and

$$(6^k-6^{k-m/2})/((1+1/\Phi_1^2)(1+1/\Phi_2^2))^{1/2} < d_1 b_1$$
$$< (6^k+6^{k-m/2})/((1+1/\Phi_1^2)(1+1/\Phi_2^2))^{1/2}.$$

Therefore, there will be at most $6^{k-m/2}/\big(b_1((1+1/\Phi_1^2)(1+1/\Phi_2^2))^{1/2}\big)+1 \ll 6^{3m/2-k}/b_1+1$ possible d_1's.

3rd step. For fixed b_1, we count how many a_1's can satisfy $(*)$.

If $b_1 = 0$, then $6^{m-k} \ll |\Phi_1| < \frac{1}{2}\cdot 6^{m/2-k}$, but this is impossible because $m \geqslant k/2$ (by Lemma 1(ii)). Thus $b_1 > 0$.

If a_1 and a_1' satisfy $(*)$, then $|b_1/a_1-b_1/a_1'| < 6^{m/2-k} \Rightarrow b_1(a_1'-a_1) \ll a_1^2 6^{m/2-k} \Rightarrow a_1'-a_1 \ll a_1^2 6^{m/2-k}/b_1 \ll b_1 6^{k-3m/2}$. Thus, for fixed b_1, there are at most $b_1 6^{k-3m/2}+1$ a_1's satisfying $(*)$.

4th step. $b_1 \ll a_1 6^{m-k} \ll 6^{m-k/2}$ because we have supposed that $a_1 < c_1$. Then the number of solutions of $(*)$ is at most

$$\sum_{b_1<6^{m-k/2}} (b_1 6^{k-3m/2}+1)(6^{3m/2-k}/b_1+1)6^{m-k/2}/b_1$$
$$\ll (m-k)6^{m-k/2}+6^{m/2}+6^{5m/2-3k/2}+(m-k)6^{m-k/2} \ll 6^{m/2}$$

because $m \leqslant 3k/4$ (by Lemma 1(ii)).

To finish the proof, we count $6^{m/2}$ for each l, m, $l < m \leqslant 3k/4$:

$$\sum_{m<3k/4}\sum_{l<m} 6^{m/2} \ll k6^{3k/8}.$$

Now, each number of the $k6^{3k/8}$ integers can be expressed, for each $\varepsilon > 0$, as a sum of two squares in at most $6^{k\varepsilon}$ different ways.

Therefore, for each $\varepsilon > 0$, we can pick up $O(6^{k(3/8+\varepsilon)})$ numbers from I_k to get A_k, in such a manner that the equation $a^2+b^2 = c^2+d^2$, $a, b, c, d \in \bigcup_{j=1}^{k} A_j$, has only trivial solutions.

Note that $6^{k(3/8+\varepsilon)} = o(6^{k/2})$, which easily yields the growth of the sequence that we wanted to show.

Acknowledgement. I would like to thank A. Schinzel for pointing out to me the proof of Lemma 2 which is much shorter than my original one.

References

[1] M. Ajtai, J. Komlós and E. Szemerédi, *On dense infinite Sidon sequences*, European J. Combin. 2 (1981), 1-11.

[2] J. Cilleruelo and A. Córdoba, *Lattice points and Gaussian sums*, to appear.

[3] H. Halberstam and K. F. Roth, *Sequences*, Clarendon Press, Oxford 1966.

DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE MADRID
28049 Madrid, Spain

Received on 27.10.1988 (1880)