Acta Math. Hung.
50 (1—2) (1987), 117—122.

ON DIVISIBILITY PROPERTIES OF INTEGERS OF THE FORM $a+a'$

P. ERDŐS, member of the Academy and A. SÁRKÖZY (Budapest)

1. Throughout this paper, we use the following notations:

For any real number x let $[x]$ denote the greatest integer less than or equal to x, and let $\|x\|$ denote the distance from x to the nearest integer: $\|x\|=\min(x-[x], 1+[x]-x)$. We write $e^{2\pi ix}=e(x)$. The cardinality of the set X is denoted by $|X|$. $\Lambda(n)$ denotes the Mangoldt symbol.

In this paper, our goal is to study the following problem: how large can $|\mathcal{A}|$ be if $\mathcal{A}\subset\{1, 2, ..., N\}$ and $a+a'$ is squarefree for all $a\in\mathcal{A}$, $a'\in\mathcal{A}$? (See [1], [2] and [4] for other somewhat related results. In fact, in all these papers arithmetic properties of sums of sequences of integers are studied.)

We will prove the following results:

THEOREM 1. *For $N>N_0$, there exists a sequence $\mathcal{A}\subset\{1, 2, ..., N\}$ such that*

$$|\mathcal{A}| > \frac{1}{248}\log N \tag{1}$$

and $a+a'$ is squarefree for all $a\in\mathcal{A}$, $a'\in\mathcal{A}$.

THEOREM 2. *If $N>N_1$, $\mathcal{A}\subset\{1, 2, ..., N\}$ and $a+a'$ is squarefree for all $a\in\mathcal{A}$, $a'\in\mathcal{A}$ then we have*

$$\mathcal{A} < 3N^{3/4}\log N. \tag{2}$$

There is a considerable gap between the lower and upper bounds above. We guess that the lower bound is nearer to the truth. In fact, we conjecture that the upper bound in (2) can be replaced by N^{ε} (for all $\varepsilon>0$ and $N>N_2(\varepsilon)$) and, perhaps, even by $(\log N)^c$. Unfortunately, we have not been able to prove this.

By similar but slightly more complicated methods we can get analogous results for k-th power free numbers.

Also the following related problem can be considered: Let $1\leqq a_1<a_2<\ldots<a_k\leqq N$, $1<b_1<b_2<\ldots<b_l\leqq N$ be two sequences of integers. Assume that all the sums

$$a_i+b_j, \quad 1\leqq i\leqq k, \quad 1\leqq j\leqq l$$

are squarefree. Our method gives that

$$kl < N^{3/2+\varepsilon}$$

and we can show that $kl/N\to\infty$ is possible, but we of course have no satisfactory upper bound for kl. Perhaps the following remark is of some interest: there is an

absolute constant c so that $k>cN$, $l\to\infty$ is possible. Here perhaps l must be less than $\log N$ or $(\log N)^c$.

2. In this section, we prove Theorem 1. Let p_i denote the i-th prime number. Let N be a large positive integer, define the positive integer K by

$$\prod_{i=1}^{K-1} p_i^2 < N^{1/2} \leqq \prod_{i=1}^{K} p_i^2, \tag{3}$$

and put

$$P = \prod_{i=1}^{K} p_i^2.$$

Then by the prime number theorem we have

$$\log P = 2\sum_{i=l}^{K} \log p_i \sim 2 \sum_{n\leqq p_K} \Lambda(n) \sim 2p_K \tag{4}$$

so that for $N\to+\infty$ we obtain from (3) that

$$\frac{4P}{(\log P)^2} \sim \frac{P}{p_K^2} < N^{1/2} \leqq P$$

hence $\log P\sim\frac{1}{2}\log N$, so that, in view of (4), for large N

$$N^{1/2} \leqq P = p_K^2 \sum_{i=1}^{K-1} p_i^2 < 1/3\,(\log P)^2 N^{1/2} < \frac{1}{11} N^{1/2}(\log N)^2. \tag{5}$$

Let us take all the integers n satisfying

$$n \equiv 2 \pmod 4 \tag{6}$$

and

$$n \not\equiv 0 \pmod{p_i^2} \quad \text{for} \quad i = 2, 3, \ldots K. \tag{7}$$

These integers lie in

$$\prod_{i=2}^{K} (p_i^2-1) = \frac{1}{3}\prod_{i=1}^{K} (p_i^2-1) = \frac{1}{3} P \prod_{i=1}^{K}\left(1-\frac{1}{p_i^2}\right) >$$

$$< \frac{1}{3} P \prod_{i=1}^{+\infty}\left(1-\frac{1}{p_i^2}\right) = \frac{1}{3} P\cdot\frac{1}{\zeta(2)} = \frac{2}{\pi^2} P > \frac{1}{5} P$$

residue classes modulo P. Let us take the intersection of the set $\{1, 2, \ldots, N\}$ with each of these residue classes. In this way, we get $\prod_{i=2}^{K} (p_i^2-1)$ arithmetic progressions; let us denote the set of them by $\mathbf{B}$, so that

$$|\mathbf{B}| = \prod_{i=2}^{K} (p_i^2-1) > \frac{1}{5} P. \tag{8}$$

Then for $\mathscr{B}\in\mathbf{B}$, clearly we have

$$[N/P] \leqq |\mathscr{B}| < [N/P]+1 \quad (\text{for} \quad \mathscr{B}\in\mathbf{B}). \tag{9}$$

If $\mathscr{B}\in\mathbf{B}$, $n\in\mathscr{B}$, then n satisfies (6) and (7), so that n is not divisible by $p_1^2, \ldots, p_K^2$. Thus if n is not squarefree then $p_i^2|n$ for some $K<i\leqq\pi(N^{1/2})$. In view of (4), the number of the integers n with $n\leqq N$, $p_i^2|n$ $(K<i\leqq\pi(N^{1/2}))$ is

$$\sum_{i=K+1}^{\pi(N^{1/2})}\left[\frac{N}{p_i^2}\right] < \sum_{i=K+1}^{+\infty} < \frac{N}{p_i^2} < N\sum_{n=p_{K+1}}^{+\infty}\frac{1}{n^2} < N\sum_{n=p_{K+1}}^{+\infty}\frac{1}{(n-1)n} =$$

$$= N\sum_{n=p_{K+1}}^{+\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right) = N\frac{1}{p_{K+1}-1} < N\frac{1}{p_K} < \frac{3N}{P\log P}$$

for N large enough. Thus, in view of (8) and (9), there exists an arithmetic progression $\mathscr{B}_0\in\mathbf{B}$ which contains less than

$$\frac{3N(\log P)^{-1}}{|\mathbf{B}|} \leqq \frac{3N(\log P)^{-1}}{P/5} < 15\frac{N}{P\log P}$$

integers which are not squarefree (for N large enough). Let $n_1<n_2<\ldots<n_t$ be those integers in $\mathscr{B}_0$ which are not squarefree so that

$$t < \frac{15\,N}{P\log P}. \tag{10}$$

Put $n_0=0$, $n_{t+1}=N+1$,

$$M = \max_{0\leqq i\leqq t}|\mathscr{B}_0\cap(n_i, n_{i+1})|,$$

and assume that this maximum is assumed at $i=r$:

$$M = |\mathscr{B}_0\subset(n_r, n_{r+1})|.$$

In view of (5), (8) and (10), for large N we have

$$\frac{N}{2P} < \left[\frac{N}{P}\right] \leqq |\mathscr{B}_0| = \sum_{i=0}^{t}\mathscr{B}_0\cap[n_i, n_{i+1})| \leqq \sum_{i=0}^{t}\left(1+|\mathscr{B}_0\cap(n_i, n_{i+1})|\right) \leqq$$

$$\leqq \sum_{i=0}^{t}(1+M) = (t+1)2M < \left(\frac{15N}{P\log P}+1\right)2M < \frac{31MN}{P\log P}$$

hence, by (3),

$$M > \frac{1}{62}\log P \geqq \frac{1}{62}\log N^{1/2} = \frac{1}{124}\log N. \tag{11}$$

Let us write

$$\mathscr{B}_0\cap(n_r, n_{r+1}) = \{2b, 2b+P, \ldots, 2b+(M-1)P\}.$$

(Note that by (6) and $\mathscr{B}_0\in\mathbf{B}$, all the elements of $\mathscr{B}_0$ are even.) The elements of $\mathscr{B}_0\cap(n_r, n_{r+1})$ are squarefree. In fact, if $n\in\mathscr{B}_0\cap(n_r, n_{r+1})$, then by (6) and (7),

n is not divisible by $p_1^2, p_2^2, \ldots, p_K^2$, and by $n_r<n<n_{r+1}$, it is not divisible by p_{K+1}^2, $p_{K+2}^2, \ldots, p_{\pi(\sqrt{N})}^2$.

Let us put

$$\mathscr{A}=\left\{b, b+P, \ldots, b+\left[\frac{M-1}{2}\right]P\right\}.$$

Then for $a\in\mathscr{A}$, $a'\in\mathscr{A}$ we have $a+a'\in\mathscr{B}_0\cap(n_r, n_{r+1})$, so that $a+a'$ is square-free.

Finally, by (11) we have

$$|\mathscr{A}|=\left[\frac{M+1}{2}\right]>\frac{M}{2}>\frac{1}{248}\log N$$

which completes the proof of Theorem 1.

3. The proof of Theorem 2 will be based on the large sieve but we shall sieve by squares of primes. In this section, we derive the sieve result needed in the proof.

LEMMA 1. *If M, N are integers, $N\geqq 1$, $a_{M+1}, a_{M+2}, \ldots, a_{M+N}$ are arbitrary complex numbers, we put*

$$S(x)=\sum_{n=M+1}^{M+N} b_n e(nx).$$

Let $\mathscr{X}$ be a set of real numbers for which

$$\|x-x'\|\geqq\delta>0 \tag{12}$$

whenever x and x' are distinct members of $\mathscr{X}$. Then

$$\sum_{x\in\mathscr{X}}|S(x)|^2\leqq(\delta^{-1}+\pi N)\sum_n|b_n|^2.$$

PROOF. This is Corollary 2.2 in [3], p. 12.

LEMMA 2. *Let M, N be integers, $N\geqq 1$, and let $\mathscr{N}$ be a set of Z integers in the interval $[M+1, M+N]$. Put*

$$Z(q, h)=\sum_{\substack{n\in\mathscr{X}\\ n\equiv h\,(\mathrm{mod}\,q)}}1. \tag{13}$$

Then for $Q>0$ we have

$$\sum_{p^2\leqq Q}p^2\sum_{h=1}^{p^2}\left(Z(p^2, h)-\frac{Z}{p^2}\right)^2\leqq(Q^2+\pi N)Z. \tag{14}$$

PROOF. Let us write

$$S(x)=\sum_{n\in\mathscr{N}}e(n\alpha).$$

Then by [3], p. 23, (3.1) we have

$$p\sum_{h=1}^{p}\left(Z(p, h)-\frac{Z}{p^2}\right)^2=\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p^2}\right)\right|. \tag{15}$$

Furthermore, by [3], p. 24, (3.4) we have

$$q\sum_{h=1}^{q}\left|\sum_{d\mid q}\frac{\mu(d)}{d}Z\left(\frac{q}{d},h\right)\right|^2=\sum_{\substack{1\leqq a\leqq q\\(a,q)=1}}\left|S\left(\frac{a}{q}\right)\right|^2.$$

Putting $q=p^2$ here, we obtain that

$$p^2\sum_{h=1}^{p^2}\left(Z(p^2,h)-\frac{1}{p}Z(p,h)\right)^2=\sum_{\substack{1\leqq a\leqq p^2\\(a,p)=1}}\left|S\left(\frac{a}{p^2}\right)\right|^2. \tag{16}$$

By (15) and (16), we have

$$\sum_{p^2\leqq Q}p^2\sum_{h=1}^{p^2}\left(Z(p^2,h)-\frac{1}{p^2}\right)^2= \tag{17}$$

$$=\sum_{p^2\leqq Q}\left(p^2\sum_{h=1}^{p^2}\left(Z(p^2,h)-\frac{1}{p}Z(p,h)\right)^2+p\sum_{h=1}^{p}\left(Z(p,h)-\frac{Z}{p}\right)^2\right)=$$

$$=\sum_{p^2\leqq Q}\left(\sum_{\substack{1\leqq a\leqq p^2\\(a,p)=1}}\left|S\left(\frac{a}{p^2}\right)\right|^2+\sum_{a=1}^{p-1}\left|S\left(\frac{a}{p}\right)\right|^2\right).$$

In order to estimate this last sum, we use Lemma 1 where $\mathscr{X}$ is taken as the set of the fractions of the form $\frac{a}{p^2}$ $(p^2\leqq Q,\ 1\leqq a\leqq p^2,\ (a,p)=1)$ and $\frac{a}{p}$ $(p^2\leqq Q,\ 1\leqq a\leqq p-1)$. Then for $x=\frac{a_1}{p_1^{\alpha_1}}\in\mathscr{X}$, $x'=\frac{a_2}{p_2^{\alpha_2}}\in\mathscr{X}$ (where $\alpha_1,\alpha_2=1$ or 2), $x\neq x'$ we have

$$\|x-x'\|=\left\|\frac{a_1}{p_1^{\alpha_1}}-\frac{a_2}{p_2^{\alpha_2}}\right\|=\left\|\frac{a_1p_2^{\alpha_2}-a_2p_1^{\alpha_1}}{p_1^{\alpha_1}p_2^{\alpha_2}}\right\|\geqq\frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}}\geqq\frac{1}{Q^2}$$

so that (12) in Lemma 1 holds with $\delta=Q^{-2}$. Thus by using Lemma 1, we obtain from (17) that

$$\sum_{p^2\leqq Q}p^2\sum_{h=1}^{p^2}\left(Z(p^2,h)-\frac{Z}{p^2}\right)^2\leqq(Q^2+\pi N)\sum_{n\in\mathscr{N}}1=(Q^2+\pi N)Z$$

which completes the proof of Lemma 2.

4. In this section, we derive Theorem 2 from Lemma 2.

Let $\mathscr{A}\subset\{1,2,\ldots,N\}$ be a sequence such that for all $a\in\mathscr{A}$, $a'\in\mathscr{A}$ the sum $a+a'$ is squarefree. Then for all p, $a+a'\not\equiv 0 \pmod{p^2}$. Thus $\mathscr{A}$ may lie in at most $\frac{p^2-1}{2}$ residue classes modulo p^2, hence, defining $Z(q,h)$ by (13) (with $\mathscr{A}$ in place of $\mathscr{N}$), we have $Z(p^2,h)=0$ for at least $p^2-\frac{p^2-1}{2}=\frac{p^2+1}{2}$ incongruent values

of h. Thus the left hand side of (14) in Lemma 2 can be estimated in the following way:

$$(18) \qquad \sum_{p^2 \leqq Q} p^2 \sum_{h=1}^{p^2} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 \geqq \sum_{p^2 \leqq Q} p^2 \sum_{\substack{1 \leqq h \leqq p^2 \\ Z(p^2, h)=0}} \frac{Z^2}{p^4} =$$

$$= \sum_{p^2 \leqq Q} \frac{Z^2}{p^2} \sum_{\substack{1 \leqq h \leqq p^2 \\ Z(p^2, h)=0}} 1 \geqq \sum_{p^2 \leqq Q} \frac{Z^2}{p^2} \frac{p^2+1}{2} > \frac{Z^2}{2} \sum_{p^2 \leqq Q} 1 = \frac{Z^2}{2} \pi(Q^{1/2}).$$

Setting $Q = N^{1/2}$, we obtain from (18) and Lemma 2 that

$$\frac{Z^2}{2} \pi(N^{1/4}) < (N + \pi N) Z$$

hence, by the prime number theorem, for large N we have

$$Z < \frac{2(1+\pi)N}{\pi(N^{1/4})} < \frac{9N}{N^{1/4} \left(\frac{1}{4} \log N \right)^{-1}} < 3N^{3/4} \log N$$

which completes the proof of Theorem 2.

References

[1] A. Balog and A. Sárközy, On sums of sequences of integers. II, *Acta Math. Hung.*, **44** (1984), 339—349.
[2] P. Erdős and A. Sárközy, On differences and sums of integers, I, *J. Number Theory*, **10** (1978), 430—450.
[3] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Springer Verlag (1971).
[4] A. Sárközy and C. L. Stewart, On divisors of sums of integers, II, *J. Reine Angew. Math.*, to appear.

(Received August 21, 1985)

MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST, REÁLTANODA U. 13—15.
H—1053

86-4013 — Szegedi Nyomda — Felelős vezető: Surányi Tibor igazgató