Periodica Mathematica Hungarica Vol. 15 (3), (1984), pp. 205—209

DIFFERENCE SETS WITHOUT SQUARES

I. Z. RUZSA (Budapest)

Abstract

A sequence of natural numbers $A = a_1, a_2, \ldots$ is constructed such that no $a_i - a_j$ is a square and there are $> x^{0,73}$ a_i's below x.

Notation

Throughout the paper, if $A, B, \ldots$ is a sequence of nonnegative integers, $a_i, b_i, \ldots$ is its i'th element and $A(x), B(x), \ldots$ the number of its elements $\leq x$. As usual,

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

1. Introduction

It was conjectured by Lovász and proved by Sárközy [2] that if S is any sequence of natural numbers of positive asymptotic density, then $S - S$ necessarily contains a square. Let $D(x)$ denote the maximal number of integers that can be selected from $[1, x]$ so that no difference between them is a square. Sárközy even proved

$$D(x) = O(x(\log x)^{-1/3+\varepsilon}).$$

Obviously $D(x) \geq \sqrt{x}/2$. In general, given any sequence Q, the greedy algorithm provides an S such that

$$(S - S) \cap Q = \emptyset, \ S(x) \geq \frac{x}{2Q(x)}.$$

Erdős stated the conjecture

$$D(x) = O(x^{1/2} \log^k x)$$

AMS (MOS) subject classifications (1970). Primary 05B10, 10L05.
Key words and phrases. Difference sets, intersective set.

with some constant k. Sárközy [3] disproved this but still conjectured

$$D(x) = O(x^{1/2+\varepsilon}).$$

Our aim is to prove

THEOREM 1. *$D(x) > c_1 x^\gamma$, where $c_1 > 0$ and*

$$\gamma = \frac{1}{2}\left(1 + \frac{\log 7}{\log 65}\right) = 0{,}733077\ldots.$$

More generally, let $D_k(x)$ denote the maximal number of integers that can be selected from $[1, x]$ so that no difference between them is a k'th power. For a natural number m let $r_k(m)$ denote the maximal number of residues (mod m) that can be selected so that no difference between them is a k'th power residue.

THEOREM 2. *For every k and squarefree m we have*

$$D_k(x) \geq m^{-1} x^{\gamma(k,m)},$$

where

$$\gamma(k, m) = 1 - \frac{1}{k} + \frac{\log r_k(m)}{k \log m}.$$

Write

$$d_k = \limsup \frac{\log D_k(x)}{\log x}.$$

COROLLARY. *If $p(k)$ is the least prime $\equiv 1 \pmod j$, then we have*

$$d_k \geq 1 - \frac{1}{k} + \frac{\log k}{k \log p(2k)}.$$

Especially

$$d_3 \geq 1 - \frac{1}{3} + \frac{\log 3}{3 \log 7} = 0{,}854858\ldots,$$

$$d_5 \geq 1 - \frac{1}{5} + \frac{\log 5}{5 \log 11} = 0{,}934237\ldots.$$

Linnik's theorem $p(k) < k^C$ yields

$$d_k > 1 - \frac{1-\delta}{k}$$

with some fixed $\delta > 0$.

2. Proof of Theorem 2

Let $R \subset [1, m]$ be a set of integers such that no difference is a k'th power residue modulo m and $|R| = r_k(m)$. Let A consist of the natural numbers of the form

$$a = \Sigma r_j m^j.$$

where $r_j \in R$ if $k|j$ and $1 \leq r \leq m$ is arbitrary otherwise. Then obviously

$$A(m^n) = R^{1+[n-1/k]} m^{n-1-[n-1/k]},$$

whence

$$A(x) \geq m^{-1} x^{\gamma(k,m)} \quad (x > m)$$

follows immediately. Now suppose $a - a' = t^k$, $a, a' \in A$.

$$a = \Sigma r_j m^j, \; a' = \Sigma r'_j m^j.$$

Let s be the first suffix for which $r_s \neq r'_s$. We have

$$t^k = a - a' = (r_s - r'_s) m^s + z m^{s+1},$$

z integer. If $k \nmid s$, then $m^s | t^k$ but $m^{s+1} \nmid t^k$ is impossible (here we need that m be squarefree). If $k|s$, $s = ku$, then

$$(t/m^u)^k \equiv r_s - r'_s \pmod{m}, \quad r_s, r'_s \in R,$$

in contradiction with the definition of R. This completes the proof.

3. Proof of Theorem 1 and the Corollary

To deduce Theorem 1 and the Corollary from Theorem 2 we have to show

(1) $$r_2(65) \geq 7$$

and

(2) $$r_k(p) \geq k \text{ if } p \equiv 1 \pmod{2k} \text{ is a prime.}$$

To get (1), consider the following 7 residues:

$$(0, 0),\ (0, 2),\ (1, 8),\ (2, 1),\ (2, 3),\ (3, 9),\ (4, 7),$$

where in each pair the first component is the residue modulo 5 and the second modulo 13.

Now we prove (2). Let Q be the set of k'adic residues modulo p: we have

$$|Q| = q = 1 + (p - 1)/k.$$

The greedy algorithm yields

$$r_k(p) \geq p/q.$$

which is $> k-1$ for large p, but for small primes we have to be more careful.

By induction we shall construct $b_1, \ldots, b_k$ so that $b_i - b_j \notin Q$ for $i \neq j$ and

$$(3) \qquad |B_j + Q| \leq 1 + j(q-1), \quad j = 1, \ldots k$$

where $B_j = \{b_1, \ldots, b_j\}$. Given $b_1, \ldots, b_j$, let b_{j+1} be any element of

$$(B_j + Q + Q) \backslash (B_j + Q).$$

Since $b_{j+1} \notin B_j + Q$, $b_{j+1} - b_i \notin Q$ for $i < j$ and since $b_{j+1} \in B_j + Q + Q$, the sets $B_j + Q$ and $b_{j+1} + Q$ are not disjoint. (Observe that $Q = -Q$, since $p \equiv 1 \pmod{2k}$ guarantees that -1 is a k'th power residue.) Hence

$$|B_{j+1} + Q| = |(B_j + Q) \cup (b_{j+1} + Q)| \leq$$
$$\leq |B_j + Q| + |b_{j+1} + Q| - 1 \leq 1 + j(q-1) + q - 1,$$

as wanted.

This procedure breaks off if $B_j + Q + Q = B_j + Q$. This can happen only if $B_j + Q$ contains all the residues, thus if b_j is the last, then $1 + j(q-1) \geq \geq p$, i.e., $j \geq k$. Q.E.D.

4. Final remarks

I first considered $k = 2$, $m = 5$, where $r_2(5) = 2$, and thus I found $d_2 > 0.7153\ldots$. A. Balog improved this by showing $r_2(41) = 5$, $d_2 > 0.71669\ldots$ He stated the conjecture that $r_2(p) > p^{1/2-\varepsilon}$ for infinitely many primes p. I highly disbelieve this. R. Freud remarked that composite numbers may also be worth considering, and after this I found $r_2(65) = 7$. On the other hand, I proved $r_2(m) < \sqrt{m}$ if m consists exclusively of primes $\equiv 1 \pmod 4$. I think $4k-1$ primes can only spoil the situation, thus I conjecture that $r_2(m) < \sqrt{m}$ always. This would mean that by this method we cannot exceed 3/4 in the original problem.

Problem. Does $\lim \dfrac{\log D(x)}{\log x}$ exists?

I am quite sure it does.

Problem. Is there a fixed sequence A without square differences such that $A(x) > cD(x)$ for all x with a fixed $c > 0$? I think the answer would be negative. like in the case of Sidon's problem (cf. Halberstam—Roth [1], Chapter 2, Section 3.). In general, the finite and infinite case may be completely different; I plan to return to this in another paper.

REFERENCES

[1] H. HALBERSTAM and K. F. ROTH, *Sequences*, Clarendon, Oxford, 1966. *MR* **35** # 1565
[2] A. SÁRKÖZY, On difference sets of sequences of integers, I, *Acta Math. Acad. Sci. Hungar.* **31** (1978), 125—149. *MR* **57** # 5942
[3] A. SÁRKÖZY, On difference sets of sequences of integers, II. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **21** (1978), 45—53. *MR* **80j**: 10062a

(Received April 2, 1982)

MTA MATEMATIKAI KUTATÓ INTÉZET
H—1364 BUDAPEST
P.O. BOX 127.
REÁLTANODA U. 13—15.
HUNGARY