PROBLEMS AND RESULTS ON COMBINATORIAL NUMBER THEORY II[1]

By P. ERDÖS

[Received April 25, 1975]

I WROTE SEVERAL papers and review articles on this subject. One of them has in fact the same title (P. Erdös, Problems and results on combinatorial number theory, *A survey of combinatorial theory*, Edited by J. N. Srivastava, North Holland 1973, 117–138. I will refer to this paper as I). To prevent this paper from becoming too long I will avoid ovelap with I as much as possible and consider the problems in I only where some progress has been made in the problems stated there. On the other hand since I is not everywhere easily accessible I will give as complete references as possible.

Before starting the discussion of our problems I give a few titles of papers where similar or related problems were discussed and where further literature can be found.

II. P. Erdös, On unsolved problems, *Publ. Math. Inst. Hung. Acad.* 6 (1961), 229–254; Some unsolved problems, *Michigan Math. J.* 4 (1957), 291–300.

III. P. Erdös, Remarks on number theory IV and V. Extremal problems in number theory I and II (in Hungarian) *Mat. Lapok* 13 (1962), 28–38; 17 (1966), 135–166. See also P. Erdös, Extremal problems in number theory, *Proc. Symp. in Pure Math.* Vol VIII Theory of Numbers, Amer. Math. Soc. Providence A. I. 1965, 181–189; several of the results stated in this paper were improved and extended in various papers of S.R.L.G. Choi.

---

1. Lecture delivered at the annual meeting of the Indian Mathematical society at Powai, Bombay in December 1974.

IV. P. Erdös, *Some recent advances and current problems in number theory*, Lectures on Modern Mathematics, L. Saaty, Editor, Wiley, New York 1965 vol III 196–244.

V. P. Erdös, *Some extremal problems in combinatorial number theory* Math. essays dedicated to A. J. Macintyre, edited by H. Shankar, Ohio Univ. Press, Athens Ohio 1970, 123–133.

VI. P. Erdös, Some problems in number theory, *Computers in number theory*, Academic Press London 1971 (conference held in Oxford 1969) 406–414.

VII. P. Erdös, Quelques problémes de la théorie des nombres, Monographie de l'Enseignement Math. No. 6, *L'Enseignement Math.* (1963), 81–135.

VIII. H. Halberstam and K. F. Roth, *Sequences*, Oxford Univ. Press London 1966.

IX. H. Rohrbach, Einige neuere Untersuchungen über die Dichte in der additiven Zahlentheorie. *Jahresbericht D. M. V.* (1938).

X. A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I and II *J. reine u. angew Math.* 194 (1955), 40–65, 111–140.

XI. Many interesting unsolved problems of a combinatorial and number-theoretic nature are mentioned in the proceedings of the meetings on number theory held in Boulder in 1959 and 1963. See also a forthcoming book of Croft and Guy.

R. L. Graham and I are preparing a longish survey paper on number theoretic problems.

This list of course does not claim completeness and is heavily biased in favour of my own work but perhaps I can be excused for this since after all I am supposed to know my own work best.

1. Denote by $r_k(n)$ the maximum number of integers not exceeding

n which do not contain an arithmetic progression of k terms. Turan and I conjectured more than 40 years ago that for every k

$$\lim_{n=\infty} r_k(n)/n = 0. \tag{1}$$

Behrend and Roth proved

$$\frac{n}{\exp(c_1(\log n)^{1/2})} < r_3(n) < \frac{c_2 n}{\log\log n} \tag{2}$$

and Szemerédi proved (1) for $k=4$. It would be very desirable to improve the upper and lower bounds in (2). I offered 1000 dollars for the proof or disproof of (1), and recently Szemerédi proved (1). His proof which is a master-piece of combinatorial reasoning will appear very soon in Acta Arithmetica.

Turán and I were led to our conjecture by trying to obtain better limits for van der Waerden's well known theorem. There is an $f(k)$ so that if we split the integers $1 \leqslant t \leqslant f(k)$ into two classes at least one of them contains an arithmetic progression of k terms, Van der Waerden's proof gives a very poor upper bound for $f(k)$. Unfortunately Szemerédi's proof does not help since his proof in fact uses van der Waerden's theorem.

It would be very desirable to obtain a better upper bound for $f(k)$ either by improving Szemerédi's proof or by some other method.

Let S be any finite set of lattice points in r-dimensional space. Gallai and Witt proved that if we split the lattice points of r-dimensional space into two classes then at least one of them contains a set similar to S. I conjectured that to every $\varepsilon > 0$ there is an $n_0 = n_0(S, \varepsilon)$ so that for every $n > n_0$ if

$$\{X_1^{(k)}, \ldots, X_r^{(k)}\},\ 0 \leqslant X_i^{(k)} \leqslant n, 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant \varepsilon n^r$$

is any set of ϵn^r lattice points in the cube $0 \leqslant X_i \leqslant n$, $1 \leqslant i \leqslant r$ then this set contains a subset similar to S. Ajtai and Szemerédi proved this for $r=2$ if S is the isosceles right angled triangle and very recently Szemerédi proved this if S is a square. The general case is still open.

It would be very desirable to get an asymptotic formula for $r_k(n)$;

this seems to be hopeless at present. Szemerédi pointed out to me that we cannot even prove

$$\lim_{n=\infty} r_k(n)/r_{k+1}(n) = 0.$$

F. Behrend, On sets of integers which contain no three terms in an arithmetic progression *Proc. Math. Acad. Sci* USA 32 (1946), 331–332.

K. F. Roth, On certain sets of integers, *J. London Math. Soc.* 28 (1953), 104–109.

E. Szemerédi, On certain sets of integers containing no four elements in arithmetic progression, *Acta Math. Acad. Sci. Hunger* 20 (1969), 89–109.

E. R. Berlekamp, A construction for partitions which avoid long arithmetic progressions, *Canad. Math. Bull.* 11 (1968), 409–414.

H. L. Abbott, A. C. Liu and J. Riddell, On sets of integers not containing arithmetic progressions of prescribed length, *J. Australian Math. Soc.* 18 (1974), 188–193.

2. An old conjecture in number theory states that for every k there are k primes in arithmetic progression. This conjecture would immediately follow if we could prove that for very k and $n > n_1(k)$, $r_k(n) < \pi(n)$. This method of proof seems very attractive, it tries to prove a difficult property of the primes by just using the facts that the primes are numerous in some cases I have been successful with this simple minded approach. In this connection I recently formulated the following conjecture for the proof or disproof of which I offer 2500 dollars: Let $a_1 < a_2 < \ldots$ be an infinite sequence of integers satisfying $\Sigma \frac{1}{a_i} = \infty$. Then for every k there are k a's in an arithmetic progression. (The truth of this conjecture would imply that for every k there are k primes in arithmetic progression). One can put this problem in a finite form as follows: Put

$$g_k(n) = \max \sum_{a_i > n} \frac{1}{a_i},\ G(k) = \lim_{n=\infty} g_k(n).$$

where the maximum is extended over all sequences $\{a_i\}$ not exceeding n which do not contain an arithmetic prcgression of k terms. The 2500 dollar conjecture is equivalent to $G(k) < \infty$ for every k (it is not quite trivial to show that $G(k) = \infty$ implies the falseness of the conjecture). It would be of great independent interest to obtain good upper and lower bounds for $g_k(n)$ and $G(k)$. First of all, observe that trivially $f(k)$ is the least integer so that if we split the positive integers $\leqslant f(k)$ into two classes at least one class contains an arithmetic progression of k terms

$$G(k) \geqslant g_k(f(k)-1) \geqslant \tfrac{1}{2} \sum_{t=1}^{f(k)-1} \frac{1}{t} > \frac{1}{2} \log f(l).$$

Probably $G(k) \geqslant c \log f(k)$ holds for every c if $K > k_0(c)$ but I can not disprove

$$\lim_{k=\infty} \frac{G(k)}{\log f(k)} = \tfrac{1}{2}. \tag{1}$$

The best known lower bound for $f(k)$ is $k\ 2^k$ (Berlekamp quoted before) and I can not disprove

$$\lim_{k=\infty} \frac{G(k)}{k} = \frac{\log 2}{2} \tag{2}$$

I am sure that (2) is false and expect (1) to be false too. (*Added in proof.* Gerver proved: $G(k) \geqslant (1 + 0(1))\ k \log k$. His proof will appear in Proc. Amer. Math. Soc).

Denote by $h_k(n)$, $k > 3$ the largest integer so that there is a sequence of integers $1 \leqslant a_1 < \ldots < a_n \leqslant$ which contains $h_k(n)$ arithmetic progressions of three terms but no progression of k terms. It seems very likely that $h_k(n) = \sigma(n^2)$ for every k, but I would not prove this even for $k = 4$. It is easy to see by probabilistic methods that $h_k(n) > c'\ n^2$ for $k > c$ logn. Perhaps the following result holds: there is an increasing continuous function $g(c)$, $g(0) = 0$, $g(\infty) = 1$ so that for $k = c\log n$, $h_k(n) = (g(c) + \sigma(1))\, n^2$.

An old problem of Cohen states: Determine or estimate a function $F(d)$ so that if we split the integers into two classes at least one class contains, for infinitely many values of d, an arithmetic progression of difference d and length $F(d)$. (This problem is stated incorrectly in I p. 121). I showed $F(d) < cd$. Petruska and Szemerédi very considerably improved this result, they showed $F(d) < cd^{1/2}$ and they are sure that their proof will give $F(d) = O(d^\varepsilon)$. Their proof will soon be published. As far as I know there is no known explicit lower bound for $F(d)$. $F(d) \to \infty$ follows from van der Waerden's theorem, and the true order of magnitude of $F(d)$ may be very difficult to establish.

Hindman proved the following conjecture of Graham and Rothschild: Divide the integers into two classes in an arbitrary way. Then there is always an infinite sequence $a_1 > a_2 > \dots$ so that all the finite sums $\sum_i \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1 belong to the same class. A simpler proof of Hindman's theorem was found recently by Baumgartner.

Is the following extension of the conjecture of Graham and Rothschild true: Split the set of integers (or real numbers) into two classes. There always is an infinite sequence $x_1 < x_2 < \dots$ so that all multilinear expressions formed from the (x_i) (where each variable occurs only once) are in the same class? I could first try to find a counterexample. A much weaker conjecture would be: To every r there are r integers $x_1, \dots, x_r$ so that the set of r^2 numbers

$$\{x_i,\ x_i + x_j,\ x_i x_j\},\ 1 \leqslant i < j \leqslant r$$

all belong to the same class. By aid of a computer Graham proved that if we divide the integers $1 \leqslant n \leqslant 252$ into two elasses, there are always four integers x, y, $x+y$, xy in the same class. This fails for $n = 251$.

P Erdös, On the sum and difference of squares of primes, *J. London Math.* I and II, 12 (1937), 133–136 and 168–171, On the integers which are the totient of a product of two primes, *Quart J. Math.* 7 (1936), 227–229. See also Copeland and P. Erdös, Note on normal numbers, *Bull. Amer. Math. Soc.* 52 (1946), 857–860.

N. Hindman, Finite sums from sequences within cells of a partition of N *.J. Comb. theory*, 17 (1974), 1–11.

J. E. Baumgartner, A short proof of Hindman's theorem, *J. Comb. theory* (A) 17 (1974), 384–386.

3. A system of congruences

$$a_i \pmod{n_i},\ 1 < n_1 < \ldots < n_k \tag{1}$$

is called a covering system if every integer satisfies at least one of the congruences (1). My old problem can n_1 be arbitrarily large is still unsolved and Choi still holds the record with his system for $n_1 = 20$.

Let $g(t)$ be the smallest integer for which there is a system (1) with $n_1 = t$ and $k = g(t)$. My conjecture states: $g(t) < \infty$ for every t. It would be interesting to estimate $g(t)$ from above and below. I think

$$\lim_{n=\infty} g(t)/t^l = \infty$$

for every l, but as far as I know this question has not yet been investigated. It would also be of interest to estimate the smallest possible value of n_k as a function of $n_1 = t$.

I conjectured and L. Mirsky and D. Newman proved that there is no exact covering system (1). A covering system is called exact if every integer satisfies exactly one of tne congruences (1). In fact their proof gives that in every exact covering system we have $n_{k-1} = n_k$. Recently Herzog and Schönheim posed the following interesting generalisation: Is it true that no finite Abelian group can be covered exactly by disjoint cosets $C_i. 1 \leqslant i \leqslant j \leqslant k$, $|C_i| \neq |C_j|$?

Let $G(n)$ be the lower bound of $\sum \frac{1}{n_1}$ where $n = n_1 < \ldots$ is a covering system. Probably $G(n) > 1$ for $n \geqslant 4$ and $G(n) \to \infty$ as $n \to \infty$. This was conjectured by Selfridge and myself.

Using covering congruences I proved that there is an arithmetic progression consisting entirely of odd numbers, no term of which is of the form $2^k + p$. If n_1 in (1) can be made arbitrarily large then we immediately get that for every r there is an arithmetic progression no term of which is the form $2^k + \theta_r$ where θ_r has at most r distinct prime factors.

Is it true that for every l there is an arithmetic progression no term of which is of the form $2^{k_1} + \ldots + 2^{k_l} + p$? Recently Gallagher proved that for large enough l the lower density of these numbers is $> 1-\varepsilon$ (previously Linnik proved that all large numbers are the sum of two primes and l powers of 2). Very likely the density of integers of the form $p+2^k$ exists, but this question is intractable at present—in fact almost nothing is known about the distribution of these numbers e.g. I cannot prove that there are arbitrarily many consecutive integers none of which are of the form $p+2^k$. This conjecture would easily follow if in (1) we can take n_1 arbitrarily large.

I conjectured that for $n > 105$ the integers

$$n-2^k,\ 1 \leqslant k \leqslant \frac{\log n}{\log 2} \tag{2}$$

can not all be primes. If true this conjecture will be very difficult to prove. Vaughan obtained a non-trivial upper bound for the number of integers $n \leqslant X$ for which all the integers (2) are primes.

Schinzel proved that there are infinitely many integers not of the form $p+2^{k_1}+2^{k_2}$, but he only obtains a very sparse sequence not of the form $p+2^{k_1}+2^{k_2}$.

I conjectured that the density of integers of the form 2^k+Q, Q sqarefree is 1. The main difficulty is to prove that if $q_1, \ldots, q_k$ is a finite set of primes then to every sufficiently large $n > n_0(\dot{q}_1, \ldots, k_k)$ there is an l

$$0 < l < \frac{\log n}{\log 2} \text{ and } q_i^2 \nmid n-2^l,\ i=1, \ldots, k.$$

Perhaps every sufficiently large odd integer is of the form 2^k+Q.

Cohen and Selfridge recently proved using covering congruences that not every integer is the sum or difference of two prime powers, (and in fact the set of exceptional integers contains infinite arithmetic progressions).

Interesting and unexpected applications of covering congruences were made by A. Schinzel.

P. Erdös, On integers of the form $2^k + p$ and some related problems, *Summa Brasil Math.* 11 (1950), 113–123.

S. L. G. Choi, Covering the set of integers by congruence classes of distinct moduli, *Math. Comp.* 25 (1971), 885–895.

F. Cohen and J. L. Selfridge, Not every integer is the sum or difference of two prime powers, *Math. Comp.* 29 (1975), 79–81.

A. Schnizel, Reducibility of polynomials and covering systems of congruences, *Acta Arith.* 13 (1967–68), 91–101.

4. Sidon calls a sequence $a_1 < a_2 < \ldots < a_k$, aB_t-sequence if the sums $\sum_{i=1}^{k} \varepsilon_i a_i$ are all distinct ($\varepsilon_i = 0$ or 1). Turán and I conjectured

$$\max B_2(x) = x^{1/2} + 0(1), \tag{1}$$

(where the maximum is taken over all the B_2 sequences) but we only could prove

$$(1 + 0(1)x^{1/2} < B_2(x) < x^{1/2} + cx^{1/4}.$$

Recently Szemerédi proved

$$B_2(x) = x^{1/2} + 0(x^{1/4})$$

his proof appears in the Colloquium of finite and infinite sets held at Keszthely Hungary, June 1973.

Perhaps the most striking unsolved problem on B_2 sequences asks: Is there an infinite B_2 sequence satisfying $a_k/k^3 \to 0$?

I proved (see X, p. 132–134) that there is an infinite B_2 sequence $a_1 < a_2 < \ldots$ for which

$$\liminf a_k/k^2 \leqslant 2, \tag{3}$$

and Krickeberg improved 2 to $\sqrt{2}$, Perhaps in (3), 2 can be replaced by 1.

I proved that for every infinite B_2 sequence

$$\liminf a_k/k^2 = 0. \tag{4}$$

My proof in fact gives that if $1 \leqslant a_1, \ldots, < a_k \leqslant x$ is a B_2 sequence then

$$\sum_{i=1}^{k} \frac{1}{a_i^{1/2}} < \frac{c \log x}{(\log \log x)^{1/2}}. \tag{5}$$

My proof given in X (p. 132–134) gives that there is a B_2 sequence for which

$$\sum_{a_i < x} \frac{1}{a_i^{1/2}} > c \log \log x. \tag{6}$$

I do not know and cannot give whether (4) or (5) is closer to the truth. Bose and Chowla (see XI) using finite fields construct for every $x > x_0(\varepsilon)$ a B_r sequence satisfying $B_r(\mathrm{x}) > (1-\epsilon)x^{1/r}$ they conjecture that for every $\varepsilon > 0$ and $X > X_0(\varepsilon)$

$$B_r(x) < (1+\varepsilon)x^{1/r}. \tag{7}$$

The proof of (2) does not seem to help at all in trying to proving (7). Let $a_1 < \ldots$ be an infinite B_r sequence I am sure that

$$\lim \sup a_l/k^r = \infty$$

is true but proof of (4) does not seem to help and I can not at present prove (8).

Rényi and I proved (see VIII) that for every $\varepsilon > 0$ there is an infinite sequence $a_k > k^{2+\varepsilon}$ for which the number of solutions of $a_i + a_j = n$ is less than c_ε, On the other hand Turan and I conjectured that if $a_1 < \ldots$ is such that if the number of solutions of $n = a_i + a_j$ is bounded then

$$\lim_{h=\infty} \sup a_k/k^2 = \infty. \tag{9}$$

I offer 300 dollars for a proof or disproof of (9).

P. Erdös and P. Turàn: On a problem of Sidon in additive number theory and on some related problems J. London Math. Soc. 10 (1941), 212–216.

F. Krückeberg: B_2-Folgen und verwandte Zahlenfolgen J. reine u. angew. Math. 206, (1961) 53–60.

5. Let $a_1 < a_2 < \dots$ be a primitive sequence i.e. **no a_i divides any** other. I proved that (see VIII)

$$\sum_i \frac{1}{a_i \log a_i} < C$$

Perhaps

$$\max \sum \frac{1}{a_i \log a_i} = \sum \frac{1}{p \log p} \tag{1}$$

But I have not been able to prove (1).

I state a few external problems on sequences of integers most of which are unsolved, Let $a_1 < \dots$ be a B_2 sequence. It is easy to see that $\sum \frac{1}{a_i}$ is bounded. It might be of some interest to determine $\max \sum \frac{1}{a_i}$ when the maximum is taken over all B_2 sequences $a_1 < \dots$. The same question can be asked for B_k sequences.

A sequence $a_1 < a_1 < \dots$ is a B_∞ sequence if all the sums $\Sigma \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1 are distinct. I conjectured that

$$\max \left(\frac{1}{a_1} + \dots \frac{1}{a_k} \right) = 2 - \frac{1}{2^{k-1}}$$

equality only for $\{2^i\}$, $i = 0, \dots, k-1$. This conjecture was proved by Ryavec and E. Szekeres in a surprisingly simply way. On the other hand the determination of $\min_{B_\infty} a_k$ seems a very difficult problem. Moser and I proved

$$\min_{B_\infty} a_k > \frac{c2^k}{k^{1/2}}.$$

and I offer 300 dollars for a proof or disproof of the conjecture

$$\min_{B_\infty} a_k > c2^k.$$

On the other hand it is a simple exercise to prove that for an infinite B_∞ sequence we have

$$\min_{B_\infty} a_k \geqslant 2^{k-1}$$

for infinitely many values of k (equality only for $a_k = 2^{k-1}$).

Let $1 \leqslant a_1 < \ldots$ be a sequence of integers where no a_i is the distinct sum of other a's. I proved that $\sum \frac{1}{a_i} < 100$. I was told at the New York meeting of the Amer. Math. Soc. in April 1973 that Sullivan replaced 100 by 5 and that $\sum \frac{1}{c_i} > 2$ is possible but that the maximum is probably close to 2. The following result might hold: $\sum_{i=1}^{\infty} \frac{1}{a_i} < \log 2 + \varepsilon$ holds for every $\varepsilon > 0$ if $a_1 > a_0(\varepsilon)$. This is best possible if true is shown by $a_i = a_1 + i - 1$, $i = 0, \ldots, a_1 - 1$.

S. J. Benkoski and P. Erdös, On weird and pseudoperfect numbers, *Math. Comp*, 28 (1974), 617–624.

P. Erdös, Problems and results in additive number theory, *Coll. Théorie des Nombres*, Bruxelles; George Thone, Liége, Masson et Cie Paris 1955, 127–137 see p. 135–137. The proof of E. Szekeres will be published in a problem in Bull. Eanad. Math. Soc.

6. Before completing the paper I state a few miscellaneous problems which were mentioned in I, and where some progress was made since I, was written.

Let $a_1 < \ldots < a_k$; $b_1 < \ldots < b_l \leqslant x$ be two sequences of integers. Assume that the products $a_i b_j$ are all different. How large can $k \, . \, l$ be and which are the extremal sequences? In this form the problem is probably hopeless but I conjectured and Szemerédi proved that

$$kl < c \frac{x^2}{\log x}$$

always holds. Szemerédi's proof will appear in the Journal of Number Theory. Szemerédi and I gave a simpler proof of (1) and obtained various extensions, also we conjecture that (1) holds with $c = 1 + \varepsilon$ for every $\varepsilon > 0$ if $x > x_0(\varepsilon)$. It is not difficult to see that if this is true then it is best possible. Our paper will appear in the Journal of the Australian Math. Soc.

It is not difficult to give two infinite sequences A and B so that the products $a_i \cdot b_j$ are all different and for every x

$$A(x) \cdot B(x) > c_1 \frac{x^2}{\log x} \left(A(x) = \sum_{a_i < x} 1 \right). \tag{2}$$

Very likely in (2) c_1 must be substantially smaller than 1.

The following question might be of some interest: Let $a_1 < \ldots < a_k \leqslant x$; $b_1 < \ldots < b_l \leqslant x$ and assume that the number of distinct products of the form $a_i b_j$, is greater than ckl, How large can $k \cdot l$ be?

A sequence of integers $\{a_i\}$ is called an essential component if for any sequence $\{b_1\}$ of Schnirelmann density $1 > \alpha > 0$ the Schnirelmann sum of $\{a_l + b_j\}$ has Schnirelmann density $> \alpha$. Essential components were introduced by Khintchine for the relevant definitions, see VIII. I proved that every basis is an essential component and Linnik proved that there is a nonbasis which is an essential component. Stöhr and Wirsing obtained a simpler proof of Linnik's theorem, but Linnik's essential component had the additional property of being very sparse, in fact

$$\sum_{a_i > x} 1 = A(x) < \exp((\log x)^\alpha)$$

for some $\alpha < 1$. I conjectured that if $a_{k+1}/a_k > c > 1$ then A is not an essential component.

Linnik's proof was very complicated. Recently Wirsing gave a fairly simply proof that for every $\varepsilon > 0$ there is an essential component satisfying

$$A(x) < \exp((\log x)^{\frac{1}{2}+\varepsilon})$$

and he conjectures that for every $\varepsilon > 0$ and $x > x_0(\varepsilon)$

$$A(x) > \exp((\log x)^{\frac{1}{2}-\varepsilon})$$

(3) if true shows that (2) is best possible. (3) is of course much stronger than my conjecture.

For the older literature see VIII. The paper of Wirsing will appear in the proceedings of the colloquium on number theory held in Debrecen (Hungary, Bolyai math. soc.) and will be publised by North Holland.

Graham conjectured (I, p. 126): Let $a_1, \ldots, a_p$ be p not necessarily distinct residues mod p. Assume that there is an r so that for every choice of $\varepsilon_1 = 0$ or 1 for which $\sum_{i=1}^{p} \varepsilon_i a_i \equiv 0 \pmod{p}$, we have $\sum_{i=1} \varepsilon_i = r$. Then there are at most two distinct residues among a's. Szemerédi and I proved this conjecture for $p > p_0$. No doubt with some calculation and lots of patience we could get rid of the assumption $p > p_0$. Our paper will appear in Publications Math. Debrecen.

I asked: Is it true that for every $\varepsilon > 0$ one can give a sequence $1 < a_1 < \ldots < a_r \leqslant x$, $r > (1 - \varepsilon) x$ so that the product of distinct a's can be equal only if the number of factors is the same. I, Ruzsa recently proved that such a sequence does not exist if ε sufficiently small. His proof of this and related results will appear in Acta Arithmetica.