Two problems
in
combinatorial number theory

Carl Pomerance, Dartmouth College

Debrecen, Hungary
October, 2010

Our story begins with:

Abram S. Besicovitch

Besicovitch showed in 1934 that there are primitive sets of natural numbers with upper density arbitrarily close to 1/2.

Here "primitive" means that no member of the set divides another. For example, the set of prime numbers is a primitive set.

But the set of primes has density 0. By the upper density of a set $\mathcal{S}$, we mean

$$\bar{d}(\mathcal{S}) := \limsup_{x\to\infty} \frac{1}{x} S(x),$$

where $S(x) := |\mathcal{S} \cap [1, x]|$.

The result of Besicovitch is somewhat of a surprise, since a first guess might be that the set of primes forms a typical example.

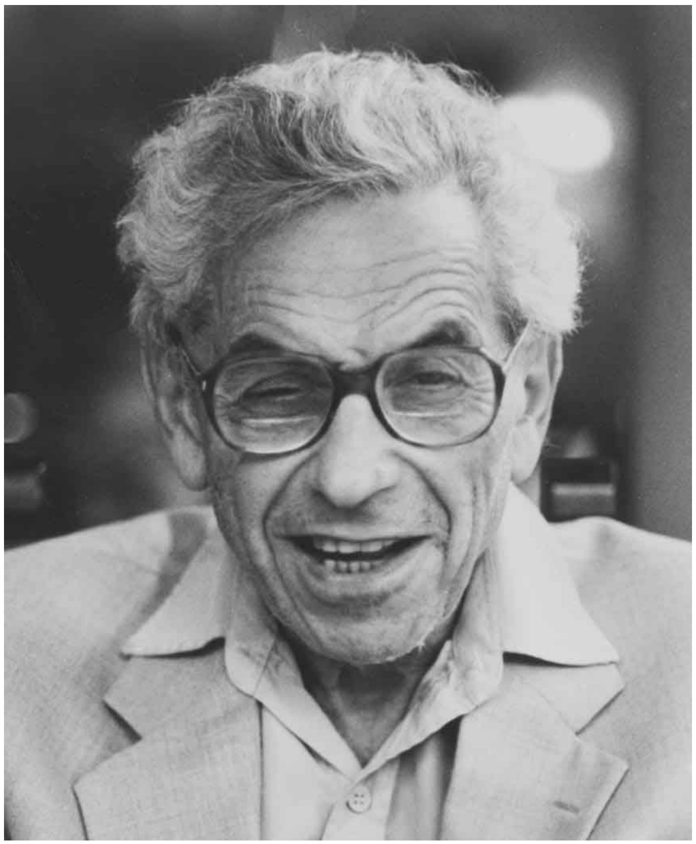
The two key ideas in the proof of the Besicovitch result:

- For any number x, the integers in $(x, 2x]$ form a primitive set.

- As $x \to \infty$, the density of the integers with a divisor in $(x, 2x]$ tends to 0.

So, by choosing a rapidly growing sequence $x_1 < x_2 < \dots$, where x_1 is already very large, and taking $\mathcal{S}_k$ as the set of numbers in $(x_k, 2x_k]$ not divisible by any number in $\mathcal{S}_i$ for $i < k$, and then letting $\mathcal{S} = \cup \mathcal{S}_k$, we have our dense primitive set.

But what about the lower density of a primitive set?



Erdős showed in 1935 that not only must the lower asymptotic density of a primitive set be 0, but

$$\sup_{\mathcal{S}\ \text{primitive}} \sum_{n\in\mathcal{S}\setminus\{1\}} \frac{1}{n\log n} < \infty.$$

It is thought that the supremum is achieved for the set of primes, but this is still not known.

Recall that $S(x) = |\mathcal{S}\cap[1,x]|$, the number of members of $\mathcal{S}$ in $[1,x]$. The case of the primes shows us that

$$S(x) \gg \frac{x}{\log x}$$

is possible for a primitive set. Can we do better? That is, can we find larger (concave down) functions here than $x/\log x$?

Erdős: "The following problem seems difficult. Let $b_1 < \ldots$ be an infinite sequence of integers. What is the necessary and sufficient condition that there should exist a primitive sequence $a_1 < \ldots$ satisfying $a_n < cb_n$ for every n? From [my old result] we obtain that we must have $\sum 1/(b_n \log b_n) < \infty$. ...."

Ahlswede, Khachatrian, Sárközy (1999): *For each* $\epsilon > 0$ *there is a primitive set* $\mathcal{S}$ *such that*

$$S(x) \gg \frac{x}{\log_2 x \cdot (\log_3 x)^{1+\epsilon}}.$$

Here we write $\log_k$ for the k-fold iteration of log.

It is clear that this result is best possible, since if the counting function satisfied

$$S(x) \gg \frac{x}{\log_2 x \cdot \log_3 x},$$

then we would have $\sum_{n \in \mathcal{S}} 1/n \log n = \infty$.

One might view the Erdős problem mentioned above as whether the criterion $\sum 1/n \log n = O(1)$ is the only limitation on the growth of a primitive set. And the answer is essentially "yes for smoothly growing sequences":

Martin, P (2010): *Suppose that $L(x)$ is positive and increasing for $x \geq 2$, $L(2x) \sim L(x)$, and*

$$\int_2^\infty \frac{dt}{t \log t \cdot L(t)} < \infty.$$

Then there is a primitive set $\mathcal{S}$ such that

$$S(x) \asymp \frac{x}{\log_2 x \cdot \log_3 x \cdot L(\log_2 x)}.$$

In particular for each $\ell \geq 3$ and $\epsilon > 0$, there is a primitive set $\mathcal{S}$ with

$$S(x) \asymp \frac{x}{\log_2 x \cdot \ldots \cdot \log_{\ell-1} x \cdot (\log_\ell x)^{1+\epsilon}}.$$

Our primitive set is based on an increasing sequence of primes $p_1, p_2, \ldots$, where $p_j \ll j^2$ and $\sum 1/p_j < 1/2$. It is the union of the sets

$$\mathcal{S}_k = \{n : \Omega(n) = k,\ p_k \mid n,\ (n, p_1 \ldots p_{k-1}) = 1\}.$$

It is immediate that each $\mathcal{S}_k$ is primitive as is their union.

We show using the Sathe–Selberg theorem that

$$S_k(x) \asymp \frac{x}{\log x} \frac{(\log_2 x)^{k-2}}{(k-2)!} \frac{1}{p_k}.$$

We then show that $x/p_B \gg S(x) \gg x/p_{B'}$, where $B = \lfloor (1/2) \log_2 x \rfloor$ and $B' = \lfloor (3/2) \log_2 x \rfloor$.
To complete the proof, we show that we may take p_k as the $\lfloor kL(k) \rfloor$th prime.

And now for something completely different . . .

Must dense sets of integers contain a solution to $ab = c$?

Some examples of sets where this equation has no solutions:

- The set of negative integers.
- The set of integers with an odd number of prime factors.
- The set of $2^a(4b+3)$ where $a \geq 0$.
- The set of np^a where n is a quadratic nonresidue mod p, $a \geq 0$.

These examples all have density $1/2$.

Recently Hajdu, Schinzel, & Skalba (2009) showed that there are sets of integers with upper density arbitrarily close to 1 that are *product free*, namely there is no solution to $ab = c$ in the set.

Must it be true that any product-free subset of $\mathbb{Z}$ (or $\mathbb{N}$) must have lower density at most $1/2$?

Hajdu, Schinzel, Skalba (2009): *If the lower asymptotic density of a set of integers exceeds* $1/2$*, then there are members* a, b, c, d *with* $abc = d^2$.

Recently Schinzel conjectured: *If* n *is a positive integer, let* $F(n)$ *be the size of the largest product-free subset of* $\mathbb{Z}/n\mathbb{Z}$. *Then* $F(n) < n/2$.

Here are some examples:

n	$F(n)$
1	0
2	0
3	1
4	1
5	2
6	2
7	3
8	3
9	4
10	4

n	$F(n)$
11	5
12	4
13	6
14	6
15	6
16	7
17	8
18	8
19	9
20	8

Maybe

$$F(n) = \max\left\{ \left\lfloor \frac{q-1}{2} \right\rfloor \frac{n}{q} \;:\; q \mid n,\; q \text{ a prime power} \right\} \text{ ?}$$

P, Schinzel (2010): *The set of possible counterexamples to* $F(n) < n/2$ *lie in a set with asymptotic density smaller than* 1.56×10^{-8}.

We show this by showing that if n has no divisor m^2 with $\omega(m) \geq 6$, then $F(n) < n/2$.

With any product-free subset $\mathcal{S}$ of $\mathbb{Z}/n\mathbb{Z}$, we organize the elements by their gcd with n, where for $d \mid n$, we let $\mathcal{S}_d$ be the set of those $s \in \mathcal{S}$ with gcd$(s, n) = d$. Further, let

$$T_d = \{a \in \mathbb{Z}/n\mathbb{Z} : \text{gcd}(a, n) = d\}.$$

Suppose $uv \mid n$ and $\mathcal{S}_u \neq \emptyset$, with $s \in \mathcal{S}_u$. Then multiplication by s maps T_v to T_{uv} and since $\mathcal{S}$ is product free, it follows that $s\mathcal{S}_v \cap \mathcal{S}_{uv} = \emptyset$.

It follows that $|s\mathcal{S}_v| + |\mathcal{S}_{uv}| \leq |T_{uv}|$.

This observation is our principal tool.

In fact, it is possible using these thoughts to prove that the Schinzel conjecture $F(n) < n/2$ follows from the following conjecture:

For m a squarefree number and a positive integer k, consider real variables x_d where d runs over the divisors of m^k. We restrict these variables as folows:

$$x_d \in [0, 1], \quad uv \mid m^k \text{ implies } x_u + x_v + x_{uv} \le 2, \quad x_1 = 0.$$

Conjecture: Subject to these constraints, the maximum value of $\sum x_d/d$ is smaller than

$$\sum_{\substack{\mathrm{rad}(u)|m \\ \Omega(u) \text{ odd}}} \frac{1}{u},$$

where $\mathrm{rad}(u)$ is the largest squarefree divisor of u.

We have proved this linear-programming conjecture in the cases where m is either a prime or the product of two primes. Actually the tools we used to do this are similar to the tools we used to directly attack the product-free problem, so it is not clear that this linear-programming perspective is making progress.

We have not exhausted all of our tools in getting the 1.56×10^{-8} result, we have just exhausted ourselves.

Perhaps a fresh effort to improve our result will allow one to see a general pattern, and not only get a smaller density for the exceptional set, but prove there are no exceptions.

THANK YOU!

Happy birthday András, Kálmán, János, and Attila!