# Product-free sets of integers

Carl Pomerance, Dartmouth College
Hanover, New Hampshire, USA

Integers Conference, Carrollton, GA, 2011

Based on joint work with
P. Kurlberg, J. C. Lagarias, & A. Schinzel

An easy problem: How large a subset of $\mathbb{Z}/n\mathbb{Z}$ can you find, where

$$a + b \not\equiv c \pmod{n}$$

for all $a, b, c$ in the set?

An easy problem: How large a subset of $\mathbb{Z}/n\mathbb{Z}$ can you find, where

$$a + b \not\equiv c \pmod{n}$$

for all $a, b, c$ in the set?

If the set has more than $n/2$ elements and $a$ is a fixed element from the set, then there are more than $n/2$ sums $a + s$ as $s$ varies over the set, so one of these sums is in the set.

On the other hand, if $n$ is even, the odd residues comprise a sum-free set of size $n/2$. (For $n = p$, a prime, one cannot beat in general taking the middle third of the residues, since if $S$ is sum-free, then $|S| + |S + S| \le p$, so the Cauchy–Davenport inequality implies that $|S| \le (p + 1)/3$.)

Thus, we know a lot about the problem for $\mathbb{Z}/n\mathbb{Z}$. What about for $\mathbb{Z}$?

The odd numbers have density 1/2 and form a sum-free set.

On the other hand, if $S$ is sum-free and $a$ is the least member of $S$, then for each $s \in S \cap [1, x]$, the number $a + s$ cannot be in $S$. Thus,

$$|S \cap [1, x]| \le |S \cap [1, x + a]| \le (x + a) - (a - 1) - |S \cap [1, x]|$$

so that $|S \cap [1, x]| \le (x + 1)/2$ and the upper density of $S$ is at most 1/2.

So, let's make a tiny, insignificant change in the problem.
Consider *product-free* sets.
That is, $ab \neq c$ for all $a, b, c$ in the set.

Well, we can see something new, since the integers in $(\sqrt{x}, x]$ form a product-free set and there are close to $x$ of them. But this construction can't be continued to infinity, while consistently keeping up such a high density.

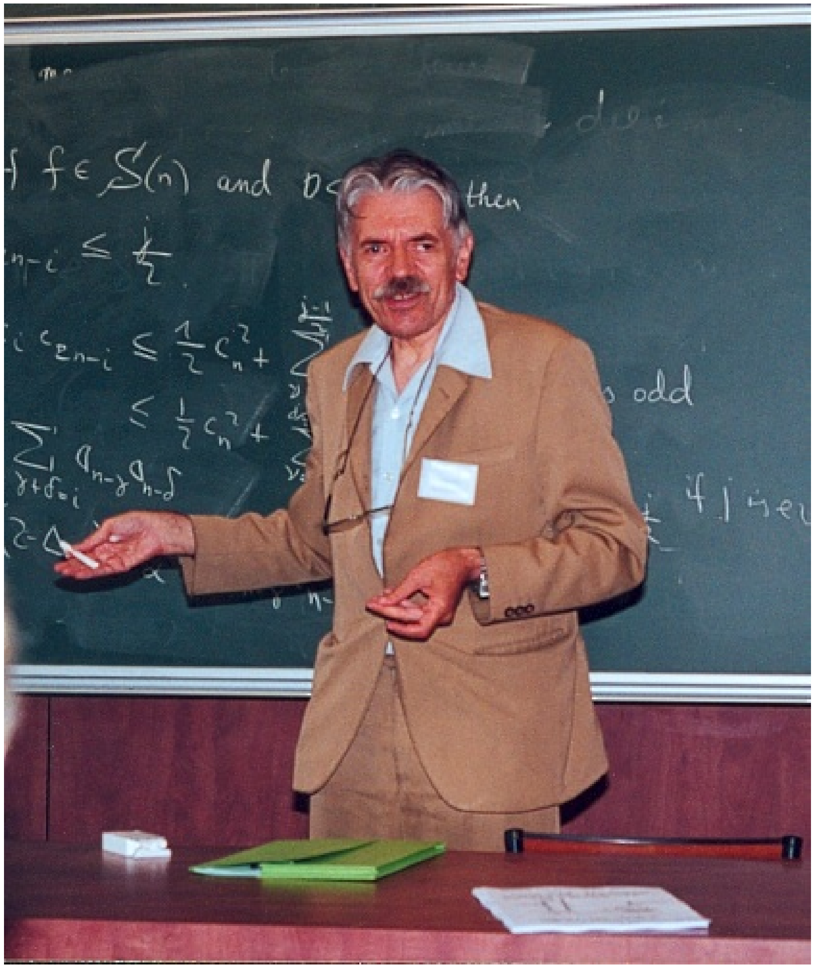
What about product-free sets (mod $n$)? Let $D(n)$ denote the maximum possible value of $|S|/n$ where $S$ runs over product-free sets in $\mathbb{Z}/n\mathbb{Z}$.

So, $D(1) = D(2) = 0$, $D(3) = 1/3$, $D(4) = 1/4$, $D(5) = 2/5$, not too exciting ...

$D(n)$ is the max of $|S|/n$ where $S$ runs over product-free sets in $\mathbb{Z}/n\mathbb{Z}$.

**P, Schinzel** (2011): *We have $D(n) < \frac{1}{2}$ for all $n$ except possibly those $n$ divisible by a squarefull number with at least 6 distinct prime factors. Further, the asymptotic density of those $n$ whose squarefull part does have at least 6 distinct prime divisors is about $1.56 \times 10^{-8}$.*

Moscow Journal of Combinatorics and Number Theory,
**1** (2011), 52–66.



Andrzej Schinzel

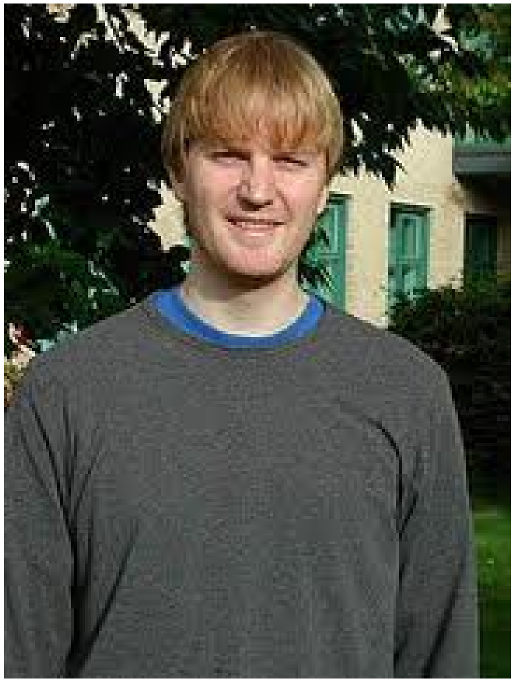
Surely that cements it, and $D(n) < \frac{1}{2}$ for all $n$, right?

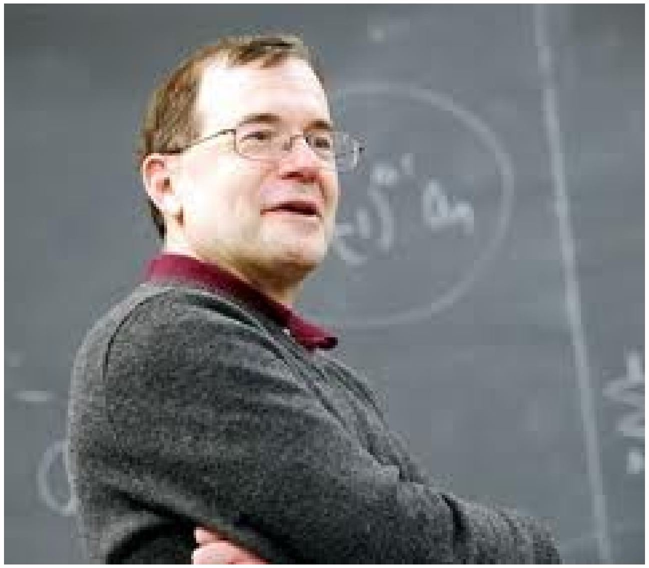
Surely that cements it, and $D(n) < \frac{1}{2}$ for all $n$, right?

Well, no.

**Kurlberg, Lagarias, P** (2011): *There are infinitely many values of $n$ with $D(n)$ arbitrarily close to* 1*. In particular, there are infinitely many values of $n$ where all of the pairwise products of a subset of* 99% *of the residues* $\pmod n$ *all fall into the remaining* 1% *of the residue classes.*

Acta Arithmetica, to appear in a special issue in honor of Andrzej Schinzel's 75th birthday.





Pär Kurlberg

Jeffrey C. Lagarias

Let's be more modest, just show me one $n$ where $D(n) \geq \frac{1}{2}$.

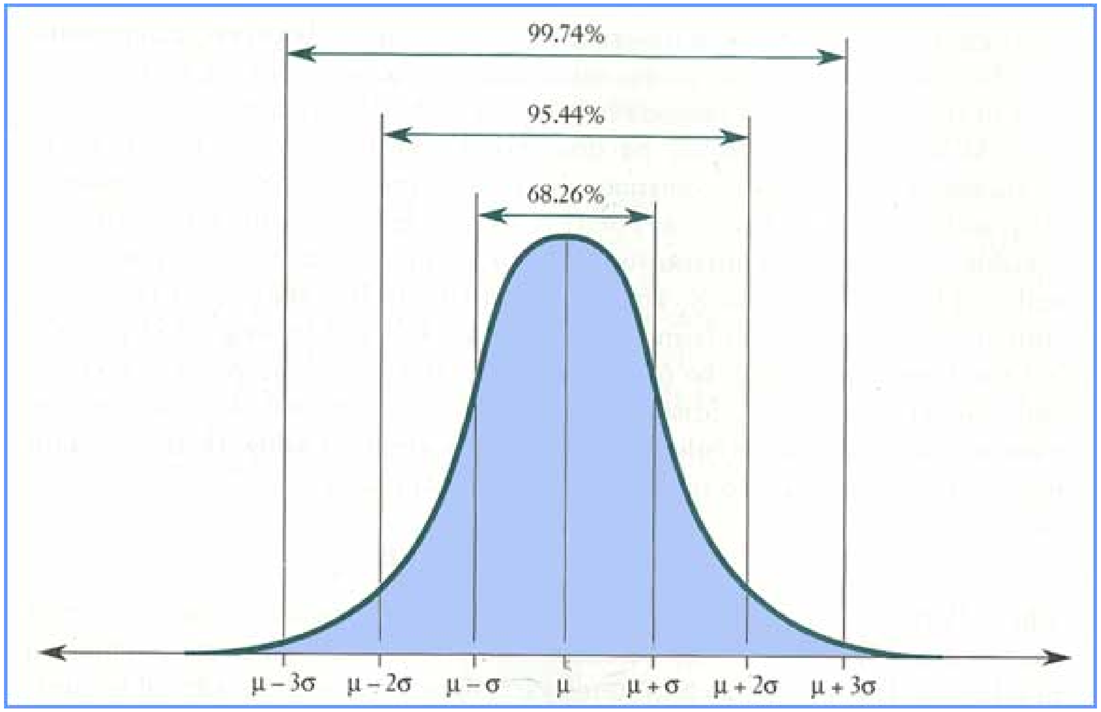
It's not so easy!

Here's a number. Take the first 10,000,000 primes. For those primes below 1,000,000, take their 14th power, and for those that are larger, take their square, and then multiply these powers together to form $N$. Then $D(N) > 0.5003$. Further, $N \approx 10^{1.61\times10^8}$.

Can you find an example with fewer than 100,000,000 decimal digits?

What is behind this construction and proof?

What is behind this construction and proof?



Yes, it is the normal distribution, the bell curve. The idea is that $\Omega(m)$, the total number of prime factors of $m$ counted with multiplicity, obeys a normal distribution; this is the Erdős–Kac theorem. Further, any set of integers which for some $t$ has $\Omega(m) \in [t, 2t)$ for all $m$ in the set, must be product-free. So, if $N$ is divisible by all small primes to high powers, and we take residues (mod $N$) whose gcd with $N$ is one of these numbers $m$, we can create a dense product-free set.

How dense?

**Kurlberg, Lagarias, P** (2011): *There are positive constants* $c_1, c_2$ *such that for infinitely many* $n$ *we have*

$$D(n) > 1 - \frac{c_1}{(\log\log n)^{1-\frac{1}{2}\mathrm{e}\log 2}\sqrt{\log\log\log n}}$$

*and for all* $n$ *we have*

$$D(n) < 1 - \frac{c_2}{(\log\log n)^{1-\frac{1}{2}\mathrm{e}\log 2}\sqrt{\log\log\log n}}.$$

The idea for the upper bound: use linear programming!

A preprint will be posted soon.

For a product-free set $S$ in $\mathbb{Z}/n\mathbb{Z}$ and for $d \mid n$, let $\alpha_d$ be the proportion of those $s \in S$ with $\gcd(s,n) = d$ among all residues $r \pmod{n}$ with $\gcd(r,n) = d$.

Then each $\alpha_d$ is in $[0,1]$.

Further, if $|S| \geq n/2$, then $\alpha_1 = 0$ and for all $u, v$ with $uv \mid n$, we have

$$\alpha_u + \alpha_v + \alpha_{uv} \leq 2.$$

In some sense, $|S|/n$ is closely modeled by $\sum_{d|n} \alpha_d/d$.

So, the LP is to maximize $\sum_{d|n} \alpha_d/d$ given the above constraints.

Since we already know that $D(n)$ can be fairly large, we need not prove we have found the maximum of the LP, just some upper bound for it. It is known that any feasible solution to the *dual* LP gives an upper bound for the primary LP. Thus, we write down the dual LP, find a fairly trivial feasible solution, and then "shift mass" to make it better.

And, voilà, our upper bound for all $n$'s tightly matches our constructed lower bound for champion $n$'s.

**Thank You!**