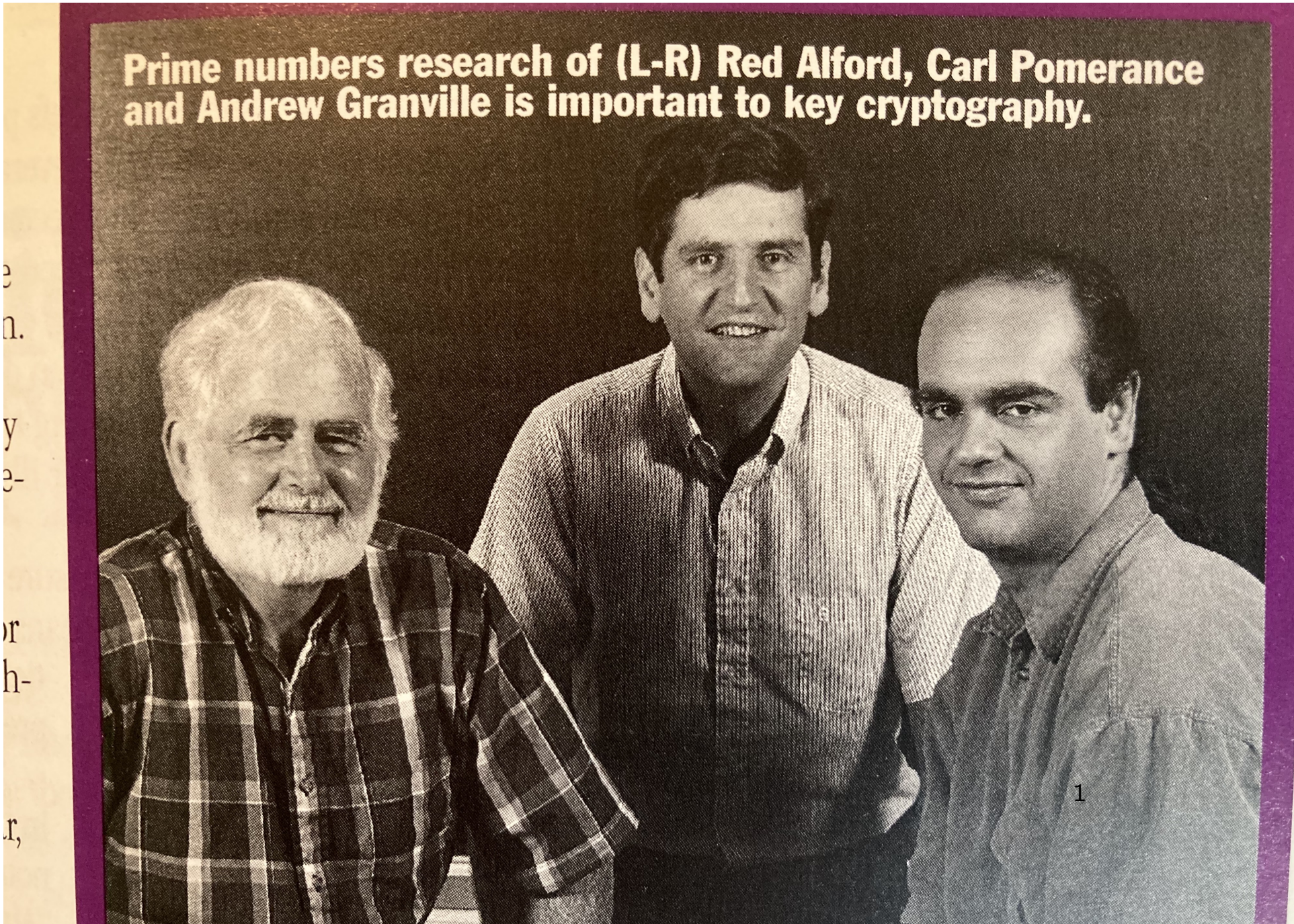
A celebration of analytic number theory,

a conference in honor of Andrew Granville

CRM, Montréal, Canada, September 5–9, 2022

Permutations and arithmetic

Carl Pomerance, Dartmouth College



Prime numbers research of (L-R) Red Alford, Carl Pomerance and Andrew Granville is important to key cryptography.

A simple question:

Given two intervals I, J of n consecutive integers is there always a one-to-one correspondence from I to J

A simple question:

Given two intervals I, J of n consecutive integers is there always a one-to-one correspondence from I to J with corresponding numbers relatively prime?
We're asking for a matching in the coprime graph.

A simple question:

Given two intervals I, J of n consecutive integers is there always a one-to-one correspondence from I to J with corresponding numbers relatively prime?
We're asking for a matching in the coprime graph.

A simple answer: No.

For example, $I = \{4\}$, $J = \{6\}$.

Or $I = \{3, 4\}$, $J = \{5, 6\}$.

Or $I = \{4, 5, 6\}$, $J = \{12, 13, 14\}$.

In the first two examples, $\{4\}$, $\{6\}$ and $\{3,4\}$, $\{5,6\}$, one set contains a number divisible by a prime divisor of each number in the other set. Namely, "6" in both cases.

The third example, $\{4,5,6\}$, $\{12,13,14\}$, has a strict majority of even numbers in both sets.

There are other "monsters" too, like

$$I = \{10,11,12,13\},\ J = \{15,16,17,18\}.$$

(Both 10 and 12 match only to 17.)

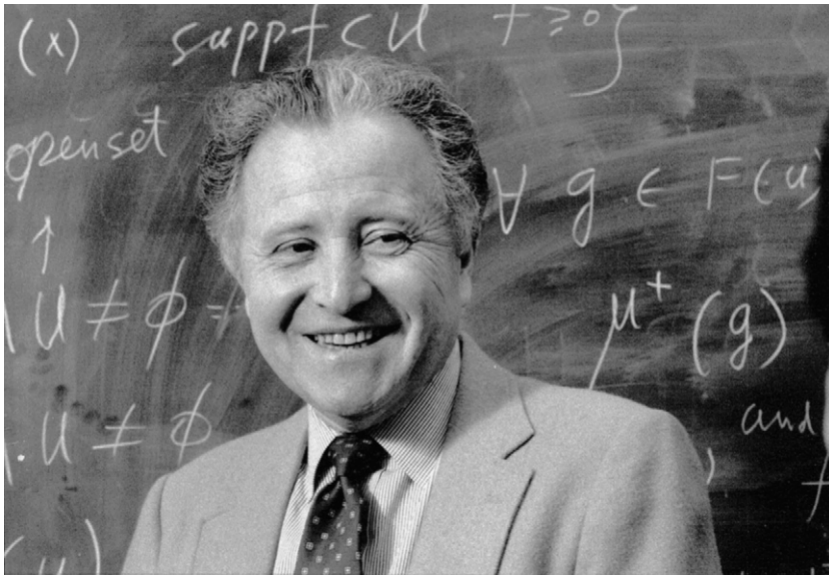
Around 1960, **D. J. Newman** conjectured that in the special case that

$I = [n] = \{1, 2, \ldots, n\}$, J is any interval of n consecutive integers,

there must be a coprime matching. (That is, there is a 1-1 correspondence with corresponding numbers coprime.)

In a lecture in 1962 at the University of Reading, **Paul Erdős** offered £5 for a proof of the weaker conjecture where $I = [n]$ and $J = \{n+1, \ldots, 2n\}$. A year later, two Reading professors, **D. E. Daykin** and **M. J. Baines** proved this weaker conjecture. Mike Baines tells me they collected £2.5 each.

In 1971, **Vašek Chvátal** proved the full Newman conjecture for $n \leq 1000$.



D. J. Newman

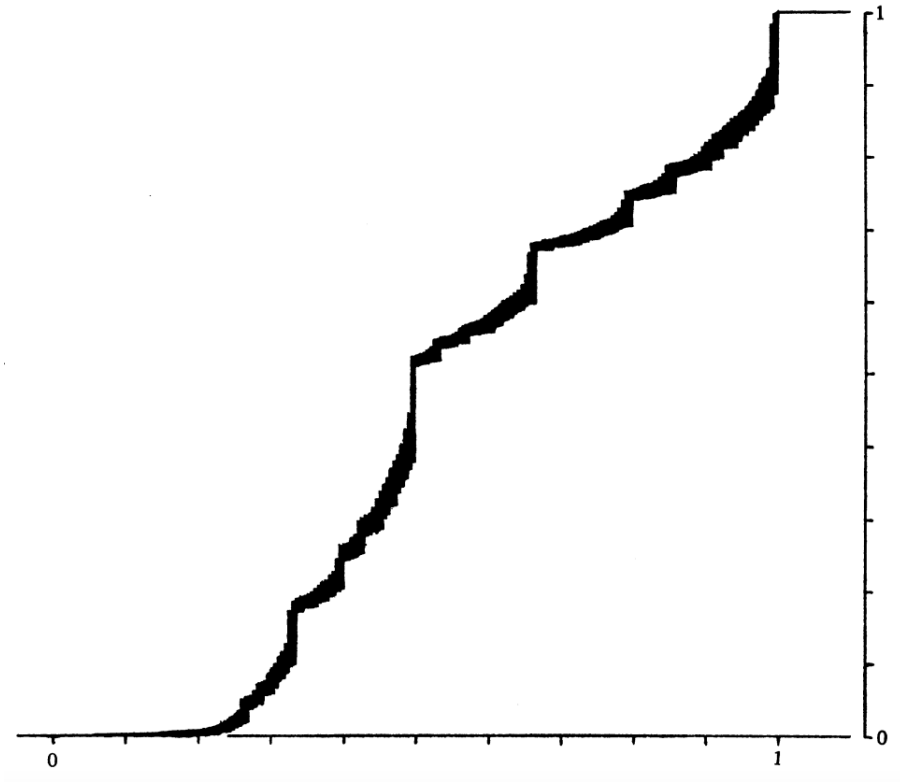
Vašek Chvátal

In 1979 I attended a conference in Carbondale, Illinois, meeting **John Selfridge** who told me about Newman's conjecture, and described an algorithm that, if correct, would give a coprime matching.

We worked on this for a few months, and ended up with a proof of Newman's conjecture, using the distribution function of $\varphi(n)/n$.

John Selfridge

The distribution function for $\varphi(n)/n$ (from a paper of Charles Wall). We were interested in the related distribution for odd n.



What about the case when $I = J = [n]$, so we would have a coprime permutation?

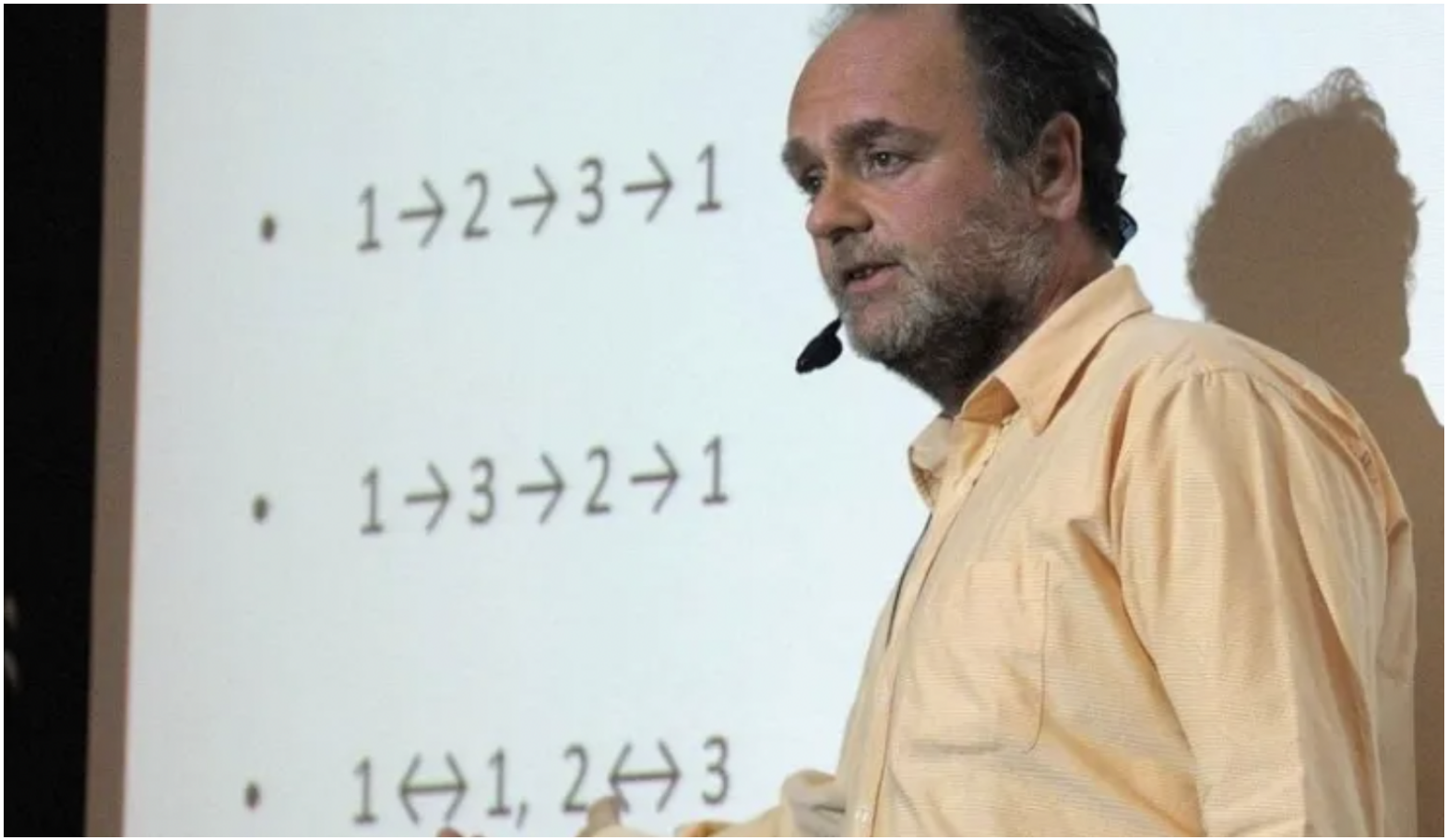
What about the case when $I = J = [n]$, so we would have a coprime permutation?

Easy! Just take the cycle $(1, 2, \ldots, n)$.

What about the case when $I = J = [n]$, so we would have a coprime permutation?

Easy! Just take the cycle $(1, 2, \ldots, n)$.

OK, a better question: Enumerate them. How many coprime permutations are there of $[n]$?



Here is Andrew enumerating the case $n = 3$; there are 3 of them.

Let $C(n)$ denote the number of permutations σ of $[n]$ where each $\gcd(j, \sigma(j)) = 1$. So, for example, $C(3) = 3$.

Also $C(4) = 4$: It's an even–odd thing. The numbers 2, 4 must be sent to 1, 3 in some order, and vice versa.

Maybe $C(n) = n$? Well no. **David Jackson** computed $C(n)$ for $n \leq 24$ in 1977, and e.g., $C(24) = 1{,}142{,}807{,}773{,}593{,}600$.

Jackson's view of the problem: Take the $n \times n$ matrix M where the i, j entry is 1 if $\gcd(i, j) = 1$ and is 0 otherwise (the adjacency matrix for the coprime graph on $[n]$). Then $C(n)$ is the *permanent* of M.

Let $C_0(n)$ be the number of coprime matchings of $[n]$ and $[n]_o$, the first n odd numbers. As we saw with $C(4)$, we have $C(n) = C_0(n/2)^2$ for n even. This observation immediately gives us a nontrivial upper bound for $C(n)$ when n is even, namely

$$C(n) \leq (n/2)!^2, \ n \text{ even.}$$

A similar argument shows that $C(n) \leq (m+1)!^2$ when $n = 2m+1$ is odd.

We conclude: $C(n) \leq n!/(2+o(1))^n$ and so most permutations are *not* coprime.

Is this the magnitude for $C(n)$, i.e., is there a similar lower bound?

Using similar methods as in my paper with **Selfridge**, I was able to prove that

$$C(n) \geq n!/3.73^n \quad \text{for all large } n,$$

and I was able to improve the upper bound to $C(n) \leq n!/(2.5 + o(1))^n$.

A former student of mine, **Nathan McNew**, came up with a clever heuristic that

$$C_n = n!/(c_0 + o(1))^n, \text{ where } c_0 = 2 \prod_{p>2} \frac{p(p-2)^{1-2/p}}{(p-1)^{2-2/p}} = 2.65044\ldots.$$

The heuristic behind this is that for a fixed prime p, the number of permutations σ of $[n]$ with $p \nmid \gcd(j, \sigma(j))$ for each j is $n!/(\gamma_p + o(1))^n$, where $\gamma_p = p(p-2)^{1-2/p}/(p-1)^{2-2/p}$. And then argue "independence".

A couple of days after posting to arXiv, two grad students at MIT proved this conjecture. These are **Ashwin Sah** and **Mehtaab Sawhney**.

Ashwin Sah

Mehtaab Sawhney

But as soon as one problem is solved, a few more arise! For example:

1. How many "anti-coprime" permutations are there of $[n]$ (meaning that each $\gcd(j, \sigma(j)) > 1$ for $j > 1$)?

2. How many permutations of $[n]$ are there where for each j either $j \mid \sigma(j)$ or $\sigma(j) \mid j$? Or, for each j, $\mathrm{lcm}[j, \sigma(j)] \leq n$?

Anti-coprime permutations of $[n]$: Each $\gcd(j, \sigma(j)) > 1$ for $j > 1$.

One way to construct these is to partition the j's in $[n]$ by their least prime factor $P^-(n)$:

$$\mathcal{L}_p = \{j \in [n] : P^-(j) = p\},$$

and then consider permutations σ where each $\sigma(\mathcal{L}_p) = \mathcal{L}_p$. Note that $\#\mathcal{L}_2 \sim \frac{1}{2}n$, $\#\mathcal{L}_3 \sim \frac{1}{6}n$, etc. For $p \le n^\epsilon$ and p large, we have

$$\#\mathcal{L}_p \sim \frac{n}{p} \prod_{q<p} \left(1 - \frac{1}{q}\right) \sim \frac{n}{e^\gamma p \log p}.$$

Doing the calculations, we get that the number $A(n)$ of anti-coprime permutations of $[n]$ has

$$A(n) \ge \frac{n!}{(\log n)^{(e^{-\gamma}+o(1))n}}.$$

But is this construction optimal? Very recently I proved this is essentially so, and in fact

$$A(n) = \frac{n!}{(\log n)^{(e^{-\gamma}+o(1))n}}, \qquad n \to \infty.$$

For a long time I tried taking the primes in order: 2, 3, ..., but then I realized that most of the difference from $n!$ comes from larger primes. Indeed, for those j with $P^-(j)$ large, there are not so many choices for a number j' with $\sigma(j) = j'$.

The permutations σ of $[n]$ where each $j \mid \sigma(j)$ or $\sigma(j) \mid j$ has its own story. In a talk at the Southeastern Conference on Combinatorics, Graph Theory, and Computing in Boca Raton, Florida in 1983, **Paul Erdős** proposed the following problem:

Consider the divisor graph on $[n]$ where two distinct numbers j, k are connected by an edge if and only if $j \mid k$ or $k \mid j$. Show that the length of the longest simple path in this graph has length $o(n)$.

Erdős offered $\$25$ for a resolution of this problem, and he paid up when I solved it a few weeks later. It's the only time I won an Erdős prize.

We now know after work of **Tenenbaum** and **Saias** that the length of the longest simple path in the divisor graph is of magnitude $n/\log n$.

But we're talking about permutations of $[n]$, and we'd like to know how many there are where each $j \mid \sigma(j)$ or $\sigma(j) \mid j$. I very recently showed that the count is between 1.93^n and 13.6^n.

Surely we should be able to do better!

And sure enough we can.

McNew just proved that the count is $(c+o(1))^n$ where $2.069 < c < 2.694$, with a similar result for the lcm problem.

Thank you,

Thank you,

and happy birthday Andrew!