Dartmouth College Combinatorics Seminar
May 17, 2022

Coprime permutations

Carl Pomerance, Dartmouth College

This talk is in the area of combinatorial number theory (aka arithmetic combinatorics). It is a branch of mathematics that considers number-theoretic problems with a combinatorial flavor. A totemic theorem from a century ago:

van der Waerden: *If* $\mathbb{N}$ *is partitioned into two sets, at least one of them contains arbitrarily long arithmetic progressions.*

Fields Medalists **Roth**, **Gowers**, and **Tao** have all found significant improvements of van der Waerden's theorem, and **Szemerédi** recently won the Abel Prize, in part for the same.

These results are unrelated to the talk, and here is another!

Say a set $\mathcal{A}$ of integers larger than 1 is *primitive* if no member divides another. For example, $\mathcal{A}$ could be the set of primes, or it could be the set of integers which are the product of two primes, or many other possibilities. **Erdős** proved in the 1930s that if $\mathcal{A}$ is primitive, then

$$\sum_{a \in \mathcal{A}} \frac{1}{a \log a} < \infty,$$

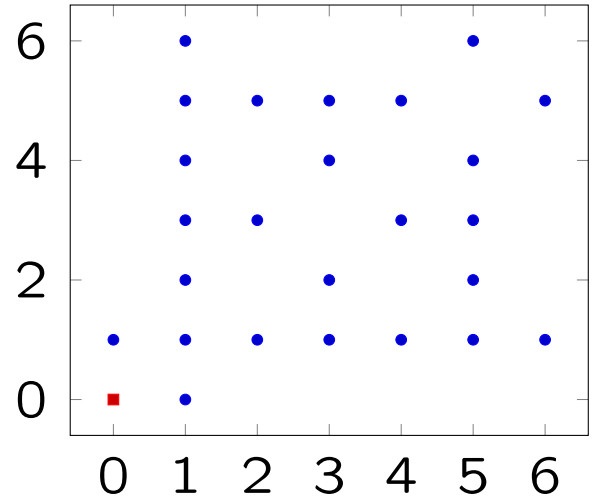
and in fact, there is a finite upper bound for all such sums. In the 1980s, he asked if the maximum value for such a sum is given when $\mathcal{A}$ is the set of primes. Known now as the "Erdős primitive set conjecture," this was just proved by **Jared Lichtman** (class of '18 and a current grad student at Oxford).

An elementary and fundamental concept: Two integers are *relatively prime*, or more briefly, *coprime*, if their greatest common divisor is 1.

This thought can lead one into number theory, and also graph theory! (Take the graph on $\mathbb{N}$ where there is an edge between m, n if they are coprime. The number 1 is connected to everything else, including itself.)

Here's a third view, through geometry:

Visible lattice points: integer points (x, y) with x, y coprime.



The proportion of lattice points that are visible is

$$\prod_{p \text{ prime}} (1 - 1/p^2) = 6/\pi^2.$$

(**Elizalde & Woods** have considered generalizations in higher dimensions.)

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.)

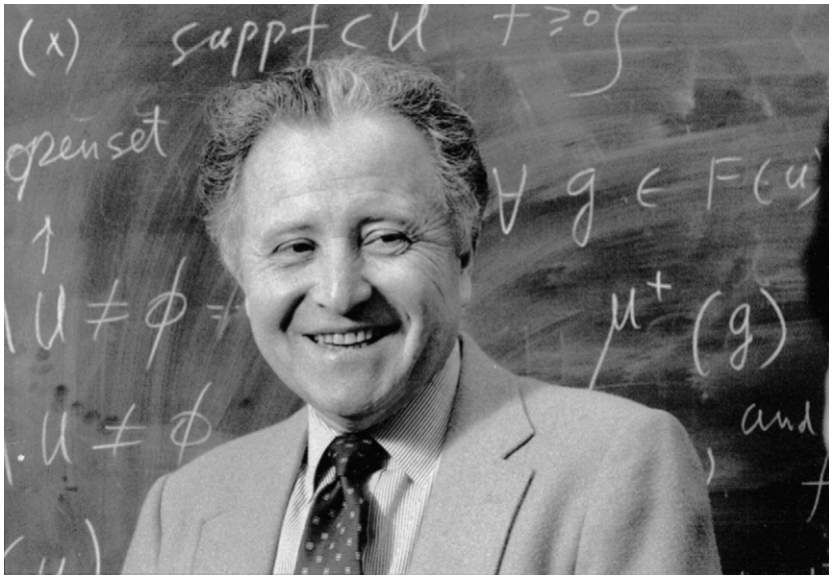
Around 1960, **D. J. Newman** conjectured that in the special case that

$I = [n] = \{1, 2, \ldots, n\}$, 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, published in Mathematika in 1980.

John Selfridge

Selfridge's algorithm:
First assume that n is even. Let J_0 be the even members of J and let J_1 be the odd members. Let m be the product of the elements of J_1. By an induction hypothesis (this is a recursive algorithm), there is a coprime matching between $[n/2]$ and $\frac{1}{2}(J_1 + m)$. This gives a coprime matching between the even members of $[n]$ and J_1.

Now take the odd members of $[n]$ and order them from hardest to match to easiest: $a_1, a_2, \ldots, a_{n/2}$, where

$$\varphi(a_1)/a_1 \leq \varphi(a_2)/a_2 \leq \ldots \leq \varphi(a_{n/2})/a_{n/2} = 1.$$

Here φ is Euler's function: $\varphi(a) =$ the number of members of $[a]$ coprime to a. Then choose $b_1 \in J_0$ coprime to a_1, then $b_2 \in J_0$ coprime to a_2 with $b_2 \neq b_1$, etc.

The algorithm in the case that n is odd is similar.

So, the hard work is in showing that one can continue with the choosing of the numbers b_i, never being blocked.

For a given a, the proportion of numbers coprime to a is $\varphi(a)/a$, while the proportion of odd numbers a' with $\varphi(a')/a' \leq \varphi(a)/a$ (so a' essentially comes before a in our ordering) is $D(\varphi(a)/a)$. Here $D(u)$ is the relative asymptotic density of the odd numbers a with $\varphi(a)/a \leq u$. (By a theorem of **I. J. Schoenberg** in 1928, this density exists.) So, basically what **Selfridge** conjectured is that $D(u) \leq u$ and that the "at infinity" asymptotics can be made rigorous at a finite level.

And this is what we proved.

Fast forward 40+ years, and last fall **Tom Bohman** and **Fei Peng** posted a paper to arXiv, proving the following:

Bohman, Peng: Suppose n is even and I, J are intervals of n consecutive integers contained in $[N]$. There is a positive constant c such that if $n > e^{c(\log\log N)^2}$ then there is coprime matching from I to J.

They used this result to prove a weak form of the "lonely runner conjecture" (more on this shortly). I was intrigued, having worked on this conjecture and coprime matchings, and I was able to improve this:

P: The same, but we only require that $n > c(\log N)^2$.

The lonely runner conjecture: Suppose $v_1, \ldots, v_k$ are distinct positive integers. There is some real number t such that the fractional parts $\{v_1 t\}, \ldots, \{v_k t\}$ are all in $[1/(k+1), 1-1/(k+1)]$.

One thinks of k runners on a circular track of length 1, with the v_i being their velocities. The special time t here makes a $(k+1)$st runner with speed 0 lonely. This was proved for $k=4$ by **Tom Cusick** and me in 1984, for $k=5$ by **Bohman, Holzman, & Kleitman** in 2001, and $k=6$ by **Barajas & Serra** in 2008.

Terry Tao (2018) showed it in the general case when all velocities are $\leq 1.2k$ and the new results on coprime matchings show it holds when the velocities are $\leq (2-\epsilon)k$. The connection, shown by **Bohman, Peng**, is not at all obvious. (My result gets a slightly smaller ϵ than the **Bohman, Peng** result.)

A brief word on my proof: Given a positive integer m one can ask for the length of the longest interval of consecutive integers each of which is *not* coprime to m. For example, if $m = 6$, we have the integers $\{2, 3, 4\}$ and for $m = 30$, we have $\{2, 3, 4, 5, 6\}$. This is the Jacobsthal function j, so $j(6) = 3$ and $j(30) = 5$. It is known that $j(m)/\log m$ is unbounded and that $j(m) = O((\log m)^2)$, a result of **Henryk Iwaniec**. (It's conjectured that $j(m) = O(\log m(\log\log m)^2)$ and that this is best possible.) My argument for the coprime matching result uses this circle of ideas.

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 $[n]$?

Let $C(n)$ denote the number of permutations σ of $[n]$ where each $\gcd(j, \sigma(j)) = 1$. So, for example, $C(4) = 4$.

Proof. It's an even–odd thing. The numbers 2, 4 must be sent to 1, 3 in some order, and vice versa.

I asked Sergi if he knew anything about this problem. He computed the first few values and then checked OEIS, finding that **David Jackson** had computed $C(n)$ for $n \leq 24$ in 1977.

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

We have seen that $C(n) = C_0(n/2)^2$ for n even. A similar argument shows that $C(n) \geq C_0(m-1)^2$ when $n = 2m+1$ is odd. So, basically we are interested in a lower bound for $C_0(n)$.

Note that $C_0(n)$ also has an OEIS page! It is the number of partitions of $[2n]$ into unordered coprime pairs.

Let's take a clue from the algorithm that gets a coprime matching in the Newman problem. We organize the first n odd numbers by increasing value of $\varphi(a)/a$. For example, how many of them have $\varphi(a)/a \leq 1/2$? In our previous notation, this would be $\sim D(1/2)n$. So, what is $D(1/2)$? This has been studied, and the best we have is

$$0.02240 < D(1/2) < 0.02352,$$

a result of **Mits Kobayashi**. So, the overwhelming majority of odd numbers have many coprime companions.

In general, consider an interval $(\alpha, \beta]$ in $[0, 1]$. The number of odd a among the first n odd numbers with $\varphi(a)/a \leq \beta$ is $\sim D(\beta)n$, while if $\varphi(a)/a > \alpha$, then there are at least $\sim \alpha n$ coprime companions for a to which it can be mapped. If $D(\beta) < \alpha$, this can be done in many ways, not interfering with assignments for other a with $\varphi(a)/a \leq \beta$.

If we have m places in which to put k numbers, the number of ways is $m!/(m-k)!$. In our case, we have $m \geq \alpha n - D(\alpha)n$ and $k = D(\beta)n - D(\alpha)n$. So, the number of assignments for these values of a with $\varphi(a)/a \in (\alpha, \beta]$ is at least

$$= \frac{(\alpha n - D(\alpha)n)!}{(\alpha n - D(\beta)n)!}.$$

We then do this for a particular numerical partition of $(0, 1]$ into intervals $(\alpha, \beta]$.

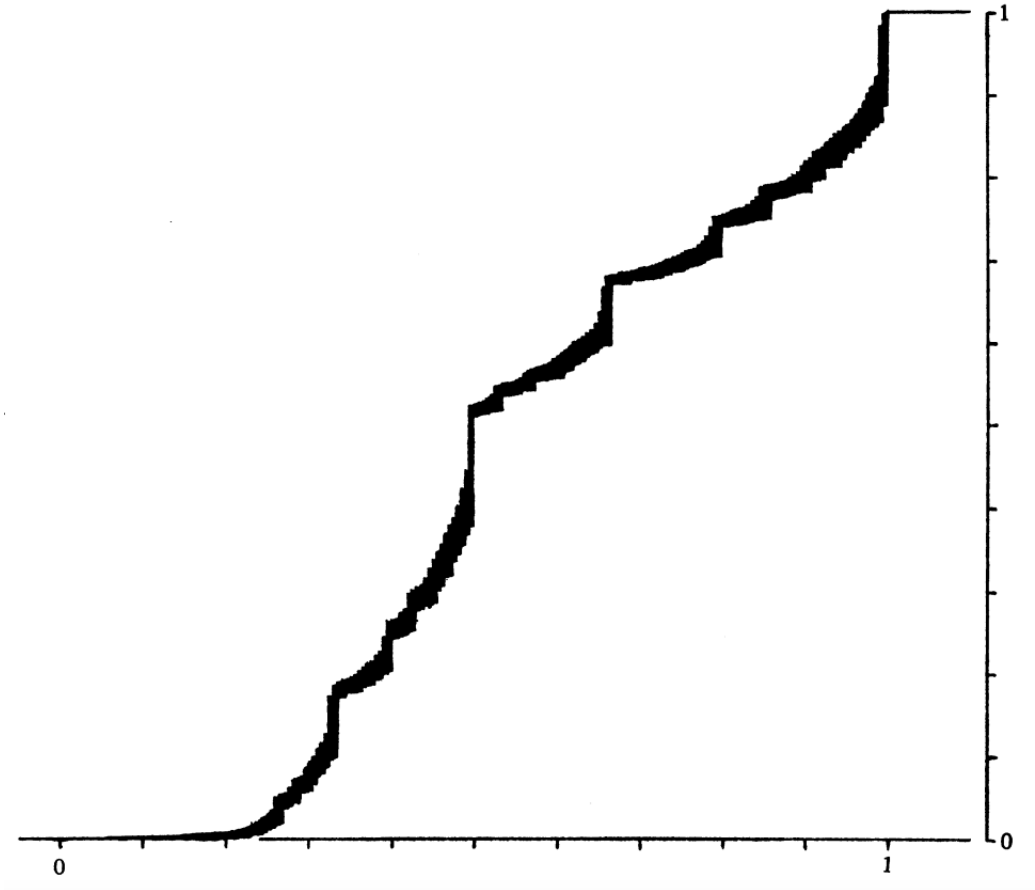
Other inequalities for the distribution function $D(u)$, due to **Charles R. Wall**, are used, as well as a strengthening of an inequality of **Paul Erdős**. When the dust settles, we have a proof that

$$C_0(n) \geq n!/1.8637^n \quad \text{for all large } n,$$

which in turn leads to

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

So, the question is if there is a constant c with $C(n) = n!/(c + o(1))^n$. My preprint has $2.5 \leq c \leq 3.73$.



From Wall's paper: the full distribution function for φ lies in the shaded area.

After showing a preliminary version of this paper to **Nathan McNew**, he came up with a conjectured value for c, namely

$$c = \prod_{p\,\text{prime}} \frac{p(p-2)^{1-2/p}}{(p-1)^{2-2/p}} = 2.65044\ldots.$$

(One takes the local factor at $p = 2$ as 2.) 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 my conjecture with McNew's constant c. These are **Ashwin Sah** and **Mehtaab Sawhney**.

Ashwin Sah

Mehtaab Sawhney

I think we'll be hearing more from these two in the future! They have already been the subject of a Quanta magazine article!

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 $j > 1$)? I have a lower bound of the shape $n!/(\log n)^{cn}$. Is this the true order of magnitude? I conjecture so, with $c = e^{-\gamma}$.

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, $\mathrm{lcm}[j, \sigma(j)] \leq n$? I can show the number of them is of the shape c^n, and have upper and lower bounds on c.

3. More problems?

Thank you