CANT 26

July 14, 2026

Two Topics in Combinatorial Number Theory

Carl Pomerance, Dartmouth College

The last few weeks have been a busy time for combinatorial number theory, broadly construed.

First, a disproof of the **Erdős** unit distance conjecture was announced. This is the conjecture that if one has n points in the plane, then the number of pairs of points at a unit distance is $\leq n^{1+o(1)}$.

REMARKS ON THE DISPROOF OF THE UNIT DISTANCE CONJECTURE

NOGA ALON, THOMAS F. BLOOM, W. T. GOWERS, DANIEL LITT, WILL SAWIN, ARUL SHANKAR, JACOB TSIMERMAN, VICTOR WANG, AND MELANIE MATCHETT WOOD

ABSTRACT. We present a short, digested, human-verified version of the recent OpenAI-generated counterexample to the Erdős unit distance conjecture, and a sequence of reflections on it. The argument relies crucially on ideas that may, at least in retrospect, be attributed to Ellenberg-Venkatesh, Golod-Shafarevich, and Hajir-Maire-Ramakrishna.

Then, there was a breakthrough on the sum-product problem. The origin of this problem, due to **Erdős** and **Szemerédi**, is to look at both the $n \times n$ addition table and multiplication table, and notice that the addition table has few distinct numbers compared with the multiplication table. If one changes the n numbers from $\{1, 2, \ldots, n\}$ to $\{2^1, 2^2, \ldots, 2^n\}$, then the addition table has many distinct numbers, while the multiplication table has few. They conjectured that this is always the case: given a set A of n integers, then $|A + A| + |A \cdot A| > n^{2-o(1)}$. In fact, this was conjectured as well when A is a set of real numbers. And now, this generalization to reals has been disproved.

THE SUM-PRODUCT CONJECTURE IS FALSE FOR REAL NUMBERS

THOMAS F. BLOOM, WILL SAWIN, CARL SCHILDKRAUT, AND DMITRII ZHELEZOV

Topic 1: Subgroups of the multiplicative group mod n.

Topic 2: Coprime matchings.

As we've seen, combinatorial number theory is quite broad and hard to pin down. And unquestionably, the master was Paul Erdős (1913–1996).

Drawing by LeUyen Pham, illustrator of The Boy Who Loved Math, by Deborah Heiligman

In 1986, **Erdős** and I published a paper about

$$\mathcal{F}(n) := \{a \pmod n : a^{n-1} \equiv 1 \pmod n\}.$$

Why is this set interesting? First, it is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

Note that if n is prime, it is the full multiplicative group mod n. And if n is composite, it is the subgroup of residues a for which n is a pseudoprime base a. Presumably this is usually a small subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, but can this be proved?

Let $F(n) = \#\mathcal{F}(n)$, so that $F(n)$ is the number of residues $a \pmod n$ such that $a^{n-1} \equiv 1 \pmod n$.

Theorem (**Erdős** & **P**, 1986) *For each real number $u \geq 0$, the set of n with $F(n) \leq (\log n)^u$ has an asymptotic density, this density function is continuous, strictly increasing, and tends to 1 as $u \to \infty$.*

Theorem (**Erdős** & **P**, 1986) *We have*

$$x^{15/23} < \frac{1}{x} \sum_{\substack{n \leq x \\ n \,\text{composite}}} F(n) \leq x^{1-(1+o(1))\log_3 x/\log_2 x},$$

the first inequality holding for sufficiently large x, the second as $x \to \infty$.

The exponent 15/23 is about 0.65. It is based on shifted primes $p-1$ with no large prime factors, and using newer results of **Lichtman**, the exponent can be increased to 0.71. However, we gave a heuristic argument that the upper bound is tight. That is,

$$\frac{1}{x} \sum_{\substack{n \le x \\ n \text{ composite}}} F(n) = x/L(x)^{1+o(1)}, \qquad (1)$$

where $L(x) := x^{1-\log_3 x/\log_2 x}$.

Based on earlier work of **Erdős** from the 1930s and 1950s, and subsequent work of mine, we had that the number $C(x)$ of Carmichael numbers $n \le x$ (these are composite numbers with $F(n) = \varphi(n)$) satisfies $C(x) \le x/L(x)^{1+o(1)}$, and that heuristically this is best possible. So the Carmichael numbers alone would give most of the story in (1).

Last November **Hendrik Lenstra** wrote to me asking about the function

$$\psi(n) = \#\{a \pmod n : a^n \equiv 1 \pmod n\}.$$

He writes: So that you may judge for yourself how interesting or non-interesting the function ψ is, let me tell you the ring-theoretic result in which I encountered it. It comes from work that I have been doing together with **Mike Daas** (a recent Leiden PhD, now in Luxemburg) and **Lars Pos** (a Leiden bachelor student), on the subject of a classical theorem of **Jacobson** from 1945. This theorem asserts that if n is a positive integer, and R is a ring with the property that all $x \in R$ satisfy $x^{n+1} = x$, then R is commutative.

Continuing: For $n = 1$ this is very classical: using $x^2 = x$ for $x = -1, a, b, a + b$, one deduces readily $ab = ba$. So, four x's are sufficient. I was quite surprised when I learnt that, still for $n = 1$, TWO x's suffice, namely $x = a$ and $x = ab - ba$. That is a charming and not entirely trivial exercise! (Whether a single x does it, we do not know!) How is this for general n? One of our results is the following upper bound for the number of (cleverly chosen) x's that suffice:

$$\varphi(n) + \psi(n) + 2\lceil \log(\tau(n))/\log 2 \rceil + E,$$

where $E \in \{0, 1, 2, 3\}$. [which he describes explicitly]

So the issue is to understand the function

$$\psi(n) = \#\{a \pmod n : a^n \equiv 1 \pmod n\}.$$

So, I thought it would be interesting to define a family of subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$:

$$\mathcal{F}_j(n) = \#\{a \pmod n : a^{n-j} \equiv 1 \pmod n\}$$

with $F_j(n) = \#\mathcal{F}_j(n)$. So Lenstra's $\psi(n)$ is $F_0(n)$ and the $F(n)$ from my paper with **Erdős** is $F_1(n)$.

It was not completely straightforward, but I did manage to show that the results for $F_1(n)$ do indeed generalize to each $F_j(n)$. (When $j > 0$, the analog of "n composite" is "when $j \mid n$, n/j is composite.") Interestingly, Lenstra's case $j = 0$ was the most difficult and required a somewhat different argument.

Let $\lambda(n)$ be Carmichael's lambda function, defined as the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$ (i.e., the maximal order of an element). We've seen that the Carmichael numbers (composites n with $\lambda(n) \mid n-1$, equivalently, $F_1(n) = \varphi(n)$) play a special role with $F_1(n)$. For $j = 0$, the special role is played by those n with $\lambda(n) \mid n$.

These numbers were considered briefly in a paper of **Luca** and myself from 2009. In this paper we noted that if $\lambda(n) \mid n$, then n is in the range of every iterate of λ. For example, $\lambda(20) \mid 20$ and $\lambda_j(5^{j+1}) = 20$ for every positive integer j. We proposed the following problem: Is the converse true? In particular, is 10 in the image of every iterate of λ?

Let Λ be the von Mangoldt function and let

$$g(n) = \sum_{d|n} \frac{\Lambda(d)}{\varphi(d)}.$$

Theorem. For each integer j, there is a set S_j of integers of asymptotic density 1, such that

$$F_j(n) = (\log n)^{g(n-j)+o(1)}$$

as $n \to \infty$, $n \in S_j$.

Erdős and I proved this for $j = 1$, and the generalization to arbitrary j is straightforward. The **Erdős–Wintner** theorem allows one to conclude that the asymptotic density of the set of n with $F_j(n) \le (\log n)^u$ exists and varies continuously and monotonically in u.

For a fixed integer $a > 1$ we can look at $P_a(x)$, the number of composite $n \le x$ with $a^{n-1} \equiv 1 \pmod{n}$. On average we have $P_a(x) \le x/L(x)^{1+o(1)}$, but we don't know this for any particular value of a, like $a = 2$. The best we have been able to prove is $P_a(x) \le x/L(x)^{1/2+o(1)}$. This in fact is known uniformly as $x \to \infty$ with $a \le x$. (**Li, P**)

How many different subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$ are of the form $\mathcal{F}_j(n)$? It turns out there are $\tau(\lambda(n))$ of them, where τ is the divisor function.

Luca and I considered some statistical properties of $\tau(\lambda(n))$ in 2007.

How many subgroups total are there? This can be for isomoprhism classes or for subsets which are subgroups. These problems have been recently considered by **Martin** and **Troupe**.

Topic 2: Coprime matchings.

A simple question:

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

Topic 2: Coprime matchings.

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.

Topic 2: Coprime matchings.

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.)

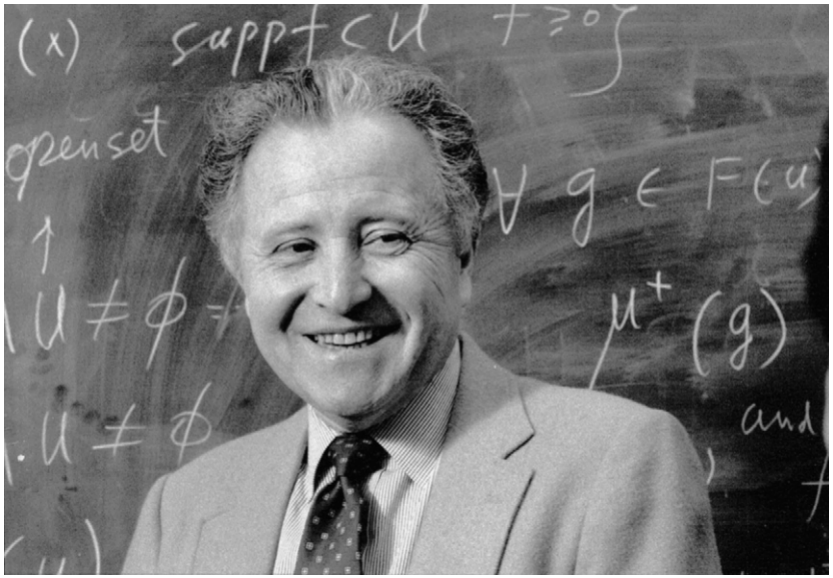
Around 1960, **D. J. Newman** conjectured that in the special case that

$I = [n] = \{1, 2, \ldots, n\}$, 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

Fast forward 41 years to 2021: **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 $n > c(\log N)^2$.

Tom Bohman

Fei Peng

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 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.)

Erdős and **Tao**

One can also ask for a coprime matching from $\{1, 2, \ldots, n\}$ to itself. These would be **coprime permutations**, and it is interesting to count them.

Let $C(n)$ denote the number of coprime permutations of $\{1, 2, \ldots, n\}$.

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

I asked a colleague, **Sergi Elizalde** 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.

Using some of the techniques from my paper with **Selfridge** on Newman's conjecture, I was able to show that for all large n,

$$\frac{n!}{3.73^n} \leq C(n) \leq \frac{n!}{2.5^n}.$$

Then, **McNew** identified a constant c where it seemed likely that $C(n) = n!/(c + o(1))^n$, and then **Sah** and **Sawhney**, grad students at MIT at the time, proved it.

Ashwin Sah

Mehtaab Sawhney

Nathan McNew

MATCHABLE NUMBERS

NATHAN MCNEW AND CARL POMERANCE

ABSTRACT. We say a natural number n is matchable if there is a bijection from the set of $\tau(n)$ divisors of n to the set $\{1, 2, \ldots, \tau(n)\}$, where corresponding numbers are relatively prime. We show that the set of matchable numbers has an asymptotic density, which we compute, and we show that every squarefree number is matchable. We also present some related unsolved problems.

(Just appeared in Mathematika)

Let $\tau(n)$ denote the divisor function. Is there a **coprime matching** between the set of $\tau(n)$ divisors of n and $\{1,2,\ldots,\tau(n)\}$? If so, we say n is matchable. This concept was introduced by Bernardo Recamán on mathoverflow in 2022. He asked if more numbers are matchable than not.

For example, 6 is matchable:

$$1 \iff 4, \quad 2 \iff 3, \quad 3 \iff 2, \quad 6 \iff 1.$$

And 8 is not matchable: The divisors are $\{1,2,4,8\}$ which contains 3 even numbers, but $\{1,2,3,4\}$ contains only 2 odd numbers. Similarly all the multiples of 4, starting with 8, are not matchable.

If m is composite, then $27m$ is not matchable. (Use a similar argument with multiples of 3: there are too many of them among the divisors of $27m$.)

So the upper density of the set of matchable numbers is $\leq (1-2^{-2})(1-3^{-3})$.

This generalizes to all primes, and we get the upper density of the matchable numbers is at most

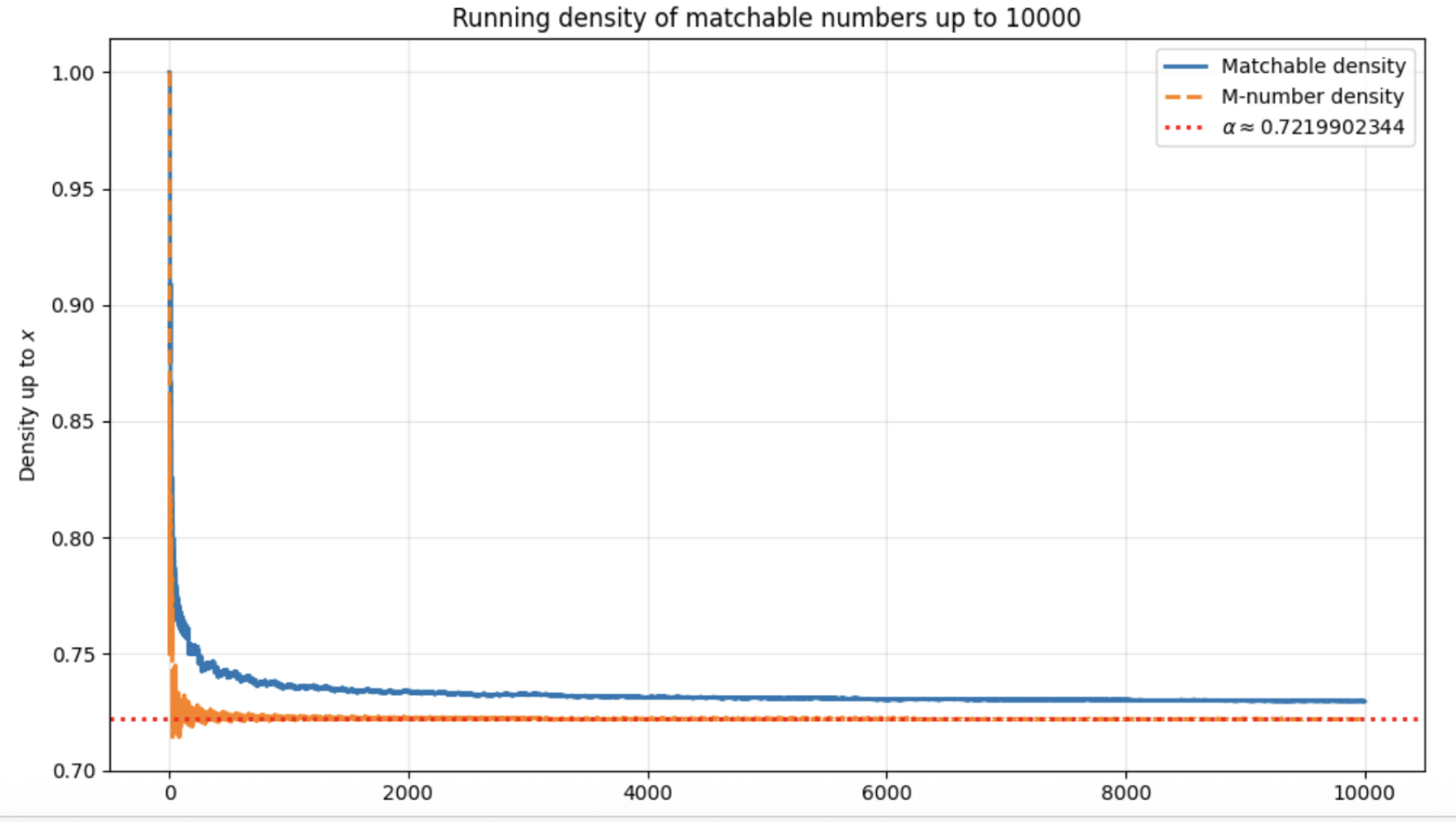
$$\alpha := \prod_p (1-p^{-p}) = 0.72199023441955\ldots.$$

Theorem. (**McNew** and **Pomerance**) The asymptotic density of the set of matchable numbers exists and is α.

On the way to proving this we show that every squarefree number is matchable.

Say an integer n is an **M-number** if it is not divisible by any p^p with p prime. So the asymptotic density of the set of M-numbers is α. We show that but for a possible exceptional set of density 0, every M-number is matchable, and that the set of non-M-numbers that are matchable has asymptotic density 0. We conjecture that the first of these density-0 sets is empty.

Say n is strongly matchable if there is a coprime matching between the $\tau(n)$ divisors of n and every coprime arithmetic progression of length $\tau(n)$. For example, though 4 is matchable, it is not strongly matchable: Try matching $\{1,2,4\}$ with $\{2,3,4\}$. Every strongly matchable number is an M-number, and we conjecture the converse. We are able to prove that a positive proportion of the M-numbers are strongly matchable.



Graph courtesy of Scott Kominers

Stay tuned for further details in McNew's talk on Thursday.

Now for the opposite of the coprime problem . . .

The **divisor graph** on $\mathbb{N}$, where there is an edge from a to b when $a \neq b$ and $a \mid b$ or $b \mid a$, is complementary to the coprime graph, and there are many attractive problems here as well.

For example, how long is the longest chain in the divisor graph restricted to $[n]$? This has been worked on by me, **Pollington**, **Saias**, **Tenenbaum**, **Weingartner**, and **McNew**.

Another example: How many permutations σ of $[n]$ have the property that for each $j \in [n]$, $j \mid \sigma(j)$ or $\sigma(j) \mid j$? See papers of me and **McNew**.

Erdős and **P** (1980): Let $f(n)$ be the least number such that in every interval $[m+1, m+f(n)]$ there are distinct integers $a_1, a_2, \ldots, a_n$ with $i \mid a_i$ for $i = 1, 2, \ldots, n$. We sandwiched $f(n)$ between $n\sqrt{\log n / \log\log n}$ and $n^{3/2}$. **van Doorn** recently improved the lower bound to $n \log n / \log\log n$, and now **Kominers** has removed the $\log\log n$ and has made inroads on improving the old upper bound of $n^{3/2}$.

van Doorn

Photo Credit: Rose Lincoln

Kominers

Thank You!