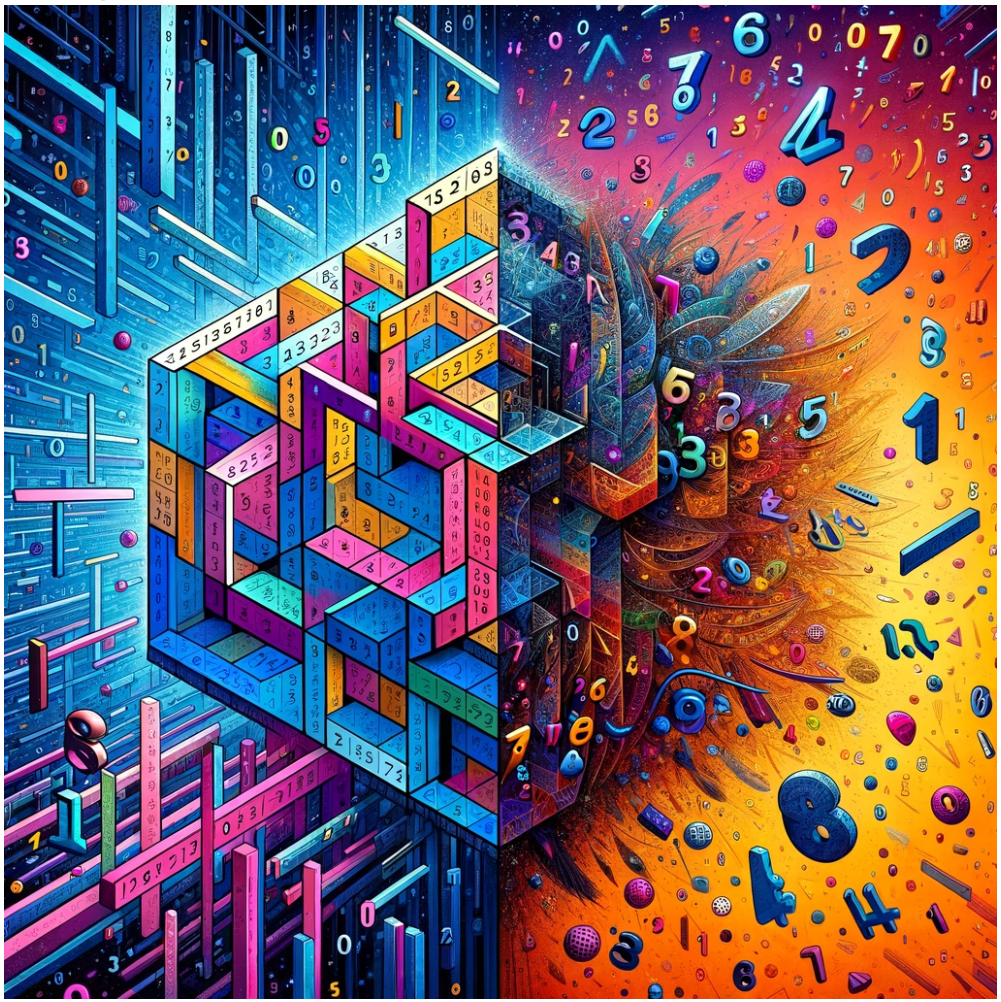
Additive combinatorics and the primes

Terence Tao

University of California, Los Angeles

Analytic number theory is often concerned with the distribution of the primes and related objects. I like to view this subject as one of the battlegrounds between **structure** and **randomness**.



Example: twin prime conjecture

Twin prime conjecture

There are infinitely many pairs of primes $p, p+2$.

- Still open, despite centuries of effort.
- From the work of Zhang (2013), Maynard (2013), and Polymath (2014) we know there are infinitely many pairs of primes p, p' with $2 \leq p' - p \leq 246$.
- There is a more general prime tuples conjecture of Hardy and Littlewood that quantifies the number of prime tuples $p + h_1, \ldots, p + h_k$ one should see in a given range.

- Prime number theorem: For large x, there should be roughly $\int_2^x \frac{dt}{\log t}$ primes up to x.
- **Randomness**: If these primes were distributed randomly, one would expect about $\int_2^x \frac{dt}{\log^2 t}$ twin primes up to x, which would solve the twin prime conjecture. (Cramér random model)
- **Structure**: The primes do not distribute completely randomly: for instance, they almost entirely avoid the even numbers, the multiples of 3, and so forth. This leads to the Cramér–Granville random model that makes an improved prediction

$$\left(2\prod_{p>2}(1-\frac{1}{(p-1)^2})\right)\int_2^x \frac{dt}{\log^2 t} \approx 1.3203\cdots \int_2^x \frac{dt}{\log^2 t}$$

for the number of twin primes up to x.

Numerically, the Cramér–Granville prediction is very accurate!

x	Twin primes up to x	Predicted twin primes up to x
10^4	205	214
10^5	1224	1249
10^6	8169	8248
10^7	58980	58754
10^8	440312	440368
10^9	3424506	3425308
10^{10}	27412679	27411417
10^{11}	224376048	224368865
10^{12}	1870585220	1870559867
10^{13}	15834664872	15834598305
10^{14}	135780321665	135780264894
10^{15}	1177209242304	1177208491861

Unfortunately, we cannot rule out the possibility of *other*, more exotic, structure also being present, which could cause the count of twin primes to deviate from the prediction.

- In many (but definitely not all) cases, we can use additive combinatorics to deal with the unknown amount of randomness in the primes.
- One way to do this is to use additive combinatorics results that apply for *all* sets of a given density, regardless of how random or structured they are.
- Another is to use the inverse theorems of additive combinatorics to identify the scenarios in which the primes are not as random as expected, and use further techniques from analytic number theory (and equidistribution theory) to rule those scenarios out.

A simple (but incomplete) example: we have the following famous additive combinatorics conjecture of Erdős,

Erdos # 3 (1979)

Any set of natural numbers whose sum of reciprocals diverges, contains arbitrarily long arithmetic progressions.

It is a classical result of Euler that the sum of reciprocals of primes diverges, so this conjecture would imply as a corollary that there are arbitrarily long arithmetic progressions of primes, purely from density considerations regarding the primes. However, the conjecture is only known for progressions of length up to three (Bloom–Sisask 2020, Kelley–Meka 2023). Nevertheless the corollary was proven by Green–T. (2008) using a more complicated additive combinatorics strategy (which we will review later).

Another early example is the following result of Schnirelmann. Define *Schnirelmann's constant* to be the least C such that every natural number greater than one is the sum of at most C primes. The even Goldbach conjecture would imply (and is essentially equivalent to) the assertion that $C = 3$.

Schnirelmann, 1930

C is finite.

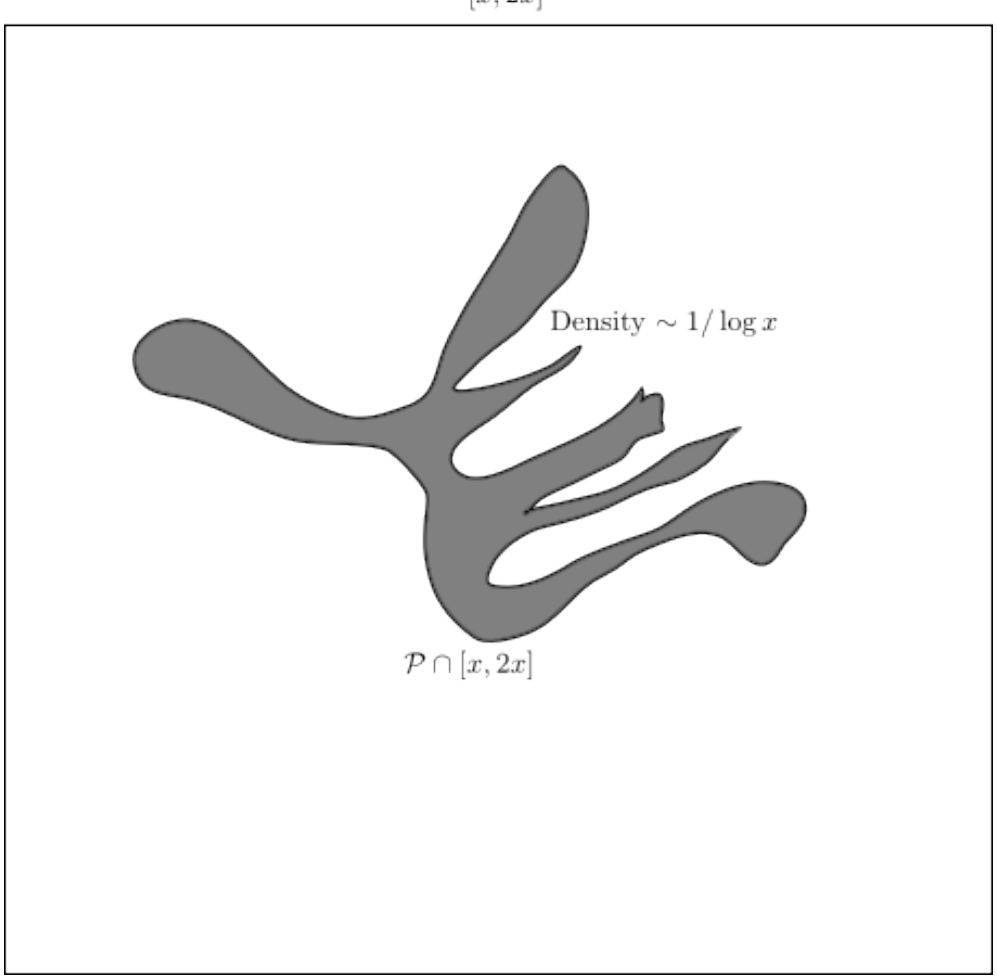
Schnirelmann's original argument using additive combinatorics was $C \leq 8 \times 10^5$. Ramaré (1995) refined the methods to show that $C \leq 7$. Using more classical analytic number theory techniques (circle method), Helfgott (2013) showed $C \leq 4$ (by establishing the odd Goldbach conjecture).

Sketch of Ramaré's argument:

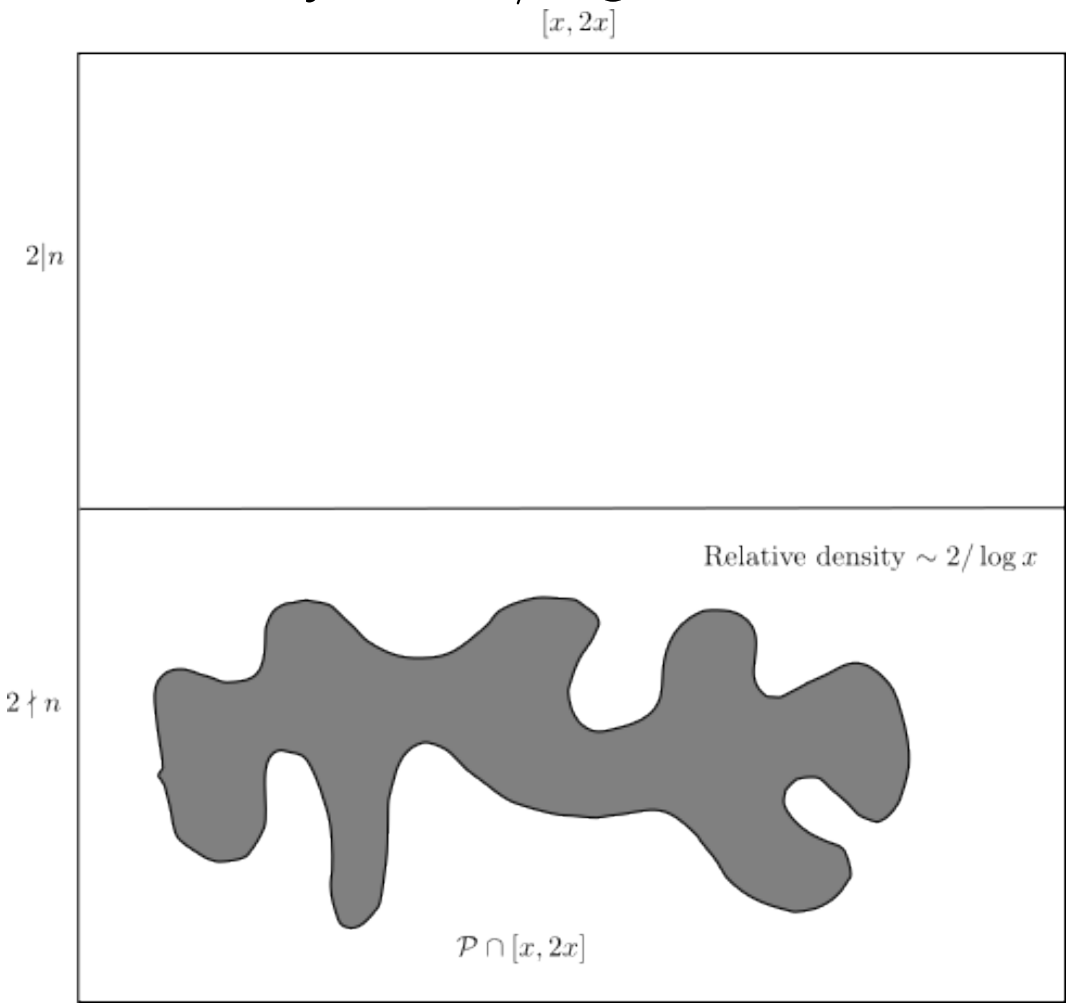
- There are about $x/\log x$ primes up to x, so about $x^2/\log^2 x$ ways to express a number up to $2x$ as the sum of two primes.
- On the other hand, by sieve theory, a typical number of size x has $O(x/\log^2 x)$ ways of being expressible as the sum of two primes.
- Hence, the set of numbers expressible as the sum of two primes has positive density.
- Additive combinatorics inequalities show that (under certain conditions) the sumset $A + B$ has somewhat larger density than A or B separately. Iterating such inequalities carefully, one can eventually show that every number is the sum of at most seven primes.

Describing the primes

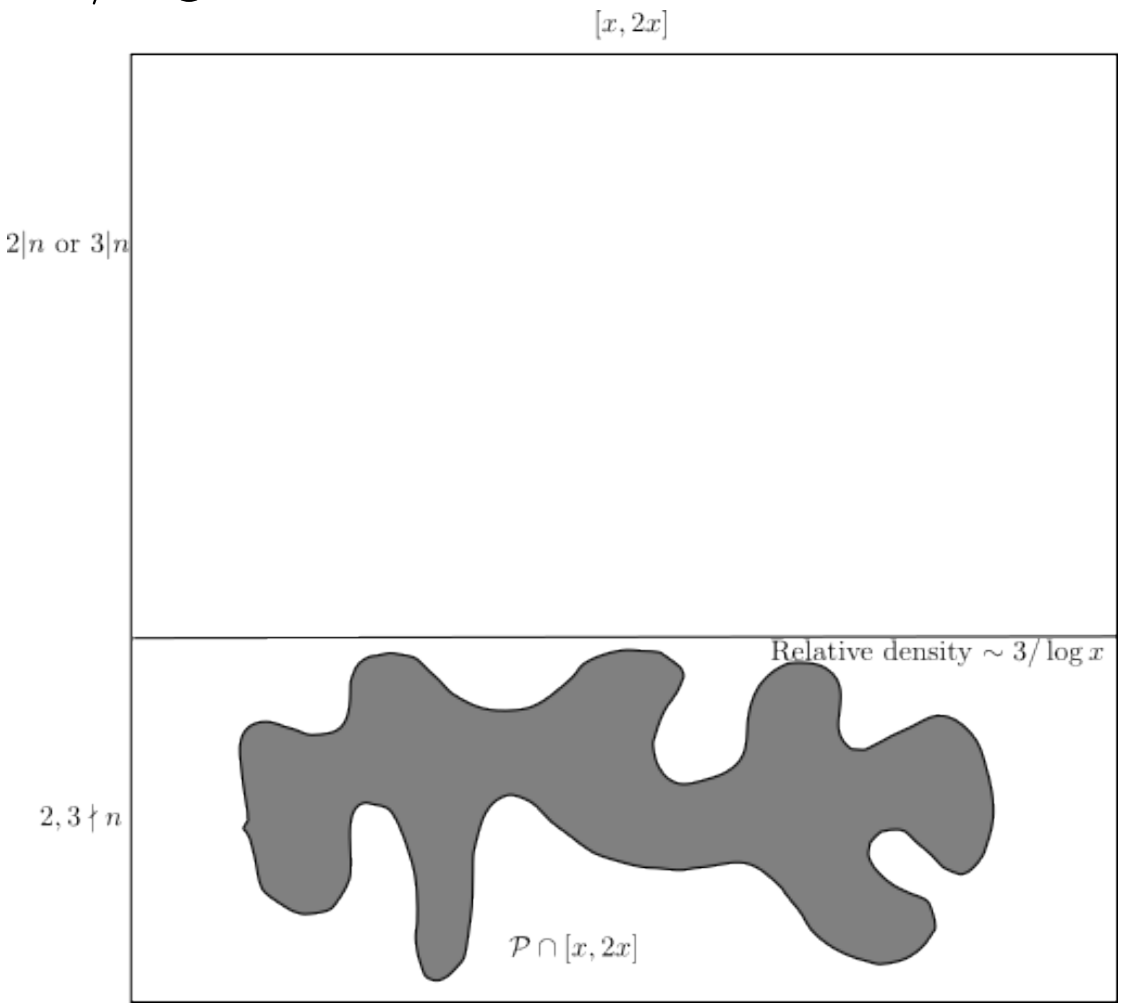
The prime number theorem tells us that the primes in say $[x, 2x]$ for a large x is a sparse subset of $[x, 2x]$ of density $\sim 1/\log x$. But it doesn't tell us much about the structure of this set.



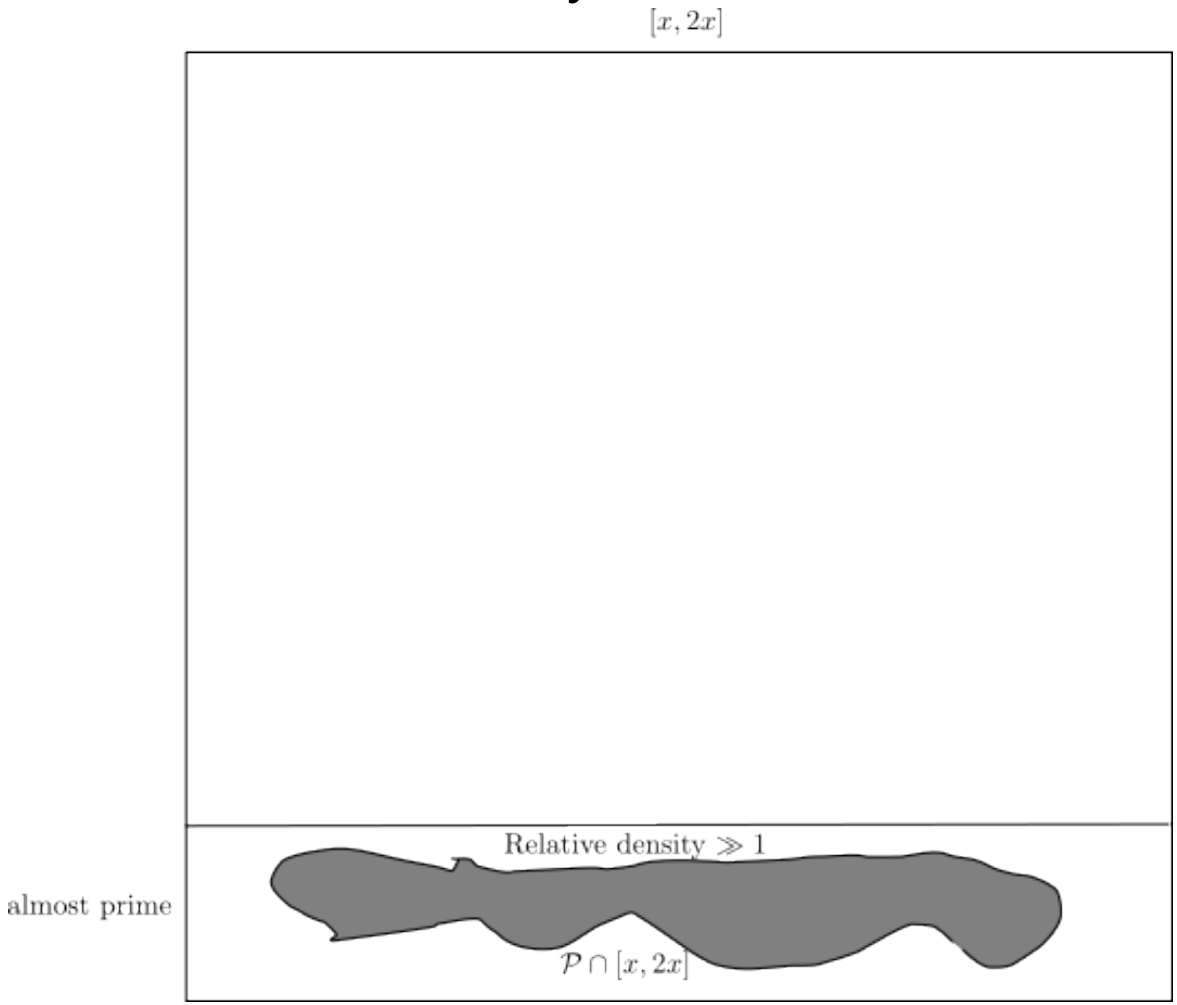
But the primes in $[x, 2x]$ are all odd, so this gives us more information, placing the primes inside the odd numbers with an elevated relative density of $\sim 2/\log x$:



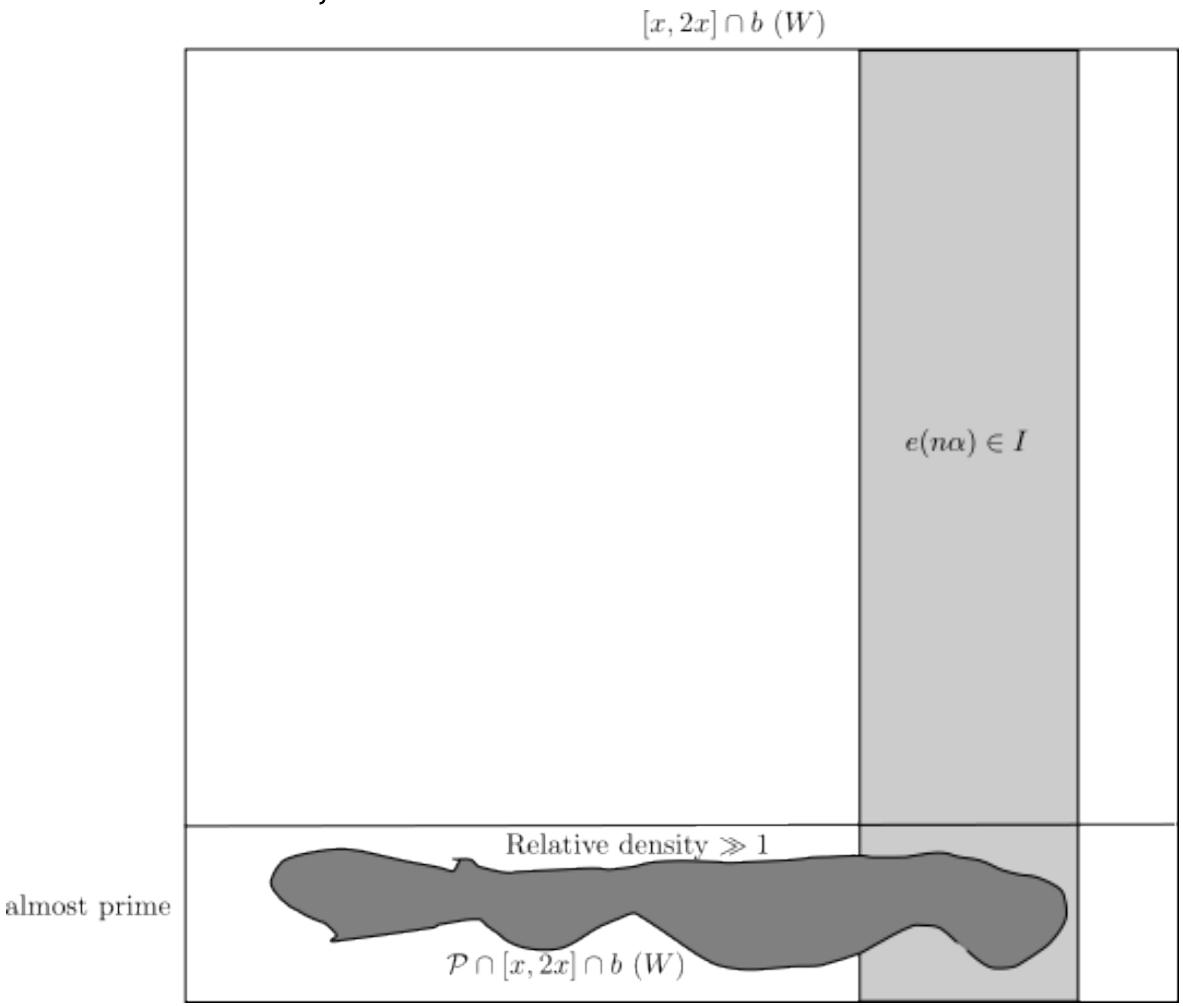
By also sieving out multiples of 3, one can increase the relative density to $\sim 3/\log x$:



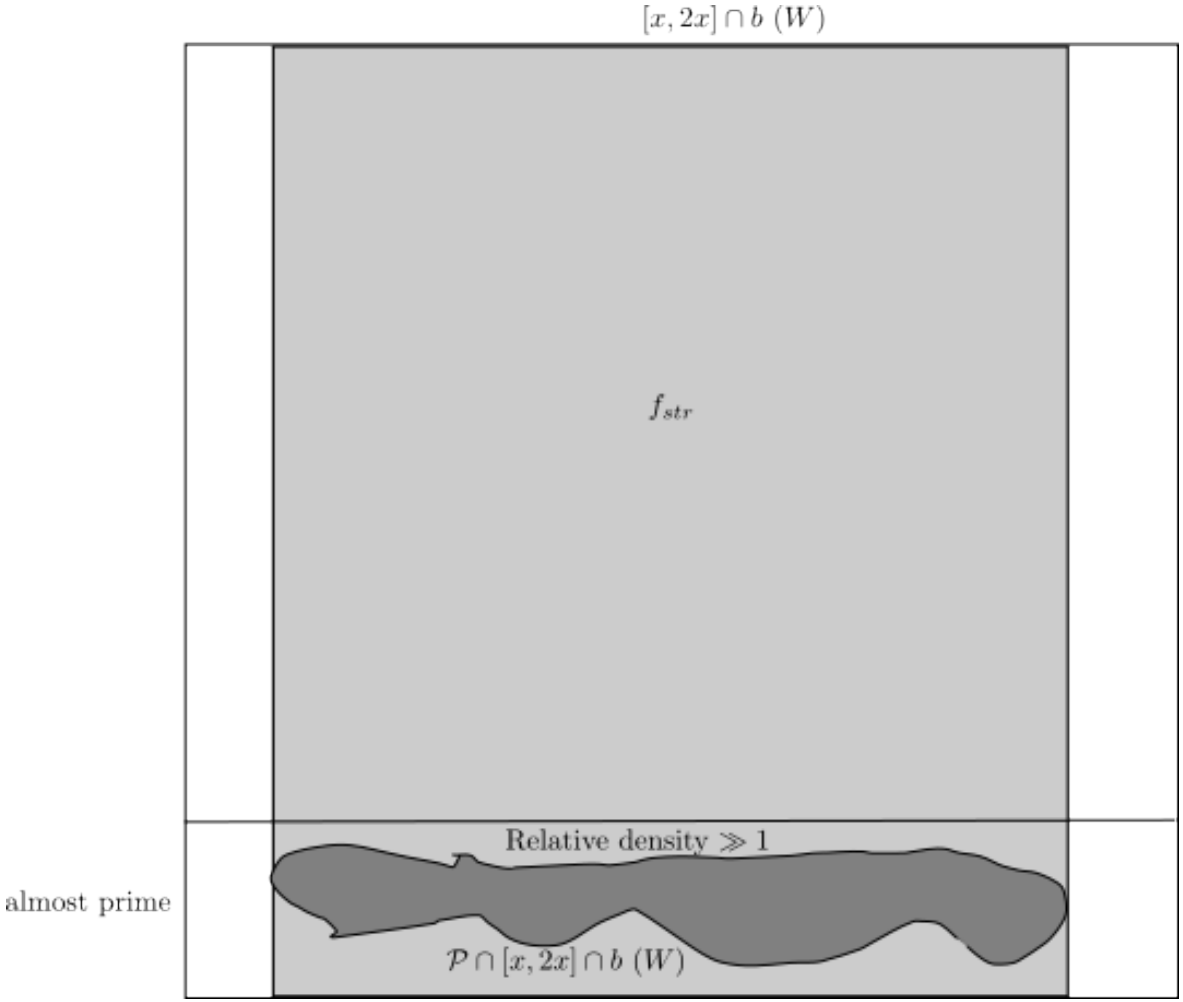
Roughly speaking, sieve theory lets us sieve down to a well-understood set of almost primes (numbers with few prime factors), and the relative density becomes $\gg 1$:



After restricting to a primitive residue class $b\ (W)$ for a medium-sized W (the W-trick), the almost primes become "pseudorandom", and thus uncorrelated with various "structured functions", such as Bohr sets.



There exist transference principles that then permit one to approximate (a normalized version of) the primes by a bounded non-negative "structured function" f_{str} of mean $\gg 1$.



- For instance, if Λ denotes the von Mangoldt function, then on a suitable primitive residue class $b\ (W)$ one can write

$$\frac{\phi(W)}{W}\Lambda(Wn+b) = f_{str}(n) + f_{err}(n)$$

where f_{str} is bounded, nonnegative, and has mean 1, and f_{err} is small in certain Gowers uniformity norms.

- This transference principle originates in (Green, 2005, Green–T., 2008).
- A simplified proof based on the Hahn–Banach theorem appears in (Reingold–Trevisan–Tulsiani–Vadhan 2008, Gowers, 2010).
- It applies for any (suitably normalized) dense subset of a suitably pseudorandom set.
- The "densification" technology from (Conlon–Fox–Zhao 2015) simplifies the proof further, and relaxes the pseudorandomness hypotheses.

As a typical application of the transference principle, Szemerédi's theorem

Szemerédi, 1975

Any set of natural numbers of positive upper density, contains arbitrarily long arithmetic progressions.

implies

Green–T., 2008

The primes contain arbitrarily long arithmetic progressions.

despite the primes themselves being of density zero.

The celebrated result

Zhang, 2014

The primes contain bounded gaps infinitely often.

is morally in the same spirit, being in some sense deduced from

Pigeonhole principle

Any set of positive density contains bounded gaps infinitely often.

although a transference principle is not explicitly used, and the sieve theory required is significantly more delicate.

In a similar spirit, in 2015 Shao established an additive combinatorial result

Shao, 2015

Let $A \subset (\mathbf{Z}/m\mathbf{Z})^\times$ have density greater than $5/8$ for some square-free m. Then $A + A + A = \mathbf{Z}/m\mathbf{Z}$.

and used (a quantitative version of) this result and the transference principle to estabish a Vinogradov type theorem for subsets of the primes:

Shao, 2015

Let A be a set of primes of relative density greater than $5/8$. Then $A + A + A$ contains all sufficiently large odd numbers.

(The threshold $5/8$ is optimal for both results.)

The above transference formalism combines well with inverse theorems from additive combinatorics, which identifies those functions that are unexpectedly non-random in behavior. Example:

$U^2(\mathbf{Z}/N\mathbf{Z})$ inverse theorem

If $f : \mathbf{Z}/N\mathbf{Z} \to \mathbf{C}$ is a bounded function with

$$\|f\|_{U^2(\mathbf{Z}/N\mathbf{Z})}^4 = \mathbf{E}_{x,h,k \in \mathbf{Z}/N\mathbf{Z}} f(x)\bar{f}(x+h)\bar{f}(x+k)f(x+h+k)$$

large, then f has a large correlation with a linear phase $n \mapsto e(\alpha n)$ for some $\alpha \in \frac{1}{N}\mathbf{Z}$.

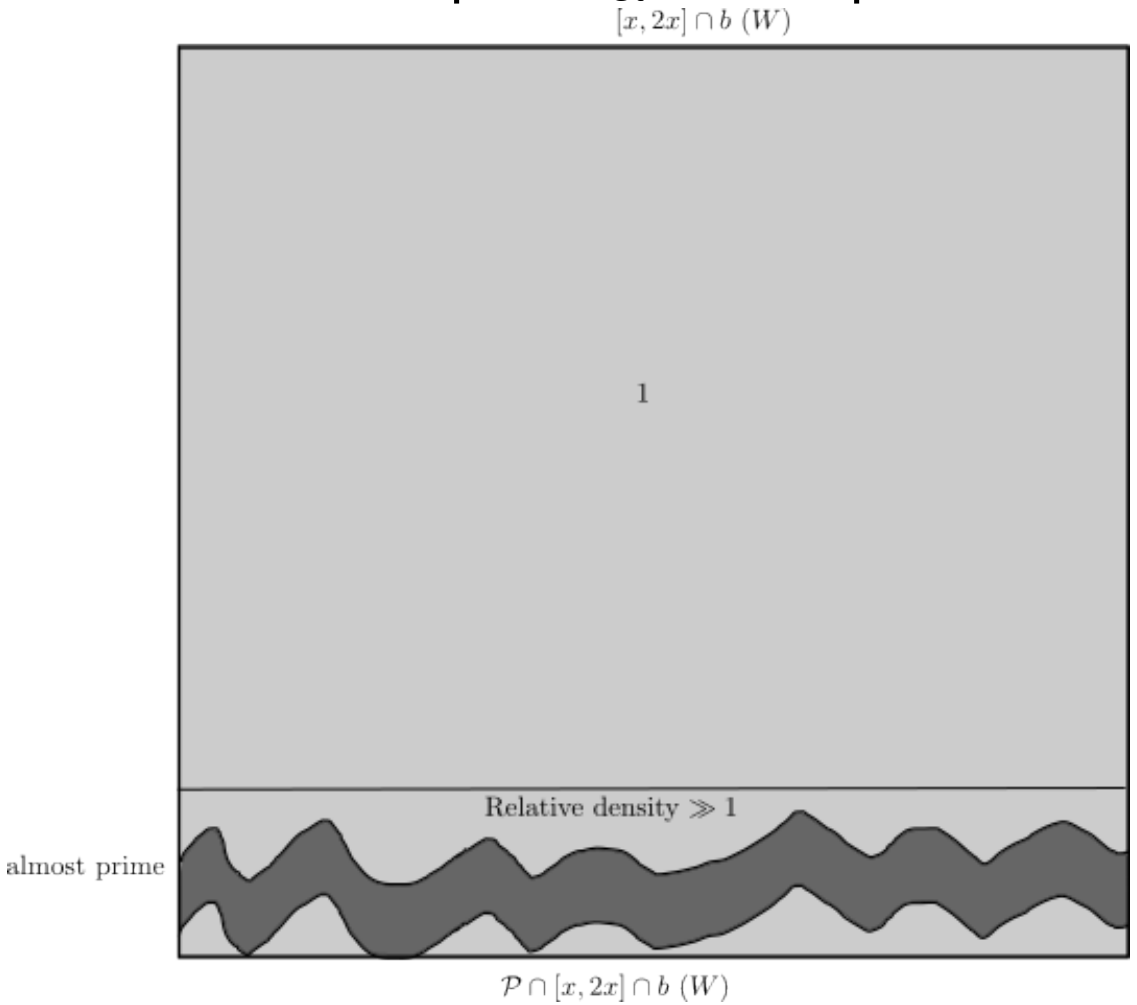
The topic of higher order Fourier analysis revolves around higher order versions of these theorems, and their applications; see (Leng-Sah–Sawhney 2024) for recent advances in this area.

- Existing methods from analytic number theory, such as multiplicative number theory and Vinogradov's method of bilinear sums, can be used to show that the primes, suitably normalized, are uncorrelated with the structured functions arising from inverse theorems.
- For instance, one can show that

$$\mathbf{E}_{n\leq N}(\frac{\phi(W)}{W}\Lambda(Wn+b)-1)e(\alpha n)=o(1)$$

  for suitable choices of parameters.
- Higher order analogues of such statements (involving nilsequences) are also available (Green–T., 2012).

When combined with the transference principle, this basically tells us that the "structured part" f_{str} of the primes is a constant.



This allows for more precise control of various "finite complexity" problems involving the primes. For instance:

Green–T. 2010, Green–T.–Ziegler 2012

The number of arithmetic progressions of length k in the primes up to N is asymptotically

$$\frac{1}{2(k-1)}(\prod_p \beta_p)\frac{N}{\log^k N} + o(\frac{N}{\log^k N})$$

where β_p is equal to $\frac{1}{p}(\frac{p}{p-1})^{k-1}$ if $p \leq k$ and $(1 - \frac{k-1}{p})(\frac{p}{p-1})^{k-1}$ if $p > k$.

As another example, the number-theoretic result

T.–Teräväinen, 2019

For any $a_0, a_1, a_2 \in \mathbf{Z}/3\mathbf{Z}$, the set of n with $\omega(n_i) = a_i$ (3) for $i = 0, 1, 2$ has positive density, where $\omega(n)$ is the number of prime factors of n.

crucially relied upon an ergodic theory variant of the transference principle, together with a "stability" version of the following additive combinatorial inverse theorem:

T., 2018

If A, B are subsets of a compact connected abelian group G with $\mu(A+B) = \mu(A) + \mu(B) < 1$, then up to null sets $A = f^{-1}(I), B = f^{-1}(J)$ for some arcs $I, J \subset \mathbf{R}/\mathbf{Z}$ and some surjective homomorphism $f : G \to \mathbf{R}/\mathbf{Z}$.

Another recent result in this spirit is the reproof by Matomäki–Merikoski–Teräväinen (2024) of the following celebrated theorem of Linnik:

Linnik, 1944

Every primitive arithmetic progression $a\ (q)$ contains a prime number of size $O(q^{O(1)})$.

Previous proofs of Linnik's theorem relied heavily on multiplicative number theory, dividing into cases depending on whether a Siegel zero existed or not. The new proof uses almost no theory about Siegel zeroes, relying instead on additive combinatorics and sieve theory for the most part.

Some very rough sketch of the proof.

- Firstly, through existing sieve theory (the Bombieri sieve), it is (essentially) possible to replace "prime" by "product of three primes".
- Thus, if A denotes the set of residue classes $b\ (q)$ that contain a prime of size $O(q^{O(1)})$, one now wants to show that $A \cdot A \cdot A$ contains a.
- By the Brun–Titchmarsh inequality from sieve theory, one can show that A has density at least $1/2 - o(1)$ in $(\mathbf{Z}/q\mathbf{Z})^\times$.

Now we use the following simple additive combinatorics lemma (provable with a bit of Fourier analysis):

Lemma

Let A be a subset of a finite abelian group $(G, \cdot)$ with $|A| \geq (1/2 - o(1))|G|$, and let $a \in G$. Then either $A \cdot A \cdot A$ contains a, or else A is (mostly) contained in a coset bH of an index two subgroup H of G that avoids a.

This handles all cases except when there is a quadratic Dirichlet character χ of period q such that $\chi(p) \neq \chi(a)$ for almost all primes p of polynomial size in q.
There are then two cases, depending on whether $\chi(a) = +1$ or $\chi(a) = -1$.

- The case when $\chi(a) = -1$ and $\chi(p) = +1$ for most primes p is relatively easy, as every number in a (q) must have at least one prime factor p with $\chi(p) = -1$; as such primes are rare, this leads to an improvement in the usual sieve theory bounds.
- The case when $\chi(a) = +1$ and $\chi(p) = -1$ for most primes p is more delicate. Here one weights the integers by $1 * \chi$ to eliminate most of the primes to again improve the sieve; this requires the elementary lower bound $L(1, \chi) \gg q^{-O(1)}$, but no more advanced theory is required.

- As a miscellaneous application of additive combinatorial methods to analytic number theory, I will mention a result of Matömaki and Shao regarding the sieving problem of counting the number $\Psi(x; \mathcal{P})$ of numbers up to x whose prime factors all lie in some collection $\mathcal{P}$ of primes up to x.
- Probabilistic heuristics suggest that this number should be comparable to $x \prod_{p \in \mathcal{P}} (1 - \frac{1}{p})$ if $\mathcal{P}$ is large enough.

The following result was first conjectured by Granville–Koukoulopoulos–Matomäki (2015):

Matömaki–Shao 2015

If $\sum_{x^{1/v}<p<x^{1/u}:p\in\mathcal{P}} \frac{1}{p} \geq \frac{1+\varepsilon}{u}$ for some $1 < u < v$ and $\varepsilon > 0$, then $\Psi(x;\mathcal{P}) \asymp_{v,\varepsilon} x \prod_{p\in\mathcal{P}}(1-\frac{1}{p})$.

The largeness condition on $\mathcal{P}$ is essentially best possible.

After subdividing the primes into short intervals and taking logarithms, the problem reduces to the following result in additive combinatorics:

Matömaki–Shao 2015

If $A \subset \{1, \dots, N\}$ is such that $\sum_{N/v<a<N/u} \frac{1}{a} \geq \frac{1+\varepsilon}{u}$ for some $1 < u < v$ and $\varepsilon > 0$, then there are many sums of elements of A of size $N - O(1)$.

Matömaki and Shao reduce this discrete problem to a continuous analogue, already proven by Bleichenbacher:

Bleichenbacher 2003

If $T \subset (0, 1/u)$ is open and $\int_T \frac{dt}{t} > \frac{1}{u}$, then some finite sum of T contains 1.

Thanks for listening!