Recent progress in additive prime number theory

Terence Tao

University of California, Los Angeles

Mahler Lecture Series

Additive prime number theory

- Additive prime number theory is the study of additive patterns in the prime numbers $2, 3, 5, 7, \ldots$.
- Examples of additive patterns include twins $p, p+2$, arithmetic progressions $a, a+r, \ldots, a+(k-1)r$, and prime gaps $p_{n+1} - p_n$.
- Many open problems regarding these patterns still remain, but there has been some recent progress in some directions.

Long arithmetic progressions in the primes

- I'll first discuss a theorem of Ben Green and myself from 2004:
- **Theorem:** The primes contain arbitrarily long arithmetic progressions.

- It was previously established by van der Corput (1929) that the primes contained infinitely many progressions of length three. In 1981, Heath-Brown showed that there are infinitely many progressions of length four, in which three elements are prime and the fourth is an almost prime (the product of at most two primes).
- The proof of the full theorem combines three separate ingredients: random models for the primes, sieve theory, and Szemerédi's theorem.

Prime counting heuristics

- While we are not able to prove everything we would like to in this subject, we do have a rather convincing set of heuristics with which to predict how to count various patterns in the primes.
- The starting point is the prime number theorem, which asserts that the number of primes less than a large number N is roughly $N/\log N$.
- One can interpret this fact probabilistically: if one picks an integer at random between 1 and N, then it has a probability of about $1/\log N$ of being prime.

Cramér's random model

- Cramér's random model for the primes asserts that the primes behave "as if" each integer n had an independent probability of $1/\log n$ of being prime, in the sense that statistics for the primes asymptotically match statistics for this random model.
- This model turns out to not be totally accurate, but there are some refinements to this model which give quite convincing predictions.
- We'll illustrate this with a study of the twin prime conjecture: there are infinitely many pairs $p, p+2$ of primes that are a distance 2 apart. This ancient conjecture remains open, despite many partial results.

A "proof" of the twin prime conjecture

- Let N be a large number, and let n be an integer chosen randomly between 1 and N.
- From the prime number theorem, n and $n+2$ each have a probability about $1/\log N$ of being prime.
- Assuming that the events "n is prime" and "$n+2$ is prime" are independent, we conclude that $n, n+2$ are simultaneously prime with probability about $1/\log^2 N$.
- In other words, there are about $N/\log^2 N$ twin primes less than N. Letting $N \to \infty$ we obtain the twin prime conjecture.

Correcting the model

- This argument is incorrect. One reason to see this is that it would also predict an infinite number of consecutive primes $n, n+1$, which is false, as all but one of the primes are odd.
- However, one can correct for this by refining the model. Right now, we are giving each integer $n \in \{1, \ldots, N\}$ an equal chance of $1/\log N$ of being prime. A smarter model would be to give the odd integers a $2/\log N$ chance of being prime and the even integers a 0 chance of being prime. (This omits the prime 2, but this is negligible in the grand scheme of things.)
- With this refined model, consecutive primes are ruled out (as they should), and the expected number of twin primes increases from $N/\log^2 N$ to $2N/\log^2 N$.

The prime tuples conjecture

- One can refine the model further, by excluding the multiples of 3 from being prime (and increasing the probability of the remaining numbers of being prime from $2/\log N$ to $3/\log N$). This turns out to adjust the expected number of twin primes downward, to $1.5\frac{N}{\log^2 N}$.
- Continuing to add information about small moduli, the expected count given by these models continues to change, but can be easily computed to converge to an asymptotic prediction, which in the case of twin primes turns out to be $\Pi_2 \frac{N}{\log^2 N}$, where Π_2 is the twin prime constant

$$\Pi_2 = 2 \prod_{p \text{ odd prime}} (1 - \frac{1}{(p-1)^2}) \approx 1.320\ldots.$$

- This is believed to be the correct asymptotic.
- More generally, there is a similar asymptotic conjectured for other patterns in the primes; this is basically the Hardy-Littlewood prime tuples conjecture. Roughly speaking, it is asserting that the sequence of adjusted Crámer models discussed earlier is asymptotically accurate for describing the primes.

- One can think of each of these models as identifying a certain amount of "structure" in the primes, and then saying that all other aspects of the primes are "random". For instance, one could observe the structure that the primes have density about $2/\log N$ in the odd numbers and $1/\log N$ in the even numbers, but assert that there is no discernible additional structure on top of this.

- Viewed in this light, the prime tuples conjecture is asserting that apart from the "obvious" structure that the primes obey (they are almost all coprime to 2, coprime to 3, etc.), there is no additional pattern or structure to this sequence of integers, and they behave as if they were random relative to the structure already identified.
- However, we are unable at this time to rigorously rule out a bizarre "conspiracy" among primes to exhibit an additional layer of structure (e.g. to avoid congregating as twins $n, n+2$ after a certain point). How does one disprove a conspiracy?

Sieve theory

- Now we turn from random models to another aspect of prime number theory, namely sieve theory.
- One way to approach the primes is to start with all the integers in a given range (e.g. from $N/2$ to N) and then sift out all the non-primes, for instance by removing the multiples of 2, then the multiples of 3, and so forth up to the multiples of $\sqrt{N}$ (the sieve of Eratosthenes).
- One can hope to count, say, twin primes, by keeping track of the number of twins at each stage of the sifting process.

- For instance, the number of twins $n, n+2$ in the entire range $[N/2, N]$ is $N/2 + O(1)$. After removing the multiples of two, the count drops to $N/4 + O(1)$; after removing the multiples of three, it drops further to $N/12 + O(1)$, and so forth.
- Unfortunately, the "$O(1)$" errors multiple rapidly, and overwhelm the main term long before one reaches the level of multiples of $\sqrt{N}$.
- One can partially address this problem by "smoothing" the sieve (rather than eliminating numbers outright, adjust their "score" upward or downward whenever they are divisible or not divisible by certain numbers), but one still cannot get to $\sqrt{N}$ by these techniques alone (there is a specific obstruction to this, known as the parity problem).

Almost primes

- Nevertheless, it is possible to use sieve theory to control things up to some partial height, e.g. up to multiples of $N^{1/10}$. The resulting sifted set consists not only of primes, but also contains almost primes - products of a bounded number (e.g. at most ten) of (large) primes.
- To summarise several decades of work in sieve theory into a single sentence, these methods can establish analogues of conjectures such as the prime tuples conjecture, but with primes replaced by almost primes. For instance, one can find infinitely many twins of almost primes. [I'm glossing over the technical issue here of exactly how to define "almost prime".]

- To put it another way, the almost primes do indeed behave like we expect the primes to, namely that they have no structure beyond the obvious ones (like the primes, the almost primes tend to be coprime to 2, coprime to 3, etc.)
- On the other hand, there are more almost primes than primes; there are about $N/\log N$ primes less than N, but there are about $CN/\log N$ almost primes less than N (where C is a constant that depends on how exactly one defines "almost prime").

Szemerédi's theorem

- To summarise so far: we have conjectures about patterns in the primes, but cannot prove them in general.
- But if we replace primes with the larger set of almost primes, we can then verify the analogous conjectures for almost primes using sieve theory.
- For a special type of pattern, namely arithmetic progressions, there is an additional powerful tool available, namely Szemerédi's theorem.

- **Szemerédi's theorem:** Any subset of the A integers of positive upper density (which means that $\limsup_{N\to\infty} \frac{\#(A\cap[-N,N])}{2N+1} > 0$) contains arbitrarily long arithmetic progressions.
- First proven by Szemerédi in 1975. Note that this type of result is false for other patterns, such as twins $n, n+2$ (e.g. the multiples of 3 have positive density, but no twins). Arithmetic progressions are more "indestructible" than other patterns.

Szemerédi's theorem is difficult to prove. There have been many different proofs, each of which has been very significant in stimulating further research, including:

- Szemerédi's original combinatorial proof using graph theory (1975);
- Furstenberg's ergodic theory proof (1977);
- Gowers' proof using "generalised Fourier analysis" and additive combinatorics (2001);
- The proofs of Gowers, Nagle-Rödl-Schacht-Skokan, and later authors using graph and hypergraph theory (2004-2006);
- The combinatorial proof of the Polymath1 collaborative project (2009).

- The proofs are too technical to describe here, but they all share some features in common.
- Namely, they all have to address the fact that the dense set A of integers could be very structured (e.g. the multiples of four), very random (e.g. a random subset of integers of density $1/4$), or a combination of both (e.g. a random subset of the even integers of density $1/2$).
- In each of these cases, arithmetic progressions can be found, but the reason for the progressions is different in different cases.
- Accordingly, all of the proofs must at some point split A up into "structured" and "random" components.

Putting it all together

- Szemerédi's theorem shows that sets of positive density have arbitrarily long progressions.
- It does not directly apply to the primes, because the primes have zero density.
- However, the primes have positive relative density with respect to the almost primes.
- And the almost primes behave quite randomly (in particular, they have plenty of progressions).
- It is possible to combine these facts to show that the primes have arbitrarily long progressions.

Very informal sketch of proof

- If the primes obeyed the (modified) Cramér random model, we would be done. But they could obey some exotic structure not predicted by this model, e.g. they could be unexpectedly dense on some structured set.
- If this occurs, we adjust the random model to take this additional structure into account. We repeat this process until no significant additional structure is found.
- We end up with some "exotic" random model that models the primes. (Showing the process terminates is non-trivial.)

- On the other hand, the primes are a dense subset of the almost primes, which behave like a random subset of the entire integers. (Here we use a particular notion of the almost primes, studied by Goldston and Yıldırım in their work on prime gaps.
- Because of this, one can show that the random model for the primes contain a random subset of a dense subset of integers.
- Dense subsets of the integers contain lots of arithmetic progressions. Many of them will survive the passage to a random subset.
- Since the model for the primes is accurate, the primes themselves contain lots of arithmetic progressions.

Other linear patterns

- An arithmetic progression of a fixed length k is a sequence of numbers $n_1, n_1 + n_2, n_1 + 2n_2, \ldots, n_1 + (k-1)n_2$ parameterised in a linear fashion by two integer parameters a, r.
- One can consider more general linear (or affine) patterns $c_{11}n_1 + \ldots + c_{1d}n_d + c_1, \ldots, c_{k1}n_1 + \ldots + c_{kd}n_d + c_k$ generated by some integer parameters $n_1, \ldots, n_d$, where the c_{ij} and c_i are fixed coefficients.
- One can then ask whether one can find choices of the parameters in which all of the elements in this pattern are prime; one can also ask the more refined question of how *many* such choices there are in a given range (e.g. with all $n_1, \ldots, n_d$ less than a threshold N).

Many classical problems in prime number theory can be viewed as special cases of this problem. For instance:

- The twin prime conjecture corresponds to the pattern $n_1, n_1 + 2$.
- The even Goldbach conjecture corresponds to the pattern $n_1, N - n_1$, where N is a fixed even number larger than 2.
- The odd Goldbach conjecture corresponds to the pattern $n_1, n_2, N - n_1 - n_2$, where N is a fixed odd number larger than 5.

There are some obvious obstructions to solvability of this problem.

- Obstructions mod p If it is not possible for all of the linear forms to be simultaneously coprime to a given modulus p, then this presents an obvious obstruction to solvability. For instance, at least one of $n, n+1$ has to be even, which makes it hard for both to be prime; similarly, at least one of $n, n+2, n+4$ has to be divisible by 3.
- Obstructions at infinity If the linear forms can be positive only finitely often, then this of course prevents having more than a finite number of solutions.

- In a series of papers, Ben Green, Tamar Ziegler and I (2006-2009) established the following result:
- **Theorem.** If a family of affine-linear forms has no obstructions mod p and at infinity, and any two forms are affinely independent, then the forms can be simultaneously prime infinitely often. Furthermore, the number of solutions obeys the asymptotic predicted by the Hardy-Littlewood prime tuples conjecture.
- Thus, for instance, there are infinitely many n_1, n_2 such that $n_1, n_2, n_1 + n_2 + 1, n_1 + 2n_2 + 2$ are all prime (i.e. there are infinitely many progressions of length three whose difference is one less than a prime). The theorem also implies our previous result that the primes contained arbitrarily long arithmetic progressions.

- Unfortunately, the requirement that no two forms are affinely dependent means that the theorem does not apply to classical problems such as the twin prime problem. (A variant of the result can however be used to recover the famous theorem of Vinogradov that the odd Goldbach conjecture is true for sufficiently large odd numbers.)
- Indeed, our methods fundamentally rely on having at least *two* free parameters n_1, n_2 to work with; one-parameter problems such as the twin prime or even Goldbach conjecture remain out of reach.

- The starting point for the arguments is similar to that used to establish long progressions in primes, namely to locate an accurate dense model for the primes.
- Previously, one used Szemerédi's theorem to generate progressions regardless of whether the primes obeyed the Crámer model or some more exotic model. Here, Szemerédi's theorem is not available. Instead, we work to eliminate the possibility of an exotic model, leaving only the Crámer model.

Dichotomy between structure and randomness

- The two key steps in the argument (in addition to the fact that the primes have a dense model) are, roughly speaking, as follows:
- **Proposition 1.** If a dense set does not have the "expected" number of patterns of a certain form, then it must be irregularly distributed with respect to some structured set.
- **Proposition 2.** The primes (or more precisely, a proxy for the primes known as the Möbius function) is uniformly distributed with respect to every structured set.
- Combining these facts with some additional arguments, one obtains the theorem.

What is structure?

- To formalise this approach, one has to define precisely the type of "structured sets" that block a set from having the expected number of patterns.
- To given an example, suppose that a set of integers A had an unusual propensity to congregate in the set P of integers with a last digit of 7. Then one would expect A to have an unusually large number of (say) arithmetic progressions $n, n+r, n+2r$ of length three, since whenever the first two elements of a progression lie in P, the third element does also.

- More generally, any infinite arithmetic progression $P = \{n : n = a \bmod q\}$ can distort the number of progressions of length three in this manner.
- A little less obviously, a *Bohr set* such as $P = \{n : \{\sqrt{2}n\} \leq 0.1\}$, where $\{x\}$ is the fractional part of n, also distorts progressions of length three. This can be explained using the identity

$$\sqrt{2}n - 2\sqrt{2}(n+r) + \sqrt{2}(n+2r) = 0.$$

- Even less obviously, for more complicated patterns such as progressions $n, n+r, n+2r, n+3r$ of length four, quadratic Bohr sets such as $P = \{n : \{\sqrt{2}n^2\} \leq 0.1\}$ can distort the number of patterns, ultimately because of identities such as

$$\sqrt{2}n^2 - 3\sqrt{2}(n+r)^2 + 3\sqrt{2}(n+2r)^2 - \sqrt{2}(n+3r)^2 = 0.$$

- It turns out (with a lot of effort, using some technology of Gowers, of Ratner, and of Leibman) that one can completely classify the types of sets that can distort these sots of patterns, in terms of the dynamics of nilmanifolds G/Γ.
- One can also show (using some powerful technology of Ratner and of Vinogradov) that the primes behave uniformly with respect to these dynamical systems.
- These are the two major ingredients used to establish the main theorem.