Linear equations in the primes: past, present and future

Goldbach (1750): Is every even integer the sum of two primes? e.g. $5+7=12$, $17+19=36$.

Vinogradov (1937, building on work of Hardy and Littlewood): Every sufficiently large odd number is the sum of three primes.

Van der Corput (1939): There are infinitely many triples of primes in arithmetic progression. E.g. $(5,11,17)$, $(19,31,43)$.

Heath-Brown (1981): There are infinitely many 4-term progressions $q_1 < q_2 < q_3 < q_4$ such that three of the q_i are prime and the other is either prime or a product of two primes.

G.– Tao (2004): There are arbitrarily long arithmetic progressions of primes.

Erdős-Turán (1936): Do the primes contain arithmetic progressions of length k on density grounds alone?

Define $r_k(N)$ to be the size of the largest $A \subseteq \{1, \ldots, N\}$ containing no k elements in arithmetic progression. Is $r_k(N) < N/\log N$?

Less optimistically, is $r_k(N) = o(N)$?

Roth (1953): Yes when $k = 3$.
In fact $r_3(N) = O(N/\log\log N)$.

Szemerédi (1969): Yes when $k = 4$.

Szemerédi's Theorem (1975): Yes for all k.

Furstenberg (1977): Yes for all k, using ergodic theory.

Gowers (1998): Yes for all k, using harmonic analysis. The first "sensible bound"
$r_k(N) = O(N/(\log\log N)^{c(k)})$.

A relative Szemerédi Theorem?

?	$\{1,\ldots,N\}$
Primes	$A \subseteq \{1,\ldots,N\}$ has density $\alpha > 0$.
G.–Tao 2004	Szemerédi

The mystery object is a function

$$\nu : \{1,\ldots,N\} \to [0,\infty).$$

The function ν. Fix $k = 4$. We need:

1. ν dominates the primes. If $p \leqslant N$ is prime then $\nu(n) \geqslant 1$. For all $n \leqslant N$, $\nu(n) \geqslant 0$.

2. The primes have positive density in ν:

$$\sum_{n \leqslant N} \nu(n) \leqslant \frac{100N}{\log N}.$$

3. ν satisfies the correlation and linear forms conditions. For example if $h_1, \ldots, h_{32} \leqslant N$ then we can find a nice asymptotic for

$$\sum_{n \leqslant N} \nu(n + h_1) \ldots \nu(n + h_{32}).$$

The appropriate definition of ν, and the verification of properties 1, 2 and 3 comes to us from work of Goldston and Yıldırım.

Set $R := N^{1/20}$ and define

$$\nu(n) := \frac{1}{(\log R)^2} \Bigg(\sum_{\substack{d|n \\ d \leqslant R}} \mu(d) \log(R/d) \Bigg)^2$$

if $R < n \leqslant N$, and $\nu(n) = 1$ otherwise.

Back to arithmetic progressions

Let $A \subseteq \{1, \ldots, N\}$ have size αN. How many 3-term APs does A contain?

In the "random" case, about $\frac{1}{4}\alpha^3 N^2$. Call this the "expected number" of 3-term APs.

The only way that A can have significantly more/less than the expected number of APs is if $A - \alpha$ has *linear bias*. That means that

$$\sup_\theta \left| \sum_{n \leqslant N} (A(n) - \alpha) e^{2\pi i n \theta} \right| \geqslant f(\alpha) N.$$

What about the primes? Convenient to weight the primes. The von Mangoldt function is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \\ 0 & \text{else.} \end{cases}$$

Λ has average value 1.

Either

$$\sum_{x,d \leqslant N} \Lambda(x)\Lambda(x+d)\Lambda(x+2d) \approx N^2,$$

in which case we are happy, or $\Lambda - 1$ has linear bias, that is

$$\sup_{\theta} \left| \sum_{n \leqslant N} (\Lambda(n) - 1) e^{2\pi i n \theta} \right| \geqslant cN.$$

To prove this we already need properties of ν.

Do the primes have linear bias? Unfortunately, they do.

Most primes are even, so

$$\left|\sum_{n\leqslant N}(\Lambda(n)-1)e^{\pi i n}\right|$$

is very large.

We can remove this "arithmetic" obstruction by quotienting out the small primes. We call this the W-trick. Set $W = 2 \times 3 \times \cdots \times w$, where $w = w(N) \to \infty$ as $N \to \infty$. Define

$$\widetilde{\Lambda}(n) = \frac{\phi(W)}{W}\Lambda(Wn+1).$$

This new function $\widetilde{\Lambda} - 1$ has no linear bias (Hardy-Littlewood method) and so

$$\sum_{x,d\leqslant N} \widetilde{\Lambda}(x)\widetilde{\Lambda}(x+d)\widetilde{\Lambda}(x+2d) \approx N^2.$$

Hence lots of 3-term APs of primes.

Remember that $\widetilde{\Lambda}$ is basically a weighted version of the primes, with arithmetic irregularities quotiented out.

If $A \subseteq \{1, \ldots, N\}$ has size αN then the "expected" number of 4-term APs is about $\frac{1}{6}\alpha^4 N^2$.

If A has significantly more/less than the expected number of 4-term APs, does $A - \alpha$ have linear bias?

Consider

$$A := \{n \leqslant N : -\alpha/2 \leqslant \{n^2\sqrt{2}\} \leqslant \alpha/2\}.$$

This set has size about αN, $A - \alpha$ does not have linear bias, yet A has about $C\alpha^3 N^2$ four-term arithmetic progressions, which is many more than the expected number.

Somewhat remarkably, such quadratic examples are essentially the only ones.

Theorem (Gowers, Host-Kra, G. – Tao). Suppose that $A \subseteq \{1, \dots, N\}$ has size αN, but that the number of 4-term arithmetic progressions in A differs from $\frac{1}{6}\alpha^4 N^2$ by at least ηN^2. Then $A - \alpha$ has quadratic bias, which means that

$$\sup_{q \in \mathcal{Q}} \left| \sum_{n \leqslant N} (A(n) - \alpha) e^{2\pi i q(n)} \right| \geqslant f(\alpha, \eta) N,$$

where $\mathcal{Q}$ is the collection of *generalised quadratics*.

What is a generalised quadratic? We won't give the precise definition, but they are not just quadratic polynomials. There are also objects like $q(n) = n\sqrt{2}[n\sqrt{3}]$, where square brackets denote the nearest integer.

Can we show that $\widetilde{\Lambda}-1$ does not have quadratic bias, where $\widetilde{\Lambda}$ is the modified von Mangoldt function?

Seemingly yes (G. - Tao, work in progress). This would give an asymptotic for the number of 4-term progressions $p_1 < p_2 < p_3 < p_4 \leqslant N$. However this is difficult and generalising to cubic bias, and so on, will be even harder.

There is a way around this, which we can phrase in the form of an algorithm.

Set $F_0 := 1$ and $f_0 := \widetilde{\Lambda} - F_0$.

If f_0 has no quadratic bias then STOP. Otherwise, we have $\langle f, e^{2\pi i q_0}\rangle \geqslant c(\alpha)N$ for some generalised quadratic q_0. Use q_0 to define a new function F_1. Set $f_1 := \widetilde{\Lambda} - F_1$.

Repeat, getting functions $F_2, \ldots, F_k$ and $f_i = \widetilde{\Lambda} - F_i$. For all i, $0 \leqslant F_i(n) \leqslant 100$ for almost all n, because of the dominating effect of ν. The functions f_i have average value 0.

Key fact: The algorithm STOPS. This is because $\|F_i\|_2$ increases by a fixed amount at each stage, yet $0 \leqslant F_i(n) \leqslant 100$ for all almost all n.

When the algorithm STOPS, we have

$$\widetilde{\Lambda} = F_k + f_k,$$

where $0 \leqslant F_k(n) \leqslant 100$, $\sum_{n \leqslant N} F_k(n) \approx N$, and f_k has no quadratic bias.

Setting $\widetilde{\Lambda} = F_k + f_k$, we can write

$$\sum_{x,d} \widetilde{\Lambda}(x)\widetilde{\Lambda}(x+d)\widetilde{\Lambda}(x+2d)\widetilde{\Lambda}(x+3d)$$

as a sum of sixteen terms.

Fifteen of these involve f_k, and so are tiny because f_k has no quadratic bias.

The other term is

$$\sum_{x,d} F_k(x)F_k(x+d)F_k(x+2d)F_k(x+3d). \quad (1)$$

Think of F_k as being a bit like a subset of $\{1,\ldots,N\}$ with density at least $1/100$. Then Szemerédi's theorem tells us that (1) is not zero (and in fact, after some combinatorial trickery, quite large).

So we used Szemerédi's theorem as a "black box".

Any subset consisting of a positive proportion of the primes contains a 4-term AP.

Generalising to longer progressions: for 5-term progressions we need cubic bias, involving objects like

$$c(n) = n\sqrt{5}[n\sqrt{3}[n\sqrt{2}]] + n\sqrt{7}[n^2\sqrt{11}].$$

Things become *much* easier if we use what I call *surrogate* linear, quadratic, cubic, ... functions.

A surrogate linear function is

$$\sum_{a,b} f(x+a)f(x+b)f(x+a+b).$$

A surrogate quadratic function is

$$\sum_{a,b,c} f(x+a)f(x+b)f(x+c)\times$$

$$\times f(x+a+b)f(x+a+c)f(x+b+c)f(x+a+b$$

Think of as generalisations of $e^{2\pi i\theta n}$ and $e^{2\pi i q(n)}$ respectively.

Future directions:

- We seem to have shown that $\widetilde{\Lambda}$ has no quadratic bias. This gives an asymptotic for the number of solutions of two linear equations in four prime unknowns, all of which are at most N.

- Can we understand this properly, then generalise this to cubic, quartic, and higher biases? This would be a kind of higher-dimensional Hardy-Littlewood method.

- Arithmetic progressions in the set of sums-of-two-squares correspond to points on a variety which as an intersection of two quadratic forms in 8 variables $x_1, \ldots, x_8$. Can we count points on more general varieties of this type?