# A Brief Introduction to Efficient Congruencing

Samantha Homfray

November 2025

## Introduction

The object we want to study is the number $J_{s,k}(X)$ of solutions to the Vinogradov system of diophantine equations

$$x_1^j + \ldots + x_s^j = x_{s+1}^j + \ldots + x_{2s}^j$$

where $1 \leq x_i \leq X$ are integers and $1 \leq j \leq k$. The result we are interested in is the

**Conjecture (Vinogradov Mean Value Theorem):** For every $s, k \geq 1$, we have the bound

$$J_{s,k}(X) \lesssim_{s,k,\epsilon} X^{\epsilon}(X^s + X^{2s-k(k+1)/2})$$

In particular, we are most interested in the "critical index" $s = k(k+1)/2$, as this case implies the full conjecture fairly easily. This conjecture has several important consequences, including the best known description of the zero-free region of the Riemann zeta function. In 2014, Wooley proved the conjecture for $k = 3$ (and later extended it to $k \geq 4$ as in [Woo19]) using his "efficient congruencing" technique, which we will discuss here.

## Motivation for the Bound

If we denote

$$f_k(\alpha, X) = \sum_{1 \leq x \leq X} e^{2\pi i(\alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k)}$$

then

$$\begin{aligned}\int_{[0,1]^k} |f(\alpha,X)|^{2s} d\alpha &= \int_{[0,1]^k} \left(f(\alpha,X)\overline{f(\alpha,X)}\right)^s d\alpha \\ &= \int_{[0,1]^k} \sum_{1\le x_1,\ldots,x_{2s}\le X} e^{2\pi i((x_1-x_{s+1}+\ldots+x_s-x_{2s})\alpha_1+\ldots+(x_1^k-x_{s+1}^k+\ldots+x_s^k-x_{2s}^k)\alpha_k)} d\alpha \\ &= J_{s,k}(X)\end{aligned}$$

since the coefficients of the $\alpha_i$ must all be simultaneously zero to make the integral nonzero.

Noting that

$$|(x_1^j - x_{s+1}^j) + \ldots + (x_s^j - x_{2s}^j)| \le sX^j$$

the diophantine equations

$$(x_1^j - x_{s+1}^j) + \ldots + (x_s^j - x_{2s}^j) + h_j = 0$$

where $|h_j| \le sX^j$ therefore capture all permutations of $x_i$s, and so have at least $X^{2s}$ solutions. Therefore, applying the same argument as above to this new system of equations,

$$X^{2s} \le \sum_{|h_j|\le sX^j} \int_{[0,1]^k} |f(\alpha,X)|^{2s} e^{2\pi i h\cdot\alpha} d\alpha \le s^k X^1 \cdots X^k J_{s,k}(X)$$

so we have the lower bound

$$J_{s,k}(X) \gtrsim X^{2s-k(k+1)/2}$$

We also have the trivial lower bound

$$J_{s,k}(X) \gtrsim X^s$$

by taking $x_1 = x_{s+1}$ and so on. This motivates the right hand side of our main conjecture; if the conjecture is true we have more or less entirely captured the asymptotic behaviour of $J_{s,k}(X)$.

## Passing to Congruences

The Vinogradov system of diophantine equations is invariant under dilations and translations. That is,

$$\sum_{i=1}^{s} x_i^j = \sum_{i=s+1}^{2s} x_i^j$$

if and only if

$$\sum_{i=1}^{s}(\lambda x_i + c)^j = \sum_{i=s+1}^{2s}(\lambda x_i + c)^j$$

Proof:

Since our system of equations is homogeneous, it is clearly dilation invariant. Now,

$$\begin{aligned}\sum_{i=1}^{s}(x_i + c)^j &= \sum_{i=1}^{s}\sum_{l=0}^{j}\binom{j}{l}x_i^l c^{j-l} \\ &= \sum_{l=0}^{j}\binom{j}{l}c^{j-l}\sum_{i=1}^{s}x_i^l\end{aligned}$$

But for $l \leq j \leq k$,

$$\sum_{i=1}^{s}x_i^l = \sum_{i=s+1}^{2s}x_i^l$$

so

$$\sum_{i=1}^{s}(x_i + c)^j = \sum_{l=0}^{j}\binom{j}{l}c^{j-l}\sum_{i=1}^{s}x_i^l = \sum_{l=0}^{j}\binom{j}{l}c^{j-l}\sum_{i=s+1}^{2s}x_i^l = \sum_{i=s+1}^{2s}(x_i + c)^j$$

so the system is also translation invariant $\square$

This fact will be useful momentarily. In the mean time, we make a new definition

$$f_a(\alpha, X, \xi) = \sum_{\substack{1 \leq x \leq X \\ x \equiv \xi \mod p^a}} e^{2\pi i(\alpha_1 x + \ldots + \alpha_k x^k)}$$

where $p > k$ will be a fixed prime.

Now,

$$|f(\alpha, X)|^{2s} = \left|\sum_{\xi=1}^{p}\sum_{\substack{1 \leq x \leq X \\ x \equiv \xi \mod p}} e^{2\pi i(\alpha_1 x + \ldots + \alpha_k x^k)}\right|^{2s} \leq p^{2s-1}\sum_{\xi=1}^{p}|f_1(\alpha, X, \xi)|^{2s}$$

by Holder's inequality with exponents $2s$ and $\frac{2s}{2s-1}$. Then,

$$\begin{aligned} J_{s+k,k} &= \int_{[0,1]^k} |f(\alpha, X)|^{2s+2k} d\alpha \\ &\leq p^{2s-1} \int_{[0,1]^k} |f(\alpha, X)|^{2k} \sum_{\xi=1}^{p} |f_1(\alpha, X, \xi)|^{2s} d\alpha \\ &\leq p^{2s} \max_{1 \leq \xi \leq p} \int_{[0,1]^k} |f(\alpha, X)|^{2k} |f(\alpha, X, \xi)|^{2s} d\alpha \end{aligned}$$

Analogously to earlier, the integral will count solutions to the equations

$$\sum_{i=1}^{k} (x_i^j - y_i^j) = \sum_{l=1}^{s} ((pu_l + \xi)^j - (pv_l + \xi)^j)$$

(for $1 \leq j \leq k$) as this will be when the exponents are zero (on the right hand side we have written the general form of $x_i$s that are congruent to $\xi$ modulo $p$). But now we can use translation invariance! This system is equivalent to

$$\sum_{i=1}^{k} ((x_i - \xi)^j - (y_i - \xi)^j) = p^j \sum_{l=1}^{s} (u_l^j - v_l^j)$$

or

$$\sum_{i=1}^{k} (x_i - \xi)^j \equiv \sum_{i=1}^{k} (y_i - \xi)^j \mod p^j$$

Thus the congruences we picked were "efficient" in the sense that we started with requiring some information modulo $p$ and ended up with some equations modulo $p^j$, which contain "more" information. If the $x_i$ all lie in different congruence class modulo $p$, we follow Wooley's terminology [Woo12] and call $x$ "well-conditioned". In a more rigorous argument, there is a step called "conditioning" which allows us to consider this as the general case. We now allow the $y_i$ to vary freely, so that we are looking for solutions to

$$\sum_{i=1}^{k} (x_i - \xi)^j \equiv n_j \mod p^j$$

We need a lemma:

**Linnik's Lemma** [Mon94]: The number of solutions to the system of congruences

$$\sum_{i=1}^{k} z_i^j \equiv n_j \mod p^j$$

where $1 \leq j \leq k$ for well conditioned $z_i$ is at most $k! p^{k(k-1)/2}$

Proof:

There are $p^{k-j}$ lifts of $n_j$ modulo $p^j$ to $n'_j$ modulo $p^k$. So there are $p^{k(k-1)/2}$ ways to turn this into a system of congruences

$$\sum_{i=1}^{k} z_i^j \equiv n'_j \mod p^k$$

Now, if

$$\sum_{i=1}^{k} z_i^j \equiv \sum_{i=1}^{k} w_i^j \mod p^k$$

then the power sum symmetric functions (and thus all symmetric functions as these form a basis) are equal on $z$ and $w$. Therefore,

$$\prod_i (t - z_i) \equiv \prod_i (t - w_i) \mod p^k$$

since the coefficients of $t^l$ are given by elementary symmetric functions in $z$ or $w$. Thus,

$$\prod_i (w_1 - z_i) \equiv 0 \mod p^k$$

and similarly for the rest of the $w$s. Thus the $w$s are necessarily a permutation of the $z$s (since being well conditioned prevents more than one zero divisor from appearing in the product), of which there are $k!$ possibilities. Multiplying our choices together, we arrive at the result $\square$

If we now choose $X < p^k < 2X$ (such a $p$ always exists due to the prime number theorem), a solution to these congruences is exactly a solution as integers. That is,

$$0 = \sum_{i=1}^{k} ((x_i - \xi)^j - (y_i - \xi)^j) = p^j \sum_{l=1}^{s} (u_l^j - v_l^j)$$

so the number of solutions to our system of equations is

$$\begin{aligned} J_{s+k,k}(X) &\lesssim p^{2s} p^{k(k-1)/2} X^k J_{s,k}(X/p) \\ &\lesssim (X^{1/k})^{2s+k(k-1)/2} X^k J_{s,k}(X/p) \end{aligned}$$

Here the first term is from earlier, the second from the $x$s, the third from the $y$s and the last term from the $u$ and $v$ equations, where we had $pu_l + \xi \leq X$ and similarly for the $v$.

So what was the point? It appears we have only complicated things thus far. Well, if we denote by $\lambda^*_{s,k}$ the smallest exponent such that

$$J_{s,k}(X) \lesssim_{s,k,\epsilon} X^{\lambda^*_{s,k}+\epsilon}$$

and then write

$$\lambda^*_{s,k} = 2s - \frac{1}{2}k(k+1) + \eta_{s,k}$$

then a reformulation of our main conjecture (at the critical index) is that $\eta_{s,k} = 0$. What we have shown here is that

$$\eta_{s+k,k} \leq \eta_{s,k}(1 - 1/k)$$

It is known by essentially the same argument as Linnik's lemma that $J_{k,k}(X) \leq k!X^k$, so we can now induct on $k$ to get Vinogradov's original result

$$\eta_{s,k} \leq \frac{k^2}{2}(1 - 1/k)^{[s/k]}$$

where the square brackets indicate rounding. You may notice that this is pretty far from zero, however.

What Wooley did was instead of choosing $p \approx X^{1/k}$, he made the more general choice of $p \approx X^\theta$ for some various small $\theta$. In particular, $p^k \not\geq X$ in his argument, so the solution modulo $p^k$ gives solutions of the form $x = y + p^k h$. This method is significantly more complicated than what has been outlined above, but the moral is that he can now perform an "induction on scales" argument, where the scales are in the $p$-adic topology (that is, passing to congruences modulo higher and higher powers of $p$ in order to obtain stronger bounds). See [Woo19], §2 for details.

An important thing to note about this method is that it is largely insensitive to the number field we are working in, and thus also implies similar results over arbitrary number (or function) fields and their localisations. This is discussed more in [Woo19], §15, 17.

## Analogy to Decoupling

The main conjecture has also been proved (by [BDG16], or [GLYZ21] for a more efficient argument) via Fourier decoupling, and the arguments bear enough similarities that it is thought they may be two examples of the same phenomena; over archimedian and non-archimedian topologies (See [Pie20] §8.5 for some idea of this).

Defining the moment curve

$$\Gamma_J = \{(t, t^2, \ldots, t^k) \mid t \in J\}$$

for $J \subset [0, 1]$ the extension operator for this curve is

$$\mathcal{E}_J f(x) = \int_J f(t) e^{2\pi i(x_1 t + x_2 t^2 + \ldots + x_k t^k)} dt$$

as changing variables from the surface measure of the curve to a one dimensional parameter introduces these weights on the $x_i$. The idea now is to decouple $\mathcal{E}_{[0,1]}f$ into $\delta$-pieces $\mathcal{E}_J f$ via the theorem of Bourgain, Demeter and Guth:

$$\|\mathcal{E}_{[0,1]}f\|_{L^{n(n+1)}} \lesssim_{n,\epsilon} \delta^{-\epsilon} \left( \sum_{\substack{J \subset [0,1] \\ |J| = \delta}} \|\mathcal{E}_J f\|^2_{L^{n(n+1)}} \right)^{1/2}$$

As a technical note, this $L^{n(n+1)}$ space is weighted and the statement holds for a particular class of weights. We omit these details here and going forward in favour of a more efficient exposition.

This then allows us to obtain "discrete decoupling", that is, an expression of the form

$$\int_{\mathbb{R}^n} \left| \sum_{i=1}^{N} a_n e^{2\pi i(x_1 t_i + \ldots + x_k t_i^k)} \right|^{n(n+1)} dx \lesssim_\epsilon N^\epsilon \left( \sum_{i=1}^{N} |a_i|^2 \right)^{n(n+1)/2}$$

where the $t_i$ lie in $\delta$-separated (we interchangeably use $\delta$ and $1/N$) sets $J$.

Note the similarity here to the efficient congruencing method; where the $x_i$ were required to be in distinct residue classes modulo $p$, that is, separated in the $p$-adic norm. In fact this analogy goes slightly further; as was briefly mentioned earlier the efficient congruencing method usese translation-dilation invariance to induct on $p$-adic scales, while the decoupling approach inducts on euclidean scales.

The rest of the argument is considerably more technical, so we omit it. Instead, let us briefly note that eventually the idea of bilinear estimates enters the decoupling argument, which bears at least some similarity to our earlier expression

$$J_{s+k,k} \leq p^{2s} \max_{1 \leq \xi \leq p} \int_{[0,1]^k} |f(\alpha, X)|^{2k} |f(\alpha, X, \xi)|^{2s} d\alpha$$

(and in the full treatment given by Wooley, several other expressions of this form appear). Effectively realising these two methods of proof as examples of the same phenomena could have powerful implications, and lead to a better understanding of analytic number theory.

# References

This report broadly follows the notation and exposition of [Pie20].


1. Bourgain, J., Demeter, C., & Guth, L. (2016). Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. https://arxiv.org/abs/1512.01565

2. Guo, S., Li, Z. K., Yung, P.-L., & Zorin-Kranich, P. (2021). A short proof of $\ell^2$ decoupling for the moment curve. American Journal of Mathematics, 143(6), 1983–1998. https://doi.org/10.1353/ajm.2021.0048

3. Montgomery, H. (1994). Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis. Regional Conference Series in Mathematics ISSN 0160-7642, no. 84.

4. Pierce, L. B. (2020). The Vinogradov Mean Value Theorem [after Wooley, and Bourgain, Demeter and Guth]. https://arxiv.org/abs/1707.00119

5. Wooley, T.D. (2012). Vinogradov's mean value theorem via efficient congruencing. Annals of Mathematics, 175(3), 1575–1627. https://doi.org/10.4007/annals.2012.175.3.12

6. Wooley, T.D. (2019), Nested efficient congruencing and relatives of Vinogradov's mean value theorem. Proc. London Math. Soc., 118: 942-1016. https://doi.org/10.1112/plms.12204