LECTURE NOTES 2 FOR CAMBRIDGE PART III COURSE ON "THE RIEMANN ZETA FUNCTION", LENT 2014

ADAM J HARPER

Abstract. These are rough notes covering the second block of lectures in "The Riemann Zeta Function" course. In these lectures we will develop the exponential sum method of Korobov and Vinogradov, and use it to prove the best known order estimate for $\zeta(s)$ close to the 1-line, and the best zero-free region known. This has important consequences for the error term in the Prime Number Theorem.

(No originality is claimed for any of the contents of these notes. In particular, they borrow from the classic books of Ivić [1] and Titchmarsh [2].)

7. First thoughts on estimating zeta sums

In section 5 we proved Landau's theorem (Theorem 5.1), which showed that if we had a bound $\zeta(\sigma+it) = O(e^{\phi(t)})$ in a region to the left of the 1-line, with $\phi(t)$ hopefully not too large a function, then we could deduce a zero-free region for the zeta function. In this Chapter we will prove a highly non-trivial bound for the zeta function, due to Vinogradov and Korobov in 1958, and deduce a wider zero-free region. (Vinogradov and Korobov worked independently, but both exploited ideas from earlier works of Vinogradov, hence their names are traditionally written non-alphabetically.)

If $t \geq 1$ and $\sigma > 0$, then using Hardy and Littlewood's approximation to the zeta function (Theorem 3.3) with the choice $x = t$ we see

$$\zeta(\sigma+it) = \sum_{n \leq t} \frac{1}{n^{\sigma+it}} + \frac{t^{1-\sigma-it}}{\sigma+it-1} + O(t^{-\sigma}) = \sum_{n \leq t} \frac{1}{n^{\sigma+it}} + O(1).$$

By partial summation, bounding $\sum_{n \leq t} \frac{1}{n^{\sigma+it}}$ is basically equivalent to bounding sums $\sum_{N < n \leq N+M} n^{-it}$, where $M \leq N \leq t$. These partial sums are sometimes called *zeta sums*. Note that, in order to bound all of the sum $\sum_{n \leq t} \frac{1}{n^{\sigma+it}}$, we need to bound zeta sums with N much smaller than t.

When we proved Theorem 3.3, we showed using Fourier analysis that certain zeta sums of length $N \gg t$ behaved like the corresponding integrals $\int_N^{N+M} w^{-it} dw$, but we do not know how to do that efficiently when N is much smaller than t. Instead we must work with the zeta sum directly, using more combinatorial arguments. The summands $n^{-it} = e^{-it \log n}$ don't seem to have much useable structure, so our first step is to introduce some polynomial structure using Taylor expansion.

Date: 18th March 2014.

Lemma 7.1. *Suppose that N is large, and $1 \le M \le N \le t$. Set $r := \lfloor \frac{5.01 \log t}{\log N} \rfloor$. Then*

$$\sum_{N < n \le N+M} n^{-it} = O\left(M \max_{N \le n \le 2N} \frac{|U(n)|}{N^{4/5}} + N^{4/5} + Mt^{-1/500} \right),$$

where

$$U(n) := \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} e(\alpha_1 xy + \alpha_2 x^2 y^2 + ... + \alpha_r x^r y^r), \qquad \alpha_j := \frac{(-1)^j t}{2\pi j n^j}.$$

Proof of Lemma 7.1. Note first that

$$\begin{aligned} \sum_{N < n \le N+M} n^{-it} &= \frac{1}{\lfloor N^{2/5} \rfloor^2} \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} \sum_{N < n \le N+M} n^{-it} \\ &= \frac{1}{\lfloor N^{2/5} \rfloor^2} \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} \left(\sum_{N < n \le N+M} (n+xy)^{-it} + O(N^{4/5}) \right) \\ &= \sum_{N < n \le N+M} n^{-it} \frac{1}{\lfloor N^{2/5} \rfloor^2} \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} (1 + \frac{xy}{n})^{-it} + O(N^{4/5}). \end{aligned}$$

The point of the above is that the shift xy is always much smaller than n, so we can apply Taylor expansion efficiently to $(1+xy/n)^{-it} = e^{-it \log(1+xy/n)}$. Indeed we have

$$\log\left(1 + \frac{xy}{n}\right) = \sum_{j=1}^{r} \frac{(-1)^{j-1}}{j} \left(\frac{xy}{n}\right)^j + O\left(\left(\frac{xy}{n}\right)^{5.01(\log t)/\log N} \right) = \sum_{j=1}^{r} \frac{(-1)^{j-1}}{j} \left(\frac{xy}{n}\right)^j + O(t^{-(1+1/500)}),$$

since $xy/n \le N^{-1/5}$. This implies that

$$\begin{aligned} \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} (1 + \frac{xy}{n})^{-it} &= \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} e\left(\sum_{j=1}^{r} \alpha_j (xy)^j \right) e\left(O(t^{-1/500}) \right) \\ &= \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} e\left(\sum_{j=1}^{r} \alpha_j (xy)^j \right) + O(N^{4/5} t^{-1/500}), \end{aligned}$$

remembering that $e(z) := e^{2\pi i z}$. The conclusion of the lemma follows immediately. □

Remark 7.2. The exact choice of many of the parameters in the proof of Lemma 7.1 (e.g. the exponents 2/5 in the shifts) is not important. Something that is important is the fact that the degree r of the polynomial in the exponent is $\asymp (\log t)/\log N$. It will turn out that we can only handle the case where the degree isn't too large relative to N, and this will ultimately set the limit of the Vinogradov–Korobov method.

Remark 7.3. It may seem strange that we introduced the two shift parameters x, y in Lemma 7.1, since we could have performed Taylor expansion in the same way with just one. However, it turns out that introducing a pair of independent variables is very often a very good idea, and we shall explore this next.

8. Bilinear forms

In this section we will think about the general problem of bounding

$$\sum_{\tilde{x}\in\mathcal{X}}\sum_{\tilde{y}\in\mathcal{Y}} e(\alpha\tilde{x}\cdot\tilde{y}),$$

where $\alpha\in\mathbb{R}$ and $\mathcal{X},\mathcal{Y}$ are general sets of r-vectors. We will start by considering a simple problem to illustrate the usefulness of the bilinear structure, and to develop some basic estimates needed later. Afterwards we will turn to the sums $U(n)$ appearing in Lemma 7.1 (in which $\tilde{x}=(x,x^2,...,x^r)$, similarly for $\tilde{y}$).

Proposition 8.1 (Toy Proposition)**.** *Let $\alpha=a/q+\theta/q^2$, where $q\geq 1$, $(a,q)=1$, and $|\theta|\leq 1$. Let N be a large natural number. Then*

$$\sum_{p\leq N}\sum_{p'\leq N} e(\alpha pp') \ll N\max\{\frac{N}{\sqrt{q}},\sqrt{q}\}\sqrt{\log(q+1)},$$

where the sums are over primes p,p'.

Note that the bound in the proposition beats the trivial bound $\pi(N)^2$ provided q is neither too big nor too small. To prove the proposition we will need a small technical result, that will also be needed later.

Lemma 8.2. *Let α and N be as in the statement of Proposition 8.1, and let $\beta,U\geq 0$ be arbitrary. Let $||x||$ denote the distance from $x\in\mathbb{R}$ to the nearest integer. Then*

$$\sum_{n\leq N}\min\{U,\frac{1}{||\alpha n+\beta||}\}\ll\left(\frac{N}{q}+1\right)(U+q\log q).$$

Proof of Proposition 8.1. The crucial first step is to *complete one sum* (using the bilinear structure), and apply the Cauchy–Schwarz inequality. Thus we have

$$\left|\sum_{p\leq N}\sum_{p'\leq N} e(\alpha pp')\right|\leq\sum_{n\leq N}\left|\sum_{p\leq N} e(\alpha pn)\right|\leq\sqrt{N}\sqrt{\sum_{n\leq N}\left|\sum_{p\leq N} e(\alpha pn)\right|^2}.$$

Now we have replaced a sum over primes, which is difficult to handle, by a sum over all integers which is much easier. Indeed we have

$$\sum_{n\leq N}\left|\sum_{p\leq N} e(\alpha pn)\right|^2=\sum_{n\leq N}\left(\sum_{p\leq N} e(\alpha pn)\right)\left(\sum_{p'\leq N} e(-\alpha p'n)\right)=\sum_{p,p'\leq N}\sum_{n\leq N} e(\alpha(p-p')n),$$

and in general by summing a geometric progression (and since $|\sin x|\geq(2/\pi)|x|$ if $|x|\leq\pi/2$) one has

$$\left|\sum_{n\leq N} e(\beta n)\right|=\left|\frac{e(\beta(N+1))-e(\beta)}{e(\beta)-1}\right|\leq\frac{2}{|e(\beta/2)-e(-\beta/2)|}=\frac{1}{|\sin(\pi\beta)|}\leq\frac{1}{2||\beta||},$$

where $||\beta||$ denotes the distance from β to the nearest integer. We also have the trivial bound $\left|\sum_{n \leq N} e(\beta n)\right| \leq N$, so we conclude that

$$\sum_{n \leq N} \left| \sum_{p \leq N} e(\alpha p n) \right|^2 \ll \sum_{p,p' \leq N} \min\{N, \frac{1}{||\alpha(p-p')||}\} \ll N \sum_{0 \leq n \leq N} \min\{N, \frac{1}{||\alpha n||}\}.$$

Here the last inequality used the fact that the numbers $(p-p')$ cover the integers between $-N$ and N at most N times each, and $||\alpha n|| = ||\alpha(-n)||$.

Finally, Lemma 8.2 implies that

$$\sum_{0 \leq n \leq N} \min\{N, \frac{1}{||\alpha n||}\} \ll \left(\frac{N}{q} + 1\right)(N + q \log q) \ll \max\{\frac{N^2}{q}, q\} \log(q+1),$$

and the proposition follows. □

Proof of Lemma 8.2. It will suffice to show that

$$\sum_{-q/2 < n \leq q/2} \min\{U, \frac{1}{||\alpha n + \beta||}\} \ll (U + q \log q),$$

since if $N \geq q$ then one can break the sum in the lemma into at most $N/q + 1$ sums of length at most q, and apply this bound (for suitable β). The bound is trivial if $q = 1$, so assume henceforth that $q \geq 2$.

To prove the bound, note that for all $-q/2 < n \leq q/2$ we have

$$\left| \alpha n - \frac{an}{q} \right| = \frac{|\theta n|}{q^2} \leq \frac{1}{2q}.$$

Since $(a, q) = 1$, as $-q/2 < n \leq q/2$ varies the numbers an vary over all the residue classes r modulo q, hitting each once. Thus, as n varies, at most $O(1)$ of the numbers αn will lie in each interval $[(r - 1/2)/q, (r + 1/2)/q]$ modulo 1. On translating by β (modulo 1), this clearly implies that at most $O(1)$ of the numbers $\alpha n + \beta$ will lie in each interval $[(r - 1/2)/q, (r + 1/2)/q]$ modulo 1.

Finally, if $\alpha n + \beta \in [-1/2q, 1/2q]$ then we cannot rule out that $||\alpha n + \beta||$ is very small, so we will use the bound $\min\{U, \frac{1}{||\alpha n + \beta||}\} \leq U$. But if $\alpha n + \beta \in [(r - 1/2)/q, (r + 1/2)/q]$ for some non-zero $-q/2 < r \leq q/2$ then we can use the bound $\min\{U, \frac{1}{||\alpha n + \beta||}\} \ll q/|r|$ instead. Therefore

$$\sum_{-q/2 < n \leq q/2} \min\{U, \frac{1}{||\alpha n + \beta||}\} \ll U + \sum_{1 \leq r \leq q/2} \frac{q}{r} \ll U + q \log q,$$

as claimed. □

In the proof of Proposition 8.1, we lost a bit when replacing sums over primes by sums over integers, since the primes are a sparse set. But they are not very sparse, so this loss (of logarithmic factors) didn't matter much. In contrast, the sums $U(n)$ in Lemma

7.1 are sums over vectors $(x, x^2, ..., x^r), (y, y^2, ..., y^r)$, which form a very sparse subset of the r-dimensional box that contains them. To overcome this we will need another idea, which we shall deploy at the same time as exploiting the bilinear structure. This is all done in the following lemma.

Lemma 8.3 (Duplication of variables)**.** *Let* $U(n) = \sum_{x\leq N^{2/5}} \sum_{y\leq N^{2/5}} e(\alpha_1 xy+\alpha_2 x^2y^2+ ... + \alpha_r x^r y^r)$ *be as in the statement of Lemma 7.1. Then for any natural number* k *we have*

$$|U(n)| \leq N^{4/5} \left(\frac{1}{N^{8k/5}} \left(J_{k,r}(N^{2/5})\right)^2 \prod_{j=1}^{r} \sum_{-kN^{2j/5}\leq \mu_j \leq kN^{2j/5}} \min\{3kN^{2j/5}, \frac{1}{||\alpha_j \mu_j||}\} \right)^{1/(4k^2)},$$

where $J_{k,r}(N^{2/5})$ *denotes the number of solutions* $(x_1, ..., x_{2k})$ *of the simultaneous equations*

$$\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j \quad \forall 1 \leq j \leq r$$

with $1 \leq x_i \leq N^{2/5}$ *integers.*

Proof of Lemma 8.3. The proof is like that of the Toy Proposition, but with the application of the Cauchy–Schwarz inequality replaced by two applications of Hölder's inequality (with exponent $2k$). This has the effect of producing $2k$ duplicate copies of each of the variables x, y, so that the *sums of the resulting duplicated vectors* $(x, x^2, ..., x^r), (y, y^2, ..., y^r)$ *cover an* r*-dimensional box much more uniformly.*

To simplify the writing, let us temporarily set $Z := N^{2/5}$. By Hölder's inequality we have

$$\begin{aligned} |U(n)|^{2k} &\leq Z^{2k-1} \sum_{x\leq Z} \left| \sum_{y\leq Z} e(\alpha_1 xy + \alpha_2 x^2y^2 + ... + \alpha_r x^r y^r) \right|^{2k} \\ &= Z^{2k-1} \sum_{x\leq Z} \sum_{y_1,...,y_{2k}\leq Z} e\left(\alpha_1 x(\sum_{i=1}^{k} y_i - \sum_{i=k+1}^{2k} y_i) + ... + \alpha_r x^r (\sum_{i=1}^{k} y_i^r - \sum_{i=k+1}^{2k} y_i^r) \right). \end{aligned}$$

So if we let $J_{k,r}(\lambda_1, ..., \lambda_r; Z)$ denote the number of solutions $(x_1, ..., x_{2k})$ of the simultaneous equations

$$\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j + \lambda_j \quad \forall 1 \leq j \leq r,$$

with $1 \leq x_i \leq Z$ integers, then we have

$$\begin{aligned} |U(n)|^{2k} &\leq Z^{2k-1} \sum_{x\leq Z} \sum_{-kZ\leq \lambda_1 \leq kZ} ... \sum_{-kZ^r \leq \lambda_r \leq kZ^r} J_{k,r}(\lambda_1, ..., \lambda_r; Z) e\left(\alpha_1 x\lambda_1 + ... + \alpha_r x^r \lambda_r\right) \\ &\leq Z^{2k-1} \sum_{-kZ\leq \lambda_1 \leq kZ} ... \sum_{-kZ^r \leq \lambda_r \leq kZ^r} J_{k,r}(\lambda_1, ..., \lambda_r; Z) \left| \sum_{x\leq Z} e\left(\alpha_1 x\lambda_1 + ... + \alpha_r x^r \lambda_r\right) \right|. \end{aligned}$$

To simplify the writing further, from now on we will usually write $\sum_{\lambda_j}$ (without a range of summation) as shorthand for $\sum_{-kZ^j \leq \lambda_j \leq kZ^j}$.

In the proof of the Toy Proposition, we were more or less finished at this point because we could explicitly evaluate the inner sum. We are not so lucky here, so we use Hölder's inequality to duplicate variables again, obtaining that

$$\begin{aligned} |U(n)|^{(2k)^2} &\leq Z^{2k(2k-1)} \left(\sum_{\lambda_1} ... \sum_{\lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z) \left| \sum_{x \leq Z} e\left(\alpha_1 x \lambda_1 + ... + \alpha_r x^r \lambda_r\right) \right| \right)^{2k} \\ &\leq Z^{2k(2k-1)} \left(\sum_{\lambda_1} ... \sum_{\lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z)^{2k/(2k-1)} \right)^{2k-1} \\ &\quad \times \sum_{\lambda_1} ... \sum_{\lambda_r} \left| \sum_{x \leq Z} e\left(\alpha_1 x \lambda_1 + ... + \alpha_r x^r \lambda_r\right) \right|^{2k}. \end{aligned}$$

To bound the first term in brackets, we note that

$$\begin{aligned} \sum_{\lambda_1} ... \sum_{\lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z)^{\frac{2k}{2k-1}} &\leq \left(\max_{\lambda_1, ..., \lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z)^{1/(2k-1)} \right) \times \sum_{\lambda_1} ... \sum_{\lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z) \\ &\leq Z^{2k} \left(\max_{\lambda_1, ..., \lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z)^{1/(2k-1)} \right), \end{aligned}$$

since $\sum_{\lambda_1} ... \sum_{\lambda_r} J_{k,r}(\lambda_1, ..., \lambda_r; Z)$ simply counts all vectors $(x_1, ..., x_{2k})$ with $1 \leq x_i \leq Z$ integers. We also note that, for any $\lambda_1, ..., \lambda_r$, the Cauchy–Schwarz inequality implies

$$\begin{aligned} J_{k,r}(\lambda_1, ..., \lambda_r; Z) &= \sum_{L_1, L_2, ..., L_r \in \mathbb{Z}} \Bigg(\#\{(x_1, ..., x_k) : 1 \leq x_i \leq Z, \text{ and } \sum_{i=1}^{k} x_i^j = L_j \; \forall 1 \leq j \leq r\} \\ &\quad \times \#\{(x_{k+1}, ..., x_{2k}) : 1 \leq x_i \leq Z, \text{ and } \sum_{i=k+1}^{2k} x_i^j = L_j - \lambda_j \; \forall 1 \leq j \leq r\} \Bigg) \\ &\leq \sum_{L_1, L_2, ..., L_r \in \mathbb{Z}} \left(\#\{(x_1, ..., x_k) : 1 \leq x_i \leq Z, \text{ and } \sum_{i=1}^{k} x_i^j = L_j \; \forall 1 \leq j \leq r\} \right)^2 \\ &= J_{k,r}(0, ..., 0; Z) =: J_{k,r}(Z). \end{aligned}$$

Therefore we have

$$|U(n)|^{(2k)^2} \leq Z^{4k(2k-1)} J_{k,r}(Z) \sum_{\lambda_1} ... \sum_{\lambda_r} \left| \sum_{x \leq Z} e\left(\alpha_1 x \lambda_1 + ... + \alpha_r x^r \lambda_r\right) \right|^{2k},$$

and on expanding the $2k$-th power as before we obtain that $|U(n)|^{(2k)^2}$ is

$$\leq Z^{4k(2k-1)} J_{k,r}(Z) \sum_{\lambda_1} ... \sum_{\lambda_r} \sum_{-kZ\leq\mu_1\leq kZ} ... \sum_{-kZ^r\leq\mu_r\leq kZ^r} J_{k,r}(\mu_1,...,\mu_r;Z) e\left(\alpha_1\mu_1\lambda_1 + ... + \alpha_r\mu_r\lambda_r\right)$$

$$\leq Z^{4k(2k-1)} \left(J_{k,r}(Z)\right)^2 \sum_{-kZ\leq\mu_1\leq kZ} ... \sum_{-kZ^r\leq\mu_r\leq kZ^r} \left| \sum_{-kZ\leq\lambda_1\leq kZ} e(\alpha_1\mu_1\lambda_1) \right| ... \left| \sum_{-kZ^r\leq\lambda_r\leq kZ^r} e(\alpha_r\mu_r\lambda_r) \right|.$$

We have finally arrived at exponential sums that we can evaluate, and proceeding as in the proof of the Toy Proposition we obtain

$$|U(n)|^{(2k)^2} \leq Z^{4k(2k-1)} \left(J_{k,r}(Z)\right)^2 \sum_{-kZ\leq\mu_1\leq kZ} ... \sum_{-kZ^r\leq\mu_r\leq kZ^r} \min\{3kZ, \frac{1}{||\alpha_1\mu_1||}\} ... \min\{3kZ^r, \frac{1}{||\alpha_r\mu_r||}\}.$$

Raising both sides to the power $1/(4k^2)$, and remembering that $Z = N^{2/5}$, the bound claimed in the lemma follows. □

Remark 8.4. Note that in the proof of Lemma 8.3 we needed to switch the order of our sums more than once (as well as duplicating variables) to arrive at sums we could estimate. This shows the power of the simple idea of introducing two independent variables x, y: at any point one can move one set of sums to the inside, surrounded by absolute value signs, and then complete the ranges of the outside sums to obtain something nicer.

In order to obtain a useful bound from Lemma 8.3, we need to give a non-trivial bound for the product over j appearing there (which will be an easy calculation using Lemma 8.2), and we need a good bound for $J_{k,r}(N^{2/5})$. We also cannot succeed unless k is chosen suitably large, since the applications of Hölder's inequality in the proof of Lemma 8.3 are very inefficient unless $J_{k,r}(\lambda_1,...,\lambda_r;N^{2/5}) \approx J_{k,r}(N^{2/5})$ for most $\lambda_1,...,\lambda_r$, which can only happen if k is large in terms of r. In the next section we will study $J_{k,r}(N^{2/5})$, and this will occupy most of the rest of Chapter 2.

9. Vinogradov's Mean Value Theorem

This section is devoted to the study of $J_{k,r}(Z)$, the number of solutions $(x_1,...,x_{2k})$ of the simultaneous equations

$$\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j \quad \forall 1 \leq j \leq r$$

with $1 \leq x_i \leq Z$ integers (for Z large). This quantity is called *Vinogradov's mean value*, and as well as its applications to the zeta function it is of great interest in its own right, and in additive number theory as well (especially in connection with Waring's problem).

We trivially always have $J_{k,r}(Z) \geq \lfloor Z \rfloor^k$, since for any choice of $x_1,...,x_k$ we can take $(x_{k+1},...,x_{2k}) = (x_1,...,x_k)$. (These trivial solutions are called *diagonal solutions*.)

Moreover, we observed in section 8 that

$$\lfloor Z \rfloor^{2k} = \sum_{-kZ \le \lambda_1 \le kZ} \dots \sum_{-kZ^r \le \lambda_r \le kZ^r} J_{k,r}(\lambda_1, \dots, \lambda_r; Z) \le J_{k,r}(Z) \sum_{-kZ \le \lambda_1 \le kZ} \dots \sum_{-kZ^r \le \lambda_r \le kZ^r} 1,$$

and therefore we see

$$J_{k,r}(Z) \ge \frac{\lfloor Z \rfloor^{2k}}{\prod_{j=1}^r (3kZ^j)} = (3k)^{-r} \lfloor Z \rfloor^{2k} Z^{-(1/2)r(r+1)}.$$

This bound would be close to the truth if the differences $\sum_{i=1}^k x_i^j - \sum_{i=k+1}^{2k} x_i^j$ were all roughly uniformly distributed as the x_i varied. It is conjectured that the true size of $J_{k,r}(Z)$ is never much bigger (as a function of Z) than the largest of our two lower bounds.

Conjecture 9.1. *Let k, r be natural numbers, and let $Z \ge 1$ and $\epsilon > 0$ be arbitrary. Then*

$$J_{k,r}(Z) \ll_{k,r,\epsilon} Z^{k+\epsilon} + Z^{2k-(1/2)r(r+1)+\epsilon},$$

where the implicit constant may depend on k, r, ϵ (but not on Z).

Note in particular that if $k \ge (1/2)r(r+1)$ then the second term is at least as big as the first, so the conjecture says that the behaviour *is* roughly uniform. This is exactly what we would like to substitute into Lemma 8.3 to obtain a good bound for zeta sums. For us it will also be important to understand how the implicit constant depends on k, r, since we have $r \asymp (\log t)/\log N$ possibly tending to infinity along with $Z = N^{2/5}$.

Recently Wooley [3, 4] has proved Conjecture 9.1 for $k \ge r^2 - 1$ (and, jointly with Ford, for some smaller k as well). We shall not prove this great result, but we shall prove an older bound that seems just as good for our application to the zeta function.

Theorem 9.2 (Vinogradov's mean value theorem, Vinogradov, 1930s (with refinements by Korobov and others))**.** *Suppose Z is large, and let k, r be natural numbers such that $k \ge r^2$. Let $F = F(k,r) = \lfloor (k/r) - r \rfloor$ and let $\delta = \delta(k,r) = (1 - 1/r)^F$. Then*

$$J_{k,r}(Z) \le (4r)^{4kF} Z^{2k-(1-\delta)(1/2)r(r+1)}.$$

Remark 9.3. Note that if k/r^2 is large then δ will be small.

The proof of Theorem 9.2 works by fixing r and inducting on k. The inductive step is carried out by examining the system of equations $\sum_{i=1}^k x_i^j = \sum_{i=k+1}^{2k} x_i^j$ modulo a suitably chosen prime p, and applying a result called Linnik's Lemma. Note that this kind of argument will heavily exploit the polynomial structure that we worked to introduce all the way back in Lemma 7.1.

Lemma 9.4 (Linnik's Lemma, 1942–1943)**.** *Let $r \ge 1$ be a natural number. Also let A and $m \ge 1$ be integers, let $p > r$ be prime, and let $\lambda_1, \dots, \lambda_r$ be any integers. Then the*

number of solutions $(x_1, ..., x_r)$ *of the simultaneous congruences*

$$\sum_{i=1}^{r} x_i^j \equiv \lambda_j \mod p^j \qquad \forall 1 \le j \le r,$$

with $A \le x_i < A + mp^r$ *integers that are distinct modulo* p*, is*

$$\le (r!)m^r p^{r(r-1)/2}.$$

Proof of Lemma 9.4. Note first that, for any given integers $(\lambda_1, ..., \lambda_r)$, there are $\prod_{j=1}^{r-1} p^{r-j} = p^{r(r-1)/2}$ different vectors $(\mu_1, ..., \mu_r)$ modulo p^r such that

$$\mu_j \equiv \lambda_j \mod p^j \qquad \forall 1 \le j \le r.$$

So it will suffice to show that for any such vector $(\mu_1, ..., \mu_r)$, there are at most $(r!)m^r$ different solutions $(x_1, ..., x_r)$ such that

$$\sum_{i=1}^{r} x_i^j \equiv \mu_j \mod p^r \qquad \forall 1 \le j \le r.$$

(Note carefully that we have now "lifted" all of our congruences to be congruences modulo p^r.)

Next, suppose that

$$\sum_{i=1}^{r} x_i^j \equiv \sum_{i=1}^{r} y_i^j \equiv \mu_j \mod p^r \qquad \forall 1 \le j \le r.$$

Since $(r!, p) = 1$, the elementary symmetric functions $\sum x_{(1)}x_{(2)}...x_{(j)}$ in the x_i are uniquely determined modulo p^r by the power sums $\sum_{i=1}^{r} x_i^j$ modulo p^r (using Newton's identities), and therefore the polynomials

$$P(z) = \prod_{i=1}^{r}(z - x_i), \qquad Q(z) = \prod_{i=1}^{r}(z - y_i)$$

are identically congruent modulo p^r.

But we have $P(x_j) \equiv 0$ modulo p^r for all $1 \le j \le r$, and so we must have

$$Q(x_j) = \prod_{i=1}^{r}(x_j - y_i) \equiv 0 \mod p^r \qquad \forall 1 \le j \le r.$$

If the y_i are distinct modulo p this implies that x_j is congruent to one of the y_i modulo p^r, and so (since the x_j are also distinct modulo p) the x_j are forced to be a permutation of the y_j modulo p^r. This implies that there are at most $(r!)m^r$ possible solution vectors $(x_1, ..., x_r)$. □

Before proceeding to develop the inductive argument for the proof of Theorem 9.2, we record a simple but important observation about the system of equations $\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j$, $1 \le j \le r$.

Lemma 9.5 (Translation Invariance)**.** *If $(x_1, ..., x_{2k})$ solves the system of equations*

$$\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j \quad \forall 1 \leq j \leq r,$$

then so does $(x_1 - x, x_2 - x, ..., x_{2k} - x)$, for any x.

Proof of Lemma 9.5. We simply note that, by the binomial theorem,

$$\sum_{i=1}^{k} (x_i - x)^j = \sum_{i=1}^{k} x_i^j - jx \sum_{i=1}^{k} x_i^{j-1} + ... + j(-x)^{j-1} \sum_{i=1}^{k} x_i + k(-x)^j,$$

and similarly

$$\sum_{i=k+1}^{2k} (x_i - x)^j = \sum_{i=k+1}^{2k} x_i^j - jx \sum_{i=k+1}^{2k} x_i^{j-1} + ... + j(-x)^{j-1} \sum_{i=k+1}^{2k} x_i + k(-x)^j.$$

So if $\sum_{i=1}^{k} x_i^j = \sum_{i=k+1}^{2k} x_i^j$ for all $1 \leq j \leq r$ then the same must be true for the translated sums. □

Now we shall use Linnik's Lemma to set up an induction on the number of variables k. Unfortunately the proof of this Induction Lemma is very long, but it does split up into several distinct parts.

Lemma 9.6 (Induction Lemma)**.** *Let $r \geq 2$, and suppose that $Z \geq (2r)^{3r}$ and $k \geq r^2 + r$. Then*

$$J_{k,r}(Z) \leq 4^{2k} Z^{2k/r + (3r-5)/2} J_{k-r,r}(4Z^{(r-1)/r}).$$

Proof of Lemma 9.6. Choose any prime $(1/2)Z^{1/r} \leq p \leq Z^{1/r}$, and set $Z_1 = \lceil Z/p \rceil$. We have $pZ_1 \geq Z$, and therefore we certainly have $J_{k,r}(Z) \leq J_{k,r}(pZ_1)$. We also certainly have $Z_1 \leq 2Z/p \leq 4Z^{(r-1)/r}$, so to prove the lemma it will suffice to show that

$$J_{k,r}(pZ_1) \leq 4^{2k} Z^{2k/r + (3r-5)/2} J_{k-r,r}(Z_1).$$

Let us also note that $p > r$, because of our hypothesis that $Z \geq (2r)^{3r}$. This means that later on we will be able to apply Linnik's Lemma to r of our variables.

(Note that we choose $p \approx Z^{1/r}$ so that the ranges mp^r of the variables in Linnik's Lemma will approximately match the ranges Z of our variables.)

Next, let J_1 denote the number of solution vectors $(x_1, ..., x_{2k})$, counted by $J_{k,r}(pZ_1)$, in which $(x_1, ..., x_k)$ and $(x_{k+1}, ..., x_{2k})$ each contain at least r numbers that are distinct modulo p. Also let J_1' denote the number of solution vectors $(x_1, ..., x_{2k})$, counted by $J_{k,r}(pZ_1)$, for which the *first* r elements $(x_1, ..., x_r)$ and $(x_{k+1}, ..., x_{k+r})$ are distinct modulo p, and let J_2 denote the number of solution vectors *not* counted by J_1. Then we have

$$J_{k,r}(pZ_1) = J_1 + J_2 \leq k^{2r} J_1' + J_2,$$

since each vector counted by J_1' corresponds to at most k^{2r} vectors counted by J_1 (by permuting the components).

We shall bound J_1' and J_2 separately.

Bounding J_1'. I claim that we have

$$J_1' \leq p^{2k-2r} \max_{1\leq x\leq p} J_1'(x),$$

where $J_1'(x)$ denotes the number of solution vectors $(x_1, ..., x_{2k})$, counted by J_1', for which all of the $2k-2r$ components $(x_{r+1}, ..., x_k)$ and $(x_{k+r+1}, ..., x_{2k})$ are congruent to x modulo p. Assuming this for the present, we can use translation invariance (Lemma 9.5) to subtract x from all the components, and obtain that

$$\begin{aligned} J_1'(x) &= \#\{(\tilde{x}_1, ..., \tilde{x}_r, y_1, ..., y_{k-r}, \tilde{x}_{r+1}, ..., \tilde{x}_{2r}, y_{k-r+1}, ..., y_{2k-2r}) : 1-x \leq \tilde{x}_j \leq pZ_1 - x \ \forall j \leq 2r, \\ &\quad 0 \leq y_j \leq Z_1 - 1 \ \forall 1 \leq j \leq 2k-2r, \quad \text{and } (\tilde{x}_1, ..., \tilde{x}_r), (\tilde{x}_{r+1}, ..., \tilde{x}_{2r}) \text{ all distinct mod } p, \\ &\quad \sum_{i=1}^{r} \tilde{x}_i^j = \sum_{i=r+1}^{2r} \tilde{x}_i^j - p^j \sum_{i=1}^{k-r} y_i^j + p^j \sum_{i=k-r+1}^{2k-2r} y_i^j \quad \forall 1 \leq j \leq r\}. \end{aligned}$$

But now for any fixed $\tilde{x}_{r+1}, ..., \tilde{x}_{2r}$, each vector $(\tilde{x}_1, ..., \tilde{x}_r)$ satisfies the conditions of Linnik's Lemma, with $A = 1-x$ and $m = \lceil (pZ_1)/p^r \rceil \leq \lceil 2Z/p^r \rceil \leq 2^{r+1}$. And for any fixed $\tilde{x}_{r+1}, ..., \tilde{x}_{2r}$ and $\tilde{x}_1, ..., \tilde{x}_r$, the number of vectors $(y_1, ..., y_{2k-2r})$ that can be counted in $J_1'(x)$ is at most $J_{k-r,r}(Z_1)$. So in total, using the trivial bound $(pZ_1)^r$ for the number of choices of $\tilde{x}_{r+1}, ..., \tilde{x}_{2r}$, and using the non-trivial Linnik's Lemma bound $(r!)m^r p^{r(r-1)/2}$ for the number of choices of $(\tilde{x}_1, ..., \tilde{x}_r)$, we have

$$J_1'(x) \leq (pZ_1)^r (r!) m^r p^{r(r-1)/2} J_{k-r,r}(Z_1) \leq (2Z)^r (r!) 2^{r(r+1)} Z^{(r-1)/2} J_{k-r,r}(Z_1),$$

remembering again that $Z_1 \leq 2Z/p$ and $p \leq Z^{1/r}$. Thus we have

$$\begin{aligned} J_1' \leq p^{2k-2r}(2Z)^r(r!)2^{r(r+1)}Z^{(r-1)/2}J_{k-r,r}(Z_1) &\leq Z^{2k/r-2}(2Z)^r(r!)2^{r(r+1)}Z^{(r-1)/2}J_{k-r,r}(Z_1) \\ &\leq 2^{r(r+1)+r}(r!)Z^{2k/r+(3r-5)/2}J_{k-r,r}(Z_1) \\ &\leq 2^{2r(r+1)}Z^{2k/r+(3r-5)/2}J_{k-r,r}(Z_1) \\ &\leq 2^{2k}Z^{2k/r+(3r-5)/2}J_{k-r,r}(Z_1), \end{aligned}$$

where the final inequalities used the facts that $r! \leq r^r \leq 2^{r^2}$ and $k \geq r(r+1)$.

It still remains to prove the claim that $J_1' \leq p^{2k-2r} \max_{1\leq x\leq p} J_1'(x)$, which helpfully allowed us to "freeze" the residue class of most of our variables. To show this, for any $1 \leq x \leq p$ write $\sum^{(x)}$ as shorthand for $\sum_{z\leq pZ_1,\ z\equiv x \bmod p}$, and in particular define

$$S(x) := \sum^{(x)} e(\beta_1 z + \beta_2 z^2 + ... + \beta_r z^r) = \sum_{z\leq pZ_1,\ z\equiv x \bmod p} e(\beta_1 z + \beta_2 z^2 + ... + \beta_r z^r).$$

Also let $\mathbf{1}$ denote the indicator function, which takes value 1 if the attached statement is true, and takes value 0 otherwise. Then by definition we have

$$J_1' = \sum_{\substack{x_1,...,x_r \\ \text{distinct mod } p}} \sum^{(x_1)} \sum^{(x_2)} ... \sum^{(x_r)} \sum_{\substack{x_{k+1},...,x_{k+r} \\ \text{distinct mod } p}} \sum^{(x_{k+1})} ... \sum^{(x_{k+r})} \sum_{\substack{x_{r+1},...,x_k \\ \text{mod } p}} \sum^{(x_{r+1})} ... \sum^{(x_k)}$$
$$\sum_{\substack{x_{k+r+1},...,x_{2k} \\ \text{mod } p}} \sum^{(x_{k+r+1})} ... \sum^{(x_{2k})} \prod_{j=1}^{r} \mathbf{1}_{\sum_{i=1}^k x_i^j - \sum_{i=k+1}^{2k} x_i^j = 0}.$$

Note carefully that the first two big sums are over all residue classes $(x_1, ..., x_r)$ and $(x_{k+1}, ..., x_{k+r})$ that are *distinct* modulo p, whilst the other two big sums are just over all residue classes modulo p (without the condition that they be distinct).

If w is an integer, then direct calculation (and remembering that $e(\beta w)$ denotes $e^{2\pi i \beta w}$) shows that $\int_0^1 e(\beta w) d\beta$ is 1 if $w = 0$, and is zero otherwise. Using this fact we can rewrite the above in terms of exponential sums, as

$$J_1' = \sum_{\substack{x_1,...,x_r \\ \text{distinct mod } p}} \sum_{\substack{x_{k+1},...,x_{k+r} \\ \text{distinct mod } p}} \sum_{\substack{x_{r+1},...,x_k \\ \text{mod } p}} \sum_{\substack{x_{k+r+1},...,x_{2k} \\ \text{mod } p}} \int_0^1 ... \int_0^1 S(x_1)...S(x_k)\overline{S(x_{k+1})...S(x_{2k})} d\beta_1...d\beta_r$$
$$= \int_0^1 ... \int_0^1 \left| \sum_{\substack{x_1,...,x_r \\ \text{distinct mod } p}} S(x_1)...S(x_r) \right|^2 \left| \sum_{x \text{ mod } p} S(x) \right|^{2k-2r} d\beta_1...d\beta_r.$$

Finally, Hölder's inequality applied to $\left|\sum_{x \text{ mod } p} S(x)\right|^{2k-2r}$ yields that

$$J_1' \leq \int_0^1 ... \int_0^1 \left| \sum_{\substack{x_1,...,x_r \\ \text{distinct mod } p}} S(x_1)...S(x_r) \right|^2 p^{2k-2r-1} \sum_{1 \leq x \leq p} |S(x)|^{2k-2r} \, d\beta_1...d\beta_r$$
$$= p^{2k-2r-1} \sum_{1 \leq x \leq p} \int_0^1 ... \int_0^1 \left| \sum_{\substack{x_1,...,x_r \\ \text{distinct mod } p}} S(x_1)...S(x_r) \right|^2 |S(x)|^{2k-2r} \, d\beta_1...d\beta_r,$$

which is clearly $\leq p^{2k-2r} \max_{1 \leq x \leq p} \int_0^1 ... \int_0^1 \left| \sum_{\substack{x_1,...,x_r \\ \text{distinct mod } p}} S(x_1)...S(x_r) \right|^2 |S(x)|^{2k-2r} \, d\beta_1...d\beta_r$
By expanding the multiple integral in terms of the indicator function $\mathbf{1}$ again, we see it exactly equals $J_1'(x)$, as claimed.

Bounding J_2. Recall that J_2 counts all those vectors $(x_1, ..., x_k, x_{k+1}, ..., x_{2k})$, counted by $J_{k,r}(pZ_1)$, in which *either* $(x_1, ..., x_k)$ *or* $(x_{k+1}, ..., x_{2k})$ does *not* contain at least r numbers that are distinct modulo p. In the first case there are at most $p^{r-1}r^k$ possibilities for $(x_1 \pmod p, ..., x_k \pmod p)$, so there are at most $p^{r-1+k}r^k$ possibilities for

$(x_1 \pmod p), ..., x_k \pmod p, x_{k+1} \pmod p, ..., x_{2k} \pmod p)$. Similarly, in the second case there are at most $p^{r-1}r^k$ possibilities for $(x_{k+1} \pmod p, ..., x_{2k} \pmod p)$, so there are at most $p^{r-1+k}r^k$ possibilities for $(x_1 \pmod p), ..., x_k \pmod p, x_{k+1} \pmod p), ..., x_{2k} \pmod p)$. Let $\mathcal{A}$ denote the set of all possibilities for $(x_1 \pmod p), ..., x_k \pmod p, x_{k+1} \pmod p), ..., x_{2k} \pmod p)$ that are allowed in J_2, so that $\#\mathcal{A} \le 2p^{r-1+k}r^k$.

Now similarly as above, using Hölder's inequality we have

$$\begin{aligned}
J_2 &= \int_0^1 ... \int_0^1 \sum_{\substack{x_1,...,x_{2k} \bmod p, \\ (x_1 \pmod p),...,x_{2k} \pmod p))\in\mathcal{A}}} S(x_1)...S(x_k)\overline{S(x_{k+1})...S(x_{2k})}d\beta_1...d\beta_r \\
&\le \int_0^1 ... \int_0^1 \left(\sum_{\substack{x_1,...,x_{2k} \bmod p, \\ (x_1,...,x_{2k} \pmod p))\in\mathcal{A}}} |S(x_1)|^{2k} \right)^{1/2k} ... \left(\sum_{\substack{x_1,...,x_{2k} \bmod p, \\ (x_1,...,x_{2k} \pmod p))\in\mathcal{A}}} |S(x_{2k})|^{2k} \right)^{1/2k} d\beta_1...d\beta_r \\
&\le (\#\mathcal{A}) \int_0^1 ... \int_0^1 \sum_{x \bmod p} |S(x)|^{2k} d\beta_1...d\beta_r \\
&\le 2p^{r+k}r^k \max_{1\le x\le p} \int_0^1 ... \int_0^1 |S(x)|^{2k} d\beta_1...d\beta_r.
\end{aligned}$$

And for any $1 \le x \le p$, if we expand the multiple integral in terms of the indicator function $\mathbf{1}$ again we see it counts all those vectors $(x_1, ..., x_k, x_{k+1}, ..., x_{2k})$, counted by $J_{k,r}(pZ_1)$, in which all of the components are $\equiv x$ modulo p. So using translation invariance (Lemma 9.5) again to subtract x from all the components, and then dividing all the translated components by their common factor p (which reduces the range of the new variables to Z_1), we find

$$J_2 \le 2p^{r+k}r^k J_{k,r}(Z_1).$$

Finally, we rework this bound into a form more like our bound for J_1', by noting that we trivially have $J_{k,r}(Z_1) \le Z_1^{2r} J_{k-r,r}(Z_1)$ (since for any fixed $(x_1, ..., x_r)$ and $(x_{k+1}, ..., x_{k+r})$, the number of choices of the other $2(k-r)$ variables that satisfy the underlying equations is $\le J_{k-r,r}(Z_1)$). So, remembering again that $Z_1 \le 2Z/p$ and $p \le Z^{1/r}$, we have

$$\begin{aligned}
J_2 \le \left(2p^{r+k}r^k Z_1^{2r}\right) J_{k-r,r}(Z_1) &= \left(2p^{k-r}r^k (pZ_1)^{2r}\right) J_{k-r,r}(Z_1) \\
&\le \left(2Z^{k/r-1}r^k (2Z)^{2r}\right) J_{k-r,r}(Z_1) \\
&\le \left(2^{2r+1}r^k Z^{2k/r+(3r-5)/2} Z^{-(k/r)+(r+3)/2}\right) J_{k-r,r}(Z_1).
\end{aligned}$$

Since we assume that $k \ge r^2+r$ and $Z \ge (2r)^{3r}$, one can check (by separately considering the cases where $2 \le r \le 8$ and $r \ge 9$, say) that the right hand side is

$$\le 2^{2r+1}8^k Z^{2k/r+(3r-5)/2} J_{k-r,r}(Z_1).$$

Putting everything together. In summary, we have

$$J_{k,r}(pZ_1) \leq k^{2r} J_1' + J_2 \leq \left(k^{2r} 2^{2k} + 2^{2r+1} 8^k\right) Z^{2k/r+(3r-5)/2} J_{k-r,r}(Z_1) \leq 16^k Z^{2k/r+(3r-5)/2} J_{k-r,r}(Z_1),$$

as claimed, since $k \geq r^2 + r$ (with $r \geq 2$). □

Now that we have proved Lemma 9.6, it is a fairly straightforward bookkeeping exercise to complete the proof of Vinogradov's Mean Value Theorem (Theorem 9.2).

Proof of Theorem 9.2. [[The details of this proof are not examinable, although it is not difficult.]]

If $r = 1$ then we obviously have $J_{k,1}(Z) \leq Z^{2k-1}$ (for any $Z \geq 1$), since fixing $(x_1, ..., x_{2k-1})$ leaves at most one possible choice of x_{2k}. This suffices to prove Theorem 9.2 when $r = 1$, so from now on we assume that $r \geq 2$.

We fix $r \geq 2$ and proceed by induction on $k \geq r^2$ (or, more accurately, on the parameter F in the statement of the theorem).

- If $r^2 \leq k \leq r^2 + r - 1$ then $F(k,r) = \lfloor 1 - 1/r \rfloor = 0$ and $\delta(k,r) = (1-1/r)^F = 1$, so the bound we need to prove is

  $$J_{k,r}(Z) \leq Z^{2k}.$$

  But this is (worse than) trivial (for any $Z \geq 1$), so we are done in this base case.
- For the inductive step, suppose that $r^2 + fr \leq k \leq r^2 + (f+1)r - 1$ for some integer $f \geq 1$, and suppose that we have already proved the theorem whenever $k \leq r^2 + fr - 1$.

  If $Z < (2r)^{3r}$ then we cannot apply Lemma 9.6, so we are forced to take a trivial approach by noting that

  $$J_{k,r}(Z) \leq Z^{2r} J_{k-r,r}(Z).$$

  Then $r^2 + (f-1)r \leq k - r \leq r^2 + fr - 1$, so by the inductive hypothesis we have

$$J_{k-r,r}(Z) \leq (4r)^{4(k-r)(f-1)} Z^{2(k-r)-(1-\delta')(1/2)r(r+1)}, \qquad \text{where } \delta' = (1-1/r)^{f-1}.$$

  So overall, if we write $\delta = (1-1/r)^f$ we have

$$\begin{aligned} J_{k,r}(Z) &\leq (4r)^{4(k-r)(f-1)} Z^{2k-(1-\delta')(1/2)r(r+1)} \\ &= (4r)^{4kf} Z^{2k-(1-\delta)(1/2)r(r+1)} (4r)^{-4k-4r(f-1)} Z^{(\delta'-\delta)(1/2)r(r+1)} \\ &= (4r)^{4kf} Z^{2k-(1-\delta)(1/2)r(r+1)} (4r)^{-4k-4r(f-1)} Z^{\delta'(1/2)(r+1)} \\ &< (4r)^{4kf} Z^{2k-(1-\delta)(1/2)r(r+1)} (4r)^{-4k-4r(f-1)} (2r)^{\delta'(3/2)r(r+1)}. \end{aligned}$$

And $\delta'(3/2)r(r+1) \le (3/2)r(r+1) < 4r(r+1) \le 4k$, so the product of the last two terms above is < 1 and we certainly have

$$J_{k,r}(Z) \le (4r)^{4kf} Z^{2k-(1-\delta)(1/2)r(r+1)},$$

which is the bound claimed in the theorem.

It remains to handle the case where $Z \ge (2r)^{3r}$, for which we can apply Lemma 9.6 to obtain that

$$J_{k,r}(Z) \le 4^{2k} Z^{2k/r+(3r-5)/2} J_{k-r,r}(4Z^{(r-1)/r}).$$

Then by the inductive hypothesis we have

$$J_{k-r,r}(4Z^{(r-1)/r}) \le (4r)^{4(k-r)(f-1)} \left(4Z^{(r-1)/r}\right)^{2(k-r)-(1-\delta')(1/2)r(r+1)}, \qquad \text{where } \delta' = (1-1/r)^{f-1}.$$

Noting that, if we write $\delta = (1-1/r)^f$, we have

$$\begin{aligned} \left(Z^{(r-1)/r}\right)^{2(k-r)-(1-\delta')(1/2)r(r+1)} &= Z^{2k-(1-1/r)(1-\delta')(1/2)r(r+1)} Z^{-2k/r-2(r-1)} \\ &= Z^{2k-(1-\delta)(1/2)r(r+1)} Z^{-2k/r-2(r-1)+(1/2)(r+1)} \\ &= Z^{2k-(1-\delta)(1/2)r(r+1)} Z^{-2k/r-(1/2)(3r-5)}, \end{aligned}$$

we find overall that

$$J_{k,r}(Z) \le 4^{2k}(4r)^{4(k-r)(f-1)} 4^{2(k-r)-(1-\delta')(1/2)r(r+1)} Z^{2k-(1-\delta)(1/2)r(r+1)} \le (4r)^{4kf} Z^{2k-(1-\delta)(1/2)r(r+1)}.$$

This is the bound claimed in the theorem.

□

10. Second thoughts on estimating zeta sums

Recall that our goal in this chapter is to estimate zeta sums $\sum_{N<n\le N+M} n^{-it}$, and use the estimates to obtain an improved zero-free region and an improved error term in the Prime Number Theorem. We have now assembled three powerful ingredients for doing this:

(i) Lemma 7.1, which reduced the estimation of zeta sums to the estimation of certain double exponential sums

$$U(n) := \sum_{x\le N^{2/5}} \sum_{y\le N^{2/5}} e(\alpha_1 xy + \alpha_2 x^2y^2 + ... + \alpha_r x^r y^r), \qquad \alpha_j := \frac{(-1)^j t}{2\pi j n^j};$$

(ii) Lemma 8.3, which used Hölder's inequality to reduce the estimation of $U(n)$ to the estimation of Vinogradov's Mean Value $J_{k,r}(N^{2/5})$ (together with certain other easy sums over μ_j);

(iii) Vinogradov's Mean Value Theorem (Theorem 9.2), which gives a good bound for $J_{k,r}(N^{2/5})$ provided k is large enough in terms of r.

We can combine these ingredients to obtain the following estimate.

Theorem 10.1 (Zeta sum estimate, Vinogradov, Korobov, 1958)**.** *There exists a small absolute constant $c > 0$ such that the following is true. For any $1 \le M \le N \le t$,*

$$\left| \sum_{N < n \le N+M} n^{-it} \right| \ll M e^{-c(\log^3 N)/\log^2(t+2)} + N^{4/5}.$$

Proof of Theorem 10.1. We may assume that t is large and that $N \ge e^{\log^{2/3} t}$, since otherwise the theorem is trivial by adjusting the $\ll$ constant appropriately.

By Lemma 7.1 we have

$$\left| \sum_{N < n \le N+M} n^{-it} \right| \ll M \max_{N \le n \le 2N} \frac{|U(n)|}{N^{4/5}} + N^{4/5} + M t^{-1/500},$$

where

$$U(n) = \sum_{x \le N^{2/5}} \sum_{y \le N^{2/5}} e(\alpha_1 xy + \alpha_2 x^2 y^2 + ... + \alpha_r x^r y^r), \qquad \alpha_j = \frac{(-1)^j t}{2\pi j n^j},$$

and $r = \lfloor \frac{5.01 \log t}{\log N} \rfloor$. Since $t \ge N$ we have $t^{-1/500} = e^{-(1/500)\log t} \le e^{-(1/500)(\log^3 N)/\log^2 t}$, so the last two terms are certainly small enough.

By Lemma 8.3, for any $N \le n \le 2N$ and any $k \in \mathbb{N}$ we have

$$\frac{|U(n)|}{N^{4/5}} \le \left(\frac{1}{N^{8k/5}} \left(J_{k,r}(N^{2/5}) \right)^2 \prod_{j=1}^{r} \sum_{-kN^{2j/5} \le \mu_j \le kN^{2j/5}} \min\{3kN^{2j/5}, \frac{1}{||\alpha_j \mu_j||}\} \right)^{1/(4k^2)}.$$

We take $k = Cr^2$, where $C \ge 1$ is a constant that we will choose later. (We will make sure to choose it such that $k = Cr^2 \in \mathbb{N}$, as required.) Since $k \ge r^2$, Vinogradov's Mean Value Theorem (Theorem 9.2) implies that

$$\left(J_{k,r}(N^{2/5}) \right)^2 \le (4r)^{8kF} N^{4/5(2k - (1-\delta)(1/2)r(r+1))}, \qquad \text{where } F = \lfloor (C-1)r \rfloor, \text{ and } \delta = (1-1/r)^F,$$

and so we see

$$\frac{|U(n)|}{N^{4/5}} \le \left((4r)^{8Ckr} N^{-(4/5)(1-\delta)(1/2)r(r+1)} \prod_{j=1}^{r} \sum_{-kN^{2j/5} \le \mu_j \le kN^{2j/5}} \min\{3kN^{2j/5}, \frac{1}{||\alpha_j \mu_j||}\} \right)^{1/(4k^2)}.$$

It remains to bound the sums over μ_j. We always have the trivial bound $\ll k^2 N^{4j/5}$, and if $\alpha_j = a_j/q_j + \theta_j/q_j^2$ for some $q_j \ge 1$, $(a_j, q_j) = 1$ and $|\theta_j| \le 1$ then by Lemma 8.2

we have

$$\sum_{-kN^{2j/5}\le\mu_j\le kN^{2j/5}} \min\{3kN^{2j/5}, \frac{1}{||\alpha_j\mu_j||}\} \ll \left(\frac{kN^{2j/5}}{q_j}+1\right)(kN^{2j/5}+q_j\log q_j)$$
$$\ll \max\{\frac{k^2N^{4j/5}}{q_j}, q_j\}\log(q_j+1).$$

But if $j \ge (\log t)/\log N$ then, remembering that $N \le n \le 2N$, we have

$$\alpha_j = \frac{(-1)^j t}{2\pi j n^j} = \frac{(-1)^j}{q_j} + \frac{\theta_j}{q_j^2}, \qquad \text{where } q_j := \lfloor 2\pi j n^j/t\rfloor \ge 1 \text{ and } \theta_j = \frac{(-1)^{j+1}\{2\pi j n^j/t\}q_j}{2\pi j n^j/t}.$$

In particular, if $2(\log t)/\log N \le j \le 3(\log t)/\log N$ then $q_j \ge n^{j-(\log t)/\log N} \ge N^{j/2}$ and also $q_j \ll jn^jN^{-j/3} \ll j2^jN^{2j/3}$, so we certainly have

$$\sum_{-kN^{2j/5}\le\mu_j\le kN^{2j/5}} \min\{3kN^{2j/5}, \frac{1}{||\alpha_j\mu_j||}\} \ll \frac{k^2N^{4j/5}}{N^{j/10}} \qquad \text{if } 2(\log t)/\log N \le j \le 3(\log t)/\log N.$$

Putting everything together, we see

$$\frac{|U(n)|}{N^{4/5}} \le \left((4r)^{8Ckr}N^{-(4/5)(1-\delta)(1/2)r(r+1)}\prod_{j=1}^{r}(Dk^2N^{4j/5})\prod_{2(\log t)/\log N\le j\le 3(\log t)/\log N}\frac{1}{N^{j/10}}\right)^{1/(4k^2)}$$
$$\le \left((4r)^{8Ckr}N^{-(4/5)(1-\delta)(1/2)r(r+1)}(Dk^2)^rN^{(4/5)(1/2)r(r+1)}N^{-(1/10)((\log t)/\log N)^2}\right)^{1/(4k^2)},$$

where D is a large absolute constant. Remember that $k = Cr^2$ and $r = \lfloor \frac{5.01\log t}{\log N}\rfloor$ here. If we choose C large enough then we will have $\delta \le 1/280$, and therefore $(4/5)\delta(1/2)r(r+1) \le 14\delta((\log t)/\log N)^2 \le (1/20)((\log t)/\log N)^2$, and therefore

$$\frac{|U(n)|}{N^{4/5}} \le \left((4r)^{8Ckr}(Dk^2)^rN^{-(1/20)((\log t)/\log N)^2}\right)^{\frac{1}{4k^2}} = \left((4r)^{8C^2r^3}(DC^2r^4)^rN^{-(1/20)(\log t/\log N)^2}\right)^{1/(4C^2r^4)}.$$

The dominant term inside the bracket is $N^{-(1/20)(\log t/\log N)^2}$, and so the conclusion of the theorem follows. □

If $M = N = t^\theta$, for some $0 < \theta \le 1$, then the bound in Theorem 10.1 takes the form

$$\left|\sum_{N<n\le 2N} n^{-it}\right| \ll Ne^{-c\theta^2\log N} = N^{1-c\theta^2}.$$

Thus we have a *power saving* if N is any fixed power of t. In general we think of a power saving as a very good result, and a squareroot-type bound $\left|\sum_{N<n\le 2N} n^{-it}\right| \ll N^{1/2+o(1)}$ would be the very best we might hope to prove (since it would mean that the summands n^{-it} oscillate "like random"). If N is smaller than any fixed power of t, but larger than $e^{C\log^{2/3}t}$ (which is a wide range), then Theorem 10.1 does not give a power saving but still gives a non-trivial bound.

11. Some spectacular (?) consequences

Using our zeta sum estimate (Theorem 10.1) we can deduce the promised upper bound for the size of the zeta function.

Theorem 11.1 (Richert, 1967, building on work of Vinogradov and Korobov)**.** *There exists a large absolute constant $C > 0$ such that the following is true. For any large t and any $0 < \sigma \leq 1$, we have*

$$\zeta(\sigma + it) \ll t^{C(1-\sigma)^{3/2}} \log^{2/3} t.$$

In particular, if $\sigma \geq 1 - 1/\log^{2/3} t$ then $\zeta(\sigma + it) \ll \log^{2/3} t$.

Note that by the Hardy–Littlewood approximation for the zeta function (Theorem 3.3) we have

$$\zeta(\sigma + it) = \sum_{n \leq t} \frac{1}{n^{\sigma+it}} + O(1).$$

The trivial bound for the sum is $\sum_{n \leq t} \frac{1}{n^\sigma} \ll t^{1-\sigma}/(1-\sigma)$, which is good enough if σ is far from 1 but is much weaker than Theorem 11.1 if $1 - \sigma$ is small. In that case we can estimate a large part of the sum better using Theorem 10.1.

Proof of Theorem 11.1. Suppose first that $1 - 1/\log^{2/3} t \leq \sigma \leq 1$. Then

$$\begin{aligned} \zeta(\sigma + it) = \sum_{n \leq e^{\log^{2/3} t}} \frac{1}{n^{\sigma+it}} + \sum_{e^{\log^{2/3} t} < n \leq t} \frac{1}{n^{\sigma+it}} + O(1) &\ll \sum_{n \leq e^{\log^{2/3} t}} \frac{1}{n} + \sum_{\lfloor \log^{2/3} t \rfloor \leq j \leq \log t} \left| \sum_{e^j < n \leq e^{j+1}} \frac{1}{n^{\sigma+it}} \right| \\ &\ll \log^{2/3} t + \sum_{\lfloor \log^{2/3} t \rfloor \leq j \leq \log t} \left| \sum_{e^j < n \leq e^{j+1}} \frac{1}{n^{\sigma+it}} \right|, \end{aligned}$$

and because the sequence $\frac{1}{n^\sigma}$ is monotone decreasing, Abel's summation lemma (as seen in the proof of Lemma 3.4) implies that

$$\left| \sum_{e^j < n \leq e^{j+1}} \frac{1}{n^{\sigma+it}} \right| \ll \frac{1}{e^{j\sigma}} \max_{e^j < n' \leq e^{j+1}} \left| \sum_{e^j < n \leq n'} n^{-it} \right|.$$

But by Theorem 10.1 we have

$$\max_{e^j < n' \leq e^{j+1}} \left| \sum_{e^j < n \leq n'} n^{-it} \right| \ll e^j e^{-cj^3/\log^2 t},$$

so we have

$$\begin{aligned}\zeta(\sigma+it) &\ll \log^{2/3} t + \sum_{\lfloor \log^{2/3} t\rfloor \le j \le \log t} e^{j(1-\sigma)-cj^3/\log^2 t} \\ &\ll \log^{2/3} t + \sum_{\lfloor \log^{2/3} t\rfloor \le j \le \log t} e^{j/\log^{2/3} t - c(j/\log^{2/3} t)^3} \\ &\ll \log^{2/3} t + \sum_{r=1}^{\lfloor \log^{1/3} t\rfloor} \sum_{r\lfloor \log^{2/3} t\rfloor \le j \le (r+1)\lfloor \log^{2/3} t\rfloor} e^{j/\log^{2/3} t - c(j/\log^{2/3} t)^3}\end{aligned}$$

The final sums here are $\ll (\log^{2/3} t)\sum_r e^{r-cr^3}$, and this is clearly $\ll \log^{2/3} t$ as required.

If instead $\sigma < 1 - 1/\log^{2/3} t$ then one can proceed in a similar way, but breaking the sum over n at a different place to obtain a saving when summing over j. In fact, for any large constant C we obtain that

$$\begin{aligned}\zeta(\sigma+it) &= \sum_{n\le e^{C\log t\sqrt{1-\sigma}}} \frac{1}{n^{\sigma+it}} + \sum_{e^{C\log t\sqrt{1-\sigma}} < n \le t} \frac{1}{n^{\sigma+it}} + O(1) \\ &\ll \frac{e^{C\log t(1-\sigma)^{3/2}}}{1-\sigma} + \sum_{\lfloor C\log t\sqrt{1-\sigma}\rfloor \le j \le \log t} \left| \sum_{e^j < n \le e^{j+1}} \frac{1}{n^{\sigma+it}} \right| \\ &\ll t^{C(1-\sigma)^{3/2}} \log^{2/3} t + \sum_{\lfloor C\log t\sqrt{1-\sigma}\rfloor \le j \le \log t} e^{j(1-\sigma)-cj^3/\log^2 t} \\ &\ll t^{C(1-\sigma)^{3/2}} \log^{2/3} t + \sum_{\lfloor C\log t\sqrt{1-\sigma}\rfloor \le j \le \log t} e^{j(1-\sigma)-cj(1-\sigma)C^2}.\end{aligned}$$

Provided C is large enough the exponents in the sum over j will all be negative, and one can bound it as we did above by breaking into intervals of length $\lfloor C\log t\sqrt{1-\sigma}\rfloor$. □

Remark 11.2. It is easy to check that the first part of the above proof also shows that $\zeta(\sigma+it) \ll \log^{2/3} t$ if t is large and $\sigma > 1$.

Finally, by combining Theorem 11.1 with Landau's theorem (Theorem 5.1) we obtain the best (i.e. widest) zero-free region known for the zeta function.

Corollary 11.3 (Vinogradov–Korobov zero-free region)**.** *There exists a small absolute constant $c > 0$ such that the zeta function has no zeros $s = \sigma + it$ in the region $\{s : \sigma \ge 1 - c/(\log^{2/3}(|t|+2)(\log\log(|t|+3))^{1/3})\}$.*

Proof of Corollary 11.3. Theorem 11.1 tells us that, for all $t \ge t_0$ (a large constant), we have

$$\zeta(\sigma+it) \ll t^{C(1-\sigma)^{3/2}} \log^{2/3} t = e^{C(1-\sigma)^{3/2}\log t + (2/3)\log\log t}.$$

In particular, if $\sigma \ge 1 - ((\log\log t)/\log t)^{2/3}$ then we have $\zeta(\sigma+it) \ll e^{(C+2/3)\log\log t}$, so we can apply Landau's theorem (Theorem 5.1) with the choices $\phi(t) = (C+2/3)\log\log t$

and $w(t) = ((\log t)/\log\log t)^{2/3}$, obtaining that $\zeta(\sigma + it) \neq 0$ in the region

$$\sigma \geq 1 - \frac{c}{\phi(2t+1)w(2t+1)} = 1 - \frac{c}{(C+2/3)\log^{2/3}(2t+1)(\log\log(2t+1))^{1/3}}, \qquad t \geq t_0.$$

By relabelling the constants, this gives the assertion of the corollary when $t \geq t_0$.

One can obtain the analogous result for $t < t_0$ using the known zero-free regions and using symmetry, exactly as in the proof of Corollary 5.2. □

By repeating the proof of the prime number theorem with the line of integration shifted into the Vinogradov–Korobov zero-free region, rather than the classical zero-free region, (and obtaining a bound for $\zeta'(s)/\zeta(s)$ in that region as in Lemma 5.5), we obtain the best known error term for the distribution of primes.

Corollary 11.4 (Prime Number Theorem with Vinogradov–Korobov error term)**.** *For all $x \geq 2$ we have*

$$\Psi(x) = x + O(xe^{-c(\log^{3/5} x)/(\log\log x)^{1/5}}).$$

Proof of Corollary 11.4. The details of the proof are omitted and non-examinable, but the idea of the argument is exactly as we have seen before [[and is examinable]].

At the end we obtain an estimate of the form

$$\Psi(x) = x + O(x\log^2 x\left(e^{-c(\log x)/(\log^{2/3}(T+2)(\log\log(T+3))^{1/3})} + e^{-\log T}\right)),$$

and choosing $T = \exp\{(\log^{3/5} x)/(\log\log x)^{1/5}\}$ is optimal and gives the claimed result. □

Remark 11.5. In our first proof of the Prime Number Theorem we obtained an error term of the form $O(xe^{-c\log^{1/10} x})$. After a great deal of hard work (which took more than sixty years to complete in real time), this was improved to the Vinogradov–Korobov error term $O(xe^{-c(\log^{3/5} x)/(\log\log x)^{1/5}})$. This error term is certainly much smaller, but it looks to be of the same "shape", and one might reasonably ask what more it really tells us about the distribution of primes.

(i) There are problems in which the exact size of the error term is of qualitative importance. For example, if one could obtain a zero-free region of the form $\sigma \geq 1 - c/\sqrt{\log(|t|+2)}$, which corresponds to an error term $O(xe^{-c\log^{2/3} x})$ in the prime number theorem, this would have applications to the distribution of numbers with only small prime factors (*smooth numbers*).

(ii) We know that the Vinogradov–Korobov error term is not just a technical sharpening of the classical error term, because we know that many new ideas were

required to prove it! In particular, the Vinogradov–Korobov error term encodes the zeta sum estimate in Theorem 10.1, which is a fundamental number-theoretic fact about the Fourier analytic properties of the integers (and which we translated, via the zeta function, into information about primes).

(iii) But it is true that the error term $O(xe^{-c(\log^{3/5} x)/(\log\log x)^{1/5}})$ is nowhere close to what we believe should be true. The *Riemann Hypothesis* conjectures that apart from the trivial zeros at $s = -2, -4, -6, ...$, all the zeros of the zeta function lie on the critical line $\{\Re(s) = 1/2\}$. If this is true then one obtains a squareroot power-saving error term $O(\sqrt{x}\log^2 x)$ in the Prime Number Theorem.

The Riemann Hypothesis is, arguably, the most important unsolved problem in mathematics, since it would imply that the error term in the distribution of primes is "like random". If one could obtain an improved zeta sum estimate (i.e. a power saving on a wider range of N than in Theorem 10.1) this would help to widen the known zero-free region, but at present we have *no plausible approach* to obtaining a zero-free region out to the 1/2-line, as in the Riemann Hypothesis.

References

[1] A. Ivić. *The Riemann zeta-function: theory and applications.* Dover edition, published by Dover Publications, Inc.. 2003

[2] E. C. Titchmarsh. *The Theory of the Riemann Zeta-function.* Second edition, revised by D. R. Heath-Brown, published by Oxford University Press. 1986

[3] T. D. Wooley. Vinogradov's mean value theorem via efficient congruencing. *Ann. of Math.*, **175**, no. 3, pp 1575-1627. 2012

[4] T. D. Wooley. Vinogradov's mean value theorem via efficient congruencing, II. *Duke Math. J.*, **162**, no. 4, pp 673-730. 2013

Jesus College, Cambridge, CB5 8BL
E-mail address: A.J.Harper@dpmms.cam.ac.uk