Analytic Number Theory
Lecture 12

Mariusz Mirek
Rutgers University

Padova, April 15, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

Waring problem

Definition

Given $k \in \mathbb{Z}_+$, define $G(k)$ to be the least integer having the property that whenever $s \geqslant G(k)$, then all sufficiently large natural numbers are the sum of s positive integer k-th powers.

- Thus, when $k \in \mathbb{Z}_+$ and $s \geqslant G(k)$, there exists $N_0 = N_0(s, k)$ such that, whenever $n \geqslant N_0$, then there exist $x_1, \ldots, x_s \in \mathbb{Z}_+$ such that
$$n = x_1^k + \ldots + x_s^k.$$
- A relatively easy exercise shows that $G(k) \geqslant k + 1$ whenever $k \geqslant 2$.

The current state of the art for $k \in [9]$

- $G(2) = 4$, a consequence of Lagrange's theorem from 1770;
- $G(3) \leqslant 7$, due to Linnik, 1942;
- $G(4) = 16$, due to Davenport, 1939;
- $G(5) \leqslant 17$, due to Vaughan and Wooley, 1995;
- $G(6) \leqslant 24$, due to Vaughan and Wooley, 1994;
- $G(7) \leqslant 31$, due to Wooley, 2016;
- $G(8) \leqslant 39$, due to Wooley, 2016 (and it is known that $G(8) \geqslant 32$);
- $G(9) \leqslant 47$, due to Wooley, 2016;

The current state of the art for large powers

- In general, for large values of k, it was shown 30 years ago that

$$G(k) \leqslant k(\log k + \log\log k + 2 + o(1)) \quad \text{(Wooley, 1992 and 1995)},$$

where $o(1) \to 0$ as $k \to \infty$.
- Within the past year, this longstanding upper bound has been improved so that for all natural numbers k one has

$$G(k) \leqslant \lceil k(\log k + 4.20032) \rceil \quad \text{(Brüdern and Wooley 2022)}.$$

- Let us now return to Hardy and Littlewood in 1920, and indeed to Hardy and Ramanujan in 1918. They considered a power series

$$g_k(z) = \sum_{m=1}^{\infty} z^{m^k}$$

- Note that this series is absolutely convergent for $|z| < 1$. If one now considers the expression $g_k(z)^s$, one sees that

$$g_k(z)^s = \left(\sum_{m_1=1}^{\infty} z^{m_1^k} \right) \left(\sum_{m_2=1}^{\infty} z^{m_2^k} \right) \cdots \left(\sum_{m_s=1}^{\infty} z^{m_s^k} \right) = \sum_{m_1=1}^{\infty} \cdots \sum_{m_s=1}^{\infty} z^{m_1^k + \ldots + m_s^k}$$

Hardy–Littlewood–Ramanujan method

- Then we can further write

$$g_k(z)^s = \left(\sum_{m_1=1}^{\infty} z^{m_1^k}\right)\left(\sum_{m_2=1}^{\infty} z^{m_2^k}\right)\cdots\left(\sum_{m_s=1}^{\infty} z^{m_s^k}\right)$$
$$= \sum_{m_1=1}^{\infty}\cdots\sum_{m_s=1}^{\infty} z^{m_1^k+\ldots+m_s^k} = \sum_{n=1}^{\infty} R_{s,k}(n) z^n,$$

where $R_{s,k}(n) = \#\left\{(m_1,\ldots,m_s) \in \mathbb{Z}_+^s : m_1^k + \ldots + m_s^k = n\right\}$.
- We can recover the coefficients $R_{s,k}(n)$ by employing Cauchy's integral formula to evaluate a suitable contour integral. Thus

$$R_{s,k}(n) = \frac{1}{2\pi i}\int_{\mathcal{C}} g_k(z)^s z^{-n-1}\,\mathrm{d}z$$

where $\mathcal{C}$ denotes a circular contour, centered at 0 with radius $r \in (0,1)$.
- When $k = 1$, the series in question is $g_1(z) = z/(1-z)$, and Hardy and Ramanujan obtained an asymptotic formula for $R_{s,k}(n)$ by evaluating their generating functions asymptotically for all values of θ.
- The method also applies even in the more delicate situation with $k = 2$. However, when $k \geqslant 3$, the situation is much more involved and here the innovative circle method of Hardy and Littlewood becomes essential.

Vinogradov's approach

- The basis of this method is the elementary orthogonality identity

$$\int_0^1 e(k\theta)d\theta = \int_0^1 e^{2\pi ik\theta}d\theta = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{if } k \neq 0. \end{cases}$$

- Fix $n \in \mathbb{Z}_+$ and let $X = n^{1/k}$. Using this identity, in a similar way as in the Vinogradov's mean value theorem we have

$$\begin{aligned} R_{s,k}(n) &= \# \left\{ (m_1, \ldots, m_s) \in \mathbb{Z}_+^s : m_1^k + \ldots + m_s^k = n \right\} \\ &= \sum_{(m_1,\ldots,m_s)\in\mathbb{Z}_+^s} \int_0^1 e\big((m_1^k + \ldots + m_s^k - n)\alpha\big)d\alpha \\ &= \int_0^1 \Big(\sum_{1\leq x\leq X} e(\alpha x^k) \Big)^s e(-n\alpha)d\alpha \end{aligned}$$

- Define

$$f(\alpha) = \sum_{1\leq x\leq X} e(\alpha x^k).$$

Major and minor arcs decomposition

- Whenever $s \geq 2^k + 1$, our goal is to asymptotically evaluate the number

$$R_{s,k}(n) = \int_0^1 f(\alpha)^s e(-n\alpha) \mathrm{d}\alpha$$

- We divide the interval of integration according to a Hardy–Littlewood dissection with major arcs $\mathfrak{M}_\delta$ equal to the union of the intervals

$$\mathfrak{M}_\delta(q,a) = \left\{ \alpha \in [0,1) : |\alpha - a/q| \leqslant X^{\delta-k} \right\}$$

with $0 \leqslant a < q \leqslant X^\delta$ and $(a,q) = 1$, and with minor arcs

$$\mathfrak{m}_\delta = [0,1] \backslash \mathfrak{M}_\delta .$$

- Subject to the condition $0 < \delta < 1/5$, the major arcs $\mathfrak{M}_\delta$ defined in this way are a disjoint union of the arcs $\mathfrak{M}_\delta(q,a)$.
- Indeed, if some real number α lies in two distinct major arcs $\mathfrak{M}_\delta\,(q_1,a_1)$ and $\mathfrak{M}_\delta\,(q_2,a_2)$ lying in $\mathfrak{M}_\delta$, then by the triangle inequality, one has

$$\frac{1}{q_1q_2} \leqslant \left| \frac{a_1q_2 - a_2q_1}{q_1q_2} \right| \leqslant \left| \frac{a_1}{q_1} - \frac{a_2}{q_2} \right| \leqslant \left| \alpha - \frac{a_1}{q_1} \right| + \left| \alpha - \frac{a_2}{q_2} \right| \leqslant 2X^{\delta-k}.$$

Thus, one finds that $1 \leqslant 2q_1q_2X^{\delta-k} \leqslant 2X^{3\delta-k}$. This is plainly impossible when $\delta < 1/3$ and X is large.

Major and minor arcs decomposition

- The exponential sum

$$f(\alpha) = \sum_{1 \leq x \leq X} e(\alpha x^k)$$

can be approximate by the integral on major arcs, whereas on minor arcs one expects that the sequence from the phase is equidistributed due to Weyl's inequality.

- We will write

$$R_{s,k}(n) = \int_{\mathfrak{m}_\delta} f(\alpha)^s e(-n\alpha) \mathrm{d}\alpha + \int_{\mathfrak{M}_\delta} f(\alpha)^s e(-n\alpha) \mathrm{d}\alpha$$

We first handle the integral over minor arcs.

Lemma (Dirichlet's approximation theorem)

Let $\alpha \in \mathbb{R}$, and suppose that $X \geqslant 1$ is a real number. Then there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(a, q) = 1$ and $1 \leqslant q \leqslant X$ such that $|\alpha - a/q| \leqslant 1/(qX)$.

Proof.

Exercise! □

Minor arcs estimates

- Given $\alpha \in [0,1)$, by Dirichlet's approximation theorem, there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $1 \leqslant q \leqslant X^{k-\delta}$, $(a,q)=1$ and
$$|\alpha - a/q| \leqslant 1/\left(qX^{k-\delta}\right) \leqslant \min\{X^{\delta-k}, q^{-2}\}.$$
- If $q \leqslant X^{\delta}$, then we would have $\alpha \in \mathfrak{M}_\delta$. Thus, when $\alpha \in \mathfrak{m}_\delta$, we may suppose that $X^\delta < q \leqslant X^{k-\delta}$. We thus conclude from Weyl's inequality that, whenever $0 < \delta < 1$, one has
$$\begin{aligned} |f(\alpha)| &= O\Big(X^{1+\varepsilon}\left(q^{-1} + X^{-1} + qX^{-k}\right)^{2^{1-k}}\Big) \\ &= O\Big(X^{1+\varepsilon}\left(X^{-\delta} + X^{-1} + X^{k-\delta}/X^{k}\right)^{2^{1-k}}\Big) \\ &= O\big(X^{1-\delta 2^{1-k}+\varepsilon}\big). \end{aligned}$$
- Provided that $s > (k/\delta)2^{k-1}$, we may conclude that
$$\begin{aligned} \left|\int_{\mathfrak{m}_\delta} f(\alpha)^s e(-n\alpha)\mathrm{d}\alpha\right| &\leqslant \Big(\sup_{\alpha\in\mathfrak{m}_\delta} |f(\alpha)|\Big)^s \int_{\mathfrak{m}_\delta} \mathrm{d}\alpha \\ &= O\Big(\big(X^{1-\delta 2^{1-k}+\varepsilon}\big)^s\Big) = o\left(X^{s-k}\right). \end{aligned}$$

Minor arcs estimates

- But our goal is to asymptotically evaluate $R_{s,k}(n)$ assuming that $s \geq 2^k + 1$.

Corollary

When $s \geqslant 2^k + 1$, *one has*

$$\left| \int_{\mathfrak{m}_\delta} f(\alpha)^s e(-n\alpha) \mathrm{d}\alpha \right| = O\big(X^{s-k-\delta 2^{-k}}\big).$$

Proof.

By Weyl's inequality in combination with Hua's lemma, one obtains

$$\begin{aligned}
\left| \int_{\mathfrak{m}_\delta} f(\alpha)^s e(-n\alpha) \mathrm{d}\alpha \right| &\leqslant \left(\sup_{\alpha \in \mathfrak{m}_\delta} |f(\alpha)| \right)^{s-2^k} \int_0^1 |f(\alpha)|^{2^k} \, \mathrm{d}\alpha \\
&= O\left(\left(X^{1-\delta 2^{1-k}+\varepsilon} \right)^{s-2^k} X^{2^k-k+\varepsilon} \right) \\
&= O\Big(X^{s-k-\left(s-2^k\right)\delta 2^{1-k}+s\varepsilon} \Big).
\end{aligned}$$

The conclusion of the corollary follows on recalling that $s \geqslant 2^k + 1$. □

Major arcs estimates

- For $s \geqslant 2^k + 1$ we have shown that

$$\left| \int_{\mathfrak{m}_\delta} f(\alpha)^s e(-n\alpha) \mathrm{d}\alpha \right| = O\left(X^{s-k-\delta 2^{-k}}\right) = o(n^{s/k-1}).$$

- Let $\alpha \in \mathfrak{M}_\delta(q,a) \subseteq \mathfrak{M}_\delta$. Write $\beta = \alpha - a/q$, so that $|\beta| \leqslant X^{\delta - k}$. By breaking the summand into arithmetic progressions modulo q, one has

$$\begin{aligned} \sum_{1 \leqslant x \leqslant X} e\left(\alpha x^k\right) &= \sum_{r=1}^{q} \sum_{(1-r)/q \leqslant y \leqslant (X-r)/q} e\left((\beta + a/q)(yq+r)^k\right) \qquad \text{(A)} \\ &= \sum_{r=1}^{q} e\left(ar^k/q\right) \sum_{(1-r)/q \leqslant y \leqslant (X-r)/q} e\left(\beta(yq+r)^k\right). \end{aligned}$$

- Since β is small, we can hope to approximate the inner sum here by a smooth function with control of the accompanying error terms.
- Here, we apply the mean value theorem to the inner sum.

Major arcs estimates

- By the mean value theorem, when $F(z)$ is a differentiable function on $[a,b]$ with $a < b$, one sees that $F(a) - F(b) = (a-b)F'(\xi)$ for some $\xi \in (a,b)$. Also, trivially, one has

$$e(F(z)) = \int_{-1/2}^{1/2} e(F(z))\mathrm{d}\eta$$

- Hence

$$\left| e(F(z)) - \int_{-1/2}^{1/2} e(F(z+\eta))\mathrm{d}\eta \right| \leqslant \sup_{|\eta|\leqslant 1/2} |e(F(z+\eta)) - e(F(z))|$$
$$= O\Big(\sup_{|\eta|\leqslant 1/2} |F'(z+\eta)| \Big).$$

- Using this approximation, we obtain

$$\sum_{(1-r)/q \leqslant y \leqslant (X-r)/q} e\left(\beta(yq+r)^k\right) - \int_{-r/q}^{(X-r)/q} e\left(\beta(zq+r)^k\right)\mathrm{d}z$$
$$= O\Big(1 + (X/q) \sup_{0\leqslant z\leqslant X/q} \left|k\beta q(qz+r)^{k-1}\right| \Big)$$
$$= O\big(1 + X^k|\beta|\big).$$

Major arcs estimates

- By substituting the last relation into (A), we deduce that

$$f(\alpha) = \sum_{r=1}^{q} e\left(ar^k/q\right)\left(\int_{-r/q}^{(X-r)/q} e\left(\beta(zq+r)^k\right)\mathrm{d}z + O\left(1 + X^k|\beta|\right)\right)$$

so that

$$f(\alpha) - \sum_{r=1}^{q} e\left(ar^k/q\right)\int_{-r/q}^{(X-r)/q} e\left(\beta(zq+r)^k\right)\mathrm{d}z = O\big(q + X^k|q\beta|\big). \quad \text{(B)}$$

- By the change of variable $\gamma = zq + r$, moreover, we have

$$\int_{-r/q}^{(X-r)/q} e\left(\beta(zq+r)^k\right)\mathrm{d}z = q^{-1}\int_{0}^{X} e\left(\beta\gamma^k\right)\mathrm{d}\gamma. \quad \text{(C)}$$

- Introducing, for $a \in \mathbb{Z}$, $q \in \mathbb{Z}_+$ and $\beta \in \mathbb{R}$ the following objects

$$S(q,a) = \sum_{r=1}^{q} e\left(ar^k/q\right), \quad \text{and} \quad v(\beta) = \int_{0}^{X} e\left(\beta\gamma^k\right)\mathrm{d}\gamma,$$

we can summarize our discussion in the form of a lemma.

Major arcs estimates

Lemma

Suppose that $\alpha \in \mathbb{R}$, $a \in \mathbb{Z}$ and $q \in \mathbb{Z}_+$. Then one has

$$|f(\alpha) - q^{-1}S(q,a)v(\alpha - a/q)| = O\big(q + X^k|q\alpha - a|\big).$$

Proof.

The desired conclusion follows by substituting (C) into (B). □

Lemma

When $\alpha \in \mathfrak{M}_\delta(q,a) \subseteq \mathfrak{M}_\delta$, one has

$$|f(\alpha) - q^{-1}S(q,a)v(\alpha - a/q)| = O(X^{2\delta}).$$

Proof.

When $\alpha \in \mathfrak{M}_\delta(q,a) \subseteq \mathfrak{M}_\delta$, one has $|q\alpha - a| = q|\alpha - a/q| \leqslant X^\delta \cdot X^{\delta-k}$, whence $q + X^k|q\alpha - a| = O(X^{2\delta})$. The claimed bound now follows from the previous lemma. □

Major arcs estimates

- Let us now substitute the conclusion of the previous lemma into the formula for the major arc contribution. Since

$$\mathfrak{M}_\delta = \bigcup_{\substack{0 \leqslant a < q \leqslant X^\delta \\ (a,q)=1}} \mathfrak{M}_\delta(q,a),$$

then

$$\int_{\mathfrak{M}_\delta} f(\alpha)^s e(-n\alpha)\mathrm{d}\alpha = \sum_{1 \leqslant q \leqslant X^\delta} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{-X^{\delta-k}}^{X^{\delta-k}} f(\beta + a/q)^s e(-n(\beta + a/q))\mathrm{d}\beta.$$

- Assuming that $\alpha \in \mathfrak{M}_\delta(q,a) \subseteq \mathfrak{M}_\delta$, we set

$$f^*(\alpha) = q^{-1} S(q,a) v(\alpha - a/q),$$

and write

$$E(\alpha) = f(\alpha) - f^*(\alpha)$$

- It follows from the previous lemma that $E(\alpha) = O(X^{2\delta})$.

Major arcs estimates

- Since
$$f(\alpha)^s - f^*(\alpha)^s = (f(\alpha) - f^*(\alpha))\left(f(\alpha)^{s-1} + \ldots + f^*(\alpha)^{s-1}\right)$$
$$= O(X^{s-1}|E(\alpha)|) = O(X^{s-1+2\delta}),$$
we obtain the asymptotic relation
$$\int_{\mathfrak{M}_\delta} f(\alpha)^s e(-n\alpha)\mathrm{d}\alpha$$
$$= \sum_{1\leqslant q\leqslant X^\delta} \sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{-X^{\delta-k}}^{X^{\delta-k}} \left(q^{-1}S(q,a)v(\beta)\right)^s e(-n(\beta + a/q))\mathrm{d}\beta$$
$$+ \sum_{1\leqslant q\leqslant X^\delta} \sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{-X^{\delta-k}}^{X^{\delta-k}} X^{s-1+2\delta}\,\mathrm{d}\alpha.$$
- The second sum is
$$O\Big(X^{s-1+2\delta} \sum_{1\leqslant q\leqslant X^\delta} q\cdot X^{\delta-k}\Big) = O(X^{s-k-1+3\delta}\cdot X^{2\delta}) = O(X^{s-k+(5\delta-1)}).$$
- This is $o\left(X^{s-k}\right)$ whenever $\delta < 1/5$.

Major arcs estimates

- Turning to the first sum, we find that it factorises in the shape

$$\sum_{1\leqslant q\leqslant X^\delta}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(q^{-1}S(q,a)\right)^s e(-na/q)\int_{-X^{\delta-k}}^{X^{\delta-k}} v(\beta)^s e(-\beta n)\mathrm{d}\beta.$$

- When $Q\in\mathbb{R}_+$, we define the truncated singular series

$$\mathfrak{S}_{s,k}(n;Q)=\sum_{1\leqslant q\leqslant Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(q^{-1}S(q,a)\right)^s e(-na/q),$$

  and the truncated singular integral

$$J_{s,k}(n;Q)=\int_{-QX^{-k}}^{QX^{-k}} v(\beta)^s e(-\beta n)\mathrm{d}\beta.$$

- Now we can summarize our discussion in the form of a lemma.

Lemma

When $0<\delta<1$, *one has*

$$\int_{\mathfrak{M}_\delta} f(\alpha)^s e(-n\alpha)\mathrm{d}\alpha=J_{s,k}\left(n;X^\delta\right)\mathfrak{S}_{s,k}\left(n;X^\delta\right)+O\left(X^{s-k+(5\delta-1)}\right).$$

Major arcs estimates

Corollary

When $s \geqslant 2^k + 1$ *and* $0 < \delta < 1/5$*, one has*

$$R_{s,k}(n) = J_{s,k}\left(n; X^{\delta}\right) \mathfrak{S}_{s,k}\left(n; X^{\delta}\right) + o\left(X^{s-k}\right)$$

in which $X = n^{1/k}$.

Proof.

Since $[0, 1)$ is the disjoint union of $\mathfrak{m}_\delta$ and $\mathfrak{M}_\delta$, one has

$$R_{s,k}(n) = \int_{\mathfrak{M}_\delta} f(\alpha)^s e(-n\alpha)\mathrm{d}\alpha + \int_{\mathfrak{m}_\delta} f(\alpha)^s e(-n\alpha)\mathrm{d}\alpha.$$

The conclusion follows from the previous results. □

- Our objective is now to analyse the truncated singular series $\mathfrak{S}_{s,k}(n; Q)$ and singular integral $J_{s,k}(n; Q)$.
- We first consider the truncated singular integral $J_{s,k}(n; Q)$, our first step being to complete this integral to obtain the (complete) singular integral

$$J_{s,k}(n) = \int_{-\infty}^{\infty} v(\beta)^s e(-n\beta)\mathrm{d}\beta.$$

The singular integral

Lemma

Whenever $\beta \in \mathbb{R}$, one has

$$v(\beta) = O\Big(X\left(1 + X^k|\beta|\right)^{-1/k}\Big).$$

Proof.

- Recall that
$$v(\beta) = \int_0^X e\left(\beta\gamma^k\right)\mathrm{d}\gamma.$$
The estimate $|v(\beta)| \leqslant X$ is trivial. Also, since $|v(\beta)| = |v(-\beta)|$, we may assume henceforth that $\beta > X^{-k}$.
- Changing the variable $u = \beta\gamma^k$, we find that when $\beta > 0$, one has
$$v(\beta) = k^{-1}\beta^{-1/k}\int_0^{\beta X^k} u^{-1+1/k}e(u)\mathrm{d}u,$$
whence
$$|v(\beta)| \leqslant k^{-1}\beta^{-1/k}\Big|\int_0^{\beta X^k} u^{-1+1/k}e(u)\mathrm{d}u\Big|.$$

Proof

- Notice that $u^{-1+1/k}$ decreases monotonically to 0 as $u \to \infty$. By Dirichlet's test for convergence of an infinite integral the last integral is uniformly bounded, and indeed

$$\left| \int_0^{\beta X^k} u^{-1+1/k} e(u) \mathrm{d}u \right| \leqslant \sup_{Y \geqslant 0} \left| \int_0^{Y} u^{-1+1/k} e(u) \mathrm{d}u \right| < \infty$$

- When $0 < Y < 1$, we are also making use of the inequality

$$\left| \int_0^{Y} u^{-1+1/k} e(u) \mathrm{d}u \right| \leqslant \int_0^{Y} u^{-1+1/k} \, \mathrm{d}u = O(1).$$

- Hence we deduce that when $|\beta| > X^{-k}$, one has

$$|v(\beta)| = O\big(|\beta|^{-1/k}\big) = O\Big(X \left(1 + X^k|\beta|\right)^{-1/k}\Big).$$

- The desired conclusion follows on combining this estimate with our earlier bound $|v(\beta)| \leqslant X$, applied in circumstances wherein $|\beta| \leqslant X^{-k}$.
- The proof is completed. □

The singular integral

Corollary

Suppose that $s \geqslant k+1$. Then the singular series $J_{s,k}(n)$ converges absolutely, and moreover,

$$|J_{s,k}(n;Q) - J_{s,k}(n)| = O(X^{s-k}Q^{-1/k}).$$

Proof.

- By applying the last lemma, one sees that

$$|J_{s,k}(n)| = O\left(\int_{-\infty}^{\infty} \frac{X^s}{(1+X^k|\beta|)^{s/k}} \, \mathrm{d}\beta \right) = O(X^{s-k}).$$

- Thus, the integral defining $J_{s,k}(n)$ is indeed absolutely convergent, and the singular integral exists. Moreover, and similarly,

$$|J_{s,k}(n;Q) - J_{s,k}(n)| = O\left(\int_{QX^{-k}}^{\infty} \frac{X^s}{(1+X^k\beta)^{1+1/k}} \right) = O(X^{s-k}Q^{-1/k})$$

This completes the proof. □

The singular integral

Lemma

When $s \geqslant k+1$*, one has*

$$J_{s,k}(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1}$$

in which

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}\,\mathrm{d}t \quad \textit{for} \quad \operatorname{Re} z > 0.$$

Proof.

- We begin by observing that

$$\begin{aligned} J_{s,k}(n) &= \lim_{B\to\infty} \int_{-B}^{B} v(\beta)^s e(-\beta n) \mathrm{d}\beta \\ &= \lim_{B\to\infty} \int_{-B}^{B} \int_{[0,X]^s} e\left(\beta\left(\gamma_1^k + \ldots + \gamma_s^k - n\right)\right) \mathrm{d}\boldsymbol{\gamma}\, \mathrm{d}\beta \\ &= \lim_{B\to\infty} \int_{[0,X]^s} \int_{-B}^{B} e\left(\beta\left(\gamma_1^k + \ldots + \gamma_s^k - n\right)\right) \mathrm{d}\beta\, \mathrm{d}\boldsymbol{\gamma}. \end{aligned}$$

The singular integral

- We make use of the observation that when $\phi \neq 0$, one has

$$\int_{-B}^{B} e(\beta\phi)\mathrm{d}\beta = \frac{\sin(2\pi B\phi)}{\pi\phi}.$$

- For $\phi = 0$, we interpret the right hand side of this formula to be $2B$. Thus we obtain the relation

$$J_{s,k}(n) = \lim_{B\to\infty} \int_{[0,X]^s} \frac{\sin\left(2\pi B\left(\gamma_1^k + \ldots + \gamma_s^k - n\right)\right)}{\pi\left(\gamma_1^k + \ldots + \gamma_s^k - n\right)} \mathrm{d}\boldsymbol{\gamma}$$

- We substitute $u_i = \gamma_i^k$ for $i \in [s]$, and recall that $n = X^k$. Thus

$$J_{s,k}(n) = k^{-s} \lim_{B\to\infty} I(B),$$

where we write

$$I(B) = \int_{[0,n]^s} \frac{\sin\left(2\pi B\left(u_1 + \ldots + u_s - n\right)\right)}{\pi\left(u_1 + \ldots + u_s - n\right)} \left(u_1 \ldots u_s\right)^{-1+1/k} \,\mathrm{d}\mathbf{u}.$$

The singular integral

- A further substitution reduces our task to one of evaluating an integral in just one variable. We put $v = u_1 + \ldots + u_s$ and make the change of variable $(u_1, \ldots, u_s) \mapsto (u_1, \ldots, u_{s-1}, v)$, obtaining the relation

$$I(B) = \int_0^{sn} \Psi(v) \frac{\sin(2\pi B(v-n))}{\pi(v-n)} \mathrm{d}v,$$

in which

$$\Psi(v) = \int_{\mathfrak{B}(v)} (u_1 \ldots u_{s-1})^{\frac{1}{k}-1} (v - u_1 - \ldots - u_{s-1})^{\frac{1}{k}-1} \, \mathrm{d}u_1 \ldots \, \mathrm{d}u_{s-1},$$

and

$$\mathfrak{B}(v) = \left\{ (u_1, \ldots, u_{s-1}) \in [0, n]^{s-1} : 0 \leqslant v - u_1 - \ldots - u_{s-1} \leqslant n \right\}.$$

- Notice that the condition on $u_1, \ldots, u_{s-1}$ in the definition of $\mathfrak{B}(v)$ may be rephrased as $v - n \leqslant u_1 + \ldots + u_{s-1} \leqslant v$.
- Since $\Psi(v)$ is a function of bounded variation, it follows from Fourier's integral theorem that since $n \in (0, sn)$, one has

$$\lim_{B \to \infty} I(B) = \Psi(n) = \int_{\mathfrak{B}(n)} (u_1 \ldots u_{s-1})^{\frac{1}{k}-1} (n - u_1 - \ldots - u_{s-1})^{\frac{1}{k}-1} \, \mathrm{d}\mathbf{u}.$$

The singular integral

- Note that
$$\mathfrak{B}(n) = \left\{(u_1, \ldots, u_{s-1}) \in [0, n]^{s-1} : 0 \leqslant u_1 + \ldots + u_{s-1} \leqslant n\right\}.$$
- Thus
$$J_{s,k}(n) = k^{-s}\Psi(n) = k^{-s}\int_{\mathfrak{B}(n)} (u_1 \ldots u_{s-1})^{\frac{1}{k}-1} (n - u_1 - \ldots - u_{s-1})^{\frac{1}{k}-1} \, \mathrm{d}\mathbf{u}.$$
- We now apply induction to show that
$$J_{s,k}(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1}.$$
- First, when $s = 2$, we have
$$\begin{aligned} J_{2,k}(n) &= k^{-2}\int_0^n u_1^{\frac{1}{k}-1} (n - u_1)^{\frac{1}{k}-1} \, \mathrm{d}u_1 \\ &= k^{-2} n^{\frac{2}{k}-1} \int_0^1 v^{\frac{1}{k}-1}(1-v)^{\frac{1}{k}-1} \, \mathrm{d}v. \end{aligned}$$
- Thus, on recalling the classical Beta function, we obtain the formula
$$J_{2,k}(n) = k^{-2} n^{\frac{2}{k}-1} \, \mathrm{B}(1/k, 1/k) = k^{-2} n^{\frac{2}{k}-1} \frac{\Gamma(1/k)^2}{\Gamma(2/k)} = \frac{\Gamma(1+1/k)^2}{\Gamma(2/k)} n^{\frac{2}{k}-1}.$$

The singular integral

- Thus, the inductive hypothesis holds for $s = 2$. Suppose now that the inductive hypothesis holds for $s = t$. Then we have

$$J_{t+1,k}(n) = k^{-1} \int_0^n u_t^{\frac{1}{k}-1} J_{t,k}(n - u_t)\, \mathrm{d}u_t$$
$$= k^{-1} \frac{\Gamma(1 + 1/k)^t}{\Gamma(t/k)} \int_0^n u_t^{\frac{1}{k}-1} (n - u_t)^{\frac{t}{k}-1}\, \mathrm{d}u_t.$$

- Recalling once again the classical Beta function, we see that

$$J_{t+1,k}(n) = k^{-1} \frac{\Gamma(1 + 1/k)^t}{\Gamma(t/k)} n^{\frac{t+1}{k}-1}\, \mathrm{B}(1/k, t/k)$$
$$= k^{-1} \frac{\Gamma(1 + 1/k)^t}{\Gamma(t/k)} n^{\frac{t+1}{k}-1} \frac{\Gamma(1/k)\Gamma(t/k)}{\Gamma((t+1)/k)}$$
$$= \frac{\Gamma(1 + 1/k)^{t+1}}{\Gamma((t+1)/k)} n^{\frac{t+1}{k}-1}.$$

- This yields the inductive hypothesis with t replaced by $t + 1$. We have therefore shown that whenever $s \geqslant k + 1$, one has

$$J_{s,k}(n) = \frac{\Gamma(1 + 1/k)^s}{\Gamma(s/k)} n^{s/k-1}.$$

The singular series

Corollary

Suppose that $s \geqslant k+1$. *Then one has*

$$J_{s,k}(n;Q) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} + O\left(n^{s/k-1}Q^{-1/k}\right),$$

as $Q \to \infty$.

Proof.

The conclusion follows by the previous two results, since $X = n^{1/k}$. □

- We next consider the truncated singular series $\mathfrak{S}_{s,k}(n;Q)$. Our first step is to complete this series to obtain the (complete) singular series

$$\mathfrak{S}_{s,k}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(q^{-1}S(q,a)\right)^s e(-na/q).$$

Again, we must consider the tail of the infinite sum.

The singular series

Lemma

Whenever $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfy $(a, q) = 1$, one has

$$|S(q,a)| = O(q^{1-2^{1-k}+\varepsilon}).$$

Proof.

We apply Weyl's inequality with $\alpha_k = a/q$ and $X = q$ to obtain

$$\Big| \sum_{r=1}^{q} e\left(ar^k/q\right) \Big| = O\Big(q^{1+\varepsilon}\left(q^{-1} + q^{-1} + q^{1-k}\right)^{2^{1-k}}\Big).$$

□

Lemma

Suppose that $s \geqslant 2^k + 1$. Then $\mathfrak{S}_{s,k}(n)$ converges absolutely, and

$$|\mathfrak{S}_{s,k}(n) - \mathfrak{S}_{s,k}(n;Q)| = O\big(Q^{-2^{-k}}\big)$$

uniformly in $n \in \mathbb{Z}_+$.

Proof

- By the previous lemma we estimate the tail of the truncated singular series as follows

$$\sum_{q>Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left| \left(q^{-1}S(q,a)\right)^s e(-na/q) \right| = O\Big(\sum_{q>Q} \phi(q) \left(q^{\varepsilon - 2^{1-k}} \right)^s \Big).$$

- Thus, when $s \geqslant 2^k + 1$, we deduce that

$$\sum_{q>Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left| \left(q^{-1}S(q,a)\right)^s e(-na/q) \right| = O\Big(\sum_{q>Q} q^{\varepsilon - 1 - 2^{1-k}} \Big) = O(Q^{-2^{-k}}).$$

- It follows that the infinite series $\mathfrak{S}_{s,k}(n)$ converges absolutely under these conditions, and moreover that

$$|\mathfrak{S}_{s,k}(n) - \mathfrak{S}_{s,k}(n;Q)| = O(Q^{-2^{-k}}).$$

- Notice that this estimate is uniform in n.

The singular series

- We shall see shortly that there is a close connection between the singular series $\mathfrak{S}_{s,k}(n)$ and the number of solutions of the congruence
$$x_1^k + \ldots + x_s^k \equiv n \pmod{q},$$
 as q varies. This suggests a multiplicative theme.

Lemma

Suppose that $(a, q) = (b, r) = (q, r) = 1$. *Then one has the quasimultiplicative relation*

$$S(qr, ar + bq) = S(q, a)S(r, b).$$

Proof.

- Each residue m modulo qr with $m \in [qr]$ is in bijective correspondence with a pair (t, u) with $t \in [q]$ and $u \in [r]$, with $m \equiv tr + uq \pmod{qr}$.
- Indeed, if we write $\bar{q}$ for any integer congruent to the multiplicative inverse of $q \pmod{r}$, and $\bar{r}$ for any integer congruent to the multiplicative inverse of $r \pmod{q}$, then claimed bijection is as follows $m \equiv (m\bar{r})r + (m\bar{q})q \pmod{qr}$, which follows from the Chinese remainder theorem.

Proof

- Thus, we see that

$$\begin{aligned} S(qr, ar+bq) &= \sum_{m=1}^{qr} e\left(\frac{ar+bq}{qr} m^k\right) \\ &= \sum_{t=1}^{q} \sum_{u=1}^{r} e\left(\frac{(ar+bq)(tr+uq)^k}{qr}\right) \\ &= \sum_{t=1}^{q} \sum_{u=1}^{r} e\left(\frac{a}{q}(tr)^k + \frac{b}{r}(uq)^k\right). \end{aligned}$$

- By the change of variable $tr \mapsto t' (\bmod q)$ and $uq \mapsto u' (\bmod r)$, bijective owing to the coprimality of q and r, we obtain the relation

$$S(qr, ar+bq) = \left(\sum_{v=1}^{q} e\left(av^k/q\right)\right)\left(\sum_{w=1}^{r} e\left(bw^k/r\right)\right) = S(q,a)S(r,b).$$

- This completes the proof of the lemma. □

The singular series

- Now define the quantity

$$A(q,n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(q^{-1}S(q,a)\right)^s e(-na/q)$$

Lemma

The quantity $A(q,n)$ is a multiplicative function of q.

Proof.

- Suppose that $(q,r) = 1$. Then by the Chinese remainder theorem, there is a bijection between the residue classes a modulo qr with $(a,qr) = 1$, and the ordered pairs (b,c) with $b \pmod{q}$ and $c \pmod{r}$ satisfying $(b,q) = (c,r) = 1$, via the relation $a \equiv br + cq \pmod{qr}$.
- Thus, we obtain

$$\begin{aligned} A(qr,n) &= \sum_{\substack{a=1 \\ (a,qr)=1}}^{qr} \left((qr)^{-1}S(qr,a)\right)^s e(-na/qr) \\ &= \sum_{\substack{b=1 \\ (b,q)=1}}^{q} \sum_{\substack{c=1 \\ (c,r)=1}}^{r} \left((qr)^{-1}S(qr,br+cq)\right)^s e\left(-\frac{br+cq}{qr}n\right). \end{aligned}$$

Proof

- By applying the previous lemma, we infer that

$$A(qr,n) = \sum_{\substack{b=1 \\ (b,q)=1}}^{q} \sum_{\substack{c=1 \\ (c,r)=1}}^{r} \left(q^{-1}S(q,b)\right)^s \left(r^{-1}S(r,c)\right)^s e(-bn/q)e(-cn/r)$$
$$= A(q,n)A(r,n).$$

- Since $A(1,n) = 1$, this confirms the multiplicative property for $A(q,n)$ and completes the proof of the lemma. □
- Observe that

$$\mathfrak{S}_{s,k}(n) = \sum_{q=1}^{\infty} A(q,n).$$

- The multiplicativity of $A(q,n)$ therefore suggests that $\mathfrak{S}_{s,k}(n)$ should factor as a product over prime numbers p of the p-adic densities

$$\sigma(p) = \sum_{h=0}^{\infty} A\left(p^h, n\right).$$

The singular series

Theorem

Suppose that $s \geqslant 2^k + 1$. *Then the following hold:*

(i) *The series* $\sigma(p)$ *converges absolutely, and one has*

$$|\sigma(p) - 1| = O(p^{-1-2^{-k}}).$$

(ii) *The infinite product*

$$\prod_{p \in \mathbb{P}} \sigma(p)$$

converges absolutely.

(iii) *One has* $\mathfrak{S}_{s,k}(n) = \prod_{p \in \mathbb{P}} \sigma(p)$.

(iv) *There exists a natural number* $C = C(k)$ *with the property that*

$$1/2 < \prod_{p \in \mathbb{P}_{\geqslant C(k)}} \sigma(p) < 3/2.$$

Proof

- We begin by establishing (i). We recall from estimates of complete exponential sums that whenever $(a,p)=1$, one has

$$|S\left(p^h,a\right)| = O\big(p^{h(1-2^{1-k}+\varepsilon)}\big).$$

- Then, whenever $s \geqslant 2^k+1$, one finds that

$$\begin{aligned} A\left(p^h,n\right) &= \sum_{\substack{a=1\\(a,p)=1}}^{p^h} \left(p^{-h}S\left(p^h,a\right)\right)^s e\left(-na/p^h\right) \\ &= O\big(p^{h\left(1-s2^{1-k}\right)+\varepsilon}\big) = O\big(p^{-h\left(1+2^{-k}\right)}\big). \end{aligned}$$

- Hence

$$\sigma(p)-1 = \sum_{h=1}^{\infty} A\left(p^h,n\right) = O\Big(\sum_{h=1}^{\infty} p^{-h\left(1+2^{-k}\right)}\Big) = O(p^{-1-2^{-k}}).$$

- Thus $\sigma(p)$ converges absolutely, and one has $|\sigma(p)-1| = O(p^{-1-2^{-k}})$.
- We next turn to the proof of (ii). By part (i), there is a positive number $B=B(k)$ with the property that $|\sigma(p)-1| \leqslant Bp^{-1-2^{-k}}$.

Proof

- Hence, whenever p is sufficiently large, one sees that

$$\log(1+|\sigma(p)-1|) \leqslant \log\left(1+Bp^{-1-2^{-k}}\right) \leqslant Bp^{-1-2^{-k-1}},$$

whence

$$\sum_{p\in\mathbb{P}} \log(1+|\sigma(p)-1|) = O\Big(B\sum_{p\in\mathbb{P}} p^{-1-2^{-k-1}}\Big) = O(1).$$

- Thus we deduce that the infinite product $\prod_p \sigma(p)$ converges absolutely.
- The proof of (iii) employs the multiplicative property of $A(q,n)$ established in the previous lemma. One finds that

$$\mathfrak{S}_{s,k}(n) = \sum_{q=1}^{\infty} A(q,n) = \sum_{q=1}^{\infty} \prod_{p^h \| q} A\left(p^h, n\right)$$

- Then since $\prod_{p\in\mathbb{P}} \sigma(p)$ converges absolutely as a product, and $\sum_{q=1}^{\infty} A(q,n)$ converges absolutely as a sum, we may rearrange summands to deduce that

$$\mathfrak{S}_{s,k}(n) = \prod_{p\in\mathbb{P}} \sum_{h=0}^{\infty} A\left(p^h, n\right) = \prod_{p\in\mathbb{P}} \sigma(p).$$

Proof

- Finally, we establish (iv). We begin by observing that from part (i), it follows that whenever p is sufficiently large in terms of k, one has

$$1 - p^{-1-2^{-k}} \leqslant \sigma(p) \leqslant 1 + p^{-1-2^{-k}}$$

- Hence, provided that $C = C(k)$ is sufficiently large, one finds that

$$\left| \prod_{p \in \mathbb{P}_{\geqslant C(k)}} \sigma(p) - 1 \right| \leqslant \sum_{n \geqslant C(k)} n^{-1-2^{-k}} = O\big(C(k)^{-2^{-k}}\big).$$

- Then, if $C(k)$ is chosen sufficiently large in terms of k, we have that

$$\left| \prod_{p \in \mathbb{P}_{\geqslant C(k)}} \sigma(p) - 1 \right| < 1/2,$$

  and we conclude that

$$1/2 < \prod_{p \in \mathbb{P}_{\geqslant C(k)}} \sigma(p) < 3/2.$$

- The final conclusion of the theorem therefore follows, and the proof of the theorem is complete. □

The singular series

- Our plan is to show that there exists a constant $c_0 > 0$ such that $\mathfrak{S}_{s,k}(n) \geq c_0$ uniformly in $n \in \mathbb{Z}_+$.
- In view of item (iv) of the previous theorem it suffices to prove that $\sigma(p) > 0$ for $p \leqslant C(k)$ with sufficient uniformity in n.
- When $q \in \mathbb{Z}_+$, we put

$$M_n(q) = \# \left\{ \mathbf{m} \in (\mathbb{Z}/q\mathbb{Z})^s : m_1^k + \ldots + m_s^k = n \right\}.$$

Lemma

For each natural number $q \in \mathbb{Z}_+$, one has

$$\sum_{d|q} A(d,n) = q^{1-s} M_n(q).$$

Proof.

We make use of the orthogonality relation

$$q^{-1} \sum_{r=1}^{q} e(hr/q) = \begin{cases} 1, & \text{when } q \mid h, \\ 0, & \text{when } q \nmid h. \end{cases}$$

Proof

- Then
$$M_n(q) = q^{-1} \sum_{r=1}^{q} \left(\sum_{m_1=1}^{q} \cdots \sum_{m_s=1}^{q} e\left(r\left(m_1^k + \ldots + m_s^k - n\right)/q\right) \right).$$
- Classifying the values of r according to their common factors q/d with q, we obtain the relation
$$\begin{aligned} M_n(q) &= q^{-1} \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} (q/d)^s \sum_{m_1=1}^{d} \cdots \sum_{m_s=1}^{d} e\left(a\left(m_1^k + \ldots + m_s^k - n\right)/d\right) \\ &= q^{-1} \sum_{d|q} q^s \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \left(d^{-1} S(d,a)\right)^s e(-na/d) \\ &= q^{s-1} \sum_{d|q} A(d,n) \end{aligned}$$
- Hence
$$\sum_{d|q} A(d,n) = q^{1-s} M_n(q),$$
and the proof of the lemma is complete. □

The singular series

Corollary

For each prime number $p \in \mathbb{P}$, one has

$$\sigma(p) = \lim_{h \to \infty} p^{h(1-s)} M_n\left(p^h\right). \qquad (*)$$

Proof.

Take $q = p^h$ in the previous lemma to obtain the relation

$$\sum_{l=0}^{h} A\left(p^l, n\right) = \left(p^h\right)^{1-s} M_n\left(p^h\right).$$

Taking the limit as $h \to \infty$, we obtain (*), since $\sigma(p) = \sum_{l=0}^{\infty} A\left(p^l, n\right)$. □

Exercise

Show that for the small primes p with $p < C(k)$, and for all large enough values of h, one has $M_n\left(p^h\right) \geq c_0 p^{h(s-1)}$ for some $c_0 > 0$. From this we deduce that $\sigma(p) > 0$, and the desired conclusion follows from item (iv) of the previous theorem.

The asymptotic formula in Waring's problem

- We have shown that when $s \geqslant 2^k + 1$ and $0 < \delta < 1/5$, one has

$$R_{s,k}(n) = J_{s,k}\left(n; X^{\delta}\right) \mathfrak{S}_{s,k}\left(n; X^{\delta}\right) + o\left(X^{s-k}\right).$$

- We also know that

$$J_{s,k}\left(n; X^{\delta}\right) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} + O\left(n^{s/k-1-\delta/k^2}\right),$$

  and

$$\mathfrak{S}_{s,k}\left(n; X^{\delta}\right) = \mathfrak{S}_{s,k}(n) + O\left(n^{-\delta 2^{-k}/k}\right),$$

  where $c < \mathfrak{S}_{s,k}(n) < C$ for some $C > c > 0$.
- Thus we conclude that when $s \geqslant 2^k + 1$, one has

$$R_{s,k}(n) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} \mathfrak{S}_{s,k}(n) + o\left(n^{s/k-1}\right).$$

- Then $R_{s,k}(n) \to \infty$ as $n \to \infty$, whence $G(k) \leqslant 2^k + 1$.