HCM Summer School: The Circle Method

An Introduction to the Circle Method
Part I

Yu-Ru Liu

University of Waterloo

Monday, May 10, 2021

Lecture Series Plan

- Part I: Waring's problem
- Part II: Vinogradov's mean value theorem
- Part III: Generalisations of Waring's problem and Vinogradov's mean value theorem

Part I: Waring's Problem

Talk Plan

- Introduction to Waring's problem
- The circle method
- Minor arcs estimates
- Major arcs estimates

1. Introduction to Waring's problem

Sums of Squares

$$1 = 1^2, \quad 2 = 1^2 + 1^2, \quad 3 = 1^2 + 1^2 + 1^2,$$

$$4 = 2^2, \quad 5 = 2^2 + 1^2, \quad 6 = 2^2 + 1^2 + 1^2, \quad 7 = 2^2 + 1^2 + 1^2 + 1^2,$$

$$8 = 2^2 + 2^2, \quad 9 = 3^2, \quad \cdots$$

$$2021 = 42^2 + 16^2 + 1^2 = 44^2 + 9^2 + 2^2, \quad \cdots$$

Question Can we write all positive integers as a sum of squares? More generally, for $k \in \mathbb{N} = \{1, 2, \cdots\}$ with $k \geq 2$, can we write all positive integers as a sum of kth powers?

Waring's Problem For $k \in \mathbb{N}$ with $k \geq 2$, can we find $s = s(k)$ such that for all $n \in \mathbb{N}$, there exist $x_1, \cdots, x_s \in \mathbb{N} \cup \{0\}$ such that

$$n = x_1^k + x_2^k + \cdots + x_s^k?$$

Let $g(k)$ denote the least s such that the above equation holds for all $n \in \mathbb{N}$.

- In 1770, Lagrange proved $g(2) = 4$.
- Before 1909, only known cases are $k = 2, 3, 4, 5, 6, 7, 8, 10$.
- In 1909, Hilbert proved that $g(k) < \infty$ for every $k \geq 2$.

Consider

$$n = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 < 3^k.$$

The most efficient way to represent n:

- Use $\left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1\right)$ copies of 2^k.
- Use $(2^k - 1)$ copies of 1^k.

Thus we obtain a result of Euler that

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

Theorem (Mahler, 1957)

The equality holds for all but finitely many k.

More Interesting Waring's Problem For $k \in \mathbb{N}$ with $k \geq 2$, let $G(k)$ denote the least integer $s = s(k)$ such that for all $n \in \mathbb{N}$ sufficiently large, there exist $x_1, \cdots, x_s \in \mathbb{N}$ such that

$$n = x_1^k + x_2^k + \cdots + x_s^k.$$

- $G(k) \leq g(k)$.
- Only known cases: $G(2) = 4$ and $G(4) = 16$.
- Hardy-Littlewood (1920): $G(k) \leq (k-2)2^{k-2} + 5$.
- Hua (1938): $G(k) \leq 2^k + 1$.
- The bound was improved by Vinogradov, Vaughan and others.

Theorem (Wooley, 1992)

For large values of k, $G(k) \leq k(\log k + \log\log k + O(1))$.

Notation For $x \in \mathbb{R}$, let $f(x)$ be a complex-valued function, and let $g(x)$ be a positive real-valued function.

1. If there exists a constant $C > 0$ such that $|f(x)| \leq Cg(x)$ for all sufficiently large $x \in \mathbb{R}$, we write $f(x) = O(g(x))$ or $f(x) \ll g(x)$.

2. If $|f(x)|/g(x) \to 0$ as $x \to \infty$, we write $f(x) = o(g(x))$.

3. If $f(x) = g(x) + o(g(x))$, we say $f(x)$ is asymptotic to $g(x)$ and we denote it by $f(x) \sim g(x)$.

• For example, $4x^2 + 9x = O(x^2)$, $9x = o(x^2)$ and $4x^2 + 9x \sim 4x^2$.

• If a statement contains ϵ, we assert that it holds for all $\epsilon > 0$. For example, $x^{2\epsilon} \log x \ll x^{\epsilon}$.

2. The Circle Method

Fix $k, s \in \mathbb{N} = \{1, 2, \cdots\}$ with $k \geq 2$. Write $\mathbf{x} = \mathbf{x}_s = (x_1, \cdots, x_s)$. For $n \in \mathbb{N}$, define

$$R(n) = R_{s,k}(n) = \#\{\mathbf{x} \in \mathbb{N}^s : n = x_1^k + \cdots + x_s^k\}.$$

Note that $x_i \leq n^{1/k}$. Write $X = \lfloor n^{1/k} \rfloor$ and hence $1 \leq x_i \leq X$.

For $\alpha \in \mathbb{R}$, let $e(\alpha) = e^{2\pi i \alpha}$. For $m \in \mathbb{Z}$, we have

$$\int_0^1 e(\alpha m) d\alpha = \begin{cases} 1, & \text{if } m = 0, \\ 0, & \text{otherwise.} \end{cases}$$

It follows that

$$\sum_{1 \leq x_1 \leq X} \cdots \sum_{1 \leq x_s \leq X} \int_0^1 e\big(\alpha(x_1^k + \cdots + x_s^k - n)\big) d\alpha = R(n).$$

Let

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

Then we can rewrite

$$\begin{aligned} R(n) &= \#\{\mathbf{x} \in \mathbb{N}^s : n = x_1^k + \cdots + x_s^k\} \\ &= \sum_{1 \le x_1 \le X} \cdots \sum_{1 \le x_s \le X} \int_0^1 e\big(\alpha(x_1^k + \cdots + x_s^k - n)\big) d\alpha \\ &= \int_0^1 f(\alpha)^s e(-\alpha n) d\alpha. \end{aligned}$$

Since

$$s \le x_1^k + \cdots + x_s^k \le sX^k,$$

the "probability" that the sum equals to n is $O(X^{-k})$. So we expect that $R(n)$ is of size $X^s \cdot X^{-k} = X^{s-k}$.

To estimate

$$R(n) = \int_0^1 f(\alpha)^s e(-\alpha n) d\alpha,$$

we divide $[0, 1]$ into two parts: the major arcs $\mathfrak{M}$ and the minor arcs $\mathfrak{m}$, where $\mathfrak{M}$ contains α close to a/q with q small.

More precisely, let δ be a parameter with $0 < \delta < 1$. For $q, a \in \mathbb{N} \cup \{0\}$ with $a < q$ and $\gcd(a, q) = 1$, define

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

Then we define the major arcs

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

Also, the minor arcs

$$\mathfrak{m} = [0, 1) \setminus \mathfrak{M}.$$

We recall that the expected size of $R(n)$ is X^{s-k}. We will show

$$\int_{\mathfrak{M}} f(\alpha)^s e(-\alpha n) d\alpha = C_{s,k}(n) X^{s-k} + o(X^{s-k})$$

for some constant $C_{s,k}(n) > 0$. Also

$$\int_{\mathfrak{m}} f(\alpha)^s e(-\alpha n) d\alpha = o(X^{s-k}).$$

Since $X = \lfloor n^{1/k} \rfloor$, it follows that

$$\begin{aligned} R(n) &= \int_0^1 f(\alpha)^s e(-\alpha n) d\alpha \\ &= C_{s,k}(n) X^{s-k} + o(X^{s-k}) \\ &= C_{s,k}(n) n^{s/k-1} + o(n^{s/k-1}). \end{aligned}$$

3. Minor Arcs Estimates

We recall that the minor arcs

$$\mathfrak{m} = [0,1) \setminus \mathfrak{M}, \quad \text{where} \quad \mathfrak{M} = \bigcup_{\substack{0 \le a < q \le X^\delta \\ \gcd(a,q)=1}} \mathfrak{M}(q,a)$$

with

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

Theorem (Dirichlet's Theorem) Let $\theta, Q \in \mathbb{R}$ with $Q > 1$. Then there exist $a, q \in \mathbb{Z}$ such that $1 \le q \le Q$, $\gcd(a,q) = 1$ and

$$|\theta - a/q| < 1/qQ.$$

By taking $Q = X^{k-\delta}$, we see that if $\mathfrak{M}(q,a) \subseteq \mathfrak{m}$, we have

$$X^\delta < q \le X^{k-\delta}.$$

We recall that

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

Since $|e(\alpha x^k)| \le 1$, a trivial bound of $f(\alpha)$ is X.

Goal We aim to show

$$\sup_{\mathfrak{m}} |f(\alpha)| = o(X).$$

This allows us to conclude that for s sufficiently large,

$$\int_{\mathfrak{m}} f(\alpha)^s e(-\alpha n) d\alpha = o(X^{s-k}).$$

Idea Relate $f(\alpha)$ to the geometric series

$$\sum_{1 \le x \le X} e(\alpha x).$$

Weyl's Differencing Consider

$$\Delta_1(x^k, h) := (x+h)^k - x^k,$$

which is a degree $(k-1)$ polynomial in x with leading coefficient k. We repeat the process to get $\Delta_2, \Delta_3 \cdots$. If we repeat the process $(k-1)$-times, we get Δ_{k-1}, a degree 1 polynomial with leading coefficient $k!$.

Theorem (Weyl's Inequality) Let $a, q \in \mathbb{N} \cup \{0\}$ with $\gcd(a, q) = 1$ and $|\alpha - a/q| \leq q^{-2}$. We have

$$f(\alpha) \ll X^{1+\epsilon}(q^{-1} + X^{-1} + qX^{-k})^{2^{1-k}}.$$

If $\alpha \in \mathfrak{m}$, then $X^\delta < q \leq X^{k-\delta}$. It follows that

$$\sup_{\mathfrak{m}} |f(\alpha)| \ll X^{1-\delta 2^{1-k}+\epsilon}.$$

By Weyl's Inequality, we have

$$\Big|\int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha)d\alpha\Big| \ll \sup_{\mathfrak{m}} |f(\alpha)|^s d\alpha \ll X^{s-s\delta 2^{1-k}+\epsilon}.$$

To bound the integral by $o(X^{s-k})$, it suffices to take

$$s - s\delta 2^{1-k} < s-k \quad \Longleftrightarrow \quad s > k\delta^{-1}2^{k-1}.$$

It follows that if $s \geq (\lfloor k\delta^{-1}2^{k-1}\rfloor + 1)$,

$$\int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha)d\alpha = o(X^{s-k}).$$

- Using Hua's Lemma, we can reduce the number of variables to (2^k+1).

Hua's lemma

For $f(\alpha) = \sum_{1 \le x \le X} e(\alpha x^k)$, consider

$$\int_0^1 |f(\alpha)|^{2s} d\alpha$$

$$= \sum_{1 \le x_1, y_1 \le X} \cdots \sum_{1 \le x_s, y_s \le X} \int_0^1 e\big(\alpha\big((x_1^k - y_1^k) + \cdots + (x_s^k - y_s^k)\big)\big) d\alpha,$$

which counts the number of $\mathbf{x}, \mathbf{y} \in \mathbb{N}^s$ satisfying

$$(x_1^k + \cdots + x_s^k) - (y_1^k + \cdots + y_s^k) = 0$$

with $x_i, y_i \le X$. Since

$$s - sX^k \le (x_1^k + \cdots + x_s^k) - (y_1^k + \cdots + y_s^k) \le sX^k - s,$$

the "probability" that the difference equals to 0 is $O(X^{-k})$. So we expect that $\int_0^1 |f(\alpha)|^{2s} d\alpha$ is of size $X^{2s} \cdot X^{-k} = X^{2s-k}$.

By applying Weyl's differencing $(k-1)$ times,

Lemma (Hua's Lemma) We have

$$\int_0^1 |f(\alpha)|^{2^k} d\alpha \ll X^{2^k - k + \epsilon}.$$

By Weyl's Inequality and Hua's Lemma, it follows that

$$\begin{aligned}\int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha) d\alpha &\leq \left(\sup_{\mathfrak{m}} |f(\alpha)|\right)^{s-2^k} \int_0^1 |f(\alpha)|^{2^k} d\alpha \\ &\ll \left(X^{1-\delta 2^{1-k}+\epsilon}\right)^{s-2^k} X^{2^k-k+\epsilon} \\ &\ll X^{s-k-\delta 2^{1-k}(s-2^k)+\epsilon}.\end{aligned}$$

Theorem (Minor Arcs Estimate) If $s \geq 2^k + 1$, we have

$$\int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha) d\alpha = o(X^{s-k}).$$

4. Major Arcs Estimates

We recall that

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

If we take $\alpha = a/q$, and write $x = yq + r$ with $1 \le r \le q$, then

$$\begin{aligned} f(a/q) &= \sum_{1 \le x \le X} e(ax^k/q) \\ &= \sum_{r=1}^{q} \sum_{\frac{1-r}{q} \le y \le \frac{X-r}{q}} e(a(qy+r)^k/q) \\ &= \sum_{r=1}^{q} e(ar^k/q) \sum_{\frac{1-r}{q} \le y \le \frac{X-r}{q}} 1. \end{aligned}$$

More generally, for $\alpha \in \mathfrak{M}(q, a)$, write $\alpha = a/q + \beta$ with $|\beta| \leq X^{\delta-k}$. Then we have

$$f(\alpha) = \sum_{r=1}^{q} e(ar^k/q) \sum_{\frac{1-r}{q} \leq y \leq \frac{X-r}{q}} e\big(\beta(yq+r)^k\big).$$

Since $e(\cdot)$ is a smooth function, we have

$$\sum_{\frac{1-r}{q} \leq y \leq \frac{X-r}{q}} e\big(\beta(yq+r)^k\big) \sim \int_{\frac{1-r}{q}}^{\frac{X-r}{q}} e\big(\beta(zq+r)^k\big) dz.$$

By a change of variables, we have

$$\int_{\frac{1-r}{q}}^{\frac{X-r}{q}} e\big(\beta(zq+r)^k\big) dz \sim q^{-1} \int_0^X e(\beta\gamma^k) d\gamma.$$

It follows that

$$f(\alpha) \sim q^{-1} \sum_{r=1}^{q} e(ar^k/q) \int_0^X e(\beta\gamma^k) d\gamma.$$

Define

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q) \qquad \text{and} \qquad \nu(\beta) = \int_0^X e(\beta\gamma^k) d\gamma.$$

Lemma 1 If $\alpha \in \mathfrak{M}(q,a) \subseteq \mathfrak{M}$ with $\alpha = a/q + \beta$, we have

$$f(\alpha) = q^{-1} S(q,a) \nu(\beta) + O(X^{2\delta}).$$

For $\alpha = a/q + \beta \in \mathfrak{M}$, since

$$f(\alpha) \sim q^{-1} S(q,a)\nu(\beta)$$

and

$$\mathfrak{M} = \bigcup_{\substack{0 \le a < q \le X^{\delta} \\ \gcd(a,q)=1}} \{\alpha \in [0,1) : |\alpha - a/q| \le X^{\delta - k}\},$$

we have

$$\begin{aligned} &\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha) d\alpha \\ &= \sum_{1 \le q \le X^{\delta}} \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \int_{|\beta| \le X^{\delta-k}} f(\alpha)^s e(-na/q) e(-n\beta) d\beta \\ &\sim \sum_{1 \le q \le X^{\delta}} \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \left(q^{-1} S(q,a)\right)^s e(-na/q) \int_{|\beta| \le X^{\delta-k}} \nu(\beta)^s e(-n\beta) d\beta. \end{aligned}$$

For a positive real number Q, define

$$\mathfrak{S}(n,Q)=\mathfrak{S}_{s,k}(n,Q)=\sum_{1\le q\le Q}\sum_{\substack{a=0\\ \gcd(a,q)=1}}^{q-1}\left(q^{-1}S(q,a)\right)^s e(-na/q)$$

and

$$\mathfrak{J}(n,Q)=\mathfrak{J}_{s,k}(n,Q)=\int_{-Q}^{Q}\nu(\beta)^s e(-n\beta)d\beta.$$

Lemma 2 For $X=\lfloor n^{1/k}\rfloor$ and $0<\delta<1/5$, we have

$$\int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha)d\alpha=\mathfrak{S}(n,X^{\delta})\mathfrak{J}(n,X^{\delta-k})+o(X^{s-k}).$$

By Lemma 2 and the Minor Arcs Estimate, if $s \geq 2^k + 1$, $0 < \delta < 1/5$ and $X = \lfloor n^{1/k} \rfloor$, then

$$\begin{aligned} R(n) &= \int_0^1 f(\alpha)^s e(-n\alpha) d\alpha \\ &= \int_{\mathfrak{M}} f(\alpha)^s e(-n\alpha) d\alpha + \int_{\mathfrak{m}} f(\alpha)^s e(-n\alpha) d\alpha \\ &= \mathfrak{S}(n, X^\delta) \mathfrak{J}(n, X^{\delta - k}) + o(X^{s-k}). \end{aligned}$$

Since $R(n)$ is independent of δ, we need to remove the dependence on the parameter δ.

We recall that

$$\mathfrak{S}(n, X^\delta) = \sum_{1 \le q \le X^\delta} \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \left(q^{-1} S(q,a)\right)^s e(-na/q)$$

and

$$\mathfrak{J}(n, X^{\delta-k}) = \int_{-X^{\delta-k}}^{X^{\delta-k}} \nu(\beta)^s e(-n\beta) d\beta.$$

Define the singular series

$$\mathfrak{S}(n) = \mathfrak{S}_{s,k}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \left(q^{-1} S(q,a)\right)^s e(-na/q)$$

and the singular integral

$$\mathfrak{J}(n) = \mathfrak{J}_{s,k}(n) = \int_{-\infty}^{\infty} \nu(\beta)^s e(-\beta n) d\beta.$$

Singular Series

By Weyl's Inequality,

Lemma 3 For $a, q \in \mathbb{N} \cup \{0\}$ with $\gcd(a, q) = 1$, we have

$$S(q, a) \ll q^{1-2^{1-k}+\epsilon}.$$

If $s \geq 2^k + 1$, we have

$$\mathfrak{S}(n) - \mathfrak{S}(n, X^\delta) = \sum_{q > X^\delta} \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \left(q^{-1} S(q, a)\right)^s e(-na/q) \ll X^{-\delta 2^{-k}}.$$

Moreover, if $s \geq 2^k + 1$, we have

$$\mathfrak{S}(n) \ll \sum_{q=1}^{\infty} q^{-1-2^{-k}} \ll 1.$$

Singular Integral

Lemma 4 For $\beta \in \mathbb{R}$, we have

$$\nu(\beta) \ll X\left(1 + |\beta| X^k\right)^{-1/k}.$$

If $s \geq k + 1$, we have

$$\mathfrak{J}(n) - \mathfrak{J}(n, X^{\delta-k}) \ll \int_{X^{\delta-k}}^{\infty} \nu(\beta)^s e(-\beta n) d\beta \ll X^{s-k-\delta/k}.$$

Moreover,

$$\mathfrak{J}(n) \ll X^{s-k}.$$

We recall that if $s \geq 2^k + 1$, $0 < \delta < 1/5$ and $X = \lfloor n^{1/k} \rfloor$, then

$$R(n) = \mathfrak{S}(n, X^{\delta})\mathfrak{J}(n, X^{\delta-k}) + o(X^{s-k}).$$

If $s \geq 2^k + 1$, then

$$\mathfrak{S}(n) - \mathfrak{S}(n, X^{\delta}) \ll X^{-\delta 2^{-k}} \quad \text{and} \quad \mathfrak{S}(n) \ll 1.$$

Moreover, if $s \geq k + 1$, we have

$$\mathfrak{J}(n) - \mathfrak{J}(n, X^{\delta-k}) \ll X^{s-k-\delta/k} \quad \text{and} \quad \mathfrak{J}(n) \ll X^{s-k}.$$

Combining the above estimates, we have

Lemma 5 If $s \geq 2^k + 1$, then

$$R(n) = \mathfrak{S}(n)\mathfrak{J}(n) + o(n^{s/k-1}).$$

More about Singular Integral

Lemma 6 If $s \geq k+1$, we have

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

where Γ is the Gamma function defined by $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$.

It follows that if $s \geq 2^k + 1$, then

$$R(n) = \mathfrak{S}(n) \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} + o(n^{s/k-1}).$$

We have seen $\mathfrak{S}(n) \ll 1$. To show that $R(n)$ is of the expected size $n^{s/k-1}$, it remains to show $\mathfrak{S}(n) \gg 1$.

More about Singular Series

Convergence of sums and products

We recall that the singular series

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \left(q^{-1}S(q,a)\right)^s e(-na/q).$$

Define

$$A(q,n) = \sum_{\substack{a=0 \\ \gcd(a,q)=1}}^{q-1} \left(q^{-1}S(q,a)\right)^s e(-na/q).$$

Lemma 7 $A(q,n)$ is a multiplicative function of q.

Define

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

Since $\mathfrak{S}(n) = \sum_{q=1}^{\infty} A(q, n)$ and $A(q, n)$ is multiplicative, we have

Lemma 8 If $s \geq 2^k + 1$, then
(a) $\mathfrak{S}(n) = \prod_p \sigma(p, n)$.
(b) There exists $C = C(k) > 0$ such that

$$\frac{1}{2} < \prod_{p \geq C} \sigma(p, n) < \frac{3}{2}.$$

- To show $\mathfrak{S}(n) \gg 1$, it suffices to show $\sigma(p, n) > 0$ for $p < C$.

p-adic Densities

For $\mathbf{x} = (x_1, \cdots, x_s) \in \mathbb{N}^s$, we recall that

$$R(n) = \#\{\mathbf{x} \in \mathbb{N}^s : n = x_1^k + \cdots + x_s^k\}.$$

For a prime p and $h \in \mathbb{N}$, define $D(p^h, n)$ to be

$$\#\{\mathbf{x} \,(\mathrm{mod}\ p^h) : n \equiv x_1^k + \cdots + x_s^k \pmod{p^h}\},$$

which is expected to be of size $(p^h)^s \cdot p^{-h} = p^{h(s-1)}$.

Given a prime p, define the p-adic density

$$d(p, n) = \lim_{h \to \infty} \frac{D(p^h, n)}{p^{h(s-1)}}.$$

- The limit exists if $s \geq (k+1)$. Moreover, $d(p, n) = \sigma(p, n)$.

Let $\tau = \tau(p, k) \in \mathbb{N} \cup \{0\}$ such that $p^\tau | k$ and $p^{\tau+1} \nmid k$. Define

$$\gamma = \gamma(p, k) = \begin{cases} \tau + 1, & \text{when } p > 2 \text{ or } p = 2 \text{ and } \tau = 0, \\ \tau + 2, & \text{when } p = 2 \text{ and } \tau > 0. \end{cases}$$

Then if $s \geq \min\{4k, 2^k + 1\}$, we have

$$D(p^h, n) \geq (p^{h-\gamma})^{s-1} \quad \Longrightarrow \quad \sigma(p, n) \geq p^{-\gamma(s-1)} > 0.$$

- The lower bound for $\sigma(p, n)$ is independent of n.

Theorem (Hardy-Littlewood & Hua) Let $s, k \in \mathbb{N}$ with $k \geq 2$. If $s \geq 2^k + 1$, then

$$R(n) = \#\{\mathbf{x} \in \mathbb{N}^s : n = x_1^k + \cdots + x_s^k\}$$
$$= \mathfrak{S}(n) \frac{\Gamma(1 + 1/k)^s}{\Gamma(s/k)} n^{s/k-1} + o(n^{s/k-1})$$

with $1 \ll \mathfrak{S}(n) \ll 1$.

Corollary We have

$$G(k) \leq 2^k + 1.$$