# C3.10 Additive and Combinatorial NT
# Lecture 8: Singular series

Joni Teräväinen

Mathematical Institute

# Two identities

In the previous lectures, we proved that

$$r_{k,s}(N) = \mathfrak{S}_{k,s}(N) N^{s/k-1} + o(N^{s/k-1}), \quad s \geq 100^k.$$

In this lecture, we will prove

**Theorem (Singular series)**

For $s \geq k^4$, we have $1 \ll \mathfrak{S}_{k,s}(N) \ll 1$ (i.e., $\mathfrak{S}_{k,s}(N) \asymp 1$).

Recall $\mathfrak{S}_{k,s}(N) = \prod_p \beta_p(N)$, where

$$\beta_p(N) = \lim_{n\to\infty} p^{-(s-1)n} |\{(x_1, ..., x_s) \in \mathbb{Z}/p^n\mathbb{Z} : \ x_1^k + \cdots + x_s^k = N\}|.$$

It suffices to show $\beta_p(N) \gg_{s,k} 1$ and $\beta_p(N) = 1 + O_{s,k}(p^{-1-1/k})$, uniformly in $N$.
Indeed, if we have an infinite product $\prod_{i\geq 1}(1+x_i)$ with $1/C \leq 1 + x_i \leq C$ and $\sum_i |x_i| \leq C$, then $\prod_{i\geq 1}(1+x_i) \asymp_C 1$.

We will need the following simple lemma on lifting congruences.

**Lemma (Hensel's lemma)**

Let $k \geq 2$ and let $p$ be a prime. Let $p^\gamma$ be the highest power of $p$ dividing $k$. Then if $x$ is coprime to $p$ and $x$ is a $k$th power modulo $p^{2\gamma+1}$, $x$ is also a $k$th power modulo $p^n$ for all $n \geq 2\gamma + 1$.

**Proof.** We proceed by induction on $n$, starting from the case $n = 2\gamma + 1$. Suppose that case $n$ has been proved and consider case $n + 1$. Let $x \equiv x_0^k \pmod{p^n}$ and $k_0 = k/p^\gamma$. Now note that

$$\begin{aligned}(x_0 + tp^{n-\gamma})^k &= x_0^k + k_0 x_0^{k-1} tp^n + \binom{k}{2} x_0^{k-2} t^2 p^{2(n-\gamma)} + \cdots \\ &\equiv x_0^k + k_0 x_0^{k-1} p^n t \pmod{p^{n+1}}.\end{aligned}$$

Since $(k_0 x_0^{k-1}, p) = 1$, we can choose $t$ so that this is $\equiv x \pmod{p^{n+1}}$. $\square$

# Lower bounding $\beta_p(N)$

**Proposition 7.1.1**

(i) For $s \geq 2k+1$, we have $\beta_p(N) = 1 + O_{s,k}(p^{-1-1/k})$, uniformly in $N$.
(ii) For $s \geq k^4$, we have $\beta_p(N) \gg_{s,k} 1$, uniformly in $p$ and $N$.

**Proof.** (i) From the previous lecture, we have

$$\beta_p(N) = 1 + \sum_{j \geq 1} A(p^j).$$

In Lecture 6, we proved that $|A(p^j)| \ll_{s,k} p^{-(1+1/k)j}$, so the claim is immediate.

# Lower bounding $\beta_p(N)$

(ii) We claim that $\beta_p(N) \gg_{s,k} 1$ for $s \geq k^4$.
For $p \geq C_{s,k}$, this is true by (i). For the small $p$, it suffices to show that $\beta_p(N) \gg_{p,s,k} 1$.
Let $p^\gamma \mid k$, $p^{\gamma+1} \nmid k$. We first claim that there is at least one solution to

$$y_1^k + \cdots + y_s^k \equiv N \pmod{p^{2\gamma+1}}, \quad y_1 \neq 0.$$

**Case 1:** $\gamma = 0$ and $p \geq k^4$. Then we can simply take $y_4 = \cdots = y_s = 0$ and apply Lemma 5.2.2 (Lecture 5).
**Case 2:** $\gamma = 0$ and $p < k^4$. Then $p < s$, so we may take $y_i \in \{0, 1\}$.
**Case 3:** $\gamma \geq 1$. Then $p^\gamma \mid k$, so $p^{2\gamma+1} \leq k^3 < s$. Therefore, we can take $y_i \in \{0, 1\}$.

Recall we have a solution to

$$y_1^k + \cdots + y_s^k \equiv N \pmod{p^{2\gamma+1}}, \quad y_1 \neq 0.$$

We are left with showing that if $n \geq 2\gamma + 1$, then there are $\geq c_{k,s,p} p^n$ solutions to

$$x_1^k + \cdots + x_s^k \equiv N \pmod{p^n}. \tag{1}$$

Fix $x_2, \ldots, x_s \pmod{p^n}$ such that $x_i \equiv y_i \pmod{p^{2\gamma+1}}$. Then Lemma 7.1.1 shows that $N - x_2^k + \cdots + x_s^k$ is a $k$th power $\pmod{p^n}$.
Therefore, (**??**) has $\geq (p^{n-2\gamma-1})^s$ solutions, so

$$\beta_{p,n}(N) \geq p^{-(2\gamma+1)s}.$$

Thus $\beta_p(N) \geq p^{-(2\gamma+1)s} \gg_{p,s,k} 1$. □

# Summary

As noted earlier, the proof of Proposition 7.1 concludes our proof that $\mathfrak{S}_{k,s}(N) \gg 1$ for $s \geq k^4$.
Combined with the result

$$r_{k,s}(N) = \mathfrak{S}_{k,s}(N)N^{s/k-1} + o(N^{s/k-1}), \quad s \geq 100^k.$$

of the previous lectures, we see that

$$r_{k,s}(N) \gg_{k,s} N^{s/k-1}, \quad s \geq 100^k.$$

This concludes our proof that $G(k) \leq 100^k$, which solves Waring's problem.