18.118 DECOUPLING
LECTURE 15

INSTRUCTOR: LARRY GUTH
TRANSCRIBED BY DONGHAO WANG

We begin our journey to analytic number theory and this lecture is an introduction to the circle method. A good reference for all this material is the book *The Hardy-Littlewood Method* by R. Vaughn.

1. Some classical problems and results

There is a theorem due to Hilbert which asserts any natural number can be written a sum of k-th powers and we can given a uniform bound on the number of k-th powers used:

Theorem 1.1 (Hilbert)**.** *For any $k \geq 2$, there exists $g(k) > 0$ such that $\forall n \in \mathbb{N}$, there is $s \leq g(k)$ and $a_i \in \mathbb{N}, 1 \leq i \leq g(k)$ such that*

$$n = \sum_{i=1}^{s} a_i^k$$

One natural question to ask is the following:

Question 1.2. *Suppose $g(k)$ is the least number of powers to make Theorem* 1.1 *hold. How big is $g(k)$?*

To provide some intuition, take $n = 2^k - 1$. In its decomposition any a_i can't be greater than 1, since $2^k > 2^k - 1$. Therefore, $a_i = 1$ for all i and $g(k) \geq s = 2^k - 1$. The real value of $g(k)$ is only a little worse than that.

Thus, the number $g(k)$ grows at least exponentially with respect to k. However, we have this estimate because some small n force it to be. Instead, one may ask what happens when n is large enough:

Definition 1.3. *Define $G(k)$ to be the smallest s such that for all $n \in \mathbb{N}$ sufficiently large, we can find $a_i \in \mathbb{N}, 1 \leq i \leq s$,*

$$n = \sum_{i=1}^{s} a_i^k$$

Here is what we know about $G(k)$:

Proposition 1.4. $G(k) \geq k + 1$. $G(2) = 4$.

Conjecture 1.5. *$G(k) = k + 1$ for $k \geq 3$.*

Remark 1.6. *Using Pigeonhole argument, one can show $G(k) \geq k$.*

The best known upper bound for $G(k)$ is due to Vinogradov,

Theorem 1.7 (Vinogradov)**.**

$$G(k) \geq Ck \log(k)$$

Another question is in how many ways we can write a natural number a sum of k-th powers.

Definition 1.8. $R_{s,k}(n) = \#\ of\{(a_1, \cdots, a_s) : \sum_i a_i^k = n, a_i \in \mathbb{N}\}$

One may try to estimate $R_{s,k}(n)$, especially to give asymptotic estimate when n is big.

Question 1.9. *Do we expect $R_{s,k}(n)$ to behavior smoothly when n is large?*

We need to reformulate this question a little bit since n is a discrete variable. A better question to ask is whether

$$|R_{s,k}(n+1) - R_{s,k}(n)|$$

is comparable to $|R_{s,k}(n)|$ when n is large. In fact, it is. It is related to its (*mod* p) behavior for some prime numbers p.

Definition 1.10. $R_{s,k}^p(n) := \#\{(a_1, \cdot, a_s) : \sum_i a_i^k \equiv n \mod p, a_i \in \mathbb{Z}_p\}$.

Usually, $R_{s,k}^3(1) \neq R_{s,k}^3(2)$. Suppose that $R_{s,k}^3(1) < R_{s,k}^3(2)$ and choose $n \equiv 1 \mod 3$. Since $n + 1 \equiv 2 \mod 3$, $R_{s,k}(n+1)$ is expected to be greater than $R_{s,k}(n)$ because (*mod* 3) the first question has more solutions. Taking into account of (*mod* p) effect, a reasonable guess should be

$$\frac{R_{s,k}(n+1)}{R_{s,k}(n)} \sim \prod_{p\ prime} \frac{R_{s,k}^p(n+1)}{R_{s,k}^p(n)} \tag{1}$$

This is in fact true if s is large enough comparing to k:

Theorem 1.11 (Hardy-Littlewood)**.** *There is a constant $s_0(k)$ depending on k such that if $s \geq s_0(k)$, then*

$$R_{s,k}(n) \sim (Avg_{|m-n| \leq n^{1-\delta}} R_{s,k}(m)) \cdot \prod_{p=q^l\ q\ prime} \frac{R_{s,k}^p(n)}{p^{s-1}}$$

The term involving the average demonstrates the asymptotic behavior of $R_{s,k}(n)$ for n large. The factor $\frac{R^p_{s,k}(n)}{p^{s-1}}$ is a correction term and it takes into account $(mod\ p)$ effect. The denominator p^{s-1} is the average value of $R^p_{s,k}(n)$ when n takes value in $\mathbb{Z}_p$.

Corollary 1.12. *If $s \geq s_0(k)$, then equation (1) is true.*

When we think of natural numbers, there are absolute norms and p-adic norms. If integers are close in all norms (therefore, close in strong sense), then $R_{s,k}$ is supposed to be close on them.

The next question is how big $s_0(k)$ has to be:

Theorem 1.13 (Hardy-Littlewood-Hua,20's+30's)**.** *Theorem* 1.11 *is true for $s_0(k) = 2^k + 1$.*

Conjecture 1.14. *Theorem* 1.11 *is true for $s_0(k) = k + 1$.*

Remark 1.15. *Conjecture* 1.14 *together with $R^p_{s,k}(n) > 0$ for all n, p will imply Conjecture* 1.5*.*

Theorem 1.16 (Vinogradov,30's)**.** *Theorem* 1.11 *is true for $s_0(k) = Ck^2 \log(k)$.*

Theorem 1.17 (Wooley,90's)**.** *Theorem* 1.11 *is true for $s_0(k) = Ck^2$.*

Theorem 1.18 (Wooely/Decoupling)**.** *Theorem* 1.11 *is true for $s_0(k) = Ck^2$ with a better constant C.*

2. Circle Method

Circle method allows us to express $R_{s,k}(n)$ in terms of Fourier Analysis. Write $e(x) = e^{2\pi ix}$ for short. Let $f_{k,A}(x) := \sum_{a=1}^{A} e(a^k x)$.

Lemma 2.1. *Let $R_{s,k,A}(n) = \#$ of $\{(a_1, \cdots, a_s) : \sum_i a_i^k = n, a_i \in \mathbb{N}, 1 \leq a_i \leq A\}$, then*

$$f^s_{k,A} = \sum_n e(nx) R_{s,k,A}(n).$$

Proof.

$$\begin{aligned} f^s_{k,A} &= \prod_{i=1}^{s} \sum_{a_i=1}^{A} e(a_i^k x) \\ &= \sum_{1 \leq a_1, \cdots, a_s \leq A} e(x \sum_i a_i^k) \\ &= \sum_n e(nx) R_{s,k,A}(n). \end{aligned}$$

□

Remark 2.2. *If $A \geq n^{1/k}$, then $R_{s,k,A}(n) = R_{s,k}(n)$.*

Corollary 2.3.

$$R_{s,k,A}(n) = \int_0^1 f_{k,A}^s(x) e(-nx) dx.$$

Since $f_{k,A}(0) = A$, $f_{k,A}(x) \sim A$ if $|x| < \frac{A^{-k}}{10}$. On the other hand, $\int_0^1 |f_{k,A}(x)|^2 = A$ by Plancherel's identity and by Höler's Inequality,

$$\int_0^1 |f_{s,A}(0)| \leq (\int_0^1 |f_{k,A}(x)|^2)^{1/2} = A^{1/2}$$

Therefore, a naive picture of $|f_{s,A}|$ is that it has a peak of Height A with width A^{-k} at the origin and it is roughly around $A^{1/2}$ with some noise in other region. However, the more accurate picture (but conjectural) is that the graph also has some small peak at rational points

Suppose we are in the naive picture. Then heuristic of Circle method tells us when $A^k = 2n$:

$$\begin{aligned} R_{s,k}(n) &= \int_0^1 f_{k,A}^s(x) e(-nx) \\ &\geq \int_{|x| \leq \frac{1}{10n}} \mathrm{Re}(f_{k,A}^s(x)) \mathrm{Re}(e(-nx)) - \int_{|x| \geq \frac{1}{10n}} \\ &\geq \frac{A^s}{20n} - A^{s/2} \end{aligned}$$

Therefore, we are supposed to get a solution when $s - k > \frac{s}{2}$ and A is large enough. We will need $s \geq 2k + 1$. This is much better than any known result on $G(k)$.

Digression. Suppose we want to study Fermat equation using circle method. Then

$$\#of\{a_1^5 + a_2^5 = a_3^5, 1 \leq a_i \leq A\} = \int_0^1 f_{5,A}^2 \overline{f_{5,A}}$$

However, this method is never useful in the literature. When trying to estimate this integral,

$$|\text{Contribution near } 0| \sim A^{-5} A^2 \sim A^{-2}.$$

$$|\text{Contribution away from } 0| \leq \int |f_{5,A}|^3 \leq A^{3/2}.$$

This will probably allow us to prove only a few solutions might exist since $A^{3/2}$ is relatively smaller than A^2. However, it is not trivial to prove that the naive picture is in fact true here.

Though our naive picture is not right in general, $f_{s,A}(x) \sim A^{1/2}$ still holds when x is away from rational points. We need to characterize this property carefully. Let

$$D_{c,\epsilon} = \{x \in [0,1] : |x - \frac{p}{q}| \geq cq^{-2-\epsilon}, \forall\ \frac{p}{q} \in \mathbb{Q}, 1 \leq p \leq q\}.$$

It is a measure theory exercise to show that

$$m([0,1] - D_{c,\epsilon}) \leq \sum_{1 \leq p \leq q} cq^{-2-\epsilon} \leq c'\epsilon^{-1}.$$

and for fixed c, $\lim_{\epsilon \to 0} m(D_{c,\epsilon}) = 1$.

Theorem 2.4 (Weyl)**.** *If $x \in D_{c,\epsilon}$, $|f_{k,A}(x)| \leq A^{1-2^{1-k}+\epsilon}$ for some $C = C(c, \epsilon, k)$.*

Let's think about what this theorem says when k is small (for ($x \in D_{c,\epsilon}$)):

- $k = 1$. $|f| \lesssim A^{\epsilon}$.
- $k = 2$. $|f| \lesssim A^{1/2+\epsilon}$.
- $k = 3$. $|f| \lesssim A^{3/4+\epsilon}$.
- $k = 4$. $|f| \lesssim A^{7/8+\epsilon}$.

Except for the first two estimates, the rest may be far from sharp.

Proof for k=1.

$$\begin{aligned} |\sum_{a=1}^{A} e(ax)| &= |\sum_{a=0}^{A-1} e(ax)| \\ &= |\frac{1 - e(Ax)}{1 - e(x)}| \\ &\lesssim |1 - e(x)|^{-1} \\ &\lesssim \|x\|^{-1} \\ &\lesssim c^{-1} \end{aligned}$$

Here, we denote $\|x\| = dist(x, \mathbb{Z})$. We take $q = 1$ in the definition of $D_{c,\epsilon}$, then $x \in D_{c,\epsilon}$ implies $\|x\| \leq c^{-1}$. □

Proof for k=2.

$$|\sum_{a=1}^{A} e(a^2x)|^2 = \sum_{a,b=1}^{A} e((a^2 - b^2)x)$$

We shall make linear change of variable $a = b + h$. Then

$$RHS = \sum_{b=1}^{A} \sum_{h=1-b}^{A-b} e(h(2b+h)x)$$

If we look at h, the summation is as bad as the original problem. But if we look at b, it is a geometric sum. Then,

$$\begin{aligned} |\sum_{a=1}^{A} e(ax)|^2 &\leq \sum_{h=-(A-1)}^{(A-1)} |\sum_{b=\max\{1-h,1\}}^{min\{A-h,A\}} e(h(2b+h)x)| \\ &\leq \sum_{h=-(A-1)}^{(A-1)} |\sum_{b=\max\{1-h,1\}}^{min\{A-h,A\}} e(2bhx)| \\ &\lesssim \sum_{h=-(A-1)}^{(A-1)} \|2hx\|^{-1} \end{aligned}$$

Since $x \in D_{c,\epsilon}$,

$$|2hx - p| = 2|h||x - \frac{p}{2h}| \geq 2|h|^{-(1+\epsilon)}.$$

Therefore, for some $C > 0$,

$$\|2hx\|^{-1} \leq C|h|^{1+\epsilon}$$

If we directly plug this expression in above, we will get

$$|f_{2,A}|^2 \lesssim \sum_{|h|\leq A} |h|^{1+\epsilon} \sim A^{2+\epsilon}$$

This is not a good estimate because triangular inequality directly tells us

$$|f_{2,A}|^2 \leq A^2$$

The point is that $\|hx\|^{-1}$ is large when hx is close to an integer and but it is not close to integers for all h. For fixed x, let

$$H(\lambda) = \{h \in \mathbb{Z} : |h| \leq A, \lambda \leq \|2hx\|^{-1} \leq 2\lambda\}$$

and we shall write $H_m = H(2^{m-1})$ for short. Take m to be the least integer such that $CA^{1+\epsilon} \leq 2^m$, then

$$H_1, H_2, \cdots, H_m$$

are all non-empty sets here. Therefore,

$$\sum_{h=-(A-1)}^{(A-1)} \|2hx\|^{-1} \leq \sum_{n=1}^{m} 2^n |H_n| \tag{2}$$

The naive attempt takes $|H_m| = 2A$ and $|H_n| = 0$ for other n. But this is not so clever. If $h_1 \neq h_2 \in H(\lambda)$, then

$$\lambda \leq \|2h_1 x\|^{-1}, \|2h_2 x\|^{-1} \leq 2\lambda$$

This shows

$$\|2(h_1 - h_2)x\| \leq \frac{2}{\lambda}.$$

and

$$\frac{\lambda}{2} \leq \|2(h_1 - h_2)x\|^{-1} \leq C|h_1 - h_2|^{1+\epsilon}$$

$$(\frac{\lambda}{2C})^{1/(1+\epsilon)} \leq |h_1 - h_2|.$$

This shows any two integers in $H(\lambda)$ cannot be too close to each other. Hence,

$$|H(\lambda)| \leq A/(\frac{\lambda}{2C})^{1/(1+\epsilon)} \lesssim A\lambda^{\epsilon-1}.$$

Plug this estimate into equation 2, we get

$$\begin{aligned}
\sum_{h=-(A-1)}^{(A-1)} \|2hx\|^{-1} &\leq \sum_{n=1}^{m} 2^n |H_n| \\
&\leq \sum_{n=1}^{m} 2^n (2^{n-1})^{\epsilon-1} A \\
&\leq \sum_{n=1}^{m} 2A \cdot 2^{\epsilon(n-1)} \\
&\leq 2mA \cdot 2^{(m-1)\epsilon} \\
&\lesssim A^{1+\epsilon}
\end{aligned}$$

This shows $|f_{2,A}|^2 \lesssim A^{1+\epsilon}$ and hence $|f_{2,A}| \lesssim A^{1/2+O(\epsilon)}$. □

The proof for higher k is postponed to the next lecture.