[Math Seminar] Lecture 1 Notes

Connor Li, csl2192

February 7, 2024

1 Top Level

- [H] 1.6, 1.7, 2.4 over the following topics: Thin Sets of Squares, Polygonal Number Theorem, Sums of Two Cubes
- Structure of the Lecture follows the textbook

2 Quantitative Estimates

2.1 Overview

- Quantitative estimates in additive number theory are mathematical calculations that provide numerical bounds or approximations for various properties and behaviors of numbers, particularly integers.
  - "How many primes are up to x?"
  - Greatest Prime Factor Bound: there exists a prime factor of x (a composite integer) that is at most $\sqrt{x}$.
- Proofs involve analysis, combinatorics, algebra
- Practical implications in areas like cryptography, CS, and mathematical modeling

2.2 Gaussian Sum

Theorem: Find an estimator for sum of the first n positive integers.

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n$$

Proof: Following Gauss's genius, arrange all the numbers from 1 to n in a line. Then, directly below the line, arrange the numbers from n to 1 in reverse order.

1	2	3	...	n-1	n
n	n-1	n-2	...	2	1

Notice, each vertical pair of numbers sums to $n+1$, and there are n such pairs of numbers. Since each number is counted twice, Gauss deduced the following formula for the sum of the numbers.

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

- Most of time, we can get estimators/bounds with error terms (instead of exact values) like the Gaussian sum

2.3 Introducing the Basis

Definition: A is a *basis of order h for N* if:

1. A is a finite set of non-negative integers
2. Every integer $x \in \mathbb{Z}$ (where $0 \leqslant x \leqslant N$) can be written as the sum of h elements of A, with repetitions allowed

Example: Define $A = \{0, 1, 2, 3\}$. A is a basis of order 3 for $N = 9$, since every integer from 0 to 9 can be written as $a_1 + a_2 + a_3$ where $a_i \in A$.

Corollary (1): $|A| \geqslant 1$. Since A must be able to sum to 0 and all integers are defined as non-negative, then the $\{0\} \in A$.

Corollary (2): If A is a basis of order h for N, then A is a basis of order $h+1$ for N.

2.4 Bounding the Basis

- Definition is important because you want to provide "quantitative estimates" on the cardinality of some basis A.
- You want to figure out the minimum number of elements needed in A to be able to satisfy the definition of basis.

Theorem: Let $h \geqslant 2$. There exists a positive constant $c = c(h)$ such that, if A is a basis of order h for N, then

$$|A| > cN^{\frac{1}{h}}$$

Proof: Define $|A| = k$. That means, the number of combinations of h elements from A (with repetitions) is a simple combination/permutation problem. If we treat one of these combinations as a distinct sum (which it probably isn't), then we have an upper bound on $N + 1$ since it includes 0.

$$N + 1 \leqslant \binom{k+h-1}{h} = \frac{k(k+1)\cdots(k+h-1)}{h!} \leqslant \frac{c_0 k^h}{h!}$$

Change of variables $c = \left(\frac{h!}{c_0}\right)^{\frac{1}{h}}$ and $k = |A|$.

$$N < \frac{c_0 k^h}{h!} \implies k > \left(\frac{h!N}{c_0}\right)^{\frac{1}{h}} \implies |A| > cN^{\frac{1}{h}}$$

Note: Why are we allowed to simply state that there exists some c_0 such that $c_0 k^h \geqslant k^h +$lower order terms? This is because of dominance of higher degree terms in polynomials. Also, known as big O notiation.

2.5 Bound for Basis of Squares

Remember the following formula from Jinoo's lecture:

Theorem: Every natural number can be represented as a sum of four non-negative integer squares.

- The collection of all squares forms a basis of order 4 for the integers.
- From the above bound, we have $cN^{\frac{1}{4}}$, but we can find a tighter bound. Define $|Q_N|$ as the set of squares up to N.

$$|Q_N| = \left\lfloor \sqrt{N} \right\rfloor + 1 > N^{\frac{1}{2}}$$

- This allows us to ask if this trend is continued writ large, i.e. if there's a better quantitative estimate for the growth rate of A_N with respect to N?

Question: We ask that if A_N represents the basis of order 4 for N, if

$$\lim_{N\to\infty} \frac{|A_N|}{N^{\frac{1}{2}}} = 0$$

2.6 Choi-Erdos-Nathanson Theorem

If this theorem holds true, then we can conclude that there does exist such an A_N as a result to the above question in Section 3.5.

$$\lim_{N\to\infty} \frac{|A_N|}{N^{\frac{1}{2}}} \leqslant \frac{4}{\log 2} \cdot \left(\lim_{N\to\infty} \frac{N^{\frac{1}{3}} \log N}{N^{\frac{1}{2}}} \right) = 0$$

Proof: The sets $A_2 = A_3 = \{0, 1\}$ and $A_4 = A_5 = \{0, 1, 4\}$ all satisfy the theorem (this you can check for yourself). So, for this proof, we will focus on the scenario where $N \geqslant 6$.

We start by defining 2 sets. Notice that the careful choosing of these sets is what gives us the $N^{\frac{1}{3}}$ bound in the theorem statement. $A_N^{(1)}$ which consists of all the squares of positive integers up to $2N^{\frac{1}{3}}$. We know, that at maximum, the cardinality of $A_N^{(1)}$ is

$$|A_N^{(1)}| \leqslant 2N^{\frac{1}{3}} + 1$$

Now define $A_N^{(2)}$ which contains all the squares of the integers of form $\left[k^{\frac{1}{2}} N^{\frac{1}{3}}\right]$ or $\left[k^{\frac{1}{2}} N^{\frac{1}{3}}\right] - 1$ where $4 \leqslant k \leqslant N^{\frac{1}{3}}$. This means that the cardinality of $A_N^{(2)}$ is upper-bounded by

$$|A_N^{(2)}| \leqslant 2(N^{\frac{1}{3}} - 3) = 2N^{\frac{1}{3}} - 6.$$

If we define some union of these two sets $A_N^{(0)}$ such that $A_N^{(0)} = A_N^{(1)} \cup A_N^{(2)}$, then we set the upper-bound as

$$|A_N^{(0)}| < 4N^{\frac{1}{3}}$$

By Lagrange's Theorem (from Avi's lecture) and the fact that our set contains every square up to $4N^{\frac{2}{3}}$, we know that every non-negative integer up to the nearest integer $4N^{\frac{2}{3}}$ can be expressed as the sum of four squares in $A_N^{(0)}$ by how we defined the set. Thus, we just have to prove that all integers between $4N^{\frac{2}{3}}$ and N can be expressed as the sum of four squares in $A_N^{(0)}$.

Now, a key takeaway from Jinoo's lecture is that if ℓ is a non-negative integer and $\ell \equiv 1$ or 2 (mod 4), then ℓ is the sum of three squares (which also means that it is the sum of four squares including 0). Since the square of an even integer is 0 mod 4 and the square of an odd integer is 1 mod 4, then we have can deduce the following. If some integer $m \not\equiv 0$ mod 4 and a is any positive integer such that

$a^2 \leqslant m$, then either $m - a^2$ or $m - (a-1)^2$ is the sum of three squares. This is because m must equal $1, 2, 3 \bmod 4$ and a^2 or $(a-1)^2$ must equal $0, 1 \bmod 4$. So in each case, you are able to reduce $m - a^2$ or $m - (a-1)^2$ to some ℓ such that $\ell \equiv 1$ or $2 \bmod 4$, which is also the sum of three squares.

As a result, we simply need to prove that for any $m \in \mathbb{Z}$ such that $4N^{\frac{2}{3}} < m \leqslant N$ and $m \not\equiv 0 \bmod 4$, then $m - a_0^2$ is the sum of three squares in $A_N^{(0)}$. Keep in mind, that we can ignore the case where $m \equiv 0 \bmod 4$ via the blurb at the end of Jinoo's lecture, since $(2x_1)^2 + (2x_2)^2 + (2x_3)^2 + (2x_4)^2 = 4(x_1^2 + x_2^2 + x_3^2 + x_4^2)$, which means we can keep factoring out 2's until it reduces to a scenario where $m \not\equiv 0 \bmod 4$ or $m < 4N^{\frac{1}{3}}$.

So, the goal is to prove that an integer $a_0 \in A_N^{(2)}$ exists such that $0 \leqslant m - a_0^2 \leqslant 4N^{\frac{2}{3}}$ and $m - a_0^2$ is the sum of three squares. Start by defining some term a such that $a^2, (a-1)^2 \in A_N^{(2)}$. To do this, define k as follows.

$$4N^{\frac{2}{3}} < m \leqslant N \implies 4 \leqslant k = \left[\frac{m}{N^{\frac{2}{3}}}\right] \leqslant N^{\frac{1}{3}}$$

Once you've defined such a k, set the following value for a so that its corresponding squares are in the desired set.

$$a = \left[k^{\frac{1}{2}} N^{\frac{1}{3}}\right] \implies a^2, (a-1)^2 \in A_N^{(2)}$$

Since we are dealing with "the closest integers", we can deduce the following results as well.

$$a^2 \leqslant kN^{\frac{2}{3}} \leqslant m < (k+1)N^{\frac{2}{3}} \quad \text{and} \quad a > k^{\frac{1}{2}} N^{\frac{1}{3}} - 1$$

This is useful because we can now pick some $a_0^2 \in \{(a-1)^2, a^2\}$ such that $m - a_0^2$ is a sum of three squares from our earlier remark that is also in the set $A_N^{(1)}$. Now, we know that if $m \not\equiv 0 \bmod 4$ and $0 \leqslant m \leqslant N$, then m is a sum of four squares.

The last check we need to do is for the scenario where $m \equiv 0 \bmod 4$. Remember that we can divide out powers of 2^i until we reach some familiar m, then apply the logic above. However, to account for that division, we need to explicitly construct the set A_N as follows.

$$A_N = \left\{(2^i a)^2 : 0 \leqslant i \leqslant \log_4(N) \quad \text{and} \quad a \in A_N^{(0)}\right\}$$

This way, we can account for all m, and we simply have to solidify the logic for our bound. An important note is the constructed $A_N^{(0)}$ is a subset of this A_N.

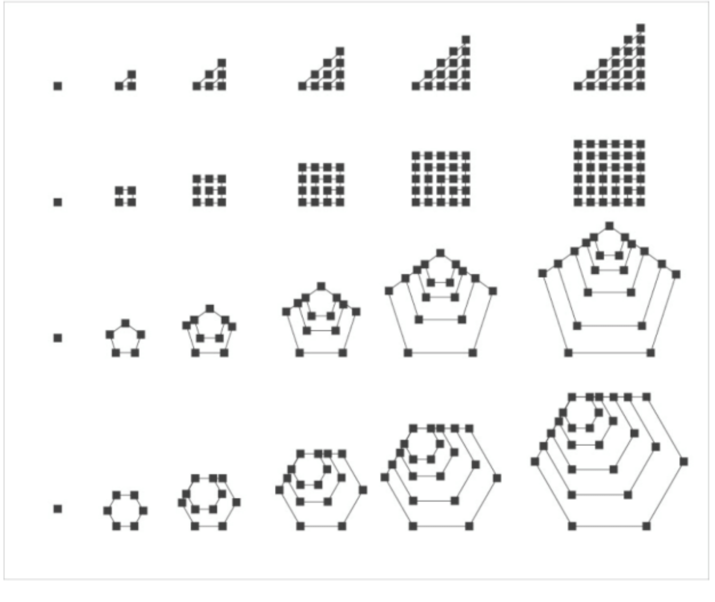
$$|A_N| \leqslant (\log_4(N) + 1)\,|AN^{(0)}| < (2\log_4(N))\,|AN^{(0)}| = \frac{4}{\log(2)} N^{\frac{1}{3}} \log(N)$$

3 Polygonal Number Theorem

3.1 Introduction

Square integers are consider quadrilateral numbers. Now, let's talk about other n-gonal numbers.

3.2 Visual Understanding



3.3 Triangle Theorem

Theorem: Every nonnegative integer is the sum of three triangles.

Proof: To prove the result, it is sufficient to prove that every positive integer $8N+3$ can be expressed as a sum of three odd squares via a theorem from Jinoo's lecture.

$$\begin{aligned} 8N+3 &= (2k_1+1)^2 + (2k_2+1)^2 + (2k_3+1)^2 \\ &= 4(k_1^2+k_2^2+k_3^2+k_1+k_2+k_3)+3 \end{aligned}$$

Rearranging the terms, we have the following result.

$$N = \frac{k_1(k_1+1)}{2} + \frac{k_2(k_2+1)}{2} + \frac{k_3(k_3+1)}{2}$$

This completes the proof of every N being able to be expressed as the sum of 3 triangular numbers.

3.4 Constructing Intervals

- Specifically, the formula for the kth polygonal number of order $m+2$ for $m \geqslant 3$ is

$$p_m(k) = \frac{m \cdot k(k-1)}{2} + k$$

- Using this formula, our goal is construct a basis of order h for any integer N using the polygonal numbers. Essentially, we want to be able to express the integers from 0 to N as the sum of h-gonal numbers all of order $m+2$.
- Let's imagine $k_1, \ldots, k_s$ are positive integers. Then for $r \in [0, m+2-s]$ where $r \in \mathbb{Z}$, we have that the following linear combination of polygonal numbers (of order $m+2$) creates an interval of $m+3-s$ consecutive integers.

$$p_m(k_1) + p_m(k_2) + \cdots + p_m(k_s) + rp_m(1)$$

- Look in Section 4.4, but you can construct intervals of length $m-2$.

Expression	Min Range	Max Range
$rp_m(1)$	0	$m+2$
$p_m(2)+rp_m(1)$	$m+2$	$2m+3$
$2p_m(2)+rp_m(1)$	$2m+3$	$3m+4$
$\vdots$	$\vdots$	$\vdots$
$p_m(5)+p_m(2)+rp_m(1)$	$11m+7$	$12m+8$

- Two more important theorems for $N > 120m$ since the extension of the table only applies there. Look in the notes to find out more, but there are good or close upper bounds on those.

4 Sums of Two Cubes

4.1 Precursors

- Remember from last lecture $G(3)$, which is the the smallest number of cubes such that any sufficiently large nonnegative integer can be written as a sum of cubes.
- $r_{3,2}(N)$ is the number of ways to write 2 cubes as points (x, y) for any sum N
- N has two distinct representations if $r_{3,2}(N) \geqslant 3$.
- $1729 = 1^3 + 12^3 = 9^3 + 10^3$ is the smallest number with two distinct representations.
- $87,539,319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3$

We will present 3 theorems and a corollary related to this.

4.2 Fermat's Theorem

In this section, we will present three theorems on the sums of two cubes.

Fermat's Result: The first is Fermat's result that there are integers with arbitrarily many representations as the sum of two cubes.

$$\lim_{N\to\infty} r_{3,2}(N) = \infty$$

Proof: Involves defining x_1, y_1 as rational numbers. Then, you prove that for a large enough N, there must exists some x_2, y_2 such that $N = x_1^3 + y_1^3 = x_2^3 + y_2^3$. Repeating iterations with increasing x_i, y_i approaching the bound for x_1, y_1 you get that there are infinitely many representations of N as a cubic.

The next step to prove that these are pairwise independnet is a little more complicated, but it's a proof by contradiction using the bounds.

Finally, you turn the rational x_i, y_i from $i = 1, \ldots, k$ into natural numbers by multiplying them by a common denominator, which completes your proof.

4.3 Other Theorems

Erdos & Mahler's Theorem: First, define $C_2(n)$ to be the number of integers up to n that can be represented as the sum of two positive cube. We can then upperbound $Q(n)$, which represents the number of cubes up to n, by the following $Q(n) < n^{\frac{1}{3}}$. This allows us to bound $C_2(n) < n^{\frac{1}{3}} \cdot n^{\frac{1}{3}} = n^{\frac{2}{3}}$.

This theorem then states that the growth rate of $C_2(n)$ is captured asymptopically by $n^{\frac{2}{3}}$. More formally, this means that there exists some c such that for all $n > n_0$, we have that $C_2(n) < c \cdot n^{\frac{2}{3}}$.

$$C_2(n) = \sum_{\substack{N \leqslant n \\ r_{3,2}(N) \geqslant 1}} 1 \gg n^{\frac{2}{3}}$$

Hooley-Wooley's Theorem: If $C_2^*(n)$ is the number of integers up to n with two distinct representations, then the following is true.

$$C_2^*(n) \ll n^{\frac{5}{9}+\epsilon}$$

All three theorems relate to the same flavor or topic that we've been convering throughout the lecture, one related to a quantitative estimate over a difficult counting problem related to additive number theory. That being said, let's jump into the proofs.

4.4 Last Corollary

All integers that can be represented as the sum of two positive cubes have essentially only one such representation. This follow directly from the Erdos Mahler theorem that states that there are at least $cn^{\frac{2}{3}}$ integers that can be expressed as the sum of two cubes, whereas the maximum number of integers expressed as two nonnegative cubes is only $c'n^{\frac{5}{9}+\epsilon}$.

$$\lim_{n\to\infty} \frac{cn^{\frac{2}{3}}}{c'n^{\frac{5}{9}+\epsilon}} = \infty$$