# [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.

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

**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.

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  $0 \le x \le N$ ) 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):  $|A| \ge 1$ . 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  $h \ge 2$ . 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.

$$N+1 \leqslant {k+h-1 \choose h} = \frac{k(k+1)\cdots(k+h-1)}{h!} \leqslant \frac{c_0k^h}{h!}$$

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

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

<u>Note</u>: Why are we allowed to simply state that there exists some  $c_0$  such that  $c_0k^h \ge k^h$  + 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.

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