[Math Seminar] Quantitative Estimates & Sums of Two Cubes

Connor Li, csl2192

February 7, 2024

Contents

1 Overview

This document will outline notes for the talk in the Additive Number Theory Math Seminar Section headed by Avi Zeff. The topic of this lecture is 'Quantitative Estimates & Sums of Two Cubes'. The chapters (1.6, 1.7, 2.4) in reference for this talk are from [H] Nathanson, Melvyn B. *Additive number theory.* New York: Springer, 1996. For questions or corrections to the notes, please email (csl2192@columbia.edu).

- (H. 1.6) Thin Sets of Squares
- (H. 1.7) The Polygonal Number Theorem
- (H 2.4) Sums of two cubes

2 Top Level

In this talk, we build off of results from the previous lectures by Jinoo and Keila. For links to those, please visit these websites:

1. Quadratic forms and sums of three squares (Jinoo)
    - Lecture
    - Notes
2. Waring's problem for cubes (Keila)
    - Lecture
    - Notes

For a link to the main seminar website, please click here.

3 Quantitative Estimates

3.1 Introduction

In this section, we want to answer the question: what are quantitative estimates?

At the highest level, quantitative estimates in additive number theory are mathematical calculations that provide numerical bounds or approximations for various properties and behaviors of numbers, particularly integers. Now, this definition may seem abstract, so let's put it into more concrete terms.

One of the most popular examples of how quantitative estimates are used is in the distribution of special sets of numbers. Specifically, an important part of number theory is to prove the estimator function for how primes are distributed among the natural numbers. Simply put, it answers the question of "how many primes are there up to some number x?" But if that's not interesting enough for you, another great example is the Greatest Prime Factor bound for composite numbers which states that, for some non-prime integer x, there exists some prime factor of x that is at most $\sqrt{x}$. And later in the course, we will see other bounds like estimates for the Riemann Zeta function, Elliptic Curves, and Waring's Problem.

What's even cooler about quantitative estimates is that they lie in the intersection of the different fields of mathematics. They often involve a variety techniques including analysis, algebra, combinatorics, and probability theory, showcasing the interdisciplinary nature of (additive) number theory. But, don't worry... they're not just theoretical! In fact, quantitative estimates have practical implications in areas like cryptography, computer science, and mathematical modeling.

3.2 Gaussian Sum

To show you an example of quantitative estimates and the according proof structure, let's start with the following (famous) exercise.

Exercise: Find a formula/estimator for the sum of the first n positive integers.

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.

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

Although this is probably a familiar proof, it gives the idea of the bound/exact formula that we are searching for when we approach problems in the rest of the section about estimators. Oftentimes, we can't get an exact formula like here, so boundedness (and a quantifiable error) is something that mathematicians strives for instead!

3.3 Basis of order h

Before we introduce some of the more complicated estimates in Nathanson, we should provide the following definition that will be used consistently throughout the notes.

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 $A = \{0, 1, 2, 3\}$. We can say that 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 $a_i \in A$ and a_i does not necessarily need to be distinct. The integer 7 can be written as $1 + 3 + 3$ and the integer 2 can be written as $0 + 0 + 2$.

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. This is simply because you can add the 0-element any number of additional times to create the same result. Similarly, if A is a basis of order h for N, then A is basis of order $h+1$ for $N-1$ as long as $N - 1 > 0$.

3.4 Bounding the Basis

The reason why the above definition is important is because you want to provide "quantitative estimates" on the cardinality of some basis A. Essentially, you want to figure out the minimum number of elements needed in A to be able to satisfy the definition of basis. How many elements do I need in A to guarantee that some combination of h elements in A can create every integer from 0 to N?

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 the number of distinct elements in $|A| = k$. That means, the number of combinations of h elements from A (with repetitions) is a simple combination. 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.

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

This is true for some constant $c_0 > 0$ and for all k, so we can complete the proof by a 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: You may asking yourself, 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. An easier example to understand is the existence of some c_0 such that $c_0 x^4 \geqslant x^4 + x^3 + 2x^2 + 1$ since the lower order terms become negligent as $x \to \infty$.

3.5 Is there a Bound for the Basis of Squares?

The above theorem tells you the lower bound for the cardinality of A. Now, remember earlier in the course when we introduced the following theorem (covered also briefly by Jinoo in his lecture).

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

This means that the collection of squares form a basis of order 4, since you can create any integer N from the sum of four squares. More formally, we have that the set of all squares Q_N up to some number $N \geqslant 0$ is a basis of order 4 for N. Since there are a maximum of $\sqrt{N}$ terms in Q_N, then we have that

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

This is a more accurate lower bound than $cN^{\frac{1}{4}}$, as implied by the above section. Using a similar line of reasoning, the next question we want to answer is about a generalization of basis of squares with order 4 for any integer N.

Question: For every $N \geqslant 0$, does there exists some basis A_N of squares with order 4 that satisfies the following condition.

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

Note: This is different from the lower bound above, because we are asking about a minimal set of squares, not all squares up to N!

To answer this question, we will employ the following theorem (Choi-Erdos-Nathanson).

3.6 Choi-Erdos-Nathanson

Before I explain why this is important to answer the question above, let's state the theorem.

Theorem: For every $N \geqslant 2$, there exists a basis A_N of order 4 for N such that

$$|A_N| \leqslant \left(\frac{4}{\log 2} N^{\frac{1}{3}} \log N\right)$$

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 $\left\lfloor k^{\frac{1}{2}} N^{\frac{1}{3}} \right\rfloor$ or $\left\lfloor k^{\frac{1}{2}} N^{\frac{1}{3}} \right\rfloor - 1$ 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 $2 \pmod 4$, 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 $m \not\equiv 0 \bmod 4$ 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.

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

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

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

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.

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

4 The Polygonal Number Theorem

4.1 Introduction

Earlier, we learned about how 4 square integers can form a basis of order 4 for any integer N. Now, we want to generalize this idea to other types of 'shaped' numbers. The Polygonal Number Theorem is a result that generalizes the idea of a basis of order h for any integer N to the set of all h-gonal numbers. And although this may sound confusing, let's start with triangle numbers.

4.2 Definition of Triangle Numbers

According to Gauss, a triangle number is a number that can be expressed as the sum of the first n natural numbers. In other words, the nth triangle number is the sum of the first n natural numbers. However, a more intuitive formula based on the Gaussian sum from above is any integer n that can be expressed as the following given $k \in \mathbb{Z}^+$.

$$n = \frac{k(k+1)}{2}$$

Now, let's prove an important theorem about triangle numbers. Another way to state this is that triangular numbers form a basis of order three for the integers.

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.

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

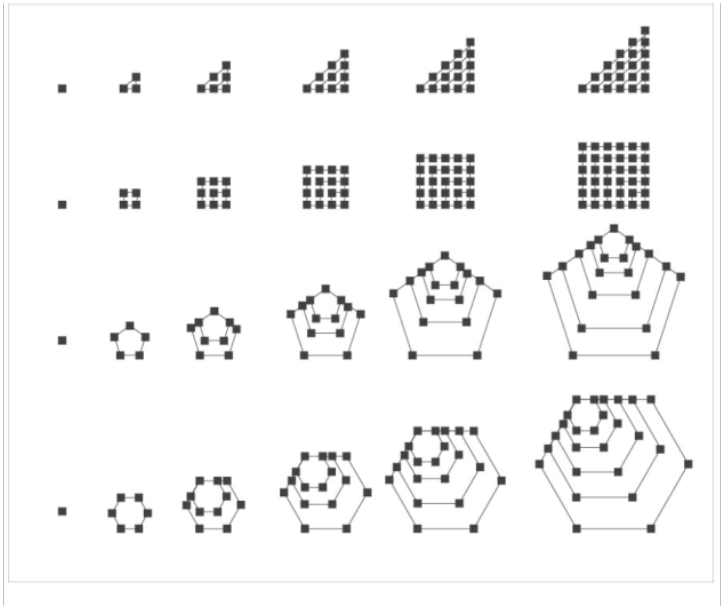
Rearranging the terms, we have the following result.

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

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

4.3 Higher-Order Polygonal Numbers

Langrange's Theorem is the polygonal number theorem for squares and Gauss's Theorem above is the polygonal number theorem for triangles. However, before we jump into the theorems, let's focus on what polygonal numbers are. Below is a good visual for how polygonal numbers evolve.



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 $m + 2$.

4.4 N-gonal Number Theorem

Like we said above, we want to be able to do something similar with n-gon numbers as we did with squares and triangle numbers. To do so, 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.

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

This may seem very abstract in practice, so let me provide you with some more concrete examples. Take $rp_m(1)$. We know that $r \in [0, m+2-s]$, so we can express the whole range of integers from 0 to $m+2$ are different variations of $rp_m(1)$. Similarly, take $p_m(2) + rp_m(1)$. This specific linear combination can express the range of integers from $m+2$ to $2m+3$. If we continue to expand this list, we have the following table.

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

The table is not very difficult to extend, and Pepin[95] and Dickon[23] have published tables of representations of N as sum of $m+2$ polygonal numbers for all $m \geqslant 3$ and $N \leqslant 120m$. And although you can prove the case where $N > 120$, the proof is quite complicated and requires a lot of setup. If you are interested in the proof, please reference section [H] 1.7 for more information.

4.5 Important Theorems

Regarding the N-gonal number theorems, although we won't explicitly cover the proofs, I think it's worth mentioning a couple of important theorems and conclusions. Similar to our goal, these theorems set upper-bounds on the order of the summation of polygonal numbers as a basis for some number N. Simply put, they bound the minimum number of $m+2$ polygonal numbers needed to sum to every integer from 0 to N.

Theorem (Cauchy): If $m \geqslant 4$ and $N \geqslant 108m$, then N can be written as the sum of $m+1$ polygonal numbers of order $m+2$, at most four of which are different from 0 or 1. If $N \geqslant 324$, then N can be written as the sum of five pentagonal numbesr, at least one of which is 0 or 1.

Proof: For the proof, reference [H] 1.7 Page 32.

Theorem (Legendre): Let $m \geqslant 3$ and $N \geqslant 28m^3$. If m is odd, then N is the sum of four polygonal numbers of order $m+2$. If m is even, then N is the sum of five polygonal numbers of order $m+2$, at least one of which if 0 or 1.

Proof: For the proof, reference [H] 1.7 Page 33.

5 Sums of Two Cubes

5.1 Precursors

Similar to Keila's talk last week, we want to explore the idea of sums of cubes. Related to the unsolved $G(3)$ problem, which is the the smallest number of cubes such that any sufficiently large nonnegative integer can be written as a sum. But before we dive into the technicalities, it's important to clarify some terminology.

First, $r_{3,2}(N)$ denotes the number of representations of the integer N as the sum of 2 positive cubes. If $N = x^3 + y^3$ and $x \neq y$, then we say that $N = y^3 + x^3$ is another representation of N as the sum of two cubes.

We consider a representation as essentially distinct from another if they cannot be transformed into each other by simply reordering the terms or applying basic algebraic identities. It's also important to remember that N has two distnct representation iff $r_{3,2}(N) \geqslant 3$.

For example, 1729 is the smallest number that has two essentially distinct representations as the sum of two positive cubes.

$$1729 = 1^3 + 12^3 = 9^3 + 10^3$$

These also correspond to four positive integral points on the curve $1729 = x^3 + y^3$, which gives that $r_{3,2}(1729) = 4$. The smallest number that has three distinct representations is $87,539,319$.

$$87,539,319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3$$

5.2 Introduction to Theorems

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.

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

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.

5.3 Fermat's Theorem

Theorem: For every $k \geqslant 1$, there exists an integer N and k pairwise disjoint sets of positive $\{x_i, y_i\}$ such that $N = x_i^3 + y_i^3$ for all i. Equivalently,

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

The idea of the proof is to define some large number N that satisfies the $N = x_1^3 + y_1^3$ condition, and show that there exists (x_k, y_k) that also satisfiy the sum of two cubes. Then, we simply have to show that these are disjoint to complete the proof.

Proof: First, let's define two functions over variables x, y.

$$f(x,y) = \frac{x(x^3 + 2y^3)}{x^3 - y^3} \qquad g(x,y) = \frac{y(2x^3 + y^3)}{x^3 - y^3}$$

The reason why we've picked these two functions is because they satisfy the identity

$$f(x,y)^3 - g(x,y)^3 = x^3 + y^3$$

Similarly, define another set of functions over variables u, v.

$$F(u,v) = \frac{u(u^3 - 2v^3)}{u^3 + v^3} = f(u,-v) \qquad G(u,v) = \frac{v(2u^3 - v^3)}{u^3 + v^3} = g(u,-v)$$

These functions satisfy the identity that

$$F(u,v)^3 + G(u,v)^3 = u^3 - v^3 = f(u,-v)^3 - g(u,-v)^3$$

Proof (continued): Now, define $0 < \epsilon < \frac{1}{4}$. Then, for some $0 < x_1, y_1 \in \mathbb{R}$, define $0 < \rho = \frac{y_1}{x_1} < \epsilon$. Finally, define

$$\left.\begin{aligned} u &= f(x_1, y_1) \\ v &= g(x_1, y_1) \end{aligned}\right\} \implies u^3 - v^3 = x_1^3 + y_1^3 > 0$$

Based on our definition of ρ, we are able to create an expression for $\frac{u}{v}$ via algebraic manipulation.

$$\frac{u}{v} = \frac{x_1}{2y_1}\left(\frac{1 + 2\rho^3}{1 + \frac{\rho^3}{2}}\right)$$

We can also bound the right term of the product by the following inequality in order to eventually bound

$$1 < \frac{1 + 2\rho^3}{1 + \frac{\rho^3}{2}} = 1 + \frac{3\rho^3}{2 + \rho^3} < 1 + \frac{3\rho^3}{2}$$

This allows us to bound the $\frac{u}{v}$ term as well as the relationship between (u, v) and (x_1, y_1), keep this in mind for later.

$$0 < \frac{u}{v} - \frac{x_1}{2y_1} < \frac{3}{4}\left(\frac{y_1}{x_1}\right)^2 < \frac{3\epsilon^2}{4} \implies \frac{u}{v} > \frac{x_1}{2y_1} > \frac{1}{2\epsilon} > 2$$

Next, we define $x_2 = F(u, v)$ and $y_2 = G(u, v)$. Then, we can show that $x_2^3 + y_2^3 = u^3 - v^3 = x_1^3 + y_1^3$. Now, define some $\sigma = \frac{u}{v}$ such that $0 < \sigma < 2\epsilon < \frac{1}{2}$. Using our bound for $\frac{u}{v}$, we have

$$\frac{x_2}{y_2} = \frac{u(u^3 - 2v^3)}{v(2u^3 - v^3)} = \frac{u}{2v}\left(\frac{1 - 2\sigma^3}{1 - \frac{\sigma^3}{2}}\right) = \frac{u}{v} - \frac{3v}{2u}\left(\frac{\sigma}{2 - \sigma^3}\right)$$

With an adjusted bound for σ, we can deduce the following inequality, which sets a bound the relationship between (u, v) and (x_2, y_2).

$$0 < \frac{\sigma}{2 - \sigma^3} < \sigma < \frac{1}{2} \implies 0 < \frac{u}{2v} - \frac{x_2}{y_2} = \frac{3v}{2u}\left(\frac{\sigma}{2 - \sigma^3}\right) \leqslant \frac{3v}{4u} < \frac{3\epsilon}{2}$$

Using the bounds above, we can deduce a condition on x_1 and y_1 to prove that some x_2, y_2 exist and satisfy the equality of summation of cubes. We can do this using the above bound,

$$\left|\frac{x_2}{y_2} - \frac{x_1}{4y_1}\right| \leqslant \left|\frac{x_2}{y_2} - \frac{u}{2v}\right| + \frac{1}{2}\left|\frac{u}{v} - \frac{x_1}{2y_1}\right| < \frac{3\epsilon}{2} + \frac{3\epsilon^2}{8} < 2\epsilon$$

By this, we can come to the conclusion that if x_1, y_1 are positive rational numbers such that $0 < \frac{y_1}{x_1} < \epsilon < \frac{1}{4}$, then there exists positive rational numbers x_2, y_2 that satisfy equality of sum of cubes.

$$\frac{x_2}{y_2} > \frac{x_1}{4y_1} - 2\epsilon > \frac{1}{4\epsilon} - 2\epsilon > \frac{1}{8\epsilon} > 0$$

In fact, we can hold the final conditions to be true.

$$x_2^3 + y_2^3 = x_1^3 + y_1^3 \quad \text{and} \quad 0 < \frac{y_2}{x_2} < 8\epsilon \implies \left|\frac{4x_2}{y_2} - \frac{x_1}{y_1}\right| < 8\epsilon$$

If $8\epsilon < \frac{1}{4}$, we can repeat the same logic to prove that there exists positive rational numbers x_3 and x_4 such that $x_3^3 + y_3^3 = x_2^3 + y_2^3$ and the following would be true.

$$\left|0 < \frac{y_3}{x_3} < 8^2\epsilon\right| \quad \text{and} \quad \left|\frac{4x_3}{y_3} - \frac{x_2}{y_2}\right| < 8^2\epsilon$$

Using this repetitive process, we can deduce that if $0 < 8^{k-2}\epsilon < \frac{1}{4}$, there exists positive rational numbers $x_1, y_1, x_2, y_2, \ldots, x_k, y_k$ such that $x_i^3 + y_i^3 = x_{i-1}^3 + y_{i-1}^3$ for all $i \in [2, k]$ and the following is true.

$$0 < \frac{y_i}{x_i} < 8^{i-1}\epsilon \quad \text{and} \quad \left|\frac{4^j x_{i+1}}{y_{i+1}} - \frac{x_i}{y_i}\right| < 8^{i-1}\epsilon \quad \text{for } i = 1, \ldots, k$$

Now, we have proven that there exist k sets of positive rational numbers $\{x_i, y_i\}$ such that $x_i^3 + y_i^3 = x_{i-1}^3 + y_{i-1}^3$ for all $i \in [2, k]$. The second (and slightly less complex) part of the proof is to show that these sets are pairwise disjoint.

Proof (continued): From the above section, we have that the following is true.

$$\left|\frac{4^j x_{i+j}}{y_{i+j}} - \frac{4^{j-1} x_{i+j-1}}{y_{i+j-1}}\right| < 4^{j-1} \cdot 8^{i+j-1}\epsilon = 8^i \cdot 32^{j-1}\epsilon$$

This means that for $j = 1, \ldots, k-1$, we can deduce the inequality for $1 \leqslant i < i + \ell \leqslant k$.

$$\begin{aligned}\left|\frac{4^\ell x_{i+\ell}}{y_{i+\ell}} - \frac{x_i}{y_i}\right| &\leqslant \sum_{j=1}^{\ell} \left|\frac{4^j x_{i+j}}{y_{i+j}} - \frac{4^{j-1}x_{i+j-1}}{y_{i+j-1}}\right| \\ &\leqslant 8^i \epsilon \sum_{j=1}^{\ell} 32^{j-1} \\ &< 8^i 32^\ell \epsilon\end{aligned}$$

Now, assume for the sake of contradiction that $x_i = x_{i+\ell}$ and $y_i = y_{i+\ell}$ for some $\ell \geqslant 1$, then we have that the following is true.

$$\frac{x_{i+\ell}}{y_{i+\ell}} = \frac{x_i}{y_i} \implies \frac{3x_i}{y_i} \leqslant (4^\ell - 1)\frac{x_i}{y_i} = \left|\frac{4^\ell x_{i+\ell}}{y_{i+\ell}} - \frac{x_i}{y_i}\right| < 8^i 32^\ell \epsilon$$

From the assumption, we have a contradiction. This means that the sets $\{x_i, y_i\}$ are pairwise disjoint, and we have proven Fermat's Theorem.

$$3 \leqslant 8^i 32^\ell \epsilon < 8^{2i-1} 32^\ell \epsilon^2 < 8^{2k}\epsilon^2 = 1$$

If you take the common denominator d for all the x_i's, then we have proven Fermat's theorem via $(dx_1)^3 + (dy_1)^3 = (dx_2)^3 + (dy_2)^3 = \cdots = (dx_k)^3 + (dy_k)^3 = N$ such that $r_{3,2}(N) \geqslant k$.

5.4 Erdos & Mahler's Theorem

To do this proof, we need four additional elemntary lemmas. Although I think that it's valuable to learn the proof, I think the technicalities of it can be left to the book.

Theorem: Let $C_2'(n)$ denote the number of integers not exceeding n that can be written as the sum of two positive, relatively prime integral cubes. Then,

$$C_2'(n) \gg n^{\frac{2}{3}}$$

Proof: If interested, please reference [H] Section 2.4, Lemmas 2.6 - 2.9 & Theorem 2.5.

A consequence of this theorem states that many integers can be written as the sum of two positive cubes. The next question would then be, how many numbers have two essentially distinct representations in this form?

5.5 Hooley-Wooley Theorem

Hooley and Wooley's theorem is an answer to the question at the end of the previous subsection. However, to prove this, you will need to know a result from the theory of binary quadratic forms (taught by Jinoo). In fact, this proof requires an additional three lemmas, and similar to the previous theorem, the proof will be left in the textbook.

Theorem: Let $D(n)$ denote the number of integers not exceeding n that have at least two essentially distinct representations as the sum of two nonnegative itnegral cubes. Then,

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

Proof: If interested, please reference [H] Section 2.4, Lemmas 2.10 - 2.12 & Theorem 2.6.

Finally, a consequence of this theorem is that almost 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 $c'n^{\frac{5}{9}+\epsilon}$.

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