EUCLID LAB

RESEARCH PAPERS

These papers have been written in the course of my mathematics research done with Euclid Lab, United States of America.

Reference:
Professor Nick Castro: nick.castro@euclidlab.org and
Professor David Gay: david.gay@euclidlab.org

Unsolved Problems in Mathematics

Saipranav Ganumpally, Lucas Hinds, Akshat Jha, Matthew Kalarickal,
Cade Reinberger, Anand Somayajula, Aditi Varma, William Zhao,
Eddie Beck, Nick Castro, Jason Joseph

August 23, 2020

Contents

Chapter 1

Introduction

In this paper, we will discuss three problems: Singmaster's Conjecture, the existence of a perfect cuboid, and the infinitude of perfect numbers.

1. Singmaster's Conjecture challenges us to find a finite upper bound of the multiplicities of entries appearing in Pascal's triangle.
2. The Perfect Cuboid Problem asks the existence of a cuboid where all sides, face diagonals, and the space diagonal have positive integer lengths.
3. The Perfect Number problem asks whether or not there exists infinitely many even perfect numbers.

In the following chapters, we will discuss how we attempted to answer these questions.

Chapter 2

Singmaster's Conjecture

2.1 Problem Statement

Definition 2.1. For a positive integer a, let $N(a)$ denote the number of times a occurs in Pascal's triangle. So, in particular we have

$$N(a) = \left| \left\{ (n,k) \in \mathbb{Z}^2 : \binom{n}{k} = a \right\} \right|.$$

Question 2.1. (Singmaster's Conjecture) Does there exist some finite upper bound $C \in \mathbb{Z}$ so that for all $a \in \mathbb{Z}_{\geq 2}$, $N(a) \leq C$?

2.2 Progress on Problem

We haven't been able to prove Singmaster's conjecture, but we have made some progress in that direction.

1. We can determine the i-th element of the j-th diagonal in Pascal's triangle as a degree j polynomial in i. (This is done in Lemma 2.1).

2. We can express binomial coefficients as weighted sums of other binomial coefficients. (This is done in Theorem 2.1).

3. We can show that $N(a) = O(\log(a))$. (This is done in Theorem 2.3).

4. We can show by computer that $N(a) \leq 8$ for all $a \leq 10000$. (This is done in Theorem 2.5).

5. We can show that there exists a finite upper bound on the multiplicities of almost all numbers in Pascal's triangle. That, is, there exists a constant $C_0 \in \mathbb{R}$ such that

$$\lim_{n \to \infty} \frac{|\{a \in \mathbb{Z} \cap [2,n] : N(a) \leq C_0\}|}{|\{a \in \mathbb{Z} \cap [2,n]\}|} = 1.$$

   (This is done in Corollary 2.3).

6. We can show that only finitely many numbers are at least two of Triangular, Tetrahedral, and Pentatopal. (This is done in Theorem 2.2).

2.3 Properties of Binomial Coefficients

2.3.1 Expressing Binomial Coefficients as Sums of Products of Binomial Coefficients

Theorem 2.1. For all $a, m, n \in \mathbb{N}$, we have

$$\binom{m}{n} = \sum_{i=0}^{a} \binom{a}{i} \cdot \binom{m-a}{n-a+i}.$$

Proof. We prove this by induction on a. To start, we will prove the base case $a = 0$,

$$\binom{m}{n} = \binom{0}{0} \cdot \binom{m}{n}.$$

Next, we will assume that $a = w$ satisfies this property, and prove that this implies $a = w + 1$ also satisfies this property. The induction hypothesis gives

$$\binom{m}{n} = \binom{w}{0} \cdot \binom{m-w}{n-w} + \binom{w}{1} \cdot \binom{m-w}{n-w+1} + ... + \binom{w}{w} \cdot \binom{m-w}{n}.$$

Using Pascal's identity, a classic result which can be found in [2],

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}$$

we have

$$\begin{aligned}\binom{m}{n} = \binom{w}{0} \cdot \left[\binom{m-(w+1)}{n-(w+1)} + \binom{m-(w+1)}{n-w}\right] + \binom{w}{1} \cdot \left[\binom{m-(w+1)}{n-w} + \binom{m-(w+1)}{n-(w-1)}\right] \\ + ... + \binom{w}{w} \cdot \left[\binom{m-(w+1)}{n-1} + \binom{m-(w+1)}{n}\right].\end{aligned}$$

Which, combining like terms and simplifying gives

$$\begin{aligned}\binom{m}{n} = \binom{m-(w+1)}{n-(w+1)} + \binom{m-(w+1)}{m-w}\left[\binom{w}{0} + \binom{w}{1}\right] + \binom{m-(w+1)}{n-(w-1)}\left[\binom{w}{1} + \binom{w}{2}\right] \\ + ... + \binom{m-(w+1)}{n-1}\left[\binom{w}{w-1} + \binom{w}{w}\right] + \binom{m-(w+1)}{n}.\end{aligned}$$

Whence applying the identity again gives

$$\binom{m}{n} = \binom{w+1}{0}\binom{m-(w+1)}{n-(w+1)} + \binom{w+1}{1}\binom{m-(w+1)}{m-w} + ... + \binom{w+1}{w+1}\binom{m-(w+1)}{n}$$

completing our induction. ■

In fact, we have two more proofs of this lemma that are quite elegant as well, and give certain insights, so we include these also.

Proof. (Alternate Proof One). We use generating functions. We also adopt the convention that if $b > a$ for integers a and b we define

$$\binom{a}{b} = 0$$

because this will simplify our notation. Using the binomial theorem we have

$$\sum_{k=0}^{i+j}\binom{i+j}{k}x^k = (1+x^{i+j}) = (1+x)^i(1+x)^j = \left(\sum_{m=0}^{i}\binom{i}{m}x^m\right)\left(\sum_{n=0}^{j}\binom{j}{n}x^n\right) = \sum_{k=0}^{i+j}\left[\sum_{\ell=0}^{k}\binom{i}{\ell}\binom{j}{k-\ell}\right]x^k$$

where the last equality uses the distributive property to multiply the polynomials. ■

Proof. (Alternate Proof Two) We use a double-counting argument. Imagine a group of i cats and j dogs. The number of ways to choose k pets from this bunch is just the sum of the number of ways one can choose ℓ cats and $k-\ell$ dogs for all ℓ. We first notice there are

$$\binom{i+j}{k}$$

ways choose k pets from the set of $i+j$ pets. Also, one can choose ℓ cats in

$$\binom{i}{\ell}$$

ways, and $k-\ell$ dogs in

$$\binom{j}{k-\ell}$$

ways, and therefore ℓ cats and $k-\ell$ dogs in

$$\binom{i}{\ell}\binom{j}{k-\ell}$$

ways. And thus, indeed, the number of ways to choose k pets from the bunch is just

$$\sum_{\ell=0}^{k}\binom{i}{\ell}\binom{j}{k-\ell}.$$

Thus, equating our first method of counting with our second we get

$$\binom{i+j}{k} = \sum_{\ell=0}^{k}\binom{i}{\ell}\binom{j}{k-\ell}.$$

■

2.3.2 Expression for the Diagonals

Lemma 2.1. For positive integers i and j

$$\binom{i+j}{j} = \frac{1}{j!}\prod_{k=1}^{j}(i+k).$$

Proof.

$$\binom{i+j}{j} = \frac{(i+j)!}{i!\,j!} = \frac{1}{j!}\frac{(i+j)!}{i!} = \frac{1}{j!}\left[\frac{\prod_{r=1}^{i+j} r}{\prod_{r=1}^{i} r}\right] = \frac{1}{j!}\left[\frac{\prod_{r=1}^{i} r \prod_{r=i+1}^{i+j} r}{\prod_{r=1}^{i} r}\right] = \frac{1}{j!}\prod_{r=i+1}^{i+j} r = \frac{1}{j!}\prod_{k=1}^{j}(i+k).$$

■

2.4 Using Diagonals of Pascal's Triangle in Singmaster's Conjecture

2.4.1 Empirical Understanding of Diagonal equations

We can actually derive formulae to represent each of the first few diagonals in Pascal's triangle, and then prod further to find helpful patterns in these functions. To achieve this, we use the graph shown in Figure 2.1.

We can express these formulas making empirical use of polynomial regression in the equations below, where $D_n(x)$ represents the function for diagonal n. Our key observation is that for each diagonal it appears, again empirically, that some finite degree polynomial regression is exact.

$$
\begin{aligned}
D_1(x) &= x + 2 \\
D_2(x) &= \frac{1}{2}x^2 + \frac{5}{2}x + 3 \\
D_3(x) &= \frac{1}{6}x^3 + \frac{3}{2}x^2 + \frac{13}{3}x + 4 \\
D_4(x) &= ax^4 + bx^3 + cx^2 + dx + e \\
&\vdots
\end{aligned}
$$

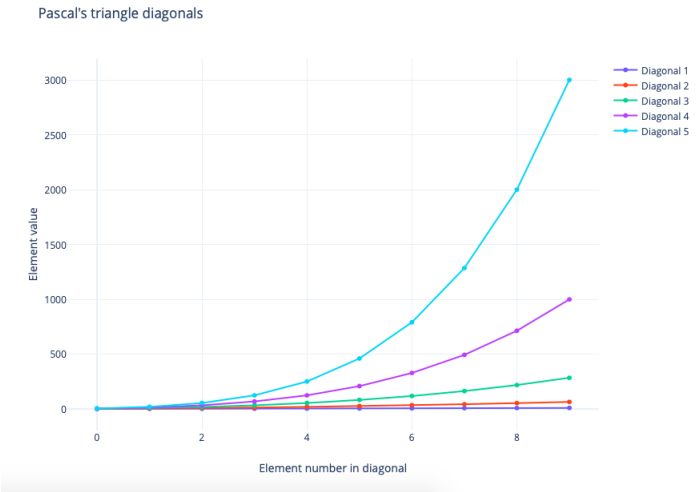


Figure 2.1: Discrete Plot of Values of Diagonals in Pascal's Triangle

And so we note that the diagonals are polynomials where the degree increases by 1 for each successive diagonal. The growth is, then, $O(x^n)$ where n is diagonals being considered. We note furthermore that the roots of these polynomials have a seemingly simple pattern.

$$
\begin{aligned}
&D_1(x) \text{ has roots } x = -2 \\
&D_2(x) \text{ has roots } x = -2, x = -3 \\
&D_3(x) \text{ has roots } x = -2, x = -3, x = -4 \\
&D_4(x) \text{ has roots } x = -2, x = -3, x = -4, x = -5 \\
&\vdots
\end{aligned}
$$

Using this new-found information and the knowledge that the y-intercept of each $D_n(x)$ is $n+1$ (since $\binom{n+1}{1} = n+1$), we can determine the equation of each polynomial.

$$\begin{aligned} D_1(x) &= \frac{(x+2)}{1} \\ D_2(x) &= \frac{(x+2)(x+3)}{2} \\ D_3(x) &= \frac{(x+2)(x+3)(x+4)}{6} \\ D_4(x) &= \frac{(x+2)(x+3)(x+4)(x+5)}{24} \\ &\vdots \end{aligned}$$

From this, we can derive a general formula for the n^{th} diagonal, given by

$$D_n(x) = \frac{(x+2)(x+3)\dots(x+n)(x+n+1)}{n!}.$$

To ensure these functions are in fact correct, we graph them (in Figure 2.2) and compare them to the original graph (Figure 2.1). Comparing the two figures yields the empirical conclusion that the equations, and thus the general formula, are correct.

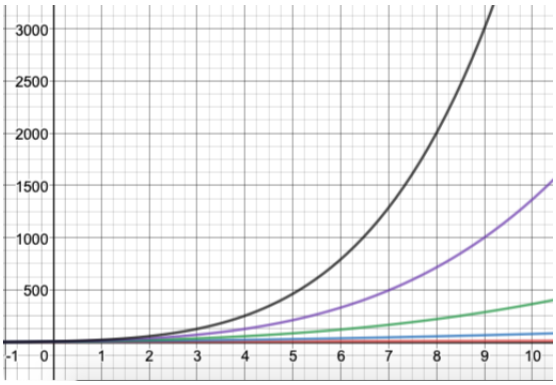


Figure 2.2: Diagonal Graph 2

Remark 2.1. Since we have

$$D_n(x) = \binom{n+x+1}{n}$$

we may note that this conclusion is formally equivalent to Lemma 2.1, which also expresses the i-th element of the j-th diagonal as a degree j polynomial in i. The two are related by a horizontal shift, in fact, since we have by Lemma 2.1

$$D_n(x) = \binom{n+x+1}{n} = \frac{1}{n!}\prod_{k=2}^{n+1}(x+k).$$

2.4.2 Computational Approach

Avoiding a purely brute-force method to find integers with high multiplicities as binomial coefficients, we can instead try to find the multiplicity of a chosen integer k, assuming k is not a central binomial coefficient, using the conditions we know.

1. k can only be found in the rows preceding row $k+1$.

2. For each row
$$\sum_{r=0}^{n} \binom{n}{r} = (1+1)^n = 2^n$$
So, k cannot be found in any row whose sum is less than or equal to $2k$ (Since the sum of a finite set of more than two positive integers is at least the sum of two of its elements, and by the symmetry of Pascal's triangle, if k is not a central binomial coefficient and did appear in such a row, it would appear twice).

Considering the general formula for diagonals (as in Lemma 2.1) as a Diophantine equation, we are interested in the integer points of intersection of the line $y = k$ and the successive diagonals, but only until the $(k-1)^{st}$ diagonal, since every later diagonal only has entries not equal to 1 in rows at least $k+1$ and therefore has no integer intersections, following from the first point above. This gives a reduction in the region of Pascal's triangle in which one has to check to find the multiplicity of k. An example of this techniques applied is given in Figure 2.3.

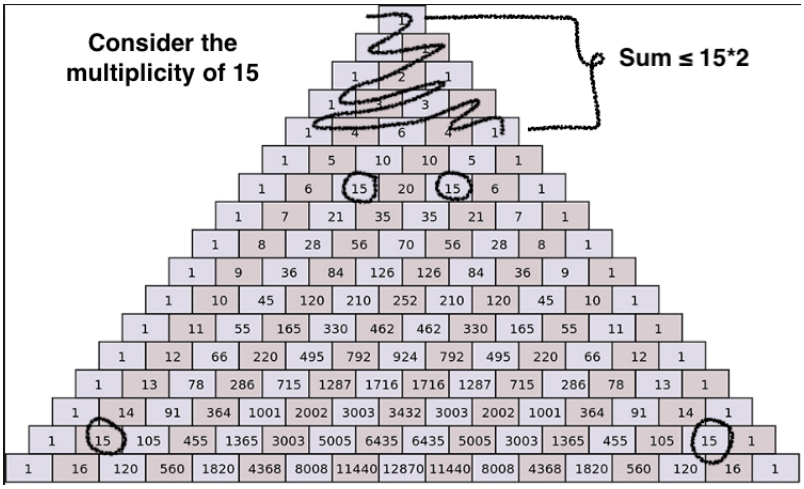


Figure 2.3: Example of Computational Bounding for $k = 15$

2.5 Triangular and Tetrahedral Numbers

Theorem 2.2. Finitely many numbers are more than one of Triangular, Tetrahedral, and Pentatopal.

Proof. We show that each of
$$\binom{x}{2} = \binom{y}{3}$$
$$\binom{x}{2} = \binom{z}{4}$$
$$\binom{y}{3} = \binom{z}{4}$$
has only finitely many diophantine solutions. The strategy is to check the conditions of a deep theorem of Siegel. Siegel's theorem, which can be found in [10], states that an algebraic variety over $\mathbb{Q}$ of genus greater

than zero has finitely many integral points. Practically, then, by considering degrees (in particular, using the genus-degree formula), it suffices for us to show that each of these curves are nonsignular to apply Siegel's theorem.

Case 1. $\binom{x}{2} = \binom{y}{3}$. All we have to show is non-singularity. Applying Lemma 2.1, we have the curve explicitly defined by

$$F_1(x, y) = (y)(y-1)(y-2) - 3x(x-1) = 0.$$

Any singularity is a simultaneous solution to the system of equations

$$\begin{cases} F_1(x,y) = 0 \\ \frac{\partial F_1(x,y)}{\partial x} = 0 \\ \frac{\partial F_1(x,y)}{\partial y} = 0 \end{cases}.$$

We have

$$\frac{\partial F_1}{\partial x} = 0 \iff x = \frac{1}{2}$$

and similarly

$$\frac{\partial F_1}{\partial y} = 0 \iff y = 1 \pm \frac{\sqrt{2}}{3}.$$

Whence we can note that $\left(\frac{1}{2}, 1 - \frac{\sqrt{2}}{3}\right)$ and $\left(\frac{1}{2}, 1 + \frac{\sqrt{2}}{3}\right)$ are not on the curve, so the curve is nonsingular.

Case 2. $\binom{x}{2} = \binom{z}{4}$. All we have to show is nonsingularity. Applying Lemma 2.1, we have the curve explicitly defined by

$$F_2(x, z) = (z)(z-1)(z-2)(z-3) - 12x(x-1) = 0.$$

Any singularity is a simultaneous solution to the system of equations

$$\begin{cases} F_2(x,z) = 0 \\ \frac{\partial F_2(x,z)}{\partial x} = 0 \\ \frac{\partial F_2(x,z)}{\partial z} = 0 \end{cases}.$$

We have

$$\frac{\partial F_2}{\partial x} = 0 \iff x = \frac{1}{2}$$

and similarly

$$\frac{\partial F_2}{\partial z} = 0 \iff z = \frac{3}{2}, \frac{3}{2} \pm \frac{\sqrt{5}}{2}.$$

And we can note that all of $\left(\frac{1}{2}, \frac{3}{2}\right)$, $\left(\frac{1}{2}, \frac{3}{2} - \frac{\sqrt{5}}{2}\right)$ and $\left(\frac{1}{2}, \frac{3}{2} + \frac{\sqrt{5}}{2}\right)$ are not on the curve, so the curve is nonsingular.

Case 3. $\binom{y}{3} = \binom{z}{4}$. All we have to show is nonsingularity. Applying Lemma 2.1, we have the curve explicitly defined by

$$F_3(y, z) = (z)(z-1)(z-2)(z-3) - 4(y)(y-1)(y-2) = 0.$$

Any singularity is a simultaneous solution to the system of equations

$$\begin{cases} F_3(y,z) = 0 \\ \frac{\partial F_3(y,z)}{\partial y} = 0 \\ \frac{\partial F_3(y,z)}{\partial z} = 0 \end{cases}.$$

We have

$$\frac{\partial F_3}{\partial y} = 0 \iff y = 1 \pm \frac{\sqrt{2}}{3}$$

and similarly

$$\frac{\partial F_3}{\partial z} = 0 \iff \frac{3}{2}, \frac{3}{2} \pm \frac{\sqrt{5}}{2}.$$

And we note none of $\left(1 - \frac{\sqrt{2}}{3}, \frac{3}{2}\right)$, $\left(1 + \frac{\sqrt{2}}{3}, \frac{3}{2}\right)$, $\left(1 - \frac{\sqrt{2}}{3}, \frac{3}{2} + \frac{\sqrt{5}}{2}\right)$, $\left(1 + \frac{\sqrt{2}}{3}, \frac{3}{2} + \frac{\sqrt{5}}{2}\right)$, $\left(1 - \frac{\sqrt{2}}{3}, \frac{3}{2} - \frac{\sqrt{5}}{2}\right)$, and $\left(1 + \frac{\sqrt{2}}{3}, \frac{3}{2} - \frac{\sqrt{5}}{2}\right)$ are on the curve, so the curve is nonsingular. ■

Remark 2.2. Computer search gives 10, 120, 1540, 7140 as the only numbers that are both triangular and tetrahedral up to 10^6. We conjecture this list is complete, though we cannot prove it. The elliptic curve defined by $E : F_1(x, y) = 0$ is rank 2 and torsion-free, so one may able to use techniques from the theory of elliptic curves to prove this conjecture. But the best general bounds on height of integral points on elliptic curves are still triple exponential, as found by Baker's Method (which can be found in [10]), which is too large to be checked by computer using brute force, but perhaps an effective version of the Hall-Lang Conjecture (Also found in [10]) could restrict the search to the computationally achievable.

2.6 Logarithmic Bound of Entry Multiplicity in Pascal's Triangle

Here we show $N(r) = O(\log(r))$. We first need to show the monotonicty of $\binom{i+j}{i}$ in both i and j.

Lemma 2.2. For all $(i_1, j_1) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ and $(i_2, j_2) \in \mathbb{Z}_{\geq i_1} \times \mathbb{Z}_{\geq j_1} - \{(i_1, j_1)\}$ we have

$$\binom{i_2 + j_2}{i_2} > \binom{i_1 + j_1}{i_1}.$$

Proof. By theorem 2.1

$$\binom{i_2 + j_2}{i_2} = \sum_{\ell=0}^{i_2} \binom{i_2}{\ell}\binom{j_2}{i_2 - \ell} \geq \sum_{\ell=0}^{i_1} \binom{i_2}{\ell}\binom{j_2}{i_2 - \ell} \geq \sum_{\ell=0}^{i_1} \binom{i_1}{\ell}\binom{j_1}{i_1 - \ell} = \binom{i_1 + j_1}{i_1}$$

where equality can only hold in the first step if $i_1 = i_2$ and in the second stop if $j_1 = j_2$, both of which can't be true by our constraints on i_2 and j_2. ■

Next we need a bound for binomial coefficients.

Lemma 2.3. For $n, k \in \mathbb{Z}^+$ with $i \geq j$ we have

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k}$$

Proof. Applying Lemma 2.1 we have

$$\binom{n}{k} = \frac{1}{k!}\prod_{j=0}^{k-1g}(n - j) = \frac{\prod_{j=0}^{k-1}(n - j)}{\prod_{j=0}^{k-1}(k - j)} = \prod_{j=0}^{k-1}\left(\frac{n - j}{k - j}\right) \geq \prod_{k=0}^{k-1}\left(\frac{n}{k}\right) = \left(\frac{n}{k}\right)^k.$$

■

Corollary 2.1. For all $n \in \mathbb{Z}^+$ we have

$$\binom{2n}{n} \geq 2^n.$$

Definition 2.2. We define $m(r)$ as the smallest positive integer so that

$$\binom{2m(r)}{m(r)} \geq r.$$

‘

Corollary 2.2. In consequence of Corollary 2.1 and thereby Lemma 2.3 we have

$$\binom{2\log_2(r)}{\log_2(r)} \geq 2^{\log_2(r)} = r$$

so that

$$m(r) \leq \log_2(r).$$

And now before we can prove our result we need only to show each row in Pascal's triangle is symmetric about its center.

Lemma 2.4. For all $n, k \in \mathbb{Z}_{\geq 0}$ with $n \geq k$ we have

$$\binom{n}{k} = \binom{n}{n-k}.$$

Proof. The proof is combinatorial. The number of ways to choose a set of k people from n people is the same as the number of ways to choose the remaining $n-k$ people to form a set of people who aren't in the set of k people. Thus

$$\binom{n}{k} = \binom{n}{n-k}.$$

■

Definition 2.3. We define

$$\mathbb{1}_{(\text{Condition})} = \begin{cases} 1 & \text{If (Condition) is true} \\ 0 & \text{Otherwise} \end{cases}$$

Theorem 2.3. $N(r) = O(\log(r))$

Proof. Using Lemma 2.2 and Definition 2.2, we can rule out the shaded portion of Pascal's triangle in figure 2.4 (included below), because every binomial coefficient in the shaded region is bigger than r.

Using the fact that there are no solutions in the shaded region, and by Lemma 2.4 we have in particular

$$N(r) \leq 2\sum_{\overline{x}\in\Omega} \mathbb{1}_{(\overline{x})=r} = 2\sum_{i=0}^{m(r)} \sum_{j\in\mathbb{Z}_{\geq 0}} \mathbb{1}_{\binom{i+j}{j}=r}.$$

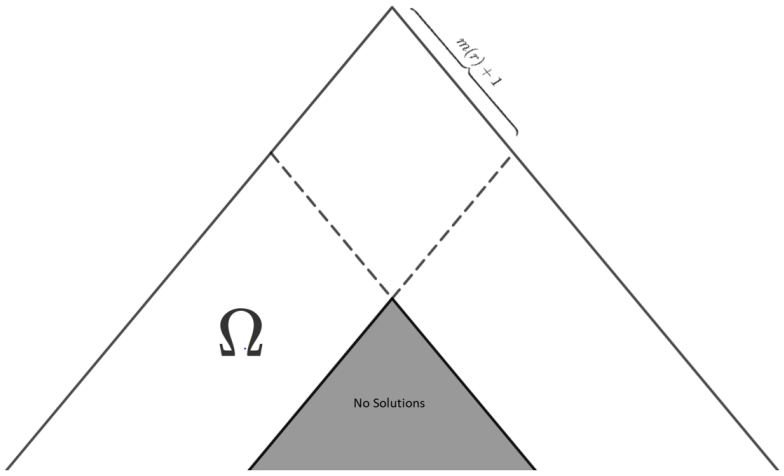
By lemma 2.2 $\binom{i+j}{j} = \binom{i+j}{i}$ is monotonously increasing with respect to j. Thus Lemma 2.2 implies that for all $i \in \mathbb{Z}_{\geq 0}$ we have

$$\sum_{j\in\mathbb{Z}_{\geq 0}} \mathbb{1}_{\binom{i+j}{j}=r} \leq 1$$

since a monotonously increasing function can take value r at most once. Thus we have

$$N(r) \leq 2\sum_{i=0}^{m(r)} \sum_{j\in\mathbb{Z}_{\geq 0}} \mathbb{1}_{\binom{i+j}{j}=r} \leq 2\sum_{i=0}^{m(r)} 1 = 2m(r) + 2.$$

Figure 2.4: The shaded region has no solutions, and the number of total solutions is at most twice the number of solutions in Ω



Putting this together with Corollary 2.2 gives

$$N(r) \leq 2 + \log_2(r) = O(\log r)$$

thus

$$N(r) = O(\log r).$$

■

2.7 A Proof of an Upper bound on the Multiplicity of Almost All Numbers as Binomial Coefficients

Here we prove that almost all numbers occur exactly twice in Pascal's triangle. In order to prove this, we use the probabilistic method, and in particular, we prove the slightly stronger Lemma 2.5.

Definition 2.4. For a finite set S, let $\text{Unif}(S)$ be the uniform distribution on S. So, in particular, let S have probability mass function $p : S \to [0, 1]$ given for all $\sigma \in S$ by

$$p(\sigma) = \frac{1}{|S|}.$$

Lemma 2.5. Let X_m be the discrete random variable defined by

$$X_m \sim \text{Unif}\left(\{2, 3, ..., M\}\right)$$

then

$$\lim_{M \to \infty} \mathbb{E}[N(X_M)] = 2.$$

Proof. Let $\mathcal{P}$ denote all of Pascal's triangle. Then we have

$$\mathbb{E}[N(X_M)] = \frac{1}{M-1} \sum_{\overline{x} \in \mathcal{P}} \mathbb{1}_{(\overline{x}) \leq M}$$

we then begin to break up $\mathcal{P}$. In particular, we break up $\mathcal{P}$ into the trivial region and the interior, $\mathcal{I}$, where the trivial region refers to the outer two layers. Since each number appears exactly twice in the trivial region, the trivial region contributes exactly 2 to the expectation. Thus

$$2 \leq \mathbb{E}[N(X_M)].$$

And adding in the interior we get

$$\mathbb{E}[N(X_M)] = 2 + \frac{1}{M-1} \sum_{\overline{x} \in \mathcal{I}} \mathbb{1}_{(\overline{x}) \leq M}.$$

Using symmetry (Lemma 2.4) and the geometry of the region Ω, defined in figure 2.5 below we have

$$\mathbb{E}[N(X_M)] = 2 + \frac{1}{M-1} \sum_{\overline{x} \in \mathcal{I}} \mathbb{1}_{(\overline{x}) \leq M} \leq 2 + \frac{2}{M-1} \sum_{\overline{x} \in \Omega} \mathbb{1}_{(\overline{x}) \leq M}.$$

Which making our zone of summation explicit is just

$$\mathbb{E}[N(X_M)] \leq 2 + \frac{2}{M-1} \sum_{\overline{x} \in \Omega} \mathbb{1}_{(\overline{x}) \leq M} = 2 + \frac{2}{M-1} \sum_{k=2}^{m(M)+1} \sum_{i \geq 2} \mathbb{1}_{\binom{i+k}{k} \leq M}.$$

Applying Lemma 2.2, bimonotonicity gives

$$\mathbb{E}[N(X_M)] \leq 2 + \frac{2}{M-1} \sum_{k=2}^{m(M)+1} \sum_{i \geq 2} \mathbb{1}_{\binom{i+k}{k} \leq M} \leq 2 + \frac{2}{M-1} \sum_{k=2}^{m(M)+1} \sum_{i \geq 2} \mathbb{1}_{\binom{i+2}{2} \leq M}.$$

By Lemma 2.3 now, we note that if $i > 2\sqrt{M}$ then

$$\binom{i+2}{2} \geq \left(\frac{i+2}{2}\right)^2 \geq \left(\frac{i}{2}\right)^2 > \left(\frac{2\sqrt{M}}{2}\right)^2 = M.$$

So that in particular we have

$$\sum_{i \geq 2} \mathbb{1}_{\binom{i+2}{2} \leq M} \leq 2\sqrt{M}.$$

Applying this to our sum above we get

$$\begin{aligned}\mathbb{E}[N(X_M)] \leq 2 + \frac{2}{M-1} \sum_{k=2}^{m(M)+1} \sum_{i \geq 2} \mathbb{1}_{\binom{i+2}{2} \leq M} &\leq 2 + \frac{2}{M-1} \sum_{k=2}^{m(M)+1} 2\sqrt{M} \\ &= 2 + \frac{4\sqrt{M}}{M-1} \sum_{k=2}^{m(M)+1} 1 = 2 + \frac{4\sqrt{M} m(M)}{M-1}.\end{aligned}$$

Thus, applying corollary 2.2 gives

$$\mathbb{E}[N(X_M)] \leq 2 + \frac{4\sqrt{M}\log_2(M)}{M-1}.$$

Thus, together with the trivial inequality from the beginning we have

$$2 \leq \mathbb{E}[N(X_M)] \leq 2 + \frac{4\sqrt{M}\log_2(M)}{M-1}.$$

From here we can apply the squeeze theorem to prove our desired result. Clearly

$$\lim_{M\to\infty} 2 = 2.$$

And to evaluate the limit on the right we first note

$$\lim_{M\to\infty} \frac{M-1}{M} = \lim_{M\to\infty} \left(1 - \frac{1}{M}\right)$$

which since both are finite gives

$$\lim_{M\to\infty} \frac{M-1}{M} = \lim_{M\to\infty} 1 - \lim_{M\to\infty} \frac{1}{M} = 1 - 0 = 1.$$

Thus, since both factors are finite, with have

$$\lim_{M\to\infty} \frac{4\log_2(M)}{\sqrt{M}} = \lim_{M\to\infty} \left(\frac{M-1}{M}\right)\left(\frac{4\sqrt{M}\log_2(M)}{M-1}\right) = \left(\lim_{M\to\infty} \frac{M-1}{M}\right)\left(\lim_{M\to\infty} \frac{4\sqrt{M}\log_2(M)}{M-1}\right)$$

so that applying the above result on our rightmost expression gives

$$\lim_{M\to\infty} \frac{4\sqrt{M}\log_2(M)}{M-1} = \lim_{M\to\infty} \frac{4\log_2(M)}{\sqrt{M}}.$$

Applying L'Hopital's rule to this last expression we get

$$\lim_{M\to\infty} \frac{4\sqrt{M}\log_2(M)}{M-1} = \frac{4}{\ln 2} \lim_{M\to\infty} \frac{\frac{1}{M}}{\frac{2}{\sqrt{M}}} = \frac{8}{\ln 2} \lim_{M\to\infty} \frac{1}{\sqrt{M}} = 0.$$

Thus, we have

$$\lim_{M\to\infty} 2 + \frac{4\sqrt{M}\log_2(M)}{M-1} = 2$$

and so, by the squeeze theorem, we get finally

$$\lim_{M\to\infty} \mathbb{E}[N(X_M)] = 2.$$

■

And in some ways, this is an interesting result on its own. But, in any case, it readily gives us the weaker result we set out to prove at the beginning.

Theorem 2.4.

$$\lim_{M\to\infty} \frac{|\{a \in \mathbb{Z} \cap [2, M] : N(a) = 2\}|}{|\mathbb{Z} \cap [2, M]|} = 1.$$

Proof. If we define

$$S_M \stackrel{\text{def}}{=} \{a \in \mathbb{Z} \cap [2, M] : N(a) > 2\}$$

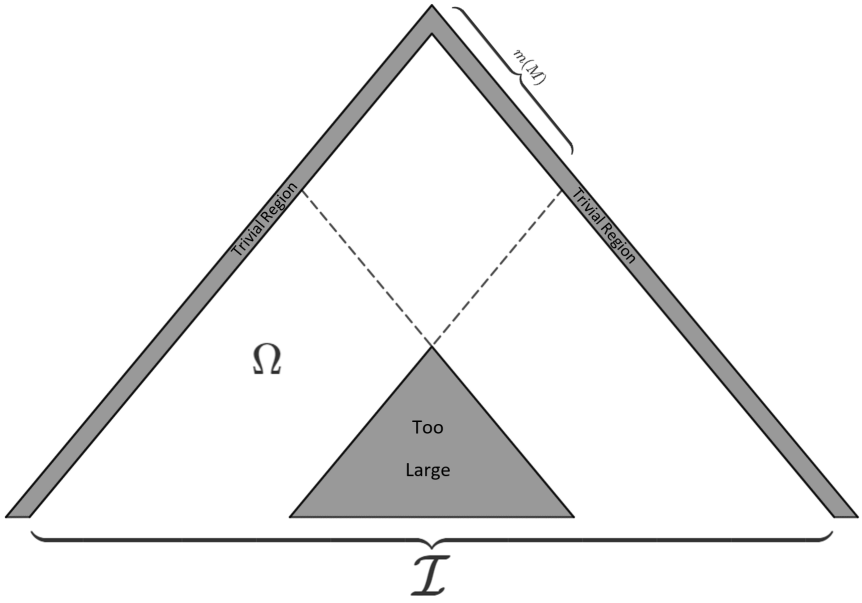
and then

$$\varepsilon_M \stackrel{\text{def}}{=} \frac{|S_M|}{M-1}$$

we can note by the definition of S_M, and using the fact N is integer-valued

$$|S_M| = \sum_{\alpha\in S_M} 1 \leq \sum_{\alpha\in S_M} (N(\alpha) - 2) \leq 4\sqrt{M}\log_2(M)$$

Figure 2.5: The definitions of $\mathcal{I}$ and Ω



where the last inequality comes from Lemma 2.5. Thus, applying the fact that for $M \geq 2$ we have ε_M is the ratio of the cardinalities of two sets, the denominator being nonempty, along with the above inequality gives

$$0 \leq \varepsilon_M \leq \frac{4\sqrt{M}\log_2(M)}{M-1}.$$

Whence applying the squeeze theorem with the limit evaluation from Lemma 2.5 gives

$$\lim_{M\to\infty} \varepsilon_M = 0.$$

Thus,

$$\lim_{M\to\infty} \frac{|\{a \in \mathbb{Z} \cap [2,M] : N(a) = 2\}|}{|\mathbb{Z} \cap [2,M]|} = \lim_{M\to\infty} (1-\varepsilon_M) = 1 - \lim_{M\to\infty} \varepsilon_M = 1 - 0 = 1.$$

■

Corollary 2.3. (In terms slightly closer to Singmaster's Conjecture Itself) There exists a fixed constant C_0, indeed $C_0 = 2$, so that the proportion of the first M natural numbers with multiplicity in Pascal's triangle less than or equal to C_0 goes to 1 as M goes to infinity.

2.8 Computation

Computer searches for binomial coefficients of especially large multiplicity are properly best done by just generating Pascal's triangle up to some appropriate value and checking how often each value occurs, to minimize redundancy in computing. But, using the techniques from above, if one wants to know $N(r)$ for some special r, one can do so in relatively little time. The idea is to consider only the diagonals $2, 3, ..., \log_2(r)$ and to solve using Newton's method (which can be found in [14]) for the intersection of each of those diagonals with r numerically, and then to check only the nearest 2 integer elements of that diagonal to the result of the

numerical method to verify the existence or nonexistance of any occurrences on r in that diagonal. To show the effectiveness of this technique, we computed the maximum value of $N(r)$ for all r less than 10000. This, can of course, be computed more efficiently by just building the triangle, since the method of repeatedly finding $N(r)$ in this way is inefficient for considering many r. But it is a satisfying application of these techniques.

Theorem 2.5.

$$\max_{r\in\{1,2,\ldots,10000\}} N(r) = 8$$

and $N(r) = 8$ for all $r \in \{1, 2, ..., 10000\}$ if and only if $r = 3003$.

Proof. By exhaustive search. The source code can be found in Appendix A. ■

2.9 One Possible Application of the Gamma function towards Singmaster's conjecture

One might be interested in applying the properties of the gamma function to Singmaster's conjecture. We note briefly that can think about the function f implicitly defined in the first quadrant by

$$\binom{f_d(x)}{x} = d$$

which can be made smooth using the Gamma function. And so, an effective version of Singmaster's conjecture would look something like this:

For all positive integers $d \geq 2$, the function f_d defined above has at most 12 integral points in the first quadrant (or maybe 8 or 10, depending on the bound C). This is perhaps nice as an approach because these curves are convex, and there are theorems already bounding lattice points on convex curves that could possibly be applied and adapted towards Singmaster's conjecture.

Chapter 3

Perfect Cuboid

3.1 Problem Statement

Definition 3.1. We define a *cuboid* to be a tuple of positive real numbers $(a, b, c, d, e, f, g) \in \mathbb{R}_+^7$ where $\mathbb{R}_+ \stackrel{\text{def}}{=} (0, \infty)$ satisfying

$$d^2 = b^2 + c^2$$
$$e^2 = a^2 + c^2$$
$$f^2 = a^2 + b^2$$
$$g^2 = a^2 + b^2 + c^2.$$

Remark 3.1. The algebraic definition of a cuboid given above corresponds geometrically to a collection of key lengths of a rectangular prism. In particular, a, b and c are the lengths of the edges of the cuboid, d, e and f the lengths of the face diagonals, and g the length of the long diagonal. This geometric interpretation is illustrated in figure 3.1.

Question 3.1. (The Perfect Cuboid Problem). Does there exist a cuboid (a, b, c, d, e, f, g) with all of a, b, c, d, e, f, g integers?

3.2 Progress on Problem

We did not solve the Perfect Cuboid Problem, but we are able to prove the following things regarding the perfect cuboids:

1. No Pythagorean triple generates a nontrivial Saunderson Euler Brick that is a Perfect Cuboid. (Theorem 3.2).
2. In a primitive perfect cuboid, every divisor of the long diagonal is congruent to 1 modulo 4. (Theorem 3.7)
3. In a primitive perfect cuboid, one of the sides, two of the face diagonals, and the body diagonal are odd and two edges and one of the face diagonal are even. Also one of the even sides is divisible by 4 and the other is divisible by 16. (Theorem 3.4 and Theorem 3.8).
4. In a primitive perfect cuboid exactly two of the sides are divisible by 3 (Theorem 3.5 and one of the sides is divisible by 9 (Theorem 3.9).
5. In a primitive perfect cuboid, at least one of the edges is divisible by all of 5, 7, 11, and 19. (Theorem 3.6).

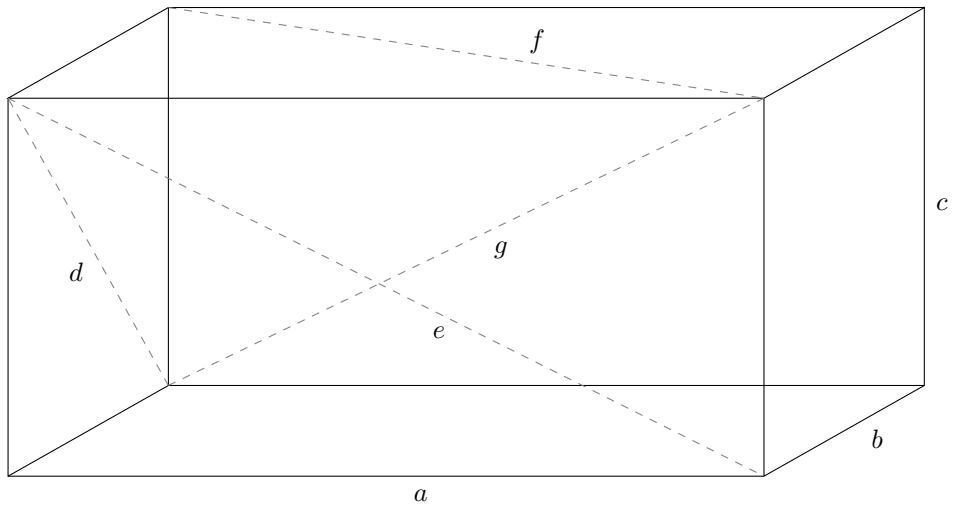


Figure 3.1: A cuboid with side lengths a, b, c, face diagonals d, e, f, and long diagonal g.

6. In a primitive perfect cuboid, at least one of the edges or diagonals is divisible by 13 and 17. (Theorem 3.6).

3.3 Diophantine Techniques

Definition 3.2. A perfect cuboid (a, b, c, d, e, f, g) is called *primitive* if

$$\gcd(a, b, c) = 1.$$

Definition 3.3. A 3-tuple of positive integers (u, v, w) is called a *Pythagorean Triple* if $u^2 + v^2 = w^2$.

Definition 3.4. A cuboid (a, b, c, d, e, f, g) is called an *Euler Brick* if all of a, b, c, d, e and f are integers.

3.3.1 Perfect Cuboids from Saunderson Parametrization

Theorem 3.1. (Saunderson). If (u, v, w) is a Pythagorean triple then the cuboid given by

$$\begin{aligned} a &= v\left|4u^2 - w^2\right| \\ b &= u\left|4v^2 - w^2\right| \\ c &= 4uvw \end{aligned}$$

is an Euler Brick. This can be found in [9].

Proof. Substituting of these values into our equations of a cuboid and simplifying gives

$$\begin{aligned} d &= v(4u^2 + w^2) \\ e &= u(4v^2 + w^2) \\ f &= w^3 \end{aligned}$$

which are all integral as long as u, v, and w are all integral. ■

Theorem 3.2. No Pythagorean triple generates a nontrivial Saunderson Euler Brick that is a Perfect Cuboid.

Proof. Recall that a Saunderson Euler Brick takes a Pythagorean triple (u, v, w) and gives the side lengths

$$\begin{aligned} a &= u\left|4v^2 - w^2\right| \\ b &= v\left|4u^2 - w^2\right| \\ c &= 4uvw \end{aligned}$$

which works out so each of the face diagonals are integral. The long diagonal can then be computed by

$$\begin{aligned} \ell^2 &= a^2 + b^2 + c^2 \\ &= u^2(4v^2 - w^2)^2 + v^2(4u^2 - w^2)^2 + 16u^2v^2w^2 \\ &= 16u^2v^4 + 16u^4v^2 + u^2w^4 + v^2w^4 \\ &= 16u^2v^2(u^2 + v^2) + w^4(u^2 + v^2) \\ &= (u^2 + v^2)(w^4 + 16u^2v^2) \\ &= w^2((u^2 + v^2)^2 + 16u^2v^2) \\ &= w^2(u^4 + 18u^2v^2 + v^4). \end{aligned}$$

And so the key point is that for some suitable $q \in \mathbb{Z}$ we have

$$q^2 = u^4 + 18u^2v^2 + v^4.$$

From here one may notice that this is a symmetric polynomial in u and v (that is, it doesn't change if we permute u and v). So, by the fundamental theorem of symmetric polynomials, we can express it as a polynomial in terms of the two elementary symmetric polynomials. In particular, if we substitute

$$\begin{aligned} \mu &\stackrel{\text{def}}{=} uv \\ \lambda &\stackrel{\text{def}}{=} u + v \end{aligned}$$

we can rewrite our diophantine equation as

$$q^2 = 20\mu^2 - 4\mu\lambda^2 + \lambda^4.$$

And, in fact, Mathematica can verify this.

```
In[1]:= SymmetricReduction[u^4 + v^4 + 18*u^2*v^2, {u, v}]
Out[1]= {20 u^2 v^2 - 4 u v (u + v)^2 + (u + v)^4, 0}
```

From here we can more or less we can try and recognize this as a conic in μ and λ^2. But, in particular, it's not an ordinary conic, since μ and λ^2 have special values. So, hoping to simplify things, we factor the λ^2 out of the above to get

$$q^2 = 20\mu^2 + \lambda^2(\lambda^2 - 4\mu).$$

But by our definitions above, we have

$$\lambda^2 - 4\mu = (u + v)^2 - 4uv = u^2 + v^2 - 2uv = (u - v)^2.$$

Substituting this result along with our value for λ we get

$$q^2 = 20\mu^2 + (u + v)^2(u - v)^2 = 20\mu^2 + (u^2 - v^2)^2.$$

That is, if we make the seemingly on-the-nose substitutions

$$\eta \stackrel{\text{def}}{=} 2\mu = 2uv$$
$$\zeta \stackrel{\text{def}}{=} \sqrt{\lambda^4 - 4\mu\lambda^2} = u^2 - v^2$$

we get simply

$$q^2 = 5\eta^2 + \zeta^2.$$

Now that's not saying much: that's more or less how we defined these variables. But looking at the form of these variables, we recognize them as being two legs of Euclid's parameterization of Pythagorean triples. That is, explicitly

$$\eta^2 + \zeta^2 = (2uv)^2 + (u^2 - v^2)^2 = u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2.$$

This means that we need some $\eta, \zeta \in \mathbb{Z}$ so that we have the integral perfect squares, let's call them $r, s \in \mathbb{Z}$ now, since this a slightly more general problem, so that

$$r^2 = \zeta^2 + 5\eta^2$$
$$s^2 = \zeta^2 + \eta^2$$

and we show that no such nontrivial $\eta, \zeta \in \mathbb{Q}^2$ can exist. We can consider the matrix equation

$$\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} \eta^2 \\ \zeta^2 \end{pmatrix} = \begin{pmatrix} r^2 \\ s^2 \end{pmatrix}$$

This is especially nice, because it gives a bit of geometric intuition. Indeed, we know that the vector on the left is of rational length. So if we scale down Euclidean 2-space so that vector is on the unit circle before applying the key linear transformation, we get a rational point on the unit circle. Algebraically, then, we multiply by the appropriate dilation matrix on both sides to get

$$\begin{pmatrix} \frac{1}{r^2} & 0 \\ 0 & \frac{1}{r^2} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} \eta^2 \\ \zeta^2 \end{pmatrix} = \begin{pmatrix} \frac{1}{r^2} & 0 \\ 0 & \frac{1}{r^2} \end{pmatrix} \begin{pmatrix} r^2 \\ s^2 \end{pmatrix}.$$

Note that our dilation is uniform in all directions, and is thus a scalar multiple of the identity matrix. This means, in particular, that it commutes with $\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix}$, since $AI = IA$ for all $A \in \mathrm{GL}(2, \mathbb{Q})$, because I is the identity of the group $\mathrm{GL}(2, \mathbb{Q})$. Thus, after re-scaling we can define

$$\eta' \stackrel{\text{def}}{=} \frac{\eta}{r}$$
$$\zeta' \stackrel{\text{def}}{=} \frac{\zeta}{r}$$
$$s' \stackrel{\text{def}}{=} \frac{s}{r}.$$

Whence our system is reduced to

$$\begin{pmatrix} 1 & 1 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} \eta'^2 \\ \zeta'^2 \end{pmatrix} = \begin{pmatrix} 1 \\ s'^2 \end{pmatrix}$$

From here, the key thing to note is that we we have $(\eta', \zeta') \in \mathbb{S}^1$; that is, that (η', ζ') lies on the unit circle. And of course $(\eta', \zeta') \in \mathbb{Q}^2$. And indeed, we can parameterize all rational points on the unit circle using the method of slopes (This calculation can be found, for instance, in [11]). In particular, we have

$$\eta'^2 + \zeta'^2 = 1$$

is a conic section with rational point at $(-1, 0)$. Thus, if we consider a line with slope m through the point $(-1, 0)$, something like

$$\zeta' = m(\eta' + 1)$$

its η' value of intersection with $\mathbb{S}^1$ is a quadratic with one rational root and rational coefficients, and so has its second root rational. And the ζ' coordinate is a line with rational coefficients evaluated at that η' value, so we get another rational point. And since any rational point on the unit circle has a rational slope to $(-1, 0)$, these points and slopes are in 1-1 correspondence. Thus we can compute all rational points on the unit circle in terms of this single rational parameter m. In particular, our quadratic for η' is

$$\eta'^2 + (m(\eta' + 1))^2 = 1.$$

Which gives

$$(1 + m^2)\eta'^2 + 2m^2\eta' + (m^2 - 1) = 0.$$

Whence the quadratic formula gives

$$\eta' = \frac{-2m^2 \pm \sqrt{4m^4 - 4\left(m^2+1\right)\left(m^2-1\right)}}{2\left(m^2+1\right)} = -1, \frac{1-m^2}{1+m^2}$$

and substituting the nontrivial solution back into our line gives

$$\zeta' = m\left(\frac{1-m^2}{1+m^2} + 1\right) = \frac{2m}{1+m^2}.$$

So, putting all this together, we can finally write (switching which is η and which is ζ, because it doesn't matter as m ranges over all of $\mathbb{Q}$, and this shall soon become slightly more convenient) that

$$(\zeta', \eta') = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right).$$

Thus, our second equation becomes

$$s'^2 = \zeta^2 + 5\eta^2 = \left(\frac{1-m^2}{1+m^2}\right)^2 + 5\left(\frac{2m}{1+m^2}\right)^2.$$

Making again substitution

$$t \stackrel{\text{def}}{=} s'(1 + m^2)$$

we get

$$t^2 = (1 - m^2)^2 + 5(2m)^2$$

or, simplifying

$$t^2 = m^4 + 18m^2 + 1.$$

This is an elliptic curve, and indeed, it has few rational points. We use standard theory to reduce the elliptic curve to Wierstrass form. There's a lot of theory on how to do this. See [7] for the particular technique behind what we do here, but skipping the algebra, with the substitution

$$m = \frac{y}{6x + 648}$$
$$t = \pm\frac{18m^2 + 54 - x}{18}$$

we get bi-rational equivalence to the elliptic curve

$$E : y^2 = x^3 - 9072x + 279936.$$

And indeed, using the theory of Elliptic curves we can show this curve has only 3 rational points and the point at infinity. In particular, SAGE can bound the corresponding L-function to show that E has analytic rank 0. Since BSD has been proven for curves with analytic rank 0 (See [15] for a reference on this proof),

```
sage: E = EllipticCurve([-9072, 279936])
sage: E.analytic_rank()
0
sage: G = E.torsion_subgroup()
sage: G
Torsion Subgroup isomorphic to Z/2 + Z/2 associated to the Elliptic Curve defined by y^2 = x^3 - 9072*x + 279936 over Rational Field
sage: G.gens()
((-108 : 0 : 1), (36 : 0 : 1))
sage: P = E(-108, 0)
sage: Q = E(36, 0)
sage: P+Q
(72 : 0 : 1)
sage:
```

Figure 3.2: SAGE finding all rational points on the elliptic curve $E : y^2 = x^3 - 9072x + 279936$

this implies that E has rank 0. Using Nagell-Lutz (which can be found in [10]), SAGE can also compute the torsion subgroup of E, which is isomorphic to the Klein 4 Group $\mathbb{Z}_2^2$. Thus, in particular we have

$$E(\mathbb{Q}) \cong \mathbb{Z}_2^2.$$

The SAGE worksheet used to show this and find all of the rational points is included in figure 3.2.

Thus E has only the rational points

$$(36, 0)$$
$$(72, 0)$$
$$(-108, 0)$$

and of course the point at infinity. The first two correspond to $m = 0$ and the other two to $m = \infty$. Either case corresponds to $\eta' = 0$. So any rational solution (as we reverse the scaling and move from $\eta' = 0$ to $\eta = 0$, since 0 times any number is 0) has $\eta = 0$. That is, we know that such a nontrivial pair (η, ζ) has $\eta = 0$. Thus, if (u, v, w) is a Pythagorean Triple that yields a Saunderson Euler Brick that is a perfect cuboid, we have that

$$\eta = 0 \iff 2uv = 0$$

so u or v is 0, so the cuboid is degenerate. Thus, there are no Saunderson perfect cuboids. ■

3.3.2 A Two-Parameter Rational Equivalent to the Perfect Cuboid Problem

Theorem 3.3. The problem of existence of a perfect cuboid is equivalent to the problem of nontrivial rational solutions to the system of equations

$$p^2 = (1 - r^2)^2(1 - s^2)^2 + 4s^2(1 + r^2)^2$$
$$q^2 = 4r^2(1 - s^2)^2 + 4s^2(1 + r^2)^2.$$

Proof. Consider an arbitrary rational perfect cuboid. Scale down all of space so that one of the face diagonals is 1 and note since the ratio of two rational squares is a rational square we still have a rational perfect cuboid. Then of two the edges, say x and y are rational numbers so that

$$x^2 + y^2 = 1.$$

This is a conic with a rational point, and therefore it can be rationally parameterized. In fact, this calculation has been done in the proof of theorem 3.2 above (also found in [11]). So, skipping the algebra and citing that result we get, with r rational, WLOG

$$x = \frac{1 - r^2}{1 + r^2}$$
$$y = \frac{2r}{1 + r^2}.$$

Then suppose the other scaled side now has length z. For some rational w (the scaled long diagonal), we then get

$$z^2 + 1 = w^2.$$

This again is a conic with a rational point, and so we can parameterize the rational z on this curve. One could again use the method of slopes from the proof of theorem 3.2, but leaving the details to the interested reader we get, with s rational

$$z = \frac{2s}{1 - s^2}.$$

Thus, the problem of a perfect cuboid is equivalent to the problem of nontrivial rational points on

$$q^2 = \left(\frac{2r}{1 + r^2}\right)^2 + \left(\frac{2s}{1 - s^2}\right)^2$$
$$p^2 = \left(\frac{1 - r^2}{1 + r^2}\right)^2 + \left(\frac{2s}{1 - s^2}\right)^2$$

which corresponds geometrically to the rationality of two non-one face diagonals. Since p and q are arbitrary, clearing denominators gives a polynomial equivalent

$$q^2 = 4r^2(1 - s^2)^2 + 4s^2(1 + r^2)^2$$
$$p^2 = (1 - r^2)^2(1 - s^2)^2 + 4s^2(1 + r^2)^2.$$

■

3.4 Modular Techniques

3.4.1 Parities of the Sides

Pythagorean Triples

Result 3.1. Modulo 2
$a^2 + b^2 = c^2$, by the Pythagorean Theorem (a proof of which can be found in [13]), where (a, b, c) is a Pythagorean Triple. Each of a, b and c can either be even or odd. So, we notice that a, b and c could have the following parities.

a	b	c
odd	odd	odd
odd	odd	even
odd	even	odd
odd	even	even
even	odd	odd
even	odd	even
even	even	odd
even	even	even

But, (a, b, c) cannot have the respective parities (o, o, o), (o, e, e), (e, o, e) or (e, e, o) because applying the rules of parity addition to them

$$o + o = e$$
$$e + o = o$$
$$e + e = e$$

and noting that squaring doesn't affect parity, contradicts the Pythagorean theorem. Eliminating these cases, we get a new list of possible parities

a	b	c
odd	odd	even
odd	even	odd
even	odd	odd
even	even	even

Also, since (o, e, o) is the same as (e, o, o) up to permutation of the legs, without loss of generality we can get rid of one of them.

a	b	c
odd	odd	even
odd	even	odd
even	even	even

Finally, after squaring a, b and c, and considering the remainders when dividing by 4, (o, o, e) does not work. One can write an odd integer as $2n+1$. Squaring, we get $4n^2+4n+1$. Taking this expression modulo 4, we get 1–that is, every odd number squared is congruent to 1 modulo 4. Likewise, every even number can be written as $2n$. Squaring gives $4n^2$, which is divisible by 4, so an even number squared is congruent to 0 modulo 4. According to the Pythagorean Theorem, $a^2 + b^2 = c^2$, and so if a and b are odd, and c is even, then the Pythagorean Theorem becomes $1 + 1 \equiv 0 \pmod 4$. Therefore, $2 \equiv 0 \pmod 4$, which is false. So, we can eliminate (o, o, e). This leaves us with our final result.

a	b	c
odd	even	odd
even	even	even

Therefore, the only two ways that the legs and hypotenuse of a Pythagorean triple can be even or odd is (o, e, o) and (e, e, e), up to permutation of the legs. An example of each is $(3, 4, 5)$ and $(6, 8, 10)$.

The Full Box

Result 3.2. The rest of the cuboid modulo 2.
In a primitive perfect cuboid, since all of a, b, c being even contradicts primitivity, WLOG let a be odd. Then by the above result b and c must be even, because they can only follow the triple parity of (o, e, o) in the Pythagorean triples (a, b, f) and (a, c, e) ($a^2 + b^2 = f^2$ and $a^2 + c^2 = e^2$). Therefore, e and f are both odd, by the same triples. Thus the triple (b, c, d) is (e, e, e), so d is even. Finally, from the triples (a, d, g), (b, e, g) and (c, f, g), all of which are (o, e, o) triples, g is odd. This is one way you can assign parities.

In a possibly not primitive cuboid, then, WLOG, if a were even, one of two things could happen. Either exactly one of b or c is odd (not both by the above result since (b, c, d) is a Pythagorean Triple), which is the same as before, up to permutation of the edges of the cuboid. So, neither b nor c can be odd, so they both must be even, and so d, e and f are all even, and so g is even. So, the other case is that a, b, c, d, e, f and g are all even. These are the two cases for the parities of the sides.

a	b	c	d	e	f	g
odd	even	even	even	odd	odd	odd
even	even	even	even	even	even	even

However, the all even case is not useful, since eventually, one can successively divide all the box's lengths by 2 to eventually get the other case. So, on only needs to consider the exactly two sides even case for a primitive perfect cuboid.

3.4.2 Parities of Sides Alternate Proof

An alternative method using modular arithmetic can be used to prove the following about a primitive perfect cuboid.

Theorem 3.4. **(I)** One edge must be odd and the other two edges must be divisible by four.
(II) Two face diagonals must be odd.
(III) The other face diagonal must be divisible by four.
(IV) The body diagonal must be odd.

Proof. We have by the definition of a cuboid (definition 3.1) that

$$\begin{aligned} d^2 &= b^2 + c^2 \\ e^2 &= a^2 + c^2 \\ f^2 &= a^2 + b^2 \\ g^2 &= a^2 + b^2 + c^2 = a^2 + d^2 = b^2 + e^2 = c^2 + f^2. \end{aligned}$$

As the cuboid is primitive, all three sides cannot be even, so WLOG we assume edge a is odd. Now suppose that edge c is also odd. This means that face diagonal e must be even. However, this leads to a contradiction. If e is even, then $e^2 \equiv 0 \pmod 4$. However, $e^2 \equiv a^2 + c^2 \equiv 1 + 1 \equiv 2 \not\equiv 0 \pmod 4$. So c cannot be odd. Similarly, edge b must also be even. If a is odd and b and c are even, then face diagonals e and f as well as the space diagonal g must be odd, while the face diagonal d must be even.

Now suppose that $c = 4x + 2$, where x is a positive integer. The square of any odd number must be equal to one modulo eight. However, since we have established e as odd $1 \equiv e^2 \equiv a^2 + c^2 \equiv 1 + 4 \equiv 5 \pmod 8$. This is a contradiction, so c must be divisible by 4. By the same logic, 4 is also a factor of b. As face diagonal $d = \sqrt{b^2 + c^2}$, and b and c are divisible by 4, d must also be divisible by 4.

■

3.4.3 Divisibility by 3

Theorem 3.5. Exactly two edges of any primitive perfect cuboid must be divisible by 3.

Proof. Note we have

$$\begin{aligned} d^2 &= b^2 + c^2 \\ e^2 &= a^2 + c^2 \\ f^2 &= a^2 + b^2 \\ g^2 &= a^2 + b^2 + c^2 = a^2 + f^2 = b^2 + e^2 = c^2 + d^2. \end{aligned}$$

As the cuboid is primitive, all three sides cannot be divisible by 3. Now suppose that a is divisible by 3, keeping the convention that a is odd. Then by the Chinese Remainder theorem we must have $a \equiv 3 \pmod 6$. Now given that b and c must be even (based on the above results), suppose that neither is divisible by 3. Then, again by the Chinese Remainder Theorem (which can be found in [1]), b and c are either congruent to 2 or 4 modulo 6.

Based on the equations above, as b and c are even, face diagonal d must also be even. So d^2 must be congruent to either 0 or 4 modulo 6. However, $b^2 + c^2 \equiv 2 \pmod 6$ regardless of the values of b and c. This creates a contradiction as

$$(0 \text{ or } 4) \equiv d^2 \equiv b^2 + c^2 \equiv 2 \pmod 6.$$

So at least one of b and c must be a multiple of 3.

Now suppose that a is not divisible by 3, and thus congruent to 1 or 5 modulo 6, b is not a multiple of 3, and thus is congruent to 2 or 4 modulo 6, and c is congruent to 0 modulo 6. (So, note chiefly that a and b are not multiples of 3, while c is a multiple of 6)

Given that g must be odd, g^2 must be congruent to 1 or 3 modulo 6. However, $a^2 + b^2 + c^2 \equiv 5 \pmod 6$. This creates a contradiction. Hence, either edge a or edge b must also be divisible by 3.

Now, the only remaining case is when none of a, b or c is divisible by 3. Suppose that edge a is then congruent to either 1 or 5 modulo 6, and edge b is congruent to either 2 or 4 modulo 6. As per the argument above, this means that face diagonal f must be odd, therefore f^2 is congruent to 1 or 3 modulo 6. However, $a^2+b^2 \equiv 5 \pmod 6$. Based on this contradiction, one of these two sides must be divisible by 3. Furthermore, using the previous cases, we can see that if a is divisible by 3, then either b or c must be divisible by 6, and if b is divisible by 3, then either a or c must also be divisible by 3. So, 2 of the edges in a primitive perfect cuboid must be divisible by 3. ■

3.4.4 Divisibility by 5, 7, 11, 19

Theorem 3.6. In a perfect cuboid (a, b, c, d, e, f, g), at least 1 of a, b, and c is divisible by 5, 7, 11, and 19, and at least 1 of (a, b, c, d, e, f, g) is divisible by 13 and 17.

Proof. By exhaustion. Checking all p^3 possibilities, we give all cuboids with 0, 1, 2, and 3 nonzero elements in $\mathbb{F}_p$ for each prime p above.

p	2 zeros	1 zero	no zeros
5	(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 1, 0, 1), (0, 0, 4, 1, 1, 0, 1), (0, 0, 2, 4, 4, 0, 4), (0, 0, 3, 4, 4, 0, 4)	(0, 1, 2, 0, 4, 1, 0), (0, 1, 3, 0, 4, 1, 0), (0, 4, 2, 0, 4, 1, 0), (0, 4, 3, 0, 4, 1, 0)	
7	(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 1, 0, 1), (0, 0, 6, 1, 1, 0, 1), (0, 0, 2, 4, 4, 0, 4), (0, 0, 5, 4, 4, 0, 4), (0, 0, 3, 2, 2, 0, 2), (0, 0, 4, 2, 2, 0, 2)	(0, 1, 1, 2, 1, 1, 2), (0, 1, 6, 2, 1, 1, 2), (0, 6, 1, 2, 1, 1, 2), (0, 6, 6, 2, 1, 1, 2), (0, 2, 2, 1, 4, 4, 1), (0, 2, 5, 1, 4, 4, 1), (0, 5, 2, 1, 4, 4, 1), (0, 5, 5, 1, 4, 4, 1), (0, 3, 3, 4, 2, 2, 4), (0, 3, 4, 4, 2, 2, 4), (0, 4, 3, 4, 2, 2, 4), (0, 4, 4, 4, 2, 2, 4)	
11	(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 1, 0, 1), (0, 0, 10, 1, 1, 0, 1), (0, 0, 2, 4, 4, 0, 4), (0, 0, 9, 4, 4, 0, 4), (0, 0, 3, 9, 9, 0, 9), (0, 0, 8, 9, 9, 0, 9), (0, 0, 4, 5, 5, 0, 5), (0, 0, 7, 5, 5, 0, 5), (0, 0, 5, 3, 3, 0, 3), (0, 0, 6, 3, 3, 0, 3)	(0, 1, 2, 5, 4, 1, 5), (0, 1, 9, 5, 4, 1, 5), (0, 10, 2, 5, 4, 1, 5), (0, 10, 9, 5, 4, 1, 5), (0, 1, 5, 4, 3, 1, 4), (0, 1, 6, 4, 3, 1, 4), (0, 10, 5, 4, 3, 1, 4), (0, 10, 6, 4, 3, 1, 4), (0, 2, 4, 9, 5, 4, 9), (0, 2, 7, 9, 5, 4, 9), (0, 9, 4, 9, 5, 4, 9), (0, 9, 7, 9, 5, 4, 9), (0, 3, 4, 3, 5, 9, 3), (0, 3, 7, 3, 5, 9, 3), (0, 8, 4, 3, 5, 9, 3), (0, 8, 7, 3, 5, 9, 3), (0, 3, 5, 1, 3, 9, 1), (0, 3, 6, 1, 3, 9, 1), (0, 8, 5, 1, 3, 9, 1), (0, 8, 6, 1, 3, 9, 1)	

13	(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 1, 0, 1), (0, 0, 12, 1, 1, 0, 1), (0, 0, 2, 4, 4, 0, 4), (0, 0, 11, 4, 4, 0, 4), (0, 0, 3, 9, 9, 0, 9), (0, 0, 10, 9, 9, 0, 9), (0, 0, 4, 3, 3, 0, 3), (0, 0, 9, 3, 3, 0, 3), (0, 0, 5, 12, 12, 0, 12), (0, 0, 8, 12, 12, 0, 12), (0, 0, 6, 10, 10, 0, 10), (0, 0, 7, 10, 10, 0, 10)	(0, 1, 3, 10, 9, 1, 10), (0, 1, 10, 10, 9, 1, 10), (0, 12, 3, 10, 9, 1, 10), (0, 12, 10, 10, 9, 1, 10), (0, 1, 4, 4, 3, 1, 4), (0, 1, 9, 4, 3, 1, 4), (0, 12, 4, 4, 3, 1, 4), (0, 12, 9, 4, 3, 1, 4), (0, 1, 5, 0, 12, 1, 0), (0, 1, 8, 0, 12, 1, 0), (0, 12, 5, 0, 12, 1, 0), (0, 12, 8, 0, 12, 1, 0), (0, 2, 3, 0, 9, 4, 0), (0, 2, 10, 0, 9, 4, 0), (0, 11, 3, 0, 9, 4, 0), (0, 11, 10, 0, 9, 4, 0), (0, 2, 5, 3, 12, 4, 3), (0, 2, 8, 3, 12, 4, 3), (0, 11, 5, 3, 12, 4, 3), (0, 11, 8, 3, 12, 4, 3), (0, 2, 6, 1, 10, 4, 1), (0, 2, 7, 1, 10, 4, 1), (0, 11, 6, 1, 10, 4, 1), (0, 11, 7, 1, 10, 4, 1), (0, 3, 4, 12, 3, 9, 12), (0, 3, 9, 12, 3, 9, 12), (0, 10, 4, 12, 3, 9, 12), (0, 10, 9, 12, 3, 9, 12), (0, 4, 6, 0, 10, 3, 0), (0, 4, 7, 0, 10, 3, 0), (0, 9, 6, 0, 10, 3, 0), (0, 9, 7, 0, 10, 3, 0), (0, 5, 6, 9, 10, 12, 9), (0, 5, 7, 9, 10, 12, 9), (0, 8, 6, 9, 10, 12, 9), (0, 8, 7, 9, 10, 12, 9)	(1, 3, 4, 12, 4, 10, 0), (1, 3, 9, 12, 4, 10, 0), (1, 10, 4, 12, 4, 10, 0), (1, 10, 9, 12, 4, 10, 0), (12, 3, 4, 12, 4, 10, 0), (12, 3, 9, 12, 4, 10, 0), (12, 10, 4, 12, 4, 10, 0), (12, 10, 9, 12, 4, 10, 0), (2, 5, 6, 9, 1, 3, 0), (2, 5, 7, 9, 1, 3, 0), (2, 8, 6, 9, 1, 3, 0), (2, 8, 7, 9, 1, 3, 0), (11, 5, 6, 9, 1, 3, 0), (11, 5, 7, 9, 1, 3, 0), (11, 8, 6, 9, 1, 3, 0), (11, 8, 7, 9, 1, 3, 0)

17	(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 1, 0, 1), (0, 0, 16, 1, 1, 0, 1), (0, 0, 2, 4, 4, 0, 4), (0, 0, 15, 4, 4, 0, 4), (0, 0, 3, 9, 9, 0, 9), (0, 0, 14, 9, 9, 0, 9), (0, 0, 4, 16, 16, 0, 16), (0, 0, 13, 16, 16, 0, 16), (0, 0, 5, 8, 8, 0, 8), (0, 0, 12, 8, 8, 0, 8), (0, 0, 6, 2, 2, 0, 2), (0, 0, 11, 2, 2, 0, 2), (0, 0, 7, 15, 15, 0, 15), (0, 0, 10, 15, 15, 0, 15), (0, 0, 8, 13, 13, 0, 13), (0, 0, 9, 13, 13, 0, 13)	(0, 1, 1, 2, 1, 1, 2), (0, 1, 16, 2, 1, 1, 2), (0, 16, 1, 2, 1, 1, 2), (0, 16, 16, 2, 1, 1, 2), (0, 1, 4, 0, 16, 1, 0), (0, 1, 13, 0, 16, 1, 0), (0, 16, 4, 0, 16, 1, 0), (0, 16, 13, 0, 16, 1, 0), (0, 1, 5, 9, 8, 1, 9), (0, 1, 12, 9, 8, 1, 9), (0, 16, 5, 9, 8, 1, 9), (0, 16, 12, 9, 8, 1, 9), (0, 1, 7, 16, 15, 1, 16), (0, 1, 10, 16, 15, 1, 16), (0, 16, 7, 16, 15, 1, 16), (0, 16, 10, 16, 15, 1, 16), (0, 2, 2, 8, 4, 4, 8), (0, 2, 15, 8, 4, 4, 8), (0, 15, 2, 8, 4, 4, 8), (0, 15, 15, 8, 4, 4, 8), (0, 2, 3, 13, 9, 4, 13), (0, 2, 14, 13, 9, 4, 13), (0, 15, 3, 13, 9, 4, 13), (0, 15, 14, 13, 9, 4, 13), (0, 2, 7, 2, 15, 4, 2), (0, 2, 10, 2, 15, 4, 2), (0, 15, 7, 2, 15, 4, 2), (0, 15, 10, 2, 15, 4, 2), (0, 2, 8, 0, 13, 4, 0), (0, 2, 9, 0, 13, 4, 0), (0, 15, 8, 0, 13, 4, 0), (0, 15, 9, 0, 13, 4, 0), (0, 3, 3, 1, 9, 9, 1), (0, 3, 14, 1, 9, 9, 1), (0, 14, 3, 1, 9, 9, 1), (0, 14, 14, 1, 9, 9, 1), (0, 3, 4, 8, 16, 9, 8), (0, 3, 13, 8, 16, 9, 8), (0, 14, 4, 8, 16, 9, 8), (0, 14, 13, 8, 16, 9, 8), (0, 3, 5, 0, 8, 9, 0), (0, 3, 12, 0, 8, 9, 0), (0, 14, 5, 0, 8, 9, 0), (0, 14, 12, 0, 8, 9, 0), (0, 4, 4, 15, 16, 16, 15), (0, 4, 13, 15, 16, 16, 15), (0, 13, 4, 15, 16, 16, 15), (0, 13, 13, 15, 16, 16, 15), (0, 4, 6, 1, 2, 16, 1), (0, 4, 11, 1, 2, 16, 1), (0, 13, 6, 1, 2, 16, 1), (0, 13, 11, 1, 2, 16, 1), (0, 5, 5, 16, 8, 8, 16), (0, 5, 12, 16, 8, 8, 16), (0, 12, 5, 16, 8, 8, 16), (0, 12, 12, 16, 8, 8, 16), (0, 5, 8, 4, 13, 8, 4), (0, 5, 9, 4, 13, 8, 4), (0, 12, 8, 4, 13, 8, 4), (0, 12, 9, 4, 13, 8, 4), (0, 6, 6, 4, 2, 2, 4), (0, 6, 11, 4, 2, 2, 4), (0, 11, 6, 4, 2, 2, 4), (0, 11, 11, 4, 2, 2, 4), (0, 6, 7, 0, 15, 2, 0), (0, 6, 10, 0, 15, 2, 0), (0, 11, 7, 0, 15, 2, 0), (0, 11, 10, 0, 15, 2, 0), (0, 6, 8, 15, 13, 2, 15), (0, 6, 9, 15, 13, 2, 15), (0, 11, 8, 15, 13, 2, 15), (0, 11, 9, 15, 13, 2, 15), (0, 7, 7, 13, 15, 15, 13), (0, 7, 10, 13, 15, 15, 13), (0, 10, 7, 13, 15, 15, 13), (0, 10, 10, 13, 15, 15, 13), (0, 8, 8, 9, 13, 13, 9), (0, 8, 9, 9, 13, 13, 9), (0, 9, 8, 9, 13, 13, 9), (0, 9, 9, 9, 13, 13, 9)	(1, 1, 4, 0, 0, 2, 1), (1, 1, 13, 0, 0, 2, 1), (1, 16, 4, 0, 0, 2, 1), (1, 16, 13, 0, 0, 2, 1), (16, 1, 4, 0, 0, 2, 1), (16, 1, 13, 0, 0, 2, 1), (16, 16, 4, 0, 0, 2, 1), (16, 16, 13, 0, 0, 2, 1), (1, 1, 7, 16, 16, 2, 0), (1, 1, 10, 16, 16, 2, 0), (1, 16, 7, 16, 16, 2, 0), (1, 16, 10, 16, 16, 2, 0), (16, 1, 7, 16, 16, 2, 0), (16, 1, 10, 16, 16, 2, 0), (16, 16, 7, 16, 16, 2, 0), (16, 16, 10, 16, 16, 2, 0), (1, 4, 4, 15, 0, 0, 16), (1, 4, 13, 15, 0, 0, 16), (1, 13, 4, 15, 0, 0, 16), (1, 13, 13, 15, 0, 0, 16), (16, 4, 4, 15, 0, 0, 16), (16, 4, 13, 15, 0, 0, 16), (16, 13, 4, 15, 0, 0, 16), (16, 13, 13, 15, 0, 0, 16), (1, 5, 5, 16, 9, 9, 0), (1, 5, 12, 16, 9, 9, 0), (1, 12, 5, 16, 9, 9, 0), (1, 12, 12, 16, 9, 9, 0), (16, 5, 5, 16, 9, 9, 0), (16, 5, 12, 16, 9, 9, 0), (16, 12, 5, 16, 9, 9, 0), (16, 12, 12, 16, 9, 9, 0), (2, 2, 3, 13, 13, 8, 0), (2, 2, 14, 13, 13, 8, 0), (2, 15, 3, 13, 13, 8, 0), (2, 15, 14, 13, 13, 8, 0), (15, 2, 3, 13, 13, 8, 0), (15, 2, 14, 13, 13, 8, 0), (15, 15, 3, 13, 13, 8, 0), (15, 15, 14, 13, 13, 8, 0), (2, 2, 8, 0, 0, 8, 4), (2, 2, 9, 0, 0, 8, 4), (2, 15, 8, 0, 0, 8, 4), (2, 15, 9, 0, 0, 8, 4), (15, 2, 8, 0, 0, 8, 4), (15, 2, 9, 0, 0, 8, 4), (15, 15, 8, 0, 0, 8, 4), (15, 15, 9, 0, 0, 8, 4), (2, 7, 7, 13, 2, 2, 0), (2, 7, 10, 13, 2, 2, 0), (2, 10, 7, 13, 2, 2, 0), (2, 10, 10, 13, 2, 2, 0), (15, 7, 7, 13, 2, 2, 0), (15, 7, 10, 13, 2, 2, 0), (15, 10, 7, 13, 2, 2, 0), (15, 10, 10, 13, 2, 2, 0), (2, 8, 8, 9, 0, 0, 13), (2, 8, 9, 9, 0, 0, 13), (2, 9, 8, 9, 0, 0, 13), (2, 9, 9, 9, 0, 0, 13), (15, 8, 8, 9, 0, 0, 13), (15, 8, 9, 9, 0, 0, 13), (15, 9, 8, 9, 0, 0, 13), (15, 9, 9, 9, 0, 0, 13), (3, 3, 4, 8, 8, 1, 0), (3, 3, 13, 8, 8, 1, 0), (3, 14, 4, 8, 8, 1, 0), (3, 14, 13, 8, 8, 1, 0), (14, 3, 4, 8, 8, 1, 0), (14, 3, 13, 8, 8, 1, 0), (14, 14, 4, 8, 8, 1, 0), (14, 14, 13, 8, 8, 1, 0), (3, 3, 5, 0, 0, 1, 9), (3, 3, 12, 0, 0, 1, 9), (3, 14, 5, 0, 0, 1, 9), (3, 14, 12, 0, 0, 1, 9), (14, 3, 5, 0, 0, 1, 9), (14, 3, 12, 0, 0, 1, 9), (14, 14, 5, 0, 0, 1, 9), (14, 14, 12, 0, 0, 1, 9), (3, 5, 5, 16, 0, 0, 8), (3, 5, 12, 16, 0, 0, 8), (3, 12, 5, 16, 0, 0, 8), (3, 12, 12, 16, 0, 0, 8), (14, 5, 5, 16, 0, 0, 8), (14, 5, 12, 16, 0, 0, 8), (14, 12, 5, 16, 0, 0, 8), (14, 12, 12, 16, 0, 0, 8), (4, 4, 6, 1, 1, 15, 0), (4, 4, 11, 1, 1, 15, 0), (4, 13, 6, 1, 1, 15, 0), (4, 13, 11, 1, 1, 15, 0), (13, 4, 6, 1, 1, 15, 0), (13, 4, 11, 1, 1, 15, 0), (13, 13, 6, 1, 1, 15, 0), (13, 13, 11, 1, 1, 15, 0), (5, 8, 8, 9, 4, 4, 0), (5, 8, 9, 9, 4, 4, 0), (5, 9, 8, 9, 4, 4, 0), (5, 9, 9, 9, 4, 4, 0), (12, 8, 8, 9, 4, 4, 0), (12, 8, 9, 9, 4, 4, 0), (12, 9, 8, 9, 4, 4, 0), (12, 9, 9, 9, 4, 4, 0), (6, 6, 7, 0, 0, 4, 2), (6, 6, 10, 0, 0, 4, 2), (6, 11, 7, 0, 0, 4, 2), (6, 11, 10, 0, 0, 4, 2), (11, 6, 7, 0, 0, 4, 2), (11, 6, 10, 0, 0, 4, 2), (11, 11, 7, 0, 0, 4, 2), (11, 11, 10, 0, 0, 4, 2), (6, 6, 8, 15, 15, 4, 0), (6, 6, 9, 15, 15, 4, 0), (6, 11, 8, 15, 15, 4, 0), (6, 11, 9, 15, 15, 4, 0), (11, 6, 8, 15, 15, 4, 0), (11, 6, 9, 15, 15, 4, 0), (11, 11, 8, 15, 15, 4, 0), (11, 11, 9, 15, 15, 4, 0), (6, 7, 7, 13, 0, 0, 15), (6, 7, 10, 13, 0, 0, 15), (6, 10, 7, 13, 0, 0, 15), (6, 10, 10, 13, 0, 0, 15), (11, 7, 7, 13, 0, 0, 15), (11, 7, 10, 13, 0, 0, 15), (11, 10, 7, 13, 0, 0, 15), (11, 10, 10, 13, 0, 0, 15)

19	(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 1, 0, 1), (0, 0, 18, 1, 1, 0, 1), (0, 0, 2, 4, 4, 0, 4), (0, 0, 17, 4, 4, 0, 4), (0, 0, 3, 9, 9, 0, 9), (0, 0, 16, 9, 9, 0, 9), (0, 0, 4, 16, 16, 0, 16), (0, 0, 15, 16, 16, 0, 16), (0, 0, 5, 6, 6, 0, 6), (0, 0, 14, 6, 6, 0, 6), (0, 0, 6, 17, 17, 0, 17), (0, 0, 13, 17, 17, 0, 17), (0, 0, 7, 11, 11, 0, 11), (0, 0, 12, 11, 11, 0, 11), (0, 0, 8, 7, 7, 0, 7), (0, 0, 11, 7, 7, 0, 7), (0, 0, 9, 5, 5, 0, 5), (0, 0, 10, 5, 5, 0, 5)	(0, 1, 2, 5, 4, 1, 5), (0, 1, 17, 5, 4, 1, 5), (0, 18, 2, 5, 4, 1, 5), (0, 18, 17, 5, 4, 1, 5), (0, 1, 4, 17, 16, 1, 17), (0, 1, 15, 17, 16, 1, 17), (0, 18, 4, 17, 16, 1, 17), (0, 18, 15, 17, 16, 1, 17), (0, 1, 5, 7, 6, 1, 7), (0, 1, 14, 7, 6, 1, 7), (0, 18, 5, 7, 6, 1, 7), (0, 18, 14, 7, 6, 1, 7), (0, 1, 9, 6, 5, 1, 6), (0, 1, 10, 6, 5, 1, 6), (0, 18, 9, 6, 5, 1, 6), (0, 18, 10, 6, 5, 1, 6), (0, 2, 4, 1, 16, 4, 1), (0, 2, 15, 1, 16, 4, 1), (0, 17, 4, 1, 16, 4, 1), (0, 17, 15, 1, 16, 4, 1), (0, 2, 8, 11, 7, 4, 11), (0, 2, 11, 11, 7, 4, 11), (0, 17, 8, 11, 7, 4, 11), (0, 17, 11, 11, 7, 4, 11), (0, 2, 9, 9, 5, 4, 9), (0, 2, 10, 9, 5, 4, 9), (0, 17, 9, 9, 5, 4, 9), (0, 17, 10, 9, 5, 4, 9), (0, 3, 4, 6, 16, 9, 6), (0, 3, 15, 6, 16, 9, 6), (0, 16, 4, 6, 16, 9, 6), (0, 16, 15, 6, 16, 9, 6), (0, 3, 6, 7, 17, 9, 7), (0, 3, 13, 7, 17, 9, 7), (0, 16, 6, 7, 17, 9, 7), (0, 16, 13, 7, 17, 9, 7), (0, 3, 7, 1, 11, 9, 1), (0, 3, 12, 1, 11, 9, 1), (0, 16, 7, 1, 11, 9, 1), (0, 16, 12, 1, 11, 9, 1), (0, 3, 8, 16, 7, 9, 16), (0, 3, 11, 16, 7, 9, 16), (0, 16, 8, 16, 7, 9, 16), (0, 16, 11, 16, 7, 9, 16), (0, 4, 8, 4, 7, 16, 4), (0, 4, 11, 4, 7, 16, 4), (0, 15, 8, 4, 7, 16, 4), (0, 15, 11, 4, 7, 16, 4), (0, 5, 6, 4, 17, 6, 4), (0, 5, 13, 4, 17, 6, 4), (0, 14, 6, 4, 17, 6, 4), (0, 14, 13, 4, 17, 6, 4), (0, 5, 7, 17, 11, 6, 17), (0, 5, 12, 17, 11, 6, 17), (0, 14, 7, 17, 11, 6, 17), (0, 14, 12, 17, 11, 6, 17), (0, 5, 9, 11, 5, 6, 11), (0, 5, 10, 11, 5, 6, 11), (0, 14, 9, 11, 5, 6, 11), (0, 14, 10, 11, 5, 6, 11), (0, 6, 7, 9, 11, 17, 9), (0, 6, 12, 9, 11, 17, 9), (0, 13, 7, 9, 11, 17, 9), (0, 13, 12, 9, 11, 17, 9), (0, 6, 8, 5, 7, 17, 5), (0, 6, 11, 5, 7, 17, 5), (0, 13, 8, 5, 7, 17, 5), (0, 13, 11, 5, 7, 17, 5), (0, 7, 9, 16, 5, 11, 16), (0, 7, 10, 16, 5, 11, 16), (0, 12, 9, 16, 5, 11, 16), (0, 12, 10, 16, 5, 11, 16)	

this exhaustive search gives the result directly. Source code for this check is given in Appendix B. ■

3.4.5 Nature of Divisors of the Body Diagonal

Theorem 3.7. Any divisor of the space diagonal in a primitve perfect cuboid must be congruent to 1 modulo 4.

Proof. We prove in particular that every prime divisor of the long diagonal must be congruent to 1 modulo 4. As the space diagonal must be odd (by Theorem 3.4), any divisor must be congruent to either 1 or 3 modulo 4.

Now suppose that $x \equiv 3 \pmod 4$ is a divisor of g. Then, the conditions of a cuboid give

$$d^2 = b^2 + c^2$$
$$e^2 = a^2 + c^2$$
$$f^2 = a^2 + b^2$$
$$g^2 = a^2 + b^2 + c^2 = a^2 + d^2 = b^2 + e^2 = c^2 + f^2$$

Taking the last of these conditions modulo x gives us

$$g^2 \equiv a^2 + d^2 \equiv 0 \pmod{x}.$$

Next we claim edge a must be divisible by x. Suppose x is not a factor of a. Then x and a are relatively prime (since x is prime), so by Bézout's identity (which can be found in [1]) there must be integers m and n such that

$$am + nx = 1.$$

Hence

$$am \equiv 1 \pmod{x}.$$

So

$$m \equiv a^{-1} \pmod{x}.$$

Let

$$\left(\frac{a}{p}\right)$$

denote the Legendre symbol. Then by Euler's criterion (which can also be found in [1]), we have

$$\left(\frac{-1}{x}\right) = (-1)^{\frac{x-1}{2}}.$$

Supposing $x = 4k + 3$ for some integer k, we get

$$\begin{aligned}\left(\frac{-1}{x}\right) &= (-1)^{\frac{x-1}{2}} \\ &= (-1)^{\frac{4k+2}{2}} \\ &= (-1)^{2k+1} \\ &= -1.\end{aligned}$$

So that -1 is a quadratic nonresidue modulo x. However

$$\begin{aligned}\left(a^{-1}d\right)^2 + 1 &\equiv (a^{-2})(a^2 + d^2) \pmod{x} \\ &\equiv a^{-2} \cdot 0 \pmod{x} \\ &\equiv 0 \pmod{x}\end{aligned}$$

since $g^2 = a^2 + d^2$ and by assumption $x \mid g$. Thus

$$(a^{-1}d)^2 \equiv -1 \pmod{x}$$

which suggests -1 is a quadratic residue modulo x. This, in turn, contradicts -1 being a quadratic nonresidue modulo x. Thus we have arbitrarily that $x \mid a$. Yet, this result uses no properties about the other two sides. Thus, in particular, by the same logic, we have $x \mid b$ and $x \mid c$. Thus, the cuboid cannot be primitive. Thus, any prime divisor of the long diagonal in a primitive perfect cuboid must be congruent to 1 modulo 4. Thus, since the long diagonal in a primitive cuboid we already have is odd, this gives us that any divisor of the long diagonal is congruent to 1 modulo 4.

■

Corollary 3.1. The body diagonal in a primitive perfect cuboid must be congruent to 1 modulo 4.

3.5 Prime Powers

3.5.1 Divisibility of One of the sides by 16

Lemma 3.1. In a Pythagorean triple (a, b, c), 4 divides at least 1 of a and b.

Proof. A theorem of Euclid (which can be found in [6]) states that any primitive Pythagorean triple can be paramaterized as

$$\left(u^2 - v^2, 2uv, u^2 + v^2\right)$$

for positive integers u and v. If b is divisible by 4, we are done. Otherwise, b is not divisible by 4, then both u and v are odd. Then

$$a \equiv u^2 - v^2 \equiv 1 - 1 \equiv 0 \pmod 4$$

so $4|a$. Since this property is invariant when scaling the triple by an integer, proving it for all primitive implies the result for all Pythagorean triples. ■

Theorem 3.8. In any Perfect Cuboid, at least one of the sides is divisible by 16.

Proof. $(a, b, f), (a, c, e),$ and $, (b, c, d)$ are all Pythagorean triples. So by the pigeonhole principle (which can be found in [1]) and the above Lemma 3.1, at least two of $a, b,$ and c must be divisible by 4. WLOG, let these be a and b. Then taking $a' = a/\gcd(a, b)$ and $b' = b/\gcd(a, b)$ gives us (a', b', f') is a Pythagorean triple for some f'. So one of a' and b' is divisible by 4. And since $4|a$ and $4|b$ we have $4|\gcd(a, b)$ so that either $16|a$ or $16|b$. ■

3.5.2 Divisibility of One of the sides by 9

Lemma 3.2. In a Pythagorean triple (a, b, c), at least one of a and b is divisible by 3.

Proof. By contradiction. Suppose not. Then a and b are both nonzero modulo 3, then a^2 and b^2 are both 1 modulo 3, so

$$a^2 + b^2 \equiv c^2 \equiv 1 + 1 \equiv 2 \pmod 3$$

which is a contradiction, since 2 is not a quadratic residue modulo 3. ■

Theorem 3.9. In any perfect Cuboid, at least one of the sides is divisible by 9

Proof. $(a, b, f), (a, c, e),$ and $, (b, c, d)$ are all Pythagorean triples. So by the pigeonhole principle and the above Lemma 3.2, at least two of $a, b,$ and c must be divisible by 3. WLOG, let these be a and b. Then taking $a' = a/\gcd(a, b)$ and $b' = b/\gcd(a, b)$ gives us (a', b', f') is a Pythagorean Triple for some f'. So one of a' and b' is divisible by 3. And since $3|a$ and $3|b$ we have $3|\gcd(a, b)$ so that either $9|a$ or $9|b$. ■

3.6 On Factors in Pythagorean Triples

3.6.1 Multiples of 3, 4, and 5 in Pythagorean Triples

Theorem 3.10. Let (a, b, c) be a Pythagorean triple, then $abc \equiv 0 \pmod{60}$.That is, $3, 4,$ and 5 are all factors of at least one of a, b, c.

Proof. Multiples of 3:
The sequence of remainders modulo 3 of the squares of all non-negative integers is 0, 1, 1, 0, 1, 1, 0, ... To prove this pattern we first consider the case of integers congruent to 0 modulo 3. For $3n$ we have

$$\begin{aligned}(3n)^2 &\equiv 3 \cdot (3 \cdot n^2) \\ &\equiv 0 \pmod 3.\end{aligned}$$

Now we can try the case $3n + 1$

$$(3n+1)^2 \equiv 9n^2 + 6n + 1 \equiv 3 \cdot (3n^2 + 2n) + 1$$
$$\equiv 0 + 1 \equiv 1 \pmod 3.$$

Now we can try $3n + 2$

$$(3n+2)^2 \equiv 9n^2 + 12n + 4 \equiv 3 \cdot (3n^2 + 4n) + 4$$
$$\equiv 0 + 4 \equiv 4 \equiv 1 \pmod 3$$

Thus the values of the squares modulo 3 are precisely 0 and 1. The only way squares can sum to squares modulo 3 are, then

$$0 + 0 \equiv 0 \pmod 3$$
$$0 + 1 \equiv 1 \pmod 3.$$

And, in each of these equations, at least one value is 0. Since values 0 modulo 3 correspond to multiples of 3, we have that there is always a multiple of 3 in any Pythagorean Triple.

Multiples of 4 We begin by noting algebraically that

$$a^2 + b^2 = c^2 \iff b^2 = c^2 - a^2 = (c + a) \cdot (c - a).$$

Now the squares modulo 4 are the following

$$0^2 \equiv 0 \pmod 4$$
$$1^2 \equiv 1 \pmod 4$$
$$2^2 \equiv 0 \pmod 4$$
$$3^2 \equiv 1 \pmod 4$$

Since we know b^2 has to be congruent to $0 \pmod 4$ or $1 \pmod 4$ we can eliminate a lot of the possibilities. Note that if both a and c have the same remainder when divided by 4 then it follows that

$$b^2 \equiv 0 \pmod 4$$

because of the $(c - a)$ factor in our above expression. Similarly if c and a have the same remainder when divided by 4 but with different signs (for example $3 \pmod 4$ and $1 \pmod 4$ satisfy that because $3 \equiv -1 \pmod 4$) then

$$b^2 \equiv 0 \pmod 4$$

and hence b is also congruent to $0 \pmod 4$ because of the $(c + a)$ factor in our above expression.

Thus, the only case to potentially have no elements of the triple be divisible by 4 is if one of a or c is equivalent to 1 or $3 \pmod 4$ and the other is equivalent to $2 \pmod 4$. Then

$$b^2 = 1 \cdot 3 \equiv 3 \pmod 4.$$

But 3 is a quadratic nonresidue modulo 4 and thus this case cannot occur. Hence, any primitive Pythagorean triple must include a multiple of 4.

Multiples of 5

The sequence of residues modulo 5 of the squares of all nonnegative integers is 0, 1, 4, 4, 1, 0, 1, ...

To prove this pattern we look first at numbers congruent to 0 modulo 5. We have for $5n$

$$(5n)^2 \equiv 5 \cdot (5 \cdot n^2)$$
$$\equiv 0 \pmod 5.$$

Now we can check $5n + 1$

$$\begin{aligned}(5n+1)^2 &\equiv 25n^2+10n+1 \equiv 5\cdot(5n^2+2n)+1\\ &\equiv 0+1 \equiv 1 \pmod 5.\end{aligned}$$

Now we can try $5n+2$

$$\begin{aligned}(5n+2)^2 &\equiv 25n^2+20n+4 \equiv 5\cdot(5n^2+4n)+4\\ &\equiv 0+4 \equiv 4 \pmod 5.\end{aligned}$$

Now we can try $5n+3$

$$\begin{aligned}(5n+3)^2 &\equiv 25n^2+30n+9 \equiv 5\cdot(5n^2+6n)+9\\ &\equiv 0+9 \equiv 9 \equiv 4 \pmod 5.\end{aligned}$$

And finally we try $5n+4$

$$\begin{aligned}(5n+4)^2 &\equiv 25n^2+40n+1 \equiv 5\cdot(5n^2+2n)+16\\ &\equiv 0+16 \equiv 16 \equiv 1 \pmod 5.\end{aligned}$$

Thus 0, 1, and 4 are the quadratic residues modulo 5. The only ways two quadratic residues can sum to another, modulo 5, are, then

$$\begin{aligned}0+0 &\equiv 0 \pmod 5\\ 1+0 &\equiv 1 \pmod 5\\ 4+0 &\equiv 4 \pmod 5\\ 4+1 &\equiv 0 \pmod 5.\end{aligned}$$

Note that each of these equations have at least one element congruent to 0 modulo 5, and therefore each corresponding triple contains an element divisible by 5. Therefore, there is always a multiple of 5 in any Pythagorean triple. ■

3.6.2 Multiples of Pythagorean Triples

In a Pythagorean triple (a, b, c), either a or b must be a multiple of 3, either a or b value must be a multiple of 4, and one of a, b or c must be multiple of 5. These divisibility properties by 3, 4, and 5 can be multiplied in different ways to create various combinations of residues classes that can be used in Pythagorean triples. The chart below shows the combinations of a, b and c which can be multiplied by constants to create Pythagorean triples:

a	b	c
3	4	5
5	12	X
X	12	5
4	15	X
3	20	X
X	60	X

where the Xs that appear in the chart signify numbers in a Pythagorean triple that are multiples of none of 3, 4, or 5. For example, take $(3, 20, X)$. By multiplying the 3 by 5 and the 20 by 1, we receive $(15, 20, X)$. We can use the Pythagorean theorem to find the value of X which would be, in this case, 25. One could think of every X as a 1, and it can be multiplied by any constant that is not a multiple of 3, 4, or 5. Note that this is not a sufficient condition for generation of Pythagorean triple, but it is a necessary one.

Chapter 4

Perfect Numbers

4.1 Problem Statement

Definition 4.1. We define a perfect number, $n \in \mathbb{Z}^+$, to be positive integer such that the sum of all its proper positive divisors is the number itself. For example,

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14$$
$$\vdots$$

Question 4.1. Are there infinitely many even perfect numbers?

4.2 Progress on Problem

We have not proven the infinitude of even perfect numbers, but we have proven some results in that direction. Namely

1. By the Euclid-Euler Theorem we know there is a one-to-one correspondence between even perfect numbers and Mersenne primes. (This is done in Theorem 4.1).
2. We can express every even perfect number greater than 6 as the sum of consecutive odd cubes starting at 1. (This is done in Theorem 4.3).
3. We can prove every even Perfect Number is Pernicious. (This is done in Theorem 4.5).
4. We can prove there are infinitely many numbers which are both triangular and the sums of consecutive odd cubes starting at 1. (This is done in Corollary 4.1).
5. We can prove that a random set of elements chosen according to the Cramér model of the primes contains infinitely many Mersenne Numbers almost surely. (This is done in Corollary 4.2).

4.3 Euclid-Euler Theorem

Theorem 4.1 (Euclid-Euler Theorem)**.** (This can be found in [3]). All even perfect numbers are of the form $2^{p-1}(2^p - 1)$ where $(2^p - 1)$ is prime, known as a *Mersenne prime*. In fact, for this to happen, p must also be prime, which we prove in Lemma 4.3, but we don't need this, strictly speaking for the Euclid-Euler Theorem. To simplify, we write this as:

$$\frac{a(a-1)}{2} \text{ where a } = 2^p.$$

Before we can prove this, we need to prove one lemma about the sum of the divisors of the product of two coprime integers.

Lemma 4.1. Let $\sigma(n)$ denote the sum of the divisors of n. So

$$\sigma(n) = \sum_{d|n} d.$$

Then if $\gcd(a, b) = 1$ we have

$$\sigma(ab) = \sigma(a)\sigma(b).$$

Proof. If $\gcd(a, b) = 1$, and $\alpha \mid a$ and $\beta \mid b$, then we can't have

$$\alpha_1\beta_1 = \alpha_2\beta_2$$

unless both factorization are equal. If we could, breaking each term up into primes, if WLOG, $\alpha_1 \neq \alpha_2$, then α_1 and α_2 have prime factorization that differ. Say again WLOG that for some prime power π^δ we have $\pi^\delta \mid \alpha_1$ but $\pi^\delta \nmid \alpha_2$. Then since $\alpha_1 \mid a$ we have $\pi^\delta \mid a$ so that $\gcd(a, b) = 1$ implies $\pi \nmid b$ so that in turn we have $\pi \nmid \beta_1$ and $\pi \nmid \beta_2$. Then, breaking up $\alpha_1\beta_1 = \alpha_2\beta_2$ gives a contradiction, since if both integers were the same, then one integer would have to have two distinct prime factorization, since π^δ divides the LHS but not the RHS, which contradicts the Fundamental Theorem of Arithmetic (which can be found in [1]). Thus factors of ab are in 1-1 correspondence with factors of a multiplied by factors of b. Thus, if a and b are coprime we have

$$\sigma(ab) = \sum_{d|ab} d = \sum_{d_a|a}\sum_{d_b|b} d_a d_b = \left(\sum_{d_a|a} d_a\right)\left(\sum_{d_b|b} d_b\right) = \sigma(a)\sigma(b).$$

■

Theorem 4.1 (Euclid-Euler Theorem)**.** The correspondence between perfect numbers (say n) and Mersenne primes (say $(2^p - 1)$) given by

$$n = \binom{2^p}{2}$$

is one-to-one.

Proof. We first show that

$$n = 2^{p-1}(2^p - 1) \text{ with } 2^p - 1 \text{ prime } \Rightarrow n \text{ is perfect.}$$

And without use of the above lemma 4.1, we can show this directly. We note that a number n is defined to be perfect if and only if the sum of its proper divisors is equal to n. We show that if n is of the above form, then the sum of all of the divisors of n is $2n$, which is equivalent. We have

$$\sum_{d|\binom{2^p}{2}} d = \sum_{i=0}^{p-1}\sum_{j=0}^{1} 2^i(2^p - 1)^j = \left(\sum_{i=0}^{p-1} 2^i\right)\left(\sum_{j=0}^{1}(2^p - 1)^j\right) = (2^p - 1)(2^p) = 2 \cdot 2^{p-1}(2^p - 1) = 2n$$

where going from the second expression to the third we summation formula for finite geometric series (which can be found in [11]). This shows that such an n is perfect. Thus we have only to show that

$$n \text{ is perfect and even } \Rightarrow n = 2^{p-1}(2^p - 1) \text{ with } 2^p - 1 \text{ prime.}$$

Now, suppose n is an even perfect number. Then write $n = 2^k x$ with x odd (i.e. with k maximal) so that $k \geq 1$. Then, if $\sigma(n) = 2n$ we have (applying Lemma 4.1 above on the second expression)

$$2^{k+1}x = \sigma\left(2^k x\right) = \sigma(2^k)\sigma(x).$$

Whence we can note that

$$\sigma(2^k) = \sum_{i=0}^{k} 2^i = 2^{k+1} - 1.$$

So that we require for an even perfect number that

$$2^{k+1}x = \left(2^{k+1} - 1\right)\sigma(x).$$

Since $k \geq 1$, we have in particular

$$\left(2^{k+1} - 1\right) \mid x.$$

And so we write

$$x = \left(2^{k+1} - 1\right)y.$$

Which gives, dividing our last equality through by $2^{k+1} - 1$

$$2^{k+1}y = \sigma(x).$$

But, in fact, since $x \mid x$ and $y \mid x$ we have

$$\sigma(x) \geq x + y = \left(2^{k+1} - 1\right)y + y = 2^{k+1}y$$

with equality holding if and only if x and y are the only two divisors of x. Since we need equality to hold for a perfect number, we note the only divisors of x can be y and x. Thus we must have $y = 1$, and x must be prime. Thus,

$$n = 2^k\left(2^{k+1} - 1\right) \text{ where } 2^{k+1} - 1 \text{ is prime.}$$

■

4.3.1 One-to-one relation

Theorem 4.2. Every number of the form $2^{n-1}(2^n - 1)$ with $2^n - 1$ prime is an even perfect number.

Proof. (Alternate proof of sufficiency in theorem 15) Consider $2^{n-1}(2^n - 1)$, with $2^n - 1$ a Mersenne prime. If we look at all the factors of $2^{n-1}(2^n - 1)$ we see we get two lists.

$$1, 2, 4, ..., 2^{n-2}, 2^{n-1}$$

and

$$(2^n - 1), 2 \cdot (2^n - 1), 4 \cdot (2^n - 1), ..., (2^{n-2}) \cdot (2^n - 1), (2^{n-1}) \cdot (2^n - 1).$$

Adding all the numbers in the first list gives

$$1 + 2 + 4 + ... + 2^{n-2} + 2^{n-1} = 2^n - 1.$$

And adding all the numbers in the second list we get

$$(2^n - 1) + 2 \cdot (2^n - 1) + 4 \cdot (2^n - 1) + ... + (2^{n-2}) \cdot (2^n - 1) + (2^{n-1}) \cdot (2^n - 1) = (2^n - 1) \cdot (2^{n-1} - 1).$$

Now we have two sums, $2^n - 1$ and $(2^n - 1) \cdot (2^{n-1} - 1)$ for the two lists of factors of the original number $2^{n-1}(2^n - 1)$. Adding the two sums we get

$$2^n - 1 + (2^n - 1) \cdot (2^{n-1} - 1) = 2^n - 1 \cdot ((2^{n-1} - 1) + 1) = (2^n - 1) \cdot \left(2^{n-1}\right)$$

which is equal to the original number. Therefore, we can conclude for every Mersenne prime $2^n - 1$ one can by multiply a factor 2^{n-1} to get a perfect number. ■

4.3.2 Infinitude of Mersenne primes

Conjecture 4.1. From the above theorem, we can conclude that proving the infinitude of Mersenne primes would show that there are infinite even perfect numbers. Indeed, we conjecture that this line of reasoning is correct. In particular, we conjecture there are infinitely many Mersenne primes.

4.4 Properties

4.4.1 Sum of Consecutive Odd Cubes

Theorem 4.3. Every even perfect number greater than 6 can be expressed as the sum of consecutive odd cubes starting at 1. For instance

$$28 = 1^3 + 3^3$$
$$496 = 1^3 + 3^3 + 5^3 + 7^3.$$

Proof. By the Euclid-Euler theorem, and the oddness of all primes greater than 2, it suffices to prove the result for all numbers of the form $2^{2a}\left(2^{2a+1}-1\right)$ for integer a. We do this directly.

$$\begin{aligned}
\sum_{k=0}^{2^a-1}(2k+1)^3 &= \sum_{k=0}^{2^a-1}(8k^3+12k^2+6k+1)\\
&= 8\sum_{k=0}^{2^a-1}k^3 + 12\sum_{k=0}^{2^a-1}k^2 + 6\sum_{k=0}^{2^a-1}k + \sum_{k=0}^{2^a-1}1\\
&= 8\left(\frac{\left(2^a-1\right)^2\left(2^a\right)^2}{4}\right) + 12\left(\frac{\left(2^a-1\right)\left(2^a\right)\left(2^{a+1}-1\right)}{6}\right) + 6\left(\frac{\left(2^a-1\right)\left(2^a\right)}{2}\right) + 2^a\\
&= 2\left[2^{4a} - 2^{3a+1} + 2^{2a}\right] + 2\left[2^{3a+1} - 2^{2a+1} - 2^{2a} + 2^a\right] + 3[2^{2a} - 2^a] + 2^a\\
&= 2^{4a+1} - 2^{3a+2} + 2^{2a+1} + 2^{3a+2} - 2^{2a+2} - 2^{2a+1} + 2^{a+1} + 2^{2a+1} + 2^{2a} - 2^{a+1} - 2^a + 2^a\\
&= 2^{4a+1} + 2^{2a+1} - 2^{2a+2} + 2^{2a}\\
&= 2^{2a}\left(2^{2a+1} + 2 - 4 + 1\right)\\
&= 2^{2a}\left(2^{2a+1}-1\right).
\end{aligned}$$

■

4.4.2 Triangular numbers

Definition 4.2. We define a *triangular number* to be the sum of the consecutive integers starting at 1. Equivalently, a number n is called *triangular* if and only if for some integer m we have

$$n = \binom{m}{2}$$

whence n is called the $m-2^{\text{nd}}$ triangular number.

Theorem 4.4. Each even perfect number is the $(2^p-1)^{\text{st}}$ triangular number. Hence, it is equal to the sum of the integers from 1 to (2^p-1). So, for example $6 = 2^1\cdot(2^2-1)$ and the 3^{rd} triangular number is $6 = 1+2+3$

Proof. To start we use the Euclid-Euler Theorem (Theorem 4.1) to write out an even perfect number n as

$$\begin{aligned} n &= 2^{p-1}(2^p - 1) \text{ where } (2^p - 1) \text{ is a Mersenne prime} \\ &= \frac{2^p(2^p - 1)}{2} \\ &\text{Substituting } m = 2^p \\ &= \frac{m(m-1)}{2}. \end{aligned}$$

Thus, from definition 4.2, we have each perfect number is triangular. ■

4.4.3 Pernicious Numbers

Definition 4.3. A pernicious number is defined as a positive integer which, when represented in binary, has the sum of its digits equal to a prime number.

Theorem 4.5. Each even perfect number is a pernicious number. For example:

$$6 = 110_2 \text{ because } 1 + 1 = 2 \text{ which is prime}$$

$$28 = 11100_2 \text{ because } 1 + 1 + 1 = 3 \text{ which is prime.}$$

Lemma 4.2. (Difference of powers). For real numbers, x, y, and nonegative integer n we have

$$x^{n+1} - y^{n+1} = (x - y)\left(\sum_{k=0}^{n} x^k y^{n-k}\right).$$

Proof. By the formula for the sum of a finite geometric series, one has

$$\sum_{k=0}^{n} \alpha^k = \frac{\alpha^{n+1} - 1}{\alpha - 1}$$

as long as $\alpha \neq 1$. Substituting

$$\alpha = \frac{x}{y}$$

we get, as long as $x \neq y$

$$\left(\frac{x}{y}\right)^{n+1} - 1 = \left(\frac{x}{y} - 1\right)\left(\sum_{k=0}^{n} x^k y^{-k}\right).$$

Multiplying both sides by y^{n+1} then directly gives us

$$x^{n+1} - y^{n+1} = (x - y)\left(\sum_{k=0}^{n} x^k y^{n-k}\right)$$

for all cases except $y = x$ and $y = 0$. In both of these cases, the result is trivial, since both the RHS and the LHS of the equality readily seen to be 0. ■

Lemma 4.3. If p is not prime, then neither is $2^p - 1$.

Proof. Suppose $a \mid p$ for a a positive integer. Then we show that

$$(2^a - 1) \mid (2^p - 1.)$$

Indeed, let $p = ab$ with b an integer. Then

$$\frac{2^p - 1}{2^a - 1} = \frac{2^{ab} - 1}{2^a - 1} = \frac{(2^a)^b - 1^b}{2^a - 1}.$$

Whence applying the difference of powers gives

$$\frac{2^p - 1}{2^a - 1} = \sum_{k=0}^{b} (-1)^{b-k} 2^{ak}$$

which is the sum of finitely many integers and therefore an integer. Thus, since their quotient is integral we have

$$(2^a - 1) | (2^p - 1).$$

So that if a is some nontrivial (i.e. neither 1 nor p) factor of p, $2^a - 1$ is some nontrivial factor of $2^p - 1$, and therefore if p is not prime, $2^p - 1$ cannot be prime. ■

Definition 4.4. For a positive integer x, let $s(x)$ denote the sum of the binary digits of s.

Lemma 4.4. For all positive integers n,

$$s(2n) = s(n)$$

Proof. Let n have some binary representation

$$n = (A_1 A_2 ... A_m)_2 .$$

then $2n$ has the binary representation

$$2n = (A_1 A_2 ... A_m 0)_2 .$$

Then we have

$$s(2n) = A_1 + A_2 + ... + A_m + 0 = A_1 + A_2 + ... + A_m = s(n).$$

■

Theorem 4.5. All even perfect numbers are pernicious.

Proof. Applying Theorem 4.1(The Euclid-Euler Theorem) we have that if n is an even perfect number, then

$$n = 2^{p-1} (2^p - 1) \text{ with } 2^p - 1 \text{ prime.}$$

Applying Lemma 4.4 successively to this gives that if n is an even perfect number

$$s(n) = s\left(2^{p-1} (2^p - 1)\right) = s(2^p - 1)$$

with $2^p - 1$ a Mersenne prime. Using the sum of a finite geometric series, we have

$$2^p - 1 = \sum_{k=0}^{p-1} 2^p = \left(\underbrace{111...11}_{p \text{ digits}} \right)_2 .$$

So that

$$s(n) = s(2^p - 1) = \sum_{k=0}^{p-1} 1 = p.$$

The Euclid-Euler theorem gives us that if n is perfect and even, $2^p - 1$ must be prime, and therefore the contrapositive of lemma 4.3 gives us that so too must p be prime. Thus n is pernicious. ■

4.4.4 Intersection

Corollary 4.1. Let set of even perfect numbers be $N = \{6, 28, 496 \dots\}$, set of triangular numbers be $T = \{1, 3, 6 \dots\}$, and the set of sums of consecutive odd cubes starting at 1 be $O = \{1, 28, 153 \dots\}$. Then we know

$$N \subset T \text{ and } N \subset O.$$

So, if can we show

$$\#(T \cap O) = \infty$$

then that might suggest that there could be infinitely many even perfect numbers.

Proof. Let O_n be the sum of the first n consecutive odd cubes and T_n be the n-th triangular number. Theorem 4.3 gives us for all positive integers a that

$$T_{2^{2a+1}} = O_{2^a - 1}.$$

Thus we have

$$\{T_{2^{2a+1}} : a \in \mathbb{N}\} = \{O_{2^a-1} : a \in \mathbb{N}\}.$$

Calling this set H, in particular, we have

$$H \subseteq T \text{ and } H \subseteq O \Rightarrow H \subseteq (O \cap T)$$

and clearly we can generate arbitrarily many elements of H just by choosing all a up to arbitrarily large values. Thus we have

$$\#H = \infty$$

and since $H \subseteq (O \cap T)$ we have

$$\#(O \cap T) = \infty.$$

■

4.5 Heuristics

4.5.1 Rough Remarks

Remark 4.1. Looking for a Heuristic for the Perfect number problem can be done using some relatively elementary considerations (In particular, using the Cramér random model of the Primes, which can be found in [12]). So, The Euclid-Euler Theorem (Theorem 4.1) gives that the problem is equivalent to the infinitude of Mersenne Primes. Conjecturing whether or not there are infinitely many Mersenne primes is pretty much a quick application of the prime number theorem. The *prime number theorem* (which can be found in [5]) is a result in analytic number theory that says the number of primes less than x, denoted $\pi(x)$ is roughly

$$\pi(x) \approx \frac{x}{\log x}$$

(where $\log x$ denotes the natural logarithm). And indeed, it says precisely that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Thus, we can roughly model the primes as a random set with the probability x is prime being

$$\frac{1}{\log x}$$

(This is slightly problematic for $x = 1, 2$, but those two finite cases shouldn't affect the infinitude of Mersenne Primes anyways). In particular, then, we should expect the total number of Mersenne primes to be given by the sum of the probabilities of primality of all of the numbers that are one less than a power of two, to infinity, so we get

$$\sum_{k\geq 2} \frac{1}{\log\left(2^k - 1\right)}.$$

And indeed this series diverges. Roughly, though, using the limit

$$\lim_{k\to\infty} \frac{\log\left(2^k\right)}{\log\left(2^k-1\right)} \overset{\text{L'Hopital}}{=} \lim_{k\to\infty} \frac{\log(2)}{\frac{2^k\log(2)}{2^k-1}} = \lim_{k\to\infty} 1 - 2^{-k} = 1$$

we can approximate this sum as a simpler one. And we then may approximate this sum as an integral to get

$$\int_2^\infty \frac{1}{\log 2^k}\,\mathrm{d}k = \frac{1}{\log 2}\int_2^\infty \frac{1}{k}\,\mathrm{d}l = \frac{1}{\log 2}\left[\log k\right]_2^\infty = \infty.$$

Thus that we might guess this sum diverges and therefore maybe roughly we should expect infinitely many Perfect numbers. Furthermore, using this logic gives us that roughly $\log N$ of the first N numbers one less than a power of two are primes, so that if we call $M(n)$ the number of Mersenne primes less than n, we might be led to believe

$$M(N) \approx \lambda \log\log N$$

for some suitable constant λ. In particular, by the Euclid-Euler theorem, then if we denote by $\mathrm{PN}(n)$ the number of perfect numbers less than n. Ignoring the possibility of odd perfect numbers, we might expect roughly that

$$\mathrm{PN}(n) \approx \lambda\sqrt{\log\log n}$$

for some constant λ.

4.5.2 Rigorous Statements

Definition 4.5. Let M be the set defined by

$$M \overset{\text{def}}{=} \{2^p - 1 : p \in \mathbb{P}\}$$

we note in particular the the set of Mersenne primes is exactly $M \cap \mathbb{P}$ by Lemma 4.2.

Theorem 4.6. Let S be a random subset of $\mathbb{Z}^+$ such that for each positive integer n greater than or equal to 3 the probability $P(n \in S) = \dfrac{1}{\log n}$. Then the expectation

$$\mathbb{E}[\#(M \cap S)]$$

is infinite.

Proof. Define

$$X_p = \mathbb{1}_{2^p-1\in S}$$

then we have

$$\#(M \cap S) = \sum_{p\in\mathbb{P}_{\geq 3}} X_p.$$

So that by the linearity of expectation we have

$$\mathbb{E}[\#(M \cap S)] = \mathbb{E}\left[\sum_{p\in\mathbb{P}_{\geq 3}} X_p\right] = \sum_{p\in\mathbb{P}_{\geq 3}} \frac{1}{\log\left(2^p-1\right)}$$

since by our definition of S we have $\mathbb{E}[\mathbb{1}_{2^p-1\in S}] = P(2^p-1 \in S) = \frac{1}{\log(2^p-1)}$. And so all we have to do is prove that this series diverges. For the sake of convenience, let us call this sum E^*. We first note that the series can be rewritten

$$E^* = \sum_{k=2}^{\infty} \frac{1}{\log\left(2^{p_k}-1\right)}$$

the next step is really just a slight formalism of what we did before. We use the limit comparison test on this sum. In particular, since p_k is a monotonously increasing sequence we have

$$\lim_{k\to\infty} \frac{\log\left(2^{p_k}\right)}{\log\left(2^{p_k}-1\right)} = \lim_{n\to\infty} \frac{\log\left(2^{n}\right)}{\log\left(2^{n}-1\right)} = 1$$

where the last limit can be evaluated using L'Hopital's rule as in the above remark 4.1. Thus, in particular, we have that the convergence of E^* is equivalent to the convergence of, by the limit comparison test

$$\sum_{k=2}^{\infty} \frac{1}{\log 2^{p_k}} = \frac{1}{\log 2} \sum_{k=2}^{\infty} \frac{1}{p_k}$$

which is well known to diverge. We sketch an argument for this here for completeness. A result of Rosser (see [8]) says that

$$p_n \leq n\log n + n\log\log n$$

for all $n \geq 6$, so that we get the to show divergence of E^* it suffices to show the divergence of (ignoring the factor of $1/\log 2$)

$$\sum_{k=6}^{\infty} \frac{1}{k\log k + k\log\log k} \geq \frac{1}{2}\sum_{k=6}^{\infty} \frac{1}{k\log k}.$$

And by the integral test since

$$\int_6^{\infty} \frac{1}{k\log k}\,\mathrm{d}k = -\log\log 6 + \lim_{k\to\infty} \log\log k = \infty$$

we have the expectation diverges. ■

Remark 4.2. The Tests for Series Convergence as Well as L'Hopital's rule can be found in [11]. Additionally, the linearity of expectation is proven in [4].

Corollary 4.2. Let S again be a random subset of $\mathbb{Z}^+$ where for each positive integer $n \geq 3$, the probability $P(n \in S) = \dfrac{1}{\log n}$. Then $M \cap S$ is infinite almost surely.

Proof. This a direct application of the converse to the Borel-Cantelli Lemma. See [4] for a proof of this converse. Directly, it says that if the sum of the probabilities an infinite sequence of independent events is infinite, infinitely many of them occur almost surely. The events $\{2^{p_n}-1 \in S\}$ form such a sequence, and the sum of their probabilities is just $\mathbb{E}(\#(M\cap S))$ which is shown to be infinite by the Theorem 4.6. ■

Remark 4.3. Note that at a high level corollary 4.2 suggests, roughly speaking, that most sets with the same asymptotic density as the primes contain infinitely many Mersenne numbers, and so it seems reasonable to expect that the primes might behave similarly. The validity of this model, however, for the specific example of Mersenne primes, could still conceivably be bad. Since the sum of the reciprocals of the primes up to n exhibits $\log\log$ growth, numerically Theorem 4.6 and corollary 4.2 suggest that

$$PN(n) = O\left(\sqrt{\log\log\log n}\right)$$

which is actually reasonably difficult to confirm numerically since perfect numbers get large so quickly. But numerical confirmation with that asymptotic growth rate would prove especially strong evidence for the infinitude of even perfect numbers.

Appendix A

Source Code for Singmaster's Conjecture

```
import math
from timeit import default_timer as tictoc
from matplotlib import pyplot as plt

#returns n choose k using the product formula
def binom(n, k):
    if k > n-k:
        return binom(n, n-k)
    else:
        numerator = 1
        denominator = 1
        for j in range(0, int(k)):
            numerator *= (n-j)
            denominator *= (k-j)
        return numerator // denominator

#returns i+j choose i--this is the i-th element on the j-th diagonal, starting from 0
def get_diag(i, j):
    return binom(i+j, i)

#returns the partial derivative of i+j choose i with respect to j. This is really just
    differentiating a polynomial in j
#that's sort of indexed by i, but the specific formula seen here is an application of the
    generalized product rule to the product formula.
def get_diag_j_deriv(i, j):
    if j < 0 and j//1 == j:
        return 1
    else:
        mult = 0
        for k in range(1, i+1):
            mult += 1/(j+k)
        return mult * get_diag(i, j)

#Uses the weak lower bound given in Lemma 2.3 of a logarithmic bound on the number of times an
    integer can occur as a
```

```
#binomial coefficient to give a rough estimate for the j_star so that (for a given i) i + j_star
    choose i is about
#r. This is used as a starting point for the Newton's method
def estimate_diag_int(i, r):
    return i * (r ** (1/i) - 1)

#The signum function of x
def signum(x):
    if x > 0:
        return 1
    elif x < 0:
        return -1
    else:
        return 0

#Defined in Definition 2.2 of a logarithmic bound on the number of times an integer can occur as a
    binomial coefficient
#this is actually an upper bound proven in Corollary 2.2 of the same section
def m(r):
    return math.ceil(math.log2(r))+1

#A slightly shiny version of Newton's method. Netwon's method uses successive linear approximation
    for root approximation
#and is very effective (in fact, it converges quadratically). This modifies pure Newton's method
    in 2 ways. First, it
#includes the logic to pertube the current x value in the right direction to move beyond critical
    points. Second, it
#dampen's the Newton's method by bounding the change in x between steps by some scalar multiple
    (scale factor c) of x. This
#make's the algorithm converge less quickly, but can greatly increase its region of convergence
def damped_newtons_method(initVal, funct, deriv, numSteps, c = 1, lambdaFac = .5, epsilon_d =
    .0001, epsilon_x = .1):
    curVal = initVal
    for i in range(0, numSteps):
        d = deriv(curVal)
        f = funct(curVal)
        if math.fabs(d) < epsilon_d:
            curVal -= epsilon_x * signum(f)
        else:
            diff = -f/d
            while math.fabs(diff) > c * math.fabs(curVal):
                diff *= lambdaFac
            curVal += diff
    return curVal


#Get's the coordinates on diagonal i of the binomial coefficient equal to r, or returns none, if
    no such value exists.
#Note that for optimal results, the damped Newton's method should really be set on a divergence
    criterion so that this
#method is provably correct, because right now technically its an empirical approximation where
    the number of steps has
#been chose empirically.
def get_diag_int(i, r):
    startVal = estimate_diag_int(i, r)
    num_steps = 1000
```

```
    def local_diag_funct(j):
        return get_diag(i, j)-r
    def local_diag_deriv_funct(j):
        return get_diag_j_deriv(i, j)
    bestVal = damped_newtons_method(startVal, local_diag_funct, local_diag_deriv_funct, num_steps)
    lowerGuess = math.floor(bestVal)
    upperGuess = math.ceil(bestVal)
    if local_diag_funct(upperGuess) == 0:
        return [(i+upperGuess)//1, upperGuess//1]
    elif local_diag_funct(lowerGuess) == 0:
        return [(i+lowerGuess)//1, lowerGuess//1]
    else:
        return None

#reflect (n, k) to give (n, n-k). A useful auxillary function for generated reflected coordinates
    in Pascal's triangle
def reflect(cordinate):
    return [cordinate[0], cordinate[0]-cordinate[1]]

#returns the number of times an integer occurs in Pascal's triangle, by determining if and where
    it appears in the first
#n diaogonals, and appropriately relfecting. If ran with verbose = true, it will also print all of
    the (n, k) pairs for
#which r = n choose k
def N(r, verbose = False):
    coords = [[r, 1], [r, r-1]]
    for i in range(2, m(r)+1):
        coord = get_diag_int(i, r)
        if not coord is None:
            if not coord in coords:
                coords.append(coord)
            coord = reflect(coord)
            if not coord in coords:
                coords.append(coord)
    if verbose:
        print(coords)
    return len(coords)

max_num = 10000
max_mult = 2
max_mult_producers = []
for i in range(2, max_num+1):
    if i % 100 == 0:
        print(i)
    n_val = N(i)
    if n_val == max_mult:
        max_mult_producers.append(i)
    elif n_val > max_mult:
        max_mult = n_val
        max_mult_producers = [i]
print("The maximum multiplicity of any number less than or equal to " + str(max_num) + " as a
    binomial coefficient is " + str(max_mult))
print(str(max_mult) +" is the multiplicty of " + str(max_mult_producers))
```

Appendix B

Source Code for Perfect Cuboid Modulo p

```
import itertools as it
from sympy import sieve

N = 20

def gen_quad_residues(p):
    if p == 2:
        return range(2)
    else:
        res = []
        for i in range(0, (p+1) // 2):
            res.append( i * i % p)
        return res

def get_pos_trios(p):
    def get_nontrivial_negations(sol):
        def get_negs(ind):
            if sol[ind] == 0:
                return [sol[ind]]
            else:
                return [sol[ind], p - sol[ind]]
        nontrivial_negs = []
        a_vals = get_negs(0)
        b_vals = get_negs(1)
        c_vals = get_negs(2)
        for a in a_vals:
            for b in b_vals:
                for c in c_vals:
                    nontrivial_negs.append([a, b, c])
        return nontrivial_negs
    res = gen_quad_residues(p)
    sols = []
    for triple in it.combinations_with_replacement(range(0, (p+1)//2), 3):
        a = triple[0] * triple[0] % p
        b = triple[1] * triple[1] % p
        c = triple[2] * triple[2] % p
```

```
        if (a+b) % p in res and (b+c) % p in res and (a+c) % p in res and (a + b + c) % p in res:
            new_sols = get_nontrivial_negations([triple[0], triple[1], triple[2]])
            for solution in new_sols:
                if not solution in sols:
                    sols.append(solution)
    return sols

primes = list(sieve.primerange(3, N))

def get_cuboid_str(el, p):
    a = el[0]
    b = el[1]
    c = el[2]
    d = (b*b + c*c) % p
    e = (a*a + c*c) % p
    f = (a*a + b*b) % p
    g = (a*a + b*b + c*c) % p
    _str = "(" + str(a) + ", " + str(b) + ", " + str(c) + ", " + str(d) + ", " + str(e) + ", " +
        str(f) + ", " + str(g) + ")"
    return _str

def get_results(p):
    sols = get_pos_trios(p)
    no_zeros = []
    one_zero = []
    two_zeros = []
    for sol in sols:
        if sol.count(0) == 0:
            no_zeros.append(sol)
        elif sol.count(0) == 1:
            one_zero.append(sol)
        else:
            two_zeros.append(sol)
    return no_zeros, one_zero, two_zeros

def get_str_from_list(the_list, p):
    if len(the_list) == 0:
        return ""
    elif len(the_list) == 0:
        return get_cuboid_str(the_list[0], p)
    res_str = ""
    for trio in the_list[0:-1]:
        res_str += get_cuboid_str(trio, p)
        res_str += ", "
    res_str += get_cuboid_str(the_list[-1], p)
    return res_str



tot = ""
for prime in primes:
    nz, oz, tz = get_results(prime)
    res = str(prime) + " & " + get_str_from_list(tz, prime) + " & " + get_str_from_list(oz, prime)
        + " & " + get_str_from_list(nz, prime) + '\\\ \hline '
    tot += res
print(tot)
```

Bibliography

[1] Andrews, George E. *Number Theory*. W.B. Saunders Co., Philideplia, PA.

[2] Brualdi, Richard A. *Introductory Combinatorics* (5th ed.), Prentice-Hall, p. 44.

[3] Caldwell, Chris K., "A proof that all even perfect numbers are a power of two times a Mersenne prime", Prime Pages.

[4] Feller, William. *An Introduction to Probability Theory and Its Application*, John Wiley & Sons.

[5] Hardy, Godfrey Harold; Wright, E. M., An introduction to the theory of numbers. (First ed.), Oxford: Clarendon Press.

[6] Joyce, D. E. "Book X , Proposition XXIX", *Euclid's Elements*, Clark University.

[7] Mordell, L.J. *Diophantine Equations*. London-New York: *Academic Press*, pp. 77.

[8] Rosser, J.B. *Explicit Bounds for Some Functions of Prime Numbers*, Amer. J. Math. 63, 211-2.

[9] Saunderson, N. *The Elements of Algebra in 10 Books, Vol. 2.* Cambridge, England: University Press, pp. 429-431, 1740.

[10] Silverman, Joseph H. *The Arithmetic of Elliptic Curves*, Springer-Verlang New York.

[11] Stewart, James. *Calculus: Early Transcendentals*. Brooks/Cole, 1991.

[12] Terry Tao. 254A, Supplement 4: Probabilistic models and heuristics for the primes (optional), section on The Cramér random model, January 2015.

[13] Tondeur, Phillippe. *Vectors and Transformations in Plane Geometry*. Public or Perish, Inc. 1993. pp. 64.

[14] Walter, Éric. *Numerical Methods and Optimization*, Springer-Verlang New York, pp. 144.

[15] Wiles, Andrew. "The Birch and Swinnerton-Dyer conjecture". *The Millennium prize problems*. American Mathematical Society. pp. 31–44.

Unsolved Problems in Mathematics

Nick Castro, Dylan Pizzo, Vincent Longo, Jai Sharma,
Akshat Jha, Sambhabi Bose, Garrett Heller, Anand Somayajula

September 7, 2020

Contents

Chapter 1

Introduction

In this paper, we will be discussing three problems: the Erdös-Moser Equation, the Lonely Runners Conjecture, and the Collatz Conjecture. The following are the statements of the conjectures:

1. **Erdös-Moser Equation** - The Erdös-Moser Equation is the equation

$$1^k + 2^k + \cdots + n^k = (n+1)^k,$$

where n and k are positive integers. It was conjectured by Paul Erdös that no solutions to this equation exist except for the trivial $1^1 + 2^1 = 3^1$.

2. **Lonely Runners Conjecture** - Consider a circular track with circumference of 1 mile and k runners running on the track starting from the same point such that they all have distinct speeds. A runner is said to be lonely if they are at least $\frac{1}{k}$ distance away from all other $k-1$ runners. The Lonely Runners Conjecture says that given any number of runners, k, and any set of k distinct speeds, there always comes an point in time after which all the runners have become lonely for at least once (at times that are not necessarily the same).

3. **Collatz Conjecture** - Consider the following function:

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ 3n+1 & \text{if } n \text{ is odd} \end{cases}$$

The Collatz Conjecture says that given any integer n, repeated iterations of the above function will always result in the number 1. In other words, $f^x(n) = 1$ for some positive intger x.

In the following chapters, we will discuss how we attempted to answer these questions as well as different representations of the problem.

Chapter 2

Explorations on the Erdös-Moser Equation

2.1 Problem Statement

Erdös-Moser Equation - Say that we have the following equation:

$$S_k(n) = 1^k + 2^k + 3^k + \cdots + (n-1)^k + n^k.$$

It was conjectured by Paul Erdös that the equation

$$S_k(n) = (n+1)^k \tag{2.1}$$

has no solutions to this equation exist except for the trivial $1^1 + 2^1 = 3^1$.

2.2 Progress on Problem

Definition 2.1. If there exist (k, n) such that $S_k(n) = (n+1)^k$, then we say that (k, n) is a solution of Equation 2.1.

Lemma 2.1. Only $k \equiv 0 \pmod 2$ satisfies the conjecture.

Proof. To prove that only even values of k satisfy this equation, we assume that there exist odd values of k satisfying the Erdös-Moser Equation and prove by contradiction.

Taking the equation $\pmod n$, we have,

$$1^k + 2^k + ... + n^k \equiv (n+1)^k \pmod n$$

Since,

$$(n+1)^k \equiv 1^k \pmod{n} \text{ and } n^k \equiv 0 \pmod{n},$$

we have

$$2^k + 3^k + ... + (n-1)^k \equiv 0 \pmod{n}. \tag{2.2}$$

Since k is odd,

$$\begin{aligned} i^k &\equiv (n-(n-i))^k \\ &\equiv (-(n-i))^k \\ &\equiv -(n-i)^k \pmod{n}. \end{aligned}$$

Using this, we have

$$-(n-2)^k + -(n-3)^k - ... - 1^k \equiv 0 \pmod{n} \tag{2.3}$$

Adding equations 1 and 2, we get

$$(n-1)^k - 1^k \equiv 0 \pmod{n} \tag{2.4}$$

Again since k is odd,$(n-1)^k \equiv (-1)^k \equiv -1 \pmod{n}$. So Equation 2.4 becomes $-2 \equiv 0 \pmod{n}$ which is never possible when $n \neq 2$. When $n = 2$, the Erdös-Moser Equation becomes $1^k + 2^k = 3^k$ which holds true only for $k = 1$.

■

Lemma 2.2. *$S_k(p) \equiv 0 \mod p$ if $p-1 \nmid k$ and $S_k(p) \equiv -1 \mod p$ if $p-1|k$.*

Proof. Consider a primitive root g. Then

$$\begin{aligned} S_k(p) &= \sum_{i=1}^{p-1} i^k + p^k \\ &\equiv \sum_{j=0}^{p-2} (g^j)^k \mod p \\ &\equiv \sum_{j=0}^{p-2} (g^k)^j \mod p \\ &\equiv \frac{(g^k)^{p-1} - 1}{g^k - 1} \mod p. \end{aligned}$$

By Fermat's Little Theorem $(g^k)^{p-1} - 1 \equiv 0 \mod p$, and since g is a primitive root $ord_p(g) = p-1$ thus $g^k - 1 \equiv 0 \mod p$ iff $p-1|k$. Therefore,

$$p-1 \nmid k \implies \frac{(g^k)^{p-1} - 1}{g^k - 1} \equiv_p S_k(p) \equiv_p 0.$$

Now if $p-1|k$. By Fermat's Little Theorem $i^k \equiv 1 \mod p$ for $p \nmid i$. So

$$S_k(p) \equiv_p \sum_{i=1}^{p-1} i^k \equiv_p p-1 \equiv_p -1. \square$$

Lemma 2.3. Let k be the exponent for a nontrivial solution to the Erdos-Moser equation. Then $S_k(\frac{p-1}{2}) \equiv 2^{-1}S_k(p) \mod p$. Thus $S_k(\frac{p-1}{2}) \equiv \frac{p-1}{2} \mod p$ if $p-1|k$ and otherwise equivalent to 0.

Proof. By Lemma **??**, $i^k \equiv (p-i)^k \mod p$. Thus

$$\begin{aligned} 2S_k(\frac{p-1}{2}) &= 2\sum_{i=1}^{\frac{p-1}{2}} i^k \\ &\equiv_p \sum_{i=1}^{\frac{p-1}{2}} i^k + \sum_{i=1}^{\frac{p-1}{2}} (p-i)^k \\ &\equiv_p \sum_{i=1}^{p-1} i^k \\ &\equiv_p S_k(p). \end{aligned}$$

Thus $S_k(\frac{p-1}{2}) \equiv 2^{-1}S_k(p) \mod p$ as desired. The last conclusion is by Lemma 2.2. $\square$

Theorem 2.1. For every $p|n$, $n \equiv -p \mod p^2$ (Alternatively $\frac{n}{p} \equiv -1 \mod p$).

Proof. Consider a $p|n$. Then we have $S_k(n) = (n+1)^k$ and

$$S_k(n) = (1^k + 2^k + \dots p^k) + ((p+1)^k + (p+2)^k + \dots (2p)^k) + \dots ((n-p+1)^k + \dots n^k)$$

so $\frac{n}{p}S_k(p) \equiv (n+1)^k \equiv 1 \mod p$. Lemma 2.2 says $S_k(p)$ is equivalent to 0 or -1 modulo p. Zero results in a contradiction here so $S_k(p) \equiv -1 \mod p$. Then,

$$\begin{aligned} &\frac{-n}{p} \equiv 1 \mod p \\ &\implies \frac{n}{p} = pj - 1 \\ &\implies n = p^2 j - p \\ &\implies n \equiv -p \mod p^2. \square \end{aligned}$$

Corollary 2.1. n is squarefree.

Proof. Assume for the sake of contradiction $p^2|n$ so $n \equiv 0 \mod p^2$. Then $p|n$ and by Theorem 2.1,

$$\begin{aligned} n &\equiv_{p^2} -p \\ &\equiv_{p^2} 0. \end{aligned}$$

Thus, $p^2|p$ which is a contradiction. ■

Corollary 2.2. If $p|n$ then $p-1|k$.

Proof. In the proof of Theorem 2.1 we got if $p|n$ then $S_k(p) \equiv -1 \mod p$. By Lemma 2.2, $p-1|k$. □

Lemma 2.4. If $p|n+2$ then $\frac{n+2}{p} \equiv -2 \mod p$.

Proof. Let $p|n+2$. Then $S_k(n) \equiv (n+1)^k \mod p$. Add $(n+1)^k + (n+2)^k$ to both sides. Then $S_k(n+2) \equiv 2(n+1)^k \mod p$. Similarly to the last proof, $S_k(p)\frac{n+2}{p} \equiv 2(-1)^k \equiv 2 \mod p$ since k is even by Lemma 2.1. Then $p-1|k$ and $S_k(p) \equiv -1 \mod p$ by Lemma 2.2 which gives $\boxed{\frac{n+2}{p} \equiv -2} \mod p$.

Lemma 2.5. If $p|2n+1$ then $\frac{2n+1}{p} \equiv -2 \mod p$ and $p-1|k$.

Proof. Let $p|2n+1$. Note

$$2n+1 \equiv 0 \mod p \implies \qquad 2n \equiv -1 \mod p \implies n \equiv \frac{p-1}{2} \mod p$$

Also using a similar method as prior proofs

$$\begin{aligned} &S_k(n) \equiv \frac{2n+1}{p} S_k(\frac{p-1}{2}) \mod p \\ \implies &\frac{2n+1}{p} S_k(\frac{p-1}{2}) \equiv (n+1)^k \mod p. \end{aligned}$$

Since $2n+1 \equiv p \mod p$ we have $n+1 \equiv \frac{p+1}{2} \mod p$. This gives $\frac{2n+1}{p} S_k(\frac{p-1}{2}) \equiv (\frac{p+1}{2})^k \mod p$. If $S_k(p) \equiv 0$ we get a contradiction so by Lemma 2.2 $p-1|k$ and $S_k(\frac{p-1}{2}) \equiv \frac{p-1}{2} \mod p$ and by Fermat's Little Theorem

$$\begin{aligned} &\frac{2n+1}{p}\frac{p-1}{2} \equiv 1 \mod p \\ \implies &\boxed{\frac{2n+1}{p} \equiv -2 \mod p} \end{aligned}$$

Lemma 2.6. If $p|2n+3$ then $\frac{2n+3}{p} \equiv -4 \mod p$ and $p-1|k$.

Proof. This proof uses the same methods as the proofs of Lemmas 2.4 and 2.5 refer to those for explanation. Let $p|2n+3$. $S_k(n) \equiv (n+1)^k \mod p \implies S_k(n+1) \equiv 2(n+1)^k \mod p \implies \frac{2n+3}{p} S_k(\frac{p-1}{2}) \equiv 2(\frac{p-1}{2})^k \mod p \implies p-1|k$ and $\frac{2n+3}{p}\frac{p-1}{2} \equiv 2 \mod p \implies \boxed{\frac{2n+3}{p} \equiv -4 \mod p}$

Corollary 2.3. All of $n, n+2, 2n+1, 2n+3$ are squarefree and if p divides one of them then $p-1|k$.

Proof. Same proof as corollary 2.1, corollary 2.2.

Lemma 2.7. $n, n+2, 2n+1, 2n+3$ have pairwise gcds of either 3, 2, or 1.

Proof. Use Euclidean algorithm. $gcd(n, 2n+3) = gcd(n, 3)$, $gcd(n, n+2) = gcd(n, 2)$ etc.

Lemma 2.8. 2 and 3 divide at most 2 of $n, n+2, 2n+1, 2n+3$.

Proof. 2 cannot divide either $2n+1, 2n+3$. Also $n \equiv 2n+3 \mod 3$ but are equivalent to neither of the other 2.

Lemma 2.9. Let a be squarefree. If $\frac{a}{p} \equiv b \mod p$ for each $p|a$, then $a|(\sum_{p|a} \frac{a}{p} - b)$.

Proof. Consider $S = \sum_{p|a} \frac{a}{p}$. Now choose a prime $q|a$. Then for $p \neq q$ we have $q|\frac{a}{p}$ but if $p = q$ then $\frac{a}{p} \equiv b \mod p$ by the conditions, so $S \equiv b \mod q$. Repeat for each $q|a$. Then by the Chinese remainder Theorem, since $S \equiv b \mod q^j$ for all prime powers $q^j|a$ (note by the definition of squarefree $j = 1$), we have $S \equiv b \mod a \implies a|S-b$. $\square$.

Corollary 2.4. Using the same variables as Lemma 2.9, $(\sum_{p|a} \frac{1}{p} - \frac{b}{a}) \in \mathbb{Z}$.

Proof. Take $a|S-b$ from Lemma 2.9 gives $\frac{S-b}{a} \in \mathbb{Z}$ gives the result.

Theorem 2.2. $n > \frac{1}{\sqrt{(2)}}(\prod_{p \leq x} p)^{\frac{1}{4}} - 1$ where $\sum_{p \leq x} \frac{1}{p} \geq \frac{19}{6}$.

Proof. By corollary 2.4, $\sum_{p|n} \frac{1}{p} + \frac{1}{n}$ is an integer and thus $\sum_{p|n} \frac{1}{p} > 1 - \frac{2}{n}$. Similarly we repeat for this $n+2, 2n+1, 2n+3$ e.g.

$$\begin{aligned}
&\frac{n+2}{p} \equiv -2 \mod p \implies \text{(Corollary 2.4)} \\
&\sum_{p|n+2} \frac{1}{p} - \frac{-2}{n+2} \in \mathbb{Z} \implies \\
&\sum_{p|n+2} \frac{1}{p} + \frac{2}{n+2} \geq 1 \implies \\
&\sum_{p|n+2} \frac{1}{p} \geq 1 - \frac{2}{n+2} \implies \\
&\sum_{p|n+2} \frac{1}{p} > 1 - \frac{2}{n}
\end{aligned}$$

Then we combine for $m = n(n+1)(2n+1)(2n+3) < 4(n+1)^4$ (and take out a $\frac{1}{2}$ and $\frac{1}{3}$ because those could be repeated once) and we get $\sum_{p|m} \frac{1}{p} - \frac{1}{2} - \frac{1}{3} - \frac{8}{n} > 4$. We ignore the $\frac{8}{n}$ because its sufficiently smaller than each $\frac{1}{p}$. So then $\sum_{p|m} \frac{1}{p} > \frac{19}{6}$. Then $4(n+1)^4 > m \geq \prod_{p|m} p$ for these distinct primes. From here we just change the expression so its independent of m to achieve the final result.

Theorem 2.3. Upcoming

2.3 Bound Manipulations

In this section, we derive that the solutions k and n of the Erdös-Moser Equation $1^k + 2^k + ... + n^k = (n+1)^k$ satisfy the inequality Upper Bound:

Theorem 2.4. $k < n$.

Proof. Note

$$S_k(n) = \int_1^{n+1} \lfloor x^k \rfloor dx.$$

Then

$$S_k(n) < \int_1^{n+1} x^k dx = \frac{(n+1)^{k+1} - 1}{k+1}$$

Using this and $S_k(n) = (n+1)^k$ implies

$$\begin{aligned}
&\frac{(n+1)^{k+1}-1}{k+1} > (n+1)^k \\
&\implies n+1-\frac{1}{(n+1)^k} > k+1 \\
&\implies k < n-\frac{1}{(n+1)^k} < n
\end{aligned}$$

so we get $k < n$.

Lower Bound:

Lemma 2.10. For positive integer n, $(1+\frac{1}{n})^n < e$.

Proof. Consider $y = (1+\frac{1}{n})^n$ then $\ln(y) = n(ln(1+\frac{1}{n}))$. Define $x = \frac{1}{n}$ and then $ln(y) = \frac{ln(1+x)}{x}$. Since $n > 1; x < 1$ and the expansion of $ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \dots$
so

$$\ln(y) = \frac{x - \frac{x^2}{2} + \frac{x^3}{3} + \dots}{x} = 1 - \frac{x}{2} + \frac{x^2}{3} + \dots.$$

Since this is an alternating series with decreasing magnitude (since $x < 1$) then we pair term $\frac{-x^{2k-1}}{2k}$ with $\frac{x^{2k}}{2k+1}$ and their sum is negative, thus $\ln(y) < 1 \implies y < e$.

Lemma 2.11. $1^k + 2^k + \dots n^k > \frac{n^{k+1}}{k+1} + \frac{n^k}{2}$. True by Bernoulli's sum formula; a partial proof is given here. We assume some properties which we will not prove:

1. $1^k + 2^k + \dots n^k = \sum_{i=0}^{k} \frac{B_i}{k+1} x^{k+1-i} \binom{k+1}{i}$ where B_i is the ith Bernoulli number.
2. $B_i < 0$ only if $4|i$
3. $|B_{2n}| = \frac{2\zeta(2n)(2n)!}{(2\pi)^{2n}}$
4. $B_0 = 1$, $B_1 = \frac{1}{2}$ and $B_2 = \frac{1}{6}$

Proof. In this proof we assume the upper bound i.e. $n > k$. Note that the Bernoulli expansion for $1^k + 2^k + \cdots n^k$ starts out with the first two terms: $\frac{n^{k+1}}{k+1} + \frac{n^k}{2}$. The next term is $\frac{kn^{k-1}}{12}$. Consider even terms after this point- they will have magnitude of the form

Then we have by Lemma 2.11

$$1^k + 2^k + \dots n^k > \frac{n^{k+1}}{k+1} + \frac{n^k}{2}$$
$$\implies (n+1)^k \frac{n^{k+1}}{k+1} + \frac{x^k}{2}$$
$$\implies (k+1)(1+\frac{1}{n})^k > n + \frac{k+1}{2}$$

. Let $c = (1+\frac{1}{n})^k$ then by our upper bound and lemma 1 $c < e$ so $c = O(1)$ so we get $k(1+\frac{1}{n})^k + O(1) > n + \frac{k}{2}$; the $O(1)$ is sufficiently small so it can be ignored. Then we get $((1+\frac{1}{n})^n)^{\frac{k}{n}} > \frac{n}{k} + \frac{1}{2}$. Substituting $x = \frac{k}{n}$ gives $((1+\frac{1}{n})^n)^x > \frac{1}{2} + \frac{1}{x}$. Applying lemma 1 again gives

$$e^x > ((1+\frac{1}{n})^n)^x > \frac{1}{2} + \frac{1}{x}$$
$$\implies e^x > \frac{1}{2} + \frac{1}{x}$$

. Plugging into Wolfram gives $x > 0.679 \implies \boxed{\frac{k}{n} > 0.679}$.

Then in total our bounds become $\boxed{0.679 < \frac{k}{n} < 1}$.

■

Theorem 2.5. $S_k(n) = (n+1)^k$ has at most 1 solution $n \in \mathbb{Z}$ for each choice of k, and further the function $f(n) = (n+1)^k - S_k(n)$ is increasing over the integers.

Proof. We present an uncompleted proof. Consider

$$\Delta(f(n)) = f(n) - f(n-1) = (n+1)^k - 2n^k$$
$$\text{and } \Delta^2(f(n)) = \Delta(f(n)) - \Delta(f(n-1)) = .$$

This proof still in progress. An alternate proof would be to use the method from the alternate proof of Theorem 4...

Theorem 2.6. $S_k(n) = (n+1)^k$ has exactly one positive solution $k \in \mathbb{R}$ for each integral choice of n.

Proof. Consider the function $f(k) = (n+1)^k - S_k(n)$. Then $f(k)$ is continuous and differentiable over k. Let $k = 0$ then $f(k) < 0$. We claim $k = n^2$ gives $f(k) > 0$. We have $f(k) > (n+1)^k - n(n^k)$ since there are n terms in $S_k(n)$ the greatest of which is n^k. By Lemma 2.10 $f(k) > n^{n^2}(2^n - n) > 0$. Thus by the Intermediate Value Theorem there exists a solution k_0. Consider the least solution k_l. We calculate $\frac{d}{dk}(f(k))$

for $k \geq k_l$. We have

$$\begin{aligned}
&\frac{d}{dk}(f(k)) \\
&= (n+1)^k \log(n+1) - n^k \log(n) - (n-1)^k \log(n) - \cdots - 2^k(\log(2)) \\
&> (n+1)^k \log(n+1) - S_k(n) \log(n+1) \\
&> \log(n+1) f(k).
\end{aligned}$$

Notice that $\log(n+1)$ is strictly positive. Thus if the sign of $f(k)$ is positive, the sign of $f'(k)$ will always be positive and the function will be increasing. Then since the function is strictly increasing whenever it is positive, it must be strictly increasing after it hits its first positive value. Note at $k = k_l$ $f'(k) > 0$ and $f(k) = 0$ so it must increase to some positive value and continue increasing after that.

Thus $f(k) > 0$ and increasing for every $k > k_l$ so there is no other solution.

Corollary 3: Let the real solution to the Erdos Moser Equation in n be k e.g. $S_k(n) = (n+1)^k$. Then $S_k(n-1) < n^k$.

Proof: By Theorem 2.5 $f(n) = (n+1)^k - S_k(n)$ is decreasing over the integers. □

Theorem 4: Stronger Upper Bound- $k < \lceil n \log 2 \rceil$

Proof: By Corollary 3, $S_k(n-1) < n^k$ so $S_k(n) < 2n^k$. Then $2n^k > (n+1)^k \implies 2 > (1+\frac{1}{n})^k \implies \log 2 > k \log(1+\frac{1}{n})$. Our earlier upper and lower bounds showed $k = O(n)$ so let $\frac{k}{n} = c$ for some constant c. Then $c < \frac{\log 2}{n \log(1+\frac{1}{n})}$. Recall the Taylor series expansion for $n \log(1+\frac{1}{n}) = 1 - \frac{1}{2n} + \frac{1}{3n^2} - \cdots > 1 - \frac{1}{2n}$. Thus $c < \frac{\log 2}{1-\frac{1}{2n}}$ and $k < \frac{n^2 \log 2}{n-\frac{1}{2}}$. For $n > 1$ we have $(n-\frac{1}{2})(n+1) > n^2$ so $k < (n+1)\log 2 = n \log 2 + \log 2$. Since $\log 2 < 1$ we have $k < \lceil n \log 2 \rceil$

Alternate Proof: Consider $f(n) = (n+1)^k - S_k(n)$ and $\Delta(f(n)) = f(n) - f(n-1) = (n+1)^k - 2n^k$. Then we find the first $\Delta(f(n)) < 0$, so where $(1+\frac{1}{n})^k < 2$. Our earlier upper and lower bounds showed $k = O(n)$ so let $\frac{k}{n} = c$ for some constant c. Then $c < \frac{\log 2}{n \log(1+\frac{1}{n})}$. Recall the Taylor series expansion for $n \log(1+\frac{1}{n}) = 1 - \frac{1}{2n} + \frac{1}{3n^2} - \cdots > 1 - \frac{1}{2n}$. Thus $c < \frac{\log 2}{1-\frac{1}{2n}}$ and $k < \frac{n^2 \log 2}{n-\frac{1}{2}}$. For $n > 1$ we have $(n-\frac{1}{2})(n+1) > n^2$ so $k < (n+1)\log 2 = n \log 2 + \log 2$. Since $\log 2 < 1$ we have $k < \lceil n \log 2 \rceil$.
We have $f(n) = f(1) + \sum_{i=1}^{n} \Delta(f(i)$. Note $f(1) = 2^k - 1 > 0$. We want to solve $f(n) = 0$, which implies at least one term is negative, but the least $\Delta(f(i)) < 0$ is $n > \frac{k}{\log 2} - 1$ completing the argument.

2.3.1 Bounds on n

A first attempt on making a bound uses a computer modeled after computing n that satisfy Theorem 2.1. We calculated that there were exactly 5 nontrivial solution candidates under $15 * 10^6$, which were

$2, 6, 42, 1806, 47058$. However, upon further inspection, these solutions all contradicted another one of our lemmas. Thus we get an initial bound of $n > 15 * 10^6$.

The next one is more detailed. Recall Theorem 2.2. We use this to make a much larger bound for n.

Theorem 2.7. For n satisfies the Erdos Moser equation, $n > 10^{10^7}$

Proof. Recall we obtained

$$n > (\prod_{p \leq x} p)^{\frac{1}{4}} - 1$$
$$\text{where} \sum_{p \leq x} \frac{1}{p} \geq \frac{19}{6}$$

We focus on $S = \sum_{p \leq x} \frac{1}{p}$. We rewrite this as $\sum_{n \leq x} \frac{1_p}{n}$ where 1_p is the prime indicator function. Then we apply Abel's sums to get

$$S = \frac{\Pi(x)}{x} + \int_2^x \frac{Pi(u)}{u^2} du$$

. Bounding $\Pi(x) < c\frac{x}{\log(x)}$ (where $c = 1.01$ is one such acceptable constant). So then

$$S < c(\frac{1}{\log(x)} + \int_2^x \frac{1}{u \log u} du$$
$$= c(\frac{1}{\log(x)} + \log(\log(x)) - \log(\log(2)))$$

We prior proved $x > 15,000,000$ so we fold in the $\frac{1}{\log x}$ with the other constants. This means $\frac{19}{6c} + \log(\log(2)) < \log(\log(x))$, $\log(\log(x)) > 2.75$, $x > e^{e^{0.25}} > 7 * 10^6$.

Now that we know $x > 6 * 10^6$ we try to find a lower bound for the product of primes less than x. We have $\Pi(x) > \frac{x}{\log x} > 4.5 * 10^6$, and $n > (\Pi(x)!)^{\frac{1}{4}}$, so we try to estimate $(4.5 * 10^6)!$. There is a common bounding of $m! < (\frac{m}{e})^m$. Also $4.5 > e$ and $4.5 > 10^{0.5}$ so $(4.5 * 10^6)!, > (10^6)^{10^{6.5}} > 10^{10^7}$.

Thus if n satisfies the Erdos Moser equation, $\boxed{n > 10^{10^7}}$

2.4 Linear Algebra Interpretation

The following section is an interpretation of the Erdös-Moser Equation in terms of Linear Algebra to express the sum in the problem statement.

Consider the following vector

$$\vec{v_1} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ \vdots \\ n \end{pmatrix}.$$

Then, let $\vec{v_2}$ be the diagonal of $\vec{v_1} \cdot \vec{v_1}^T$ from the element in the top left to the bottom right. Then,

$$\vec{v_2} = \begin{pmatrix} 1^2 \\ 2^2 \\ 3^2 \\ \vdots \\ n^2 \end{pmatrix}.$$

Similarly, let $\vec{v_3}$ be the diagonal of $\vec{v_2} \cdot \vec{v_1}^T$. Then,

$$\vec{v_3} = \begin{pmatrix} 1^3 \\ 2^3 \\ 3^3 \\ \vdots \\ n^3 \end{pmatrix}.$$

Similarly, let $\vec{v_m}$ be the diagonal of $\vec{v_{m-1}} \cdot \vec{v_1}^T$. Then,

$$\vec{v_m} = \begin{pmatrix} 1^m \\ 2^m \\ 3^m \\ \vdots \\ n^m \end{pmatrix}.$$

Now, note that the sum of the elements of $\vec{v_m}$ is $\vec{v_{m-1}} \cdot \vec{v_1}$. If we could find a nice way to take the diagonal of a matrix and put it into a vector, this approach may help us prove the Erdös-Moser Equation.

2.4.1 Geometric Representation

This subsection is a graphical approach to the Erdös-Moser Equation.

We have included a proof in this paper that k must be even if it is not 1. Now, consider $\vec{v_{\frac{k}{2}}}$ (see the last section for the definition of $\vec{v_m}$). We have that

$$\vec{v_{\frac{k}{2}}} \cdot \vec{v_{\frac{k}{2}}} = \|\vec{v}_{\frac{k}{2}}\|^2.$$

This is the desired sum on the left hand side of the Erdös-Moser Equation! Geometrically speaking, this is the square of the length of the vector represented by $\vec{v_{\frac{k}{2}}}$ in n dimensions. This must be equal to $(n+1)^k$, so we try to find a way to describe this geometrically as well. If we draw the equivalent of a sphere centered at the origin in $\frac{k}{2}$ dimensions with $\vec{v_{\frac{k}{2}}}$ as one radius, we must get the same sphere as if we had drawn a sphere at the origin in $\frac{k}{2}$ dimensions with radius $(n+1)^k$.

While this representation may not provide use in proving the conjecture, it does provide aesthetic value to the problem.

Chapter 3

Explorations on the Lonely Runners Conjecture

3.1 Problem Statement

Lonely Runners Conjecture - Consider a circular track with circumference of 1 mile and k runners running on the track starting from the same point such that they all have distinct speeds. A runner is said to be lonely if they are at least $\frac{1}{k}$ distance away from all other $k-1$ runners. The Lonely Runners Conjecture says that given any number of runners, k, and any set of k distinct speeds, there always comes an point in time after which all the runners have become lonely for at least once (at times that are not necessarily the same).

3.2 Progress on Problem

3.3 Angular Velocity Attempt

Here is an attempt at using the angular velocity of the runners to parameterize the times at which any two of the k runners would be lonely with respect to each other. The hope is that we can use this work to find out all the times when one runner is lonely with respect to everyone else. In this way, we could find when all of the runners are lonely, and if we prove that there exists a time at which all runners are lonely (at different times), then we will have proved the conjecture.

Assume the track is the unit circle in the complex plane. Assign speeds to the runners such that the speed of runner i is a_i, where a_i is an angular velocity of how much of the track in radians a certain runner

covers in a unit of time. Then, runner i completes one lap in $\frac{2\pi}{a_i}$ hours. Therefore, the number of laps run by runner i after t hours is $\frac{t}{\frac{2\pi}{a_i}} = \frac{a_i \cdot t}{2\pi}$. Therefore, the fraction of a lap that runner i has run after t hours (corresponding to the runner's final location) is $\{\frac{a_i \cdot t}{2\pi}\}$ (fractional part). Then, consider the position of runner a and runner b (let their speeds also be a and b in terms of angular velocity). If the two runners are lonely with respect to one another, then their positions are at least $\frac{1}{k}$ apart, so

$$|\ \{\frac{bt}{2\pi}\} - \{\frac{at}{2\pi}\}\ | \geq \frac{1}{k},$$

where a and b are the speeds of the corresponding runners. We can also write this as (WLOG)

$$\{\frac{bt}{2\pi}\} - \{\frac{at}{2\pi}\} \leq -\frac{1}{k} < \frac{1}{k} \leq \{\frac{at}{2\pi}\} - \{\frac{bt}{2\pi}\}.$$

However, there is not much else to do from largely due to the fractional parts that are hard to get rid of.

3.4 Parameterization of Pairwise Loneliness (Relative Velocities)

In this attempt, we use the relative speeds of the k runners (in miles per hour) to parameterize the times at which any two runners will be lonely with respect to one another.

Assume that the track is set in the complex plane such that it is circular and centered at the origin with radius $\frac{1}{2\pi}$ miles (so that the circumference is 1 mile). Let all of the runners start at the point corresponding to $\frac{1}{2\pi}$ on the complex plane (the rightmost point on this circular graph). Note that we are not doing any scaling or adjustment to this problem. Now, let the velocities of the k runners be $v_1, v_2, \cdots, v_k$, where v_i is the speed of runner i in miles per hour. Wish to take the relative to the speeds of the runners.

WLOG, let us focus on runner 1. Let the track have speed $-v_1$, meaning that it rotates clockwise (in this example, we say that forward velocities travel counter clockwise while backward velocities travel clockwise). Because the track is rotating in the opposite direction of runner 1 at the same speed, we note that runner 1 stays in the same place throughout the duration of the race. Also note that in order for this to work, we must subtract v_1 from the velocities of all other runners. So, runner i will travel at $v_i - v_1$ miles per hour now. Note that this new speed may be negative, which would mean that runner i is running in a clockwise direction. If this is positive, runner i will be slower than their original speed. Also note that since all v_i's are in miles per hour, $v_i - v_1$ is a speed in miles per hour as well.

Since the track has circumference 1 mile, runner i completes one lap (travels 1 mile) in $\frac{1}{v_i - v_1}$ hours. We wish to find when runner 1 and runner i will be $\frac{1}{k}$ miles apart (parameterizing the pairwise loneliness). Remember that runner 1 is stationary at the rightmost point of the track on the graph. Therefore, runner i is lonely with respect to runner 1 when runner i has run $n_i + \frac{1}{k}$ to $n_i + 1 - \frac{1}{k}$ laps for some integer n_i (this is the period of time at which runner i is between $\frac{1}{k}$ to $-\frac{1}{k}$ miles away from runner 1). Since runner i completes a lap every $\frac{1}{v_i - v_1}$ hours, we find that between $\left(n_i + \frac{1}{k}\right) \cdot \left(\frac{1}{v_i - v_1}\right) = \frac{n_i + \frac{1}{k}}{v_i - v_1}$ and $\left(n_i + 1 - \frac{1}{k}\right) \cdot \left(\frac{1}{v_i - v_1}\right) = \frac{n_i + 1 - \frac{1}{k}}{v_i - v_1}$

hours from the start time, runner 1 and runner i will be lonely with respect to one another. Since n_i is defined as any nonnegative integer, there are an infinite points in time at which runner 1 and runner i are lonely with respect to one another. Specifically, $n_i \in [0, \infty)$, and n_i is an integer. We can repeat this for all integers $i \in [2, 3, 4, \cdots, k]$.

We find that for a common time

$$t \in \left[\frac{n_i + \frac{1}{k}}{v_i - v_1}, \frac{n_i + 1 - \frac{1}{k}}{v_i - v_1}\right]$$

(number of hours after start), there must be integers $n_2, n_3, n_4, \cdots, n_k$ such that there exists such a time t. At this time t, runner 1 is lonely with respect to all other runners. Note that this time may be negative due to the fact that runner i's speed is negative. In this case, we must always take the absolute value of the times in the above parameterization. After finding this common time t, we focus our attention toward runner 2 instead of runner 1. We do this because we now know that there exists a time at which runner 1 is lonely. Similarly, we can find integers $n_1, n_3, n_4, \cdots, n_k$ such that t is constant, and so now we know that runner 2 will be lonely at some point in time. We can do this same process for runners $3, 4, 5, \cdots, k$ and prove that they will all be lonely at some point in time. If we can prove that such integers $n_1, n_2, \cdots, n_k$ must always exist, where these values of n change based on which runner we are taking the relative speed of, we will have proved the Lonely Runners Conjecture.

3.4.1 Example of Parameterization

As an example, we take $k = 3$ and set $v_1 = 6, v_2 = 7, v_3 = 8$ (miles per hour). Taking the relative speeds with respect to runner 1, we find that

$$t \in \left[\frac{n_2 + \frac{1}{3}}{v_2 - v_1}, \frac{n_2 + 1 - \frac{1}{3}}{v_2 - v_1}\right] = \left[n_2 + \frac{1}{3}, n_2 + 1 - \frac{1}{3}\right] = \left[n_2 + \frac{1}{3}, n_2 + \frac{2}{3}\right]$$

and

$$t \in \left[\frac{n_3 + \frac{1}{3}}{v_3 - v_1}, \frac{n_3 + 1 - \frac{1}{3}}{v_3 - v_1}\right] = \left[\frac{n_3 + \frac{1}{3}}{2}, \frac{n_3 + 1 - \frac{1}{3}}{2}\right] = \left[\frac{n_3 + \frac{1}{3}}{2}, \frac{n_3 + \frac{2}{3}}{2}\right].$$

If we set $n_2 = n_3 = 0$, the intervals become

$$\left[\frac{1}{3}, \frac{2}{3}\right]$$

and

$$\left[\frac{\frac{1}{3}}{2}, \frac{\frac{2}{3}}{2}\right] = \left[\frac{1}{6}, \frac{1}{3}\right].$$

So, when $t = \frac{1}{3}$, or when $\frac{1}{3}$ of an hour passes, runner 2 will be $\frac{1}{k} = \frac{1}{3}$ of a mile in front of runner 1, and runner 3 will be $\frac{1}{k} = \frac{1}{3}$ behind runner 1. Therefore, runner 1 is lonely. A similar process can be done to find if there exist times such that runner 2 and runner 3 are lonely. However, we could also note that since runner 1 and runner 2 are $\frac{1}{3}$ of a mile apart and runner 1 and runner 3 are $\frac{1}{3}$ of a mile apart and the track is 1 mile long, that runner 2 and runner 3 are $\frac{1}{3}$ mile apart. In other words, at this point in time, we have

coincidentally found an instance in which all runners are lonely at the same time! Note that the method described in the problem will also yield the same results if performed on runner 2 and runner 3 as well. Additionally, we could have found other points in time t that satisfy the conditions above, but we chose all the n's to be 0 for simplicity.

3.4.2 Consecutive Speeds for 3 runners

In the last example, there was nothing special about the speeds $6, 7, 8$ other than the fact that they were all consecutive (and only 3 runners). So, we try to generalize this. Set $v_1 = v, v_2 = v + 1, v_3 = v + 2$. We take the relative speeds with respect to runner 1 to find that runner 2 and runner 3 will be lonely with respect to runner 1 at the times

$$t \in [\frac{n_2 + \frac{1}{3}}{v_2 - v_1}, \frac{n_2 + 1 - \frac{1}{3}}{v_2 - v_1}] = [n_2 + \frac{1}{3}, n_2 + 1 - \frac{1}{3}] = [n_2 + \frac{1}{3}, n_2 + \frac{2}{3}]$$

and

$$t \in [\frac{n_3 + \frac{1}{3}}{v_3 - v_1}, \frac{n_3 + 1 - \frac{1}{3}}{v_3 - v_1}] = [\frac{n_3 + \frac{1}{3}}{2}, \frac{n_3 + 1 - \frac{1}{3}}{2}] = [\frac{n_3 + \frac{1}{3}}{2}, \frac{n_3 + \frac{2}{3}}{2}]$$

. If we set $n_2 = n_3 = 0$, the intervals become

$$[\frac{1}{3}, \frac{2}{3}]$$

and

$$[\frac{\frac{1}{3}}{2}, \frac{\frac{2}{3}}{2}] = [\frac{1}{6}, \frac{1}{3}].$$

So, when $t = \frac{1}{3}$, or when $\frac{1}{3}$ of an hour passes, runner 2 will be $\frac{1}{k} = \frac{1}{3}$ of a mile in front of runner 1, and runner 3 will be $\frac{1}{k} = \frac{1}{3}$ behind runner 1. This is exactly the same as before! We find that all runners are lonely after $\frac{1}{3}$ of an hour. Can we generalize this even more?

3.4.3 Consecutive Speeds for k runners

Let the speeds of the k runners be $v_1 = v, v_2 = v + 1, v_3 = v + 2, \cdots, v_k = v + k - 1$. From these last two examples, it is trivial to show that: It is sufficient to show that the end element of the interval for t given by the above formulas for runner k is greater than or equal to the first element of the range for t for runner 2 (if we are taking the relative speeds with respect to runner 1 and when all n are set to 0) in order to show that runner 1 will be lonely. From the formulas, we can calculate that the end element of the interval for t given by the above formulas for runner k is $\frac{1}{k \cdot 1} = \frac{1}{k}$. Additionally, we can show that the first element of the range for t for runner 2 is $\frac{k-1}{k \cdot (k-1)} = \frac{1}{k}$. Wait, at the time $\frac{1}{k}$ hours from the start, both runner 2 and runner k are $\frac{1}{k}$ miles from runner 1. What about the positions of the other runners? Well, we know the speeds of the runners, and we have a time ($\frac{1}{k}$ hours from the start), so let's multiply to find distance! The speed of runner i is $v_i - v_1 = i - 1$. We multiply these by $\frac{1}{k}$, and we get that the distance runner i has run after $\frac{1}{k}$

hours is $\frac{i-1}{k}$. So, the distances of runners $1, 2, 3, 4, \cdots, k$ from the start are $0, \frac{1}{k}, \frac{2}{k}, \frac{3}{k}, \frac{4}{k}, \cdots, \frac{k-1}{k}$. Therefore, all of the k runners are $\frac{1}{k}$ miles apart, so all of the runners are lonely after $\frac{1}{k}$ hours of the start.

In conclusion, if k runners have consecutive speeds, then they will all be lonely after $\frac{1}{k}$ hours of starting the race. More generally, if the k runners have speeds that all differ by 1, then they will all be lonely after $\frac{1}{k}$ hours of starting the race. (This means that v in the proof need not be an integer. It just must be real.)

3.5 Velocities in Arithmetic Progression

We can generalize our last claim from the previous section. Let us start with k runners so that the velocities of the runners are

$$v, v+j, v+2j, v+3j, v+4j, \cdots, v+j(k-1).$$

In other words, these speeds are in arithmetic progression. Taking the relative velocities of the k runners with respect to runner 1, who has velocity v, we find the relative speeds to be

$$0, j, 2j, 3j, 4j, \cdots, j(k-1).$$

We can use the parameterization at the beginning of the section to show that after $\frac{1}{jk}$ hours, all of the runners will be lonely, therefore satisfying the conjecture. While the derivation provides aesthetic value, the proof for this is much more trivial and easier to communicate:

The relative speed with respect to runner 1 of runner i is $j(i-1)$. We claim that after $\frac{1}{jk}$ hours, all of the runners will be lonely, so this serves as the "time." We multiply the respective "times" and "speeds" for each runner to find the location of runner i after $\frac{1}{jk}$ hours. We get

$$\frac{j(i-1)}{jk} = \frac{i-1}{k}.$$

Therefore, runner i has run $\frac{i-1}{k}$ miles after $\frac{1}{jk}$, meaning that all of the k runners are equidistant around the circle at this time, or all $\frac{1}{k}$ miles from each other. This position satisfies the conjecture.

In conclusion, if we have k runners with velocities in arithmetic progression such that the k velocities in miles per hour are

$$v, v+j, v+2j, v+3j, v+4j, \cdots, v+j(k-1),$$

then they will all be simultaneously lonely after $\frac{1}{jk}$ hours. (Note that the only restriction on v and j is that they must be real.)

3.5.1 Scaling

We show we can scale all the velocities by a nonzero constant and the existence of the solution is unchanged. Recall we can use relative velocities, thus set $v_0 = 0$. Then consider the set of speeds

$$V = \{0, v_1, v_2 \dots v_{k-1}\}$$

. Now consider as well the scaled set

$$cV = \{0, cv_1, cv_2 \dots cv_{k-1}\}$$

Let a lonely position for runner i be where it is lonely with respect with runner 0. We want to find solutions for the time t s.t. for $1 \leq i \leq k-1$ runner i is at a lonely position at time t. Assume there is such a time t_0 s.t. runners with their velocities in V are lonely. Then $t = \frac{t_0}{c}$ gives the same final positions and is such a lonely time. Since there are no restrictions other than nonzero on c this same proof applies in the other direction as well because$V = \frac{1}{c}(cV)$, thus scaling is allowed.

3.6 Restriction to Integers using Kronecker's Theorem

Statement: We show that if the lonely runner conjecture holds true with the speeds ranging over integers with total gcd 1, then it holds true for any set of speeds over the reals. Remember we can scale by a constant, and add and subtract velocities. We also set the speed of runner 0 with $v_0 = 0$ by using relative velocities. We define a lonely position as lonely as respect to runner 0. So throughout this proof we assume that any set of speeds where all are integers must have a solution for time where all the runners are in lonely positions.

Lemma 3.1. If the conjecture holds for a set of speeds of integers with total gcd 1, it holds true for all rationals.

Proof: Consider any set of rational speeds. We scale the velocities by the lcm of the denominators such that they become all integers. Then we divide by the total gcd of these integers. This gives integers with total gcd 1. Now we can assume that any set of speeds that are all rational has a solution for time where they are all lonely.

Lemma 3.2. After an integer time, a runner with integer speed returns to its position before this time.

Proof. The proof is a simply that $d = rt$ and if r, t are integers then $d \in \mathbb{Z}$ so $d \equiv 0 \mod 1$ and it stays in the same spot.

Theorem 3.1. Kronecker's Theorem: Given an n-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{R}^n$, $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{R}^n$, there exists $q, p_j \in \mathbb{Z}$ s.t. $|q\alpha_j - p_j - \beta_j| < \epsilon$ for all j iff for all integer n-tuples $(r_1 \ldots r_n) \in \mathbb{Z}^n$ whenever $\sum_{j=1}^{n} \alpha_j r_j \in \mathbb{Z}$ so is $\sum_{j=1}^{n} \beta_j r_j \in \mathbb{Z}$. Proof not given.
Since $\mathbb{Z} \subset \mathbb{Q}$ we look at the r_js as $\mathbb{Q}$ coefficients, which suggests working in a $\mathbb{Q}$-vector space. So now we can visualize Kronecker's Theorem over a $\mathbb{Q}$-vector space.

Reformulation of the original problem: Consider k runners with different speeds, where runner 0 has speed 0. We want to show that we only need to consider integer speeds with gcd 1. By Lemma 3.1, this means we can consider any rational set of speeds to work. Say we are given a set of irrational and rational speeds. We scale so that all speeds are either irrational or integer. By assumption there is a time t_0 when all integer speeds are at a lonely position. Then we show that there is some time $t_1 \in \mathbb{Z}$ s.t. at $t = t_1 + t_0$ all runners are lonely with respect to runner 0. By Lemma 3.2, all runners with integer speeds are at lonely positions at this time.

Let the α_i from Kronecker's Theorem represent the irrational speeds, the β_i represent their positions, and q represent the time. Then we have two cases:
1. $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is linearly independent in $\mathbb{Q}$-space. Then if $\sum r_j \alpha_j \in \mathbb{Q}$ all the $r_1, \ldots r_n$ are 0, and thus $\sum_j r_j \beta_j = 0 \in \mathbb{Z}$ so we can apply Kronecker Theorem. We then choose β_i to be in the lonely range.
2. $(\alpha_1, \alpha_2 \ldots \alpha_n)$ are linearly dependent. Consider a $\mathbb{Q}$ basis $(\alpha_1, \alpha_2, \ldots \alpha_b)$. Similarly to part 1, consider a time q when everything in the basis is at a lonely position $\beta_i = \beta$ for $i \leq b$, which exists for every choice of β by Kronecker's Theorem as above. Then since the basis spans the set in $\mathbb{Q}$ we have every $\alpha_i = r_i \beta$ for $r_i \mathbb{Q}$. Now we show there exists some β where $r_i \beta$ is also a lonely position for every $b < i \leq n$. Consider the set $(1, r_{b+1}, r_{b+2} \ldots r_n)$ removing duplicates if necessary. Though these represent scaled positions, we think about this as a set of speeds in the conjecture. Since $r_i \in \mathbb{Q}$, by lemma 2 and our assumption of the lonely runners proposition working over integers $\exists T \in \mathbb{R}$ s.t. $(T, Tr_{b+1}, Tr_{b+2} \ldots Tr_n)$ are lonely positions. Here T represents what would be our time solution to this rational set if they were speeds of runners. Then choose $\beta = T$ and we get lonely positions $(\beta, \beta r_{b+1}, \ldots \beta r_n$ completing the proof. $\square$

Thus when doing the lonely runners conjecture if we can prove Kronecker's Theorem we only need to consider integer values.

We then present a simpler problem that becomes the same as the Lonely Runners Conjecture. For every $k-1$-tuples of integers $a_1, a_2, \ldots a_{k-1}$ does there exist a $t \in \mathbb{R}$ and integers $p_1, p_2 \ldots p_{k-1}$ s.t. $\forall i < k$ we

have $\frac{1}{k} \leq ta_i - p_i \leq \frac{k-1}{k}$

Chapter 4

Explorations on the Collatz Conjecture

4.1 Problem Statement

Collatz Conjecture - Consider the following function:

$$C(n) = \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \pmod 2 \\ 3n+1 & \text{if } n \equiv 1 \pmod 2 \end{cases}.$$

The Collatz Conjecture says that given any integer n, repeated iterations of the above function will always result in the number 1. In other words, $C^x(n) = 1$ for some positive integer x.

For the natural numbers until 2^{68}, the conjecture has been shown to hold true using computation.

4.2 Progress on Problem

4.3 Research and Other Approaches

4.3.1 Representations and Examples

Take a number a. Repeatedly applying f, the Collatz Conjecture states that $f^n(a) = 1$ for some n commonly referred to as the stopping time of a. For example, the number 27 has a relatively high stoppage time of 111:

$$27, 82, 41, 124, 62, 31, 94, \cdots, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1.$$

Many sources represent the Collatz Conjecture in the form of several types of diagrams. The first type of diagram starts at 1 and works backwards to create a sort of tree, where branches split every time a new

number is found from the inverse of the two rules of f (explained in detail later). As a short description,this drawing strangely resembles coral from the sea. Another common type of diagram regarding this conjecture is achieved by plotting on the Cartesian Plane. The number a is the x-coordinate and the highest number that is reached in the sequence

$$a, f(a), f^2(a), \cdots, f^n(a)$$

is the y-coordinate. When this plot is done for a significantly large number of x-values, the image starts to look like the rays of a light emitting object, casting relatively solid lines in a positive slope.

4.3.2 Common Strategies

One way to prove this conjecture false is to prove that for some number a, the sequence

$$a, f(a), f^2(a), \cdots, f^n(a)$$

is periodic and that none of the elements are 1. Additionally, proving that this sequence increases without bound could disprove the conjecture, but no such numbers have been found that satisfy either case. Rather than proving the Collatz Conjecture, a myriad of mathematicians have considered the probability of it being true. For example, when we consider

$$a, f(a), f^2(a), \cdots, f^n(a)$$

it has been observed that every odd number is on average $\frac{3}{4}$ of the previous odd number. If this could be rigorously proved, the Collatz Conjecture is almost surely true. Finally, there is a strategy in, instead of proving that every positive integer ends up in the said cycle $4, 2, 1, \cdots$ (or ends up at 1), proving that when we work backwards from 1 in the aforementioned inverse tree, we get every positive integer. This last strategy is the one that I decided to contribute my attempts towards.

4.3.3 A Binary Viewpoint of the Conjecture

The Collatz Conjecture can very elegantly be represented in binary. Take a number a in base 2. Now, remove all trailing 0's. For example, 101000 becomes 101. If a number has a trailing 0 in binary, it must be divisible by 2. Removing all of these trailing 0's is therefore the same as dividing by 2 until our result becomes odd. Now that our result is odd, We must multiply by 3 and add 1. Let our odd number be a. In order to perform the needed operation, we divide our work into adding $2a + 1$ and a, which will give $2a + 1 + a = 3a + 1$, as desired. The number a is already in binary. The number $2a + 1$ is the same as adding a trailing 0 to a and then adding 1 in place of that trailing 0. This whole operation can be described simply by “appending" a 1 to the end of a. Now, we add our representations of a and $2a + 1$, giving us $3a + 1$, an even number. Even numbers in base 2 (binary) have trailing 0's. If we repeat the above steps, we are doing the same thing as implementing the rules of the Collatz Conjecture.

4.4 Exploring the Collatz Conjecture

Instead of trying to prove that every number x results in this sequence, we try to work backwards from 1. The only number that can result in 1 is 2 because $\frac{2}{2} = 1$ or $1 \cdot 2 = 2$. Similarly, the only number that can result in 2 is 4. Now, we come to a bit of a dilemma when we arrive at what numbers x give $f(x) = 4$. On the one hand, if our number is odd, then we can solve to find that $x = 1$ works because $\frac{4-1}{3} = 1$. However, we can also solve for x if x is even. This gives us $\frac{x}{2} = 4$ or $x = 8$ (applying the rule of f). We can continue in this manner to work backwards. Our strategy is to find whether or not every positive integer lies on this "tree." In order to effectively work backwards, we find the inverse for the two rules of the function. This would be

$$x = 2 \cdot f(x) \tag{1}$$

when x is even and

$$x = \frac{f(x) - 1}{3} \tag{2}$$

when x is odd. Then, we can easily calculate that the number 1 can only come from 2 by (1). Note that we cannot use (2) because this results in a number that is not in the domain of f (namely 0). Similarly, we can use (1) to see that one can arrive at 2 starting with $x = 4$ (again, we cannot use rule (2) for the same reason as before). When we arrive at the number 4, we see that both rule (1) and rule (2) give us numbers in the domain of f. Rule (1) gives $x = 8$ while rule (2) takes us back to $x = 1$. Note that we can keep on applying rule (1) since we are simply multiplying by 2 (no chance for a fraction) and the x that we end up with will be even. Therefore, we can continue in this manner to get

$$16, 32, 64, \cdots, 2^n$$

for some $0 \leq n < \infty$. But for which of these numbers can we use rule (2)? Since rule (2) subtracts 1 and then divides by 3, in order for this to be an integer, our number must have a remainder of 1 when divided by 3. Additionally, our number must be even because applying the rule of $f(x)$ for an odd x always results in an even number. Combining this with the rule that we multiply by 2 each time this above sequence, we know that we can apply the rule to 4 (because $4 \equiv 1 \pmod 3$). Multiplying any number $n \equiv 1 \pmod 3$ by 2 does not result in another number that has a remainder of 1 when divided by 3. However, multiplying by 2 again does produce a number $4n \equiv 1 \pmod 3$ because $2 \equiv -1 \pmod 3$. Therefore, rule (2) can be applied to

$$4, 4 \cdot 4, 4 \cdot 4^2, 4 \cdot 4^3, \cdots, 4 \cdot 4^n. \tag{3}$$

Applying the rule, we get

$$\frac{4-1}{3}, \frac{4 \cdot 4 - 1}{3}, \frac{4 \cdot 4^2 - 1}{3}, \frac{4 \cdot 4^3 - 1}{3}, \cdots, \frac{4 \cdot 4^n - 1}{3}. \tag{4}$$

Adding the pairwise elements of (3) and (4) in sequential order, we find that the sum of the first element of (3) and (4) is equal to the second element of (4). Similarly, the second element of (3) and (4) added together results in the third element of (4). We can continue in this manner and find that This happens for all the listed examples. In fact, it can be shown that this happens for all elements of these two sequences. We now develop yet another strategy to simplify our search. Say that we wish to see if a is on our inverse tree. Because all a can be written as $a = 2^k \cdot b$, We only have to prove that b is on the tree. Then, applying rule (1) repeatedly, we can show that a is on the tree as well. Therefore, we are interested in somehow parameterizing the odd numbers that lie on our tree. Let us focus on which odd numbers result from (3) for now. So, let $a = 4$ and $b = 1$ because these are the first two elements of (3) and (4) (note that this has nothing to do with the previous definitions of a and b). We can rewrite (3) as

$$a, 4a, 4^2a, 4^3a, \cdots, 4^n a.$$

Then, the kth element of (4) becomes the sum of the first $k-1$ elements of (3) and the first element of (4) (this is an extension of the fact that the pairwise sums of the elements of (3) and (4) result in the next term of (4)). Then, the kth element of (4) becomes

$$a + 4a + 4^2a + \cdots + 4^{k-2}a + b.$$

Note that we use a and b to show that the following result is not specific to the values of a and b. They are only two terms that result from the rule of the original conjecture for odd numbers (in other words, $a = 3b+1$). Our above expression can be simplified because of the sum of a geometric sequence. It becomes $a\left(\frac{4^{k-1}-1}{4-1}\right) + b = a\left(\frac{4^{k-1}-1}{3}\right) + b$. In summary, all of the odd numbers that result from the inverse tree (3) can be written in the form $a\left(\frac{4^m-1}{3}\right) + b$ for some $0 \leq m < \infty$ and a and b are the two smallest numbers in (3) and (4). Now, each of these resulting odd numbers forms its own tree similar to (3). For example, the second element of (4) is 5. Multiplying this number by 2 repeatedly gives us

$$5, 5 \cdot 2, 5 \cdot 2^2, 5 \cdot 2^3, \cdots, 5 \cdot 2^n.$$

Note that we use rule (1) to achieve this list. Now, we find the numbers in this list which are congruent to 1 (mod 3) and are even in order to find which numbers we can apply (2) to. These are

$$5 \cdot 2, 5 \cdot 2^3, 5 \cdot 2^5, \cdots, 5 \cdot 2^{2n-1}$$

or

$$(5 \cdot 2), (5 \cdot 2) \cdot 2^2, (5 \cdot 2) \cdot 2^4, \cdots, (5 \cdot 2) \cdot 2^{2n-2}$$

or

$$(5 \cdot 2), (5 \cdot 2) \cdot 4^1, (5 \cdot 2) \cdot 4^2, \cdots, (5 \cdot 2) \cdot 4^{n-1}.$$

This looks extremely similar to (3). If we replace 4 with $(5 \cdot 2)$ in (3), we will get the above list. Letting $a = (5 \cdot 2) = 10$ and $b = \frac{(5\cdot 2)-1}{3} = 3$, we get the same parameterization as before, or $10\left(\frac{4^m-1}{3}\right) + 3$. We now realize through this example that we can eliminate the b variable altogether because of the relationship $b = \frac{a-1}{3}$. Our parameterization $a\left(\frac{4^m-1}{3}\right) + b$ becomes

$$a\left(\frac{4^m-1}{3}\right) + \frac{a-1}{3} = a\left(\frac{4^m-1}{3}\right) + \frac{a}{3} - \frac{1}{3} = a\left(\frac{4^m-1}{3} + \frac{1}{3}\right) - \frac{1}{3} = a\left(\frac{4^m}{3}\right) - \frac{1}{3} = \frac{a4^m-1}{3}.$$

To reiterate, $\frac{a4^m-1}{3}$ is the form of an odd number that results from the tree which has a at the bottom of it. Just like we did with the specific case of 5, we can form a list similar to (3):

$$\frac{a4^m-1}{3}, \frac{a4^m-1}{3}\cdot 2, \frac{a4^m-1}{3}\cdot 2^2, \frac{a4^m-1}{3}\cdot 2^3, \frac{a4^m-1}{3}\cdot 2^4, \cdots, \frac{a4^m-1}{3}\cdot 2^n.$$

From this list, we aim to find the numbers that are congruent to 1 (mod 3) even in order to find which numbers we can apply (2) to (just like before, but in general now). By definition, $\frac{a4^m-1}{3}$ is odd, so it cannot be in our list. If $\frac{a4^m-1}{3} \equiv -1 \pmod 3$, then our list is

$$\left(\frac{a4^m-1}{3}\cdot 2\right), \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 2^2, \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 2^4, \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 2^6, \cdots, \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 2^{2n}.$$

for some n. This is the same as

$$\left(\frac{a4^m-1}{3}\cdot 2\right), \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 4, \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 4^2, \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 4^3, \cdots, \left(\frac{a4^m-1}{3}\cdot 2\right)\cdot 4^n.$$

On the other hand, if $\frac{a4^m-1}{3} \equiv 1 \pmod 3$, then our list is

$$\left(\frac{a4^m-1}{3}\cdot 2^2\right), \left(\frac{a4^m-1}{3}\cdot 2^2\right)\cdot 2^2, \left(\frac{a4^m-1}{3}\cdot 2^2\right)\cdot 2^4, \left(\frac{a4^m-1}{3}\cdot 2^2\right)\cdot 2^6, \cdots, \left(\frac{a4^m-1}{3}\cdot 2^2\right)\cdot 2^{2n}.$$

This can also be written in a similar form as the first list:

$$\left(\frac{a4^m-1}{3}\cdot 4\right), \left(\frac{a4^m-1}{3}\cdot 4\right)\cdot 4, \left(\frac{a4^m-1}{3}\cdot 4\right)\cdot 4^2, \left(\frac{a4^m-1}{3}\cdot 4\right)\cdot 4^3, \cdots, \left(\frac{a4^m-1}{3}\cdot 4\right)\cdot 4^n.$$

Both of these lists are extremely similar to (3) where $a_1 = \frac{a4^m-1}{3}\cdot 2$ or $a_1 = \frac{a4^m-1}{3}\cdot 4$. Substituting this in the parameterization we stated before, we get

$$\frac{2\cdot\left(\frac{a4^m-1}{3}\right)\cdot 4^{m_1}-1}{3} = \frac{2\cdot(a\cdot 4^{m+m_1}-4^{m_1})-3}{9}$$

for some value m_1 with the same restrictions as m. Let's keep going and see if we can find a pattern. For now, let's stick to the alternative where $a_1 = \frac{a4^m-1}{3}\cdot 2$. The case where $a_1 = \frac{a4^m-1}{3}\cdot 4$ is exactly the same but with the 4 instead of the 2. Now, let $a_2 = 2\cdot\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}$ (again, $a_2 = 4\cdot\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}$ is essentially the same case).

To wit, there is always only one option for a_2 (as well as all a_i's): either one of $2\cdot\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}$ or $4\cdot\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}$. We choose which one of the two based on which one is congruent to 1 (mod 3). Also, if

$\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}$ is congruent to 0 (mod 3), we can only apply rule (1) to this tree and not rule (2). In this example, we are assuming that $2\cdot\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}\equiv 1$ (mod 3), but the case that $4\cdot\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}\equiv 1$ (mod 3) is the same, so we essentially cover all such cases.

We take the parameterization of all of the odd numbers resulting from rule (2) applied to tree with the number a_2 at the base:

$$\frac{2\cdot\left(\frac{2\cdot\left(a\cdot 4^{m+m_1}-4^{m_1}\right)-3}{9}\right)\cdot 4^{m_2}-1}{3}=\frac{2\cdot(2\cdot(a\cdot 4^{m+m_1+m_2}-4^{m_1+m_2})-3\cdot 4^{m_2})-9}{27}$$

for some m_2 with the same restrictions as m. Putting our 3 parameters together, we have

$$\frac{a4^m-1}{3},\frac{2\cdot(a\cdot 4^{m+m_1}-4^{m_1})-3}{9},\frac{2\cdot(2\cdot(a\cdot 4^{m+m_1+m_2}-4^{m_1+m_2})-3\cdot 4^{m_2})-9}{27}.$$

There seems to be a pattern. It can be proved using induction (by using these examples as the base case and replacing the 2's with x_i's to cover all cases of 2 and 4) that all parameterizations are in the form:

$$\left(x_i\left(x_{i-1}\left(x_{i-2}\left(\cdots\left(x_1(a\cdot 4^{m_1+m_2+\cdots m_{i+1}}-3^0\cdot 4^{m_2+m_3+\cdots+m_{i+1}}\right)-3^1\cdot 4^{m_3+m_4+\cdots+m_{i+1}}\right)\right)\cdots-3^{i-1}\cdot 4^{m_{i+1}}\right)-3^i\right)\div\left(3^{i+1}\right)$$

where:

- all x_i's are 2 or 4 depending on (mod 3) of the inner term. If the inner term is congruent to -1 (mod 3), then $x_i=2$. If the inner term is congruent to 1 (mod 3), then $x_i=4$ (of course, if the inner term is congruent to 0 (mod 3), we cannot apply rule (2) to this tree);
- For all m_i's, $0\leq m_i<\infty$;
- a is the smallest even number on a given inverse tree produced by rule (1) such that $a\equiv 1$ (mod 3);
- i is the number of x_i's.

From such parameterizations, we can try to find out whether all odd numbers satisfy the Collatz Conjecture. If they do, this finishes the proof. If not, we can disprove the Collatz Conjecture as well.

4.5 Summary of Approach

The above approach was to work backwards from 1 to see if every positive integer would satisfy the Collatz Conjecture. Because all even numbers must be divided by 2 by the rule of the function f, I narrowed my search to see if all odd numbers lied on this "inverse tree." In the end, I came up with a parameterization or form in which all of these odd numbers produced can be written in. I believe that we can use this form to prove or disprove the conjecture as follows: if we can prove that all positive odd integers can be written in this form, this will prove the Collatz Conjecture. If we prove that a certain number cannot be written in this form, we will disprove the conjecture. As such, this is my Recommendations for Further Experimentation.

4.6 Attempt By Strong Induction

We will attempt this problem by Strong Induction. Our Base Case, $n = 2$ is satisfied, since dividing by 2 results in 1. Now, say that $1, 2, 3, \ldots, n-1$ are satisfied by the Collatz Conjecture. If we can prove that n is also satisfied, or that n eventually simplifies to a number less than n, then the Collatz Conjecture is proved. We will do this by examining the parity of n. If n is even, then employing the second rule, the first iteration of n is $\frac{n}{2}$, which is satisfied by our inductive hypothesis. Now, the case where n is odd is a bit more tricky.

Consider n an odd number $2\alpha_1+1$. Then, through the Odd Rule, we have $C^1(n) = 3(2\alpha_1+1)+1 = 6\alpha_1+4$, which is an even number. Hence, we have that $C^2(n) = 3\alpha_1 + 2$. Now, we cannot determine the parity of $C^2(n)$ without knowing the parity of α_1. Hence, there are two cases to consider. If α_1 is even, then we can say that $\alpha_1 = 2\beta_1$. Then, we have $C^2(n) = 6\beta_1 + 2 \Rightarrow C^3(n) = 3\beta_1 + 1$. Since we have $n = 2\alpha_1 + 1 = 4\beta_1 + 1$, we see that $C^3(n) < n$, and by the Inductive Hypothesis, n is satisfied by the Collatz Conjecture. Now, we need to consider the case where $\alpha_1 \equiv 1 \pmod 2 \Rightarrow \alpha_1 = 2\alpha_2 + 1$. Then, we have that $C^2(n) = 6\alpha_2 + 5$, which is odd. Hence, by the Odd Rule, we have that $C^3(n) = 18\alpha_2 + 16$. Employing the Even Rule, we have $C^4(n) = 9\alpha_2 + 8$. To proceed, we will introduce a new definition.

4.6.1 Parity Sequences and Strong Induction

Definition 4.1. A *parity sequence* of a number's Collatz reduction refers to the parity of the numbers in that sequence, and is denoted in a string of either o, denoting odd, or e, denoting even.

Example 4.1. Consider the number 7. Its Collatz reduction is $22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1$. Hence, the parity sequence for 7 is *e-o-e-o-e-e-o-e-e-e-o-e-e-e-e-o*.

Theorem 4.1. In reducing a number n, there cannot be a parity sequence *o-o*.

Proof. Consider an odd number $2k+1$. By Rule 2 of the function C, the next iteration would be $3(2k+1)+1 = 6k + 4$, which has an even parity. ■

We will continue in the manner of *e-o-e-o-* ... continuing forwards. We cannot directly find the parity of $C^4(n)$ without knowing the parity of α_2. Since we are continuing on in the manner of *e-o-e-o-* ..., we have that $\alpha_2 \equiv 1 \pmod 2 \Rightarrow \alpha_2 = 2\alpha_3 + 1$. Hence, we have $C^4(n) = 18\alpha_3 + 17$. By the Odd Rule, we have $C^5(n) = 54\alpha_3 + 52$. Employing the Even Rule, we have $C^6(n) = 27\alpha_3 + 26$. Continuing on in the *e-o-e-o-*

... parity sequence, we find the following pattern:

$$C^2(n) = 3\alpha_1 + 2 = 3^1\alpha_1 + 2.$$
$$C^4(n) = 9\alpha_2 + 8 = 3^2\alpha_2 + 8.$$
$$C^6(n) = 27\alpha_3 + 26 = 3^3\alpha_3 + 26.$$
$$C^8(n) = 81\alpha_4 + 80 = 3^4\alpha_4 + 80.$$

Combining the above four equations, we get the following theorem:

Theorem 4.2. Consider an odd number n following a parity sequence of *e-o-e-o-* ... for b iterations, where $n = 2\alpha_1 + 1$ and $\alpha_i = 2\alpha_{i+1} + 1, \alpha_j \in \mathbb{Z}$. Then, $\forall 1 \leq d \leq b$ we have the following:

$$C^{2d}(n) = 3^d\alpha_d + 3^d - 1.$$

Proof. We will prove this by induction. Our Base Case is $d = 1$. As demonstrated above, we already have $C^2 = 3\alpha_1 + 2$. Now consider our Inductive Hypothesis: we will assume that for all $1 \leq d \leq d$, we have that $C^{2d}(n) = 3^d\alpha_d + 3^d - 1$. We know that $C^{2d}(n)$ is an odd number (we are assuming that n is following an alternating parity sequence), so we can employ the Odd Rule to get $C^{2d+1}(n)$:

$$C^{2d+1}(n) = 3(3^d\alpha_d + 3^d - 1) + 1 = 3^{d+1}\alpha_d + 3^{d+1} - 2.$$

Taking the above equation $\pmod 2$, we get that $C^{2d+1}(n) \equiv \alpha_d - 1 \pmod 2$. Since we have an alternating parity sequence, we know that $C^{2d+1} \equiv 0 \pmod 2 \Rightarrow \alpha_d \equiv 1 \pmod 2 \Rightarrow \alpha_d = 2\alpha_{d+1} + 1$. Then, we have the following:

$$C^{2d+1}(n) = 3^{d+1}(2\alpha_{d+1} + 1) + 3^{d+1} - 2 = 2 \cdot 3^{d+1}\alpha_{d+1} + 2 \cdot 3^{d+1} - 2.$$

We know that C^{2d+1} is an even number, so using the Even Rule and dividing by 2, we get

$$C^{2d+2} = 3^{d+1}\alpha_{d+1} + 3^{d+1} - 1,$$

which is the form we wanted. ■

4.7 Examining the Conjecture $\pmod 3$ and $\pmod 4$

We have already addressed $n \pmod 2$, namely that we have proved that all even numbers are satisfied under the conjecture through Strong Induction. We have yet to prove it for all odd numbers. This leads us to consider the problem in different mods, especially powers of 2 (from the Even Rule), and the powers of 3 (from the Odd Rule). We will consider them below.

Theorem 4.3. Consider the smallest number M that is not satisfied by the rules of the Collatz Conjecture. Then, we have $M \not\equiv 1 \pmod 4$, or, $M \equiv 3 \pmod 4$.

Proof. Consider a number congruent to 1 (mod 4), which we can write as $4e+1$. We know that it is an odd number, so using the Odd Rule, we get that $C^1(4e+1) = 3(4e+1)+1 = 12e+4$, which is even, so using the Even Rule, we have that $C^2(4e+1) = 6e+2$, which is also an even number. Hence, using the Even Rule again, we have that $C^3(4e+1) = 3e+1$. Since $C^3(4e+1) < 4e+1$, by our Inductive Hypothesis, we have that $4e+1\ \forall e \in \mathbb{Z}^+$ are satisfied by the Collatz Conjecture.

If we appply the same technique to $4e+3$, we don't get much success. In fact, we get the following Collatz reduction: $12e+10 \to 6e+5$. The parity of $6e+5$ is dependent upon the parity of e, which we do not know. ■

Corollary 4.1. If we can prove that all numbers of the form $n = 5+6r$ can be reduced to 1 by the rules of the Collatz function by using strong induction on $3+4r$, then we can prove the Collatz Conjecture.

Theorem 4.4. Say that M is the smallest number that is not satisfied by the Collatz Conjecture. Then, we have $M \equiv 0, 1 \pmod 3$, or, all $n \equiv 2 \pmod 3$ are satisfied by the Collatz Conjecture.

Proof. Since M is the smallest number that is not satisfied by the Collatz Conjecture, we can say that every element in the set $\{1, 2, 3, \ldots, M-2, M-1\}$ is satisfied by the Collatz Conjecture Before we consider $M \pmod 3$, we must consider its Collatz reduction. Namely, we can say that any number that M reduces through the rules of the function C cannot be reduced to 1, nor can any number that can be reduced to M. That is, consider the following:

$$\ldots \phi_t \to \phi_{t-1} \to \ldots \to \phi_2 \to \phi_1 \to M \to \psi_1 \to \psi_2 \to \ldots \to \psi_{y-1} \to \psi_y \ldots,$$

where an arrow represents a Collatz reduction. Since M does not work, we can say that all ϕ_i, ψ_j also do not work. Additionally, if any of ϕ_i, ψ_j are able to be reduced, then M is also able to be reduced by the Collatz Conjecture. Now back to M.

Instead of considering $M \pmod 3$, we will consider $M \pmod 6$. Immediately, we know that $M \not\equiv 0, 2, 4 \pmod 6$. Now, let us consider $M \equiv 5 \pmod 6$. Then, we can write $M = 5+6u, u \in \mathbb{Z}$. We will concentrate on computing the ϕ_i for M. To calculate ϕ_1, we can either apply the inverse of the Odd Rule (which would just be subtracting 1 and dividing by 3, or apply the inverse of the Even Rule (which is multiplying by 2). If we apply the Inverse of the Odd Rule, we do not get an integer ($\frac{M-1}{3} = \frac{4+6u}{3} \notin \mathbb{Z}$), so we must apply the inverse of the Even Rule, to get $\phi_1 = 10+12u$. Applying the Inverse of the Odd Rule to ϕ_1, we get $\phi_2 = 3+4u < M$, which is an odd number, and, under the fact that all elements in $\{1, 2, 3, \ldots, M-2, M-1\}$ are satisfied by the Collatz Conjecture, means that if $M \equiv 5 \pmod 6$, it is able to be reduced. ■

4.8 General Sequences

Consider a number N. Without loss of generality, say that N is an odd number. Then, we can say that the first step in its Collatz reduction is by applying the odd rule, where we get $3N+1$. And then, if $3N+1$ is even, then we divide it by 2^e, where e is the greatest number such that $2^e \mid 3N+1$. And this process continues for some period of time. Say that this number N follows a Collatz reduction of the following:

$$N : \{\mathsf{O}, \alpha_1, \mathsf{O}, \alpha_2, \mathsf{O}, \alpha_3, \mathsf{O}, \alpha_4, \ldots, \mathsf{O}, \alpha_{n-1}, \mathsf{O}, \alpha_n\},$$

where each "O" represents applying the Odd Rule, and each α_i represents dividing the previous number by 2^{α_i}. We also have that all $\alpha_i \in \mathbb{Z}^+$. Now, we wish to find a general form of the number that we get at the end of the application of this. We will take examples and try to find a pattern. Say that the number that we get at the end is N_i, where i represents how many αs there are. Consider $N : \{\mathsf{O}, \alpha_1\}$. we get the following:

$$N_1 = \frac{3N+1}{2^{\alpha_1}}.$$

Now, consider $N : \{\mathsf{O}, \alpha_1, \mathsf{O}, \alpha_2\}$:

$$\begin{aligned} N_2 &= \frac{1}{2^{\alpha_2}}\left[3\left(\frac{3N+1}{2^{\alpha_1}}\right)+1\right] \\ \implies N_2 &= \frac{1}{2^{\alpha_2}}\left[\frac{3^2N}{2^{\alpha_1}}+\frac{3}{2^{\alpha_1}}+1\right] \\ \implies N_2 &= \frac{3^2N}{2^{\alpha_1+\alpha_2}}+\frac{3}{2^{\alpha_1+\alpha_2}}+\frac{1}{2^{\alpha_2}}. \end{aligned}$$

Now, let us consider $N : \{\mathsf{O}, \alpha_1, \mathsf{O}, \alpha_2, \mathsf{O}, \alpha_3\}$:

$$\begin{aligned} N_3 &= \frac{1}{2^{\alpha_3}}\left[3\left(\frac{3^2N}{2^{\alpha_1+\alpha_2}}+\frac{3}{2^{\alpha_1+\alpha_2}}+\frac{1}{2^{\alpha_2}}\right)+1\right] \\ \implies N_3 &= \frac{1}{2^{\alpha_3}}\left(\frac{3^3N}{2^{\alpha_1+\alpha_2}}+\frac{3^2}{2^{\alpha_1+\alpha_2}}+\frac{3}{2^{\alpha_2}}+1\right) \\ \implies N_3 &= \frac{3^3N}{2^{\alpha_1+\alpha_2+\alpha_3}}+\frac{3^2}{2^{\alpha_1+\alpha_2+\alpha_3}}+\frac{3}{2^{\alpha_2+\alpha_3}}+\frac{1}{2^{\alpha_3}}. \end{aligned}$$

Now, to introduce a new notation. Say that we have $b > a$ such that

$$\beta(a,b) = \sum_{i=a}^{b} \alpha_i.$$

Before we preceed, there are some properties about $\beta(a,b)$ which are easily provable:

Property 4.1. $\beta(a,a) = \alpha_a$.

Property 4.2. $\beta(a,b) \geq b-a+1$.

Property 4.3. $\beta(a,b) = \beta(1,a) + \beta(a+1,b)$.

Now that we have the properties of $\beta(a,b)$, we can say the following:

$$N_n = \frac{3^n N}{2^{\beta(1,n)}} + \frac{3^{n-1}}{2^{\beta(1,n)}} + \frac{3^{n-2}}{2^{\beta(2,n)}} + \frac{3^{n-3}}{2^{\beta(3,n)}} + \cdots + \frac{3^2}{2^{\beta(n-2,n)}} + \frac{3^1}{2^{\beta(n-1,n)}} + \frac{1}{2^{\beta(n,n)}}$$
$$\implies N_n = \frac{3^n N}{2^{\beta(1,n)}} + \frac{1}{2^{\beta(1,n)}}[3^{n-1} + 3^{n-2}\cdot 2^{\beta(1,1)} + 3^{n-3}\cdot 2^{\beta(1,2)} + 3^{n-4}\cdot 2^{\beta(1,3)} + \cdots +$$
$$3^2 \cdot 2^{\beta(1,n-3)} + 3^1 \cdot 2^{\beta(1,n-2)} + 2^{\beta(1,n-1)}].$$

We can generalize the equation inside of the brackets into summation and we get the following:

$$N_n = \frac{1}{2^{\beta(1,n)}}\left[3^n N + 3^{n-1} + \sum_{i=1}^{n-1} 3^{n-1-i}\cdot 2^{\beta(1,i)}\right]. \tag{4.1}$$

We will prove Equation 4.1 below.

Theorem 4.5. Say that you have an odd number N which follows the following set of Collatz reductions: $N : \{\mathsf{O}, \alpha_1, \mathsf{O}, \alpha_2, \mathsf{O}, \alpha_3, \mathsf{O}, \alpha_4, \ldots, \mathsf{O}, \alpha_{n-1}, \mathsf{O}, \alpha_n\}$ where an O represents the number going through the Odd Rule and α_i represents the previous number being divided by 2^{α_i}. Say that N_n represents the number that comes out of this cycle. Then, we have the following:

$$N_n = \frac{1}{2^{\beta(1,n)}}\left[3^n N + 3^{n-1} + \sum_{i=1}^{n-1} 3^{n-1-i}\cdot 2^{\beta(1,i)}\right].$$

Proof. We can prove this by induction. Our Base Case is $n = 1$, and we already know that N_1 is $\frac{3N+1}{2^{\alpha_1}}$, so our Base Case is proved. Now, onto our Inductive Hypothesis: say that Equation 4.1 is true. Now, let us consider N_{n+1}.

$$N_{n+1} = \left(\frac{1}{2^{\alpha_{n+1}}}\right)\cdot(3N_n + 1)$$
$$\implies N_{n+1} = \left(\frac{1}{2^{\alpha_{n+1}}}\right)\cdot\left[3\left\{\frac{1}{2^{\beta(1,n)}}\cdot\left(3^n N + 3^{n-1} + \sum_{i=1}^{n-1} 3^{n-1-i}\cdot 2^{\beta(1,i)}\right)\right\} + 1\right]$$
$$\implies N_{n+1} = \left(\frac{1}{2^{\alpha_{n+1}}}\right)\cdot\left[\left\{\frac{1}{2^{\beta(1,n)}}\cdot\left(3^{n+1} N + 3^n + \sum_{i=1}^{n-1} 3^{n-i}\cdot 2^{\beta(1,i)}\right)\right\} + 1\right]$$
$$\implies N_{n+1} = \left(\frac{1}{2^{\alpha_{n+1}}}\right)\cdot\left(\frac{1}{2^{\beta(1,n)}}\right)\cdot\left[3^{n+1} N + 3^n + 2^{\beta(1,n)} + \sum_{i=1}^{n-1} 3^{n-i}\cdot 2^{\beta(1,i)}\right]$$
$$\implies N_{n+1} = \left(\frac{1}{2^{\beta(1,n+1)}}\right)\left[3^{n+1} N + 3^n + \sum_{i=1}^{n} 3^{n-i}\cdot 2^{\beta(1,i)}\right],$$

which is the form we wanted. Hence, proved. ∎

4.9 Cases Where the Collatz Conjecture Fails

There are exactly two cases in which the Collatz Conjecture fails. The first would be if an element "loops" back to an element previously on its Collatz Reduction. (We will more formally define this in the section below.) The second case is if the reduction simply goes onto infinity, or it diverges to infinity.

4.9.1 Looping

Let us begin to more formally define looping. A *Collatz reduction* is the process in which a number is getting reduced through the rules of the function C. Hence, the Collatz reduction of 5 is $16 \to 8 \to 4 \to 2 \to 1$. Now, consider a number q, and say that its Collatz Reduction is the following:

$$\gamma_1 \to \gamma_2 \to \gamma_3 \to \gamma_4 \to \ldots \to \gamma_{w-2} \to \gamma_{w-1} \to \gamma_w,$$

where γ_w is an arbitrary stopping point. If an element of the Collatz reduction *loops* back to another, then $\exists\ 1 \leq i, j \leq w$ such that $\gamma_i = \gamma_j$.

Lemma 4.1. Looping does not exist for $n = 1$.

Proof. It is sufficient to prove that there does not exist a positive integer N such that $N_1 = N$. Assume for the sake of contradiction that there does exist such an N. Then, we have the following:

$$\begin{aligned} N &= \frac{3N+1}{2^{\alpha_1}} \\ \implies 2^{\alpha_1} N &= 3N + 1 \\ \implies (2^{\alpha_1} - 3)N &= 1. \end{aligned}$$

We know that $\alpha_1 > 0$. If $\alpha_1 = 1$, then $2^{\alpha_1} - 3 = -1 \Rightarrow N < 0$, which is not possible. If $\alpha_1 = 2$, then N = 1 (which is just the trivial loop 1-4-2-1). If $\alpha_1 > 2$, then N is not an integer. Hence, proved. ■

Lemma 4.2. For $\alpha_i = 1$, or a number N that follows an *e-o-e-o-* ... sequence, looping does not exist.

Proof. By Theorem 4.2, we have that the $2d$th iteration is of the form $C^{2d}(N) = 3^d \alpha_d + 3^d - 1$. There are two cases to consider:

1. if an even iteration is equal to an even iteration,
2. if an even iteration is equal to an odd iteration.

We do not have to consider the case where an odd iteration is equal to an odd iteration because you can just divide each iteration by 2, and we get Case 1. First, let us consider Case 1. Let us consider two numbers $p \neq q$ such that $C^{2p}(N) = C^{2q}(N)$. Without loss of generality, say that $p > q \Rightarrow \alpha_p > \alpha_q \Rightarrow \alpha_p = \alpha_q + c$,

where $c > 0$. Then, we can say the following:

$$\begin{aligned}
& C^{2p}(N) = C^{2q}(N) \\
\implies & 3^p\alpha_p + 3^p - 1 = 3^q\alpha_q + 3^q - 1 \\
\implies & 3^p\alpha_p + 3^p = 3^q\alpha_q + 3^q \\
\implies & 3^p\alpha_p - 3^q\alpha_q = 3^q - 3^p \\
\implies & 3^p(\alpha_q + c) - 3^q\alpha_q = 3^q - 3^p \\
\implies & 3^p\alpha_q + 3^p c - 3^q\alpha_q = 3^q - 3^p \\
\implies & 3^p c + \alpha_q(3^p - 3^q) = 3^q - 3^p \\
\implies & 3^p c = (3^q - 3^p)(1 + \alpha_q) \\
\implies & c = (3^{q-p} - 1)(1 + \alpha_q).
\end{aligned}$$

We know that $p > q \Rightarrow 3^p > 3^q \Rightarrow 1 > 3^{q-p} \Rightarrow 3^{q-p} - 1 < 0 \Rightarrow c < 0$, which is a contradiction because we have previously said that $c > 0$. Now, we must consider Case 2, where an even iteration is equal to an odd iteration. However, we must remember parity. In Theorem 4.2, we have have proven that an odd iteration is even, and every even iteration is odd. Since an odd number cannot be equal to an even number, Case 2 is proven. Hence, we can say that looping is not allowed for *e-o-e-o-* ... sequences. ■

Theorem 4.6. Except for the trivial loop, looping does not exist.

Proof. It is sufficient to prove that there does not exist a positive integer such that $N_n = N$. Assume for the sake of contradiction that there does exist such an n and N. Using Theorem 4.5, we have the following:

$$N = \frac{1}{2^{\beta(1,n)}}\left[3^n N + 3^{n-1} + \sum_{i=1}^{n-1} 3^{n-1-i} \cdot 2^{\beta(1,i)}\right] \tag{4.2}$$

$$\implies 2^{\beta(1,n)}N = 3^n N + 3^{n-1} + \sum_{i=1}^{n-1} 3^{n-1-i} \cdot 2^{\beta(1,i)} \tag{4.3}$$

$$\implies N(2^{\beta(1,n)} - 3^n) = 3^{n-1} + \sum_{i=1}^{n-1} 3^{n-1-i} \cdot 2^{\beta(1,i)} \tag{4.4}$$

$$\implies N(2^{\beta(1,n)} - 3^n) = 3^{n-1} + 3^{n-2} \cdot 2^{\beta(1,1)} + 3^{n-3} \cdot 2^{\beta(1,2)} + \cdots + 3^1 \cdot 2^{\beta(1,n-2)} + 2^{\beta(n-1)}. \tag{4.5}$$

We take $\mod 4$ of each side of the equation. If $\beta(1,1) = \alpha_1 = 1$, we cannot have looping (we will prove this down below). So, we can assume that $\beta(1,1) > 1$. We also know that all $\beta(1,i) \geq 2$. Taking the equation

mod 4, we get the following:

$$\begin{aligned} & N(-(-1)^n) \equiv (-1)^{n-1} \pmod 4 \\ \implies & N \cdot (-1)^{n-1} \equiv (-1)^{n-1} \pmod 4 \\ \implies & N \equiv 1 \pmod 4. \end{aligned}$$

However, this is a contradiction. We have by Theorem 4.3 that every number congruent to 1 (mod 4) is able to be reduced to 1, which means that looping does not exist. However, by our assumption by contradiction, the number N is not able to be reduced and its Collatz reduction is infinite. However, since $N \equiv 1 \pmod 4$, the element is able to be reduced. Hence, proved. (It must be noted that if $N = 1$, we get the trivial loop 1-4-2-1.) ■

Before we proceed with our proof that if $\beta(1,1) = 1$, then looping does not exist, there are some observations we must make about Equation 4.1, or, more specifically, from Equation 4.5, which is the following:

$$N(2^{\beta(1,n)} - 3^n) = 3^{n-1} + 3^{n-2} \cdot 2^{\beta(1,1)} + 3^{n-3} \cdot 2^{\beta(1,2)} + \cdots + 3^1 \cdot 2^{\beta(1,n-2)} + 2^{\beta(n-1)}.$$

We take (mod 3) of each side of the equation, and we get the following:

$$\begin{aligned} & N \cdot 2^{\beta(1,n)} \equiv 2^{\beta(1,n-1)} \\ \implies & N \cdot 2^{\alpha_n} \equiv 1 \pmod 3. \end{aligned}$$

Now, let us examine $N \pmod 3$. If $N \equiv 0 \pmod 3$, then we get a contradiction, since we will have that $N \cdot 2^{\alpha_n} \equiv 0 \not\equiv 1 \pmod 3$. Now, let us examine the case where $N \equiv 2 \pmod 3$. By Theorem 4.4, we know that all $N \equiv 2 \pmod 3$ are able to be reduced, so looping is not allowed. Hence, the only case that we must consider is if $N \equiv 1 \pmod 3 \Rightarrow \frac{3N+1}{2} \equiv 2 \pmod 3$. Now, we can proceed.

Lemma 4.3. If we have $\beta(1,1) = 1$, then looping does not exist.

Proof. If we have $\alpha_1 = 1$, then we can take the sequence from α_2. If α_2 is also equal to 1, then we can consider the sequence from α_3, and so on. If we have all $\alpha_i = 1$, then we will have an *o-e-o-e-...* sequence, which we have already proved in Lemma 4.2. ■

4.10 2-adic Representations

In this section we use the reduced Collatz map i.e.

$$T(n) = \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \pmod 2 \\ \frac{3n+1}{2} & \text{if } n \equiv 1 \pmod 2 \end{cases}.$$

Define an s-parity sequence

$$V_s = (n, T(n), T^2(n), \ldots, T^{s-1}(n)) \mod 2$$

(each value is either 1 or 0 depending on the parity of $T^k(n)$) and a (general) parity sequence as

$$V_\infty = (n, T(n), T^2(n), \ldots) \mod 2$$

.

Claim 4.1. Let S_s represent all binary sequences of length s. We claim there is a natural bijection between S_s and $\mathbb{Z}/2^s\mathbb{Z}$ using the collatz map.

Every integer maps to some sequence $V_s(n)$ by its Collatz transform, thus the natural mapping is injective. Let s_k denote the kth digit of S. Consider the function $\sigma_k(S)$ is the partial sum of a sequence S, specifically $\sigma_k(s) = s_0 + s_1 + \ldots s_k$. Then the inverse function of the Collatz map is given by

$$n \equiv -\sum_{k=0}^{s-1} s_k 2^k 3^{-\sigma_k(S)} \mod 2^s$$

Proof is by induction but not given here. Thus this mapping is surjective. Since it is both injective and surjective it is by definition bijective.

We extend this argument to the 2-adic integers, $\mathbb{Z}_2$, and we show a similar bijection between $\mathbb{Z}_2$ and S_∞ under the Collatz map.
In a similar way $n \in \mathbb{Z}_2$ maps to V_∞.
Our new inverse function becomes

$$n = -\sum_{k=0}^{s-1} s_k 2^k 3^{-\sigma_k(S)}$$

which is a corollary of the old inverse function. Thus the reduced collatz map of parity sequences is a bijection between $\mathbb{Z}_2$ and S_∞.

Let $A = 2^N$ denote the set of infinite binary sequences. As a natural notation on our bijection let $Q : A \to \mathbb{Z}_2$ be defined as a mapping to the Hensel representation of p-a positive integers i.e. $Q(S) = \sum_{k\geq 0} s_k 2^k$.

Then if we take $Q(V(n))$ from each Collatz map we have a mapping from $\mathbb{Z}_2 \to \mathbb{Z}_2$

Restating Collatz Conjecture

Note the loop for 1 is $(1, 2, 1, 2 \ldots)$ so the parity sequence of 1, $V(1) = (1, 0, 1, 0 \ldots)$. Then $Q(V(1)) = \frac{1}{3}$. Also note if the Collatz map of n terminates in 1, its parity sequence terminates in $V(1)$ so $Q(n) = \frac{r}{3}$ for

$r \in \mathbb{Z}^+$ and gcd(r, 3) = 1. Thus if we want to prove the Collatz conjecture, we need to show that for $n \in \mathbb{Z}$ we have $Q(n) \in \frac{1}{3}\mathbb{Z}^+$ (it is easily shown that integers cannot converge into integers as that would mean it terminates in $(0, 0, \ldots 0)$ which means every power of 2 divides it so it would be unbounded, which is impossible).

Looping versus Divergence

We consider each $2-adic$ representation to be equal to a real number according to the natural mapping. Then

Lemma 4.4. S is repeating iff $Q(S)$ is rational.

Proof. Let $Q(S) = \frac{p}{q}$ for positive integers, p, q (note if $Q(S) < 0$ then we consider $-Q(S)$ which is just flipping all the digits and adding one, so it repeats with $Q(S)$). Then recall that since p,q are positive integers, they have finitely many terms in their 2-adic representation. So we have $qQ(S) = p$ but note that $qQ(S)$ is just a finite sum of digits shifts of $Q(S)$ when written in binary, but since these must eventually sum to 0s this represents a repitition.

For the other direction we use geometric series expansion. It is not shown in full here but rather is left to the reader.

Claim 4.2. For positive integers n, if $Q(V(n)) \in \mathbb{Q} \subset \mathbb{Z}_2$ the Collatz convergence of n will loop eventually (possibly going to 1). Else if $Q(V(n)) \in \mathbb{R}/\mathbb{Q} \subset \mathbb{Z}_2$ then the Collatz convergence will diverge.

Proof. Recall by the Pigeonhole principle the Collatz sequence for n either loops or diverges. We show first for a rational $Q(V(n))$ the sequence loops. Note if $Q(V(n))$ is rational then $V(n)$ must be eventually repeating by Lemma 4.4. Consider the first digit d s.t. after d it strictly repeats. Let the length of our repeating sequence be r. Note $V(T^d(n)) = V(T^{d+r}(n))$. Thus since we showed there was a bijection between S and $\mathbb{Z}_{\not 2}$ we have $T^{d+r}(n) = T^d(n)$ and thus it loops.
Now if $Q(V(n))$ is irrational, by the other direction in Lemma 4.4 $V(n)$ is not repeating. Assume for the sake of contradiction $T^{d+r}(n) = T^d(n) \implies V(T^{d+r}(n)) = V(T^d(n))$ which implies $V(T^d(n))$ repeats so $V(n)$ is eventually repeating which is a contradiction. □

Corollary 4.2. Any repeated cycle of even odd trith total coefficient greater than 1 cannot be the Collatz sequence of a positive integer. Since the total coefficient is greater than 1, and the constant term is strictly positive, it must strictly increase and thus cannot loop. However, since it is a repeated cycle of transformations, $V(n)$ is repeated and thus by Claim 4.2 n loops but doesn't diverge, but we have already shown looping does not work in these circumstances so we are done.

A popular conjecture says that for integer n we have $Q(V(n)) \in \mathbb{Z}$ (this is equivalent to disproving divergence). One possible approac to proving this could be to experiment with plugging in nonrepeating sequences to the inverse formula previously mentioned and seeing if it is possible to restrict to rationals.

4.11 Different Modulos

Suppose n is a natural number, and suppose that the progression for n-1 eventually reaches 1. Using induction, I aim to show that n will also reach 1.

Now, we know that, any element before n must follow the sequence and reach 1. So we're effectively trying to show that the sequence for n reaches a number smaller than it.

Odd Numbers

Now, lets take a look at the cases for n being an odd number.

An odd number n of the form 2k+1 will follow the pattern of : 2k+1, 6k+4, 3k+2, and either k is even, and it eventually reaches one, or its odd, and it might not reach 1. So 50% of the cases here reach 1.

Modulo 4

Now we look at the the congruence cases using mod 4. Even numbers, i.e. $0 mod(4)$ and $2 mod(4)$, have been taken care of already based on what we discussed previously.

Looking at the case of $1 mod(4)$, we get the pattern:

$4k-3$, $12k-8$, $6k-4$, and $3k-2$. This last result is especially important, because it is less than the value of the number we started with. Based on the initial assumption, this case also reaches 1.

However, the case of $3 mod(4)$ might not reach 1. $4k-1$, $12k-2$,$6k-1$. So $4k-1$ is just like $1 mod(2)$. So 75% of the cases here are guaranteed to reach 1.

Modulo 6

Now we move to the congruence cases using mod 6. Again, we can simply skip the cases of $nmod(6)$, where n is even, because these cases were covered by $0mod(2)$. The only case that works is $1mod(6)$. This can be seen by considering the sequence pattern for $1mod(8)$ (which has already been proves to reach 1 through $4k+1$):

$8k+1$, $24k+4$, $12k+2$, $6k+1$.

The first term of the pattern for the case of $1mod(6)$, is the third term of the pattern for the cases for $1mod(8)$, which we've shown must reach 1. So, sequences for members of $1mod(6)$ reach 1 by assumption.

Now, to calculate the percentage of cases for modulo 6 that reach 1, we can see begin with the fact that $1mod(6)$ and $1mod(8)$ overlap. So, we look at the cases for $mod(12)$, the LCM of 2, 4, and 6.

The successful cases:
$0mod(2)$: $0mod(12)$, $2mod(12)$, $4mod(12)$, $6mod(12)$, $8mod(12)$, and $10mod(12)$

$1mod(4)$: $1mod(12)$, $5mod(12)$, and $9mod(12)$

$1mod(6)$:to $1mod(12)$ and $7mod(12)$

So there are two cases that are not covered here:
$5mod(12)$ and $9mod(12)$. So 83% of the cases reach 1.

Now, the aim is to continue this process using an algorithm.

For the proof to be complete, the requisite number of congruence cases will need to exist, such that the case modulo the least common denominator of the modulo reaches 1.

Computation

The even numbers have been taken care of, based on 0 (mod 2). (mod 4) is the only odd case that reaches 1. Now, the aim is to find as many cases r (mod m) with m is even, and greater than 6, r is odd, and $1 \leq r \leq m$, where the $3n+1$ case has a member of a preceding case. Basically, we want to find cases $n = bk - c$ that have a member of a case that is less than n. We'll start with $m = 6$ and look at the sequence $6k+1$. Essentially, we proceed until the factor becomes odd. Check if the result is less than the initial

case. If it is not, we can look at all previous sequences, like $4k-3$, and search for members of the $6k+1$ pattern. If a pattern reaches 1, then the corresponding congruence cases are restated modulo the LCM of all the previous cases. The percentage of the congruence cases that reach 1 represent the percent of total cases that will eventually reach 1. This process is repeated with m for every even number. For each m and r, the pattern for $mk-r$ is checked as far as possible to see if a member of the pattern is less than the initial term.

Unfortunately, this method appears to lead us to an infinitely long "tree" of possibilities. For example, for all $n = 2k$, the cases reach 1. Now for $n = 2k+1$, if $k = 2m$, then the cases also reach 1, but if $k = 2m+1$, they might now reach 1, and so on. So while the percentage of cases that reach 1 tends to 100, it technically won't reach it.

4.12 Infinite Sequences formed by Finite Parity Cycles

In this exploration, we will disprove the existence of infinite sequences which have finite parity cycles. This means that

- Looping does not exist in general;
- Divergence in which a parity cycle repeats does not exist.

Therefore, the only way that a certain number does not satisfy the Collatz Conjecture is when it diverges. If we write down the parity of each of the numbers resulting from applying the Collatz Conjecture function, the parity cannot repeat. In other words, we must have an infinitely long parity cycle that does not repeat.

4.13 One Odd and k Evens Collatz Cycle

We start with a simpler example as a prologue to the much more general proof. Here, we consider the cases in which the parities of the numbers resulting from applying the Collatz Conjecture function occur in the fashion

$$odd, k\ evens, \ldots,$$

where the parity cycle repeats after the ... Here, we first some up with a general form for this kind of sequence. Then, we use this general form to prove that such cycles cannot exist. In hindsight, this prologue will prove that cycles with recurring parity of this form cannot exist in some specific cases. This will also prove that divergence cannot exist with parity cycles of this form. We will later extend this argument to all sequences with repeating parity cycles.

We start by defining an important variable that we will be using in this proof. We define k to be the number of even numbers in the Collatz Cycle after which we get another odd number. Then, we can define

the function that returns the next odd number in this cycle as $\frac{3m+1}{2^k}$, where m is the previous odd number in the sequence/cycle.

4.13.1 Claim

We claim that when we apply this function a times, we will get the odd number

$$\frac{3^a m + 3^{a-1} + 3^{a-2}2^k + 3^{a-3}2^{2k} + \cdots + 3^{a-q}2^{(q-1)k} + \cdots + 2^{(a-1)k}}{2^{ak}}.$$

4.13.2 Proof by Induction

Base Case When we apply the function to m itself, we get $\frac{3m+1}{2^k}$ by the rule of the function. Additionally, when $a = 1$ in the claimed term above, we get

$$\frac{3^1 m + 3^0 2^0}{2^{1\cdot k}} = \frac{3m+1}{2^k}.$$

Inductive Hypothesis Assume that a certain a satisfies the above claim.

Inductive Step We wish to show that the statement holds true for $a+1$ because it holds for a. Let the function $f(m) = \frac{3m+1}{2^k}$. Then we know by the inductive hypothesis that $f^a(m)$ is the claimed expression. Then, we wish to show that $f^{a+1}(m) = f(f^a(m))$ is the claimed expression as well. When we take the function of $f^a(m)$, we get

$$\frac{3\left(\frac{3^a m+3^{a-1}+3^{a-2}2^k+3^{a-3}2^{2k}+\cdots+3^{a-q}2^{(q-1)k}+\cdots+2^{(a-1)k}}{2^{ak}}\right)+1}{2^k}.$$

$$= \frac{3^{a+1}m + 3^a + 3^{a-1}2^k + 3^{a-2}2^{2k} + \cdots + 3^1 2^{(a-1)k} + 2^{(a)k}}{2^{(a+1)k}},$$

completing the proof. $\square$

4.13.3 Shortened Formula

This claimed formula is a bit long, so we collapse it using the sum of a geometric series. The constant sum in the numerator becomes

$$\frac{\frac{2^{ak}}{3} - 3^{a-1}}{\frac{2^k}{3} - 1} = \frac{2^{ak} - 3^a}{2^k - 3}.$$

Therefore, the term $f^a(m)$ becomes

$$\frac{3^a m + \frac{2^{ak}-3^a}{2^k-3}}{2^{ak}} = \boxed{\left(\frac{3}{2^k}\right)^a \cdot \left(m - \frac{1}{2^k-3}\right) + \frac{1}{2^k-3}}.$$

4.14 $Odd, Even, Odd, \ldots$ Loops and Divergence: Collatz Cycle where $k = 1$

In this section, we consider sequences of infinite length with the pattern of outputs $odd, even, odd, even, odd, \ldots$ We will use modular arithmetic to prove that an infinite sequence with such a pattern cannot exist. **This means that there cannot be a sequence in the form** $odd, even, odd, even, odd, \ldots$ **which diverges or loops.** Because we only have one even number between each of the odd numbers in the sequence, we have that $k = 1$. Then, our formula for the odd numbers in this sequence after a repeated $odd, even$ cycles is given by the formula found in the last section when we set $k = 1$. The formula becomes

$$\left(\frac{3}{2^1}\right)^a \cdot \left(m - \frac{1}{2^1 - 3}\right) + \frac{1}{2^1 - 3} = \left(\frac{3}{2}\right)^a \cdot \left(m - \frac{1}{2 - 3}\right) + \frac{1}{2 - 3} = \left(\frac{3}{2}\right)^a \cdot (m + 1) - 1.$$

As a reminder, this expression on the far right is a representation of the odd number achieved after a repeated $odd, even$ cycles. We can apply this function (where we perform the rule to get to the next odd number in the sequence) as many times as we want because the sequence is said to be infinite, (either caused by divergence or a loop) an assumption that we are trying to disprove. So, $a \in [0, \infty)$, where we simply get m when $a = 0$, or when we do not apply the function at all. We also have that this expression must be odd, which means that

$$\left(\frac{3}{2}\right)^a \cdot (m + 1) - 1 \equiv 1 \pmod 2.$$

Adding 1 to both sides, we get

$$\left(\frac{3}{2}\right)^a \cdot (m + 1) \equiv 2 \equiv 0 \pmod 2.$$

In order for the left hand side to be an integer, we must have that the denominator of the fraction, or 2^a divides $m + 1$. Furthermore, in order for the left side to be an integer, $m + 1$ must divide another 2, or 2^{a+1} must divide $m + 1$. However, since a can be anything, we have that 2^{a+1} approaches ∞ as a approaches ∞. Therefore, in order for this statement to be true, we must have that $m + 1$ is ∞. Therefore, $m + 1$ cannot exist. It quickly follows that m**, the starting number in this infinite sequence, cannot exist either.**

4.15 $Odd, Even, Odd, Even, Even, Odd \ldots$ Loops and Divergence: Collatz Cycle where $p = 1$ $q = 2$

Similar to the formula we proved near the beginning, there is another formula to represent all of the odd numbers outputted by a cycle of odd, p $evens, odd$,q $evens, \ldots$, after which we get another odd and the parity cycle repeats. The formula is

$$\left(\frac{3^2}{2^{p+q}}\right)^a m + \left(\frac{2^p}{2^{p+q}} + \frac{3}{2^{p+q}}\right) \cdot \left(\frac{2^{(p+q)a} - 3^{2a}}{(2^{p+q} - 3^2) \cdot 2^{(p+q)(a-1)}}\right).$$

We will be using this representation to prove that the sequence

$$odd, even, odd, even, even, odd, \ldots$$

cannot continue in an infinite sequence. This will prove that both looping and divergence cannot exist with a pattern of outputs of the form

$$odd, even, odd, even, even, odd, \ldots$$

Note that when we take this sequence, we get $p = 1$ and $q = 2$. Substituting these into the representation, we get

$$\left(\frac{3^2}{2^{1+2}}\right)^a m + \left(\frac{2^1}{2^{1+2}} + \frac{3}{2^{1+2}}\right) \cdot \left(\frac{2^{(1+2)a} - 3^{2a}}{(2^{1+2} - 3^2) \cdot 2^{(1+2)(a-1)}}\right).$$

This is the same as

$$\begin{aligned}
&\left(\frac{9}{8}\right)^a m + \left(\frac{2}{8} + \frac{3}{8}\right) \cdot \left(\frac{8^a - 9^a}{(8-9) \cdot 8^{a-1}}\right) \\
&= \left(\frac{9}{8}\right)^a m - \left(\frac{5}{8}\right) \cdot \left(\frac{8^a - 9^a}{8^{a-1}}\right) \\
&= \left(\frac{9}{8}\right)^a m - \left(\frac{5 \cdot (8^a - 9^a)}{8^a}\right) \\
&= \left(\frac{9}{8}\right)^a (m+5) - 5.
\end{aligned}$$

This last expression is also a representation of one of the odd numbers outputted from the

$$odd, even, odd, even, even, odd, \ldots$$

sequence. Therefore, it must also be odd, so we must have

$$\left(\frac{9}{8}\right)^a (m+5) - 5 \equiv 1 \pmod 2$$

or

$$\left(\frac{9}{8}\right)^a (m+5) \equiv 6 \equiv 0 \pmod 2.$$

From this, we find that 8^a must divide $m + 5$ in order for the left hand side to be an integer. Furthermore, we must also have that $2 \cdot 8^a = 2^{3a+1}$ divides $m + 5$ in order for the congruence statement to be satisfied and for the left hand side to be even. Remember that $a \in [0, \infty)$, so we must have that 2^{3a+1} divides $m + 5$ for any non-negative a. Therefore, we see that $m + 5$ must be (or approach) ∞, meaning that $m + 5$ cannot exist. Because of this, neither can m.

Therefore, we cannot have divergence or looping with a sequence that is in the form

$$odd, even, odd, even, even, odd, \ldots$$

4.16 Infinite Sequences with Finite Parity Cycles

Now, we move onto the general case in which we prove that infinite sequences formed by finite parity cycles cannot exist. As said before, this will disprove looping and divergence with sequences that have finite parity cycles.

4.16.1 Proof

Consider an odd number m. If we perform the Collatz Conjecture function upon m multiple times, consider the parity of each of the outputs after each application of the Collatz Conjecture function. Say that we end up repeating the parity sequence infinitely. This will happen if and only if m ends up being in a loop or diverges and does not reach 1. Note that we stop this procedure of applying the Collatz Conjecture function once we reach 1, as this means that the number satisfies the conjecture.

Take one iteration of this parity cycle. The one iteration cycle could be (in the parentheses)

$$(odd, even), odd, even, \ldots$$

It could also be

$$(odd, even, odd, even, even), odd, even, odd, even, even \ldots$$

At the end of each of these sequences, we must return to another odd number. Every time *odd* shows up, we must multiply our number by 3 and add 1. Every time an *even* shows up, we must divide our number by 2. A general parity cycle of one iteration would look like

$$odd, p_1 \ evens, odd, p_2 \ evens, odd, p_3 \ evens, odd, p_4 \ evens, \ldots, odd, p_b \ evens.$$

In the case of p_i *evens*, we must divide by 2 exactly p_i times. After this (when *odd* shows up), we must multiply our number by 3 and add 1. If m is the odd number at the beginning of our sequence, after one iteration of this parity cycle, we will get the odd number

$$\frac{3\left(\frac{3\left(\frac{3\left(\frac{(3m+1)}{2^{p_1}}\right)+1}{2^{p_2}}\right)+1}{2^{p_3}}\right)+1}{\frac{\ldots}{2^{p_b}}}.$$

$$= \frac{3^b m + 3^{b-1} + 3^{b-2}2^{p_1} + 3^{b-3}2^{p_1+p_2} + \ldots + 2^{p_1+p_2+p_3+\ldots+p_{b-1}}}{2^{p_1+p_2+p_3+p_4+\ldots+p_b}}.$$

We see that this expression is of the form

$$\frac{rm+q}{2^s},$$

where $r = 3^b$ and $q \equiv 1 \pmod 2$. We are trying to prove that such an infinite sequence (made by some finite parity cycle) cannot exist. Since this parity cycle goes on forever, if we let

$$f(m) = \frac{rm+q}{2^s},$$

then $f^a(m)$ represents the odd number resulting after a iterations of the parity cycle. We have that

$$f^a(m) = \frac{r\left(\frac{r\left(\frac{r\left(\frac{(rm+q)}{2^s}\right)+q}{2^s}\right)+q}{2^s}\right)+q}{\frac{\ldots}{2^s}}$$

$$= \frac{r^a m + qr^{a-1} + qr^{a-2}2^s + qr^{a-3}2^{2s} + \ldots + q2^{(a-1)s}}{2^{as}}.$$

Using the sum of a geometric sequence, we can shorten the form of the constant term in the numerator. Our term then becomes

$$\frac{r^a m + q\left(\frac{2^{as}-r^a}{2^s-r}\right)}{2^{as}}$$

$$= \left(\frac{r}{2^s}\right)^a \left(m - \frac{q}{2^s-r}\right) + \frac{q}{2^s-r}.$$

Remember, this is the odd number given after a parity cycles. So, it must be congruent to 1 with respect to modulus 2. So, we have

$$\left(\frac{r}{2^s}\right)^a \left(m - \frac{q}{2^s-r}\right) + \frac{q}{2^s-r} \equiv 1 \pmod 2.$$

Multiplying this entire congruence statement by the odd number $2^s - r$, we get

$$\left(\frac{r}{2^s}\right)^a (m(2^s-r) - q) + q \equiv 1 \pmod 2.$$

The number q is odd by definition, so when we subtract q on both sides, we get

$$\left(\frac{r}{2^s}\right)^a (m(2^s-r) - q) \equiv 0 \pmod 2.$$

We see that if we set $m = 1, s = 2, r = 3, q = 1$, we get the trivial loop $1, 2, 4, \ldots$ This makes $m(2^s-r)-q = 0$, causing this statement to be true. This cannot hold true for the cases in which $\frac{r}{2^s} > 1$ because we would have that $r > 2^s$, which would make m negative in $m(2^s-r)-q = 0$, a contradiction. If $\frac{r}{2^s} < 1$, or the coefficient of m is less than 1, it is possible for looping to occur if and only if m, s, r, q satisfy $m(2^s-r) - q = 0$, or $m = \frac{q}{2^s-r}$. Note that if we simply have $m(2^s-r) - q \equiv 0 \pmod 2$, then the following argument disproves the existence of a loop in this scenario. If we can find such numbers m, s, r, q that satisfy $m(2^s-r) - q = 0$ (without leading to the trivial loop), we will have found a loop in the Collatz Conjecture.

In all other cases, we must have $2^{as} \mid m(2^s-r) - q$ in order for the congruence statement to be satisfied. We also have that $a \in [0, \infty)$, so we know that $m(2^s-r) - q$ cannot possibly exist as it tends to ∞ if it is able to be divided by 2^{as}, so we conclude that m cannot exist either (as s, r, q are constants and cannot be infinite since the parity cycle is finite).

4.16.2 Conclusion

Above, we disproved the existence of any infinite sequence with a repeating parity cycle unless $\frac{r}{2^s} < 1$ and $m(2^s - r) - q = 0$. This greatly reduces the area to search when searching for a loop in the Collatz Conjecture.

In summary, no infinite sequences formed by finite parity cycles including looping and divergence (caused by finite parity cycle) can occur in the Collatz Conjecture (except for the condition above), proving that every number must eventually reach 1 when the number undergoes enough iterations of the Collatz Conjecture function unless the number diverges and has a parity cycle that does not repeat.

In other words, the only exception to this argument occurs if and when a number diverges and forms one infinitely long parity cycle or $\frac{r}{2^s} < 1$ and $m(2^s - r) - q = 0$.