Diophantine Equations to the Power of n

MATC15 - Project - Final Submission

Andrew D'Amario, Kevin Santos, Dawson Brown

March 2021

Conjecture 1:

$$x^n = \sum_{i=1}^{n} y_i^n \text{ has an integer solution such that } y_i \neq x \wedge y_i > 0, \forall i.$$

Andrew D'Amario (A.D.), February 18, 2021

1 Introduction

The objective of this project is to investigate the conjecture above: whether or not we can always find at least one integer solution to equations of the form $x^n = y_1^n + \cdots + y_n^n$ given any x, excluding trivial solutions involving y_i's$= 0$ or x.
Some of this investigation and research will involve:

- Finding parameters and conditions for possible valid solutions
- Computational analysis on random integers raised to the power of n and finding an integer solution to the sum.
- Noting differences between even and odd n.
- Identifying different families of solutions that take on a similar form.

Though this conjecture may be false, we hope to investigate as much as we can on the matter, as well as summarize and provide some deeper research to the subject.

In MATC15, we work with certain linear Diophantine equations in two variables, equations of the form $ax + by = c$. In general, a Diophantine equation can be written in terms of any number of variables. The important thing about these equations is that we only care about the *integer* solutions to these equations. In this project, we're interested in the integer solutions of the following equation, with some fixed $n \in \mathbb{Z}$:

$$x^n = y_1^n + \cdots + y_n^n \tag{1}$$

We only want to find nontrivial solutions; an example of a trivial solution, given some x, would be $y_1 = x$ with zeroes for the rest: $y_i = 0$ for $i = 2, ..., n$. We also only want to keep *imprimitive* solutions, solutions where all of $(x, y_1, ..., y_n)$ are coprime; if they share a common divisor, they can be reduced into a lesser (possibly already known) imprimitive solution. Some work has previously been done with finding integer solutions to certain cases of the above equation.

1.1 $n = 3$

The problem of representing integers as a sum of three cubes has received a lot of attention. It is conjectured, but it hasn't been proven, that any integer not equivalent to 4 or 5 modulo 9 can be represented as a sum of three integer cubes, i.e. for any integer x where $x \not\equiv 4$ or $x \not\equiv 5 \mod 9$:

$$\exists a, b, c \in \mathbb{Z} \text{ s.t. } x = a^3 + b^3 + c^3 \tag{2}$$

The condition on $x \mod 9$ arises from considering the possible values of cubes modulo 9. We can find the value of any cube modulo 9 by looking at all the cubes of a reduced residue system mod 9, such as $\{0, 1, 2, 3, 4, -4, -3, -2, -1\}$:

$$\begin{aligned}
0^3 &\equiv 0 \mod 9 \\
1^3 &\equiv 1 \mod 9 \\
2^3 = 8 &\equiv -1 \mod 9 \\
3^3 = 27 &\equiv 0 \mod 9 \\
4^3 = 64 &\equiv 1 \mod 9 \\
(-4)^3 = -64 &\equiv -1 \mod 9 \\
(-3)^3 = -27 &\equiv 0 \mod 9 \\
(-2)^3 = -8 &\equiv 1 \mod 9 \\
(-1)^3 &\equiv -1 \mod 9
\end{aligned}$$

Mordell [4] summarized work on the particular case where the sum of three cubes equals another cube, which is case $n = 3$ of our equation (1):

$$x_1^3 + x_2^3 + x_3^3 = y^3 \tag{3}$$

An infinite family of solutions can be found for any given cube a^3, as found by Mahler, qtd. in Mordell [4]. For any integer t, the following is a solution to (3):

$$x_1 = 9at^4, \quad x_2 = 3at - 9at^4, \quad x_3 - a - 9at^3, \quad y = a^3$$

1.2 $n = 4$

When $n = 4$, our equation (1) can be rewritten as

$$a^4 + b^4 + c^4 + d^4 = e^4 \tag{4}$$

Leech [3] summarizes known solutions to (3), up to $e = 4267$. The smallest known solution, found by Norrie in 1911 [3], is $a = 30$, $b = 120$, $c = 272$, $d = 315$, and $e = 353$. Leech also examines properties of fourth powers under the modulo classes of 16 and 5. These observations, explained below, allow one to greatly reduce the number of possible solutions that need to be checked by brute force.

For any integer x, it can be shown that when x is even, $x^4 \equiv 0$, and when x is odd, $x^4 \equiv 1 \mod 16$ (see Appendix 1).

Therefore, on the right side of our equation, $e^4 \equiv 0$ or $e^4 \equiv 1 \mod 16$. If $e^4 \equiv 0$, then all of a^4, b^4, c^4, d^4 must also be congruent to 0, which will give an imprimitive solution (we can factor 16 out of each of the values to get a more simplified and essentially equivalent solution). Therefore, we must have $e^4 \equiv 1 \mod 16$. The only way to add up the fourth powers on the left hand side to get 1 mod 16 is to have only one of them, say d, such that $d^4 \equiv 1$, and to have the rest $a^4, b^4, c^4 \equiv 0$. This means we need exactly one of the numbers a, b, c, d on the left hand side to be odd. Taking d to be this lone odd number, we can rearrange the equation and write

$$a^4 + b^4 + c^4 = e^4 - d^4$$

And it follows that

$$\left(\frac{a}{2}\right)^4 + \left(\frac{b}{2}\right)^4 + \left(\frac{c}{2}\right)^4 = \frac{e^4 - d^4}{16}$$

All of these values are integers because a, b, c, are assumed to be odd and we assumed $d^4, e^4 \equiv 1 \mod 16$.

Since each of $(\frac{a}{2})^4$, $(\frac{b}{2})^4$, and $(\frac{c}{2})^4$ must be themselves congruent to either 0 or 1 mod 16, taking all combinations, the only possible values of $\frac{e^4-d^4}{16} \mod 16$ are 0, 1, 2, and 3. Therefore we don't need to check values of d and e where $\frac{e^4-d^4}{16} \not\equiv 0, 1, 2, 3 \mod 16$.

This greatly reduces the space of possible values that we need to consider when checking possible solutions to the equation. We can reduce them further by considering the values of the fourth powers mod 5, again as per Leech [3].

By Fermat's Little Theorem, for any integer x coprime to 5, $x^4 \equiv 1 \mod 5$. Therefore, the only integers x where $x^4 \not\equiv 1 \mod 5$ are multiples of 5, in which case $x^4 \equiv 0 \mod 5$. Applying similar reasoning as in the above case, we must have that $e^4 \equiv 1 \mod 5$ and exactly three of a, b, c, d must be multiples of 5. Supposing d is the only one of these congruent to 1 mod 5 (this might not be the same d as above that was assumed to be odd), we then have that $e^4 - d^4 \equiv 0 \mod 5$, so $e^4 - d^4$ must be divisible by $5^4 = 625$. It follows that a valid solution requires $d \equiv \pm e$ or $d \equiv \pm 182e \mod 625$ (since $182^2 \equiv -1 \mod 625$) [3].

1.3 $n = 5$

When $n = 5$, we can rewrite our equation (1) as follows:

$$x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 = y^5 \tag{5}$$

The smallest known solution [6] is as follows:

$$x_1 = 7, \quad x_2 = 43, \quad x_3 = 57, \quad x_4 = 80, \quad x_5 = 100, \quad y = 107$$

It has been proven that there are infinitely many solutions to this equation, as Sastry [6] found a parametrization of the equation in two variables; for any $g, n \in \mathbb{Z}$, the following is a solution to (5):

$$x_1 = 75n^5 - g^5, \quad x_2 = g^5 + 25n^5, \quad x_3 = g^5 - 25n^5,$$
$$x_4 = 10g^3n^2, \quad x_5 = 50gn^4, \quad y = g^5 + 75n^5$$

1.4 $n = 6$

No solutions have been found for the $n = 6$ case of our equation [2] [5]:

$$x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 + x_6^6 = y^6 \tag{6}$$

By 1967 [2], all possible values up to $y = 38314$ were searched, and still no solutions to (6) have been found.

However, even though no integer solutions to this equation have been found, we can still ascertain certain properties that a solution would need to have, described in [1] and [2]. By Fermat's Little Theorem, applying the similar argument as above in the $n = 4$ case, for any integer x, $x^6 \equiv 0$ or $x^6 \equiv 1 \mod 7$. It can also be found that any sixth power is congruent to either 0 or 1 mod 8, and the same holds for mod 9. Applying similar arguments as above, this allows us to describe all possible cases that satisfy (6) under divisibility by 2, 3, and 7.

1.5 Our topic

After researching the problem we presented initially and investigating the methods that have been applied in searching for solutions to above equations, we can see that examining properties of certain powers under certain moduli allows us to greatly reduce the number of sets of values we need to check when searching for integer solutions to our equation (1). In particular, for example, in the $n = 4$ case, identifying values that fourth powers must take when reducing them mod 16 or mod 5 allows us to reject a subset of possible values that would need to be checked. In order to best optimize the algorithms we use to search for solutions of some nth case of (1), a good initial step would be to search for some nice patterns that nth powers take under different moduli.

2 Searching for Solutions

Computing these solutions purely by trial and error is prohibitively expensive, even for modern computers. Given some $x \in \mathbb{N}$, if we wish to find a potential solution to the equation in Conjecture 1 (Eqn 1.) naively, we could search all potential combinations of y_i s.t. $y_i \in \{0, 1, 2, ..., x\}$. This, however, results in an algorithm which performs x^n operations in the worst case, which for large values of x - and even moderately sized values of n - is incredibly slow. Thus, before any searching can be done, the potential values of each y_i must be narrowed down.

We first establish a more resonable upper bound on each y_i. Without loss of generality, consider the upper bound for y_1. This can be easily extended to any other y_i due to the commutativity of addition, and the fact that they are all raised to the same power. We have: $x^n = \sum_{i=1}^{n} y_i^n$
$\implies x^n = y_1^n + \sum_{i=2}^{n} y_i^n$
$\implies y_1^n = x^n - \sum_{i=2}^{n} y_i^n$
Note that due to our restrictions, $y_i \geq 1 \forall i$
$\implies y_1^n \leq x^n - (n-1)$
$\implies y_1 \leq \sqrt[n]{x^n - n + 1}$
$\implies y_1 \leq \lfloor \sqrt[n]{x^n - n + 1} \rfloor$ (since $y_1 \in \mathbb{N}$)

While this is indeed less than x, for large values of x or n it does not significantly reduce the running time of the algorithm. This means other methods must be employed.

Another significant reduction comes from the elimination of repeated cases. Due to the commutativity of addition, if we have two cases: $(y_1, \ldots, y_i, \ldots, y_j, \ldots, y_n)$ and $(y_1, \ldots, y_j, \ldots, y_i, \ldots, y_n)$, they will be equivalent, and do not need to be checked twice. Thus, instead of checking $x^n - n + 1$ cases, we need to check a number of cases equivalent to how many ways $\{0, 1, \ldots, \lfloor \sqrt[n]{x^n - n + 1} \rfloor\}$ can be uniquely placed in n unordered elements. Employing a common method in statistics, this can be considered a case of 'dividers and buckets'. We have n 'buckets', and $\lfloor \sqrt[n]{x^n - n + 1} \rfloor$ 'dividers', which we place between the buckets. Any bucket to the left of the first divider will contain $y_i = 0$, between the first and second divider will be $y_i = 1$, between the second and third will be $y_i = 2$, and so on. Given $\lfloor \sqrt[n]{x^n - n + 1} \rfloor$ slots which are sufficient to hold either a divider or a bucket, there are $\sqrt[n]{x^n - n + 1} - 1 + n$ choose $n = \binom{\lfloor \sqrt[n]{x^n - n + 1} \rfloor}{n}$ ways to place these elements, which is the new running time of the algorithm. While this is still $O(x^n)$ (see appendix 5.3), removing repeated cases clearly reduces the running time, resulting in a faster search.

One final strategy used by Leech is to examine $x^n \mod k$ for some k, then eliminate solutions based on those findings (Leech 1958). For example, knowing that $x^4 \mod 16 \in \{0, 1\}$ implies 3 of the y_i's must be even, while the last must be odd (when the y_i's do not share a common factor), since their sum

must be 1 mod 16 (Leech, 1958). This makes patterns appearing in powers mod n particularly important to this topic, which lead to some of the proposed patterns in section 4. One such case of this strategy is discussed in section 3.

To assist in finding these reductions, we created an algorithm which checked $x^n \mod N$ for given x, n, and all N up to a given K. Since $a \equiv b \mod N \implies a^n \equiv b^n \mod N \; \forall a, b, n, N \in \mathbb{N}$, it was sufficient to check all elements of the complete residue system of N, sort the resulting set, and find the unique elements. We then iterated over the different values of N in order to find a 'good' one. A 'good' N is one that efficiently eliminates a significant number of cases, discussed below. Once a good N was found, and restrictions on the y_i's were imposed, we simply ran the naive algorithm and discarded all cases where some y_i did not meet the requirements, usually by changing the 'step size' which each y_i was increased by per iteration.
Finally, we analyze what constitutes a 'good' N. For a given N and n, let $\{a_1, a_2, \ldots, a_l\} = A_N$ be the unique values of $z^n \mod N$, where z runs over a complete residue system mod N. Let x, y_i be defined as in Eqn. (1). We know $x^n \mod N \in A_N$, so for any solution $y_1^*, y_2^*, \ldots, y_n^*$ with corresponding residues $r_1, r_2, \ldots, r_n \mod N$, it must be that $(y_1^*)^n + (y_2^*)^n + \ldots + (y_n^*)^n \equiv x^n \mod N$ (as a direct application of Eqn. (1))
$\implies r_1^n + r_2^n + \ldots + r_n^n \equiv x^n \mod N$ (Since each y_i^* is equivalent to it's residue mod N)
$\implies a'_{r_1} + a'_{r_2} + \ldots + a'_{r_n} \equiv a'_x$ (where $a'_i \in A_N$ represents the value of $i^n \mod N$)
This means by observing the number of combinations of n elements $b'_1, b'_2, \ldots b'_n \in A_N$ such that $b'_1 + b'_2 + \ldots + b'_n \mod N \in A_N$, we can categorize every possible solution to Eqn. (1) based on each y_i modulo N. In theory, a 'good' N is one such that the number of combinations described above is significantly less than the total number of combinations of a_i's (given by n^l, where $l = |A_N|$). This can be difficult to implement efficiently, however, as the equation would have to be checked every time to ensure it matched one of the forms found. Instead, a 'good' N for us was one where all of the forms described above were easily recognizable, such as 'only one b_i can equal 1'. To analyze this, we first had the program recommend N such that $|A_N|$ was minimized, as a lower number of possible values is easy to analyze, and often leads to less complex forms (if $|A_N| = |A_{N'}|$ for some $N \neq N'$, we selected $\max(N, N')$, as a larger complete residue system with the same number of unique mods is likely to eliminate more values). Then, we performed the analysis of the forms manually, and if they were all easily recognizable, and provided any reduction in the number of cases, the N was considered 'good'.

3 The Case Of Near-Primes

One of the broadest searches we were able to perform was for $n = 10$. Running the mod-search algorithm described above, we found that $x^{10} \mod 11$ was 0

or 1 for all x in a complete residue system of 10 (meaning $x^{10} \mod 11$ was 0 or 1 for all $x \in \mathbb{N}$). Moreover, the only numbers x such that $x^{10} \equiv 0 \mod 11$ were $11k, k \in \mathbb{N}$. Because of this, we know if $x^{10} \equiv 1 \mod 11$, then $\sum_{i=1}^{10} y_i^{10} \equiv 1 \mod 11 \implies$ one y_i is congruent to $1 \mod 11$, and the rest must be congruent to $0 \mod 11$. If $x^{10} \equiv 0 \mod 11$, all y_i must be congruent to $0 \mod 11$. Due to the commutativity of addition, we were able to only consider $y_1 \equiv 0$ or $1 \mod 11$, and every other value could be incremented in steps of 11, allowing us to eliminate a significant number of cases.

This can be extended to the following theorem: Let $n \in \mathbb{N}$ such that $n = p - 1$ for some prime $p \in \mathbb{N}$, then for any solution $(y_1^*)^n + (y_2^*)^n + \ldots, (y_n^*)^n = (x^*)^n$ to Eqn. (1):

1. If $(x^*)^n \equiv 1 \mod p$, then (1.1) $\exists i \in \{1, \ldots, n\}$ such that $(y_i^*)^n \equiv 1 \mod p$, and (1.2) $\nexists i, j \in \{1, \ldots, n\}, i \neq j$ such that $(y_i^*)^n \equiv (y_j^*)^n \equiv 1 \mod p$ (i.e. the i in (1.1) is the only value for which $(y_i^*)^n \equiv 1 \mod p$)

2. If $(x^*)^n \equiv 0 \mod p$, then $\forall i \in \{1, \ldots, n\}, y_i \equiv 0 \mod p$.

Proof. First note by Fermat's little theorem, given p prime, $\forall x \in \mathbb{N}, p \nmid x \implies x^{p-1} \equiv x^n \equiv 1 \mod p$.

1. Suppose $(x^*)^n \equiv 1 \mod p$. Since $a \equiv b \mod N \wedge c \equiv d \mod N \implies a + c \equiv b + d \mod N \; \forall a, b, n, N \in \mathbb{N}$ (property (**)), if every $(y_i^*)^n \equiv 0 \mod p$, then $(y_1^*)^n + (y_2^*)^n + \ldots + (y_n^*)^n \equiv 0 \not\equiv (x^*)^n \mod p$, leading to a contradiction. This means $\exists i \in \{1, \ldots, n\}$ such that $(y_i^*)^n \not\equiv 0 \mod p \implies (y_i^*)^n \equiv 1 \mod p$ (as that is the only other option), which proves (1.1).
   Now, suppose to the contradiction $\exists i, j \in \{1, \ldots, n\}, i \neq j$ such that $(y_i^*)^n \equiv y*_j^n \equiv 1 \mod p$. Without loss of generality (due to the commutativity of addition), assume $i = 1, j = 2$.
   $\implies (y_1^*)^n + (y_2^*)^n + \ldots + (y_n^*)^n \equiv 1 + 1 + (y_3^*)^n + \ldots + (y_n^*)^n \equiv 2 + (y_3^*)^n + \ldots + (y_n^*)^n \mod p$ (***)
   Furthermore, since $(y_1^*)^n + (y_2^*)^n + \ldots + (y_n^*)^n \equiv x*_n^n \equiv 1 \mod p$, by property (**) and the definition of mod we have $(y_1^*)^n \mod p + (y_2^*)^n \mod p + \ldots + (y_n^*)^n \mod p = kp + 1$ for some $k \in \mathbb{N}$. By (***) and property (**), we have $(y_1^*)^n \mod p + (y_2^*)^n \mod p + \ldots + (y_n^*)^n \mod p \geq 2 > 1$, so $k > 0$. However, since $(y_i^*)^n \mod p \equiv 0$ or $1 \mod p \; \forall i \in \{1, \ldots, n\}$, we have $(y_1^*)^n \mod p + (y_2^*)^n \mod p + \ldots + (y_n^*)^n \mod p \leq 1 + 1 + \ldots + 1 = n = p - 1 < p + 1$, so $k < 1$. We cannot have $k \in \mathbb{N}$ such that $0 < k < 1$, so we have a contradiction, and it must be the case that $\nexists i, j \in \{1, \ldots, n\}, i \neq j$ such that $(y_i^*)^n \equiv y*_j^n \equiv 1 \mod p$.

2. Suppose to the contradiction $\exists i \in \{1, \ldots, n\}$ such that $(y_i^*)^n \equiv 1 \mod p$ (assume without loss of generality $i = 1$). By a similar argument to the one made in (1.2), $(y_1^*)^n \mod p + (y_2^*)^n \mod p + \ldots + (y_n^*)^n \mod p = kp$ for some $k \in \mathbb{N}$. Additionally, following the same steps, $(y_1^*)^n \mod p + (y_2^*)^n \mod p + \ldots + (y_n^*)^n \mod p \geq 1 \implies k > 0$, and

$(y_1^*)^n \mod p + (y_2^*)^n \mod p + \ldots + (y_n^*)^n$
$\mod p \leq 1 + 1 + \ldots + 1 = n = p - 1 < p$, so $k < 1$, and we have a contradiction.

□

Ultimately, due to the commutativity of addition, this allows us to let one y_i be coprime to p at a given time, while all other y_j's can be divisible by p, leading to significant cost reductions. Due to this, in future research, we recommend performing searches on values of n which are equal to $p-1$, as the algorithm is easy to implement, and very efficient compared to the naive approach.

4 Patterns of Powers $\mod N$

In order to find integer solutions for different n, we investigated checking the reduced residues of $x^n \mod N$ through computational analysis, so that we could eliminate solutions that would not lead to a possible solution, and thus reduce the complexity of finding one. Expanding on Leech's [3] notion of reducing the residue of x to the 4th power to $\{0, 1\} \mod N = 16$, our hope was to find different families of n such that N is maximal and the reduced residue of x to the nth power is minimal. In this way we could eliminate as many solutions as possible and hopefully greatly increase our chances of finding more integer solutions to Conjecture 1. for higher n.

While investigating different positive integers n and N we found certain patterns for the reduced residues.

Let us introduce some notation to better convey the sequence we investigated. Fix $N \in \mathbb{N}$. Let A be the sequence $A = \{0^n, 1^n, 2^n, 3^n, 4^n, 5^n, ...\}$, and $A_r = \{a \mod N\}_{a \in A}$ be the reduced residue of $A \mod N$. Here are some potential conjectures on the set A given the data we have collected:

Conjecture 2: For all natural numbers d, If $n \geq d$ and $N = 2^d$, every other element starting with the first in A_r is 0, $A_r = \{0, \_, 0, \_, 0, \_, ...\}$.

i.e. $\forall d \in \mathbb{N}$, if x is even and $n \geq d$, then $x^n \equiv 0 \mod 2^d$.

A.D.

Since, Leech [3] had $n = 4$ and $N = 16$ we thought there could be something potentially significant about even positive integers and powers of 2. After trying random even n and N we found that certain N resulted in a sequence such that every other element was 0. Through further investigation we found this to appear to be exactly when N was a power of 2. Moreover, after collecting more and more data, it seemed to suggest that it was so for all powers of 2. However, after attempting to prove the conjecture, the theory surfaced that this was in fact incorrect, and was only true when the power of 2 was less than n, but it also surfaced that it was true for odd n as well and not just even ones.

For certain n and N, the other numbers in the sequence increasingly vary as the absolute difference between n and N is increased. This would not help much with reducing the complexity, but at least Conjecture 2. reduces the possible congruencies for the sum in Conjecture 1. to $0 \mod N$ for every even x.

Proof. Consider $x^n \mod N$, $\forall d \in \mathbb{N}$, $n \geq d$ and $N = 2^d$.
We want to show that if x is even, then $x^n \equiv 0 \mod N$.
i.e. $N|x^n - 0 \iff x^n = Nm$ for some $m \in \mathbb{N}$.
Since x is even, $x = 2b$ for some $b \in \mathbb{N}$.
We have $x^n = (2b)^n = 2^n b^n$.

$$\frac{x^n}{N} = \frac{2^n b^n}{2^d} = 2^{n-d} b^n = m \in \mathbb{N} \text{ exists, since } n - d \geq 0 \text{ as wanted.}$$

Hence, Conjecture 2 holds. A.D. □

Collected data for Conjecture 2. A_r for even n:

- $n = 24$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 24$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 24$, $N = 8$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 24$, $N = 16$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 24$, $N = 32$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 24$, $N = 64$: 0, 1, 0, 33, 0, 33, 0, 1, 0, 1, 0, 33, 0, 33, 0, 1, ...
  $n = 24$, $N = 128$: 0, 1, 0, 97, 0, 33, 0, 65, 0, 65, 0, 33, 0, 97, 0, 1, ...
  $n = 24$, $N = 256$: 0, 1, 0, 225, 0, 161, 0, 65, 0, 193, 0, 33, 0, 97, 0, 129, ...
  $n = 24$, $N = 512$: 0, 1, 0, 225, 0, 417, 0, 65, 0, 449, 0, 33, 0, 97, 0, 129, ...
  $n = 24$, $N = 1024$: 0, 1, 0, 225, 0, 417, 0, 65, 0, 449, 0, 545, 0, 97, 0, ...
  $n = 24$, $N = 8192$: 0, 1, 0, 6369, 0, 3489, 0, 5185, 0, 5569, 0, 7713, 0, ...
  this data seemed to suggest all powers of 2 had this property, but this was missleading since n was very large
- $n = 10$, $N = 32$: 0, 1, 0, 9, 0, 25, 0, 17, 0, 17, 0, 25, 0, 9, 0, 1, ...
- $n = 12$, $N = 64$: 0, 1, 0, 49, 0, 17, 0, 33, 0, 33, 0, 17, 0, 49, 0, 1, ...
- $n = 14$, $N = 512$: 0, 1, 0, 377, 0, 489, 0, 81, 0, 305, 0, 137, 0, 473, 0, ...
- $n = 18$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 34$, $N = 128$: 0, 1, 0, 9, 0, 25, 0, 49, 0, 81, 0, 121, 0, 41, 0, 97, ...
- $n = 235676$, $N = 128$: 0, 1, 0, 49, 0, 17, 0, 33, 0, 97, 0, 81, 0, 113, 0, ...
- $n = 35$, $N = 8192$: 0, 1, 0, 6043, 0, 4605, 0, 3671, 0, 6105, 0, 7603, 0, 2837, 0, 7983, 0, 1329, 0, 3147, 0, 8109, 0, 7815, 0, 5129, ...

- $n = 5$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 5$, $N = 4$: 0, 1, 0, 3, 0, 1, 0, 3, 0, 1, 0, 3, 0, 1, 0, 3, ...
  $n = 5$, $N = 8$: 0, 1, 0, 3, 0, 5, 0, 7, 0, 1, 0, 3, 0, 5, 0, 7, ...
  $n = 5$, $N = 16$: 0, 1, 0, 3, 0, 5, 0, 7, 0, 9, 0, 11, 0, 13, 0, 15, ...
  $n = 5$, $N = 32$: 0, 1, 0, 19, 0, 21, 0, 7, 0, 9, 0, 27, 0, 29, 0, 15, ...
  $n = 5$, $N = 64$: 0, 1, 32, 51, 0, 53, 32, 39, 0, 41, 32, 27, 0, 29, 32, 15, ...
  here is an example of when it fails since the power of 2 ($N = 2^6$) is greater than $n = 5$

Conjecture 2.1: If $n = 2^k$ for some natural number k, there exists a natural number N such that A_r is of the form $\{0, 1, 0, 1, 0, 1, ...\}$.
Moreover, for $k > 1$, A_r has this form for all $N = 2^d$, $d \in \{1, ..., k + 2\}$.

$$\text{i.e. } \forall k \in \mathbb{N}, k > 1,\ x^{2^k} \equiv \begin{cases} 0 \mod 2^d & \text{if } x \text{ is even} \\ 1 \mod 2^d & \text{if } x \text{ is odd} \end{cases}, d \in \{1, ..., k + 2\}.$$

A.D.

Through the investigation of Conjecture 2. we observed that for certain even n, there existed $N =$ a power of 2 such that A_r did in fact reduce to $\{0, 1\}$ just as Leech's [3]. After trying different powers of 2, we observed this to be the case for all n that were also a power of 2. Moreover, for n greater than 2, this appeared to be the case for all $N =$ powers of 2 less than n up to and including the next two powers greater than n, but no greater.

Interestingly, the gap between k and $k + 2$ (the max power) did not seem to increase nor decrease for greater n, however it did fall in line with Leech's [3] findings where $n = 2^2$ and $N = 16 = 2^{2+2}$. Given $n = 4 = 2^2$, Conjecture 2.1. suggests the maximal N for the minimal reduced resides ($\{0, 1\}$) is in fact $2^{2+2} = 16$.

If Conjecture 2.1. holds, it definitely proves to provide the most promising foundation to finding more solutions to Conjecture 1. for all $n =$ powers of 2. It significantly reduces the possible congruencies for the sum in Conjecture 1. to $0 \mod N$ for every even x and $1 \mod N$ for every odd x.

Proof. Let $k > 1$ be an arbitrary natural number and $d \in \{1, ..., k + 2\}$.
(*) Note: $k > 1 \iff 2^k \geq k + 2 \geq d \iff 2^k - d \geq 0$

We want to show: $\begin{cases} \text{if } x \text{ is even, then} & x^{2^k} \equiv 0 \mod 2^d \iff 2^d | x^{2^k} \\ \text{if } x \text{ is odd, then} & x^{2^k} \equiv 1 \mod 2^d \iff 2^d | x^{2^k} - 1 \end{cases}$

Case 1: Suppose x is even. Then $x = 2b$ for some $b \in \mathbb{N}$.
We have $x^{2^k} = (2b)^{2^k} = 2^{2^k} b^{2^k}$.

$$\frac{x^n}{2^d} = \frac{2^{2^k} b^{2^k}}{2^d} = 2^{2^k - d} b^{2^k} \in \mathbb{N} \text{ since } k > 1 \text{ (*)} \iff 2^d | x^{2^k} \text{ as wanted.}$$

Case 2: Suppose x is odd. Then $x = 2b + 1$ for some $b \in \mathbb{N}$.

We have $x^{2^k} = (2b+1)^{2^k}$.

By the binomial theorem the ith term is of the form

$$\binom{2^k}{i}(2b)^i 1^{2^k-i} = \binom{2^k}{i}(2b)^i = \frac{(2^k)!}{i!(2^k-i)!}2^i b^i$$

So $x^{2^k} = (2b+1)^{2^k}$

$$\begin{aligned}
&= \frac{(2^k)!}{0!(2^k)!}2^0b^0 + \frac{(2^k)!}{1!(2^k-1)!}2^1b^1 + \frac{(2^k)!}{2!(2^k-2)!}2^2b^2 + ... \\
&\quad ... + \frac{(2^k)!}{(2^k-1)!(2^k-(2^k-1))!}2^{2^k-1}b^{2^k-1} + \frac{(2^k)!}{(2^k)!(2^k-2^k)!}2^{2^k}b^{2^k} \\
&= 1 + (2^k)2b + (2^k)(2^k-1)2b^2 + ... + (2^k)2^{2^k-1}b^{2^k-1} + 2^{2^k}b^{2^k}
\end{aligned}$$

Note, the $i = 3$rd term for example:
$\frac{(2^k)!}{3!(2^k-3)!}2^3b^3 = (2^k)(2^k-1)(2^k-2)\frac{1}{3}2^2b^3$ is in fact $\in \mathbb{N}$, since $(2^k)(2^k-1)(2^k-2)$ are three consecutive integers $\implies$ one is divisible by 3. Moreover, it is also contains 2^k and another 2 which are both used for all the inner terms below.

Then

$$\begin{aligned}
\frac{x^n-1}{2^d} &= \frac{(2b+1)^{2^k}-1}{2^d} \\
&= \frac{1 + (2^k)2b + (2^k)(2^k-1)2b^2 + ... + (2^k)2^{2^k-1}b^{2^k-1} + 2^{2^k}b^{2^k} - 1}{2^d} \\
&= \frac{1}{2^d} + \frac{2^k}{2^d}2b + \frac{2^k}{2^d}(2^k-1)2b^2 + ... + \frac{2^k}{2^d}2^{2^k-1}b^{2^k-1} + \frac{2^{2^k}}{2^d}b^{2^k} - \frac{1}{2^d} \\
&= (2^{k-d})2b + (2^{k-d})(2^k-1)2b^2 + ... + (2^{k-d})2^{2^k-1}b^{2^k-1} + 2^{2^k-d}b^{2^k}
\end{aligned}$$

Since $2^k - d \geq 0$ (*) and $k+2 \geq d$, in the worse case $2^k - d = 0$ and $k+2 = d$. This is indeed the worst case, since if the terms can be divided by 2^{k+2}, they can most certainly be divided by 2^d for $d < k+2$.

In the worst case we have

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

Which implies that

$$\begin{aligned}
(x^{2^k}-1) &\equiv 2^{k+1}\left(b + (2^k-1)b^2 + ... + 2^{2^k-2}b^{2^k-1}\right) + 2^{k+2}b^{2^k} \mod 2^{k+2} \\
&\equiv (2^k - 2 \text{ terms} \equiv 2^{k+1}) + (0) \mod 2^{k+2} \\
&\equiv (2^{k+2}(2^{k-1}-1)) + (0) \mod 2^{k+2} \\
&\equiv (0) + (0) \mod 2^{k+2}
\end{aligned}$$

$\equiv 0 \mod 2^d$ as wanted i.e. $2^d | x^{2^k} - 1$.

Hence, Conjecture 2.1 holds. A.D. $\square$

Collected data for Conjecture 2.1. A_r for $n = 2^k$:

- $n = 1$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 2$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 2$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 4$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 4$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 4$, $N = 8$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 4$, $N = 16$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 8$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 8$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 8$, $N = 8$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 8$, $N = 16$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 8$, $N = 32$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 16$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 16$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 16$, $N = 8$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 16$, $N = 16$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 16$, $N = 32$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 16$, $N = 64$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 32$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 32$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 32$, $N = 8$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 32$, $N = 16$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 32$, $N = 32$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 32$, $N = 64$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 32$, $N = 128$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
- $n = 64$, $N = 2$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 4$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 8$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 16$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 32$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 64$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 128$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...
  $n = 64$, $N = 256$: 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, ...

Conjecture 3: If n is prime, there exists a natural number N such that A_r is of the form: $A_r = \{0, 1, 2, 3, ..., n-1, 0, 1, 2, 3, ..., n-1, ...\}$.

A.D.

Throughout the search for Patterns of Powers $\mod N$, we found that it appeared that for prime n there existed an N such that A_r was a repeating sequence from 0 all the way to $n-1$. Though this would be very interesting if it were true, it was not actually helpful in the search to find ways to reduce to a minimal set. If Conjecture 3. were true, for prime n, the sum in Conjecture 1. could be congrunent to $0, 1, 2, ...,$ or $n-1 \mod N$ for some N, which may not eliminate any possible solutions at all. Conjecture 3. may suggest, however, that finding solutions to Conjecture 1. for prime n is much more challenging.

Collected data for Conjecture 3. A_r for prime n:

- $n = 3$, $N = 3$: 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, 1, 2, 0, ...
- $n = 5$, $N = 5$: 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, ...
- $n = 7$, $N = 7$: 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, ...
- $n = 11$, $N = 11$: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 0, 1, 2, ...

5 Conclusion

In conclusion, even though we were unable to find more integer solutions to the sum in Conjecture 1. and neither prove nor disprove it, we hope we were better able to provide a stronger foundation to build upon in search for solutions for higher n. Perhaps, much of our research may provide itself useful to optimize the finding of such solutions algorithmically and theoretically by excluding impossible solutions that don't match the required reduced residue $\mod N$. This approach seemed most promising for certain families of n, such as in Conjecture 2.1. for $n =$ powers of 2, where the sum in Conjecture 1. can be reduced to $\{0, 1\} \mod N$. Our hope is that this paper provides a stepping stone to new findings of integer solutions to Diophantine Equations to the Power of n.

6 Appendices

6.1 Fourth powers can only be congruent to 0 or 1 mod 16

If x is even, it can be written as $2n$ where $n \in \mathbb{Z}$, and
$(2n)^4 = 2^4(n^4) = 16(n^4) \equiv 0 \mod 16$.
If x is odd, it can be written as $2n+1$ where $n \in \mathbb{Z}$, then

$$\begin{aligned}(2n+1)^4 &= 16n^4 + 32n^3 + 24n^2 + 8n + 1 \\ &\equiv 24n^2 + 8n + 1 \mod 16\end{aligned}$$

If this n is even, it can be written $n = 2k$ where $k \in \mathbb{Z}$:

$$\begin{aligned}(2n+1)^4 &= 24n^2 + 8n + 1 \\ &= 96k^2 + 16k + 1 \\ &\equiv 1 \mod 16\end{aligned}$$

And if this n is odd, it can be written $n = 2k+1$ where $k \in \mathbb{Z}$:

$$\begin{aligned}(2n+1)^4 &= 24n^2 + 8n + 1 \\ &= 24(2k+1)^2 + 8(2k+1) + 1 \\ &= 96k^2 + 96k + 16k + 32 + 1 \\ &\equiv 1 \mod 16\end{aligned}$$

Thus, when x is even, $x^4 \equiv 0 \mod 16$, and when x is odd, $x^4 \equiv 1 \mod 16$.
Alternatively, this could be proven by looking at the 4th powers of any reduced residue system mod 16.

6.2 Naive Algorithm Without Duplicates to Find An Integer Solution to Conjecture 1.

language: C, complexity: $O(x^n)$

```
typedef unsigned long long big;

void powerSum(int n) {
    big* arr = (big*)malloc((n+1)*sizeof(big));
    arr[n] = n;
    int maxY = ceil(pow(pow(arr[n],n)-n+1, 0.5));
    for (int i = 0; i < n; i++) arr[i] = 1;
    arr[0] = 0;

    while (arr[n] <= 10000) {
        arr[0]++;
        int i = 0;
```

```
            int last_modified = 0;

            while (i < n-1 && arr[i] > maxY) {
                arr[i + 1]++;
                i++;
                last_modified = i;
            }

            if (arr[n-1] > maxY) {
                arr[n]++;
                for (int i = 0; i < n; i++) arr[i] = 1;
                maxY = floor(pow(pow(arr[n],n)-n+1, 1/(float)n));
                printf("n = %u, maxY = %u\n", arr[n], maxY);
                last_modified = 0;
            }

            for (int j = 0; j < last_modified; j++)
                arr[j] = arr[last_modified];

            if (sumEqual(arr, n)) {
                printf("%u^%d = %u^%d",arr[n],n,arr[n-1],n);
                for (int i = n-2; i >= 0; i--) printf(" + %u^%d",arr[i],n);
                printf("\n");
                break;
            }
        }
        free(arr);
    }
```

6.3 Proof of the Running Time of The Naive Algorithm Without Duplicates.

As shown in section 2, the running time of this algorithm is $\binom{\lfloor \sqrt[n]{x^n-n+1} \rfloor}{n}$. As x grows large, the difference between $\lfloor \sqrt[n]{x^n-n+1} \rfloor$ and x^n becomes negligible, so we will consider the running time as $\binom{x}{n}$ for the purpose of this analysis (this will result in a slight overestimate, but since we are establishing an upper bound this is fine). Additionally, assume $x > 1$ (running time analysis is typically only concerned with large values, so this is also acceptable).

$\binom{x}{n} = \frac{x!}{n!(x-n)!}$ (By definition of choose)
$= \frac{1}{n!} * (x * (x-1) * (x-2) * \ldots * (x-n+1))$ (Cancelling the terms in $\frac{x!}{(x-n)!}$)
$\leq x * (x-1) * (x-2) * \ldots * (x-n+1)$ (Since $\frac{1}{n!} \leq 1$)
$= x^n * (1 - \frac{1}{x}) * (1 - \frac{2}{x}) * \ldots * (1 - \frac{n-1}{x})$
$\leq x^n$ (Since $0 < 1 - \frac{i}{x} < 1 \forall i \in \mathbb{N}$)

Which implies the algorithm is $O(x^N)$.

References

[1] Peter J. Ansell, https://sites.google.com/site/sevensixthpowers/

[2] L. J. Lander, T. R. Parkin and J. L. Selfridge, **A survey of equal sums of like powers**, *Mathematics of Computation*, 21, 446-459 (1967). https://www.ams.org/journals/mcom/1967-21-099/S0025-5718-1967-0222008-0/S0025-5718-1967-0222008-0.pdf

Presents various solutions to powers of Diophantine equations, including the $n = 4$ and $n = 5$ cases of the conjecture.

[3] J. Leech, **On** $A^4 + B^4 + C^4 + D^4 = E^4$ *Mathematical Proceedings of the Cambridge Philosophical Society*, 54(4), 554-555, (1958). doi.org/10.1017/S0305004100003091

Brief paper outlining found solutions for the $n = 4$ case and considerations that reduce the number of possible solutions that need to be checked.

[4] L. J. Mordell, **On Sums of Three Cubes** *Journal of the London Mathematical Society*, 17(3), 139-144 (1942). https://londmathsoc-onlinelibrary-wiley-com.myaccess.library.utoronto.ca/doi/abs/10.1112/jlms/s1-17.3.139

[5] https://mathworld.wolfram.com/DiophantineEquation6thPowers.html

[6] S. Sastry, **On Sums of Powers**, *Journal of the London Mathematical Society*, 9(4), 242-246 (1934). https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-9.4.242