

Diophantine Equations to the Power of n

MATC15 - Project - Draft 2

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 $x^n = y_1^n + \dots + y_n^n$ 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 $n \in \mathbb{Z}$:

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

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 $i = 2, \dots, n$. We also only want to keep *imprimitive* solutions, solutions where all of (x, y_1, \dots, 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 $x \not\equiv 5 \pmod{9}$:

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

The condition on $x \pmod{9}$ 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 $\{0, 1, 2, 3, 4, -4, -3, -2, -1\}$:

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

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):

$$x_1^3 + x_2^3 + x_3^3 = y^3 \quad (3)$$

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

$$a^4 + b^4 + c^4 + d^4 = e^4 \quad (4)$$

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, $x^4 \equiv 1 \pmod{16}$ (see Appendix 1).

Therefore, on the right side of our equation, $e^4 \equiv 0$ or $e^4 \equiv 1 \pmod{16}$. 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 $e^4 \equiv 1 \pmod{16}$. 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 $d^4, e^4 \equiv 1 \pmod{16}$.

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

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, $x^4 \equiv 1 \pmod{5}$. Therefore, the only integers x where $x^4 \not\equiv 1 \pmod{5}$ are multiples of 5, in which case $x^4 \equiv 0 \pmod{5}$. Applying similar reasoning as in the above case, we must have that $e^4 \equiv 1 \pmod{5}$ 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 $e^4 - d^4 \equiv 0 \pmod{5}$, so $e^4 - d^4$ must be divisible by $5^4 = 625$. It follows that a valid solution requires $d \equiv \pm e$ or $d \equiv \pm 182e \pmod{625}$ (since $182^2 \equiv -1 \pmod{625}$) [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):

$$\begin{aligned} x_1 &= 75n^5 - g^5, & x_2 &= g^5 + 25n^5, & x_3 &= g^5 - 25n^5, \\ x_4 &= 10g^3n^2, & x_5 &= 50gn^4, & y &= g^5 + 75n^5 \end{aligned}$$

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 $x^6 \equiv 1 \pmod{7}$. 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 n th case of (1), a good initial step would be to search for some nice patterns that n th 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. $y_i \in \{0, 1, 2, \dots, x\}$. 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, $y_i \geq 1 \forall i$

$$\implies y_1^n \leq x^n - (n-1)$$

$$\implies y_1 \leq \sqrt[n]{x^n - n + 1}$$

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:

$(y_1, \dots, y_i, \dots, y_j, \dots, y_n)$ and $(y_1, \dots, y_j, \dots, y_i, \dots, y_n)$, 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 $\{0, 1, \dots, \sqrt[n]{x^n - n + 1}\}$ 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 $\sqrt[n]{x^n - n + 1} - 1$ '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 $\sqrt[n]{x^n - n + 1} - 1 + n$ slots which are sufficient to hold either a divider or a bucket, there are $\sqrt[n]{x^n - n + 1} - 1 + n$ choose $\binom{\sqrt[n]{x^n - n + 1} - 1 + n}{n}$ ways to place these elements, which is the new running time of the algorithm. Since $\binom{a}{b} = \frac{a!}{b!(a-b)!}$, the running time of this new algorithm is in the order of $x!$ instead of x^n , which is far better.

One final strategy used by Leech is to examine $x^n \bmod k$ for some k , then eliminate solutions based on those findings (Leech 1958). For example, knowing that $x^4 \bmod 16 \in \{0, 1\}$ 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 $1 \bmod 16$ (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 $x^n \bmod k$ for given x, n , and all x up to a given K . Since $a \equiv b$

$\text{mod } k \implies a^n \equiv b^n \pmod k \forall a, b, n, k \in \mathbb{N}$, it was sufficient to check all elements of the reduced residue system of k , sort the resulting set, and find the unique elements. Once a good k 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.

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 $x^{10} \pmod{11}$ was 0 or 1 for all $x \in \mathbb{N}$. Moreover, the only numbers x such that $x^{10} \equiv 0 \pmod{11}$ were $11k, k \in \mathbb{N}$. Because of this, we know if $x^{10} \equiv 1 \pmod{11}$, then $\sum_{i=1}^{10} y_i^{10} \equiv 1 \pmod{11} \implies$ one y_i is congruent to 1 $\pmod{11}$, and the rest must be congruent to 0 $\pmod{11}$. If $x^{10} \equiv 0 \pmod{11}$, all y_i must be congruent to 0 $\pmod{11}$. Due to the commutativity of addition, we were able to only consider $y_1 \equiv 0$ or 1 $\pmod{11}$, 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 any n s.t. $n = p - 1$ for some prime $p \in \mathbb{N}$. By Fermat's little theorem, given p prime, $\forall x \in \mathbb{N}, p \nmid x \implies x^{p-1} \equiv x^n \equiv 1 \pmod p$, and, by the definition of mod, $p|x \implies x \equiv 0 \pmod p$. Since $n = p - 1$, we cannot sum enough y_i 's such that $y_i \equiv 1 \pmod p$ to exceed or equal p , so it must be that if $x \equiv 0 \pmod p \implies p|x$, then $\forall i \in \{1, \dots, n\}, y_i \equiv 0 \pmod p \implies p|y_i$, and if $x \equiv 1 \pmod p$, there is only one y_i congruent to 1 $\pmod p$. Thus, for further exploration regarding this topic, we recommend searching on values of n that satisfy this condition, as solutions will be found far more easily.

4 Patterns of Powers $\pmod N$

In order to find solutions for different n we investigated checking the reduced residues if $x^n \pmod N$ so that we could eliminate solutions that would not lead to a possible solution.

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

Let A be the sequence $A = \{0^n, 1^n, 2^n, 3^n, 4^n, 5^n, \dots\}$, and $A_r = \{a \pmod N\}_{a \in A}$ be the reduced residue of $A \pmod N$ for some $N \in \mathbb{N}$. Here may be some potential conjectures on the set A given the data we have collected:

Conjecture 2: If n is even, every other element starting with the first in A_r is 0, $A_r = \{0, -, 0, -, 0, -, \dots\}$, for $N = 2^d$ for all integers d .
i.e. $a_{2i} = 0$, where $a_{2i} \in A_r$ is the $2i^{\text{th}}$ element in A_r .

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, ...
- $n = 10, N = 32$: 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, 33, ...
- $n = 18, N = 2$: 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, 65, ...

Conjecture 2.1: If $n = 2^k$ for some integer k , there exists a natural number N such that A_r is of the form $\{0, 1, 0, 1, 0, 1, \dots\}$.

Moreover, for $k > 1$, A_r has this form for all $N = 2^d$, $d \in \{1, \dots, k + 2\}$.

A.D.

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: $A_r = \{0, 1, 2, 3, \dots, n-1, 0, 1, 2, 3, \dots, n-1, \dots\}$.

A.D.

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 Appendices

5.1 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
 $(2n)^4 = 2^4(n^4) = 16(n^4) \equiv 0 \pmod{16}$.

If x is odd, it can be written as $2n + 1$ where $n \in \mathbb{Z}$, then

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

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

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

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

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

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

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>