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 $x^n = y_0^n + \cdots + y_n^n$ given any x, excluding trivial solutions involving y_i's$= 0$ or x. This project will be a Type II project.
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 and provide some deeper research to the subject.

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, $y_i \geq 1 \forall i$

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

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

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 $\{0, 1, \ldots, \sqrt[n]{x^n - n + 1}\}$ 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 $\binom{n=}{\sqrt[n]{x^n-n+1}-1+nn}$ ways to place these elements, which is the new running time of the algorithm. Since $\binom{}{ab=\frac{a!}{b!(a-b)!}}$, 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 $x^n \mod k$ 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 $x^n \mod k$ for given x, n, and all x up to a given K. Since $a \equiv b \mod k \implies a^n \equiv b^n \mod k \forall a, b, n, k \in \ltimes$, 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 $x^{10} \mod 11$ 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 any n s.t. $n = p - 1$ for some prime $p \in \ltimes$. By Fermat's little theorem, given p prime, $\forall x \in \mathbb{N}, p \not| x \implies x^{p-1} \equiv x^n \equiv 1 \mod p$, and, by the definition of mod, $p|x \implies x \equiv 0 \mod p$. Since $n = p - 1$, we cannot sum enough y_i's such that $y_i \equiv 1 \mod p$ to exceed or equal p, so it must be that if $x \equiv 0 \mod p \implies p|x$, then $\forall i \in \{1, \ldots, n\}, y_1 \equiv 0 \mod p \implies p|y_i$, and if $x \equiv 1 \mod p$, there is only one y_i congruent to 1 mod 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 $\mod N$

In order to find solutions for different n we investigated checking the reduced residues if $x^n \mod N$ 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 $A = \{0^n, 1^n, 2^n, 3^n, 4^n, 5^n, ...\}$, and $A_r = \{a \bmod N\}_{a \in A}$ be the reduced residue of A mod N for some $N \in \mathbb{N}$. Here may be some potential conjetures 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, $A_r = \{0, \_, 0, \_, 0, \_, ...\}$, for $N = 2^d$ for all integers d.

i.e. $a_{2i} = 0$, where $a_{2i} \in A_r$ is the $2i^{th}$ 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 $\{0, 1, 0, 1, 0, 1, ...\}$.
Moreover, for $k > 1$, A_r has this form for all $N = 2^d$, $d \in \{1, ..., k+2\}$.

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

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 References

- Drago Bajc, **Power solutions of some Diophantine equations**, *The Mathematical Gazette*, 97:538, 107-110 (2013). https://www.jstor.org/stable/24496765

  Mentions form of above conjecture and states that solutions have been found in some cases but not in other cases, such as $n = 6$. Considers above conjecture with x^k instead of x^n, where $(k, n) = 1$ and provides a general form for these solutions.

- **Computing Minimal Equal Sums Of Like Powers**, http://euler.free.fr/index.htm

  Website dedicated to finding and compiling examples and counterexamples of Euler's sums of powers conjecture, which states that if a sum of n positive kth powers equals one kth power, then $n >= k$. Includes many resources we can look into.

- **BEST KNOWN SOLUTIONS**, http://euler.free.fr/records.htm

  Extensive list of aforementioned examples and counterexamples to Euler's sums of powers conjecture.

- L. Jacobi, D. Madden, **On** $a^4 + b^4 + c^4 + d^4 = (a + b + c + d)^4$, *The American Mathematical Monthly*, 115:3, 230-236 (2008). https://doi.org/10.1080/00029890.2008.11920519

  Discusses specific case of the conjecture with $n = 4$. Also discusses relation of Euler's conjecture and related Diophantine equations to the topic of elliptic curves.

- T. Roy and F. J. Sonia, **A Direct Method To Generate Pythagorean Triples And Its Generalization To Pythagorean Quadruples And n-tuples**, https://arxiv.org/ftp/arxiv/papers/1201/1201.2145.pdf

  Gives methods for finding Pythagorean n-tuples, sums of n squares that result in a square. Might be able to reduce some cases into one of these cases.

- D. R. Heath-Brown, W. M. Lioen and H. J. J. Te Riele, **On Solving the Diophantine Equation** $x^3 + y^3 + z^3 = k$ **on a Vector Computer**, *Mathematics of Computation*, 61:203, 235-244 (1993)

  Presents detailed algorithm for the $n = 3$ case, might be able to apply similar principles with higher n values.

- 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.

- 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.