Solutions to Fermat's Last Theorem with Matrices

Erin Smajdek and Jyotsana Sharma
Mentors: Marcos Reyes
2020 Mathematics Directed Reading Program, University of California, Santa Barbara

Abstract

In the year 1637, Pierre de Fermat conjectured the idea that for $n \geq 3$ there exists an equation:

$$A^n + B^n = C^n \tag{1}$$

for three positive integers A, B, C; this is known as Fermat's Last Equation. Fermat never proved this though, he stated that he knew the proof but that it merely would not fit in the margin of the paper. Then in 1995, professor Andrew Wiles proved that this equation has no integer solutions. Our goal is to see if we can find solutions for the modified equation:

$$A^2 + B^2 = C^2 \tag{2}$$

where A, B, C are 2 X 2 matrices with integer components.

In a paper by Maxim Arnold and Anatoly Eydelzon, a method was created to find solutions to Fermat's Last Theorem for noncommutable matrices using eigenvalues. These steps are exemplified later. We first give immediate results for equation (2).

Pythagorean Triples

A Pythagorean triple is a list of positive integers $\{a, b, c\}$ where $n = 2$ fulfilling equation (1).

- Let $\{a_1, b_1, c_1\}$, $\{a_2, b_2, c_2\}$ be Pythagorean triples. Consider the following matrices:

$$A = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}^2, B = \begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}^2, C = \begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix}^2$$

Then we find that:

$$A^2 + B^2 = C^2$$

Let $M \in \mathrm{M}_2(\mathbb{Q})$. Then consider MAM^{-1}, MBM^{-1}, MCM^{-1}. Note that these matrices may not belong to $M_2(\mathbb{Z})$. But there exists an integer α where multiplying each matrix by α we will get $X = \alpha MAM^{-1}, Y = \alpha MBM^{-1}, Z = \alpha MCM^{-1}$ are elements of $M_2(\mathbb{Z})$. Then clearly (X, Y, Z) satisfy equation (2). This is also true for any n x n matrix when we have n Pythagorean triples.

Commutable Matrices

In the case when two matrices commute they resemble the Pythagorean triple parameterization.
Let $A, B \in M_2(\mathbb{Z})$ such that $AB = BA$. Then consider the matrices:

$$X = A^2 - B^2,$$
$$Y = 2AB,$$
$$Z = A^2 + B^2.$$

Then the triple (X, Y, Z) satisfy equation (2). This method works when $A, B \in M_n(\mathbb{Z})$ as well.

Non Commutable Methodology

The steps to find the solution for non commutable matrices is as follows:
Start with a matrix $U \in M_n(\mathbb{Q})$ such that:

1. The eigenvalues λ_i, λ_j where $\lambda_i + \lambda_j \neq 0$
2. The eigenvectors of U must span the whole space $\mathbb{R}^n$

Then for $P \in M_n$ there exists $V \in M_n(\mathbb{Q})$ where $P = 2(UV + VU)$ we see this is true by the following.

Let $\{x_j\}_{j=1}^n$ be a basis of $\mathbb{R}^n$ then we want to find V such that

$$2(UV + VU)x_j = Px_j \tag{3}$$

Since we know x_j is an eigenvector for U we can write:

$$(UV + VU)x_j = U(Vx_j) + \lambda_j V x_j = (U + \lambda_j I)Vx_j \tag{4}$$

From condition 1, we know that $U + \lambda_j I$ is invertible for all j, so we can write:

$$2Vx_j = (U + \lambda_j I)^{-1} P x_j \tag{5}$$

From here, let's denote $y_j = (U + \lambda_j I)^{-1} P x_j$ then for $X = [x_1|x_2|...|X_N]$ and $Y = [y_1|y_2|...|y_n]$ we have $2VX = Y$ so we find:

$$V = \frac{1}{2} Y X^{-1} \tag{6}$$

and V is unique.

Further since $M_n(\mathbb{Q})$ is a ring, we can start with an invertible matrix $X \in M_n(\mathbb{Q})$ and any diagonal matrix $\Lambda = diag[\lambda_1, \lambda_2, ...\lambda_n] \in M_n(\mathbb{Q})$ satisfying our given condition 1 and construct:

$$U = X\Lambda X^{-1} \tag{7}$$

Then we can find V using (7):

$$V = \frac{1}{2} Y X^{-1}$$

And $V \in M_n(\mathbb{Q})$ so we can take $C = U + V$ and $A = U - V$. And we can use these values.

Theorem

In the article written by Arnold and Eydelzon the methodology explained above leads to the following theorem.
Theorem: For any nxn matrix with rational entries $P \in M_n(\mathbb{Q})$, there exists an n^2 - parametric family of matrices A and C from $M_n(\mathbb{Q})$ such that $P = C^2 - A^2$.
Following equation provides with the proof of the theorem. The square of matrices U and V holds the following identity:

$$(U - V)^2 + 2UV + 2VU = (U + V)^2 \tag{8}$$

Therefore, P can be written as 2(UV+VU) and as well as $(U + V)^2 - (U - V)^2$.
According to the conditions, the matrices U and V have to be Non Commutable.This theorem can be proved by the methodology above and produces the following example.

Example

Let's begin with $B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ then we have $B^2 = \begin{bmatrix} 7 & 10 \\ 15 & 22 \end{bmatrix}$

Now we choose a Λ that follows our given condition (1a). Say $\Lambda = \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix}$. From here we create two integer-valued eigenvectors that satisfy (1b), $x_1 = (1, 1)$ and $x_2 = (-1, 1)$ so we can form the matrix $X = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$. Since $U = X\lambda X^{-1}$ we find that $U = \frac{1}{2}\begin{bmatrix} 1 & -3 \\ -3 & 1 \end{bmatrix}$. Then we find the vectors $y_1 = \frac{1}{2}(-47, -7)$ and $y_2 = \frac{1}{2}(9, 11)$ and we use these to form $Y = \frac{1}{2}\begin{bmatrix} -47 & 9 \\ -7 & 11 \end{bmatrix}$. From here we find that $V = \frac{1}{4}\begin{bmatrix} -28 & -19 \\ -9 & 2 \end{bmatrix}$ We can see that U and V have rational entries so we can multiply by the least common multiple so the entries will be integers. Therefore we get the triple:

$$\begin{bmatrix} 30 & 13 \\ 3 & 0 \end{bmatrix}^2 + \begin{bmatrix} 4 & 8 \\ 12 & 16 \end{bmatrix}^2 = \begin{bmatrix} -26 & -25 \\ -15 & 4 \end{bmatrix}^2$$

Afterword

- One naturally ask the question if we can generalize equation (2) for any positive natural number. The paper [2] shows that certain permutation matrices satisfy the generalized form of our question.
- In this project we focused on finding a suitable definition for a solution to be trivial for equation (2). We quickly came to the realization that nilpotent and idempotent matrices must be included in this definition, but it is our conviction that there are other families of matrices that should be included as well.
- We know that the construction provided for non commutable matrices does not encompass all elements of $M_n(\mathbb{Z})$ but other methods can be further investigated.

References

[1] Maxim Arnold, Anatoly Eydelzon.2019.
On Matrix Pythagorean Triples,
The American Mathematical Monthly, 126:2, 158-160
[2] Paulo Ribenboim, 1979.
13 Lectures on Fermat's Last Theorem, 275-277.