RAMReS Sciences des Structures et de la Matière Vol. 9, N°1 (2025) 86 - 105
http://publication.lecames.org/index.php/mat ISSN: 2630-1180

On congruent circulant matrices

V. Kouassi Kouakou[1,*], F. Emmanuel Tanoé[2], P. Kouadio Kimou[3]

[1]*Applied Fondamental Sciences Department Nangui ABROGOUA University, Abidjan, 02 BP 801 ABIBDJAN 02, Côte d'Ivoire*
[2]*Mathematics and Computer Sciences Department, Félix Houphouët Boigny University, Abidjan, 22 BP 1102 ABIDJAN 22, Côte d'Ivoire*
[3]*Laboratoire d'Informatique et de Télécommunications, Institut National Polytechnique Felix Houphouët BOIGNY, BP 1093 Yamoussoukro Côte d'Ivoire*

Received: 13 March 2025 / Received in revised form: 10 June 2025 / Accepted: 24 June 2025

***Abstract*:**
In this work, we investigate congruent circulant matrices and provide a parametrization of congruent matrices in $M_2(\mathbb{Q})$. We introduce a matrix analogue of Fermat's algorithm, which enables the construction of sequences of matrix Pythagorean triples associated with a given 2×2 congruent circulant matrix N. Furthermore, we establish a matrix version of Pythagoras' theorem within the Euclidean vector space $M_m(\mathbb{Q})$; $m \geq 2$.
Mathematics Subject Classification (MSC2020). 11C20, 15A15, 15A18, 15A20, 15A27, 15A60, 11D72.

***Keywords*:** Congruent numbers; Pythagorean triples; Congruent circulant matrix; Matrix Pythagorean triples; Eigenvalues.

1 Introduction

The congruent number problem is a classical unsolved question with origins dating back several centuries. As noted by Coates [1]: "*The congruent number problem, the written history of which can be traced back at least a millennium, and is the oldest unsolved major problem in number theory, and perhaps in the whole of mathematics.*" A natural number is called a congruent number if it can be realized as the area of a right triangle with rational side lengths. Recall that a right (or right-angled) triangle is a triangle in which one of the angles is a right angle. If all three side lengths are integers, the triangle is referred to as a Pythagorean triangle, whereas if all side lengths are rational numbers, it is called a rational

* Corresponding author:
Email address: *kouakouassivincent@gmail.com (V.K. Kouakou)*
https://doi.org/10.70974/mat09125086

triangle. For example: $\frac{3}{2}, \frac{20}{3}, \frac{49}{12}$ are the rational numbers identified by Fibonacci, and the triple $\left(\frac{3}{2}, \frac{20}{3}, \frac{49}{12}\right)$ represents a right triangle with area 5 showing that 5 is a congruent number. While every rational right triangle has a rational area, the converse is not true; for instance, there is no rational right triangle with area 1. Formally, a positive square-free integer n, is called a congruent number if there exits a rational right-angled triangle with area n. It means that there exist rational numbers $a, b, c > 0$, such that

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = n. \end{cases}$$

Equivalently, the problem can be stated as the existence of a right-angled triangle with positive rational sides $a, b, c > 0$, satisfying:

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = nd^2 \end{cases}, \ d \in \mathbb{Q}_+^*.$$

In mathematics, and in number theory in particular, it is common to encounter problems that are straightforward to state yet whose resolution requires deep and highly sophisticated techniques. The history of congruent numbers is discussed in [2], which notes that an Arab manuscript referred to the study of congruent numbers as the "principal object of the theory of rational right triangles". The Congruent Number Problem is to find an algorithm to determine whether a given natural number is congruent or not.

"*Mille ans de chasse aux nombres congruents*" is the title of Cuculière's article [3]. This title shows that the problem of congruent numbers dates back a long time. Congruent numbers have been the subject of several seminars [1, 3, 4, 6, 7], master thesis [8] and papers [9–12]. Keuméan and Tanoé [13] gave a nice new method to characterize the fact that an integer n is congruent, by using the notion of Pythagorean divisors. In 2022, Mouanda, Tsiba and Kangni [14] built sequences of triples of the set of circulant square matrices of order m, with positive integers as entries $Circ_m(\mathbb{N})$, which are solutions of the equation:

$$A^2 + B^2 = C^2, ABC \neq 0.$$

They introduced Mouanda's choice function for matrices which allows them to build galaxies of sequences of circulant matrix Pythagorean triples with positive integers as entries. Recently [15], they developed an algorithm that allows to build the sequences of matrix Pythagorean triples of any size. In analogy with congruent numbers, we may define a circulant matrix N to be a congruent matrix if there exists a circulant Pythagorean triple (A, B, C) and, an invertible matrix $P \in M_m(\mathbb{Q})$ such that

$$\begin{cases} A^2 + B^2 = C^2 \\ \frac{1}{2}AB = P^2N. \end{cases}$$

The problem of circulant congruent circulant matrices is the matrix version of the congruent numbers problem mentioned above.

The importance of congruent numbers is no longer in doubt in cryptography. Circulant matrices also play an important role in cryptography, where we use the circulant matrices in the Mix-Columns step of the Advanced Encryption Standard.

In this paper, we investigate congruent

circulant matrices. In particular, we characterize all the 2×2-congruent circulant matrices and we introduce the matrix version of the Pythagoras' Theorem in the Euclidean vector space $M_m(\mathbb{Q})$. We also give the matrix version of Fermat's Algorithm which allows us to build sequences of circulant matrix Pythagorean triples, for a given congruent circulant matrix N. For the sake of completeness and to facilitate an independent reading of this article, we begin by presenting some definitions and preliminary results. We commence our results by constructing a fundamental family of congruent circulant matrix Pythagorean triples $M_m(\mathbb{Q}), m \geq 2$.

2 Preliminaries

For the entirety of this paper, let $m \geq 2$, $be a positive integer, and let (M_m(\mathbb{Q}), \langle - \mid - \rangle)$ denote the space of $m \times m$-matrices with rationals as entries, endowed with the canonical scalar product defined as follows:

$$\begin{array}{rccc} \langle - \mid - \rangle : & M_m(\mathbb{Q}) \times M_m(\mathbb{Q}) & \longrightarrow & \mathbb{Q} \\ & (M, N) & \longmapsto & tr(M^T N). \end{array}$$

Let us recall some basic notions of circulant matrices. For fundamental notions on circulant matrices, we cite the following complete general references [16–18].

2.1 On Circulant Matrices

Definition 2.1. *A circulant matrix is a square of order m where each row is a cycle right shift of the previous one. Given a vector line:*

$$C = (c_1, \ c_2, \ \ldots, \ c_m),$$

the circulant matrix noted: $C = circ\ (c_1, \ c_2, \ \ldots, \ c_m)$, *is:*

$$C = \begin{pmatrix} c_1 & c_2 & \ldots & c_m \\ c_m & c_1 & \ldots & c_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \ldots & c_1 \end{pmatrix}.$$

Properties 2.1. *1. If* $C = circ\ (c_1, \ c_2, \ \ldots, \ c_m)$ *is a circulant matrix, then it is diagonalizable by the Discrete Fourier Transform. More precisely we have:*

$$C = F^{-1} diag(\lambda_1, \lambda_2, ..., \lambda_m) F,$$

where F is the Fourier matrix and $(\lambda_i)_i$ is the family of the eigenvalues of C. By a Fourier matrix of order m, we shall understand the matrix defined as follows:

$$F = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega^{1.1} & \omega^{2.1} & \ldots & \omega^{(m-1).1} \\ 1 & \omega^{1.2} & \omega^{2.2} & \ldots & \omega^{(m-1).2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{1.(m-1)} & \omega^{2.(m-1)} & \ldots & \omega^{(m-1)(m-1)} \end{pmatrix}$$

with

$$\omega = e^{\frac{2\pi}{m} i} = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}, \ i = \sqrt{-1}.$$

$$m = 2, F = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$m = 4, F = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \end{pmatrix}.$$

2. The $Circ_m(\mathbb{C})$ of $m \times m$-complex circulant matrices is a commutative algebra. In particular, circulant matrices commute with each other.

3. The eigenvalues of circulant matrices are given by the first row. The eigenvalues λ_k of the circulant matrix

$C = circ\ (c_1,\ \ c_2,\ \ ...,\ \ c_m)$ *are:*

$$\lambda_k = \sum_{j=0}^{m} c_j \omega_n^{(jk)},$$

where $\omega_n = \exp(-\frac{2\pi}{n}i)$ *is the primitive n-th root of unity. These are exactly the row of the matrix.*

4. *Each circulant* $C = circ\ (c_0,\ \ c_2,\ \ ...,\ \ c_m)$ *corresponds to the polynomial:*

$$P(X) = c_0 + c_1 X + ... + c_m X^m.$$

It is possible to write the matrix C *as one variable complex polynomial. Indeed, let* P *be the cyclic permutation* m *matrix given by:*

$$P = \begin{pmatrix} 0 & 1 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & ... & 0 & 0 & 1 \\ 1 & 0 & ... & 0 & 0 & 0 \end{pmatrix}.$$

It is simple to see that

$$C = \sum_{k=0}^{m-1} c_k P_k$$

2.2 On Congruent Circulant Matrix Pythagorean Triples

Definition 2.2. *1.* ***A circulant matrix Pythagorean triple*** *is a circulant matrix triple* $(A, B, C) \in (M_m(\mathbb{Q}))^3$ *such that*

$$A^2 + B^2 = C^2 : ABC \neq 0.$$

2. *Let* $A, B \in (M_m(\mathbb{Q}), \langle - \mid - \rangle)$*, we say that* A *and* B *are orthogonal and we note* $A \perp B$ *if and only if* $\langle A \mid B \rangle = tr(A^T B) = 0$.

3. *When* (A, B, C) *is a circulant matrix Pythagorean triple such that* $A \perp B$*, we say that* (A, B, C) *is a right-angled matrix triangle.*

From the second characterization of congruent numbers in the introduction, we deduce the following matrix version definitions.

Definition 2.3. *1.* ***Congruent circulant matrix***
A circulant matrix $N \in M_m(\mathbb{Q}), m \geq 2$ *is a* ***congruent circulant matrix*** *if there exists a circulant matrix Pythagorean triple* (A, B, C) *and an invertible matrix* $P \in M_m(\mathbb{Q})$ *(said to be* ***associated to*** N*) such that*

$$\begin{cases} A^2 + B^2 = C^2 \\ \frac{1}{2}AB = P^2 N. \end{cases} \quad (1)$$

2. *Let* $N \in M_m(\mathbb{Q}), m \geq 2$*, be a fixed congruent circulant matrix. Then the circulant matrix Pythagorean triple* (A, B, C) *is called a* ***circulant matrix Pythagorean*** N***-triple****, if* (2.1) *holds for the matrix* N.
That is if (A', B', C') *is an other circulant matrix triple such that* (1) *holds, then* (A', B', C') *is also a circulant matrix Pythagorean* N*-triple.*

3. *Let* N *be a fixed congruent circulant matrix of* $M_m(\mathbb{Q})$*, then we define the set:*

$$\mathcal{P}_T(N) = \Big\{(A, B, C) \in Circ_m(\mathbb{Q})^3 :$$

$$\left\{ \begin{array}{l} A^2+B^2=C^2 \\ \frac{1}{2}AB=P^2N \end{array} \right\} \subset (M_m(\mathbb{Q}))^3.$$

4. *In the point* 3.(*b*) *of Theorem* 3.4 *below, the circulant matrix:* $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *is called a* ***strict congruent circulant matrix****.*

Remarks 2.1. *a) Note that for a circulant matrix Pythagorean N-triple* (A,B,C) *in* $M_m(\mathbb{Q})$*, we have:* $AB=BA$ *and* $P^2N=NP^2$*.*

b) Denote that $\overline{N}=\mathcal{P}_T(N)$*, is the equivalence class of* N *defined in the set of matrix Pythagorean triples by:* $(A,B,C)\underset{\overline{N}}{\simeq}(A',B',C') \Longleftrightarrow \frac{1}{2}AB=P^2N=\frac{1}{2}A'B'$.

Such congruent circulant matrix Pythagorean triples exist and can be built from a congruent number $n\in\mathbb{N}$. In the following section, we give the results, followed by their proof and possible examples. Calculations (in particular for the matrices: eigenvalues, products, ..., formal calculations) were done with the calculation software Scientific_Workplace_pro5.5 [20].

3 Main Results

3.1 Construction of a trivial family of $\mathcal{P}_T(N)\subset M_m(\mathbb{Q})^3$, $m\geq 2$

We know how to get congruent numbers and Pythagorean triples (see in [4, 6, 7]) which allow us to establish the following theorem.

Theorem 3.1. *Let* $n\in\mathbb{N}^*$ *be a congruent number,* (a,b,c) *be a positive rational Pythagorean triple and* $d\in\mathbb{Q}_+^*$ *such that*

$$\left\{ \begin{array}{l} a^2+b^2=c^2 \\ \frac{1}{2}ab=nd^2. \end{array} \right.$$

For $m\geq 2$*, let* $\left(A=\begin{pmatrix} a & \dots & a \\ \vdots & \ddots & \vdots \\ a & \dots & a \end{pmatrix}, \right.$
$B=\begin{pmatrix} b & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & b \end{pmatrix}, C=\left.\begin{pmatrix} c & \dots & c \\ \vdots & \ddots & \vdots \\ c & \dots & c \end{pmatrix}\right)$
be a circulant matrix triple. Then:

1. *The circulant matrix triple* (A,B,C) *is a circulant matrix Pythagorean triple i.e.* $A^2+B^2=C^2$, $ABC\neq 0$.
2. *There exists an invertible matrix* $P\in M_m(\mathbb{Q})$ *and a congruent circulant matrix* N *such that*

$$\left\{ \begin{array}{l} A^2+B^2=C^2 \\ \frac{1}{2}AB=P^2N, \end{array} \right.$$

with: $P=\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ nd^2 & 0 & \dots & 0 & 0 \end{pmatrix}$, *and*

$$N=mP^{m-2}\times \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & \ddots & 1 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & 1 & \ddots & \ddots & 1 \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix} \in M_m(\mathbb{Q}),$$

and

$$P^{m-2}=\begin{pmatrix} 0 & \dots & \dots & 0 & 1 & 0 \\ 0 & \dots & \dots & 0 & 0 & 1 \\ nd^2 & 0 & \dots & 0 & 0 & 0 \\ 0 & nd^2 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & nd^2 & 0 & 0 \end{pmatrix}$$

in which the " nd^2*-diagonal" begins at the third line.*

3. *The matrices A and B are not orthogonal.*

4. *Moreover we have the following* ***Pythagoras' Theorem matrix version***.

$$\|A\|^2 + \|B\|^2 = \|C\|^2.$$

Proof: Let consider the Euclidean vector space $(M_m(\mathbb{R}), \langle - \mid - \rangle)$, (a, b, c) be a positive rational Pythagorean triple, a congruent number $n \in \mathbb{N}^*$ and $d \in \mathbb{Q}_+^*$, such that

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = nd^2. \end{cases}$$

Consider the circulant matrices:

$$A = \begin{pmatrix} a & \dots & a \\ \vdots & \ddots & \vdots \\ a & \dots & a \end{pmatrix}, B = \begin{pmatrix} b & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & b \end{pmatrix},$$

$$C = \begin{pmatrix} c & \dots & c \\ \vdots & \ddots & \vdots \\ c & \dots & c \end{pmatrix}.$$

By simple calculations, we have:

$A^2 + B^2 = C^2$. In fact:

$$A^2 = \begin{pmatrix} a & \dots & a \\ \vdots & \ddots & \vdots \\ a & \dots & a \end{pmatrix}^2 = \begin{pmatrix} ma^2 & \dots & ma^2 \\ \vdots & \ddots & \vdots \\ ma^2 & \dots & ma^2 \end{pmatrix},$$

$$B^2 = \begin{pmatrix} b & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & b \end{pmatrix}^2 = \begin{pmatrix} mb^2 & \dots & mb^2 \\ \vdots & \ddots & \vdots \\ mb^2 & \dots & mb^2 \end{pmatrix},$$

$$C^2 = \begin{pmatrix} c & \dots & c \\ \vdots & \ddots & \vdots \\ c & \dots & c \end{pmatrix}^2 = \begin{pmatrix} mc^2 & \dots & mc^2 \\ \vdots & \ddots & \vdots \\ mc^2 & \dots & mc^2 \end{pmatrix},$$

and

$$A^2+B^2 = \begin{pmatrix} m(a^2+b^2) & \dots & m(a^2+b^2) \\ \vdots & \ddots & \vdots \\ m(a^2+b^2) & \dots & m(a^2+b^2) \end{pmatrix}$$

$$= \begin{pmatrix} mc^2 & \dots & mc^2 \\ \vdots & \ddots & \vdots \\ mc^2 & \dots & mc^2 \end{pmatrix} = C^2.$$

Then $\left(\begin{pmatrix} a & \dots & a \\ \vdots & \ddots & \vdots \\ a & \dots & a \end{pmatrix}, \begin{pmatrix} b & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & b \end{pmatrix}, \begin{pmatrix} c & \dots & c \\ \vdots & \ddots & \vdots \\ c & \dots & c \end{pmatrix} \right)$ is a circulant matrix Pythagorean triple as announced in 1. For the second point of the Theorem, we have:

$$\frac{1}{2}AB = \frac{1}{2}\begin{pmatrix} a & \dots & a \\ \vdots & \ddots & \vdots \\ a & \dots & a \end{pmatrix} \times \begin{pmatrix} b & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & b \end{pmatrix}$$

$$= m\begin{pmatrix} \frac{1}{2}ab & \dots & \frac{1}{2}ab \\ \vdots & \ddots & \vdots \\ \frac{1}{2}ab & \dots & \frac{1}{2}ab \end{pmatrix} = m\begin{pmatrix} nd^2 & \dots & nd^2 \\ \vdots & \ddots & \vdots \\ nd^2 & \dots & nd^2 \end{pmatrix}.$$

Taking, $P = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & & 1 \\ nd^2 & 0 & \dots & 0 & 0 \end{pmatrix}$,

we have: $P^m = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & & 1 \\ nd^2 & 0 & \dots & 0 & 0 \end{pmatrix}^m$

$$= \begin{pmatrix} nd^2 & 0 & \dots & 0 \\ 0 & nd^2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & nd^2 \end{pmatrix},$$

and

$$\begin{pmatrix} nd^2 & 0 & \dots & 0 \\ 0 & nd^2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & nd^2 \end{pmatrix} \times m\begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$$

$$= m\begin{pmatrix} nd^2 & \dots & nd^2 \\ \vdots & \ddots & \vdots \\ nd^2 & \dots & nd^2 \end{pmatrix} = m\begin{pmatrix} \frac{1}{2}ab & \dots & \frac{1}{2}ab \\ \vdots & \ddots & \vdots \\ \frac{1}{2}ab & \dots & \frac{1}{2}ab \end{pmatrix}.$$

So that,

$$\frac{1}{2}AB = \begin{pmatrix} nd^2 & 0 & \dots & 0 \\ 0 & nd^2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & nd^2 \end{pmatrix} = P^m \times m \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$$

$$\frac{1}{2}AB = P^2 \times \underbrace{mP^{m-2} \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}}_{\begin{array}{c} \| \\ N \end{array}} = P^2 N.$$

• We have: $\left\langle \begin{pmatrix} a & \dots & a \\ \vdots & \ddots & \vdots \\ a & \dots & a \end{pmatrix} \mid \begin{pmatrix} b & \dots & b \\ \vdots & \ddots & \vdots \\ b & \dots & b \end{pmatrix} \right\rangle$

$= tr(A^T B) = tr(AB) = tr\left(\begin{pmatrix} ab & \dots & ab \\ \vdots & \ddots & \vdots \\ ab & \dots & ab \end{pmatrix}\right)$

$= mab \neq 0$, so the vectors A and B are not perpendicular.

• Since the matrices A, B and C are symmetric, we have:

$\|A\|^2 = tr(A^T A) = tr(A^2)$,
$\|B\|^2 = tr(B^T B) = tr(B^2)$,
$\|C\|^2 = tr(C^T C) = tr(C^2)$.

In other words, we have:

$\|A\|^2 + \|B\|^2 = tr(A^2 + B^2) = tr(C^2)$
$= tr(A^2) + tr(B^2) = \|C\|^2$.

3.2 Construction of the elements of $\mathcal{P}_T(N) \subset M_2(\mathbb{Q})^3$

In this section, we characterize all the congruent circulant matrix of the set $M_2(\mathbb{Q})$.

Lemma 3.1. *Let the matrix* $A = \begin{pmatrix} a & a' \\ a' & a \end{pmatrix} \in M_2(\mathbb{Q})$ *be a circulant matrix. Then A is diagonalizable in $\mathbb{Q}$. More precisely, the set of the eigenvalues of the matrix A is $\{\lambda_{A,1} = a+a', \lambda_{A,2} = a-a'\}$.*

Proof: Since the rational matrix $A = \begin{pmatrix} a & a' \\ a' & a \end{pmatrix}$ is a circulant, it is diagonalizable. Suppose that $\lambda_{A,1}, \lambda_{A,2}$ are the eigenvalues of the matrix A. Then, with the polynomial characteristic:
$P_A(X) = X^2 - 2aX + a^2 - a'^2$, we have the system $\begin{cases} \lambda_{A,1} = a + a' \in \mathbb{Q} \\ \lambda_{A,2} = a - a' \in \mathbb{Q}. \end{cases}$
Then we determine quickly the eigenvalues of the matrix A as follow:

$$A = \begin{pmatrix} a & a' \\ a' & a \end{pmatrix} = \begin{pmatrix} \frac{\lambda_{A,1} + \lambda_{A,2}}{2} & \frac{\lambda_{A,1} - \lambda_{A,2}}{2} \\ \frac{\lambda_{A,1} - \lambda_{A,2}}{2} & \frac{\lambda_{A,1} + \lambda_{A,2}}{2} \end{pmatrix} \quad (2)$$

Remarks 3.1. *1. In $M_2(\mathbb{Q})$, circulant matrices are symmetric (that is $A^T = A$) and are of the form:*

$$\begin{pmatrix} a & a' \\ a' & a \end{pmatrix}.$$

2. The unit matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a congruent one. We will just have to choose $\lambda_{A,1}\lambda_{B,1} = \lambda_{A,2}\lambda_{B,2}$.

Note that the second point of Remarks 3.1 is fundamental for our proofs. In fact, the matrices symmetric property ($A^T = A$) of the 2×2-circulant matrices allows 2-2-circulant matrix Pythagorean triples to verify the matrix version of Pythagoras' Theorem.

Theorem 3.2. ***Parametrization of*** 2×2-***congruent circulant matrices***

The following assertions are equivalent.

1. *The circulant matrix $N \in M_2(\mathbb{Q})$ is a congruent circulant matrix.*

2. *There exists a circulant matrix Pythagorean triple (A, B, C) of the type:*

$$\left(\begin{pmatrix} a & a' \\ a' & a \end{pmatrix}, \begin{pmatrix} b & b' \\ b' & b \end{pmatrix}, \begin{pmatrix} c & c' \\ c' & c \end{pmatrix}\right)$$

such that $\begin{cases} A^2 + B^2 = C^2 \\ \frac{1}{2}AB = P^2N \end{cases}$, *with an invertible matrix $P \in M_2(\mathbb{Q})$.*

3. *There exists $\lambda_{A,1}, \lambda_{A,2}, \lambda_{B,1}, \lambda_{B,2} \in \mathbb{Q}$ such that $\lambda_{A,1}^2 + \lambda_{B,1}^2$ and $\lambda_{A,2}^2 + \lambda_{B,2}^2$ are non-zero squares in $\mathbb{Q}$, and we have the following two cases:*
   3.*a. If $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} \neq 0$, then the congruent circulant matrix N is of the type:*
   $$N = \begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} \\ \frac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}.$$
   3.*b. If $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} = 0$, then the congruent circulant matrix N is:*
   $$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof: $\boxed{1. \Longrightarrow 2.}$ Let us suppose that the circulant matrix $N \in M_2(\mathbb{Q})$ is congruent. Then by the first point of Definition 2.3, there exists a circulant matrix Pythagorean triple $(A, B, C) \in Circ_2(\mathbb{Q}) \subset M_2(\mathbb{Q})$ such that (1) holds for the matrix N. Since A, B, C are circulant matrices, the first observation of Remark 3.1, allows us to take the matrices of the form:

$$\left(\begin{pmatrix} a & a' \\ a' & a \end{pmatrix}, \begin{pmatrix} b & b' \\ b' & b \end{pmatrix}, \begin{pmatrix} c & c' \\ c' & c \end{pmatrix}\right).$$

$\boxed{2. \Longrightarrow 3.}$ Let the matrix $\left(A = \begin{pmatrix} a & a' \\ a' & a \end{pmatrix}, B = \begin{pmatrix} b & b' \\ b' & b \end{pmatrix}, C = \begin{pmatrix} c & c' \\ c' & c \end{pmatrix}\right) \in M_2(\mathbb{Q})^3$, be a matrix Pythagorean triple and denote by $\{\lambda_{A,1}, \lambda_{A,2}\}$ and $\{\lambda_{B,1}, \lambda_{B,2}\}$ the set of the eigenvalues of A and B, respectively. By the relation (2), we have:

$$A = \begin{pmatrix} \frac{\lambda_{A,1} + \lambda_{A,2}}{2} & \frac{\lambda_{A,1} - \lambda_{A,2}}{2} \\ \frac{\lambda_{A,1} - \lambda_{A,2}}{2} & \frac{\lambda_{A,1} + \lambda_{A,2}}{2} \end{pmatrix}$$

$$B = \begin{pmatrix} \frac{\lambda_{B,1} + \lambda_{B,2}}{2} & \frac{\lambda_{B,1} - \lambda_{B,2}}{2} \\ \frac{\lambda_{B,1} - \lambda_{B,2}}{2} & \frac{\lambda_{B,1} + \lambda_{B,2}}{2} \end{pmatrix}.$$

Let us show that $\lambda_{A,1}^2 + \lambda_{B,1}^2$ and $\lambda_{A,2}^2 + \lambda_{B,2}^2$ are non-zero squares.

We have:

$$A^2 + B^2 = \begin{pmatrix} \frac{\lambda_{A,1}^2 + \lambda_{B,1}^2 + \lambda_{A,2}^2 + \lambda_{B,2}^2}{2} & \frac{\lambda_{A,1}^2 - \lambda_{A,2}^2 + \lambda_{B,1}^2 - \lambda_{B,2}^2}{2} \\ \frac{\lambda_{A,1}^2 - \lambda_{A,2}^2 + \lambda_{B,1}^2 - \lambda_{B,2}^2}{2} & \frac{\lambda_{A,1}^2 + \lambda_{B,1}^2 + \lambda_{A,2}^2 + \lambda_{B,2}^2}{2} \end{pmatrix}.$$

Then $A^2 + B^2 = C^2$, if and only if

$$\begin{pmatrix} \frac{\lambda_{A,1}^2 + \lambda_{B,1}^2 + \lambda_{A,2}^2 + \lambda_{B,2}^2}{2} & \frac{\lambda_{A,1}^2 - \lambda_{A,2}^2 + \lambda_{B,1}^2 - \lambda_{B,2}^2}{2} \\ \frac{\lambda_{A,1}^2 - \lambda_{A,2}^2 + \lambda_{B,1}^2 - \lambda_{B,2}^2}{2} & \frac{\lambda_{A,1}^2 + \lambda_{B,1}^2 + \lambda_{A,2}^2 + \lambda_{B,2}^2}{2} \end{pmatrix}$$

$$= \begin{pmatrix} c & c' \\ c' & c \end{pmatrix}^2$$

$$= \begin{pmatrix} c^2 + c'^2 & 2cc' \\ 2cc' & c^2 + c'^2 \end{pmatrix}.$$

So we have:

$$\begin{cases} 2(c^2+c'^2) = \lambda_{A,1}^2+\lambda_{B,1}^2+\lambda_{A,2}^2+\lambda_{B,2}^2 \quad (i) \\ \\ 2(2cc') = \lambda_{A,1}^2-\lambda_{A,2}^2+\lambda_{B,1}^2-\lambda_{B,2}^2 \quad (ii) \end{cases}$$

$$\begin{cases} (i)+(ii): \quad (c+c')^2 = \lambda_{A,1}^2+\lambda_{B,1}^2 \in \mathbb{Q}^2 \\ \\ (i)-(ii): \quad (c-c')^2 = \lambda_{A,2}^2+\lambda_{B,2}^2 \in \mathbb{Q}^2 \end{cases}. \tag{3}$$

Now let consider the following two cases.
(a) If $\lambda_{A1}\lambda_{B1}+\lambda_{A2}\lambda_{B2} \neq 0$, then

$$\frac{1}{2}AB = \frac{1}{4}\begin{pmatrix} \lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} & 0 \\ \\ 0 & \lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} \end{pmatrix}$$

$$\times \begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} \\ \\ \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix} 0 & 1 \\ \\ \lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} & 0 \end{pmatrix}^2$$

$$\times \begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} \\ \\ \frac{\lambda_{A1}\lambda_{B1}-\lambda_{A2}\lambda_{B2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}.$$

Putting $P = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ \\ \lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} & 0 \end{pmatrix}$ and

$$N = \begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} \\ \\ \frac{\lambda_{A1}\lambda_{B1}-\lambda_{A2}\lambda_{B2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix},$$

we have the result.

(b) If $\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} = 0$, then $\lambda_{A,1}\lambda_{B,1} = -\lambda_{A,2}\lambda_{B,2} \neq 0$ (since $\lambda_{A,1}^2+\lambda_{B,1}^2$ and $\lambda_{A,2}^2+\lambda_{B,2}^2$ are non-zero squares). So we have:

$$\begin{aligned} \frac{1}{2}AB &= \begin{pmatrix} \frac{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}}{4} & \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{4} \\ \\ \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{4} & \frac{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}}{4} \end{pmatrix} \\ &= \begin{pmatrix} 0 & \frac{1}{2}\lambda_{A,1}\lambda_{B,1} \\ \\ \frac{1}{2}\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix} \\ &= \left[\frac{1}{2}\begin{pmatrix} 0 & 1 \\ 2\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix}\right]^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned}$$

Putting $P = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 2\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix}$ and $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we have the result.

3. $\Longrightarrow$ 1. Suppose that there exists $\lambda_{A,1}, \lambda_{A,2}, \lambda_{B,1}, \lambda_{B,2} \in \mathbb{Q}$, such that $\lambda_{A,1}^2+\lambda_{B,1}^2$ and $\lambda_{A,2}^2+\lambda_{B,2}^2$ are rational squares and

(a) N= $\begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} \\ \\ \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}$

if $\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} \neq 0$

or

(b) $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

if $\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2} = 0$.

Let us build a rational matrix Pythagorean triple $\left(A, B, C = \begin{pmatrix} c & c' \\ c' & c \end{pmatrix}\right)$ of $M_2(\mathbb{Q})$ such that relation (1) holds for the matrix N.

Let put $A = \begin{pmatrix} \frac{\lambda_{A,1}+\lambda_{A,2}}{2} & \frac{\lambda_{A,1}-\lambda_{A,2}}{2} \\ \\ \frac{\lambda_{A,1}-\lambda_{A,2}}{2} & \frac{\lambda_{A,1}+\lambda_{A,2}}{2} \end{pmatrix}$,

and $B = \begin{pmatrix} \frac{\lambda_{B,1}+\lambda_{B,2}}{2} & \frac{\lambda_{B,1}-\lambda_{B,2}}{2} \\ \\ \frac{\lambda_{B,1}-\lambda_{B,2}}{2} & \frac{\lambda_{B,1}+\lambda_{B,2}}{2} \end{pmatrix}$.

It is clear by the relation (2) that

$\{\lambda_{A,1}, \lambda_{A,2}\}$ and $\{\lambda_{B,1}, \lambda_{B,2}\}$ are the sets of eigenvalues of the circulant matrices A and B, respectively. (a) If $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} \neq 0$, then we have by the hypothesis, $\begin{cases} \alpha^2 = \lambda_{A,1}^2 + \lambda_{B,1}^2 \in \mathbb{Q}^2 \\ \\ \beta^2 = \lambda_{A,2}^2 + \lambda_{B,2}^2 \in \mathbb{Q}^2 \end{cases}$

$$\Longrightarrow \begin{cases} \alpha = \pm\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} \\ \\ \beta = \pm\sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2} \end{cases}.$$

Obviously $\begin{cases} c = \dfrac{\alpha+\beta}{2} \\ \\ c' = \dfrac{\alpha-\beta}{2} \end{cases}$ agrees.

So, $(c,c') \in \left\{ \left(\dfrac{\pm\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} \pm \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}}{2}, \dfrac{\pm\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} \mp \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}}{2} \right) \right\}$,

such that

$$\frac{1}{2}AB = \frac{1}{4}\begin{pmatrix} 0 & 1 \\ \\ \lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} & 0 \end{pmatrix}^2 \times \begin{pmatrix} 1 & \dfrac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} \\ \\ \dfrac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}$$

$$= P^2 N.$$

So that we have:

$$\text{N} = \begin{pmatrix} 1 & \dfrac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} \\ \\ \dfrac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}$$

which is a congruent rational circulant matrix with $P = \dfrac{1}{2}\begin{pmatrix} 0 & 1 \\ \lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} & 0 \end{pmatrix}$.

(b) If $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} = 0$, then we have by the hypothesis,

$$\begin{cases} \alpha^2 = \lambda_{A,1}^2 + \lambda_{B,1}^2 \\ \\ \beta^2 = \lambda_{A,2}^2 + \lambda_{B,2}^2 \end{cases}.$$

Then we get,

$(c,c') \in \left\{ \left(\pm\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} \pm \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}, \pm\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} \mp \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2} \right) \right\}$
as in the previous situation.

Since $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} = 0$, we have: $\lambda_{A,1}\lambda_{B,1} = -\lambda_{A,2}\lambda_{B,2} \neq 0$ (since $\lambda_{A,1}^2 + \lambda_{B,1}^2$ and $\lambda_{A,2}^2 + \lambda_{B,2}^2$ are non-zero rational squares), and

$$\frac{1}{2}AB = \frac{1}{2}\begin{pmatrix} \dfrac{\lambda_{A,1}}{\lambda_{B,2}}(\lambda_{B,2} - \lambda_{B,1}) & \dfrac{\lambda_{A,1}}{\lambda_{B,2}}(\lambda_{B,2} + \lambda_{B,1}) \\ \\ \dfrac{\lambda_{A,1}}{\lambda_{B,2}}(\lambda_{B,2} + \lambda_{B,1}) & \dfrac{\lambda_{A,1}}{\lambda_{B,2}}(\lambda_{B,2} - \lambda_{B,1}) \end{pmatrix} \times \begin{pmatrix} \dfrac{\lambda_{B,1}}{\lambda_{A,2}}(\lambda_{A,2} - \lambda_{A,1}) & \dfrac{\lambda_{B,1}}{\lambda_{A,2}}(\lambda_{A,2} + \lambda_{A,1}) \\ \\ \dfrac{\lambda_{B,1}}{\lambda_{A,2}}(\lambda_{A,2} + \lambda_{A,1}) & \dfrac{\lambda_{B,1}}{\lambda_{A,2}}(\lambda_{A,2} - \lambda_{A,1}) \end{pmatrix}$$

$$= \frac{\lambda_{A,1}}{\lambda_{A,2}}\frac{\lambda_{B,1}}{\lambda_{B,2}}\begin{pmatrix} \lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} & -2\lambda_{A,1}\lambda_{B,1} \\ \\ -2\lambda_{A,1}\lambda_{B,1} & \lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 2\lambda_{A,1}\lambda_{B,1} \\ 2\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix}$$

$$\frac{1}{2}AB = \frac{1}{4}\begin{pmatrix} 0 & 2\lambda_{A,1}\lambda_{B,1} \\ 2\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix} = \left[\frac{1}{2}\begin{pmatrix} 0 & 1 \\ 2\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix}\right]^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= P^2 N.$$

Then, for $P = \dfrac{1}{2}\begin{pmatrix} 0 & 1 \\ 2\lambda_{A,1}\lambda_{B,1} & 0 \end{pmatrix}$, we can conclude that: $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a congruent rational circulant matrix. Now, we can give some examples.

Example 3.1. *Let* $\{\lambda_{A,1}, \lambda_{A,2}\}$ *and* $\{\lambda_{B,1}, \lambda_{B,2}\}$ *be the sets of eigenvalues of*

the circulant rational matrices A and B, respectively. In the following, for $i = 1, 2$, the notation $\lambda_{\bullet,i}$ is a function of the matrix A or the matrix B.

1.

	A	B
$\lambda_{\bullet,1}$	6	8
$\lambda_{\bullet,2}$	4	3

Then, $\lambda_{A,1}^2 + \lambda_{B,1}^2 = (\pm 6)^2 + (\pm 8)^2 = 100$ *and* $\lambda_{A,2}^2 + \lambda_{B,2}^2 = (\pm 4)^2 + (\pm 3)^2 = 25$.

By the relation (2)*, we have:*

$$A = \begin{pmatrix} \frac{\lambda_{A,1} + \lambda_{A,2}}{2} & \frac{\lambda_{A,1} - \lambda_{A,2}}{2} \\ \frac{\lambda_{A,1} - \lambda_{A,2}}{2} & \frac{\lambda_{A,1} + \lambda_{A,2}}{2} \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix},$$

$$B = \begin{pmatrix} \frac{\lambda_{B,1} + \lambda_{B,2}}{2} & \frac{\lambda_{B,1} - \lambda_{B,2}}{2} \\ \frac{\lambda_{B,1} - \lambda_{B,2}}{2} & \frac{\lambda_{B,1} + \lambda_{B,2}}{2} \end{pmatrix} = \begin{pmatrix} \frac{11}{2} & \frac{5}{2} \\ \frac{5}{2} & \frac{11}{2} \end{pmatrix}.$$

For

$c = \frac{-\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} - \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}}{2} = \frac{-15}{2}$, *and*

$c' = \frac{-\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} + \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}}{2} = \frac{-5}{2}$, *we have:*

$$C = \begin{pmatrix} \frac{-15}{2} & \frac{-5}{2} \\ \frac{-5}{2} & \frac{-15}{2} \end{pmatrix}.$$

Let us show first that the circulant matrix triple (A, B, C) is a Pythagorean triple. A simple calculation gives:

$$\begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix}^2 + \begin{pmatrix} \frac{11}{2} & \frac{5}{2} \\ \frac{5}{2} & \frac{11}{2} \end{pmatrix}^2 = \begin{pmatrix} \frac{125}{2} & \frac{75}{2} \\ \frac{75}{2} & \frac{125}{2} \end{pmatrix} = \begin{pmatrix} \frac{-15}{2} & \frac{-5}{2} \\ \frac{-5}{2} & \frac{-15}{2} \end{pmatrix}^2.$$

So, $\left(\begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} \frac{11}{2} & \frac{5}{2} \\ \frac{5}{2} & \frac{11}{2} \end{pmatrix}, \begin{pmatrix} \frac{-15}{2} & \frac{-5}{2} \\ \frac{-5}{2} & \frac{-15}{2} \end{pmatrix} \right)$ *is a circulant matrix Pythagorean triple. And we have:*

$$\frac{1}{2}AB = \frac{1}{2}\begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} \frac{11}{2} & \frac{5}{2} \\ \frac{5}{2} & \frac{11}{2} \end{pmatrix} = \begin{pmatrix} 15 & 9 \\ 9 & 15 \end{pmatrix}.$$

Let us calculate P^2N, with

$$P = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ (6 \times 8) + (3 \times 4) & 0 \end{pmatrix},$$

and $N = \begin{pmatrix} 1 & \frac{(6 \times 8) - (3 \times 4)}{(6 \times 8) + (3 \times 4)} \\ \frac{(6 \times 8) - (3 \times 4)}{(6 \times 8) + (3 \times 4)} & 1 \end{pmatrix}$

$$P^2N = \frac{1}{4}\begin{pmatrix} 0 & 1 \\ 60 & 0 \end{pmatrix}^2 \begin{pmatrix} 1 & \frac{3}{5} \\ \frac{3}{5} & 1 \end{pmatrix} = \begin{pmatrix} 15 & 9 \\ 9 & 15 \end{pmatrix}.$$

We have: $\frac{1}{2}AB = P^2N$.

Note that $\langle A \mid B \rangle = tr(A^T B)$

$$= \left\langle \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix} \mid \begin{pmatrix} \frac{11}{2} & \frac{5}{2} \\ \frac{5}{2} & \frac{11}{2} \end{pmatrix} \right\rangle \neq 0,$$

so that the matrices A and B are not perpendicular. By the Pythagoras' Theorem (matrix version), we have:

$$\left\|\begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix}\right\|^2 + \left\|\begin{pmatrix} \frac{11}{2} & \frac{5}{2} \\ \frac{5}{2} & \frac{11}{2} \end{pmatrix}\right\|^2 = 125$$
$$= \left\|\begin{pmatrix} \frac{-15}{2} & \frac{-5}{2} \\ \frac{-5}{2} & \frac{-15}{2} \end{pmatrix}\right\|^2.$$

2. *Let consider:*

	A	B
$\lambda_{\bullet,1}$	18	-24
$\lambda_{\bullet,2}$	24	18

We have: $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} = 0$.

By the relation (2)*, we have:*

$$A = \begin{pmatrix} 21 & -3 \\ -3 & 21 \end{pmatrix}, B = \begin{pmatrix} -3 & -21 \\ -21 & -3 \end{pmatrix}.$$

For $c = \dfrac{-\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} + \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}}{2}$
$= \dfrac{-\sqrt{18^2 + 24^2} + \sqrt{24^2 + 18^2}}{2} = 0,$

$c' = \dfrac{-\sqrt{\lambda_{A,1}^2 + \lambda_{B,1}^2} - \sqrt{\lambda_{A,2}^2 + \lambda_{B,2}^2}}{2}$
$= \dfrac{-\sqrt{18^2 + 24^2} - \sqrt{24^2 + 18^2}}{2}$
$= -30,$
we have:

$$C = \begin{pmatrix} 0 & -30 \\ -30 & 0 \end{pmatrix}.$$

Let us show first that the circulant matrix triple (A, B, C) *is a Pythagorean triple. A simple calculation gives:*

$$\begin{pmatrix} 21 & -3 \\ -3 & 21 \end{pmatrix}^2 + \begin{pmatrix} -3 & -21 \\ -21 & -3 \end{pmatrix}^2 = \begin{pmatrix} 900 & 0 \\ 0 & 900 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & -30 \\ -30 & 0 \end{pmatrix}^2.$$

Then, $\left(\begin{pmatrix} 21 & -3 \\ -3 & 21 \end{pmatrix}, \begin{pmatrix} -3 & -21 \\ -21 & -3 \end{pmatrix}, \begin{pmatrix} 0 & -30 \\ -30 & 0 \end{pmatrix}\right)$ *is a circulant matrix Pythagorean triple. And we have:*

$$\tfrac{1}{2}AB = \tfrac{1}{2}\begin{pmatrix} 21 & -3 \\ -3 & 21 \end{pmatrix}\begin{pmatrix} -3 & -21 \\ -21 & -3 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & -216 \\ -216 & 0 \end{pmatrix}.$$

We also have:

$$\left[\frac{1}{2}\begin{pmatrix} 0 & 1 \\ 2 \times 18 \times (-24) & 0 \end{pmatrix}\right]^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & -216 \\ -216 & 0 \end{pmatrix}. \text{ So,}$$
$$P = \tfrac{1}{2}\begin{pmatrix} 0 & 1 \\ 2 \times 18 \times (-24) & 0 \end{pmatrix}$$
and $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Note that $\langle A \mid B \rangle = tr(A^T B)$
$= \left\langle \begin{pmatrix} 21 & -3 \\ -3 & 21 \end{pmatrix} \mid \begin{pmatrix} -3 & -21 \\ -21 & -3 \end{pmatrix} \right\rangle$
$= 0,$
so that the matrices A *and* B *are perpendicular.*

By The Pythagoras' Theorem (matrix version), we have:

$$\left\|\begin{pmatrix} 21 & -3 \\ -3 & 21 \end{pmatrix}\right\|^2 + \left\|\begin{pmatrix} -3 & -21 \\ -21 & -3 \end{pmatrix}\right\|^2 = 1800$$
$$= \left\|\begin{pmatrix} 0 & -30 \\ -30 & 0 \end{pmatrix}\right\|^2.$$

Algorithm 3.1. ***Computation of a congruent circulant matrix N***

We fix a bound K *for four rational numbers in* $\mathbb{Q}$.

1. *If we can find two pairs* $\lambda_{A,1}, \lambda_{B,1}$, $\lambda_{A,2}, \lambda_{B,2} \leq K$ *in such that* $\lambda_{A,1}^2 + \lambda_{B,1}^2$ *and* $\lambda_{A,2}^2 + \lambda_{B,2}^2$, *are non-zero squares in* $\mathbb{Q}$. *Then, we calculate* $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}$.

(*a*) *If* $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} = 0$, *then*

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(*b*) *If* $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} \neq 0$, *then*

$$N = \begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} \\ \frac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}.$$

2. *If we can not find such pairs* $(\lambda_{A,1}, \lambda_{B,1}), (\lambda_{A,2}, \lambda_{B,2})$, *then we start again.*

Proposition 3.1. *1. In the point* 3. *of Theorem* 3.4, *the circulant matrix Pythagorean* N*-triple* (A, B, C) *is such that the matrices* A *and* B *are not orthogonal in the case* (a) *but they are orthogonal in the case* (b).

2. Moreover in the two cases, we have the following ***Pythagoras' Theorem matrix version****.*

$$\|A\|^2 + \|B\|^2 = \|C\|^2.$$

Proof: Let $(A, B, C) \in M_2(\mathbb{Q})^3$ be a circulant matrix triple and denote by $\{\lambda_{A,1}, \lambda_{A,2}\}$ and $\{\lambda_{B,1}, \lambda_{B,2}\}$ respectively the set of their eigenvalues. And let consider the Euclidean vector space $(M_2(\mathbb{R}), \langle - \mid - \rangle)$, and

$$A = \begin{pmatrix} \frac{\lambda_{A,1} + \lambda_{A,2}}{2} & \frac{\lambda_{A,1} - \lambda_{A,2}}{2} \\ \frac{\lambda_{A,1} - \lambda_{A,2}}{2} & \frac{\lambda_{A,1} + \lambda_{A,2}}{2} \end{pmatrix},$$

$$B = \begin{pmatrix} \frac{\lambda_{B,1} + \lambda_{B,2}}{2} & \frac{\lambda_{B,1} - \lambda_{B,2}}{2} \\ \frac{\lambda_{B,1} - \lambda_{B,2}}{2} & \frac{\lambda_{B,1} + \lambda_{B,2}}{2} \end{pmatrix}.$$

Then we have:

$$A^TB = \begin{pmatrix} \frac{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}}{2} & \frac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{2} \\ \frac{\lambda_{A,1}\lambda_{B,1} - \lambda_{A,2}\lambda_{B,2}}{2} & \frac{\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}}{2} \end{pmatrix}$$

and $\langle A \mid B \rangle = tr(A^TB) = \lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2}$.

1. So, if:
   (a) $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} \neq 0$, then the vectors A and B are not orthogonal.
   (b) $\lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} = 0$, then the vectors A and B are orthogonal.

2. Let (A, B, C) be a circulant matrix Pythagorean triple of $M_2(\mathbb{Q})$, that is

   $$A^2 + B^2 = C^2, \ ABC \neq 0.$$

   Since the matrices A, B, C are circulant, by the first point Remarks 3.3, we have: $A^TA = A^2$, $B^TB = B^2$, $C^TC = C^2$.

   Then,

   $$\begin{aligned} tr(C^TC) &= tr(C^2) \\ &= tr(A^2 + B^2) \\ &= tr(A^2) + tr(B^2) \\ &= tr(A^TA) + tr(B^TB). \end{aligned}$$

   It means that,

   $$\|C\|^2 = \|A\|^2 + \|B\|^2,$$

   as announced.

Remarks 3.2. *1. In our construction of section* 3.1, *(cases* $m \geq 3$*), the cir-*

culant congruent matrix N is not invertible.

2. *The third observation of Theorem* 3.4, *allows us to calculate the matrices A, B of a circulant matrix Pythagorean triple, when we have their eigenvalues by the relation* (2). *And the matrix C is obtained by the system* (3).

The following Lemma 3.2 is the necessary condition to establish Theorem 3.3 and Corollary 3.1. In fact, the realization of Theorem 3.3. and Corollary 3.1. requires that in the circulant matrix Pythagorean triple (A, B, C), the matrices $A^2 - B^2$ and C are invertible.

Lemma 3.2. *Let the 2×2-circulant matrix triple (A, B, C) be a circulant matrix Pythagorean triple, i.e. such that $A^2 + B^2 = C^2$, $ABC \neq 0$. Let us denote by $\{\lambda_{A,1}, \lambda_{A,2}\}$ and $\{\lambda_{B,1}, \lambda_{B,2}\}$ respectively the sets of eigenvalues of the matrices A and B such that $\lambda_{A,1} \neq \pm\lambda_{B,1}$ and $\lambda_{A,2} \neq \pm\lambda_{B,2}$. Then:*

1. *The matrix $A^2 - B^2$ is invertible.*

2. *The matrix C is invertible.*

Proof: Let $(A, B, C) \in M_2(\mathbb{Q})^3$ be a circulant matrix Pythagorean triple. We denote their respective sets of their eigenvalues by $\{\lambda_{A,1}, \lambda_{A,2}\}$ and $\{\lambda_{B,1}, \lambda_{B,2}\}$. Then, we have by the relation (2):

$$A = \begin{pmatrix} \dfrac{\lambda_{A,1} + \lambda_{A,2}}{2} & \dfrac{\lambda_{A,1} - \lambda_{A,2}}{2} \\ \dfrac{\lambda_{A,1} - \lambda_{A,2}}{2} & \dfrac{\lambda_{A,1} + \lambda_{A,2}}{2} \end{pmatrix},$$

$$B = \begin{pmatrix} \dfrac{\lambda_{B,1} + \lambda_{B,2}}{2} & \dfrac{\lambda_{B,1} - \lambda_{B,2}}{2} \\ \dfrac{\lambda_{B,1} - \lambda_{B,2}}{2} & \dfrac{\lambda_{B,1} + \lambda_{B,2}}{2} \end{pmatrix},$$

where $\{\lambda_{A,1}, \lambda_{A,2}\}$ and $\{\lambda_{B,1}, \lambda_{B,2}\}$ are the sets of eigenvalues of the matrices A and B, respectively. Consequently,
$\det(A^2 - B^2) = (\lambda_{A,1} - \lambda_{B,1}) \times (\lambda_{A,1} + \lambda_{B,1})$
$\times (\lambda_{A,2} - \lambda_{B,2})(\lambda_{A,2} + \lambda_{B,2}) = 0$
$\iff [\lambda_{A,1} = \lambda_{B,1}]$, or $[\lambda_{A,1} = -\lambda_{B,1}]$ or $[\lambda_{A,2} = \lambda_{B,2}]$ or $[\lambda_{A,2} = -\lambda_{B,2}]$. However, these cases are excluded, since we assume $\lambda_{A,1} \neq \pm\lambda_{B,1}$ and $\lambda_{A,2} \neq \pm\lambda_{B,2}$. Therefore, we prove 1.

For the second point of the theorem, we have:
$\det(A^2 + B^2) = \det(C^2)$
$= \left(\lambda_{A,2}^2 + \lambda_{B,2}^2\right)\left(\lambda_{A,1}^2 + \lambda_{B,1}^2\right) \geq 0.$
So, $\det(C^2) = 0$
$\iff \left(\lambda_{A,1}^2 + \lambda_{B,1}^2\right)\left(\lambda_{A,2}^2 + \lambda_{B,2}^2\right) = 0$
$\iff [\lambda_{A,1}^2 + \lambda_{B,1}^2 = 0$ or $\lambda_{A,2}^2 + \lambda_{B,2}^2 = 0]$.
Suppose that $\lambda_{A,1}^2 + \lambda_{B,1}^2 = 0$,
then $\lambda_{A,1} = \lambda_{B,1} = 0$.

If $\lambda_{A,2}^2 + \lambda_{B,2}^2 = 0$, therefore $\lambda_{A,2} = \lambda_{B,2} = 0$. Such instances fall under the cases already excluded from our study by hypothesis .

Fermat [10] gave an algorithm to build different right-angled triangles with three rational sides having the same area (see also [5]). Moreover, Fermat asserted that his algorithm produces infinitely many such right-angled triangles, although he did not supply a proof of this assertion. In what follows, we shall present the matrix version of Fermat's algorithm [5]. This matrix-version algorithm generates infinitely many circulant matrix Pythagorean triples. Observe that, just as a given congruent integer n corresponds to infinitely many right-angled

triangles [5], in the matrix setting a congruent circulant matrix N, is likewise associated with infinitely many rational circulant matrix Pythagorean triples (see the third point of Definition 2.3. and Corollary 3.1.).

Fermat's Algorithm matrix version

We recall Fermat's algorithm [5], which produces infinitely many distinct right-angled triangles associated with a congruent number, provided that at least one such triangle exists.

Theorem: (**Fermat's Algorithm)**

Assume that $n \in \mathbb{N}$, square-free, is a congruent number, and that (a_0, b_0, c_0) is a n-triple of rational Pythagorean numbers , i.e. $n = \frac{1}{2}|a_0 b_0|$.
Then, $a_1 = \frac{4c_0^2 a_0 b_0}{2c_0(a_0^2 - b_0^2)}$, $b_1 = \frac{c_0^4 - 4c_0^2 a_0 b_0}{2c_0(a_0^2 - b_0^2)}$,
$c_1 = \frac{c_0^4 + 4c_0^2 a_0 b_0}{2c_0(a_0^2 - b_0^2)}$
is also a rational Pythagorean n-triple. Moreover, $a_0 b_0 = a_1 b_1$.

We now present the matrix analogue of Fermat's algorithm, which, under the assumptions of Lemma 3.9′s, generates infinitely many circulant matrix Pythagorean N-triples through iteration of the procedure (see Corollary 3.1.).

Theorem 3.3. *Assume that N is a congruent rational circulant matrix, and (A_0, B_0, C_0) is a rational circulant matrix Pythagorean N-triple. Then the following rational circulant matrix triple (A_1, B_1, C_1) is also a rational circulant matrix Pythagorean N-triple, with,*

$$A_1 = \frac{1}{2}(4C_0^2 A_0 B_0) C_0^{-1}(A_0^2 - B_0^2)^{-1},$$
$$B_1 = \frac{1}{2}(C_0^4 - 4A_0^2 B_0^2) C_0^{-1}(A_0^2 - B_0^2)^{-1},$$
$$C_1 = \frac{1}{2}(C_0^4 + 4A_0^2 B_0^2) C_0^{-1}(A_0^2 - B_0^2)^{-1}$$

Moreover, we have:
$\frac{1}{2}A_0 B_0 = \frac{1}{2}A_1 B_1 = P^2 N,\ P \in GL_2(\mathbb{Q})$.

Let note that the following proof is a naive algorithm to build the sequence of circulant matrix Pythagorean N-triples of Corollary 3.1.

Proof: Let note that Lemma 3.2. ensures that the matrices $A_0^2 - B_0^2$ and C_0 are invertible.

Suppose that N is a congruent rational circulant matrix, and (A_0, B_0, C_0) is a circulant matrix Pythagorean N-triple. Let $X = C_0^2$, $Y = 2A_0 B_0$ and let, $A = 2XY$, $B = X^2 - Y^2, C = X^2 + Y^2$
be auxiliary matrices.
We have:
$A = 4C_0^2 A_0 B_0, B = C_0^4 - 4A_0^2 B_0^2, C = C_0^4 + 4A_0^2 B_0^2$.
It is then immediate that, $A^2 + B^2 = C^2$; hence the matrix triple (A, B, C) constitutes a matrix Pythagorean triple such that

$$\begin{aligned} AB &= 4C_0^2 A_0 B_0 (C_0^4 - 4A_0^2 B_0^2) \\ &= 4C_0^2 A_0 B_0 ((A_0^2 + B_0^2)^2 - 4A_0^2 B_0^2) \\ &= 4C_0^2 A_0 B_0 (A_0^2 - B_0^2)^2 \\ &= 2C_0(A_0^2 - B_0^2) \times 2C_0(A_0^2 - B_0^2) \times 2P^2 N \end{aligned}$$

It follows that

$\left(\frac{1}{2}AC_0^{-1}(A_0^2 - B_0^2)^{-1}\right) \times \left(\frac{1}{2}BC_0^{-1}(A_0^2 - B_0^2)^{-1}\right)$
$= 2P^2 N$.

Thus, for
$A_1 = \frac{1}{2}AC_0^{-1}(A_0^2 - B_0^2)^{-1}$,
$B_1 = \frac{1}{2}BC_0^{-1}(A_0^2 - B_0^2)^{-1}$,
$C_1 = CC_0^{-1}(A_0^2 - B_0^2)^{-1}$,

we have

$$\begin{aligned} A_1 &= 4C_0^2A_0B_0C_0^{-1}(A_0^2-B_0^2)^{-1} \\ B_1 &= (C_0^4-4A_0^2B_0^2)C_0^{-1}(A_0^2-B_0^2)^{-1} \\ C_1 &= (C_0^4+4A_0^2B_0^2)C_0^{-1}(A_0^2-B_0^2)^{-1}, \end{aligned}$$

therefore,

$$\frac{1}{2}A_1B_1 = P^2N = \frac{1}{2}A_0B_0,$$

and

$$A_1^2+B_1^2 = C_1^2.$$

By induction, we deduce the rational circulant matrix Pythagorean N-triple (A_k, B_k, C_k) from the rational circulant matrix Pythagorean N-triple $(A_{k-1}, B_{k-1}, C_{k-1})$.

Let note that the set $\overline{\overline{N}} = \{(A_k, B_k, C_k) \in \mathcal{P}_T(N)\}$ yielded by Fermat's Algorithm matrix version is contained in $\overline{N}$. The following corollary asserts that, under the assumptions of Lemma 3.2′s, iterating the procedure described in Theorem 3.3. produces infinitely many rational circulant matrix Pythagorean N - triples.

Corollary 3.1. ***Computation of a sequence of rational circulant matrix Pythagorean N-triples***

Let (A_0, B_0, C_0) be a rational circulant matrix Pythagorean N-triple. Then the sequence of rational circulant matrix Pythagorean N-triples $(A_k, B_k, C_k)_{k\in\mathbb{N}}$ is defined recursively by the relation:

$$\begin{cases} A_k = \frac{1}{2}(4C_{k-1}^2A_{k-1}B_{k-1})C_{k-1}^{-1}(A_{k-1}^2-B_{k-1}^2)^{-1} \\ B_k = \frac{1}{2}(C_{k-1}^4-4A_{k-1}^2B_{k-1}^2)C_{k-1}^{-1}(A_{k-1}^2-B_{k-1}^2)^{-1}, \\ C_k = \frac{1}{2}(C_{k-1}^4+4A_{k-1}^2B_{k-1}^2)C_{k-1}^{-1}(A_{k-1}^2-B_{k-1}^2)^{-1} \end{cases}.$$

$\forall k \geq 1$

We present an example in which the second generation of a sequence of circulant matrix Pythagorean triples is constructed, yielding a congruent circulant matrix N.

Example 3.2. *Let consider the circulant matrices,*

$$A_0 = \begin{pmatrix} 5 & 2 \\ 2 & 5 \end{pmatrix}, B_0 = \begin{pmatrix} 14 & 10 \\ 10 & 14 \end{pmatrix},$$

$$C_0 = \begin{pmatrix} 15 & 10 \\ 10 & 15 \end{pmatrix}.$$

Let us show that we have a matrix Pythagorean.

$$\begin{pmatrix} 5 & 2 \\ 2 & 5 \end{pmatrix}^2 + \begin{pmatrix} 14 & 10 \\ 10 & 14 \end{pmatrix}^2 = \begin{pmatrix} 325 & 300 \\ 300 & 325 \end{pmatrix}$$

$$= \begin{pmatrix} 15 & 10 \\ 10 & 15 \end{pmatrix}^2.$$

So, $\left(\begin{pmatrix} 5 & 2 \\ 2 & 5 \end{pmatrix}, \begin{pmatrix} 14 & 10 \\ 10 & 14 \end{pmatrix}, \begin{pmatrix} 15 & 10 \\ 10 & 15 \end{pmatrix}\right)$ *is a circulant matrix Pythagorean triple such that*

$$\frac{1}{2}A_0B_0 = \frac{1}{2}\begin{pmatrix} 5 & 2 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 14 & 10 \\ 10 & 14 \end{pmatrix} = \begin{pmatrix} 45 & 39 \\ 39 & 45 \end{pmatrix}.$$

Let calculate the congruent matrix N. The eigenvalues of the matrices A and B are:

	A_0	B_0
$\lambda_{\bullet,1}$	7	24
$\lambda_{\bullet,2}$	3	4

.

A simple calculation gives:

$$N = \begin{pmatrix} 1 & \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} \\ \frac{\lambda_{A,1}\lambda_{B,1}-\lambda_{A,2}\lambda_{B,2}}{\lambda_{A,1}\lambda_{B,1}+\lambda_{A,2}\lambda_{B,2}} & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \frac{45}{39} \\ \frac{45}{39} & 1 \end{pmatrix},$$

$$P = \begin{pmatrix} 0 & 1 \\ \lambda_{A,1}\lambda_{B,1} + \lambda_{A,2}\lambda_{B,2} & 0 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 0 & 1 \\ 180 & 0 \end{pmatrix}.$$

And we get:

$$P^2N = \begin{pmatrix} 0 & 1 \\ 45 & 0 \end{pmatrix}^2 \begin{pmatrix} 1 & \frac{39}{45} \\ \frac{39}{45} & 1 \end{pmatrix} = \frac{1}{2}A_0B_0.$$

Calculation of A_1, B_1, C_1

▷ ***Calculation of the first auxiliary matrix Pythagorean triple***

We have:

$$A = 4C_0^2A_0B_0 = \begin{pmatrix} 210\,600 & 209\,400 \\ 209\,400 & 210\,600 \end{pmatrix},$$

$$B = C_0^4 - 4A_0^2B_0^2 = \begin{pmatrix} 138\,889 & 138\,840 \\ 138\,840 & 138\,889 \end{pmatrix},$$

$$C = C_0^4 + 4A_0^2B_0^2 = \begin{pmatrix} 252\,361 & 251\,160 \\ 251\,160 & 252\,361 \end{pmatrix}.$$

$$A^2+B^2 = \begin{pmatrix} 126\,767\,419\,921 & 126\,765\,977\,520 \\ 126\,765\,977\,520 & 126\,767\,419\,921 \end{pmatrix} = C^2.$$

▷ ***Calculation of the first circulant matrix Pythagorean*** N***-triple*** (A_1, B_1, C_1)

We have:

$$A_1 = \frac{1}{2}AC_0^{-1}(A_0^2 - B_0^2)^{-1} = \begin{pmatrix} -\frac{61\,020}{3689} & \frac{2220}{3689} \\ \frac{2220}{3689} & -\frac{61\,020}{3689} \end{pmatrix},$$

$$B_1 = \frac{1}{2}BC_0^{-1}(A_0^2 - B_0^2)^{-1} = \begin{pmatrix} -\frac{281}{50} & -\frac{123}{25} \\ -\frac{123}{25} & -\frac{281}{50} \end{pmatrix},$$

$$C_1 = \frac{1}{2}CC_0^{-1}(A_0^2 - B_0^2)^{-1} = \begin{pmatrix} -\frac{3344\,641}{184\,450} & -\frac{90\,003}{92\,225} \\ -\frac{90\,003}{92\,225} & -\frac{3344\,641}{184\,450} \end{pmatrix}.$$

Let us verify that (A_1, B_1, C_1) *is a matrix Pythagorean* N*-triple.*

$$\begin{pmatrix} -\frac{61\,020}{3689} & \frac{2220}{3689} \\ \frac{2220}{3689} & -\frac{61\,020}{3689} \end{pmatrix}^2 + \begin{pmatrix} -\frac{281}{50} & -\frac{123}{25} \\ -\frac{123}{25} & -\frac{281}{50} \end{pmatrix}^2 = \begin{pmatrix} \frac{11\,219\,025\,578\,917}{34\,021\,802\,500} & \frac{301\,027\,723\,923}{8505\,450\,625} \\ \frac{301\,027\,723\,923}{8505\,450\,625} & \frac{11\,219\,025\,578\,917}{34\,021\,802\,500} \end{pmatrix}.$$

$$\begin{pmatrix} -\frac{3344\,641}{184\,450} & -\frac{90\,003}{92\,225} \\ -\frac{90\,003}{92\,225} & -\frac{3344\,641}{184\,450} \end{pmatrix}^2 = \begin{pmatrix} \frac{11\,219\,025\,578\,917}{34\,021\,802\,500} & \frac{301\,027\,723\,923}{8505\,450\,625} \\ \frac{301\,027\,723\,923}{8505\,450\,625} & \frac{11\,219\,025\,578\,917}{34\,021\,802\,500} \end{pmatrix}.$$

Moreover,

$$\frac{1}{2}\begin{pmatrix} -\frac{61\,020}{3689} & \frac{2220}{3689} \\ \frac{2220}{3689} & -\frac{61\,020}{3689} \end{pmatrix}\begin{pmatrix} -\frac{281}{50} & -\frac{123}{25} \\ -\frac{123}{25} & -\frac{281}{50} \end{pmatrix} = \begin{pmatrix} 45 & 39 \\ 39 & 45 \end{pmatrix} = P^2N.$$

Calculation of A_2, B_2, C_2

▷ ***Calculation of the second auxiliary matrix Pythagorean triple***

We have:

$$A = 4C_1^2A_1B_1 = \begin{pmatrix} \frac{1103\,632\,951\,966\,506}{8505\,450\,625} & \frac{983\,453\,975\,767\,806}{8505\,450\,625} \\ \frac{983\,453\,975\,767\,806}{8505\,450\,625} & \frac{1103\,632\,951\,966\,506}{8505\,450\,625} \end{pmatrix},$$

$$B = C_1^4 - 4A_1^2B_1^2 = \begin{pmatrix} \frac{61\,645\,459\,928\,596\,898\,899\,051\,753}{1157\,483\,045\,349\,006\,250\,000} & -\frac{4748\,293\,243\,694\,721\,949\,668\,609}{144\,685\,380\,668\,625\,781\,250} \\ -\frac{4748\,293\,243\,694\,721\,949\,668\,609}{144\,685\,380\,668\,625\,781\,250} & \frac{61\,645\,459\,928\,596\,898\,899\,051\,753}{1157\,483\,045\,349\,006\,250\,000} \end{pmatrix}$$

$$C = C_1^4 + 4A_1^2B_1^2 = \begin{pmatrix} \frac{192\,987\,376\,050\,439\,336\,099\,051\,753}{1157\,483\,045\,349\,006\,250\,000} & \\ & \frac{11\,502\,768\,713\,005\,325\,800\,331\,391}{144\,685\,380\,668\,625\,781\,250} \end{pmatrix}$$

$$\left.\begin{array}{c} \frac{11\,502\,768\,713\,005\,325\,800\,331\,391}{144\,685\,380\,668\,625\,781\,250} \\ \\ \frac{192\,987\,376\,050\,439\,336\,099\,051\,753}{1157\,483\,045\,349\,006\,250\,000} \end{array}\right).$$

$$A^2+B^2=C^2=circ^T\left(\begin{array}{c} \frac{45\,712\,203\,350\,986\,914\,997\,562}{1339\,767\,000\,270\,409\,659\,069} \\ \\ \frac{2219\,889\,151\,237\,986\,917\,415}{83\,735\,437\,516\,900\,603\,691} \end{array}\right.$$

$$\left.\begin{array}{c} \frac{498\,247\,359\,840\,405\,770\,332\,652\,045\,393}{867\,862\,539\,062\,500\,000\,000} \\ \\ \frac{987\,682\,729\,131\,360\,855\,328\,259\,478\,423}{866\,741\,408\,691\,406\,250\,000} \end{array}\right).$$

It should be emphasized that $circ^T$ represents a 2×1 matrix, rather than 2×2 matrix, as its two-line presentation might suggest.

▷ ***Calculation of the first circulant matrix Pythagorean N-triple*** (A_2,B_2,C_2)

$$A_2=\frac{1}{2}AC_1^{-1}(A_1^2-B_1^2)^{-1}$$

$$=\left(\begin{array}{cc} -\frac{3304\,533\,260\,540\,138\,760}{142\,705\,568\,572\,215\,841} & -\frac{3104\,245\,021\,888\,895\,640}{142\,705\,568\,572\,215\,841} \\ \\ -\frac{3104\,245\,021\,888\,895\,640}{142\,705\,568\,572\,215\,841} & -\frac{3304\,533\,260\,540\,138\,760}{142\,705\,568\,572\,215\,841} \end{array}\right);$$

$$B_2=\frac{1}{2}BC_1^{-1}(A_1^2-B_1^2)^{-1}$$

$$=\left(\begin{array}{cc} -\frac{1370\,954\,408\,265\,839}{223\,084\,425\,176\,900} & \frac{268\,210\,040\,276\,163}{111\,542\,212\,588\,450} \\ \\ \frac{268\,210\,040\,276\,163}{111\,542\,212\,588\,450} & -\frac{1370\,954\,408\,265\,839}{223\,084\,425\,176\,900} \end{array}\right),$$

$$C_2=\frac{1}{2}CC_1^{-1}(A_1^2-B_1^2)^{-1}$$

$$=\left(\begin{array}{c} -\frac{855\,243\,027\,955\,095\,825\,704\,174\,021\,355\,599}{31\,835\,389\,734\,475\,456\,945\,801\,407\,272\,900} \\ \\ -\frac{289\,703\,588\,744\,545\,528\,483\,576\,513\,501\,917}{15\,917\,694\,867\,237\,728\,472\,900\,703\,636\,450} \end{array}\right.$$

$$\left.\begin{array}{c} -\frac{289\,703\,588\,744\,545\,528\,483\,576\,513\,501\,917}{15\,917\,694\,867\,237\,728\,472\,900\,703\,636\,450} \\ \\ -\frac{855\,243\,027\,955\,095\,825\,704\,174\,021\,355\,599}{31\,835\,389\,734\,475\,456\,945\,801\,407\,272\,900} \end{array}\right).$$

Let us verify that (A_2,B_2,C_2) is a matrix Pythagorean N-triple.

$$\left(\begin{array}{cc} -\frac{3304\,533\,260\,540\,138\,760}{142\,705\,568\,572\,215\,841} & -\frac{3104\,245\,021\,888\,895\,640}{142\,705\,568\,572\,215\,841} \\ \\ -\frac{3104\,245\,021\,888\,895\,640}{142\,705\,568\,572\,215\,841} & -\frac{3304\,533\,260\,540\,138\,760}{142\,705\,568\,572\,215\,841} \end{array}\right)^2$$

$$+\left(\begin{array}{cc} -\frac{1370\,954\,408\,265\,839}{223\,084\,425\,176\,900} & \frac{268\,210\,040\,276\,163}{111\,542\,212\,588\,450} \\ \\ \frac{268\,210\,040\,276\,163}{111\,542\,212\,588\,450} & -\frac{1370\,954\,408\,265\,839}{223\,084\,425\,176\,900} \end{array}\right)^2$$

$$=circ^T\left(\begin{array}{c} \frac{1067\,153\,314\,191\,675\,886\,478\,591\,125\,607\,227}{1013\,492\,039\,545\,945\,305\,098\,876\,290\,304\,177} \\ \\ \frac{247\,766\,974\,447\,342\,935\,821\,042\,864\,057\,963}{253\,373\,009\,886\,486\,326\,274\,719\,072\,576\,044} \end{array}\right.$$

$$\left.\begin{array}{c} \frac{605\,303\,018\,294\,760\,552\,454\,924\,659\,348\,357}{995\,150\,189\,884\,198\,057\,015\,074\,410\,000} \\ \\ \frac{647\,560\,317\,807\,553\,562\,009\,723\,025\,183\,283}{498\,787\,547\,471\,049\,514\,253\,768\,602\,500} \end{array}\right),$$

$$C^2=\left(\begin{array}{c} -\frac{855\,243\,027\,955\,095\,825\,704\,174\,021\,355\,599}{31\,835\,389\,734\,475\,456\,945\,801\,407\,272\,900} \\ \\ -\frac{289\,703\,588\,744\,545\,528\,483\,576\,513\,501\,917}{15\,917\,694\,867\,237\,728\,472\,900\,703\,636\,450} \end{array}\right.$$

$$\left.\begin{array}{c} -\frac{289\,703\,588\,744\,545\,528\,483\,576\,513\,501\,917}{15\,917\,694\,867\,237\,728\,472\,900\,703\,636\,450} \\ \\ -\frac{855\,243\,027\,955\,095\,825\,704\,174\,021\,355\,599}{31\,835\,389\,734\,475\,456\,945\,801\,407\,272\,900} \end{array}\right)^2$$

$$=circ^T\left(\begin{array}{c} \frac{1067\,153\,314\,191\,675\,886\,478\,591\,125\,607}{1013\,492\,039\,545\,945\,305\,098\,876\,290\,304} \\ \\ \frac{247\,766\,974\,447\,342\,935\,821\,042\,864\,057}{253\,373\,009\,886\,486\,326\,274\,719\,072\,576} \end{array}\right.$$

$$\left.\begin{array}{c} \frac{227\,605\,303\,018\,294\,760\,552\,454\,924\,659\,348\,357}{177\,995\,150\,189\,884\,198\,057\,015\,074\,410\,000} \\ \\ \frac{963\,647\,560\,317\,807\,553\,562\,009\,723\,025\,183\,283}{044\,498\,787\,547\,471\,049\,514\,253\,768\,602\,500} \end{array}\right).$$

As previously noted, $circ^T$ is a 2×1 matrix and not a 2×2 matrix.

Moreover,

$$\frac{1}{2}A_2B_2=\frac{1}{2}\left(\begin{array}{cc} -\frac{3304\,533\,260\,540\,138\,760}{142\,705\,568\,572\,215\,841} & -\frac{3104\,245\,021\,888\,895\,640}{142\,705\,568\,572\,215\,841} \\ \\ -\frac{3104\,245\,021\,888\,895\,640}{142\,705\,568\,572\,215\,841} & -\frac{3304\,533\,260\,540\,138\,760}{142\,705\,568\,572\,215\,841} \end{array}\right)$$

$$\times\left(\begin{array}{cc} -\frac{1370\,954\,408\,265\,839}{223\,084\,425\,176\,900} & \frac{268\,210\,040\,276\,163}{111\,542\,212\,588\,450} \\ \\ \frac{268\,210\,040\,276\,163}{111\,542\,212\,588\,450} & -\frac{1370\,954\,408\,265\,839}{223\,084\,425\,176\,900} \end{array}\right)$$

$$=\begin{pmatrix} 45 & 39 \\ 39 & 45 \end{pmatrix}=P^2N.$$

4 Conclusion and outlook

The Diophantine problem of congruent numbers, classically posed within the set of positive integers and well known in number theory, remains only partially resolved. As demonstrated in our study, this problem naturally extends to the setting of square matrices of order $m \geq 2$.

For $m > 2$, we have constructed a family of congruent matrices arising from trivial families of circulant matrix Pythagorean N-triples. The question remains open, however, for non-trivial families.

For $m = 2$, the problem has been completely solved in the case of circulant matrices. In this situation, analogously to the classical theory of congruent numbers, we have been able to construct elliptic curves − this time in a matrix setting − from which cryptographic applications may potentially be developed. This direction constitutes an open avenue for further research.

References

[1] J.H. Coaste, The Congruent Number Problem, Enrichment Programme For Young Mathmatics Talents Dept of Math & IMS CUHK GUEST Lecture Series Autumn Class 2002-03 (2002).

[2] L.E. Dickson, History of the Theory of Numbers, Vol. II. New York, Chelsea (1952).

[3] R. Cuculière, Mille ans de chasse aux nombres congruents Séminaire de Philosophie et Mathématiques, fascicule 2, «Mille ans de chasse aux nombres congruents»(1988) 1-17.

[4] R. Alter, T. B. Curtz, *A note on congruent numbers*, Math. of comput. t. 28 (1974) 303-305.

[5] L. Halbeisen, Norbert Hungerbühler, *A Theorem of Fermat on Congruent Number Curves*, Hardy-Ramanujan Journal, Atelier Digit_Hum (2019) 15-21. 10.46298/hrj.2019.5101. hal-01983260

[6] J. Lagrange, Nombres congruents et courbes elliptiques Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n°1 (1974-1975), exp. n°16, 1-17.

[7] J. Lagrange, Construction d'une table de nombres congruents Mémoires de la S. M. F., tome 49-50 (1977) 125-130.

[8] B.R. Hemenway,On Recognizing Congruent Prime. Master Thesis, Simon Fraiser University, Burnaby (2006). http://summit.sfu.ca/item/6418

[9] T. Evink, J. Top, J.D. Top, *A Remark on Prime (non) Congruent Numbers*, Quaestiones Mathematicae 45 (2021) 1841-1853. https://doi.org/ 10.2989/16073606.2021.1977410

[10] P. de Fermat, Fermat's Diophanti Alex. Arith., 1670 in Œuvres III (Ministère de l'instruction publique, ed.), Gauthier-Villars et ls, Paris (1896) 254-256.

[11] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Mathematische Zeitschrift 204 (1990) 45-67. https://doi.org/10.1007/BF02570859

[12] K. Conrad, The Congruent Number Problem, University of Connecticut Storrs, CT 06269 (2015).

[13] L.D. Keuméan, F.E. Tanoé, *A New Proof for Congruent Number's Problem via Pythagorean Divisors*, Advances in Pure Mathematics 14 (2024) 283-302. https://doi.org/10.4236/apm.2024.144016

[14] J.M. Mouanda, J.R. Tsiba, K. Kangni, *On Fermat's Last Theorem Matrix Version and Galaxies of Sequences of Circulant Matrices with Positive Integers as Entries*, Global Journal of Science Frontier Research: F Mathematics and Decision Sciences, 22(2) (2022) 1.

[15] J.M. Mouanda, J.R. Tsiba, K. Kangni, *On galaxies of sequences of matrix Pythagorean triples and completely Pythagorean maps*, Journal of AppliedMath. 3(3) (2025) 2609. https://doi.org/10.59400/jam2609

[16] P.J. Davis, circulant Matrices 1st edition, John Wiley and Sons, New York (1979).

[17] D. Kalman, J.E. White, Polynomial Equations and Circulant Matrices, The Mathematical Association of America, Monthly 108 (2001).

[18] K. Irwan, S.R. Simanca, On Circulant Matrices, American Mathematical Society (2004). DOI: 10.1090/noti804

[19] N.M. Stephens, *Congruence Properties of Congruent Numbers*, Bulletin of the London Mathematical Society 7 (1975) 182-184. https://doi.org/10.1112/blms/7.2.182.

[20] Scientific_Workplace_pro5.5. Available onligne. https://scientific-workplace.software.informer.com