WIP: Using GeoGebra to Learn the Basics of Post-Quantum Cryptography

Édgar Pérez-Ramos, Pino Caballero-Gil, Héctor Reboso-Morales
Department of Computer Engineering and Systems
University of La Laguna
Tenerife, Spain
alu0101207667@ull.edu.es, pcaballe@ull.edu.es, hreboso@ull.es

***Abstract*—This work in progress paper describes a proposal to use the GeoGebra environment as a useful didactic and conceptual tool to introduce the basic concepts of the increasingly relevant area of Post-Quantum Cryptography (PQC). The advancement and threat posed by quantum computing present significant challenges to information security. This situation has generated an urgent need to develop cryptographic systems capable of resisting quantum attacks. In this context, PQC has emerged as a crucial research field. However, one of the main challenges facing this field is the scarcity of available educational resources. This paper addresses this issue by creating educational resources focused on lattices using GeoGebra. An activity has been designed to introduce and relate lattices to various mathematical concepts taught in the classroom. The developed activity is completely innovative and aims to make the understanding of PQC more accessible by providing visual and manipulable tools that help students internalize the mathematical and computational principles involved in information security in the post-quantum era.**

***Index Terms*—Mathematics, Educational software, High school**

I. Introduction

Currently, cryptography plays an essential role in all communication technologies, as it is necessary to protect the security of systems and messages. Among the most relevant cryptographic techniques, encryption is used to protect secrets, while digital signatures are employed to verify the authenticity and integrity of digital information. However, with the potential future deployment of quantum computing, it has been discovered that many cryptographic algorithms currently used in different technologies, such as RSA or ECDSA, will be entirely vulnerable, prompting the need for new cryptographic schemes resistant to the so-called quantum threat.

The National Institute of Standards and Technology (NIST) has recently dedicated several years of effort to the search for standardized algorithms that are resistant to quantum computing. In 2022, the four finalists of this exhaustive process were announced, among which algorithms like CRYSTALS-Kyber, [3], designed for encryption, and CRYSTALS-Dilithium, [4], intended for digital signatures, stood out.

Since then, numerous efforts have been devoted to verifying the robustness of these schemes, given the importance they will acquire in the coming years. In particular, NIST has recently developed the corresponding drafts of the Federal Information Processing Standards (FIPS), FIPS 203 [5] and FIPS 204 [6] which specify the Module-Lattice Key Encapsulation Mechanism (ML-KEM) and the Module-Lattice Digital Signature Algorithm (ML-DSA), derived from CRYSTALS-Kyber and CRYSTALS-Dilithium, respectively.

Lattices are the common factor in most quantum-resistant algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium and FALCON, [7]). However, becoming familiar with the fundamentals of lattice theory can be seen as a necessity at various educational levels, in order to more effectively prepare future engineers and scientists.

This paper is structured as follows: Firstly, Section II presents the tools necessary to understand the work. It explains what GeoGebra is, justifies the type of students the activity is aimed at and introduces the mathematical concepts that are worked on in the exercise and Section III develops and explains the activity, which can be consulted in [8]. Finally, a last section is devoted to future work and conclusions.

II. Preliminaries

Lattices are the most predominant algebraic object in current encryption and signature standards. In the literature, the available educational material on lattices is often scarce and can sometimes be complex and abstract for inexperienced students. Therefore, this work has developed a series of activities using the GeoGebra software [9].

GeoGebra is an open-source mathematics software project founded that combines aspects of geometry, algebra, calculus, and other fields of mathematics. It is widely used in educational settings, ranging from primary schools to university levels, as well as by researchers, mathematics professionals, and related disciplines. Some of its features include:

- Dynamic Interface: GeoGebra provides a dynamic interface that allows users to create, manipulate, and explore mathematical objects in real-time. This facilitates the understanding of abstract mathematical concepts by enabling interactive visualization.
- Interactive Geometry: Users can construct and manipulate geometric figures such as points, lines, segments, polygons, circles, and more. These figures can be easily dragged, rotated, scaled, and modified.

Identify applicable funding agency here. If none, delete this.

- Dynamic Algebra: GeoGebra allows working with algebraic expressions, equations, and functions interactively. Users can graph functions, solve equations, find derivatives and integrals, and perform algebraic manipulations.
- Data Visualization: GeoGebra enables the visualization of data by creating function plots, scatter plots, histograms, and other types of visual representations. This facilitates the analysis and interpretation of data in mathematical and scientific contexts.
- Additional Tools: In addition to its core capabilities in geometry and algebra, GeoGebra also includes tools for working with differential and integral calculus, statistics, probability, and more.

Thus, due to all those advantages, GeoGebra has been chosen for its high efficiency and utility in educational environments, as evidenced, for example, in [10] and [11].

To justify the relevance of this innovative project in the educational context, we have referenced the LOMLOE [12], which is the current educational law in Spain. This work can be suitable from high school, since, as stated in [13], both Mathematics A and Mathematics B align on:

- Evaluation criteria:
  - Specific competency 7.2: "Selecting among different tools, including digital ones, and forms of representation (pictorial, graphical, verbal, or symbolic), assessing their usefulness for sharing information."
- Basic knowledge:
  - Spatial sense:
    - Two and three-dimensional geometric figures: "Geometric properties of mathematical objects and everyday life: investigation using dynamic geometry software."
    - Motions and transformations: "Elementary transformations in everyday life: investigation using technological tools such as dynamic geometry programs, augmented reality..."
  - Algebraic sense:
    - Computational thinking: "Problem-solving through decomposition, automation, and algorithmic thinking."

On the other hand, it is worth noting that a fundamental motivation for developing this work has been the latest PISA Report (available at [14] and [15]), in which Spain has achieved its worst result since the test began. Specifically, Spanish students in the final year of compulsory secondary education have dropped by 8 points in mathematics compared to the previous edition. The evolution can be seen in Fig. 1.

The objective of PISA (Program for International Student Assessment) proposed by the OECD (Organization for Economic Co-operation and Development) is to measure 15-year-old students' ability to use their knowledge and skills in reading, mathematics, and science to tackle real-life challenges.

Therefore, after these results, creating useful and innovative educational material on mathematics becomes urgently needed. The aspiration is to address the identified deficiencies and strengthen students' numerical and conceptual skills.

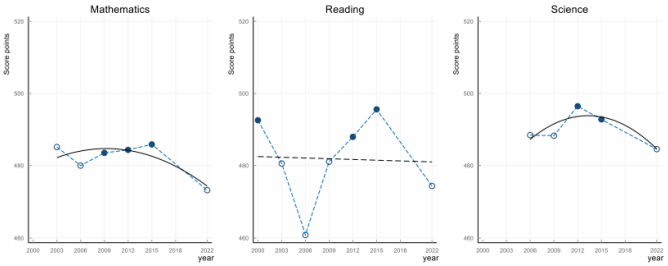

Fig. 1. Evolution of mathematics, reading and science scores

Mathematical concepts

The activity developed in [8] serves a dual purpose: to use the mathematical principles taught in high school to introduce PQC to students, or to use PQC as a tool to enhance the understanding of various mathematical concepts addressed in the classroom. These concepts include:

- Lattices
- Dot product of two vectors
- Orthogonality
- Affine and usual reference system
- Euclidean and taxi distance

Formally, a lattice can be defined as follows:

Definition 1: Let V be a vector space over a field K, $\{v_1, v_2, \ldots, v_n\}$ a basis of a subspace of V, and A a ring contained in K. Then the lattice $\mathcal{L} \subset V$ generated by the basis $\{v_1, v_2, \cdots, v_n\}$ is the set:

$$\mathcal{L}(v_1, v_2, \ldots, v_n) = \{\sum_{i=1}^{n} a_i \cdot v_i : a_i \in A\} \tag{1}$$

Generally, $A = \mathbb{Z}$ is considered, and for this activity, $V = \mathbb{Z}^m$, so that the lattice $\mathcal{L}(v_1, v_2, \ldots, v_n)$ is defined from a basis $v_i \in \mathbb{Z}^m$:

$$\mathcal{L}(v_1, v_2, \ldots, v_n) = \{\sum_{i=1}^{n} a_i \cdot v_i : a_i \in \mathbb{Z}, \} \tag{2}$$

Therefore, a lattice can always be generated from a basis of the vector space in which it is defined, through all linear combinations of elements of that basis. However, far from this formality, the message that wants to be conveyed to students is that a lattice is nothing more than the integer linear combinations of a set of vectors, and that different bases can give rise to the same lattice.

Definition 2: In a vector space $\mathbb{V}$, an inner product (or dot product) is a function such that:

$$\langle \cdot, \cdot \rangle : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{K},$$
$$(u, v) \longmapsto a = \langle u, v \rangle$$

where $\mathbb{V}$ is a vector space and $\mathbb{K}$ is the ordered field over which it is defined, with $\mathbb{K} = \mathbb{R}$. This binary operation must satisfy the following conditions, where $a, b \in \mathbb{K}$ and $u, v, w \in \mathbb{V}$:

- Linearity holds both on the left and on the right. That is:

$$\langle au + bv, w\rangle = a \cdot \langle u, w\rangle + b \cdot \langle v, w\rangle \tag{3}$$

y

$$\langle u, av + bw\rangle = \bar{a} \cdot \langle u, v\rangle + \bar{b} \cdot \langle u, w\rangle \tag{4}$$

- Hermiticity: $\langle u, v\rangle = \langle \bar{v, u}\rangle$
- Positive definiteness: $\langle u, u\rangle \geq 0$ y $\langle u, u\rangle = 0 \iff u = 0$, $\forall u \in \mathbb{V}$

Usually, this operation is denoted by "$\cdot$". Then, if we also consider $\mathbb{V} = \mathbb{R}^2$ and $\mathbb{K} = \mathbb{R}$, we can consider the common dot product known to students in high school courses. Additionally, to connect this definition with lattices on the plane, the following relationship is recalled:

$$u \cdot v = \| u \| \cdot \| v \| \cdot cos(\alpha) \tag{5}$$

where $u, v \in \mathbb{R}^2$ and α is the angle formed between the two vectors. Below, the definition of the norm associated with Eq. 5 is recalled. For further depth on this, one can refer to [16].

Definition 3: A vector space $\mathbb{V}$ is called a normed space if, for each $x \in \mathbb{V}$, a real number is defined, denoted by $\| x \|$, which satisfies the following properties:

- $\| x \| \geq 0, \quad \forall x \in \mathbb{V}$ (Positivity)
- $\| x \| = 0 \iff x = 0, \quad \forall x \in \mathbb{V}$ (Definedness)
- $\| \alpha \cdot x \| = |\alpha| \cdot \| x \| \quad \forall \alpha \in \mathbb{R}$ y $\forall x \in \mathbb{V}$ (Homogeneity)
- $\| x + y \| \leq \| x \| + \| y \|, \quad \forall x, y \in \mathbb{V}$ (Triangle inequality)

The quantity $\| x \|$ is known as the norm of x. Generally, the normed vector space is denoted as $(\mathbb{V}, \cdot)$. In the case where the second condition of Definition 3 is not satisfied but the others are, $\| \cdot \|$ is said to be a seminorm.

From Eq. 5, we know that if $\alpha = (2k+1) \cdot \frac{\pi}{2}$, with $k \in \mathbb{Z}$, then $u \cdot v = 0$. It is at this point where lattices are related to the dot product and orthogonality, allowing us to work with lattices of orthogonal bases.

Definition 4: Given a vector space $\mathbb{V}$ over a field $\mathbb{K}$ with an inner product $\langle \cdot, \cdot \rangle$, two vectors $u, v \in \mathbb{V}$ are said to be orthogonal if their inner product is equal to zero, that is:

$$\langle u, v\rangle = 0 \tag{6}$$

In the following, in order to link the lattices with orthogonal bases and the concept of both affine and Cartesian reference system, we will rely on [17], where all the necessary definitions and examples can be found.

Definition 5: A collection of points $p_0, p_1, \ldots, p_k$, with $k \in \mathbb{N}$ in an affine space $\mathcal{A}$ is said to be affinely independent if the vectors $\overrightarrow{p_0p_1}, \overrightarrow{p_1p_2}, \ldots, \overrightarrow{p_{k-1}p_k}$ are linearly independent.

Definition 6: Given an affine space $\mathcal{A}$ with $dim(\mathcal{A}) = n$, where $n \in \mathbb{N}$, a reference system $\mathcal{R}$ in $\mathcal{A}$ is an ordered reference system $p_0, p_1, \ldots, p_n$ of $n+1$ affinely independent points, or equivalently, satisfying:

$$\langle \{p_0, p_1, \ldots, p_n\} \rangle = \mathcal{A} \tag{7}$$

Once an affine reference system is defined, the euclidean affine reference system in $\mathbb{R}^n$, commonly referred to as the usual or Cartesian system, can be defined.

Definition 7: In the euclidean affine space $\mathbb{R}^n$ endowed with the canonical affine structure, the reference system:

$$\mathcal{R}_0 = \{(0, 0, \ldots, 0), B_0\} \tag{8}$$

where $B_0 = (1, 0, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)$ is the canonical basis of $\mathbb{R}^n$, meaning that every point $x \in \mathbb{R}^n$ can be expressed in terms of $\mathcal{R}_0$.

In general, in the classroom, we work with the reference system defined by $(0,0), (1,0), (0,1)$ in the case of the plane, and $(0,0,0), (1,0,0), (0,1,0), (0,0,1)$ in space. When it comes to conveying abstract concepts like Def. 6 in the classroom, the goal is to teach that the dot product, whether 0 or nonzero, allows the creation of Cartesian reference systems or, alternatively, the imposition of an affine reference system using the available points and vectors. This is done in order to construct lattices that can have orthogonal bases (a usual scenario) or non-orthogonal bases. Through this approach, students not only understand how to construct perpendicular axes following a unit of measure, but also learn to construct non-perpendicular axes using arbitrary points.

Finally, stemming from Def. 8, we introduce the taxi distance, which on the plane can have a geometric representation similar to that of lattices. This concept allows both the teacher and the students to group the previous definitions and bring them closer to reality, making them a bit more tangible.

Definition 8: The taxi distance, also known as Manhattan distance or rectilinear distance, is a metric used in geometry to calculate the distance between two points in a euclidean space with rectangular coordinates. Formally, the taxi distance between two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ in a euclidean plane is expressed as:

$$d_{\text{taxi}}(P, Q) = |x_1 - x_2| + |y_1 - y_2| \tag{9}$$

Where $|x_1 - x_2|$ represents the absolute difference between the horizontal coordinates of the points and $|y_1 - y_2|$ represents the absolute difference between the vertical coordinates of the points. The sum of these absolute differences provides the taxi distance between the two points. An illustrative example of this concept is shown in Fig. 2.

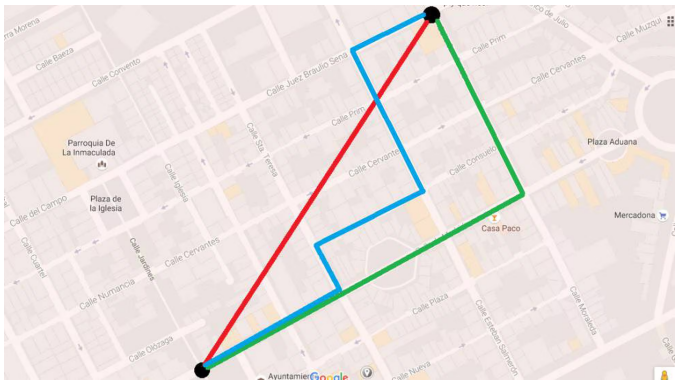

Fig. 2. Example of the application of the taxi distance, [18].

III. GeoGebra activity

As mentioned earlier, the activity developed in [8] serves two distinct purposes: leveraging mathematical principles taught in high school to introduce PQC to students, or employing PQC as a tool to enhance the understanding of various mathematical concepts addressed in the classroom.

When presenting this resource, it is not necessary to teach the mathematical content that is provided here only to understand the underlying mathematics of the activity. However, the developed educational resource is designed as an alternative method to introduce those concepts or as a motivating supplement to reinforce topics already covered in the classroom.

A brief introduction to lattice theory

The GeoGebra activity titled "A Brief Introduction to Lattice Theory" aims to provide insights into the mathematics underlying PQC through concise definitions and various exercises, including both short-answer and open-ended questions.

In the initial stage, the rationale behind PQC and the threat posed by quantum computing are presented to spark curiosity among students. Following this, a comparison is drawn between two definitions of lattices: an informal one and a formal definition (Def. 1).

ChatGPT is used to give this informal definition. ChatGPT is a relatively novel tool. It has been chosen to be used in this activity (particularly at the beginning, to maintain the reader's interest) with the aim of fostering greater engagement from students. Since this tool is often associated with a stigma that distances it from conventional educational environments, the goal is to present an appealing definition that sparks the interest and participation of the students.

Once the definitions have been provided, simple examples are presented to reinforce these concepts, along with dynamic representations as seen in Fig. 3 and Fig. 4. Additionally, short-answer and open-ended questions are also included.

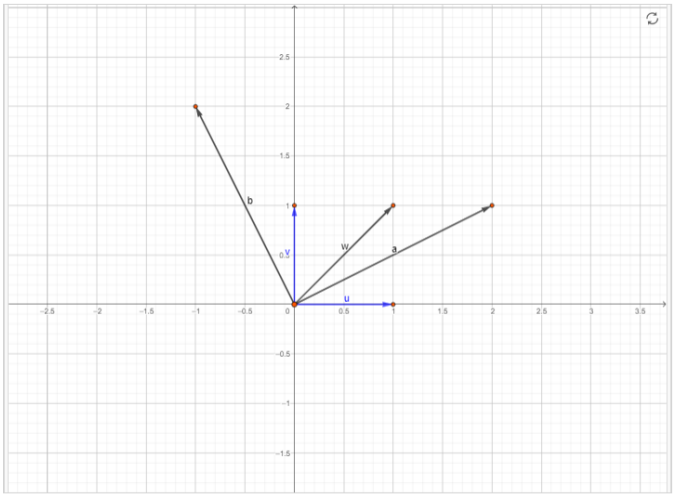

Fig. 3. First example of the elements of a lattice

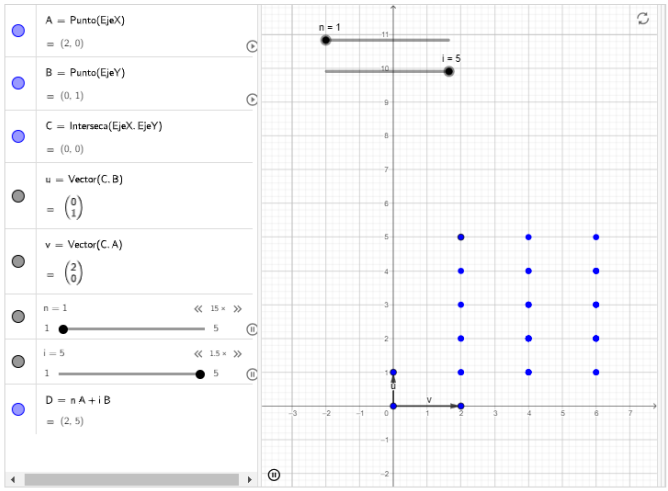

Fig. 4. Dynamic example of the elements of a lattice

One of the main advantages of these dynamic representations is that students themselves can vary the vectors and observe the changes reflected. In this way, through interactive learning, students can manipulate concepts and become directly involved in constructing their knowledge. Therefore, the construction of their own lattices is also proposed in open-ended questions.

Furthermore, dynamic representations are also used to empirically demonstrate that the only null lattice is composed of null vectors. Alternatively, students learn interactively that using non-null vectors with infinite coefficients will result in an infinite lattice.

In the second part of the activity, the aim is to establish connections between the previously mentioned concepts so that the reader can successfully comprehend their interrelations. At this juncture, reference is made to the scalar product between two vectors and, derived from it, orthogonality. Additionally, as depicted in Fig. 5, affine and usual reference systems are also introduced.

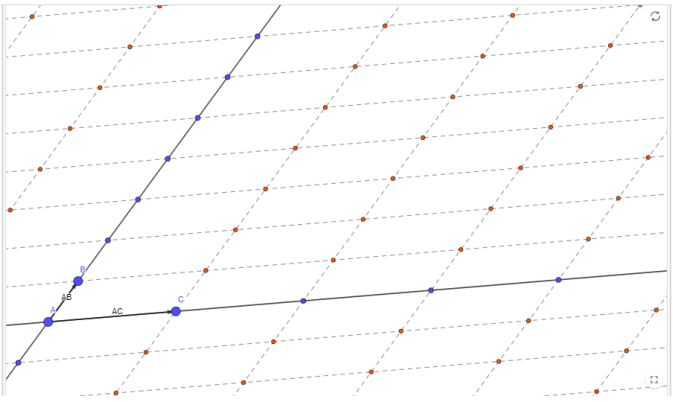

Fig. 5. Non-orthogonal lattice

To complete the activity and provide a more integrative and practical conclusion, various branches of mathematics are mentioned, with particular emphasis on geometry and topology. This approach leads us to the aforementioned taxi distance in Definition 8. For this practical example, an image of the city of Barcelona with an aerial view has been proposed, as it stands out for its urban, orderly, and representative layout.

To take advantage of GeoGebra's capabilities, an aerial view image of the city of Barcelona is integrated into the software, and lattice elements are superimposed at each intersection of both vertical and horizontal streets (see Fig. 6). This allows posing to the student how to navigate from point A to point B solely moving through lattice points. Thus, it becomes evident that the solution is not to draw a straight line between A and B, but that there are multiple possible routes, highlighting the non-unique nature of the solution and the direct, tangible application of the concepts.

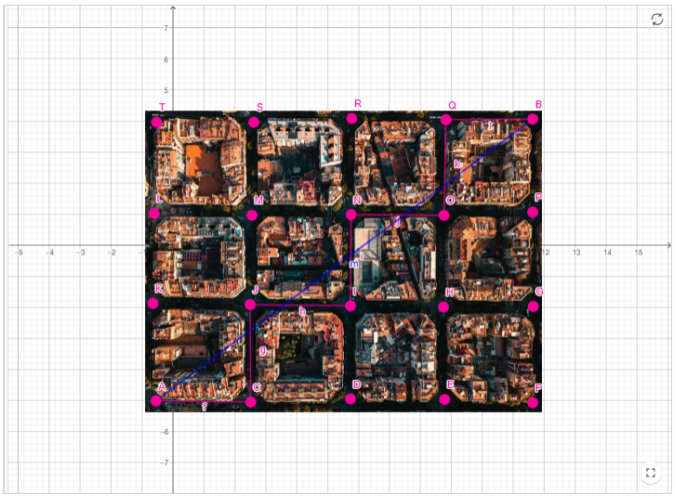

Fig. 6. Taxi distance over a lattice

IV. Conclusions

This paper has presented an innovative methodology for teaching lattices using GeoGebra. Throughout the activity, fundamental concepts of the topic have been explored, such as the structure of the lattice itself, through dynamic examples, various types of questions, and its relationship with seemingly disparate concepts like scalar product, orthogonality, affine references, and taxi distance. This research stands out for its originality, as it has not been preceded by similar works. As future work, workshops with students and teachers are planned to gather statistical results that allow evaluating the usefulness of the activity, as well as considering possible modifications for its continuous improvement.

Acknowledgment

This research is possible thanks to the agreement between Atlantis SL and the University of La Laguna, the Cybersecurity Chair financed by Binter SA, and the grant PID2022-138933OB-I00 funded by MCIN/AEI/ 10.13039/501100011033 and the European Union NextGenerationEU/PRTR.

References

[1] NIST: "PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates", *NIST News*, 2022. [Online], Available in: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

[2] Deeb, F.A., Hickey, T.J. Teaching introductory cryptography using a 3D escape-the-room game. IEEE Frontiers in Education Conference. 2019.

[3] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J., Schwabe, P., Seiler, G., Stehlé, D., "CRYSTALS-Kyber algorithm specifications and supporting documentation", NIST PQC Round, vol. 2, no. 4, pp. 1–43, 2019.

[4] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D., "CRYSTALS-Dilithium: Algorithm specifications and supporting documentation (version 3.1)", NIST Post-Quantum Cryptography Standardization Round, vol. 3, 2021.

[5] National Institute of Standards and Technology (NIST), "FIPS 203 (Draft) Module-Lattice-based Key-Encapsulation Mechanism Standard", 2023. [Online], Available in: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf

[6] National Institute of Standards and Technology (NIST), "FIPS 204 (Draft) Module-Lattice-Based Digital Signature Standard", 2023. [Online], Available in: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf

[7] Fouque, P., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte,W., Zhang, Z., "Falcon: Fast-Fourier lattice-based compact signatures over NTRU.", *Submission to the NIST's post-quantum cryptography standardization process*, 2018.

[8] "Una breve introducción a la teoría de retículos", 2024. [Online], Available in: https://www.geogebra.org/m/cm2e42fk

[9] GeoGebra. (s/f). GeoGebra. Disponible en: https://www.geogebra.org/

[10] Arbain, N., Shukor, N. A., "The Effects of GeoGebra on Students Achievement". *Procedia - Social and Behavioral Sciences*, vol. 172, pp. 208–214, 2015. [Online], Available in: https://doi.org/10.1016/j.sbspro.2015.01.356

[11] Dogan, M., İçel, R. "The role of dynamic geometry software in the process of learning: GeoGebra example about triangles". *Journal of Human Sciences*, vol. 8, pp. 1441—1458. [Online], Available in: https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/1547

[12] Government of Spain, "LOMLOE: Nueva ley de educación", Ministerio de Educación, Formación Profesional y Deportes.

[13] Ministerio de Educación y Formación Profesional y Deportes. "Real Decreto 217/2022, de 29 de marzo, por el que se establece la ordenación y las enseñanzas mínimas de la Educación Secundaria Obligatoria". *BOE*, núm. 76, de 30 March 2022. Reference: BOE-A-2022-4975.

[14] OECD (2023), PISA 2022 Results (Volume I): The State of Learning and Equity in Education, PISA, OECD Publishing, Paris, https://doi.org/10.1787/53f23881-en

[15] Instituto Nacional de Evaluación Educativa. "PISA 2022. Programa para la Evaluación Internacional de los Estudiantes. Informe español.",2023

[16] Águila Hernández, E.J., "Algunos Tópicos en Teoría de Aproximación", Undergraduate Thesis, University of La Laguna, 2023. [Online], Available in: https://riull.ull.es/xmlui/handle/915/33370

[17] López, Francisco J. Geometría III. Department of Geometry and Topology, University of Granada. Granada, Spain. [Online], Available in: https://www.ugr.es/~fjlopez/_private/Geometria_III.pdf

[18] El País. "Manhattan, distancias y "el juicio de Pitágoras"". Ciencia/Materia, 2016. [Online] Available in: https://elpais.com/elpais/2016/10/18/el_aleph/1476813443_840074.html