GeoGebra para introducir los fundamentos de la criptografía basada en retículos

Édgar Pérez-Ramos
Universidad de La Laguna
Tenerife, España
alu0101207667@ull.edu.es

Pino Caballero-Gil
Universidad de La Laguna
Tenerife, España
pcaballe@ull.edu.es

Héctor Reboso-Morales
Universidad de La Laguna
Tenerife, España
hreboso@ull.edu.es

***Resumen*—El avance y la amenaza que representa la computación cuántica plantean desafíos significativos para la seguridad de la información. Esta situación ha generado la necesidad imperiosa de desarrollar sistemas criptográficos capaces de resistir ataques cuánticos. En este contexto, la criptografía post-cuántica ha surgido como un campo de investigación crucial. Sin embargo, uno de los principales desafíos que enfrenta este campo es la escasez de recursos didácticos disponibles. El presente trabajo aborda esta problemática mediante la creación de recursos didácticos centrados en retículos utilizando GeoGebra. Se ha diseñado una actividad que introduce y relaciona los retículos con diversos conceptos matemáticos impartidos en el aula. La actividad desarrollada es totalmente novedosa y tiene como objetivo hacer más accesible la comprensión de la criptografía post-cuántica al proporcionar herramientas visuales y manipulables que ayuden a los estudiantes a interiorizar los principios matemáticos y computacionales implicados en la seguridad de la información en la era post-cuántica.**

***Index Terms*—Retículos, GeoGebra, Criptografía post-cuántica**

Tipo de contribución: Formación e innovación educativa

I. Introducción

En la actualidad, la criptografía juega un papel esencial en todas las tecnologías de la comunicación, ya que es necesaria para proteger la seguridad de los sistemas y mensajes. Entre las técnicas criptográficas más relevantes, el cifrado se utiliza para proteger secretos, mientras que la firma digital se emplea para verificar la autenticidad e integridad de documentos y mensajes digitales. Sin embargo, con el posible despliegue futuro de la computación cuántica, se ha descubierto que muchos algoritmos criptográficos utilizados actualmente en diferentes tecnologías, como RSA o ECDSA, serán totalmente vulnerables, motivo por el cual emana la necesidad de nuevos esquemas criptográficos resistentes a la llamada amenaza cuántica.

El Instituto Nacional de Normas y Tecnología (NIST) ha dedicado recientemente varios años de esfuerzo a la búsqueda de algoritmos estandarizados capaces de resistir los retos que plantea la computación cuántica. En 2022, se dieron a conocer los cuatro finalistas de este exhaustivo proceso, entre los que destacaban algoritmos como CRYSTALS-Kyber, [1], diseñado para el cifrado, y CRYSTALS-Dilithium, [2], destinado a las firmas digitales.

Desde entonces, se han dedicado numerosos esfuerzos a verificar la solidez de estos esquemas, dada la importancia que adquirirán en los próximos años. En particular, el NIST ha desarrollado recientemente los correspondientes borradores de los Estándares Federales de Procesamiento de la Información (FIPS), FIPS 203 [3] y FIPS 204 [4], que especifican el Mecanismo de Encapsulación de Claves Módulo-Lattice (ML-KEM) y el Algoritmo de Firma Digital Módulo-Lattice (ML-DSA), derivados de CRYSTALS-Kyber y CRYSTALS-Dilithium, respectivamente.

Los retículos son el factor común de la mayoría de los algoritmos resistentes a la cuántica (CRYSTALS-Kyber, CRYSTALS-Dilithium y FALCON, [5]). No obstante, la familiarización con los fundamentos de la teoría de retículos puede ser vista como una necesidad en diversos niveles educativos, con el fin de preparar de manera más efectiva a los futuros ingenieros y científicos.

Este trabajo se estructura de la siguiente forma: En primer lugar, en la Sección II se presentan las herramientas necesarias para comprender el trabajo. Se expone qué es el GeoGebra, se justifica para qué tipo de alumnado está enfocada la actividad y se introducen los conceptos matemáticos que se trabajan en el ejercicio. En la Sección III se desarrolla y explica la actividad, que puede consultarse en [6] y la sección IV trata sobre una propuesta de cuestionarios para la evaluación de la actividad. Por último, se dedica una última sección a los trabajos futuros y las conclusiones.

II. Preliminares

Los retículos son el objeto algebraico más predominante en los estándares tanto de cifrado como de firma actuales. En la literatura, el material didáctico disponible sobre los retículos suele ser escaso y en ocasiones puede llegar a ser complejo y abstracto para el alumnado poco experimentado. Es por ello que en este trabajo se ha desarrollado una serie de actividades con el software GeoGebra, [7].

GeoGebra es un proyecto de software de matemáticas libre que nació en el año 2001 por parte de Markus Hohenwarter. GeoGebra combina aspectos de la geometría, el álgebra, el cálculo y otros campos de las matemáticas. Es ampliamente utilizado en entornos educativos, desde escuelas primarias hasta niveles universitarios, así como por investigadores, profesionales en matemáticas y disciplinas relacionadas. Algunas características son:

- Interfaz dinámica: GeoGebra proporciona una interfaz dinámica que permite a los usuarios crear, manipular y explorar objetos matemáticos en tiempo real. Esto facilita la comprensión de conceptos matemáticos abstractos al permitir la visualización interactiva.
- Geometría interactiva: Los usuarios pueden construir y manipular figuras geométricas, como puntos, líneas, segmentos, polígonos, círculos y mucho más. Estas figuras

pueden ser arrastradas, rotadas, escaladas y modificadas fácilmente.
- Álgebra dinámica: GeoGebra permite trabajar con expresiones algebraicas, ecuaciones y funciones de manera interactiva. Los usuarios pueden graficar funciones, resolver ecuaciones, encontrar derivadas e integrales, y realizar manipulaciones algebraicas.
- Visualización de datos: GeoGebra permite la visualización de datos mediante la creación de gráficos de funciones, diagramas de dispersión, histogramas y otros tipos de representaciones visuales. Esto facilita el análisis y la interpretación de datos en contextos matemáticos y científicos.
- Herramientas adicionales: Además de sus capacidades principales en geometría y álgebra, GeoGebra también incluye herramientas para trabajar con cálculo diferencial e integral, estadísticas, probabilidad, y más.

Por tanto, por todas las ventajas anteriormente mencionadas, se ha escogido GeoGebra por su alta eficiencia y utilidad en entornos didácticos, como por ejemplo se evidencia en [8] y [9].

Este trabajo puede encajar a partir de 4º de ESO, incluyendo el Bachillerato, puesto que, como aparece en [10] tanto Matemáticas A como Matemáticas B coinciden en:

- Criterios de evaluación:
  - Competencia específica 7.2 " Seleccionar entre diferentes herramientas, incluidas las digitales, y formas de representación (pictórica, gráfica, verbal o simbólica) valorando su utilidad para compartir información."
- Saberes básicos:
  - Sentido espacial:
    - Figuras geométricas de dos y tres dimensiones. "Propiedades geométricas de objetos matemáticos y de la vida cotidiana: investigación con programas de geometría dinámica."
    - Movimientos y transformaciones. "Transformaciones elementales en la vida cotidiana: investigación con herramientas tecnológicas como programas de geometría dinámica, realidad aumentada..."
  - Sentido algebraico:
    - Pensamiento computacional. "Resolución de problemas mediante la descomposición en partes, la automatización y el pensamiento algorítmico."

Por otra parte, cabe destacar que una motivación fundamental para desarrollar este trabajo ha sido el último Informe PISA (se puede consultar en [11]), en el cual España ha obtenido su peor resultado desde que comenzó a realizarse dicha prueba. En particular, el alumnado español de último curso de ESO ha bajado 8 puntos en matemáticas respecto a la edición anterior. La evolución puede verse en Fig. 1

Por lo tanto, tras estos resultados crear material didáctico útil sobre matemáticas se vuelve de carácter urgente. La aspiración es abordar las deficiencias identificadas y fortalecer las habilidades numéricas y conceptuales de los estudiantes.

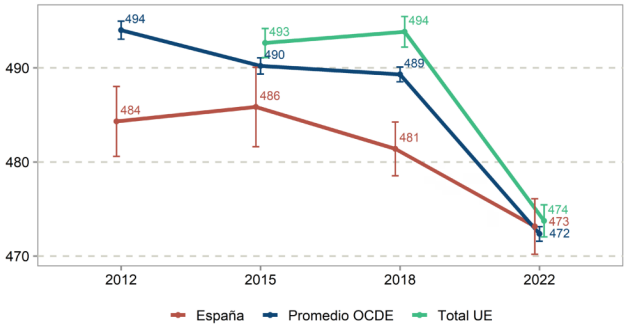

Figura 1. Evolución de las puntuaciones de matemáticas

Conceptos matemáticos

La actividad desarrollada en [6] tiene un doble propósito: emplear los principios matemáticos enseñados en Secundaria y Bachillerato para introducir la criptografía post-cuántica a los estudiantes, o utilizar la criptografía post-cuántica como herramienta para mejorar la comprensión de diversos conceptos matemáticos abordados en el aula. Estos conceptos incluyen:

- Retículos
- Producto escalar de dos vectores
- Ortogonalidad
- Sistema de referencia afín y usual
- Distancia euclídea y taxi

A continuación se procede a definir de manera formar los conceptos previamente mencionados.

Formalmente un retículo se puede definir de la siguiente forma:

Definición 1: Sean V un espacio vectorial sobre un cuerpo K, $\{v_1, v_2, \ldots, v_n\}$ una base de un subespacio vectorial de V, y A un anillo contenido en K. Entonces el retículo $\mathcal{L} \subset V$ generado por la base $\{v_1, v_2, \cdots, v_n\}$ es el conjunto:

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

Generalmente se considera que $A = \mathbb{Z}$ y para esta actividad $V = \mathbb{Z}^m$, de forma que el retículo $\mathcal{L}(v_1, v_2, \ldots, v_n)$ definido a partir de una base $v_i \in \mathbb{Z}^m$:

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

Por tanto, un retículo siempre se puede generar a partir de una base del espacio vectorial en el que se defina, mediante todas las combinaciones lineales de elementos de esa base. No obstante, lejos de esta formalidad, el mensaje que se quiere transmitir al alumnado es que un retículo no es más que las combinaciones lineales enteras de un conjunto de vectores y que distintas bases pueden dar lugar a un mismo retículo.

Definición 2: En un espacio vectorial $\mathbb{V}$, un producto interno (o producto escalar) es una aplicación tal que:

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

donde $\mathbb{V}$ es un espacio vectorial y $\mathbb{K}$ el cuerpo ordenado sobre el que está definido, siendo $\mathbb{R}$. Esta operación binaria

debe satisfacer las siguientes condiciones siendo $a, b \in \mathbb{K}$ y $u, v, w \in \mathbb{V}$:

- Linealidad tanto por la izquierda como por la derecha. Es decir:

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

y

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

- Hermiticidad: $\langle u, v\rangle = \langle \bar{v, u}\rangle$
- Definida positiva: $\langle u, u\rangle \geq 0$ y $\langle u, u\rangle = 0 \iff u = 0$, $\forall u \in \mathbb{V}$

Usualmente se suele representar a esta operación por "$\cdot$". Luego, si además consideramos $\mathbb{V} = \mathbb{R}^2$ y $\mathbb{K} = \mathbb{R}$ podremos considerar el producto escalar común que conocen los estudiantes de cursos de ESO y Bachillerato. Además, para conectar esta definición con los retículos sobre el plano, se recuerda la siguiente relación:

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

siendo $u, v \in \mathbb{R}^2$ y α el ángulo formado entre los dos vectores. A continuación se recuerda la definición de la norma, asociada a la Eq. 5. Para profundizar aún más sobre ello se puede consultar [12].

Definición 3: Un espacio vectorial $\mathbb{V}$ se denomina espacio normado, si para cada $x \in \mathbb{V}$, se define un número real, que se denota por $\| x \|$ y que satisface las siguientes propiedades:

- $\| x \| \geq 0, \ \forall x \in \mathbb{V}$ (Positividad)
- $\| x \| = 0 \iff x = 0, \ \forall x \in \mathbb{V}$ (Definido)
- $\| \alpha \cdot x \| = |\alpha| \cdot \| x \| \ \ \forall \alpha \in \mathbb{R}$ y $\forall x \in \mathbb{V}$ (Homogeneidad)
- $\| x + y \| \leq \| x \| + \| y \|, \ \forall x, y \in \mathbb{V}$ (Desigualdad triangular)

La cantidad $\| x \|$ es conocida como la norma de x. Generalmente, se denota como $(\mathbb{V}, \cdot)$ al espacio vectorial normado. En el caso de que no se verifique la segunda condición de la Def. 3 pero sí las restantes, se dice que $\| \cdot \|$ es una seminorma.

A partir de la Eq. 5 sabemos que si $\alpha = (2k + 1) \cdot \frac{\pi}{2}$, con $k \in \mathbb{Z}$ entonces $u \cdot v = 0$. Es en este instante donde se relaciona los retículos con el producto escalar y con la ortogonalidad, pudiendo así trabajar con retículos de bases ortogonales.

Definición 4: Dado un espacio vectorial $\mathbb{V}$ sobre un cuerpo $\mathbb{K}$ con un producto interno $\langle \cdot, \cdot \rangle$, dos vectores u y v en $\mathbb{V}$ se dicen ortogonales si su producto interno es igual a cero, es decir:

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

A continuación, para poder enlazar los retículos con bases ortogonales y el concepto tanto de sistema de referencia afín como cartesiano, nos basaremos en [13], donde se pueden consultar todas las definiciones y ejemplos necesarios.

Definición 5: Una colección de puntos $\{p_0, p_1, \ldots, p_k\}$, con $k \in \mathbb{N}$ en un espacio afín $\mathcal{A}$ se dice afínmente independiente si los vectores $\{\overrightarrow{p_0p_1}, \overrightarrow{p_1p_2}, \ldots \overrightarrow{p_{k-1}p_k}\}$ son linealmente independientes.

Definición 6: Dado un espacio afín $\mathcal{A}$ con $dim(\mathcal{A}) = n$, siendo $n \in \mathbb{N}$, un sistema de referencia $\mathcal{R}$ en $\mathcal{A}$ es un sistema de referencia ordenado $\{p_0, p_1, \ldots, p_n\}$ de $n + 1$ puntos afínmente independientes o equivalentemente satisfaciendo:

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

Una vez definido un sistema de referencia afín, se puede definir el sistema de referencia afín euclidiano en $\mathbb{R}^n$ o comúnmente llamado el usual o cartesiano.

Definición 7: En el espacio afín euclidiano $\mathbb{R}^n$ dotado de estructura afín canónica, el sistema de referencia

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

donde $B_0 = \{(1, 0, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)\}$ es la base canónica de $\mathbb{R}^n$, esto es, que todo punto $x \in \mathbb{R}^n$ se puede expresar en términos de $\mathcal{R}_0$

En general, en el aula se trabaja con el sistema de referencia definido por $\{(0, 0), (1, 0), (0, 1)\}$ en el caso del plano, y $\{(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ en el espacio. Cuando se trata de transmitir conceptos abstractos como la Def. 6 en el aula, el objetivo es enseñar que el producto escalar, ya sea 0 o distinto de 0, permite la creación de sistemas de referencia cartesianos o, alternativamente, la imposición de un sistema de referencia afín utilizando los puntos y vectores disponibles. Esto se hace con el fin de construir retículos que pueden tener bases ortogonales (un escenario usual) o bases no ortogonales. A través de este enfoque, los alumnos no solo comprenden cómo construir ejes perpendiculares que sigan una unidad de medida, sino que también aprenden a construir ejes que no sean perpendiculares utilizando puntos arbitrarios.

Por último, y a raíz de la Def. 8 introducimos la distancia taxi, la cuál sobre el plano puede tener una representación geométrica similar a la de los retículos. Este concepto permite tanto al docente como al alumnado agrupar las definiciones anteriores y acercarlas a la realidad, hacerlas un poco más tangibles.

Definición 8: La distancia taxi, también conocida como distancia de Manhattan o distancia rectilínea, es una métrica utilizada en geometría para calcular la distancia entre dos puntos en un espacio euclidiano con coordenadas rectangulares. Formalmente, la distancia taxi entre dos puntos $P(x_1, y_1)$ y $Q(x_2, y_2)$ en un plano euclidiano se expresa como:

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

Donde $|x_1 - x_2|$ representa la diferencia absoluta entre las coordenadas horizontales de los puntos y $|y_1 - y_2|$ representa la diferencia absoluta entre las coordenadas verticales de los puntos. La suma de estas diferencias absolutas proporciona la distancia taxi entre los dos puntos. En la Fig. 2 se puede observar un ejemplo ilustrativo sobre el siguiente concepto.

III. Actividad de GeoGebra

Como se mencionó anteriormente, la actividad desarrollada en [6] puede tener dos propósitos: emplear los principios matemáticos enseñados en Secundaria y Bachillerato para introducir la criptografía post-cuántica a los estudiantes, o utilizar la criptografía post-cuántica como herramienta para mejorar la comprensión de diversos conceptos matemáticos abordados en el aula.

Luego, a la hora de presentar dicho recurso, no es necesario que se impartan los contenidos matemáticos descritos en el

Figura 2. Ejemplo de la aplicación de la distancia taxi, [14]

presente trabajo. En cambio, la actividad puede servir como una manera alternativa de introducir esos conceptos o como un complemento motivador para reforzar los temas ya abordados en el aula.

Una breve introducción a la teoría de retículos

La actividad de GeoGebra titulada "Una breve introducción a la teoría de retículos", tiene por objetivo ofrecer nociones sobre la matemática subyacente a la criptografía post-cuántica, a través de breves definiciones y diferentes ejercicios, tanto de respuesta corta como respuesta larga y abierta.

En un primer instante, se presenta el por qué de la criptografía post-cuántica y la amenaza de la computación cuántica, de modo que el alumno sienta curiosidad por el tema. Acto seguido, se hace una comparación entre dos definiciones de retículo, tanto informal (ver Fig. 3) como formal (Def. 1).

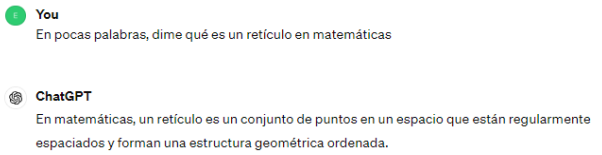

Figura 3. Definición informal de retículo

ChatGPT es una herramienta relativamente novedosa. Se ha elegido utilizarla en esta actividad (en particular al principio, para no perder el interés del lector) con el objetivo de generar un mayor compromiso por parte del alumnado. Dado que esta herramienta suele estar asociada a un estigma que la aleja de los entornos educativos convencionales, se busca presentar una definición atractiva que despierte el interés y la participación de los estudiantes.

Una vez se han dado las definiciones correspondientes, para reforzar estos conceptos se presentan ejemplos simples, representaciones dinámicas como se pueden ver en Fig. 4 y Fig. 5 y preguntas cortas y abiertas, como se puede observar en Fig. 6 y Fig. 7.

Una de las principales ventajas de estas representaciones dinámicas, es que el propio estudiante puede hacer variar los vectores y así ver reflejados los cambios. De esta manera, mediante el aprendizaje interactivo los estudiantes pueden manipular los conceptos y se involucran de manera directa

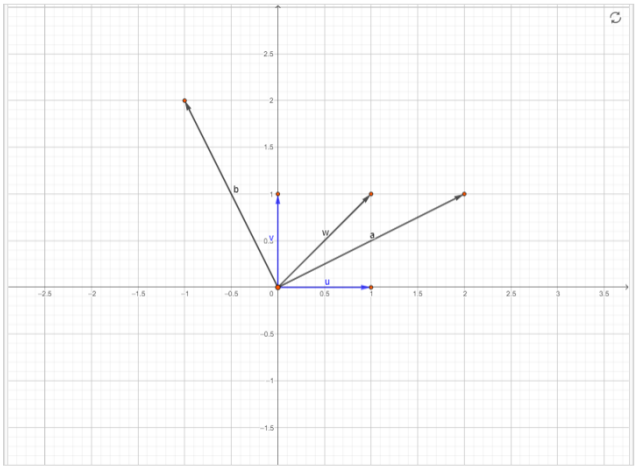

Figura 4. Primer ejemplo de los elementos de un retículo

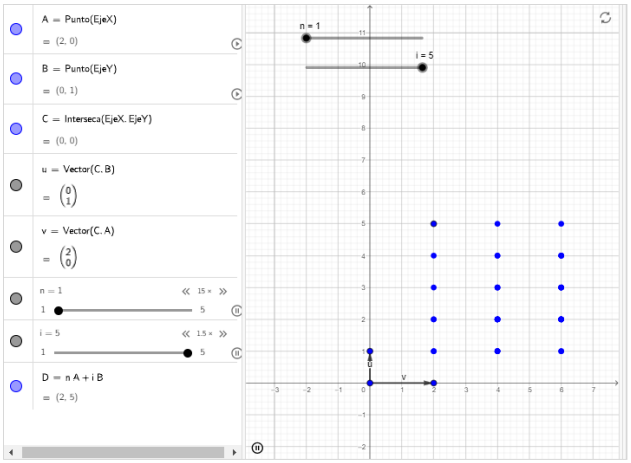

Figura 5. Ejemplo dinámico de los elementos de un retículo

en la construcción de su conocimiento. Es por ello, que también se propone la construcción de sus propios retículos en preguntas abiertas.

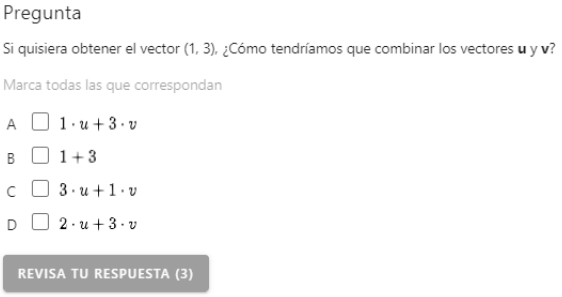

Figura 6. Primera pregunta corta

Además, como se puede observar en Fig. 8 se emplean también las representaciones dinámicas para demostrar de manera empírica que el único retículo nulo es aquel compuesto por los vectores nulos. De manera alternativa, el estudiante

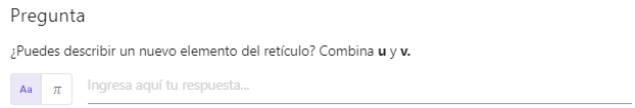

Figura 7. Pregunta abierta en la actividad

aprende de forma interactiva que al utilizar vectores no nulos con coeficientes infinitos, el retículo resultante será infinito.

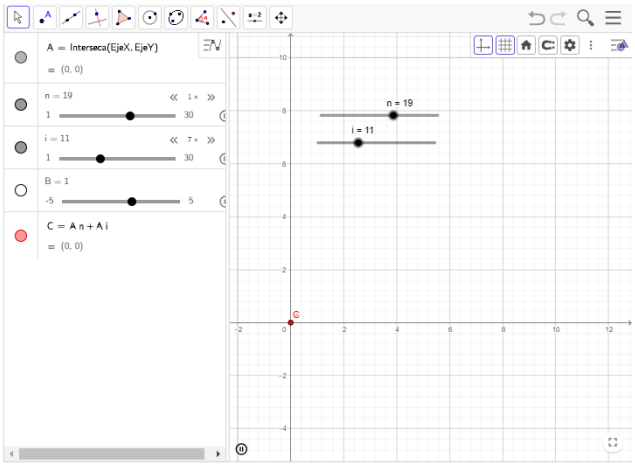

Figura 8. Retículo compuesto por vectores cero

En la segunda parte de la actividad, se busca intentar relacionar los conceptos mencionados anteriormente de forma que el lector pueda llegar a comprender sus conexiones con éxito. En este punto se hace mención al producto escalar entre dos vectores y derivando del mismo, la ortogonalidad. Así mismo, como se puede ver en Fig. 9 también se introducen los sistemas de referencia afines y usuales.

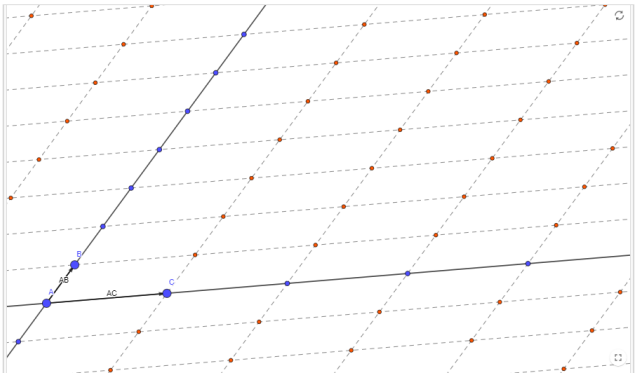

Figura 9. Retículo no ortogonal

Para completar la actividad y proporcionarle una conclusión más integradora y práctica, se mencionan las diversas ramas de las matemáticas, con especial énfasis en la geometría y la topología. Este enfoque nos conduce a la ya mencionada distancia taxi en Def. 8. Para este ejemplo práctico se ha propuesto una imagen de la ciudad de Barcelona con vista aérea, pues esta destaca por su disposición urbana, ordenada y representativa. Se puede observar en Fig. 10.

Figura 10. Barcelona desde el aire

Para aprovechar las capacidades de GeoGebra, se integra la Fig. 10 en el software y se superpone elementos de un retículo en cada intersección tanto de las calles verticales como horizontales (ver Fig. 11. Esto permite plantear al estudiante cómo llegar de un punto A a un punto B moviéndose únicamente a través de los puntos del retículo. De esta manera, se evidencia que la solución no es trazar una línea recta entre A y B, sino que existen múltiples rutas posibles, resaltando así la naturaleza no única de la solución y la aplicación directa y tangible de los conceptos aprendidos.

IV. Diseño de evaluación

Un primer estudio sobre el impacto del recurso didáctico propuesto podría realizarse con varias poblaciones, como puede ser un grupo de profesores y un grupo de alumnos. De este modo, podría medirse con más precisión el alcance del trabajo desarrollado, consiguiendo la opinión de los profesionales que imparten el recurso y la opinión de quienes lo reciben, a esta metodología la denominamos “Enfoque de Doble Audiencia”. La metodología es la siguiente:

- Se llevan a cabo varios cuestionarios durante el proceso: un primer cuestionario demográfico para comprender la composición de la población, un segundo cuestionario intermedio y un último cuestionario para evaluar el progreso a lo largo del taller.

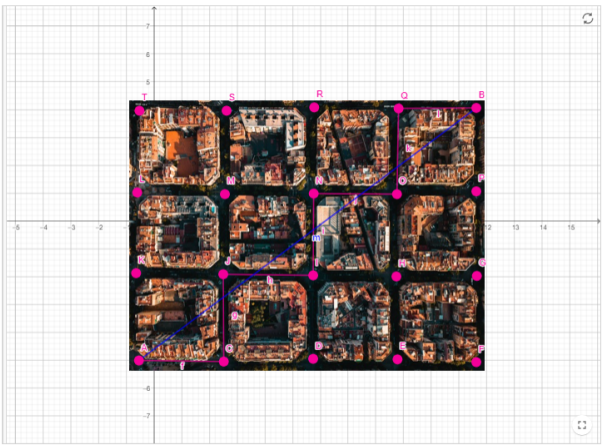

Figura 11. Distancia taxi sobre un retículo

- Después del cuestionario inicial, se sugiere realizar una charla donde se exponen el desarrollo y los fundamentos teóricos de la criptografía post-cuántica. Tras su finalización, la cual puede tener una duración variable de 20 a 30 minutos, se administra el cuestionario intermedio.
- En la segunda parte del taller, se presenta el recurso didáctico. Dependiendo de la audiencia (docentes o estudiantes), esta parte adopta un enfoque más pragmático, donde se muestra la utilidad de la herramienta para una mejor comunicación y explicación de los conceptos matemáticos, o más formativo, donde simplemente se exponen las relaciones y los términos matemáticos directamente al alumnado.

Las preguntas que se proponen para incluir en los cuestionarios son las siguientes:

- Preguntas a los docentes:
  - **Q1** ¿Sabes algo sobre las bases de la criptografía post-cuántica?
  - **Q2** ¿Te parecen sencillos los conceptos asociados a la criptografía post-cuántica?
  - **Q3** ¿Consideras que la criptografía post-cuántica puede tener interés en el aula?
  - **Q4** ¿Consideras que la criptografía post-cuántica puede aplicarse en el aula para explicar conceptos matemáticos?
  - **Q5** ¿Te parece útil la actividad desarrollada para comprender algunos conceptos de las matemáticas?
  - **Q6** ¿Te gustaría aplicar estas actividades en el aula?
  - **Q7** Indica el concepto que te parezca más interesante:
    - Retículo
    - Paralelepípedo
    - El problema de aprendizaje sobre errores
    - El problema del vector más corto
    - El problema del vector más cercano
    - Criptografía de clave pública
  - **Q8** ¿Qué concepto crees que sale más reforzado tras la actividad?
    - Producto escalar
    - Sistema de referencia
    - Combinaciones lineales de vectores
    - Ortogonalidad
    - Determinantes y matrices
- Preguntas al alumnado:
  - **Q1** ¿Sabes algo sobre las bases de la criptografía post-cuántica?
  - **Q2** ¿Te parecen sencillos los conceptos asociados a la criptografía post-cuántica?
  - **Q3** ¿Te parece interesante la criptografía post-cuántica?
  - **Q4** ¿Qué nivel de abstracción consideras que tiene la criptografía post-cuántica?
  - **Q5** ¿Te parece útil la actividad desarrollada para comprender algunos conceptos de las matemáticas?
  - **Q6** ¿Te han ayudado las actividades de GeoGebra a comprender los conceptos?
  - **Q7** Indica el concepto que te parezca más interesante:
    - Retículo
    - Paralelepípedo
    - El problema de aprendizaje sobre errores
    - El problema del vector más corto
    - El problema del vector más cercano
    - Criptografía de clave pública
    - Polinomios
  - **Q8** ¿Qué concepto consideras que sale más reforzado tras la actividad?
    - Producto escalar
    - Sistema de referencia
    - Combinaciones lineales de vectores
    - Ortogonalidad
    - Determinantes y matrices

Se sugiere responder a las preguntas **Q1** - **Q6** utilizando la escala de Likert, mientras que las preguntas **Q7** y **Q8** se abordan con respuestas múltiples. Cabe destacar que varias de las preguntas se repiten a lo largo de los cuestionarios que se realizan, de ese modo se permite medir la evolución y el impacto a lo largo del taller.

Conclusiones

Este trabajo ha presentado una metodología innovadora para la enseñanza de los retículos utilizando GeoGebra. Durante la actividad, se han explorado conceptos fundamentales del tema, como la estructura del propio retículo, mediante ejemplos dinámicos, preguntas de distinto tipo y su relación con otros conceptos aparentemente disímiles, como el producto escalar, la ortogonalidad, referencias afines y la distancia taxi. Esta investigación se distingue por su originalidad, al no haber sido precedida por trabajos similares. Como trabajo futuro, se planea llevar a cabo talleres con estudiantes y docentes para recopilar resultados estadísticos que permitan evaluar la utilidad de la actividad, así como contemplar posibles modificaciones en la misma para su mejora continua.

Agradecimientos

Este trabajo ha sido posible gracias al acuerdo entre Atlantis SL y la Universidad de La Laguna, y a las Cátedras de Ciberseguridad patrocinadas por Binter, y por INCIBE mediante iniciativa realizada en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiada por

la Unión Europea (Next Generation). Además forma parte del proyecto PID2022-138933OB-I00 financiado por MCIN/AEI/ 10.13039/501100011033/FEDER, UE.

REFERENCIAS

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

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

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

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

[5] P. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, "Falcon: Fast-Fourier lattice-based compact signatures over NTRU." *Submission to the NIST's post-quantum cryptography standardization process*, 2018, https://www.di.ens.fr/~prest/Publications/falcon.pdf

[6] Pérez, É. "Una breve introducción a la teoría de retículos", 2024. Disponible en: https://www.geogebra.org/m/cm2e42fk

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

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

[9] 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. Disponible en: https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/1547

[10] Ministerio de Educación y Formación Profesional. "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 de marzo de 2022. Referencia: BOE-A-2022-4975.

[11] Instituto Nacional de Evaluación Educativa. "PISA 2022. Programa para la Evaluación Internacional de los Estudiantes. Informe español.",2023. Disponible en: https://acortar.link/afkH6B

[12] Águila Hernández, E.J., "Algunos Tópicos en Teoría de Aproximación", Trabajo fin de grado, Universidad de La Laguna, 2023. [Online], Disponible en: https://riull.ull.es/xmlui/handle/915/33370

[13] López, Francisco J. Geometría III. Departamento de Geometría y Topología, Universidad de Granada. Granada, España. [Online], Disponible en: https://www.ugr.es/~fjlopez/_private/Geometria_III.pdf

[14] El País. "Manhattan, distancias y "el juicio de Pitágoras. Ciencia/Materia, 2016. Disponible en: https://acortar.link/8BQt7X