El juego de los abalorios: del Último Teorema de Fermat a los Solitones Ópticos

The glass bead game: from Fermat´s Last Theorem to Optical Solitons

DOI: 10.46932/sfjdv2n5-016

Received in: Jun1st, 2021
Accepted in: Sep 30th, 2021

Jorge Fujioka
Dr. en Ciencias (Física de Materiales)
Departamento de Sistemas Complejos,
Instituto de Física,
Universidad Nacional Autónoma de México.
Ciudad de México, CP 04510, México.
E-mail: fujioka@fisica.unam.mx

Alfredo Gómez Rodríguez
PhD in Physics
Departamento de Materia Condensada,
Instituto de Física,
Universidad Nacional Autónoma de México.
Ciudad de México, CP 04510, México.
E-mail: alfredo@fisica.unam.mx

Áurea Espinosa Cerón
Dra. en Ciencias (Física No Lineal)
Facultad de Ciencias,
Universidad Nacional Autónoma de México.
Ciudad de México, CP 04510, México.
E-mail: ecasmir@gmail.com

RESUMEN
Siguiendo la idea del Juego de los Abalorios (de Hermann Hesse), en este trabajo investigamos qué relación existe entre el último Teorema de Fermat (UTF) y los solitones ópticos. Para encontrar esta relación examinamos los pasos principales que condujeron a la demostración del UTF, empezando por la conjetura de Taniyama-Shimura, y pasando por las contribuciones de Hellegouarch, Frey y Ribet, hasta llegar al trabajo de Wiles. Posteriormente examinamos algunas de las ecuaciones que describen a los solitones ópticos. De este análisis se desprende que las curvas elípticas constituyen el puente que relaciona ambos temas. Veremos, además, que las ecuaciones que describen solitones ópticos también podrían tener alguna relación con la criptografía. Finalmente veremos que los resultados encontrados en este trabajo nos permiten proponer 2 conjeturas que constituyen temas de investigación para el futuro.

Palabras Clave: Último Teorema de Fermat, solitones ópticos, curvas elípticas, criptografía.

ABSTRACT
Following the idea of the Glass Bead Game (by Hermann Hesse), in this work we investigate what relation exists between Fermat´s Last Theorem (FLT) and the optical solitons. To find such a relationship we examine the principal steps which lead to the demonstration of FLT, starting from Taniyama-Shimura´s conjecture, then paying attention to the contributions of Hellegouarch, Frey and Ribet, and finally the

work of Wiles. Then we examine some of the equations which describe optical solitons. From this analysis it follows that the elliptic curves constitute the bridge that connects both topics. Moreover, we will observe that the equations which describe optical solitons might also be related to cryptography. Finally, we will see that the results found in this communication permit us to propose 2 conjectures that constitute research topics for future works.

Keywords: Fermat´s Last Theorem, optical solitons, elliptic curves, cryptography.

1 INTRODUCCIÓN

En su novela “El Juego de los Abalorios”, Hermann Hesse menciona que a lo largo del siglo XX los artistas, intelectuales y científicos fueron corrompiéndose paulatinamente, y en lugar de buscar un conocimiento verdadero, o la creación de auténticas obras de arte, empezaron a buscar simplemente prestigio, fama y dinero [1]. Y como reacción a ese estado de cosas empezaron a surgir grupos de verdaderos intelectuales, que anhelaban sinceramente una comprensión más profunda de la realidad, y un desarrollo verdadero de las artes. Estos grupos de intelectuales, artistas y científicos empezaron a organizarse en varios países de Europa, y posteriormente estas organizaciones se conectaron entre sí. Curiosamente, esta organización tenía una cierta similitud con las órdenes monásticas, pues se pedía que sus miembros, además de ser expertos en sus respectivas áreas, obedecieran un código ético y moral estricto. Por este motivo los integrantes de esta organización empezaron a referirse a ella como “la Orden”.

Dado que los miembros de la Orden provenían de áreas muy diversas, era necesario encontrar un común denominador que les permitiera sentirse hermanados entre sí. Y a partir de un ejercicio usual entre los músicos, se encontró que ese común denominador podía ser una especie de *juego*, que puede ser jugado de 2 formas distintas:

• Primera: dado un tema inicial (un tema musical, una figura, una ecuación, el inicio de un argumento literario, etc.), el jugador debe proponer extensiones o variantes interesantes, y estas extensiones pueden ser propuestas de manera alternada entre 2 o más jugadores. Y mientras más interesantes sean estas extensiones, mejor es el jugador.

• Segunda: dados 2 temas muy diferentes (posiblemente provenientes de campos totalmente distintos), el jugador debe encontrar alguna relación verdadera entre ellos (posiblemente encontrando una cadena de asociaciones que conecten a los 2 temas propuestos).

Dado que el origen de este *juego* apareció en la música, en un tiempo en que las notas de una partitura acostumbraban representarse por cuentas de vidrio (abalorios) que podían deslizarse a lo largo de alambres paralelos, los miembros de la Orden decidieron que su *juego* podría ser llamado ***“El Juego de los Abalorios”***.

En este trabajo mostraremos un ejemplo de este *Juego de los Abalorios*, y este ejemplo nos mostrará cómo el desarrollo de este juego nos ayuda a tener una comprensión más amplia de los temas que constituyeron el punto de partida del juego.

Tomaremos como punto de partida para iniciar el Juego de los Abalorios la siguiente propuesta:

Hállese alguna relación entre el Último Teorema de Fermat y los Solitones Ópticos.

Éste es un buen punto de partida para un Juego de los Abalorios, ya que los 2 temas propuestos no parecen tener ninguna relación entre sí. Así pues, es un juego no trivial.

Para poder hallar alguna relación entre los temas propuestos no basta saber qué dice el *Último Teorema de Fermat* (UTF) y qué son los *solitones ópticos* (SOs). Es necesario profundizar un poco más en estos 2 temas. Por lo tanto, en la Sección 2, no sólo recordaremos cuál es el enunciado del UTF, sino que examinaremos cómo se demostró este teorema. Y en la Sección 3 explicaremos qué son los SOs, y veremos cómo son algunas de las ecuaciones que describen a estas ondas. Una vez habiendo examinado estas cosas (los pasos esenciales de la demostración del UTF, y las ecuaciones típicas que describen SOs), en la Sección 4 pensaremos cómo podríamos hallar una relación entre estos 2 temas, ***y encontraremos esa relación***. Veremos que en el estudio del UTF y de los solitones ópticos aparecen *curvas elípticas*, de manera que estas curvas constituyen el punto de contacto entre estos 2 temas. Veremos también que las ecuaciones que describen pulsos luminosos, y que además se relacionan con las curvas elípticas, son ecuaciones que conducen a *problemas mal planteados* (en inglés: *ill-posed problems*), lo cual es algo inesperado e interesante. En la Sección 5 examinaremos qué posibles consecuencias tiene la aparición de curvas elípticas en el estudio de solitones ópticos. Veremos, en particular, que el hecho de que algunas de las ecuaciones que describen a los solitones ópticos estén relacionadas con curvas elípticas y con problemas mal planteados, sugiere que podría haber una relación entre este tipo de ecuaciones y la criptografía. Finalmente, mostraremos que el comprender el papel que juegan las curvas elípticas en la demostración del UTF, en la descripción de solitones ópticos, y en la criptografía, nos permite proponer 2 conjeturas que pueden dar lugar a investigaciones futuras.

2 EL ÚLTIMO TEOREMA DE FERMAT

El enunciado del Último Teorema de Fermat es muy sencillo. Este teorema afirma que *si* $n > 2$ *no existe ninguna terna de números enteros positivos* $\{x, y, z\}$ *que satisfagan la ecuación:*

$$x^n + y^n = z^n \tag{1}$$

Fermat escribió esta afirmación en el margen de un ejemplar de su propio libro de *Aritmética*, y además anotó el siguiente comentario:

Poseo una prueba en verdad maravillosa para esta afirmación a la que este margen viene demasiado estrecho.

Durante más de 300 años los matemáticos de todo el mundo intentaron descubrir cuál podría haber sido esa demostración de Fermat … sin encontrarla jamás. Sin embargo, en 1993 Andrew Wiles (un matemático inglés), anunció que había logrado demostrar el Último Teorema de Fermat (UTF) … pero esa afirmación no era del todo exacta. En primer lugar porque la demostración que presentó Wiles en 1993 tenía un error, y en segundo lugar porque lo que en realidad casi había demostrado Wiles, no era realmente el UTF, sino una forma restringida de ***la conjetura de Taniyama-Shimura***. Por lo tanto, para tener una idea más precisa de cómo se demostró realmente el UTF, es necesario conocer qué es la conjetura de Taniyama-Shimura, y cómo es que esa conjetura se relaciona con el UTF.

2.1 LA CONJETURA DE TANIYAMA-SHIMURA

En septiembre de 1955 se celebró en Tokio un congreso internacional de matemáticas, y un grupo de matemáticos jóvenes aprovecharon ese congreso para presentar una lista de 36 problemas no resueltos en los cuales ellos estaban trabajando. La idea era que los participantes del congreso contribuyeran con ideas que pudieran ayudar a la resolución de esos problemas. Cuatro de esos problemas habían sido propuestos por Yutaka Taniyama, un joven matemático de 27 años [2]. Sus problemas giraban en torno de 2 conceptos bastante diferentes: las curvas elípticas y las formas modulares.

Las curvas elípticas son curvas relativamente sencillas, descritas por ecuaciones de la forma:

$$y^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

siempre y cuando los coeficientes de la ecuación satisfagan la condición:

$$\Delta \neq 0 \tag{3}$$

donde Δ está definido por la expresión:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{4}$$

y las constantes b_n están definidas así:

$$b_2 = (a_1^2 + 4a_2)/a_0 \quad (5)$$

$$b_4 = (2a_4 + a_1a_3)/a_0 \quad (6)$$

$$b_6 = (a_3^2 + 4a_6)/a_0 \quad (7)$$

$$b_8 = (a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2)/a_0^2 \quad (8)$$

Las ecuaciones de la forma (2) son conocidas como *ecuaciones de Weierstrass* [3], y pueden describir curvas como las mostradas en las Figuras 4.2-1 y 4.2-2 de la Ref. [4]. La condición (3) garantiza que las curvas no tengan *puntos singulares*, en los cuales las curvas presenten picos o intersecciones, como en las gráficas de la Fig. 4.2-2 de [4]. Cuando esta condición se cumple decimos que la ec. (2) es una *ecuación de Weierstrass regular*, y su gráfica es una ***curva elíptica***. Por lo tanto, las gráficas mostradas en la Fig. 4.2-1 de [4] nos muestran las formas típicas de las curvas elípticas.

Las curvas elípticas, a pesar de su aparente sencillez, se relacionan con estructuras matemáticas sumamente complejas, como puede verse en las Refs. [3-5]. Sin embargo, para entender en qué consiste la conjetura de Taniyama-Shimura sólo necesitamos saber que cada curva elíptica puede asociarse con una sucesión de números enteros $\{a_1, a_2, a_3, \dots\}$, y esa asociación es una relación biunívoca, de manera que dada una curva elíptica, la sucesión que le corresponde $\{a_1, a_2, a_3, \dots\}$ constituye una especie de *huella digital*, que identifica exactamente a la curva elíptica dada. Conviene, pues, entender, cómo se calculan los números a_N de la sucesión $\{a_1, a_2, a_3, \dots\}$. Estos números son los coeficientes de una serie de potencias, a la cual se le llama usualmente *serie L*, y esta serie caracteriza unívocamente a la curva elíptica considerada.

Consideremos una ecuación elíptica particular. Fijémonos, por ejemplo, en la ecuación:

$$y^2 + y = x^3 + x^2 \quad (9)$$

y preguntémonos si habrá parejas de números **enteros** (x, y) que satisfagan esta ecuación. La respuesta es claramente SÍ, y la pareja $(x, y) = (2, 3)$ es un ejemplo. Pero si ahora nos preguntamos:

*¿cuáles son **todas** las parejas de enteros (x, y) que satisfacen la ecuación (9)?,*

¡no podremos contestar esta pregunta! No hay forma de saber cuáles son **todas** las parejas de enteros (x, y) que satisfacen (9). Ante esta imposibilidad a los matemáticos se les ocurrió algo muy interesante: buscar únicamente soluciones enteras (x, y) de la ecuación (9), tales que $0 \leq x \leq N$ y $0 \leq y \leq N$, donde N es un número natural, pero reemplazando el signo de igualdad que aparece en (9) por el

símbolo de *congruencia* (módulo *N*). Es decir, ahora nos preguntamos cuáles serán las soluciones enteras (x, y) de la congruencia:

$$y^2 + y \equiv x^3 + x^2 \pmod{N} \tag{10}$$

con $0 \leq x \leq N$ y $0 \leq y \leq N$. Una pareja (x, y) será solución de esta *congruencia* si las divisiones:

$$\frac{y^2 + y}{N}, \quad y \quad \frac{x^3 + x^2}{N} \tag{11}$$

dejan el mismo residuo. Por ejemplo, la pareja $(x, y) = (2, 1)$ es solución de la congruencia:

$$y^2 + y \equiv x^3 + x^2 \pmod{5} \tag{12}$$

ya que ambas divisiones, $(2^3 + 2^2)/5$ y $(1^2 + 1)/5$, tienen un residuo igual a 2.

Si ahora consideramos el caso en que $N = 1$, podemos ver que la congruencia:

$$y^2 + y \equiv x^3 + x^2 \pmod{1} \tag{13}$$

tiene 4 soluciones: $(x, y) = (0, 0), (0, 1), (1, 0)$ y $(1, 1)$. En el caso en que $N = 2$ tenemos 9 soluciones: $(0, 0)$, $(0, 1)$, $(0, 2)$, $(1, 0)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 1)$ y $(2, 2)$. En el caso en que $N = 3$ hay 10 soluciones: $(0, 0)$, $(0, 2)$, $(0, 3)$, $(1, 1)$, $(2, 0)$, $(2, 2)$, $(2, 3)$, $(3, 0)$, $(3, 2)$ y $(3, 3)$. Y en el caso en que $N = 4$ hay 14 soluciones: $(0, 0)$, $(0, 3)$, $(0, 4)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 3)$, $(2, 4)$, $(3, 0)$, $(3, 3)$, $(3,4)$, $(4,0)$, $(4,3)$ y $(4, 4)$. Y si ahora usamos el símbolo a_N para denotar el número de soluciones enteras (x, y), con $0 \leq x \leq N$ y $0 \leq y \leq N$, que satisfacen la congruencia (10), tendremos que:

$$a_1 = 4, \quad a_2 = 9, \quad a_3 = 10, \quad a_4 = 14, \quad \ldots \tag{14}$$

y podríamos calcular el valor de a_N para otros valores de *N*. Estos números definen la serie *L* correspondiente a la curva elíptica (9). Vemos, pues, que aunque no podemos calcular *todas* las soluciones enteras (x, y) de la ecuación (9), sí podemos calcular los valores de a_N para cualquier valor de *N* que deseemos.

Y ahora pasemos al segundo de los temas que aparecían en los problemas que Taniyama presentó en el congreso de 1955: las *formas modulares*.

Una forma modular es una función compleja de variable compleja $F(z)$ que satisface la siguiente condición:

$$F\left(\frac{az+b}{cz+d}\right) = (cz+d)^k\, F(z) \tag{15}$$

donde *a*, *b*, *c*, *d* y *k* son enteros tales que $ad - bc = 1$, y *z* es un complejo con parte imaginaria positiva.

A cada una de estas funciones se le puede asociar una serie de potencias, a la cual llamaremos *serie M* [5], la cual caracteriza de forma unívoca a la forma modular.

Y ahora podemos entender lo que Taniyama encontró un poco antes del congreso de 1955. Al calcular la serie M de una forma modular que le interesaba, Taniyama se dio cuenta que los primeros términos de esa serie coincidían con los primeros términos de la serie L de una curva elíptica que había estudiado con anterioridad. Esto le llamó la atención, y calculó más términos de la serie M de la forma modular, y más términos de la serie L de la curva elíptica … y también coincidieron. Taniyama compartió este descubrimiento con Goro Shimura, un amigo suyo que también se interesaba en las formas modulares y las curvas elípticas. Y entre los 2 examinaron más formas modulares, y encontraron que en cada caso era posible encontrar una curva elíptica cuya serie L coincidía con la serie M de la forma modular. En base a estas observaciones intuyeron que *debería existir una relación biunívoca entre formas modulares y curvas elípticas*. Esta propuesta es la famosa *conjetura de Taniyama-Shimura*.

2.2 LAS CONTRIBUCIONES DE HELLEGOUARCH, FREY Y RIBET

En 1955 la conjetura de Taniyama-Shimura no parecía tener ninguna relación con el último teorema de Fermat (UTF). Sin embargo, 20 años después, Yves Hellegouarch encontró que la curva elíptica:

$$y^2 = x(x - a^p)(x - b^p) \tag{16}$$

con *a*, *b* y *p* enteros mayores que 2, tendría propiedades rarísimas si existiera otro entero *c* tal que:

$$a^p + b^p = c^p \tag{17}$$

Es decir, la curva elíptica (16) sería rarísima *si el último teorema de Fermat fuera falso*. Este hallazgo fue de una importancia capital para que el UTF pudiera ser demostrado, de modo que Yves Hellegouarch debe ser recordado siempre que se hable del UTF.

El siguiente descubrimiento central en la historia del UTF ocurrió en 1984. En ese año Gerhard Frey demostró (casi demostró) que si existieran enteros *a*, *b* y *c* que cumplieran (17) [es decir, *si fuera falso el UTF*], entonces la curva elíptica (14) no tendría una forma modular asociada. Es decir, Frey encontró que:

$$\textit{Si UTF fuera falso} \Rightarrow \textit{la conjetura de Taniyama-Shimura sería falsa}$$

y esto quería decir que:

$$\textbf{\textit{Si la conjetura de Taniyama-Shimura es cierta}} \Rightarrow \textbf{\textit{el UTF es cierto ¡!!!}} \qquad (18)$$

Es decir: ***Frey había demostrado que bastaba demostrar la conjetura de Taniyama-Shimura para demostrar el Último Teorema de Fermat !!!***

Sin embargo, poco después de que Frey anunciara su resultado, se encontró que en su demostración había un pequeño error. Pero en 1986 Ken Ribet logró corregir ese error, con lo cual se confirmó que la afirmación (18) sí era correcta. Por lo tanto, gracias a los trabajos de Taniyama, Shimura, Yves Hellegouarch, Gerhard Fey y Ken Ribet, se había descubierto un camino totalmente novedoso para demostrar el UTF: demostrar la conjetura de Taniyama-Shimura. Y este nuevo camino se veía prometedor, ya que para demostrar la conjetura de Taniyama-Shimura se podía utilizar la teoría ya existente sobre formas modulares.

2.3 ANDREW WILES

En cuanto el resultado de Frey-Ribet fue conocido, Andrew Wiles, un joven matemático inglés de 33 años, Wiles se dio cuenta de que posiblemente él podría demostrar la conjetura de Taniyama-Shimura.

Durante 7 años Andrew Wiles fue avanzando en la construcción de una prueba de la conjetura de Taniyama-Shimura. Y durante esos 7 años Wiles comprendió que bastaba demostrar una versión restringida de la conjetura de Taniyama-Shimura para probar el UTF. Finalmente, en 1993, Wiles anunció que había demostrado el UTF (en realidad lo que había demostrado era la versión restringida de la conjetura de Taniyama-Shimura), e hizo pública su demostración.

La demostración de Wiles era muy larga y complicada, y los expertos se llevaron un tiempo en revisar la demostración. Pero finalmente ¡encontraron un error en la demostración!.

Andrew Wiles pensó inicialmente que el error era fácil de corregir, pero después de examinar con cuidado el punto defectuoso de su demostración, se dio cuenta de que el problema era más serio de lo que había pensado al principio. Y después de algunos meses de intentos infructuosos por corregir su demostración, Wiles decidió pedirle a Richard Taylor, un profesor de Cambridge y antiguo estudiante suyo, que trabajaran juntos para tratar de encontrar cómo corregir la demostración defectuosa. Y después de 2 años de trabajo frenético, en 1995 Andrew Wiles publicó un artículo en el que presentaba una demostración intachable de la versión restringida de la conjetura de Taniyama-Shimura [6], con lo cual el UTF había quedado finalmente demostrado. Y Christopher Breuil, Brian Conrad, Fred Diamond y Richard Taylor demostraron en 2001 la conjetura completa de Taniyama-Shimura, finalizando así la aventura intelectual iniciada por Yutaka Taniyama y Goro Shimura en 1955 [7].

Así pues, la demostración del UTF no es el resultado del trabajo de un solo hombre. En realidad es el fruto del trabajo de al menos 6 personas:

Taniyama, Shimura, Hellegouarch, Frey, Ribet y Wiles

quienes fueron construyendo el camino que conduciría a la demostración del UTF a lo largo de 40 años (entre 1955 y 1995).

3 ECUACIONES CON SOLITONES ÓPTICOS

La propagación de ondas y los modelos no lineales son temas que aparecen en muchísimos sistemas: en el aire [8], en el agua [9], en los sólidos [10] y, de manera particularmente importante, en sistemas no lineales en los cuales puede propagarse la luz [11]. En este trabajo nos interesan los modelos que describen la propagación de pulsos de luz en fibras ópticas. Y, sobre todo, nos interesa un tipo de pulsos de luz particulares: los *solitones ópticos*. Empecemos, pues, esta sección, definiendo qué es un *solitón óptico*:

Un solitón óptico es un pulso luminoso
que puede propagarse por un medio no lineal sin dispersarse. (19)

A primera vista esta parecería ser una definición satisfactoria de lo que es un *solitón óptico*, pero involucra algo que no parece estar claramente definido: *un medio no lineal*. Y si intentamos dar definiciones "físicas" de lo que es "un medio no lineal", entraremos en un laberinto sin salida, ya que hay muchos sistemas físicos que pueden ser considerados "medios no lineales", y la física en cada uno de ellos puede ser muy diferente, de manera que no será evidente cuál es el común denominador (en términos físicos) entre estos sistemas.

Y la forma de evitar ese laberinto, es enfocar nuestra atención *en las matemáticas* que describen la propagación de la luz en estos sistemas. De esta forma podemos llegar a la siguiente definición:

Un medio no lineal es cualquier medio en el cual la propagación de la luz esté gobernada por una ecuación diferencial parcial no lineal (EDPNL), o por un sistema de ecuaciones de este tipo. (20)

Y de las definiciones (19) y (20) podemos concluir algo importante:

Un solitón óptico es una solución localizada de una EDPNL (o de un sistema de ecuaciones de este tipo) (21)

Esta afirmación es *muy importante*, ya que pone en evidencia que hablar de *solitones ópticos* implica (necesariamente) hablar de EDPNLs. No es posible hablar de *solitones ópticos* si no precisamos de qué EDPNL estamos hablando.

En vista, pues, que cada solitón óptico está asociado a una EDPNL (o a un sistema de EDPNLs), una buena forma de aproximarnos al estudio de los solitones ópticos es conocer cómo son las EDPNLs que gobiernan el comportamiento de estos pulsos. Por lo tanto a continuación mostraremos algunas de las ecuaciones que describen a estos solitones.

3.1 LA ECUACIÓN NLS

La ecuación central en el estudio de los solitones ópticos es la llamada "ecuación no lineal de Schrödinger" (NLS), la cual tiene la forma:

$$iu_z + \frac{1}{2}u_{tt} + |u|^2 u = 0 \tag{22}$$

en la cual *z* es la distancia a lo largo de una fibra óptica, *t* es el llamado *tiempo retardado* ($t = T - z/v$, donde T es el tiempo normal, y v es la velocidad de la luz en la fibra), y $u(z,t)$ es una función compleja que se relaciona con el campo eléctrico de la luz mediante la ecuación:

$$E(z,t) = \frac{1}{2}u(z,t)e^{i(\beta z - \omega t)} + c.c \tag{23}$$

donde β es el número de onda del láser, ω es su frecuencia, y "c.c." indica al complejo conjugado del primer término que aparece en el miembro derecho de (23).

La ecuación NLS es adecuada para describir el comportamiento de pulsos ópticos cuya duración temporal es cercana a 5 ps, y los solitones de la ec. (22) son soluciones de la forma:

$$u(z,t) = A\,\mathrm{sech}(At)exp\left(i\frac{A^2}{2}z\right) \tag{24}$$

donde *A* es una constante real arbitraria.

3.2 NLS CON DISPERSIÓN DE CUARTO ORDEN

Cuando queremos describir pulsos cuya duración es menor a 5 ps (1ps o menor) es necesario añadirle a la ec. NLS términos dispersivos de tercer y cuarto orden. En particular, si sólo añadimos dispersión de cuarto orden, tenemos una ecuación de la forma:

$$iu_z + \alpha u_{tt} - \varepsilon u_{4t} + |u|^2 u = 0 \tag{25}$$

la cual tiene solitones de la forma [12]:

$$u(z,t) = \left(\frac{3\alpha^2}{10\varepsilon}\right)^{1/2} sech^2\left[\left(\frac{\alpha}{20\varepsilon}\right)^{1/2} t\right] exp\left(i\frac{4\alpha^2}{25\varepsilon}z\right) \tag{26}$$

3.3 NLS CON NO-LINEALIDAD DE QUINTO ORDEN

Cuando queremos describir pulsos un poco más intensos que los que se usan habitualmente en las telecomunicaciones es necesario agregar en la ec. NLS términos no lineales de orden superior. En particular, podemos utilizar una ecuación de la forma:

$$iu_z + u_{tt} - \gamma_1|u|^2 u + \gamma_2|u|^4 u = 0 \tag{27}$$

la cual tiene *solitones algebraicos* de la forma [13]:

$$u(t) = \left(\frac{2\gamma_2}{3\gamma_1} + \frac{1}{2}\gamma_1 t^2\right)^{-1/2} \tag{28}$$

y en el caso en que $\gamma_1 < 0$ también tiene solitones hiperbólicos de la forma [14]:

$$u(z,t) = \left[\frac{A}{B + \cosh(Dt)}\right]^{1/2} e^{i\Omega z} \tag{29}$$

donde Ω es una constante arbitraria positiva y *D*, *B* y *A* están definidas en la forma:

$$D = 2\sqrt{\Omega} \tag{30}$$

$$B = \left(1 + \frac{16\gamma_2}{3\gamma_1^2}\Omega\right)^{-1/2} \tag{31}$$

$$A = 2B\Omega \tag{32}$$

3.4 NLS CON DISPERSIÓN DE CUARTO ORDEN Y NO-LINEALIDAD DE QUINTO ORDEN

Si queremos describir pulsos cortos e intensos es necesario tomar en cuenta términos dispersivos y no lineales de órdenes superiores. La siguiente generalización de la ec. NLS es útil en esos casos:

$$iu_z + \varepsilon_2 u_{tt} - i\varepsilon_3 u_{ttt} + \varepsilon_4 u_{4t} + \gamma_1|u|^2 u - \gamma_2|u|^4 u = 0 \tag{33}$$

y en este caso los solitones tienen la forma [15]:

$$u(z,t) = A\, sech\left(\frac{t - az}{w}\right) e^{i(qz+rt)} \tag{34}$$

donde:

$$A = \left(\frac{6}{5\gamma_2}\right)^{1/2}\left[\gamma_1 - \left(2\varepsilon_2 + \frac{3}{4}\frac{\varepsilon_3^2}{\varepsilon_4}\right)\left(\frac{\gamma_2}{24\varepsilon_4}\right)^{1/2}\right]^{1/2} \tag{35}$$

$$w = \left(\frac{24\varepsilon_4}{\gamma_2}\right)^{1/4}\frac{1}{A} \tag{36}$$

$$a = 2\varepsilon_2 r + 8\varepsilon_4 r^3 \tag{37}$$

$$r = \frac{\varepsilon_3}{4\varepsilon_4} \tag{38}$$

$$q = -\varepsilon_2 r^2 - 3\varepsilon_4 r^4 + (\varepsilon_2 + 6\varepsilon_4 r^2)\left(\frac{\gamma_2}{24\varepsilon_4}\right)^{1/2} A^2 + \frac{\gamma_2}{24}A^4 \tag{39}$$

3.5 NLS DE ORDEN SUPERIOR CON DISPERSIÓN RAMAN Y AUTO-INCLINAMIENTO

Existen también generalizaciones de la ec. NLS que toman en cuenta efectos más finos, como la dispersión Raman y términos que tienden a inclinar los pulsos ópticos (llamados en inglés términos de *self-steepening*). La siguiente ecuación es un ejemplo:

$$iu_z + c_1 u_{tt} - ic_2 u_{ttt} + c_3 u_{4t} + c_4|u|^2 u - c_5|u|^4 u + ic_6|u|^2 u_t + ic_7(|u|^2)_t u = 0 \quad (40)$$

Los solitones de esta ecuación también tienen la forma que vemos en la ec. (34), pero ahora los parámetros *A*, *w*, *a*, *r* y *q* tienen otros valores, definidos por las siguientes ecuaciones [16]:

$$r = \frac{1}{24c_3}\left[6c_2 + (c_6 + 2c_7)\left(24\frac{c_3}{c_5}\right)^{1/2}\right] \quad (41)$$

$$\frac{20c_3}{w^2} = 12c_3 r^2 - 2c_1 - \left[6c_2 - \frac{6c_6(c_2 + 4c_3 r)}{c_6 + 2c_7}\right] r - \frac{6c_4(c_2 - 4c_3 r)}{c_6 + 2c_7} \quad (42)$$

$$A = \left(24\frac{c_3}{c_5}\right)^{1/4}\frac{1}{w} \quad (43)$$

$$a = -4c_3 r\left(\frac{5}{w^2} + r^2\right) + c_2\left(\frac{5}{w^2} + 3r^2\right) - \frac{6}{w^2}(c_2 - 4c_3 r) + 2c_1 r \quad (44)$$

$$q = c_3\left(\frac{5}{w^4} + \frac{6r^2}{w^2} + r^4\right) - c_2 r\left(\frac{3}{w^2} + r^2\right) - c_1\left(\frac{1}{w^2} + r^2\right) - \frac{\beta_1}{A} \quad (45)$$

donde hemos definido:

$$\beta_1 = c_5 A^5 - A^3(c_4 - c_6 r) \quad (46)$$

Estos son algunos ejemplos de EDPNLs que tienen solitones entre sus soluciones. Existen muchas otras EDPNLs con solitones, pero el conocer las 5 ecuaciones que hemos mencionado arriba será suficiente para que encontremos una relación entre los solitones ópticos y el último teorema de Fermat.

4 ÚLTIMO TEOREMA DE FERMAT Y SOLITONES ÓPTICOS

Una vez habiendo visto los pasos esenciales que condujeron a la demostración del UTF, y algunas de las EDPNLs que describen la propagación de solitones ópticos, estamos en condiciones de empezar a buscar qué relación podría haber entre estos 2 temas tan diferentes: el UTF y los solitones ópticos.

Si revisamos el proceso que condujo a la demostración del UTF notaremos que hay un concepto geométrico sencillo que jugó un papel absolutamente central en esa demostración: el concepto de *curva elíptica*. Y ya teniendo esta idea en mente nos podemos preguntar si las curvas elípticas tendrán alguna relación con los solitones ópticos …

Es bastante claro que las curvas elípticas no parecen estar relacionadas con *la forma* de los solitones ópticos. Y tampoco parece que aparezcan curvas elípticas entre las ecuaciones que relacionan a los parámetros que definen a los solitones ópticos (altura, anchura, número de onda, velocidad, …, etc.). Sin embargo, si pensamos en cada uno de esos parámetros, recordaremos que *los números de onda de los solitones* frecuentemente se estudian junto con *las relaciones de dispersión* de los sistemas donde se propagan los solitones. Es decir, casi siempre, al estudiar un sistema donde es posible la propagación de solitones, uno examina cómo es *la relación de dispersión* $k(\omega)$, la cual nos dice cómo se relacionan los números de onda y las frecuencias de *los modos de radiación* (*i.e.*, las ondas lineales de pequeña amplitud) capaces de propagarse en el sistema. En el caso de solitones "normales", los números de onda de los solitones estarán siempre fuera del rango de la relación de dispersión. Dicho de forma geométrica: si dibujamos la curva $k(\omega)$, y dibujamos una recta horizontal $k = k_{sol}$ (donde k_{sol} es el número de onda del solitón), encontraremos que esa recta horizontal *no intersecta a la curva* $k(\omega)$. Sin embargo, existe una clase especial de solitones, denominados *solitones embebidos*, cuyo número de onda sí intersecta a la relación de dispersión $k(\omega)$. Es decir, el número de onda del solitón k_{sol} está inmerso (*embebido*) en el rango de la función $k(\omega)$. Hasta antes de 1997 se creía que era imposible que un solitón tuviera un número de onda que estuviera dentro del rango de la relación de dispersión, pues se pensaba que si eso sucediera, sería inevitable que el solitón entrara en resonancia con las ondas lineales de pequeña amplitud, lo cual conduciría eventualmente a la destrucción del solitón. Sin embargo, en 1997 se encontró un ejemplo de un solitón "extraño", que tenía un número de onda que estaba dentro del rango de $k(\omega)$, *y no se producía la resonancia esperada* [17]. Esto fue una sorpresa, pero posteriormente se empezaron a encontrar otros solitones de este tipo, y se acuñó el término "*solitón embebido*" para referirnos a estos peculiares solitones [18,19].

A raíz del descubrimiento de los solitones embebidos, *siempre* que se encuentran nuevos solitones es preciso examinar si sus números de onda, k_{sol}, están dentro del rango de la relación de dispersión del sistema estudiado, para saber si se trata de solitones *embebidos*, o son solitones "normales". De ahí que ahora se ponga más atención en la forma de las curvas $k(\omega)$. Sabiendo esto, resulta comprensible que nos preguntemos:

¿es posible tener una relación de dispersión $k(\omega)$ *con forma de curva elíptica?*

Si examinamos las 5 ecuaciones mencionadas en la sección anterior encontraremos que en esos 5 casos las relaciones de dispersión están dadas por ecuaciones de la forma:

$$k = c_3\omega^4 + c_2\omega^3 - c_1\omega^2 \tag{47}$$

que no son curvas elípticas. Sin embargo, en el caso en que $c_3 = 0$ el miembro derecho de (47) ya se parece al miembro derecho de la curva elíptica (9) [si identificamos x con ω]. Para tener una curva elíptica sólo necesitaríamos que en el miembro izquierdo de (47) apareciera un término cuadrático k^2. Por lo tanto, la pregunta crucial es:

¿hay alguna razón física que justifique la aparición de un término k^2 en el miembro izquierdo de (47)?

Si pensamos en esta pregunta veremos que en la relación de dispersión $k(\omega)$ aparecería un término c_0k^2 si en la ecuación tuviéramos un término de la forma c_0u_{zz}. ¡Y este término sí debería aparecer en la ecuación NLS y en sus generalizaciones, pero usualmente se desprecia! Es decir, la ecuación:

$$iu_z + c_0u_{zz} + c_1u_{tt} - ic_2u_{ttt} + |u|^2u = 0 \tag{48}$$

sí es una ecuación físicamente realista, que describe la propagación de pulsos cortos en fibras ópticas. Sin embargo, usualmente se desprecia el término c_0u_{zz} aduciendo la aproximación conocida en inglés como "*slowly varying envelope approximation*" (SVEA). De acuerdo a este argumento, el término c_0u_{zz} se desprecia porque es más pequeño que los demás. Sin embargo, esto no es del todo cierto. Es verdad que el término c_0u_{zz} puede ser un poco más pequeño que los otros términos que aparecen en (48), pero *la auténtica razón* por la cual este término se elimina, es porque si se mantiene este término en la ecuación, el problema de condiciones iniciales para esta ecuación resulta ser *un problema mal planteado* (en inglés: *ill-posed*), y es casi imposible resolver numéricamente este tipo de problemas.

Tenemos, pues, que la ecuación (48) es una ecuación físicamente realista, y su relación de dispersión es:

$$k + c_0k^2 = c_2\omega^3 - c_1\omega^2 \tag{49}$$

¡que es precisamente una curva elíptica! En las Figs. 1 y 2 de la Ref. [20] podemos ver las formas que toma esta curva cuando $(c_0, c_2, c_3) = (1/30, 1/2, 1/15)$ y cuando $(c_0, c_2, c_3) = (1/40, 1/2, 1/50)$. Estas curvas son inesperadas. Nunca antes de la publicación de la referencia [20] se habían reportado

relaciones de dispersión con estas formas. La curva que se observa en la Fig. 2 de [20] es particularmente interesante. De acuerdo a esta curva hay 2 intervalos de frecuencia *prohibidos*:

$$\omega < 10\left(1-\sqrt{2}\right) \qquad \text{y} \qquad 5 < \omega < 10\left(1-\sqrt{2}\right)$$

La existencia de intervalos de frecuencias prohibidas podría parecer una predicción poco realista en el contexto de los solitones ópticos. Sin embargo, en el 2003 se encontró experimentalmente que en fibras ópticas construídas con cristales fotónicos realmente se observan intervalos de frecuencias prohibidas [21]. Por lo tanto, sí es posible la existencia de sistemas físicos cuyas relaciones de dispersión estén dadas por curvas elípticas.

De esta forma hemos alcanzado el objetivo de nuestro Juego de Abalorios: hemos encontrado una relación entre el UTF y los solitones ópticos. En ambos temas aparecen curvas elípticas. Las curvas elípticas son, pues, el punto de unión entre ambos temas.

5 DISCUSIÓN Y CONCLUSIONES

Como se mencionó en la Introducción, el Juego de los Abalorios que nos describe Hermann Hesse en su novela de 1943 se puede presentar de 2 formas distintas. En la primera forma se le propone un tema inicial al jugador, y éste debe construir generalizaciones, variantes, o extensiones de ese tema. Y en la segunda forma se le proponen 2 temas diferentes al jugador, y éste debe encontrar alguna relación oculta entre los temas propuestos. En este trabajo hemos considerado un Juego de los Abalorios del segundo tipo. Los 2 temas propuestos son:

• el Último Teorema de Fermat (UTF),

• los solitones ópticos.

¿Qué relación existe entre estos 2 temas?

Contestar esta pregunta ha sido el objetivo de este trabajo.

Después de analizar los pasos esenciales que condujeron a la demostración del UTF, y algunas de las ecuaciones más importantes que describen a los solitones ópticos, encontramos que existe un concepto geométrico que juega un papel importante en ambos campos: ***las curvas elípticas***. Por lo tanto, el UTF y los solitones ópticos están relacionados entre sí porque en el estudio de ambos temas aparecen *curvas elípticas*. Esta es la respuesta a la pregunta planteada.

Debemos observar, además, que el hecho de que encontremos curvas elípticas al estudiar el UTF y a los solitones ópticos, no sólo nos indica que existe “alguna” relación entre ambos temas. Nos sugiere una idea más precisa.

En la sección 2 vimos que el punto de partida para demostrar el UTF fue el descubrimiento de Taniyama y Shimura de que había una relación inesperada entre curvas elípticas y formas modulares. Por otra parte, en la sección 4, vimos que una relación de dispersión $k(\omega)$ con forma de curva elíptica nos determina una generalización de la ecuación NLS. Tenemos, pues, 2 relaciones:

Formas modulares $\leftrightarrow$ Curvas elípticas Curvas elípticas $\leftrightarrow$ Variantes de la ec. NLS

y estas 2 relaciones sugieren que debe haber una tercera relación de la forma:

$$\text{Formas modulares} \leftrightarrow \text{Variantes de la ec. NLS} \tag{50}$$

Es decir: debe haber alguna variante de la ec. NLS que se relacione con formas modulares. ¿Y cómo podría ser esa relación? Pues, podría ser que existan *soluciones* para esa ecuación que puedan expresarse en términos de formas modulares. Podríamos, pues, proponer la siguiente *conjetura*:

Debe existir alguna variante de la ecuación NLS
que posea soluciones que se expresen en términos de formas modulares. (51)

Esta es una conjetura que jamás había surgido en el campo de los solitones ópticos. Hasta ahora nadie ha investigado si existe alguna relación entre formas modulares y ecuaciones tipo NLS. Es una idea un tanto intrigante, y probablemente merecería estudiarse con más profundidad en el futuro.

Es importante añadir que el hecho de que las ecuaciones tipo NLS se relacionen con curvas elípticas sugiere que estas ecuaciones podrían también relacionarse con otros campos en los que surgen estas curvas. Y uno de estos campos merece mencionarse explícitamente: la criptografía.

Entre los métodos para encriptar datos hay algoritmos basados en curvas elípticas. De hecho, hay todo un campo conocido en inglés como "*Elliptic Curve Cryptography*" [22-24]. Los algoritmos de encriptación de datos basados en curvas elípticas son muy interesantes, pero a primera vista no parecen poder relacionarse con ecuaciones diferenciales similares a la ec. NLS.

Sin embargo, al investigar qué variante de la ec. NLS podría conducir a una relación de dispersión con forma de curva elíptica, hallamos algo interesante: la ecuación (48), cuya relación de dispersión es una curva elíptica, es una ecuación cuyo problema de condiciones iniciales es *un problema mal planteado*. Y esto, además de ser una idea interesante por sí misma, ***establece un segundo vínculo entre solitones ópticos y criptografía***, ya que los algoritmos criptográficos están basados en procesos que son fáciles de recorrer en un sentido, pero muy difíciles de recorrer en el sentido opuesto. Esa es la esencia de un algoritmo de encriptación de datos. Y los *problemas mal planteados* son precisamente problemas que surgen en sistemas de ese tipo: sistemas en los que es fácil calcular la evolución del sistema en un sentido, pero en los que es casi imposible calcular la evolución en el sentido inverso. La ecuación de difusión

constituye un ejemplo de este tipo de sistemas. Si arrojamos varias gotas de tinta en un recipiente con agua, es fácil calcular cuál será la distribución de tinta 1000 horas después ($t = 1000\ hrs$). Pero, si lo que nos dan es la distribución final de la tinta al tiempo $t = 1000\ hrs$, y nos preguntan cuál fue la distribución inicial de tinta en el tiempo inicial $t = 0$, ¡será casi imposible que podamos contestar! Así pues, los *problemas mal planteados* cumplen exactamente el requisito esencial para crear un algoritmo de encriptación, y de hecho ya se han desarrollado algunos algoritmos basados en problemas mal planteados. Por lo tanto, tenemos que:

la criptografía se relaciona con curvas elípticas y problemas mal planteados,

y ahora, en este trabajo, hemos encontrado que:

las ecuaciones con solitones ópticos se relacionan con curvas elípticas y problemas mal planteados.

La similitud es sorprendente, y estas 2 premisas sugieren que podríamos proponer otra *conjetura* de la forma siguiente:

Debe ser posible construír algoritmos criptográficos
basados en ecuaciones diferenciales parciales que describan solitones ópticos. (52)

y esta es una idea que nunca antes había sido considerada.

Así pues, el Juego de los Abalorios propuesto inicialmente en este trabajo:

hallar alguna relación entre el UTF y los solitones ópticos,

el cual parecía un simple juego intelectual, sin consecuencias importantes, nos ha conducido a la formulación de 2 conjeturas interesantes [(51) y (52)]. Y el estudio de estas 2 conjeturas podría conducir a resultados interesantes en el futuro.

REFERENCIAS

1. Hermann Hesse, *El Juego de los Abalorios*, Alianza Editorial, 2020.

2. Simon Singh, *El Enigma de Fermat*, Editorial Planeta, 2010.

3. Carlos Ivorra Castillo, *Curvas Elípticas*, www.uv.es/ivorra/Libros/Elipticas.pdf

4. Alex Kasman, *Glimpses of Soliton Theory: The Algebra and Geometry of Nonlinear PDEs* (Chapter 4: *Elliptic curves and KdV traveling waves*), American Mathematical Society, The Student Mathematical Library, Volume 54 (2010).

3. J.S. Milne, *Elliptic curves*, BookSurge Publishing, 2006.

4. Andrew Wiles, Annals of Mathematics **141** (3) (1995) 443.

7. C. Breuil, B. Conrad, F. Diamond and R. Taylor, J. Am. Math. Soc. **14** (2001) 843.

8. S.T. Bustamante, K.S. Gutiérrez, J.C. Tay, V.S. Ruiz, J. Reto y N. Santamaría, South Florida Journal of Development **2** (4) (2021) 5049.

5. N. Akhmediev, A. Ankiewicz and M. Taki, Phys. Lett. A **373** (2009) 675.

10. M.M. Cortez, H.O. Cortez, G.L. Cortez, L.J. Cortez and D.E. Fuentes, South Florida Journal of Development **2** (1) (2021) 633.

6. Y.S. Kivshar and G.P. Agrawal, *Optical Solitons: From Fibers to Photonic Crystals*, Academic Press, 2003.

7. M. Karlsson and A. Höök, Optics Communications **104** (1994) 303.

8. J. Fujioka and A. Espinosa, J. Phys. Soc. Japan **65** (1996) 2440.

14. R.W. Micallef, V.V. Afanasjev, Y.S. Kivshar and J.D. Love, Phys. Rev. E **54** (1996) 2936.

9. A. Espinosa-Cerón, J. Fujioka and A. Gómez-Rodríguez, Physica Scripta **67** (2003) 314.

16. J. Fujioka and A. Espinosa, Chaos **25** (2015) 113114.

10. J. Fujioka and A. Espinosa, J. Phys. Soc. Japan **66** (1997) 2601.

18. J. Yang, B.A. Malomed and D.J. Kaup, Phys. Rev. Lett. **83** (1999) 1958.

19. J. Yang, B.A. Malomed, D.J. Kaup and A.R. Champneys, Mathematics and Computers in Simulation **56** (2001) 585.

11. J. Fujioka, A. Gómez-Rodríguez and A. Espinosa-Cerón, Applied Sciences **7** (4) (2017) 340.

21. X. Fang, N. Karasawa, R. Morita, R.S. Windeler and M. Yamashita, IEEE Photonics Technol. Lett. **15** (2003) 233.

12. J. Holden, *The Mathematics of Secrets*, Princeton University Press, 2017.

13. Andrea Corbellini, *Elliptic curve cryptography: a gentle introduction*, https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction

24. A. Fúster, L. Hernández, A. Martín, F. Montoya y J. Muñoz, *Criptografía, protección de datos y aplicaciones*, Alfaomega Grupo Editor, 2013.