CUADRADOS LATINOS Y CÓDIGOS SECRETOS: ACTIVIDADES CON LAS QUE INTERACTUAR EN EL AULA DE MATEMÁTICAS.

Raúl Manuel Falcón Ganfornina
Dpto. Geometría y Topología
Universidad de Sevilla
rafalgan@us.es

Óscar Jesús Falcón Ganfornina
Universidad de Sevilla
almijeri@hotmail.com

RESUMEN

El *"fenómeno Sudoku",* iniciado en España en el año 2005, ha alcanzado un éxito destacable. Tratándose de un juego en el que la lógica matemática está en todo momento presente, los Sudokus han logrado una adición que pocos pasatiempos han logrado crear anteriormente. Se han realizado publicaciones expresamente dedicadas únicamente a dicho juego y existen manuales acerca de cómo proceder para resolverlo satisfactoriamente. Sin embargo, no es tan conocido el hecho de que un Sudoku no es más que un caso particular de los denominados cuadrados Latinos, concepto introducido por Euler en 1783 y que en la actualidad ocupa a importantes matemáticos de todo el mundo, debido a las diversas aplicaciones que tienen dichos cuadrados en Economía o Criptografía.

Aprovechando este último aspecto, en el presente taller se mostrarán una serie de actividades lúdicas relacionadas con cuadrados Latinos y códigos secretos, las cuales pueden realizarse en el aula de Matemáticas, permitiendo un desarrollo lógico-matemático en el pensamiento del alumnado. Además de la técnica usual en la resolución de Sudokus, estas actividades permiten aunar técnicas de juegos tan conocidos como el *"Hundir la flota",* que consiste en descubrir en qué casillas se encuentran los barcos del oponente, o *"El Cluedo",* que consiste en descubrir quién es el asesino entre varios posibles candidatos. Por otra parte, el trabajo en equipo es fundamental si se quiere ganar en los juegos que vamos a proponer. En concreto, éste último aspecto fue la razón por la que estas actividades fueron propuestas a los alumnos y alumnas participantes en la fase regional de la XXII Olimpiada Matemática Thales, destinada al alumnado de 2º de E.S.O., organizada por la Sociedad Andaluza de Educación Matemática THALES y que se celebró en Sevilla entre los días 17 y 21 de mayo de 2006.

Actas de las XIII Jornadas sobre Enseñanza y Aprendizaje de las Matemáticas, pp. 95 - 98. Granada, 2007. ISBN: 84-611-2311-5

1. ALGUNAS NOCIONES SOBRE CUADRADOS LATINOS

Si bien no hace mucho tiempo que ha llegado a las secciones de pasatiempos de la mayoría de nuestros periódicos y revistas habituales, está claro que el *Sudoku* (término japonés que tiene su origen en la expresión *Suji wa dokushin ni kagiru – "los números deben permanecer solteros"*-) ha arrasado en España, al igual que ya lo había hecho anteriormente en el resto de países donde se había introducido. De hecho, en poco tiempo podremos disponer en nuestro país de una variante del mismo, el juego denominado *Kakuro*, el cual está instalado ya de por sí en varios países europeos, logrando una adición que supera si cabe a su predecesor. Ambos juegos se basan en el concepto de cuadrado Latino, introducido por Euler en 1783 como *"una nueva especie de cuadrado mágico"*. Euler también introdujo el concepto de cuadrados Latinos ortogonales, dando lugar a la noción de cuadrado Greco-Latino y a una conjetura que no se demostró falsa hasta 1960 por los matemáticos Bose, Shrikhande y Parker.

Un *cuadrado Latino de orden n* es una matriz *n x n* cuyos elementos son tomados de un conjunto de *n* símbolos $N=\{x_1, x_2,..., x_n\}$, de tal forma que cada símbolo aparece exactamente una vez en cada fila y exactamente una vez en cada columna. En nuestro caso tomaremos el conjunto $N=\{1,2,...,n\}$. Así, el siguiente es un ejemplo de cuadrado Latino de orden 4:

L_0 =

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Obsérvese que cada celda de un cuadrado Latino puede representarse por una terna *(f,c,s),* donde *f* y *c* corresponden respectivamente a la fila y a la columna en la que está situada la celda en cuestión, mientras que *s* es el símbolo que aparece en dicha celda. Así, en el caso anterior, se puede representar por ejemplo las celdas de la tercera fila a partir de las ternas (3,1,3), (3,2,4), (3,3,1) y (3,4,2).

Si en un cuadrado Latino eliminamos los símbolos de algunas de sus celdas obtenemos lo que se conoce como *cuadrado Latino parcial*. Se dice entonces que un cuadrado Latino parcial *P* está *contenido unívocamente* en un cuadrado Latino *L* si al completar las celdas vacías de *P* de tal forma que no se repita ningún símbolo por fila ni por columna, únicamente podemos obtener el cuadrado latino *L*. Así, el siguiente cuadrado Latino parcial está contenido unívocamente en el cuadrado Latino L_0 del ejemplo anterior:

P_0 =

*	*	*	4
*	1	*	*
3	4	*	*
*	*	2	*

En este sentido, obsérvese que lo que comúnmente es conocido como *un Sudoku de solución única* no es más que un cuadrado Latino parcial contenido unívocamente en un cuadrado Latino de orden nueve, que verifica además la regla de que en cada una de las nueve zonas en que está dividido aparecen a su vez los nueve símbolos correspondientes al Sudoku.

Indiquemos por último que se llama *conjunto crítico* de un cuadrado Latino *L* a cualquier cuadrado Latino parcial *P* contenido unívocamente en *L*, tal que si eliminamos cualquiera de las celdas no vacías de *P*, el cuadrado Latino parcial que resulta puede completarse a dos o más cuadrados Latinos. Así, en nuestro ejemplo, puede observarse que P_0 es de hecho un conjunto crítico de L_0.

Actas de las XIII Jornadas sobre Enseñanza y Aprendizaje de las Matemáticas, pp. 95 - 98. Granada, 2007. ISBN: 84-611-2311-5

2. CUADRADOS LATINOS Y CÓDIGOS SECRETOS

Los conjuntos críticos que acabamos de ver se usan en Criptografía para construir *esquemas de compartición de secretos*. Un tal esquema consiste en descomponer un secreto en m trozos, los cuales se reparten entre m personas distintas, de tal forma que cada persona por sí sola no puede recuperar el secreto a partir del trozo que posee, pero que, en cambio, si comparte su información con otros participantes del esquema, entonces dicho grupo de personas sí puede recuperar el secreto.

Un ejemplo concreto de esquema de compartición de secretos usando conjunto críticos es el siguiente (Cooper, Donovan y Seberry, 1994): El secreto a descubrir será un cuadrado Latino L fijado de antemano, cuyo orden se hace público. Los trozos a repartir entre los participantes serán entonces el conjunto de ternas (f,c,s) correspondientes a las celdas de L. De esta forma, si un grupo de participantes comparten sus ternas y obtienen un conjunto crítico de L, entonces dicho grupo podrá como consecuencia recuperar el cuadrado Latino L y por tanto lograr conocer el secreto. Para ello le bastará ir determinando de forma lógica las celdas de los participantes que no están en dicho grupo.

Así, si consideramos como secreto el cuadrado Latino P_0, haciendo público que es de orden cuatro, podemos obtener un esquema con 16 participantes, cada uno de los cuales dispondrá de una única terna de P_0:

$$P_0 = \{(1,1,1), (1,2,2), (1,3,3), (1,4,4), (2,1,2), (2,2,1), (2,3,4), (2,4,3), (3,1,3), (3,2,4), (3,3,1), (3,4,2), (4,1,4), (4,2,3), (4,3,2), (4,4,1)\}.$$

Como posibles grupos capaces de recuperar el secreto tendremos por ejemplo los dos siguientes:

$$\{(1,4,4), (2,2,1), (3,1,3), (3,2,4), (4,3,2)\};$$
$$\{(1,1,1), (1,4,4), (2,4,3), (3,1,3), (3,3,1), (4,3,2)\}.$$

3. ACTIVIDADES PARA INTERACTUAR EN EL AULA DE MATEMÁTICAS.

Pasamos seguidamente a exponer varios juegos donde se pueden aplicar las nociones anteriores. Es de suponer que el profesor o profesora ha dedicado un cierto tiempo a explicar la teoría anterior a su grupo de alumnos y alumnas.

Todas las actividades que presentaremos a continuación pueden realizarse con cualquier número de alumnos, sin más que tomar cuadrados Latinos de órdenes convenientes. En concreto, si tenemos un grupo de m alumnos y alumnas, lo ideal sería encontrar el mayor número natural n tal que $n^2 + 1 < m$. Como ejemplo, en la fase regional de la Olimpiada Matemática Thales teníamos $m = 42$ participantes, por lo que en dicha ocasión tomamos $n = 6$.

Atendiendo al número de alumnos, el profesor tendrá que disponer de antemano de cierta cantidad de:

- Fichas de cartulina, en cada una de las cuales aparezca un número del conjunto $\{1,2,...,n\}$.
- Cartulinas, en las que estará dibujada una tabla $n \times n$ con todas las celdas vacías.

El material anterior puede servir para cualquier juego y será manipulado por los alumnos, por lo que es conveniente realizarlo suficientemente resistente. Por otra parte, antes de decidir la actividad a realizar, el profesor o profesora debe fijar un cuadrado Latino de orden n y determinar las ternas correspondientes a cada una de sus n^2 celdas. Deberá entonces diseñar n^2 tarjetas de cartulinas, en cada una de las cuales escribirá una de las ternas anteriores. Es importante tener en cuenta que el docente debe ser la única persona que sepa de antemano cuál es dicho cuadrado Latino. Una vez disponga de las n^2 ternas, podrá realizar una de las siguientes actividades:

Actas de las XIII Jornadas sobre Enseñanza y Aprendizaje de las Matemáticas, pp. 95 - 98. Granada, 2007. ISBN: 84-611-2311-5

3.1 Primera actividad: Jugando a detectives para recuperar el secreto.

Para esta primera actividad se forma en primer lugar un grupo A de n^2 alumnos. El resto de los alumnos se dividen en dos grupos B y C (si $m - n^2$ es impar, uno de los grupos deberá tener un miembro más). Los miembros del grupo A permanecen sentados en sus lugares usuales, mientras que los grupos B y C se sientan en lugares apartados para evitar que se copien entre sí.

La dinámica a seguir es la siguiente:

- Se repartirán las tarjetas con las ternas del cuadrado Latino secreto entre los alumnos del grupo A, los cuales deberán cuidar de que nadie les vea sus tarjetas. Por su parte, se entregará una tabla $n \times n$ a cada uno de los grupos B y C, junto a n^2 fichas, cada n de las cuales corresponderá a un número distinto del conjunto $\{1,2,...,n\}$.
- A continuación, por turnos, los grupos B y C irán indicando en voz alta que quieren conocer el símbolo correspondiente a una determinada celda. Para ello indicarán la fila y la columna de la celda que quieren conocer. En ese momento, la persona del grupo A que disponga de la terna correspondiente a dicha celda se desplazará hasta donde se encuentra el grupo que ha solicitado la información, les entregará su tarjeta y se incorporará a dicho grupo.

- A medida que se vayan sucediendo los turnos, cada equipo deberá ir intentando completar el cuadrado Latino a partir de las ternas que vaya consiguiendo. Para ello se ayudará de la tabla y de las fichas que se les entregaron al principio del juego. Además, teniendo en cuenta que no se pueden repetir símbolos ni por filas ni por columnas, llegará un momento en que puedan aplicar la lógica para rellenar celdas sin necesidad de solicitarla al grupo A. En cualquier caso deberán ir apuntando las celdas que hayan pedido el otro equipo, aunque no sepan el símbolo que contienen, pues en otro caso, si solicitan una celda que ya ha sido pedida anteriormente, perderán el turno al no existir nadie en el grupo A que conserve la terna correspondiente.

- Si llegase un momento en que no quedase nadie en el grupo A, los grupos B y C podrán solicitar por turnos al otro equipo la entrega de la tarjeta correspondiente a una determinada celda.
- En el momento en que un grupo crea haber descubierto el cuadrado Latino lo hará saber en su turno correspondiente. En ese instante, el profesor deberá comprobar si efectivamente han descubierto el secreto. Si lo han hecho ganarán el juego. Si no, perderán el turno y deberán revisar cómo han ido completando las celdas vacías a partir de las ternas conocidas, pues en algún momento habrán supuesto erróneamente que una celda deba tener obligatoriamente un determinado símbolo.

El juego acabará cuando uno de los dos equipos consiga obtener el cuadrado Latino. Se puede observar por tanto una cierta similitud con el conocido juego de hundir los barcos, pues en ambos casos se solicita información acerca de la celda correspondiente a unas determinadas fila y columna.

Actas de las XIII Jornadas sobre Enseñanza y Aprendizaje de las Matemáticas, pp. 95 - 98. Granada, 2007. ISBN: 84-611-2311-5

3.2 Segunda actividad: Jugando a detectives para recuperar el secreto (variante).

La dinámica es análoga a la anterior actividad, si bien en esta ocasión, a partir de los $m - n^2$ alumnos que no forman parte del grupo A, se formarán más de dos equipos. De esta forma, el mecanismo es totalmente idéntico al anterior, salvo que ahora, cuando se agotan los miembros del grupo A, cada equipo deberá elegir a qué grupo solicita la tarjeta correspondiente a una determinada celda. Si ese grupo dispone de dicha tarjeta se la hará llegar. En caso contrario, el equipo que haya solicitado la información perderá el turno. Esta diferencia es de vital importancia en la dinámica de este segundo juego, pues ahora cada equipo deberá estar atento más que nunca a lo que pida cada uno de los otros grupos. De esta forma se podrá evitar solicitar una tarjeta a un equipo al que ya se le haya pedido esa misma tarjeta. En este sentido, esta actividad incorpora la técnica que se utiliza en el conocido juego de *"El Cluedo"* para encontrar al asesino.

3.3 Tercera actividad: Creando conjuntos críticos.

En esta actividad se pueden hacer cuantos grupos se estimen oportunos o bien dejar que los alumnos trabajen individualmente. Además, la dinámica de este juego difiere de la de los anteriores. En esta ocasión, los alumnos conocen el cuadrado Latino *L*. Lo que tienen que hacer, por turnos, es ir vaciando celdas, de tal forma que el cuadrado Latino parcial que se obtenga se complete unívocamente a *L*. Gana el juego el equipo que, tras vaciar una celda, obtenga un conjunto crítico de *L*. Aunque pueda parecer que es una actividad más sencilla que las anteriores, este juego requiere de una mayor concentración por parte de los participantes, pues para demostrar que un cuadrado Latino parcial es un conjunto crítico hay que probar que, eliminando cualquiera de las celdas que aún no están vacías, el cuadrado Latino parcial resultante puede completarse a al menos dos cuadrados Latinos. La dificultad de este tercer juego permite en particular que los alumnos comprueben que crear un Sudoku de solución única no es tan sencillo como pueda parecer.

4. CONCLUSIÓN FINAL

Desde nuestro punto de vista pensamos que las actividades propuestas fomentan en gran medida la participación e interés del alumnado, pues, en cierta medida, mezclan juegos bastantes conocidos por ellos. Al mismo tiempo, a medida que se repita alguna de las actividades, los mismos alumnos irán descubriendo técnicas que les ayuden a decidir qué celdas son las mejores para seleccionar en cada turno. En este sentido es recomendable favorecer las "*revanchas*" cuando éstas sean solicitadas, pues será señal de que la actividad les atrae y de que piensan que han encontrado la manera de ganar a los equipos rivales. En cualquier caso, el aprovechamiento que pueda resultar de las técnicas lógico-matemáticas implicadas debe venir dado por el profesor o profesora de la asignatura, si bien creemos segura la aceptación que esta actividad tendrá entre sus alumnado.

REFERENCIAS

COOPER, J. A., DONOVAN, D., SEBERRY, J., 1994. *Secret Sharing Schemes arising from Latin squares*. Bull. Inst. Combin. Appl. 12, pp. 33 - 43.