Dos juegos programables.

«En lugar de preocuparnos por lo que las máquinas pueden hacer,
debemos preocuparnos más por lo que todavía no pueden hacer.»

Garry Kasparov.

Propuesta para el alumnado.

Introducción.

"Si pudiera resucitar dentro de 500 años, lo primero que preguntaría es si ya se ha resuelto la Hipótesis de Riemman". Tal afirmación fue hecha por David Hilbert al ser preguntado por los retos más importantes que las matemáticas del s. XX tenían por delante. En la Unidad Didáctica "Aquellos Maravillosos años" tienes la oportunidad de entender el ambiente histórico y matemático en el que Hilbert formuló la respuesta que encabeza esta introducción.

Tanto Hilbert como sus coetáneos, contagiados por el ambiente de bonanza, felicidad y progreso que se vivía a finales del s. XIX y comienzos del s. XX, eran optimistas también en cuanto a la evolución y desarrollo de las Matemáticas. El Programa de Hilbert establecía algunas líneas maestras de la Física y las Matemáticas como preferentes para investigar en ellas, de tal forma que se alcanzase una fundamentación rigurosa de estas disciplinas. En particular, y aunque recibieron respuestas en el sentido contrario al esperado (puedes leer sobre los teoremas de Gödel) la propuesta de Hilbert sirvió como impulso para el desarrollo de la lógica. Y ésta, para establecer las bases de la computación moderna.

¿Qué es un *programa* de ordenador?

Un programa de ordenador es lo que en matemáticas recibe el nombre de algoritmo, es decir, una serie de pasos a seguir según ciertas reglas que, ejecutados de forma automática, producen cierto resultado. Lo que podríamos entender como los primeros programas de ordenador, fueron concebidos de forma abstracta por Ada Lovelace, alrededor de 1843, basándose en el uso de tarjeatas perforadas para la máquina analítica descrita por Charles Babbage. Indaga sobre los creadores de los primeros algoritmos y el uso de *tarjetas perforadas*.

Al comienzo los programas fueron concebidos como grandes calculadoras que ahorraban tiempo en operaciones matemáticas pero, posteriormente, se pensó en cualquier tarea susceptible de ser algoritmizada y, tras los mensajes encriptados durante la II Guerra Mundial, no tardaron en llegar los primeros computadores, videojuegos, internet, virus,... Busca información sobre la vertiginosa evolución de los ordenadores y los programas informáticos.

Dos juegos...

Proponemos dos actividades para recrear, a mano, dos algoritmos complejos.

Actividad 1: el juego de la vida.

Sobre hojas cuadriculadas, vamos a partir de un patrón de casillas coloreadas (¡las que quieras al inicio!) y seguiremos en cada paso unas instrucciones para borrar o pintar casillas. Ten en cuenta que cada casilla está rodeada de otras ocho adyacentes y, en cada turno, debes hacer (a la vez con todas las casillas, como si fuera un único paso) las siguientes modificaciones:

- Si una casilla está vacía...
  - y tiene justamente alrededor tres casillas coloreadas, entonces hay que colorearla.
  - en otro caso, continúa vacía.
- Si una casilla está coloreada...
  - y alrededor tiene dos o tres casillas coloreadas, seguirá coloreada.
  - en otro caso (si no hay ninguna, o solo hay una, o cuatro o más) se volverá vacía.

Tras experimentar diferentes situaciones, trata de sacar conclusiones sobre la evolución del juego.

Actividad 2: comunicación de mensajes con RSA.

Por grupos de tres, se asignan los roles de una persona, Alice (A), que quiere hacer llegar un mensaje a la otra persona, Bob (B), mientras que la tercera persona, Evil (E), quiere interceptar el mensaje y descubrirlo. Por simplicidad, Alice y Bob van a tratar de enviarse un número sin que Evil lo descubra. Alice y Bob deben comunicarse siguiendo los siguientes pasos:

- Alice elige dos números primos **p** y **q**. Calcula las multiplicaciones **n**=p·q y **m**=(p-1)·(q-1).
  - Elige un número **r**, tal que mcd(m,r)=1 y comunica a Bob los números **n** y **r.**
  - Antes de recibir el mensaje de Bob, calcula un número **s** tal que al hacer la multiplicación r·s quede resto 1 al dividir entre **m** (ver tablas de ayuda).
  - Cuando reciba de Bob el mensaje cifrado **c**, realiza la operación $\mathbf{c^s}$ y calcula el resto que deja al dividirlo entre **n**.
- Bob elige el número **x** que quiere transmitir a Alice.
  - Al recibir la clave de Alice, realiza la operación $\mathbf{x^r}$ y obtiene el resto de dividir entre **n**. Este será su mensaje **c** que está cifrado y comunica en alto, de tal forma que tanto Alice como Evil los conocen.
- Evil, al mismo tiempo que Bob le dice a Alice su mensaje cifrado, se le comunidcan los valores de **n**, **r** y **c**. Y si quiere espiar el mensaje que Bob le ha enviado a Alice, deberá:
  - factorizar **n**, calcular **m** y localizar la tarjeta de ayuda correspondiente para obtener el número **s** que ya tiene Alice.
  - realizar la operación $\mathbf{c^s}$ y calcular el resto que deja al dividirlo entre **n.**
  - Si Evil es capaz de obtener el mensaje antes que Alice, se considera que ha interceptado el mensaje y gana el juego. En otro caso, ganan Alice y Bob.

Guía para el profesorado.

Introducción:

La presente propuesta didáctica está algo alejada de los contenidos tradicionales que se abordan en la etapa de Educación Secundaria Obligatoria, pero pueden constituir una puerta de entrada al mundo de la programación, los algoritmos y los computadores. Es por ello que la Unidad Didáctica se puede desarrollar con dos o tres sesiones en cualquier momento del curso y sin prerrequisitos.

Para contextualizar históricamente la Unidad, se inicia con una frase referente a la hipótesis de Riemann, que comparte el enunciado del 8º problema, junto a la conjetura de Goldbach, de la lista de los 23 problemas que propuso Hilbert en el Congreso Internacional de Matemáticos del año 1900 en París. Aunque aún es demasiado pronto para que los alumnos puedan entender las herramientas matemáticas que se requieren para comprender la Hipótesis de Riemann, en la Unidad Didáctica *"Aquellos Maravillosos años"* hay algunas claves que se pueden explorar para entender el ambiente histórico y matemático en el que Hilbert formuló su lista de problemas.

Como consecuencia los teoremas de (in)completitud de Gödel, como resultado negativo a alguno de los problemas de la lista de Hilbert, y los resultados de, entre otros, Turing o Von Neumann, varios matemáticos coqueteaban con la idea de la fabricación de un ordenador en el sentido de máquina que, de forma automática y sin la intervención humana, fuera capaz de realizar acciones o tomar decisiones. Para ello, sería necesario establecer unas instrucciones que hicieran "funcionar" la máquina una vez inicializada.

Sesión 1: Surgimiento de los algoritmos y la computación.

Incluso antes de la inminente llegada de los computadores modernos, existieron algunos resultados teóricos que avanzaron la llegada de los autómotas. Lo que podríamos entender como los primeros programas de ordenador, fueron concebidos de forma abstracta por Ada Lovelace, alrededor de 1843, basándose en el uso de tarjetas perforadas para la máquina analítica descrita por Charles Babbage. El uso de tarjetas perforadas ha sido la forma habitual de introducir un programa de ordenador hasta la década de los 80 del s. XX. El sistema de numeración binario, la aritmética en módulo 2, ayuda a representar los estados de cada célula de la tarjeta (perforado=1, no perforado=0). Un programa de ordenador es, simplificando mucho, una serie de instrucciones que a cada paso "decide" qué hacer según el estado que encuentre en la sucesión de ceros y unos encadenados.

Al comienzo los programas fueron concebidos como grandes calculadoras que ahorraban tiempo en operaciones matemáticas pero, posteriormente, se pensó en cualquier tarea susceptible de ser algoritmizada. Las intuiciones y predicciones sobre la potencia que podrían alcanzar los autómatas fue rápidamente superada por la realidad, y aunque la fundamentación teórica avanzó en un siglo mucho más rápido que la capacidad tecnológica para construir las máquinas y los programas ideados por los matemáticos, con el tiempo, surgieron los primeros modelos de ordenador en el sentido moderno, y no tardaron en llegar los primeros computadores, videojuegos, encriptación de mensajes, internet, virus, inteligencia artificial,... Es de reseñar el avance que experimentó el campo de la computación desde el descifrazado del código de la máquina Enigma y, de ahí, el surgimiento del primer computador moderno, el ENIAC.

Sesión 2: El juego de la vida.

La primera actividad que se propone es ejecutar a mano una versión de "El juego de la vida" ideado por J. Conway en 1970, concebido como un autómata celular en el que las casillas de una cuadrícula cambian de estado (vacías=0, pintadas=1) según una serie de reglas concretas (las instrucciones del programa). La importancia de este juego radica en que se ha demostrado que es una máquina universal de Turing, concepto profundamente teórico que viene a decir que cualquier concepto computable algorítmicamente puede ser programado como un patrón del juego de la vida. La versión que aquí proponemos es, simplemente, ver la evolución que desarrollan partiendo de las diferentes piezas del tetris (o de cualquier otra configuración propuesta por el alumnado).

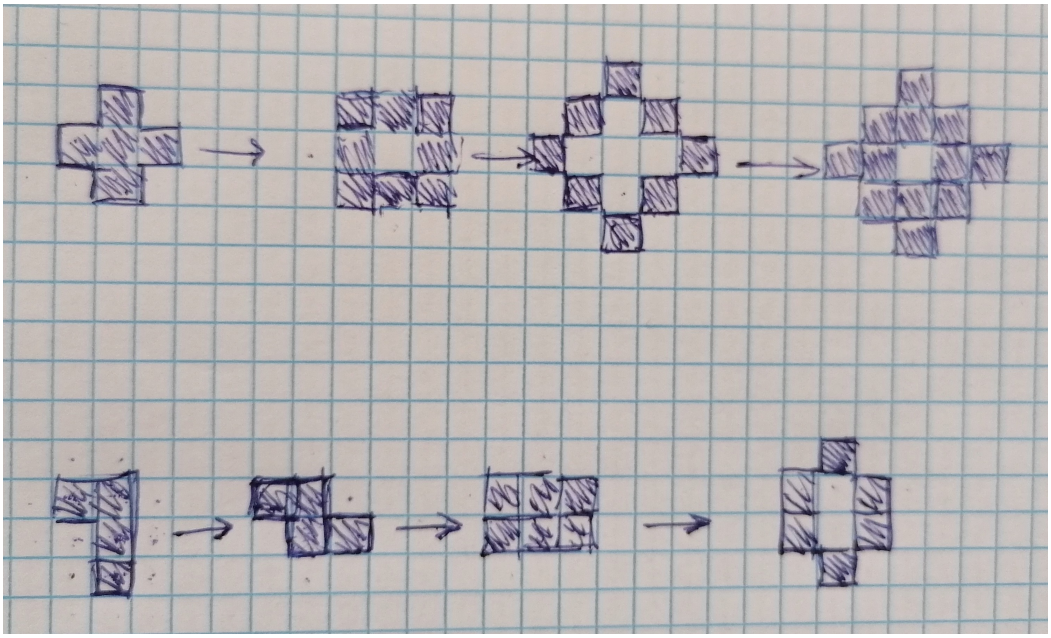

Imagen 1. Evolución de dos estados iniciales diferentes tras cuatro iteraciones del algoritmo

Se pueden explorar configuraciones más complejas y su evolución en el tiempo mediante el uso de cualquier recursos web, como por ejemplo este. Pueden realizarse conjeturas sobre las configuraciones que permanecen constantes, cuáles son periódicas, cuáles desaparecen, etc...

Sesión 3: el algoritmo RSA.

La segunda actividad, esta sí con contenido numérico, es el algoritmo RSA de encriptación de mensajes que se utiliza tan frecuentemente en las comunicaciones hoy día (fue ideado por Rivest-Shamir-Adleman, de ahí las siglas, en 1979). Evidentemente, las operaciones con números primos elevados son inabarcables para el alumnado, e incluso con primos bajos algunas son complicadas, y solo se pretende que sea un incentivo a la mejora del cálculo mental, manejando conceptos relativos a la aritmética modular según las instrucciones del algoritmo y entiendan la filosofía detrás de la idea informática de dos comunicadores intentando ser interceptados.

Una de las dificultades principales para romper el código RSA reside precisamente en la factorización de n, que en la práctica es un número con un elevado número de cifras al proceder

de la multiplicación de dos números primos grandes (y por tanto supone un coste computacional alto). Puesto que a poco que crecen p y q las operaciones se vuelven tediosas, los primos utilizados son pequeños y en esta versión del juego se propone sustituir la dificultad de la factorización por la de encontrar la tarjeta que facilita el inverso multiplicativo módulo **m** para la clave pública **r** de Alice (se sugiere confeccionar, recortar y barajar tarjetas).

Para realizar la potenciación modular, es recomendable reducir a cada paso los correspondientes cuadrados mediante las propiedades de potencias. Por ejemplo, para p=5, q=11 querríamos hacer 13^7 (mod 55). Se escribe: $13^7=(13^2)^3\cdot 13=169^3\cdot 13=49^3\cdot 13=...=7$ (mod 55). Para revertir la operación haremos 7^{23} que resulta ser, claro, 13 mod 55.

---

m=2 (p=2, q=3)

La única posibilidad es tomar r=1 y por tanto s=1.

---

m=4 (p=2, q=5)

Posibles r=1,3. Sus inversos son ellos mismos: 1·1=1 y 3·3=9, que dejan resto 1 al dividir entre 4.

---

m=6 (p=2, q=7)

Posibles r=1, 3, 5, y de nuevo sus inversos son ellos mismos. Por ejemplo, 5·5=25=6·4+1.

---

m=8 (p=3, q=5)

Posibles r=1, 3, 5, 7. También ellos son sus propies inversos, 7·7=49=8·6+1.

---

m=12 (p=3, q=7)

Posibles r=1, 5, 7, 11. Una vez más, coinciden con sus propios inversos, 11·11=121=12·10+1.

---

m=24 (p=5, q=7)

Posibles r= 1, 5, 7, 11, 13, 17, 19, 23 y también son sus propios inversos.

Los primeros casos interesantes los obtenemos al hacer crecer los números primos, como por ejemplo en las siguientes tablas. Observa que los pares r-s son intercambiables y por tanto solo es necesario emparejarlos.

m=40 (p=5, q=11)

Posibles r= 1, 3, 7, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37.

r	1	3	7	9	11	13	17	19	23	27	29	31	33	37
s	1	3	23	9	11	37	33	19	7	3	29	31	17	13

---

m=72 (p=7, q=13)

Posibles r= 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67.

r	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47	49	53	55	59	61	65	67
s	1	29	31	59	61	17	19	47	49	5	7	35	37	65	67	23	25	53	55	11	13	41	43

Sesión 4: reflexión sobre el futuro.

Se sugiere hacer una sesión de cierre en la que los alumnos reflexionen individual o grupalmente sobre algunos de los siguientes aspectos.

La máquina universal de Turing es un concepto teórico que se pregunta sobre la posibilidad de un programa de ordenador que albergue en su interior a todos los demás programas. Turing también se planteó la posibilidad de que un programa tomara decisiones sobre la veracidad de cualquier afirmación lógica (hoy en la base de la inteligencia artificial) y trabajó en el *Problema de la parada* (Entscheidungsproblem) estableciendo que era no computable. Este problema es, en cierto modo, el que sufrimos en nuestros ordenadores cuando "se cuelgan": ¿por qué no responde el ordenador? ¿está aún ejecutando un programa? ¿no hemos esperado lo suficiente a que termine, o es que no va a arrancar de nuevo nunca? Y cuando se sobrepasa una cota de tiempo de espera (en el caso humano, nuestra paciencia), entonces apagamos súbitamente el equipo.

Algunas preguntas susceptibles de ser tratadas: ¿crees que será posible crear un súper ordenador que sustituya la emoción y el pensamiento humano? Intentos no faltan... (quizá el más conocido sea Deep Blue, diseñada para jugar y vencer al ajedrez). Y en tal caso, ¿podremos distinguir a los humanos de las máquinas que los imitan? Ahí está el test de Turing para ello, pues es el fundamento en el que se basan los CAPTCHA.

Por otro lado, la comunicación entre dispositivos está hoy a la orden del día. Uno de los algoritmos más utilizados es el que aquí hemos descrito pero está en serio entredicho con el desarrollo de la computación cuántica. La fiabilidad del método RSA, y de otros de clave pública, se basa en operaciones computacionalmente costosas de revertir con los algoritmos clásicos. ¿Existirá un ordenador cuántico que ponga en peligro la seguridad de las comunicaciones? Ya hay algunas pruebas modestas...