Curso preliminar de Matemáticas: Técnicas y herramientas

1. Matrices y determinantes

Notas y resultados de teoría que se deben recordar:

- Concepto de matriz. Operaciones con matrices. Matriz inversa. Dependencia e independencia lineal de filas y columnas.
- Determinante de una matriz cuadrada. Cálculo de determinantes de órdenes 2 y 3. Propiedades de los determinantes. Aplicación de estas propiedades para hallar el valor de un determinante de orden mayor.
- Concepto de menor de orden r en una matriz cualquiera. Definición de rango de una matriz y cálculo del rango por menores.

1.1.

Determinar el rango de la matriz A, según los valores de los parámetros a y b.

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & a & 1 & 2 \\ 0 & 1 & a & b \end{pmatrix}$$

1.2.

Este problema consiste en responder *verdadera* o *falsa* en cada una de las siguientes afirmaciones. Si se contesta *verdadera* hay que justificarla y si se contesta *falsa* hay que poner un contraejemplo:

1. $\begin{vmatrix} a+a' & b+b' \\ c+c' & d+d' \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} a' & b' \\ c' & d' \end{vmatrix}$
2. $\begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix} = \begin{vmatrix} a & b & c \\ a' & b' & c' \\ a+a'+a'' & b+b'+b'' & c+c'+c'' \end{vmatrix}$
3. Si A es una matriz cuadrada real de orden n, entonces:
   a) $\det(kA) = k\det(A)$.
   b) $\det(-A) = (-1)^n \det(A)$.

1.3.

Probar los siguientes resultados. Si se encuentra dificultad en alguno de ellos, comenzar con algún ejemplo concreto sencillo, por ejemplo de dimensión 2×2 y tratar de obtener de ahí la respuesta general.

1. Si A es una matriz cuadrada real de orden n, diremos que A es *antisimétrica* si $A^t = -A$ (A^t es la traspuesta de A). Se verifica que:
   - Una *condición necesaria*, pero no suficiente, para que A sea antisimétrica es que todos los elementos de la diagonal principal de A sean nulos. Es decir,

     $$A \text{ antisimétrica } \Longrightarrow a_{ii} = 0, \quad (i = 1, 2, \ldots, n).$$

   - Si A es antisimétrica y n es impar entonces $\det(A) = 0$.

2. Sabemos que, si A y B son matrices cuadradas de orden n, se verifica que $\det(AB) = \det(A)\cdot\det(B)$. Entonces:

   - $\det(AB) = \det(BA)$.
   - Si A es invertible, entonces $\det(A^{-1}) = \big(\det(A)\big)^{-1}$.

2. Sistemas de ecuaciones lineales

Notas y resultados de teoría que se deben recordar:

- Definición de sistema de ecuaciones lineales: solución de un sistema de ecuaciones. Método de Gauss.
- Resolución de un sistema de ecuaciones lineales por determinantes. Regla de Cramer.
- Teorema de Rouché-Fröbenius. Resolución y discusión de sistemas de ecuaciones con m ecuaciones y n incógnitas.

2.1.

1. Si un sistema tiene 4 ecuaciones y 3 incógnitas y al calcular el rango de la matriz de los coeficientes nos sale 4, podemos afirmar que

   a) el sistema es compatible determinado.
   b) el sistema es incompatible.
   c) el sistema es compatible indeterminado.
   d) hemos cometido un error.

2. Si un sistema tiene 3 ecuaciones y 2 incógnitas y al calcular el rango de la matriz ampliada nos sale 3, podemos afirmar que

   a) el sistema es compatible determinado.
   b) el sistema es incompatible.
   c) el sistema es compatible indeterminado.
   d) hemos cometido un error.

3. En un sistema homogéneo con 3 ecuaciones y 3 incógnitas hemos comprobado que el determinante de su matriz de coeficientes es 0, entonces podemos afirmar que

   a) el sistema carece de soluciones.
   b) el sistema tiene infinitas soluciones.
   c) el sistema tiene una única solución.
   d) no es posible asegurar cuántas soluciones tiene, caso de que las tenga.

2.2.

Resolver el siguiente sistema formado por la única ecuación:

$$3x - 2y + z = 7$$

3. Geometría

Temas / resultados a recordar:

- Definición de seno, coseno y tangente. Propiedades fundamentales.
- Vectores: concepto de vector, módulo de un vector, producto escalar de dos vectores, ángulo entre dos vectores. Condición para que dos vectores sean perpendiculares. Idem para que sean paralelos.
- Distancia entre dos puntos.
- Rectas: ecuación de la recta, representación gráfica, distintas formas de la ecuación de una recta, pendiente de una recta, posición relativa de dos rectas, punto de intersección.

3.1. Rectas y puntos notables en un triángulo.

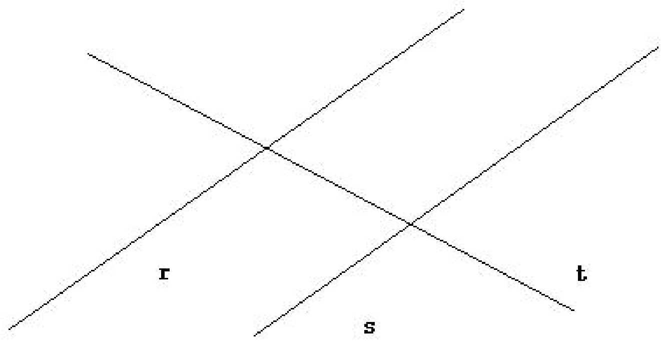
En un triángulo existen rectas y puntos importantes, que merecen especial atención. He aquí un cuadro con los más relevantes:

Rectas	**Definición**	**Intersección**	**Notación**
medianas	Rectas que unen cada vértice con el punto medio del lado opuesto.	Baricentro.	**G**
mediatrices	Rectas perpendiculares a cada lado por su punto medio.	Circuncentro (Centro de la circunferencia circunscrita).	**D**
alturas	Rectas perpendiculares a cada lado trazadas desde el vértice opuesto.	Ortocentro.	**H**
bisectrices	Rectas cuyos puntos equidistan de los lados de cada ángulo (dividen al ángulo en dos ángulos iguales).	Incentro (Centro de la circunferencia inscrita).	**I**

El siguiente ejercicio se propone como trabajo para entregar por escrito.

Dado el triángulo de vértices $A = (0, 1)$, $B = (2, 3)$ y $C = (4, 0)$, hallar su baricentro, circuncentro y ortocentro. Comprobar que estos tres puntos están alineados (*recta de Euler*).

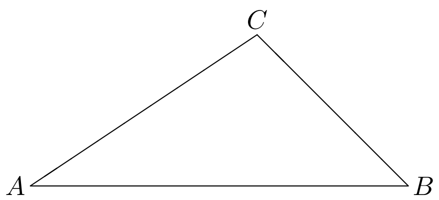
3.2. Ángulos entre paralelas cortadas por una secante.



De los ángulos que forman las rectas r, s y t, decir cuáles son iguales y cuáles son suplementarios. Sus nombres son, por parejas, alternos internos, alternos externos, opuestos por el vértice, etc. ¿Sabrías señalarlos?

3.3. Suma de los ángulos de un triángulo.

Consideramos un triángulo de vértices A, B y C.

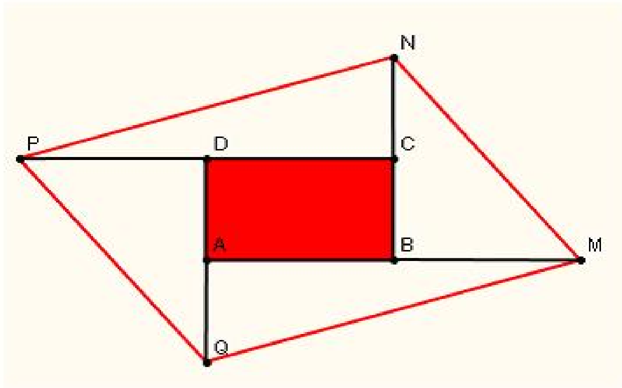


Probar que la suma de sus ángulos es 180°. (Sugerencia: buscar ángulos comprendidos entre rectas paralelas).

3.4.

A partir de un rectángulo ABCD que mide k unidades de área se alargan los lados, todos "en la misma dirección", hasta que la longitud sea el doble de la inicial y se unen los puntos que resultan (observa la figura de la página siguiente).

1. Probar que el cuadrilátero PQMN, construido de esta manera, tiene $5k$ unidades de área.
2. ¿Qué ocurre si el cuadrilátero central es un paralelogramo (lo más general es dibujar un romboide)?
3. A la vista de lo anterior, seguro que "sospechas"(esto es intuir o hacer una conjetura) lo que ocurre si la figura central es un cuadrilátero cualquiera (dibuja un trapezoide). ¿Sabrías probarlo?



4. Límites y continuidad

Temas / resultados a recordar:

- El concepto de límite de una sucesión y su interpretación gráfica. Indeterminaciones: Cuándo aparecen y por qué. Cómo se resuelven los casos más sencillos.
- El concepto de límite de una función $f : \mathbb{R} \mapsto \mathbb{R}$ cuando nos acercamos a un punto $x_0 \in \mathbb{R}$ y su interpretación gráfica. Las relaciones que hay entre límites de sucesiones y límites de funciones.
- Continuidad. Cuándo una función $f : \mathbb{R} \mapsto \mathbb{R}$ es continua. Interpretación gráfica.

A continuación se hablará de funciones monótonas y su comportamiento, de las discontinuidades evitables y no evitables, asíntotas, de las funciones trigonométricas, sus propiedades de continuidad y las de sus inversas, de los logaritmos, exponenciales, etc. En particular, se insistirá en las funciones definidas a trozos.

4.1.

1. La definición de límite de una sucesión es la siguiente:

   El límite de una sucesión $\{a_n\}$ es l si y sólo si se puede hacer que a_n esté tan cerca como queramos de l para todos los valores de n, de uno en adelante.

   a) ¿Qué quiere decir “esté tan cerca como queramos”?

   b) ¿Qué quiere decir “para todos los valores de n, de uno en adelante”?

   c) Traducir esta definición a lenguaje simbólico.

2. La definición de límite de una función es la siguiente:

   El límite de la función f cuando x tiende a a es l si y sólo si se puede hacer que $f(x)$ esté tan cerca como queramos de l haciendo que x esté suficientemente cerca de a, pero siendo distinto de a.

   ¿Podemos repetir el procedimiento del apartado anterior?

4.2.

Estudiar, usando la Definición 1 anterior, los límites de las sucesiones $\{a_n\}$, $\{b_n\}$, $\{c_n\}$ y $\{d_n\}$, dadas por $a_n = 1/n$, $b_n = (-1)^n$, $c_n = n$ y $d_n = (-1)^n + 1/n$.

4.3.

Se define la sucesión de Fibonacci de la siguiente manera: $a_0 = 0$, $a_1 = 1$ y $a_n = a_{n-1} + a_{n-2}$ para $n \geq 2$. Por tanto, la sucesión es: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, . . . Prueba que:

a) a_n y a_{n+1} no tienen factores comunes propios, es decir m.c.d.$(a_n, a_{n+1}) = 1$.

b)
$$a_n = \frac{(1+\sqrt{5})^n/2^n - (1-\sqrt{5})^n/2^n}{\sqrt{5}}$$

c) $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = (1+\sqrt{5})/2$.

d) El número anterior se denomina *razón áurea* y es la razón a/b tal que $\frac{a}{b} = \frac{a+b}{a}$. Por el apartado anterior se tiene que la razón áurea se aproxima por razones de números consecutivos de Fibonacci.

4.4.

Calcular, usando la Definición 2 del Ejercicio 4.1:
$$\lim_{x\to 0} x \operatorname{sen} \frac{1}{x}.$$

4.5.

A la vista de las definiciones del Ejercicio 4.1, proponer definiciones para los límites infinitos, tanto de una sucesión como de una función.

4.6.

Una sucesión, ¿puede tener más de un límite?

4.7.

Probar las siguientes propiedades:

1. Si una sucesión $\{a_n\}$ es convergente y tiende a a y otra sucesión convergente $\{b_n\}$ tiende a b, probar que la sucesión $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ es convergente y tiende a $a + b$.
2. Si dos funciones reales de una variable real, $f(x)$ y $g(x)$, son continuas en un punto x_0, entonces la función $f(x) + g(x)$ también es continua en x_0.

4.8.

Analizar la continuidad de las siguientes funciones:

1. $f(x) = [x]$ (parte entera de x) $\forall x \in \mathbb{R}$.
2. $f(x) = \frac{1}{2-x}$ si $x < 2$; $f(x) = \frac{ax}{2}$ si $x \geq 2$ $(a \in \mathbb{R})$.
3. $f(x) = x \arctan x$ si $x \leq 1$; $f(x) = \log x$ si $x > 1$.
4. $f(x) = \operatorname{sen} x$ si $x \leq 0$; $f(x) = e^x - 1$ si $0 < x \leq 1$; $f(x) = e - 1$ si $x > 1$.
5. $f(x) = \cos\left(\frac{\pi}{2} - \frac{1}{x}\right)$ si $x > 0$; $f(x) = 0$ si $x \leq 0$.

El siguiente ejercicio se propone como trabajo para entregar por escrito.

6. $f(x) = (x-1)\operatorname{sen} \frac{1}{x-1}$ si $x > 1$; $f(x) = 0$ si $x \leq 1$.

En los dos últimos casos, conviene resaltar, sobre todo, el aspecto geométrico de las funciones que aparecen.

5. Derivabilidad

Temas / resultados a recordar:

- El concepto de la derivada de una función. Interpretaciones geométrica, analítica, numérica y cinemática.
- Derivadas de algunas funciones elementales y cálculo diferencial elemental (reglas de derivación de sumas, productos y cocientes; regla de la cadena).
- Las derivadas de orden superior.

A continuación, se aprovecha para practicar con fórmulas trigonométricas. Se aplican las reglas elementales del cálculo diferencial. Se manejan expresiones más o menos complicadas y se analiza cuándo podemos derivar varias veces una función.

5.1.

Determinar en qué puntos $x \in \mathbb{R}$ las siguientes funciones son derivables. En los puntos en que sea posible, calcular la derivada.

1. $f(x) = |x|$.
2. $f(x) = \operatorname{sen} x$.
3. $f(x) = \operatorname{sen} \frac{1}{x}$ si $x > 0$; $f(x) = 0$ si $x \leq 0$.
4. $f(x) = x\operatorname{sen} \frac{1}{x}$ si $x > 0$; $f(x) = 0$ si $x \leq 0$.
5. $f(x) = x^2\operatorname{sen} \frac{1}{x}$ si $x > 0$; $f(x) = 0$ si $x \leq 0$.
6. **Las funciones de los apartados (3), (4), (5) y (6) del ejercicio 4.8 se proponen como trabajo para entregar por escrito.**

5.2.

Calcular la derivada primera y la derivada segunda de las funciones siguientes, siempre que sea posible:

1. $f(x) = \operatorname{tg} x$.
2. $f(x) = \log(1 + |x|^2)$.

5.3.

Probar que $f'(x_0)$ es el límite de las pendientes de las rectas que pasan por los puntos $(x_0, f(x_0))$ y $(x_0 + h, f(x_0 + h))$, cuando $h \to 0$.

Nuevos temas / resultados a recordar:

- Los conceptos de extremos locales y globales y su interpretación gráfica. Condiciones necesarias y suficientes de extremo local de una función.

- Representación gráfica de funciones $f : \mathbb{R} \mapsto \mathbb{R}$: puntos de continuidad y discontinuidad, determinación de extremos locales, comportamiento en el infinito, determinación de asíntotas, etc.

5.4.

El ejercicio siguiente permitirá recordar criterios que conduzcan a la determinación de extremos locales y globales, el comportamiento en el ∞, asíntotas, etc. de diversas funciones.

1. Representar gráficamente las funciones que aparecen en el ejercicio 5.1.

2. En el caso particular de las funciones (5) y (6) del ejercicio 4.8, calcular los máximos y mínimos locales y globales, si existen.

5.5.

A continuación, se aprovecha para recordar/introducir reglas "rápidas" para el cálculo de límites indeterminados. Se profundiza en el significado de éstos.

Determinar los siguientes límites aplicando, si es preciso, la regla de L'Hôpital:

1. $\displaystyle\lim_{x\to\infty} \frac{x^4 - x^3 \cos x + 1}{2x^4 - 1}$.

2. $\lim_{x\to\infty} \left(3x - \sqrt{9x^2 + 5x - 2}\right)$.

3. $\displaystyle\lim_{x\to\infty} \frac{\operatorname{sen} x}{x}$.

4. $\displaystyle\lim_{x\to+\infty} \frac{|x-1|}{(\log|x-1|)^b} \quad (b \in \mathbb{R}).$

5.6.

En el ejercicio siguiente, se aprovecha para recordar fórmulas y resultados elementales de la Geometría plana. Se acostumbra también a los alumnos a que manejen datos generales y operen con constantes genéricas.

1. Calcular el área del mayor triángulo isósceles de perímetro fijo P.

2. Calcular el área del mayor rectángulo de perímetro fijo Q.

El siguiente ejercicio se propone como trabajo para entregar por escrito.

3. En un trapecio rectángulo, conocemos la base menor b y la longitud del lado oblicuo l. Hallar el ángulo que éste debe formar con la base para que el área sea máxima.

6. Números: 1,2,3,...

6.1. Un truco: la prueba del 9.

¿Te acuerdas de cómo se comprobaba una multiplicación o división mediante la prueba del 9? Está basada en algo muy sencillo y vamos a profundizar un poco en su justificación.

Definición.- Fijemos un entero positivo n y sean $a, b \in \mathbb{Z}$. Se dice que a es congruente con b módulo n, si a y b dan el mismo resto al dividirlos por n.
Decir que a y b dan el mismo resto al dividirlos entre n es equivalente a decir que $a - b$ es múltiplo de n, como es fácil comprobar. **Se propone como ejercicio**.
En notación simbólica

$$a \equiv b \text{ (mod n)} \Leftrightarrow a - b \in \mathbb{Z}n \quad (\mathbb{Z}n \text{ representa el conjunto de los múltiplos de } n)$$

Ejemplo: $82 \equiv 34$ (mod 6) porque al dividir 82 entre 6 da resto 4 y al dividir 34 entre 6 da resto 4. Observar que la diferencia, 48, es múltiplo de 6.
Propiedades:

1.- *a*) *Reflexiva* $a \equiv a$ (mod n), $\forall a \in \mathbb{Z}$.
   b) *Simétrica* Si $a \equiv b$ (mod n), entonces $b \equiv a$ (mod n).
   c) *Transitiva* Si $a \equiv b$ (mod n) y $b \equiv c$ (mod n), entonces $a \equiv c$ (mod n).

2.- Si $a \equiv a'$ (mod n), y $b \equiv b'$ (mod n), entonces $a + b \equiv a' + b'$ (mod n) y $ab \equiv a'b'$ (mod n).

Las demostraciones de estas propiedades son muy sencillas y directas. **Se proponen como ejercicio**.

La primera propiedad reúne las tres condiciones que debe cumplir una relación para ser una relación de equivalencia, concepto fundamental en toda la matemática, sobre todo, porque una relación de equivalencia clasifica los elementos del conjunto en el que está definida.
Así, en el ejemplo anterior, todos los números enteros, al dividirlos por 6, dan de resto $0, 1, 2, 3, 4$, ó 5. De esta manera el conjunto $\mathbb{Z}$ queda *clasificado* en seis partes, que se llaman clases de restos (módulo 6) y que se representan por $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$.

Actividades:

1. Los números pares son congruentes dos a dos, módulo 2.

2. Los números impares son congruentes dos a dos, módulo 2.

3. Los múltiplos de n son congruentes con 0, módulo n.

4. Todo número es congruente, módulo n, con el resto de su división por n.

5. Todo número es congruente, módulo 9, con la suma de sus dígitos. Por ejemplo, 1234567890 es congruente con 45, módulo 9, y por tanto es múltiplo de 9.

   Para probarlo sólo hay que tener en cuenta que cualquier número entero se puede escribir como un polinomio en las potencias de 10 ($5384 = 5{\cdot}10^3 + 3{\cdot}10^2 + 8{\cdot}10 + 4$) y todas las potencias de 10 son congruentes con 1 (mod 9). **¿Sabrías terminar la demostración?**

6. En esta propiedad se basa el criterio de divisibilidad por 9: *un número es divisible por 9 si, y sólo si, la suma de sus cifras es un múltiplo de 9.*

7. **Prueba del 9:** Dados dos números enteros a y b, hemos realizado su producto, obteniendo c. Queremos comprobar de un modo rápido, sin repetir la operación, si hemos cometido un error. El truco está en hacer la operación módulo 9, es decir: $a \equiv \overline{a}$ (mod 9), $b \equiv \overline{b}$ (mod 9), $c \equiv \overline{c}$ (mod 9). Por la propiedad 2) anterior, $c = ab \equiv \overline{ab}$ (mod 9) $\equiv \overline{a}\overline{b}$ (mod 9). Por la propiedad transitiva $\overline{c} \equiv \overline{a}\overline{b}$ (mod 9), luego

$$\overline{c} = \overline{\overline{a}\overline{b}}.$$

8. Si nos dicen que el resultado del producto 1234567890×789 es 974074065110, podemos asegurar rápidamente que el resultado no es correcto, con un sencillo cálculo mental.

9. No se puede uno hacer falsas ilusiones con este truco. Hemos probado: $c = ab \Rightarrow \overline{c} = \overline{\overline{a}\overline{b}}$, pero no es cierto el recíproco. Es un ejercicio muy sencillo encontrar productos erróneos que no son detectados por la prueba del 9. **¡Inténtalo!**

10. Formula una "prueba del 9" para la división entera.

Existe una preciosa teoría matemática que ahonda en el problema de la corrección de errores, y que se aplica, por ejemplo para que se detecten los errores que se producen en la lectura de un CD y puedan ser corregidos, para que nosotros podamos escuchar nuestra música favorita sin molestos sobresaltos.

Ideas para desarrollar:

1. La asignación de una letra a nuestro DNI para construir el NIF, es un procedimiento similar a la prueba del 9.

   a) Se divide el DNI entre 23.

   b) Sea r el resto de la división, un número entre 0 y 22.

   c) La letra que se asigna es la que ocupa el lugar $r + 1$ en la siguiente tabla:

   $T \quad R \quad W \quad A \quad G \quad M \quad Y \quad F \quad P \quad D \quad X \quad B \quad N \quad J \quad Z \quad S \quad Q \quad V \quad H \quad L \quad C \quad K \quad E$

   En cuanto al orden de las letras, éste parece ser aleatorio.

   El cálculo de los dígitos de control de las tarjetas de crédito y de las cuentas bancarias siguen algoritmos igual de simples.

2. Criterios de divisibilidad por 2, por 3 y por 11.

6.2. Euclides y Bézout

Recordamos que el máximo común divisor de dos números naturales a, b es otro número natural d tal que :

1.- $d|a$ y $d|b$.

2.- Si $e \in \mathbb{N}$, $e|a$ y $e|b$, entonces $e|d$.

Lo calculamos tomando, en la descomposición en factores primos de ambos, los factores primos comunes a a y b afectados de los menores exponentes. No nos detenemos en la justificación detallada de este aserto.

Debes conocer o recordar el siguiente resultado, que usaremos sin demostración en este curso.

Identidad de Bézout: Dados dos números naturales a, b, sea $d = \text{mcd}(a, b)$. Entonces existen números enteros x, y tales que

$$d = ax + by.$$

El cálculo de los enteros x, y que aparecen en la identidad de Bézout se basa en el algoritmo de Euclides para hallar el máximo común divisor de dos números, en la inteligencia de que los enteros que se obtienen no son únicos.

Algoritmo de Euclides: Sean dados $a, b \in \mathbb{N}$, $a \geq b$. Construimos la siguiente sucesión $z_0 = a$, $z_1 = b$, z_2 es el resto de dividir z_0 por z_1. En general, z_n =resto de dividir z_{n-2} por z_{n-1}. Se obtiene así una sucesión decreciente $z_0 \geq z_1 > z_2 > \ldots$. Supongamos que $z_{r+1} = 0$. Se puede comprobar que $z_r = \text{mcd}(a, b)$.

Actividades:

1.- Aplicar el Algoritmo de Euclides a 33 y 10, para calcular su máximo común divisor.

2.- Idem a 456 y 108.

El algoritmo, decíamos, nos permite resolver la ecuación de la identidad de Bézout.

Ejemplo: Hacemos un caso particular, cuando $r = 4$:

$$\begin{aligned} z_0 = a, \quad z_1 = b \\ z_0 = q_1 z_1 + z_2 \\ z_1 = q_2 z_2 + z_3 \\ z_2 = q_3 z_3 + z_4 \\ z_3 = q_4 z_4. \end{aligned}$$

Entonces

$$\begin{aligned} mcd\ (a, b) &= z_4 = z_2 - q_3 z_3 = z_2 - q_3(z_1 - q_2 z_2) = (1 + q_2 q_3) z_2 - q_3 z_1 = \\ &= (1 + q_2 q_3)(z_0 - q_1 z_1) - q_3 z_1 = (1 + q_2 q_3) z_0 - (q_1 + q_3 + q_1 q_2 q_3) z_1 \end{aligned}$$

Ejercicios:

1.- Encontrar una solución a la identidad de Bézout para 33 y 10.

2.- Idem a 456 y 108.

3.- Aplicar los ejercicios anteriores para resolver el problema de medir el tiempo con relojes de arena siguiente: ¿qué puedes hacer para medir un período de 1 minuto si tienes un reloj de 33 minutos y otro de 10 minutos?

4.- Aplicar el algoritmo de Euclides a un par de números consecutivos de la sucesión de Fibonacci.

6.3. Un enigma: emulando a Sherlock Holmes.

Extraído de "El Paraíso de las Matemáticas" (www.matematicas.net—juegos, allí atribuido a José A. Cañizo).

La escena transcurre en Granada en junio de 2005.

> Hace poco he tenido que ir a renovarme el carnet de identidad, que llevaba ya un par de meses caducado. Es una de esas cosas que tiene uno que hacer tarde o temprano, así que el otro día iba yo todo dispuesto a plantar allí la huella de mi pulgar y marcharme, hasta que me encontré en la comisaría con una cola de unas quince personas, todas ellas esperando a renovar su carnet o hacerse el pasaporte. Una verdadera pesadez. En fin, paciencia.
> Delante de mí iba una mujer con un bolso naranja que aparentemente se aburría tanto o más que yo, así que empezamos a quejarnos por pasar el rato:
>
> - – Yo no sé por qué no pueden poner a más gente, si ven que ahora, antes de las vacaciones, todo el mundo quiere renovarse el carnet. Hacernos esperar aquí, con este calor ..., decía ella.
> - – Desde luego, desde luego, contesté, porque yo me tengo que ir y podían darse un poco de prisa. Claro que hay que entenderlos, todo el día rellenando lo mismo ... – Dije eso porque tampoco me gusta meterles mucha prisa a los pobres.
> - – Pues por eso mismo. Si llevan todo el día así, podían tener ya un poco más de práctica, ¿no? Que yo me tengo que ir esta tarde a Chiclana con mi hermana y todavía no tengo ni las maletas hechas, ¿sabes? – Al decirlo, me fijé en que tenía acento de Cádiz y le pregunté por eso. – ¡Sí, en mi familia somos todos de Cádiz! Yo estuve allí hasta los catorce años y luego me vine a Granada, y mi hermana se fue a Málaga. Desde entonces alternamos las visitas cada tres años: uno me voy yo a Málaga, otro la invito yo aquí a mi casa, y el tercero nos vamos las dos a Chiclana a ver a mis padres. Hemos hecho eso

desde que nos fuimos de Cádiz; recuerdo el verano que pasamos con mis padres cuando yo tenía diecisiete años ... Me encanta esa playa ... – En ese momento pareció acordarse de la cola, y dijo – ¡A ver si terminan ya y puedo irme de una vez!

Sólo quedaban tres personas delante de nosotros; tres o cuatro minutos más.

- – ¿Sabes? Cuando tenía dieciocho años me hice el carnet de identidad. Desde entonces lo he renovado puntualmente cada cinco años, como debe ser, y nunca he tenido que esperar tanto. Hoy todo el mundo se ha puesto de acuerdo para venir ¿eh?
- – Sí, eso parece.

Estuvimos esperando un poco más y cuando sólo quedaba una persona delante de nosotros nos dieron el impreso para poner nuestros datos ('rellenen esto, y firmen aquí, aquí y aquí'). Mientras escribíamos, vi casualmente que la mujer con la que había estado hablando se llamaba Amparo y que había nacido un 29 de febrero. 'Vaya, curioso día', pensé. Terminamos, entregamos los impresos y las fotos, pusimos la huella donde correspondía y nos limpiamos con la toallita que nos dieron. Le dije a la mujer que hasta luego, le deseé que se lo pasara bien en la playa con su hermana y me quedé pensando mientras me iba a casa que, verdaderamente, Amparo parecía mucho más joven de lo que en realidad era.

¿Cuántos años tenía Amparo?

Actividades:

1.- Intenta resolver lógicamente el enigma.

2.- Comprueba que la solución del enigma se halla resolviendo el siguiente sistema de ecuaciones "modulares", donde x es la edad de Amparo:

$$\begin{aligned} x &\equiv 17 (\text{mod } 3) \\ x &\equiv 18 \ (\text{mod } 5) \\ 2005 - x &\equiv 0 \ (\text{mod } 4) \end{aligned}$$

o equivalentemente

$$\begin{aligned} x &\equiv 2 \ (\text{mod } 3) \\ x &\equiv 3 \ (\text{mod } 5) \\ x &\equiv 1 \ (\text{mod } 4) \end{aligned}$$

3.- Intenta resolver ahora el siguiente sistema modular:

$$(S_1) \left\{ \begin{aligned} x_1 &\equiv 1 \ (\text{mod } 3) \\ x_1 &\equiv 0 \ (\text{mod } 5) \\ x_1 &\equiv 0 \ (\text{mod } 4) \end{aligned} \right.$$

Indicación: Como $\text{mcd}(3, 20) = 1$, por la identidad de Bézout tenemos que $7 \cdot 3 - 1 \cdot 20 = 1$. Así, tenemos una solución:

$$\left\{ \begin{aligned} -20 &\equiv 1 \ (\text{mod } 3) \\ -20 &\equiv 0 \ (\text{mod } 5) \\ -20 &\equiv 0 \ (\text{mod } 4) \end{aligned} \right.$$

4.- Idem con

$$(S_2) \left\{ \begin{aligned} x_2 &\equiv 0 \ (\text{mod } 3) \\ x_2 &\equiv 1 \ (\text{mod } 5) \\ x_2 &\equiv 0 \ (\text{mod } 4) \end{aligned} \right.$$

Utiliza Bézout con 5 y 12.

5.- Idem con

$$(S_3) \left\{ \begin{aligned} x_3 &\equiv 0 \ (\text{mod } 3) \\ x_3 &\equiv 0 \ (\text{mod } 5) \\ x_3 &\equiv 1 \ (\text{mod } 4) \end{aligned} \right.$$

Utiliza Bézout con 4 y 15.

6.- Comprueba que $x = 2x_1 + 3x_2 + x_3 = -127$ es una solución del sistema del ejercicio 2. Demuestra que sumando múltiplos enteros de $60 = 3{\cdot}5{\cdot}4$ se obtienen otras soluciones, entre ellas las del enigma inicial.

Este problema está basado en el Teorema Chino del Resto, conocido desde hace más de 2000 años. La formulación más antigua que se conoce, datada entre el 280 a.C y 473 a.C, figura en el libro Sun Tzu Suan-Ching. Pero hay otras formulaciones más recientes de Fibonacci (1202), Euler(1734), Sockley (1967), ... (Se pueden ver referencias históricas en *"Experiencia Matemática"de Davis y Hersh*).

Un enunciado muy completo es el siguiente:

Teorema Chino del Resto. Sean $m_1, m_2, \dots, m_n$ números naturales primos entre sí dos a dos, y $M = m_1 m_2 \dots m_n$. Para cada $j = 1, \dots, n$ sea b_j una solución de la ecuación $x_j(M/m_j) \equiv 1 \pmod{\mathrm{m}_j}$ (*existe siempre porque M/m_j y m_j son primos entre sí, con la ayuda de Bézout*). Entonces una solución del sistema de ecuaciones

$$\begin{cases} x & \equiv a_1 \pmod{\mathrm{m}_1} \\ x & \equiv a_2 \pmod{\mathrm{m}_2} \\ & \vdots \\ x & \equiv a_n \pmod{\mathrm{m}_n} \end{cases}$$

es $x = M(\frac{a_1 b_1}{m_1} + \cdots + \frac{a_n b_n}{m_n})$.

Ideas para desarrollar:

1.- La demostración es sencilla a la vista del ejercicio precedente.

2.- Si x es una solución, también lo son: $x + M$, $x - M$, $x + 2M$, etc.

3.- Si los $\{m_j\}$ no son primos entre sí dos a dos, puede no haber solución, por ejemplo:

$$\begin{cases} x & \equiv 3 \pmod{15} \\ x & \equiv 4 \pmod{10} \end{cases}$$

La resolución de ecuaciones modulares fue en la época de Gauss uno de los problemas de interés. Por ejemplo, resolver ecuaciones cuadráticas modulares, como las de los ejercicios que siguen.

Ejercicios: Dado un entero impar a, demostrar que:

1.- a es siempre un cuadrado módulo 2.

2.- a es un cuadrado módulo 4 si y sólo si $a \equiv 1 \pmod 4$.

3.- a es un cuadrado módulo 8 si y sólo si $a \equiv 1 \pmod 8$.