Ejercicios: Sistemas numéricos
Unal 2025-II

Sergio A. Carrillo
sacarrillot@unal.edu.co

0. Índice general

1. Operaciones binarias. Grupos. Homomorfismos

1.1. Operaciones binarias

1. (Bloch 7.1.1.) ¿Cuáles de las siguietes fórmulas definen una operación binaria en el conjunto dado?

   a) Sea $*$ definida por $x * y = xy$ para todo $x, y \in \{-1, -2, -3, \dots\}$.

   b) Sea $\diamond$ definida por $x \diamond y = \sqrt{xy}$ para todo $x, y \in [2, \infty)$.

   c) Sea $\oplus$ definida por $x \oplus y = x - y$ para todo $x, y \in \mathbb{Q}$.

   d) Sea $\circ$ definida por $(x, y) \circ (z, w) = (x + z, y + w)$ para todo $(x, y), (z, w) \in \mathbb{R}^2 \setminus \{(0, 0)\}$.

   e) Sea $\odot$ definida por $x \odot y = |x + y|$ para todo $x, y \in \mathbb{N}$.

   f) Sea $\otimes$ definida por $x \otimes y = \ln(|xy| - e)$ para todo $x, y \in \mathbb{N}$.

2. (Bloch 7.1.2.) Para cada una de las siguientes operaciones binarias, determine si es asociativa, conmutativa, si existe un elemento identidad y, en caso de que exista, qué elementos tienen inverso.

   a) $\oplus$ en $\mathbb{Z}$ definida por $x \oplus y = -xy$ para todos $x, y \in \mathbb{Z}$.

   b) $\star$ en $\mathbb{R}$ definida por $x \star y = x + 2y$ para todos $x, y \in \mathbb{R}$.

   c) $\otimes$ en $\mathbb{R}$ definida por $x \otimes y = x + y - 7$ para todos $x, y \in \mathbb{R}$.

   d) $*$ en $\mathbb{Q}$ definida por $x * y = 3(x + y)$ para todos $x, y \in \mathbb{Q}$.

   e) $\circ$ en $\mathbb{R}$ definida por $x \circ y = x$ para todos $x, y \in \mathbb{R}$.

   f) $\diamond$ en $\mathbb{Q}$ definida por $x \diamond y = x + y + xy$ para todos $x, y \in \mathbb{Q}$.

   g) $\odot$ en $\mathbb{R}^2$ definida por $(x, y) \odot (z, w) = (4xz, y + w)$ para todos $(x, y), (z, w) \in \mathbb{R}^2$.

1.2. Grupos y Homomorfismos

1. Sea A un conjunto. Defina la operación binaria $\triangle$ en $\mathcal{P}(A)$ (partes de A) por

$$X \triangle Y = (X - Y) \cup (Y - X), \qquad X, Y \in \mathcal{P}(A),$$

   (esta operación binaria se llama *diferencia simétrica*). Compruebe que $(\mathcal{P}(A), \triangle)$ es un grupo abeliano. ¿Qué grupos se obtienen si $|A| = 0, 1, 2$?

2. Mostrar que el conjunto $G = \{5, 15, 25, 35\}$ es un grupo con la multiplicación, módulo 40. Misma pregunta para $S = \{3, 9, 15, 21\}$, con la multiplicación, módulo 24. Identifique estos grupos con $\mathbb{Z}/4\mathbb{Z}$ o el grupo 4 de Klein, según sea el caso.[1]

3. En clase se vio que salvo isomorfismo solo hay dos grupos de orden 4, a saber, $\mathbb{Z}/4\mathbb{Z}$ y el grupo de Klein V. Considere los siguientes grupos: G_1, el grupo de simetrías de un rectángulo en $\mathbb{R}^2$ digamos con vértices en $(\pm 2, \pm 1)$, con la operación de composición. Argumentar por qué

$$G_1 = \{\mathrm{id}, R, S, T\},$$

donde $R(x, y) = (-x, y)$, $S(x, y) = (x, -y)$, $T(x, y) = (-x, -y)$. Considere además $G_2 = \{\pm 1, \pm i\}$, donde $i \in \mathbb{C}$ es la unidad imaginaria ($i^2 = -1$). Comprobar que en efecto G_1 es un grupo y que G_2 es un grupo con la multiplicación de números complejos. Realiza la tabla de grupos en ambos casos y decidir con qué grupo de orden 4 son isomorfos.

4. Sea $G = \mathbb{R} \setminus \{-1\}$ con la operación $a * b = a + b + ab$. Demostrar que $(G, *)$ es un grupo. Además, él es isomorfo a $(\mathbb{R}^*, \cdot)$.

5. En $\mathbb{C}$, mostrar que $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$, para todo $z, w \in \mathbb{C}$. En particular, la conjugación $c : \mathbb{C} \to \mathbb{C}$, $c(z) = \overline{z}$ es un homomorfismo entre $(\mathbb{C}^*, \cdot)$ y si mismo.

6. El conjunto

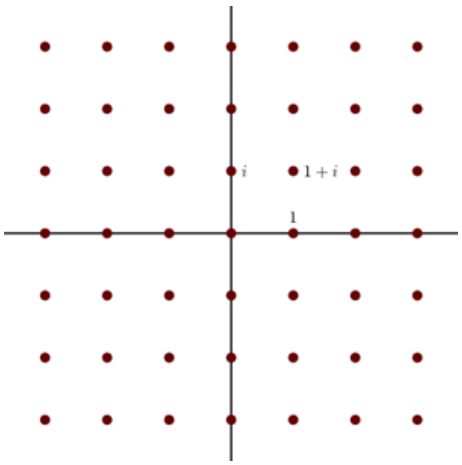
$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$$

se conoce como el *anillo de los enteros de Gauss*.

   a) Mostrar que $(\mathbb{Z}[i], +)$ es un grupo abeliano. También que es cerrado bajo productos.

   b) Demostrar que la *norma* $N : \mathbb{Z}[i] \to \mathbb{Z}$ dada por $N(z) = z\overline{z}$ o explícitamente $N(a+ib) = a^2 + b^2$, satisface que $N(z \cdot w) = N(z) \cdot N(w)$.

   c) Mostrar que si $z \in \mathbb{Z}[i]$ es invertible respecto a la multiplicación entonces $z = \pm 1$ ó $\pm i$.



7. Sea $(G, \cdot)$ un grupo con elemento neutro e. Demuestre que si $a^2 = e$ para todo elemento $a \in G$, entonces G es abeliano. Recuerde que $a^2 = a \cdot a$.

8. Si $(G, *)$ es un grupo, $\iota : G \to G$ dada por $\iota(g) = g^{-1}$ (tomar inverso) es un homomorfismo de grupos si y solo si G es abeliano.

[1] Ruth I. Berger (2005) Hidden Group Structure, Mathematics Magazine, 78:1, 45-48, doi: 10.1080/0025570X.2005.11953299

9. Sea $(G, \cdot)$ un grupo y fije $a \in G$. Comprobar que $c_a : G \to G$ dada por $c_a(g) = aga^{-1}$ es un isomorfismo de G. Mostrar además que $c_a \circ c_b = c_{a \cdot b}$, para todo $a, b \in G$. ¿Qué significa que $c_a(g) = g$? ¿Qué es c_e?

2. Números naturales

2.1. Axiomas de Peano

1. Demostrar todas las afirmaciones sobre las operaciones y el orden en $\mathbb{N}$ que no se hicieron en clase (11.09.2025). Note que por definición $n^+ = (n+0)^+ = n+0^+ = n+1$ y así $n < n^+$.

2. Mostrar a partir de las propiedades desarrolladas con los axiomas de Peano que

   a) Si $n, m \in \mathbb{N}$ y $n + m = 0$, entonces $n = 0$ y $m = 0$.

   b) Si $n \in \mathbb{N}$ y $n \neq 0$ y $n \neq 1$ entonces existe $k \in \mathbb{N}$ tal que $n = (k^+)^+$.

   c) Si $n, m \in \mathbb{N}$ y $nm = 1$ entonces $n = 1$ y $m = 1$.

3. En clase demostramos que no existe $m \in \mathbb{N}$ tal que $0 < m < 1$. Demostrar más generalmente que dado $n \in \mathbb{N}$, no existe $m \in \mathbb{N}$ tal que $n < m < n^+$. Como $n < n+1$, esto justifica que escribamos

   $$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

   También muestre que $m < n$ equivale a que $m + 1 \leq n$.

4. (**Potencias**) Sean $a, n \in \mathbb{N}$. Se define la potenciación por las reglas $a^0 = 1$ y $a^{n^+} = a^n \cdot a$. Demostrar por inducción que

   $$a^{m+n} = a^m \cdot a^n, \qquad a^{n \cdot m} = (a^n)^m, \quad (a \cdot b)^n = a^n \cdot b^n, \qquad a, b, n, m \in \mathbb{N}.$$

   Además $1^n = 1$ y $m^1 = m$. ¿Qué pasa con 0^0? Mostrar también que si $a < b$ y $n > 0$, entonces $a^n < b^n$. Además, si $n < m$ y $a > 1$, entonces $a^n < a^m$.

5. (Extra - Tarski's high school algebra problem) Las *identidades del bachillerato* de Tarski son 11 axiomas para la suma ($+$), multiplicación ($\times$) y exponenciación ($\uparrow$) dadas por

   (1) $x + y = y + x$

   (2) $(x + y) + z = x + (y + z)$

   (3) $x \cdot 1 = x$

   (4) $x \cdot y = y \cdot x$

   (5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

   (6) $x \cdot (y + z) = x \cdot y + x \cdot z$

   (7) $1^x = 1$

   (8) $x^1 = x$

   (9) $x^{y+z} = x^y \cdot x^z$

   (10) $(x \cdot y)^z = x^z \cdot y^z$

   (11) $(x^y)^z = x^{y \cdot z}$

   Como hemos visto, $\mathbb{N}^+$ satisface estas propiedades. El problema de Tarski es responder: ¿existen identidades que involucran solo suma, multiplicación y exponenciación, que son

verdaderas para todos los números enteros positivos, pero que no pueden demostrarse usando solo los axiomas 1-11? En 1980 Alex Wilkie respondió negativamente planteando la propiedad

$$W(x,y): \quad \begin{aligned} &\left((1+x)^y+(1+x+x^2)^y\right)^x\cdot\left((1+x^3)^x+(1+x^2+x^4)^x\right)^y= \\ &\left((1+x)^x+(1+x+x^2)^x\right)^y\cdot\left((1+x^3)^y+(1+x^2+x^4)^y\right)^x. \end{aligned}$$

que relaciona estas operaciones. Wilkie mostró que existen sistemas finitos con las tres operaciones que satisfacen los axiomas pero no $W(x,y)$ [1].

Para el caso de $\mathbb{N}^+$ demuestre $W(x,y)$. Indicación: factorice $1-x+x^2$ de $1+x^3$ y de $1+x^2+x^4$. Intuitivamente, $W(x,y)$ no es demostrable de los axiomas porque esta solución depende de la resta.

2.2. Inducción

1. Demuestre que

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots+\frac{1}{1999}-\frac{1}{2000}=\frac{1}{1001}+\frac{1}{1002}+\cdots+\frac{1}{2000}$$

donde los signos se van alternando en el lado izquierdo de la ecuación. Este es un ejemplo donde es más fácil demostrar un hecho general (¿cuál?) que un caso particular.

2. $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\cdots+\dfrac{1}{n(n+1)}=\dfrac{n}{n+1}$.

3. *a*) (Sumas y productos telescópicos) Si $a_0,...,a_n\in\mathbb{R}$, $b_0,...,b_n\in\mathbb{R}^*$, entonces

$$\sum_{j=0}^{n-1} a_{j+1}-a_j=a_n-a_0, \qquad \prod_{j=0}^{n-1}\frac{b_{j+1}}{b_j}=\frac{b_n}{b_0}.$$

b) Calcular $\displaystyle\sum_{k=1}^{n}\frac{1}{k(k+1)}$.

c) Si $x\neq 1$ entonces $\displaystyle\prod_{k=1}^{n}\left(1+x^{2^{k-1}}\right)=\frac{1-x^{2^n}}{1-x}$. ¿Cuanto vale este producto cuando $x=1$?

4. Mostrar que todo $n\in\mathbb{N}^+$ se puede escribir como sumas de potencias de 2 ($2^0=1, 2^1=2, 2^2=4,\dots$). Por ejemplo,

$$5=2^2+2^0. \qquad 14=2^3+2^2+2^1.$$

5. Resolver la recurrencia $a_n=11a_{n-1}-10a_n, n\geq 3$, donde $a_1=9$ y $a_2=99$.

6. Considere la recurrencia

$$a_n=\alpha a_{n-1}+\beta a_{n-2}, \qquad n\geq 2$$

, con $\alpha,\beta,a_0,a_1\in\mathbb{R}$ fijados. Si $r^2=\alpha r+\beta$ tiene una única solución r_0, mostrar que $a_n=(c_0+c_1n)r_0^n$, para ciertas constante c_0,c_1. ¿Cuáles son?

7. *a*) Si $x\in\mathbb{R}$, $r\neq 1$, entonces

$$1+x+x^2+\cdots+x^n=\frac{x^{n+1}-1}{x-1}, \qquad n\in\mathbb{N}.$$

[1] Burris, S., Lee, S. (1993). Tarski's High School Identities. The American Mathematical Monthly, 100(3), 231–236. doi: 10.1080/00029890.1993.11990393

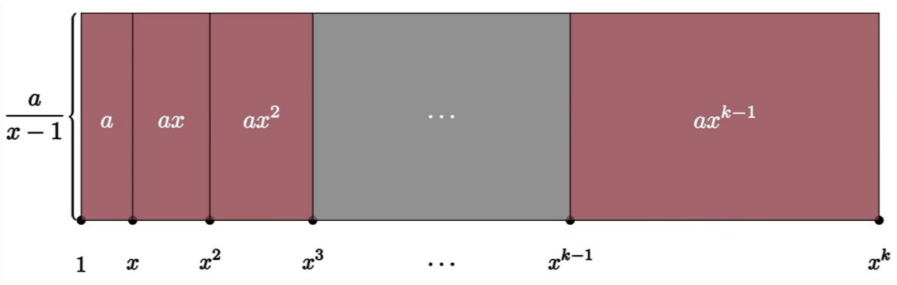
b) Si $x = k + 1 \in \mathbb{N}$, muestre que la anterior igualdad implica que k divide a $(k+1)^n - 1$, para todo $n \in \mathbb{N}$. Por ejemplo, 3 divide a $4^n - 1$, 4 divide a $5^n - 1$ y así sucesivamente.

c) Si ponemos $x = a/b$, comprobar que la anterior igualdad implica que

$$a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + a^{m-3}b^2 + \cdots + ab^{m-2} + b^{m-1}), \qquad m \in \mathbb{N}^+.$$

¿Qué casos de factorización reconoce en esta igualdad para valores pequeños de m?

d) ¿Cómo la siguiente figura ilustra una demostración sin palabras de la primera igualdad?



8. El número áureo es el valor numérico de la proporción que guardan entre sí dos segmentos de recta a y b ($a > b$), que cumplen la siguiente relación: la longitud total, suma de los dos segmentos a y b, es al segmento mayor a, lo que este segmento a es al menor b. Como ecuación algebraica esto significa que

$$\frac{a+b}{a} = \frac{a}{b}.$$

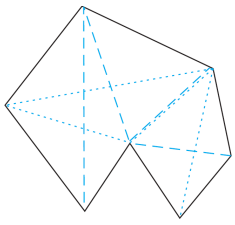
a) Si $\phi = a/b$, muestre que ϕ satisface $\phi = 1 + \frac{1}{\phi}$ y por tanto $\phi = \frac{1+\sqrt{5}}{2}$.

b) Demostrar que para todo $n \in \mathbb{N}^+$ valen las identidades

$$\phi + \phi^2 + \cdots + \phi^n = \phi^{n+2} - \phi - 1, \qquad \phi + \phi^3 + \cdots + \phi^{2n-1} = \phi^{2n} - 1,$$
$$\phi^2 + \phi^4 + \cdots + \phi^{2n} = \phi^{2n+1} - \phi.$$

9. (Triangulación de Polígonos) Un polígono P es una figura geométrica cerrada plana que consisten en una sucesión de segmentos $s_1, s_2, \ldots, s_n$ llamados *lados*. Cada par de lados consecutivos se intersecan en un punto común llamado vértice. Un polígono es *simple* si ningún par de lados consecutivos se intersecan.

Una *diagonal* de un polígono simple P es un segmento que conecta dos vértices no consecutivos de P. La diagonal es *interior* si está contenida dentro del polígono (salvo por sus vértices). Una triangulación de P consiste en dividir a P en triángulos añadiendo diagonales interiores.



Demostrar que un polígono simple de $n \geq 3$ lados se puede triangular con $n - 2$ triángulos. Para ello puede usar el siguiente resultado (no trivial): Cada polígono simple con al menos cuatro lados tiene una diagonal interior.

2.3. Coeficientes binomiales.

1. De dos demostraciones, una algebraica y otra combinatoria, de la identidad

$$\binom{n+m}{2} = \binom{n}{2} + \binom{m}{2} + nm.$$

En particular, obtenga que

$$\binom{2n}{2} = 2\binom{n}{2} + n^2.$$

2. *a*) Calcule el coeficiente de x^k de dos maneras en la expansión $(1+x)^m(1+x)^n = (1+x)^{m+n}$, para demostrar la *identidad de Vandermonde*

$$\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}.$$

En particular, deduzca que

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

b) Suponga que uno tiene m manzanas y n naranjas. Eligiendo k frutas de entre estas $m+n$ y contando de dos maneras, argumente nuevamente esta identidad.

3. Supongamos que debemos formar un comité de n personas a partir de un grupo de $2n$ personas, compuesto por n mujeres y n hombres. Además, el comité debe tener como presidenta a una mujer. Contando de dos formas distintas la forma de integrar este grupo de personas, argumente la identidad

$$\sum_{k=1}^{n} k\binom{n}{k}^2 = n\binom{2n-1}{n-1}, \qquad n \geq 1.$$

4. Demuestre de manera combinatoria y utilizando el Teorema del Binomio las identidades

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}, n \geq 1, \qquad \sum_{k=2}^{n} k(k-1)\binom{n}{k} = n(n-1)2^{n-2}, \quad n \geq 2.$$

¿Cómo se pueden generalizar estas fórmulas? Note que otra forma posible de establecer la primera fórmula es partir de la identidad $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$, derivar respecto a x y luego evaluar en $x = 1$.

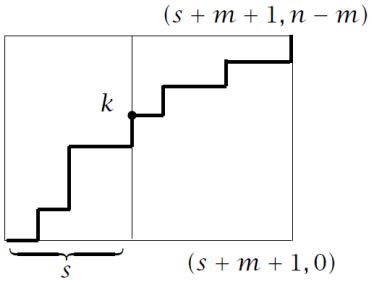
5. Si $0 < k < n$ son enteros, entonces $k\binom{n}{k} = n\binom{n-1}{k-1}$ y $\binom{n}{k} = \dfrac{k+1}{n-k}\binom{n}{k+1}$. ¿Qué pasa si $k = 0$ ó n?

6. Conjeture y demuestre el valor de la suma $\displaystyle\sum_{k=1}^{n}(-1)^k k\binom{n}{k}$.

7. La siguiente es una variante de la identidad de Vandermonde

$$\sum_{k=0}^{n} \binom{s+k}{k}\binom{n-k}{m} = \binom{s+n+1}{s+m+1} \qquad (s, m, n \in \mathbb{N}^+).$$

Asuma que $n \geq m$. Argumente de manera combinatoria esta identidad considerando el total de caminos reticulares de $(0,0)$ a $(s+m+1, n-m)$. Indicación: k en la suma corresponde a la coordenada $y = k$ más alta donde el camino interseca la recta vertical $x = s$.



8. Sean $f, g : \mathbb{R} \to \mathbb{R}$ funciones.

   a) Si ambas son n veces diferenciables, entonces su n-ésima derivada se calcula por

   $$(f \cdot g)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}.$$

   b) Considere el operador de diferencias $\Delta f(x) := f(x+1) - f(x)$. Si para $n > 1$ definimos $\Delta^n f = \Delta\left(\Delta^{n-1} f\right)$, entonces

   $$\Delta^n f(x) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} f(x + n - j).$$

9. El n-ésimo número de Bell B_n cuenta el número de particiones (o clases de equivalencia) de un conjunto de n elementos. Por ejemplo $B_0 = B_1 = 1$ y $B_2 = 5$. Justifique por qué estos valores se pueden calcular de manera recursiva por

   $$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

   Indicación: a partir de una partición arbitraria de $n+1$ elementos, al eliminar el conjunto que contiene el primer elemento, se obtiene una partición de un conjunto más pequeño de $0 \leq k \leq n$ elementos.

2.4. Algunos problemas de conteo

1. Encontrar el número de cadenas binarias de longitud n que contengan un número par de 0's.
2. Encontrar una recurrencia para el número s_n de cadenas binarias de longitud n que contengan la cadena 00.
3. *a*) Un grupo contiene n hombres y n mujeres. ¿Cuántas maneras hay de ordenarlos en una fila si los hombres y las mujeres se alternan?

   b) Si hay un grupo de n hombres y m mujeres. ¿Cuántas maneras hay de ordenarlos en una fila si los hombres están juntos?
4. ¿Cuántos enteros n con $1000 \leq n \leq 9999$ hay que sean pares?
5. ¿Cuántos números enteros positivos entre 100 y 999 inclusive son: divisibles por 7?, impares?, tienen los mismos tres dígitos decimales?, no son divisibles por 4?, son divisibles por 3 o por 4?, no son divisibles por 3 ni por 4?, son divisibles por 3 pero no por 4?, son divisibles por 3 y por 4?

6. ¿Cuántos subconjuntos con más de dos elementos tiene un conjunto con 100 elementos?

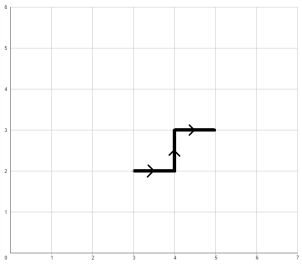
7. Se lanza una moneda 10 veces, y en cada lanzamiento sale cara o cruz. ¿Cuántos resultados posibles hay en total?, ¿cuántos con dos caras?, ¿cuántos con máximo tres cruces?, ¿cuántos con el mismo número de caras y cruces?

8. ¿Cuántas cadenas se pueden formar al permutar las letras de ABRACADABRA? Mista pregunta para ELECTROENCEFALOGRAMA.

9. ¿De cuántas formas se pueden ubicar 8 torres de ajedrez del mismo color (indistinguibles) en un tablero 8×8 de tal manera que no se ataquen entre sí. Aquí es válido que las torres del mismo color se ataquen. ¿Qúe pasa si tenemos 8 torres de 8 colores diferentes?

10. Tome una matriz de $n \times n$ con 0's en todas sus entradas. ¿De cuántas maneras podemos posicionar n 1's en ella de forma que en cada fila y columna haya exactamente un 1? Establezca una biyección entre estas matrices y el conjunto S_n de permutaciones de $[n]$.

11. Consideramos caminatas formadas avanzando en cada paso una unidad hacia el frente o hacia arriba. ¿Cuántos caminos de esta forma hay del punto $(0, 0)$ al punto $(7, 6)$ que contengan el trayecto señalado en la figura?



12. *a*) ¿Cuántas cadenas de bits contienen exactamente ocho 0's y diez 1's si cada 0 debe ir seguido inmediatamente de un 1?

    b) Una cadena palíndroma es aquella cuya inversión es idéntica a si misma (por ejemplo 1001). ¿Cuántas cadenas de bits de longitud n son palíndromas? Misma pregunta si se consideran cadenas formadas por las letras $a_1, \ldots, a_m$.

13. Recuerde que un *grafo* es una pareja $G = (V, E)$, donde V es el conjunto de vértices y E es el conjunto de ejes o aristas (edges). Un *ciclo* (loop) en G es una arista $e \in V$ que va de un vértice en si mismo, es decir, $e = \{v\}$. El *grado* de un vértice v (deg(v)) es el número de aristas incidentes con él. Note que un ciclo suma 2 al grado.

    Demostrar el *Lema del apretón de manos* (Handshaking lemma): Si $G = (V, E)$ es un grafo con $m = |E|$ aristas, entonces

    $$\sum_{v \in V} \deg(v) = 2m.$$

    Use esta fórmula para determinar el número de aristas del grafo simple completo $K_n = ([n], E_n)$, donde $E_n = \{\{i, j\} : i \neq j\}$.

14. *a*) Sean $(x_i, y_i) \in \mathbb{R}^2$, $i = 1, 2, 3, 4, 5$ cinco puntos distintos en el plano, con coordenadas enteras. Demostrar que el punto medio del segmento que une al menos una pareja de estos puntos tiene coordenadas enteras.

    b) Sean $(x_i, y_i, z_i) \in \mathbb{R}^3$, $i = 1, \ldots, 9$ nueve puntos distintos, con coordenadas enteras. Demostrar que el punto medio del segmento que une al menos una pareja de estos puntos tiene coordenadas enteras.

c) ¿Cómo se generalizan estos enunciados para puntos en $\mathbb{R}^d$?

15. Considere cinco puntos distintos sobre una esfera. Demostrar que siempre es posible dividir al esfera en dos hemisferios de forma que 4 puntos están en un solo hemisferio (incluido su borde).

16. Considere un dígito $j \in \{1, 2, \ldots, 9\}$ y $n \in \mathbb{N}$. Mostrar que siempre existe un número formado solo por j's y 0's que es divisible por n. En clase vimos el caso $j = 1$.

17. Tome $a_1, \ldots, a_n \in \mathbb{Z}$, no necesariamente distintos. Entonces, siempre existe un conjunto de números consecutivos a_{k+1}, a_{k+2}, $\ldots$, a_ℓ cuyo suma $\sum_{i=k+1}^{\ell} a_i$ es un múltiplo de n. Indicación: considere $a_1 + \cdots + a_m \mod n$.

18. Considere una baraja estándar (52 cartas, 4 símbolos de 13 cartas cada uno). ¿Cuál es el mínimo número de cartas que se necesitan tomar para tener 3 cartas de la misma pinta? ¿Cuál es el mínimo número de cartas que se deben tomar para tener al menos una de cada pinta?

19. *a*) ¿Cuántos números en $\{1, \ldots, 1000\}$ no son divisibles por $7, 11$ ni 13?

    b) ¿Cuántas permutaciones de las 27 letras de nuestro alfabeto no contienen ninguna de las cadenas "pero", "pues"ni "año" ?

20. - Una bandera debe consistir en n franjas horizontales, donde cada franja puede ser de uno de tres colores: rojo, blanco o azul, y ninguna franja adyacente puede tener el mismo color. ¿Cuál es el total de diseños posibles?
    - Supongamos ahora que, para evitar la posible confusión de izar la bandera al revés, se decreta que las franjas superior e inferior deben ser de colores diferentes. Sea a_n el número de tales banderas con n franjas. Hallar los valores a_1 y a_2.
    - Determine una relación de recurrencia entre a_n y a_{n-1}. Indicación: ¿cómo se pueden relacionar una bandera de n franjas con el mismo color en la primera y última franja y una bandera de $n-1$ franjas con las franjas superior e inferior de colores diferentes?
    - A partir de la recurrencia obtenida, obtenga una relación de recurrencia lineal de orden 2 entre a_n, a_{n-1} y a_{n-2}.
    - Determine una fórmula cerrada para a_n, es decir, resuelva la recurrencia obtenida.

21. Recuerde que una permutación $\pi \in S_n$ es un *desarreglo* (derangement) si no tiene puntos fijos, es decir, $\pi(k) \neq k$, para todo $k \in [n]$. Si D_n denota el número de tales permutaciones, sabemos del Ejemplo 2.17 de las notas de clase que

$$D_n = (n-1)(D_{n-1} + D_{n-2}), n \geq 3 \qquad D_1 = 0, D_2 = 1.$$

    Emplee esta recurrencia para demostrar que también

$$D_n = nD_{n-1} + (-1)^n, \qquad n \geq 1.$$

22. Sean $n > 2$ y $r, s \geq 1$ enteros. Calcular el número de formas de escribir

$$n = (k_1 + \cdots + k_r)(j_1 + \cdots + j_s),$$

    donde $k_i, j_l \in \mathbb{N}$. ¿A qué se reduce el resultado si $n = p$ es primo? Investigue en qué consiste la convolución entre dos funciones $f, g : \mathbb{N} \to \mathbb{R}$ y exprese su respuesta general en términos de esta operación.

2.5. Extra: Sobre sumas y funciones características.

Estos ejercicios recogen algunas propiedades que usamos en clase, al discutir la regla de inclusión-exclusión.

1. Sea I un conjunto finito de índices, $\{I_1, \ldots, I_n\}$ una partición de I y para cada $i \in I$ considere $a_i \in \mathbb{R}$. Entonces
$$\sum_{i\in I} a_i = \sum_{k=1}^{n} \sum_{i\in I_k} a_i.$$
¿Qué propiedades de la suma requerimos para justificar esta igualdad?

2. Fije un conjunto universal A. Dado $X \subseteq A$, la función $1_X : A \to \{0, 1\}$ dada por
$$1_X(a) = \begin{cases} 1, & \text{si } a \in X, \\ 0, & \text{si } a \in A \setminus X, \end{cases}$$
se conoce como la *función característica* de X en A. Ella satisface las siguientes propiedades, válidas para todo $a \in A$:

   a) $1_\emptyset(a) = 0$ y $1_A(a) = 1$. Más generalmente, $1_{A\setminus X}(a) = 1 - 1_X(a)$.

   b) $1_{X\cap Y}(a) = 1_X(a)\cdot 1_Y(a)$. Además, si $X\Delta Y = (X\cup Y)\setminus(X\cap Y)$ es la diferencia simétrica entre X e Y, entonces $1_{X\Delta Y}(a) = |1_X(a) - 1_Y(a)|$.

   c) $1_{X_1\cup\cdots\cup X_n}(a) = 1 - \prod_{j=1}^{n}(1 - 1_{X_j}(a))$.

   d) $X \subseteq Y$ si y solo sí $1_X(a) \leq 1_Y(a)$, para todo $a \in A$.

   e) Si A es finito, entonces $\sum_{a\in A} 1_X(a) = |X|$.

   f) $X = \{a \in A : 1_X(a) = 1\} = 1_X^{-1}(\{1\})$. Emplee la asignación $X \mapsto 1_X$ y $f \mapsto f^{-1}(\{1\})$ para establecer una biyección entre $\wp(A)$ y $2^A := \{f : A \to \{0, 1\} : f \text{ función}\}$ y concluir que $|\wp(A)| = 2^{|A|}$.

2.6. Extra: Números de Fibonacci

Los siguientes ejercicios contienen algunas, de las numerosas identidades que satisfacen los números de Fibonacci, donde $n \geq 1, m \geq 0$. Los ejercicios se pueden resolver por inducción.

1. $F_{n+m+1} = F_nF_m + F_{n+1}F_{m+1}$.
2. $F_n = 5F_{n-4} + 3F_{n-5}$, $n \geq 5$.
3. $F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_nF_{n+1}$.
4. $F_0 + F_2 + \cdots + F_{2n} = F_{2n+1} - 1$.
5. $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.
6. $F_0 - F_1 + F_2 - F_3 + \cdots - F_{2n-1} + F_{2n} = F_{2n-1} - 1$.
7. $F_1F_2 + F_2F_3 + \cdots + F_{2n-1}F_{2n} = F_{2n}^2$.
8. Si $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$. Aplique determinantes para concluir que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.
9. $\left(\frac{3}{2}\right)^{n-2} \leq F_n < 2^n$.
10. $F_{n+1} < \left(\frac{7}{4}\right)^n$.
11. Mostrar[2] que $F_j^2 - F_{j-1}^2 = (F_j - F_{j-1})(F_j + F_{j-1}) = F_{j-2}F_{j+1}$ para comprobar la fórmula
$$\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} F_{n-1}F_{n+2} & F_n^2 \\ F_n^2 & F_{n-2}F_{n+1} \end{bmatrix}.$$

[2] Óscar Ciaurri (2022) An "Esoteric" Proof of Gelin-Cesàro Identity, American Mathematical Monthly, 129:5, 465-465, doi: 10.1080/00029890.2022.2043096

Luego tome determinantes para demostrar la identidad de *Gelin-Cesàro*

$$F_{n-2}F_{n-1}F_{n+1}F_{n+2} - F_n^4 = -1.$$

3. Números enteros

3.1. Divisibilidad

1. Encuentre un número natural positivo n tal que $n/2$ sea un cuadrado, $n/3$ sea un cubo y $n/5$ sea un número elevado a la 5.

2. *a)* Muestre que cualquier primo de la forma $3k+1$ es de la forma $6m+1$.
   b) Muestre que todo primo mayor que 3 es de la forma $6k+1$ ó $6k-1$.
   c) Muestre que todo primo mayor que 5 es de la forma $10k \pm 1$ ó $10k \pm 3$.
   d) Comprobar que todo primo $p > 5$ siempre termina en $1, 3, 7$ ó 9.

3. *a)* Supongamos que S contiene $2n$ elementos, y que S está particionado en n subconjuntos disjuntos, cada uno conteniendo exactamente dos elementos de S. Muestre que esto se puede hacer en precisamente de

$$(2n-1)(2n-3)\cdots 5 \cdot 3 \cdot 1 \;=\; \frac{(2n)!}{2^n n!}$$

   formas.
   b) Muestre que $(n+1)(n+2)\cdots(2n)$ es divisible por 2^n, pero no por 2^{n+1}.
   c) Si $a, b > 0$, entonces $a!^b \cdot b! | (ab)!$. Por ejemplo, $(3n)!/n!(3!)^n \in \mathbb{N}^+$. Indicación: coeficientes multinomiales.

4. Sean $k \in \mathbb{Z}$ y $n \in \mathbb{N}^+$. En lo siguientes ejercicios establezca las propiedades de divisibilidad planteadas. Intente resolver las preguntas de dos formas, una directa y otra empleando congruencias (cuando lo considere posible):

   a) $3 \mid (k^3 + 2k)$.
   b) $6 \mid (17k^3 + 103k)$.
   c) $30 \mid (k^5 - k)$.
   d) $21 \mid (4^{n+1} + 5^{2n-1})$.
   e) $7 \mid (5^{2n+1} + 2^{2n+1})$.
   f) $7 \mid 3^{2n+1} + 2^{n+2}$.
   g) $a^{2^n} - 1$ es divisible por 2^{n+2}, para todo entero impar a.
   h) $3^{2^n} + 1$ es divisible por 2, pero no por 4.

5. Mostrar que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es entero, para todo $n \in \mathbb{Z}$.

3.2. Máximo común divisor

1. Dados $a, b \in \mathbb{N}^+$, determine condiciones sobre la descomposición prima de a y b para determinar cuando $\gcd(a, b) = 1$.

2. Dados $a, b \in \mathbb{N}^+$, si $\gcd(a, b) = \operatorname{lcm}(a, b)$, entonces $a = b$. Por otra parte, si $a|b$, determine los valores $\gcd(a, b), \operatorname{lcm}(a, b)$.

3. Encontrar el máximo común divisor de los números dados y expresarlo como combinación lineal entera de estos:

   a) $a = 7469$ y $b = 2464$.
   b) $a = 1000$ y $b = 10101$.
   c) $a = -202$ y $b = 189$.
   d) $a = 6, b = 10, c = 15$.

4. *a)* Sea $n \in \mathbb{N}^+$. Si $1 < d \leq n$, entonces $d \mid n!$, pero $d \nmid n! + 1$.
   b) Muestre que $\gcd(n! + 1, (n + 1)! + 1) = 1$.

5. Si $k \in \mathbb{Z}$, calcular $\gcd(2k + 1, 9k + 4)$ y $\gcd(2k - 1, 9k + 4)$.

6. Asuma que $d|a$ y $d|b$, donde $d \geq 1$. Entonces $\operatorname{lcm}(a/d, b/d) = \operatorname{lcm}(a, b)/d$.

7. Demostrar las siguientes afirmaciones suponiendo que $\gcd(a, b) = 1$.

   a) Si $c|a$, entonces $\gcd(b, c) = 1$.
   b) $\gcd(a + b, ab) = 1$.
   c) $\gcd(a + b, a - b) = 1$ ó 2.
   d) $\gcd(a + b, a^2 - ab + b^2) = 1$ ó 3.

8. Sean n, a y b enteros positivos.

   a) Si $b = aq + r, 0 \leq r < a$, entonces $n^b - 1 = (n^a - 1)(n^{b-a} + n^{b-2a} + \cdots + n^r) + (n^r - 1)$. Por tanto, al dividir $n^b - 1$ por $n^a - 1$ se obtiene como residuo $n^r - 1$.
   b) Demuestre que si $n \geq 2$, entonces $\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1$.
   c) Si $n > 1$, $a \mid b$ si y solo si $(n^a - 1) \mid (n^b - 1)$.

9. (Divisibilidad y números de Fibonacci)

   a) $2 \mid F_n$ si y sólo si $3 \mid n$.
   b) $4 \mid F_n$ si y sólo si $6 \mid n$.
   c) ¿Qué se obtiene de dividir F_{n+2} por F_{n+1}? Use esto para establecer que $\gcd(F_n, F_{n+1}) = 1$.
   d) Si $m, n \geq 1$, se tiene que $F_n \mid F_{mn}$. Por ejemplo, $5 \mid F_{5n}$.

10. *a)* Considere $x, y \in \mathbb{Z}$, no nulos, y la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con coeficientes enteros y tal que $ad - bc = \pm 1$. Mostrar que $\gcd(x, y) = \gcd(ax + by, cx + dy)$. ¿Recupera esta ecuación resultados de algunos de los ejercicios anteriores? Indicación: si $x' = ax + by$ y $y' = cx + dy$, escriba x, y en términos de x', y'.
    b) (Tal vez requiere álgebra lineal) Generalice este resultado a $\gcd(x_1, \ldots, x_n) = \gcd(x'_1, \ldots, x'_n)$, donde $x_j \in \mathbb{Z}$ no son nulos, $x' = (x'_1, \ldots, x'_n)^t = Ax$, y A es una matriz con entradas enteras y $\det(A) = \pm 1$.

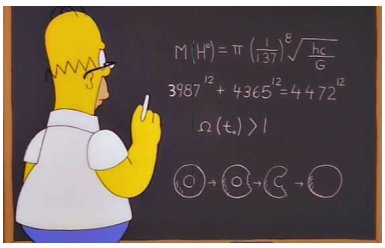
3.3. Congruencias

1. *a*) ¿Cuál es el último dígito en la representación decimal de 2^{400}?
   b) Encuentre los dos últimos dígitos de la representación decimal de 9^{500}.
   c) ¿Cuál son los dos últimos dígitos en la representación decimal de 3^{400}?
   d) Emplear exponenciación modular rápida para calcular $3^{2003} \bmod 99$.

2. En un capítulo de los Simpsons, Homero escribió

$$3987^{12} + 4365^{12} = 4472^{12}.$$

   Emplear congruencias para decidir que si esta igualdad es verdadera o falsa.



3. Resolver las siguientes congruencias (ecuaciones lineales en $\mathbb{Z}/m\mathbb{Z}$):

   a) $19x \equiv 4 (\text{mod } 141)$.
   b) $55x \equiv 34 (\text{mod } 89)$.
   c) $89x \equiv 2 (\text{mod } 232)$.

4. *a*) Sean $a \in \mathbb{Z}$ y $k, l, m, n \in \mathbb{N}^+$. Suponga que $a^k \equiv 1 \pmod{n}$ y que $m \equiv l \pmod{k}$. Pruebe que $a^m \equiv a^l \pmod{n}$.
   b) ¿Es cierto que si $a^k \equiv b^k (\text{mod } n)$ y $k \equiv j (\text{mod } n)$, entonces $a^j \equiv b^j (\text{mod } n)$?

5. Si $a \in \mathbb{Z}$ y $m \in \mathbb{N}^+$, entonces $a(a+1)(a+2)\cdots(a+m-1) \equiv 0 \pmod{m}$ mód m.

6. (Pequeño teorema de Fermat) Sea $n \in \mathbb{Z}$.

   a) Si $\gcd(n, 7) = 1$, entonces $n^6 - 1$ es divisible por 7. Además, $n^7 - n$ es divisible por 42.
   b) $n^{13} - n$ es divisible por $2, 3, 5, 7$ y 13.
   c) Si $p \neq q$ son primos, entonces $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

7. Tienes un montón de monedas desconocido. Si las agruparas de 3 en 3 sobrarían 2 monedas. Si las agrupas de 5 en 5 sobrarían 3 monedas. Si las agrupas de 7 en 7 sobrarían 2 monedas. ¿Cuál es el menor número posible de monedas que puedes tener?

8. (Criterios de divisibilidad) Sea

$$n = \sum_{j=0}^{k} a_j 10^j = (a_k \cdots a_1 a_0)_{10}, \qquad a_j \in \{0, 1, 2, \ldots, 9\}$$

   la escritura de n en base decimal. Las siguientes afirmaciones son válidas:

a) $2 \mid n$ si y solo si a_0 es par.

b) $3 \mid n$ si y solo si $3 \mid \sum_{j=0}^{k} a_j$.

c) $4 \mid n$ si y solo si $4 \mid a_1 10 + a_0$.

d) $5 \mid n$ si y solo si $a_0 = 0$ ó 5.

e) $7 \mid n$ si y solo si $7 \mid (a_k \cdots a_1) - 2a_0$.

f) $8 \mid n$ si y solo si $8 \mid a_2 10^2 + a_1 10 + a_0$.

g) $9 \mid n$ si y solo si $9 \mid \sum_{j=0}^{k} a_j$.

h) $10 \mid n$ si y solo si $a_0 = 0$.

i) $11 \mid n$ si y solo si $11 \mid \sum_{j=0}^{k} (-1)^j a_j$.

j) $13 \mid n$ si y solo si $13 \mid (a_k \cdots a_1) - 9a_0$.

3.4. Números primos

1. Si $n > 4$ no es primo, $n \mid (n-1)!$. Concluya que p es primo si y solo si $(p-1)! \equiv -1 (\text{mod } p)$.

2. Demuestre que si p es primo, entonces $\binom{p-1}{k} \equiv (-1)^k (\text{mod } p)$.

3. Si p es primo y $a^2 \equiv b^2 (\text{mod } p)$, entonces $a \equiv b (\text{mod } p)$ ó $a \equiv -b (\text{mod } p)$. Por ejemplo, si $a^2 \equiv 1 (\text{mod } p)$, entonces $a \equiv \pm 1 (\text{mod } p)$.

4. Sea p_n el n-ésimo primo. Mostrar que $P_n = (p_1 p_2 \cdots p_n) + 1$ nunca es un cuadrado perfecto.

5. Sea p un número primo y sean $a \neq b$ enteros positivos menores que p. Entonces p divide a $a^{p-2} + a^{p-3}b + a^{p-4}b^2 + \cdots + b^{p-2}$.

6. *a*) Si $x \in \mathbb{C}$ y $n \in \mathbb{N}$ es impar, entonces $x^n + 1 = (x+1)\left[\sum_{k=0}^{n-1} (-1)^k x^k\right]$.

   b) Si $n = ab$ con b impar, entonces $2^a + 1 \mid 2^n + 1$.

   c) Demuestre que si $2^m + 1$ es primo entonces m es una potencia de 2.

   d) Los *números de Fermat* se definen por $F_n = 2^{2^n} + 1$. El primer número de Fermat que no es primo es F_5 porque

   $$(2^9 + 2^7 + 1)(2^{23} - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^9 - 2^7 + 1) = 2^{32} + 1.$$

   Mostrar que $F_0 F_1 \cdots F_{n-1} + 2 = F_n$, $n \geq 1$. Concluya que $\gcd(F_n, F_m) = 1$ si $n \neq m$. ¿Por qué esto demuestra que hay infinitos primos?

   e) Compruebe también las propiedades para $n \geq 2$:

   $$F_n = (F_{n-1} - 1)^2 + 1, \qquad F_n = F_{n-1} + 2^{2^{n-1}} F_0 \cdots F_{n-2}, \qquad F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2.$$

7. Demostrar que existen infinitos primos de la forma $4n+3$. Indicación: Por contracción, asuma que existen solo finitos primos $p_1, \ldots, p_m$ de la forma $4n+3$ y considere $N = 4(p_1 \cdots p_m) - 1$. Si q es primo con $q|N$, entonces $q = 4r + 1$. Así $N = (4m_1 + 1)(4m_2 + 1) \cdots (4m_k + 1)$, llegando a una contradicción.

8. (Infinitud de primos -Auric, 1915-) Supongamos que hay solo un número finito de primos $p_1 < p_2 < \cdots < p_r$ y sean $N = p_r^t$, con $t \geq 1$ entero.

   a) Todo entero $1 \leq m \leq N$ puede escribirse de manera única en la forma

   $$m = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r},$$

   donde $(f_1, \ldots, f_r) \in \mathbb{N}$.

b) De $p_1^{f_i} \leq p_i^{f_i} \leq m \leq N = p_r^t$, deduzca que

$$f_i \leq tE, \qquad E = \frac{\log p_r}{\log p_1}, \qquad i = 1, \ldots, r.$$

c) Contando de dos formas distintas el número de enteros $1 \leq m \leq N$, concluya que

$$p_r^t = N \leq (tE+1)^r.$$

Pero si t es suficientemente grande $p_r^t > (tE+1)^r$, obteniendo una contradicción. Concluye que hay infinitos números primos.

9. Empleando el teorema de Dirichlet, mostrar que existen infinitos números primos que terminan en 7777. De más ejemplos sobre este tipo de fenómenos.

10. *a*) (Legendre-Polignac) Si p es primo, entonces la máxima potencia de p que divide a $n!$ es

$$\nu_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

En realidad esta suma es finita, ¿hasta qué termino se detiene?

b) (Requiere cálculo) [Existen infinitos primos] Por contradicción, asuma que existen finitos primos. Dado $k \in \mathbb{N}^+$, podemos escribir $k! = \prod_p p^{\nu_p(k!)}$. Por la fórmula anterior,

$$\nu_p(k!) \leq \sum_{j=1}^{\infty} \frac{k}{p^j} = \frac{k}{p-1} \leq k.$$

Por tanto, $k! \leq (\prod_p p)^k$. Pero esto contradice que $\lim\limits_{k\to+\infty} \dfrac{(\prod_p p)^k}{k!} = 0$. Por tanto, no pueden haber finitos primos.

11. Mostrar que todo primo $p > 3$ se puede escribir de la forma $\sqrt{24n+1}$, para cierto $n \in \mathbb{N}$. Por ejemplo,

$$5 = \sqrt{24 \cdot 1 + 1}, \qquad 41 = \sqrt{24 \cdot 70 + 1}.$$

12. Si n tiene k factores primos impares distintos entonces $2^k \mid \varphi(n)$.

13. Mostrar que si $p_1, \ldots, p_n$ son primos mayores a 5 y 6 divide a $p_1^2 + \cdots + p_n^2$, entonces $6|n$.

14. Empleando el postulado de Bertrand demostrar las siguientes afirmaciones:

a) $p_n < 2^n$, donde p_n denota el n-ésimo primo y $n > 1$.
b) Existe un primo $p \in (n, 2n]$ que divide a $\binom{2n}{n}$.
c) $\binom{2n}{n} \neq m^k$, para todo $m, k \in \mathbb{N}^+$.

15. Mostrar que para $n \geq 2$ se tiene que

$$\left\lfloor \cos^2\left(\pi \frac{(n-1)!+1}{n}\right)\right\rfloor = \begin{cases} 1, & n \text{ es primo,} \\ 0, & \text{otros.} \end{cases}$$

Este tipo de fórmulas son la base de expresiones del tipo

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{n} \left(\sum_{j=1}^{m} \left\lfloor \cos^2\left(\pi \frac{(j-1)!+1}{j}\right)\right\rfloor \right)^{-1/n} \right\rfloor$$

para calcular el n-ésimo primo p_n [1], aunque imprácticas computacionalmente.

[1] C. P. Willans (1964) On Formulae for the nth Prime Number. The Mathematical Gazette, 48(366), 413-415

4. Números racionales

4.1. Propiedades generales

1. Completar las demostraciones sobre las propiedades de las operaciones y orden de $\mathbb{Z}$ y $\mathbb{Q}$ que no se hicieron en clase.

2. Muestre que en la construcción de $\mathbb{Q}$, si en vez de trabajar con $\mathbb{Z} \times \mathbb{Z}^*$ se hace con $\mathbb{Z} \times \mathbb{Z}$, la relación de equivalencia: $(a, b) \sim (c, d)$ si $ad = bc$, resulta ser trivial, es decir, $(\mathbb{Z} \times \mathbb{Z})/\sim$ tiene un solo elemento.

3. Considere la recta $\ell_\alpha = \{(x, y) \in \mathbb{R}^2 : y = \alpha x\}$, donde $\alpha \in \mathbb{R}$ es fijo. Demostrar que ℓ_α interseca a $\mathbb{Z}^2 \setminus \{(0, 0)\}$ si y solo si $\alpha \in \mathbb{Q}$. En dicho caso determinar esta intersección.

4. Muestre que para todo $n \in \mathbb{N}^+$, la fracción $\dfrac{12n + 1}{30n + 2}$ es irreducible.

5. Expresar los siguientes racionales en la forma a/b:

   a) $0,1212 + 3,\overline{1415}$.

   b) $9,\overline{9} + (6,\overline{6} \times 3,\overline{3})$.

   c) 0,123456789/0,987654321.

   d) $0.a_1a_2a_3a_4\ldots$, donde $a_j = \text{res}(j, 10)$ es el residuo de dividir j por 10.

   e) $1 + \dfrac{1}{1 + \dfrac{1}{1 + \dfrac{1}{1}}}$.
   ¿Qué se obtiene si se añaden más 1's a la fracción?

6. Si $r \in \mathbb{Q}^*$, $r + \frac{1}{r} \in \mathbb{Z}$ si y solo si $r = \pm 1$.

7. Sean $r < s$ racionales y $0 \leq \lambda \leq 1$ racional. Entonces:

   a) $r \leq \lambda r + (1 - \lambda)s \leq s$. ¿Qué se obtiene si $\lambda = 1/2$?

   b) Recíprocamente, si $r < t < s$ y t es racional, entonces $t = \lambda r + (1 - \lambda)s$, para cierto $\lambda \in [0, 1] \cap \mathbb{Q}$. ¿Por qué esto demuestra que entre dos racionales existen infinitos racionales?

   c) Si $\frac{a}{b} < \frac{c}{d}$ son racionales $(b, d > 0)$, entonces $\frac{a}{b} < t = \frac{a+c}{b+d} < \frac{c}{d}$. Esta fracción se conoce como la *mediante* entre a/b y c/d. ¿Cuál es el valor de λ en este caso?

   d) Responda la misma pregunta siendo ahora $t = \frac{na+mc}{nb+md}$, con $n, m \in \mathbb{N}^+$.

8. Considere la función $f : \mathbb{Q}^+ \to \mathbb{Q}$ dada por

$$f(p) = p - \frac{p^2 - 2}{p + 2}.$$

Mostrar que si $p^2 < 2$, entonces $p < f(p)$ y $f(p)^2 < 2$. De la misma forma, si $p^2 > 2$, entonces $f(p) < p$ y $f(p)^2 > 2$. Concluir que

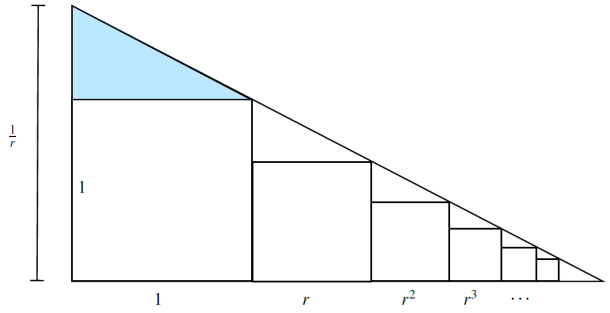
a) $A = \{p \in \mathbb{Q}^+ : p^2 < 2\}$ es acotado superiormente y no tiene supremo en $\mathbb{Q}$.

b) $B = \{p \in \mathbb{Q}^+ : p^2 > 2\}$, aunque acotado inferiormente, no tiene ínfimo en $\mathbb{Q}$.

4.2. Representaciones de $\mathbb{Q}$

1. Justifique geométricamente a través de la figura (semejanza de triángulos) la suma de la serie geométrica

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}, \qquad 0 < r < 1.$$



2. Encontrar el número real asociado a las siguientes fracciones continuas simples:

a) $[1; 2, 2, 2, \dots]$.

b) $[2; 1, 1, 1, \dots]$.

c) $[0; k, \dots, k]$, $k \in \mathbb{N}^+$.

d) $[1, 2, 1, 2, 1, 2, \dots]$.

e) $[4; 1, 2, 3, 2, 3, 2, 3, \dots]$.

3. Dados $r = [a_0; a_1, a_2, \dots, a_n], s = [b_0; b_1, b_2, \dots, b_n] \in \mathbb{Q}$, determine condiciones sobre los coeficientes a_j, b_j para decidir cuando $r < s$.

4. *a*) Mostrar que $-[0; a_1, a_2, \dots, a_n] = [-1; 1, a_1 - 1, a_2, \dots, a_n]$, donde los $a_j \geq 1, j = 1, \dots, n$ son enteros.

   b) Emplear esto para expandir a $-27/56$ como fracción continua simple finita de la forma $[-1; 1, ...]$.

5. Considere los enteros $a = 59$ y $b = 13$.

   a) Hallar $\gcd(a, b)$ y escribirlo como combinación lineal de ellos.

   b) Expandir a $\dfrac{a}{b}$ como fracción continua simple finita.

   c) Determine la posición de $\dfrac{a}{b}$ en el árbol de Calkin–Wilf.

6. Demostrar por inducción que $r \in \mathbb{Q}^+$ y $1/r \in \mathbb{Q}^+$ están en el mismo nivel del árbol de Calkin–Wilf.

7. Sea $r \in \mathbb{Q}^+$ que aparece en el nivel n del árbol de Calkin–Wilf. Si $r = [a_0; a_1, \ldots, a_k]$ es su fracción continua simple finita (donde $a_i \geq 0$ para todo i y $a_k \geq 1$), entonces

$$a_0 + a_1 + \cdots + a_k = n.$$

8. Si $x \in \mathbb{Q}^*$, comprobar que

$$|x| \cdot \prod_{p \text{ primo}} |x|_p = 1.$$

9. (Números armónicos) Los números armónicos se definen por

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}, \qquad n \geq 1.$$

A continuación se presentan dos argumentos para mostrar que H_n nunca es entero[1], salvo en el caso $n = 1$.

a) Sea p el máximo primo tal que $p < n$. Por el postulado de Bertrand $n < 2p$. Asuma por contradicción que H_n es entero. Mostrar que $pH_n - 1 = p\frac{a}{b}$, donde $\gcd(p, b) = 1$ y obtener así una contradicción.

b) Sea r el máximo talque $2^r \leq n < 2^{r+1}$. Si $L = \operatorname{lcm}(1, 2, \ldots, n)$, entonces $L = 2^r c$, con c impar ($\nu_2(L) = 2^r$). Si $L = ka_k, k = 1, \ldots, n$, entonces $LH_n = a_1 + a_2 + \cdots + a_n = M$. Mostrar que cada $a_j, j \neq 2^r$ es par y por tanto M es impar, mientras que L es par. Por tanto, $H_n = M/L$ es una fracción irreducible, no entera.

10. (Kürschák) Si $m > n$, entonces $H_m - H_n$ nunca es entero[2].

11. *a*) Si $n, p, q \in \mathbb{N}^+$, entonces $\dfrac{1}{n} = \dfrac{1}{n+1} + \dfrac{1}{n(n+1)}$ y $\dfrac{1}{pq} = \dfrac{1}{p(p+q)} + \dfrac{1}{q(p+q)}$.

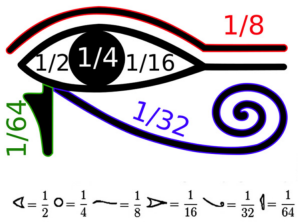
b) Si n es impar, mostrar que $\dfrac{2}{n} = \dfrac{1}{(n+1)/2} + \dfrac{1}{n(n+1)/2}$.

c) Una *fracción egipcia* es un número racional de la forma

$$\frac{1}{a_1} + \cdots + \frac{1}{a_n},$$

donde $n \in \mathbb{N}^+$ y $a_1 < a_2 < \cdots < a_n$ son naturales. Por ejemplo $\frac{2}{3} = \frac{1}{2} + \frac{1}{6}$. Estas expansiones no son únicas, por ejemplo

$$\frac{5}{121} = \frac{1}{25} + \frac{1}{757} + \frac{1}{763\,309} + \frac{1}{873\,960\,180\,913} + \frac{1}{1\,527\,612\,795\,642\,093\,418\,846\,225} = \frac{1}{33} + \frac{1}{121} + \frac{1}{363}.$$



Investigue el algoritmo de Fibonacci (inducción fuerte sobre m) para demostrar que cada racional $0 < m/n < 1$ se puede escribir como una fracción egipcia.

[1] Parece que el primer lugar donde aparece una prueba de este resutaldo es en: Theisinger (Bemerkung über die harmonische Reihe, Monatsh. f. Mathematik und Physik 26 (1915), 132–134, donde emplean el postulado de Bertrand y determinantes.

[2] Para más información puede consultar la nota Conrad K. The p-adic growth of harmonic sums

5. Números reales

5.1. Cuerpos ordenados. Números reales, algebraicos, trascendentes.

1. Mostrar que $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{R} : a, b, c \in \mathbb{Q}\}$ es un cuerpo con las operaciones usuales. Determinar el recíproco de $1 + \sqrt[3]{2}$ como elemento de $\mathbb{Q}[\sqrt[3]{2}]$.

2. Determinar si los siguientes números son racionales o irracionales:

   a) $\sqrt{3} - \sqrt{2}$.
   b) $\sqrt{2} + \sqrt{3} + \sqrt{5}$.
   c) $\log_{10} 2$.
   d) $1 + 2^{1/3} + 2^{2/3}$.
   e) $1 + 3^{1/5} + 3^{2/5} + 3^{3/5} + 3^{4/5}$.
   f) $0{,}10110011100011110000111100000\ldots$
   g) $0, 12345678910111212131415161718\ldots$
   h) $\sqrt{2025 - \pi} + \sqrt{2025 + \pi}$.

3. Determine si los siguientes números son algebraicos, trascendentes y/o construibles:

   a) $\sqrt{3} + \sqrt{7}$.
   b) $e^2 + 1$.
   c) $\sqrt{2 + \sqrt{3 + \sqrt{19}}}$.
   d) $a + bi \in \mathbb{Q}[i]$.
   e) $\cos\left(\frac{2\pi}{3}\right)$.
   f) $\frac{1}{\pi^4+1}$.
   g) $\sin\left(\frac{2\pi}{5}\right)$.
   h) $e + \frac{1}{e}$.

4. Sea K un cuerpo y $a, b, c \in K$. Comprobar que

   $$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ac) = \frac{(a+b+c)}{2}\left[(a-b)^2+(b-c)^2+(c-a)^2\right],$$

   donde la última igualdad es válida si $\mathrm{char}(K) \neq 2$. Si $K = \mathbb{R}$ concluya que $a^3+b^3+c^3 = 3abc$ si y solo si $a + b + c = 0$ ó $a = b = c$.

5. Sea K un cuerpo ordenado y asuma que cada $x \in K$ con $x > 0$ tiene una raíz cuadrada, es decir, existe $\xi \in K$ con $\xi > 0$ tal que $\xi^2 = x$ (se denotará $\xi = \sqrt{x}$).

   a) Mostrar que dicha raíz es única.
   b) Si $x > 0$ y $a > 0$. Entonces

   $$x + \frac{a}{2\sqrt{x^2 + a}} \;<\; \sqrt{x^2 + a} \;<\; x + \frac{a}{2x}.$$

c) Si $x, y \in K$ y $x \geq y$, entonces

$$\sqrt{x+y} = \sqrt{\frac{x+\sqrt{x^2-y^2}}{2}} + \sqrt{\frac{x-\sqrt{x^2-y^2}}{2}}.$$

Por ejemplo, comprobar que en $\mathbb{R}$ $\sqrt{\frac{7+\sqrt{13}}{2}} = \frac{1+\sqrt{13}}{2}$.

6. *a*) Sea $r \in \mathbb{Q}$ y $x \in \mathbb{R} \setminus \mathbb{Q}$. Entonces $r + x, r \cdot x \in \mathbb{R} \setminus \mathbb{Q}$. Además $x^{1/n} \in \mathbb{R} \setminus \mathbb{Q}$ si $n \in \mathbb{N}^+$.
   b) ¿Existen números irracionales x, y tales que $x^y \in \mathbb{Q}$? Indicación: La solución usual es $x = \sqrt{2}^{\sqrt{2}}$ (la *constante de Gelfond–Schneider* que se sabe que es irracional. ¿Quién debería ser y?
   c) Considere ahora $x = \log_{10}(4)$ e $y = \sqrt{10}$. Mostrar que son irracionales y calcular x^y.

7. Denotemos por $\mathfrak{C} \subseteq \mathbb{R}$ al conjunto de números construibles (con regla y compás).
   a) Demostrar que si $y \in \mathfrak{C}$ y $y \neq 0$, entonces $1/y \in \mathfrak{C}$.
   b) Si $y \in \mathfrak{C}$ y $y > 0$ entonces $\sqrt{y} \in \mathfrak{C}$. Indicación: Calcular la longitud r del segmento de recta perpendicular al eje x que une $(1, 0)$ con la parte superior del círculo con centro $(y + 1/2, 0)$ y radio $y + 1/2$.
   c) Sea $\theta \in \mathbb{R}$. Demostrar que $\cos(\theta) \in \mathfrak{C}$ si y solo si $\sin(\theta) \in \mathfrak{C}$. Además si $\cos(\theta) \in \mathfrak{C}$ entonces $\cos(2\theta), \cos\left(\frac{\theta}{2}\right), \sin(2\theta), \sin\left(\frac{\theta}{2}\right) \in \mathfrak{C}$.

8. Si $\alpha, \beta \in \mathbb{R}$, entonces

$$\text{máx}(\alpha, \beta) = \frac{\alpha + \beta + |\alpha - \beta|}{2}, \qquad \text{mín}(\alpha, \beta) = \frac{\alpha + \beta - |\alpha - \beta|}{2}.$$

Además $\text{máx}(\alpha, \beta) + \text{mín}(\alpha, \beta) = \alpha + \beta$.

9. Sean $a, b \in \mathbb{R}$ y $0 \leq \lambda \leq 1$. Entonces:
   a) $\text{mín}\{a, b\} \leq \lambda a + (1 - \lambda)b \leq \text{máx}\{a, b\}$.
   b) (Densidad de los números irracionales) Dados $a, b \in \mathbb{R}$ con $a < b$, existe $x \in \mathbb{R} \setminus \mathbb{Q}$ tal que $a < x < b$.

10. Sea $x \in \mathbb{R} \setminus \mathbb{Q}$. Determinar condiciones sobre $a, b, c, d \in \mathbb{Q}$ para que $\frac{ax+b}{cx+d}$ sea irracional.

11. Sea $\zeta \in \mathbb{R}$ un número trascendente sobre $\mathbb{Q}$, $n \in \mathbb{N}^+, r \in \mathbb{Q}^*$ y $p \in \mathbb{Q}[x]$. Entonces $r\zeta, \zeta^n, p(\zeta)$ y $\frac{1}{\zeta}$ son trascendentes. ¿Qué afirmaciones sobre números algebraicos se obtienen al aplicar la contrarecíproca de la anterior afirmación?

12. Es posible demostrar que el conjunto de números algebraicos reales $\mathbb{A}$ es un cuerpo con las operaciones de $\mathbb{R}$. Además F. von Lindermann demostró en 1882 que $\pi \notin \mathbb{A}$. Empleando estas observaciones se puede demostrar directamente que $\mathbb{R} \setminus \mathbb{A}$ no es contable. Para ello considere la función $f : [0, +\infty) \to \mathbb{R} \setminus \mathbb{A}$ dada por

$$f(x) = \begin{cases} \pi + x, & \text{si } \pi + x \notin \mathbb{A}, \\ \pi - x, & \text{si } \pi + x \in \mathbb{A}. \end{cases}$$

Demostrar que f está bien definida. Además es inyectiva: si $f(x) = f(y)$, entonces

$$x = |f(x) - \pi| = |f(y) - \pi| = y.$$

Por tanto, $\mathbb{R} \setminus \mathbb{A}$ contiene un conjunto no contable, concluyendo así el resultado. [1]

5.2. Sobre la construcción de $\mathbb{R}$

1. Sea $C \subseteq \mathbb{R}$ un conjunto acotado superiormente. Mostrar que $c = \sup C$ si y solo si c es cota superior de C y para todo $\epsilon > 0$, existe $x \in C$ tal que $c - \epsilon < x$. Formular y demostrar la afirmación análoga para el caso del ínfimo.

2. Sean $A, B \subseteq (0, +\infty)$ acotados superiormente. Si definimos $A \cdot B := \{ab \in \mathbb{R} : a \in A, b \in B\}$, mostrar que $A \cdot B$ es acotado superiormente y $\sup(A \cdot B) = \sup(A) \cdot \sup(B)$.

3. $A \subseteq \mathbb{R}$ se dice *inductivo* si $0 \in A$ y si para todo $a \in A$, se tiene que $a + 1 \in A$. Demostrar que $\mathbb{N}$ es la intersección de todos los conjuntos inductivos de $\mathbb{R}$ (y por tanto el conjunto inductivo más pequeño contenido en $\mathbb{R}$).

4. Demostrar que toda sucesión de Cauchy en $\mathcal{C}_{\mathbb{Q}}$ es acotada.

5. Comprobar que si $\lim_{n \to +\infty} a_n = a$ y $\lim_{n \to +\infty} b_n = b$ en $\mathbb{Q}$, entonces $\lim_{n \to +\infty} a_n b_n = ab$. Mostrar además que el producto de sucesiones de Cauchy en $\mathbb{Q}$ es de nuevo una sucesión de Cauchy.

6. Comprobar que si α, β son cortaduras de Dedekind, entonces $\alpha < \beta, \alpha = \beta$ ó $\beta < \alpha$.

7. Mostrar que si $\alpha_1, \ldots, \alpha_n$ son contaduras de Dedekind, lo mismo es válido para $\bigcup_{j=1}^{n} \alpha_j$ y $\bigcap_{j=1}^{n} \alpha_j$. ¿Qué números reales representan estas nuevas cortaduras?

8. Dado $x \in \mathbb{R}$ y $n \in \mathbb{N}^+$ considere el intervalo $I_n = [x - \frac{1}{n}, x + \frac{1}{n}]$. Demostrar que $\bigcap_{n=1}^{\infty} I_n = \{x\}$.

[1] J. Gaspar. Direct Proof of the Uncountability of the Transcendental Numbers. The American Mathematical Monthly, 121(1):78–80, 2014. doi: 10.4169/amer.math.monthly.121.01.080

6. Números complejos

6.1. Representación cartesiana

1. Calcular la siguientes expresiones:

   a) $(2+i)^3, \dfrac{1}{(1+i)^5}, \displaystyle\sum_{j=0}^{n-1} i^j.$

   b) Las partes reales e imaginarias de $\frac{z+1}{z-1}$, en términos de $x = \mathrm{Re}(z)$ y $y = \mathrm{Im}(z)$.

2. Muestre que para todo $n \in \mathbb{N}^+$, la función $z \to z^n + \overline{z}^n$ solo asume valores reales, mientras que $z \to z^n - \overline{z}^n$ solo asume valores imaginarios puros.

3. Determinar los siguientes conjuntos, graficando de ser posible:

   $$\{z \in \mathbb{C} : \overline{z} = -z\}, \quad \{z \in \mathbb{C} : \mathrm{Im}(iz-2) > 0\}, \quad \{z \in \mathbb{C} : |z+2|+|z-4| = 7\}, \quad \left\{z \in \mathbb{C} : \left|z + \frac{1}{z}\right| = 2\right\}.$$

4. Dado $z \in \mathbb{C}^*$, mostrar que existen $a, b \in \mathbb{R}$ tales que $z^2 = az + b$. Más generalmente, que dado $n \in \mathbb{N}^+$, existen $a_n, b_n \in \mathbb{R}$ tales que $z^n = a_n z + b_n$.

5. Mostrar que tres puntos distintos $z_0, z_1, z \in \mathbb{C}$ son colineales si y solo si $(z-z_0)/(z_1-z_0) \in \mathbb{R}$.

6. Comprobar que $|\mathrm{Re}(z)| + |\mathrm{Im}(z)| \leq \sqrt{2}|z|$, para todo $z \in \mathbb{C}$.

7. Dados $z, w \in \mathbb{C}$ se tiene que

   $$|z+w|^2 + |z-w|^2 = 2(|z|^2 + |w|^2).$$

   Interprete esta fórmula geométricamente.

8. Demuestre que $\left|\frac{a-b}{1-\overline{a}b}\right| < 1$ si $|a| < 1$ y $|b| < 1$. Además $\left|\frac{a-b}{1-\overline{a}b}\right| = 1$ si $|a| = 1$ ó $|b| = 1$.

6.2. Representación polar

1. Emplear la forma polar para calcular los números

   $$(1+i)^8, \qquad (1+i)^{-6}, \qquad \frac{(1+i)^2}{(1-i)^4}.$$

   Además hallar las posibles raíces $\sqrt[4]{i}, \sqrt{1+i}$.

2. Mostrar que $\frac{z}{|z|} + \frac{|z|}{z} \in \mathbb{R}$ para todo $z \in \mathbb{C}^*$. Además si $|z| = 1$, entonces $\frac{z^{2n}+1}{z^n} \in \mathbb{R}$, para todo $n \in \mathbb{N}$.

3. Comprobar que $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ es un subgrupo de $(\mathbb{C}^*, \cdot)$. Además $I = \{z \in \mathbb{C} :$ existe $n \in \mathbb{N}$ tal que $z^n = 1\}$ es subgrupo de S^1.

4. Demostrar que $(1+i)^n + (1-i)^n = 2\sqrt{2}^n \cos(n\pi/4)$ y $(\sqrt{3}+i)^n + (\sqrt{3}-i)^n = 2^{n+1}\cos(n\pi/6)$, para todo $n \in \mathbb{N}$. Indicación: Escriba $e^{\pi i/4}$ y $e^{\pi i/6}$ en forma cartesiana.

5. Si $z \in \mathbb{C}$ y $\mathrm{Re}(z^n) \geq 0$, para todo $n \in \mathbb{N}$, entonces z es un número real positivo.

6. *a*) Fije $z \in \mathbb{C}$. Suponiendo que puede usar derivadas, mostrar que para todo entero positivo n, se verifica que

$$1 + 2z + \cdots + nz^{n-1} = \frac{nz^{n+1} - (n+1)z^n + 1}{(z-1)^2}.$$

¿Qué identidad conocida se obtiene al tomar $z \to 1$?

b) Sea $\omega \in \mathbb{C} \setminus \{1\}$ una raíz $n-$ésima de la unidad. Calcular $1 + \omega + \omega^2 + \cdots + \omega^{n-1}$ y $1 + 2\omega + 3\omega^2 + \cdots + n\omega^{n-1}$.

7. Sean $z = e^{i\theta}, z' = e^{i\theta'} \in S^1$. Comprobar que

$$\frac{z+z'}{1+zz'} = \frac{\cos\left(\frac{\theta-\theta'}{2}\right)}{\cos\left(\frac{\theta+\theta'}{2}\right)}.$$

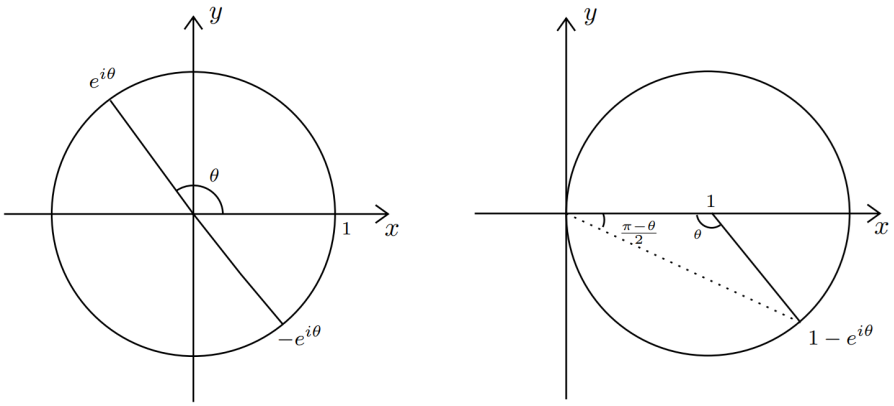
Encontrar expresiones similares para $\dfrac{z+z'}{1-zz'}, \dfrac{z-z'}{1+zz'}$ y $\dfrac{z-z'}{1-zz'}$.

8. Mostrar que

$$\left(\frac{1+i\tan t}{1-i\tan t}\right)^n = \frac{1+i\tan(nt)}{1-i\tan(nt)}, \quad n \geq 1.$$

9. Utilice la siguiente figura para comprobar las identidades

$$|1-e^{i\theta}|^2 = 2(1-\cos(\theta)) = 4\sin(\theta/2)^2, \qquad \arg(1-e^{i\theta}) = \begin{cases} \frac{\theta-\pi}{2}, & \text{si } 0 < \theta < \pi, \\ \frac{\pi+\theta}{2}, & \text{si } -\pi < \theta < 0. \end{cases}$$



10. Empleando las fórmulas para la extracción de raíces cuadradas en forma cartesiana comprobar que

$$\cos(\theta/2)^2 = \frac{1+\cos\theta}{2}, \qquad \sin(\theta/2)^2 = \frac{1-\cos\theta}{2},$$

donde los signos se determinan según cada caso. Emplear estas fórmulas para comprobar que

$$e^{i\pi/8} = \frac{\sqrt{2+\sqrt{2}}}{2} + \frac{\sqrt{2-\sqrt{2}}}{2}i, \qquad e^{i\pi/12} = \frac{\sqrt{6}+\sqrt{2}}{4} + i\frac{\sqrt{6}-\sqrt{2}}{4}.$$

11. Mostrar que

$$e^{2\pi i/5} = \frac{\sqrt{5}-1}{4} + i\frac{\sqrt{5+\sqrt{5}}}{2\sqrt{2}}, \quad e^{i\pi/5} = \frac{\sqrt{5}+1}{4} + i\frac{\sqrt{5-\sqrt{5}}}{2\sqrt{2}},$$

observando que $e^{2\pi i/5}$ satisface $(z+1/z)^2 + (z+1/z) = 1$, que se puede resolver empleando la fórmula cuadrática dos veces.

12. (Identidades de Lagrange) Si $\theta \in \mathbb{R} \setminus \{0, \pm 2\pi, \pm 4\pi, \dots\}$ y $n \in \mathbb{N}^+$ se verifica que:

$$\cos\theta + \cos(2\theta) + \cdots + \cos(n\theta) = \frac{\sin\left(\frac{n\theta}{2}\right)\cos((n+1)\theta/2)}{\sin\left(\frac{\theta}{2}\right)},$$

$$\sin\theta + \sin(2\theta) + \cdots + \sin(n\theta) = \frac{\sin\left(\frac{n\theta}{2}\right)\sin((n+1)\theta/2)}{\sin\left(\frac{\theta}{2}\right)},$$

$$\frac{1}{2} + \cos(\theta) + \cos(2\theta) + \cdots + \cos(n\theta) = \frac{\sin\left((n+\frac{1}{2})\theta\right)}{2\sin(\theta/2)}.$$

Puede establecer estas identidades empleando la expansión $1 + z + \cdots + z^{n-1} = \frac{z^n-1}{z-1}$, para $z = e^{i\theta} \neq 1$ y luego igualando partes reales e imaginarias, ver Proposición 13.4 del Libro Introducción al Análisis Real, guía actualizada de clase. Puede consultar demostraciones geométricas recientes en los artículos:

- Jonathan Balsam (2022) Proof Without Words: Lagrange's Trigonometric Identity, The College Mathematics Journal, 53:5, 399-399, doi: 10.1080/07468342.2022.2118996
- Jonathan Balsam (2023) Proof Without Words: Lagrange's Trigonometric Identity (Part II), The College Mathematics Journal, 54:3, 235-235, doi: 10.1080/07468342.2023.2206782

13. Empleando la congruencia de Wilson, demostrar que dado $n \in \mathbb{N}^+$, entonces

$$\frac{e^{2\pi i(n-1)!/n} - 1}{e^{-2\pi i/n} - 1} = \begin{cases} 1, & n \text{ es primo,} \\ 0, & \text{otros.} \end{cases}$$

14. (Complejos como matrices) Considere $R : \mathbb{C} \to C \subset \mathbb{R}^{2\times 2}$, dada por $R(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

   a) R preserva las operaciones. Además $|z|^2 = \det(R(z))$, $z \in \mathbb{C}$.

   b) $1/z$, $z \neq 0$, se corresponde a la matriz inversa de $R(z)$.

   c) Todo elemento de C admite una representación $r \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, con $r \geq 0$, $\theta \in \mathbb{R}$, que corresponde a la forma polar de un complejo.

7. Polinomios en una variable

7.1. Polinomios

En adelante K denotará un cuerpo.

1. Encontrar polinomios $S, T \in K[t]$ tales que $\gcd(p, q) = Sp + Tq$, donde:

   - $p(t) = t^2 + 1, q(t) = t^5 + 1 \in \mathbb{Q}[t]$.
   - $p(t) = t^2 + 2t + 1, q(t) = t^3 + 2t^2 + 2$ en $\mathbb{Z}/3\mathbb{Z}[t]$.

2. Mostrar que si $p \cdot q = 0$, donde $p, q \in K[t]$, entonces $p = 0$ ó $q = 0$. ¿Esto sigue siendo válido si asumimos que K es solo un anillo?

3. Comprobar que si $p(t) = a_n(t - \alpha_1) \cdots (t - \alpha_n) \in K[t]$, entonces $p(0) = a_n(-1)^n(\alpha_1 \cdots \alpha_n)$. Además, si $\alpha_j \neq 0$ para todo j, también podemos escribir

$$p(t) = p(0) \prod_{j=1}^{n} \left(1 - \frac{t}{\alpha_j}\right),$$

   dando otra representación de la factorización de $p(t)$.

4. Sean $a_0, \ldots, a_n \in K$ con $a_i \neq a_j$ si $i \neq j$. Mostrar que si $p, q \in K[t]$ tienen grado n y $p(a_j) = q(a_j), j = 0, \ldots, n$, entonces $p(t) = q(t)$.

5. Si F es un cuerpo, mostrar que existen infinitos polinomios mónicos irreducibles en $F[x]$.

6. Mostrar que si F es un cuerpo finito, existen polinomios no constantes en $F[t]$ que no tienen raíces en F.

7. *a)* Factorizar $t^4 + 2$ en $\mathbb{R}[t]$ y en $\mathbb{C}[t]$ como producto de factores irreducibles.
   b) De un ejemplo de un polinomio no constante en $(\mathbb{Z}/4\mathbb{Z})[t]$ que sea una unidad.
   c) ¿Cómo se factoriza $t^p + a^p \in (\mathbb{Z}/p\mathbb{Z})[t]$, donde $a \in \mathbb{Z}/p\mathbb{Z}$?

8. Considere el polinomio $P(t) = t^p - t$, donde $p \in \mathbb{Z}$ es primo.

   a) Mostrar que $t^p - t = \prod_{j=0}^{p-1}(t - j)$ se factoriza en $\mathbb{Z}/p\mathbb{Z}$. Por tanto, $t^{p-1} - 1 = \prod_{j=1}^{p-1}(t - j)$.
   b) Emplear estos polinomios para deducir la congruencia de Wilson $(p - 1)! \equiv -1 (\mathrm{mod} p)$.
   c) Comprobar que $P(t - a) = P(t)$, para todo $a \in \mathbb{Z}/p\mathbb{Z}$.

9. *a*) Sea $f \in \mathbb{R}[t]$ mónico tal que $f(t_0) > 0$ para todo $t_0 \in \mathbb{R}$. Demuestre que $f = P^2 + Q^2$ para ciertos $P, Q \in \mathbb{R}[t]$.

   b) Sea $f \in \mathbb{R}[t]$ tal que $f(t_0) \geq 0$ para todo $t_0 \in \mathbb{R}$. Demuestre que $f = P^2 + Q^2$ para ciertos $P, Q \in \mathbb{R}[t]$.

   c) Encuentre $P, Q \in \mathbb{R}[t]$ tales que $t^6 + t^4 + t^2 + 1 = P^2 + Q^2$.

10. Sea K un cuerpo y $p(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$. La *derivada* de p se define formalmente como $p'(t) = a_1 + 2a_2 t + \cdots + n a_n t^{n-1}$.

   a) Demuestre que $(p+q)' = p' + q'$ y $(pq)' = p'q + pq'$, para todo $p, q \in K[t]$.

   b) Si $a \in K$ y $p(t) = q(t)(t-a) + p(a)$, entonces $q(a) = p'(a)$. Más generalmente, comprobar la fórmula de Taylor
   $$p(t) = \sum_{j=0}^{n} \frac{p^{(j)}(a)}{j!}(t-a)^j.$$

   c) Dados $p = a_0 + a_1 t + \cdots + a_n t^n, q \in K[t]$, se define la *composición entre p y q* por $(p \circ q)(t) := a_0 + a_1 q(t) + \cdots + a_n q(t)^n$. ¿Qué grado tiene $p \circ q$? Mostrar que $(p \circ q)'(t) = (p' \circ q)(t) \cdot q'(t)$.

   d) Demostrar que p no tiene raíces repetidas si y sólo si $\gcd(p, p') = 1$.

   e) ¿Bajo qué condiciones podemos concluir que $p' = 0$ si $p \in \mathbb{R}[t], \mathbb{C}[t], \mathbb{Z}/p\mathbb{Z}[t]$, p primo, respectivamente?

11. *a*) Si $p(t) = \prod_{j=1}^{n}(t - a_j) \in K[t]$, donde $a_1, \ldots, a_n \in K$ son elementos distintos entre si, entonces
   $$\frac{1}{(t-a_1)\cdots(t-a_n)} = \sum_{j=1}^{n} \frac{c_j}{t-a_j}, \qquad \frac{1}{c_j} = p'(a_j) = \prod_{l \neq j}(a_j - a_l).$$

   b) (Interpolación de Lagrange) Sea $f \in K[t]$ con $\deg f < n$ y considere la función racional $f(t)/p(t)$. Al escribir $f(t) = f(a_j) + (t - a_j)g_j(t)$ con $g_j \in K[t]$ y $\deg g_j \leq n-2$ se obtiene que
   $$\frac{f(t)}{p(t)} = \sum_{j=1}^{n} \frac{f(t)}{(t-a_j)p'(a_j)} = \sum_{j=1}^{n} \frac{f(a_j)}{(t-a_j)p'(a_j)} + \sum_{j=1}^{n} \frac{g_j(t)}{p'(a_j)}.$$

   Demostrar que el polinomio $R(t) = \sum_{j=1}^{n} \frac{g_j(t)}{p'(a_j)}$ de grado $\leq n-2$ es el polinomio cero. Concluya la fórmula de interpolación de Lagrange
   $$f(t) = \sum_{j=1}^{n} f(a_j) \prod_{k \neq j} \frac{t - a_k}{a_j - a_k}.$$

   c) Encontrar un polinomio de grado 5 en $\mathbb{Q}[x]$ tal que $p(0) = 1$, $p(1) = -1$, $p(-1) = 0$, $p(2) = 0$, $p(-2) = 3$ y $p(10) = 10$.

   d) Dado $p \in \mathbb{C}[t]$, demostrar que $p(\mathbb{Z}) \subseteq \mathbb{Q}$ si y solo si $p \in \mathbb{Q}[t]$. Indicación: interpolar p en $0, 1, \ldots, n$, con $n = \deg p$.

   e) Considere los polinomios $p_k(x) = \binom{x}{k} := \frac{x(x-1)\cdots(x-k+1)}{k!}$.$k \geq 1$, y $\binom{x}{0} = 1$. Mostrar que $\deg p_k = k$ y aunque $p_k(\mathbb{Z}) \subseteq \mathbb{Z}$, $p_k \in \mathbb{Q}[t] \setminus \mathbb{Z}[t]$.

12. Si $p(t) = c\prod_{j=1}^{n}(t-\alpha_j)^{m_j} \in \mathbb{C}[t]$, mostrar que

$$\frac{p'(t)}{p(t)} = \sum_{j=1}^{n} \frac{m_j}{t-\alpha_j}.$$

13. Sea $a = x + \frac{1}{x} \in \mathbb{Q}(x)$. Demostrar que $x^n + \frac{1}{x^n}$ se puede escribir como un polinomio en a con coeficientes enteros. De hecho

$$x^n + \frac{1}{x^n} = P_n(a), \qquad P_{n+1}(a) = aP_n(a) - P_{n-1}(a)$$

donde $P_0 = 2$ y $P_1 = a$. En términos de los polinomios de Chebyshev $T_n(\cos\theta) = \cos(n\theta)$ se puede escribir

$$x^n + \frac{1}{x^n} = 2T_n\left(\frac{x+x^{-1}}{2}\right).$$