Soluciones de Problemas propuestos
Fundamentos de Informática

Horst H.~von Brand

16 de octubre de 2015

1. Preliminares

1. Las definiciones son:

   $f(n) = O(g_1(n))$**:** Hay $n_0 \in \mathbb{N}$ y $c > 0$ tales que para todo $n \geq n_0$ se cumple $f(n) < cg_1(n)$

   $f(n) = \Omega(g_2(n))$**:** Hay $n_0 \in \mathbb{N}$ y $c > 0$ tales que para todo $n \geq n_0$ se cumple $f(n) > cg_2(n)$

   $f(n) = \Theta(g_3(n))$**:** Hay $n_0 \in \mathbb{N}$ y $c_1, c_2 > 0$ tales que para todo $n \geq n_0$ se cumple $c_1 g_3(n) < f(n) < c_2 g_3(n)$

   $f(n) \sim g(n)$**:** Esto significa

   $$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1$$

   La relación es que si $f(n) = \Omega(g(n))$ y $f(n) = O(g(n))$, entonces $f(n) = \Theta(g(n))$. La última es la más fuerte de todas, si $f(n) \sim g(n)$ entonces $f(n) = O(g(n))$, $f(n) = \Omega(g(n))$ y $f(n) = \Theta(g(n))$.

2. Las definiciones son:

   $f(n) = O(g(n))$ si hay constantes $c > 0$ y n_0 tales que para $n \geq n_0$ $f(n) \leq c \cdot g(n)$
   $f(n) = o(g(n))$ si para todo $\epsilon > 0$ existe n_0 tal que para $n \geq n_0$ $f(n) \leq \epsilon \cdot g(n)$

   En castellano, O da una cota superior para una función creciente, o acota una función que tiende a cero.

3. Las definiciones son:

   $f(n) = O(g_1(n))$**:** Hay $n_0 \in \mathbb{N}$ y $c > 0$ tales que para todo $n \geq n_0$ se cumple $f(n) < cg_1(n)$

   $f(n) = \Omega(g_2(n))$**:** Hay $n_0 \in \mathbb{N}$ y $c > 0$ tales que para todo $n \geq n_0$ se cumple $f(n) > cg_2(n)$

   $f(n) = \Theta(g_3(n))$**:** Hay $n_0 \in \mathbb{N}$ y $c_1, c_2 > 0$ tales que para todo $n \geq n_0$ se cumple $c_1 g_3(n) < f(n) < c_2 g_3(n)$

   La relación es que si $f(n) = \Omega(g(n))$ y $f(n) = O(g(n))$, entonces $f(n) = \Theta(g(n))$.

4. La diferencia simétrica contiene aquellos elementos que están en A o en B, pero no en ambos. O sea, es $A \mathbin{\triangle} B = (A \cup B) \smallsetminus (A \cap B)$. Esto puede expresarse como $(A \cup B) \cap \overline{(A \cap B)}$.

5. Por definición

   $$\lim_{n \to \infty} \frac{f(n)}{g(n)} = a$$

   con a finito cuando para todo $\epsilon > 0$ hay n_0 tal que siempre que $n \geq n_0$ $|\frac{f(n)}{g(n)} - a| \leq \epsilon$. Esto puede expresarse como

   $$(a - \epsilon) g(n) \leq f(n) \leq (a + \epsilon) g(n) \text{ cuando } n \geq n_0$$

   La segunda desigualdad corresponde a la definición de $f(n) = O(g(n))$.

   Si $a > 0$, podemos elegir $\epsilon < a$, con lo que ambas desigualdades son con constantes positivas, y esto corresponde a $f(n) = \Theta(g(n))$.

6. Tenemos:

   a) Como $0 \leq \sin^2 n \leq 1$, para $n \geq 0$ tenemos que $n/2 \leq f(n) \leq 3n^2$. Según las definiciones:

   $$\begin{array}{ll} f(n) = \Omega(g(n)) & \text{hay } n' \geq 0 \text{ y } c' > 0 \text{ tales que siempre que } n \geq n',\ f(n) \geq c' g(n) \\ f(n) = O(g(n)) & \text{hay } n'' \geq 0 \text{ y } c'' > 0 \text{ tales que siempre que } n \geq n'',\ f(n) \leq c'' g(n) \end{array}$$

   En este caso, podemos tomar $n' = n'' = 1$, y la desigualdad anterior indica que se cumplen con $c' = 1/2$ y $c'' = 3$.

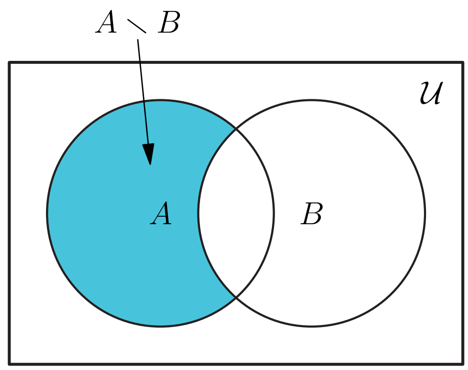


Figura 1: Diferencia entre conjuntos

b) No hay un único k tal que $f(n) = \Theta(n^k)$, las cotas inferior y superior indicadas son en realidad las mejores posibles.

7. La relación entre los conjuntos la ilustra la figura 1. Se ve que es simplemente $A \setminus B = A \cap \overline{B}$.

8. *Demostración.* Demostramos cada problema por separado.

a) Usando la definición de potencia factorial descendiente, el lado derecho de la expresión resulta

$$\begin{aligned} m^{\underline{n+k}} &= \prod_{0 \leq i < n+k} m - i \\ &= \left(\prod_{0 \leq i < n} m - i \right) \cdot \left(\prod_{n \leq j < n+k} m - j \right) \end{aligned}$$

el producto izquierdo corresponde a la definición de $m^{\underline{n}}$, reemplazando en la ecuación anterior se tiene

$$m^{\underline{n+k}} = m^{\underline{n}} \cdot \left(\prod_{n \leq j < n+k} m - j \right)$$

En el segundo producto realizamos un ajuste de índices. Primero desplazamos el rango n veces hacia la izquierda. Para mantener el mismo producto, reemplazamos la variable i por $i + n$. Resulta

$$\begin{aligned} \prod_{n \leq i < n+k} m - i &= \prod_{0 \leq i < k} m - (i + n) \\ &= \prod_{0 \leq i < k} (m - n) - i \\ &= (m - n)^{\underline{k}} \end{aligned}$$

Juntando ambos productos se obtiene

$$m^{\underline{n+k}} = m^{\underline{n}} (m - n)^{\underline{k}}$$

que es el resultado buscado.

b) El desarrollo es análogo al planteado en el ejercicio anterior. La definición de las potencias factoriales ascendentes indica que

$$\begin{aligned} m^{\overline{n+k}} &= \prod_{0 \leq i < n+k} m + i \\ &= \left(\prod_{0 \leq i < n} m + i \right) \cdot \left(\prod_{n \leq j < n+k} m + i \right) \end{aligned}$$

El producto de la izquierda corresponde a la definición de $m^{\overline{n}}$. Ajustamos el índice del segundo producto usando el mismo sistema anterior, luego

$$\begin{aligned}\prod_{n\leq j<n+k} m+j &= \prod_{0\leq j<k} m+(j+n)\\ &= \prod_{0\leq j<k} (m+n)+j\\ &= (m+n)^{\overline{k}}\end{aligned}$$

Uniendo ambos resultados resulta la expresión

$$m^{\overline{n+k}} = m^{\overline{n}}(m+n)^{\overline{k}}$$

que corresponde a la expresión buscada.

c) Nuevamente recurrimos a la definición de potencias factoriales descendentes.

$$x^{\underline{k}} = \prod_{0\leq i<k} x-i$$

Si factorizamos por (-1) cada factor del producto, y considerando que son k factores, se concluye la expresión

$$\begin{aligned}x^{\underline{k}} &= (-1)^k \cdot \prod_{0\leq i<k} i-x\\ &= (-1)^k \cdot \prod_{0\leq i<k} (-x)+i\\ &= (-1)^k \cdot (-x)^{\overline{k}}\end{aligned}$$

Que corresponde a la expresión buscada.

□

9. *Demostración.* Procedemos con cada relación por separado. En primer lugar consideramos la relación de diferencia. Según su definición

$$\begin{aligned}\Delta(\alpha f(n)+\beta g(n)) &= \alpha f(n+1)-\alpha f(n)+\beta g(n+1)-\beta g(n)\\ &= \alpha(f(n+1)-f(n))+\beta(g(n+1)-g(n))\\ &= \alpha\Delta f(n)+\beta\Delta g(n)\end{aligned}$$

por lo que el operador es lineal.

Para el siguiente operador se procede de similar manera. Según su definición

$$\begin{aligned}\Sigma(\alpha f(n)+\beta g(n)) &= \sum_{0\leq k<n} (\alpha f(k)+\beta g(k))+c\\ &= \alpha \sum_{0\leq k<n} f(k)+\beta \sum_{0\leq k<n} g(k)+c\\ &= \alpha\Sigma f(n)+\beta\Sigma g(n)\end{aligned}$$

Recordar que c es un parámetro constante, que en este caso se dividió en dos para ajustar la expresión final a la definición del operador $\Sigma f(n)$. □

10. *Demostración.* Demostramos de manera directa, cada relación por separado. De la definición de los operadores sabemos que

$$\Sigma f(n) = \sum_{0\leq k<n} f(k)+c$$

Al aplicar el operador Δ se tiene

$$\begin{aligned}
\Delta\Sigma f(n) &= \Delta\left(\sum_{0\le k<n} f(k) + c\right) \\
&= \Delta\left(\sum_{0\le k<n} f(k)\right) + \Delta c \\
&= \sum_{0\le k<n+1} f(k) - \sum_{0\le k<n} f(k)
\end{aligned}$$

La suma izquierda tiene un sumando más que la derecha, correspondiente a evaluar k como n. Separando el término de la sumatoria, se concluye

$$\begin{aligned}
\Delta\Sigma f(n) &= \sum_{0\le k<n} f(k) + f(n) - \sum_{0\le k<n} f(k) \\
&= \left(\sum_{0\le k<n} f(k) - \sum_{0\le k<n} f(k)\right) + f(n) \\
&= f(n)
\end{aligned}$$

Por lo que la primera relación es correcta.

Usando nuevamente la definición de los operadores, se tiene para la segunda relación

$$\begin{aligned}
\Sigma\Delta f(n) &= \Sigma\left(f(n+1) - f(n)\right) + c \\
&= \sum_{0\le k<n+1} f(k) - \sum_{0\le k<n} f(k) + c \\
&= \left(\sum_{0\le k<n} f(k) - \sum_{0\le k<n} f(k)\right) + f(n) + c \\
&= f(n) + c
\end{aligned}$$

Por lo cual esta relación también es correcta. $\square$

11. Basta usar la definición de coeficiente binomial y aplicar algunas identidades simples, como:

$$\begin{aligned}
\alpha^{\underline{k+1}} &= \alpha^{\underline{k}} \cdot (\alpha - k) \\
(\alpha+1)^{\underline{k+1}} &= (\alpha+1) \cdot \alpha^{\underline{k}}
\end{aligned}$$

que resultan directamente de:

$$\alpha^{\underline{k}} = \alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)$$

Resulta:

$$\begin{aligned}
\binom{\alpha}{k} + \binom{\alpha}{k+1} &= \frac{\alpha^{\underline{k}}}{k!} + \frac{\alpha^{\underline{k+1}}}{(k+1)!} \\
&= \frac{(k+1)\alpha^{\underline{k}} + \alpha^{\underline{k+1}}}{(k+1)!} \\
&= \frac{\alpha^{\underline{k}}((k+1) + (\alpha - k))}{(k+1)!} \\
&= \frac{\alpha^{\underline{k}}(\alpha+1)}{(k+1)!} \\
&= \frac{(\alpha+1)^{\underline{k+1}}}{(k+1)!}
\end{aligned}$$

2. Relaciones y funciones

1. Debemos verificar las siguientes propiedades:

   Reflexividad: $(a, b) \sim (a, b)$ significa que $a \cdot b = b \cdot a$, lo que se cumple en $\mathbb{Z}$.

   Transitividad: Como se excluye $(0, 0)$, podemos decir que:

   $$(a, b) \sim (c, d) \Longleftrightarrow a \cdot d = b \cdot c \Longleftrightarrow \frac{a}{b} = \frac{c}{d}$$

   Si $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$ tenemos que:

   $$\frac{a}{b} = \frac{c}{d}$$
   $$\frac{c}{d} = \frac{e}{f}$$

   por lo que:

   $$\frac{a}{b} = \frac{e}{f}$$

   Simetría: Si $(a, b) \sim (c, d)$ entonces $a \cdot d = b \cdot c$, o también $c \cdot b = d \cdot a$, vale decir $(c, d) \sim (a, b)$.

   Se cumplen las tres propiedades, es relación de equivalencia.

2. Si R es asimétrica, si fuera $a \mathrel{R} a$ por asimetría debe ser $a \not\mathrel{R} a$, lo que es contradictorio. Por tanto para todo a es $a \not\mathrel{R} a$, o sea, R es antireflexiva.

3. Esto corresponde a definir que $a \mathrel{R} b$ si y solo si $a \mathrel{R_1} b$ y $a \mathrel{R_2} b$. Para demostrar que R es una relación de equivalencia, debemos demostrar:

   Reflexividad: Para todo a tenemos $a \mathrel{R} a$.
   Como R_1 y R_2 son relaciones de equivalencia, son reflexivas, y $a \mathrel{R_1} a$ y $a \mathrel{R_2} a$ siempre se cumplen, con lo que se cumple $a \mathrel{R} a$.

   Simetría: Para todo a y b tenemos que si $a \mathrel{R} b$ entonces $b \mathrel{R} a$.
   Si $a \mathrel{R} b$ es que $a \mathrel{R_1} b$ y $a \mathrel{R_2} b$; por ser R_1 y R_2 relaciones de equivalencia son ambas simétricas, y $b \mathrel{R_1} a$ y $b \mathrel{R_2} a$; o sea $b \mathrel{R} a$.

   Transitividad: Para todo a, b y c tenemos que si $a \mathrel{R} b$ y $b \mathrel{R} c$ entonces $a \mathrel{R} c$.
   Nuevamente, si $a \mathrel{R} b$ y $b \mathrel{R} c$ es que $a \mathrel{R_1} b$ y $a \mathrel{R_2} b$; $b \mathrel{R_1} c$ y $b \mathrel{R_2} c$; siendo R_1 y R_2 relaciones de equivalencia es $a \mathrel{R_1} c$ y $a \mathrel{R_2} c$, con lo que $a \mathrel{R} c$.

   Como R cumple las tres propiedades, es una relación de equivalencia.

   Las clases de equivalencia de R son un refinamiento de las clases de equivalencia de R_1 y R_2, en el sentido que son subconjuntos.

4. Las propiedades son independientes, por lo que a lo más podríamos comentar sobre la misma propiedad en la transpuesta.

   a) Que R sea simétrica significa que siempre que $a \mathrel{R} b$ se tiene que $b \mathrel{R^{-1}} a$. En términos de la relación transpuesta, esto es siempre que $b \mathrel{R^{-1}} a$ se tiene que $a \mathrel{R^{-1}} b$. La transpuesta es simétrica también.

   b) Es antisimétrica si siempre que $a \mathrel{R} b$ y $b \mathrel{R} a$ entonces $a = b$. En términos de la relación transpuesta, esto es siempre que $b \mathrel{R^{-1}} a$ y $a \mathrel{R} b$ se cumple $a = b$. La transpuesta es antisimétrica también.

   c) Si R es transitiva, es que siempre que $a \mathrel{R} b$ y $b \mathrel{R} c$ también $a \mathrel{R} c$. En términos de la relación transpuesta, esto es siempre que $b \mathrel{R^{-1}} a$ y $c \mathrel{R^{-1}} b$ también $c \mathrel{R^{-1}} a$. La relación transpuesta también es transitiva.

   d) La relación R es reflexiva si para todo $a \in \mathcal{U}$ $a \mathrel{R} a$, que es $a \mathrel{R^{-1}} a$, y la transpuesta también es reflexiva.

5. Para que $\sim$ sea relación de equivalencia, debe ser:

Reflexiva: $a \sim a$ para todo a

Transitiva: Si $a \sim b$ y $b \sim c$ entonces $a \sim c$

Simétrica: Si $a \sim b$ entonces $b \sim a$

a) No es transitiva. Por ejemplo, $\gcd(3,4) = \gcd(4,9) = 1$, con lo que $3 \sim 4$ y $4 \sim 9$; pero $\gcd(3,9) = 3$, o sea $3 \not\sim 9$.
No es relación de equivalencia.

b) Es reflexiva, ya que $(x_1, y_1) \sim (x_1, y_1)$ corresponde a $x_1^2 + y_1^2 = x_1^2 + y_1^2$.
Es transitiva, $(x_1, y_1) \sim (x_2, y_2)$ y $(x_2, y_2) \sim (x_3, y_3)$ se traducen en $x_1^2 + y_1^2 = x_2^2 + y_2^2$ y $x_2^2 + y_2^2 = x_3^2 + y_3^2$, que dan $x_1^2 + y_1^2 = x_3^2 + y_3^2$, vale decir $(x_1, y_1) \sim (x_3, y_3)$
Es simétrica, porque $(x_1, y_1) \sim (x_2, y_2)$ es $x_1^2 + y_1^2 = x_2^2 + y_2^2$, o sea $x_2^2 + y_2^2 = x_1^2 + y_1^2$, que corresponde a $(x_2, y_2) \sim (x_1, y_1)$
Es relación de equivalencia.
Geométricamente, (x_1, y_1) y (x_2, y_2) son equivalentes si están sobre la misma circunferencia centrada en el origen.

c) Es reflexiva, ya que para todo $x \in \mathbb{R}$ tenemos $x - x = 0 \in \mathbb{Q}$, o sea $x \sim x$.
Es transitiva, ya que si $x \sim y$ y $y \sim z$ corresponden a $x - y = a \in \mathbb{Q}$ y $y - z = b \in \mathbb{Q}$. Pero entonces $x - z = (x - y) + (y - z) = a + b \in \mathbb{Q}$, lo que es decir $x \sim z$.
Es simétrica, ya que $x \sim y$ corresponde a $x - y = a \in \mathbb{Q}$, con lo que $y - x = -a \in \mathbb{Q}$, o sea $y \sim x$.
Es relación de equivalencia.

6. Para investigar preguntas del tipo “¿Es R una relación de equivalencia sobre $\mathcal{A}$?” en muchos casos es útil buscar una función f tal que $a \mathrel{R} b$ si y solo si $f(a) = f(b)$, porque:

   - $f(a) = f(a)$ para todo a (reflexividad)
   - $f(a) = f(b) \implies f(b) = f(a)$ (simetría)
   - $f(a) = f(b) \wedge f(b) = f(c) \implies f(a) = f(c)$ (transitividad)

   En tal caso las clases de equivalencia son *fibras* de f, conjuntos de la forma:

   $$[a] = \{b \in \mathcal{A} \colon f(b) = f(a)\}$$

   El número de clases de equivalencia es simplemente la cardinalidad del rango de f.

   Aplicando esto a nuestro caso, la función $n \mapsto$ máximo dígito de n claramente cumple lo indicado, y hay 10 clases de equivalencia.

7. Hay muchos ejemplos posibles.

   a) La función $f(k) = 2k$ es uno a uno, pero no sobre (ningún número impar tiene preimagen).

   b) La función $g(k) = \lfloor (k+1)/2 \rfloor$ es sobre, pero no uno a uno ($g(1) = g(2) = 1$).

8. Una relación es simétrica si siempre que $a \mathrel{R} b$ entonces $b \mathrel{R} a$. Si tenemos dos relaciones R_1 y R_2, su composición $R_2 \circ R_1$ se define mediante:

   $$x \mathrel{R_2 \circ R_1} y \text{ si existe } z \text{ tal que } x \mathrel{R_1} z \text{ y } \ z \mathrel{R_2} y$$

   Veamos cuándo es simétrica $R_2 \circ R_1$:

   $$y \mathrel{R_2 \circ R_1} x \text{ significa que hay } z' \text{ con } y \mathrel{R_1} z' \text{ y } z' \mathrel{R_2} x$$

   Esto *no* resulta automáticamente de lo anterior (podemos ir de x a z y de allí a y, pero perfectamente puede ser que y no esté relacionado con nada vía R_1). No siempre es simétrica.

9. Si la relación R es simétrica, entonces siempre que $a \mathrel{R} b$ también se cumple $b \mathrel{R} a$. Si es transitiva, si $a \mathrel{R} b$ y $b \mathrel{R} c$ entonces también $a \mathrel{R} c$. Puede darse el caso que algún elemento a no esté relacionado con ninguno, con lo que no se pueden encadenar estas propiedades. Por ejemplo, sobre cualquier conjunto U la relación $\emptyset$ es simétrica y transitiva, pero no reflexiva.

10. Clasifique las siguientes relaciones:

   a) Si $f(n) = \Theta(g(n))$, hay n_0 y constantes positivas c_1 y c_2 tales que para todo $n \geq n_0$ se cumple $c_1 g(n) \leq f(n) \leq c_2 g(n)$.

   Claramente esta relación es reflexiva (podemos tomar simplemente $c_1 = 1/2$, $c_2 = 2$).

   Además es simétrica, ya que podemos concluir que para $n \geq n_0$

   $$\frac{1}{c_2} f(n) \leq g(x) \leq \frac{1}{c_1} f(n)$$

   vale decir, $g(n) = \Theta(f(n))$.

   También es transitiva, ya que si $f(n) = \Theta(g(n))$ y además $g(n) = \Theta(h(n))$, existen constantes n_0' y c_1' y c_2' con $c_1' h(n) \leq g(n) \leq c_2' h(n)$ cuando $n \geq n_0'$. Si ahora tomamos $n \geq \max(n_0, n_0')$, resulta al combinar: $c_1 c_1' h(n) \leq f(n) \leq c_2 c_2' h(n)$. Esto corresponde a la definición de $f(n) = \Theta(g(n))$.

   Como la relación es reflexiva, simétrica y transitiva es una relación de equivalencia.

   De forma similar puede demostrarse que $f(n) = O(g(n))$ y $f(n) = \Omega(g(n))$ dan relaciones de orden. Si consideramos $f(n) = \Theta(g(n))$ como una "igualdad," $f(n) = O(g(n))$ corresponde a un "menor o igual," mientras $f(n) = \Omega(g(n))$ es un "mayor o igual."

   b) Si consideramos (x, y) y $u, v)$ como puntos en el plano, dos puntos están relacionados por R_2 si están a lo más a distancia 1 entre sí.

   Esta relación es reflexiva, y simétrica. No es transitiva, ya que por ejemplo $(0, 0)$ R_2 $(0, 1)$, y también $(0, 1)$ R_2 $(0, 2)$, pero $(0, 0)$ y $(0, 2)$ no están relacionados. No es antisimétrica, ya que por ejemplo $(0, 0)$ R_2 $(0, 1)$ y viceversa, pero no son iguales.

11. Ejemplos de tales funciones $f \colon \mathbb{N} \to \mathbb{N}$ son:

   a) f es uno a uno, pero no sobre: $f(n) = n^2$

   b) f es sobre, pero no uno a uno: $f(n) = \lfloor \frac{n+1}{2} \rfloor$

   c) f es biyectiva: $f(n) = n$

12. Si R es simétrica, quiere decir que siempre que $a \mathrel{R} b$ se cumple que $b \mathrel{R} a$. La transpuesta de R es simplemente la relación R^{-1} tal que $a \mathrel{R^{-1}} b$ si y sólo si $b \mathrel{R} a$. Por tanto, si R es simétrica, también lo es R^{-1}.

13. Si R_1 es transitiva, significa que siempre que $a \mathrel{R_1} b$ y $b \mathrel{R_1} c$ se cumple que $a \mathrel{R_1} c$. Ejemplos de relaciones transitivas son $<$ y $>$, pero nada cuerdo puede decirse de $< \circ >$. Por ejemplo, si tomamos a y b tales que $15 > a$ y $b < 15$, tenemos que $a < \circ > b$, pero no hay orden entre ellos.

14. Una función debe estar definida para todo elemento del dominio, y debe asignarle un único valor a cada uno de ellos. Si la función no es biyectiva, la transpuesta no es función. Si consideramos por ejemplo la función $f : \mathbb{R} \to \mathbb{R}$ tal que$y = x^2$, la transpuesta no asocia valores a y negativos, además que asigna los dos valores $\pm\sqrt{y}$ a un valor de y.

15. *a*) Primero, $f(n) = \Omega(g(n))$ significa que existen constantes $n_0 \in \mathbb{N}$ y $c \in \mathbb{R}$ con $c > 0$ tales que $f(n) \geq c \cdot g(n)$ si $n \geq n_0$

   Reflexiva: Claramente $f(n) = \Omega(f(n))$ (podemos tomar $n_0 = 1$, $c = 1$)

   Transitiva: Si $f(n) = \Omega(g(n))$, y $g(n) = \Omega(h(n))$, quiere decir que hay $n', n'' \in \mathbb{N}$ y $c', c'' \in \mathbb{R}$ con $c', c'' > 0$ tales que:

   $$\begin{aligned} f(n) &\geq c' \cdot g(n) && n \geq n' \\ g(n) &\geq c'' \cdot h(n) && n \geq n'' \end{aligned}$$

   Combinando ambas:

   $$f(n) \geq c'c'' \cdot h(n) \qquad n \geq \max(n', n'')$$

   Esto corresponde a la definición con $n_0 = \max(n', n'')$ y $c = c'c''$

Simétrica: No. Tenemos por ejemplo $n^2 = \Omega(n)$ (tomar $n_0 = 1$, $c = 1$ basta) pero no $n = \Omega(n^2)$ (para cualquier c, $c \cdot n^2 > n$ cuando $n > c$).

Antisimétrica: No. Por ejemplo, $5n = \Omega(3n)$ y $3n = \Omega(5n)$, pero estas funciones no son iguales.

b) Tenemos $x \mathrel{R_2} y$ cuando $x - y \in \mathbb{Z}$.

Reflexiva: Si, $x - x = 0 \in \mathbb{Z}$.

Transitiva: $x \mathrel{R_2} y$ y $y \mathrel{R_2} z$ significan $x - y \in \mathbb{Z}$ y $y - z \in \mathbb{Z}$, en cuyo caso $(x - y) + (y - z) = x - z \in \mathbb{Z}$, o sea $x \mathrel{R_2} z$.

Simétrica: Si $x - y \in \mathbb{Z}$, también $y - x \in \mathbb{Z}$, o sea si $x \mathrel{R_2} y$ entonces $y \mathrel{R_2} x$.

Antisimétrica: No. Por ejemplo $1 \mathrel{R_2} 3$ y $3 \mathrel{R_2} 1$, pero $1 \neq 3$.

Total: No. Por ejemplo, $1 \not\mathrel{R}_2 \sqrt{2}$ y $\sqrt{2} \not\mathrel{R}_2 1$.

16. Cada relación en turno.

$\mathcal{R}_1$**: Reflexiva:** Debiera ser $\sin x = \cos x$ para todo x, que no se cumple. Por ejemplo, para $x = 0$ tenemos $\sin 0 = 0$ mientras $\cos 0 = 1$.

Transitiva: Esto sería que si $\sin x = \cos y$ y $\sin y = \cos z$ entonces $\sin x = \cos z$. Para construir un contraejemplo, sabemos que $\cos x = \sin(\pi/2 + x)$. O sea, podemos elegir x, luego:

$$\begin{aligned} y &= \frac{\pi}{2} - x \\ z &= \frac{\pi}{2} - y = x \end{aligned}$$

Siempre que $\sin x \neq \cos x$ será un contraejemplo. Un ángulo "simple" es $x = \pi/3$, que da $y = \pi/6$ y $z = \pi/3$:

$$\begin{aligned} \cos x &= \cos \frac{\pi}{3} = \frac{1}{2} \\ \sin y &= \sin \frac{\pi}{6} = \frac{1}{2} \\ \cos y &= \cos \frac{\pi}{6} = \frac{\sqrt{3}}{2} \\ \sin z &= \sin \frac{\pi}{3} = \frac{\sqrt{3}}{2} \\ \cos x &\neq \sin z \end{aligned}$$

Simétrica: Para que se cumpla esta propiedad, debe ser que $\cos x = \sin y$ siempre que $\cos y = \sin x$. Pero $\cos x = \sin y$ siempre que $y = \pi/2 \pm x + 2n\pi$

$\mathcal{R}_2$**:** Por completar

$\mathcal{R}_3$**:** Por completar

17. Para que f sea una inyección, debe ser que si $a \neq b$ es $f(a) \neq f(b)$, cosa que claramente se cumple.

    Si es sobreyectiva, para todo $\mathcal{A} \subseteq \mathbb{N}$ hay $x \in \mathbb{N}$ tal que $f(x) = \mathcal{A}$. Pero ninguno de los conjuntos $f(n)$ incluye 1, con lo que en particular no hay $x \in \mathbb{N}$ tal que $f(x) = \mathbb{N}$. No es sobreyectiva.

18. Para determinar si es relación de equivalencia, debemos considerar:

Reflexividad: Debe ser $(x, y) \sim (x, y)$ para todo $(x, y) \in \mathbb{R}^2$.
Siempre tenemos $x^2 - y^2 = x^2 - y^2$, o sea $(x, y) \sim (x, y)$. Es reflexiva.

Simetría: Para todo (r, s) y (x, y), si $(r, s) \sim (x, y)$ entonces $(x, y) \sim (r, s)$.
Si $(r, s) \sim (x, y)$ entonces $r^2 - y^2 = x^2 - s^2$, que es $x^2 - s^2 = r^2 - y^2$, o sea $(x, y) \sim (r, s)$. Es simétrica.

Transitividad: Para todo (r, s), (u, v) y (x, y) en $\mathbb{R}^2$ tenemos que si $(r, s) \sim (u, v)$ y $(u, v) \sim (x, y)$ entonces $(r, s) \sim (x, y)$.

De la definición de $(r,s) \sim (x,y)$ vemos que:

$$r^2 - y^2 = x^2 - s^2$$
$$r^2 + s^2 = x^2 + y^2$$

Por tanto, $(r,s) \sim (u,v)$ significa que $r^2 + s^2 = u^2 + v^2$, $(u,v) \sim (x,y)$ significa que $u^2 + v^2 = x^2 + y^2$. Concluimos que $r^2 + s^2 = x^2 + y^2$, o sea $r^2 - y^2 = x^2 - s^2$, vale decir, $(r,s) \sim (x,y)$. Es transitiva.

Como $\sim$ cumple las tres propiedades, es una relación de equivalencia.

19. Para demostrar que f es uno a uno debemos demostrar que si $f(a) = f(b)$ entonces $a = b$. Consideremos:

$$\begin{aligned} f(a) - f(b) &= (a^3 + 2a^2 + 3a + 4) - (b^3 + 2b^2 + 3b + 4) \\ &= (a^3 - b^3) + 2(a^2 - b^2) + 3(a - b) \\ &= (a - b)(a^2 + ab + b^2 + 2a + 2b + 3) \end{aligned}$$

Debemos demostrar que el segundo factor no se anula si $a \in \mathbb{R}$, o sea, ambos ceros son complejos. Escribimos:

$$a^2 + (b+2)a + (b^2 + 2b) = 0$$

El discriminante de esta cuadrática en a es:

$$\begin{aligned} (b+2)^2 - 4(b^2 + 2b + 3) &= b^2 + 4b + 4 - 4b^2 - 8b - 12 \\ &= -(3b^2 + 4b + 8) \end{aligned}$$

Para el máximo de esta última expresión derivamos respecto de b:

$$6b + 4 = 0$$

Resulta que $b^* = -2/3$ es punto crítico, donde es:

$$\begin{aligned} 3 \cdot \left(\frac{-2}{3}\right)^2 + 4 \cdot \left(\frac{-2}{3}\right) + 8 &= \frac{4}{3} - \frac{8}{3} + 8 \\ &= \frac{4 - 8 + 24}{3} \\ &= \frac{20}{3} \\ &> 0 \end{aligned}$$

El discriminante es siempre negativo, no hay ceros reales.

Otra manera es determinar que $f(x)$ es escrictamente creciente, vale decir, que su derivada es siempre mayor a cero:

$$\begin{aligned} f'(x) &= 3x^2 + 4x + 3 \\ f''(x) &= 6x + 4 \\ f'''(x) &= 6 \end{aligned}$$

Vemos que $f'(x)$ es convexa, tiene un mínimo. El punto crítico es $x^* = -2/3$, donde:

$$\begin{aligned} f'(x^*) &= 3 \cdot \left(\frac{-2}{3}\right)^2 + 4 \cdot \left(\frac{-2}{3}\right) + 3 \\ &= \frac{3 \cdot 4}{9} - \frac{4 \cdot 2}{3} + 3 \\ &= \frac{4 - 8 + 9}{3} \\ &= \frac{5}{3} \\ &> 0 \end{aligned}$$

Nuevamente, $f(x)$ es estrictamente creciente, y por tanto es inyectiva.

Más fácil: $f(x)$ es la suma de términos crecientes, con lo que es creciente y por tanto inyectiva.

3. Lógica

1. Es $\neg Q \Rightarrow \neg P$
2. En términos de los predicados dados:

   a) Usemos J por Juan, y F por Fundamentos. Entonces

   $$\exists p.(D(p,\mathrm{F}) \wedge C(\mathrm{J},\mathrm{F}) \wedge E(\mathrm{J},\mathrm{F})) \Rightarrow A(\mathrm{J},\mathrm{F})$$

   Esto exige que haya un profesor p dictando el ramo (o sea, el ramo se dicta).

   b) $\forall a \forall p \forall r.(D(p,r) \wedge C(a,r) \wedge R(p)) \Rightarrow \neg A(a,r)$

   c) $\forall p \forall r \forall a.(R(p) \wedge D(p,r) \wedge C(a,r) \wedge \neg R(a)) \Rightarrow A(a,r)$

3. *a*) Esto es decir que es falso que hay un profesor muy carretero que dicta dos o más ramos. Sea p el profesor, y x e y dos ramos. Entonces:

   $$\neg\left(\exists p,x,y.(R(p) \wedge x \neq y \wedge D(p,x) \wedge D(p,y))\right)$$

   b) Esto es un poco más directo. Sea a un alumno, x algún ramo que toma. Entonces:

   $$\exists a.\left(R(a) \wedge (\forall x.(C(a,x) \Rightarrow A(a,x)))\right)$$

   c) Sea p el profesor, x sus ramos y a los alumnos. Implícitamente estamos diciendo que se cumple para todo profesor:

   $$\forall p,x,a.\left(\neg R(p) \wedge D(p,x) \wedge C(a,x) \wedge (E(a,x) \Rightarrow A(a,x))\right)$$

4. *a*) $\neg L \Rightarrow Q$

   b) $\neg L \Rightarrow B$

   c) $\neg L \Leftrightarrow N$

   d) $\neg Q \Rightarrow B$

   e) $\neg B$

5. **Caso 1:** B es Verdadero.
   En este caso, se obtiene que la especificación (5) del problema anterior sea Falsa y, por lo tanto, toda la demás especificación completa sea Falsa.

   Caso 2: B es Falso.
   En este caso, (2) y (4) serán verdaderas sólo si Q y L son verdaderas. Como L es verdadero, (3) puede ser verdadero sólo si N es falsa.

   En resumen, hemos deducido que para lograr la consistencia del sistema, en las especificaciones debemos tener lo siguiente:

   - L = Verdadero
   - N = Falso
   - Q = Verdadero
   - B = Falso

   Y es la única asignación que satisface la consistencia.

4. Demostraciones

1. Por contradicción, siguiendo la pista. Supongamos que $\sin\theta + \cos\theta < 1$ para algún $0 \leq \theta \leq \pi/2$. Entonces:

$$\begin{aligned}
\sin\theta + \cos\theta &< 1 \\
(\sin\theta + \cos\theta)^2 &< 1 \\
\sin^2\theta + 2\sin\theta\cos\theta + \cos^2\theta &< 1
\end{aligned}$$

   Como $\sin^2\theta + \cos^2\theta = 1$:

$$2\sin\theta\cos\theta < 0$$

   Pero en el rango indicado $\sin\theta \geq 0$ y $\cos\theta \geq 0$, la última relación es imposible. En consecuencia $\sin\theta + \cos\theta \geq 1$.

   (Una manera más simple de verlo es que $\sin\theta$ y $\cos\theta$ son los catetos de un triángulo de hipotenusa 1, por la desigualdad triangular sigue lo indicado).

2. La demostración es por contradicción. Supongamos que $\log_2 5$ es racional, vale decir hay enteros a y b, con $b \neq 0$, tales que:

$$\begin{aligned}
\log_2 5 &= \frac{a}{b} \\
2^{a/b} &= 5 \\
2^a &= 5^b
\end{aligned}$$

   Esto es absurdo, el lado izquierdo es par (salvo si $a = 0$, pero $\log_2 5 \neq 0$), mientras el derecho siempre es impar.

3. Demostramos el contrapositivo: Si n es un cuadrado perfecto, entonces $n \bmod 4 \neq 2$ y $n \bmod 4 \neq 3$. Sea $n = a^2$, debemos considerar los casos:

   ***a* es par:** En este caso $a = 2u$, $a^2 = 4u^2$ y $n \bmod 4 = 0$. Se cumple.

   ***a* es impar:** En este caso $a = 2u + 1$, $a^2 = 4u^2 + 4u + 1$, y $n \bmod 4 = 1$. También se cumple.

   Como se cumple en todos los casos, siempre se cumple.

4. Bastante directo.

   Base: Para $n = 1$ la expresión es:

$$\frac{2!}{1! \cdot 2^1} = 1$$

   que es impar.

   Inducción: Calculemos para $n + 1$:

$$\begin{aligned}
\frac{(2n+2)!}{(n+1)!2^{n+1}} &= \frac{(2n)!(2n+1)(2n+2)}{n!2^n \cdot 2(n+1)} \\
&= \frac{(2n)!}{n!2^n} \cdot \frac{(2n+1)(2n+2)}{2(n+1)} \\
&= \frac{(2n)!}{n!2^n} \cdot (2n+1)
\end{aligned}$$

   Por la hipótesis de inducción, el primer factor es impar, el segundo es impar. Luego el producto es impar.

5. Usamos inducción sobre n.

   Base: Cuando $n = 2$, ambos lados se reducen a $3/2$.

Inducción: Para $n \geq 2$, supongamos:

$$\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{3}\right)\cdots\left(1 + \frac{1}{n}\right) = \frac{n+1}{2}$$

Entonces:

$$\begin{aligned}\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{3}\right)\cdots\left(1 + \frac{1}{n}\right)\left(1 + \frac{1}{n+1}\right) &= \frac{n+1}{2}\cdot\left(1 + \frac{1}{n+1}\right)\\ &= \frac{n+1}{2}\cdot\frac{n+2}{n+1}\\ &= \frac{n+2}{2}\end{aligned}$$

Por inducción vale para $n \geq 2$.

6. Usamos inducción fuerte sobre n.

   Base: Si tiene 1 caja, no hay movidas posibles. Su puntaje es 0, que coincide con la fórmula.
   Si tiene 2 cajas, la única movida es a dos torres de 1, que da puntaje 1. Nuevamente coincide con la fórmula.

   Inducción: Supongamos que para todo $k < n$ el puntaje siempre es $k(k-1)/2$. Entonces al dividir una torre de tamaño n en torres de tamaños k y $n-k$ obtenemos:

$$\frac{k(k-1)}{2} + \frac{(n-k)(n-k-1)}{2} = \frac{n(n-1)}{2}$$

   Por inducción fuerte, se cumple lo anunciado.

7. Usamos inducción.

   Base: Para $n = 1$ se reduce a:

$$(-1)^1 \cdot 1^2 = \frac{(-1)^1 \cdot 1 \cdot 2}{2}$$

   que claramente se cumple.

   Inducción: Tenemos:

$$\sum_{1 \leq k \leq n+1} (-1)^k k^2 = \sum_{1 \leq k \leq n} (-1)^k k^2 + (-1)^{n+1}(n+1)^2$$

   Por la hipótesis de inducción:

$$\begin{aligned}&= \frac{(-1)^n n(n+1)}{2} + (-1)^{n+1}(n+1)^2\\ &= (-1)^n \frac{n(n+1) - 2(n+1)^2}{2}\\ &= (-1)^n \frac{(n+1)(n-2n-2)}{2}\\ &= (-1)^{n+1}\frac{(n+1)(n+2)}{2}\end{aligned}$$

   Esto es la relación para $n+1$.

   Por inducción, vale para todo $n \geq 1$.

8. Usamos inducción, partiendo con $n = 2$.

Base: Para $n = 2$ es:

$$1 - \frac{1}{2^2} = \frac{2+1}{2 \cdot 2}$$

Se cumple el caso $n = 2$.

Inducción: Para $n + 1$ tenemos:

$$\prod_{2 \leq k \leq n+1} \left(1 - \frac{1}{k^2}\right) = \prod_{2 \leq k \leq n} \left(1 - \frac{1}{k^2}\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right)$$

Por la hipótesis de inducción:

$$\begin{aligned}
&= \frac{n+1}{2n} \cdot \frac{(n+1)^2 - 1}{(n+1)^2} \\
&= \frac{(n+1)^2 - 1}{2n(n+1)} \\
&= \frac{(n+2)n}{2n(n+1)} \\
&= \frac{(n+1)+1}{2(n+1)}
\end{aligned}$$

Obtenemos el caso siguiente.

Por inducción, vale para todo $n \geq 2$.

9. Usamos inducción sobre n. También requeriremos las identidades trigonométricas:

$$\begin{aligned}
\sin(\alpha + \beta) &= \sin\alpha\cos\beta + \sin\beta\cos\alpha \\
\cos(\alpha + \beta) &= \cos\alpha\cos\beta - \sin\alpha\sin\beta
\end{aligned}$$

Base: Para $n = 1$, la identidad es evidente.

Inducción: Suponiendo que vale para n, calculamos la potencia $n + 1$:

$$\begin{aligned}
(\cos\theta + \mathrm{i}\sin\beta)^{n+1} &= (\cos\theta + \mathrm{i}\sin\beta)^n \cdot (\cos\theta + \mathrm{i}\sin\beta) \\
&= (\cos n\theta + \mathrm{i}\sin n\theta) \cdot (\cos\theta + \mathrm{i}\sin\beta) \\
&= (\cos n\theta\cos\theta - \sin n\theta\sin\theta) + \mathrm{i}(\cos n\theta\sin\theta + \sin n\theta\cos\theta) \\
&= \cos(n+1)\theta + \mathrm{i}\sin(n+1)\theta
\end{aligned}$$

Exactamente el caso $n + 1$.

Por inducción vale para $n \in \mathbb{N}$.

10. **Base:** Para $n = 1$, se reduce a:

$$\frac{1}{1(1+1)} = \frac{1}{1+1}$$

lo que es cierto.

Inducción: Suponiendo que vale para n, veamos el caso siguiente:

$$\begin{aligned}
\sum_{1 \leq k \leq n+1} \frac{1}{k(k+1)} &= \sum_{1 \leq k \leq n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n(n+2)+1}{(n+1)(n+2)} \\
&= \frac{n^2 + 2n + 1}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2}
\end{aligned}$$

que es exactamente la relación para $n+1$.

Por inducción vale para $n \in \mathbb{N}$.

11. Usamos inducción sobre n.

Base: Para $n = 0$, queda $0 \cdot 0! = 1! - 1$, que es cierto.

Inducción: Suponemos que vale para n, y vemos el caso $n+1$:

$$\begin{aligned}
\sum_{0 \leq k \leq n+1} k \cdot k! &= \sum_{0 \leq k \leq n} k \cdot k! + (n+1) \cdot (n+1)! \\
&= ((n+1)! - 1) + (n+1) \cdot (n+1)! \\
&= (n+1)! \cdot (1 + n + 1) - 1 \\
&= (n+2)! - 1
\end{aligned}$$

que es exactamente el caso $n+1$.

Por inducción, vale para todo $n \in \mathbb{N}_0$.

12. Usamos el esquema clásico de inducción sobre n.

Base: Para $n = 1$ queda:

$$(1+x)^1 \geq 1 + 1 \cdot x$$

que ciertamente es verdad.

Inducción: Suponiendo que vale para n, demostramos que vale para $n+1$:

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n \cdot (1+x) \\
&\geq (1+nx)(1+x) \\
&= 1 + (n+1)x + nx^2 \\
&\geq 1 + (n+1)x
\end{aligned}$$

Por inducción, vale para todo $n \in \mathbb{N}$.

13. Por inducción sobre n.

Base: Para $n = 2$ tenemos:

$$\begin{aligned}
4^2 &= 16 \\
3^2 + 2^2 &= 9 + 4 = 13
\end{aligned}$$

Se cumple.

Inducción: Consideremos:

$$\begin{aligned}
4^{n+1} &= 4 \cdot 4^n \\
&> 4 \cdot 3^n + 4 \cdot 2^n \\
&> 3 \cdot 3^n + 2 \cdot 2^n \\
&= 3^{n+1} + 2^{n+1}
\end{aligned}$$

Por inducción vale para $n \geq 2$.

14. La demostración es por inducción fuerte sobre n. Eso sí, requerimos tres casos base.

Bases: Para los tres primeros valores tenemos:

$$\begin{aligned}
T_0 &= 0 \leq 2^0 = 1 \\
T_1 &= 1 \leq 2^1 = 2 \\
T_2 &= 1 \leq 2^2 = 4
\end{aligned}$$

Las tres se cumplen.

Inducción: Suponiendo que lo aseverado vale para $0 \leq k \leq n-1$, analizamos el caso n donde $n \geq 3$:

$$\begin{aligned}
T_n &= T_{n-1} + T_{n-2} + T_{n-3} \\
&\leq 2^{n-1} + 2^{n-2} + 2^{n-3} \\
&\leq 2^{n-1} + 2^{n-2} + 2^{n-2} \\
&\leq 2^{n-1} + 2^{n-1} \\
&= 2^n
\end{aligned}$$

Por inducción fuerte vale para $n \in \mathbb{N}_0$.

15. Bastante directo.

Base: Para $n = 1$ la expresión es:

$$\frac{2!}{1! \cdot 2^1} = 1$$

que es impar.

Inducción: Calculemos para $n + 1$:

$$\begin{aligned}
\frac{(2n+2)!}{(n+1)!2^{n+1}} &= \frac{(2n)!(2n+1)(2n+2)}{n!2^n \cdot 2(n+1)} \\
&= \frac{(2n)!}{n!2^n} \cdot \frac{(2n+1)(2n+2)}{2(n+1)} \\
&= \frac{(2n)!}{n!2^n} \cdot (2n+1)
\end{aligned}$$

Por la hipótesis de inducción, el primer factor es impar, el segundo es impar. Luego el producto es impar.

16. El contrapositivo es que si n es un cuadrado perfecto, entonces $n \not\equiv 2 \pmod 3$. Sea $n = a^2$. Consideremos las posibilidades de a módulo 3:

$a \equiv 0$: En este caso $a^2 \equiv 0 \not\equiv 2 \pmod 3$. Se cumple.

$a \equiv 1$: En este caso $a^2 \equiv 1 \not\equiv 2 \pmod 3$. Se cumple.

$a \equiv 2$: En este caso $a^2 \equiv 1 \not\equiv 2 \pmod 3$. Se cumple.

Se cumple en todos los casos.

Alternativamente, podríamos decir que si $a \equiv 0$ entonces $a^2 \equiv 0$, y que si $a \equiv \pm 1$ entonces $a^2 \equiv 1$.

17. Supongamos que $\sin x + \cos x < 1$ en el rango indicado, con lo que su cuadrado es menor que 1. Pero:

$$\begin{aligned}
(\sin x + \cos x)^2 &= \sin^2 x + 2 \sin x \cos x + \cos^2 x \\
&= 1 + 2 \sin x \cos x
\end{aligned}$$

En el rango indicado $\sin x$ y $\cos x$ no son negativos, y el cuadrado es mayor o igual a cero.

18. Lo demostramos por inducción.

Base: Cuando $n = 1$, queda:

$$5^2 - 1 = 24$$

que ciertamente es divisible por 24.

Inducción: Supongamos que vale para $n = k$, veamos el caso $n = k + 1$. Por la hipótesis de inducción, hay $c \in \mathbb{Z}$ tal que:

$$5^{2k} - 1 = 24c$$

$$
\begin{aligned}
5^{2(k+1)} - 1 &= 5^2 \cdot \left(5^{2k} - 1\right) + 5^2 - 1 \\
&= 5^2 \cdot 24c + 24 \\
&= 24 \cdot (5^2 c + 1)
\end{aligned}
$$

y $24 \mid 5^{2(k+1)} - 1$.

Por inducción, vale para todo $n \in \mathbb{N}$.

19. Los primeros n números impares son 1, 3, ..., $2n - 1$. Se asevera entonces que:

$$
\sum_{1 \le k \le n} (2k - 1) = n^2
$$

La demostración es por inducción.

Base: Cuando $n = 1$, queda simplemente $1 = 1^2$.

Inducción: Suponiendo que vale para n, demostramos que vale para $n + 1$. En detalle:

$$
\begin{aligned}
\sum_{1 \le k \le n} (2k - 1) &= n^2 \\
\sum_{1 \le k \le n+1} (2k - 1) &= \sum_{1 \le k \le n} (2k - 1) + (2(n + 1) - 1) \\
&= n^2 + 2n + 1 \\
&= (n + 1)^2
\end{aligned}
$$

Por inducción vale para todo $n \in \mathbb{N}$.

20. Podemos partir de

$$
\sum_{1 \le k \le n} k = \frac{n(n + 1)}{2}
$$

que por linealidad hace sospechar:

$$
\sum_{1 \le k \le n} ak + b = a\frac{n(n + 1)}{2} + bn = \frac{(an + a + 2b)n}{2}
$$

Vamos a la inducción con esto.

Base: Cuando $n = 1$ queda

$$
a + b = \frac{1 \cdot (a \cdot 1 + a + 2b)}{2}
$$

lo que es correcto.

Inducción: Suponemos:

$$
\sum_{1 \le k \le n} ak + b = \frac{(an + a + 2b)n}{2}
$$

Con esto:

$$
\begin{aligned}
\sum_{1 \le k \le n+1} ak + b &= \sum_{1 \le k \le n} (ak + b) + (a(n + 1) + b) \\
&= \frac{(an + a + 2b)n}{2} + an + a + b \\
&= \frac{an^2 + (3a + 2b)n + 2a + 2b}{2}
\end{aligned}
$$

Factorizamos:

$$\begin{aligned} an^2 + (3a + 2b)n + 2a + 2b &= (an + 2a + 2b)(n + 1) \\ &= (a(n + 1) + a + 2b)(n + 1) \end{aligned}$$

O sea, se cumple para $n + 1$.

Por inducción, es válido para todo $n \in \mathbb{N}$.

21. La demostración es por inducción sobre n.

Base: Cuando $n = 1$, la suma del lado izquierdo es

$$1^{\overline{m}} = m!$$

y el lado derecho es

$$\frac{1^{\overline{m+1}}}{m + 1} = \frac{(m + 1)!}{m + 1} = m!$$

Lo indicado se cumple para todo $m \in \mathbb{N}$.

Inducción: Por la hipótesis de inducción tenemos

$$\sum_{1 \le k \le n} k^{\overline{m}} = \frac{n^{\overline{m+1}}}{m + 1}$$

Tenemos entonces:

$$\begin{aligned} \sum_{1 \le k \le n+1} k^{\overline{m}} &= \sum_{1 \le k \le n} k^{\overline{m}} + (n + 1)^{\overline{m}} \\ &= \frac{n^{\overline{m+1}}}{m + 1} + (n + 1)^{\overline{m}} \\ &= \frac{n(n + 1)^{\overline{m}}}{m + 1} + (n + 1)^{\overline{m}} \\ &= \frac{(n + m + 1) \cdot (n + 1)^{\overline{m}}}{m + 1} \\ &= \frac{(n + 1)^{\overline{m+1}}}{m + 1} \end{aligned}$$

que es precisamente el caso siguiente, y vale para todo $m \in \mathbb{N}$.

Por inducción, vale para todo $n \in \mathbb{N}$, y por la derivación para todo $m \in \mathbb{N}$.

22. La demostración es por inducción.

Base: Cuando $n = 1$, se reduce a $1 = 1$, que claramente es cierto.

Inducción: Supongamos que la aseveración es cierta para n, vale decir:

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$

y queremos demostrar para el caso siguiente, $n + 1$. Tenemos:

$$\begin{aligned} ((1 + 2 + \ldots + n) + (n + 1))^2 &= (1 + 2 + \ldots + n)^2 + 2(1 + 2 + \ldots + n)(n + 1) + (n + 1)^2 \\ &= \left(1^3 + 2^3 + \ldots + n^3\right) + n(n + 1)^2 + (n + 1)^2 \\ &= 1^3 + 2^3 + \ldots + n^3 + (n + 1)^3 \end{aligned}$$

Esto es lo pedido.

23. Por inducción sobre n.

    Base: Cuando $n = 1$, se reduce a:

    $$1 \cdot 2 = \frac{1 \cdot 2 \cdot 3}{3}$$

    lo que ciertamente es verdadero.

    Inducción: Suponiendo que es cierto para n, demostramos que es cierto para $n+1$. O sea, suponemos:

    $$\sum_{1 \leq k \leq n} k(k+1) = \frac{n(n+1)(n+2)}{3}$$

    Si sumamos $(n+1)(n+2)$ a ambos lados de esta igualdad:

    $$\begin{aligned} \sum_{1 \leq k \leq n} k(k+1) + (n+1)(n+2) &= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\ \sum_{1 \leq k \leq n+1} k(k+1) &= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} \\ &= \frac{(n+1)(n+2)(n+3)}{3} \end{aligned}$$

    que es exactamente lo que se quería demostrar.

    De exactamente la misma forma puede demostrarse que

    $$\sum_{1 \leq k \leq n} k^{\overline{m}} = \frac{n^{\overline{m+1}}}{m+1}$$

    Compárese esto con

    $$\int_0^x x^m dx = \frac{x^{m+1}}{m+1}$$

24. Por inducción sobre n.

    Base: Para $n = 0$ se reduce a:

    $$F_0^2 = F_0 F_1$$

    que claramente se cumple.

    Inducción: Suponemos que vale para n, y vemos el caso $n+1$:

    $$\begin{aligned} \sum_{0 \leq k \leq n+1} F_k^2 &= \sum_{0 \leq k \leq n} F_k^2 + F_{n+1}^2 \\ &= F_n F_{n+1} + F_{n+1}^2 \\ &= F_{n+1}(F_n + F_{n+1}) \\ &= F_{n+1} F_{n+2} \end{aligned}$$

25. Por inducción.

    Base: Para $n = 1$ se reduce a la identidad:

    $$\frac{1}{1 \cdot 3} = \frac{1}{3}$$

    Se cumple.

Inducción: Suponiendo que vale para n, consideremos:

$$\begin{aligned}
\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}+\frac{1}{(2n+1)(2n+3)} &= \frac{n}{2n+1}+\frac{1}{(2n+1)(2n+3)} \\
&= \frac{n(2n+3)+1}{(2n+1)(2n+3)} \\
&= \frac{n+1}{2n+3}
\end{aligned}$$

Exactamente el caso siguiente.

26. Por contradicción. Supongamos $\sqrt{10}$ racional, entonces podemos escribir para números naturales a y b con $\gcd(a,b)=1$:

$$\begin{aligned}
\sqrt{10} &= \frac{a}{b} \\
a^2 &= 10\cdot b^2
\end{aligned}$$

Entonces tenemos que $2 \mid a^2$, ya que $2 \mid 10$. Pero como 2 es primo, debe ser $2 \mid a$, digamos $a = 2c$. Con esto queda:

$$\begin{aligned}
(2c)^2 &= 10b^2 \\
2c^2 &= 5b^2
\end{aligned}$$

De forma similar, $2 \mid b^2$ y por tanto $2 \mid b$. Pero de ser así, 2 es factor común de a y b, que habíamos supuesto *no* tienen factores comunes.

Otra alternativa es tomar $a^2 = 2\cdot 5\cdot b^2$ y considerar sus descomposiciones en primos. Al lado izquierdo 2 aparece con una potencia par, al lado derecho aparece con una potencia impar. Por el teorema fundamental de la aritmética, esto es imposible.

27. Las raíces de la ecuación son

$$\frac{1\pm\sqrt{5}}{2}$$

La raíz positiva es

$$\varphi = \frac{1+\sqrt{5}}{2}$$

Demostramos que φ es irracional por contradicción. Supongamos que φ es racional, entonces es racional $2\varphi - 1 = \sqrt{5}$. O sea, es

$$\begin{aligned}
\sqrt{5} &= \frac{a}{b} \\
5 &= \frac{a^2}{b^2} \\
a^2 &= 5b^2
\end{aligned}$$

Por el teorema fundamental de la aritmética esto es imposible (en el lado izquierdo la potencia de 5 es par, en el izquierdo es impar).

Otra forma es recordar que si tenemos un polinomio $a_n x^n + \ldots + a_0$ con coeficientes enteros, donde a_n y a_0 son diferentes de cero los ceros racionales $r = u/v$ en mínimos términos cumplen $u \mid a_0$ y $v \mid a_n$. En este caso ($a_n = 1$ y $a_0 = -1$) sólo son posibles $u = \pm 1$ y $v = \pm 1$, con lo que las únicas opciones son ± 1, ninguna de las cuales es raíz. Todas las raíces de $x^2 - x - 1$ son irracionales, incluyendo la positiva.

28. Para demostrar que $\sqrt[3]{2}$ es irracional, usamos la misma idea que en su oportunidad para demostrar que $\sqrt{2}$ es irracional. Supongamos que $\sqrt[3]{2}$ es racional, entonces existen enteros a y b tales que:

$$\begin{aligned} \sqrt[3]{2} &= \frac{a}{b} \\ 2 &= \frac{a^3}{b^3} \\ 2b^3 &= a^3 \end{aligned}$$

Si analizamos las factorizaciones en primos de ambos lados de la última relación, al lado izquierdo 2 aparece con una potencia congruente a 1 módulo 3, mientras al lado derecho es congruente con 0. Esto es imposible, luego $\sqrt[3]{2}$ es irracional.

Suponiendo ahora que podemos escribir:

$$\begin{aligned} x^3 - 2 &= (a_2 x^2 + a_1 x + a_0)(b_1 x + b_0) \\ &= a_2 b_1 x^3 + (a_2 b_0 + a_1 b_1) x^2 + (a_1 b_0 + a_0 b_1) x + a_0 b_0 \end{aligned}$$

Comparando coeficientes:

$$\begin{aligned} 1 &= a_2 b_1 \\ 0 &= a_2 b_0 + a_1 b_1 \\ 0 &= a_1 b_0 + a_0 b_1 \\ -2 &= a_0 b_0 \end{aligned}$$

De la primera relación tenemos que $a_2 = b_1 = \pm 1$, y la última demuestra que $a_0 \neq 0$ y que $b_0 \neq 0$. Podemos fijar sin pérdida de generalidad que $a_2 = b_1 = 1$. Entonces las demás se reducen a:

$$\begin{aligned} 0 &= b_0 + a_1 \\ b_0 &= -a_1 \end{aligned}$$

En particular, $a_1 \neq 0$. Siguiendo:

$$\begin{aligned} 0 &= a_1^2 + a_0 a_1 \\ &= a_1 + a_0 \\ a_0 &= -a_1 \end{aligned}$$

Obtenemos también:

$$\begin{aligned} -2 &= a_0 b_0 \\ -2 &= a_1^2 \end{aligned}$$

Pero esto es imposible con a_1 entero.

29. La demostración es por contradicción. Si $\sqrt{2} + \sqrt{3}$ fuera racional, lo sería su cuadrado. Pero:

$$\left(\sqrt{2} + \sqrt{3}\right)^2 = 5 + 2\sqrt{6}$$

Si esto es racional, lo es $\sqrt{6}$. Supongamos entonces que $\sqrt{6}$ es racional, vale decir hay $a, b \in \mathbb{N}$ tales que

$$\sqrt{6} = \frac{a}{b}$$

Pero entonces

$$a^2 = 6b^2$$

Si consideramos la factorización de ambos lados de esta ecuación, al lado izquierdo el primo 2 aparece con potencia par, mientras al lado izquierdo aparece con potencia impar. Esto es imposible, y esta contradicción demuestra lo aseverado.

30. La manera obvia de demostrar esto es por inducción.

    Base: Cuando $n = 1$, ciertamente se cumple (ambos lados de la igualdad se reducen a 1).

    Inducción: Suponiendo que la identidad vale para n, debemos demostrar que vale para $n + 1$.

    Suponemos entonces que

$$\sum_{1 \leq k \leq n} k^3 = \left(\sum_{1 \leq k \leq n} k \right)^2$$

    Si consideramos el valor siguiente de n:

$$\begin{aligned}
\left(\sum_{1 \leq k \leq n+1} k \right)^2 &= \left(\sum_{1 \leq k \leq n} k + (n+1) \right)^2 \\
&= \left(\sum_{1 \leq k \leq n} k \right)^2 + 2 \cdot (n+1) \cdot \left(\sum_{1 \leq k \leq n} k \right) + (n+1)^2 \\
&= \sum_{1 \leq k \leq n} k^3 + 2 \cdot (n+1) \cdot \frac{n(n+1)}{2} + (n+1)^2 \\
&= \sum_{1 \leq k \leq n} k^3 + n(n+1)^2 + (n+1)^2 \\
&= \sum_{1 \leq k \leq n} k^3 + (n+1)^3 \\
&= \sum_{1 \leq k \leq n+1} k^3
\end{aligned}$$

    Acá usamos

$$\sum_{1 \leq k \leq n} k = \frac{n(n+1)}{2}$$

    Por inducción, la equivalencia es válida para todo $n \in \mathbb{N}$

31. Procedemos por contradicción. Supongamos que existen números naturales a y b tales que $a^2 - b^2 = 1$, y $a > b$. Podemos factorizar:

$$\begin{aligned}
a^2 - b^2 &= (a+b)(a-b) \\
&= 1
\end{aligned}$$

    Entonces $a - b \mid 1$. Por el otro lado, también $a + b \mid 1$, con lo que $a + b = 1$. Esto nos da el sistema:

$$\begin{aligned}
a + b &= 1 \\
a - b &= 1
\end{aligned}$$

    La solución es $a = 1$, $b = 0$, y $b \notin \mathbb{N}$. O sea, hemos demostrado lo pedido.

32. La manera obvia de demostrar esto es por inducción.

    Base: Cuando $n = 1$, ciertamente se cumple (ambos lados de la igualdad se reducen a 1).

    Inducción: Suponiendo que la identidad vale para n, debemos demostrar que vale para $n + 1$.

    Suponemos entonces que

$$\sum_{1 \leq k \leq n} 2k - 1 = n^2$$

Si consideramos el valor siguiente de n:

$$\begin{aligned}
\sum_{1\le k\le n+1} 2k-1 &= 2n+1+\sum_{1\le k\le n} 2k-1 \\
&= n^2+2n+1 \\
&= (n+1)^2
\end{aligned}$$

como queríamos demostrar.

Por inducción, la equivalencia es válida para todo $n \in \mathbb{N}$

33. Sabemos que $k^{\underline{2}} = k(k-1)$, y que $k^{\underline{3}} = k(k-1)(k-2)$. Nuestra demostración es por inducción.

    Base: Cuando $n = 1$, la suma es simplemente 0, así como el lado derecho. Se cumple.

    Inducción: Supongamos que la fórmula vale para n, queremos demostrar que vale para $n+1$:

$$\begin{aligned}
\sum_{1\le k\le n} k^{\underline{2}} &= \frac{(n+1)^{\underline{3}}}{3} \\
\sum_{1\le k\le n+1} k^{\underline{2}} &= \sum_{1\le k\le n} k^{\underline{2}} + (n+1)n \\
&= \frac{(n+1)n(n-1)}{3} + \frac{3(n+1)n}{3} \\
&= \frac{(n+1)n(n-1+3)}{3} \\
&= \frac{(n+2)(n+1)n}{3}
\end{aligned}$$

    Esta es exactamente la fórmula supuesta para $n+1$.

    Por inducción, la fórmula vale para todo $n \in \mathbb{N}$.

34. **Base:** Para $n = 13$ se tiene que

$$13^2 = 169 < 194 < \frac{1594323}{8192} = \left(\frac{3}{2}\right)^{13}$$

    Esto es verdadero.

    Inducción: Ahora suponemos $n > 13$ y $n^2 < (3/2)^n$. Entonces:

$$(n+1)^2 = \left(1+\frac{1}{n}\right)^2 < \left(1+\frac{1}{13}\right)^2 n^2 = \frac{196}{169}n^2 < \frac{3}{2}n^2$$

35. **Base:** Para $n = 1$, se tiene $1 + x \geq 1 + x$, lo que se cumple.

    Inducción: Supongamos que $x \geq 0$, $k \in \mathbb{N}$ y $(1+x)^k \geq 1 + x^k$. Entonces:

$$\begin{aligned}
(1+x)^{k+1} &= (1+x)^k(1+x) \\
&= 1 + x^k + x + x^{k+1} \\
&\geq 1 + x^{k+1}
\end{aligned}$$

    que era lo que debía demostrarse.

36. Por partes.

a) Multiplicando el lado derecho tenemos:

$$2(n+2-(n+1))=2$$

Al lado izquierdo queda:

$$\frac{\sqrt{n+2}}{\sqrt{n+1}}+1>2$$

Esto demuestra la desigualdad, ya que $\sqrt{n+2}+\sqrt{n+1}>1$.

b) Por inducción sobre n.

Base: Para $n=1$ queda $1 \geq 2(\sqrt{2}-1)$, lo que es cierto.

Inducción: Supongamos que vale para n, veamos el caso $n+1$:

$$\begin{aligned}
1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}+\frac{1}{n+1} &\geq 2\left(\sqrt{n+1}-1\right)+\frac{1}{\sqrt{n+1}} \\
&\geq 2\left(\sqrt{n+1}-1\right)+2\left(\sqrt{n+2}-\sqrt{n+1}\right) \\
&= 2\left(\sqrt{n+2}-1\right)
\end{aligned}$$

Esto es lo que había que demostrar.

Por inducción vale para $n \in \mathbb{N}$.

37. Nuevamente por turno.

a) Para $m=0$, se reduce a:

$$\sum_{1 \leq k \leq n} k^{\underline{0}} = \frac{n^{\underline{1}}}{1}$$

$$\sum_{1 \leq k \leq n} 1 = \frac{n}{1}$$

lo que es cierto. La demostración para $m \geq 1$ es por inducción sobre n.

Base: Es el caso $n=1$, o sea:

$$1^{\underline{m}} = \frac{1^{\underline{m+1}}}{m+1}$$

En nuestro caso $m>0$, se reduce a $0=0$, lo que se cumple.

Inducción: Suponemos que vale para n, consideremos el caso $n+1$:

$$\sum_{1 \leq k \leq n+1} k^{\underline{m}} = \sum_{1 \leq k \leq n} k^{\underline{m}} + (n+1)^{\underline{m}}$$

Por la hipótesis:

$$\begin{aligned}
&= \frac{n^{\underline{m+1}}}{m+1}+(n+1)^{\underline{m}} \\
&= \frac{1}{m+1}\left(n \cdot (n+1)^{\underline{m}}+(m+1)\cdot(n+1)^{\underline{m}}\right) \\
&= \frac{1}{m+1}\left((n+1)^{\underline{m}}\cdot(n+m+1)\right) \\
&= \frac{(n+1)^{\underline{m+1}}}{m+1}
\end{aligned}$$

Por inducción, vale para todo $n \in \mathbb{N}$.

b) Esto es más sencillo:

$$\begin{aligned}
\Delta k^{\underline{m}} &= (k+1)^{\underline{m}} - k^{\underline{m}} \\
&= k^{\underline{m-1}} \cdot \frac{(k+m-1)(k+m)}{k} - k^{\underline{m-1}} \cdot (k+m-1) \\
&= k^{\underline{m-1}} \left(\frac{(k+m-1)(k+m)}{k} - (k+m-1) \right) \\
&= k^{\underline{m-1}} \cdot (k+m-1) \left(\frac{k+m}{k} - 1 \right) \\
&= m k^{\underline{m-1}}
\end{aligned}$$

38. Usamos inducción sobre n.

Base: $(x+1) + x^2$ ciertamente es divisible por $x^2 + x + 1$.

Inducción: Consideremos:

$$\begin{aligned}
(x+1)^{2n+3} + x^{n+3} &= (x^2 + 2x + 1) \cdot (x+1)^{2n+1} + x \cdot x^{n+2} \\
&= (x^2 + x + 1) \cdot (x+1)^{2n+1} + x \cdot \left((x+1)^{2n+1} + x^{n+2} \right)
\end{aligned}$$

Por la hipótesis de inducción el segundo término es divisible por $x^2 - x + 1$, y lo es la expresión completa.

Por inducción lo anunciado vale para $n \in \mathbb{N}_0$.

Una solución alternativa viene de reconocer que $x^3 - 1 = (x-1) \cdot (x^2 + x + 1)$. si α es cero de $x^2 + x + 1$, sabemos que:

$$\begin{aligned}
\alpha + 1 &= -\alpha^2 \\
\alpha^3 &= 1
\end{aligned}$$

Sea $p(x) = (x+1)^{2n+1} + x^{n+2}$, y evaluemos:

$$\begin{aligned}
p(\alpha) &= (-\alpha^2)^{2n+1} + \alpha^{n+2} \\
&= -\alpha^{4n+2} + \alpha^{n+2} \\
&= -\alpha^{n+2} + \alpha^{n+2} \\
&= 0
\end{aligned}$$

Como esto se cumple para ambos ceros de $x^2 + x + 1$, $x^2 + x + 1$ es factor de $(x+1)^{2n+1} + x^{n+2}$.

39. Siguiendo la pista, definimos la secuencia auxiliar $v_n = 4 - u_n$, por hipótesis es $0 < v_1 < 4$. La recurrencia queda:

$$v_{n+1} = \frac{v_n}{6 - v_n}$$

Así la demostración es simple: Si $0 \leq v_n < 4$, claramente $v_{n+1} > 0$. Para acotar por arriba, consideremos:

$$f(v) = \frac{v}{6 - v}$$

Nos interesa el máximo en el rango $0 < v < 4$. Derivando:

$$f'(v) = \frac{6}{(v-6)^2}$$

En el rango de interés es $f'(v) > 0$, y el máximo se da para $f(4) = 2$. En consecuencia $v_{n+1} < 2 < 4$.

Para la segunda parte, como sabemos que $0 < v_n < 4$:

$$\begin{aligned}
u_{n+1} - u_n &= v_n - v_{n+1} \\
&= v_n \left(1 - \frac{1}{6 - v_n} \right) \\
&> 0
\end{aligned}$$

40. Esto clama por inducción.

Base: Cuando $n = 3$ se reduce a:

$$\begin{aligned} 3^4 &> 4^3 \\ 81 &> 64 \end{aligned}$$

lo que se cumple.

Inducción: La desigualdad a demostrar es equivalente a:

$$\begin{aligned} n^n \cdot n &> (n+1)^n \\ n &> \left(1 + \frac{1}{n}\right)^n \end{aligned}$$

Suponiendo que esto es válido para n, vemos que:

$$\begin{aligned} \left(1 + \frac{1}{n+1}\right)^{n+1} &< \left(1 + \frac{1}{n}\right)^{n+1} \\ &= \left(1 + \frac{1}{n}\right) \cdot \left(1 + \frac{1}{n}\right)^n \\ &< \frac{n+1}{n} \cdot n \\ &= n + 1 \end{aligned}$$

Esto es lo que debíamos demostrar.

41. Por inducción.

Base: Para $n = 1$ el lado izquierdo es:

$$\frac{1}{2!} = \frac{1}{2}$$

El lado derecho es:

$$1 - \frac{1}{2!} = \frac{1}{2}$$

Se cumple.

Inducción: Suponiendo que vale para n, consideremos el caso $n + 1$:

$$\begin{aligned} \sum_{1 \le k \le n+1} \frac{k}{(k+1)!} &= \sum_{1 \le k \le n} \frac{k}{(k+1)!} + \frac{n+1}{(n+2)!} \\ &= 1 - \frac{1}{(n+1)!} + \frac{n+1}{(n+2)!} \\ &= 1 - \frac{n+2-(n+1)}{(n+2)!} \\ &= 1 - \frac{1}{(n+2)!} \end{aligned}$$

Se verifica.

Por inducción vale para $n \in \mathbb{N}$.

42. Por inducción.

Base: Para $n = 0$ resulta:

$$\frac{(2 \cdot 0)!}{2^0 \cdot 0!} = \frac{0!}{1 \cdot 0!} = 1$$

Cumple.

Inducción: Suponiendo que vale para n, consideremos:

$$\begin{aligned}
\frac{(2(n+1))!}{2^{n+1}(n+1)!} &= \frac{(2n)!}{2^n n!} \cdot \frac{(2n+1)(2n+2)}{2(n+1)} \\
&= \frac{(2n)!}{2^n n!} \cdot (2n+1)
\end{aligned}$$

Por inducción, el primer factor es entero, con lo que es entera la expresión completa.

Por inducción vale para $n \in \mathbb{N}_0$.

43. Por contradicción. Supongamos que $\log_2 5$ es racional, vale decir hay $a \in \mathbb{Z}$, $b \in \mathbb{N}$ tales que:

$$\begin{aligned}
\log_2 5 &= \frac{a}{b} \\
2^{a/b} &= 5 \\
2^a &= 5^b
\end{aligned}$$

Sabemos que $\log_2 5 > 0$, con lo que $a \geq 1$. Así el lado izquierdo es par, el derecho impar. Esto es absurdo. Concluimos que nuestra suposición que $\log_2 5$ es racional es incorrecta, $\log_2 5$ es irracional.

44. La demostración es por inducción sobre n.

Base: Para $n = 1$ tenemos:

$$\begin{aligned}
a_1 &= \frac{2a_0}{1 \cdot 0 \cdot a_0 + 2} \\
&= a_0
\end{aligned}$$

y directamente de la recurrencia:

$$\begin{aligned}
a_1 &= \frac{a_0}{0 \cdot a_0 + 1} \\
&= a_0
\end{aligned}$$

y esto coincide.

Inducción: Suponiendo que vale para n, evaluemos a_{n+1} por la recurrencia:

$$\begin{aligned}
a_{n+1} &= \frac{a_n}{na_n + 1} \\
&= \frac{\frac{2a_0}{n(n-1)a_0+2}}{n\frac{2a_0}{n(n-1)a_0+2} + 1} \\
&= \frac{2a_0}{2na_0 + n(n-1)a_0 + 2} \\
&= \frac{2a_0}{(2n + n(n-1))\,a_0 + 2} \\
&= \frac{2a_0}{(n+1)na_0 + 2}
\end{aligned}$$

Se ve que esta es la expresión prometida para $n + 1$.

La expresión dada para $n = 0$ da:

$$\begin{aligned}
a_0 &= \frac{2a_0}{0 \cdot (-1) \cdot a_0 + 2} \\
&= a_0
\end{aligned}$$

Uniendo esto con el resultado de la inducción, vemos que vale para $n \in \mathbb{N}_0$.

45. La demostración es por inducción fuerte sobre n. Eso sí, requerimos dos casos base.

Bases: Para los dos primeros valores tenemos:

$$
\begin{aligned}
F_0 &= 0 \leq 2^0 = 1 \\
F_1 &= 1 \leq 2^1 = 2
\end{aligned}
$$

Las dos se cumplen.

Inducción: Suponiendo que lo aseverado vale para $0 \leq k \leq n-1$, analizamos el caso n donde $n \geq 2$:

$$
\begin{aligned}
F_n &= F_{n-1} + F_{n-2} \\
&\leq 2^{n-1} + 2^{n-2} \\
&< 2^{n-1} + 2^{n-1} \\
&= 2^n
\end{aligned}
$$

Por inducción fuerte vale para $n \in \mathbb{N}_0$.

5. Estructuras algebraicas

1. A completar
2. Por el padre del teorema chino de los residuos, basta descomponer $100 = 2^2 \cdot 5^2$, por lo que $\mathbb{Z}_{100} \sim \mathbb{Z}_4 \otimes \mathbb{Z}_{25}$.
3. Por completar
4. Por completar
5. Por completar
6. Para mostrar que $H_1 \cap H_2$ subgrupo de G, debemos demostrar que para todo $a, b \in H_1 \cap H_2$ tenemos $a \cdot b^{-1} \in H_1 \cap H_2$. Si $a, b \in H_1 \cap H_2$, entonces $a, b \in H_1$ y $a, b \in H_2$. Como H_1 y H_2 son subgrupos, es $a \cdot b^{-1} \in H_1$ y también $a \cdot b^{-1} \in H_2$, o sea $a \cdot b^{-1} \in H_1 \cap H_2$, y $H_1 \cap H_2 \leq G$.
7. Considerando la secuencia de valores

   $$a^1, a^2, \ldots, a^k, \ldots$$

   Por el principio del palomar esta secuencia tiene que contener repeticiones, digamos que $a^m = a^n$, con $m < n$, es la primera. Pero entonces:

   $$a^n = a^n \cdot a^{m-n} = a^{m-n} \cdot a^n$$

   O sea, $a^{m-n} = e$.
8. Si $H = H_1 \cap H_2$ es subgrupo de G, contiene el neutro e y es cerrado respecto de la operación e inversos. La asociatividad viene de ser la operación de G.

   Por partes:

   - El neutro e pertenece a H_1 y a H_2, por ser subgrupos. Luego pertenece a la intersección H.
   - Elijamos $a, b \in H$. Entonces $a, b \in H_1$, como es subgrupo $a \odot b \in H_1$; similarmente $a \odot b \in H_2$. O sea, $a \odot b \in H$.
   - Similar al caso anterior, si elegimos $a \in H$ entonces $a \in H_1$, al ser subgrupo $a^{-1} \in H_1$; de la misma forma $a^{-1} \in H_2$. O sea, $a^{-1} \in H$.

   O sea, $H \leq G$.
9. Llamemos G y H a los grupos involucrados, con $H \leq G$. Como G es cíclico, es abeliano. Como $G = \langle g \rangle$ para un generador $g \in G$, y $H \subseteq G$, podemos expresar los elementos de H como potencias de G. Sea $h = g^n$ el elemento de H que se expresa como la mínima potencia positiva de g. Sea $x \in H$ cualquiera, que podemos expresar como $x = g^a$. Por el algoritmo de división, $a = nq + r$ con $0 \leq r < n$. Pero $x \cdot h^{-q} = g^r \in H$, como n es mínimo es $r = 0$. Todo elemento de H puede expresarse como potencia de h, H es cíclico.
10. Sea R un anillo finito, y $a \in R$ distinto de cero. Consideremos el conjunto:

    $$aR = \{ar \colon r \in R\}$$

    Si este conjunto contiene repeticiones, digamos $ar_1 = ar_2$ con $r_1 \neq r_2$, podemos escribir:

    $$\begin{aligned} ar_1 &= ar_2 \\ ar_1 - ar_2 &= 0 \\ a(r_1 - r_2) &= 0 \end{aligned}$$

    Por hipótesis $r_1 - r_2 \neq 0$, y a es un divisor de cero.

    Si aR no contiene repeticiones, al ser R finito $1 \in aR$, o sea hay $b \in R$ tal que $ab = 1$.

Pero entonces:

$$\begin{aligned}
ab &= 1 \\
(ab)a &= a \\
a(ba) - a &= 0 \\
a(ba - 1) &= 0
\end{aligned}$$

Sabemos que $a \cdot 0 = 0$, y de la hipótesis de que aR no tiene repeticiones, es:

$$\begin{aligned}
ba - 1 &= 0 \\
ba &= 1
\end{aligned}$$

Como a tiene inverso b, es una unidad.

11. Llamemos $U = G \cap H$ para comodidad. Un campo es un grupo abeliano con la suma, y un grupo abeliano para la multiplicación si excluimos el 0. Debemos demostrar que $(U, +) \leq (F, +)$ y que $(U^\times, \cdot) \leq (F^\times, \cdot)$. Para esto basta demostrar que U es cerrado respecto de $a - b$ y que $U^\times$ lo es respecto de $a \cdot b^{-1}$. Por turno:

    - Si $a, b \in U$, entonces $a, b \in G$ y $a, b \in H$. Así es $a - b \in G$ y $a - b \in H$, con lo que $a - b \in U$.
    - Supongamos ahora $a, b \in U$ con $a \neq 0$ y $b \neq 0$. Entonces $a, b \in G$ y $a, b \in H$. Con esto $a \cdot b^{-1} \in G$ y $a \cdot b^{-1} \in H$, con lo que $a \cdot b^{-1} \in U$.

    El único cabo suelto es 0 con la multiplicación, pero eso se "hereda" de F.

12. Basta un contraejemplo: En el anillo $\mathbb{Z}$ las unidades son ± 1, y $2 = 1 + 1$ no es unidad.

13. Por completar

14. El nombre formal para esta estructura es $\mathbb{Z}_{(2)}$, que usaremos de ahora en adelante.

    Debemos verificar que las operaciones estén bien definidas, o sea, que son funciones $f \colon \mathbb{Z}_{(2)} \times \mathbb{Z}_{(2)} \to \mathbb{Z}_{(2)}$. Veamos suma y multiplicación de fracciones:

    $$\begin{aligned}
    \frac{a}{b} + \frac{c}{d} &= \frac{ad + cb}{bd} \\
    \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}
    \end{aligned}$$

    En ambos casos el denominador es impar, es imposible que resulte un denominador par al simplificar estas expresiones.

    Luego debemos verificar los axiomas de anillo:

    G1: $a + (b + c) = (a + b) + c$

    G2: Hay $0 \in \mathbb{Z}_{(2)}$ tal que para todo $a \in \mathbb{Z}_{(2)}$ se cumple $a + 0 = 0 + a = a$

    G3: Para todo $a \in \mathbb{Z}_{(2)}$ existe $-a \in \mathbb{Z}_{(2)}$ tal que $a + (-a) = 0$

    G4: $a + b = b + a$

    R1: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

    R2: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ y $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

    R3: Hay $1 \in \mathbb{Z}_{(2)}$ tal que para todo $a \in \mathbb{Z}_{(2)}$ se cumple $a \cdot 1 = 1 \cdot a = a$

    R4: $a \cdot b = b \cdot a$

    Acá G1 y G4, R1, R2 y R4 se cumplen por ser operaciones en $\mathbb{Q}$.

    Para G2, vemos que:

    $$0 = \frac{0}{1} \in \mathbb{Z}_{(2)}$$

Para G3, si a es una fracción con denominador impar, lo es $-a$. Para R3,

$$1 = \frac{1}{1} \in \mathbb{Z}_{(2)}$$

O sea, es un anillo conmutativo.

Como en $\mathbb{Q}$ no hay divisores de cero, tampoco los hay en $\mathbb{Z}_{(2)}$, y es un dominio integral.

15. Esto no es más que las tradicionales reglas para manejar signos al multiplicar.

16. Llamémosle $\mathbb{Q}[\sqrt{3}]$ a este conjunto. Para que sea un anillo, debe cumplir las propiedades de las operaciones. Como es un subconjunto de los enteros, debemos verificar que para todo $u, v \in \mathbb{Q}[\sqrt{3}]$ es miembro $u + (-v)$ (es un subgrupo de $\mathbb{R}$ con la suma), que $1 \in \mathbb{Q}[\sqrt{3}]$ y que es cerrado respecto de la multiplicación (las demás propiedades se heredan de los reales). En detalle, sean $u = a + b\sqrt{3}$ y $v = c + d\sqrt{3}$, luego:

    - Es subgrupo aditivo: $u + (-v) = (a - c) + (b - d)\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$
    - Está el 1: $1 = 1 + 0\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$
    - La multiplicación es cerrada: $u \cdot v = (ac + 3bd) + (ad + bc)\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$

    Es anillo. Para unidades, tomemos $u = a + b\sqrt{3} \neq 0$ y busquemos su inverso:

    $$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2}$$

    Los coeficientes son siempre racionales (sólo para $a = b = 0$ es $a^2 - 3b^2$), así que incluso es un campo.

    Como son reales, no hay divisores propios de cero.

17. Debemos verificar si R es reflexiva, transitiva y simétrica. Por turno:

    Reflexiva: Corresponde a $a \mathrel{R} a$ para todo $a \in G$. En términos de la definición de la relación esto es que hay $g \in G$ tal que:

    $$a = gag^{-1}$$

    Esto claramente se cumple con $g = e$, el neutro del grupo, la relación es reflexiva.

    Transitiva: Es que si $a \mathrel{R} b$ y $b \mathrel{R} c$, entonces $a \mathrel{R} c$. En términos de la definición de la relación, hay elementos $g, h \in G$ tales que:

    $$\begin{aligned} a &= gbg^{-1} \\ b &= hch^{-1} \end{aligned}$$

    Esto es lo mismo que:

    $$\begin{aligned} b &= g^{-1}ag \\ c &= h^{-1}bh \end{aligned}$$

    de donde:

    $$\begin{aligned} c &= (h^{-1}g^{-1})a(gh) \\ &= (gh)^{-1}a(gh) \end{aligned}$$

    Si bautizamos:

    $$k = gh$$

    – que claramente es un elemento del grupo – esto corresponde a:

    $$\begin{aligned} c &= k^{-1}ak \\ a &= kck^{-1} \end{aligned}$$

    Vale decir, $a \mathrel{R} c$, y es transitiva.

Simétrica: Esto es que siempre que $a \mathrel{R} b$ también es $b \mathrel{R} a$. En terminos de la definición de la relación, hay $g \in G$ tal que:

$$a = gbg^{-1}$$

Esto podemos escribirlo como:

$$b = g^{-1}a(g^{-1})^{-1}$$

donde $g^{-1} \in G$, con lo que es simétrica.

Al ser reflexiva, transitiva y simétrica, es una relación de equivalencia.

18. Claramente, $x = 0$ es una posibilidad por los axiomas de anillo.

Consideremos $x \in R$, diferente de cero, y el conjunto de elementos:

$$xR = \{xa \colon a \in R\}$$

Como R es finito, es finito xR, y tiene a lo más $|R|$ elementos distintos. Si xR contiene elementos repetidos, quiere decir que hay $a, b \in R$ con $a \neq b$ tales que:

$$\begin{aligned} xa &= xb \\ x(a - b) &= 0 \end{aligned}$$

Acá usamos sólo las propiedades del grupo aditivo, y la distributividad de la multiplicación sobre la suma. Pero esto último indica que x es un divisor de cero.

Si xR no contiene elementos repetidos, debe ser $1 \in xR$, o sea hay $a \in R$ tal que:

$$xa = 1$$

con lo que también:

$$\begin{aligned} xa &= 1 \\ (xa)x &= x \\ x(ax - 1) &= 0 \end{aligned}$$

Como no hay elementos repetidos en xR, sólo $x0 = 0$, con lo que concluimos:

$$\begin{aligned} ax - 1 &= 0 \\ ax &= 1 \end{aligned}$$

y este a es el inverso de x.

19. Como τ es irracional, si $a + b\tau = a' + b'\tau$ entonces $a = a'$ y $b = b'$.

Debemos verificar que las operaciones son cerradas:

$$\begin{aligned} (a + b\tau) + (c + d\tau) &= (a + c) + (b + d)\tau \\ (a + b\tau) \cdot (c + d\tau) &= ac + (a + d)\tau + bd\tau^2 \\ &= ac + (a + d)\tau + bd(1 + \tau) \\ &= (ac + bd) + (a + d + bd)\tau \end{aligned}$$

Los coeficientes que aparecen son todos enteros, son cerradas.

Tenemos los elementos distinguidos:

$$\begin{aligned} 0 &= 0 + 0\tau \\ 1 &= 1 + 0\tau \end{aligned}$$

Claramente $\mathbb{Z}[\tau]$ es un subconjunto de $\mathbb{R}$. con lo que las operaciones son asociativas y conmutativas, y la multiplicación distribuye sobre la suma.

Al haber una única manera de representar 0, no hay más divisores de cero.

Uniendo todas las anteriores, $\mathbb{Z}[\tau]$ es un anillo conmutativo sin divisores de cero.

20. Por completar

21. Debemos determinar si se cumplen los axiomas de anillo para las operaciones de suma ($\oplus$) y multiplicación ($\otimes$). Buena parte del álgebra puede simplificarse usando algún paquete al efecto.

    Analizando las definiciones, se ve que las operaciones son cerradas siempre que m y k sean enteros, y que ambas son conmutativas. Además tenemos:

    $$\begin{aligned}(a \oplus b) \oplus c &= a + b + c - 2k \\ a \oplus (b \oplus c) &= a + b + c - 2k\end{aligned}$$

    Con esto, $\oplus$ es asociativa. Para determinar el cero, tenemos:

    $$\begin{aligned}a \oplus z &= a + z - k \\ &= a\end{aligned}$$

    con lo que $z = k$. El inverso aditivo resulta de:

    $$\begin{aligned}a \oplus b &= z \\ b &= -a + k\end{aligned}$$

    Expandiendo ambos lados resulta:

    $$(a \otimes b) \otimes c = a \otimes (b \otimes c)$$

    Queda por ver la distributividad:

    $$a \otimes (b \oplus c) - (a \otimes b) \oplus (a \otimes c) = -a(km + 1)$$

    por lo que:

    $$k = -1/m$$

    Como k y m deben ser enteros, quedan las opciones $m = \pm 1$, con correspondientes $k = \mp 1$.

    Para determinar si hay un uno:

    $$\begin{aligned}a \otimes u &= a \\ a + u + mau &= a\end{aligned}$$

    y esto se cumple con $u = 0$. Para determinar las unidades:

    $$\begin{aligned}a \otimes b &= u \\ a + b + mab &= 0\end{aligned}$$

    que sólo se cumple para enteros $a = b = 0$.

    En resumen:

    - Es un anillo para $m = 1$, $k = -1$ y para $m = -1$, $k = 1$.
    - En los casos anteriores, es un anillo conmutativo con uno. Hay una única unidad.

22. Nuevamente, se ve sin dificultades que las operaciones son cerradas. La suma claramente cumple con las propiedades de la suma en un anillo dado que es simplemente coeficiente a coeficiente. Para simplificar la notación, si:

    $$\mathbf{a} = \sum_{0 \leq i} a_i x^i$$

    entonces el coeficiente de x^i le llamaremos $\mathbf{a}[i]$, o sea $\mathbf{a}[i] = a_i$ según lo anterior.

En particular, tenemos para el cero $\mathbf{z}$ y el inverso aditivo de $\mathbf{a}$:

$$
\begin{aligned}
\mathbf{z}[i] &= z \\
(-\mathbf{a})[i] &= -a_i
\end{aligned}
$$

Analizar el producto es un poco más complejo. Sean:

$$
\begin{aligned}
\mathbf{a} &= \sum_{0 \leq i} a_i x^i \\
\mathbf{b} &= \sum_{0 \leq i} b_i x^i \\
\mathbf{c} &= \sum_{0 \leq i} c_i x^i
\end{aligned}
$$

En particular:

$$
\begin{aligned}
(\mathbf{a} \cdot \mathbf{b})[i] &= \sum_{0 \leq j \leq i} a_j b_{i-j} \\
&= \sum_{j+k=i} \mathbf{a}[j] \cdot \mathbf{b}[k]
\end{aligned}
$$

Esta última se justifica porque la suma en R es conmutativa, y así el orden de los sumandos no importa; y bajo el entendido que los índices son números naturales. Entonces tenemos:

$$
\begin{aligned}
(\mathbf{a} \cdot (\mathbf{b} \cdot \mathbf{c}))[i] &= \sum_{j+r=i} \mathbf{a}[j] \cdot (\mathbf{b} \cdot \mathbf{c})\,[r] \\
&= \sum_{j+r=i} a_j \cdot \left(\sum_{k+l=r} b_k \cdot c_l \right) \\
&= \sum_{j+r=i} \sum_{k+l=r} a_j \cdot b_k \cdot c_l \\
&= \sum_{j+k+l=i} a_j \cdot b_k \cdot c_l
\end{aligned}
$$

Estas operaciones se justifican por distributividad izquierda, y luego por la conmutatividad de la suma y asociatividad del producto en R. De forma similar:

$$
\begin{aligned}
((\mathbf{a} \cdot \mathbf{b}) \cdot \mathbf{c})[i] &= \sum_{l+r=i} (\mathbf{a} \cdot \mathbf{b})[r] \cdot \mathbf{c}[l] \\
&= \sum_{l+r=i} \left(\sum_{j+k=r} a_j \cdot b_k \right) \cdot c_l \\
&= \sum_{j+k+l=i} a_j \cdot b_k \cdot c_l
\end{aligned}
$$

Nótese que nada de esto requiere más que las propiedades de un anillo, con lo que $R[\![x]\!]$ es un anillo siempre que R lo sea.

De la definición del producto se ve que $R[\![x]\!]$ es un anillo conmutativo cuando lo es R. Hay divisores de cero en $R[\![x]\!]$ si y sólo si los hay en R (considérese el término constante de la serie).

Si R tiene uno u, claramente tenemos uno en $R[\![x]\!]$:

$$
\mathbf{u}[i] = \begin{cases} lu & \text{si } i = 0 \\ z & \text{si } i > 0 \end{cases}
$$

y si a es una unidad en R, entonces $\mathbf{a}$ con los coeficientes dados abajo lo es en $R[\![x]\!]$:

$$\mathbf{a}[i] = \begin{cases} la & \text{si } i = 0 \\ z & \text{si } i > 0 \end{cases}$$

Nótese que podrían haber otras unidades.

23. *a*) El grupo generado por a es un subgrupo y contiene a a. Sea A un subgrupo cualquiera que contiene a, claramente contiene todas las potencias de a (porque es cerrado, y están los respectivos inversos), con lo que contiene el subgrupo generado por a. (En realidad, algunos *definen* el subgrupo generado por un conjunto de elementos como el mínimo conjunto que los contiene a todos.)

    b) Si el grupo es cíclico, es generado por algún elemento, en cuyo caso es el subgrupo generado por ese elemento. Si es el subgrupo generado por un elemento, es cíclico por el punto anterior.

    c) Sea el grupo G de orden primo p. Entonces $p > 1$, por lo que existe un elemento $a \in G$ que no es el neutro. Consideremos el subgrupo generado por g. Por el teorema de Lagrange, su orden divide a p, con lo que *es* p, y por los anteriores G es cíclico.

24. Sean A y B subgrupos de G, y consideremos $C = A \cap B$. El elemento neutro de G pertenece a todos los subgrupos, así que está en la intersección. Si a y b pertenecen a A y a B, están en ambos $a \cdot b$ y a^{-1} dado que son grupos. Luego están en la intersección.

25. Para que sea campo, debe cumplir las siguientes condiciones para todos $a, b, c \in C$ con las operaciones $+$ y $\cdot$

    (I) $a + (b + c) = (a + b) + c$
    (II) $a + b = b + a$
    (III) Hay un elemento 0 tal que $a + 0 = a$
    (IV) Para cada a hay un $-a$ tal que $a + (-a) = 0$
    (V) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
    (VI) $a \cdot b = b \cdot a$
    (VII) Hay un elemento 1 tal que $a \cdot 1 = a$
    (VIII) Para cada $a \neq 0$ hay un a^{-1} tal que $a \cdot (a^{-1}) = 1$
    (IX) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

    Como estamos trabajando con números reales y las operaciones de los mismos, sólo hace falta demostrar que al operar dos elementos de C nuevamente obtenemos un elemento en C, que 0 y 1 pertenecen a C, y que están $-a$ y a^{-1}. Las demás propiedades vienen "gratis".

    En detalle:

    - Claramente:

      $$\begin{aligned} 0 &= 0 + 0 \cdot \sqrt{2} \\ 1 &= 1 + 0 \cdot \sqrt{2} \end{aligned}$$

      y ambos pertenecen.

    - Para las operaciones, si $a = u + v\sqrt{2}$ y $b = x + y\sqrt{2}$, tenemos que:

      $$\begin{aligned} -a &= -u + (-v) \cdot \sqrt{2} \\ a + b &= (u + x) + (v + y) \cdot \sqrt{2} \\ a \cdot b &= (ux + 2vy) + (uy + vx) \cdot \sqrt{2} \end{aligned}$$

      Todo lo que aparece acá son racionales.

- Para el inverso multiplicativo, supongamos $a = u + v\sqrt{2} \neq 0$, y buscamos $a^{-1} = x + y\sqrt{2}$ tal que:

$$\begin{aligned} a \cdot a^{-1} &= 1 \\ (ux + 2vy) + (uy + vx) \cdot \sqrt{2} &= 1 \end{aligned}$$

  Esto significa:

$$\begin{aligned} ux + 2vy &= 1 \\ vx + uy &= 0 \end{aligned}$$

  Este último sistema de ecuaciones tiene solución para (x, y) sólo si su determinante $u^2 - 2v^2$ no es cero. Pero que esto sea cero con $u, v \neq 0$ significa:

$$\begin{aligned} u^2 - 2v^2 &= 0 \\ \left(\frac{u}{v}\right)^2 &= 2 \end{aligned}$$

  Como u y v son racionales, esto es imposible (sabemos que $\sqrt{2}$ es irracional), y a^{-1} existe para todo $a \neq 0$.
  En detalle, resulta:

$$\begin{aligned} x &= \frac{u}{u^2 - 2v^2} \\ y &= \frac{-v}{u^2 - 2v^2} \end{aligned}$$

Es un campo.

26. Los elementos invertibles de $\mathbb{R}$ son simplemente los elementos distintos de 0. Si $\mathbb{R}^*$ fuera cíclico con generador g, podríamos escribir para cada $a \neq 0$ con algún k:

$$a = g^k$$

Pero entonces $\mathbb{R}^*$ sería contable, y sabemos que no lo es.

Otra forma de verlo es:

$$\begin{aligned} 2 &= g^k \\ 2^{\sqrt{2}} &= g^{k\sqrt{2}} \end{aligned}$$

Pero entonces $k\sqrt{2}$ debiera ser un entero, que sabemos no es posible.

27. Para que R sea una relación de equivalencia, debe cumplir:

Reflexiva: Para todo $a \in A$: $a \mathrel{R} a$
  Siempre tenemos $1 \cdot a \cdot 1^{-1} = a$, con lo que $a \mathrel{R} a$, y es reflexiva.

Transitiva: Para todo $a, b, c \in A$: Si $a \mathrel{R} b$ y $b \mathrel{R} c$, entonces $a \mathrel{R} c$.
  Supongamos $a \mathrel{R} b$ y $b \mathrel{R} c$, lo que significa que hay elementos invertibles g y h tales que:

$$\begin{aligned} gag^{-1} &= b \\ hbh^{-1} &= c \\ (hg)a(g^{-1}h^{-1}) &= \\ (hg)a(hg)^{-1} &= c \end{aligned}$$

  Como hg es invertible, esto es $a \mathrel{R} c$, y es transitiva.

Simétrica: Para todo $a, b \in A$: Si $a \mathrel{R} b$ entonces $b \mathrel{R} a$.

Supongamos $a \mathrel{R} b$, lo que significa que hay un elemento invertible g tal que:

$$\begin{aligned} gag^{-1} &= b \\ a &= g^{-1}bg \\ &= (g^{-1})b(g^{-1})^{-1} \end{aligned}$$

Esto cumple con la definición de $b \mathrel{R} a$, y es simétrica.

28. Si a es invertible, entonces $a \cdot b \neq 0$ para todo $b \neq 0$, ya que podemos tomar $a \cdot b = 0$, multiplicar por a^{-1} para obtener $b = 0$. O sea, no es divisor de cero.

Por el otro lado, siguiendo la pista, consideramos $\{a \cdot x \colon x \neq 0\}$. Si no hay elementos repetidos, debe contener todos los elementos distintos de cero, y así contiene a 1; con lo que a es invertible. Si hay elementos repetidos, digamos $a \cdot x = a \cdot y$ con $x \neq y$, entonces podemos escribir:

$$\begin{aligned} a \cdot x &= a \cdot y \\ a \cdot (x - y) &= 0 \\ a \cdot z &= 0 \end{aligned}$$

donde $z = x - y \neq 0$, y a es un divisor de cero.

29. Cada punto en turno.

a) Para demostrar que es un grupo abeliano, debemos demostrar:

1) La operación propuesta realmente es una operación, lo que en este caso se reduce a verificar que es cerrada. Cumple.
2) La operación es asociativa. Como es operar bit a bit sobre un arreglo de bits, basta verificar para un bit. En nuestro caso, eso se reduce a las siguientes 8 opciones:

$$\begin{aligned} (0 \oplus 0) \oplus 0 = 0 = 0 \oplus (0 \oplus 0) \\ (0 \oplus 0) \oplus 1 = 1 = 0 \oplus (0 \oplus 1) \\ (0 \oplus 1) \oplus 0 = 1 = 0 \oplus (1 \oplus 0) \\ (0 \oplus 1) \oplus 1 = 0 = 0 \oplus (1 \oplus 1) \\ (1 \oplus 0) \oplus 0 = 1 = 1 \oplus (0 \oplus 0) \\ (1 \oplus 0) \oplus 1 = 0 = 1 \oplus (0 \oplus 1) \\ (1 \oplus 1) \oplus 0 = 0 = 1 \oplus (1 \oplus 0) \\ (1 \oplus 1) \oplus 1 = 1 = 1 \oplus (1 \oplus 1) \end{aligned}$$

También cumple.
3) Hay un elemento neutro. En este caso es el byte 0, cumple.
4) Cada elemento tiene un inverso. En este caso cada elemento es su propio inverso, también cumple.
5) Para que sea grupo abeliano, debe ser conmutativa la operación, y la operación sobre cada bit lo es. Cumple.

Una manera alternativa de ver esto es que $\{0, 1\}$ con $\oplus$ es isomorfo al grupo $\mathbb{Z}_2$ con suma, y la estructura propuesta es entonces isomorfa a $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, y esto sabemos que es un grupo abeliano ya que lo es $\mathbb{Z}_2$.

b) El orden del grupo es el número de elementos, o sea $2^8 = 256$.

c) Vimos que cada elemento es su propio inverso, con lo que el orden máximo es 2.

30. Esto es falso. Un contraejemplo simple lo pone $\mathbb{Z}_6$, que puede descomponerse en $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ (esencialmente el padre del teorema chino de los residuos), y definitivamente $\mathbb{Z}_2$ no es subgrupo de $\mathbb{Z}_3$.

Otra forma de verlo es considerar un par de grupos abelianos A y B, y construir el grupo abeliano $A \oplus B$, que tiene subgrupos isomorfos a A y a B, pero que sólo tienen 0 en común.

31. Para que sea homomorfismo de anillo, deben cumplirse:

$$\begin{aligned}\phi(f+g) &= \phi(f)+\phi(g)\\ \phi(f\cdot g) &= \phi(f)\cdot\phi(g)\end{aligned}$$

Sean los polinomios:

$$\begin{aligned}f(x) &= a_0 + a_1x + \cdots + a_mx^m\\ g(x) &= b_0 + b_1x + \cdots + b_nx^n\end{aligned}$$

Para la suma tenemos:

$$\begin{aligned}f(x)+g(x) &= (a_0+b_0)+(a_1+b_1)x+\cdots\\ \phi(f+g) &= a_0+b_0\\ &= \phi(f)+\phi(g)\end{aligned}$$

Para la multiplicación tenemos:

$$\begin{aligned}f(x)\cdot g(x) &= (a_0\cdot b_0)+(a_0b_1+a_1b_0)x+\cdots\\ \phi(f\cdot g) &= a_0\cdot b_0\\ &= \phi(f\cdot\phi(g)\end{aligned}$$

Como las condiciones se cumplen, ϕ es un homomorfismo.

32. Sabemos que $\mathbb{Z}_3$ es un campo, con lo que un polinomio de grado n tiene a lo más n raíces. Si el polinomio f tiene un cero α, o sea $f(\alpha)=0$, podemos factorizar $f(x)=(x-\alpha)g(x)$ para algún polinomio $g(x)$.

Por inspección:

$$x^4+x^3+x = x(x^3+x^2+1)$$

El polinomio $p_1(x)=x^3+x^2+1$ se anula para $x=1$, dividiendo por $x-1=x+2$ tenemos:

$$x^3+x^2+1=(x+2)(x^2+2x+2)$$

Si el polinomio $p_2(x)=x^2+2x+2$ puede factorizarse, debe ser un par de factores lineales y tendría al menos un cero. Pero $p_2(0)=2$, $p_2(1)=2$ y $p_2(2)=1$. Como $p_2(x)$ no tiene ceros en $\mathbb{Z}_3$, no se puede factorizar.

La factorización completa solicitada es:

$$x^4+x^3+x=x(x+2)(x^2+2x+2)$$

33. Un polinomio de grado 3 sólo puede ser irreductible (un factor de grado 3), tener factores irreductibles de grado 1 y 2 o tres factores de grado 1. Si no es irreductible, tiene un factor de grado 1.

Los polinomios mónicos de grado 1 sobre $\mathbb{Z}_3$ son x, $x-1$ y $x-2$. Está claro que $x \nmid x^3+x^2+1$, resta probar los otros dos. Para comodidad futura, llamemos $p(x)=x^3+x^2+1$. Si $x-r \mid p(x)$, entonces $p(r)=0$. Probemos:

$$\begin{aligned}&1^3+1^2+1=0\\ &2^3+2^2+1=-1+1+1=1\neq 0\end{aligned}$$

Luego sólo $x-1 \mid p(x)$. Para determinar si $(x-1)^2 \mid p(x)$, vemos si $x-1 \mid p'(x)$, o, lo que es lo mismo, si 1 es un cero de $p'(x)$:

$$\begin{aligned}&p'(x)=3x^2+2x=2x\\ &p'(1)=2\neq 0\end{aligned}$$

Vale decir, $p(x)=(x-1)q(x)$, donde $q(x)$ es un polinomio irreductible de grado 2. Calculamos, dado que $x-1=x+2$ en $\mathbb{Z}_3[x]$:

$$x^3+x^2+1=(x+2)(x^2+2x+2)$$

34. Si $p(x) = x^4 + 1$ tiene factores lineales, entonces alguno de los elementos de $\mathbb{Z}_3$ son ceros. Pero $p(0) = 1$ y $p(1) = p(2) = 2$, no hay factores lineales. Si tiene factores cuadráticos:

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$$

Vemos que:

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= 0 \\ ad + bc &= 0 \\ bd &= 1 \end{aligned}$$

Si $a = c = 0$ tendríamos:

$$x^4 + 1 = (x^2 + b)(x^2 + d) = x^4 + (b + d)x^2 + bd$$

Esto es imposible. Elijamos $a = 1$, con lo que $c = 2$. El sistema de ecuaciones se reduce a:

$$\begin{aligned} b + d &= 1 \\ 2b + d &= 0 \\ bd &= 1 \end{aligned}$$

De las primeras dos ecuaciones:

$$2d = 1$$

Con esto $d = 2$, $b = 2$. La factorización es:

$$x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$$

Esto coincide con el resultado de multiplicar.

35. Usamos el algoritmo de Euclides. Podemos multiplicar por unidades que simplifiquen los cálculos. Vemos que

$\boldsymbol{a(x)}$	$\boldsymbol{b(x)}$	$\boldsymbol{r(x)}$
$15x^5 - 11x^4 - 5x^3 + 16x^2 - 10x + 4$	$3x^4 + 2x^3 - 15x^2 + 16x - 6$	$84x^3 - 169x^2 + 132x - 38$
$3x^4 + 2x^3 - 15x^2 + 16x - 6$	$84x^3 - 169x^2 + 132x - 38$	$-\frac{2781}{784}x^2 + \frac{927}{196}x - \frac{927}{392}$
Multiplicamos por $-784/927$		
$84x^3 - 169x^2 + 132x - 38$	$3x^2 - 4x + 2$	0

Cuadro 1: Algoritmo de Euclides de polinomios

el polinomio mónico buscado es:

$$x^2 - \frac{4}{3}x + \frac{1}{2}$$

36. Cada punto por turno.

   a) Si un polinomio cúbico puede factorizarse, deberá ser en un factor lineal y uno cuadrático o tres factores lineales. Si tiene un factor lineal, tiene un cero. Por tanto, basta probar los distintos valores de $x \in \mathbb{Z}_3$:

   $$\begin{aligned} 0^3 + 0^2 + 2 &= 2 \\ 1^3 + 1^2 + 2 &= 1 \\ 2^3 + 2^2 + 2 &= 2 \end{aligned}$$

   Como no tiene ceros en $\mathbb{Z}_3$, es irreductible.

b) Sabemos que si F es un campo finito, su grupo de unidades $F^\times$ es cíclico. Hay al menos un elemento primitivo. Serán primitivos todos las elementos que son potencias relativamente primas a $|F^\times|$ de un generador. O sea, en nuestro caso hay $\phi(p^n - 1)$ elementos primos.

c) Del teorema de Lagrange sabemos que el orden de todo elemento divide a $|F^\times|$. Un elemento primitivo tiene orden exactamente $|F^\times|$, basta calcular el candidato a las potencias $(p^n - 1)/q$ para cada primo q que divide a $p^n - 1$. Ninguna de las potencias debe ser 1.

37. Sabemos que $\mathbb{C}$ es un campo, con lo que un polinomio de grado n tiene a lo más n raíces. Si el polinomio f tiene un cero α, o sea $f(\alpha) = 0$, entonces podemos factorizar $f(x) = (x - \alpha)g(x)$ para algún polinomio $g(x)$.

    Por la regla de raíces racionales, de haberlas serán divisores de 1. Probando $x = 1$ vemos que es un cero. Dividiendo:

    $$x^3 - 2x + 1 = (x - 1)(x^2 + x - 1)$$

    Por la fórmula para la ecuación cuadrática, el factor $x^2 + x - 1$ tiene ceros:

    $$\frac{-1 \pm \sqrt{1 + 4}}{2}$$

    Como es un polinomio cúbico, no puede tener más de tres ceros, y los tenemos todos.

38. Por completar

39. En esta representación los elementos del campo $\mathbb{F}_4$ son polinomios en x hasta de grado 1 sobre $\mathbb{Z}_2$, o sea, la lista completa es $0, 1, x, x + 1$.

40. Si el polinomio cúbico $p(x) = x^3 + 2x + 1$ se factoriza sobre $\mathbb{Z}_3$, debe tener un factor lineal. Pero esto es sólo si tiene un cero en $\mathbb{Z}_3$. Curiosamente tenemos $p(0) = p(1) = p(2) = 1$. No hay factores lineales, con lo que es irreductible.

41. Siguiendo la pista, si es entera la expresión dada, es entera:

    $$3 \cdot \frac{k^2 - 87}{3k + 117} = \frac{k^2 - 87}{k + 39} = k - 39 + \frac{1434}{k + 39}$$

    Pero la expresión completa debe ser divisible por 3, con lo que como $39 = 3 \cdot 13$ y $1434 = 2 \cdot 3 \cdot 239$ son múltiplos de 3, lo debe ser k, digamos $k = 3j$:

    $$3j - 39 + \frac{1434}{3j + 39} = j - 13 + \frac{478}{3j + 39}$$

    La última fracción no puede ser entera, ya que el denominador es divisible por 3 y el numerador no lo es. No hay soluciones.

42. Los polinomios de grado 12 sobre $\mathbb{Z}_2$ tienen coeficiente 1 para x^{12} y coeficientes 0 o 1 para x^0 hasta x^{11}, un total de 12 coeficientes. En total hay $2^{12} = 4096$ polinomios distintos de grado 12.

    Vimos que el número N_n de polinomios irreductibles de grado n sobre $\mathbb{F}_q$ está dado por:

    $$N_n = \frac{1}{n} \sum_{d \mid n} \mu(n/d) q^d$$

    En nuestro caso específico, $q = 2$ y $n = 12$. Los divisores de interés están dados en el cuadro 2. Vemos que:

    $$N_{12} = \frac{1}{12} (4096 - 64 - 16 + 4) = 335$$

43. Debemos demostrar que lo indicado es realmente una operación (una función $\circ \colon \mathrm{D}_\infty \times \mathrm{D}_\infty \to \mathrm{D}_\infty$), pero esto es obvio de la definición. Luego debemos verificar que cumple con los axiomas de grupo:

    G1: Para todo $a, b, c \in \mathrm{D}_\infty$ se cumple $a \circ (b \circ c) = (a \circ b) \circ c$

d	n/d	$\mu(n/d)$	2^d
1	12	0	2
2	6	1	4
3	4	0	8
4	3	-1	16
6	2	-1	64
12	1	1	4096

Cuadro 2: Divisores de 12

G2: Hay $e \in \mathrm{D}_\infty$ tal que para todo $a \in \mathrm{D}_\infty$ se cumple $a \circ e = a$

G3: Para todo $a \in \mathrm{D}_\infty$ existe $a^{-1} \in \mathrm{D}_\infty$ tal que $a \circ a^{-1} = e$

Para G1 consideremos $(x, r), (y, s), (z, t) \in \mathrm{D}_\infty$:

$$\begin{aligned}((x, r) \circ (y, s)) \circ (z, t) &= (x + yr, rs) \circ (z, t)\\ &= (x + yr + zrs, rst)\end{aligned}$$

Pero también:

$$\begin{aligned}(x, r) \circ ((y, s) \circ (z, t)) &= (x, r) \circ (y + zs, st)\\ &= (x + (y + zs)r, rst)\\ &= (x + yr + zrs, rst)\end{aligned}$$

Coinciden, la operación es asociativa.

Para G2 debemos hallar el elemento $e = (a, b)$. Consideremos $(x, s) \in \mathrm{D}_\infty$ cualquiera, y planteamos:

$$\begin{aligned}(x, s) \circ (a, b) &= (x, s)\\ (x + as, bs) &= (x, y)\end{aligned}$$

Esto da las ecuaciones:

$$\begin{aligned}x &= x + as\\ s &= bs\end{aligned}$$

La solución es $e = (a, b) = (0, 1)$, hay un neutro.

Para G3 debemos hallar el inverso de (x, s):

$$\begin{aligned}(x, s) \circ (y, t) &= (0, 1)\\ (x + ys, st) &= (0, 1)\end{aligned}$$

Nuevamente un sistema de ecuaciones:

$$\begin{aligned}0 &= x + ys\\ 1 &= st\end{aligned}$$

Como s y t son ± 1, la segunda es $s = t$, la primera entrega $y = -sx$. Tenemos el inverso $(-sx, s)$ para todo elemento (x, s).

Como satisface los tres axiomas, es un grupo.

Este grupo no es abeliano, por ejemplo:

$$\begin{aligned}(2, 1) \circ (3, -1) &= (2 + 3 \cdot 1, 1 \cdot (-1))\\ &= (5, -1)\\ (3, -1) \circ (2, 1) &= (3 + 2 \cdot (-1), (-1) \cdot 1)\\ &= (1, -1)\end{aligned}$$

44. Cada punto por turno.

   a) Lo demostramos por inducción.

   Base: Cuando $n = 1$, claramente se cumple. También se cumple para $n = 2$.
   Inducción: Supongamos que $x^n = x$, y consideremos:

$$\begin{aligned} x^{n+1} &= x^n \cdot x && \text{definición de } x^n \\ &= x \cdot x && \text{por inducción} \\ &= x^2 && \text{definición de } x^n \\ &= x && \text{idempotencia} \end{aligned}$$

   Por inducción, vale para $n \in \mathbb{N}$.

   b) Calculamos:

$$\begin{aligned} (1 - x) \cdot (1 - x) &= 1 - 2x + x^2 && \text{1 conmuta con todos} \\ &= 1 - 2x + x && x \text{ es idempotente} \\ &= 1 - x && 2x - x = x \end{aligned}$$

   y $1 - x$ también es idempotente.

   c) Nuevamente calculamos:

$$\begin{aligned} xy \cdot xy &= xy \cdot yx && x \text{ e } y \text{ conmutan} \\ &= xyx && y \text{ idempotente} \\ &= x^2 y && x \text{ e } y \text{ conmutan} \\ &= xy && x \text{ idempotente} \end{aligned}$$

   Ahora, usando idempotencia y que x e y conmutan, y el resultado anterior, junto con la asociatividad de la suma y la multiplicación en el anillo:

$$\begin{aligned} (x + y - xy) \cdot (x + y - xy) &= x^2 + xy - xyx + yx + y^2 - yxy - xy \cdot xy \\ &= x + xy - x^2 y + xy + y - xy^2 - xy \\ &= x + xy - xy + xy + y - xy - xy \\ &= x + y - xy \end{aligned}$$

   También idempotente.

6. Teoría de números

1. Necesitamos demostrar las propiedades de las operaciones. De partida, ambas son operaciones.

   G1: La diferencia simétrica es lo que pertenece a los conjuntos, pero no está en la intersección, así que para cualquiera conjuntos $\mathcal{A}$, $\mathcal{B}$ y $\mathcal{C}$:

   $$(\mathcal{A} \triangle \mathcal{B}) \triangle \mathcal{C} = \mathcal{A} \triangle (\mathcal{B} \triangle \mathcal{C})$$

   Véase la figura 2. La operación es asociativa.

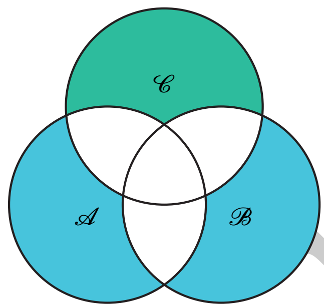


Figura 2: Diferencia simétrica entre tres conjuntos

   G2: Sabemos que para todo conjunto $\mathcal{A}$:

   $$\mathcal{A} \triangle \varnothing = \varnothing \triangle \mathcal{A} = \mathcal{A}$$

   Hay un neutro.

   G3: Para todo $\mathcal{A}$ es:

   $$\mathcal{A} \triangle \mathcal{A} = \varnothing$$

   Esto da inversos, $-\mathcal{A} = \mathcal{A}$. Curiosamente cada elemento es su propio inverso.

   G4: Es claro que para todo $\mathcal{A}$ y $\mathcal{B}$:

   $$\mathcal{A} \triangle \mathcal{B} = \mathcal{B} \triangle \mathcal{A}$$

   Es conmutativa.

   R1: Para cualquiera $\mathcal{A}$, $\mathcal{B}$ y $\mathcal{C}$:

   $$(\mathcal{A} \cap \mathcal{B}) \cap \mathcal{C} = \mathcal{A} \cap (\mathcal{B} \cap \mathcal{C})$$

   La intersección es asociativa.

   R2: Para cualquiera $\mathcal{A}$, $\mathcal{B}$ y $\mathcal{C}$:

   $$(\mathcal{A} \triangle \mathcal{B}) \cap \mathcal{C} = (\mathcal{A} \cap \mathcal{C}) \triangle (\mathcal{B} \cap \mathcal{C})$$

   y (como la intersección es conmutativa) al revés también. Véase la figura 3.

   R3: Sabemos que para todo $\mathcal{A}$:

   $$\mathcal{A} \cap \mathcal{U} = \mathcal{U} \cap \mathcal{A} = \mathcal{A}$$

   con lo que tenemos un neutro.

   R4: También para todo $\mathcal{A}$ y $\mathcal{B}$:

   $$\mathcal{A} \cap \mathcal{B} = \mathcal{B} \cap \mathcal{A}$$

   También es conmutativa.

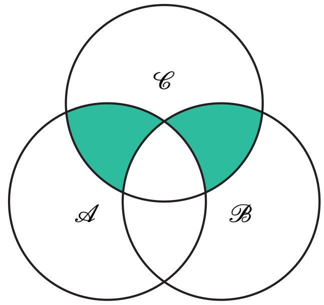


Figura 3: Intersección con la diferencia simétrica entre dos conjuntos

En resumen, es un anillo conmutativo, con $0 = \varnothing$ y $1 = \mathcal{U}$.

2. Cada punto por turno.

   a) Si f y g son funciones aritméticas, lo es $f * g$. La definición no da lugar a ninguna posible ambigüedad.

   b) Para demostrar que $*$ es conmutativa basta:

   $$f * g(n) = \sum_{ab=n} f(a)g(b) = \sum_{ba=n} g(b)f(a) = g * f(n)$$

   c) Para demostrar que $*$ es asociativa:

   $$(f*g)*h(n) = \sum_{c \mid n} \left(\sum_{ab=n/c} f(a)f(b) \right) h(c) = \sum_{abc=n} f(a)g(b)h(c) = \sum_{a \mid n} f(a) \left(\sum_{bc=n/a} g(b)h(c) \right) = f*(g*h)(n)$$

   d) El elemento neutro es la función que cumple:

   $$\begin{aligned} \epsilon * f(n) &= f(n) \\ \sum_{ab=n} \epsilon(a)f(b) &= f(n) \end{aligned}$$

   Esto se cumple para toda función f si $\epsilon(n) = [n = 1]$.

   e) Podemos plantear el sistema de ecuaciones:

   $$f * f^{-1}(n) = \sum_{ab=n} f(a)f^{-1}(b)$$

   Siempre que $f(1) \neq 0$ podemos calcular $f^{-1}(1) = 1/f(1)$, y luego determinar sucesivamente:

   $$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d \mid n \\ d>1}} f^{-1}(d)f(n/d)$$

   Esto determina una función $f^{-1}(n)$.

   f) Tenemos:

   $$f * (g + h)(n) = \sum_{ab=n} f(a)(g(b) + h(b)) = \sum_{ab=n} f(a)g(b) + \sum_{ab=n} f(a)h(b) = (f * g + f * h)(n)$$

   Cumple los axiomas de anillo conmutativo.

3. La factorización completa de $10!$ es:

   $$10! = 1 \cdot 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$

   Por tanto la factorización de n es:

   $$n = 2^4 \cdot 3^2 \cdot 5 = 720$$

4. La ecuación corresponde a:

$$ax \equiv c - b \pmod{m}$$

lo que a su vez significa que para algún $k \in \mathbb{Z}$:

$$ax + km = c - b$$

Sabemos que esto es posible si y sólo si $\gcd(a, m)$ divide a $c - b$.

5. Tenemos la ecuación:

$$ax + by = c$$

Es claro que si $\gcd(a, b)$ no es un factor de c, esta ecuación no tiene soluciones. Para simplificar lo que viene, sea $d = \gcd(a, b)$.

De la identidad de Bézout sabemos que hay enteros u y v tales que:

$$au + bv = d \tag{1}$$

En realidad, todas las soluciones están dadas por las expresiones siguientes, donde $k \in \mathbb{Z}$:

$$\begin{aligned} u' &= u + \frac{kb}{d)} \\ v' &= v - \frac{ka}{d} \end{aligned}$$

De acá obtenemos los posibles valores de x e y:

$$\begin{aligned} x &= \frac{uc}{d} + \frac{kbc}{d^2} \\ y &= \frac{vc}{d} - \frac{kac}{d^2} \end{aligned}$$

Hay soluciones si $\gcd(a, b) \mid c$. Si $c \geq 0$, debe ser también que a y b tengan distinto signo. Si $c < 0$, a y b deben ser negativos.

6. La teoría de anillos cuadráticos desarrollada en el apunte indica que debemos considerar el anillo $\mathbb{Z}[\sqrt{17}]$. La pista nos indica que la solución fundamental de $x^2 - 17y^2 = -1$ es $(4, 1)$, con lo que la solución fundamental de la ecuación de Pell dada es:

$$(4 - \sqrt{17})^2 = 33 - 8\sqrt{17}$$

Las soluciones solicitadas están dadas por:

$$x_n - y_n\sqrt{17} = (33 - 8\sqrt{17})^n$$

La ecuación nos dice que x_n/y_n es una buena aproximación de la raíz. Incluso obtenemos aproximaciones intermedias adicionales con la raíz de la solución fundamental en este caso. Dado que los elementos (x_n, y_2) tienen norma $N(x_n - y_n\sqrt{d}) = (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) = 1$, el error de la aproximación:

$$\sqrt{d} \approx \frac{x_n}{y_n}$$

está dado por:

$$e_n = \left|\sqrt{d} - \frac{x_n}{y_n}\right| = \frac{1}{y_n}\left|y_n\sqrt{d} - x_n\right| = \frac{1}{y_n(x_n + y_n\sqrt{d})} \approx \frac{1}{2x_n y_n}$$

Acá usamos la aproximación para la raíz. Interesa calcular los valores (x_n, y_n) en forma simple. Supongamos:

$$\begin{aligned}
x_n - y_n\sqrt{d} &= (x_0 - y_0\sqrt{d})^n \\
&= (x_{n-1} - y_{n-1}\sqrt{d})(x_0 - y_0\sqrt{d}) \\
&= (x_0 x_{n-1} + d y_0 y_{n-1}) - (x_{n-1} y_0 + x_0 y_{n-1})\sqrt{d}
\end{aligned}$$

por lo que podemos calcularlos partiendo de (x_0, y_0) mediante:

$$\begin{aligned}
x_{n+1} &= x_n x_0 + d y_0 y_n \\
y_{n+1} &= x_n y_0 + x_0 y_n
\end{aligned}$$

En nuestro caso particular, interesa $e_n \leq 5 \cdot 10^{-5}$ o sea $2x_n y_n \geq 2000$. La recurrencia partiendo de $(4, 1)$ da la tabla 3, donde $n = 1$ da $2 \cdot 33 \cdot 8 = 528$ y $n = 2$ cumple $2 \cdot 268 \cdot 65 = 34\,840$. La aproximación solicitada es:

$$\sqrt{17} \approx \frac{268}{65}$$

n	$\mathbf{x_n}$	$\mathbf{y_n}$
0	4	1
1	33	8
2	268	65
3	2177	528
4	17684	4289

Cuadro 3: Potencias de $4 - \sqrt{17}$

7. Por turno.

   a) Si $d = a^2$, donde podemos suponer $a > 0$ sin pérdida de generalidad, la ecuación queda:

   $$\begin{aligned}
   1 &= x^2 - (ay)^2 \\
   &= (x + ay)(x - ay)
   \end{aligned}$$

   Esto solo es posible si ambos factores son ± 1. Como suponemos que x e y son no-negativos, al menos el primer factor es positivo, y debe serlo el segundo también:

   $$x + ay = x - ay = 1$$

   de donde $y = 0$ y en consecuencia $x = 1$, la solución trivial.

   b) Sean x, y soluciones positivas a la ecuación dada. Entonces:

   $$x \cdot x - dy \cdot y = 1$$

   Hemos escrito:

   $$sx + ty = 1$$

   con lo que son relativamente primos.

8. El caso $n = 1$ es claro.

   Si $n > 1$, tenemos:

   $$a^n - 1 = (a - 1) \sum_{0 \leq k \leq n-1} a^k$$

   Esto es compuesto, salvo si $a - 1 = 1$, o sea $a = 2$.

   Demostramos que n es primo por contradicción. Supongamos $n = rs$ con $r, s > 1$. Nuevamente:

   $$2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1) \sum_{0 \leq k \leq s-1} 2^{rk}$$

   Como $2^r > 2$, esto es compuesto.

9. Vamos por turno.

   a) Si $a \equiv b \pmod{c}$, entonces $a = b + k \cdot c$ para algún $k \in \mathbb{Z}$. O sea, $\gcd(b, c) \mid a$, por lo que también $\gcd(b, c) \mid \gcd(a, c)$. Por simetría, también es $\gcd(a, c) \mid \gcd(b, c)$. En consecuencia, como el máximo común divisor es positivo, $\gcd(a, c) = \gcd(b, c)$.

   Alternativamente, $a \equiv b \pmod{c}$ significa que dejan el mismo resto al dividir por c; después de la primera iteración del algoritmo de Euclides este sigue igual para ambos, y el resultado final será el mismo.

   b) Cuando n es par, tanto $n + 1$ como $n^{2k} + 1$ son impares; para n impar ambos son pares. Vale decir, $n + 1 \equiv n^{2k} + 1 \pmod{2}$. Aplicando la parte 9*a*, es como se indica.

   c) Con $a = F_n = 2^{2^n} + 1$ y $b = F_m = 2^{2^m} + 1$, vemos que $2^{2^m} / 2^{2^n} = 2^{2^m - 2^n}$, y claramente $2^m - 2^n$ es par y mayor a cero. En consecuencia, aplicando 9*b* es $\gcd(F_n, F_m) = \gcd(F_n, 2) = 1$.

10. Como sólo aparecen cuadrados, los signos no importan. Considerando la mínima solución para $u \geq 0$, es claro que u, x, y, z no tienen factores comunes. En particular, no pueden ser todos pares.

    Derivaremos contradicciones para el caso en que u es par e impar, con lo que demostramos que no hay soluciones posibles.

    Si u es par, es par $7u^2$, y por tanto exactamente dos de x, y, z son impares. Si x es impar, es $x \equiv \pm 1 \pmod{4}$, con lo que $x^2 \equiv 1 \pmod{4}$. Así $7u^2 \equiv 0 \pmod{4}$, mientras $x^2 + y^2 + z^2 \equiv 2 \pmod{4}$. Contradicción.

    Si u es impar, es impar $7u^2$, con lo que uno o tres de x, y, z son impares. Si x es impar, entonces:

$$\begin{aligned} x &= 2c + 1 \\ x^2 &= 4c^2 + 4c + 1 \\ &= 4(c^2 + c) + 1 \end{aligned}$$

    Pero $c^2 + c = c(c + 1)$, que es siempre par, con lo que $x^2 \equiv 1 \pmod{8}$. Así $x^2 + y^2 + z^2 \equiv 1$ ó $3 \pmod{8}$, mientras $7u^2 \equiv 7 \pmod{8}$. Nuevamente imposible.

11. Por turno.

    a) Esto indica que pasa la prueba de Fermat para base 3, lo que dice que es un posible primo pero no es concluyente.

    b) Esto es el test de Miller-Rabin, como $3^{474} \equiv 729 \not\equiv \pm 1 \pmod{949}$ falla la prueba. Es compuesto.

12. Esto significa:

$$\begin{aligned} 3x - 17 &\equiv 0 \pmod{4} \\ 3x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{4} \\ 5x + 18 &\equiv 0 \pmod{7} \\ 5x &\equiv 3 \pmod{7} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

    Como $\gcd(4, 7) = 1$, del teorema chino de los residuos sabemos que hay una solución única módulo $4 \cdot 7 = 28$. Tenemos:

$$\begin{aligned} 7^{-1} &= 3 \quad \text{en } \mathbb{Z}_4 \\ m_4 &= 3 \cdot 7 = 21 \\ 4^{-1} &= 2 \quad \text{en } \mathbb{Z}_7 \\ m_7 &= 2 \cdot 4 = \ \ 8 \end{aligned}$$

    La solución es:

$$x \equiv m_4 \cdot 3 + m_7 \cdot 2 \equiv 21 \cdot 3 + 8 \cdot 2 \equiv 23 \pmod{28}$$

13. Las relaciones indicadas se transforman en el sistema de congruencias:

$$\begin{aligned} n + 1 &\equiv 0 \pmod{3} \\ 3n + 1 &\equiv 0 \pmod{4} \\ 7n - 3 &\equiv 0 \pmod{5} \end{aligned}$$

El inverso de 3 módulo 4 es 3, el inverso de 7 módulo 5 es 3. Usando esto obtenemos:

$$\begin{aligned} n &\equiv -1 \\ &\equiv 2 \pmod{3} \\ n &\equiv -3 \\ &\equiv 1 \pmod{4} \\ n &\equiv 9 \\ &\equiv 4 \pmod{5} \end{aligned}$$

El teorema chino de los residuos asegura que hay solución única módulo $3 \cdot 4 \cdot 5 = 60$. Tenemos:

$$\begin{aligned} s_3 &= (4 \cdot 5)^{-1} = 20^{-1} = 2^{-1} = 2 \\ m_3 &= 2 \cdot (4 \cdot 5) \qquad = 40 \\ s_4 &= (3 \cdot 5)^{-1} = 15^{-1} = 3^{-1} = 3 \\ m_4 &= 3 \cdot (3 \cdot 5) = 45 \\ s_5 &= (3 \cdot 4)^{-1} = 12^{-1} = 2^{-1} = 3 \\ m_5 &= 3 \cdot (3 \cdot 4) = 36 \end{aligned}$$

En consecuencia, la solución es:

$$\begin{aligned} n &\equiv m_3 \cdot 2 + m_4 \cdot 1 + m_5 \cdot 4 \\ &\equiv 40 \cdot 2 + 45 \cdot 1 + 36 \cdot 4 \\ &\equiv 269 \\ &\equiv 29 \pmod{60} \end{aligned}$$

Esto cumple las congruencias de las que partimos.

14. Por el padre del teorema chino de los residuos sabemos que $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$. Sabemos también que $\mathbb{Z}_a$ y $\mathbb{Z}_b$ son campos, dado que a y b son primos. En el campo $\mathbb{Z}_p$ el polinomio $x^2 - 1$ puede tener a lo más dos ceros, y tiene exactamente dos: ± 1 (o 1 y $p - 1$).

En $\mathbb{Z}_a \times \mathbb{Z}_b$ tenemos:

$$(\pm 1, \pm 1)^2 = (1, 1)$$

Las raíces buscadas son las soluciones de cuatro sistemas de congruencias como:

$$\begin{aligned} x &\equiv x_1 \pmod{a} \\ x &\equiv x_2 \pmod{b} \end{aligned}$$

Sabemos que las soluciones son todas diferentes, ya que los pares (x_1, x_2) son todos diferentes. Hay cuatro en total.

Si llamamos a' al inverso de a módulo b, y similarmente b', la solución se expresa:

$$x \equiv bb'x_1 + aa'x_2 \pmod{ab}$$

O sea, tenemos las cuatro raíces de 1:

$$\begin{aligned} (1, 1) &\mapsto aa' + bb' \equiv 1 \pmod{ab} \\ (1, b - 1) &\mapsto aa'(b - 1) + bb' \\ (a - 1, 1) &\mapsto aa' + (a - 1)bb' \\ (a - 1, b - 1) &\mapsto aa'(b - 1) + (a - 1)bb' \equiv -1 \pmod{ab} \end{aligned}$$

15. Por el teorema de Lagrange, el orden de un elemento del grupo divide al orden del grupo. Si el orden del grupo es un primo p, sólo pueden haber elementos de orden 1 y p. Pero sólo puede haber un elemento de orden 1 (el neutro es único). En consecuencia, los demás elementos tienen orden p. y el grupo es cíclico.

16. El producto de una secuencia de k enteros consecutivos podemos describirlo como $m^{\underline{k}}$.

    Usamos inducción, sobre k.

    Base: Para $k = 1$, siempre se cumple $1! \mid m^{\underline{1}}$.

    Inducción: Suponiendo que vale para k, demostramos que vale para $k+1$.

    Podemos escribir:

    $$m^{\underline{k+1}} = (k+1) \sum_{1 \le r \le m} r^{\underline{k}}$$

    Por inducción para k, cada término de la suma es divisible por $k!$, con lo que el lado derecho es divisible por $(k+1) \cdot k! = (k+1)!$.

    Por inducción vale para $k \in \mathbb{N}$

17. Como los módulos son relativamente primos a pares, esta es una tarea para el teorema chino de los residuos. Con la notación del apunte:

    $$\begin{aligned} s_5 &= (7 \cdot 8)^{-1} = 1^{-1} = 1 && \text{en } \mathbb{Z}_5 \\ s_7 &= (5 \cdot 8)^{-1} = 5^{-1} = 3 && \text{en } \mathbb{Z}_7 \\ s_8 &= (5 \cdot 7)^{-1} = 3^{-1} = 3 && \text{en } \mathbb{Z}_8 \end{aligned}$$

    Con los valores anteriores, ahora módulo $5 \cdot 7 \cdot 8 = 280$:

    $$\begin{aligned} m_5 &= (7 \cdot 8) \cdot 1 = 56 \\ m_7 &= (5 \cdot 8) \cdot 3 = 120 \\ m_8 &= (5 \cdot 7) \cdot 3 = 105 \end{aligned}$$

    Los valores buscados son:

    $$m_5 \cdot b_5 + m_7 \cdot b_7 + m_8 \cdot b_8 = 56 \cdot 3 + 120 \cdot 2 + 105 \cdot 6 \equiv 198 \pmod{280}$$

18. Como $\gcd(9, 12) \neq 1$, no es aplicable el teorema chino de los residuos.

    Las congruencias significan que para $i, j \in \mathbb{Z}$:

    $$x = 6 + 9i \tag{2}$$
    $$x = 5 + 12j \tag{3}$$

    Igualando (2) con (3) obtenemos:

    $$\begin{aligned} 6 + 9i &= 5 + 12j \\ 1 &= -9i + 12j \\ &= 3(-3i + 4j) \end{aligned}$$

    Esta última relación es imposible, $3 \nmid 1$. No hay soluciones.

19. Por completar

20. Esto es equivalente a trabajar en $\mathbb{Z}_{64}$. También $\phi(64) = 32$:

    $$\begin{aligned} 73^{33} + 5 &\equiv 9^{33} + 5 && \text{Reducir módulo 64} \\ &\equiv 3^{2 \cdot 33} + 5 && \text{Propiedades de las potencias} \\ &\equiv 3^{66} + 5 \\ &\equiv 3^4 + 5 && \text{Por el teorema de Euler} \\ &\equiv 81 + 5 \\ &\equiv 22 \pmod{64} \end{aligned}$$

21. Por completar
22. Aplicando las propiedades de congruencias:

$$\begin{aligned}
0^2 &\equiv 0 \pmod{4} \\
1^2 &\equiv 1 \pmod{4} \\
2^2 &\equiv 0 \pmod{4} \\
3^2 &\equiv 1 \pmod{4}
\end{aligned}$$

En consecuencia, módulo 4 la suma de cuadrados puede ser 0, 1 ó 2. Pero $10\,003 \equiv 3 \pmod{4}$.

23. Como 11 es primo, es aplicable el teorema de Fermat y $117^{10} \equiv 1 \pmod{11}$. En consecuencia, $117^{100} + 1 \equiv 2 \pmod{11}$, y no es divisible.
24. Factorizamos:

$$1\,268\,064 = 2^5 \cdot 3^2 \cdot 7 \cdot 17$$

Con esto:

$$\phi(1\,268\,064) = 2^4 \cdot (2-1) \cdot 3 \cdot (3-1) \cdot (7-1) \cdot (17-1) = 9\,216$$

25. Por completar
26. Por completar
27. Por completar
28. Por completar
29. Tenemos las respectivas tablas para las operaciones del cuadro 4. Supongamos un isomorfismo $\theta \colon \mathbb{Z}_6 \to \mathbb{Z}_7^\times$.

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(a) $(\mathbb{Z}_7^\times, \cdot)$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) $(\mathbb{Z}_6, +)$

Cuadro 4: Tablas de $\mathbb{Z}_7^\times$ y $\mathbb{Z}_6$

Es claro que los respectivos neutros son 0 y 1, por lo que $\theta(0) = 1$. Se ve que ambos son grupos abelianos (las tablas son simétricas). Incluso más, sabemos que $\mathbb{Z}_6$ es cíclico. De haber un isomorfismo, deberá ser de la forma $\theta(k) = g^k$ para algún generador $g \in \mathbb{Z}_7^\times$. Una posibilidad es elegir algún candidato y verificar sus potencias, como muestra el cuadro 5. Se ve que 3 y 5 son generadores, y los grupos son isomorfos.

De no haber tenido la doble suerte de un grupo cíclico y hallar un generador rápidamente, nos habría quedado una larga tarea por delante para completar el isomorfismo, o demostrar que no puede existir.

30. Por completar
31. Vemos que $\gcd(39, 13) \neq 1$, es posible que no haya solución. Analizando las congruencias en posible conflicto:

$$\begin{aligned}
x &\equiv 37 \pmod{39} \\
&\equiv 11 \pmod{13}
\end{aligned}$$

Esto contradice la segunda congruencia. No hay soluciones.

1	2	3	4	5	0
2	4	1			
3	2	6	4	5	1
4	2	1			
5	4	6	2	3	1
6	1				

Cuadro 5: Potencias en $\mathbb{Z}_7^\times$

32. Por completar

33. Por completar

34. Lo más fácil es usar el siguiente teorema:

    Teorema. *Sea $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ un polinomio con coeficientes enteros, $a_n \neq 0$ y $a_0 \neq 0$, y sin factores comunes entre los coeficientes. Entonces toda raíz racional $r = u/v$ en mínimos términos de $p(x) = 0$ cumple $v \mid a_n$ y $u \mid a_0$.*

    Demostración. Tomamos $p(r) = 0$ y multiplicamos por v^n:

    $$a_n v^n + a_{n-1} u v^{n-1} + \ldots + a_1 u^{n-1} v + a_0 u^n = 0$$

    El lado derecho es divisible por u y por v, luego lo es el lado izquierdo. Esto lleva a $u \mid a_n$ y $v \mid a_0$. $\square$

    Ahora bien, $\sqrt{n}$ es raíz de $x^2 - n = 0$, por el teorema su denominador es 1 de ser racional.

35. Cada punto por turno.

    a) Si $d = a^2$ es un cuadrado perfecto, la ecuación se reduce a:

    $$x^2 - (ay)^2 = 1$$

    Esto sólo puede cumplirse para $x = 1$, $y = 0$, o sea la solución trivial.

    b) La relación indicada es decir:

    $$x_{n+1} + y_{n+1}\sqrt{d} = (x_n + y_n\sqrt{d}) \cdot (x_0 + y_0\sqrt{d})$$

    Esto es:

    $$\begin{aligned} x_{n+1} &= x_0 x_n + d y_0 y_n \\ y_{n+1} &= y_0 x_n + x_0 y_n \end{aligned}$$

36. El conjunto I siempre contiene $a^2 + b^2 + c^2$, que es positivo a menos que $a = b = c = 0$. Podemos también suponer que $a, b, c \geq 0$, los signos no afectan al conjunto.

    Sea m el mínimo elemento de I, eso significa que puede escribirse $m = ax + by + cz$ para $x, y, z \in \mathbb{Z}$. Sea $n \in I$, entonces podemos escribir $n = ax' + by' + cz'$ para $x', y', z' \in \mathbb{Z}$. Por el algoritmo de división:

    $$n = qm + r \qquad \text{donde } 0 \leq r < m$$

    O sea:

    $$\begin{aligned} r &= n - qm \\ &= (ax' + by' + cz') - q(ax + by + cz) \\ &= a(x' - qx) + b(y' - qy') + c(z' - qz) \end{aligned}$$

    Esto es $r \in I$, con lo que $r = 0$. Esto es $m \mid n$.

37. De la identidad de Bézout para $\gcd(a^m, b^n) = 1$ sabemos que hay s y t tales que

$$\begin{aligned} sa^m + tb^n &= 1 \\ (sa^{m-1})a + (tb^{n-1})b &= 1 \end{aligned}$$

Claramente este es el mínimo valor posible de expresiones de la forma $ua + vb$, y en consecuencia $\gcd(a, b) = 1$.

38. La ecuación dada es equivalente a decir que existe $c \in \mathbb{Z}$ tal que:

$$ax + cm = b$$

Esto sólo es posible si $\gcd(a, m) \mid b$. En tal caso podemos dividir todo por $\gcd(a, m)$:

$$a_1 x \equiv b_1 \pmod{m}$$

con $a_1 = a/\gcd(a, m)$ y $b_1 = b/\gcd(a, m)$. Pero a_1 es invertible, y hay una solución única $x = a_1^{-1} b_1$.

39. El número corresponde a:

$$x = \sum_{0 \leq k \leq n} d_k \cdot 10^k$$

a) Como $10 \equiv 1 \pmod{9}$, la expresión para x es:

$$x \equiv \sum_{0 \leq k \leq n} d_k \cdot 1^k \equiv \sum_{0 \leq k \leq n} d_k \pmod{9}$$

b) Como $10 \equiv -1 \pmod{11}$, la expresión para x es:

$$x \equiv \sum_{0 \leq k \leq n} d_k \cdot (-1)^k \pmod{11}$$

40. Interesa el conjunto de elementos de $\mathbb{Z}_{100}$ que son cuadrados perfectos. La forma más simple es directamente contarlos:

00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96

Esto puede resumirse con e un dígito par y o uno impar:

00, e1, e4, 25, o6, e9

41. Sabemos que si para primos p_r diferentes

$$N = \prod_{1 \leq r \leq n} p_r^{k_r}$$

entonces:

$$\phi(N) = \prod 1 \leq r \leq n p_r^{k_r - 1}(p_r - 1)$$

Para que esto sea par, basta que tenga un factor par. Pero salvo 2 todos los primos son impares, así que $\phi(N)$ será par siempre que sea divisible por un primo impar o si es al menos 4 si es una potencia de 2.

Para que sea una potencia de 2, deben ser potencias de 2 todos los factores. Si N es divisible por un primo impar p, debe aparecer con exponente 1 y ser tal que $p = 2^s + 1$, y eso sólo es posible si s es a su vez una potencia de 2: $p = 2^{2^t} + 1$. A tales primos se les llama *primos de Fermat*, se sabe que esto es primo para $0 \leq t \leq 4$, los demás valores que se han revisado son todos compuestos.

42. Por el teorema de Fermat, sabemos que si $p \not| x$:

$$\begin{aligned} x^{p-1} &\equiv 1 \pmod{p} \\ x^p &\equiv x \pmod{p} \end{aligned}$$

Por el otro lado, si $p \mid x$, entonces

$$
\begin{aligned}
x &\equiv 0 \pmod{p} \\
x^p &\equiv 0 \pmod{p} \\
x^p &\equiv x \pmod{p}
\end{aligned}
$$

Aplicando esto a lo solicitado:

$$
\begin{aligned}
(a+b)^p &\equiv a+b \pmod{p} \\
&\equiv a^p + b^p \pmod{p}
\end{aligned}
$$

43. De la descripción tenemos:

$$
\begin{aligned}
c_1 &= g^y \\
c_2 &= m \cdot h^y = m \cdot g^{xy} \\
m' &= c_2 \cdot c_1^{-x} \\
&= (m \cdot g^{xy}) \cdot c_1^{-x} \\
&= m \cdot g^{xy} \cdot (g^y)^{-x} \\
&= m \cdot g^{xy} \cdot g^{-xy} \\
&= m
\end{aligned}
$$

44. Típico caso en que vale la pena resolver un problema más general para luego especializar.

Aplicamos el principio de inclusión y exclusión.

- Nuestro universo son los números dados, $[1, N]$, y la propiedad $\mathcal{P}_{\surd}$ es que el número sea divisible por el primo p.
- Nos interesan los elementos que tengan al menos una propiedad, o sea $|\Omega| - e_0$.
- $N(\supseteq \mathcal{S})$ son los números divisibles por todos los elementos de $\mathcal{S}$, vale decir, los que son divisibles por su producto. La cantidad de números en $[1, N]$ divisibles por m es simplemente $\lfloor N/m \rfloor$.

Especialicemos ahora:

a) **Números hasta 100 divisibles por 2 y 5:** Tenemos:

$$
\begin{aligned}
N_0 &= 100 \\
N_1 &= N(\supseteq \{2\}) + N(\supseteq \{5\}) = 50 + 20 = 70 \\
N_2 &= N(\supseteq \{2, 5\}) = 10
\end{aligned}
$$

La función generatriz es $N(z) = 100 + 70z + 10z^2$, obtenemos $e_0 = E(0) = N(-1) = 40$ y el resultado final $100 - 40 = 60$.

b) **Números hasta N divisibles por p_1, p_2 ó p_3:** Tenemos:

$$
\begin{aligned}
N_0 &= N \\
N_1 &= N(\supseteq \{p_1\}) + N(\supseteq \{p_2\}) + N(\supseteq \{p_3\}) \\
&= \lfloor \frac{N}{p_1} \rfloor + \lfloor \frac{N}{p_2} \rfloor + \lfloor \frac{N}{p_3} \rfloor \\
N_2 &= N(\supseteq \{p_1, p_2\}) + N(\supseteq \{p_1, p_3\}) + N(\supseteq \{p_2, p_3\}) \\
&= \lfloor \frac{N}{p_1 p_2} \rfloor + \lfloor \frac{N}{p_1 p_3} \rfloor + \lfloor \frac{N}{p_2 p_3} \rfloor \\
N_3 &= N(\supseteq \{p_1, p_2, p_3\}) \\
&= \lfloor \frac{N}{p_1 p_2 p_3} \rfloor
\end{aligned}
$$

Conociendo estos valores tenemos $N(z)$, y el resultado final nuevamente es $N - N(-1) = N - (N_0 - N_1 + N_2 - N_3) = N_1 - N_2 + N_3$.

45. Para demostrar que no es cierto en general, basta exhibir un contraejemplo:

$$6 \cdot 9 \equiv 1 \cdot 9 \pmod{15}$$

Para que se pueda cancelar c debe ser una unidad de $\mathbb{Z}_m$, o sea $\gcd(c, m) = 1$.

46. Como 31 es primo y $31 \not| 29$, es aplicable el teorema de Fermat:

$$29^{3965} \equiv (-2)^{132 \cdot 30 + 5} \equiv (-2)^5 \equiv -32 \equiv -1 \equiv 30 \pmod{31}$$

47. *a*) Demostraremos la implicación en cada dirección por separado.
Primeramente, suponemos $\gcd(a, b) = 1$, queremos demostrar que $\gcd(a^2, b^2) = 1$. Usamos el hecho que $\gcd(x, y) = \gcd(y, x)$ y que si tenemos $\gcd(x, y) = \gcd(x, z) = 1$, entonces $\gcd(x, yz) = 1$. Aplicando esto con $x = a$ e $y = z = b$ nos queda $\gcd(a, b^2) = 1$, y aplicándola nuevamente ahora con $x = b^2$ e $y = z = a$ obtenemos $\gcd(a^2, b^2) = 1$.
Otra manera es demostrarlo por contradicción. Si $\gcd(a^2, b^2) > 1$, sabemos que hay un primo que lo divide, llamémosle p. Como $p \mid \gcd(a^2, b^2)$, debe ser $p \mid a^2$ y $p \mid b^2$, pero entonces $p \mid a$ y $p \mid b$ por las propiedades de los primos, y en consecuencia $p \mid 1$. Esto es absurdo.
Por el otro lado, si $\gcd(a^2, b^2) = 1$, existen $s, t \in \mathbb{Z}$ tales que:

$$\begin{aligned} s \cdot a^2 + t \cdot b^2 &= 1 \\ (sa) \cdot a + (tb) \cdot b &= 1 \end{aligned}$$

En esta última expresión sa y tb son enteros, lo que nos asegura que $\gcd(a, b) = 1$.

b) Sea $d = \gcd(a, b)$. En tal caso:

$$\gcd(a/d, b/d) = 1$$

Entonces, usando las propiedades del máximo común divisor y el resultado anterior:

$$\begin{aligned} \gcd(a^2, b^2) &= \gcd(d^2 \cdot (a/d)^2, d^2 \cdot (b/d)^2) \\ &= d^2 \cdot \gcd((a/d)^2, (b/d)^2) \\ &= d^2 \\ &= (\gcd(a, b))^2 \end{aligned}$$

ya que $\gcd(a/d, b/d) = 1$, y aplicando lo anterior $\gcd((a/d)^2, (b/d)^2) = 1$.
Nótese que esto no puede aplicarse en reversa, por ejemplo $\gcd(8, 12) = 4 = 2^2$), pero ni 8 ni 12 son cuadrados perfectos.
Además, se puede hacer exactamente lo mismo con otras potencias.

Una manera adicional de demostrar las anteriores es descomponer a y b en sus factores primos, y expresar $\gcd(a, b)$ en términos de éstos.

48. Siempre podemos escribir:

$$\begin{aligned} ax + b &\equiv c \pmod{m} \\ ax &\equiv c - b \pmod{m} \end{aligned}$$

De partida, si $\gcd(a, m) = 1$, a tiene inverso multiplicativo módulo m y la solución es $(c - b) \cdot a^{-1}$. Si $m \mid a$, no hay solución a menos que $m \mid c - b$, en cuyo caso cualquier x sirve. Si $\gcd(a, m) \neq 1$, debe ser que $\gcd(a, m) \mid c - b$ también (porque nos queda $ax + my = c - b$), o no hay solución posible.

Una manera simple de resumir todo lo anterior es:

- Si $m \mid a$ y $m \mid b - c$, todo $x \in \mathbb{Z}$ es solución.
- Si $\gcd(a, m) \not| b - c$, no hay solución posible.

49. Hay dos maneras de proceder acá:

    Trabajosa: Podemos expandir:

    $$(a+b)^p = \sum_{0 \leq k \leq p} \binom{p}{k} a^{p-k} b^k$$

    Ahora, como:

    $$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

    tenemos que p divide al coeficiente binomial para $1 \leq k \leq p-1$, con lo que todos los términos de la suma (salvo los extremos) son divisibles por p, y:

    $$(a+b)^p \equiv a^p + b^p \pmod{p}$$

    Astuta: El teorema de Fermat asegura que si $p \nmid u$, entonces:

    $$u^{p-1} \equiv 1 \pmod{p}$$

    Cuando $p \mid u$, tenemos $u \equiv 0 \pmod{p}$. O sea, *siempre* se cumple:

    $$u^p \equiv u \pmod{p}$$

    Aplicando esto resolver el problema es trivial:

    $$\begin{aligned} (a+b)^p &\equiv a + b \pmod{p} \\ &\equiv a^p + b^p \pmod{p} \end{aligned}$$

50. Esto corresponde a:

    $$\begin{aligned} 5n + 1 &\equiv 0 \pmod{7} \\ 3n - 4 &\equiv 0 \pmod{5} \end{aligned}$$

    O sea:

    $$\begin{aligned} 5n &\equiv 6 \pmod{7} \\ 3n &\equiv 4 \pmod{5} \end{aligned}$$

    pero

    $$\begin{aligned} 5 \cdot 3 &\equiv 1 \pmod{7} \\ 3 \cdot 2 &\equiv 1 \pmod{5} \end{aligned}$$

    y resulta:

    $$\begin{aligned} n &\equiv 6 \cdot 3 \equiv 4 \pmod{7} \\ n &\equiv 4 \cdot 2 \equiv 3 \pmod{5} \end{aligned}$$

    Esto se resuelve apelando al teorema chino de los residuos:

    $$\begin{aligned} m_1 &= 5 \cdot 5^{-1} = 5 \cdot 3 \quad \text{en } \mathbb{Z}_7 \\ &= 15 \\ m_2 &= 7 \cdot 7^{-1} = 7 \cdot 3 \quad \text{en } \mathbb{Z}_5 \\ &= 21 \end{aligned}$$

    y tenemos finalmente:

    $$\begin{aligned} n &\equiv 15 \cdot 4 + 21 \cdot 3 \pmod{7 \cdot 5} \\ &\equiv 18 \pmod{35} \end{aligned}$$

51. Primeramente, como $10 \equiv 1 \pmod{9}$, es $10^r \equiv 1 \pmod{9}$, lo que demuestra la equivalencia.

    El efectuar las operaciones de la forma que se indica para verificar es efectuarlas módulo 9, lo que justifica el método.

    Como $10 \equiv -1 \pmod{11}$, tenemos $10^r \equiv (-1)^r \pmod{11}$, y resulta la equivalencia indicada.

    El mecanismo de verificación será entonces reducir los datos al rango 0 a 10 usando la fórmula indicada, y efectuar los cálculos verificando contra la reducción del resultado.

    Si, tiene sentido usar ambos. Si aplicamos el primero, el resultado es correcto módulo 9; aplicando el segundo, es correcto módulo 11. Por el teorema chino de los residuos, si ambos cuadran es que el resultado es correcto módulo $9 \cdot 11 = 99$.

52. Evaluar el polinomio módulo $m_1 m_2 \ldots m_r$ es evaluarlo en $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_r}$, donde será cero exactamente cuando es cero en cada uno de los $\mathbb{Z}_{m_i}$, y combinando las raíces de todas las maneras posibles se obtiene lo pedido.

53. Primeramente, $\phi(16) = 8$. También, usando el teorema de Euler:

$$\begin{aligned}
45 &\equiv -3 \pmod{16} \\
45^{17} &\equiv (-3)^1 \pmod{16} \\
&\equiv -3 \pmod{16} \\
31 &\equiv -1 \pmod{16} \\
31^9 &\equiv (-1)^1 \pmod{16} \\
&\equiv -1 \pmod{16}
\end{aligned}$$

    y finalmente:

$$\begin{aligned}
45^{17} + 31^9 &\equiv -3 - 1 \pmod{16} \\
&\equiv -4 \pmod{16} \\
&\equiv 12 \pmod{16} \\
(45^{17} + 31^9) \bmod 16 &= 12
\end{aligned}$$

54. Hay pq números de 1 a pq, de los cuales p son múltiplos de q y q son múltiplos de p, y hay un único múltiplo de ambos. O sea, hay en total

$$\begin{aligned}
pq - q - p + 1 &= p(q-1) - q + 1 \\
&= (p-1)(q-1)
\end{aligned}$$

    números relativamente primos a pq, y $\phi(pq) = (p-1)(q-1)$.

55. De la factorización dada sabemos que $\phi(52) = \phi(4) \cdot \phi(13) = 2 \cdot 12 = 24$.

    En $\mathbb{Z}_{52}$, y usando el teorema de Euler:

$$\begin{aligned}
55 &\equiv 3 \pmod{52} \\
55^{50} &\equiv 3^{50} \pmod{52} \\
&\equiv 3^{2 \cdot 24} \cdot 3^2 \pmod{52} \\
&\equiv 3^2 \pmod{52} \\
&\equiv 9 \pmod{52}
\end{aligned}$$

56. Primeramente, $16 = 2^4$, con lo que $\phi(16) = 2^{4-1}(2-1) = 8$. También tenemos que $\gcd(33, 16) = \gcd(25, 16) =$

1, y podemos aplicar el teorema de Euler. Así:

$$\begin{aligned}
33^{193} &\equiv 1^{193} \pmod{16} \\
&\equiv 1 \pmod{16} \\
25^9 &\equiv 9^9 \pmod{16} \\
&\equiv 9^8 \cdot 9 \pmod{16} \\
&\equiv 9 \pmod{16} \\
33^{193} + 25^9 &\equiv 1 + 9 \pmod{16} \\
&\equiv 10 \pmod{16}
\end{aligned}$$

57. Primeramente, $\phi(1) = 1$, que es impar. Luego sabemos que si $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ con los p_i primos distintos, entonces

$$\phi(n) = p_1^{k_1 - 1}(p_1 - 1) p_2^{p_2 - 1}(p_2 - 1) \dots p_r^{k_r - 1}(p_r - 1)$$

Ahora bien, todos los números primos (salvo 2) son impares, por lo que si p_i es un primo impar aporta el factor par $p_i - 1$. En consecuencia, n no puede tener factores primos impares, y $n = 2^k$ para algún $k \geq 1$. Pero $\phi(2^k) = 2^{k-1}(2 - 1) = 2^{k-1}$, que es impar únicamente si $k = 1$. Por tanto, los únicos casos en que $\phi(n)$ es impar son $\phi(1) = \phi(2) = 1$.

58. *a*) No hay mucho más que explicar en este método.

    Funciona bien si el número sólo tiene factores primos chicos (o para eliminar éstos en preparación a usar alguno de los otros).

    b) Por el teorema chino de los residuos, calcular un polinomio módulo n es lo mismo que calcularlo módulo los factores de n. La idea entonces es detectar ciclos módulo los factores, cosa que se hace mediante el algoritmo de Floyd.

    Este método es muy efectivo si el número a factorizar tiene un factor relativamente pequeño.

    c) Por el teorema de Fermat, si p es primo y $p \not| \, a$, entonces $a^{p-1} \equiv 1 \pmod{p}$. O sea, para todo k, $p \mid a^{k(p-1)} - 1$. La idea es construir m con muchos factores primos (por ejemplo, un factorial o el producto de los primos hasta cierto límite) con la esperanza que $p - 1 \mid m$, en cuyo caso $p \mid a^m - 1$, y podemos obtener un factor no trivial de n calculando $\gcd(a^m \bmod n - 1, n)$.

    Este método es muy efectivo si $p - 1$ sólo tiene factores primos chicos.

    d) El método de Fermat se basa en la factorización:

$$\begin{aligned}
n &= uv \\
&= x^2 - y^2 \\
n + y^2 &= x^2
\end{aligned}$$

    donde $u = x + y$ y $v = x - y$. La idea es entonces calcular $n + 1^2$, $n + 2^2$, ..., $n + k^2$ hasta caer en un cuadrado perfecto.

    Este método es muy efectivo cuando n tiene dos factores cercanos entre sí.

59. No pueden ser pares a y b, ya que en tal caso $\gcd(a, b)$ sería al menos 2. Las posibilidades restantes son:

    - Tanto a como b son impares: En este caso, $a + b$ y $a - b$ son ambos pares, y $\gcd(a + b, a - b) = 2$.
    - Uno de los dos es par, el otro impar: Tanto $a + b$ como $a - b$ son impares, y $\gcd(a + b, a - b) = 1$.

    En mayor detalle, si anotamos:

$$\begin{aligned}
u &= a + b \\
v &= a - b
\end{aligned}$$

tenemos que:

$$\begin{aligned} u + v &= 2a \\ u - v &= 2b \end{aligned}$$

De la identidad de Bézout sabemos que hay s y t tales que

$$sa + tb = 1$$

Combinando esto con lo anterior nos queda:

$$\begin{aligned} s(u + v) + t(u - v) &= 2(ta + sb) \\ &= 2 \end{aligned}$$

Esta es una combinación lineal de u y v, y por tanto $\gcd(a + b, a - b) \mid 2$. Como 2 es primo, las únicas posibilidades son 1 y 2. Para $a = 3$, $b = 1$ tenemos $\gcd(3 + 1, 3 - 1) = \gcd(4, 2) = 2$; para $a = 2$, $b = 1$ queda $\gcd(2 + 1, 2 - 1) = \gcd(3, 1) = 1$, con lo que ambas se dan.

60. Como $22 = 2 \cdot 11$, y ninguno de sus factores primos divide a 175, sabemos que $\gcd(22, 175) = 1$. Así, 22 tiene inverso multiplicativo módulo 175. Si lo tiene 22, lo tiene también cualquier potencia de 22, en particular $22^{12\,007}$.

61. Lo aseverado puede expresarse en términos de congruencia como $a^p \equiv a \pmod{p}$. Del teorema de Fermat sabemos que si $p \not| a$, entonces $a^{p-1} \equiv 1 \pmod{p}$, por lo que en tal caso $a^p \equiv a \pmod{p}$. Por otro lado, si $p \mid a$, quiere decir que $a \equiv 0 \pmod{p}$, y en tal caso también $a^p \equiv a \pmod{p}$.

62. Se define $\phi(m)$ como el número de valores entre 1 y m que son relativamente primos a m.

63. Basta mostrar un ejemplo, como $3 \cdot 4 \equiv 6 \cdot 4 \equiv 0 \pmod{12}$, pero $3 \not\equiv 6 \pmod{12}$.

64. Como $360 = 2^3 \cdot 3^2 \cdot 5$, tenemos $\phi(360) = 2^2\,(2 - 1) \cdot 3^1\,(3 - 1) \cdot 5^0\,(5 - 1) = 96$.

65. Demostramos por inducción sobre n que F_n y F_{n+1} son relativamente primos.

    Base: Cuando $n = 0$, tenemos $F_n = 0$ y $F_{n+1} = 1$, que ciertamente son relativamente primos.

    Inducción: Suponiendo que F_n y F_{n+1} son relativamente primos, buscamos demostrar que lo son F_{n+1} y F_{n+2}.

    Si son relativamente primos F_n y F_{n+1}, hay constantes enteras s y t tales que:

    $$\begin{aligned} 1 &= sF_n + tF_{n+1} \\ F_n &= (1 - tF_{n+1})/s \end{aligned}$$

    Substituyendo en la recurrencia:

    $$\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ &= F_{n+1} + (1 - tF_{n+1})/s \\ 1 &= sF_{n+2} + (t - s)F_{n+1} \end{aligned}$$

    En consecuencia, como tanto s como $t - s$ son enteros, $\gcd(F_{n+1}, F_{n+2}) = 1$. Son relativamente primos como se quería demostrar.

    Por inducción, para todo n, F_n y F_{n+1} son relativamente primos.

66. Siguiendo la pista se obtiene:

    $$a_n u^n + a_{n-1} u^{n-1} v + \ldots + a_0 v^n = 0$$

    Si esta ecuación la consideramos módulo u, queda:

    $$\begin{aligned} a_0 v^n &\equiv 0 \pmod{u} \\ a_0 &\equiv 0 \pmod{u} \end{aligned}$$

Lo último sigue ya que $\gcd(u, v) = 1$, con lo que v^n tiene inverso módulo u. De forma similar:

$$\begin{aligned} a_n u^n &\equiv 0 \pmod{v} \\ a_n &\equiv 0 \pmod{v} \end{aligned}$$

Las congruencias indicadas no son más que otra forma de decir que $u \mid a_0$ y $v \mid a_n$.

Nótese que esto reduce la búsqueda de raíces racionales de polinomios a un conjunto finito de candidatos. Más aún, si $a_n = 1$ esto nos asegura que las raíces racionales son todas enteras. Esto nos da una demostración simple de que las raíces de los naturales o son enteras o son irracionales (considérese $x^n - a = 0$).

67. Supongamos que hay una raíz $x = u/v$, con $\gcd(u, v) = 1$. Siguiendo la pista, se obtiene:

$$u^n + a_{n-1}u^{n-1}v + \ldots + a_0 v^n = 0$$

Del segundo término en adelante todos los términos de esto son divisibles por v, por lo que debe serlo el primero. Como $\gcd(u, v) = 1$, las únicas posibilidades son $v = \pm 1$, en cuyo caso x es un entero como debía demostrarse.

68. Primeramente, $16 = 2^4$, con lo que $\phi(16) = 2^{4-1}(2 - 1) = 8$. Tenemos que $\gcd(33, 16) = \gcd(25, 16) = 1$, y podemos aplicar el teorema de Euler. Así:

$$\begin{aligned} 33^{193} &\equiv 1^{193} \pmod{16} \\ &\equiv 1 \pmod{16} \\ 25^9 &\equiv 9^9 \pmod{16} \\ &\equiv 9^8 \cdot 9 \pmod{16} \\ &\equiv 9 \pmod{16} \\ 33^{193} + 25^9 &\equiv 1 + 9 \pmod{16} \\ &\equiv 10 \pmod{16} \end{aligned}$$

69. Si $\gcd(a, b^2) = 1$, de la identidad de Bézout sabemos que hay $s, t \in \mathbb{Z}$ tales que $1 = s \cdot a + t \cdot b^2$, y éste es el mínimo valor positivo posible de esta expresión. Pero entonces $1 = s \cdot a + (tb) \cdot b$, y claramente no puede haber valor positivo menor para una expresión de la forma $s' \cdot a + t' \cdot b$, y así $\gcd(a, b) = 1$.

Otra forma de demostrarlo es usando las propiedades de gcd: Sabemos que si $\gcd(a, b) = 1$ y $\gcd(a, c) = m$, entonces $\gcd(a, bc) = m$. Aplicando esto a la situación dada con $c = b$ y $(m = 1$, resulta directamente $\gcd(a, b^2) = 1$.

70. Esto se traduce en las siguientes congruencias:

$$\begin{aligned} 5n + 2 &\equiv 0 \pmod{3} \\ n &\equiv 2 \pmod{3} \\ 7n - 3 &\equiv 0 \pmod{5} \\ n &\equiv 4 \pmod{5} \end{aligned}$$

Por el teorema chino de los residuos, como $\gcd(3, 5) = 1$ hay una solución única módulo $3 \cdot 5 = 15$. Tenemos, en la notación del apunte:

$$\begin{array}{ll} s_3 = (15/3)^{-1} = 5^{-1} = 2 \text{ en } \mathbb{Z}_3 & m_3 = (15/3) \cdot s_3 = 10 \\ s_5 = (15/5)^{-1} = 3^{-1} = 2 \text{ en } \mathbb{Z}_5 & m_5 = (15/5) \cdot s_5 = 6 \end{array}$$

En consecuencia $n \equiv 10 \cdot 2 + 6 \cdot 4 \equiv 14 \pmod{15}$.

71. *a*) Igual que para el caso de los enteros, consideremos el conjunto $I = \{n(x) - c(x) \cdot d(x) : c(x) \text{ polinomio}\}$. Este conjunto no es vacío, contiene el polinomio $n(x) = n(x) - 0 \cdot d(x)$. Por tanto, contiene un polinomio de grado mínimo, llamémosle $r(x)$, y consecuentemente hay $q(x)$ tal que $n(x) = q(x) \cdot d(x) + r(x)$.

Primero demostraremos por contradicción que $\deg(r(x)) < \deg(d(x))$. Supongamos que $\deg(r(x)) \geq \deg(d(x))$. En tal caso podemos restar múltiplos de $d(x)$ a $r(x)$ para eliminar el término de mayor grado, y obtendríamos

$$r'(x) = r(x) - m(x) \cdot d(x) = n(x) - (q(x) + m(x)) \cdot d(x) \in I$$

con $r'(x)$ de menor grado que $r(x)$, lo cual contradice la elección de éste.

Para demostrar que $q(x)$ y $r(x)$ son únicos, supongamos que hay dos juegos distintos:

$$\begin{aligned} n(x) &= q'(x) \cdot d(x) + r'(x) \\ &= q''(x) \cdot d(x) + r''(x) \end{aligned}$$

Pero entonces:

$$(q''(x) - q'(x)) \cdot d(x) = r''(x) - r'(x)$$

Analizando el grado del lado derecho tenemos que $\deg(r''(x) - r'(x)) \leq \text{máx}(\deg(r'(x), r''(x))) < \deg(d(x))$. Si $q''(x) - q'(x)$ no es cero, el grado del lado izquierdo es a lo menos $\deg(d(x))$, lo cual es una contradicción. Por tanto, $q'(x) = q''(x)$, y por tanto también $r'(x) = r''(x)$.

b) Al multiplicar polinomios, el término de mayor grado se obtiene de multiplicar los términos de mayor grado de ellos. Si los coeficientes de éstos son 1, lo es el coeficiente del término de mayor grado del resultado. Por otro lado, como se indica en el enunciado, en $\mathbb{Q}$ siempre es posible dividir un polinomio por el coeficiente de su término de mayor grado dando un polinomio mónico. En particular se puede hacer esto con los factores del polinomio dado, y por lo anterior sólo el producto de factores así normalizados puede dar un resultado mónico.

c) Procedemos por contradicción. Sea $N(x)$ un polinomio mónico de grado mínimo que no puede descomponerse en un producto de polinomios irreducibles. En particular, $N(x)$ no es irreducible (sería el producto de un único polinomio irreducible), y puede escribirse $N(x) = A(x) \cdot B(x)$, con $1 < \deg(A(x)), \deg(B(x) < \deg(N(x))$. Por la parte 71*b*, podemos suponer que $A(x)$ y $B(x)$ son mónicos, y al tener grados menores que el de $N(x)$, pueden escribirse como productos de polinomios irreducibles. Pero entonces lo es el producto de ambos, o sea $N(x)$, lo que contradice su misma definición.

72. Si $ax + by = c$ es una ecuación lineal donde a, b y c son coeficientes enteros, por las propiedades del máximo común divisor sabemos que debe ser $\gcd(a, b) \mid c$. Si esto no se cumple, no hay solución posible.

Sea ahora $d = \gcd(a, b)$, y $d \mid c$. Por la identidad de Bézout sabemos que hay s, t tales que $sa + tb = d$. Multiplicando por c/d, que por hipótesis es un entero, tenemos que:

$$\frac{sc}{d} \cdot a + \frac{tc}{d} \cdot b = c$$

Así tenemos una solución:

$$\begin{aligned} x_0 &= \frac{sc}{d} \\ y_0 &= \frac{tc}{d} \end{aligned}$$

La relación entre x e y es lineal, para entero k y enteros u, v debe ser algo como:

$$\begin{aligned} x &= x_0 - ku \\ y &= y_0 + kv \end{aligned}$$

Substituyendo en nuestra ecuación original:

$$\begin{aligned} a \cdot (x_0 - ku) + b \cdot (y_0 + kv) &= (ax_0 + by_0) - (aku - bkv) \\ &= c - k(au - bv) \end{aligned}$$

Para que sea solución debe cumplirse $au = bv$, y nos interesan los mínimos valores posibles de u y v. Tenemos:

$$\frac{a}{b} = \frac{v}{u}$$

Al reducir la fracción a/b a sus mínimos términos, queda:

$$\frac{a/d}{b/d} = \frac{v}{u}$$

y queda finalmente:

$$x = x_0 - k \cdot \frac{b}{d}$$
$$y = y_0 + k \cdot \frac{a}{d}$$

como se aseveraba. Estas son todas las soluciones.

73. Cada uno en turno:

   a) Se requiere el inverso de 5 módulo 14, es $5^{-1} = 3$, y resulta:

   $$\begin{aligned} 3 \cdot 17 - 4/5 &= 3 \cdot 3 - 4 \cdot 3 \\ &= 9 - 12 \\ &= -3 \\ &= 11 \end{aligned}$$

   b) Como $\gcd(6, 14) = 2$, 6 no tiene inverso y esta expresión no puede evaluarse.

   c) Como $\gcd(7, 14) = 7$, 7 no tiene inverso y esta expresión no puede evaluarse. ¡No se dejen engañar por $21/7 = 3$ en $\mathbb{Z}$!

74. Como estamos trabajando en un anillo, podemos usar la operatoria algebraica acostumbrada, teniendo cuidado al dividir eso sí. La ecuación lineal $ax + b = c$ tiene solución única $x = (c - b) \cdot a^{-1}$ si a es unidad. En caso que no lo sea pueden haber múltiples soluciones o ninguna.

   a) Tenemos:

   $$\begin{aligned} 3x + 10 &= 7 \\ 3x &= 12 \end{aligned}$$

   Como 3 no es unidad, probamos las distintas alternativas y resulta $x \in \{4, 9, 14\}$

   b) Tenemos:

   $$\begin{aligned} 4x - 5 &= 8 \\ 4x &= 13 \end{aligned}$$

   Ahora 4 es unidad, con $4^{-1} = 4$, y resulta $x = 13 \cdot 4 = 7$.

   c) Tenemos:

   $$\begin{aligned} 5x + 11 &= 0 \\ 5x &= 4 \end{aligned}$$

   Como 5 no es unidad, probamos y vemos que no hay solución.

75. En un anillo finito, un elemento o es una unidad o es un divisor de cero. Y los elementos de $\mathbb{Z}_m$ que son unidades son aquellos que son relativamente primos a m. Es fácil calcular así:

   - Como 24 es compuesto, en $\mathbb{Z}_{24}$ son unidades $\{1, 5, 7, 11, 13, 17, 19, 23\}$ (los relativamente primos a 24), los demás son divisores de cero. Este anillo no es un campo.
   - Como 31 es primo, todos los números entre 1 y 30 son relativamente primos a 31, y todos ellos son unidades de $\mathbb{Z}_{31}$. El único divisor de cero es 0. Esto es un campo.

76. No todos los elementos tienen raíz cuadrada. Un programa entrega:

- Para $\mathbb{Z}_{24}$:

a	$\sqrt{a}$
0	$\{0, 12\}$
1	$\{1, 5, 7, 11, 13, 17, 19, 23\}$
4	$\{2, 10, 14, 22\}$
9	$\{3, 9, 15, 21\}$
12	$\{6, 18\}$
16	$\{4, 8, 16, 20\}$

  Nótese que las raíces cuadradas se pueden agrupar en pares que son inversos aditivos. En el caso de 0, nótese que $-0 = 0$ y $-12 = 12$.

- Para $\mathbb{Z}_{31}$:

a	$\sqrt{a}$
0	$\{0\}$
1	$\{\ 1, 30\}$
2	$\{\ 8, 23\}$
4	$\{\ 2, 29\}$
5	$\{\ 6, 25\}$
7	$\{10, 21\}$
8	$\{15, 16\}$
9	$\{\ 3, 28\}$
10	$\{14, 17\}$
14	$\{13, 18\}$
16	$\{\ 4, 27\}$
18	$\{\ 7, 24\}$
19	$\{\ 9, 22\}$
20	$\{12, 19\}$
25	$\{\ 5, 26\}$
28	$\{11, 20\}$

  En este caso se aprecia que salvo cero, todos los elementos que tienen raíces cuadradas tienen dos, y que son inversos aditivos. En general, para m primo las raíces cuadradas siempre vendrán en pares (salvo 0), y por tanto exactamente la mitad de los elementos no nulos tendrán raíz cuadrada. El caso $m = 2$ es particular, pero la aseveración anterior igual se cumple.

77. Si tomamos la fórmula para las raíces de la ecuación cuadrática:

$$\begin{aligned} ax^2 + bx + c &= 0 \\ x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

y substituimos en la ecuación, vemos que es una identidad (como debiera serlo), y en el proceso usamos únicamente operaciones válidas en un anillo (salvo posiblemente cancelar factores comunes entre numerador y denominador de fracciones, cosa que es válida sólo si son unidades) Por otro lado, las operaciones posiblemente sospechosas en la fórmula son la raíz (vimos que no siempre existe, y de existir pueden haber no sólo dos) y la división por $2a$. Formalmente, las raíces de la ecuación dada son:

$$x = \frac{-1 + \sqrt{1 - 4}}{2} = \frac{-1 + \sqrt{-3}}{2}$$

En los casos indicados:

$\mathbb{Z}_{24}$: Acá $-3 = 21$, que no tiene raíz cuadrada. No hay soluciones.

$\mathbb{Z}_{26}$: Tenemos $-3 = 23$, que tiene raíces cuadradas ± 7. Pero 2 no tiene inverso en $\mathbb{Z}_{26}$, la fórmula no es aplicable. Recurrimos a probar por fuerza bruta, y no hay soluciones.

$\mathbb{Z}_{31}$**:** Tenemos $-3 = 28$, que tiene las raíces cuadradas 11 y 20. Además $2^{-1} = 16$, así que:

$$\begin{aligned} x &= \frac{-1 \pm \sqrt{-3}}{2} \\ &= 16 \cdot (-1 \pm 11) \\ &= \begin{cases} 5 \\ 25 \end{cases} \end{aligned}$$

78. Usamos los teoremas de Fermat y Euler para simplificar los cálculos.

   a) Como 41 es primo, es aplicable Fermat, $7^{40} \equiv 1 \pmod{41}$:

   $$7^{401} \bmod 41 = 7 \bmod 41 \qquad = 7$$

   b) Acá 45 no es primo, es aplicable el teorema de Euler. Como $45 = 3^2 \cdot 5$, tenemos $\phi(45) = 3 \cdot (3-1) \cdot (5-1) = 24$. Pero $\gcd(50, 45) = 5$, así que hay que irse con cuidado...

   $$\begin{aligned} 50^{50} \bmod 45 &= 25^{50} \cdot 2^{50} \bmod 45 \\ &= 5^{100} \cdot 2^2 \bmod 45 \\ &= 5^{100} \cdot 4 \bmod 45 \end{aligned}$$

   Veamos las potencias de 5 en $\mathbb{Z}_{45}$:

   $$\begin{aligned} 5^1 &= 5 \\ 5^2 &= 25 \\ 5^3 &= 35 \\ 5^4 &= 40 = -5 \end{aligned}$$

   ¡Bien! Esto simplifica las cosas:

   $$\begin{aligned} 5^{100} &= \left(5^4\right)^{25} \\ &= (-1)^{25} \cdot (5)^{25} \\ &= -1 \cdot \left(5^{24}\right) \cdot 5 \\ &= -5 \cdot \left(5^4\right)^6 \\ &= -5 \cdot (-5)^6 \\ &= -5 \cdot (-1)^6 \cdot 5^6 \\ &= -5 \cdot 5^4 \cdot 5^2 \\ &= -5 \cdot (-5) \cdot 5^2 \\ &= 5^2 \cdot 5^2 \\ &= 5^4 \\ &= -5 \\ &= 40 \end{aligned}$$

   Para nuestro valor original tenemos entonces:

   $$50^{50} \bmod 45 = 5^{100} \cdot 4 \bmod 45 = 40 \cdot 4 \bmod 45 = 25$$

79. Sea x el número de alumnos del curso del profesor Carroll. El enunciado indica:

   $$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Como 3, 5 y 7 son relativamente primos, es aplicable el teorema chino de los residuos. En los términos del apunte, $m = 3 \cdot 5 \cdot 7 = 105$, y nuestra solución será única módulo 105. Usando el módulo como subíndice:

$$\begin{aligned} s_3 &= (5 \cdot 7)^{-1} = (2 \cdot 1)^{-1} = 2^{-1} = 2 \text{ en } \mathbb{Z}_3 \\ m_3 &= 2 \cdot 5 \cdot 7 = 70 \\ s_5 &= (3 \cdot 7)^{-1} = (3 \cdot 2)^{-1} = 6^{-1} = 1 \text{ en } \mathbb{Z}_5 \\ m_5 &= 1 \cdot 3 \cdot 7 = 21 \\ s_7 &= (3 \cdot 5)^{-1} = 1^{-1} = 1 \text{ en } \mathbb{Z}_7 \\ m_7 &= 1 \cdot 3 \cdot 5 = 15 \end{aligned}$$

Substituyendo en la fórmula:

$$x = 70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 = 233 \equiv 23 \pmod{105}$$

Seguramente hay 23 estudiantes en el curso, aunque podrían ser 128 también…

80. Vemos que la ecuación es exactamente la identidad de Bézout, así que aplicando el algoritmo extendido de Euclides tenemos la solución:

$$119 \cdot (-10) + 399 \cdot 3 = 7$$

Ahora bien, si tenemos:

$$as + bt = m$$

con $m = \gcd(a, b)$, y buscamos otras soluciones a esta ecuación, serán de la forma:

$$\begin{aligned} a(s + x) + b(t - y) &= m \\ ax - by &= 0 \\ \frac{a}{m} \cdot x &= \frac{b}{m} \cdot y \end{aligned}$$

Esto lleva a concluir que:

$$\begin{aligned} x &= k \cdot \frac{b}{m} \\ y &= k \cdot \frac{a}{m} \end{aligned}$$

En nuestro caso:

$$\begin{aligned} 119 \cdot \left(-10 + k \cdot \frac{399}{7}\right) + 399 \cdot \left(3 - k \cdot \frac{119}{7}\right) &= 7 \\ 119 \cdot (-10 + 57k) + 399 \cdot (3 - 17k) &= 7 \end{aligned}$$

81. El criterio de ceros racionales es que si:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \tag{4}$$

con $a_n \neq 0$ y $a_0 \neq 0$, y los a_i no tienen factores comunes, entonces un cero racional r de (4) debe cumplir:

$$r = \frac{u}{v}$$

donde $u \mid a_0$ y $v \mid a_n$. En el caso del problema las únicas posibilidades son $u = \pm 1$ y $v = \pm 1$, con lo que los únicos candidatos a ceros racionales son $r = \pm 1$. Pero ninguno de los dos es un cero, por lo que los ceros son ambos irracionales. En particular, el cero positivo es irracional.

82. Analizamos la ecuación de Pell, $x^2 - dy^2 = 1$, con $d \in \mathbb{N}$. Nos restringimos a soluciones en $\mathbb{N}_0$, ya que podemos elegir cualquier signo para x e y.

a) Si d es un cuadrado perfecto, digamos $d = a^2$, quedaría:

$$x^2 = (ay)^2 + 1$$

Pero los únicos cuadrados que difieren en uno son 0 y 1, la solución trivial $x = 1$, $y = 0$. No hay otras soluciones.

b) Podemos reescribir la ecuación como:

$$x \cdot x - (dy) \cdot y = 1$$

Así tenemos que el máximo común divisor de x e y divide a 1, con lo que $\gcd(x, y) = 1$.

83. Sabemos que $\mathbb{Z}_7$ es un campo, ya que 7 es primo. Por la ecuación para las raíces de una cuadrática:

$$\begin{aligned} x &= \frac{-3 \pm \sqrt{3^2 - 4 \cdot 4 \cdot 4}}{2 \cdot 4} \\ &= \frac{4 \pm \sqrt{1}}{1} \\ &= 4 \pm 1 \end{aligned}$$

Verificando, tanto $x = 3$ como $x = 5$ cumplen.

84. Nos interesa demostrar que:

$$2^{2^{n+1}} \equiv 1 \pmod{p}$$

pero que ningún exponente menor da 1, vale decir

$$2^{2^n} \not\equiv 1 \pmod{p}$$

Como $p \mid F_n$ tenemos que:

$$\begin{aligned} 2^{2^n} + 1 &\equiv 0 \pmod{p} \\ 2^{2^n} &\equiv -1 \pmod{p} \\ \left(2^{2^n}\right)^2 &\equiv (-1)^2 \pmod{p} \\ 2^{2^{n+1}} &\equiv 1 \pmod{p} \end{aligned}$$

Esto es exactamente lo solicitado, y $\operatorname{ord}_p(2) = 2^{n+1}$.

85. Por inducción sobre n.

Base: Cuando $n = 0$, se reduce a:

$$F_0 = 2^{2^0} + 1 = 2$$

lo que ciertamente se cumple.

Inducción: Suponiendo que vale para n:

$$\begin{aligned} \prod_{0 \le k \le n+1} F_k + 2 &= \prod_{0 \le k \le n} F_k \cdot F_{n+1} + 2 \\ &= (F_n - 2) \cdot F_{n+1} + 2 \\ &= (2^{2^n} - 2) \cdot (2^{2^{n+1}} + 1) + 2 \\ &= 2^{2^n(1+2)} + 2^{2^{n+1}} - 2^{2^n(2+1)} - 1 + 2 \\ &= 2^{2^{n+1}} + 1 \end{aligned}$$

Exactamente el caso $n + 1$.

Por inducción, vale para $n \in \mathbb{N}_0$.

86. Cada punto en turno.

   a) Como p es un primo impar, $|\mathbb{Z}_p^*| = p - 1$ es par. Los elementos de $\mathbb{Z}_p^*$ pueden representarse como las potencias r^1 hasta r^{p-1}, de las cuales exactamente la mitad es par (dando residuos cuadráticos) y la otra mitad impar (dando no-residuos cuadráticos).

   b) En el fondo, lo que dice el símbolo de Legendre es:

   $$\left(\frac{r^k}{p}\right) = (-1)^k$$

   Sea $a = r^m$, $b = r^n$, de donde:

   $$\left(\frac{ab}{p}\right) = (-1)^{m+n} = (-1)^m \cdot (-1)^n = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

   c) Tenemos:

   $$\left(\frac{a}{p}\right) = \left(\frac{r^m}{p}\right) = (-1)^m$$

   Pero también:

   $$\begin{aligned} r^{(p-1)/2} &\equiv -1 \pmod{p} \\ r^{m(p-1)/2} &\equiv (-1)^m \pmod{p} \\ a^{(p-1)/2} &\equiv \left(\frac{a}{p}\right) \pmod{p} \end{aligned}$$

87. Sea c un divisor común de $a + b$ y $a - b$. Entonces c divide a:

   $$\begin{aligned} (a + b) + (a - b) &= 2a \\ (a + b) - (a - b) &= 2b \end{aligned}$$

   Por Bézout, sabemos que hay enteros u y v tales que:

   $$\begin{aligned} au + bv &= 1 \\ (2a)u + (2b)v &= 2 \end{aligned}$$

   En consecuencia:

   $$\gcd(a + b, a - b) \mid 2$$

   y tenemos nuestro resultado.

   Corresponde completar vía demostrar que ambas opciones son posibles. Consideremos:

   $$\begin{aligned} \gcd(2, 1) &= 1 \\ \gcd(2 + 1, 2 - 1) &= 1 \\ \gcd(3, 1) &= 1 \\ \gcd(3 + 1, 3 - 1) &= 2 \end{aligned}$$

88. Bastante directo:

   a) Si expresamos $a = p_1 p_2 \dots p_r$ y $b = q_1 q_2 \dots q_s$, con los p_i y q_j primos no necesariamente distintos, vemos que $\gcd(a, b) = 1$ significa que los conjuntos de primos son disjuntos.

   En la factorización de c^n todo primo debe aparecer n veces, por lo que debe aparecer n veces en ab, y por lo anterior aparece n veces en a o en b, y ambos son n-ésimas potencias perfectas.

b) Factoricemos el lado derecho:

$$x^3 = y(y+1)$$

Pero $\gcd(y, y+1) = 1$, por 88*a* tanto y como $y+1$ son cubos perfectos. Los únicos cubos sucesivos son $-1, 0, 1$, lo que da $y = -1, x = 0$ o $y = 0, x = 0$ como únicas soluciones.

89. Tenemos la identidad de Gauß:

$$\sum_{d \mid n} \phi(d) = n$$

Por inversión de Möbius:

$$\begin{aligned} \phi(n) &= \sum_{d \mid n} \mu(d) \frac{n}{d} \\ &= n \sum_{d \mid n} \frac{\mu(d)}{d} \end{aligned}$$

La función $\iota_{-1}(n) = 1/n$ claramente es multiplicativa, aplicando el resultado citado:

$$\phi(n) = n \prod_k \left(1 - \frac{1}{p_k}\right)$$

90. Por completar

91. Queremos demostrar que $10a + b \equiv 0 \pmod{19}$ si y solo si $a + 2b \equiv 0 \pmod{19}$.

Demostramos una secuencia de si y solo si. Partiendo con la segunda equivalencia:

$$a + 2b \equiv 0 \pmod{19}$$

Multiplicando por 10:

$$\begin{aligned} 10a + 20b &\equiv 0 \pmod{19} \\ 10a + b &\equiv 0 \pmod{19} \end{aligned}$$

El paso de multiplicación por 10 podemos revertirlo, al ser $\gcd(10, 19) = 1$ sabemos que 10 tiene inverso en $\mathbb{Z}_{10}$. (Es simple ver que $2 \cdot 10 \equiv 1 \pmod{19}$).

92. De la fórmula para la suma geométrica sabemos que:

$$\sum_{0 \le k < n} a^k = \frac{a^n - 1}{a - 1}$$

En consecuencia, si a es entero $(a-1) \mid (a^n - 1)$. Vale decir, $a^n - 1$ solo puede ser primo para $n \ge 2$ si $a - 1 = 1$, o sea $a = 2$; o es $n = 1$ y $a - 1$ primo.

Ahora bien, para $a = 2$, si n es compuesto, digamos $n = rs$, tenemos:

$$2^n - 1 = (2^r)^s - 1$$

que es el mismo caso analizado antes, con $a = 2^r$, y esta expresión es divisible por $2^r - 1$, con lo que no es prima.

Los primeros casos en que la expresión no es un primo son:

$$\begin{aligned} 2^{11} - 1 &= 23 \cdot 89 \\ 2^{23} - 1 &= 47 \cdot 178\,481 \\ 2^{29} - 1 &= 233 \cdot 1\,103 \cdot 2\,089 \\ 2^{37} - 1 &= 223 \cdot 616318177 \\ 2^{41} - 1 &= 3367 \cdot 164\,511\,353 \end{aligned}$$

93. Tenemos las congruencias:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

Como los módulos son relativamente primos, el teorema chino de los residuos nos asegura que hay una solución única módulo $3 \cdot 4 \cdot 5 = 60$.

Nos interesan:

En $\mathbb{Z}_3$: Tenemos $m_3 = 60/3 = 20$, $20^{-1} = 2^{-1} = 2$. Resulta $s_3 = 2 \cdot 20 = 40$.
En $\mathbb{Z}_4$: Tenemos $m_4 = 60/4 = 15$, $15^{-1} = 3^{-1} = 3$. Resulta $s_3 = 3 \cdot 15 = 45$.
En $\mathbb{Z}_5$: Tenemos $m_5 = 60/5 = 12$, $12^{-1} = 2^{-1} = 3$. Resulta $s_3 = 3 \cdot 12 = 36$.

Con esto la solución a las recurrencias es:

$$\begin{aligned} x &\equiv 40 \cdot 1 + 45 \cdot 2 + 36 \cdot 3 \pmod{60} \\ &\equiv 238 \pmod{60} \\ &\equiv 58 \pmod{60} \end{aligned}$$

Vemos que este valor cumple las tres congruencias.

94. Supongamos $\gcd(a, b) = 1$. Esto significa que a y b no tienen factores primos en común, o sea $\omega(ab) = \omega(a) \cdot \omega(b)$. Pero entonces:

$$\begin{aligned} \gamma(ab) &= (-1)^{\omega(ab)} \\ &= (-1)^{\omega(a)+\omega(b)} \\ &= (-1)^{\omega(a)} \cdot (-1)^{\omega(b)} \\ &= \gamma(a) \cdot \gamma(b) \end{aligned}$$

y la función es multiplicativa.

Incidentalmente, a una función como ω se le llama *aditiva*.

95. Por turno.

a) Si $d = a^2$ podemos factorizar:

$$x^2 - a^2y^2 = (x - ay)(x + ay) = 1$$

Sin pérdida de generalidad, podemos suponer que las variables no son negativas. O sea, $x - ay = \pm 1$ y $x + ay = \mp 1$. Pero $x + ay = 1$ solo es posible si $x = 1$ e $y = 0$, la solución trivial.

b) Sabemos que para todo $u, v \in \mathbb{Z}$ es:

$$\min_{u,v \in \mathbb{Z}} \{ux + by\} = \gcd(x, y)$$

Podemos escribir la ecuación de Pell como:

$$x^2 - dy^2 = x \cdot x - dy \cdot y = 1$$

con lo que $\gcd(x, y) = 1$. Son relativamente primos.

c) Primero notamos que:

$$\begin{aligned} (u + v\sqrt{d}) \cdot (x + y\sqrt{d}) &= (ux + vyd) + (uy + vy)\sqrt{d} \\ (u - v\sqrt{d}) \cdot (x - y\sqrt{d}) &= (ux + vyd) - (uy + vy)\sqrt{d} \end{aligned}$$

con lo que si:

$$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n$$

también es:

$$x_n - y_n\sqrt{d} = (x_0 - y_0\sqrt{d})^n$$

Pero en tal caso, multiplicando ambas:

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + y_n\sqrt{d}) \cdot (x_n - y_n\sqrt{d}) \\ &= (x_0 + y_0\sqrt{d})^n \cdot (x_0 - y_0\sqrt{d})^n \\ &= (x_0^2 - dy_0^2)^n \\ &= 1 \end{aligned}$$

y se confirma lo aseverado.

7. Criptografía

1. Por completar
2. Por completar
3. Por completar
4. Por turno.

   a) Bob envía $(c_1, c_2) = (g^y, m \cdot s)$ a Alice. Alice calcula:

   $$s = c_1^x = h^{xy}$$

   Este valor coincide con s calculado por Bob.

   $$m' = c_2 \cdot s^{-1} = m \cdot s \cdot s^{-1} = m$$

   Alice recupera el mensaje original.

   b) Si conocemos $(c_1, c_2) = (g^y, m \cdot s)$ y m, podemos obtener s. Con este valor de s podemos decifrar otros mensajes que reusan y.

5. Requiere computación...
6. En el campo $\mathbb{Z}_p$ un polinomio de grado $k-1$ puede tener a lo más $k-1$ raíces. Si definimos un polinomio $g(x)$ de grado $k-1$ que coincide con $f(x)$ en los k puntos $(x_i, f(x_i))$ que aportan k participantes, coincide con $f(x)$, y podemos obtener $s = a_0 = g(0)$.

   Si menos de k participantes aportan sus puntos, no se determina el polinomio, y el valor de s queda en el secreto.

   Otra manera de enfrentar esto es que k puntos dan un sistema de k ecuaciones en las k incógnitas a_{k-1}, a_{k-2}, $\dots a_0$, con lo que se determina a_0. Con menos de k puntos no hay suficientes ecuaciones para determinar a_0.

7. En $\mathbb{Z}_p$, tenemos lo que hace Alice:

   $$h = r^x$$

   Lo que hace Bob es:

   $$\begin{aligned} c_1 &= r^y \\ s &= h^y \\ &= r^{xy} \\ c_2 &= m \cdot s \end{aligned}$$

   Para descifrar, Alice hace lo siguiente:

   $$\begin{aligned} s' &= c_1^x \\ &= (r^y)^x \\ &= r^{xy} \\ &= s \\ m' &= c_2 \cdot (s')^{-1} \\ &= (m \cdot s) \cdot (s)^{-1} \\ &= m \end{aligned}$$

8. Expresamos las operaciones de RSA en términos del isomorfismo entre $\mathbb{Z}_n$ y $\mathbb{Z}_p \oplus \mathbb{Z}_q$. El exponente de descifrado d cumple con $ed \equiv 1 \pmod{(p-1)(q-1)}$. El mensaje debe ser menor que n, por lo que $0 < k < q$ en este caso.

Cifrar: Para cifrar el mensaje $m \rightsquigarrow (m_p, m_q)$, calculamos $m^e \bmod n \rightsquigarrow (m_p^e, m_q^e)$. En nuestro caso tenemos $m = kp$, con lo que $(kp)^e \rightsquigarrow (0, (kp)^e)$.

Descifrar: Para descifrar el mensaje cifrado $c \rightsquigarrow (c_p, c_q)$ calculamos $c^d \rightsquigarrow (c_p^d, c_q^d)$. Como $(p-1)(q-1) \mid de-1$, sabemos que $q - 1 \mid de - 1$. En nuestro caso, esto es:

$$\begin{aligned}(0, c_q^d) &= \big(0, ((kp)^e)^d\big) \\ &= \big(0, (kp)^{ed-1} \cdot kp\big) \\ &= (0, kp)\end{aligned}$$

Lo último sigue del teorema de Fermat dado que q y kp son relativamente primos. Por el teorema chino de los residuos, hay exactamente un mensaje posible módulo $n = pq$, y es $m = kp$.

El mensaje se descifra correctamente.

9. Cada punto por turno.

   a) Si cooperan k de los participantes, conocen k pares $(s \bmod m_i, m_i)$, por el teorema chino de los residuos pueden determinar s módulo el producto de los m_i que poseen. Pero el producto de k de los m_i es mayor que s (ya que es mayor que el producto de los k menores), con lo que éste queda determinado.

   b) Si participan menos de k, se conoce s sólo módulo el producto de sus m_i, que por hipótesis es menor a s (el producto de los $k - 1$ mayores es menor que s), con lo que s no queda determinado en forma única.

10. Consideremos las propuestas de sistemas de Turing en turno, primero dados mensajes desconocidos m_1, m_2, ... que se cifran dando respectivamente c_1, c_2, ... (ataque de mensajes desconocidos). Luego consideramos el caso de un mensaje conocido m con su texto cifrado c (ataque de mensaje conocido).

Versión 1: Mensajes desconocidos: Sabemos que:

$$\begin{aligned}c_1 &= m_1 \cdot k \\ c_2 &= m_2 \cdot k \\ c_3 &= m_3 \cdot k\end{aligned}$$

Podemos obtener k mediante $\gcd(c_1, c_2)$. En rigor, lo que sabemos es que $k \mid \gcd(c_1, c_2)$, pero dados suficientes mensajes (o pudiendo adivinar lo suficiente de los mensajes para eliminar factores espurios) fácilmente obtenemos k.

Mensaje conocido: En este caso la solución es trivial: $k = c/m$.

Versión 2: Mensajes desconocidos: El ataque anterior no ayuda en este caso.

Mensaje conocido: Sabiendo m y $c = m \cdot k$ en $\mathbb{Z}_p$, podemos calcular $k = c \cdot m^{-1}$ sin problemas.

8. Combinatoria elemental

1. Suponenos el alfabeto inglés, de 26 letras.

   En el primer caso, tenemos una secuencia de 4 elementos tomados entre $26 - 5 = 21$:

   $$21^4 = 194\,481$$

   Al permitir una única vocal, tenemos dos caminos:

   - Razonar que por simetría cualquiera de las 4 posiciones de la vocal da el mismo número, y son alternativas exhaustivas y excluyentes. En el orden vocal y tres consonantes por la regla del producto son $5 \cdot 21^3$ posibilidades. Por simetría:

     $$4 \cdot 5 \cdot 21^3 182\,220$$

     Esto se agrega a las anteriores (regla de la suma, nuevamente):

     $$21^4 + 4 \cdot 5 \cdot 21^3 = 379\,701$$

   - Razonar que podemos describir los códigos extra como una secuencia que indica la vocal (5 opciones), las 3 consonantes (21^3 posibilidades) y la posición de la vocal (1 entre 4):

     $$5 \cdot 21^3 \cdot \binom{4}{1}$$

     Se completa igual que el otro caso.

2. Cada propuesta por turno.

   a) La patente en este caso es una secuencia de 4 letras y 3 dígitos, para un total de

   $$26^4 \cdot 10^3 = 456\,976\,000$$

   b) Que los dígitos estén en las últimas 3 posiciones o otras 3 posiciones cualquiera no afecta el número de posibilidades, son las mismas que en el caso 2*a*:

   $$26^4 \cdot 10^3 = 456\,976\,000$$

   c) Acá elegimos 4 consonantes y 3 dígitos, y luego las posiciones para los 3 dígitos entre las 7 posiciones totales:

   $$21^4 \cdot 10^3 \cdot \binom{7}{3} = 6\,806\,835\,000$$

   d) Hay dos posibilidades excluyentes:

   La patente no contiene dígitos: En caso de una patente de largo k, estamos eligiendo una secuencia de k letras, lo que da

   $$26^k$$

   Para los largos posibles queda

   $$\sum_{3 \leq k \leq 6} 26^k = 26^3 \sum_{0 \leq k \leq 3} 26^k = 26^3 \cdot \frac{26^4 - 1}{26 - 1} = 321\,271\,704$$

La patente contiene un dígito: Si es de largo k, estamos eligiendo una secuencia de $k-1$ letras y 1 dígito, y luego debemos elegir la posición del dígito entre las k posibilidades:

$$26^{k-1} \cdot 10 \cdot \binom{k}{1} = 26^{k-1} \cdot 10 \cdot k$$

Para los largos permitidos:

$$\sum_{3 \leq k \leq 6} 26^{k-1} \cdot 10 \cdot k = 26^2 \cdot 10 \sum_{0 \leq k \leq 3} 26^k (k+3) = 736\,454\,680$$

Por la regla de la suma, el total de patentes personalizadas es

$$26^3 \cdot \frac{26^4 - 1}{26 - 1} + 26^2 \cdot 10 \sum_{0 \leq k \leq 3} 26^k (k+3) = 1\,057\,726\,384$$

3. Un subconjunto del multiconjunto está determinado por el número de elementos de cada tipo. Podemos describir cada subconjunto mediante una secuencia de k valores, el i-ésimo de ellos entre 0 y n_i. Por lo tanto, el número total de subconjuntos es:

$$\prod_{1 \leq i \leq k} (n_i + 1)$$

Siguiendo el desarrollo en el apunte, el número buscado es el número de soluciones del sistema de inecuaciones:

$$\begin{aligned} x_1 + x_2 + \cdots + x_k &= m \\ 0 \leq x_i &\leq n_i \end{aligned}$$

No hay una fórmula simple para esto

4. Cada punto en turno.

   a) Un sándwich puede describirse mediante una secuencia que da el tipo de pan (2 opciones) y el contenido (3 opciones). Por la regla del producto, son $2 \cdot 3 = 6$ posibilidades.

   b) La merienda del jugador queda descrita por una secuencia formada por el sándwich (6 opciones, por lo anterior), la bebida (2 opciones) y la fruta (3 opciones). Por la regla del producto, son $6 \cdot 2 \cdot 3 = 36$ alternativas.

   c) Una manera de calcular esto es razonar comno sigue: Pueden elegirse tres sabores distintos, o dos del mismo sabor y un tercero, o tres sabores iguales. Estas tres alternativas son exhaustivas y excluyentes, podemos calcularlas por separado y sumar (regla de la suma). Así:

   Tres sabores diferentes: Esto es simplemente elegir 3 entre 17, o sea $\binom{17}{3}$.

   Dos sabores diferentes: Acá importa cuál es el que se repìte (dos de vainilla y uno de pistacho es distinto de uno de vainilla y dos de pistacho). Podemos representarlo mediante una secuencia que da el que se repite y el otro, que debe ser diferente del primero. Por la regla del producto son $17 \cdot 16$ opciones.

   Tres del mismo sabor: Podemos elegir ese sabor de 17 maneras.

   En resumen, el número total de porciones de helado que pueden servirse son:

   $$\binom{17}{3} + 17 \cdot 16 + 17 = 969$$

   d) Esto lo calculamos ya como parte del caso anterior. Es elegir 3 sabores entre 17, o sea:

   $$\binom{17}{3} = 680$$

5. Cada juego por turno.

a) Una pieza de dominó puede considerarse como un subconjunto de 2 de los 7 números, a lo que hay que agregar los repetidos ("chanchos"). Por la regla de la suma, son

$$\binom{7}{2} + 7 = 28$$

b) De forma similar, un triomino puede considerarse un conjunto de 3 valores tomados entre 6. A esto hay que agregar las situaciones con dos valores repetidos, corresponde a una secuencia que da el valor repetido (1 entre 6) y el tercer valor (1 entre 5). Y finalmente hay que agregar el caso de tres valores repetidos (1 entre 6). Por la regla de la suma:

$$\binom{6}{3} + \binom{6}{1} \cdot \binom{5}{1} + \binom{6}{1} = 56$$

6. Siguiendo la pista, vemos que:

$$x_1 + x_2 + \cdots + x_{k+1} = n - 1$$

Acá las variables tienen la única restricción que $x_i \geq 0$. Por tanto, las soluciones están dadas por el número de multiconjuntos de $n-1$ elementos tomados entre $k+1$:

$$\left(\!\!\binom{k+1}{n-1}\!\!\right) = \binom{n-1+k+1-1}{k+1-1} = \binom{n+k-1}{k}$$

7. Por la regla de la suma, esto es el número total de permutaciones menos las que contienen cada una de las palabras prohibidas. Por suerte no tienen subpalabras en común.

El número de permutaciones de las 26 letras es $26!$; el número de permutaciones que contienen una secuencia dada de n letras es $(26 - n + 1)!$, con lo que el número buscado es

$$26! - (21! + 23! + 2 \cdot 24!) = 402\,024\,661\,215\,458\,100\,019\,200\,000$$

8. Basta construir una secuencia que incluye las condiciones:

- Primera letra: 2
- Segunda y tercera letra: 26
- Primer dígito: 2
- Segundo dígito: 1
- Tercer dígito: 2
- Cuarto dígito: 9

Por la regla del producto: $2 \cdot 26 \cdot 26 \cdot 2 \cdot 1 \cdot 2 \cdot 9 = 48\,672$.

9. Cada situación por turno:

- Sin restricciones: Simplemente $12! = 479\,001\,600$.
- Si hay 4 tareas prioritarias, y las demás se hacen después: Es una secuencia con la secuencia de las primeras 4 tareas, y luego las otras 8, la regla del producto da $4! \cdot 8! = 967\,680$ ordenamientos posibles.
- Si hay tres grupos, el mismo razonamiento da $4! \cdot 5! \cdot 3! = 17\,280$ órdenes.

10. Por completar

11. Sabemos que $P(n, r) = n^{\underline{r}}$, basta aplicar las identidades para potencias factoriales:

$$P(n+1, r) = (n+1)^{\underline{r}} = (n+1) \cdot n^{\underline{r-1}} = (n+1) \cdot \frac{n^{\underline{r}}}{n-r+1} = \frac{n+1}{n-r+1} \cdot n^{\underline{r}} = \frac{n+1}{n-r+1}\, P(n, r)$$

12. Cada cual por turno, usando la identidad $P(n, r) = n^{\underline{r}}$:

a) Basta plantear la ecuación, expandiendo las potencias factoriales:

$$\begin{aligned} n(n-1) &= 90 \\ n^2 - n - 90 &= 0 \end{aligned}$$

Las raíces de esta cuadrática son $n = -9$ y $n = 10$. Permutar -9 elementos no tiene sentido, $n = 10$.

b) Nuevamente plantear la ecuación:

$$\begin{aligned} n(n-1)(n-2) &= 3n(n-1) \\ n^3 - 6n^2 + 5n &= 0 \end{aligned}$$

Soluciones de esta ecuación son $n = 0$, $n = 1$ y $n = 5$.

c) Igual a las anteriores:

$$\begin{aligned} 2n(n-1) + 50 &= 2n(2n-1) \\ 2n^2 - 50 &= 0 \end{aligned}$$

Por inspección $n = \pm 5$, como permutar -5 elementos no tiene sentido es $n = 5$.

13. Claramente se requieren 5 pasos hacia arriba y 17 a la derecha, o sea tenemos un multiconjunto $\{A^5, D^17\}$, lo que nos da:

$$\binom{5+17}{5\ 17} = 26\,334$$

Esta idea es fácil de generalizar: Debemos dar $x_2 - x_1 + 1$ pasos a la derecha y $y_2 - y_1 + 1$ pasos hacia arriba, lo que da:

$$\binom{x_2 - x_1 + y_2 - y_1 + 2}{x_2 - x_1 + 1}$$

14. Hay un total de $m+n$ movidas, de las cuales exactamente m son hacia el norte. Podemos elegir las posiciones de las movidas hacia el norte de $\binom{m+n}{m}$ maneras diferentes.

Mediante el Tao, esto es permutar m letras N y n letras E, lo que da:

$$\frac{(m+n)!}{m!n!} = \binom{m+n}{m}$$

Igual que antes.

15. Sin restricciones, es una secuencia de un elemento con 9 opciones (el primer dígito) y luego 5 de 10 opciones:

$$9 \cdot 10^5 = 900\,000$$

Si no se permiten repeticiones, hay 9 opciones para el primer dígito, 9 para el segundo, 8 para el tercero, etc. O sea $9 \cdot 9^{\underline{5}} = 136\,080$ posibilidades.

16. Por completar

17. Hay 26 letras en el alfabeto inglés (MS-DOS no hace diferencia entre mayúsculas y minúsculas), a lo que se suman 10 dígitos. Para el nombre propiamente tal son entre 1 y 8 caracteres, para la extensión entre 0 y 3. Para contar todas las secuencias de entre m y n elementos de entre a opciones:

$$\begin{aligned} \sum_{m \le k \le n} a^k &= \sum_{0 \le k \le n} a^k - \sum_{0 \le k \le m-1} a^k \\ &= \frac{a^{n+1} - 1}{a - 1} - \frac{a^m - 1}{a - 1} \\ &= \frac{a^{n+1} - a^m}{a - 1} \end{aligned}$$

El nombre mismo es una secuencia de estas dos cosas:

$$\frac{36^9 - 36^1}{36 - 1} \cdot \frac{36^4 - 36^1}{36 - 1} = 139\,250\,307\,444\,539\,652$$

18. Igual que el caso anterior, básicamente:

$$\frac{126^{15} - 126^1}{126 - 1} = 319\,408\,025\,254\,357\,014\,550\,350\,413\,952$$

19. Por completar

20. Cada caso por turno.

- Podemos representar estas manos como una secuencia de los valores de cada una de las 4 pintas (13 cada una), el valor y la pinta de la quinta carta (12 valores, 4 pintas). Pero la quinta carta repite una de las pintas anteriores, es un mapa 2 a 1:

$$\frac{1}{2} \cdot 13^4 \cdot (12 \cdot 4) = 685\,464$$

  Para la probabilidad hay que dividir esto por el número total de posibilidades:

$$\frac{13^4 \cdot (12 \cdot 4)}{2\binom{52}{5}} = 0{,}264$$

- Si no aparecen los tréboles, estamos eligiendo 5 cartas entre $52 - 13 = 39$. La probabilidad es:

$$\frac{\binom{39}{5}}{\binom{52}{5}} = 0{,}221$$

- Si sólo aparecen 3 pintas, es que falta una. Esto es sumar el resultado anterior para cada una de las pintas:

$$\frac{4 \cdot \binom{39}{5}}{\binom{52}{5}} = 0{,}886$$

21. Por turno.

a) Un polinomio mónico de grado n está determinado por los coeficientes a_0 hasta a_{n-1}, n en total, que se eligen independientemente. Es una secuencia de n elementos tomados entre p, resulta:

$$T_n = p^n$$

b) Todos los polinomios de grado 1 son irreductibles:

$$N_1 = T_1 = p$$

c) Los polinomios de grado 2 reductibles son el producto de dos factores lineales, que pueden ser iguales (hay $T_1 = p$ posibilidades) o son diferentes (en cuyo caso estamos eligiendo dos entre N_1, para $\binom{N_1}{2}$). Por la regla de la suma, los reductibles en total son:

$$N_1 + \binom{N_1}{2}$$

con lo que los irreductibles son:

$$N_2 = T_2 - \left(N_1 + \binom{N_1}{2}\right) = p^2 - \left(p + \frac{p(p-1)}{2}\right) = \frac{p(p-1)}{2} = \binom{p}{2}$$

d) Un polinomio cúbico reductible es:

- El producto de tres factores lineales diferentes, elegimos 3 entre N_1
- Tres factores lineales, dos iguales y el otro diferente. Esto queda representado por un par indicando el cuadrado y el factor simple, $N_1 \cdot N_1$
- El producto de un factor lineal y uno cuadrático irreductible, $N_1 \cdot N_2$.

Por la regla de la suma, los reductibles son la suma de estos; los irreductibles son:

$$N_3 = T_3 - \left(\binom{N_1}{3} + N_1^2 + N_1 \cdot N_2\right) = p^3 - \left(\binom{p}{3} + p^2 + p \cdot \frac{p(p-1)}{2}\right) = \frac{p^3 - p}{3}$$

22. Por completar

23. Los valores entre el trío y el par no pueden repetirse, ya que hay sólo 4 cartas de cada valor. Así, hay una biyección entre las manos de interés secuencias que describen:

- El valor del trío, se elige 1 entre 13
- Las pintas de las cartas del trío, se eligen 3 entre 4
- El valor del par, se elige 1 entre 12 (no puede coincidir con el trío)
- Las pintas del par, se eligen 2 entre 4

En consecuencia, por la regla del producto el valor buscado es:

$$\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{12}{1} \cdot 42 = 3\,744$$

24. La palabra `CHUPACABRAS` como multiconjunto es $\{\mathtt{A}^3, \mathtt{B}, \mathtt{C}^2, \mathtt{H}, \mathtt{P}, \mathtt{R}, \mathtt{S}, \mathtt{U}\}$

a) Como son 11 letras en total:

$$\binom{11}{3\ 1\ 2\ 1\ 1\ 1\ 1\ 1} = \frac{11!}{3!\,2!} = 3\,326\,400$$

b) Esto es considerar `SAP` como una nueva "letra," con lo que el multiconjunto es $\{\mathtt{SAP}, \mathtt{A}^2, \mathtt{B}, \mathtt{C}^2, \mathtt{H}, \mathtt{R}, \mathtt{U}\}$, con un total de $11 - 3 + 1 = 9$ símbolos:

$$\binom{9}{1\ 2\ 1\ 2\ 1\ 1\ 1} = \frac{9}{2!\,2!} = 90\,720$$

c) Si las vocales $\{\mathtt{A}^3, \mathtt{U}\}$ están juntas, hay

$$\binom{4}{3\ 1} = \frac{4!}{3!\,1!} = 4$$

combinaciones de vocales, que cuentan como un símbolo; y quedan $11 - 4 + 1 = 8$ símbolos por ordenar:

$$\binom{8}{1\ 1\ 1\ 1\ 1\ 1\ 1\ 1} \cdot \binom{4}{3\ 1} = 8! \cdot \frac{4!}{3!} = 161\,280$$

25. El término para i, j, k de la suma corresponde a elegir i de entre r, j entre s y k entre t. La condición es que $i + j + k = n$, por lo que al considerar todas las opciones estamos eligiendo n elementos en total entre $r + s + t$.

26. Por completar

27. El lado izquierdo suma las formas de elegir $0, 1, \ldots, n$ elementos de un conjunto de n, o sea, el número total de subconjuntos de un conjunto de n elementos, exactamente lo que expresa el lado derecho.

28. Una manera de verlo es escribir los valores con palitos, o sea por ejemplo $3 = |||$. Lo que estamos haciendo es dividir un grupo de 17 palitos en 3 grupos separados por signos $+$, sin que queden grupos vacíos. Esto es distribuir 3 signos $+$ en las $17 - 1 = 16$ posiciones entre palitos. Resultan ser:

$$\binom{17-1}{3} = 560$$

En general, si la suma es n y hay k variables, el número de soluciones es

$$\binom{n-1}{k}$$

29. Primeramente, una escala queda descrita por su punto de partida en valor y su pinta. Un trío queda descrito por el valor y las pintas de las tres cartas.

   a) **Una escala** y tres cartas adicionales

   Quedan descritas por secuencias:

   - Valor de la primera carta de la escala; si hay más de 4 cartas seguidas, la primera de éstas (uno de 13)
   - Pinta de la escala (una de 4)
   - Tres cartas adicionales (3 de entre $52 - 4 = 48$)

   O sea, son

   $$13 \cdot \binom{4}{1} \cdot \binom{48}{3}$$

   b) **Dos tríos** y una carta adicional

   Existe la posibilidad de tener 4 cartas del mismo valor, situación que hay que manejar aparte. Esto queda descrito por:

   - Valor del trío (1 de 13)
   - Pintas del trío (3 de 4)
   - Valor del cuarteto (1 de 12)

   Los otros casos son:

   - Los valores de los tríos (2 entre 13)
   - Las pintas del trío de menor valor (3 entre 4)
   - Las pintas del trío de mayor valor (3 entre 4)
   - La carta adicional, excluyendo las que completarían cuartetos (1 entre $52 - 4 - 4 = 44$

   En resumen,

   $$13 \cdot 12 \cdot \binom{4}{3} + \binom{13}{2} \cdot \binom{4}{3} \cdot \binom{4}{3} \cdot \binom{44}{1}$$

   c) **Una escala y un trío** sin cartas adicionales

   Quedan descritos por dos tipos de secuencias. Si el trío no incluye cartas de la pinta de la escala:

   - El valor de la primera carta de la escala (1 entre 13)
   - La pinta de la escala (1 entre 4)
   - El valor del trío (1 entre 13)
   - Las pintas del trío (3 entre 3)

   Si incluye una carta de la misma pinta de la escala:

   - El valor de la primera carta de la escala (1 entre 13)
   - La pinta de la escala (1 entre 4)
   - El valor del trío (1 entre $13 - 4 = 9$)

- Las otras dos pintas del trío (2 entre 3)

Esto hace un total de:

$$13 \cdot \binom{4}{1} \cdot 13 \cdot \binom{3}{3} + 13 \cdot \binom{4}{1} \cdot 9 \cdot \binom{3}{2}$$

30. Punto a punto:

a) Son secuencias de n elementos, cada uno de los cuales se puede elegir de 3 formas:

$$3^n$$

b) Según el tao de `BOOKKEEPER`, esto es simplemente:

$$\frac{n!}{i!j!k!} = \binom{n}{i\ j\ k}$$

c) Siguiendo la receta dada, tenemos:

$$3^n = \sum_{i+j+k=n} \binom{n}{i\ j\ k}$$

Esto lamentablemente no es nada nuevo, considere $x = y = z = 1$ en:

$$(x + y + z)^n = \sum_{i+j+k=n} \binom{n}{i\ j\ k} x^i y^j z^k$$

31. Esto es contar por filas y columnas. Sea $S = \{(x, y) \colon x \text{ estudió con } y\}$. Contando por filas (hombres) tenemos $40 \cdot 6 = 240$, lo que debe coincidir a contar por columnas (mujeres), que es $m \cdot 5 = 240$. Así, $m = 48$, y hay $40 + 48 = 88$ estudiantes en total en el curso.

32. Como multiconjunto es $\{\mathtt{I}^4, \mathtt{M}, \mathtt{P}^2, \mathtt{S}^4\}$, para un total de 11 letras. Se pueden ordenar de

$$\binom{11}{4\ 1\ 2\ 4} = \frac{11!}{4!\, 2!\, 4!} = 34\,650$$

maneras.

Las consonantes pueden ordenarse entre sí de

$$\binom{7}{1\ 2\ 4} = \frac{7!}{2!\, 4!} = 105$$

maneras, y podemos ubicar las consonantes juntas en 5 posiciones diferentes, con las `I` ocupando las otras 4; dando un total de

$$\binom{5}{1} \cdot \binom{7}{1\,2\,4} = 5 \cdot \frac{7!}{2!\, 4!} = 525$$

formas.

33. Suponiendo que la escala no “da la vuelta”, podemos describir esta situación mediante una secuencia que da:

- El valor de la primera carta, que puede tomarse de $13 - 6 + 1 = 8$ maneras (`A` a `6` hasta `8` a `K`)
- Las pintas de las 6 cartas, cada una de las cuales se puede elegir independientemente de entre 4, para un total de 4^6

Por ejemplo, tenemos la correspondencia:

$$(2, \heartsuit, \heartsuit, \spadesuit, \clubsuit, \diamondsuit, \clubsuit) \leftrightarrow \{2\heartsuit, 3\heartsuit, 4\spadesuit, 5\clubsuit, 6\diamondsuit, 7\clubsuit\}$$

En total, hay

$$8 \cdot 4^6 = 32\,768$$

maneras.

Si aceptamos que la escala "dé la vuelta", como en

$$(9, \clubsuit, \heartsuit, \spadesuit, \diamondsuit, \diamondsuit, \spadesuit) \leftrightarrow \{9\clubsuit, 10\heartsuit, J\spadesuit, K\diamondsuit, A\diamondsuit, 2\spadesuit\}$$

hay 13 puntos de partida posibles, y son

$$13 \cdot 4^6 = 53\,248$$

manos diferentes.

34. Esto se resuelve contando por filas y columnas. Sea $S = \{(x, y) \colon x \text{ e } y \text{ estudiaron juntos}\}$. Si llamamos m al número de mujeres en el curso, el enunciado dice:

$$\begin{aligned} \sum_x r_x(S) &= 32 \cdot 5 \\ \sum_y c_y(S) &= m \cdot 8 \end{aligned}$$

Ambos deben ser iguales:

$$\begin{aligned} 32 \cdot 5 &= m \cdot 8 \\ m &= 20 \end{aligned}$$

con lo que hay $20 + 32 = 52$ estudiantes en el curso.

35. Son 10 letras en total: $\{\mathtt{E}^2, \mathtt{G}, \mathtt{I}^2, \mathtt{L}^2, \mathtt{N}, \mathtt{P}, \mathtt{R}\}$ Hay

$$\binom{10}{2\ 1\ 2\ 2\ 1\ 1\ 1} = \frac{10!}{2!\,2!\,2!} = 453\,600$$

Hay 6 consonantes ($\{\mathtt{G}, \mathtt{L}^2, \mathtt{N}, \mathtt{P}, \mathtt{R}\}$) y 4 vocales ($\{\mathtt{E}^2, \mathtt{I}^2\}$). Las vocales pueden ordenarse entre sí de

$$\binom{4}{2\ 2}$$

formas. Si consideramos las vocales como una superletra, tenemos un total de

$$\binom{7}{1\ 1\ 2\ 1\ 1\ 1}$$

manera de ordenar los símbolos; y considerando los distintos órdenes de las vocales el número pedido es

$$\binom{7}{1\ 1\ 2\ 1\ 1\ 1} \cdot \binom{4}{2\ 2} = \frac{7!}{2!} \cdot \frac{4!}{2!2!} = 15\,120$$

36. Una mano de poker de éstas se describe mediante una secuencia que da:

- Las pintas de los 3 ases, se eligen 3 entre 4
- Las otras dos cartas, se eligen 2 entre $52 - 4 = 48$.

Por ejemplo:

$$\langle \{\spadesuit, \heartsuit, \diamondsuit\}, \{2\clubsuit, 5\spadesuit\} \rangle \leftrightarrow \{A\spadesuit, A\diamondsuit, 2\clubsuit, A\heartsuit, 5\spadesuit\}$$

En consecuencia, el número solicitado es

$$\binom{4}{3} \cdot \binom{48}{2} = 4 \cdot \frac{48 \cdot 47}{1 \cdot 2} = 4\,512$$

37. La palabra `EMBAJADOR` tiene 9 letras, de las que se repite la `A` 2 veces.

    a) Si debe comenzar con `A`, es lo mismo que contar las palabras que se pueden formar con las demás letras. No hay repeticiones en esas 8 letras, es simplemente $8! = 40\,320$.

    b) Como hay dos `A`, el número total de posibilidades es

    $$\frac{9!}{2!} = 181\,440$$

    Si las `A` están juntas, las consideramos como "una sola letra", con lo que tenemos $9 - 1 + 1 = 8$ "letras" diferentes a ordenar, dando

    $$8! = 40\,320$$

    Los casos de interés son todos menos éstos, y resulta

    $$\frac{9!}{2!} - 8! = 181\,440 - 40\,320 = 141\,120$$

    c) Si comienza con una vocal hay varios casos a considerar: Si comienza en `E` o `O`, se repite la `A` en las 8 letras restantes. Cada uno de estos dos casos aporta

    $$\frac{8!}{2!} = 20\,160$$

    La otra opción es que comience con `A`, en cuyo caso entre las otras 8 letras no hay repeticiones, y aporta

    $$8! = 40\,320$$

    Estas tres posibilidades son excluyentes, y podemos aplicar la regla de la suma:

    $$2 \cdot \frac{8!}{2!} + 8! = 2 \cdot 20\,160 + 40\,320 = 80\,640$$

    d) Las vocales juntas forman una "superletra." De las 4 vocales hay 2 que se repiten, y hay

    $$\frac{4!}{2!} = 12$$

    posibilidades para la "superletra." Para una secuencia específica de las vocales, tenemos $9 - 4 + 1 = 6$ símbolos diferentes a ordenar, para $6! = 720$ posibilidades. Considerando los órdenes de las vocales hay

    $$\frac{4!}{2!} \cdot 6! = 12 \cdot 720 = 8\,640$$

    posibilidades en total.

38. Contar los anagramas de `VUVUZELA` se hace con el *Tao de `BOOKKEEPER`*. Ya que hay 8 letras en total, con 2 `V`, 2 `U`, 1 `Z`, 1 `E`, 1 `L` y 1 `A` son simplemente:

$$\begin{aligned} \binom{8}{2\ 2\ 1\ 1\ 1\ 1} &= \frac{8!}{2!2!1!1!1!1!} \\ &= 10\,080 \end{aligned}$$

39. Al ordenar las letras de `JABULANI` (8 letras en total; 2 `A`, 1 cada una de las demás) de forma que comience con una vocal se dan dos situaciones excluyentes:

    a) Comienza con `A`: Debemos ordenar las 7 letras restantes, que no tienen repeticiones. Esto da

    $$7! = 5\,040$$

    posibilidades.

    b) Comienza con `U` o `I`: Estas dos opciones son excluyentes, y dan el mismo número de posibilidades. Deben ordenarse las restantes 7 letras, donde se repiten 2 `A`. Cada caso da

    $$\binom{7}{2\ 1\ 1\ 1\ 1\ 1} = \frac{7!}{2!} = 2\,520$$

    posibilidades.

    En total, usando la regla de la suma, tenemos

    $$7! + 2 \cdot \binom{7}{2\ 1\ 1\ 1\ 1\ 1} = 7! + 2 \cdot \frac{7!}{2!} = 2 \cdot 7! = 10\,080$$

40. Para especificar manos de poker con dos pares se requieren:

    - Los valores de los dos pares, se eligen 2 entre 13
    - Las pintas del par más bajo, se eligen 2 entre 4
    - Las pintas del par más alto, se eligen 2 entre 4
    - El valor de la carta restante, se elige 1 entre 13 - 2
    - La pinta de la carta restante, se elige 1 entre 4

    Una mano queda representada por una secuencia de estos elementos, por la regla del producto:

    $$\binom{13}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \binom{13-2}{1} \cdot \binom{4}{1} = 78 \cdot 6 \cdot 6 \cdot 11 \cdot 4 = 123\,552$$

41. Como multiconjunto de 12 elementos $\{\mathtt{A}, \mathtt{C}, \mathtt{E}^2, \mathtt{I}, \mathtt{O}, \mathtt{P}, \mathtt{R}^2, \mathtt{T}, \mathtt{U}, \mathtt{V}\}$ son

    $$\binom{12}{1\ 1\ 2\ 1\ 1\ 1\ 2\ 1\ 1\ 1} = \frac{12!}{2!\,2!} = 119\,750\,400$$

42. Esto es reordenar el multiconjunto $\{\mathtt{E}, \mathtt{I}^2, \mathtt{M}^2, \mathtt{N}, \mathtt{O}^2, \mathtt{T}, \mathtt{V}\}$.

    a) El número total de órdenes, por el tao de `BOOKKEEPER` es

    $$\binom{10}{1\ 2\ 2\ 1\ 2\ 1\ 1} = 453\,600$$

    b) Si las vocales iguales están juntas, podemos considerar los pares como "supersímbolos," y el número de órdenes es

    $$\binom{8}{1\ 1\ 2\ 1\ 1\ 1\ 1} = 20\,160$$

    c) El número de órdenes en que las `O` no están juntas es el número de órdenes sin restricciones menos los órdenes en que las `O` están juntas, vale decir:

    $$\binom{10}{1\ 2\ 2\ 1\ 2\ 1\ 1} - \binom{9}{1\ 2\ 2\ 1\ 1\ 1\ 1} = 362\,880$$

43. Cada cual por turno.

    a) Una de estas manos es un conjunto de 4 cartas del tipo indicado (en total son $3 \cdot 4 = 12$) y una carta adicional (hay $52 - 12 = 40$ de éstas), esta situación se representa mediante una secuencia de un conjunto de las 4 cartas y la última; o un conjunto de 5 de las cartas indicadas. Estas dos alternativas son disjuntas, y podemos aplicar la regla de la suma:

    $$\binom{12}{4} \cdot 40 + \binom{12}{5}$$

    b) Hay 4 `K` y 4 `Q`, lo que nos interesa se representa mediante el conjunto de pintas de las `K` (2 entre 4), el conjunto de las pintas de las `Q` (nuevamente 2 entre 4), y la carta restante (1 entre $52 - 2 \cdot 4 = 44$), lo que da:

    $$\binom{4}{2} \cdot \binom{4}{2} \cdot 44$$

    c) En caso que las pintas de las `K` y las de las `Q` sean iguales, representamos lo que nos interesa por las pintas de las cartas (2 entre 4), y luego la carta restante (1 entre 44). Resulta:

    $$\binom{4}{2} \cdot 44$$

44. Es sacar 5 cartas de las 52, que da:

    $$\binom{52}{5} = 2\,598\,960$$

    a esto hay que restarle el número de maneras de sacar al menos un par para tener las maneras de hacerlo sin obtener un par. Una mano con al menos un par puede ser una de las siguientes posibilidades excluyentes y exhaustivas:

    Un par y tres cartas diferentes: Lo representamos como una secuencia que da:

    - El valor del par, se elige 1 entre 13.
    - Las pintas del par, se eligen 2 entre 4.
    - El valor de la tercera carta, se elige 1 entre 12
    - La pinta de la tercera carta, se elige 1 entre 4.
    - El valor de la cuarta carta, se elige 1 entre 11
    - La pinta de la cuarta carta, se elige 1 entre 4.
    - El valor de la quinta carta, se elige 1 entre 10
    - La pinta de la quinta carta, se elige 1 entre 4.

    Pero el orden de las tres últimas cartas no importa, hay que dividir por 3!. Resulta:

    $$\frac{1}{3!} \cdot \binom{13}{1} \cdot \binom{4}{2} \cdot \binom{12}{1} \cdot \binom{4}{1} \cdot \binom{11}{1} \cdot \binom{4}{1} \cdot \binom{10}{1} \cdot \binom{4}{1} = 1\,098\,240$$

    Un trío y dos cartas distintas: Secuencia que da el valor del trió (1 entre 12), las pintas del trió (3 entre 4) y las 2 cartas entre las 48 de valor distinto.

    $$\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{48}{2} = 109\,824$$

    Un cuarteto y una carta: Esto es elegir el valor del cuarteto (1 entre 13), y 1 carta restante entre las 48 de valor distinto.

    $$\binom{13}{1} \cdot \binom{48}{1} = 624$$

Dos pares y una carta extra: Secuencia con los valores de los pares (2 entre 13), las pintas del par de menor valor (2 entre 4), las pintas del par de mayor valor (2 entre 4), el valor de la carta extra (1 entre 11) y su punta (1 entre 4):

$$\binom{13}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot \binom{11}{1} \cdot \binom{4}{1} = 123\,552$$

Un trió y un par: Queda representado por el valor del trió (1 entre 13) y sus pintas (3 entre 4), el valor del par (1 entre 12) y sus pintas (2 entre 4):

$$\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{12}{1} \cdot \binom{4}{2} = 3\,744$$

En resumen, las maneras de tener al menos un par son

$$1\,098\,240 + 109\,824 + 624 + 123\,552 + 3\,744 = 1\,335\,984$$

Así, en número total de manos sin pares es

$$2\,598\,960 - 1\,335\,984 = 1\,262\,976$$

La otra parte de la pregunta (exactamente un par) la respondimos ya.

45. Esto corresponde a elegir 5 sabores entre los 37, y luego cada uno de los estudiantes elige un tamaño en forma independiente:

$$\binom{37}{5} \cdot 3^5 = 105\,922\,971$$

46. Cada punto en turno.

a) La palabra `MOVIMIENTO` corresponde al multiconjunto de letras $\{\mathtt{E}, \mathtt{I}^2, \mathtt{M}^2, \mathtt{N}, \mathtt{O}^2, \mathtt{T}, \mathtt{V}\}$. Usando el tao:

$$\binom{10}{1\;2\;2\;1\;2\;1\;1} = \frac{10!}{1!\;2!\;2!\;1!\;2!\;1!\;1!} = \frac{10!}{(2!)^3} = 453\,600$$

b) Separando en consonantes y vocales es $\{\mathtt{M}^2, \mathtt{N}, \mathtt{T}, \mathtt{V}\}$ y $\{\mathtt{E}, \mathtt{I}^2, \mathtt{O}^2, \}$, respectivamente. Hay 5 consonantes y 5 vocales, por lo que hay dos opciones: El resultado comienza con consonante o vocal, luego hay que distribuir las consonantes y vocales en las 5 posiciones que corresponden a cada tipo de letra. Esto se hace usando el tao. Resulta:

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

c) Esto es tomar el número total de posibilidades y restar los números de opciones con letras iguales juntas. Hay 3 pares de letras iguales, así basta calcular las posibilidades con un par junto y multiplicar por 3. Para obtener las posibilidades con, digamos, `II`, consideramos esto como un único símbolo, y tenemos el multiconjunto $\{\mathtt{E}, \mathtt{II}, \mathtt{M}^2, \mathtt{N}, \mathtt{O}^2, \mathtt{T}, \mathtt{V}\}$. Por el tao, para esto hay

$$\binom{9}{1!\;1!\;2!\;1!\;2!\;1!\;1!}$$

y el total resulta ser

$$3 \cdot \binom{9}{1!\;1!\;2!\;1!\;2!\;1!\;1!} = \frac{3 \cdot 9!}{(2!)^2} = 136\,080$$

con lo que finalmente el valor buscado es:

$$453\,600 - 136\,080 = 317\,520$$

47. Por turno.

    a) Elegir la directiva es formar una secuencia sin repeticiones de 4 tomados entre 15. O sea:

    $$P(15, 4) = 15^{\underline{4}} = 32\,760$$

    b) Podemos elegir al presidente de 3 maneras, el resto de la directiva es una secuencia sin repeticiones de 3 entre los 14 restantes:

    $$3 \cdot P(15 - 1, 4 - 1) = 3 \cdot 14^{\underline{3}} = 6\,552$$

    c) Tenemos 4 posiciones posibles para el informático, los demás puestos son elegir 3 en orden entre los 12 no informáticos:

    $$4 \cdot P(15 - 3, 4 - 1) = 4 \cdot 12^{\underline{3}} = 5\,280$$

    d) Por la regla de la suma, esto es el número total de directivas posibles menos las que no incluyen informáticos. El número total es tomar 4 en orden entre 15, los sin informáticos son tomar 4 en orden entre los 12 no informáticos:

    $$P(15, 4) - P(15 - 3, 4) = 15^{\underline{4}} - 12^{\underline{4}} = 20\,880$$

48. Por turno.

    a) El total es una secuencia de largo 4 tomada entre 10. O sea:

    $$10^4 = 10\,000$$

    b) Como hay 4 dígitos gastados, la clave es una permutación de estos 4 dígitos. Son:

    $$4! = 24$$

    c) Hay uno de los dígitos que se repite en la clave. Supongamos que el que se repite es el 1 (por simetría, lo que obtengamos basta multiplicarlo por 3). Lo que tenemos son permutaciones del multiconjunto $\{1^2, 5, 9\}$. Aplicando el Tao, y luego la regla de la suma el total de claves posibles es:

    $$3 \cdot \binom{4}{2\;1\;1} = 3 \cdot \frac{4!}{2!\,1!\,1!} = 36$$

    d) El resultado de 48*c* es mayor que el de 48*b*. Intuitivamente se pensaría que es al revés.

49. Hay 10 números de un único dígito. Para números formados por exactamente dos dígitos, podemos elegitr los dígitos de $\binom{10}{2}$ formas, y estos dos dígitos se pueden ordenar de 2^7 maneras. Pero de estas hay 2 que están formadas por un solo dígito, debemos omitirlas. Usando la regla de la suma:

    $$10 + \binom{10}{2}(2^7 - 2) = 5\,680$$

50. Varias opciones. Antes que nada, podemos extender la suma al rango $0 \leq k \leq n$ sin cambiar el valor de la suma.

    Inducción: Es una sumatoria, inducción es la herramienta lógica:

    Base: El caso $n = 0$ se reduce a $0 = 0$.

    Inducción: Evaluamos:

    $$\begin{aligned}
    \sum_{0 \leq k \leq n+1} k \binom{n+1}{k} &= \sum_{0 \leq k \leq n} k \left(\binom{n}{k} + \binom{n}{k-1} \right) \\
    &= \sum_{0 \leq k \leq n} k \binom{n}{k} + \sum_{0 \leq k \leq n} (k+1) \binom{n}{k} \\
    &= n \cdot 2^{n-1} + \sum_{0 \leq k \leq n} k \binom{n}{k} + \sum_{0 \leq k \leq n} \binom{n}{k} \\
    &= n \cdot 2^n + 2^n \\
    &= (n+1) \cdot 2^n
    \end{aligned}$$

Series de potencias: Sabemos que:

$$\begin{aligned}
(1+z)^n &= \sum_{0 \le k \le n} \binom{n}{k} z^k \\
\frac{\mathrm{d}}{\mathrm{d}z}(1+z)^n &= \sum_{0 \le k \le n} k \binom{n}{k} z^{k-1} \\
&= n(1+z)^{n-1}
\end{aligned}$$

Evaluando en $z = 1$ se obtiene el resultado anunciado. En realidad todas las expresiones mencionadas son polinomios, temas de convergencia y validez de las operaciones son triviales.

Manipular la suma: Lo siguiente es simplemente sumar en una u otra dirección, y usar la simetría de los coeficientes binomiales:

$$\begin{aligned}
\sum_{0 \le k \le n} k \binom{n}{k} &= \sum_{0 \le k \le n} (n-k) \binom{n}{n-k} \\
&= \sum_{0 \le k \le n} (n-k) \binom{n}{k}
\end{aligned}$$

O sea:

$$\begin{aligned}
2 \sum_{0 \le k \le n} k \binom{n}{k} &= \sum_{0 \le k \le n} k \binom{n}{k} + \sum_{0 \le k \le n} (n-k) \binom{n}{k} \\
&= n \sum_{0 \le k \le n} \binom{n}{k} \\
&= n \cdot 2^n
\end{aligned}$$

lo que es equivalente a lo anunciado.

Identidad para coeficientes binomiales: Tenemos que:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{n}{k} \binom{n-1}{k-1}$$

Usando esto en nuestra suma original (la identidad vale siempre que $k > 0$):

$$\begin{aligned}
\sum_{1 \le k \le n} k \binom{n}{k} &= \sum_{1 \le k \le n} n \binom{n-1}{k-1} \\
&= n \cdot 2^{n-1}
\end{aligned}$$

51. Siguiendo la idea de *stars and bars*, podemos representar n mediante palitos. Una composición de n corresponde a insertar + entre palitos, lo que es lo mismo que el número total de subconjuntos de las posiciones entre palitos, vale decir, 2^{n-1}. Incluso más, una combinación de n en k partes es elegir $k-1$ posiciones para los signos, o sea:

$$\binom{n-1}{k-1}$$

52. Hay varias formas de obtener este resultado:

- Considerar que elegimos parejas sucesivamente, con lo que sobrecontamos por los ordenamientos de las parejas:

$$\begin{aligned}
\frac{1}{7!} \cdot \binom{14}{2} \cdot \binom{12}{2} \cdot \binom{10}{2} \cdot \binom{8}{2} \cdot \binom{6}{2} \cdot \binom{4}{2} \cdot \binom{2}{2} &= \frac{1}{7!} \cdot \frac{14!}{10!2!} \cdot \frac{12!}{10!2!} \cdot \frac{10!}{8!2!} \cdot \frac{8!}{6!2!} \cdot \frac{6!}{4!2!} \cdot \frac{4!}{2!2!} \cdot \frac{2!}{0!2!} \\
&= \frac{14!}{7!\,(2!)^7} \\
&= 135\,135
\end{aligned}$$

- Si numeramos a cada persona con la pareja a la que pertenece, tenemos un problema à la `BOOKKEEPER` (cada uno de los 7 números aparece 2 veces); pero esto sobrecuenta por los reordenamientos de las 7 parejas:

$$\begin{aligned}\frac{1}{7!}\cdot\binom{14}{2,2,2,2,2,2,2} &= \frac{14!}{7!\,(2!)^7}\\ &= 135\,135\end{aligned}$$

- Consideremos las personas en orden alfabético, por ejemplo. Elegimos 7 personas para ser el primero de la pareja entre las 14, luego ordenamos las restantes 7 como parejas de las primeras en orden; pero esto supone orden al interior de las parejas:

$$\begin{aligned}\binom{14}{7}\cdot 7!\cdot\frac{1}{2^7} &= \frac{14!\,7!}{7!\,7!,\,2^7}\\ &= \frac{14!}{7!\,2^7}\\ &= 135\,135\end{aligned}$$

53. Siguiendo las indicaciones dadas en clase, construimos una secuencia que está en biyección con las manos buscadas. Un par de ejemplos son:

$$\begin{array}{l}\{A\diamondsuit\ \ K\diamondsuit\ \ 3\heartsuit\ \ J\clubsuit\ \ 7\spadesuit\}\\ \{A\spadesuit\ \ 2\spadesuit\ \ 3\heartsuit\ \ 4\clubsuit\ \ 5\diamondsuit\}\end{array}$$

Vemos que podemos describirlas mediante:

- La pinta que tiene dos cartas, se eligen una entre cuatro
- Los valores de las cartas de la misma pinta, se eligen dos entre trece
- Los valores sucesivos de las demás cartas, en el orden de las pintas. Se eligen entre once, diez y nueve, respectivamente. $\spadesuit$, $\heartsuit$, $\clubsuit$, $\diamondsuit$.

Nuestros ejemplos quedan descritos por:

$$\begin{array}{ll}(\diamondsuit,\{A,K\},7,3,J) & \longleftrightarrow \{A\diamondsuit\ \ K\diamondsuit\ \ 3\heartsuit\ \ J\clubsuit\ \ 7\spadesuit\}\\ (\spadesuit,\{A,2\},3,4,5) & \longleftrightarrow \{A\spadesuit\ \ 2\spadesuit\ \ 3\heartsuit\ \ 4\clubsuit\ \ 5\diamondsuit\}\end{array}$$

Bien. Aplicando la regla del producto a la descripción dada, el número buscado es:

$$\binom{4}{1}\cdot\binom{13}{2}\cdot 11\cdot 10\cdot 9 = 308\,880$$

54. Esta palabra, vista como multiconjunto, es $\{\mathrm{A}^2,\mathrm{B},\mathrm{C},\mathrm{I}^2,\mathrm{M},\mathrm{N},\mathrm{O}^2,\mathrm{R},\mathrm{T}\}$. Debemos considerar los anagramas que comienzan con A, los que terminan en A, y los que comienzan y terminan en A. Al sumar los primeros dos estamos sumando dos veces el tercer conjunto, debemos restarlo.

Es claro que comenzar o terminar con A contempla el mismo conjunto de anagramas, completado iniciando o terminando en A. Comenzar y terminar en A da el conjunto de anagramas de las demás letras. O sea, el número buscado es:

$$2\cdot\binom{11}{1,1,1,2,1,1,2,1,1} - \binom{10}{1,1,2,1,1,2,1,1} = 19\,051\,200$$

55. Construiremos una descripción de horarios válidos como una secuencia, dado que éstas son fáciles de contar. Ordenamos los exámenes de nuestra intrépida heroína de alguna forma, y en ese orden les asignamos horarios. Para el primer examen están disponibles todos los $5\cdot 3 = 15$ horarios. Para el segundo están disponibles sólo los horarios en los 4 días en que no está en primero ($4\cdot 3$ posibilidades), para el tercero los horarios salvo los días ya ocupados ($3\cdot 3$ posibilidades), para la prueba final restan $2\cdot 3$ posibilidades, para un total de:

$$\begin{aligned}(5\cdot 3)\cdot(4\cdot 3)\cdot(3\cdot 3)\cdot(2\cdot 3) &= 5^{\underline{4}}\cdot 3^4\\ &= 9\,720\end{aligned}$$

Otra manera de plantearlo es asignando los días de los 4 exámenes, una permutación de 4 tomados entre 5 días ($5^{\underline{4}}$ opciones), y luego para cada examen elegir uno de los tres horarios en el día (3^4 posibilidades), esto nuevamente da:

$$5^{\underline{4}} \cdot 3^4 = 9\,720$$

56. Hay dos posibilidades excluyentes para tener una mano con exactamente dos pintas: hay una carta de una pinta (y cuatro cartas de otra), o hay dos cartas de una pinta (y tres cartas de otra). Contamos las dos por separado, y usamos la regla de la suma. Cada opción queda descrita por la pinta menos numerosa, los valores de esas cartas, la pinta más numerosa y los respectivos valores.

    Una carta de una pinta: La pinta menos numerosa es una entre cuatro, elegimos el valor de esa única carta entre 13; la pinta más numerosa es una en tres (no se repite la anterior), los valores son 4 elegidos entre 12 (el valor de la primera carta se excluye). Esto resulta en:

    $$\binom{4}{1} \cdot \binom{13}{1} \cdot \binom{3}{1} \cdot \binom{12}{4}$$

    Dos cartas de la misma pinta: Igual que el otro caso, la pinta menos numerosa es una entre cuatro, elegimos el valor de esas dos cartas entre 13; la pinta más numerosa es una en tres (no se repite la anterior), los valores son 3 elegidos entre 11 (los valores de las dos cartas de la pinta menos numerosa se excluyen). Esto resulta en:

    $$\binom{4}{1} \cdot \binom{13}{2} \cdot \binom{3}{1} \cdot \binom{11}{3}$$

    Aplicando la regla de la suma, el número buscado es:

    $$\binom{4}{1} \cdot \binom{13}{1} \cdot \binom{3}{1} \cdot \binom{12}{4} + \binom{4}{1} \cdot \binom{13}{2} \cdot \binom{3}{1} \cdot \binom{11}{3} = 231\,660$$

57. Esto podemos describirlo usando x_i para representar el número de elementos de tipo i elegidos:

    $$x_1 + x_2 + \cdots + x_n = 2k$$

    con las restricciones que $x_i \geq 0$ y x_i es par. Pero esto es decir:

    $$2y_1 + 2y_2 + \cdots + 2y_n = 2k$$

    donde $x_i = 2y_i$, y nuevamente $y_i \geq 0$. Pero esto es:

    $$y_1 + y_2 + \cdots + y_n = k$$

    y el número de soluciones de ésto es el poco sorprendente resultado:

    $$\left(\!\!\binom{n}{k}\!\!\right)$$

58. Estamos frente al multiconjunto: $\{\mathrm{A}, \mathrm{B}, \mathrm{D}, \mathrm{E}, \mathrm{O}^2, \mathrm{P}, \mathrm{R}^2\}$. Por el Tao, sus letras se pueden ordenar de

    $$\binom{9}{1, 1, 1, 1, 2, 1, 2}$$

    maneras. Pero esto incluye los ordenamientos que contienen OO, debemos restarlos. Se obtienen vía considerar esta combinación como un nuevo símbolo. El número de órdenes con RR es el mismo:

    $$\binom{8}{1, 1, 1, 1, 1, 1, 2}$$

Pero si restamos estos, al restar los que contienen OO estamos incluyendo los que también contienen RR (y viceversa), debemos reponerlos. Los que tienen las dos letras repetidas adyacentes son

$$\binom{7}{1,1,1,1,1,1,1}$$

En total, lo que buscamos es:

$$\binom{9}{1,1,1,1,2,1,2} - 2\binom{8}{1,1,1,1,1,1,2} + \binom{7}{1,1,1,1,1,1,1} = 15\,120$$

59. Consideremos $2n$ bolitas diferentes (por ejemplo, numeradas), n negras y n blancas. El lado derecho corresponde al número de maneras de elegir n bolitas del total, sin importar el color.

    El término para k del lado izquierdo cuenta el número de formas de elegir k bolitas negras y $n-k$ blancas, como las elecciones de las bolitas de ambos colores son independientes se aplica la regla del producto. A su vez, las elecciones de distintos números de bolitas blancas son excluyentes, y para $0 \le k \le n$ exhaustivas. Se aplica la regla de la suma.

    Como ambas expresiones cuentan la misma situación, son iguales.

60. Podemos describir las palabras solicitadas indicando:

    - La primera letra, 1 de 5 vocales
    - La última letra, 1 de 4 vocales restantes
    - Una permutación de $7-2=5$ letras tomadas de las $26-2=24$ restantes

    Es fácil contar las secuencias que describen lo buscado:

    $$5 \cdot 4 \cdot 24^{\underline{5}} = 102\,009\,600$$

9. Problemas misceláneos

1. Resolvemos los problemas planteados por turno.

    a) Estamos dividiendo los 16 equipos en 4 grupos, que podemos considerar como elegir 4 de los 16 para formar el primer grupo, luego 4 de los 12 restantes para formar el segundo, y finalmente 4 de los 8 que quedan para formar el tercero (lo que automáticamente determina el cuarto grupo). Así, el número total de distribuciones es:

    $$\binom{16}{4} \cdot \binom{12}{4} \cdot \binom{8}{4} = \frac{16!}{4!12!} \cdot \frac{12!}{4!\,8!} \cdot \frac{8!}{4!\,4!} = \frac{16!}{4!\,4!\,4!\,4!} = \binom{16}{4\;4\;4\;4} = 63\,063\,000$$

    Otra manera de obtener la última expresión directamente es considerar que estamos distribuyendo los números de los grupos (4 de cada uno) entre los 16 equipos.

    b) Como no hay empates y siempre gana el mejor, en cada grupo el mejor ganará los 3 partidos que disputa. El segundo mejor ganará contra todos (salvo el mejor), con lo que se lleva 2 victorias. El tercero del grupo pierde contra los dos mejores y le gana al cuarto, con lo que tiene 1 victoria. El peor pierde todos sus encuentros, y queda sin victorias.

    Los que pasan a la segunda vuelta ganan 3 y 2 partidos, respectivamente.

    c) Como el mejor equipo siempre gana en cada encuentro, el mejor de los 16 equipos se lleva la copa.

    d) Nombraremos los equipos A a P en orden del mejor al peor. Por simetría podemos suponer que A está en el grupo 1, y B puede estar en cualquiera de los cuatro grupos. El único que puede eliminar a B es A, así que debe jugar con éste antes de la final para no llegar a disputarla. Para simplificar, anotaremos $x : y$ para el x (1^{o} o 2^{o}) del grupo y. En la segunda ronda juegan: $1 : 1$ contra $2 : 2$ (1^{er} partido), $1 : 2$ contra $2 : 3$ (2^{o} partido), $1 : 3$ contra $2 : 4$ (3^{er} partido) y $1 : 4$ contra $2 : 1$ (4^{o} partido). Sabemos que A es $1 : 1$, y gana el primer partido de la segunda ronda. A su vez, B puede ser (2:1) (si le tocó estar en el mismo grupo que A) o es (1:y) con $2 \leq y \leq 4$. No le puede tocar jugar con A en la segunda ronda, ya que en ella juega el primero de un grupo con el segundo de otro. Si B es $1 : 2$, le toca jugar con $2 : 3$ (partido que gana), y luego juega con A en la tercera ronda, donde es eliminado.

    Es posible que la final no sea disputada por los dos mejores.

10. Series de potencias

1. Determine explícitamente los coeficientes siguientes:

   a) $\left[x^k\right] \dfrac{1}{(1-x^2)^3}$

   Acá hay al menos dos maneras de proceder. La primera es usar el teorema de Taylor sobre la función indicada. La otra es expandir la potencia en serie directamente:

$$\begin{aligned}(1-x^2)^{-3} &= \sum_{k\geq 0}\binom{-3}{k}(-x^2)^k \\ &= \sum_{k\geq 0}\binom{k+2}{2}x^{2k}\end{aligned}$$

   Con esto tenemos, finalmente:

$$\begin{aligned}\left[x^{2k}\right]\frac{1}{(1-x^2)^3} &= \binom{k+2}{k} \\ &= \frac{(k+1)(k+2)}{2} \\ \left[x^{2k+1}\right]\frac{1}{(1-x^2)^3} &= 0\end{aligned}$$

   b) $\left[\dfrac{x^k}{k!}\right]\sqrt{1-4x}$

   Nuevamente, una tarea para el teorema del binomio…

$$\begin{aligned}\sqrt{1-4x} &= \sum_{k\geq 0}\binom{1/2}{k}(-4x)^k \\ &= \sum_{k\geq 0}(-1)^k 2^{2k}\binom{1/2}{k}x^k \\ &= \sum_{k\geq 0}(-1)^k 2^{2k}\cdot\frac{(-1)^{k-1}}{k\,2^{2k-1}}\binom{2k-2}{k-1}x^k \\ &= -\sum_{k\geq 0}\frac{2}{k}\binom{2k-2}{k-1}x^k\end{aligned}$$

   y finalmente:

$$\left[\frac{x^k}{k!}\right]\sqrt{1-4x} = -2(k-1)!\binom{2k-1}{k-1}$$

   c) $\left[\alpha x^k\right]\dfrac{1}{(1-\alpha x)(1-\beta x)}$

   Acá lo más simple es usar fracciones parciales. `maxima` mediante:

$$\frac{1}{(1-\alpha x)(1-\beta x)} = \frac{\alpha}{(\alpha-\beta)(1-\alpha x)} - \frac{\beta}{(\alpha-\beta)(1-\beta x)}$$

   con lo que:

$$\left[\alpha x^k\right]\frac{1}{(1-\alpha x)(1-\beta x)} = \frac{\alpha^{k+1}-\beta^{k+1}}{\alpha(\alpha-\beta)}$$

d) $\left[x^k\right] \dfrac{1}{(1-\alpha x)^3}$

Otra vez un trabajo para el teorema del binomio:

$$\begin{aligned}\frac{1}{(1-\alpha x)^3} &= \sum_{k\geq 0}\binom{-3}{k}(-\alpha x)^k \\ &= \sum_{k\geq 0}\binom{k+2}{2}\alpha^k x^k\end{aligned}$$

con lo que:

$$\begin{aligned}\left[x^k\right]\frac{1}{(1-\alpha x)^3} &= \binom{k+2}{2}\alpha^k \\ &= \frac{(k+1)(k+2)\alpha^k}{2}\end{aligned}$$

e) $\left[x^k\right](1+x^2)^m$

Nuevamente, el teorema del binomio al rescate:

$$\left[x^k\right](1+x^2)^m = \left[x^k\right]\sum_{k\geq 0}\binom{m}{k}x^{2k}$$

de donde:

$$\begin{aligned}\left[x^{2k}\right] &= \tbinom{m}{k} \\ \left[x^{2k+1}\right] &= 0\end{aligned}$$

2. Determine los siguientes coeficientes:

a)

$$\begin{aligned}\left[x^n\right](a-bz)^{-2} &= a^{-2}\binom{-2}{n}\left(-\frac{b}{a}\right)^n \\ &= a^{-2}(-1)^n\binom{n+1}{1}(-1)^n\frac{b^n}{a^n} \\ &= \frac{(n+1)b^n}{a^{n-2}}\end{aligned}$$

b)

$$\begin{aligned}\left[x^n\right]e^{1-x} &= e\left[x^n\right]e^{-x} \\ &= e(-1)^n\frac{1}{n!} \\ &= \frac{(-1)^n e}{n!}\end{aligned}$$

c)

$$\begin{aligned}\left[x^n y^k\right](1+y(1-x))^{-3} &= \sum_{i\geq 0}\binom{-3}{i}y^i(1-x)^i \\ \left[x^n\right]\binom{-3}{k}(1-x)^k &= \binom{-3}{k}(-1)^n\binom{k}{n} \\ &= (-1)^{n+k}\binom{k+2}{2}\binom{k}{n} \\ &= (-1)^{k+n}\frac{(k+2)(k+1)}{2}\,\frac{k!}{k!(k-n)!} \\ &= (-1)^{k+n}\binom{k+2}{2\;\;n\;\;k-n}\end{aligned}$$

Esto no es tan raro... realmente es un trinomio.

$$(1 + y(1 - x))^{-3} = (1 + y - xy)^{-3}$$

d)

$$\begin{aligned}
[x^n]\,(1 - nx)^{-2n} &= \binom{-2n}{n}(-n)^n \\
&= \binom{3n-1}{n} n^n
\end{aligned}$$

3. *a*) Acá tenemos dos opciones. Una es reconocer esto como una serie geométrica en x^2, o sea $1 + x^2 + x^4 + \ldots$ y obtener directamente:

$$\begin{aligned}
\left[x^k\right] \frac{1}{1 - x^2} &= \begin{cases} 1 & \text{si } k \text{ es par} \\ 0 & \text{si } k \text{ es impar} \end{cases} \\
&= \frac{1}{2}\left(1 + (-1)^k\right)
\end{aligned}$$

La otra es hacer toda la calistenia de fracciones parciales Nuevamente, (cortesía de `maxima`):

$$\frac{1}{1 - x^2} = \frac{1}{2} \cdot \frac{1}{1 + x} + \frac{1}{2} \cdot \frac{1}{1 - x}$$

y luego "leer" los coeficientes de las series geométricas resultantes:

$$\left[x^k\right] \frac{1}{1 - x^2} = \frac{1}{2}\left(1 + (-1)^k\right)$$

b) Una serie geométrica:

$$\left[x^k\right] \frac{1}{1 - x/3} = 3^{-k}$$

c) Una manera de verlo es como es un binomio a potencia:

$$\begin{aligned}
\left[x^k\right] (1 - x^2)^3 &= \left[x^k\right] \sum_{n \geq 0} \binom{-3}{n} (-1)^n x^{2n} \\
&= \left[x^k\right] \sum_{n \geq 0} \binom{2 + n}{2} x^{2n} \\
&= \begin{cases} \binom{2 + k/2}{2} & \text{si } k \text{ es par} \\ 0 & \text{si } k \text{ es impar} \end{cases}
\end{aligned}$$

donde usamos:

$$\binom{-n}{k} = (-1)^k \binom{n + k - 1}{n - 1}$$

La manera *no* recomendable es aplicar el teorema de Maclaurin...

4. Tenemos:

$$\begin{aligned}
\ln(1 - x) &= -\sum_{n \geq 1} \frac{x^n}{n} \\
&= -x \sum_{n \geq 0} \frac{x^n}{n + 1}
\end{aligned}$$

Simplemente multiplicando por lo mismo queda:

$$
\begin{aligned}
\ln^2(1-x) &= x^2 \biggl(\sum_{n \geq 0} \frac{x^n}{n+1} \biggr)^2 \\
&= x^2 \sum_{n \geq 0} \biggl(\sum_{0 \leq k \leq n} \frac{1}{(k+1)(n+1-k)} \biggr) x^n \\
&= x^2 \left(\frac{1}{1 \cdot 1} + \left(\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 1} \right) x \right. \\
&\qquad + \left(\frac{1}{1 \cdot 3} + \frac{1}{2 \cdot 2} + \frac{1}{3 \cdot 1} \right) x^2 \\
&\qquad \left. + \left(\frac{1}{1 \cdot 4} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 2} + \frac{1}{4 \cdot 1} \right) x^3 + \dots \right) \\
&= x^2 \left(1 + x + \frac{11}{12} x^2 + \frac{5}{6} x^3 + \frac{137}{180} x^4 + \frac{7}{10} x^5 \right. \\
&\qquad \left. + \frac{363}{560} x^6 + \frac{761}{1260} x^7 + \frac{7129}{12600} x^8 + \dots \right)
\end{aligned}
$$

El coeficiente de x^n lo calcula la siguiente función escrita en maxima:

```
t(n) := block([s:0],
  for i:0 thru n do
    (s:s + 1 / ((i + 1) * (n + 1 - i))), s);
```

5. Partimos por dejar sólo potencias positivas, y expandimos por el teorema del binomio:

$$
\begin{aligned}
\left[x^{15}\right] \left(3x^2 - \frac{2}{x} \right)^{12} &= \left[x^{15}\right] x^{-12} \left(3x^3 - 2 \right)^{12} \\
&= \left[x^{27}\right] \sum_{0 \leq k \leq 12} \binom{12}{k} 3^k x^{3k} \left(-2\right)^{12-k}
\end{aligned}
$$

El único término que aporta x^{27} es $k = 9$:

$$
\begin{aligned}
\left[x^{15}\right] \left(3x^2 - \frac{2}{x} \right)^{12} &= \binom{12}{9} 3^9 \left(-2\right)^3 \\
&= -34\,642\,080
\end{aligned}
$$

6. El factor $j(j-1)$ sugiere una segunda derivada, y el límite inferior en realidad es superfluo:

$$
\begin{aligned}
\sum_{j \geq 0} \binom{n}{j} z^j &= (1+z)^n \\
D^2 \sum_{j \geq 0} \binom{n}{j} z^j &= \sum_{j \geq 0} j(j-1) \binom{n}{j} z^{j-2} \\
&= n(n-1)(1+z)^{n-2}
\end{aligned}
$$

Evaluando para $z = 1$:

$$
\sum_{2 \leq j \leq n} j(j-1) \binom{n}{j} = n(n-1) 2^{n-2}
$$

7. Tenemos la suma:

$$\sum_{n\geq 0} \binom{n}{k} z^n = \frac{z^k}{(1-z)^{k+1}}$$

Para sumas parciales, teniendo en cuenta que si $r < k$ los coeficientes binomiales se anulan permite escribir:

$$\begin{aligned}
\sum_{n\geq 0} z^n \sum_{0\leq r\leq n} \binom{r}{k} &= \frac{z^k}{(1-z)^{k+2}} \\
&= \frac{1}{z} \sum_{n\geq 0} \binom{n}{k+1} z^n \\
&= \sum_{n\geq 0} \binom{n}{k+1} z^{n-1} \\
&= \sum_{n\geq 0} \binom{n+1}{k+1} z^n
\end{aligned}$$

Nuevamente, como para $r < k$ el coeficiente binomial se anula:

$$\sum_{k\leq r\leq n} \binom{r}{k} = \binom{n+1}{k+1}$$

8. Por turno.

   a) Para el caso $d(z) = h(z) = (1-z)^{-1}$, directamente:

   $$\begin{aligned}
   d_{n,k} &= [z^n] \, \frac{1}{1-z} \cdot \frac{z^k}{(1-z)^k} \\
   &= [z^n] \, \frac{z^k}{(1-z)^{k+1}} \\
   &= \binom{n}{k}
   \end{aligned}$$

   b) El doctor receta untar generosamente con aceite de serpiente:

   $$\begin{aligned}
   \sum_{n\geq 0} z^n \sum_{k\geq 0} d_{n,k} f_k &= \sum_{k\geq 0} f_k \sum_{n\geq 0} d_{n,k} z^n \\
   &= \sum_{k\geq 0} f_k \cdot d(z) \left(zh(z)\right)^k \\
   &= d(z) \sum_{k\geq 0} f_k \left(zh(z)\right)^k \\
   &= d(z) F\left(zh(z)\right)
   \end{aligned}$$

   Esto es equivalente a lo solicitado.

   c) Del punto anterior:

   $$\sum_{0\leq k\leq n} f_k = [z^n] \, \frac{1}{1-z} F(z)$$

   Nuestra regla para sumas parciales.

11. Funciones generatrices

1. Cada uno de los niños recibe 1 o 2 dulces, con lo que se le representa por:

$$z + z^2$$

Los 10 niños y los dulces que reciben se representan por:

$$(z + z^2)^{10} = z^{10}(1 + z)^{10}$$

Nos interesa el coeficiente de z^{17}:

$$\begin{aligned}\left[z^{17}\right] z^{10}(1 + z)^{10} &= \left[z^7\right] (1 + z)^{10} \\ &= \binom{10}{7} \\ &= 120\end{aligned}$$

Este último resultado es evidente, si consideramos que debemos dar un dulce a cada uno, y luego elegir a los 7 que reciben un segundo dulce.

2. Usamos funciones generatrices ordinarias para contar los tipos de flores. Para lirios:

$$\begin{aligned}L(z) &= 1 + z + z^2 + z^3 \\ &= \frac{1 - z^4}{1 - z}\end{aligned}$$

Para tulipanes:

$$\begin{aligned}T(z) &= z + z^3 + z^5 + \cdots \\ &= z\frac{1}{1 - z^2}\end{aligned}$$

Para rosas:

$$\begin{aligned}R(z) &= 1 + z + z^2 + \cdots \\ &= \frac{1}{1 - z}\end{aligned}$$

La función generatriz para ramilletes es:

$$\begin{aligned}F(z) &= L(z) \cdot T(z) \cdot R(z) \\ &= \frac{1 - z^4}{1 - z} \cdot z\frac{1}{1 - z^2} \cdot \frac{1}{1 - z} \\ &= \frac{z(1 - z^4)}{(1 - z)^2(1 - z^2)} \\ &= \frac{z(1 + z^2)}{(1 - z)^2} \\ &= z(1 + z^2) \sum_{k \geq 0} (-1)^k \binom{-2}{k} z^k \\ &= z(1 + z^2) \sum_{k \geq 0} \binom{2 + k - 1}{1} z^k \\ &= z(1 + z^2) \sum_{k \geq 0} (k + 1) z^k\end{aligned}$$

De acá obtenemos el número de ramilletes con n flores:

$$\begin{aligned}
f_n &= [z^n]F(z) \\
&= [z^n]z(1+z^2)\sum_{k\geq 0}(k+1)z^k \\
&= [z^{n-1}](1+z^2)\sum_{k\geq 0}(k+1)z^k \\
&= [z^{n-1}]\sum_{k\geq 0}(k+1)z^k + [z^{n-3}\sum_{k\geq 0}(k+1)z^k \\
&= n + (n-2) \\
&= 2n-2
\end{aligned}$$

3. *a*) Como son secuencias, corresponde usar funciones generatrices exponenciales. A cada símbolo le corresponde:

$$z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots = \mathrm{e}^z - 1$$

Para los s símbolos:

$$(\mathrm{e}^z - 1)^s$$

Nos interesan cuántas hay de n símbolos:

$$\begin{aligned}
n![z^n]\left(\mathrm{e}^z - 1\right)^s &= n![z^n]\sum_{k\geq 0}(-1)^{s-k}\binom{s}{k}\mathrm{e}^{kz} \\
&= n!\sum_{k\geq 0}(-1)^{s-k}\binom{s}{k}\frac{k^n}{n!} \\
&= \sum_{k\geq 0}(-1)^{s-k}\binom{s}{k}k^n
\end{aligned}$$

b) Tenemos:

Ω: El universo son las s^n secuencias sin restricciones

Propiedades: Diremos que la secuencia tiene la propiedad i si no contiene el símbolo i

Buscamos: El número de secuencias sin propiedades (no faltan símbolos), e_0.

Tenemos para un conjunto $\mathcal{S}$ de propiedades dado (corresponde a armar la secuencia con los restantes $s - |\mathcal{S}|$ símbolos):

$$N(\supseteq \mathcal{S} = (s - |\mathcal{S}|)^n$$

Como podemos elegir r de las s propiedades:

$$N_r = \binom{s}{r}(s-r)^n$$

Con esto queda:

$$N(z) = \sum_{r\geq 0}\binom{s}{r}(s-r)^n z^r$$

Finalmente, usando nuestra fórmula mágica:

$$\begin{aligned}
e_0 &= E(0) \\
&= N(-1) \\
&= \sum_{r\geq 0}(-1)^r\binom{s}{r}(s-r)^n
\end{aligned}$$

Cambiando variables $k = s - r$ con la simetría de los coeficientes binomiales resulta:

$$= \sum_{k \geq 0} (-1)^{s-k} \binom{s}{k} k^n$$

4. Cada uno por turno.

   a) Calculamos el producto de Cauchy:

$$\begin{aligned}
\left(\sum_{n \geq 0} a_n \frac{z^n}{n!} \right) \cdot \left(\sum_{n \geq 0} b_n \frac{z^n}{n!} \right) &= \sum_{n \geq 0} \left(\sum_{0 \leq k \leq n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} \right) z^n \\
&= \sum_{n \geq 0} \left(\sum_{0 \leq k \leq n} \frac{n!}{k!(n-k)!} a_k b_{n-k} \right) \frac{z^n}{n!} \\
&= \sum_{n \geq 0} \left(\sum_{0 \leq k \leq n} \binom{n}{k} a_k b_{n-k} \right) \frac{z^n}{n!}
\end{aligned}$$

   b) Tenemos al lado izquierdo:

$$\mathrm{e}^{(a+b)z} = \sum_{n \geq 0} (a+b)^n \frac{z^n}{n!}$$

   El lado derecho es:

$$\mathrm{e}^{az} \cdot \mathrm{e}^{bz} = \sum_{n \geq 0} \left(\sum_{0 \leq k \leq n} \binom{n}{k} a^k b^{n-k} \right) z^n$$

   Comparando coeficientes de z^n:

$$(a+b)^n = \sum_{0 \leq k \leq n} \binom{n}{k} a^k b^{n-k}$$

5. Sean $\widehat{A}(z)$ y $\widehat{B}(z)$ las funciones generatrices exponenciales respectivas:

$$\widehat{A}(z) = \sum_{n \geq 0} a_n \frac{z^n}{n!}$$
$$\widehat{B}(z) = \sum_{n \geq 0} b_n \frac{z^n}{n!}$$

   La relación entre las secuencias no es más que la convolución binomial entre $\langle a_n \rangle_{n \geq 0}$ y $\langle 1 \rangle_{n \geq 0}$, como $\langle 1 \rangle_{n \geq 0} \stackrel{\text{egf}}{\longleftrightarrow} \mathrm{e}^z$:

$$\widehat{B}(z) = \mathrm{e}^z \widehat{A}(z)$$

   Esto es lo mismo que:

$$\widehat{A}(z) = \mathrm{e}^{-z} \widehat{B}(z)$$

   A su vez es $\langle (-1)^n \rangle_{n \geq 0} \stackrel{\text{egf}}{\longleftrightarrow} \mathrm{e}^{-z}$, y la última ecuación corresponde a la convolución binomial de ésto con $\langle b_n \rangle_{n \geq 0}$, lo solicitado.

6. Aplicamos las propiedades directamente:

$$\frac{F^{(\alpha)}(z) - F_0^{(\alpha)} - F_1^{(\alpha)} z}{z^2} = \alpha \frac{F^{(\alpha)}(z) - F_0^{(\alpha)}}{z} + F^{(\alpha)}(z)$$

   Substituyendo los valores iniciales y despejando $F^{(\alpha)}(z)$ resulta:

$$F^{(\alpha)}(z) = \frac{z}{1 - \alpha z - z^2}$$

7. La secuencia $\langle H_n \rangle_{n \geq 1}$ es la convolución de las secuencias $\langle 1 \rangle_{n \geq 1}$ y $\langle 1/n \rangle_{n \geq 1}$:

$$\begin{aligned}
\sum_{n \geq 0} H_n z^n &= \left(\sum_{n \geq 0} z^n \right) \cdot \left(\sum_{n \geq 1} \frac{1}{n} z^n \right) \\
&= \frac{1}{1 - z} \cdot (- \ln(1 - z)) \\
&= \frac{1}{1 - z} \cdot \ln \frac{1}{1 - z}
\end{aligned}$$

8. La función generatriz exponencial es simplemente:

$$\begin{aligned}
\widehat{G}(u; z) &= \sum_{n \geq 0} u^{\underline{n}} \frac{z^n}{n!} \\
&= \sum_{n \geq 0} \frac{u^{\underline{n}}}{n!} z^n \\
&= \sum_{n \geq 0} \binom{u}{n} z^n \\
&= (1 + z)^u
\end{aligned}$$

9. Aplicamos la receta. Definimos:

$$\widehat{U}(z) = \sum_{n \geq 0} u_n \frac{z^n}{n!}$$

Multiplicamos la recurrencia por $z^n/n!$ y sumamos para $n \geq 1$:

$$\begin{aligned}
\sum_{n \geq 1} u_n \frac{z^n}{n!} &= \sum_{n \geq 1} n u_{n-1} \frac{z^n}{n!} + \sum_{n \geq 1} \frac{z^n}{n!} \\
\widehat{U}(z) - u_0 &= z \widehat{U}(z) + \mathrm{e}^z - 1
\end{aligned}$$

Despejando, como $u_0 = 1$:

$$\widehat{U}(z) = \frac{\mathrm{e}^z}{1 - z}$$

Por la propiedad de sumas parciales esto nos dice que:

$$\begin{aligned}
\frac{u_n}{n!} &= \sum_{0 \leq k \leq n} \frac{1}{k!} \\
u_n &= \sum_{0 \leq k \leq n} \frac{n!}{k!} \\
&= \sum_{0 \leq k \leq n} n^{\underline{n-k}} \\
&= \sum_{0 \leq k \leq n} n^{\underline{k}}
\end{aligned}$$

Lo último viene del cambio de variable $k \mapsto n - k$.

Otra manera de verlo es que es la suma truncada para e, que converge rápido, con lo que:

$$u_n \approx n! \, \mathrm{e}$$

10. Según el enunciado, $p_k = ca^k$ para algún c. Definamos:

$$\begin{aligned} P(z) &= \sum_{k \geq 0} ca^k z^k \\ &= \frac{c}{1 - az} \end{aligned}$$

Entonces:

$$\begin{aligned} P'(z) &= \frac{ac}{(1 - az)^2} \\ E(k) &= \frac{P'(1)}{P(1)} \\ &= \frac{ac}{(1 - a)^2} \cdot \frac{1 - a}{c} \\ &= \frac{a}{1 - a} \\ P(1) &= \frac{c}{1 - a} \end{aligned}$$

Como $P(1) = 1$, debe ser $c = 1 - a$.

11. La manera más simple de obtener el promedio de una distribución discreta $\langle p_n \rangle_{n \geq 0}$ es:

$$\begin{aligned} P(z) &= \sum_{k \geq 0} p_k z^k \\ P'(z) &= \sum_{k \geq 1} k p_k z^{k-1} \\ E(k) &= P'(1) \end{aligned}$$

Además debe ser $P(1) = 1$. Veamos:

$$\begin{aligned} P(z) &= \sum_{k \geq 0} f(k; r, p) z^k \\ &= \sum_{k \geq 0} \binom{r - 1 + k}{k} \cdot p^r \cdot (1 - p)^k z^k \\ &= p^r \sum_{k \geq 0} \binom{-r}{k} (-(1 - p)z)^k \\ &= p^r (1 - (1 - p)z)^{-r} \end{aligned}$$

Vemos que se cumple $P(1) = 0$. Derivando:

$$\begin{aligned} P'(z) &= p^r (-r)(1 - (1 - p)z)^{-r-1}(-(1 - p)) \\ &= rp^r (1 - p)(1 - (1 - p)z)^{-r-1} \\ P'(1) &= \frac{r(1 - p)}{p} \end{aligned}$$

12. Claramente:

$$\frac{G(z) + G(-z)}{2} = \sum_{n \geq 0} g_{2n} z^{2n}$$

y por lo tanto:

$$\frac{G(z^{1/2}) + G(-z^{1/2})}{2} = \sum_{n \geq 0} g_{2n} z^n \tag{5}$$

Incidentalmente, tenemos de forma similar:

$$\frac{G(z^{1/2}) - G(-z^{1/2})}{2z^{1/2}} = \sum_{n \geq 0} g_{2n+1} z^n \tag{6}$$

La función generatriz de los números de Fibonacci es:

$$F(z) = \frac{z}{1 - z - z^2} \tag{7}$$

por lo que buscamos:

$$\begin{aligned} F_2(z) &= \frac{F(z^{1/2}) + F(-z^{1/2})}{2} \\ &= \frac{z}{1 - 3z + z^2} \end{aligned} \tag{8}$$

13. Encuentre funciones generatrices ordinarias para las siguientes secuencias:

a) $\langle \cos k\pi \rangle_{k \geq 0}$

Esta secuencia no es más que $\langle (-1)^k \rangle_{k \geq 0}$, que corresponde a la serie geométrica con razón $-z$:

$$\sum_{k \geq 0} (-1)^k z^k = \frac{1}{1+z}$$

b) $\langle k^2 \rangle_{k \geq 0}$

Por lo visto en clase, podemos obtener esto aplicando el operador $z \frac{d}{dz}$ dos veces a la serie para la secuencia $\langle 1 \rangle$. O sea, `maxima(1)` mediante:

$$z \frac{d}{dz} \left(z \frac{d}{dz} \frac{1}{1-z} \right) = \frac{2z^2}{(1-z)^3} + \frac{z}{(1-z)^2}$$

c) $\langle k(k-1) \rangle_{k \geq 0}$

Esta secuencia no es más que $\langle k^2 - k \rangle_{k \geq 0}$, y basta entonces obtener la función generatriz para $\langle k^2 \rangle_{k \geq 0}$ y para $\langle k \rangle_{k \geq 0}$, y combinarlas. La primera la tenemos de la pregunta anterior, 13*b*, la de la segunda se obtiene de forma similar a lo hecho allí, y nuevamente nos rescata `maxima`:

$$z \frac{d}{dz} \frac{1}{1-z} = \frac{z}{(1-z)^2}$$

El resultado es entonces:

$$\frac{2z^2}{(1-z)^3} + \frac{z}{(1-z)^2} - \frac{z}{(1-z)^2} = \frac{2z^2}{(1-z)^3}$$

d) $\langle (-1)^k \rangle_{k \geq 0}$

Esto lo resolvimos antes (pregunta 13*a*):

$$\sum_{k \geq 0} (-1)^k z^k = \frac{1}{1+z}$$

e) $\langle \alpha^k \rangle_{k \geq 0}$

Acá buscamos:

$$\begin{aligned} \sum_{k \geq 0} \alpha^k z^k &= \sum_{k \geq 0} (\alpha z)^k \\ &= \frac{1}{1 - \alpha z} \end{aligned}$$

14. Por turno:

   a) De lo visto en clase, esto no es más que aplicar dos veces el operador zD a la serie exponencial:

$$\begin{aligned} (zD)^2 e^z &= zD(ze^z) \\ &= (z^2 + z)e^z \end{aligned}$$

   b) Una combinación lineal:

$$\begin{aligned} ((zD)^2 - zD)e^z &= \big((z^2 + z) - z\big)\, e^z \\ &= z^2 e^z \end{aligned}$$

   c) Esta serie es simplemente:

$$\sum_{k \geq 0} \frac{(-1)^k z^k}{k!} = e^{-z}$$

   d) Similar al caso anterior:

$$\sum_{k \geq 0} \frac{\alpha^k z^k}{k!} = e^{\alpha z}$$

15. Cada una en turno.

   a) Sabemos que:

$$\begin{aligned} \int_0^z z^{n-1} \mathrm{d}z &= \frac{z^n}{n} \\ \frac{1}{z} \int_0^z \int_0^u v^{n-1} \mathrm{d}v \mathrm{d}u &= \frac{z^n}{n^2} \end{aligned}$$

   por lo que:

$$\begin{aligned} \sum_{n \geq 1} \frac{z^n}{n^2} &= \sum_{n \geq 1} \frac{1}{z} \int_0^z \int_0^u v^{n-1} \mathrm{d}v \mathrm{d}u \\ &= \frac{1}{z} \int_0^z \int_0^u \sum_{n \geq 1} v^{n-1} \mathrm{d}v \mathrm{d}u \\ &= \frac{1}{z} \int_0^z \int_0^u \frac{\mathrm{d}v}{1 - v} \mathrm{d}u \\ &= -\frac{1}{z} \int_0^z \ln(1 - u) \mathrm{d}u \\ &= \frac{1 + (1 - z)\ln(1 - z)}{z} \end{aligned}$$

   La misma estrategia pero partiendo de $z^n/n!$ da:

$$\sum_{n \geq 1} \frac{z^n}{n^2\, n!} = \frac{1}{z} \int_0^z \frac{1}{u} \int_0^u \frac{\mathrm{e}^v - 1}{v} \mathrm{d}v \mathrm{d}u$$

   Esto no tiene una forma simple.

   b) Directamente aplicando las definiciones:

$$\begin{aligned} B(z) &= \sum_{n \geq 0} \alpha^n z^n = \sum_{n \geq 0} (\alpha z)^n = \frac{1}{1 - \alpha z} \\ \widehat{B}(z) &= \sum_{n \geq 0} \alpha^n \frac{z^n}{n!} = \sum_{n \geq 0} \frac{(\alpha z)^n}{n!} = e^{\alpha z} \end{aligned}$$

c) Como son términos alternados, podemos expresar la función generatriz ordinaria en términos de z^2. Esto resulta en

$$C(z) = \sum_{n \geq 0} (-1)^n z^{2n} = \frac{1}{1 + z^2}$$

Para función generatriz exponencial:

$$\sum_{n \geq 0} (-1)^n \frac{z^{2n}}{(2n)!} = \cos z$$

d) Como son términos alternados, podemos expresar la función generatriz ordinaria en términos de z^2. Esto resulta en

$$D(z) = \sum_{n \geq 0} 2^n z^{2n} = \frac{1}{1 - \sqrt{2} z^2}$$

Para función generatriz exponencial:

$$\sum_{n \geq 0} 2^n \frac{z^{2n}}{(2n)!} = \sum_{n \geq 0} \frac{(z\sqrt{2})^{2n}}{(2n)!} = \cosh(z\sqrt{2})$$

16. Cada caso en turno.

a) Expandiendo lo indicado:

$$A(z) - A(-z) = \sum_{k \geq 0} a_k z^k - \sum_{k \geq 0} (-1) a_k z^k = 2 \sum_{k \geq 0} a_{2k+1} z^{2k+1}$$

b) Expandiendo lo indicado:

$$A(z) + A(-z) = \sum_{k \geq 0} a_k z^k + \sum_{k \geq 0} (-1) a_k z^k = 2 \sum_{k \geq 0} a_{2k} z^{2k}$$

c) La expansión es muy similar:

$$A(z) + A(\omega z) + A(\omega^2 z) = \sum_{k \geq 0} (1 + \omega^k + \omega^{2k}) a_k z^k$$

Hace falta obtener el valor del factor. Si $3 \mid k$, cada término es 1 y la suma es 3. Por la fórmula exponencial se ve que

$$\omega^m = \omega^{m \bmod 3}$$

Veamos la expresión en cada caso:

$k \equiv 0 \pmod 3$:

$$1 + \omega^k + \omega^{2k} = 1 + \omega^0 + \omega^0 = 3$$

$k \equiv 1 \pmod 3$:

$$1 + \omega^k + \omega^{2k} = 1 + \omega^1 + \omega^2 = 0$$

$k \equiv 2 \pmod 3$:

$$1 + \omega^k + \omega^{2k} = 1 + \omega^2 + \omega^1 = 0$$

d) Vemos la expansión general:

$$\sum_{0 \le r \le n-1} A(\omega_n^r z) = \sum_{k \ge 0} \left(\sum_{0 \le r \le n-1} \omega_n^{kr} \right) a_k z^k$$

Hace falta obtener el valor del factor. Debemos considerar dos casos:

$n \not| k$**:** En tal caso $\omega_n^k \neq 1$, y podemos escribir:

$$\sum_{0 \le r \le n-1} \omega_n^{kr} = \frac{\omega_n^{kn} - 1}{\omega_n^k - 1} = 0$$

$n \mid k$**:** En este caso $\omega_n^k = 1$, y:

$$\sum_{0 \le r \le n-1} \omega_n^{kr} = n$$

En resumen:

$$\sum_{0 \le r \le n-1} \omega_n^{kr} = [n \mid k]$$

Esto sirve para elegir cada n-ésimo término:

$$\begin{aligned} \frac{1}{n} \sum_{0 \le r \le n-1} A(\omega_n^r z) &= \sum_{k \ge 0} [n \mid k] a_k z^k \\ &\overset{\text{ogf}}{\longleftrightarrow} \langle [n \mid k] a_k \rangle_{k \ge 0} \end{aligned}$$

Métodos similares sirven para elegir los demás términos a distancia n.

17. Por completar

18. La idea es expandir ambos lados de la identidad:

$$\begin{aligned} e^{(x+y)t} &= \sum_{n \ge 0} \frac{((x+y)t)^n}{n!} \\ &= \sum_{n \ge 0} (x+y)^n \frac{t^n}{n!} \\ e^{xt} \cdot e^{yt} &= \sum_{n \ge 0} \frac{(xt)^n}{n!} \cdot \sum_{n \ge 0} \frac{(xt)^n}{n!} \\ &= \sum_{n \ge 0} \left(\sum_{0 \le k \le n} \binom{n}{k} x^k y^{n-k} \right) \frac{t^n}{n!} \end{aligned}$$

Si comparamos coeficientes:

$$(x+y)^n = \sum_{0 \le k \le n} \binom{n}{k} x^k y^{n-k}$$

19. Esto es sumas parciales. Con la función generatriz de los números de Fibonacci:

$$F(z) = \frac{z}{1 - z - z^2}$$

para las sumas parciales tenemos:

$$\begin{aligned} \frac{1}{1-z} \cdot F(z) &= \frac{1+z}{1-z-z^2} - \frac{1}{1-z} \\ &= \frac{F(z) - F_0}{z} + F(z) - \frac{1}{1-z} \end{aligned}$$

La secuencia correspondiente es

$$F_{n+1} + F_n - 1 = F_{n+2} - 1$$

20. Alguna notación no viene mal:

$$\begin{aligned} s_n &= \sum_{0 \le k \le n} F_k F_{n-k} \\ S(z) &= \sum_{n \ge 0} s_n z^n \end{aligned}$$

El término s_n es una convolución, por lo que la función generatriz ordinaria es:

$$S(z) = F(z) \cdot F(z) \qquad = \frac{1-z}{(1-z-z^2)^2} - \frac{1}{1-z-z^2}$$

El segundo término es simple de manejar, veamos el primero:

$$\frac{1-z}{(1-z-z^2)^2} = \frac{6\tau}{5\sqrt{5}} \cdot \frac{1}{1-\tau z} - \frac{6(1-\tau)}{5\sqrt{5}} \cdot \frac{1}{1-(1-\tau)z} + \frac{1}{5} \cdot \frac{1}{(1-\tau z)^2} + \frac{1}{5} \cdot \frac{1}{(1-(1-\tau)z)^2}$$

Leemos los coeficientes:

$$[z^n]\, \frac{1-z}{(1-z-z^2)^2} = \frac{6}{5\sqrt{5}} \cdot \left(\tau^{n+1} - (1-\tau)^{n+1}\right) + \frac{1}{5} \cdot \frac{n+1}{1} \cdot (\tau^n + (1-\tau)^n)$$

Verificar, completar

21. Por completar

22. Atacamos cada punto en orden.

   a) Usamos el principio extendido del palomar. Los valores de la expresión:

   $$\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 5\alpha_5$$

   donde $\alpha_i \in \{0, 1\}$ van desde 0 (sólo cuando todos los $\alpha_i = 0$) hasta 15 (sólo cuando todos los $\alpha_i = 1$). Entonces hay un total de 16 valores posibles, generados por $2^5 = 32$ combinaciones de valores de los α_i. Pero hay dos valores que se generan de una única manera, por lo que hay $16 - 2 = 14$ valores generados por $32 - 2 = 30$ combinaciones. Como $30/14 = 2{,}14\ldots$, tiene que haber un valor con al menos tres representaciones.

   b) El aporte al valor de la expresión de α_i es 0 ó i, por lo que cada uno queda representado por un factor $1 + x^i$ en la función generatriz. Con esto, tenemos la función generatriz, y de ella el número de maneras de obtener el valor n de la expresión, v_n:

   $$\begin{aligned} g(x) &= (1+x^1)(1+x^2)(1+x^3)(1+x^4)(1+x^5) \\ v_n &= [x^n]\, g(x) \end{aligned}$$

   Incidentalmente, `maxima` nos dice que:

   $$\begin{aligned} g(x) = x^{15} &+ x^{14} + x^{13} + 2x^{12} + 2x^{11} + 3x^{10} + 3x^9 + x^8 \\ &+ 3x^7 + 3x^6 + 3x^5 + 2x^4 + 2x^3 + x^2 + x + 1 \end{aligned}$$

23. El número k aporta entre 0 y k^2 a la suma, en múltiplos de k, así que le corresponde el factor $1 + x^k + x^{2k} + \ldots + x^{k^2}$ en la función generatriz:

$$\begin{aligned} P_r(x) &= \prod_{k \ge 1} (1 + x^k + x^{2k} + \ldots + x^{k^2}) \\ &= \prod_{k \ge 1} \frac{1 - x^{k(k+1)}}{1 - x^k} \end{aligned}$$

Esto no se puede simplificar mucho más.

24. Al considerar la pista:

$$\begin{aligned}
H(z,1) &= \sum_{\substack{n\geq 0\\ k\geq 0}} \begin{bmatrix} n \\ k \end{bmatrix} \frac{z^n}{n!} \frac{1}{1-z} \\
&= \sum_{n\geq 0} \frac{z^n}{n!} \sum_{0\leq k\leq n} \begin{bmatrix} n \\ k \end{bmatrix}
\end{aligned}$$

$$\sum_{n\geq 0} z^n = \frac{1}{1-z}$$

Acá usamos el hecho que $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right] = 0$ cuando $k > n$. Comparando coeficientes:

$$\frac{1}{n!} \sum_{0\leq k\leq n} \begin{bmatrix} n \\ k \end{bmatrix} = 1$$

25. La identidad sugerida es simplemente

$$(1+z)^u \cdot (1+z)^v = (1+z)^{u+v}$$

que claramente es correcto.

De la identidad anterior, aplicando la fórmula para el producto de funciones generatrices exponenciales

$$\begin{aligned}
\sum_{n\geq 0} (u+v)^{\underline{n}} \frac{z^n}{n!} &= \left(\sum_{n\geq 0} u^{\underline{n}} \frac{z^n}{n!} \right) \cdot \left(\sum_{n\geq 0} v^{\underline{n}} \frac{z^n}{n!} \right) \\
&= \sum_{n\geq 0} \left(\sum_{0\leq k\leq n} \binom{n}{k} u^{\underline{k}} v^{\underline{n-k}} \right) \frac{z^n}{n!}
\end{aligned}$$

Comparando coeficientes, resulta:

$$(u+v)^{\underline{n}} = \sum_{0\leq k\leq n} \binom{n}{k} u^{\underline{k}} v^{\underline{n-k}}$$

Curiosamente parecido al teorema del binomio.

26. Cada incógnita de la ecuación puede tomar valores entre α y β, es decir, la función generatriz que cuenta las formas en que cada incógnita puede tomar un valor dado es:

$$A(z) = 1 \cdot z^{\alpha} + 1 \cdot z^{\alpha+1} + \ldots + 1 \cdot z^{\beta-1} + 1 \cdot z^{\beta}$$

Esto se lee como: x puede tomar el valor α de 1 forma, hay 1 sola forma de que x tome el valor $\alpha+1$, ... y finalmente x puede tomar el valor β de sólo una forma. Tenemos n incógnitas, y las formas de elegir el valor de cada incógnita está dada por la función generatriz $A(z)$, por lo que $A(z)^n$ representa las formas en total de elegir los valores para las incógnitas. Luego $\left[z^k\right] A(z)^n$ será el número total de formas de elegir los valores de los x_i para que cumplan con las condiciones (sumen k).

Resulta que:

$$\begin{aligned}
A(z) &= z^{\alpha} + z^{\alpha+1} + \ldots + z^{\beta} \\
&= z^{\alpha} \cdot \frac{1 - z^{\beta-\alpha+1}}{1-z}
\end{aligned}$$

con lo que:

$$
\begin{aligned}
\left[z^k\right] A^n(z) &= \left[z^k\right] z^{n\alpha} \left(\frac{1 - z^{\beta-\alpha+1}}{1 - z} \right)^n \\
&= \left[z^{k-n\alpha}\right] \left(\frac{1 - z^{\beta-\alpha+1}}{1 - z} \right)^n \\
&= \left[z^{k-n\alpha}\right] (1 - z^{\beta-\alpha+1})^n \cdot (1 - z)^{-n} \\
&= \left[z^{k-n\alpha}\right] \left(\sum_{r\geq 0} \binom{n}{r} (-1)^r z^{r(\beta-\alpha+1)} \right) \cdot \left(\sum_{r\geq 0} \binom{-n}{r} (-1)^r z^r \right) \\
&= \left[z^{k-n\alpha}\right] \left(\sum_{r\geq 0} \binom{n}{r} (-1)^r z^{r(\beta-\alpha+1)} \right) \cdot \left(\sum_{r\geq 0} \binom{n+r-1}{n} z^r \right)
\end{aligned}
$$

27. Primero algunos valores simples, para contrastar luego:

$k = 1$: Claramente es n.

$k = 2$: Podemos elegir dos elementos de $\binom{n}{2}$ maneras, de las cuales debemos restar las $n-1$ formas de tenerlos de vecinos, para un total de $(n-1)(n-2)/2$.

$n = 2k - 1$: Esto es poner los elementos en posiciones alternas, lo que puede hacerse de una única forma.

Sea el conjunto $\{a_1, a_2, \dots, a_k\}$ con elementos crecientes, con lo que:

$$
\begin{aligned}
a_1 &\geq 1 \\
a_2 &\geq a_1 + 2 \\
&\vdots \\
a_k &\geq a_{k-1} + 2 \\
n &\geq a_k
\end{aligned}
$$

Definamos nuevas variables:

$$
\begin{aligned}
x_1 &= a_1 && \geq 1 \\
x_2 &= a_2 - a_1 && \geq 2 \\
&\vdots \\
x_k &= a_k - a_{k-1} && \geq 2 \\
x_{k+1} &= n - a_k && \geq 0
\end{aligned}
$$

Tenemos además:

$$
\sum_{1\leq r\leq k+1} x_r = n
$$

Planteando funciones generatrices para cada una de las variables, resulta que el valor que nos interesa no es más que:

$$
\begin{aligned}
[z^n] \frac{z}{1-z} \cdot \left(\frac{z^2}{1-z} \right)^{k-1} \cdot \frac{1}{1-z} &= [z^n] \frac{z^{2k-1}}{(1-z)^{k+1}} \\
&= [z^{n-2k+1}] (1-z)^{-k-1} \\
&= \binom{-k-1}{n-2k+1} \\
&= \binom{n-k+1}{k}
\end{aligned}
$$

Esto coincide con los valores calculados al comienzo.

28. Sabemos que la función generatriz ordinaria de los números de Fibonacci es:

$$F(z) = \frac{z}{1 - z - z^2}$$

Con esto y las propiedades de las funciones generatrices ordinarias:

a) Para la secuencia $\langle nF_n \rangle_{n \geq 0}$:

$$zDF(z) = \frac{z + z^3}{1 - 2z - z^2 + 2z^3 + z^4}$$

b) Estas son sumas parciales:

$$\begin{aligned} \frac{F(z)}{1 - z} &= \frac{1 + z}{1 - z - z^2} - \frac{1}{1 - z} \\ &= F(z) + \frac{F(z) - F_0}{z} - \frac{1}{1 - z} \end{aligned}$$

Esto corresponde directamente a:

$$F_n + F_{n+1} - 1 = F_{n+2} - 1$$

29. Podemos elegir 1, 3 ó 5 globos amarillos, lo que se traduce en un factor $z + z^3 + z^5$. Los rojos aportan $z^2 + z^3 + z^4$, los blancos $z + z^4 + z^5$. En total, las maneras de elegir n globos será

$$[z^n] \, (z + z^3 + z^5) \cdot (z^2 + z^3 + z^4) \cdot (z + z^4 + z^5)$$

El polinomio resultante es

$$z^{14} + 2z^{13} + 3z^{11} + 4z^10 + 4z^9 + 4z^8 + 2z^7 + 2z^6 + z^5 + z^4$$

Esto nos dice que hay 4 maneras de elegir 10 globos. Pero también que no hay forma de elegir 12, y que el mínimo número de globos es 4 y el máximo 14.

30. Como el orden de las preguntas no interesa y son todas igual, las series representativas son todas las mismas y corresponden a:

$$x^{15} + x^{20} + x^{25} + x^{30} + x^{35}$$

Dado que son 4 preguntas la función generatriz es:

$$(x^{15} + x^{20} + x^{25} + x^{30} + x^{35})^4$$

La cantidad buscada es el coeficiente de la potencia de x^{100}. Pero esto es feo y difícil de calcular, el truco está en que todos son múltiplos de 5, incluso 100, por lo que con la substitución $y = x^5$ todo se reduce a:

$$\begin{aligned} \left[x^{100}\right] (x^{15} + x^{20} + x^{25} + x^{30} + x^{35})^4 &= \left[y^{20}\right] (y^3 + y^4 + y^5 + y^6 + y^7)^4 \quad = \left[y^{20}\right] y^{12}(1 + y + y^2 + y^3 + y^4)^4 \\ &= \left[y^8\right] (1 + y^2 + y^3 + y^4 + y^5)^4 \end{aligned}$$

El coeficiente buscado es 85.

31. Como importa el orden, debemos usar funciones generatrices exponenciales. El resultado es:

$$\left[\frac{z^8}{8!}\right] \left(\frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!}\right) \left(\frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!}\right) \left(1 + \frac{z^2}{2!} + \frac{z^4}{3!}\right)$$

El resultado es 1 680.

32. El primer término aporta:

$$\begin{aligned}\binom{-3}{n}(-2)^n &= (-1)^n\binom{3+n-1}{3-1}(-2)^n = \binom{n+2}{2}2^n \\ &= \frac{(n+2)(n+1)}{2}\cdot 2^n = (n+2)(n+1)\cdot 2^{n-1} \\ &= (n^2+3n+2)\cdot 2^{n-1}\end{aligned}$$

El segundo da:

$$-5\cdot(-3)^n$$

El tercero es la suma parcial de los términos de e^{-1}:

$$\sum_{0\le k\le n}\frac{(-1)^n}{n!}$$

En resumen:

$$a_n = (n^2+3n+2)\cdot 2^{n-1} - 5\cdot(-3)^n + \sum_{0\le k\le n}\frac{(-1)^n}{n!}$$

33. Veamos primero las situaciones planteadas, luego comentamos. No usaremos sólo funciones generatrices, en todo caso.

   a) Si la consideramos como un conjunto de letras, la palabra `BOOKKEEPER` es simplemente $\{\mathtt{B},\mathtt{E},\mathtt{K},\mathtt{O},\mathtt{P},\mathtt{R}\}$, un conjunto de 6 letras. Estamos eligiendo 5, o sea hay:

   $$\binom{6}{5} = \binom{6}{1} = 6$$

   formas de hacer esto.

   Si consideramos esto como multiconjuntos, estamos preguntando cuántos subconjuntos de 5 elementos tiene $\{\mathtt{B},\mathtt{E}^3,\mathtt{K}^2,\mathtt{O}^2,\mathtt{P},\mathtt{R}\}$. El aporte que hacen, por ejemplo, las letras `E` es 0, 1, 2 ó 3; como función generatriz ordinaria (porque el orden no importa) esto es $1+x+x^2+x^3$. Similarmente para las demás letras, y nos queda para la función generatriz ordinaria $m(x)$ de las formas de obtener multisubconjuntos de n elementos:

   $$\begin{aligned}m(x) &= (1+x)^3(1+x+x^2+x^3)(1+x+x^2)^2 \\ &= 1+6x+18x^2+36x^3+53x^4+60x^5+53x^6+36x^7+18x^8+6x^9+x^{10}\end{aligned}$$

   Basta leer el coeficiente de x^5, o sea hay 60 formas.

   b) Esto es similar al caso anterior, sólo que ahora el orden sí importa, y deben usarse funciones generatrices exponenciales. Con un razonamiento similar al anterior:

   $$\begin{aligned}p(x) &= \left(1+\frac{x}{1!}\right)^3\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}\right)\left(1+\frac{x}{1!}+\frac{x^2}{2!}\right)^2 \\ &= 1+6\,\frac{x}{1!}+33\,\frac{x^2}{2!}+166\,\frac{x^3}{3!}+758\,\frac{x^4}{4!}+3\,100\,\frac{x^5}{5!}+11\,130\,\frac{x^6}{6!}+34\,020\,\frac{x^7}{7!}+84\,000\,\frac{x^8}{8!} \\ &\qquad +151\,200\,\frac{x^9}{9!}+151\,200\,\frac{x^{10}}{10!}\end{aligned}$$

   El valor pedido es 3 100. También resulta que las formas de tener palabras de largo 10 es

   $$151\,200 = \binom{10}{1\;1\;1\;3\;2\;2}$$

   como debiera ser.

Las diferencias entre estos tres resultados se explican por la diferencia entre conjuntos (cada elemento está representado una única vez), multiconjuntos (un elemento puede aparecer varias veces, el orden no importa) y palabras (el elemento puede aparecer varias veces, el orden importa).

34. Podemos plantear esto como el coeficiente de un producto de funciones generatrices ordinarias. Para x_1 tenemos:

$$1 + x + x^2 + x^3 = \frac{1 - x^4}{1 - x}$$

Similarmente para x_2 y x_3, y queda:

$$[x^{11}] \, \frac{1 - x^4}{1 - x} \cdot \frac{1 - x^5}{1 - x} \cdot \frac{1 - x^7}{1 - x} = 6$$

35. La función generatriz es:

$$\begin{aligned}\frac{6 + 5x + x^2}{3 - 4x^2 + x^4} &= -\frac{3^{5/2} - 15}{12} \cdot \frac{1}{x + \sqrt{3}} + \frac{3^{5/2} + 15}{12} \cdot \frac{1}{x - \sqrt{3}} + \frac{1}{2} \cdot \frac{1}{x + 1} - 3 \cdot \frac{1}{x - 1} \\ &= -\frac{9 + 5\sqrt{3}}{12} \cdot \frac{1}{1 - x/\sqrt{3}} + 3 \cdot \frac{1}{1 - x} + \frac{1}{2} \cdot \frac{1}{1 + x} - \frac{9 - 5\sqrt{3}}{12} \cdot \frac{1}{1 + x/\sqrt{3}}\end{aligned}$$

Podemos leer los coeficientes de esto:

$$s_n = -\frac{9 + 5\sqrt{3}}{12} \cdot \left(\sqrt{3}\right)^{-n} - \frac{9 - 5\sqrt{3}}{12} \cdot \left(-\sqrt{3}\right)^{-n} + 3 + \frac{1}{2}(-1)^n$$

Los valores pedidos son:

$$2, \frac{5}{3}, 3, \frac{20}{9}$$

Otra forma es hacer trampa, y expandir directamente mediante serie de Maclaurin…

Tipo	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Manzanas	6	4	4	2	2	0	0
Plátanos	0	0	0	0	0	5	5
Naranjas	0	2	1	4	3	1	0
Peras	0	0	1	0	1	0	1

Cuadro 6: Canastos con seis frutas

36. Por ejemplo, tomemos un canasto de seis frutas. Hay siete posibilidades en total, como se ve de explorar sistemáticamente las opciones que tenemos (ver el cuadro 6).

Las funciones generatrices correspondientes a cada tipo de fruta en nuestro problema son:

- Para manzanas se tiene:

$$1 + x^2 + x^4 + \ldots = \frac{1}{1 - x^2}$$

- Para plátanos se tiene:

$$1 + x^5 + x^{10} + \ldots = \frac{1}{1 - x^5}$$

- Para las naranjas:

$$1 + x + x^2 + x^3 + x^4 = \frac{1 - x^5}{1 - x}$$

- Las peras aportan:

$$1 + x$$

La función generatriz para el número de canastos con n frutas es el producto de todas las anteriores:

$$\begin{aligned}
g(x) &= \frac{1}{1 - x^2} \cdot \frac{1}{1 - x^5} \cdot \frac{1 - x^5}{1 - x} \cdot (1 + x) \\
&= \frac{1}{(1 - x)^2}
\end{aligned}$$

Por lo tanto hay $\binom{n+1}{1} = n + 1$ maneras diferentes de llenar el canasto con n frutas, lo que es consistente con el resultado que obtuvimos directamente para canastos con seis frutas.

37. Por turno:

    a) Por la regla de la cadena:

    $$\widehat{B}'(z) = e^{e^z - 1} e^z = \widehat{B}(z) e^z$$

    Complementamos esto con el valor $\widehat{B}(0) = 1$, obtenido de la función generatriz.

    b) Por las propiedades de funciones generatrices exponenciales, el lado izquierdo de esta ecuación diferencial corresponde a un desplazamiento y el derecho a una convolución binomial. La condición inicial de la ecuación diferencial da el valor inicial para la recurrencia:

    $$B_{n+1} = \sum_{0 \le k \le n} \binom{n}{k} B_k \qquad B_0 = 1$$

38. Usamos la técnica de aceite de serpiente. Como n siempre aparece como $2n$, parece probable que deberemos extraer coeficientes pares luego, así evaluaremos:

$$\begin{aligned}
&\sum_{n \ge 0} \sum_{0 \le k \le n} (-1)^k \binom{2n - k}{k} 2^{2n - 2k} z^{2n} \\
&\qquad = \sum_{k \ge 0} (-1)^k \sum_{n \ge k} \binom{2n - k}{2n - 2k} 2^{2n - 2k} z^{2n}
\end{aligned}$$

Con el cambio de variables $r = n - k$:

$$\begin{aligned}
&= \sum_{k \ge 0} (-1)^k \sum_{r \ge 0} \binom{k + 2r}{2r} 2^{2r} z^{2k + 2r} \\
&= \sum_{k \ge 0} (-1)^k z^{2k} \sum_{r \ge 0} \binom{k + 2r}{2r} (2z)^{2r}
\end{aligned}$$

La última suma son los términos pares de:

$$\sum_{r \ge 0} \binom{k + r}{r} (2z)^r = (1 - 2z)^{-k-1}$$

O sea:

$$\sum_{r \ge 0} \binom{k + 2r}{2r} (2z)^{2r} = \frac{(1 - 2z)^{-k-1} + (1 + 2z)^{-k-1}}{2}$$

Uniendo las partes:

$$
\begin{aligned}
&\sum_{n \geq 0} \sum_{0 \leq k \leq n} (-1)^k \binom{2n-k}{k} 2^{2n-2k} z^{2n} \\
&\qquad = \frac{1}{2} \sum_{k \geq 0} (-1)^k z^{2k} \frac{(1-2z)^{-k-1} + (1+2z)^{-k-1}}{2} \\
&\qquad = \frac{1}{2(1-2z)} \sum_{k \geq 0} \left(-\frac{z^2}{1-2z} \right)^k + \frac{1}{2(1+2z)} \sum_{k \geq 0} \left(-\frac{z^2}{1+2z} \right)^k \\
&\qquad = \frac{1}{2} \left(\frac{1}{(1-z)^2} + \frac{1}{(1+z)^2} \right)
\end{aligned}
$$

De acá, como los valores que nos interesan son los coeficientes pares:

$$
\begin{aligned}
\sum_{0 \leq k \leq n} (-1)^k \binom{2n-k}{k} 2^{2n-2k} &= [z^{2n}] \frac{1}{2} \left(\frac{1}{(1-z)^2} + \frac{1}{(1+z)^2} \right) \\
&= \frac{1}{2} \left(\binom{-2}{2n} (-1)^{2n} + \binom{-2}{2n} \right) \\
&= \frac{1}{2} \left(\binom{2n+1}{1} + \binom{2n+1}{1} (-1)^{2n} \right) \\
&= 2n+1
\end{aligned}
$$

39. Funciones generatrices al rescate. Definamos:

$$
\begin{aligned}
A(t) &= \sum_{x \geq 0} x t^x \\
B(t) &= \sum_{y \geq 0} y^2 t^y \\
C(t) &= \sum_{z \geq 0} z^3 t^z
\end{aligned}
$$

con lo que buscamos $[t^{2014}] A(t) \cdot B(t) \cdot C(t)$. En detalle:

$$
\begin{aligned}
A(t) &= t \frac{\mathrm{d}}{\mathrm{d}t} \frac{1}{1-t} \\
&= \frac{t}{(1-t)^2} \\
B(t) &= t A'(t) \\
&= \frac{t + t^2}{(1-t)^3} \\
C(t) &= t B'(t) \\
&= \frac{t + 4t^2 + t^3}{(1-t)^4}
\end{aligned}
$$

Maxima mediante, tenemos:

$$
A(t) \cdot B(t) \cdot C(t) = \frac{1}{(1-t)^3} - \frac{11}{(1-t)^4} + \frac{45}{(1-t)^5} - \frac{91}{(1-t)^6} + \frac{98}{(1-t)^7} - \frac{54}{(1-t)^8} + \frac{12}{(1-t)^9}
$$

El valor buscado es el coeficiente de t^{2014} en esto. Cada término queda multiplicado por $(-1)^{2014} = 1$, que omitimos para ahorrar espacio::

$$
\binom{-3}{2014} - 11 \cdot \binom{-4}{2014} + 45 \cdot \binom{-5}{2014} - 91 \cdot \binom{-6}{2014} + 98 \cdot \binom{-7}{2014} - 54 \cdot \binom{-8}{2014} + 12 \cdot \binom{-9}{2014}
$$

Resulta:

$$80\,563\,059\,846\,280\,425\,949\,392$$

40. Podemos elegir las tres variables a tomar valor impar de $\binom{6}{3}$ maneras. Como funciones generatrices, una variable con valor par queda representada por:

$$1 + z^2 + \cdots = \frac{1}{1 - z^2}$$

mientras para una variable de valor impar:

$$z + z^2 + \cdots = \frac{z}{1 - z^2}$$

Nos interesa:

$$\begin{aligned}
[z^{29}]\frac{z^3}{(1 - z^2)^6} &= [z^{26}](1 - z^2)^{-6} \\
&= [u^{13}](1 - u)^{-6} \\
&= (-1)^{13}\binom{-6}{13} \\
&= \binom{13 + 6 - 1}{6 - 1}
\end{aligned}$$

Según posibles distribuciones de paridad:

$$\binom{6}{3} \cdot \binom{18}{5} = 171\,360$$

41. Podemos expresar el lado derecho como:

$$\begin{aligned}
\sum_{1 \le k \le n} \frac{1}{k} &= \sum_{1 \le k \le n} \int_0^1 x^{k-1}\,\mathrm{d}x \\
&= \int_0^1 \frac{1 - x^n}{1 - z}\,\mathrm{d}x \\
&= \int_0^1 \frac{1 - (1 - y)^n}{y}\,\mathrm{d}y \\
&= \int_0^1 \sum_{1 \le k \le n} \binom{n}{k}(-1)^{k+1} y^{k-1}\,\mathrm{d}y \\
&= \sum_{1 \le k \le n} \binom{n}{k}(-1)^{k+1} \int_0^1 y^{k-1}\,\mathrm{d}y \\
&= \sum_{1 \le k \le n} \frac{(-1)^{k+1}}{k}\binom{n}{k}
\end{aligned}$$

Exactamente el lado izquierdo de la identidad.

42. Podemos representar esto mediante funciones generatrices. Cada variable aporta:

$$1 + z + z^2$$

por lo que con 3 variables:

$$
\begin{aligned}
[z^n](1+z+z^2)^3 &= [z^n]\frac{(1-z^3)^3}{(1-z)^3} \\
&= [z^n](1-3z+3z^2-z^3)\sum_{k\geq 0}(-1)^k\binom{-3}{k}z^k \\
&= ([z^n]-3[z^{n-1}+3[z^{n-2}]-[z^{n-3}])\sum_{k\geq 0}\binom{k+3-1}{3-1}z^k \\
&= \binom{n+2}{2}-3\binom{n+1}{2}+3\binom{n}{2}-\binom{n-1}{2} \\
&= \frac{(n+2)(n+1)n}{2}-3\frac{(n+1)n(n-1)}{2}+3\frac{n(n-1)(n-2)}{2}-\frac{(n-1)(n-2)(n-3)}{2} \\
&= 4n^2+2
\end{aligned}
$$

12. Aceite de serpiente

1. Usamos aceite de serpiente. Definimos:

$$S(z) = \sum_{n \geq 0} s(n) z^n$$

O sea, como el límite sobre k en realidad es superfluo:

$$\begin{aligned}
S(z) &= \sum_{n \geq 0} z^n \sum_{k \geq 0} \binom{n}{2k} \binom{2k}{k} 4^{-k} \\
&= \sum_{k \geq 0} \binom{2k}{k} 4^{-k} \sum_{n \geq 0} \binom{n}{2k} z^n \\
&= \sum_{k \geq 0} \binom{2k}{k} 4^{-k} \cdot \frac{z^{2k}}{(1-z)^{2k+1}} \\
&= \frac{1}{1-z} \sum_{k \geq 0} \binom{2k}{k} \left(\frac{z}{2(1-z)} \right)^{2k} \\
&= \frac{1}{1-z} \left(1 - 4 \cdot \frac{z^2}{4(1-z)^2} \right)^{-1/2} \\
&= (1-2z)^{-1/2} \\
s(n) &= [z^n]\, S(z) \\
&= (-2)^n \binom{-1/2}{n} \\
&= (-2)^n \cdot \frac{(-1)^n}{2^{2n}} \binom{2n}{n} \\
&= \frac{1}{2^n} \binom{2n}{n}
\end{aligned}$$

2. Usamos la técnica de aceite de serpiente. Como n siempre aparece como $2n$, parece probable que deberemos extraer coeficientes pares luego, así evaluaremos:

$$\begin{aligned}
&\sum_{n \geq 0} \sum_{0 \leq k \leq n} (-1)^k \binom{2n-k}{k} 2^{2n-2k} z^{2n} \\
&\qquad = \sum_{k \geq 0} (-1)^k \sum_{n \geq k} \binom{2n-k}{2n-2k} 2^{2n-2k} z^{2n}
\end{aligned}$$

Con el cambio de variables $r = n - k$:

$$\begin{aligned}
&= \sum_{k \geq 0} (-1)^k \sum_{r \geq 0} \binom{k+2r}{2r} 2^{2r} z^{2k+2r} \\
&= \sum_{k \geq 0} (-1)^k z^{2k} \sum_{r \geq 0} \binom{k+2r}{2r} (2z)^{2r}
\end{aligned}$$

La última suma son los términos pares de:

$$\sum_{r \geq 0} \binom{k+r}{r} (2z)^r = (1-2z)^{-k-1}$$

O sea:

$$\sum_{r \geq 0} \binom{k+2r}{2r} (2z)^{2r} = \frac{(1-2z)^{-k-1} + (1+2z)^{-k-1}}{2}$$

Uniendo las partes:

$$\begin{aligned}
\sum_{n\geq 0}\sum_{0\leq k\leq n}(-1)^k\binom{2n-k}{k}2^{2n-2k}z^{2n} &= \frac{1}{2}\sum_{k\geq 0}(-1)^k z^{2k}\,\frac{(1-2z)^{-k-1}+(1+2z)^{-k-1}}{2} \\
&= \frac{1}{2(1-2z)}\sum_{k\geq 0}\left(-\frac{z^2}{1-2z}\right)^k + \frac{1}{2(1+2z)}\sum_{k\geq 0}\left(-\frac{z^2}{1+2z}\right)^k \\
&= \frac{1}{2}\left(\frac{1}{(1-z)^2}+\frac{1}{(1+z)^2}\right)
\end{aligned}$$

De acá, como los valores que nos interesan son los coeficientes pares:

$$\begin{aligned}
\sum_{0\leq k\leq n}(-1)^k\binom{2n-k}{k}2^{2n-2k} &= [z^{2n}]\frac{1}{2}\left(\frac{1}{(1-z)^2}+\frac{1}{(1+z)^2}\right) \\
&= \frac{1}{2}\left(\binom{-2}{2n}(-1)^{2n}+\binom{-2}{2n}\right) \\
&= \frac{1}{2}\left(\binom{2n+1}{1}+\binom{2n+1}{1}(-1)^{2n}\right) \\
&= 2n+1
\end{aligned}$$

3. Por completar
4. Aplicación directa de la técnica, variable libre es n:

$$\sum_{n\geq 0}z^n\sum_k\binom{k}{n-k} = \sum_k\sum_{n\geq 0}\binom{k}{n-k}z^n$$

Para $n<k$ los términos de la suma interna se anulan. Cambiamos de variable a $r=n-k$:

$$\begin{aligned}
&= \sum_k\sum_{r\geq 0}\binom{k}{r}z^{r+k} \\
&= \sum_k z^k\sum_{r\geq 0}\binom{k}{r}z^r \\
&= \sum_k z^k(1+z)^k \\
&= \frac{1}{1-z(1+z)} \\
&= \frac{1}{1-z-z^2}
\end{aligned}$$

Esta última se parece sospechosamente a la función generatriz de los números de Fibonacci:

$$\begin{aligned}
F(z) &= \sum_{n\geq 0}F_n z^n \\
&= \frac{z}{1-z-z^2}
\end{aligned}$$

Como $F_0=0$, resulta:

$$\frac{1}{1-z-z^2} = \frac{F(z)-F_0}{z}$$

O sea:

$$\sum_k\binom{k}{n-k} = F_{n+1}$$

5. Vemos que los límites son irrelevantes, los dejaremos de lado para evitarnos tener que considerarlos. Elegimos m como variable libre:

$$\begin{aligned}\sum_{m\geq 0} S_m z^m &= \sum_{m\geq 0} z^m \sum_k (-1)^k \binom{n}{k}\binom{k}{m} \\ &= \sum_k (-1)^k \binom{n}{k} \sum_{m\geq 0} \binom{k}{m} z^m\end{aligned}$$

Por el teorema del binomio tenemos la suma interna:

$$= \sum_k (-1)^k \binom{n}{k} (1+z)^k$$

Nuevamente teorema del binomio:

$$\begin{aligned}&= (1-(1+z))^n \\ &= (-1)^n z^n\end{aligned}$$

Vale decir:

$$\sum_{m\leq k\leq n} (-1)^k \binom{n}{k}\binom{k}{m} = \begin{cases} 0 & m \neq n \\ (-1)^n & m = n\end{cases}$$

6. Vemos que los límites son irrelevantes, los dejaremos de lado para evitar considerarlos. Elegimos m como variable libre:

$$\begin{aligned}\sum_{m\geq 0} z^m \sum_k \binom{n}{k}\binom{k}{m} &= \sum_k \binom{n}{k} \sum_{m\geq 0} \binom{k}{m} z^m \\ &= \sum_k \binom{n}{k} (1+z)^k \\ &= (1+(1+z))^n \\ &= (2+z)^n\end{aligned}$$

En consecuencia:

$$\begin{aligned}\sum_{m\leq k\leq n} \binom{n}{k}\binom{k}{m} &= [z^m](2+z)^n \\ &= \binom{n}{m} 2^{n-m}\end{aligned}$$

7. La parte entera solo está para confundir... la suma puede escribirse:

$$\begin{aligned}\sum_k \binom{n}{k} \left(x^{2k} + x^{2k+1}\right) &= (1+x) \sum_k \binom{n}{k} x^{2k} \\ &= (1+x)(1+x^2)^n\end{aligned}$$

8. Elegimos n como variable de suma:

$$\begin{aligned}\sum_n z^n \sum_k \binom{n+k}{m+2k}\binom{2k}{k}\frac{(-1)^k}{k+1} &= \sum_k \binom{2k}{k}\frac{(-1)^k}{k+1} z^{-k} \sum_n \binom{n+k}{m+2k} z^{n+k} \\ &= \sum_k \binom{2k}{k}\frac{(-1)^k}{k+1} z^{-k} \frac{z^{m+2k}}{(1-z)^{m+2k+1}} \\ &= \frac{z^m}{(1-z)^{m+1}} \sum_k \frac{1}{k+1}\binom{2k}{k} \cdot \left(\frac{-z}{(1-z)^2}\right)^k\end{aligned}$$

Completar...

9. Trabajamos sobre el lado izquierdo:

$$\sum_{n\geq 0} z^n \sum_k \binom{2n}{2k}\binom{2k}{k} 2^{2n-2k} = \sum_k \binom{2k}{k} 2^{-2k} \sum_{n\geq 0} \binom{2n}{2k} 2^{2n} z^n$$

La suma interna es de los términos pares de:

$$\sum_{r\geq 0} \binom{r}{2k} (2\sqrt{z})^r = \frac{(2\sqrt{z})^{2k}}{(1-2\sqrt{z})^{2k+1}}$$

por lo que:

$$\sum_{n\geq 0} \binom{2n}{2k} 2^{2n} z^n = \frac{1}{2}\left(\frac{(2\sqrt{z})^{2k}}{(1-2\sqrt{z})^{2k+1}} + \frac{(-2\sqrt{z})^{2k}}{(1+2\sqrt{z})^{2k+1}}\right)$$

Completar…

10. El cambio de variable $r = p + k$ junto con la simetría de los coeficientes binomiales simplifica la fórmula dada a:

$$\sum_k \binom{2n+1}{2r+1}\binom{r}{p}$$

Como solo aparece $2n + 1$ es natural intentar:

$$\sum_n z^{2n+1} \sum_k \binom{2n+1}{2r+1}\binom{r}{p} = \sum_r \binom{r}{p} \sum_n \binom{2n+1}{2r+1} z^{2n+1}$$

La suma interna es de los términos impares en:

$$\sum_s \binom{s}{2r+1} z^s = \frac{z^{2r+1}}{(1-z)^{2r+2}}$$

por lo que:

$$\sum_n \binom{2n+1}{2r+1} z^{2n+1} = \frac{z^{2r+1}}{2}\left(\frac{1}{(1-z)^{2r+2}} + \frac{1}{(1+z)^{2r+2}}\right)$$

Substituyendo y separando en dos sumas:

$$\begin{aligned}\sum_n z^{2n+1} \sum_k \binom{2n+1}{2r+1}\binom{r}{p} &= \frac{1}{2}\cdot\frac{z}{(1-z)^2}\sum_r \binom{r}{p}\left(\frac{z^2}{(1-z)^2}\right)^r + \frac{1}{2}\cdot\frac{z}{(1-z)^2}\sum_r \binom{r}{p}\left(\frac{z^2}{(1+z)^2}\right)^r \\ &= \frac{z}{2(1-z)^2}\cdot\frac{\left(\frac{z^2}{(1-z)^2}\right)^p}{\left(1-\frac{z^2}{(1-z)^2}\right)^{p+1}} + \frac{z}{2(1+z)^2}\cdot\frac{\left(\frac{z^2}{(1+z)^2}\right)^p}{\left(1-\frac{z^2}{(1+z)^2}\right)^{p+1}}\end{aligned}$$

Revisar y completar…

11. Vemos que el rango en la suma dada no limita (si $k < m$ se anula el segundo coeficiente binomial, para $k > n$ se anula el primero). Podemos omitir los límites para simplificar.

Multiplicamos la definición de S_m por z^m y sumamos sobre $m \geq 0$:

$$\begin{aligned}\sum_{m\geq 0} S_m z^m &= \sum_{m\geq 0} z^m \sum_k (-1)^k \binom{n}{k}\binom{k}{m} \\ &= \sum_k (-1)^k \binom{n}{k} \sum_{m\geq 0} \binom{k}{m} z^m\end{aligned}$$

Por el teorema del binomio tenemos la suma interna:

$$= \sum_k (-1)^k \binom{n}{k} (1+z)^k$$

Nuevamente teorema del binomio:

$$\begin{aligned}
&= (1 - (1+z))^n \\
&= (-1)^n z^n
\end{aligned}$$

Vale decir:

$$S_m = \begin{cases} 0 & m \neq n \\ (-1)^n & m = n \end{cases}$$

Una manera alternativa de obtener esta suma es aplicar la transformación de Euler. De partida, podemos escribir:

$$S_m = \sum_{0 \le k \le n} (-1)^k \binom{n}{k} \binom{k}{m}$$

Definimos:

$$\begin{aligned}
A(z) &= \sum_{k \ge 0} (-1)^k \binom{k}{m} z^k \\
&= \frac{(-z)^m}{(1+z)^{m+1}}
\end{aligned}$$

Aplicando la transformación de Euler:

$$\begin{aligned}
S_m &= [z^n] \frac{1}{1-z} A\left(\frac{z}{1-z}\right) \\
&= [z^n] \frac{1}{1-z} \frac{(-z)^m}{(1-z)^m (1 - z/(1-z))^{m+1}} \\
&= [z^n] (-z)^m \\
&= (-1)^m [m = n]
\end{aligned}$$

13. Recurrencias

1. La recurrencia obvia es:

$$S_{n+1} = S_n + (n+1)^2 \quad S_0 = 0$$

Definimos la función generatriz:

$$S(z) = \sum_{n \geq 0} S_n z^n$$

Aplicando las propiedades:

$$\begin{aligned}
\frac{S(z) - S_0}{z} &= S(z) + ((zD)^2 + 2zD + 1)\frac{1}{1-z} \\
&= S(z) + \frac{1+z}{(1-z)^3}
\end{aligned}$$

Despejando:

$$S(z) = \frac{z(1+z)}{(1-z)^4}$$

Tenemos dos caminos:

Manual: Expandir la potencia y multiplicar por los términos del numerador:

$$\begin{aligned}
S_n &= [z^n]\, S(z) \\
&= [z^n]\,(z + z^2) \sum_{k \geq 0} (-1)^k \binom{-4}{k} z^k \\
&= [z^n]\,(z + z^2) \sum_{k \geq 0} \binom{k+3}{3} z^k \\
&= \left[z^{n-1}\right] \sum_{k \geq 0} \binom{k+3}{3} z^k + \left[z^{n-2}\right] \sum_{k \geq 0} \binom{k+3}{3} z^k \\
&= \binom{n+2}{3} + \binom{n+1}{3} \\
&= \frac{(n+2)(n+1)n}{3!} + \frac{(n+1)n(n-1)}{3!} \\
&= \frac{n(2n+1)(n+1)}{6}
\end{aligned}$$

Automatizado: Expandir en fracciones parciales:

$$S(z) = \frac{2}{(1-z)^4} - \frac{3}{(1-z)^3} + \frac{1}{(1-z)^2}$$

Tenemos:

$$\begin{aligned}
S_n &= 2(-1)^n \binom{-4}{n} - 3(-1)^n \binom{-3}{n} + (-1)^n \binom{-2}{n} \\
&= 2\binom{n+3}{3} - 3\binom{n+2}{2} + \binom{n+1}{1} \\
&= \frac{2(n+3)(n+2)(n+1)}{3!} - \frac{3(n+2)(n+1)}{2!} + \frac{n+1}{1!} \\
&= \frac{n(2n+1)(n+1)}{6}
\end{aligned}$$

2. De la recurrencia misma vemos que $a_0 = 1$. Ajustamos índices:

$$a_{n+1} = 1 + \frac{1}{2} \sum_{0 \leq j \leq n} a_j$$

Definimos la función generatriz ordinaria:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicando las propiedades:

$$\frac{A(z) - a_0}{z} = \frac{1}{1 - z} + \frac{1}{2} \frac{A(z)}{1 - z}$$

Despejando:

$$A(z) = \frac{1}{1 - 3z/2}$$

En consecuencia:

$$a_n = \left(\frac{3}{2} \right)^n$$

3. Ajustamos índices:

$$a_{n+2} = 6a_{n+1} - 9a_n$$

Definimos:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicamos las propiedades:

$$\begin{aligned} \frac{A(z) - a_0 - a_1 z}{z^2} &= 6 \frac{A(z) - a_0}{z} - 9A(z) \\ \frac{A(z) - 1 - 9z}{z^2} &= 6 \frac{A(z) - 1}{z} - 9A(z) \end{aligned}$$

Despejamos:

$$A(z) = \frac{1 + 3z}{(1 - 3z)^2}$$

Expandiendo la potencia en serie:

$$\begin{aligned} A(z) &= (1 + 3z) \sum_{n \geq 0} 3^n (n + 1) z^n \\ &= \sum_{n \geq 0} 3^n (n + 1) z^n + \sum_{n \geq 0} 3 \cdot 3^n (n + 1) z^{n+1} \\ &= \sum_{n \geq 0} 3^n (n + 1) z^n + \sum_{n \geq 1} 3^n n z^n \\ &= \sum_{n \geq 0} \left(3^n (n + 1) + 3^n n \right) z^n \end{aligned}$$

Directamente:

$$a_n = 3^n (2n + 1)$$

Otro camino, menos apropiado para cálculo manual, es recurrir a fracciones parciales:

$$A(z) = \frac{2}{(1-3z)^2} - \frac{1}{1-3z}$$

y nuevamente:

$$a_n = 2 \cdot \binom{-2}{n} \cdot 3^n - 3^n = 2 \cdot 3^n \binom{n+2-1}{1} - 3^n = 3^n(2n+1)$$

4. Estamos clasificando las secuencias de largo n en cuatro grupos, dependiendo de la paridad de rojo y naranja. Llamemos:

   $\boldsymbol{a_n}$**:** Número de secuencias con número par de cuadraditos rojos y par de cuadraditos naranja

   $\boldsymbol{b_n}$**:** Número de secuencias con número par de cuadraditos rojos e impar de cuadraditos naranja

   $\boldsymbol{c_n}$**:** Número de secuencias con número impar de cuadraditos rojos y par de cuadraditos naranja

   $\boldsymbol{d_n}$**:** Número de secuencias con número impar de cuadraditos rojos e impar de cuadraditos naranja

   Vemos además que $a_0 = 1$ y $b_0 = c_0 = d_0 = 0$.

   Podemos construir las a_{n+1} secuencias par/par agregando verde o azul a las a_n par/par (en total $2a_n$ formas), naranja a las b_n par/impar (b_n maneras) o rojo a las c_n (agrega c_n nuevas). Por el mismo razonamiento:

$$\begin{aligned}
a_{n+1} &= 2a_n + b_n + c_n \\
b_{n+1} &= a_n + 2b_n + d_n \\
c_{n+1} &= a_n + b_n + 2c_n \\
d_{n+1} &= b_n + c_n + 2d_n
\end{aligned}$$

   Multiplicar por z^n y sumar para $n \geq 0$ da:

$$\begin{aligned}
\frac{A(z) - a_0}{z} &= 2A(z) + B(z) + C(z) \\
\frac{B(z) - b_0}{z} &= A(z) + 2B(z) + D(z) \\
\frac{C(z) - c_0}{z} &= A(z) + 2C(z) + D(z) \\
\frac{D(z) - d_0}{z} &= B(z) + C(z) + 2D(z)
\end{aligned}$$

   En realidad sólo nos interesa:

$$B(z) = \frac{z}{1-4z} = \frac{1}{4} \cdot \frac{1}{1-4z} - \frac{1}{4}$$

   De acá:

$$b_n = 4^{n-1} - \frac{1}{4}[n=0]$$

5. Partimos definiendo la función generatriz:

$$L(z) = \sum_{n \geq 0} L_n z^n$$

   Entonces:

   a) Reescribimos la recurrencia como:

$$L_{n+2} = L_{n+1} + L_n \qquad L_0 = 2, L_1 = 1$$

Aplicando propiedades de funciones generatrices ordinarias:

$$\frac{L(z) - 2 - z}{z^2} = \frac{L(z) - 2}{z} + L(z)$$

De donde:

$$L(z) = \frac{2 - z}{1 - z - z^2} = \frac{1}{1 - \phi z} + \frac{1}{1 - \hat{\phi} z}$$

Acá:

$$1 - z - z^2 = (1 - \phi z)(1 - \hat{\phi} z)$$

con lo que:

$$\phi = \frac{1 + \sqrt{5}}{2}$$
$$\hat{\phi} = \frac{1 - \sqrt{5}}{2}$$

Esto da:

$$L_n = \phi^n + \hat{\phi}^n$$

b) Sabemos que la función generatriz de las sumas para $0 \leq k \leq n$ se obtiene dividiendo por $1 - z$. Debemos compensar los L_0 que sumamos demás:

$$\begin{aligned} \frac{L(z)}{1 - z} - \frac{L_0}{1 - z} &= -\frac{\phi}{\hat{\phi}} \cdot \frac{1}{1 - \phi z} - \frac{\hat{\phi}}{\phi} \cdot \frac{1}{1 - \hat{\phi} z} - \frac{3}{1 - z} \\ &= \phi^2 \cdot \frac{1}{1 - \phi z} + \hat{\phi}^2 \cdot \frac{1}{1 - \hat{\phi} z} - \frac{3}{1 - z} \end{aligned}$$

Acá usamos que $\phi \cdot \hat{\phi} = -1$, que resulta de las fórmulas de Vieta (o directamente de comparar coeficiente del producto que las define). Podemos leer el resultado directamente:

$$\sum_{1 \leq k \leq n} L_n = \phi^{n+2} + \hat{\phi}^{n+2} - 3 = L_{n+2} - 3$$

6. Reordenando:

$$\frac{a_{n+1}}{n + 1} = \frac{2}{3} a_n + \frac{5}{3} n!$$

Esto sugiere intentar una función generatriz exponencial:

$$\widehat{A}(z) = \sum_{n \geq 0} a_n \frac{z^n}{n!}$$

Multiplicando la recurrencia por $z^n / n!$ y sumando sobre $n \geq 0$ resulta:

$$\begin{aligned} \sum_{n \geq 0} a_{n+1} \frac{z^n}{(n + 1)!} &= \frac{2}{3} \sum_{n \geq 0} a_n \frac{z^n}{n!} + \frac{5}{3} \sum_{n \geq 0} z^n \\ \frac{\widehat{A}(z) - a_0}{z} &= \frac{2}{3} \widehat{A}(z) + \frac{5}{3} \cdot \frac{1}{1 - z} \\ \widehat{A}(z) &= \frac{5}{1 - z} \end{aligned}$$

Por tanto:

$$a_n = \left[\frac{z^n}{n!} \right] \frac{5}{1 - z} = 5 \cdot n!$$

7. Consideremos los n elementos, y llamemos K_n al número de maneras de organizarlos. Si n está solo, habrá que organizar los restantes $n-1$ dando K_{n-1} casos; si n está en un par con alguno de los demás, su pareja se puede elegir de $n-1$ maneras y los restantes $n-2$ quedan por organizar, para $(n-1)K_{n-2}$ formas. O sea:

$$K_n = K_{n-1} + (n-2)K_{n-2}$$

Además $K_0 = K_1 = 1$.

Para resolver la recurrencia usamos una función generatriz exponencial (ayuda a compensar el factor $n-2$):

$$\widehat{K}(z) = \sum_{n \geq 0} K_n \frac{z^n}{n!}$$

Escribimos:

$$K_{n+1} = K_n + nK_{n-1}$$

y por las propiedades de funciones generatrices exponenciales queda:

$$\begin{aligned}
\widehat{K}'(z) &= \widehat{K}(z) + z\mathrm{D} \int \widehat{K}(z)\,\mathrm{d}z \\
&= (1+z)\widehat{K}(z)
\end{aligned}$$

La solución de esta ecuación diferencial separable con condición inicial $\widehat{K}(0) = 1$ es

$$\widehat{K}(z) = e^{z+z^2/2}$$

de donde:

$$K_n = 1, 1, 2, 4, 5, 13, 28, \ldots$$

8. Por turno aplicamos las propiedades de funciones generatrices ordinarias a $X(z) = \sum_n x_n z^n$:

a)

$$\begin{aligned}
\frac{X(z)-3}{z} &= 5X(z) + 3 \cdot \frac{1}{1-5z} - 2 \cdot \frac{1}{1-z/5} + 4 \cdot \frac{1}{1+5z} \\
X(z) &= \frac{3}{5} \cdot \frac{1}{(1-5z)^2} + \frac{143}{60} \cdot \frac{1}{1-5z} + \frac{5}{12} \cdot \frac{1}{1-z/5} - \frac{2}{5} \cdot \frac{1}{1+5z}
\end{aligned}$$

De acá se leen los coeficientes:

$$\begin{aligned}
x_n &= \frac{3}{5} \cdot (-1)^n \binom{-2}{n} \cdot 5^n + \frac{143}{60} \cdot 5^n + \frac{5}{12} \cdot 5^{-n} - \frac{2}{5} \cdot (-5)^n \\
&= \frac{36n^2 + 108n + 215}{60} \cdot 5^n + \frac{5}{12} \cdot 5^{-n} - \frac{2}{5} \cdot (-5)^n
\end{aligned}$$

b)

$$\begin{aligned}
\frac{X(z) - 1 - z - z^2 - z^3}{z^4} + 5\frac{X(z) - 1 - z - z^2}{z^3} + 7\frac{X(z) - 1 - z}{z^2} + 5\frac{X(z) - 1}{z} + X(z) = 0 \\
X(z) = \frac{1 + 6z + 13z^2 + 18z^3}{1 + 5z + 7z^2 + 5z^3 + z^4}
\end{aligned}$$

El polinomio $d(z) = z^4 + 5z^3 + 7z^2 + 5z + z$ del denominador es bastante feo, pero tratable:

$$\begin{aligned}
\frac{d(z)}{z^2} &= (z^2 + z^{-2}) + 5(z + z^{-1}) + 7 \\
&= \big((z + z^{-1})^2 - 2\big) + 5(z + z^{-1}) + 7 \\
&= u^2 + 5u + 5
\end{aligned}$$

donde $u = z + z^{-1}$. Las raíces de esto último son:

$$\begin{aligned}
u &= \frac{-5 \pm \sqrt{5^2 - 4 \cdot 1 \cdot 5}}{2 \cdot 1} \\
&= \frac{-5 \pm \sqrt{5}}{2}
\end{aligned}$$

Esto a su vez da lugar a las ecuaciones para z:

$$\begin{aligned}
z + z^{-1} &= u \\
z^2 - uz + 1 &= 0
\end{aligned}$$

Finalmente:

$$\begin{aligned}
z &= \frac{u \pm \sqrt{u^2 - 4 \cdot 1 \cdot 1}}{2 \cdot 1} \\
&= \frac{u \pm \sqrt{u^2 - 4}}{2}
\end{aligned}$$

Continuará…

c)

$$\begin{aligned}
\frac{X(z) - z}{z^2} - 10\frac{X(z)}{z} + 25X(z) &= 3 \cdot \frac{1}{1 - 5z} - 3 \cdot \frac{1}{1 - z/5} \\
X(z) &= \frac{3}{25} \cdot \frac{1}{(1 - 5z)^3} - \frac{33}{200} \cdot \frac{1}{(1 - 5z)^2} + \frac{841}{4800} \cdot \frac{1}{1 - 5z} - \frac{25}{192} \cdot \frac{1}{1 - z/5}
\end{aligned}$$

Leemos los coeficientes:

$$\begin{aligned}
x_n &= \frac{3}{25} \cdot (-1)^n \binom{-3}{n} \cdot 5^n - \frac{33}{200} \cdot (-1)^2 \binom{-2}{n} \cdot 5^n + \frac{841}{4800} \cdot 5^n - \frac{25}{192} \cdot 5^{-n} \\
&= \frac{36n + 179}{60} \cdot 5^n - \frac{25}{192} \cdot 5^{-n}
\end{aligned}$$

9. Para la función generatriz ordinaria $A(z)$ las propiedades de las funciones generatrices ordinarias dan:

$$\frac{A(z) - 1 - 2z - 4z^2}{z^3} - 2\frac{A(z) - 1}{z} + A(z) = z\mathrm{D}\frac{1}{1 - 3z} - \frac{1}{1 - z/5} + \frac{1}{1 - z}$$

La solución a esta ecuación en fracciones parciales es:

$$A(z) = \frac{2988 + 3350z}{2299(1 - z - z^2)} - \frac{97}{484(1 - 3z)} + \frac{1}{22(1 - 3z)^2} + \frac{1}{2(1 - z)} + \frac{1}{1 - z)^2} - \frac{125}{76(1 - z/5)}$$

El primer término recuerda la función generatriz de los números de Fibonacci:

$$F(z) = \frac{z}{1 - z - z^2}$$

Como $F_0 = 0$, tenemos que:

$$\frac{F(z) - F_0}{z} = \frac{1}{1 - z - z^2}$$

Con esto, y expresando los restantes términos, resulta:

$$\begin{aligned}
a_n &= \frac{2988}{2299}F_{n+1} + \frac{3350}{2299}F_n - \frac{97}{484} \cdot 3^n + \frac{1}{22}\binom{-2}{n} \cdot 3^n + \frac{1}{2} \cdot 1^n - \frac{125}{76} \cdot 5^{-n} \\
&= \frac{2988}{2299}F_{n+1} + \frac{3350}{2299}F_n + \frac{22n - 75}{484} \cdot 3^n - \frac{5^{3-n}}{76} + \frac{1}{2}
\end{aligned}$$

10. Por completar
11. Llamemos C_n al número de llamadas para calcular F_n. Entonces:

$$C_{n+2} = C_{n+1} + C_n + 2 \qquad C_0 = C_1 = 0$$

Para la función generatriz ordinaria $C(z)$ las propiedades dan:

$$\begin{aligned}\frac{C(z)}{z^2} &= \frac{C(z)}{z} + C(z) + 2\frac{1}{1-z} \\ C(z) &= \frac{2}{1-z-z^2} - 2\frac{1}{1-z}\end{aligned}$$

Comparando con la función generatriz de los números de Fibonacci:

$$C(z) = 2\frac{F(z) - F_0}{z} - 2\frac{1}{1-z}$$

resulta:

$$C_n = 2F_{n+1} - 2$$

12. Por completar
13. Por completar
14. Por completar
15. Por completar
16. Por completar
17. Por completar
18. Por completar
19. Usamos funciones generatrices ordinarias. Definimos:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicando las propiedades, resulta directamente:

$$\frac{A(z) - 1 - z}{z^2} - 3\frac{A(z) - 1}{z} + 2A(z) = \frac{1}{1-4z} - zD\frac{1}{1-z}$$

Despejando y expresando en fracciones parciales:

$$A(z) = \frac{1}{6} \cdot \frac{1}{1-4z} - \frac{3}{2} \cdot \frac{1}{1-2z} + \frac{7}{3} \cdot \frac{1}{1-z} - \frac{1}{(1-z)^2} + \frac{1}{(1-z)^3}$$

De acá se leen los coeficientes:

$$\begin{aligned}a_n &= \frac{1}{6} \cdot 4^n - \frac{3}{2} \cdot 2^n + \frac{7}{3} - \binom{-2}{n} + \binom{-3}{n} \\ &= \frac{1}{6} \cdot 4^n - \frac{3}{2} \cdot 2^n + \frac{7}{3} - (n+1) + \frac{(n+1)(n+2)}{2} \\ &= \frac{1}{6} \cdot 4^n - \frac{3}{2} \cdot 2^n + \frac{7}{3} + \frac{n(n+1)}{2}\end{aligned}$$

20. Podemos aplicar nuestra teoría módulo m, ya que $\mathbb{Z}_m$ es un campo al ser m primo. Para la función generatriz ordinaria

$$G(z) = \sum_{n \geq 0} x_n z^n$$

las propiedades dan:

$$\frac{G(z) - x_0}{z} = aG(z) + \frac{a}{1 - z}$$

En fracciones parciales:

$$G(z) = \frac{(a-1)x_0 + c}{a - 1} \cdot \frac{1}{1 - az} - \frac{c}{a - 1} \cdot \frac{1}{1 - z}$$

Esto vale sólo si $a \not\equiv 1 \pmod{m}$. En tal caso la solución es

$$x_n = \frac{(a-1)x_0 + c}{a - 1} \cdot a^n - \frac{c}{a - 1}$$

Cuando $a \equiv 1 \pmod{m}$, la recurrencia es

$$x_{i+1} = x_i + c$$

y la solución es obviamente

$$x_n = x_0 + nc$$

En resumen, en $\mathbb{Z}_m$:

$$x_n = \begin{cases} x_0 + nc & \text{si } a \equiv 1 \pmod{m} \\ \dfrac{(a-1)x_0 + c}{a - 1} \cdot a^n - \dfrac{c}{a - 1} & \text{caso contrario} \end{cases}$$

21. En este caso la recurrencia define sólo los elementos pares de la secuencia. Para la función generatriz ordinaria

$$X(z) = \sum_{n \geq 0} x_{2n} z^n$$

las propiedades dan:

$$\frac{X(z) - 3}{z} = 4X(z) + 3 \cdot \frac{1}{1 - 2z} - 2 \cdot \frac{1}{1 - z/5} + 4 \cdot \frac{1}{1 + 2z}$$

En fracciones parciales:

$$X(z) = \frac{529}{114} \cdot \frac{1}{1 - 4z} - \frac{3}{2} \cdot \frac{1}{1 - 2z} + \frac{10}{19} \cdot \frac{1}{1 - z/5} - \frac{2}{3} \cdot \frac{1}{1 + 2z}$$

Resulta, recordando que se definen sólo los términos pares:

$$x_{2n} = \frac{529}{114} \cdot 4^n - \frac{3}{2} \cdot 2^n + \frac{10}{19} \cdot 5^{-n} - \frac{2}{3} \cdot (-2)^n$$

22. Definimos la función generatriz ordinaria:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicando las propiedades a la recurrencia:

$$\frac{A(z) - 0 - z}{z^2} + A(z) = 0$$

En fracciones parciales:

$$A(z) = \frac{z}{1 + z^2}$$

Expandiendo como serie geométrica:

$$A(z) = z \sum_{n \geq 0} (-1)^n z^{2n}$$

En consecuencia:

$$a_n = \begin{cases} (-1)^k & \text{si } n = 2k + 1 \\ 0 & \text{caso contrario} \end{cases}$$

23. Definimos la función generatriz ordinaria:

$$B(z) = \sum_{n \geq 0} b_n z^n$$

El segundo término es la convolución de $\langle n \rangle_{n \geq 0}$ y $\langle b_n \rangle_{n \geq 0}$. Aplicando las propiedades:

$$\frac{B(z) - 1}{z} = 2 \frac{1}{1 - 2z} + \left(zD \frac{1}{1 - z} \right) \cdot B(z)$$

En fracciones parciales:

$$\begin{aligned} B(z) &= \frac{2 - z}{1 - 3z + z^2} - \frac{1}{1 - 2z} \\ &= -\frac{5 - 2\sqrt{5}}{5} \cdot \frac{1}{1 - \frac{3 - \sqrt{5}}{2} z} - \frac{5 + 2\sqrt{5}}{5} \cdot \frac{1}{1 - \frac{3 + \sqrt{5}}{2} z} - \frac{1}{1 - 2z} \end{aligned}$$

Podemos leer los coeficientes:

$$b_n = -\frac{5 - 2\sqrt{5}}{5} \cdot \left(\frac{3 - \sqrt{5}}{2} \right)^n - \frac{5 + 2\sqrt{5}}{5} \cdot \left(\frac{3 + \sqrt{5}}{2} \right)^n - 2^n$$

24. Buscar pauta en papel, rehacer o eliminar.

25. Por completar

26. Definimos:

$$\widehat{D}(z) = \sum_{n \geq 0} d_n \frac{z^n}{n!}$$

Aplicando las propiedades:

$$\begin{aligned} d_{n+1} &\longleftrightarrow \widehat{D}'(z) \\ n d_n &\longleftrightarrow z \widehat{D}'(z) \end{aligned}$$

Falta el término $n d_{n-1}$. Podemos enfrentarlo de dos maneras:

- Directamente de las definiciones:

$$\begin{aligned}\sum_{n\geq 0} n d_{n-1}\frac{z^n}{n!} &= z\sum_{n\geq 1} d_{n-1}\frac{z^{n-1}}{(n-1)!}\\ &= z\sum_{n\geq 0} d_n\frac{z^n}{n!}\\ &= z\widehat{D}(z)\end{aligned}$$

- Alternativamente, correr la secuencia una posición a la izquierda sería la antiderivada:

  $$d_{n-1} \longleftrightarrow D^{-1}\widehat{D}(z)$$

  Multiplicar esto por n es aplicar el operador zD:

  $$n d_{n-1} \longleftrightarrow zD(D^{-1}\widehat{D}(z)) = z\widehat{D}(z)$$

De cualquier forma, uniendo las piezas anteriores:

$$\widehat{D}'(z) = z\widehat{D}'(z) + z\widehat{D}(z) \qquad \widehat{D}(0) = d_0 = 1$$

Separando variables:

$$\begin{aligned}\frac{\widehat{D}'(z)}{\widehat{D}(z)} &= \frac{z}{1-z}\\ \int_1^{\widehat{D}}\frac{dD}{D} &= \int_0^z \frac{z\,dz}{1-z}\\ \ln\widehat{D} &= -\ln(1-z) - z\\ \widehat{D}(z) &= \frac{e^{-z}}{1-z}\end{aligned}$$

Esto corresponde a sumas parciales:

$$\begin{aligned}\frac{d_n}{n!} &= \sum_{0\leq k\leq n}\frac{(-1)^k}{k!}\\ &\approx e^{-1}\end{aligned}$$

27. Partimos escribiendo:

$$d_{n+2} = (n+1)d_{n+1} + (n+1)d_n \quad d_0 = 1,\, d_1 = 0$$

Aplicando las propiedades:

$$\frac{D(z)-1}{z^2} = (zD+1)\frac{D(z)-1}{z} + (zD+1)D(z)$$

Esto lleva a la ecuación diferencial: Completar desarrollo

28. Definiendo la función generatriz ordinaria:

$$A(z) = \sum_{n\geq 0} a_n z^n$$

y aplicando las propiedades a la recurrencia:

$$\frac{A(z) - 1 - 2z - 3z^2}{z^3} + A(z) = 2\cdot\ \frac{1}{1-5z}$$

En fracciones parciales:

$$A(z) = -\frac{1}{21} \cdot \frac{9 + 43z}{1 - z - z^2} + \frac{1}{63} \cdot \frac{1}{1 - 5z} + \frac{5}{9} \cdot \frac{1}{1 + z}$$

Ahora bien, para los números de Fibonacci:

$$\begin{aligned} F_n &\longleftrightarrow \frac{z}{1 - z - z^2} \\ F_{n+1} &\longleftrightarrow \frac{1}{1 - z - z^2} \end{aligned}$$

Con esto podemos leer los coeficientes:

$$a_n = -\frac{3}{7} F_{n+1} - \frac{43}{63} F_n + \frac{1}{63} \cdot 5^n + (-1)^n$$

29. Ajustamos índices:

$$b_{n+1} = (n + 1) + \sum_{0 \leq k \leq n} b_k \qquad b_0 = 0$$

Definiendo la función generatriz ordinaria:

$$B(z) = \sum_{n \geq 0} b_n z^n$$

y aplicando propiedades:

$$\frac{B(z) - b_0}{z} = (zD + 1) \frac{1}{1 - z} + \frac{1}{1 - z} \cdot B(z)$$

Como fracciones parciales:

$$B(z) = \frac{1}{1 - 2z} - \frac{1}{1 - z}$$

Los coeficientes son inmediatos:

$$b_n = 2^n - 1$$

30. La suma es simplemente una serie geométrica:

$$A(z) = \frac{1}{1 - zA(z)}$$

Reordenando:

$$A(z) = 1 + zA^2(z)$$

Sabemos que esto lleva a los números de Catalan:

$$a_n = C_n$$

31. Sabemos que:

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = [n = 0] \tag{9}$$

y es fácil ver que:

$$\begin{bmatrix} n \\ n \end{bmatrix} = 1 \quad \text{si } n > 0 \tag{10}$$

y adoptaremos la convención:

$$\begin{bmatrix} n \\ k \end{bmatrix} = 0 \quad \text{si } k > n \text{ ó } k < 0 \tag{11}$$

Usando la convención (11) para no tener que preocuparse de los rangos de las sumas:

$$z^{\overline{n+1}} = \sum_k n + 1k \cdot z^k \tag{12}$$

Podemos escribir también:

$$\begin{aligned}
z^{\overline{n+1}} &= z^{\overline{n}} \cdot (z + n) \\
&= \sum_k \begin{bmatrix} n \\ k \end{bmatrix} \cdot z^k \cdot (z + n) \\
&= \sum_k \left(\begin{bmatrix} n \\ k \end{bmatrix} \cdot z^{k+1} + n \cdot \begin{bmatrix} n \\ k \end{bmatrix} \cdot z^k \right) \\
&= \sum_k \left(\begin{bmatrix} n \\ k-1 \end{bmatrix} + n \cdot \begin{bmatrix} n \\ k \end{bmatrix} \right) \cdot z^k
\end{aligned} \tag{13}$$

Igualando coeficientes en (12) y (13) se obtiene:

$$\begin{bmatrix} n+1 \\ k \end{bmatrix} = \begin{bmatrix} n \\ k-1 \end{bmatrix} + n \cdot \begin{bmatrix} n \\ k \end{bmatrix} \tag{14}$$

Esta recurrencia es válida para todo n y k, en particular muestra que las condiciones iniciales (9) son consistentes con las convenciones:

$$\begin{aligned}
\begin{bmatrix} n+1 \\ 0 \end{bmatrix} &= \begin{bmatrix} n \\ -1 \end{bmatrix} + n \cdot \begin{bmatrix} n \\ 0 \end{bmatrix} \\
&= 0 \quad \text{para todo } n \geq 0
\end{aligned} \tag{15}$$

32. Definimos la función generatriz ordinaria:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicando las propiedades a la recurrencia:

$$\frac{A(z) - 0 - z}{z^2} = 2\frac{A(z) - 0}{z} - A(z) + zD\frac{1}{1 - 2z}$$

En fracciones parciales:

$$A(z) = -5\frac{1}{1 - 2z} + \frac{1}{(1 - 2z)^2} + \frac{1}{1 - z} + 3\frac{1}{(1 - z)^2}$$

De acá se leen los coeficientes:

$$\begin{aligned}
a_n &= -5 \cdot 2^n + \binom{-2}{n} 2^n + 1 + 3\binom{-2}{n} \\
&= (n - 4) \cdot 2^n + 3n + 4
\end{aligned}$$

33. Escribiendo la recurrencia como:

$$b_{n+1} = \sum_{0 \leq k \leq n} \binom{n}{k} b_k \qquad b_0 = 1$$

El lado derecho es la convolución binomial de las secuencias $\langle 1 \rangle_{n \geq 0}$ y $\langle b_n \rangle_{n \geq 0}$, así que definimos una función generatriz exponencial:

$$\widehat{B}(z) = \sum_{n \geq 0} b_n \frac{z^n}{n!}$$

Aplicando las propiedades respectivas resulta la ecuación diferencial:

$$\widehat{B}'(z) = B(z) e^z \qquad B(0) = 1$$

Para resolver esto separamos variables:

$$\begin{aligned}
\frac{B'}{B} &= e^z \\
\int_1^B \frac{dB}{B} &= \int_0^z e^z \\
\ln B &= e^z \\
B(z) &= e^{e^z}
\end{aligned}$$

Falta obtener los coeficientes, pero eso no es demasiado simple...

34. Definimos la función generatriz ordinaria:

$$C(z) = \sum_{n \geq 0} c_n z^n$$

Reescribimos la recurrencia como:

$$(n+1) c_{n+1} = \sum_{0 \leq k \leq n} c_{n-k} c_k \qquad c_0 = 2$$

El lado derecho es una convolución, aplicamos las propiedades:

$$(zD + 1) \frac{C(z) - 2}{z} = C^2(z)$$

35. Primero reescribimos la recurrencia:

$$s_{n+1} = \alpha a_{n+1} + (1 - \alpha) s_n \qquad s_0 = a_0$$

Aplicamos las propiedades:

$$\frac{S(z) - s_0}{z} = \alpha \frac{A(z) - a_0}{z} + (1 - \alpha) S(z)$$

Despejando:

$$S(z) = \frac{\alpha}{1 - (1 - \alpha) z} \cdot A(z)$$

36. Definamos funciones generatrices ordinarias:

$$\begin{aligned}
A(z) &= \sum_{n \geq 0} a_n z^n \\
U(z) &= \sum_{n \geq 0} u_n z^n
\end{aligned}$$

Por las condiciones del problema, se supone conocida $U(z)$ y se busca $A(z)$.

a) Aplicando propiedades, directamente es:

$$\frac{A(z) - 2 - 2z}{z^2} + \frac{A(z) - 2}{z} - 3A(z) = U(z)$$

Despejando:

$$A(z) = \frac{1}{3} \cdot \frac{U(z)(1 + z) + 6(2z + 1)}{1 - z - 3z^2} - \frac{U(z)}{3}$$

b) Esta es una convolución:

$$\frac{A(z) - 1}{z} = A(z) \cdot U(z)$$

Despejando $A(z)$:

$$A(z) = \frac{1}{1 - zU(z)}$$

37. Por turno:

a) Aplicando la receta, definimos:

$$A(x) = \sum_{k \geq 0} a_k x^k$$

y la recurrencia nos entrega:

$$\begin{aligned} \frac{A(x)}{x} &= 3A(x) + \frac{2}{1 - x} \\ A(x) &= \frac{2x}{3x^2 - 4x + 1} \\ &= \frac{1}{1 - 3x} - \frac{1}{1 - x} \end{aligned}$$

con lo que resulta:

$$a_k = 3^k - 1$$

b) Nuevamente aplicamos la receta, definiendo:

$$B(x) = \sum_{k \geq 0} b_k x^k$$

y la recurrencia da:

$$\begin{aligned} \frac{B(x) - x}{x^2} &= 2\frac{B(x)}{x} - B(x) \\ B(x) &= \frac{x}{x^2 - 2x + 1} \\ &= \frac{1}{(1 - x)^2} - \frac{1}{1 - x} \end{aligned}$$

y resulta, dado que $\binom{-2}{k} = \binom{k+1}{1}$:

$$\begin{aligned} b_k &= \binom{k + 1}{1} - 1 \\ &= k \end{aligned}$$

c) Nuevamente la receta indica definir:

$$C(x) = \sum_{k \geq 0} c_k x^k$$

y la recurrencia entrega:

$$\begin{aligned}
\frac{C(x) - \beta}{x} &= C(x) + \frac{1}{1 - \alpha x} \\
C(x) &= -\frac{(\alpha\beta - 1)x - \beta}{\alpha x^2 - (\alpha + 1)x + 1} \\
&= \frac{1}{\alpha - 1} \cdot \frac{1}{1 - \alpha x} + \frac{(\alpha - 1)\beta - 1}{\alpha - 1} \cdot \frac{1}{1 - x}
\end{aligned}$$

de donde concluimos:

$$c_k = \frac{\alpha^k}{\alpha - 1} + \frac{(\alpha - 1)\beta - 1}{\alpha - 1}$$

38. Cada caso en orden.

a) Definiendo:

$$\widehat{A}(x) = \sum_{k \geq 0} a_k \frac{x^k}{k!}$$

se obtiene directamente usando las propiedades vistas en clase:

$$D\widehat{A} = 3\widehat{A} + 2e^x \quad \widehat{A}(0) = 0$$

La solución general a esta ecuación diferencial está dada por:

$$\widehat{A}(x) = \alpha e^{3x} - e^x$$

Con la condición inicial, resulta $\alpha = 1$, y:

$$\begin{aligned}
\widehat{A}(x) &= e^{-3x} - 1 \\
a_k &= 3^k - 1^k \\
&= 3^k - 1
\end{aligned}$$

b) Definiendo:

$$\widehat{B}(x) = \sum_{k \geq 0} b_k \frac{x^k}{k!}$$

tenemos directamente:

$$D^2\widehat{B} = 2D\widehat{B} - \widehat{B} \quad \widehat{B}(0) = 0,\ \widehat{B}'(0) = 1$$

La solución general a esta ecuación es:

$$\widehat{B}(x) = \alpha x e^x + \beta e^x$$

Con las condiciones iniciales:

$$\alpha = 1 \quad \beta = 0$$

con lo que:

$$\begin{aligned}
\widehat{B}(x) &= x e^x \\
b_k &= k
\end{aligned}$$

c) Definimos:

$$\widehat{C}(x) = \sum_{k \geq 0} c_k \frac{x^k}{k!}$$

y la recurrencia entrega:

$$D\widehat{C} = \widehat{C} + e^{\alpha x} \quad \widehat{C}(0) = \beta$$

La solución general de esta ecuación diferencial es:

$$\widehat{C}(x) = \frac{e^{\alpha x}}{\alpha - 1} + ae^x$$

Con la condición inicial:

$$\begin{aligned}
\widehat{C}(x) &= \frac{e^{\alpha x}}{\alpha - 1} + \frac{(\alpha - 1)\beta - 1}{\alpha - 1} e^x \\
c_k &= \frac{\alpha^k}{\alpha - 1} + \frac{(\alpha - 1)\beta - 1}{\alpha - 1} \\
&= \frac{\alpha^k - 1}{\alpha - 1} + \beta
\end{aligned}$$

39. Vemos cada uno de los puntos.

a) Definimos la función generatriz

$$F(z) = \sum_{n \geq 1} f(n) z^{n-1}$$

Multiplicando las tres últimas expresiones para $f(n)$ por z^{3n-1}, z^{3n} y z^{3n+1}, respectivamente, y sumando se tiene:

$$\begin{aligned}
&\sum_{n \geq 1} \left(f(3n) z^{3n-1} + f(3n+1) z^{3n} + f(3n+2) z^{3n+1} \right) \\
&\quad = \sum_{n \geq 1} \left(3f(n) z^{3n-1} + 2f(n) z^{3n} + f(n+1) z^{3n} + 2f(n) z^{3n+1} + 2f(n+1) z^{3n+1} \right)
\end{aligned}$$

Se aprecia que la suma del lado izquierdo no es más que $F(z)$, pero le faltan los primeros términos. Al lado derecho aparece $F(z^3)$:

$$\begin{aligned}
F(z) - 1 - 2z &= (1 + 2z + 3z^2 + 2z^3 + z^4) F(z^3) - 1 - 2z^2 \\
F(z) &= (1 + z + z^2)^2 F(z^3) \\
&= \left(\frac{1 - z^3}{1 - z} \right)^2 F(z^3)
\end{aligned}$$

b) Aplicando varias veces la última relación queda:

$$\begin{aligned}
F(z) &= \left(\frac{1 - z^3}{1 - z} \right)^2 \cdot \left(\frac{1 - z^{3^2}}{1 - z^3} \right)^2 \cdot F(z^{3^2}) \\
&= \dots \\
&= \prod_{k \geq 0} \left(\frac{1 - z^{3^k}}{1 - z^{3^{k-1}}} \right)^2
\end{aligned}$$

Considerando esta última relación como puramente formal, está claro que cumple la ecuación funcional para $F(z)$ obtenida antes.

c) En la expresión para $F(z)$ podríamos haber simplificado:

$$
\begin{aligned}
F(z) &= \frac{(1-z^3)^2}{(1-z)^2} \cdot F(z^3) \\
&= \frac{(1-z^{3^2}}{(1-z)^2} \cdot F(z^{3^2}) \\
&= \dots \\
&= \frac{1}{(1-z)^2}
\end{aligned}
$$

Ahora bien, esta última expresión resuelve nuestra ecuación para $F(z)$:

$$
\frac{1}{(1-z)^2} = \frac{(1-z^3)^2}{(1-z)^2} \cdot \frac{1}{(1-z^3)^2}
$$

40. Usando la receta para resolver recurrencias, definimos:

$$
L(z) = \sum_{n \geq 0} L_n z^n
$$

De la recurrencia, por las propiedades:

$$
\frac{L(z) - 2 - z}{z^2} = \frac{L(z) - 2}{z} + L(z)
$$

Despejando:

$$
L(z) = \frac{2 - z}{1 - z - z^2}
$$

Esto se puede expresar en términos de números de Fibonacci:

$$
\begin{aligned}
L(z) &= 2\frac{F(z) - F_0}{z} - F(z) \\
L_n &= 2F_{n+1} - F_n
\end{aligned}
$$

También puede resolverse directamente. Como fracciones parciales:

$$
L(z) = \frac{1}{1 - \tau z} + \frac{1}{1 - (1 - \tau) z}
$$

con lo que

$$
L_n = \tau^n + (1 - \tau)^n
$$

Podemos hacer una cosa más truculenta. Por la forma de la función generatriz (o directamente de la relación de recurrencia, que es la de los números de Fibonacci)), sabemos que la solución será de la forma:

$$
L_n = \alpha \cdot \tau^n + \beta \cdot (1 - \tau)^n
$$

para constantes α y β. También:

$$
\begin{aligned}
L_0 &= 2 = \alpha + \beta \\
L_1 &= 1 = \beta
\end{aligned}
$$

En consecuencia, $\alpha = \beta = 1$, y tenemos simplemente:

$$
L_n = \tau^n + (1 - \tau)^n
$$

41. De las solicitadas podemos formar 1 de largo 0, 2 de largo 1, $2 \times 2 + 3 \times 3 = 13$ de largo 2, ... Estos valores sirven para verificar luego.

Una alternativa es definir u_n para el número de palabras de largo n con un número par de vocales fuertes, y v_n para el número de palabras de largo n con un número impar de vocales fuertes. Tenemos que $u_0 = 1$, $v_0 = 0$. Definiendo funciones generatrices:

$$\begin{aligned} U(z) &= \sum_{n \geq 0} u_n z^n \\ V(z) &= \sum_{n \geq 0} v_n z^n \end{aligned}$$

podemos escribir, como podemos alargar la palabra en uno y hay 2 vocales débiles y 3 fuertes que se pueden agregar:

$$\begin{aligned} \frac{U(z) - 1}{z} &= 2U(z) + 3V(z) \\ \frac{V(z) - 0}{z} &= 3U(z) + 2zV(z) \end{aligned}$$

Nos interesa únicamente $U(z)$, despejando esto:

$$\begin{aligned} U(z) &= \frac{1 - 2x}{1 - 4x - 5x^2} \\ &= \frac{1}{2} \cdot \frac{1}{1 + z} + \frac{1}{2} \cdot \frac{1}{1 - 5z} \end{aligned}$$

Podemos leer los u_n de esto, que son simplemente dos series geométricas:

$$u_n = \frac{1}{2} \left(5^n + (-1)^n\right)$$

42. La "recurrencia de BonJovi" del aturdido del ayudante del profesor Upham es:

$$b_{n+1} = \sum_{0 \leq k \leq n} b_k \quad n \geq 1,\ b_0 = 0,\ b_1 = 1$$

Aplicando nuestra receta de siempre, definimos:

$$B(z) = \sum_{n \geq 0} b_n z^n$$

Tenemos que el término siguiente es la suma de términos parciales:

$$\frac{B(z) - b_0}{z} = \frac{1}{1 - z} \cdot B(z)$$

Lo malo es que esto no lleva a una ecuación para $B(z)$, lo que no es para nada extraño ya que si comenzamos con $b_0 = 0$ la recurrencia define todos los valores como 0. así que recurrimos a las bases. En realidad, debemos comenzar con b_1 y dejar b_0 como caso especial. Hay varias formas de proceder:

- "Corregir" b_0 para enlazar con $b_1 = 1$, y resolver el resultado
- Plantear la recurrencia partiendo de $n = 1$, básicamente definiendo $b'_n = b_{n+1}$

Usaremos la primera, llamando b^*_n a la secuencia, que hace que debiera ser $b^*_0 = 1$:

$$\frac{B^*(z) - 1}{z} = \frac{1}{1 - z} \cdot B^*(z)$$

En fracciones parciales:

$$B^*(z) = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{1 - 2z}$$

Se leen los coeficientes:

$$b_n^* = \begin{cases} \dfrac{1}{2} + \dfrac{1}{2} & \text{si } n = 0 \\[2ex] \dfrac{1}{2} \cdot 2^n & \text{si } n > 0 \end{cases}$$

Pero considerando nuestro “ajuste,” en realidad debiera ser:

$$b_n = \begin{cases} 0 & \text{si } n = 0 \\ 2^{n-1} & \text{si } n > 0 \end{cases}$$

43. Llamemos s_n al número de palabras de largo n. Los primeros valores de s_n los tenemos:

n	s_n	Palabras
1	1	S
2	2	L, SS
3	3	LS, SL, SSS
4	5	LL, LSS, SLS, SSL, SSSS

Tiene sentido definir $s_0 = 1$ (hay una única palabra de largo cero). Para obtener una palabra de largo n puedo tomar una palabra de largo $n - 1$ y agregar S, o tomar una palabra de largo $n - 2$ y agregar L. O sea:

$$s_{n+2} = s_{n+1} + s_n \quad n \geq 0,\ s_0 = 1,\ s_1 = 1$$

Esto es consistente con la tabla anterior.

O sea, $s_n = F_{n+1}$, son simplemente los números de Fibonacci.

44. Por completar

45. Por completar

46. Por la forma de la recurrencia, usamos una función generatriz exponencial:

$$\widehat{A}(z) = \sum_{n \geq 0} a_n \frac{z^n}{n!}$$

La suma que llega a $n - 1$ al lado derecho producirá problemas. Escribamos:

$$a_{n+1} = \frac{1}{2} \sum_{0 \leq k \leq n} \binom{n}{k} a_k a_{n-k}$$

Aplicando las propiedades de funciones generatrices exponenciales:

$$\widehat{A}'(z) = \frac{1}{2} \widehat{A}^2(z) \qquad \widehat{A}(0) = a_0 = 1$$

Separando variables:

$$\begin{aligned} \int_1^{\widehat{A}} \frac{dy}{y^2} &= \frac{1}{2} \int_0^z dx \\ 1 - \frac{1}{\widehat{A}} &= \frac{z}{2} \\ \widehat{A}(z) &= \frac{1}{1 - z/2} \end{aligned}$$

Pero entonces:

$$\left[\frac{z^n}{n!}\right] \widehat{A}(z) = n!\, [z^n]\, \widehat{A}(z) = n! 2^{-n}$$

47. Ajustamos la suma para cubrir el rango completo:

$$E_n + \frac{1}{2} \sum_{0 \leq k \leq n-1} \binom{n}{k} 2^{n-k} E_k = 1$$

$$E_n + \frac{1}{2} \left(\sum_{0 \leq k \leq n} \binom{n}{k} 2^{n-k} E_k - E_n \right) = 1$$

$$E_n + \sum_{0 \leq k \leq n} \binom{n}{k} 2^{n-k} E_k = 2$$

Por la convolución binomial usamos una función generatriz exponencial:

$$\widehat{E}(z) = \sum_{n \geq 0} E_n \frac{z^n}{n!}$$

Necesitamos también:

$$\sum_{n \geq 0} 2^n \frac{z^n}{n!} = e^{2z}$$

Aplicando las propiedades a la recurrencia:

$$\widehat{E}(z) + e^{2z} \widehat{E}(z) = 2e^z$$

Despejando:

$$\widehat{E}(z) = \frac{2}{e^z + e^{-z}} = \coth z$$

48. Hay una única manera de llenar un rectángulo de largo 0, y una única forma de llenar uno de largo 1, y dos de llenar uno de largo 2 (vertical u horizontal).

Sea r_n el número de formas de llenar un rectángulo de largo n. En un rectángulo de largo n el último dominó puede estar vertical, quedan por llenar las primeras $n-1$ posiciones, de r_{n-1} maneras; o puede estar horizontal (junto a otro), en cuyo caso hay que llenar $n-2$ posiciones, lo que se hace de r_{n-2} maneras. O sea, tenemos la recurrencia:

$$r_n = r_{n-1} + r_{n-2} \qquad r_0 = 1,\, r_1 = 1$$

Ajustando índices:

$$r_{n+2} = r_{n+1} + r_n \qquad r_0 = 1,\, r_1 = 1$$

Definimos:

$$R(z) = \sum_{n \geq 0} r_n z^n$$

De la recurrencia:

$$\frac{R(z) - 1 - z}{z^2} = \frac{R(z) - 1}{z} + R(z)$$

Despejando:

$$R(z) = \frac{1}{1 - z - z^2} = \frac{F(z) - F_0}{z}$$

O sea, $r_n = F_{n+1}$.

49. Definimos la función generatriz ordinaria:

$$U(z) = \sum_{n \geq 0} u_n z^n$$

Aplicando las propiedades:

$$3\frac{U(z) - 1 - 2z}{z^2} - U(n) = 6(zD)^2 \frac{1}{1-z}$$

En términos de fracciones parciales:

$$U(z) = -\frac{5}{1-z} + \frac{18}{(1-z)^2} - \frac{18}{(1-z)^3} + \frac{6}{(1-z)^4}$$

Leemos los coeficientes:

$$\begin{aligned} u_n &= -1 + 18 \cdot \binom{-2}{n} - 18 \cdot \binom{-3}{n} + 6 \cdot \binom{-4}{n} \\ &= -1 + 18 \cdot \binom{n+1}{1} - 18 \cdot \binom{n+2}{2} + 6 \cdot \binom{n+3}{3} \\ &= n^3 - 3n^2 + 2n + 5 \end{aligned}$$

50. Aplicamos las propiedades con funciones generatrices ordinarias.

   a) Ajustando índices:

   $$a_{n+2} = 5a_{n+1} - 6a_n \quad a_0 = 0,\ a_1 = 1$$

   Definimos la función generatriz ordinaria $A(z)$ y tenemos:

   $$\begin{aligned} \frac{A(z) - z}{z^2} &= 5\frac{A(z)}{z} - 6A(z) \\ A(z) &= \frac{1}{1-3z} - \frac{1}{1-2z} \end{aligned}$$

   de donde

   $$a_n = 3^n - 2^n$$

   b) Ajustamos índices:

   $$b_{n+2} = b_{n+1} + 6b_n \quad b_0 = b_1 = 1$$

   Para $B(z)$ las propiedades dan:

   $$\begin{aligned} \frac{B(z) - 1 - z}{z^2} &= \frac{B(z) - 1}{z} + 6B(z) \\ B(z) &= \frac{3}{5} \cdot \frac{1-3z}{+} \frac{2}{5} \cdot \frac{1}{1+2z} \end{aligned}$$

   Se lee directamente:

   $$b_n = \frac{3^{n+1} + (-2)^{n+1}}{5}$$

   c) Ajustando índices:

   $$c_{n+1} = c_n + n + 1 \quad c_0 = 0$$

Para $C(z)$ las propiedades dan:

$$\begin{aligned}\frac{C(z)}{z} &= C(z) + (zD)^2 \frac{1}{1-z} \\ C(z) &= -\frac{1}{1-z} + 4 \cdot \frac{1}{(1-z)^2} - 5 \cdot \frac{1}{(1-z)^3} + 2 \cdot \frac{1}{(1-z)^4}\end{aligned}$$

Leemos los coeficientes:

$$\begin{aligned}c_n &= -1 + 4\binom{-2}{n} - 5\binom{-3}{n} + 2\binom{-4}{n} \\ &= -1 + 4\binom{n+1}{1} - 5\binom{n+2}{2} + 2\binom{n+3}{3} \\ &= -1 + 4 \cdot \frac{n+1}{1} - 5 \cdot \frac{(n+1)(n+2)}{2} + 2 \cdot \frac{(n+1)(n+2)(n+3)}{3} \\ &= \frac{4n^3 + 9n^2 + 23n + 12}{6}\end{aligned}$$

51. Esto se reduce a mover una pila de $n-1$ discos de la pila 1 a la pila 2 (los $n-1$ discos más pequeños de la pila 1) usando la pila 3 como espacio intermedio, luego mover el disco mayor de la pila 1 a la 3, y luego mover los $n-1$ discos de la pila 2 a la 3 usando la pila 1 como espacio intermedio, así completando la tarea.

    Esta descripción recursiva es suficiente para expresar la recurrencia. Llamemos h_n al número de movidas para mover una pila de n discos. Mover 0 discos significa no hacer nada:

    $$h_{n+1} = 2h_n + 1 \quad h_0 = 0$$

    Aplicando nuestras técnicas a la función generatriz ordinaria $H(z)$:

    $$\begin{aligned}\frac{H(z)-0}{z} &= 2H(z) + \frac{1}{1-z} \\ H(z) &= \frac{1}{1-2z} - \frac{1}{1-z} \\ h_n &= 2^n - 1\end{aligned}$$

    En rigor, lo que hemos hecho es demostrar que se puede hacer en $2^n - 1$ movidas, aún hace falta demostrar que no es posible hacerlo en menos

52. Ajustamos índices:

    $$u_{n+2} = 5u_{n+1} - 6u_n \qquad u_0 = 1,\, u_1 = 3$$

    Para la función generatriz ordinaria:

    $$U(z) = \sum_{n \geq 0} u_n z^n$$

    las propiedades dan:

    $$\frac{U(z) - 1 - 3z}{z^2} = 5\frac{U(z)-1}{z} - 6U(z)$$

    En fracciones parciales:

    $$U(z) = \frac{1}{1-3z}$$

    Y simplemente es:

    $$u_n = 3^n$$

53. Esta es la convolución binomial de la secuencia $\langle F_n \rangle_{n \geq 0}$ con la secuencia $\langle 1 \rangle_{n \geq 0}$, usamos funciones generatrices exponenciales. La función generatriz exponencial de la secuencia $\langle 1 \rangle_{n \geq 0}$ es simplemente e^x, para los números de Fibonacci se dedujo en el apunte:

$$\widehat{F}(z) = \frac{1}{\sqrt{5}} \left(e^{\tau z} - e^{(1-\tau)z} \right)$$

Así tenemos que la función generatriz exponencial de los S_n es:

$$\begin{aligned}
S(x) &= \sum_{n \geq 0} S_n \frac{x^n}{n!} \\
&= e^x \cdot \frac{1}{\sqrt{5}} \left(e^{\tau x} - e^{(1-\tau)x} \right) \\
&= \frac{1}{\sqrt{5}} \left(e^{(1+\tau)x} - e^{(2-\tau)x} \right)
\end{aligned}$$

En consecuencia, tenemos:

$$\begin{aligned}
S_n &= \left[\frac{x^n}{n!} \right] \frac{1}{\sqrt{5}} \left(e^{(1+\tau)x} - e^{(2-\tau)x} \right) \\
&= \frac{1}{\sqrt{5}} \left(\left[\frac{x^n}{n!} \right] e^{(1+\tau)x} - \left[\frac{x^n}{n!} \right] e^{(2-\tau)x} \right) \\
&= \frac{1}{\sqrt{5}} \left((1+\tau)^n - (2-\tau)^n \right)
\end{aligned}$$

54. Para simplificar, escribimos la recurrencia como

$$a_{n+2} = a_{n+1} + 2a_n + 2n + (-1)^n \qquad a_0 = 11,\ a_1 = 8$$

a) Definimos la función generatriz ordinaria:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Aplicando las propiedades de funciones generatrices ordinarias:

$$\begin{aligned}
\frac{A(z) - a_0 - a_1 z}{z^2} &= \frac{A(z) - a_0}{z} + A(z) + zD \frac{2}{1-z} + \frac{1}{1+z} \\
\frac{A(z) - 11 - 8z}{z^2} &= \frac{A(z) - 11}{z} + A(z) + \frac{2z}{(1-z)^2} + \frac{1}{1+z}
\end{aligned}$$

Despejando y reduciendo a fracciones parciales queda lo que se da como dato para la parte (b):

$$A(z) = \frac{1}{2} \cdot \frac{1}{1+z} + \frac{29}{2} \cdot \frac{1}{1-z} - \frac{6}{(1-z)^2} + \frac{2}{(1-z)^3}$$

b) De la expresión dada se "leen" los coeficientes:

$$\begin{aligned}
a_n &= \frac{(-1)^n}{2} + \frac{29}{2} - 6 \cdot \binom{-2}{n} + 2 \cdot \binom{-3}{n} \\
&= \frac{(-1)^n}{2} + \frac{29}{2} - 6 \cdot \binom{n+1}{1} + 2 \cdot \binom{n+2}{2} \\
&= \frac{(-1)^n}{2} + \frac{29}{2} - 6(n+1) + (n+1)(n+2) \\
&= n^2 - 3n + \frac{21 + (-1)^n}{2}
\end{aligned}$$

55. Para que el árbol tenga el número mínimo de nodos debe tener un subárbol menor que el otro. O sea, el árbol balanceado mínimo de altura n consta de la raíz y un subárbol balanceado mínimo de altura $n-1$ y otro de altura $n-2$. La relación de recurrencia es:

$$t_n = 1 + t_{n-1} + t_{n-2}$$

Hay un árbol balanceado de altura 0 (la raíz sola), y dos de altura 1 (la raíz y un único descendiente izquierdo o derecho). Ajustando índices resulta la recurrencia:

$$t_{n+2} = t_{n+1} + t_n + 1 \qquad t_0 = 1,\ t_1 = 2$$

Para resolver la recurrencia, definimos la función generatriz ordinaria:

$$T(z) = \sum_{n \geq 0} t_n z^n$$

Al aplicar las propiedades:

$$\frac{T(z) - 1 - 2z}{z^2} = \frac{T(z) - 1}{z} + T(z) + \frac{1}{1-z}$$

Despejamos y expresamos en fracciones parciales:

$$T(z) = \frac{2+z}{1-z-z^2} + \frac{1}{1-z}$$

El primer término es sospechosamente similar a la función generatriz de los números de Fibonacci. Tenemos, dado que $F_0 = 0$:

$$T(z) = 2\frac{F(z) - F_0}{z} + F(z) - \frac{1}{1-z}$$

De acá leemos:

$$\begin{aligned} t_n &= 2F_{n+1} + F_n - 1 \\ &= F_{n+1} + F_{n+2} - 1 \\ &= F_{n+3} - 1 \end{aligned}$$

56. Siguiendo la pista, consideramos los dos casos:

- Si n no pertenece al conjunto, tenemos simplemente los s_{n-1} conjuntos hasta $n-1$.
- Si n está contenido en el conjunto, no puede estar $n-1$. De este tipo de conjuntos hay s_{n-2}.

Como estas dos alternativas son exhaustivas y excluyentes:

$$s_n = s_{n-1} + s_{n-2}$$

Ajustando índices y adosando los valores iniciales dados:

$$s_{n+2} = s_{n+1} + s_n \qquad s_0 = 1,\ s_1 = 2$$

Definiendo la función generatriz:

$$S(z) = \sum_{n \geq 0} s_n z^n$$

$$\frac{S(z) - 1 - z}{z^2} = \frac{S(z) - 1}{z} + S(z)$$

Despejando:

$$S(z) = \frac{1}{1-z-z^2}$$

En términos de la función generatriz de los números de Fibonacci:

$$S(z) = \frac{F(z) - F_0}{z}$$

O sea, $s_n = F_{n+1}$.

57. Agregando una a a una palabra cambia la paridad, agregando b o c la deja tal cual:

$$\begin{aligned} u_{n+1} &= 2u_n + v_n & u_0 &= 1 \\ v_{n+1} &= u_n + 2v_n & v_0 &= 0 \end{aligned}$$

Para resolver este sistema, definimos las funciones generatrices ordinarias:

$$\begin{aligned} U(z) &= \sum_{n \geq 0} u_n z^n \\ V(z) &= \sum_{n \geq 0} v_n z^n \end{aligned}$$

Aplicando las propiedades:

$$\begin{aligned} \frac{U(z) - 1}{z} &= 2U(z) + V(z) \\ \frac{V(z) - 0}{z} &= U(z) + 2V(z) \end{aligned}$$

Del sistema de ecuaciones, como fracciones parciales:

$$\begin{aligned} U(z) &= \frac{1}{2} \cdot \frac{1}{1 - 3z} + \frac{1}{2} \cdot \frac{1}{1 - z} \\ V(z) &= \frac{1}{2} \cdot \frac{1}{1 - 3z} - \frac{1}{2} \cdot \frac{1}{1 - z} \end{aligned}$$

Se leen los coeficientes:

$$\begin{aligned} u_n &= \frac{1}{2}\left(3^n + 1\right) \\ v_n &= \frac{1}{2}\left(3^n - 1\right) \end{aligned}$$

58. Por completar

59. Podemos reescribir las recurrencias dadas como:

$$U_{n+2} = 2V_{n+1} + U_n \tag{16}$$
$$V_{n+2} = U_{n+1} + V_n \tag{17}$$

Estas recurrencias son válidas para $n \geq 0$. Definiendo:

$$u(z) = \sum_{n \geq 0} U_n z^n \tag{18}$$
$$v(z) = \sum_{n \geq 0} V_n z^n \tag{19}$$

Aplicando las propiedades:

$$\begin{aligned} \frac{u(z) - 1}{z^2} &= 2\frac{v(z) - 0}{z} + u(z) \\ \frac{v(z) - z}{z^2} &= \frac{u(z) - 1}{z} + v(z) \end{aligned}$$

Despejando y expresando en fracciones parciales:

$$\begin{aligned} u(z) &= \frac{1 - z^2}{1 - 4z^2 + z^4} \\ v(z) &= \frac{z}{1 - 4z^2 + z^4} \end{aligned}$$

Como estas funciones generatrices son "casi" en z^2, factorizamos y expandimos en fracciones parciales:

$$\begin{aligned}
u(z) &= \frac{\sqrt{3}-1}{2\sqrt{3}} \cdot \frac{1}{1-(2-\sqrt{3})z^2} - \frac{\sqrt{3}+1}{2\sqrt{3}} \cdot \frac{1}{1-(2+\sqrt{3})z^2} \\
v(z) &= \frac{\sqrt{3}-2}{2\sqrt{3}} \cdot \frac{1}{1-(2-\sqrt{3})z^2} - \frac{\sqrt{3}+2}{2\sqrt{3}} \frac{1}{1-(2+\sqrt{3})z^2}
\end{aligned}$$

Se leen los coeficientes:

$$\begin{aligned}
u_{2n} &= \frac{\sqrt{3}-1}{2\sqrt{3}} \cdot (2-\sqrt{3})^n - \frac{\sqrt{3}+1}{2\sqrt{3}} \cdot (2+\sqrt{3})^n \\
u_{2n+1} &= 0 \\
v_{2n} &= 0 \\
v_{2n+1} &= \frac{\sqrt{3}-2}{2\sqrt{3}} \cdot (2-\sqrt{3})^n - \frac{\sqrt{3}+2}{2\sqrt{3}} \cdot (2+\sqrt{3})^n
\end{aligned}$$

60. Para la función generatriz

$$U(z) = \sum_{n \geq 0} u_n z^n$$

suponiendo dada

$$A(z) = \sum_{n \geq 0} a_n z^n$$

las propiedades dan:

$$\frac{U(z)-1}{z} = U(z) \cdot A(z)$$

de donde

$$U(z) = \frac{1}{1-A(z)z}$$

61. Para la función generatriz

$$V(z) = \sum_{n \geq 0} v_n z^n$$

las propiedades directamente entregan

$$\frac{V(z)-1-2z}{z^2} = 3\frac{V(z)-1}{z} - 2V(z) + 5\frac{1}{1-7z}$$

En fracciones parciales es

$$V(z) = \frac{1}{6} \cdot \frac{1}{1-7z} + \frac{5}{6} \cdot \frac{1}{1-z}$$

Leemos los coeficientes:

$$v_n = \frac{7^n+5}{6}$$

62. Definimos la función generatriz ordinaria (no hay nada que indique que otra cosa valga la pena):

$$U(z) = \sum_{n \geq 0} u_n z^n$$

Las propiedades de funciones generatrices ordinarias dan:

$$\frac{U(z)-1}{z} = a \cdot \frac{1}{1-z} \cdot U(z)$$

La solución a esta ecuación es

$$\begin{aligned} U(z) &= \frac{1-z}{1-(a+1)z} \\ &= \frac{1}{a+1} + \frac{a}{a+1} \cdot \frac{1}{1-(a+1)z} \end{aligned}$$

Con esto los coeficientes son inmediatos:

$$u_n = \begin{cases} 1 & \text{si } n = 0 \\ a \cdot (a+1)^{n-1} & \text{caso contrario} \end{cases}$$

63. Aplicando las propiedades de funciones generatrices ordinarias:

$$\left((zD)^2 + 2\right) \frac{V(z) - 1 - 3z}{z^2} - 5V(z) = \frac{1}{1-2z} - 5(zD)^3 \frac{1}{1-z}$$

Gracias a `maxima`, esto se reduce a:

$$z^2 V''(z) - zV'(z) - (5z-1)V(z) = \frac{z - 9z^2 - 4z^3 + 31z^4 + 11z^5}{(1-z)^4\,(1-2z)}$$

64. Por turno:

   a) Definimos la función generatriz ordinaria:

   $$A(z) = \sum_{n \geq 0} a_n z^n$$

   Aplicando las propiedades de funciones generatrices ordinarias:

   $$\begin{aligned} \frac{A(z) - a_0 - a_1 z}{z^2} - A(z) &= 6z\mathrm{D}\frac{1}{1-z} \\ &= \frac{6z}{(1-z)^2} \end{aligned}$$

   Listing 1: Código maxima para recurrencia

```
/*
 * 20122c1p1: Find partial fraction expansion
 */

sol : solve((A - 5 * z - 3) / z^2 - A = 6 * z / (1 - z)^2, A) $
partfrac(rhs(sol[1]), z);
```

   Despejando y reduciendo a fracciones parciales (ver programa `maxima` en el listado 1) queda lo que se da como dato para la parte (b):

   $$A(z) = \frac{37}{4(1-z)} - \frac{7}{4(1+z)} - \frac{15}{2(1-z)^2} + \frac{3}{(1-z)^3}$$

   b) De la expresión dada se "leen" los coeficientes:

   $$\begin{aligned} a_n &= \frac{37}{4} - \frac{7}{4}(-1)^n - \frac{15}{2}(-1)^n \binom{-2}{n} + 3(-1)^n \binom{-3}{n} \\ &= \frac{37 - 7(-1)^n}{4} - \frac{15}{2}\binom{n+1}{1} + 3\binom{n+2}{2} \\ &= \frac{37 - 7(-1)^n + 6n^2 - 18}{4} \end{aligned}$$

65. Como los nodos son los números de 0 a n, estamos frente a estructuras rotuladas. Nos interesan entonces el número de estructuras de tamaño $n+1$.

    Llamemos $\mathcal{R}$ a la clase de objetos que nos interesa, $\mathcal{A}$ a la clase de los árboles binarios y $\mathcal{B}$ a la clase de árboles binarios con al menos un nodo. Tenemos las expresiones simbólicas:

$$\begin{aligned}
\mathcal{R} &= \textsc{Cyc}(\mathcal{B}) \\
\mathcal{B} &= \mathcal{Z} \star \mathcal{A} \star \mathcal{A} \\
\mathcal{A} &= \mathcal{E} + \mathcal{Z} \star \mathcal{A} \star \mathcal{A}
\end{aligned}$$

    Vía el método simbólico da el sistema de ecuaciones:

$$\begin{aligned}
\widehat{R}(z) &= -\ln(1 - \widehat{B}(z)) \\
\widehat{B}(z) &= z\widehat{A}^2(z) \\
\widehat{A}(z) &= 1 + z\widehat{A}^2(z)
\end{aligned}$$

66. Definamos la función generatriz bivariada:

$$C(x, y) = \sum_{\substack{k \geq 0 \\ n \geq 0}} c_{k,n} x^k y^n$$

    Aplicando las propiedades de las funciones generatrices ordinarias a la recurrencia queda:

$$\frac{C(x, y) - C(x, 0) - C(0, y) + C(0, 0)}{xy} = \frac{C(x, y) - C(x, 0)}{y} + \frac{C(x, y) - C(0, y)}{x}$$

    De las condiciones de contorno:

$$\begin{aligned}
C(0, 0) &= 1 \\
C(x, 0) &= \sum_{k \geq 0} c_{0,k} x^k = \frac{1}{1 - x} \\
C(0, y) &= \sum_{n \geq 0} c_{n,0} y^n = \frac{1}{1 - y}
\end{aligned}$$

    Substituyendo y despejando $C(x, y)$ resulta:

$$\begin{aligned}
C(x, y) &= \frac{1}{1 - (x + y)} \\
&= \sum_{\substack{r \geq 0 \\ s \geq 0}} \binom{r}{s} x^s y^{r-s} \\
&= \sum_{\substack{r \geq 0 \\ s \geq 0}} \binom{r + s}{s} x^r y^s
\end{aligned}$$

    De aquí directamente:

$$c_{n,k} = \binom{n + k}{k}$$

67. Para la función generatriz ordinaria $A(z)$ las propiedades de las funciones generatrices ordinarias dan:

$$\frac{A(z) - 1 - 2z - 4z^2}{z^3} - 2\frac{A(z) - 1}{z} + A(z) = z\mathrm{D}\frac{1}{1 - 3z} - \frac{1}{1 - z/5} + \frac{1}{1 - z}$$

La solución a esta ecuación en fracciones parciales es:

$$A(z) = \frac{2988 + 3350z}{2299(1 - z - z^2)} - \frac{97}{484(1 - 3z)} + \frac{1}{22(1 - 3z)^2} + \frac{1}{2(1 - z)} + \frac{1}{1 - z)^2} - \frac{125}{76(1 - z/5)}$$

El primer término recuerda la función generatriz de los números de Fibonacci:

$$F(z) = \frac{z}{1 - z - z^2}$$

Como $F_0 = 0$, tenemos que:

$$\frac{F(z) - F_0}{z} = \frac{1}{1 - z - z^2}$$

Con esto, y expresando los restantes términos, resulta:

$$\begin{aligned} a_n &= \frac{2988}{2299} F_{n+1} + \frac{3350}{2299} F_n - \frac{97}{484} \cdot 3^n + \frac{1}{22} \binom{-2}{n} \cdot 3^n + \frac{1}{2} \cdot 1^n - \frac{125}{76} \cdot 5^{-n} \\ &= \frac{2988}{2299} F_{n+1} + \frac{3350}{2299} F_n + \frac{22n - 75}{484} \cdot 3^n - \frac{5^{3-n}}{76} + \frac{1}{2} \end{aligned}$$

68. Es claro que el caso base es $n = 3$; hay un total de 3^3 palabras de tres letras, de las cuales debemos descontar las $3!$ palabras formadas por tres letras diferentes, para un total de $3^3 - 3! = 21$.

Debemos ver cómo construir palabras más largas con las que ya tenemos. Consideremos dos casos, dependiendo de si los últimos dos símbolos son iguales o no:

. . . $\boldsymbol{xx}$: Podemos construir una nueva palabra añadiendo una letra cualquiera. Si agregamos otra x, tenemos un nuevo $\ldots xx$ (una forma), si agregamos $y \neq x$ tenemos $\ldots xy$ (dos formas).

. . . $\boldsymbol{xy}$: Podemos cumplir la restricción añadiendo una x (queda un $\ldots xy$, una forma) o agregando y (queda un $\ldots yy$, una forma).

Si llamamos u_n al número de palabras $\ldots xx$ de largo n, y v_n al número de palabras $\ldots xy$ de largo n, obtenemos el sistema de recurrencias:

$$\begin{aligned} u_{n+1} &= u_n + v_n \\ v_{n+1} &= 2u_n + v_n \end{aligned}$$

Nos interesa $|\mathcal{B}_n| = u_n + v_n$, que coincidentalmente es u_{n+1}.

Restando las recurrencias entre sí tenemos:

$$v_{n+1} - u_{n+1} = u_n$$

substituyendo v_{n+1} de esto en la recurrencia para u_{n+2} resulta:

$$u_{n+2} = 2u_{n+1} + u_n$$

Como $|\mathcal{B}_n| = u_{n+1}$, satisface la misma recurrencia. Hace falta un segundo valor, que obtenemos cómodamente con $u_2 = 3$ y $v_2 = 3 \cdot 2 = 6$ del sistema de recurrencias:

$$\begin{aligned} u_2 = 3, u_3 &= 9, u_4 = 21, u_5 = 51 \\ v_2 = 6, v_3 &= 12, v_4 = 30, v_5 = 72 \end{aligned}$$

O sea, tenemos $|\mathcal{B}_3| = 21$ (esto coincide con el valor calculado antes) y $|\mathcal{B}_4| = 51$.

La recurrencia solicitada es:

$$|\mathcal{B}_{n+2}| = 2 \cdot |\mathcal{B}_{n+1}| + |\mathcal{B}_n| \qquad |\mathcal{B}_3| = 21, |\mathcal{B}_4| = 51$$

69. Esta recurrencia es lineal de primer orden, por lo tanto puede resolverse en términos de sumatorias. Escribamos:

$$y_{k+1} - \frac{2k+2}{k+2} y_k = \frac{k+1}{k+2}$$

El factor sumador es:

$$\prod_{0 \le r \le k} \frac{2k+2}{k+1} = \frac{2 \cdot 4 \cdot \ldots \cdot (2k+2)}{2 \cdot 3 \cdot \ldots \cdot (k+2)} = \frac{2^k \cdot (k+1)!}{(k+2)!} = \frac{2^k}{k+2}$$

Dividir la recurrencia por esto deja:

$$\frac{(k+2)y_{k+1}}{2^k} - \frac{(k+1)y_k}{2^{k-1}} = \frac{k+1}{2^k}$$

Sumando sobre $0 \le k \le n-1$, recordando $y_0 = 4$ entrega:

$$\frac{(n+1)y_n}{2^{n-1}} = 8 + 2 \sum_{0 \le k \le n-1} (k+1) \cdot 2^{-k}$$

La sumatoria sugiere:

$$\frac{\mathrm{d}}{\mathrm{d}z} \sum_{0 \le k \le n} z^k = \frac{\mathrm{d}}{\mathrm{d}z} \frac{1 - z^{n+1}}{1 - z}$$

$$\sum_{0 \le k \le n-1} (k+1) z^k = \frac{1 - (n+1)z^n + nz^{n+1}}{(1-z)^2}$$

Evaluando en $z = 1/2$ y substituyendo:

$$y_n = 2^{n+5} - 8n - 16$$

70. Sucio truco el del coeficiente binomial. Pero nos aprovecharemos...

Reescribimos la recurrencia sin restas en índices:

$$a_{n+1} = 3a_n + \binom{n+1}{2}$$

Definimos:

$$A(z) = \sum_{n \ge 0} a_n z^n$$

Multiplicamos la recurrencia por z^n, sumamos sobre $n \ge 0$, y reconocemos (ponga atención a los índices, para $n \le 1$ el coeficiente binomial se anula):

$$\sum_{n \ge 0} \binom{n+1}{2} z^n = z \sum_{n \ge 1} \binom{n+1}{2} z^{n-1}$$

Cambiamos índices $r = n - 1$:

$$\begin{aligned} &= z \sum_{r \ge 0} \binom{r+2}{2} z^r \\ &= \frac{z}{(1-z)^3} \end{aligned}$$

con lo que resulta:

$$\frac{A(z) - 1}{z} = 3A(z) + \frac{z}{(1-z)^3}$$

Expresado en fracciones parciales:

$$A(z) = \frac{11}{8(1-3z)} - \frac{1}{2(1-z)^3} + \frac{1}{4(1-z)^2} - \frac{1}{8(1-z)}$$

Leemos directamente los coeficientes:

$$\begin{aligned} a_n &= \frac{11}{8} \cdot 3^n - \frac{1}{2}\binom{-3}{n}(-1)^n + \frac{1}{4}\binom{-2}{n}(-1)^n - \frac{1}{8} \\ &= \frac{11 \cdot 3^n - 1}{8} - \frac{1}{2}\binom{n+3-1}{3-1} + \frac{1}{4}\binom{n+2-1}{2-1} \\ &= \frac{11 \cdot 3^n - 1}{8} - \frac{1}{2} \cdot \frac{(n+2)(n+1)}{2!} + \frac{1}{4} \cdot \frac{n+1}{1!} \\ &= \frac{11 \cdot 3^n - 2n^2 - 4n - 3}{8} \end{aligned}$$

71. Definimos la función generatriz $A(z)$ y aplicamos las propiedades:

$$\frac{A(z) - 1 - 3z}{z^2} = 9\frac{A(z) - 1}{z} - 18A(z)$$

Esto entrega:

$$A(z) = \frac{1}{1-3z}$$

con lo que:

$$a_n = 3^n$$

Vemos que cumple con la recurrencia y las condiciones iniciales.

72. Definamos $u_n = n^2 a_n$, lo que transforma la recurrencia en:

$$u_{n+1} - 5u_n + 2 = 0$$

Definimos $U(z) = \sum_{n \geq 0} u_n z^n$, aplicando las propiedades:

$$\frac{U(z)}{z} - 5U(z) + \frac{2}{1-z} = 0$$

Como fracciones parciales:

$$U(z) = \frac{1}{2(1-5z)} - \frac{1}{2(1-z)}$$

Los coeficientes son inmediatos:

$$\begin{aligned} u_n &= \frac{5^n - 1}{2} \\ a_n &= \begin{cases} 0 & n = 0 \\ \dfrac{5^n - 1}{2n^2} & n \geq 1 \end{cases} \end{aligned}$$

73. La danza tradicional entrega para la función generatriz

$$g(z) = \sum_{n \geq 0} x_n z^n$$

la siguiente ecuación:

$$\frac{g(z) - 1 - z}{z^2} + \frac{g(z) - 1}{z} + g(z) = 0$$

o sea:

$$g(z) = \frac{1 + 2z}{1 + z + z^2}$$

El camino normal sería dividir en fracciones parciales, que nos lleva a enredarnos con números complejos. Podemos simplificar la tarea reconociendo:

$$1 - z^3 = (1 - z)(1 + z + z^2)$$

con lo que:

$$\begin{aligned} g(z) &= \frac{1 + z - 2z^2}{1 - z^3} \\ &= (1 + z - 2z^2) \sum_{n \geq 0} z^{3n} \\ &= \sum_{n \geq 0} (z^{3n} + z^{3n+1} - 2z^{3n+2}) \end{aligned}$$

Vale decir, la secuencia repite $\langle 1, 1, -2 \rangle$.

74. Definimos la función generatriz ordinaria de los coeficientes $G(z)$, escribimos la recurrencia sin restas en índices:

$$g_{n+3} = 12g_{n+1} - 16g_n + 48 \cdot 2^n + 25n + 75$$

Aplicar las propiedades de funciones generatrices ordinarias entrega:

$$\frac{G(z) - 23 - 37z - 42z^2}{z^3} = 12\frac{G(z) - 23}{z} - 16G(z) + 48\frac{1}{1 - 2z} + 25\frac{z}{(1 - z)^2} + 75\frac{1}{1 - z}$$

que da:

$$\begin{aligned} G(z) &= \frac{23 - 55z - 267z^2 + 1198z^3 - 1540z^4 + 612z^5}{1 - 4z + 7z^2 - 62z^3 + 124z^4 - 104z^5 + 32z^6} \\ &= \frac{19}{1 - z} + \frac{5}{(1 - z)^2} - \frac{2}{(1 - 2z)^2} + \frac{2}{(1 - 2z)^3} - \frac{1}{1 + 4z} \end{aligned}$$

Podemos leer los coeficientes:

$$\begin{aligned} g_n &= 19 + 5\binom{n + 2 - 1}{2 - 1} - 2\binom{n + 2 - 1}{2 - 1} \cdot 2^n + 2\binom{n + 3 - 1}{3 - 1} \cdot 2^n - 4^n \\ &= 24 + 5n + (n^2 + n) \cdot 2^n - 4^n \end{aligned}$$

75. Hacemos el cambio de variables:

$$\begin{aligned} n &= 2^k \\ f(n) &= f_k \end{aligned}$$

con lo que la recurrencia queda:

$$f_k = 5f_{k-1} - 4f_{k-2} \qquad f_0 = 1, f_1 = 2$$

Escribiendo sin restas en índices;

$$f_{k+2} = 5f_{n+1} - 4f_k$$

Para la función generatriz ordinaria de los términos $F(z)$ tenemos:

$$\frac{F(z) - 1 - 2z}{z^2} = 5\frac{F(z) - 1}{z} - 4F(z)$$

que resulta en:

$$F(z) = \frac{2}{3} \cdot \frac{1}{1 - z} + \frac{1}{3} \cdot \frac{1}{1 - 4z}$$

En consecuencia:

$$f_k = \frac{2 + 4^k}{3}$$

Volvemos a las variables originales:

$$f(n) = \frac{2 + n^2}{3}$$

76. El lado derecho de la recurrencia se ve sospechosamente como el recíproco de una suma de fracciones, lo que sugiere el cambio de variable:

$$u_n = \frac{1}{a_n}$$

Substituyendo resulta:

$$u_{n+2} = \frac{u_{n+1} + u_n}{2}$$

Definimos la función generatriz ordinaria $U(z)$, las propiedades dan:

$$\frac{U(z) - 1 - z/m}{z^2} = \frac{U(z) - 1}{2z} + \frac{U(z)}{2}$$

lo que da:

$$U(z) = \frac{2m + 1}{3m(1 - z)} - \frac{2(m - 1)}{3m(1 + z/2)}$$

de donde directamente:

$$u_n = \frac{m + 2}{3m} - \frac{2(m - 1)}{3m} \left(-\frac{1}{2}\right)^n$$

Claramente:

$$\lim_{n \to \infty} u_n = \frac{m + 2}{3m}$$
$$\lim_{n \to \infty} a_n = \frac{3m}{m + 2}$$

77. Tenemos:

$$u_{n+1} = s_{n+1} - s_n = s_n^2 - s_n$$

Por lo tanto:

$$s_{n+1} = s_n^2$$

Con el cambio de variables $b_n = \log_2 s_n$ queda:

$$b_{n+1} = 2b_n \qquad b_0 = 1$$

por lo que:

$$b_n = 2^n$$
$$s_n = 2^{2^n}$$
$$u_n = s_n - s_{n-1} = 2^{2^n} - 2^{2^{n-1}}$$

Tenemos el valor exacto, si se requiere una cota más simple puede extraerse de acá.

78. Llamemos a_n al número de formas de ingresar n dólares a la máquina. Claramente, ingresar $0 \leq n \leq 4$ dólares puede hacerse de 2^n maneras (es una secuencia de n elecciones entre dos alternativas). Para ingresar 5 o más nos fijamos en la última moneda o billete introducidos. Si es una moneda o billete de 1 dólar, antes de eso se ingresaron a_{n-1}, y con esta última selección son $2a_{n-1}$ formas; si es un billete de 5 dólares, antes de eso fueron a_{n-5}. O sea, para $n \geq 5$:

$$a_n = 2a_{n-1} + a_{n-5}$$

Alternativamente:

$$a_{n+5} = 2a_{n+4} + a_n \qquad a_0 = 1, a_1 = 2.a_2 = 4, a_3 = 8, a_4 = 16$$

79. Definimos la función generatriz doble:

$$g(x, y) = \sum_{r,s} A(r, s) x^r y^s$$

Escribimos la recurrencia sin restas en los índices:

$$A(r + 1, s + 1) = A(r, s + 1) + (c - 1)A(r, s)$$

De la condición de contorno:

$$g(x, 0) = \sum_r A(r, 0) x^r = \frac{1}{1 - x}$$

La correspondiente función $g(0, y)$ quedará de incógnita por ahora.

Multiplicando la recurrencia por $x^r y^s$ y sumando sobre $r, s \geq 0$ queda:

$$\frac{g(x, y) - g(0, y) - 1/(1 - x) + 1}{xy} = \frac{g(x, y) - 1/(1 - x)}{y} + (c - 1)g(x, y)$$

Resolviendo para $g(x, y)$:

$$\begin{aligned} g(x, y) &= \frac{g(0, y)}{1 - x - (c - 1)xy} \\ &= g(0, y) \frac{1}{1 - ((c - 1)y + 1)x} \\ &= g(0, y) \sum_r ((c - 1)y + 1)^r x^r \end{aligned}$$

En consecuencia:

$$A(r, r) = [x^r y^r] g(x, y) = [y^r] g(0, y)((c - 1)y + 1)^r = c^r$$

Vale decir:

$$\sum_{0 \leq k \leq r} \binom{r}{k} (c - 1)^{r-k} A(0, k) = c^r$$

Multiplicando la última ecuación por $z^r/r!$ y sumando sobre $r \geq 0$ reconocemos:

$$\left(\sum_{k\geq 0} A(0,k)\frac{z^k}{k!}\right)\cdot \exp((c-1)z) = \exp(cz)$$

$$\sum_{k\geq 0} A(0,k)\frac{z^k}{k!} = \exp(z)$$

con lo que $A(0,k) = 1$, y:

$$g(0,y) = \frac{1}{1-y}$$

Resulta:

$$\begin{aligned}
A(r,s) &= [x^r y^s]\frac{1}{(1-y)(1-x-(c-1)xy)} \\
&= [x^r y^s]\frac{1}{1-y}\sum_k (1+(c-1)y)^k x^k \\
&= [y^s]\frac{(1+(c-1)y)^r}{1-y} \\
&= \sum_{0\leq k\leq s}\binom{r}{k}(c-1)^k
\end{aligned}$$

80. Definimos la función generatriz ordinaria:

$$A(z) = \sum_{n\geq 0} a_n z^n$$

Reescribimos la recurrencia sin restas en los índices:

$$(n+2)a_{n+2} = 2a_{n+1} + 2a_n$$

Aplicando las propiedades de funciones generatrices ordinarias:

$$(z\mathrm{D}+2)\frac{A(z)-a_0-a_1z}{z^2} = 2\frac{A(z)-a_0}{z} + 2A(z)$$

Resulta la ecuación diferencial separable:

$$A'(z) = (2z+2)A(z)$$

cuya solución es:

$$A(z) = \exp(z^2+2z)$$

81. Sea a_n el número de secuencias de largo n que cumplen lo pedido. Entonces $a_2 = a_3 = 3$ (sólo un tipo de símbolo). Para crear una secuencia de largo n, podemos agregar el símbolo final a una de largo $n-1$ (una manera) o dos símbolos diferentes al final a una de largo $n-2$ (dos elecciones). O sea:

$$a_{n+2} = a_{n+1} + 2a_n \qquad a_2 = a_3 = 3$$

Definimos:

$$A(z) = \sum_{n\geq 0} a_{n+2} z^n$$

Las propiedades de funciones generatrices ordinarias dan:

$$\frac{A(z)-3-3z}{z^2} = \frac{A(z)-3}{z} + 2A(z)$$

De acá:

$$A(z) = \frac{2}{1 - 2z} + \frac{1}{1 + z}$$

Podemos leer los coeficientes:

$$a_{n+2} = 2 \cdot 2^n + (-1)^n$$

82. Llamemos $s_{xy}^{(n)}$ al número de secuencias de largo n con paridad x de ceros e y de unos. Claramente es:

$$s_{00}^{(0)} = 1 \quad s_{01}^{(0)} = s_{10}^{(0)} = s_{11}^{(0)} = 0$$

Considerando las maneras en que se crean las distintas opciones de largo $n + 1$ a partir de las de largo n tenemos:

$$\begin{aligned}
s_{00}^{(n+1)} &= 2s_{00}^{(n)} + s_{01}^{(n)} + s_{10}^{(n)} \\
s_{01}^{(n+1)} &= s_{00}^{(n)} + 2s_{01}^{(n)} + s_{11}^{(n)} \\
s_{10}^{(n+1)} &= s_{00}^{(n)} + 2s_{10}^{(n)} + s_{11}^{(n)} \\
s_{11}^{(n+1)} &= s_{01}^{(n)} + s_{10}^{(n)} + 2s_{11}^{(n)}
\end{aligned}$$

Definimos las funciones generatrices ordinarias respectivas $S_{xy}(z)$, con las propiedades resulta el sistema de ecuaciones:

$$\begin{aligned}
\frac{S_{00}(z) - 1}{z} &= 2S_{00}(z) + S_{01}(z) + S_{10}(z) \\
\frac{S_{01}(z)}{z} &= S_{00}(z) + 2S_{01}(z) + S_{11}(z) \\
\frac{S_{10}(z)}{z} &= S_{00}(z) + 2S_{10}(z) + S_{11}(z) \\
\frac{S_{11}(z)}{z} &= S_{01}(z) + S_{10}(z) + 2S_{11}(z)
\end{aligned}$$

De acá nos interesa únicamente:

$$S_{00}(z) = \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{1 - 2z} + \frac{1}{4} \cdot \frac{1}{1 - 4z}$$

Leemos los coeficientes:

$$s_{00}^{(n)} = \frac{1}{4} \cdot [n = 0] + 2^{n-1} + 4^{n-1}$$

83. El cambio de variables $n = 4^k$, $t(4^k) = t_k$, al correr índices para evitar restas en índices deja:

$$t_{k+1} = t_k + 2 \cdot 2^k + 16 \cdot 16^k + \frac{32k}{3} \cdot 16^k$$

Definimos la función generatriz ordinaria $T(z)$, las propiedades entregan:

$$\frac{T(z) - t_0}{z} = T(z) + 2 \cdot \frac{1}{1 - 2z} + 16 \cdot \frac{1}{1 - 16z} + \frac{32}{3} \cdot \frac{16z}{(1 - 16z)^2}$$

Podemos leer los coeficientes:

$$\begin{aligned}
t_k &= \frac{32}{45}(k + 1) \cdot 16^k - \frac{272}{675} \cdot 16^k + 2 \cdot 2^k + \frac{675t_0 - 1558}{675} \\
&= \frac{32}{45} \cdot k \cdot 16^k + \frac{208}{675} \cdot 16^k + 2 \cdot 2^k + \frac{675t_0 - 1558}{675}
\end{aligned}$$

En términos de las variables originales:

$$\begin{aligned}
t(n) &= \frac{32}{45} n^2 \log_4 n - \frac{272}{675} n^2 + 2\sqrt{n} + \frac{675t_0 - 1558}{675} \\
&= \frac{16}{45} n^2 \log_2 n - \frac{272}{675} n^2 + 2\sqrt{n} + \frac{675t_0 - 1558}{675}
\end{aligned}$$

84. Sea a_n el número de secuencias solicitadas. Está claro que si b_n es el número de secuencias de largo n sin unos seguidos:

$$a_n = 2^n - b_n$$

Ahora bien, una secuencia que no contiene unos seguidos de largo n está formada por una secuencia sin unos seguidos de largo $n-1$ y un cero, o termina en un uno, en cuyo caso el penúltimo símbolo es un cero y antes de eso hay una secuencia sin ceros seguidos de largo $n-2$. O sea, agregando las condiciones iniciales:

$$b_{n+2} = b_{n+1} + b_n \qquad b_0 = 1, b_1 = 2$$

Se ve que $b_n = F_{n+2}$, con lo que:

$$a_n = 2^n - F_{n+2}$$

85. Notar que las condiciones se pueden resumir en que cada 0 viene seguido inmediatamente por un 2. O sea, una secuencia de largo n es una de largo $n-1$ seguida por 1 o 2, o es una secuencia de largo $n-2$ seguida por 02. Si s_n es el número de secuencias de interés de largo n, esto se traduce en:

$$s_{n+2} = 2s_{n+1} + s_n$$

Condiciones iniciales son $s_0 = 1$, $s_1 = 2$. La danza tradicional da:

$$\begin{aligned} S(z) &= \frac{1}{1 - 2z - z^2} \\ &= \frac{1+\sqrt{2}}{2\sqrt{2}} \cdot \frac{1}{1-(1+\sqrt{2})z} + \frac{1-\sqrt{2}}{2\sqrt{2}} \cdot \frac{1}{1-(1-\sqrt{2})z} \end{aligned}$$

y en consecuencia:

$$s_n = \frac{(\sqrt{2}+1)^{n+1}}{2\sqrt{2}} - \frac{(1-\sqrt{2})^{n+1}}{2\sqrt{2}}$$

86. Consideremos una secuencia binaria comenzada en 1, hay tres posibilidades módulo 3. Llamemos a_n al número de secuencias que dejan resto 0 al dividir por 3, b_n al número de secuencias que deja resto 1, y c_n las que dejan resto 2. Como el primer bit es uno, es claro que:

$$a_n + b_n + c_n = 2^{n-1}$$

Considerando lo que ocurre al añadir bits 0 y 1 a cada una de las opciones, lo que corresponde a multiplicar por 2 y sumar el bit indicado: La tabla 7 resume las opciones, que indican que:

	0	1
0	0	1
1	2	0
2	1	2

Cuadro 7: Añadir bits a números módulo 3

$$\begin{aligned} a_{n+1} &= a_n + b_n \\ b_{n+1} &= a_n + c_n \\ c_{n+1} &= b_n + c_n \end{aligned}$$

Sabemos también que $a_1 = 0$, $b_1 = 1$, $c_1 = 0$. Definamos funciones generatrices:

$$\begin{aligned} A(z) &= \sum_{n \geq 0} a_{n+1} z^n \\ B(z) &= \sum_{n \geq 0} b_{n+1} z^n \\ C(z) &= \sum_{n \geq 0} c_{n+1} z^n \end{aligned}$$

Las recurrencias dan:

$$\begin{aligned}
\frac{A(z)}{z} &= A(z) + B(z) \\
\frac{B(z) - 1}{z} &= A(z) + C(z) \\
\frac{C(z)}{z} &= B(z) + C(z)
\end{aligned}$$

Nos interesa únicamente:

$$\begin{aligned}
A(z) &= \frac{z}{1 - z - 2z^2} \\
&= \frac{1}{3} \cdot \frac{1}{1 - 2z} - \frac{1}{3} \cdot \frac{1}{1 + z}
\end{aligned}$$

Leemos los coeficientes:

$$a_n = \frac{2^{n-1} - (-1)^{n-1}}{3}$$

14. Aplicaciones a probabilidades

1. Por turno.

   a) Dada la función generatriz $P(z)$, la función generatriz de la secuencia $\langle g(n) p_n \rangle_{n \geq 0}$ es $g(z\mathrm{D})P(z)$. La suma de estos valores es simplemente $g(z\mathrm{D})P(z)|_{z=1}$.

   b) Los valores p_n indicados claramente son positivos. Además:

   $$\sum_{n \geq 0} \frac{(\lambda t)^n}{n!} = e^{\lambda t}$$

   con lo que suman 1 (y ninguno puede sobrepasarlo). Es una distribución de probabilidad.

   c) La función generatriz de probabilidad es

   $$P(z) = \sum_{n \geq 0} \frac{(\lambda t z)^n}{n!} e^{-\lambda t} = e^{(z-1)\lambda t}$$

   Por el primer punto, tenemos:

   $$\begin{aligned}
   \mu &= z\mathrm{D}P(z)|_{z=1} \\
   &= P'(1) \\
   \sigma^2 &= E((n-\mu)^2) \\
   &= E(n^2 - 2\mu n + \mu^2) \\
   &= \left((z\mathrm{D})^2 - 2\mu z\mathrm{D} + \mu^2\right) P(z)|_{z=1} \\
   &= (zP'(z) + z^2 P''(z) - 2\mu z P'(z) + \mu^2 P(z))|_{z=1} \\
   &= P''(1) + P'(1) - (P'(1))^2
   \end{aligned}$$

   Esto último porque $P(1) = 1$ y $P'(1) = \mu$. En nuestro caso:

   $$\begin{aligned}
   \mu &= P'(1) \\
   &= \lambda t \\
   \sigma^2 &= P''(1) + P'(1) - (P'(1))^2 \\
   &= (\lambda t)^2 + \lambda t - (\lambda t)^2 \\
   &= \lambda t
   \end{aligned}$$

15. Aplicaciones combinatorias

1. Esto es el número de desarreglos (derangements) de 10 elementos, que sabemos que es aproximadamente e^{-1} del total, que da 0,368 como la probabilidad de tan mala suerte.

2. La más simple es notar que el número de Stirling de primera especie $\left[{n \atop k}\right]$ es el número de permutaciones de n elementos con k ciclos. Como hay un total de $n!$ de permutaciones de n elementos, y estas tienen entre 1 y n ciclos si $n > 0$, al sumar sobre el número de ciclos estamos contabilizando todas las permutaciones, o sea para $n > 0$:

$$\sum_{0 \le k \le n} \left[{n \atop k}\right] = n!$$

La convención es que una permutación de 0 elementos tiene 1 ciclo de largo 0 (o sea $\left[{0 \atop 0}\right] = 1$), con lo que también

$$\sum_{0 \le k \le 0} \left[{0 \atop k}\right] = 0!$$

3. Para cada tipo de fruta tenemos las respectivas funciones generatrices:

Frutillas: En múltiplos de 6.

$$1 + z^6 + z^{12} + \cdots = \frac{1}{1 - z^6}$$

Manzanas: Un número impar.

$$z + z^3 + \cdots = \frac{z}{1 - z^2}$$

Plátanos: Entre 2 y 7.

$$z^2 + z^3 + z^4 + z^5 + z^6 + z^7 = \frac{z^2(1 - z^6)}{1 - z}$$

Naranjas: Sólo 0 o 1.

$$1 + z$$

Uniendo las piezas, la función generatriz $P(z)$ del número p_n de postres con n frutas es:

$$\begin{aligned} P(z) &= \frac{1}{1 - z^6} \frac{z}{1 - z^2} \frac{z^2(1 - z^6)}{1 - z} (1 + z) \\ &= \frac{z^3}{(1 - z)^2} \end{aligned}$$

O sea:

$$\begin{aligned} p_n &= [z^n] z^3 (1 - z)^{-2} \\ &= \binom{-2}{n - 3} (-1)^{n-3} \\ &= \binom{n - 3 + 2 - 1}{2 - 1} \\ &= \binom{n - 2}{1} \\ &= [n \ge 2](n - 2) \end{aligned}$$

4. Como 10 000 es mayor que 2 013, podemos asumir que el número de pelotas de cada color es infinito para simplificar.

   Usamos funciones generatrices. Un número cualquiera de pelotas queda descrito por:

$$1 + z + z^2 + \cdots = \frac{1}{1 - z}$$

   El número de pelotas rojas, si debe ser par, queda representado por:

$$1 + z^2 + z^4 + \cdots = \frac{1}{1 - z^2}$$

   Esta situación lleva a la función generatriz para el número total de formas de elegir 2 013 pelotas con un número par de pelotas rojas:

$$(1 + z^2 + z^4 + \cdots) \cdot (1 + z + z^2 + \cdots) \cdot (1 + z + z^2 + \cdots) = \frac{1}{1 - z^2} \cdot \frac{1}{1 - z} \cdot \frac{1}{1 - z}$$

   Para un número impar de pelotas amarillas es:

$$(z + z^3 + z^5 + \cdots) \cdot (1 + z + z^2 + \cdots) \cdot (1 + z + z^2 + \cdots) = \frac{z}{1 - z^2} \cdot \frac{1}{1 - z} \cdot \frac{1}{1 - z}$$

   La unión de ambos es lo que nos interesa, lo que es sumar ambas funciones generatrices. Pero así contamos la intersección (número par de pelotas rojas e impar de amarillas) dos veces, debemos restar lo que corresponde, que es:

$$(1 + z^2 + z^4 + \cdots) \cdot (z + z^3 + z^5 + \cdots) \cdot (1 + z + z^2 + \cdots) = \frac{1}{1 - z^2} \cdot \frac{z}{1 - z^2} \cdot \frac{1}{1 - z}$$

   Uniendo las piezas, la función generatriz es:

$$\frac{1}{1 - z^2} \cdot \frac{1}{(1 - z)^2} + \frac{z}{1 - z^2} \cdot \frac{1}{(1 - z)^2} - \frac{1}{1 - z^2} \cdot \frac{z}{1 - z^2} \cdot \frac{1}{1 - z} = \frac{1 + z + z^2}{(1 - z)^3 (1 + z)^2}$$

   El número que nos interesa es:

$$\begin{aligned}
\left[z^{2\,013}\right] \frac{1 + z + z^2}{(1 - z)^3 (1 + z)^2} &= \left[z^{2\,013}\right] \frac{1}{16(1 + z)} + \frac{1}{8(1 + z)^2} + \frac{1}{16(1 - z)} + \frac{3}{4(1 - z)^3} \\
&= (-1)^{2\,013} \frac{1}{16} + (-1)^{2\,013} \frac{1}{8} \binom{-2}{2\,013} + \frac{1}{16} + \frac{3}{4} \binom{-3}{2\,013} \\
&= -\frac{1}{16} - \frac{1}{8} \binom{2\,013 + 2 - 1}{2 - 1} + \frac{1}{16} + \frac{3}{4} \binom{2\,013 + 3 - 1}{3 - 1} \\
&= 1\,521\,577
\end{aligned}$$

5. El primer dígito no puede ser 0, así que estamos eligiendo 4 dígitos entre 1 y 9, cualquier conjunto de dígitos puede ordenarse de menor a mayor de una única manera. En consecuencia hay:

$$\binom{9}{4} = 126$$

6. El número de progresiones $\langle a - k, a, a + k \rangle$ es $a - 1$ si $2 \leq a \leq n$ y $2n - a$ si $n + 1 \leq a \leq 2n - 1$. Sumando ambas:

$$\sum_{2 \leq a \leq n} (a - 1) + \sum_{n+1 \leq a \leq n} (2n - a) = 2 \sum_{1 \leq a \leq n-1} a = n(n - 1)$$

   Otra manera es notar que los extremos $a - k$ y $a + k$ son ambos pares o ambos impares (la diferencia entre los dos es el número par $2k$). Si ambos son pares, pueden elegirse de $\binom{n}{2}$ maneras; si ambos son impares pueden elegirse de $\binom{n}{2}$ maneras. En total:

$$2\binom{n}{2} = n(n - 1)$$

16. Método simbólico

1. Por completar

2. Por completar

3. Un genoma está formado por genes diferentes, por lo que debemos considerar objetos rotulados (y funciones generatrices exponenciales).

   Sean $\mathcal{L}$ la clase de genomas lineales, y $\mathcal{C}$ la de los compuestos de ciclos. Simbólicamente:

$$\begin{aligned}\mathcal{L} &= \textsc{Seq}(\mathcal{Z})\\ \mathcal{C} &= \textsc{MSet}(\textsc{Cyc}(\mathcal{Z}))\end{aligned}$$

   Las funciones generatrices respectivas son:

$$\begin{aligned}\widehat{L}(z) &= \frac{1}{1-z}\\ \widehat{C}(z) &= \exp\left(\ln\frac{1}{1-z}\right)\\ &= \frac{1}{1-z}\end{aligned}$$

   Como las funciones generatrices son iguales, el número de genomas con n genes es exactamente el mismo.

4. Los nudos son intercambiables, son objetos no rotulados (y funciones generatrices ordinarias). Son m nudos, por lo que un nudo queda representado por:

$$\mathcal{N} = m\mathcal{Z}$$

   La clase $\mathcal{Q}$ de quipus queda descrita por:

$$\mathcal{Q} = \textsc{Seq}(\textsc{Seq}_{\geq 1}(\mathcal{N}))$$

   O sea:

$$\begin{aligned}Q(z) &= \frac{1}{1-(1/(1-mz)-1)}\\ &= \frac{1-mz}{1-2mz}\\ &= \frac{1}{2} + \frac{1}{2}\cdot\frac{1}{1-2mz}\end{aligned}$$

   De acá se leen los coeficientes directamente:

$$q_n = \frac{[n=0] + (2m)^n}{2}$$

5. Usamos el método simbólico para derivar directamente una ecuación para la función generatriz. Sea $\mathcal{S}_k$ la clase de las secuencias que nos interesan. Son:

   - La secuencia vacía
   - Un único 0
   - Si termina en 0, el número anterior no puede ser 0

   Podemos escribir:

$$\mathcal{S}_k = \mathcal{E} + \{0\} + \mathcal{S}_k \times \{1, 2, \ldots, k\} + \mathcal{S}_k \times \{1, 2, \ldots, k\} \times \{0\}$$

Si z marca el largo, para cada una de las clases involucradas:

$$\begin{aligned}
\{0\} &\longleftrightarrow z \\
\{1, 2, \ldots, k\} &\longleftrightarrow kz
\end{aligned}$$

y tenemos para la función generatriz ordinaria para la clase:

$$S_k(z) = 1 + z + kzS_k(z) + kz^2 S_k(z)$$

Despejando:

$$S_k(z) = \frac{1 + z}{1 - kz - kz^2}$$

En fracciones parciales:

$$S_k(z) = \frac{k + 2 + \sqrt{k^2 + 4k}}{2\sqrt{k^2 + 4k}} \cdot \frac{1}{1 - (k + \sqrt{k^2 + 4k})z/2} - \frac{k + 2 - \sqrt{k^2 + 4k}}{2\sqrt{k^2 + 4k}} \cdot \frac{1}{1 - (k - \sqrt{k^2 + 4k})z/2}$$

Leemos los coeficientes:

$$[z^n]\, S_k(z) = \frac{k + 2 + \sqrt{k^2 + 4k}}{2\sqrt{k^2 + 4k}} \cdot \left(\frac{k + \sqrt{k^2 + 4k}}{2} \right)^n - \frac{k + 2 - \sqrt{k^2 + 4k}}{2\sqrt{k^2 + 4k}} \cdot \left(\frac{k - \sqrt{k^2 + 4k}}{2} \right)^n$$

6. Ambos casos son independientes, se resuelven en forma diferente.

   a) **Secuencias sin 00:** Pueden describirse como la secuencia vacía, un único 0 o una secuencia de éstas seguida por 1 o por 10. Simbólicamente:

   $$\mathcal{S}_{00} = \mathcal{E} + \{0\} + \mathcal{S}_{00} \times \{1\} + \mathcal{S}_{00} \times \{1\} \times \{0\}$$

   Como sólo interesan los largos:

   $$S_{00}(z) = 1 + z + S_{00}(z)(z + z^2)$$

   Despejando:

   $$S_{00}(z) = \frac{1 + z}{1 - z + z^2}$$

   Esto corresponde a la función generatriz de los números de Fibonacci desplazados:

   $$s_n^{(00)} = F_n + F_{n+1} = F_{n+2}$$

   b) **Secuencias sin 01:** En cuanto aparece un 0, ya no pueden haber más 1. Vale decir, son secuencias de 1 seguidas por secuencias de 0. Simbólicamente:

   $$\mathcal{S}_{01} = \textsc{Seq}(\{1\}) \times \textsc{Seq}(\{0\})$$

   O sea:

   $$S_{01}(z) = \frac{1}{(1 - z)^2}$$

   de donde:

   $$\begin{aligned}
   s_n^{(01)} &= (-1)^n \binom{-2}{n} \\
   &= \binom{2 + n - 1}{2 - 1} \\
   &= \binom{n + 1}{1} \\
   &= n + 1
   \end{aligned}$$

   Esto tiene una explicación simple: Quedan determinadas por el número de 1, en el rango 0 a n.

7. Es aplicable el método simbólico para clases rotuladas. Si nuestra clase es $\mathcal{B}$, queda representada por:

$$\mathcal{B} = \mathcal{E} + \mathcal{Z} \star \mathcal{B} \star \mathcal{B}$$

Para la respectiva función generatriz:

$$\widehat{B}(z) = 1 + z\widehat{B}^2(z)$$

Esta es la función generatriz de Catalan. Sabemos así:

$$\frac{b_n}{n!} = C_n = \frac{1}{n+1}\binom{2n}{n}$$

(No es particularmente sorprendente, C_n cuenta el número de árboles binarios sin rotular; podemos distribuir n rótulos entre los n nodos de $n!$ formas.)

8. Definamos la clase $\mathcal{A}$ para arbustos. Directamente de la definición:

$$\mathcal{A} = \mathcal{Z} + \mathcal{Z} \times \textsc{Seq}_{\geq 2}(\mathcal{A})$$

De acá, o también directamente:

$$\mathcal{A} = \mathcal{Z} + \mathcal{Z} \times \mathcal{A} \times \mathcal{A} \times \textsc{Seq}(\mathcal{A})$$

lo que da:

$$A(z) = z\left(1 + \frac{A^2(z)}{1 - A(z)}\right)$$

Es aplicable la fórmula de inversión de Lagrange:

$$\begin{aligned}
a_n &= \frac{1}{n}\left[u^{n-1}\right]\left(1 + \frac{u^2}{1-u}\right)^n \\
&= \frac{1}{n}\left[u^{n-1}\right]\sum_{k\geq 0}\binom{n}{k}u^{2k}(1-u)^{-k} \\
&= \frac{1}{n}\sum_{k\geq 0}\binom{n}{k}\left[u^{n-2k-1}\right](1-u)^{-k} \\
&= \frac{1}{n}\sum_{k\geq 0}\binom{n}{k}\cdot(-1)^{n-2k-1}\binom{-k}{n-2k-1} \\
&= \frac{1}{n}\sum_{k\geq 0}\binom{n}{k}\binom{n-k-2}{k-1}
\end{aligned}$$

Lamentablemente esta última suma no tiene forma cerrada.

9. Sea M_l el número de secuencias Morse de largo l. El largo solicitado es el primer l tal que:

$$S_l = \sum_{1\leq k\leq k} M_k \geq n$$

Sea entonces $m(z)$ la función generatriz de los M_l, y $s(z)$ la de las sumas que nos interesan, o sea:

$$\begin{aligned}
m(z) &= \sum_{l\geq 0} M_l z^l \\
s(z) &= \sum_{l\geq 0}\left(\sum_{1\leq k\leq l} M_k\right)z^l
\end{aligned}$$

Acá z marca una unidad de duración, y como una secuencia es nada, o es una secuencia seguida por un punto (duración 1) o una raya (duración 2) tenemos:

$$\begin{aligned} m(z) &= 1 + zm(z) + z^3 m(z) \\ &= \frac{1}{1 - z - z^3} \end{aligned}$$

Revisar/completar

10. Para la clase $\mathcal{M}$ que nos interesa tenemos la expresión simbólica:

$$\mathcal{M} = \mathcal{E} + \mathcal{M} \times \{\cdot, -\}$$

Con z marcando las duraciones esto da:

$$\begin{aligned} M(z) &= 1 + M(z)(z + z^3) \\ M(z) &= \frac{1}{1 - z - z^3} \end{aligned}$$

11. Llamando $\mathcal{T}$ a la clase de estos extraños árboles, vemos que se compone del árbol vacío ($\mathcal{E}$) o de una raíz y tres subárboles ($\mathcal{Z} \times \mathcal{T} \times \mathcal{T} \times \mathcal{T}$) (el caso de un único nodo queda cubierto por los tres subárboles vacíos). La ecuación simbólica es:

$$\mathcal{T} = \mathcal{E} + \mathcal{Z} \times \mathcal{T} \times \mathcal{T} \times \mathcal{T}$$

Esto lleva directamente a la ecuación:

$$T(z) = 1 + zT^3(z)$$

Lo malo es que resulta una cúbica...

Nuestra versión de inversión de Lagrange está calculada para resolver esta clase de ecuaciones. Haciendo el cambio de variable $u(z) = T(z) - 1$ queda:

$$u(z) = z(u(z) + 1)^3$$

de donde tenemos directamente los coeficientes de $u(z)$ (que coinciden con los de $T(z)$ salvo para $n = 0$):

$$\begin{aligned} [z^n]u(z) &= \frac{1}{n}[u^{n-1}](u + 1)^{3n} \\ &= \frac{1}{n}\binom{3n}{n-1} \\ &= \frac{1}{2n+1}\binom{3n}{n} \end{aligned}$$

Por casualidad la última expresión da 1 para $n = 0$, el valor correcto de t_0; queda entonces:

$$t_n = \frac{1}{2n+1}\binom{3n}{n}$$

Si fuéramos a árboles m-arios, un desarrollo similar lleva a:

$$t_n^{(m)} = \frac{1}{(m-1)n+1}\binom{mn}{n}$$

12. Definimos una clase $\mathcal{A}$ para los árboles de interés. Por la descripción, tenemos la expresión simbólica:

$$\mathcal{A} = \mathcal{Z} + \mathcal{Z} \times \mathcal{A} + \mathcal{Z} \times \mathcal{A} \times \mathcal{A}$$

El método simbólico da:

$$A(z) = z(1 + A(z) + A^2(z))$$

Es aplicable la fórmula de inversión de Lagrange:

$$\begin{aligned}
[z^n]A(z) &= \frac{1}{n}[u^{n-1}](1 + u + u^2)^n \\
&= \frac{1}{n}[u^{n-1}] \sum_{i,j} \binom{n}{i \; j \; n-i-j} u^{i+2j} \\
&= \frac{1}{n} \sum_j \binom{n}{n-2j-1 \; j \; j-1}
\end{aligned}$$

Alternativamente, resolvemos la cuadrática:

$$A(z) = \frac{1 - z \pm \sqrt{1 - 2z - 3z^2}}{2z}$$

De la definición de la clase (o de la ecuación para la función generatriz) sabemos que $A(0) = 0$, por lo que la rama correcta es:

$$A(z) = \frac{1 - z - \sqrt{1 - 2z - 3z^2}}{2z}$$

De cualquier forma, la serie comienza:

$$A(z) = z + z^2 + 2z^3 + 4z^4 + 9z^5 + 21z^6 + 51z^7 + 127z^8 + 323z^9 + 835z^{10} + \cdots$$

Véase el listado 2.

Listing 2: Código maxima para árboles 1-2

```
/*
 * 20122c1p4: Algebra for problem 4 solution
 */

sol : solve(A = z * (1 + A + A^2), A);

taylor(rhs(sol[1]), z, 0, 10);
```

13. Representamos:

$$\mathbb{N} = \mathcal{Z} \times \textsc{Seq}(\mathcal{Z})$$

Una combinación no es más que una secuencia de naturales:

$$\mathcal{C} = \textsc{Seq}(\mathbb{N})$$

De acá es inmediato:

$$\begin{aligned}
N(z) &= \frac{z}{1 - z} \\
C(z) &= \frac{1}{1 - N(z)} \\
&= \frac{1 - z}{1 - 2z} \\
&= \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{1 - 2z}
\end{aligned}$$

Directamente:

$$\begin{aligned}
c(n) &= \frac{1}{2}[n = 0] + \frac{1}{2} \cdot 2^n \\
&= \frac{1}{2}[n = 0] + 2^{n-1}
\end{aligned}$$

Esto es consistente con el valor $c(4) = 8 = 2^{4-1}$ dado en la pregunta.

14. Sea $\mathcal{B}$ la clase de árboles binarios considerados por nodos externos. La descripción del enunciado se traduce en:

$$\mathcal{B} = \mathcal{Z} + \mathcal{B} \times \mathcal{B}$$

Para objetos no rotulados esto da:

$$B(z) = z + B^2(z)$$

de donde:

$$B(z) = \frac{1 \pm \sqrt{1 - 4z}}{2}$$

Sabemos que $b_0 = 0$, por lo que el signo correcto es el negativo:

$$B(z) = \frac{1 - \sqrt{1 - 4z}}{2}$$

Notamos que esto es similar a la función generatriz de los números de Catalan:

$$B(z) = zC(z)$$

con lo que:

$$b_n = \begin{cases} 0 & \text{si } n = 0 \\ C_{n-1} & \text{caso contrario} \end{cases}$$

17. Principio de Inclusión y Exclusión

1. Esto se ataca en forma más simple mediante el principio de inclusión y exclusión, ya que hay intersecciones.

   - El universo son las permutaciones de las 26 letras. Las propiedades son incluir cada una de las secuencias indicadas. Nos interesan las permutaciones sin propiedades.
   - Tenemos para los conjuntos no vacíos:

   $$\begin{aligned}
   N(\supseteq \{ola\}) &= (26-3+1)! &&= 620\,448\,401\,733\,239\,439\,360\,000 \\
   N(\supseteq \{ayer\}) &= (26-4+1)! &&= 25\,852\,016\,738\,884\,976\,640\,000 \\
   N(\supseteq \{barco\}) &= (26-5+1)! &&= 1\,124\,000\,727\,777\,607\,680\,000 \\
   N(\supseteq \{grande\}) &= (26-6+1)! &&= 51\,090\,942\,171\,709\,440\,000 \\
   N(\supseteq \{ola,\ ayer\}) &= (26-3+1-4+1)! &&= 51\,090\,942\,171\,709\,440\,000 \\
   N(\supseteq \{ola,\ barco\}) &= (26-3+1-5+1)! &&= 2\,432\,902\,008\,176\,640\,000 \\
   N(\supseteq \{ola,\ ayer,\ barco\}) &= (26-3+1-4+1-5+1)! &&= 355\,687\,428\,096\,000
   \end{aligned}$$

     Con estas:

   $$\begin{aligned}
   N_0 &= 26! \\
   N_1 &= 24! + 23! + 22! + 21! \\
   N_2 &= 21! + 20! \\
   N_3 &= 17!
   \end{aligned}$$

   - La función generatriz es $N(z) = N_0 + N_1 z + N_2 z^2 + N_3 z^3$, nos interesa $e_0 = E(0) = N(-1) = N_0 - N_1 + N_2 - N_3$. Esto resulta ser:

   $$\begin{aligned}
   e_0 &= 26! - (24! + 23! + 22! + 21!) + (21! + 20!) - 17! \\
   &= 26! - 24! - 23! - 22! - 2 \cdot 21! - 20! + 17! \\
   &= 402\,643\,932\,092\,975\,069\,392\,896\,000
   \end{aligned}$$

2. Primero definimos:

   $$M(z) = \sum_{r \geq 0} M_r z^r$$

   Lo que se pide es una suma parcial de los e_k, por lo que podemos directamente aplicar las propiedades a su función generatriz:

   $$M(z) = \frac{E(z)}{1-z}$$

3. Aplicamos nuestra receta para el principio de inclusión-exclusión.

   - El universo es el conjunto de todos las secuencias de 10 dígitos. Una secuencia tiene la propiedad i si la secuencia no contiene el dígito i para $i \in \{1, 3, 5, 7, 9\}$. Nos interesan las secuencias sin ninguna de las propiedades.
   - Si la secuencia no contiene los dígitos en $\mathcal{S}$, es una secuencia de 10 dígitos tomados entre $10 - |\mathcal{S}|$ posibilidades, o sea:

   $$N(\supseteq \mathcal{S}) = (10 - |\mathcal{S}|)^{10}$$

   - Un conjunto de r propiedades se elige libremente entre las 5:

   $$N_r = \binom{5}{r}(10-r)^{10}$$

- La función generatriz es:

$$N(z) = \sum_{0 \leq r \leq 5} \binom{5}{r} (10 - r)^{10} z^r$$

- Nos interesa:

$$e_0 = E(0) = N(-1) = 771\,309\,000$$

4. Acá $\Omega = \{1, 2, \dots, n\}$, y la propiedad i es que $p_i \mid \omega$. Para obtener $\phi(n)$ nos interesa contar los números que no son divisibles por ninguno de los p_i, que son exactamente aquellos que no tienen factores en común con n. Los múltiplos de p_i en Ω son los números $\{1 \cdot p_i, 2 \cdot p_i, \dots, (n/p_i) \cdot p_i\}$, o sea, n/p_i en total:

$$N(\supseteq \{i\}) = \frac{n}{p_i} \tag{20}$$

O, en general:

$$N(\supseteq \{i, j, k, \dots\}) = \frac{n}{p_i p_j p_k \dots} \tag{21}$$

Al dar el conjunto $\{i, j, k, \dots\}$ va implícito el orden de sus elementos:

$$\begin{aligned} N_1 &= \sum_i \frac{n}{p_i} \\ N_2 &= \sum_{i<j} \frac{n}{p_i p_j} \\ N_3 &= \sum_{i<j<k} \frac{n}{p_i p_j p_k} \\ &\vdots \\ N_r &= \sum_{i_1 < i_2 < \dots < i_r} \frac{n}{p_{i_1} p_{i_2} \dots p_{i_r}} \end{aligned} \tag{22}$$

Aplicando la fórmula general con los valores (22), obtenemos una fórmula para $\phi(n) = e_0 = E(0) = N(-1)$:

$$\begin{aligned} \phi(n) &= N - N_1 + N_2 - \dots \\ &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \dots + (-1)^r \sum_{i_1 < i_2 < \dots < i_r} \frac{n}{p_{i_1} p_{i_2} \dots p_{i_r}} \\ &= n \left(1 - \sum_i \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - \sum_{i<j<k} \frac{1}{p_i p_j p_k} + \dots + (-1)^r \sum_{i_1 < i_2 < \dots < i_r} \frac{1}{p_{i_1} p_{i_2} \dots p_{i_r}} \right) \end{aligned} \tag{23}$$

Si escribimos:

$$n_1 = p_1 \cdot p_2 \cdot \ldots \cdot p_r \tag{24}$$

podemos escribir (23) como:

$$\begin{aligned} \phi(n) = \frac{n}{n_1} \big(& p_1 p_2 \dots p_r \\ & - (p_2 p_3 \dots p_r + p_1 p_3 \dots p_r + \dots + p_1 p_2 \dots p_{r-1}) \\ & + (p_3 p_4 \dots p_r + \dots + p_1 \dots p_{r-2}) \\ & - \dots \\ & + (-1)^{r-1} (p_1 + \dots + p_r) \\ & + (-1)^r \big) \end{aligned} \tag{25}$$

$$= \frac{n}{n_1} (p_1 - 1)(p_2 - 1) \dots (p_r - 1) \tag{26}$$

$$= n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_r} \right) \tag{27}$$

Que la factorización (25) a (26) es válida se ve agrupando los términos que contienen p_i y los que no, y observar que ambas colecciones sólo difieren en signos y el factor p_i, con lo que el paréntesis de (25) es divisible por $p_i - 1$ para cada i; y el término $p_1 \ldots p_r$ tiene coeficiente uno.

5. Primeramente, el resultado claramente es cero si $m < n$. Aplicando la receta:

   a) Ω es el conjunto de las n^m funciones $f : A \to B$ (podemos elegir $f(1)$, $f(2)$, ..., $f(m)$ independientemente de n maneras cada uno), la propiedad i corresponde a que el valor i no aparece entre los valores de la función. Nos interesa saber cuántas funciones no tienen ninguna de las propiedades, vale decir, e_0.

   b) Si $S \subseteq B$, las funciones que hay que contabilizar sólo pueden tomar $n - |S|$ valores, o sea, de estas hay:

   $$N(\supseteq S) = (n - |S|)^m$$

   c) Cuando $|S| = r$, hay $\binom{n}{r}$ formas de elegir las r propiedades de entre las n, o sea:

   $$N_r = \binom{n}{r}(n-r)^m$$

   y la función generatriz de los N_r es:

   $$N(x) = \sum_{0 \le r \le n} \binom{n}{r}(n-r)^m x^r$$

   d) Nos interesa:

   $$\begin{aligned} e_0 &= E(0) = N(-1) \\ &= \sum_{0 \le r \le n} (-1)^r \binom{n}{r}(n-r)^m \end{aligned}$$

6. Siguiendo la receta, el universo son matrices que tienen columnas no sólo ceros (por la pista). Decimos que la matriz tiene la propiedad i si la fila i es sólo ceros. Nos interesa el número de matrices sin propiedades.

   Podemos considerar la matriz como m columnas de n elementos 0-1, con lo que cada columna tiene $2^n - 1$ posibilidades (estamos excluyendo columnas sólo ceros) con lo que $|\Omega| = (2^n - 1)^m$. Por simetría, los $N(\supseteq \mathcal{S})$ dependen sólo de $|\mathcal{S}|$. Si hay r filas con ceros, hay $(2^{n-r} - 1)^m$ matrices (en cada columna hay $n - r$ posiciones a definir, y tenemos la restricción que ninguna columna es sólo ceros). Elegimos esas r filas entre n:

   $$N_r = \binom{n}{r}(2^{n-r} - 1)^m$$

   En consecuencia:

   $$\begin{aligned} N(z) &= \sum_{r \ge 0} N_r z^r \\ &= \sum_{r \ge 0} \binom{n}{r}(2^{n-r} - 1)^m z^r \end{aligned}$$

   Por la fórmula mágica:

   $$\begin{aligned} e_0 &= E(0) \\ &= N(-1) \\ &= \sum_{r \ge 0} (-1)^r \binom{n}{r}(2^{n-r} - 1)^m \end{aligned}$$

   Esto no parece tener una forma simple.

7. El universo son todas las manos (conjuntos de cinco cartas). Las propiedades son que la pinta respectiva no aparezca, interesan las manos sin propiedades. (Elegimos esas propiedades porque es fácil calcular cuántas manos no tienen cierta pinta, calcular el número de manos que la incluyen es mucho más difícil.)

   Si en una mano faltan r pintas dadas, significa que son 5 cartas tomadas entre las restantes $52 - 13r$; podemos elegir r pintas libremente entre 4:

$$N_r = \binom{4}{r} \cdot \binom{52 - 13r}{5}$$

   Vale decir:

$$\begin{aligned} N(z) &= \sum_{r \geq 0} N_r z^r \\ &= \sum_{r \geq 0} \binom{4}{r} \cdot \binom{52 - 13r}{5} z^r \end{aligned}$$

   De la fórmula mágica:

$$\begin{aligned} e_0 &= E(0) \\ &= N(-1) \\ &= \sum_{r \geq 0} (-1)^r \binom{4}{r} \cdot \binom{52 - 13r}{5} \end{aligned}$$

8. Consideremos un número en base b de b dígitos de largo, y digamos que tiene la propiedad i si su i-ésimo dígito es i. Nos interesan aquellos que tienen al menos una de las propiedades, o sea el total menos aquellos que no tienen ninguna.

   En total, hay b^b números, de los cuales b^{b-1} tienen la propiedad i (el i-ésimo dígito está fijo, los demás pueden tomar cualquiera de b valores). En general, dado un conjunto cualquiera de propiedades S:

$$N(\supseteq S) = b^{b-|S|}$$

   Así tenemos:

$$\begin{aligned} N_r &= \sum_{|S|=r} N(\supseteq S) \\ &= \sum_{|S|=r} b^{b-r} \\ &= \binom{b}{r} b^{b-r} \end{aligned}$$

   Con esto:

$$\begin{aligned} N(z) &= \sum_{r \geq 0} N_r z^r \\ &= \sum_{r \geq 0} \binom{b}{r} b^{b-r} z^r \\ &= b^b \sum_{r \geq 0} \binom{b}{r} \left(\frac{z}{b}\right)^r \\ &= b^b \left(1 + \frac{z}{b}\right)^b \\ &= (b + z)^b \end{aligned}$$

En nuestro caso nos interesa:

$$\begin{aligned} b^b - e_0 &= b^b - E(0) \\ &= b^b - N(-1) \\ &= b^b - (b-1)^b \end{aligned}$$

En realidad, que $e_0 = (b-1)^b$ es obvio, ya que estamos diciendo que para cada uno de los b dígitos hay $b-1$ opciones.

Y si quisiéramos cuántos números famosos hay para cada b, eso también es fácil:

$$\sum_{0 \le l \le b} (b^l - (b-1)^l) = \frac{b^{b+1} - 1}{b-1} - \frac{(b-1)^{b+1} - 1}{b-2}$$

9. De las solicitadas podemos formar 1 de largo 0, 2 de largo 1, $2 \times 2 + 3 \times 3 = 13$ de largo 2, …Estos valores sirven para verificar luego.

   Aplicamos las ideas del principio de inclusión-exclusión. Tenemos:

   - El universo Ω es el conjunto de palabras de largo n formadas por vocales. La propiedad i es que una vocal fuerte aparezca en la posición i de la palabra. Nos interesa saber cuántas palabras tienen un número par de propiedades, vale decir:

     $$e_0 + e_2 + \ldots = \sum_{t \ge 0} e_{2t}$$

     Además:

     $$\begin{aligned} e_0 + e_2 x^2 + e_4 x^4 + \ldots &= \sum_{t \ge 0} e_{2t} x^{2t} \\ &= \frac{E(x) + E(-x)}{2} \end{aligned}$$

     con lo que:

     $$\sum_{t \ge 0} e_{2t} = \frac{E(1) + E(-1)}{2}$$

   - Podemos calcular los e_t directamente. Si la palabra tiene t propiedades, tenemos $\binom{n}{t}$ formas de distribuir las vocales fuertes en las n posiciones, y cada una de ellas son 3 posibilidades; mientras hay $n-t$ vocales débiles, cada una de ellas elegida de entre 2. O sea:

     $$e_t = \binom{n}{t} \cdot 3^t \cdot 2^{n-t}$$

     En consecuencia:

     $$\begin{aligned} E(x) &= \sum_{t \ge 0} \binom{n}{t} \cdot 2^{n-t} \cdot 3^t \cdot x^t \\ &= (2 + 3x)^n \end{aligned}$$

   - El resultado buscado es:

     $$\begin{aligned} \frac{E(1) + E(-1)}{2} &= \frac{(2+3)^n + (2-3)^n}{2} \\ &= \frac{5^n + (-1)^n}{2} \end{aligned}$$

     Esto coincide con los valores obtenidos antes.

10. Para simplificar la notación, sin pérdida de generalidad consideramos funciones $f\colon [m] \to [n]$, donde $m \geq n$. Aplicamos nuestra receta:

   a) El universo Ω es el conjunto de n^m funciones (para cada uno de los m valores de x hay n valores de $g(x)$ que se pueden elegir independientemente). Siguiendo la pista, la función g tiene la propiedad i si i no tiene preimagen. Nos interesa contar el número de funciones para las que todo elemento de Y tiene preimagen, vale decir sin ninguna de las propiedades.

   b) Los $N(\supseteq S)$ son los números de funciones en las cuales ninguno de los elementos de S tiene preimagen, vale decir son funciones de un conjunto de m elementos a uno de $n - |S|$. Tenemos entonces:

   $$N(\supseteq S) = \big(n - |S|\big)^m$$

   c) Para calcular N_r, consideramos que los r elementos de S se eligen de entre los n elementos de Y, y como $N(\supseteq S)$ depende sólo del tamaño de S resulta:

   $$N_r = \binom{n}{r}(n - r)^m$$

   La función generatriz es

   $$\begin{aligned} N(z) &= \sum_{r \geq 0} N_r z^r \\ &= \sum_{r \geq 0} \binom{n}{r}(n - r)^m z^r \end{aligned}$$

   d) Nos interesa e_0:

   $$\begin{aligned} e_0 &= N(-1) \\ &= \sum_{r \geq 0} (-1)^r \binom{n}{r}(n - r)^m \end{aligned}$$

11. Aplicamos la receta.

   - El universo son todas las palabras de largo n. Hay 6^n de estas. Las propiedades son no incluir cada uno de los símbolos. Nos interesan entonces $e_0 + e_1 + e_2 = N_0 - N_3$ y e_3.
   - Sea $S \subset P$. $N(\supset S)$ son las palabras sin excluir esos símbolos, vale decir, pueden incluir cualquiera de los demás $6 - |S|$, y así:

     $$N(\supset S) = (6 - |S|)^n$$

   - Los elementos de S pueden elegirse de entre 6 de $\binom{6}{|S|}$ maneras:

     $$\begin{aligned} N_r &= \sum_{|S| = r} N(\supset S) \\ &= \sum_{|S| = r} (6 - r)^n \\ &= \binom{n}{r}(6 - r)^n \end{aligned}$$

   Con esto:

   $$\begin{aligned} N(x) &= \sum_{r \geq 0} \binom{n}{r}(6 - r)^n x^r \\ E(x) &= \sum_{0 \leq r \leq n} \binom{n}{r}(6 - r)^n (x - 1)^r \end{aligned}$$

   $$\binom{n}{r}\left(\sum_{0 \leq k \leq n} \binom{n}{k} 6^k r^{n-k}\right) x^r$$

Revisar y completar

12. Por completar

13. El universo son los estudiantes presentes. Las propiedades son el estudiar cada una de las materias (abreviamos con la primera letra), lo que acá son casi todos datos dados. Lo que buscamos es cuántos no tienen ninguna de las propiedades, vale decir, e_0.

    Tenemos los $N(\supseteq S)$ dados para muchos de los posibles S. Calculamos los N_r:

$$\begin{aligned}
N_0 &= 18 \\
N_1 &= N(\supseteq \{C\}) + N(\supseteq \{M\}) + N(\supseteq \{P\}) \\
&= 10 + 7 + 10 \\
&= 27 \\
N_2 &= N(\supseteq \{C, M\}) + N(\supseteq \{C, P\}) + N(\supseteq \{M, P\}) \\
&= 3 + 5 + 4 \\
&= 12 \\
N_3 &= N(\supseteq \{C, M, P\}) \\
&= 1
\end{aligned}$$

    La función generatriz de los N_r es:

$$N(x) = 18 + 27x + 12x^2 + x^3$$

    Sabemos que:

$$e_0 = N(-1) = 2$$

14. Aplicamos el principio de inclusión-exclusión. El universo Ω son los asistentes de la noche. Las propiedades son los tragos ingeridos (llamémosles A, R y T). Se pide $N(= \{A, T\}) = N(\supseteq \{A, T\}) - N(\supseteq \{A, R, T\})$ (quienes tomaron al menos aguardiente y tequila, pero excluyendo aquellos que bebieron de los tres).

    Del enunciado tenemos:

$$\begin{aligned}
N(\supseteq \emptyset) &= 26 \\
N(\supseteq \{A\}) &= 16 \\
N(\supseteq \{R\}) &= 10 \\
N(\supseteq \{T\}) &= 14 \\
N(\supseteq \{A, R\}) &= 4 \\
N(\supseteq \{R, T\}) &= 5 \\
N(\supseteq \{A, R, T\}) &= 2
\end{aligned}$$

    No conocemos $N(\supseteq \{A, T\})$. Tenemos también:

$$\begin{aligned}
N_0 &= N(\supseteq \emptyset) = 26 \\
N_1 &= N(\supseteq \{A\}) + N(\supseteq \{R\}) + N(\supseteq \{T\}) = 16 + 10 + 14 = 40 \\
N_2 &= N(\supseteq \{A, R\}) + N(\supseteq \{A, T\}) + N(\supseteq \{R, T\}) = 4 + N(\supseteq \{A, T\}) + 5 = 9 + N(\supseteq \{A, T\}) \\
N_3 &= N(\supseteq \{A, R, T\}) = 2
\end{aligned}$$

    Por tanto, la función generatriz $N(x)$ es:

$$N(x) = 26 + 40\,x + (9 + N(\supseteq \{A, T\}))\;x^2 + 2\,x^3$$

    Sabemos que todos los asistentes tomaron, o sea $e_0 = N(-1) = 0$, por lo que:

$$0 = 26 - 40 + (9 + N(\supseteq \{A, T\})) - 2$$

Obtenemos:

$$N(\supseteq \{A, T\}) = 7$$

Pero esto es todos los que tomaron aguardiente y tequila, y posiblemente también ron. Restando a quienes tomaron de los tres, obtenemos el número de los que bebieron exactamente aguardiente y tequila:

$$N(= \{A, T\}) = N(\supseteq \{A, T\}) - N(\supseteq \{A, R, T\}) = 7 - 2 = 5$$

15. Nuestro universo son las palabras de n letras, la propiedad i es que la posición i es una vocal. En estos términos nos interesa $e_0 + e_1 + e_2$.

    En total hay:

    $$N_0 = 26^n$$

    Si la posición i es vocal, podemos elegirla de 5 maneras, y las restantes $n - 1$ posiciones las elegimos de 26 maneras. O sea:

    $$N(\supseteq \{i\}) = 26^{n-1} \cdot 5$$

    Como hay n posiciones, y elegimos una:

    $$N_1 = \binom{n}{1} \cdot 26^{n-1} \cdot 5$$

    De forma similar:

    $$N_r = \binom{n}{r} \cdot 26^{n-r} \cdot 5^r$$

    La función generatriz de los N_r es simplemente:

    $$\begin{aligned} N(x) &= \sum_{r \geq 0} \binom{n}{r} \cdot 26^{n-r} \cdot 5^r \cdot x^r \\ &= (26 + 5x)^n \end{aligned}$$

    En consecuencia, para los e_t tenemos:

    $$\begin{aligned} E(x) &= N(x - 1) \\ &= (21 + 5x)^n \\ e_t &= \left[x^t\right] E(x) \\ &= \binom{n}{t} \cdot 21^{n-t} \cdot 5^t \end{aligned}$$

    Nos interesa:

    $$\begin{aligned} e_0 + e_1 + e_2 &= \binom{n}{0} \cdot 21^n + \binom{n}{1} \cdot 21^{n-1} \cdot 5 + \binom{n}{2} \cdot 21^{n-2} \cdot 25 \\ &= \frac{1}{2} \cdot \left(882 + 210n + 185n^2\right) \cdot 21^{n-2} \end{aligned}$$

16. Siguiendo la receta:

    - El universo Ω es el conjunto de todos las palabras de largo n formadas con las letras a, b, c, d, e, f.
    - Las propiedades $P = a, b, c, d, e, f$ corresponden a no incluir la letra indicada, vale decir, si una palabra tiene la propiedad b está formada únicamente por las 5 letras restantes.
    - En estos términos, nos piden:

a) Si tienen al menos 3 letras distintas significa que tienen a lo más 3 de las propiedades, o sea interesa $e_0 + e_1 + e_2 + e_3$.

b) Si tienen exactamente 4 letras diferentes, es que tienen 2 de las propiedades, interesa e_2.

c) El caso del número de vocales no puede tratarse en este esquema, lo veremos aparte.

- Los $N(\supseteq S)$ son simples de calcular: Para un conjunto S de propiedades, estamos hablando de palabras de largo n formadas por $6 - |S|$ letras, o sea:

$$N(\supseteq S) = (6 - |S|)^n$$

- Tenemos de lo anterior:

$$\begin{aligned} N_r &= \sum_{|S|=r} (6 - |S|)^n \\ &= \binom{6}{r}(6 - r)^n \end{aligned}$$

- Obtenemos:

$$N(z) = \sum_r \binom{6}{r}(6 - r)^n z^r$$

- Tenemos de la fórmula mágica:

$$\begin{aligned} E(z) &= N(z - 1) \\ &= \sum_r \binom{6}{r}(6 - r)^n (z - 1)^r \\ e_t &= \left[z^t\right] \sum_r \binom{6}{r}(6 - r)^n (z - 1)^r \\ &= \left[z^t\right] \sum_r \binom{6}{r}(6 - r)^n \sum_k (-1)^{r-k}\binom{r}{k} z^k \\ &= \sum_r (-1)^{r-t}\binom{6}{r}\binom{r}{t}(6 - r)^n \end{aligned}$$

Con lo anterior estamos en condiciones de responder las primeras dos partes:

a) Resulta:

$$e_0 + e_1 + e_2 + e_3 = 6^n - 15 \cdot 2^n + 24$$

b) Tenemos:

$$e_2 = 15 \cdot 4^n - 20 \cdot 3^{n+1} + 45 \cdot 2^{n+1} - 60$$

Para la última parte debemos hacer un planteo diferente. Sea nuevamente Ω el conjunto de palabras de n letras. Sean ahora P las propiedades i, que corresponden a que en la posición i hay una vocal. Nos interesa el número de objetos con un número par de propiedades, vale decir:

$$e_0 + e_2 + e_4 + \ldots = \frac{E(1) + E(-1)}{2}$$

Resulta que los e_t son fáciles de evaluar directamente. Elegimos t posiciones de entre las n en las cuales ubicar las vocales (cada posición tiene 2 opciones) mientras las demás posiciones quedan con consonantes (cada una con 4 opciones):

$$e_t = \binom{n}{t} 2^t 4^{n-t}$$

Tenemos entonces directamente:

$$
\begin{aligned}
E(z) &= \sum_t e_t z^t \\
&= \sum_t \binom{n}{t} 4^{n-t} (2z)^t \\
&= (4+2z)^n
\end{aligned}
$$

Esto da lugar a la solución para el caso restante:

c) El número de palabras con un número par de vocales está dado por:

$$\frac{E(1)+E(-1)}{2} = \frac{6^n + 2^n}{2}$$

17. Podemos calcular el número de soluciones de la ecuación sin restricciones, y determinar cuántas de ellas violan cada subconjunto de las restricciones. Tenemos entonces como universo Ω el conjunto de soluciones sin restricciones, y una solución tiene la propiedad i si x_i sobrepasa su límite. Nos interesa el número de soluciones que no violan los límites, vale decir, no tienen ninguna de las propiedades.

    Si llamamos s_k al número de soluciones enteras de

    $$x_1 + x_2 + \ldots + x_n = k \qquad x_i \geq 0$$

    sabemos que

    $$s_k = \binom{n+k-1}{k-1}$$

    Si ahora imponemos por ejemplo el límite $x_1 \leq L$, contar cuántas de las anteriores violan este límite es considerar un nuevo problema, donde ahora la restricción es que $x_1 > L$, o lo que es lo mismo:

    $$x_1' + x_2 + \ldots + x_n = k - (L+1)$$

    Este es un problema del mismo tipo anterior. La misma idea puede aplicarse a cualquier subconjunto de las variables.

    En nuestro caso es imposible violar juntas las condiciones $\{2,3\}$, ya que $4+6+2 = 12 > 11$; ni las tres condiciones juntas, ya que $3+4+6+3 = 16 > 11$. Así nos queda:

    $$
    \begin{aligned}
    N(\supseteq \emptyset) &= \binom{11+3-1}{3-1} && = 78 \\
    N(\supseteq \{1\}) &= \binom{(11-3-1)+3-1}{3-1} && = 36 \\
    N(\supseteq \{2\}) &= \binom{(11-4-1)+3-1}{3-1} && = 28 \\
    N(\supseteq \{3\}) &= \binom{(11-6-1)+3-1}{3-1} && = 15 \\
    N(\supseteq \{1,2\}) &= \binom{(11-3-4-2)+3-1}{3-1} && = \ \ 6 \\
    N(\supseteq \{1,3\}) &= \binom{(11-3-6-2)+3-1}{3-1} && = \ \ 1 \\
    N(\supseteq \{2,3\}) & && = \ \ 0 \\
    N(\supseteq \{1,2,3\}) & && = \ \ 0
    \end{aligned}
    $$

    Tenemos en consecuencia:

    $$
    \begin{aligned}
    N_0 & &= 78 \\
    N_1 &= 36 + 28 + 15 &= 79 \\
    N_2 &= \ \ 6 + \ \ 1 + \ \ 0 &= \ \ 7 \\
    N_3 & &= \ \ 0
    \end{aligned}
    $$

Resulta así:

$$N(x) = 78 + 79x + 7x^2$$

Nos interesa:

$$e_0 = E(0) = N(-1) = 6$$

18. Nuestro universo son los 2 054 alumnos del curso. Las propiedades $P = \{C, J, P\}$ corresponden a saber C, Java y Python, respectivamente. Nos interesan $e_2 + e_3$ y e_0. Tenemos algunos de los $N(\supseteq S)$ dados en el enunciado:

$$\begin{aligned}
N(\supseteq \emptyset) &= 2\,054 \\
N(\supseteq \{C\}) &= 345 \\
N(\supseteq \{J\}) &= 999 \\
N(\supseteq \{P\}) &= 1\,786 \\
N(\supseteq \{C, J\}) &= 231 \\
N(\supseteq \{C, P\}) &= 290 \\
N(\supseteq \{J, P\}) &= 876 \\
N(\supseteq \{C, J, P\}) &= 189
\end{aligned}$$

Así tenemos:

$$\begin{aligned}
N_0 &= N(\supseteq \emptyset) \\
&= 2\,054 \\
N_1 &= N(\supseteq \{C\}) + N(\supseteq \{J\}) + N(\supseteq \{P\}) \\
&= 3\,130 \\
N_2 &= N(\supseteq \{C, J\}) + N(\supseteq \{C, P\}) + N(\supseteq \{J, P\}) \\
&= 1{,}397 \\
N_3 &= N(\supseteq \{C, J, P\}) \\
&= 189
\end{aligned}$$

Así:

$$\begin{aligned}
N(x) &= 2\,054 + 3\,130\,x + 3\,397\,x^2 + 189\,x^3 \\
E(x) &= N(x-1) \\
&= 132 + 903\,x + 830\,x^2 + 189\,x^3
\end{aligned}$$

Con los valores de e_t que pueden leerse de $E(x)$ estamos en condiciones de responder las preguntas:

- Los que dicen manejar a lo menos dos lenguajes son $e_2 + e_3 = 830 + 189 = 1\,019$
- Quienes no sabe programar son $e_0 = 132$

19. Nuestro universo Ω es el conjunto de selecciones de 7 cartas. Diremos que una selección de cartas tiene la propiedad de la pinta si no incluye cartas de esa pinta. En estos términos nos interesa el número de selecciones sin propiedades.

    Necesitamos calcular los diferentes $N(\supseteq S)$. Pero esto es fácil: Basta calcular las selecciones entre las cartas de las otras pintas. Así tenemos:

$$N(\supseteq \emptyset) = \binom{52}{7} = 133\,784\,560$$

Todas las pintas son iguales, así que qué pinta (o par de pintas, o trío) elijamos da lo mismo:

$$\begin{aligned}
N(\supseteq \{\spadesuit\}) = \binom{39}{7} &= 15\,380\,937 \\
N(\supseteq \{\spadesuit, \heartsuit\}) = \binom{26}{7} &= 657\,800 \\
N(\supseteq \{\spadesuit, \heartsuit, \clubsuit\}) = \binom{13}{7} &= 1\,716 \\
N(\supseteq \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}) = \binom{0}{7} &= 0
\end{aligned}$$

Tenemos:

$$\begin{aligned}
N_0 &= 133\,784\,560 \\
N_1 &= \binom{4}{1} \cdot N(\supseteq \{\spadesuit\}) \\
&= 61\,523\,748 \\
N_2 &= \binom{4}{2} \cdot N(\supseteq \{\spadesuit, \heartsuit\}) \\
&= 3\,946\,800 \\
N_3 &= \binom{4}{3} \cdot N(\supseteq \{\spadesuit, \heartsuit, \clubsuit\}) \\
&= 6\,864 \\
N_4 &= \binom{4}{4} \cdot N(\supseteq \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}) \\
&= 0
\end{aligned}$$

La función generatriz $N(x)$ resulta ser:

$$N(x) = 6\,864x^3 + 3\,946\,800x^2 + 61\,523\,748x + 133\,784\,560$$

El valor que nos interesa es $e_0 = N(-1) = 76\,200\,748$.

20. Primeramente, si $m < n$, el valor es 0.

    Para $m \geq n$ planteamos nuestra receta. Sin pérdida de generalidad, tomamos $\mathcal{A} = [m]$ y $\mathcal{B} = [n]$.

    Universo: Ω es el conjunto de todas las funciones $f\colon \mathcal{A} \to \mathcal{B}$. Hay n^m funciones en total.

    Propiedades: La función f tiene la propiedad i si no hay x tal que $f(x) = i$. Nos interesa el número de funciones sin propiedades.

    $N(\supseteq S)$: Si $S \subseteq [n]$ es un conjunto de propiedades, el número de funciones que tienen esas propiedades (no incluyen los valores de S) son

    $$N(\supseteq S) = (n - |S|)^m$$

    N_r: Los $N(\supseteq S)$ sólo dependen de la cardinalidad de S, así que:

    $$N_r = \sum_{|S|=r} N(\supseteq S) = \binom{n}{r}(n-r)^m$$

    N(z): Tenemos:

    $$N(z) = \sum_{r \geq 0} N_r z^r = \sum_r \binom{n}{r}(n-r)^m z^r$$

El resultado: Interesa:

$$e_0 = E(0) = N(-1) = \sum_r \binom{n}{r} (-1)^r (n-r)^m$$

Claro que todo esto es complicarse demasiado, el resultado es simplemente $n!\left\{ {m \atop n} \right\}$, un número de Stirling de segunda especie (estamos particionando los elementos de $\mathcal{A}$ en $|\mathcal{B}|$ clases según el valor que toma la función, y podemos ordenar las particiones de $n!$ maneras).

21. Nuestro universo son los 65 empleados, las propiedades son las cosas que cada cual trae. Lo que nos interesa se puede expresar en términos de los e_t. Usemos las letras H para hot dogs, E para ensalada, P para pollo frito y F para postre (por ser lo que se engulle al final). Tenemos los siguientes datos:

$$\begin{aligned}
\Omega &= 65 \\
N(\supseteq \{E\}) &= 28 \\
N(\supseteq \{F\}) &= 32 \\
N(\supseteq \{H\}) &= 21 \\
N(\supseteq \{P\}) &= 35 \\
N(\supseteq \{E, F\}) &= 14 \\
N(\supseteq \{E, H\}) &= 10 \\
N(\supseteq \{E, P\}) &= 12 \\
N(\supseteq \{F, H\}) &= 9 \\
N(\supseteq \{F, P\}) &= 17 \\
N(\supseteq \{H, P\}) &= 13 \\
N(\supseteq \{E, F, H\}) &= 5 \\
N(\supseteq \{E, F, P\}) &= 7 \\
N(\supseteq \{E, H, P\}) &= 4 \\
N(\supseteq \{F, H, P\}) &= 6 \\
N(\supseteq \{E, F, H, P\}) &= 2
\end{aligned}$$

De la anterior lista:

$$\begin{aligned}
N_0 &= 65 \\
N_1 &= 28 + 32 + 21 + 35 \\
&= 116 \\
N_2 &= 14 + 10 + 12 + 9 + 17 + 13 \\
&= 75 \\
N_3 &= 5 + 7 + 4 + 6 \\
&= 22 \\
N_4 &= 2
\end{aligned}$$

Resulta así:

$$N(z) = 65 + 116z + 75z^2 + 22z^3 + 2z^4$$

a) Los que no traen nada son:

$$e_0 = N(-1) = 4$$

b) Para los que traen solo hot dogs debemos hacer un nuevo planteamiento, con el universo ahora los que traen hot dogs. Las propiedades a considerar son los item además de hot dog, interesa el número de quienes no traen nada más, o sea $e_0^{(H)}$.

Planteamos:

$$
\begin{aligned}
N_0^{(H)} &= \Omega^{(H)} \\
&= 21 \\
N_1^{(H)} &= N(\supseteq \{E, H\}) + N(\supseteq \{F, H\}) + N(\supseteq \{H, P\}) \\
&= 10 + 9 + 13 \\
&= 32 \\
N_2^{(H)} &= N(\supseteq \{E, F, H\}) + N(\supseteq \{E, H, P\}) + N(\supseteq \{F, H, P\}) \\
&= 5 + 4 + 6 \\
&= 15 \\
N_3^{(H)} &= N(\supseteq \{E, F, H, P\}) \\
&= \ \ 2
\end{aligned}
$$

Con esto:

$$N^{(H)}(z) = 21 + 32z + 15z^2 + 2z^3$$

y resulta:

$$e_0^{(H)} = N^{(H)}(-1) = 2$$

c) Los que traen un item solamente son:

$$e_1 = \frac{E'(0)}{1!} = N'(-1) = 24$$

22. Usamos la receta:

Universo: Las funciones de $[m]$ a $[n]$, hay n^m de ellas.

Propiedades: Decimos que f tiene la propiedad i si no hay $x \in [m]$ tal que $f(x) = i$.

Resultado: Buscamos las funciones sin propiedades, e_0.

$\boldsymbol{N(\supseteq \{S\})}$**:** Significa que excluimos los valores en S entre los valores de la función, quedan $n - |S|$ posibles valores, con lo que:

$$N(\supseteq \{S\}) = (n - |S|)^m$$

$\boldsymbol{N_r}$**:** Elegimos r valores a excluir entre n, cada conjunto de valores excluidos da lo mismo:

$$N_r = \binom{n}{r}(n - r)^m$$

Con esto:

$$N(z) = \sum_{r \geq 0} N_r z^r$$

Fórmula mágica al rescate: Sabemos que:

$$
\begin{aligned}
e_0 &= E(0) \\
&= N(-1) \\
&= \sum_{r \geq 0} N_r (-1)^r \\
&= \sum_{r \geq 0} (-1)^r \binom{n}{r} (n - r)^m
\end{aligned}
$$

18. Fórmula de inversión de Lagrange

1. Por completar

2. Sea a_n el número de árboles m-arios de n nodos, y definamos:

$$A(z) = \sum_{n \geq 0} a_n z^n$$

Como hay un único árbol m-ario de cero nodos, y un árbol m-ario con n nodos se construye con una raíz y m árboles m-arios cuyos tamaños suman $n - 1$, tenemos:

$$A(z) = 1 + zA^m(z)$$

Con la substitución $u = A(z) - 1$, esto se traduce en:

$$u(z) = z\,(u(z) + 1)^m$$

Podemos aplicar la fórmula de inversión de Lagrange con $\phi(u) = (u + 1)^m$ (cumple $\phi(0) = 1$) y $f(u) = u$. En consecuencia, para $n \geq 1$ tenemos:

$$\begin{aligned} a_n &= [z^n]u(z) \\ &= \frac{1}{n}\left[u^{n-1}\right]\phi^n(u) \\ &= \frac{1}{n}\left[u^{n-1}\right](u + 1)^{mn} \\ &= \frac{1}{n}\binom{mn}{n-1} \\ &= \frac{1}{mn+1}\binom{mn}{n} \end{aligned}$$

Esta última fórmula resulta que es válida incluso para $n = 0$. Y el caso $m = 2$ da nuevamente los números de Catalan, que sabemos es el número de árboles binarios.

19. Grafos

1. *a*) Las listas de adyacencia son las dadas por el cuadro 8.

V	**Ady**
A	a, e, g
B	a, e, g
C	a, e, g
a	A, B, C
e	A, B, C
g	A, B, C

Cuadro 8: Listas de adyacencia para casas y servicios

   b) La figura 4 muestra el grafo.

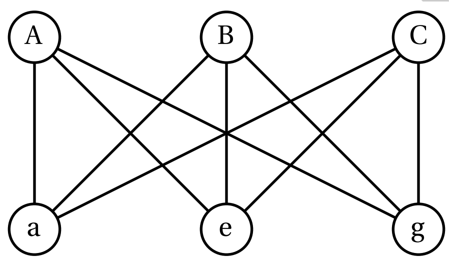


Figura 4: Grafo para casas y servicios

   No es posible dibujar este grafo sin que se crucen líneas.

2. El grafo K_n tiene n vértices. Como hay un arco entre cada par de vértices, esto corresponde a elegir todos los pares posibles, con lo que el número de arcos es:

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

   Es posible dibujarlo sin que se crucen arcos para $n = 1, 2, 3, 4$.

3. Es simple traducir los grafos dados al lenguaje de GraphViz. Resultan las figuras 5.

4. Este grafo en rigor es dirigido (la matriz de adyacencia no es simétrica).

   Si tomamos $V = \{A, B, C, D\}$; de la fila 1 tenemos A conectado con B, de la fila 2 está conectado con C. Por la última fila A está conectado con D, es conexo.

5. Por completar

6. Por turno:

   a) El grafo completo K_n tiene el máximo de arcos, que se puede contar como el máximo número de pares que se pueden crear con n elementos:

$$m \leq \binom{n}{2} = \frac{n(n-1)}{2}$$

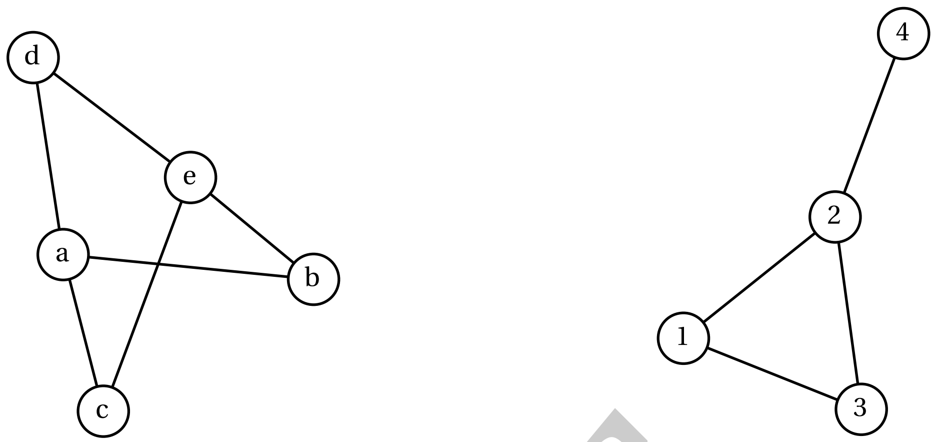


Figura 5: Dibujos solicitados

b) Entre los grafos bipartitos con r y s vértices en las partes el grafo $K_{r,s}$ tiene el máximo número de arcos, que es $r \cdot s$. Interesa maximizar esta cantidad sujeto a $r + s = n$. Podemos expresar:

$$\begin{aligned} s &= n - r \\ e(r) &= r(n - r) \end{aligned}$$

Cálculo elemental da:

$$\begin{aligned} e'(r^*) &= n - 2r^* = 0 \\ r^* &= \frac{n}{2} \\ e''(r^*) &= -2 \end{aligned}$$

con lo que es un máximo. Así:

$$e(r^*) = \frac{n^2}{2}$$

Como este es el máximo:

$$m \leq \frac{n^2}{2}$$

7. Por turno:

a) Por completar

b) Por completar

c) Veamos cada secuencia por turno:

- $\langle 6, 6, 6, 6, 5, 3, 3, 3, 3 \rangle$ es imposible, tiene 5 vértices de grado impar.
- Aplicamos el teorema de Havel:

$$\langle 9, 8, 6, 5, 3, 3, 3, 3, 1, 1 \rangle \to \langle 7, 5, 4, 2, 2, 2, 2, 0, 0 \rangle$$

Esta secuencia no es gráfica, el primer vértice tendría 7 vecinos, pero hay sólo 6 otros vértices no aislados.

8. Sea $G = (X \cup Y, E$ un grafo bipartito. Al construir el doble conectamos los vértices de la copia con los vértices del original, o sea estamos conectando los vértices en X' (la copia de los vértices en X) con los originales X, y similarmente los vértices en Y' con los en Y. Podemos colorear los vértices en X e Y' del mismo color, y similarmente los vértices de Y y X', no hay conexiones entre esos conjuntos.
9. Por completar
10. Sabemos que un grafo es bipartito si y sólo si no tiene ciclos de largo impar. Pero un árbol por definición no tiene ciclos.

    Como los árboles con conexos, sólo el árbol de un único vértice tiene $\chi(T) = 1$, todo árbol mayor tiene $\chi(T) = 2$.
11. Por completar
12. Por completar
13. Sea $n \geq 2$ el número de vértices del grafo. Si hay vértices aislados, los grados van de 0 a $n - 2$; si no hay vértices aislados van de 1 a $n - 1$. En cualquier caso, hay más vértices que grados posibles, por el principio del palomar hay al menos dos vértices con el mismo grado.
14. Por completar
15. Por turno.

    a) Como el grafo es regular de grado 4, sabemos que $\chi(G) \leq 5$. El grafo contiene ciclos de largo 3 (impar), por lo que su número cromático es al menos 3. El coloreo dado por el cuadro 9 demuestra que bastan 3 colores, $\chi(G) = 3$. La figura 6 ilustra el coloreo de el cuadro 9, usando los colores rojo, azul y amarillo.

v	$c(v)$
a	0
b	1
c	2
d	1
e	2
f	0

Cuadro 9: Coloreo de vértices

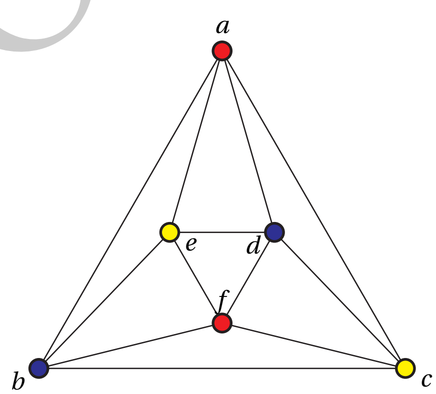


Figura 6: Coloreo del grafo

    b) Como el grado máximo es 4, $\chi'(G) \geq 4$. El cuadro 10 da un coloreo con 4 colores, $\chi'(G) = 4$. La figura 7 ilustra el coloreo del cuadro 10, usando los colores rojo, azul, amarillo y verde.

    c) Como todos los vértices tienen grado par, sabemos que hay un circuito de Euler.

uv	$c(uv)$
ab	0
ac	1
ad	2
ae	3
bc	2
be	1
bf	3
cd	3
cf	0

Cuadro 10: Coloreo de arcos

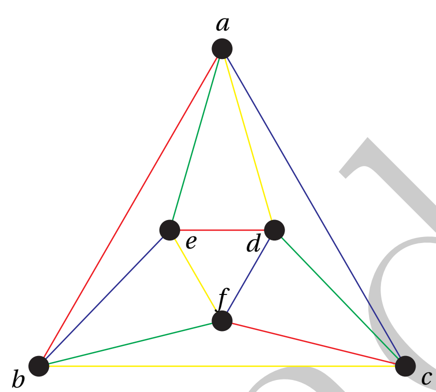


Figura 7: Coloreo de arcos del grafo

d) Construir un circuito de Hamilton es más difícil. Pero en este caso es sencillo ver que podemos recorrer el triángulo externo y luego el interno, vale decir por ejemplo $\langle a, b, c, d, f, e, a \rangle$. Este circuito se ilustra en la figura 8.

16. Por completar

17. Por completar

18. Por completar

19. Por completar

20. Cada parte por turno.

    a) Un grafo es regular si todos los vértices tienen el mismo grado. En este caso, cada vértice de un grupo está conectado únicamente a todos los del otro grupo, con lo que esto se da solamente cuando $m = n$.

    b) Hay un camino de Euler en un grafo conexo siempre que haya 2 vértices de grado impar, y un circuito de Euler si no hay vértices de grado impar. En nuestro caso:

    - Hay un camino de Euler si $m = 2$ y n es impar o m es impar y $n = 2$.
    - Hay un circuito de Euler si tanto m como n son pares.

    c) Un ciclo Hamiltoniano visita cada vértice exactamente una vez, y en $K_{m,n}$ una vez visitado uno de los vértices de un grupo hay que ir al otro grupo, ya que esas son los únicos arcos que hay. Si los números de vértices no son iguales, uno de los grupos se acaba antes y no podemos completar el ciclo. Por otro lado, si el número de vértices en los dos grupos es el mismo, podemos siempre visitar a continuación uno del otro grupo que no hayamos visitado ya, y volver al comienzo al final, ya que están todas las conexiones posibles entre vértices de los dos grupos. O sea, debe ser $m = n$.

21. Se demostró en clase que un grafo es bipartito si y sólo si no contiene ciclos de largo impar. El tipo de grafos descritos claramente cumple con esto.

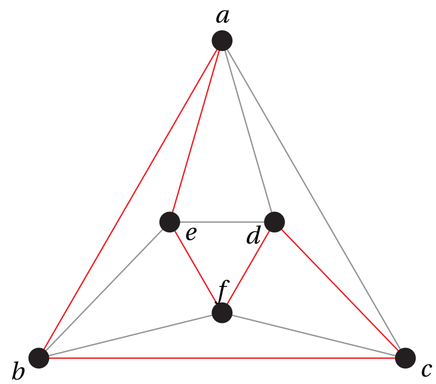


Figura 8: Circuito de Hamilton

La condición de Hall sólo puede cumplirse si se cumple por separado en cada componente del grafo bipartito, o sea en nuestro caso cada camino simple la cumple. Y la condición no se cumple en un camino sólo cuando el número de vértices en X sea mayor que en Y, o sea, el camino comienza y termina en X.

22. En el cálculo de E se requiere contar el valor de E para todos los predecesores del vértice, y la manera de lograr esto es con búsqueda a lo ancho (respetando la dirección de los arcos) partiendo con el vértice inicial del proyecto.

23. Sabemos que un grafo es un árbol si es conexo y no tiene ciclos. Una manera de verificar esto es usando un algoritmo de búsqueda: Si quedan vértices sin visitar, quiere decir que no es conexo y no es árbol; si durante la búsqueda un arco nos lleva a un vértice ya visitado, detectamos un ciclo y no es árbol.

    Otra forma es determinar si es conexo como antes, y contar el número de arcos, que debe ser $|E| = |V| - 1$ para que sea árbol.

24. Intuitivamente, obtiene un "maximal spanning tree", un spanning tree de costo máximo. Para ver que esto es cierto, consideremos el grafo $G = (V, E)$ con costo $w : E \to \mathbb{N}$. Si $m = \text{máx}_{e \in E}\{w(e)\}$, podemos definir por ejemplo:

    $$w'(e) = m + 1 - w(e)$$

    con lo cual el algoritmo equivocado estaría eligiendo el valor mínimo de w' en cada paso, obteniendo el minimal spanning tree para este caso. Construye un spanning tree, o sea, el resultado será un árbol con $|V| - 1$ arcos, y los costos del original y de la variante están relacionados simplemente vía:

    $$C' = (|V| - 1)m - C$$

    con lo que minimizar C' es maximizar C.

25. Interesa hallar el camino alternante más corto posible, y para este tipo de situaciones debe usarse búsqueda a lo ancho.

26. Supongamos el grafo bipartito $G = (X \cup Y, E)$, donde los arcos $e = \{x, y\}$ son todos tales que $x \in X$ y $y \in Y$. Definamos

    $$J(A) = \{v \colon \text{Hay } a \in A \text{ tal que } \{a, v\} \in E\}$$

    (El conjunto de vértices a los que están conectados los vértices en A). Entonces el teorema de Hall asegura que hay un matching completo siempre que para todo $A \subseteq X$ se cumple $|J(A)| \geq |A|$.

27. En clase demostramos que el valor del flujo en la red es el flujo neto a través de un corte cualquiera en la red, o sea en particular a través de los cortes (S, T) y (S', T'):

    $$\begin{aligned} \text{val}(f) &= f(S, T) \\ &= f(S', T') \end{aligned}$$

    En consecuencia, los flujos netos son iguales.

28. Un circuito hamiltoniano es un circuito que pasa por todos los vértices. Obviamente todo K_n contiene un ciclo C_n, que es el circuito hamiltoniano pedido. Incluso tiene $(n-1)!$ circuitos hamiltonianos (fijamos un vértice como inicio y fin, cada una de las $(n-1)!$ permutaciones de los demás da un orden posible de visitas).

29. En el grafo $G = (V, E)$ sea $|V| = n$, luego se analiza por casos:

hay nodos de grado 0: Dado que no hay nodos desconectados, los n nodos sólo pueden tener grados en el rango $[1, n-1]$. Por el principio del palomar, hay al menos dos con el mismo grado.

Hay nodos de grado 0: En este caso, los grados de los vértices pueden tomar valores en $[0, n-2]$, nuevamente por el principio del palomar hay dos con el mismo grado.

30. Por completar

31. Por completar

32. Por completar

33. Supongamos que el grafo bipartito $K_{m,n}$ tiene conjuntos de vértices X e Y. Si $m > n$, un matching completo es imposible. En caso que $m \leq n$, cualquier subconjunto de X tendrá a Y completo como vecindario, con lo que por el teorema de Hall siempre hay un matching completo. Si elegimos $x \in X$, podemos elegir cualquiera de los elementos de Y como pareja, y esto claramente podremos repetirlo para todos los X, dejando fuera cada vez los ya elegidos. O sea, el número de matchings posibles es simplemente:

$$m^{\underline{n}}$$

Otra manera de ver esto es que podemos elegir parejas entre los n elementos de Y para los m elementos de X de $\binom{n}{m}$ maneras, y estas parejas se pueden ordenar de $m!$ maneras, con lo que:

$$m! \cdot \binom{n}{m} = m! \cdot \frac{n!}{m!(n-m+1)!} = n^{\underline{m}}$$

34. Un *matching* en $K_{m,n} = (X \cup Y, X \times Y)$ corresponde a elegir un subconjunto de X (digamos de $0 \leq k \leq m$ elementos) y a cada uno de sus elementos asignarle un elemento diferente de Y. Desglosando:

- Elegir un subconjunto de k elementos de X puede hacerse de $\binom{m}{k}$ formas
- A los k elementos de X se les pueden asignar elementos distintos de Y de $n^{\underline{k}}$ maneras (n maneras para el primero, $n-1$ para el segundo, ..., $n-k+1$ para el último)
- Finalmente, debemos sumar para $0 \leq k \leq m$

O sea:

$$\sum_{0 \leq k \leq m} \binom{m}{k} n^{\underline{k}}$$

35. Si $s \in S_1$ y $s \in S_2$ entonces $s \in S_1 \cap S_2$; de la misma forma $t \notin S_1$ y $t \notin S_2$ hace que $t \notin S_1 \cap S_2$, que es $t \in \overline{S_1 \cap S_2}$. Como $S_1 \cap S_2$ y $\overline{S_1 \cap S_2}$ son complementos, el primero de ellos contiene a s y el segundo a t, esto es un corte.

36. Estos son grafos de 2^n vértices. Además:

   a) Su número cromático es 2: Podemos particionar los vértices en los que tienen un número par de unos y en los que tienen un número impar de unos. Los arcos van entre estos dos conjuntos.

   b) Cada vértice puede ser distinto de otros en exactamente n posiciones, es un grafo regular de grado n.

37. Un grafo admite un camino euleriano si tiene exactamente dos vértices de grado impar, y un circuito euleriano si todos sus vértices son de grado par. En el grafo K_n todos los vértices tienen grado $n-1$, así que hay un circuito euleriano en K_n cuando n es impar. En W_n hay $n-1$ vértices de grado 3 y 1 de grado n. No hay circuito ni camino euleriano posible, ya que acá $n \geq 4$.

38. Si consideramos “A conoce a B” como un arco entre los dos, las condiciones darían una suma impar para los grados de los vértices. Esta fiesta es imposible.

39. Cada punto por turno:

    a) Los grados son:

$$\begin{array}{lll} \delta(a) = 3 & \delta(b) = 2 & \delta(c) = 3 \\ \delta(d) = 2 & \delta(e) = 2 & \end{array}$$

    b) Una representación gráfica de G es la de la figura 9.

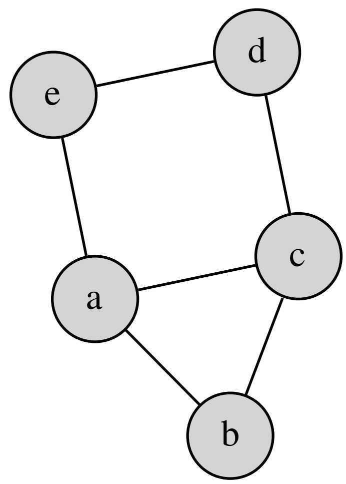


Figura 9: Representación gráfica del grafo de la pregunta 39

    c) La matriz de adyacencia (con los vértices en orden alfabético) es:

$$M_G = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

40. Si el grafo es regular, todos sus vértices tienen el mismo grado, llamémosle g. Si el grafo tiene n vértices, significa que tiene $ng/2$ arcos, o sea en nuestro caso:

$$ng = 30$$

Esto significa que g (y n) dividen a 30. Los divisores de 30 son 1, 2, 3, 5, 6, 10, 15 y 30. Por otro lado, el número máximo de arcos entre n vértices lo da el grafo completo K_n, en el cual hay $n(n-1)/2$ arcos. Por tanto tenemos la restricción:

$$\frac{n(n-1)}{2} \geq 15$$

Resulta $n \geq 6$, con lo que las posibilidades para n se reducen al conjunto $\{6, 10, 15, 30\}$. Analicemos cada caso:

Caso $n = 6$: Es el grafo K_6, que tiene 15 arcos. Cumple.

Caso $n = 10$: Acá el grado deberá ser 3 para cada vértice. Partiendo con C_{10} y uniendo vértices opuestos, obtenemos un grafo que demuestra que es posible, ver la figura 10.

Caso $n = 15$: El grado deberá ser 2, tenemos por ejemplo a C_{15}, o grafos formados por C_k que suman 15 vértices. También es posible.

Caso $n = 30$: El grado deberá ser 1, cosa que se logra con 15 pares de vértices unidos entre sí.

En resumen, son posibles grafos regulares con 15 arcos sólo para 6, 10, 15 y 30 vértices. Hay grafos conexos para 6, 10 y 15 vértices.

41. Veamos cada punto en turno.

 a) Si un grafo tiene n vértices tiene a lo más $n(n-1)/2$ arcos (el caso de K_n). Si G tiene dos componentes conexas de k y $n-k$ vértices, el máximo número de arcos que puede tener G es el caso en que sean K_k y K_{n-k}, o sea:

$$|E| \leq \binom{k}{2} + \binom{n-k}{2}$$

 b) Nos interesa determinar el máximo en el rango $1 \leq k \leq n-1$ de la expresión anterior. Pero:

$$\begin{aligned} f(k) &= \binom{k}{2} + \binom{n-k}{2} \\ &= \frac{1}{2}((k(k-1) + (n-k)(n-k-1)) \end{aligned}$$

 Esta función cuadrática tiene su mínimo en $k = n/2$; por simetría es máxima en los extremos, para $k = 1$ y $k = n-1$. En ambos casos resulta:

$$\begin{aligned} |E| &\leq \binom{1}{2} + \binom{n-1}{2} \\ &= \binom{n-1}{2} \end{aligned}$$

 c) Si el grafo tiene más de los arcos indicados, debe ser conexo.

42. Cada uno por turno.

 a) Por la descripción, se ve que son 2^n vértices, y cada vértice está conectado con n otros. Por el *handshaking lemma*:

$$\sum_{v \in V} \delta(v) = 2|E|$$

 vemos que:

$$2|E| = 2^n \cdot n$$

 O sea: $|V| = 2^n$, $|E| = 2^{n-1} \cdot n$.

 b) Del punto 42*a* se desprende que Q_n es regular de grado n.

 c) Podemos dividir los vértices de Q_n en dos grupos: Los que tienen un número par de 1 y los que tienen un número impar de 1. Sólo hay arcos entre los grupos, no entre vértices del mismo grupo. Es bipartito, o sea, $\chi(Q_n) = 2$ siempre que $n \geq 2$.

43. El grafo C_n es regular de grado 2. En el grafo complementario de C_n cada vértice tiene grado $n-1-2$, y esto es 2 sólo para $n = 5$, con lo que sólo para $n = 5$ puede ser un ciclo. El grafo resultante se muestra en la figura 11, y se ve que es isomorfo a C_5.

 Más formalmente, si consideramos C_5 con vértices $\{0, 1, 2, 3, 4\}$, y arcos $\{x, y\}$ cuando $y \equiv x \pm 1 \pmod{5}$, $\bar{C}_5$ tiene un arco $\{x, y\}$ exactamente si $y \equiv x \pm 2 \pmod{5}$. Como 2 y 5 son relativamente primos, el orden (aditivo) de 2 en $\mathbb{Z}_5$ es 5, o sea si partimos de 0 y sucesivamente sumamos 2 visitamos todos los elementos antes de volver a 0, y este grafo realmente es isomorfo a C_5.

44. Podemos representar cada una de las ciudades por un vértice a, b, c, d y e, obteniendo un conjunto de 5 vértices $V = \{a, b, c, d, e\}$. Queremos que ninguno de estos vértices quede aislado. Nuestro universo Ω es el conjunto de grafos sobre V. Como hay $\binom{5}{2} = 10$ posibles arcos entre las 5 ciudades:

$$|\Omega| = 2^{\binom{5}{2}} = 2^{10}$$

Definimos la propiedad i indicando que la ciudad i se encuentra aislada por las carreteras, para cada $1 \le i \le 5$. Nos interesa e_0, el número de grafos que no tienen ninguna de las propiedades (ninguna de las ciudades aislada). Necesitamos calcular los $N(\supseteq S)$. Pero esto no es más que el número de grafos en que las ciudades en S (al menos) estén aisladas, lo que significa que sólo pueden haber carreteras entre las demás:

$$N(\supseteq S) = 2^{\binom{5-|S|}{2}}$$

Podemos elegir las r ciudades en S de $\binom{5}{r}$ maneras, o sea:

$$N_r = \binom{5}{r} \cdot 2^{\binom{5-r}{2}}$$

Con esto nos queda la función generatriz:

$$N(x) = x^5 + 5x^4 + 20x^3 + 80x^2 + 320x + 1024$$

de la que obtenemos $e_0 = N(-1) = 768$.

45. En la discusión que sigue, k es fijo. Veamos cada punto por turno, considerando como universo todas las posibles asignaciones de a lo más k colores a los vértices.

   a) En los términos planteados en el problema, $p_G(k)$ es el número de coloreos en los cuales ninguno de los arcos tiene extremos del mismo color, vale decir, el número de coloreos sin ninguna de las propiedades. En la notación del principio de inclusión y exclusión, es $p_G(k) = e_0$.

   b) Sea $S \subseteq E$. En tal caso, $N(\supseteq S)$ cuenta el número de coloreos en los cuales los arcos en S conectan vértices del mismo color. Si consideramos el subgrafo $G_S = (V, S)$, esto significa que los vértices de cada uno de sus componentes conexos tienen todos el mismo color, si hay c_S componentes conexos en G_S, habrán $N(\supseteq S) = k^{c_S}$ coloreos que cumplan esto. Entonces también es un polinomio en k el valor:

   $$N_r = \sum_{|S|=r} N(\supseteq S)$$

   c) De nuestra derivación del principio de inclusión y exclusión sabemos que:

   $$\begin{aligned} N(z) &= \sum_{r \ge 0} N_r z^r \\ E(z) &= \sum_{s \ge 0} e_s z^s \\ E(z) &= N(z-1) \\ e_0 &= E(0) = N(-1) \end{aligned}$$

   Como por el punto anterior los N_r son polinomios en k, lo es:

   $$p_G(k) = e_0 = N(-1) = \sum_{r \ge 0} (-1)^r N_r$$

Al polinomio $p_G(x)$ se le conoce como el *polinomio cromático* de G. De la derivación vemos que su grado es el número de vértices del grafo, y en particular que es mónico. Por la definición de número cromático, vemos que para $0 \le k \le \chi(G)$ es $p_G(k) = 0$, lo que da una factorización parcial de $p_G(x)$.

46. En el caso en que $|V| = 1$ (los árboles son un único vértice), claramente basta un solo color, y se cumple lo pedido. Supongamos entonces $|V| > 1$, en cuyo caso ambos árboles son bipartitos, o sea $\chi(T_1) = \chi(T_2) = 2$. Supongamos que el color del vértice i en T_1 es a_i, mientras en T_2 es b_i. Un coloreo de $T_1 \cup T_2$ está dado por $c_i = (a_i, b_i)$ (los colores de vértices adyacentes en T_1 difieren al menos en la primera componente, mientras los colores de vértices adyacentes en T_2 difieren al menos en la segunda componente). A cada vértice le asigna uno de 4 colores, como se pide.

47. Llamémosle $A = (V, E)$ al árbol. Si $\Delta = 0$, el árbol consta de exactamente un vértice, y hay $1 > 0$ hojas. De tener grado $\Delta \geq 1$, el árbol tiene al menos dos vértices, por lo que tiene al menos dos hojas. Consideremos uno de los vértices de grado Δ, llamémosle v. La vecindad de v consta de Δ vértices, demostraremos que desde cada uno de ellos hay un camino diferente que llega al menos a una hoja sin pasar por v. Sea u adyacente a v. Si u no tiene vecinos fuera de v, es hoja y estamos listos. Si u tiene vecinos fuera de v, elegimos uno cualquiera de ellos y repetimos el proceso. Como V es finito, este proceso debe terminar en una hoja (no puede caer en un ciclo, por ser un árbol; ni puede terminar en v, ya que entre u y v hay un único camino). Las hojas así identificadas son todas diferentes, ya que de otra forma habrían dos caminos desde v a la misma hoja, y no sería árbol.

48. Cada punto por turno:

   a) Sea $V = \{1, 2, \ldots, n\}$ el conjunto de vértices, tomamos grafos $G = (V, E)$ y $\overline{G} = (V, \overline{E})$ con coloreos mínimos $a : V \to A$ para G y $b : V \to B$ para $\overline{G}$. Así $|A| = \chi(G)$ y $|B| = \chi(\overline{G})$. Entonces $c : V \to A \times B$, donde $c(v) = (a(v), b(v))$, es un coloreo de K_n, ya que cuando $u \neq v$ si $uv \in G$ entonces $a(u) \neq a(v)$, en caso contrario $uv \in \overline{G}$ y $b(u) \neq b(v)$. Pero todo coloreo de K_n usa exactamente n colores, y el dominio de la función tiene $\chi(G) \cdot \chi(\overline{G})$ elementos. Así debe ser $n \leq \chi(G) \cdot \chi(\overline{G})$.

   b) El caso extremo en que un color se usa el máximo de veces en un grafo de n vértices con $\chi(G) = k$ es cuando G es K_k y $n - k$ vértices de grado 0. Entonces $\overline{G}$ es K_{n-k} y k vértices de grado 0, y $\chi(\overline{G}) = n - k$, y en este caso $\chi(G) + \chi(\overline{G}) = n$. Igual no veo cómo sea relevante esto...

   c) Suponiendo $\chi(G) = k$ con n vértices, tenemos $n = qk + r$ con $q = \lfloor n/k \rfloor$ y $0 \leq r < k$. La distribución más uniforme posible se da con q copias de K_k y un K_r. El complemento de este grafo es k copias de K_q, con todos sus vértices conectados a r otros, para $\chi(\overline{G}) = q + 1$. En consecuencia, en este caso:

   $$\chi(G) + \chi(\overline{G}) = k + q + 1 \qquad = k + \lfloor \frac{n}{k} \rfloor + 1 \geq k + \frac{n}{k}$$

   Consideremos la función:

   $$f(x) = x + \frac{n}{x}$$

   Nos interesa su mínimo en el rango $1 \leq x \leq n - 1$:

   $$f'(x) = 1 - \frac{n}{x^2} = 0$$
   $$f''(x) = \frac{2n}{x^3} > 0$$

   El mínimo está en $x = \sqrt{n}$, y $\chi(G) + \chi(\overline{G}) \geq 2\sqrt{n}$. Nuevamente, ni idea que relevancia pueda tener esto ...

   d) Ni idea cómo hacer esto y crear grafos posibles

49. A pesar de tratarse de una familia de grafos, los tres casos se tratan separadamente.

   a) Vemos que $M_2 \cong K_4$, por lo que $\chi(M_2) = \chi(K_4) = 4$.

   b) Si $r > 2$ es par, está el ciclo $\langle 0, 1, \ldots, 2r - 1, 0 \rangle$ (de largo $2r$, par) y ciclos como $\langle a, a + 1, \ldots, a + r, a \rangle$ (de largo $r + 1$, impar). Por haber ciclos de largo impar, $\chi(M_r) \geq 3$ en este caso. La figura 12 muestra una manera de colorear M_4 con 3 colores. Este coloreo puede extenderse a todo $r > 2$ par (en la figura, el color 0 es rojo, el color 1 es azul y el color 2 es amarillo):

   $$c(i) = \begin{cases} i \bmod 2 & \text{si } 0 \leq i < r \\ 2 & \text{si } i = r \\ 1 - i \bmod 2 & \text{si } r < i < 2r - 1 \\ 2 & \text{si } r = 2r - 1 \end{cases}$$

Vemos que no hay vecinos en C_{2r} con el mismo color. Como r es par, los vértices opuestos en C_{2r} son i e $i + r$, ambos pares o ambos impares. La definición de c hace que sus colores sean distintos. O sea, en este caso $\chi(M_r) = 3$.

c) Si $r > 2$ es impar, tenemos nuevamente el ciclo $\langle 0, 1, \ldots, 2r - 1, 0\rangle$ (de largo $2r$, par) y ciclos como $\langle a, a + 1, \ldots, a + r, a\rangle$ (de largo $r + 1$, par). Al no haber ciclos de largo impar, parecen bastar 2 colores. El coloreo:

$$c(i) = i \text{ mód } 2$$

funciona: Los vecinos en C_{2r} son de colores distintos, y vértices opuestos son i e $i + r$, uno de los cuales es par y el otro impar. Acabamos de exhibir un coloreo con 2 colores, con lo que $\chi(M_r) = 2$ en este caso.

Alternativamente, el grafo sólo tiene ciclos de largo par; al no tener ciclos de largo impar es bipartito.

50. Consideremos un árbol cualquiera T.

    Si el árbol tiene un único vértice, $\chi(T) = 1$. Si $|T| \geq 2$, podemos elegir cualquiera de los vértices y pintarlo de rojo, sus vecinos de azul, y así sucesivamente ir pintando vecinos de colores opuestos. Como no hay ciclos en T, no pueden crearse conflictos.

    Alternativamente, sabemos que un grafo es bipartito si y sólo si no tiene ciclos de largo impar. Como los árboles no tienen ciclos por definición, son bipartitos.

    Para el índice cromático, si $|T| = 1$, realmente no lo hemos definido (aunque tiene sentido definir $\chi'(T) = 0$ en tal caso). En caso contrario, sabemos que $\chi'(T) \geq \text{máx}_{v \in T}\{\delta(v)\}$. Como no hay ciclos en T, no pueden interferirse y $\chi'(T) = \text{máx}_{v \in T}\{\delta(v)\}$.

51. El algoritmo conecta dos clases siempre que haya un arco entre ellas. Como resultado obtiene los conjuntos de vértices que forman componentes conexas. Sea c el número de componentes conexas de G, y $n = |V|$ su número de vértices. La estructura general del algoritmo es la del algoritmo de Kruskal para hallar árboles recubridores. Si el grafo fuera conexo, agregaría $n - 1$ arcos; como hay c componentes agrega sólo $n - c - 1$. En resumen:

    a) Se efectúan exactamente $n - c - 1$ uniones

    b) El número de $C(v)$ diferentes es c, el número de componentes de G

52. La primera suma es el número de arcos vistos desde los vértices a los que llegan, la segunda desde los vértices de los cuales salen.

53. Este grafo contiene al menos un ciclo de largo impar (a, b, c, d, e), así que su número cromático es al menos 3.

    El grado máximo es $\delta(k) = 5$, y no es regular (por ejemplo, $\delta(a) = 4$ y $\delta(f) = 3$), por lo que su número cromático es a lo más 5.

    Resulta que el número cromático es 4. Para demostrar que no es tres, considerando el ciclo (a, b, c, d, e) vemos que este requiere tres colores. Habrá un color que aparezca una vez (amarillo, digamos) y dos que aparezcan dos veces (sean azul y rojo). Sin pérdida de generalidad, podemos suponer que a es amarillo y b azul. Esto hace que sea rojo c, azul d y rojo e. Ahora f tiene vecinos azul y rojo, y debe ser amarillo. De la misma forma, g es azul (tiene vecinos amarillo y rojo); h y j pueden ser rojos o amarillos, e i puede ser azul o amarillo. Como k tiene vecinos de tres colores distintos (los forzados f, g y j), necesita un cuarto color (verde). El coloreo resultante con cuatro colores es válido (vea la figura 13), y el razonamiento previo demuestra que tres colores no son suficientes. En consecuencia, el número cromático es 4.

54. El grafo A tiene cuatro vértices de grado 3 (A, B, C y D) y uno de grado 2 (E); mientras B tiene uno de grado 4 (e), dos de grado 3 (a y d) y uno de grado 2 (c). No hay vértice de grado 4 en A que pueda corresponder a e de B, no hay isomorfismo posible.

55. El grafo tiene cuatro vértices de grado 3 (A, B, C y D) y uno de grado 2 (E). Al tener cuatro vértices de grado impar no tiene camino ni circuito de Euler.

56. En la discusión que sigue, k es fijo. Veamos cada punto por turno, considerando como universo todas las posibles asignaciones de a lo más k colores a los vértices.

a) En los términos planteados en el problema, $p_G(k)$ es el número de coloreos en los cuales ninguno de los arcos tiene extremos del mismo color, vale decir, el número de coloreos sin ninguna de las propiedades. En la notación del principio de inclusión y exclusión, es $p_G(k) = e_0$.

b) Sea $S \subseteq E$. En tal caso, $N(\supseteq S)$ cuenta el número de coloreos en los cuales los arcos en S conectan vértices del mismo color. Si consideramos el subgrafo $G_S = (V, S)$, esto significa que los vértices de cada uno de sus componentes conexos tienen todos el mismo color, si hay c_S componentes conexos en G_S, habrán $N(\supseteq S) = k^{c_S}$ coloreos que cumplan esto. Entonces también es un polinomio en k el valor:

$$N_r = \sum_{|S|=r} N(\supseteq S)$$

c) De nuestra derivación del principio de inclusión y exclusión sabemos que:

$$\begin{aligned} N(z) &= \sum_{r \geq 0} N_r z^r \\ E(z) &= \sum_{s \geq 0} e_s z^s \\ E(z) &= N(z-1) \\ e_0 &= E(0) = N(-1) \end{aligned}$$

Como por el punto anterior los N_r son polinomios en k, lo es:

$$p_G(k) = e_0 = N(-1) = \sum_{r \geq 0} (-1)^r N_r$$

Al polinomio $p_G(x)$ se le conoce como el *polinomio cromático* de G. De la derivación vemos que su grado es el número de vértices del grafo, y en particular que es mónico. Por la definición de número cromático, vemos que para $0 \leq k \leq \chi(G)$ es $p_G(k) = 0$, lo que da una factorización parcial de $p_G(x)$.

57. La primera suma es el número de arcos vistos desde los vértices a los que llegan, la segunda desde los vértices de los cuales salen.

58. Si en $G = (X \cup Y, E)$ numeramos los elementos de X de 1 a m, vemos que para 1 tenemos n opciones, para 2 quedan $n - 1$, y así sucesivamente. En realidad, es lo mismo que el número de permutaciones de n elementos de los que tomamos m:

$$P(n, m) = n^{\underline{m}}$$

59. Si el grafo es regular de grado 2, es una colección de ciclos. Si es bipartito son solo ciclos de largo par. Como todo ciclo de largo par tiene un *matchhing* completo (asocie vértices alternos), lo tiene el grafo planteado.

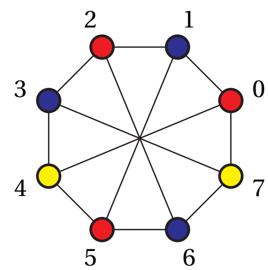


Figura 12: Coloreo de M_4

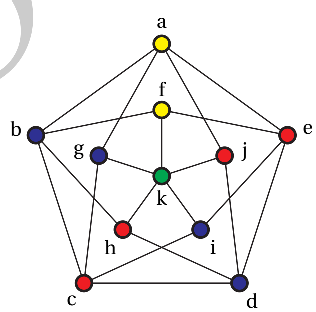


Figura 13: Un coloreo válido

20. Permutaciones

1. Por completar
2. Por completar
3. Por completar
4. Sabemos que:

   $$I(z) = \sum_{n \geq 0} I_n \frac{z^n}{n!} = \exp\left(z + \frac{z^2}{2}\right)$$

   Aplicando $zD \log$:

   $$\begin{aligned} \frac{zI'(z)}{I(z)} &= z + z^2 \\ I'(z) &= (1 + z)I(z) \\ \sum_{n \geq 0} I_{n+1} \frac{z^n}{n!} &= \sum_{n \geq 0} I_n \frac{z^n}{n!} + \sum_{n \geq 0} I_n \frac{z^{n+1}}{n!} \end{aligned}$$

   Pero:

   $$\sum_{n \geq 0} I_n \frac{z^{n+1}}{n!} = \sum_{n \geq 0} (n+1) I_n \frac{z^{n+1}}{(n+1)!} = \sum_{n \geq 1} n I_{n-1} \frac{z^n}{n!} = \sum_{n \geq 0} n I_{n-1} \frac{z^n}{n!}$$

   con lo que resulta:

   $$\sum_{n \geq 0} I_{n+1} \frac{z^n}{n!} = \sum_{n \geq 0} (I_n + n I_{n-1}) \frac{z^n}{n!}$$

   Comparando coeficientes:

   $$I_{n+1} = I_n + n I_{n-1}$$

   Para condiciones iniciales, por las propiedades de funciones generatrices exponenciales sabemos que:

   $$I_0 = I(0) = 1 \qquad I_1 = I'(0) = 1$$

   La recurrencia final es:

   $$I_{n+2} = I_{n+1} + (n+1) I_n \qquad I_0 = I_1 = 1$$

5. Por completar

21. Teoría de coloreo de Pólya

1. Cada punto por turno.

   a) Primeramente, las operaciones acá son rotaciones en 180 grados, y reflexiones en ejes vertical y horizontal. Estas corresponden a:

`id`	(1)(2)(3)(4)
Rotación	(1 4)(2 3)
Reflejo vertical	(1 2)(3 4)
Reflejo horizontal	(1 3)(2 4)

   b) Con lo anterior el índice de ciclos es:

   $$\zeta_B(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + 3x_2^2)$$

   c) Si son 3 colores, el número de configuraciones distintas se obtiene como $\zeta_B(3, 3, 3, 3) = 27$.

   d) En este caso necesitamos saber cuántas hay con un área de cada color. Si definimos variables z_1, z_2, z_3, z_4 para indicar cada color, requerimos:

   $$[z_1 z_2 z_3 z_4]\zeta_B(z_1 + z_2 + z_3 + z_4, z_1^2 + z_2^2 + z_3^2 + z_4^2, z_1^3 + z_2^3 + z_3^3 + z_4^3, z_1^4 + z_2^4 + z_3^4 + z_4^4) = 6$$

   (En total, hay 33 términos.)

   Aquí lo único que puede aportar términos lineales en los z_i son las potencias de x_1, por lo que sólo nos interesa:

   $$\begin{aligned}[z_1 z_2 z_3 z_4]\frac{1}{4}(z_1 + z_2 + z_3 + z_4)^4 &= \frac{1}{4}\binom{4}{1\ 1\ 1\ 1} \\ &= \frac{1}{4}\frac{4!}{1!1!1!1!} \\ &= 6\end{aligned}$$

2. Por el lema de Burnside, el número de órbitas de G es:

   $$\frac{1}{|G|}\sum_{\pi \in G} |F(\pi)|$$

   donde

   $$F(\pi) = \{x \in X : \pi(x) = x\}$$

   son los puntos fijos de π. Pero los puntos fijos de π son los ciclos de largo 1, y la información sobre cuántos de estos hay en cada elemento de G está codificada en $\zeta_G(x_1, \ldots, x_n)$ en forma de los exponentes de x_1:

   $$\zeta_G(x_1, \ldots, x_n) = \sum_{\pi \in G} \zeta_\pi(x_1, \ldots, x_n)$$

   y a su vez

   $$\zeta_\pi(x_1, \ldots, x_n) = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

   si π tiene tipo $[1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n}]$. El valor pedido puede entonces leerse de la expresión para ζ_G, o más elegantemente calcularse vía:

   $$\left.\frac{\partial \zeta_G}{\partial x_1}\right|_{x_1 = x_2 = \ldots = x_n = 1}$$

3. Cada punto por turno.

a) Básicamente, podemos permutar los elementos de una de las particiones (llamemos a y b a los vértices respectivos) e independientemente la otra (vértices c, d y e). En el fondo, es una combinación de S_2 actuando sobre $(a\ b)$ y S_3 operando sobre $(c\ d\ e)$. Tenemos:

$(a)(b)$	$[1^2]$
$(a\ b)$	$[2^1]$

$(c)(d)(e)$	$[1^3]$
$(c)(d\ e)$	$[1^1 2^1]$
$(c\ d)(e)$	$[1^1 2^1]$
$(c\ e)(d)$	$[1^1 2^1]$
$(c\ d\ e)$	$[3^1]$
$(c\ e\ d)$	$[3^1]$

El orden del grupo es $2! \times 3! = 12$

b) Las órbitas son $\{a, b\}$ y $\{c, d, e\}$.

c) Con lo anterior, como las 12 operaciones de G son simplemente combinaciones de las operaciones de S_2 y S_3, tenemos:

$$\begin{aligned}
\zeta_{S_2}(x_1, x_2) &= \frac{1}{2}(x_1^2 + x_2) \\
\zeta_{S_3}(x_1, x_2, x_3) &= \frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3) \\
\zeta_G(x_1, x_2, x_3, x_4, x_5) &= \zeta_{S_2}(x_1, x_2) \cdot \zeta_{S_3}(x_1, x_2, x_3) \\
&= \frac{1}{12}(x_1^5 + 4x_1^3x_2 + 2x_1^2x_3 + 2x_2x_3)
\end{aligned}$$

d) El número de coloreos está dado por:

$$\zeta_G(3, 3, 3, 3, 3) = 60$$

4. El número de coloreos pedido es simplemente:

$$[z_1z_2 \ldots z_n]\zeta_G(z_1 + z_2 + \ldots + z_n, z_1^2 + z_2^2 + \ldots + z_n^2, \ldots, z_1^n + z_2^n + \ldots + z_n^n)$$

Ahora bien, el término $z_1z_2 \ldots z_n$ puede provenir únicamente de expandir términos que sólo incluyen x_1, y los únicos de este tipo serán x_1^n, en donde aporta $\binom{n}{11\ldots1} = n!$; además la única operación con n ciclos de largo 1 es la identidad. En consecuencia:

$$\begin{aligned}
&[z_1z_2 \ldots z_n]\zeta_G(z_1+z_2 + \ldots + z_n, z_1^2 + z_2^2 + \ldots + z_n^2, \ldots, z_1^n + z_2^n + \ldots + z_n^n) \\
&\qquad = \frac{1}{|G|}[z_1z_2 \ldots z_n](z_1 + z_2 + \ldots + z_n)^n \\
&\qquad = \frac{n!}{|G|}
\end{aligned}$$

5. El número de coloreos pedido es simplemente:

$$[z_1z_2 \ldots z_n]\zeta_G(z_1 + z_2 + \ldots + z_n, z_1^2 + z_2^2 + \ldots + z_n^2, \ldots, z_1^n + z_2^n + \ldots + z_n^n)$$

Ahora bien, el término $z_1z_2 \ldots z_n$ puede provenir únicamente de expandir términos que sólo incluyen x_1, y los únicos de este tipo serán x_1^n, en donde aporta $\binom{n}{1\ 1\ \ldots\ 1} = n!$; además la única operación con n ciclos de largo 1 es la identidad. En consecuencia:

$$\begin{aligned}
&[z_1z_2 \ldots z_n]\zeta_G(z_1+z_2 + \ldots + z_n, z_1^2 + z_2^2 + \ldots + z_n^2, \ldots, z_1^n + z_2^n + \ldots + z_n^n) \\
&\qquad = \frac{1}{|G|}[z_1z_2 \ldots z_n](z_1 + z_2 + \ldots + z_n)^n \\
&\qquad = \frac{n!}{|G|}
\end{aligned}$$

6. Antes de entrar en el tema, es útil hacerse una idea del grupo que buscamos. Para determinar el orden del grupo hay dos posibilidades. La tradicional es tomar algún elemento y analizar su órbita y estabilizador. Tomando 3, su órbita es $G3 = \{3, 4, 6, 7\}$, mientras su estabilizador es $G_3 = \{\mathrm{id}, (6\ 7)\}$, con lo que $|G| = |G3| \cdot |G_3| = 4 \cdot 2 = 8$. Otra opción es considerar los órdenes en que pueden estar las hojas. Podemos dejarlas fijas, intercambiar el primer par y el segundo (o ambos), lo que da un total de 4 posibilidades; luego podemos intercambiar 2 y 5, lo que da 4 opciones adicionales con el mismo razonamiento anterior. Esto también da un total de 8 operaciones.

   a) Los elementos del grupo son:

Operación	**Término**
id	x_1^7
(3 4)	$x_1^5 x_2$
(6 7)	$x_1^5 x_2$
(3 4)(6 7)	$x_1^3 x_2^2$
(2 5)(3 6)(4 7)	$x_1 x_2^3$
(2 5)(3 7)(4 6)	$x_1 x_2^3$
(2 5)(3 6 4 7)	$x_1 x_2 x_4$
(2 5)(3 7 4 6)	$x_1 x_2 x_4$

   El grupo es de orden 8, así que:

$$\zeta_G(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = \frac{1}{8}\left(x_1^7 + 2x_1^5 x_2 + x_1^3 x_2^2 + 2x_1 x_2^3 + x_1 x_2 x_4\right)$$

   b) Por el teorema previo a Pólya, el número de coloreos diferentes con 2 colores es simplemente:

$$\zeta_G(2, 2, 2, 2, 2, 2, 2) = 42$$

   c) Por el teorema de Pólya, el número de coloreos con l azules, m rojos y n verdes es el coeficiente:

$$[u^l v^m w^n]\zeta_G(u+v+w, u^2+v^2+w^2, u^3+v^3+w^3, u^4+v^4+w^4, u^5+v^5+w^5, u^6+v^6+w^6, u^7+v^7+w^7)$$

   O sea, requerimos:

$$\sum_{m+n=4} [u^3 v^m w^n]\zeta_G(u+v+w, u^2+v^2+w^2, u^3+v^3+w^3, u^4+v^4+w^4, u^5+v^5+w^5, u^6+v^6+w^6, u^7+v^7+w^7)$$

   Bastante lioso... Una manera más simple de obtener lo mismo es reconocer que la función generatriz para el número de maneras de formar órbitas de l nodos donde u marca el número de nodos azules es simplemente $2 + u^l$ (dos formas de ningún azul, vale decir sólo rojos o sólo verdes; y una forma de l azules), y nos interesa:

$$\begin{aligned}&\zeta_G(2+u, 2+u^2, 2+u^3, 2+u^4, 2+u^5, 2+u^6, 2+u^7)\\ &\qquad = u^7 + 6u^6 + 25u^5 + 68u^4 + 120u^3 + 146u^2 + 105u + 42\end{aligned}$$

   lo que nos da el resultado como el coeficiente de u^3, o sea 120. También nos da el resultado de la parte anterior como el coeficiente de u^0, que corresponde a ningún nodo azul (sólo rojos y verdes, dos colores).

7. Cada uno por turno.

   a) En términos de los elementos de la matriz dada, las permutaciones permitidas de los elementos son:

Operación	**Ciclos**	**Tipo**
Identidad	$(a)(b)(c)(d)$	$[1^4]$
Intercambiar columnas	$(a\ b)(c\ d)$	$[2^2]$
Intercambiar filas	$(a\ c)(b\ d)$	$[2^2]$
Intercambiar filas y columnas	$(a\ d)(b\ c)$	$[2^2]$

   El grupo es de orden 4, como predice la fórmula del enunciado.

b) En consecuencia, el índice de ciclos es:

$$\zeta_G(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + 3x_2^2)$$

c) Si hay dos valores posibles de los elementos de la matriz, esto corresponde a colorear con dos colores, y nos interesa el número total de posibilidades distintas. O sea:

$$\begin{aligned}\zeta_G(2, 2, 2, 2) &= \frac{1}{4}(2^4 + 3 \cdot 2^2)\\ &= 7\end{aligned}$$

d) Acá interesa saber cuántas posibilidades hay con dos elementos de un color y dos del otro, o sea:

$$[z_1^2 z_2^2]\zeta_G(z_1 + z_2, z_1^2 + z_2^2, z_1^3 + z_2^3, z_1^4 + z_2^4)$$

Si no se quiere recurrir a `maxima` o similares, se ve que términos que contienen $z_1^2 z_2^2$ pueden provenir únicamente de potencias de $z_1 + z_2$ y de $z_1^2 + z_2^2$. Así tenemos:

$$\begin{aligned}[z_1^2 z_2^2](z_1 + z_2)^4 &= \binom{4}{2}\\ &= 6\\ [z_1^2 z_2^2](z_1^2 + z_2^2)^2 &= \binom{2}{1}\\ &= 2\end{aligned}$$

con lo que:

$$\begin{aligned}[z_1^2 z_2^2]\zeta_G(z_1 + z_2, z_1^2 + z_2^2, z_1^3 + z_2^3, z_1^4 + z_2^4) &= \frac{1}{4}(6 + 3 \cdot 2)\\ &= 3\end{aligned}$$

8. Vamos paso a paso.

a) Los elementos del grupo son:

Operación	**Término**
id	x_1^6
Rotación en 1/3	x_3^2
Rotación en 2/3	x_3^2
Reflexión en cada eje (3)	$x_1^2 x_2^2$

El grupo es de orden 6, así que:

$$\zeta_G(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{6}\left(x_1^6 + 3x_1^2 x_2^2 + 2x_3^2\right)$$

b) Por el teorema previo a Pólya, el número de coloreos con 5 colores es simplemente:

$$\zeta_G(5, 5, 5, 5, 5, 5) = 2\,925$$

c) Por el teorema de Pólya, si marcamos con z_r el número de piezas de color r el número de coloreos con i de color 1, j de color 2, k de color 3, l de color 4, y m de color 5 es el coeficiente:

$$\begin{aligned}[z_1^i z_2^j z_3^k z_4^l z_5^m]\zeta_G(&z_1 + z_2 + z_3 + z_4 + z_5, z_1^2 + z_2^2 + z_3^2 + z_4^2 + z_5^2, z_1^3 + z_2^3 + z_3^3 + z_4^3 + z_5^3,\\ &z_1^4 + z_2^4 + z_3^4 + z_4^4 + z_5^4, z_1^5 + z_2^5 + z_3^5 + z_4^5 + z_5^5, z_1^6 + z_2^6 + z_3^6 + z_4^6 + z_5^6)\end{aligned}$$

Para responder a la pregunta requerimos el número de términos que contienen exactamente tres de los z_r.

En realidad, acá estamos frente a una aplicación típica del principio de inclusión y exclusión.

1) El universo Ω es el conjunto de coloreos con 5 colores. Un coloreo tiene la propiedad i si el color i no está presente, y nos interesa el número de los que tienen exactamente 2 propiedades (los otros 3 colores presentes).
2) Acá $N(\supseteq S)$ es el número de coloreos que no consideran los colores en S, vale decir son coloreos tomando a lo más $5 - |S|$ colores:

$$N(\supseteq S) = \zeta_G(5 - |S|, 5 - |S|, 5 - |S|, 5 - |S|, 5 - |S|, 5 - |S|)$$

3) Como los r colores a excluir se eligen de entre los 5, y sólo influye el número de colores restantes con los que se colorea:

$$N_r = \binom{5}{r} \zeta_G(5 - r, 5 - r, 5 - r, 5 - r, 5 - r, 5 - r)$$

En este caso tenemos:

$$\begin{aligned}
N_0 &= \binom{5}{0} \zeta_G(5, 5, 5, 5, 5, 5) = 2\,925 \\
N_1 &= \binom{5}{1} \zeta_G(4, 4, 4, 4, 4, 4) = 4\,080 \\
N_2 &= \binom{5}{2} \zeta_G(3, 3, 3, 3, 3, 3) = 1\,650 \\
N_3 &= \binom{5}{3} \zeta_G(2, 2, 2, 2, 2, 2) = 200 \\
N_4 &= \binom{5}{2} \zeta_G(1, 1, 1, 1, 1, 1) = 5 \\
N_5 &= \binom{5}{5} \zeta_G(0, 0, 0, 0, 0, 0) = 0
\end{aligned}$$

La función generatriz es

$$N(z) = 5z^4 + 200z^3 + 1\,650z^2 + 4\,080z + 2\,925$$

4) Nos interesa e_2, que se obtiene de la función generatriz de los e_t, que sabemos es $E(z) = N(z - 1)$:

$$E(z) = 5z^4 + 180z^3 + 1\,080z^2 + 1\,360z + 300$$

Se pueden formar 1 080 brazaletes de tres colores.

9. Las operaciones son sólo rotaciones, en múltiplos de $\pi/4$. Son 8 operaciones en total, girando cada vez en $\pi/4$.

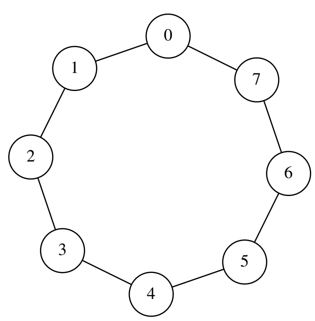


Figura 14: Esquema de $\mathtt{C}_8$ para la pregunta 9

Corresponden a ir sumando 1 módulo 8 cada vez. En detalle, son:

Operación	Ciclos
Identidad	(0)(1)(2)(3)(4)(5)(6)(7)
Rotación en 1	(0 1 2 3 4 5 6 7)
Rotación en 2	(0 2 4 6)(1 3 5 7)
Rotación en 3	(0 3 6 1 4 7 2 5)
Rotación en 4	(0 4)(1 5)(2 6)(3 7)
Rotación en 5	(0 5 2 7 4 1 6 3)
Rotación en 6	(0 6 4 2)(1 7 5 3)
Rotación en 7	(0 7 6 5 4 3 2 1)

En resumen:

Operación	Nº	Término
Identidad	1	x_1^8
Rotaciones en 1, 3, 5, 7	4	x_8
Rotaciones en 2, 6	2	x_4^2
Rotación en 4	1	x_2^4

En consecuencia:

$$\zeta_{C_8}(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = \frac{1}{8}\left(x_1^8 + 4x_8 + 2x_4^2 + x_4^2\right)$$

10. Sabemos que el orden del grupo es el orden de un estabilizador por el tamaño de una órbita. Si nos fijamos en un vértice, hay 3 operaciones que lo mantienen fijo (rotaciones en 0, $2\pi/3$ y $4\pi/3$, mientras podemos ubicar ese vértice en cualquiera de las 20 posiciones. En consecuencia, $|G| = |G_x| \cdot Gx| = 3 \cdot 20 = 60$.

    Otra forma de obtenerlo es aplicar la misma idea a una cara: Hay 5 rotaciones que mantienen la cara en su lugar, y la cara puede ocupar 12 posiciones, o sea $|G| = 5 \cdot 12 = 60$.

11. Aplicamos el teorema de Pólya. Paso a paso:

    a) Debemos encontrar el grupo que actúa acá. En este caso, es el grupo $\mathtt{C}_5$, de rotaciones del pentágono en el plano.

    b) Encontramos los efectos de las operaciones sobre las 11 áreas de la figura. En nuestro caso es simple:

Operación	Nº	Término
Identidad	1	x_1^{11}
Rotaciones en $2k\pi/5$	4	$x_1 x_5^2$

    c) Calcular el índice de ciclos:

    $$\zeta_P(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) = \frac{1}{5}\left(x_1^{11} + 4x_1 x_5^2\right)$$

    d) Como interesan los coloreos inequivalentes con 3 colores:

    $$\zeta_P(3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3) = \frac{1}{5}\left(3^{11} + 4 \cdot 3 \cdot 3^2\right) = 35\,451$$

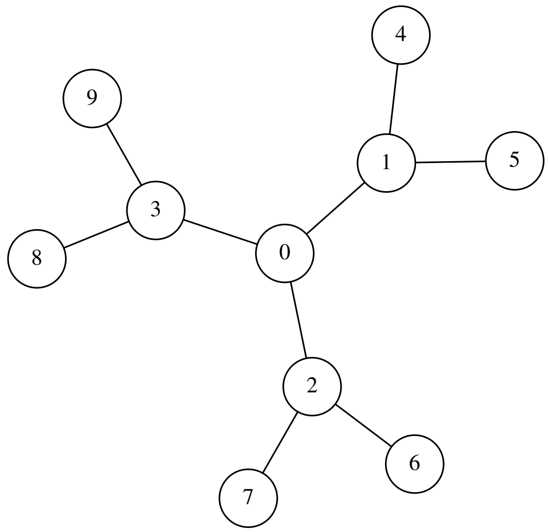
12. La estrategia general es aplicar el teorema de Pólya, encontrando el índice de ciclos del grupo (en alarde de creatividad, llamémosle G al grupo), y luego (asignando variables z_1 a z_3 a los distintos colores) calcular el término:

$$[z_1^3 z_2^3 z_3^3]\zeta_G(z_1+z_2+z_3, z_1^2+z_2^2+z_3^2, z_1^3+z_2^3+z_3^3, z_1^4+z_2^4+z_3^4, z_1^5+z_2^5+z_3^5, z_1^6+z_2^6+z_3^6, z_1^7+z_2^7+z_3^7, z_1^8+z_2^8+z_3^8, z_1^9+z_2^9+z_3^9)$$

    Para calcular el índice de ciclos, deben encontrarse los tipos de cada una de las operaciones del grupo, obteniendo los términos propios de cada operación.

    Para calcular el orden de nuestro grupo, fijemos un arco (digamos 1 4) y determinamos el estabilizador y la órbita. En este caso, la órbita tiene tamaño 6, y el estabilizador consta de 8 operaciones (podemos intercambiar ninguno, uno o ambos pares de hojas 6 7 y 8 9; y podemos intercambiar 6 8 y 7 9, luego podemos nuevamente reordenar de 3 maneras más). Así, el orden del grupo es $|G_{14}| \cdot |G\,14| = 8 \cdot 6 = 48$.

    En detalle (ver figura),



las operaciones son:

Operación tipo	**Nº**	**Término**
Identidad	1	x_1^9
(4 5)	3	$x_1^7x_2$
(4 5)(6 7)	3	$x_1^5x_2^2$
(4 5)(6 7)(8 9)	1	$x_1^3x_2^3$
(1 3)(4 8)(5 9)	12	$x_1^3x_2^3$
(1 3)(4 8)(5 9)(6 7)	12	$x_1x_2^4$