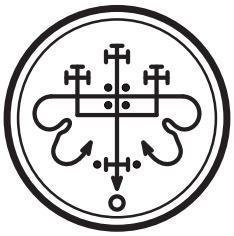
Soluciones de Problemas Propuestos
Fundamentos de Informática I

Horst H.~von Brand

17 de marzo 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 $A \triangle B = (A \cup B) \smallsetminus (A \cap B)$. 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

   $(a - \epsilon)g(n) \leq f(n) \leq (a + \epsilon)g(n)$ 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:

   $f(n) = \Omega(g(n))$ hay $n' \geq 0$ y $c' > 0$ tales que siempre que $n \geq n'$, $f(n) \geq c'g(n)$
   $f(n) = O(g(n))$ hay $n'' \geq 0$ y $c'' > 0$ tales que siempre que $n \geq n''$, $f(n) \leq c''g(n)$

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

   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 $A \smallsetminus B = A \cap \overline{B}$.

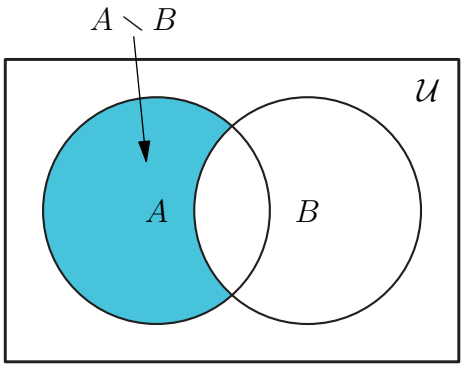


Figura 1: Diferencia entre conjuntos

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

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

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

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

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

   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

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

   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

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

   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

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

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.

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

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

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

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

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

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

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

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. □

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:

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

   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 $a\ R\ a$ por asimetría debe ser $a\ \not R\ a$, lo que es contradictorio. Por tanto para todo a es $a\ \not R\ a$, o sea, R es antireflexiva.

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

   Reflexividad: Para todo a tenemos $a\ R\ a$.

   Como R_1 y R_2 son relaciones de equivalencia, son reflexivas, y $a\ R_1\ a$ y $a\ R_2\ a$ siempre se cumplen, con lo que se cumple $a\ R\ a$.

   Simetría: Para todo a y b tenemos que si $a\ R\ b$ entonces $b\ R\ a$.

   Si $a\ R\ b$ es que $a\ R_1\ b$ y $a\ R_2\ b$; por ser R_1 y R_2 relaciones de equivalencia son ambas simétricas, y $b\ R_1\ a$ y $b\ R_2\ a$; o sea $b\ R\ a$.

   Transitividad: Para todo a, b y c tenemos que si $a\ R\ b$ y $b\ R\ c$ entonces $a\ R\ c$.

   Nuevamente, si $a\ R\ b$ y $b\ R\ c$ es que $a\ R_1\ b$ y $a\ R_2\ b$; $b\ R_1\ c$ y $b\ R_2\ c$; siendo R_1 y R_2 relaciones de equivalencia es $a\ R_1\ c$ y $a\ R_2\ c$, con lo que $a\ R\ c$.

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

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

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

   d) La relación R es reflexiva si para todo $a \in \mathcal{U}$ $a\ R\ a$, que es $a\ R^{-1}\ a$, 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. 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 ($g(1) = g(2) = 1$).

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

$x\ R_2 \circ R_1\ y$ si existe z tal que $x\ R_1\ z$ y $z\ R_2\ y$

Veamos cuándo es simétrica $R_2 \circ R_1$:

$y\ R_2 \circ R_1\ x$ significa que hay z' con $y\ R_1\ z'$ y $z'\ R_2\ x$

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.

8. Si la relación R es simétrica, entonces siempre que $a\ R\ b$ también se cumple $b\ R\ a$. Si es transitiva, si $a\ R\ b$ y $b\ R\ c$ entonces también $a\ R\ c$. 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.

9. 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.

10. Ejemplos de tales funciones $f : \mathbb{N} \to \mathbb{N}$ 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: $f(n) = n$

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

12. Si R_1 es transitiva, significa que siempre que $a\ R_1\ b$ y $b\ R_1\ c$ se cumple que $a\ R_1\ c$. 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.

13. 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.

14. *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:

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

    Combinando ambas:

    $$f(n) \geq c'c'' \cdot h(n) \qquad n \geq \text{máx}(n', n'')$$

    Esto corresponde a la definición con $n_0 = \text{máx}(n', n'')$ 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 $x\ R_2\ y$ cuando $x - y \in \mathbb{Z}$.

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

    Transitiva: $x\ R_2\ y$ y $y\ R_2\ z$ 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 $x\ R_2\ z$.

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

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

    Total: No. Por ejemplo, $1 \not R_2 \sqrt{2}$ y $\sqrt{2} \not R_2\ 1$.

15. Cada relación en turno.

    $\mathscr{R}_1$**: 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:

$$y = \frac{\pi}{2} - x$$
$$z = \frac{\pi}{2} - y = x$$

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

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

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 $y = \pi/2 \pm x + 2n\pi$

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

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

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
   $$\exists p.(D(p,\text{F}) \wedge C(\text{J},\text{F}) \wedge E(\text{J},\text{F})) \Rightarrow A(\text{J},\text{F})$$
   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:
   $$\neg\big(\exists p,x,y.(R(p) \wedge x \neq y \wedge D(p,x) \wedge D(p,y))\big)$$
   b) Esto es un poco más directo. Sea a un alumno, x algún ramo que toma. Entonces:
   $$\exists a.\,(R(a) \wedge (\forall x.(C(a,x) \Rightarrow A(a,x))))$$
   c) Sea p el profesor, x sus ramos y a los alumnos. Implícitamente estamos diciendo que se cumple para todo profesor:
   $$\forall p,x,a.\big(\neg R(p) \wedge D(p,x) \wedge C(a,x) \wedge (E(a,x) \Rightarrow A(a,x))\big)$$
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 $0 \le \theta \le \pi/2$. 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 $\sin\theta \ge 0$ y $\cos\theta \ge 0$, la última relación es imposible. En consecuencia $\sin\theta + \cos\theta \ge 1$.

   (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 mód $4 \neq 2$ y n mód $4 \neq 3$. Sea $n = a^2$, debemos considerar los casos:

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

   ***a* es impar:** En este caso $a = 2u + 1$, $a^2 = 4u^2 + 4u + 1$, y n mód $4 = 1$. 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:

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

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 $n\ge 2$.

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:

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

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 $n+1$:

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

    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:

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

    que ciertamente es verdad.

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

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

    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 $n \ge 2$.

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

    Bases: Para los tres primeros valores tenemos:

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

    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 $1, 3, \ldots, 2n-1$. 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:

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

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

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

que es exactamente lo que se quería demostrar.

De exactamente la misma forma puede demostrarse que

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

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:

$$F_0^2 = F_0F_1$$

que claramente se cumple.

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

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

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:

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

Acá usamos

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

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

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

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 $1 + x \ge 1 + x$, lo que se cumple.

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

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

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 $1 \ge 2(\sqrt{2}-1)$, lo que es cierto.

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

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

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:

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

lo que es cierto. La demostración para $m \ge 1$ 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 $n+1$:

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

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 $0 \le v_n < 4$, 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.

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:

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

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

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

    Esto es lo mismo que:

    $$b = g^{-1}ag$$
    $$c = h^{-1}bh$$

    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:

    $$c = k^{-1}ak$$
    $$a = kck^{-1}$$

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

Simétrica: Esto es que siempre que $a\ R\ b$ también es $b\ R\ a$. 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:

    $$(a \oplus b) \oplus c = a + b + c - 2k$$
    $$a \oplus (b \oplus c) = a + b + c - 2k$$

    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:

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

    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:

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

En particular:

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

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:

$$0 = 0 + 0 \cdot \sqrt{2}$$
$$1 = 1 + 0 \cdot \sqrt{2}$$

y ambos pertenecen.

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

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

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:

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

Esto significa:

$$ux + 2vy = 1$$
$$vx + uy = 0$$

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 $a \in A$: $a \, R \, a$

Siempre tenemos $1 \cdot a \cdot 1^{-1} = a$, con lo que $a \, R \, a$, y es reflexiva.

Transitiva: Para todo $a, b, c \in A$: Si $a \, R \, b$ y $b \, R \, c$, entonces $a \, R \, c$.

Supongamos $a \, R \, b$ y $b \, R \, c$, 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 $a \, R \, c$, y es transitiva.

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

Supongamos $a \, R \, b$, 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 $b \, R \, a$, 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 $\{a \cdot x : x \neq 0\}$. 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:

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_m x^m \\ g(x) &= b_0 + b_1 x + \cdots + b_n x^n \end{aligned}$$

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 el

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

Cuadro 1: Algoritmo de Euclides de polinomios

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:

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

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

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

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

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 $\mathscr{A}$, $\mathscr{B}$ y $\mathscr{C}$:

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

   Véase la figura 2. La operación es asociativa.

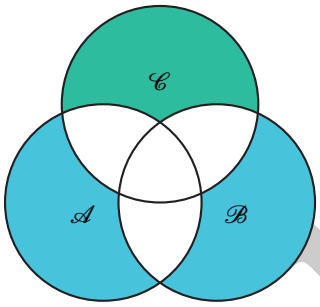


Figura 2: Diferencia simétrica entre tres conjuntos

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

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

   Hay un neutro.

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

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

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

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

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

   Es conmutativa.

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

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

   La intersección es asociativa.

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

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

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

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

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

   con lo que tenemos un neutro.

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

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

   También es conmutativa.

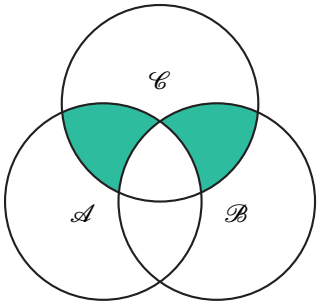


Figura 3: Intersección con la diferencia simétrica entre dos conjuntos

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

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:

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

   d) El elemento neutro es la función que cumple:

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

   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:

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

   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 $k \in \mathbb{Z}$:

$$u' = u + \frac{kb}{d)}$$
$$v' = v - \frac{ka}{d}$$

De acá obtenemos los posibles valores de x e y:

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

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 $e_n \le 5 \cdot 10^{-5}$ o sea $2x_n y_n \ge 2000$. 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:

   $$x \cdot x - d\,y \cdot y = 1$$

   Hemos escrito:

   $$sx + ty = 1$$

   con lo que son relativamente primos.

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

   Si $n > 1$, tenemos:

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

   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:

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

   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 $3^{474} \equiv 729 \neq \text{ñ}pm1 \pmod{949}$ 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:

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

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:

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

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

    $$m_5 = (7 \cdot 8) \cdot 1 = \ 56$$
    $$m_7 = (5 \cdot 8) \cdot 3 = 120$$
    $$m_8 = (5 \cdot 7) \cdot 3 = 105$$

    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:

$$\phi(1\,268\,064) = 2^4 \cdot (2-1) \cdot 3 \cdot (3-1) \cdot (7-1) \cdot (17-1) = 9216$$

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 $\theta\colon \mathbb{Z}_6 \to \mathbb{Z}_7^\times$. Es

$\cdot$	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 $\mathbb{Z}_6$

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 $v \mid a_0$. □

    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:

    $$x_{n+1} = x_0 x_n + d y_0 y_n$$
    $$y_{n+1} = y_0 x_n + x_0 y_n$$

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

$$sa^m + tb^n = 1$$
$$(sa^{m-1})a + (tb^{n-1})b = 1$$

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:

$$x = \sum_{0 \le k \le n} d_k \cdot 10^k$$

a) Como $10 \equiv 1 \pmod 9$, la expresión para x es:

$$x \equiv \sum_{0 \le k \le n} d_k \cdot 1^k \equiv \sum_{0 \le k \le n} d_k \pmod 9$$

b) Como $10 \equiv -1 \pmod{11}$, la expresión para x es:

$$x \equiv \sum_{0 \le k \le n} d_k \cdot (-1)^k \pmod{11}$$

40. Interesa el conjunto de elementos de $\mathbb{Z}_{\mathbb{1}}$ 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, *e*1, *e*4, 25, *o*6, *e*9

41. Sabemos que si para primos p_r diferentes

$$N = \prod_{1 \le r \le n} p_r^{k_r}$$

entonces:

$$\phi(N) = \prod 1 \le r \le n p_r^{k_r - 1}(p_r - 1)$$

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 $0 \le t \le 4$, los demás valores que se han revisado son todos compuestos.

42. Por el teorema de Fermat, sabemos que si $p \not| x$:

$$x^{p-1} \equiv 1 \pmod p$$
$$x^p \equiv x \pmod p$$

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 $\mathscr{P}_{\surd}$ es que el número sea divisible por el primo p.
- Nos interesan los elementos que tengan al menos una propiedad, o sea $|\Omega| - e_0$.
- $N(\supseteq \mathscr{S})$ son los números divisibles por todos los elementos de $\mathscr{S}$, 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:

$$\begin{aligned} \gcd(a^2, b^2) &= \gcd(d^2 \cdot (a/d)^2, d^2 \cdot (b/d)^2) \\ &= d^2 \cdot \gcd((a/d)^2, (b/d)^2) \\ &= d^2 \\ &= \big(\gcd(a, b)\big)^2 \end{aligned}$$

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:

$$(a+b)^p = \sum_{0\le k\le p} \binom{p}{k} a^{p-k}b^k$$

Ahora, como:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

tenemos que p divide al coeficiente binomial para $1 \le k \le p-1$, 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 $p \not| u$, 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 $p \nmid a$, 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:

$$u = a + b$$
$$v = a - b$$

tenemos que:

$$u + v = 2a$$
$$u - v = 2b$$

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:

$$\begin{aligned} s_3 &= (15/3)^{-1} = 5^{-1} = 2 \text{ en } \mathbb{Z}_3 \quad & m_3 &= (15/3) \cdot s_3 = 10 \\ s_5 &= (15/5)^{-1} = 3^{-1} = 2 \text{ en } \mathbb{Z}_5 \quad & m_5 &= (15/5) \cdot s_5 = 6 \end{aligned}$$

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 $\deg(r''(x) - r'(x)) \leq \max(\deg(r'(x), r''(x))) < \deg(d(x))$. 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:

    $$x_0 = \frac{sc}{d}$$
    $$y_0 = \frac{tc}{d}$$

    La relación entre x e y es lineal, para entero k y enteros u, v debe ser algo como:

    $$x = x_0 - ku$$
    $$y = y_0 + kv$$

    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:

$$ax^2 + bx + c = 0$$
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

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...

$$\begin{aligned} 50^{50} \text{ mód } 45 &= 25^{50} \cdot 2^{50} \text{ mód } 45 \\ &= 5^{100} \cdot 2^2 \text{ mód } 45 \\ &= 5^{100} \cdot 4 \text{ mód } 45 \end{aligned}$$

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:

$$50^{50} \text{ mód } 45 = 5^{100} \cdot 4 \text{ mód } 45 = 40 \cdot 4 \text{ mód } 45 = 25$$

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:

$$r^{(p-1)/2} \equiv -1 \pmod{p}$$
$$r^{m(p-1)/2} \equiv (-1)^m \pmod{p}$$
$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

87. Sea c un divisor común de $a+b$ y $a-b$. Entonces c divide a:

$$(a+b)+(a-b) = 2a$$
$$(a+b)-(a-b) = 2b$$

Por Bézout, sabemos que hay enteros u y v tales que:

$$au + bv = 1$$
$$(2a)u + (2b)v = 2$$

En consecuencia:

$$\gcd(a+b, a-b) \mid 2$$

y tenemos nuestro resultado.

Corresponde completar vía demostrar que ambas opciones son posibles. Consideremos:

$$\gcd(2,1) = 1$$
$$\gcd(2+1, 2-1) = 1$$
$$\gcd(3,1) = 1$$
$$\gcd(3+1, 3-1) = 2$$

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:

$$\sum_{d|n} \phi(d) = n$$

Por inversión de Möbius:

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$
$$= n\sum_{d|n} \frac{\mu(d)}{d}$$

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

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 $a_{k-1}, a_{k-2}, \ldots a_0$, 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 mód $n \rightsquigarrow (m_p^e, m_q^e)$. 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:

$$\begin{aligned}(0, c_q^d) &= \left(0, \left((kp)^e\right)^d\right) \\ &= \left(0, (kp)^{ed-1} \cdot kp\right) \\ &= (0, kp)\end{aligned}$$

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 mód 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 $m_1, m_2, \ldots$ que se cifran dando respectivamente $c_1, c_2, \ldots$ (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

   $$\sum_{3\le k\le 6} 26^k = 26^3 \sum_{0\le k\le 3} 26^k = 26^3\cdot \frac{26^4-1}{26-1} = 321\,271\,704$$

   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:

$$\sum_{3\le k\le 6} 26^{k-1}\cdot 10\cdot k = 26^2\cdot 10\sum_{0\le k\le 3} 26^k(k+3) = 736\,454\,680$$

Por la regla de la suma, el total de patentes personalizadas es

$$26^3\cdot\frac{26^4-1}{26-1} + 26^2\cdot 10\sum_{0\le k\le 3} 26^k(k+3) = 1\,057\,726\,384$$

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:

$$\prod_{1\le i\le k}(n_i+1)$$

Siguiendo el desarrollo en el apunte, el número buscado es el número de soluciones del sistema de inecuaciones:

$$\begin{aligned} x_1 + x_2 + \cdots + x_k &= m \\ 0 \le x_i &\le n_i \end{aligned}$$

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:

$$n(n-1)(n-2) = 3n(n-1)$$
$$n^3 - 6n^2 + 5n = 0$$

Soluciones de esta ecuación son $n = 0$, $n = 1$ y $n = 5$.

c) Igual a las anteriores:

$$2n(n-1) + 50 = 2n(2n-1)$$
$$2n^2 - 50 = 0$$

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 $\{A^5, D^1 7\}$, lo que nos da:

$$\binom{5+17}{5\ 17} = 26334$$

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:

$$9 \cdot 10^5 = 900000$$

Si no se permiten repeticiones, hay 9 opciones para el primer dígito, 9 para el segundo, 8 para el tercero, etc. O sea $9 \cdot 9^{\underline{5}} = 136080$ 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:

$$\frac{36^9 - 36^1}{36-1} \cdot \frac{36^4 - 36^1}{36-1} = 139250307444539652$$

18. Igual que el caso anterior, básicamente:

$$\frac{126^{15}-126^{1}}{126-1} = 319408025254357014550350413952$$

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:

  $$\frac{1}{2}\cdot 13^4\cdot(12\cdot 4) = 685464$$

  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, …, 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 $S = \{(x, y) : x \text{ estudió con } y\}$. 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 $S = \{(x, y) : x \text{ e } y \text{ estudiaron juntos}\}$. Si llamamos m al número de mujeres en el curso, el enunciado dice:

$$\sum_x r_x(S) = 32 \cdot 5$$
$$\sum_y c_y(S) = m \cdot 8$$

Ambos deben ser iguales:

$$32 \cdot 5 = m \cdot 8$$
$$m = 20$$

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:

$$\binom{8}{2\,2\,1\,1\,1\,1} = \frac{8!}{2!2!1!1!1!1!} = 10\,080$$

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 $0 \le k \le n$ 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:

$$\begin{aligned}
\sum_{0\le k\le n+1} k\binom{n+1}{k} &= \sum_{0\le k\le n} k\left(\binom{n}{k} + \binom{n}{k-1}\right) \\
&= \sum_{0\le k\le n} k\binom{n}{k} + \sum_{0\le k\le n} (k+1)\binom{n}{k} \\
&= n\cdot 2^{n-1} + \sum_{0\le k\le n} k\binom{n}{k} + \sum_{0\le k\le n}\binom{n}{k} \\
&= n\cdot 2^n + 2^n \\
&= (n+1)\cdot 2^n
\end{aligned}$$

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:

$\{A\diamondsuit\ K\diamondsuit\ 3\heartsuit\ J\clubsuit\ 7\spadesuit\}$
$\{A\spadesuit\ 2\spadesuit\ 3\heartsuit\ 4\clubsuit\ 5\diamondsuit\}$

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:

$(\diamondsuit,\{A,K\},7,3,J) \longleftrightarrow \{A\diamondsuit\ K\diamondsuit\ 3\heartsuit\ J\clubsuit\ 7\spadesuit\}$
$(\spadesuit,\{A,2\},3,4,5) \longleftrightarrow \{A\spadesuit\ 2\spadesuit\ 3\heartsuit\ 4\clubsuit\ 5\diamondsuit\}$

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 $\{A^2,B,C,I^2,M,N,O^2,R,T\}$. 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:

$$2\cdot\binom{11}{1,1,1,2,1,1,2,1,1} - \binom{10}{1,1,2,1,1,2,1,1} = 19\,051\,200$$

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 (1º o 2º) del grupo y. En la segunda ronda juegan: $1:1$ contra $2:2$ (1$^{\text{er}}$ partido), $1:2$ contra $2:3$ (2º partido), $1:3$ contra $2:4$ (3$^{\text{er}}$ partido) y $1:4$ contra $2:1$ (4º 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 $2 \le y \le 4$. 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.