Facultad de Ciencias MATEMÁTICAS

UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

Tema 2: Números, inducción y recursión

Rafael del Vado Vírseda, Simon Pickin

Matemática Discreta y Lógica Matemática I

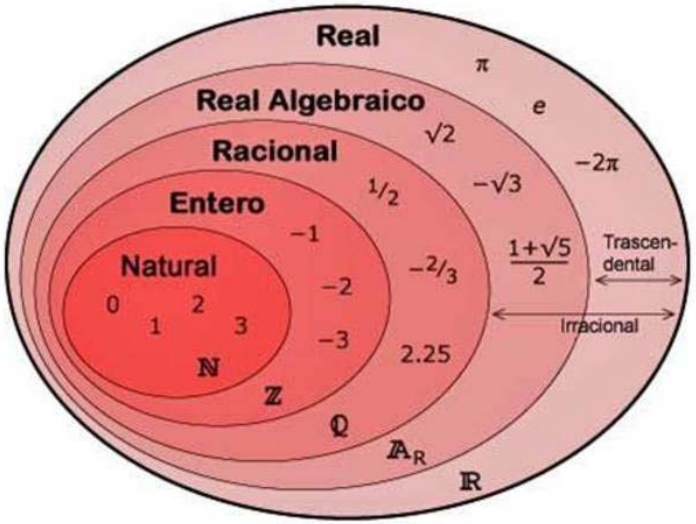
Doble Grado en Ingeniería Informática y Matemáticas

Curso 2020-2021

Conjuntos Numéricos

- Denotamos $\mathbb{N} = \{0, 1, 2, \ldots\}$ al conjunto de los **números naturales**. Fijamos 0 como el primer número natural.

- A lo largo de la historia de las matemáticas, el conjunto de los números naturales se ha ido ampliando sucesivamente



"Dios creó los números naturales, el resto es obra del hombre"

Leopold Kronecker
(1823-1891)

- Llamaremos **segmento de $\mathbb{N}$ para $m \in \mathbb{N}$** al siguiente subconjunto $\mathbb{N}_m$ de $\mathbb{N}$:

$$\mathbb{N}_m = \{m, m+1, m+2, \ldots\} = \{n \in \mathbb{N} : m \leq n\}$$

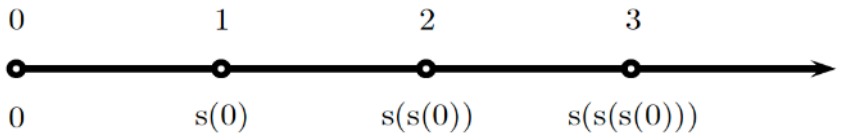
- Por ejemplo:

$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\} = \mathbb{N}$
$\mathbb{N}_1 = \{1, 2, 3, 4, \ldots\} = \mathbb{N}^+$ (conjunto de los **números naturales positivos**)
$\mathbb{N}_7 = \{7, 8, 9, 10, 11, 12, \ldots\}$

- El conjunto $\mathbb{N}$ puede generarse a partir del 0 y de la aplicación reiterada de la función **sucesor** $s : \mathbb{N} \longrightarrow \mathbb{N}$, que asigna a cada número natural n su siguiente o sucesor $n+1$ ($s(n) = n+1$):

$$0$$
$$1 = s(0)$$
$$2 = s\big(s(0)\big) = s^2(0)$$
$$3 = s\Big(s\big(s(0)\big)\Big) = s^3(0)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$n = s\Big(s\big(\cdots s(0)\big)\Big) = s^n(0)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$\mathbb{N}$:



- El conjunto de los números enteros $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{N} \cup \{-1, -2, -3, \dots\}$ puede generarse a partir del 0, la función sucesor s, y la función **predecesor** $p : \mathbb{Z} \longrightarrow \mathbb{Z}$, que asigna a cada número entero n su anterior o predecesor $n-1$ ($p(n) = n-1$):

$$-1 = p(0)$$
$$-2 = p\big(p(0)\big) = p^2(0)$$
$$-3 = p\Big(p\big(p(0)\big)\Big) = p^3(0)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

- La relación entre ambas funciones generadoras es la siguiente:

$$s\big(p(n)\big) = n \qquad p\big(s(n)\big) = n$$

- El conjunto de los números **racionales** es $\mathbb{Q} = \left\{\frac{m}{n} : m, n \in \mathbb{Z}\right\}$. Se cumple que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

- Todo número racional tiene un desarrollo decimal finito o periódico. Por ejemplo:

$$\frac{1}{5} = 0.2 \qquad \frac{1}{3} = 0.3333\ldots. \qquad \frac{17}{6} = 2.8333\ldots. \qquad \frac{41}{3330} = 0.0123123\ldots$$

- Existen números con un desarrollo decimal no periódico: 8.101001000100001 … A estos números se les denomina **irracionales**. Otros números irracionales son:

$$\pi = 3.14159265358979323846264\ldots$$
$$\sqrt{2} = 1.41421356237309504880168872420969\ldots$$

El conjunto de los números irracionales se denota por $\mathbb{I}$.

- El conjunto de los números **reales** es $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Por tanto, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

- También se distingue entre números **algebraicos** y **trascendentes**. Un número real es *algebraico* si es solución de una ecuación polinómica. En caso contrario se dice que es *trascendente*. Por ejemplo, $\sqrt{2}$ es un número algebraico, pues es solución de la ecuación polinómica $x^2 - 2 = 0$. Tanto π como e son números trascendentes.

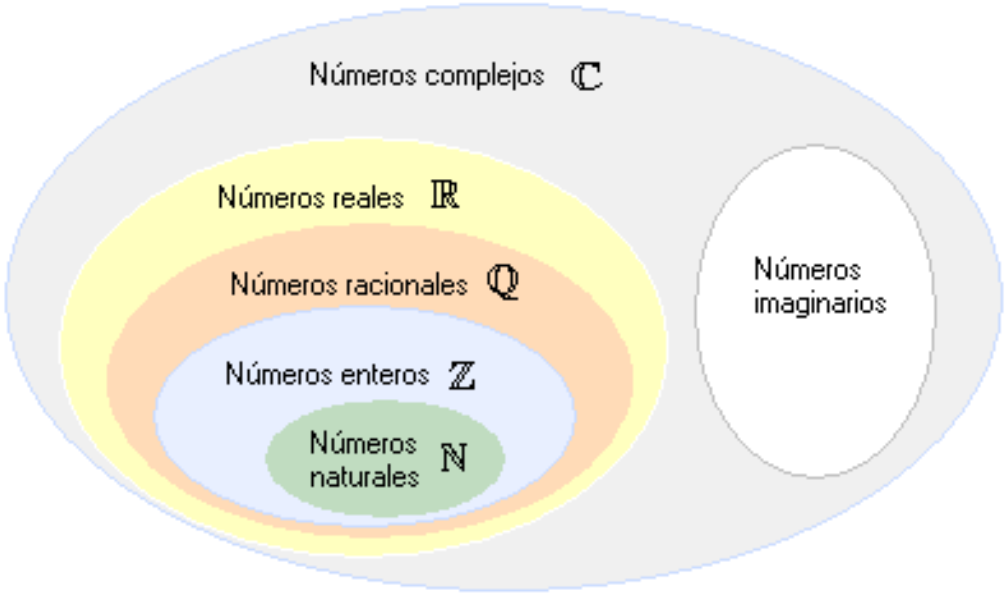
- Todo número racional es un número algebraico, pues $q = \frac{m}{n}$ es solución de la ecuación polinómica $nx - m = 0$.

- La ecuación $x^2 + 1 = 0$ no tiene solución en los números reales. Es necesario considerar un conjunto más amplio de números, los números **complejos**:

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

donde $i = \sqrt{-1}$ es la *unidad imaginaria*. Los números complejos de la forma bi se denominan **imaginarios**. En consecuencia, se verifica $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

- El conjunto de los números complejos $\mathbb{C}$ verifica que todo polinomio con coeficientes en $\mathbb{C}$ tiene siempre solución en $\mathbb{C}$ (**Teorema Fundamental del Álgebra**). En consecuencia, el proceso algebraico que nos ha obligado a ir extendiendo los conjuntos numéricos finaliza con el conjunto de los números complejos $\mathbb{C}$.



Axiomas de Peano

- Se define el conjunto $\mathbb{N}$ de los números naturales mediante los cinco axiomas siguientes:

$(\mathbf{Ax})_1$ Existe un elemento de $\mathbb{N}$ al que llamamos 0 (**primer número natural**).

$(\mathbf{Ax})_2$ Existe la llamada función **sucesor** $s : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\forall n \in \mathbb{N} : s(n) \in \mathbb{N}$.

$(\mathbf{Ax})_3$ El 0 no es el sucesor de ningún número natural:

$$\forall n \in \mathbb{N} : s(n) \neq 0$$

$(\mathbf{Ax})_4$ No existen dos números naturales distintos con el mismo sucesor:

$$\forall n, m \in \mathbb{N} : \big(s(n) = s(m)\big) \Longrightarrow (n = m)$$

$(\mathbf{Ax})_5$ Todo conjunto numérico A al que pertenece el 0 y dónde todo elementos de A tiene su sucesor en A, necesariamente coincide con $\mathbb{N}$ (**principio de inducción matemática**):

$$\forall A \subseteq \mathbb{N} : \big((0 \in A) \wedge (\forall n \in A : s(n) \in A)\big) \Longrightarrow (A = \mathbb{N})$$

- Sea $P(n)$ una **propiedad** definida para un número natural $n \in \mathbb{N}$. Para demostrar que $P(n)$ se verifica **para todo** número natural $n \in \mathbb{N}$, es decir

$$\forall n \in \mathbb{N} : P(n)$$

aplicamos el **principio de inducción matemática** sobre el conjunto $A = \{n \in \mathbb{N} : P(n)\} \subseteq \mathbb{N}$:

$$\forall n \in \mathbb{N} : \Big(P(0) \wedge \big(\forall k \geq 0 : P(k) \Longrightarrow P(k+1)\big)\Big) \Longrightarrow P(n)$$

Para ello, razonamos por **inducción sobre $n \in \mathbb{N}$**, probando los siguientes casos:

- **Caso base:** $n = 0$

  Probamos que $P(0)$ es cierta.

- **Paso inductivo:** $n > 0$

  Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple $P(k)$:

$$\forall k \in \mathbb{N} : P(k) \qquad (\mathbf{HI})$$

  Apoyándonos en la $(\mathbf{HI})$, probamos que se cumple $P(k+1)$ (**caso inductivo**):

$$\forall k \geq 0 : P(k) \Longrightarrow P(k+1)$$

Si se cumplen ambos casos (**caso base** y **caso inductivo**), entonces se cumple

$$\forall n \in \mathbb{N} : P(n) \qquad \blacksquare$$

Ejemplo 1

- **Ejercicio 1.36:** Demostrar que se cumple $\forall n \in \mathbb{N} : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 0 + 1 + 2 + 3 + 4 + \cdots + n = \frac{n \cdot (n+1)}{2}$$

Demostración

Razonamos por **inducción sobre** $\boldsymbol{n} \in \mathbb{N}$:

- **Caso base:** $n = 0$

$$P(0) \equiv \frac{0 \cdot (0+1)}{2} = \frac{0 \cdot 1}{2} = \frac{0}{2} = 0$$

Se cumple $P(0)$.

- **Paso inductivo:** $n > 0$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple

$$P(k) \equiv 0 + 1 + 2 + 3 + 4 + \cdots + k = \frac{k \cdot (k+1)}{2} \quad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N} : P(k) \Longrightarrow P(k+1)$.

$$P(k+1) \equiv 0 + 1 + 2 + 3 + 4 + \cdots + k + (k+1) = \quad \textit{Aplicamos la } (\mathrm{HI})$$

$$\frac{k \cdot (k+1)}{2} + (k+1) = \frac{k \cdot (k+1) + 2 \cdot (k+1)}{2} = \quad \textit{Sacamos factor común a } (k+1)$$

$$\frac{(k+1) \cdot (k+2)}{2} = \frac{(k+1) \cdot \big((k+1)+1\big)}{2}$$

Por tanto, se cumple $\forall n \in \mathbb{N} : P(n)$. ■

Ejemplo 2

- **Ejercicio 1.13:** Demostrar que se cumple $\forall n \in \mathbb{N} : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 0 + 2 + 4 + \cdots + 2n = n \cdot (n+1)$$

Demostración

Demostramos que se verifica

$$P(n) \equiv \sum_{i=0}^{n} 2i = n \cdot (n+1)$$

razonando por **inducción sobre $n \in \mathbb{N}$**:

- **Caso base:** $n = 0$

$$P(0) \equiv \sum_{i=0}^{0} 2i = 2 \cdot 0 = 0 = 0 \cdot 1 = 0 \cdot (0+1)$$

Se cumple $P(0)$.

- **Paso inductivo:** $n > 0$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple

$$P(k) \equiv \sum_{i=0}^{k} 2i = k \cdot (k+1) \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N} : P(k) \Longrightarrow P(k+1)$.

Ejemplo 2 (Continuación)

$$P(k+1) \equiv \sum_{i=0}^{k+1} 2i = \sum_{i=0}^{k} 2i + 2 \cdot (k+1) =$$

Aplicamos la (HI)

$$k \cdot (k+1) + 2 \cdot (k+1) =$$

Sacamos factor común a $(k+1)$

$$(k+1) \cdot (k+2) = (k+1) \cdot \big((k+1)+1\big)$$

Por tanto, se cumple $\forall n \in \mathbb{N} : P(n)$. ■

Ejemplo 3

- **Ejercicio 1.32:** Demostrar que se cumple $\forall n \in \mathbb{N} : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 0^2 + 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$$

Demostración

Demostramos que se verifica

$$P(n) \equiv \sum_{i=0}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$$

razonando por **inducción sobre** $\boldsymbol{n} \in \mathbb{N}$:

- **Caso base:** $n = 0$

$$P(0) \equiv \sum_{i=0}^{0} i^2 = 0^2 = \frac{0 \cdot (0+1) \cdot (2 \cdot 0 + 1)}{6} = \frac{0 \cdot 1 \cdot 1}{6} = 0$$

Se cumple $P(0)$.

- **Paso inductivo:** $n > 0$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple

$$P(k) \equiv \sum_{i=0}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2k+1)}{6} \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N} : P(k) \Longrightarrow P(k+1)$.

Ejemplo 3 (Continuación)

$$P(k+1) \equiv \sum_{i=0}^{k+1} i^2 =$$

$$\sum_{i=0}^{k} i^2 + (k+1)^2 = \qquad \textit{Aplicamos la } (\mathrm{HI})$$

$$\frac{k \cdot (k+1) \cdot (2k+1)}{6} + (k+1)^2 =$$

$$\frac{k \cdot (k+1) \cdot (2k+1) + 6 \cdot (k+1)^2}{6} =$$

$$\frac{(k+1) \cdot \big(k \cdot (2k+1) + 6 \cdot (k+1)\big)}{6} = \qquad \textit{Sacamos factor común a } (k+1)$$

$$\frac{(k+1) \cdot (2k^2 + 7k + 6)}{6} = \qquad \textit{Factorizamos } 2k^2 + 7k + 6$$

$$\frac{(k+1) \cdot (k+2) \cdot (2k+3)}{6} =$$

$$\frac{(k+1) \cdot \big((k+1)+1\big) \cdot (2 \cdot (k+1)+1)}{6}$$

Por tanto, se cumple $\forall n \in \mathbb{N} : P(n)$. ■

Ejemplo 4

- **Ejercicio 1.34:** Demostrar que se cumple $\forall n \in \mathbb{N}_1 : P(n)$, siendo $P(n)$ la siguiente propiedad:

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

Demostración

Demostramos que se verifica

$$P(n) \equiv \sum_{i=1}^{n} i^3 = \left(\frac{n \cdot (n+1)}{2}\right)^2$$

razonando por **inducción sobre $n \in \mathbb{N}_1$**:

- **Caso base:** $n = 1$

$$P(1) \equiv \sum_{i=1}^{1} i^3 = 1^3 = 1 = 1^2 = \left(\frac{1 \cdot 2}{2}\right)^2 = \left(\frac{1 \cdot (1+1)}{2}\right)^2 \quad \checkmark$$

Se cumple $P(1)$.

Ejemplo 4 (Continuación)

- **Paso inductivo:** $n > 1$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 1$ se cumple

$$P(k) \equiv \sum_{i=1}^{k} i^3 = \left(\frac{k \cdot (k+1)}{2}\right)^2 \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple

$$P(k+1) \equiv \sum_{i=1}^{k+1} i^3 = \left(\frac{(k+1) \cdot (k+2)}{2}\right)^2$$

En efecto:

$$P(k+1) \equiv \sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3 =^{\mathrm{HI}} \left(\frac{k \cdot (k+1)}{2}\right)^2 + (k+1)^3 =$$

$$\frac{k^2 \cdot (k+1)^2 + 2^2 \cdot (k+1)^3}{2^2} = \qquad \textit{Sacamos factor común a } (k+1)^2$$

$$\frac{(k+1)^2 \cdot \left(k^2 + 4 \cdot (k+1)\right)}{2^2} = \frac{(k+1)^2 \cdot (k^2 + 4k + 4)}{2^2} = \frac{(k+1)^2 \cdot (k+2)^2}{2^2} =$$

$$\left(\frac{(k+1) \cdot (k+2)}{2}\right)^2$$

✓

- **Ejercicio 1.37:** Demostrar que se cumple $\forall n \in \mathbb{N}_2 : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (n-1) \cdot n = \frac{(n-1) \cdot n \cdot (n+1)}{3}$$

Demostración

Demostramos que se verifica

$$P(n) \equiv \sum_{i=2}^{n} (i-1) \cdot i = \frac{(n-1) \cdot n \cdot (n+1)}{3}$$

razonando por **inducción sobre** $\boldsymbol{n} \in \mathbb{N}_2$:

- **Caso base:** $n = 2$

$$P(2) \equiv \sum_{i=2}^{2} (i-1) \cdot i = (2-1) \cdot 2 = \frac{(2-1) \cdot 2 \cdot 3}{3} = \frac{(2-1) \cdot 2 \cdot (2+1)}{3}$$ ✓

Se cumple $P(2)$.

Ejemplo 5 (Continuación)

- **Paso inductivo:** $n > 2$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 2$ se cumple

$$P(k) \equiv \sum_{i=2}^{k} (i-1) \cdot i = \frac{(k-1) \cdot k \cdot (k+1)}{3} \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple

$$P(k+1) \equiv \sum_{i=2}^{k+1} (i-1) \cdot i = \frac{\big((k+1)-1\big) \cdot (k+1) \cdot \big((k+1)+1\big)}{3} = \frac{k \cdot (k+1) \cdot (k+2)}{3}$$

En efecto:

$$P(k+1) \equiv \sum_{i=2}^{k+1} (i-1) \cdot i = \sum_{i=2}^{k} (i-1) \cdot i + \big((k+1)-1\big) \cdot (k+1) =$$

$$\sum_{i=2}^{k} (i-1) \cdot i + k \cdot (k+1) \ =^{\mathrm{HI}} \frac{(k-1) \cdot k \cdot (k+1)}{3} + k \cdot (k+1) =$$

$$\frac{(k-1) \cdot k \cdot (k+1) + 3 \cdot k \cdot (k+1)}{3} = \qquad \textit{Sacamos factor común a } k \cdot (k+1)$$

$$\frac{k \cdot (k+1) \cdot \big((k-1)+3\big)}{3} = \frac{k \cdot (k+1) \cdot (k+2)}{3} \qquad \checkmark$$

Ejemplo 6

- **Ejercicio 1.14:** Demostrar que se cumple $\forall n \in \mathbb{N} : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

Demostración

Demostramos que se verifica

$$P(n) \equiv \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

razonando por **inducción sobre** $\boldsymbol{n} \in \mathbb{N}$:

- **Caso base:** $n = 0$

$$P(0) \equiv \sum_{i=0}^{0} 2^i = 2^0 = 1 = 2 - 1 = 2^{0+1} - 1$$

Se cumple $P(0)$.

- **Paso inductivo:** $n > 0$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple

$$P(k) \equiv \sum_{i=0}^{k} 2^i = 2^{k+1} - 1 \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N} : P(k) \Longrightarrow P(k+1)$.

Ejemplo 6 (Continuación)

$$P(k+1) \equiv \sum_{i=0}^{k+1} 2^i = \sum_{i=0}^{k} 2^k + 2^{k+1} = \qquad \textit{Aplicamos la } (\mathrm{HI})$$

$$2^{k+1} - 1 + 2^{k+1} = \qquad \textit{Sacamos factor común a } 2^{k+1}$$

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

Por tanto, se cumple $\forall n \in \mathbb{N} : P(n)$. ■

Ejemplo 7

- **Ejercicio 1.20:** Demostrar que se cumple $\forall n \in \mathbb{N}_1 : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv n < 2^n$$

Demostración

Razonamos por **inducción sobre** $n \in \mathbb{N}_1$:

- **Caso base:** $n = 1$

$$P(1) \equiv 1 < 2 = 2^1 \quad \checkmark$$

Se cumple $P(1)$.

- **Paso inductivo:** $n > 1$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 1$ se cumple

$$P(k) \equiv k < 2^k \quad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N}_1 : P(k) \Longrightarrow P(k+1)$.

$$\begin{aligned} P(k+1) \equiv\ & k + 1 < \\ & 2^k + 1 < \\ & 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} \end{aligned}$$

Aplicamos la (HI)

Por inducción: $2^k > 1$, para todo $k \geq 1$ ✓

■

$$\forall k \in \mathbb{N}_1 : 2^k > 1$$

- **Caso base:** $k = 1$

$$2^1 = 2 > 1 \quad \checkmark$$

- **Paso inductivo:** $k > 1$

$$\forall k \in \mathbb{N}_1 : 2^k > 1 \quad (\mathrm{HI})$$

$$2^{k+1} = 2^k \cdot 2 \geq^{\mathrm{HI}} 1 \cdot 2 = 2 > 1 \quad \checkmark$$

Ejemplo 8

- **Ejercicio 1.18:** Demostrar que se cumple $\forall n \in \mathbb{N}_4 : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 2^n < n!$$

Demostración

Razonamos por **inducción sobre** $\boldsymbol{n} \in \mathbb{N}_4$:

- **Caso base:** $n = 4$

$$P(4) \equiv 2^4 = 16 < 24 = 4 \cdot 3 \cdot 2 \cdot 1 = 4! \quad \checkmark$$

Se cumple $P(4)$.

- **Paso inductivo:** $n > 4$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 4$ se cumple

$$P(k) \equiv 2^k < k! \quad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N}_4 : P(k) \Longrightarrow P(k+1)$.

$$\begin{aligned} P(k+1) \equiv\ & 2^{k+1} = 2 \cdot 2^k <^{\mathrm{HI}} 2 \cdot k! \\ & < (k+1) \cdot k! = (k+1)! \end{aligned}$$

Se cumple que $k + 1 > 2$, pues $k \geq 4$ ✓ ■

- **Ejercicio 1.16:** Demostrar que se cumple $\forall n \in \mathbb{N} : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv \left(1 + \frac{1}{3}\right)^n \geq 1 + \frac{n}{3}$$

Demostración

Razonamos por **inducción sobre** $\boldsymbol{n} \in \mathbb{N}$:

- **Caso base:** $n = 0$

$$P(0) \equiv \left(1 + \tfrac{1}{3}\right)^0 = 1 \geq 1 = 1 + 0 = 1 + \tfrac{0}{3} \qquad \checkmark$$

Se cumple $P(0)$.

- **Paso inductivo:** $n > 0$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple

$$P(k) \equiv \left(1 + \tfrac{1}{3}\right)^k \geq 1 + \tfrac{k}{3} \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple $P(k+1)$, es decir, $\forall k \in \mathbb{N} : P(k) \Longrightarrow P(k+1)$.

Ejemplo 9 (Continuación)

En concreto, tenemos que probar que se cumple

$$P(k+1) \equiv \left(1+\frac{1}{3}\right)^{k+1} \geq 1+\frac{k+1}{3}$$

En efecto

$$P(k+1) \equiv \left(1+\frac{1}{3}\right)^{k+1} =$$

$$\left(1+\frac{1}{3}\right)^{k} \cdot \left(1+\frac{1}{3}\right) \geq^{\text{HI}}$$

$$\left(1+\frac{k}{3}\right) \cdot \left(1+\frac{1}{3}\right) =$$

$$\left(1+\frac{k}{3}\right) \cdot 1 + \left(1+\frac{k}{3}\right) \cdot \frac{1}{3} =$$

$$\left(1+\frac{k}{3}\right) + \frac{1}{3} + \frac{k}{9} \geq$$

Como $k \geq 0$, también se cumple que $\frac{k}{9} \geq 0$

$$\left(1+\frac{k}{3}\right) + \frac{1}{3} + 0 =$$

$$\left(1+\frac{k}{3}\right) + \frac{1}{3} =$$

$$1 + \left(\frac{k}{3} + \frac{1}{3}\right) =$$

$$1+\frac{k+1}{3}$$

✓ ■

Ejemplo 10

- **Ejercicio 1.16:** Demostrar que se cumple $\forall n \in \mathbb{N} : P(n)$, siendo $P(n)$ la siguiente propiedad:

$$P(n) \equiv 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$$

Demostración

Demostramos que se verifica

$$P(n) \equiv \sum_{i=1}^{2^n} \frac{1}{i} \geq 1 + \frac{n}{2}$$

razonando por **inducción sobre $n \in \mathbb{N}$**:

- **Caso base:** $n = 0$

$$P(0) \equiv \sum_{i=1}^{2^0} \frac{1}{i} = \sum_{i=1}^{1} \frac{1}{i} = \frac{1}{1} = 1 \geq 1 = 1 + 0 = 1 + \frac{0}{2} \quad \checkmark$$

Se cumple $P(0)$.

Ejemplo 10 (Continuación)

- **Paso inductivo:** $n > 0$

Supongamos, por **Hipótesis de Inducción** $(\mathbf{HI})$, que para todo $k \geq 0$ se cumple

$$P(k) \equiv \sum_{i=1}^{2^k} \frac{1}{i} \geq 1 + \frac{k}{2} \qquad (\mathrm{HI})$$

Apoyándonos en la (HI), probamos que se cumple

$$P(k+1) \equiv \sum_{i=1}^{2^{k+1}} \frac{1}{i} \geq 1 + \frac{k+1}{2}$$

$$2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

En efecto:

$$P(k+1) \equiv \sum_{i=1}^{2^{k+1}} \frac{1}{i} = \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k}\right) + \left(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \frac{1}{2^k+3} + \cdots + \frac{1}{2^k+2^k}\right) =$$

$$\sum_{i=1}^{2^k} \frac{1}{i} + \sum_{j=1}^{2^k} \frac{1}{2^k+j} \geq^{\mathrm{HI}} 1 + \frac{k}{2} + \sum_{j=1}^{2^k} \frac{1}{2^k+j} \geq$$

Suma descendiente de 2^k sumandos:

$$\frac{1}{2^k+1} \geq \frac{1}{2^k+2} \geq \cdots \geq \frac{1}{2^k+2^k}$$

Luego

$$\sum_{j=1}^{2^k} \frac{1}{2^k+j} = \frac{1}{2^k+1} + \cdots + \frac{1}{2^k+2^k} \geq \frac{1}{2^k+2^k} + \cdots + \frac{1}{2^k+2^k} = \left(\frac{1}{2^k+2^k}\right) \cdot 2^k$$

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

$$1 + \frac{k}{2} + \frac{1}{2} = 1 + \frac{k+1}{2} \qquad \checkmark$$

■

- En ocasiones, el principio de inducción que hemos visto no es suficiente para probar propiedades que dependen de valores anteriores. Veamos un ejemplo:

$P(n) \equiv$ El producto de n números naturales requiere $n-1$ multiplicaciones

Razonamos por inducción sobre $n \geq 1$ para demostrar que se cumple $\forall n \in \mathbb{N}_1 : P(n)$.

- **Caso base:** $n = 1$

$P(1) \equiv$ El producto de 1 número natural requiere 0 multiplicaciones ✓

- **Paso inductivo:** $n > 1$

Supongamos, por **Hipótesis de Inducción (HI)**, que para todo $k \geq 1$ se cumple:

$P(k) \equiv$ El producto de k números naturales requiere $k-1$ multiplicaciones **(HI)**

Apoyándonos en la **(HI)**, probamos que se cumple:

$P(k+1) \equiv$ El producto de $k+1$ números naturales requiere k multiplicaciones

Consideramos el producto de $k+1$ números naturales:

$$a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1} = (a_1 \cdot a_2 \cdot \cdots \cdot a_k) \cdot a_{k+1}$$

Por **(HI)**, para realizar el producto de los k números naturales $a_1 \cdot a_2 \cdot \cdots \cdot a_k$, se necesitan $k-1$ multiplicaciones, y para realizar la última multiplicación $\cdots a_k) \cdot a_{k+1}$ se necesita una multiplicación más. En total, se necesitan $(k-1)+1 = k$ multiplicaciones para realizar el producto de $k+1$ números $a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1}$. Por tanto, se cumple la propiedad.

Ahora bien, ¿por qué tiene que ser la última multiplicación que se haga en el producto $a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1}$ la que se encuentra situada más a la derecha? En general, la última multiplicación que hagamos podría ser otra cualquiera:

$$a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1} = (a_1 \cdot a_2 \cdot \cdots \cdot a_l) \cdot (a_{l+1} \cdot a_{l+2} \cdot \cdots \cdot a_{k+1})$$

- En este caso, $a_1 \cdot a_2 \cdot \cdots \cdot a_l$ es el producto de l números naturales, donde l puede ser menor que k. Por lo tanto, no se puede aplicar la **(HI)**.

- Del mismo modo, $a_{l+1} \cdot a_{l+2} \cdot \cdots \cdot a_{k+1}$ es el producto de $(k+1)-(l+1)+1 = k-l+1$ números naturales, donde $k-l+1$ también podría ser menor que k, luego tampoco podríamos aplicar la **(HI)**.

Para poder aplicar la **(HI)** es obligatorio que el producto sea de exactamente k números naturales, y no una cantidad menor. Por eso no podemos aplicar la **(HI)** en estos casos.

- La solución consiste en fortalecer la **(HI)** para que la propiedad se pueda cumplir para todos los valores anteriores a $k+1$, no solo para k.

- Esta hipótesis se denomina **Hipótesis Inducción Completa (HIC)**:

  (HIC) El producto de l números naturales requiere $l-1$ multiplicaciones, para todo $1 \leq l \leq k$. Es decir, se cumple $P(l)$ para cualquier $1 \leq l \leq k$.

Ahora ya, por **(HIC)**, para realizar el producto de $k+1$ números naturales

$$a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1} = (a_1 \cdot a_2 \cdot \cdots \cdot a_l) \cdot (a_{l+1} \cdot a_{l+2} \cdot \cdots \cdot a_{k+1})$$

- Se requieren $l-1$ multiplicaciones para realizar el producto $a_1 \cdot a_2 \cdot \cdots \cdot a_l$ de $1 \leq l \leq k$ números naturales.

- Se requieren $k-l$ multiplicaciones para realizar el producto $a_{l+1} \cdot a_{l+2} \cdot \cdots \cdot a_{k+1}$ de $1 \leq k-l+1 \leq k$ números naturales.

- Además, hemos de contar la última multiplicación $\cdots a_l) \cdot (a_{l+1} \cdots$

En total, tenemos que realizar $(l-1)+(k-l)+1 = k$ multiplicaciones. ✓

Se cumple así el resultado, no solo ya para el caso particular $l = k$ y $k-l+1 = 1$ que representa $a_1 \cdot a_2 \cdot \cdots \cdot a_k \cdot a_{k+1} = (a_1 \cdot a_2 \cdot \cdots \cdot a_k) \cdot a_{k+1}$, sino que queda probado para cualquier otro caso.

- En general, para demostrar que la propiedad $P(n)$ se verifica para todo $n \geq m$, es decir:

$$\forall n \in \mathbb{N}_m : P(n)$$

si la propiedad depende de los valores anteriores (más allá del exactamente valor anterior), razonamos por **inducción completa** sobre $n \geq m$:

  - **Casos base:** $n = m, n = m + 1, n = m + 2, \dots, n = m + i$

    Puede que sea necesario probar varios casos: $P(m), P(m + 1), P(m + 2), \dots, P(m + i)$.

  - **Paso inductivo:** $n > m + i$

    Suponiendo que se verifica la **Hipótesis de Inducción Completa (HIC)**:

    (HIC) Para cualquier $k > m + i$ se verifica $\forall\, m \leq l < k : P(l)$.

    Demostramos que se verifica $P(k)$ (**caso inductivo**).

- Si usamos la inducción como hemos visto antes, se denominará **principio de inducción simple**, para distinguirlo de esta nueva versión.

Ejemplo 1 (Inducción Completa)

- **Ejercicio 1.30:** Demostrar que se verifica $\forall n \in \mathbb{N}_{14} : P(n)$, siendo $P(n)$ la propiedad

$$P(n) \equiv \exists a, b \in \mathbb{N} : n = 3a + 8b$$

Razonamos por **inducción completa** sobre $n \geq 14$:

- **Casos base:** $n = 14, n = 15, n = 16$

$P(14) \equiv \exists a, b \in \mathbb{N} : 14 = 3a + 8b$ ✓ $(a = 2 \text{ y } b = 1)$
$P(15) \equiv \exists a, b \in \mathbb{N} : 15 = 3a + 8b$ ✓ $(a = 5 \text{ y } b = 0)$
$P(16) \equiv \exists a, b \in \mathbb{N} : 16 = 3a + 8b$ ✓ $(a = 0 \text{ y } b = 2)$

- **Paso inductivo:** $n \geq 17$ (es decir, $n > 16$)

(HIC) Para cualquier $k \geq 17$ se verifica $\forall\, 14 \leq l < k : P(l) \equiv \exists a', b' \in \mathbb{N} : l = 3a' + 8b'$.

Apoyándonos en la **(HIC)**, probamos que se cumple $P(k) \equiv \exists a, b \in \mathbb{N} : k = 3a + 8b$.

$$k = (\boldsymbol{k - 3}) + 3 =^{\mathbf{HIC}} (\boldsymbol{3a' + 8b'}) + 3 = 3 \cdot (a' + 1) + 8b' = 3a + 8b,$$

con $a = a' + 1$ y $b = b'$ números naturales.

- Como $k \geq 17$, se verifica que $14 \leq k - 3 < k$, luego podemos aplicar la **(HIC)** para $l = k - 3$. Se cumple así $P(l) \equiv P(k - 3) \equiv \exists a', b' \in \mathbb{N} : k - 3 = 3a' + 8b'$.
- Para que $14 \leq k - 3 < k$ y hayamos podido aplicar la **(HIC)**, se necesita pedir que $k \geq 17$. Por eso hemos tenido que probar los casos base: $n = 14, n = 15, n = 16$. ■

Ejemplo 1 (Inducción Simple)

- **Ejercicio 1.30:** Demostrar que se verifica $\forall n \in \mathbb{N}_{14} : P(n)$, siendo $P(n)$ la propiedad

$$P(n) \equiv \exists a, b \in \mathbb{N} : n = 3a + 8b$$

- Razonamos por **inducción simple** sobre $n \geq 14$:
  - **Casos base:** $n = 14$

    $P(14) \equiv \exists a, b \in \mathbb{N} : 14 = 3a + 8b$ ✓ $(a = 2 \text{ y } b = 1)$

  - **Paso inductivo:** $n > 14$

    (HI) Se verifica $P(k) \equiv \exists a', b' \in \mathbb{N} : k = 3a' + 8b'$, para cualquier $k \geq 14$

    Probamos que se verifica $P(k+1) \equiv \exists a, b \in \mathbb{N} : k + 1 = 3a + 8b$.

    $\boldsymbol{k} + 1 =^{\mathbf{HI}} \boldsymbol{3a'} + \boldsymbol{8b'} + 1 = 3a' + 8b' + 9 - 8 = 3 \cdot (a' + 3) + 8 \cdot (b' - 1) = 3a + 8b$

    donde $a = a' + 3$ es un número natural, y $b = b' - 1$ solo es natural si $b' > 0$.

    Hemos probado el resultado para el caso en el que $b' > 0$. Nos queda el caso $b' = 0$:

$$k+1 =^{\mathbf{HI}} 3a' + 8b' + 1 = 3a' + 8 \cdot 0 + 16 - 15 = 3 \cdot (a' - 5) + 8 \cdot 2 = 3a + 8b$$

Ahora $b = 2$ sí es un número natural, pero $a = a' - 5$ solo es natural para $a' \geq 5$.

Sin embargo, como $k =^{\mathbf{HI}} 3a' + 8b' = 3a' + 8 \cdot 0 = 3a'$ y $k \geq 14$, se cumple que $a' \geq 5$.

Por tanto, se cumple el resultado en todos los casos. ✓

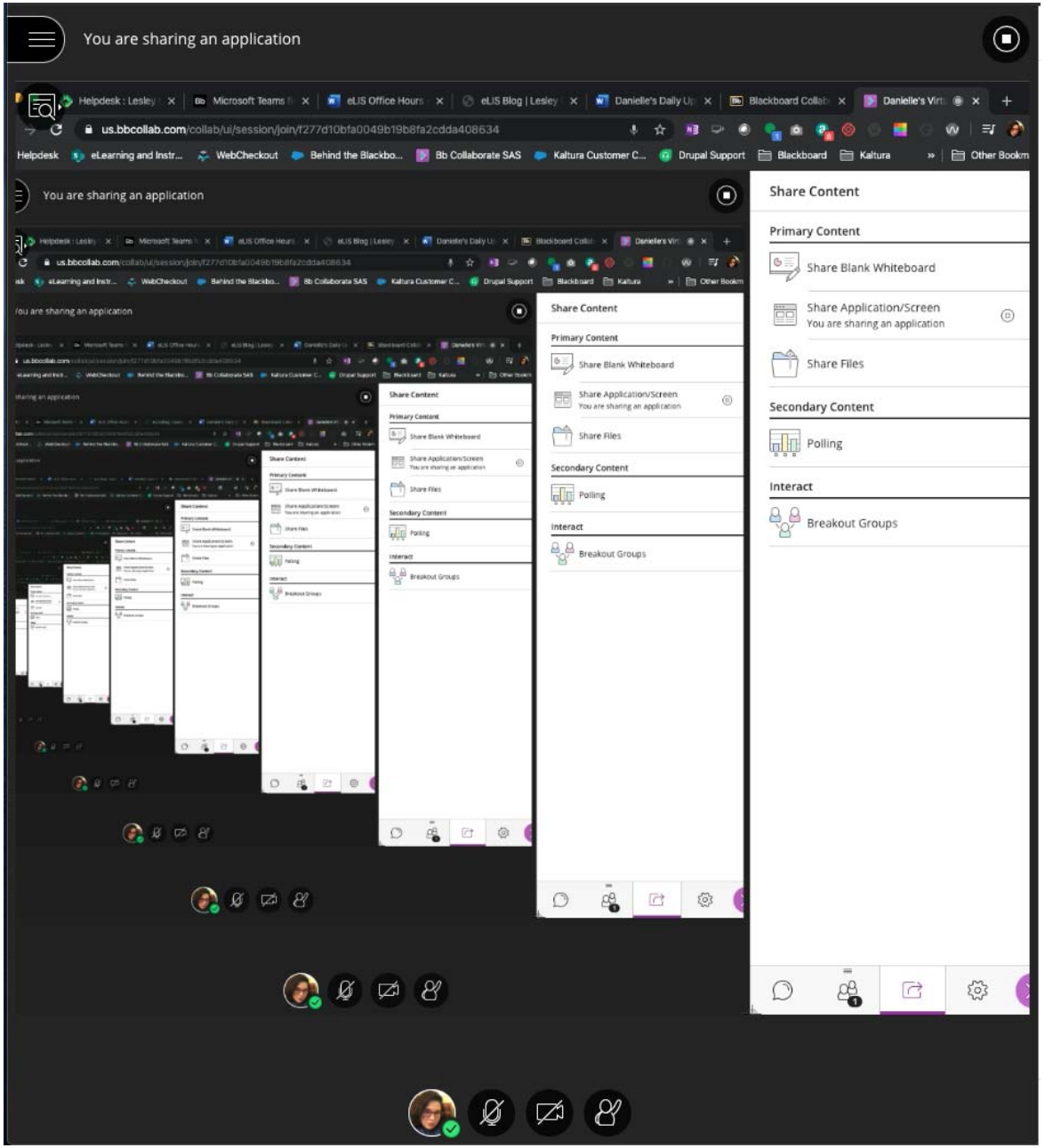
■

- **Ejercicio 1.28:** Demostrar que se verifica $\forall n \in \mathbb{N}_{24} : P(n)$, siendo $P(n)$ la propiedad

$$P(n) \equiv \exists a, b \in \mathbb{N} : n = 5a + 6b$$

Definiciones Recursivas

Definiciones Recursivas



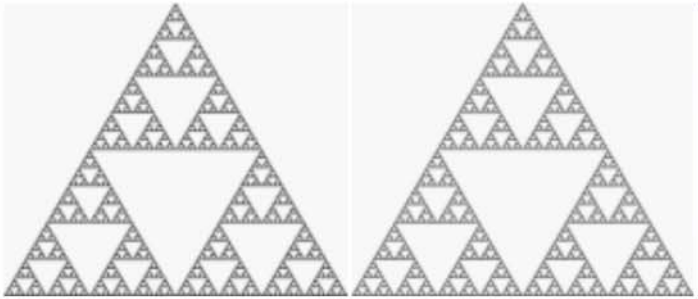
Google

recursión

Todo Vídeos Imágenes Shopping Libros Más Configuración Herramientas

Aproximadamente 150.000 resultados (0,51 segundos)

Quizás quisiste decir: ***recursión***



$$\begin{aligned} 3! &= 3 \cdot (3-1)! \\ &= 3 \cdot 2! \\ &= 3 \cdot 2 \cdot (2-1)! \\ &= 3 \cdot 2 \cdot 1! \\ &= 3 \cdot 2 \cdot 1 \cdot (1-1)! \\ &= 3 \cdot 2 \cdot 1 \cdot 0! \\ &= 3 \cdot 2 \cdot 1 \cdot 1 \\ &= 6 \end{aligned}$$

Ver todo

Recursión o recursividad es la forma en la cual se especifica un proceso basado en su propia definición. La **recursión** tiene esta característica discernible en términos de autorreferencialidad, autopoiesis, fractalidad, o, en otras palabras, construcción a partir de un mismo tipo.

es.wikipedia.org › wiki › Recursión

Recursión - Wikipedia, la enciclopedia libre

Información sobre los fragmentos destacados Enviar comentarios

- Una función $f : \mathbb{N}_m \longrightarrow B$ está *definida recursivamente* sobre $\mathbb{N}_m$ si para cada $n \in \mathbb{N}_m$ verifica que, o bien

  1) f está definida explícitamente por un valor $b \in B$ **(Caso Base)**, o bien
  2) f se define recurriendo al propio valor de f para algún o algunos valores anteriores de n : $f(n-1), f(n-2), \ldots$ **(Caso Recursivo)**.

$$\begin{cases} f(m) = b & \textbf{(Caso Base, CB)} \\ f(n) = exp(n, f(n-1), f(n-2), \cdots) \quad \text{si} \quad n > m & \textbf{(Caso Recursivo, CR)} \end{cases}$$

Si B es el conjunto $\mathbb{N}$ se dice que la función es una **sucesión** definida recursivamente.

- **Ejemplo 1 (recursión simple)**

La función *factorial*

$$fact : \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \mapsto fact(n) = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$$

admite un definición recursiva sobre $\mathbb{N}$:

$$\begin{cases} fact(0) = 1 & \textbf{(CB)} \\ fact(n) = n \cdot fact(n-1) \quad \text{si} \quad n \geq 1 & \textbf{(CR)} \end{cases}$$

- Ejemplo de cálculo recursivo:

$$
\begin{aligned}
\boldsymbol{fact}(\mathbf{4}) &=^{\mathbf{CR}} 4 \cdot \boldsymbol{fact}(\mathbf{3}) \\
&=^{\mathbf{CR}} 4 \cdot 3 \cdot \boldsymbol{fact}(\mathbf{2}) \\
&=^{\mathbf{CR}} 4 \cdot 3 \cdot 2 \cdot \boldsymbol{fact}(\mathbf{1}) \\
&=^{\mathbf{CR}} 4 \cdot 3 \cdot 2 \cdot 1 \cdot \boldsymbol{fact}(\mathbf{0}) \\
&=^{\mathbf{CB}} 4 \cdot 3 \cdot 2 \cdot 1 \cdot \mathbf{1} \\
&= 24 \\
&= 4!
\end{aligned}
$$

$$
\begin{cases}
fact(0) = 1 & \textbf{(CB)} \\
fact(n) = n \cdot fact(n-1) \quad \text{si} \quad n \geq 1 & \textbf{(CR)}
\end{cases}
$$

- Implementación en el lenguaje de programación C :

```
int fact ( int n ) {    // n >= 0
        int resultado ;
        if ( n == 0 ) {    // Caso Base (n = 0)
                resultado = 1 ;
        }
        else {    // Caso Recursivo (n >= 1)
                resultado = n * fact(n – 1) ;
        }
        return resultado ;
}
```

- Podemos demostrar por inducción propiedades sobre los números naturales que incluyan funciones definidas recursivamente. Por ejemplo, demostramos la siguiente propiedad:

$$fact(n) = n! \quad \text{para todo } n \in \mathbb{N}$$

Razonamos por **inducción simple** sobre $n \in \mathbb{N}$:

- **Caso base:** $n = 0$

  $\boldsymbol{fact(0)} =^{\mathbf{CB}} \boldsymbol{1} = 0!$

- **Paso inductivo:** $n > 0$

  (HI) $fact(k) = k!$ para todo $k \geq 0$

  ¿Se cumple $fact(k+1) = (k+1)!$? En efecto:

  $\boldsymbol{fact(k+1)} =^{\mathbf{CR}} (k+1) \cdot \boldsymbol{fact(k)} =^{\mathbf{HI}} (k+1) \cdot \boldsymbol{k}! = (k+1)!$

  Como $k \geq 0$ se tiene que $k + 1 \geq 1$, por lo que podemos aplicar el **caso recursivo** a $fact(k+1)$.

$$\begin{cases} fact(0) = 1 & \textbf{(CB)} \\ fact(n) = n \cdot fact(n-1) \quad \text{si} \quad n \geq 1 & \textbf{(CR)} \end{cases}$$

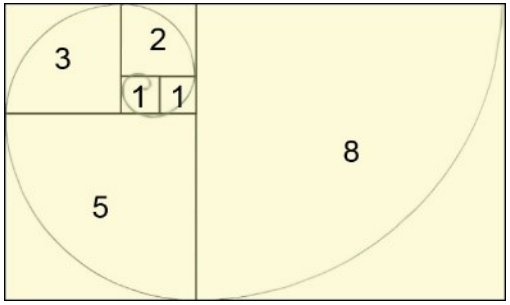
- **Ejemplo 2 (recursión múltiple)**

La función de *fibonacci*

$$fib : \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \mapsto fib(n) = 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

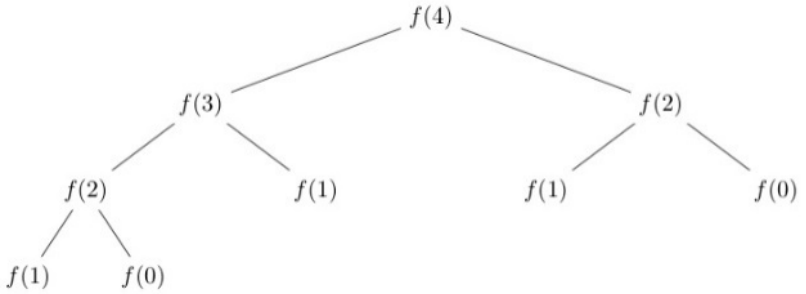
admite un definición recursiva sobre $\mathbb{N}$:

$$\begin{cases} fib(0) = 0 & \textbf{(CB}_1\textbf{)} \\ fib(1) = 1 & \textbf{(CB}_2\textbf{)} \\ fib(n) = fib(n-1) + fib(n-2) \quad \text{si} \quad n \geq 2 & \textbf{(CR)} \end{cases}$$



Ejemplo de cálculo recursivo:

$$\begin{aligned} \boldsymbol{fib(4)} &=^{\textbf{CR}} \boldsymbol{fib(3)} + \boldsymbol{fib(2)} \\ &=^{\textbf{CR}} (\boldsymbol{fib(2)} + fib(1)) + (fib(1) + fib(0)) \\ &=^{\textbf{CR}} \big(fib(1) + fib(0) + fib(1)\big) + \big(fib(1) + fib(0)\big) \\ &= \quad 3 \cdot \boldsymbol{fib(1)} + 2 \cdot fib(0) \\ &=^{\textbf{CB}_2} 3 \cdot \mathbf{1} + 2 \cdot \boldsymbol{fib(0)} \\ &=^{\textbf{CB}_1} 3 \cdot 1 + 2 \cdot \mathbf{0} \\ &= \quad 3 + 0 \\ &= \quad 3 \end{aligned}$$



- Implementación en el lenguaje de programación C :

$$\begin{cases} fib(0) = 0 & \textbf{(CB}_1\textbf{)} \\ fib(1) = 1 & \textbf{(CB}_2\textbf{)} \\ fib(n) = fib(n-1) + fib(n-2) \quad \text{si} \quad n \geq 2 & \textbf{(CR)} \end{cases}$$

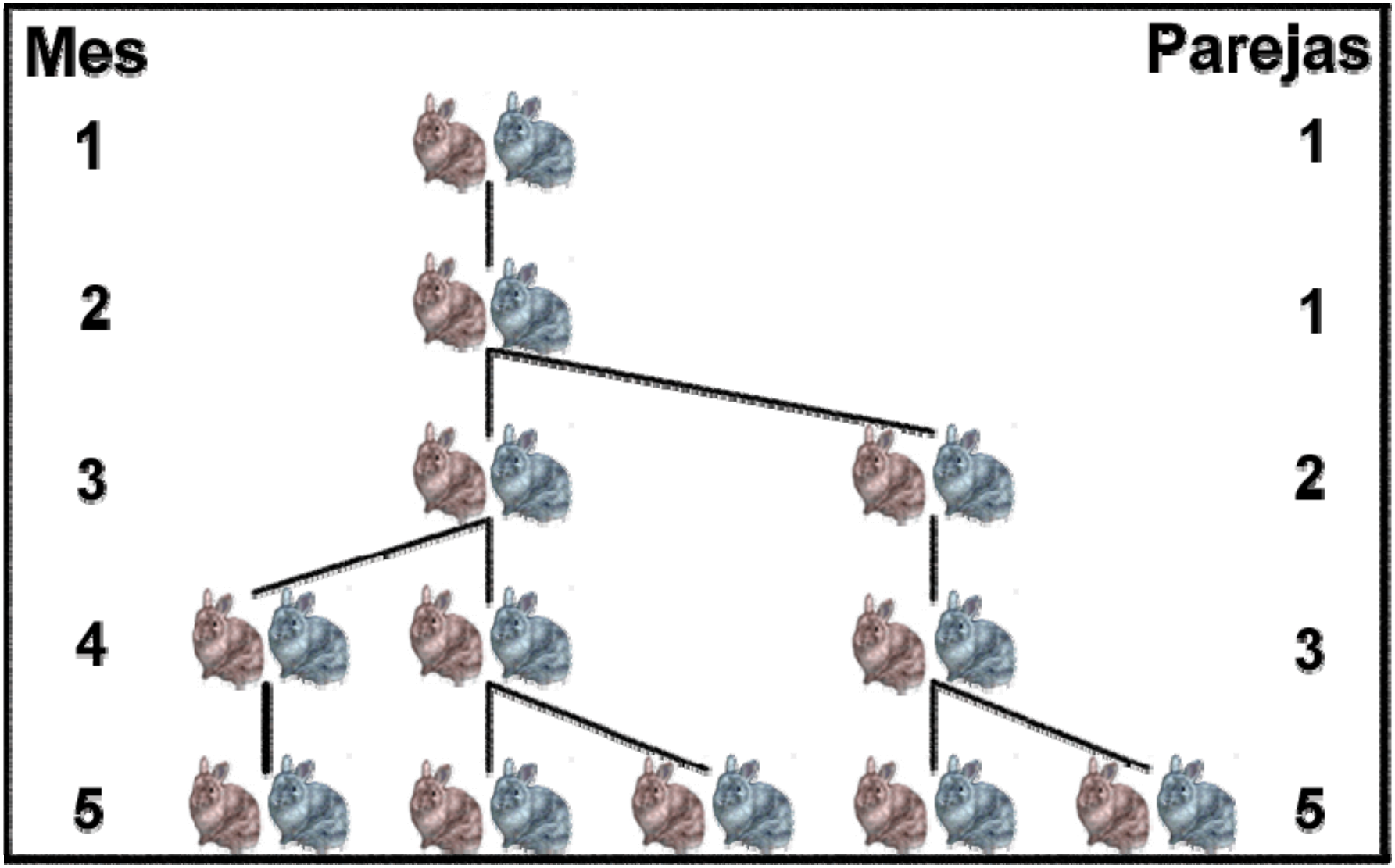
```
int fib ( int n ) {     // n >= 0
        int resultado ;
        if ( n == 0 ) {     // Caso Base 1 (n = 0)
                resultado = 0 ;
        }

        else if ( n == 1 ) {     // Caso Base 2 (n = 1)
                resultado = 1 ;
        }

        else {     // Caso Recursivo (n >= 2)
               resultado = fib(n – 1) + fib(n – 2) ;
        }

        return resultado ;

}
```


Mes
Parejas
1
1
2
1
3
2
4
3
5
5

- **Ejercicio 1.55:** Demostrar que se verifica $fib(n) \leq n!$ para todo $n \geq 0$.

Razonamos por **inducción completa** sobre $n \geq 0$:

- **Casos base:** $n = 0$ y $n = 1$

¿ $fib(0) \leq 0!$? Sí: $\boldsymbol{fib(0)} =^{\mathbf{CB_1}} \mathbf{0} \leq 1 = 0!$
¿ $fib(1) \leq 1!$? Sí: $\boldsymbol{fib(1)} =^{\mathbf{CB_2}} \mathbf{1} \leq 1 = 1!$

$$\begin{cases} fib(0) = 0 & \textbf{(CB}_1\textbf{)} \\ fib(1) = 1 & \textbf{(CB}_2\textbf{)} \\ fib(n) = fib(n-1) + fib(n-2) \quad \text{si} \quad n \geq 2 & \textbf{(CR)} \end{cases}$$

- **Paso inductivo:** $n \geq 2$

(HIC) Para cada $k \geq 2$ se verifica: $fib(l) \leq l!$ para todo $0 \leq l < k$.

Demostramos que se verifica $fib(k) \leq k!$ para $k \geq 2$:

$$\begin{aligned} \boldsymbol{fib(k)} &=^{\mathbf{CR}} \boldsymbol{fib(k-1) + fib(k-2)} && \text{Se puede aplicar \textbf{CR} pues } k \geq 2 \\ &\leq^{\mathbf{HIC}} \boldsymbol{(k-1)! + (k-2)!} && \text{Se puede aplicar \textbf{HIC} pues } 0 \leq k-1 < k \text{ y} \\ & && 0 \leq k-2 < k \text{ ya que } k \geq 2 \\ &= (k-1) \cdot (k-2)! + (k-2)! \\ &= (k-1+1) \cdot (k-2)! \\ &= k \cdot (k-2)! \\ &= k \cdot 1 \cdot (k-2)! && \text{Como } k \geq 2 \text{ se tiene que } k-1 \geq 1 \\ &\leq k \cdot (k-1) \cdot (k-2)! \\ &= k! \end{aligned}$$

- **Ejercicio 1.54:** Demostrar que se verifica $fib^2(0) + fib^2(1) + \cdots + fib^2(n) = fib(n) \cdot fib(n+1)$ para todo $n \geq 3$.

Razonamos por **inducción simple** sobre $n \geq 3$ que se verifica

$$\sum_{i=0}^{n} fib^2(i) = fib(n) \cdot fib(n+1)$$

- **Caso base:** $n = 3$

$$\sum_{i=0}^{3} fib^2(i) = fib^2(0) + fib^2(1) + fib^2(2) + fib^2(3) = 0^2 + 1^2 + 1^2 + 2^2 = 6$$

$$fib(3) \cdot fib(4) = 2 \cdot 3 = 6 \longleftarrow fib(n) = 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

- **Paso inductivo:** $n > 3$

(HI) Para cada $k \geq 3$ se verifica

$$\sum_{i=0}^{k} fib^2(i) = fib(k) \cdot fib(k+1)$$

Demostramos que se verifica

$$\sum_{i=0}^{k+1} fib^2(i) = fib(k+1) \cdot fib(k+2)$$

En efecto:

$$\sum_{i=0}^{k+1} fib^2(i) = \sum_{i=0}^{k} fib^2(i) + fib^2(k+1)$$

Se puede hacer la descomposición pues $k+1 \geq 1$, es decir, $k \geq 0$, ya que $k \geq 3$ por **HI**.

$$\begin{aligned} &=^{\mathbf{HI}} fib(k) \cdot fib(k+1) + fib(k+1) \cdot fib(k+1) \\ &= fib(k+1) \cdot \big(fib(k) + fib(k+1)\big) \\ &=^{\mathbf{CR}} fib(k+1) \cdot fib(k+2) \end{aligned}$$

Se puede aplicar **CR** pues $k+2 \geq 2$, es decir, $k \geq 0$, ya que $k \geq 3$ por **HI**.

$$\begin{cases} fib(0) = 0 & \textbf{(CB}_1\textbf{)} \\ fib(1) = 1 & \textbf{(CB}_2\textbf{)} \\ fib(n) = fib(n-1) + fib(n-2) \quad \text{si} \quad n \geq 2 & \textbf{(CR)} \end{cases}$$

- **Ejercicio 1.57:** Dada la siguiente sucesión definida recursivamente:

$$\begin{cases} s_2 = 20 & \textbf{(CB)} \\ s_n = 5 \cdot 4^{n-1} - s_{n-1} \quad \text{si} \quad n \geq 3 & \textbf{(CR)} \end{cases}$$

Demostrar que se verifica $s_n = 4 \cdot (-1)^n + 4^n$ para todo $n \geq 2$.

Razonamos por **inducción simple** sobre $n \geq 2$:

- **Caso base:** $n = 2$

$$s_2 =^{\mathbf{CB}} 20 = 4 + 16 = 4 \cdot 1 + 4^2 = 4 \cdot (-1)^2 + 4^2$$

- **Paso inductivo:** $n > 2$

(HI) Para cada $k \geq 2$ se verifica $s_k = 4 \cdot (-1)^k + 4^k$.

Demostramos que se verifica $s_{k+1} = 4 \cdot (-1)^{k+1} + 4^{k+1}$ para $k \geq 2$:

$$\begin{aligned} s_{k+1} &=^{\mathbf{CR}} 5 \cdot 4^k - s_k \\ &=^{\mathbf{HI}} 5 \cdot 4^k - \left(4 \cdot (-1)^k + 4^k\right) \\ &= 5 \cdot 4^k + 4 \cdot (-1)^{k+1} - 4^k \\ &= (4+1) \cdot 4^k + 4 \cdot (-1)^{k+1} - 4^k \\ &= 4 \cdot 4^k + 4^k + 4 \cdot (-1)^{k+1} - 4^k \\ &= 4 \cdot (-1)^{k+1} + 4^{k+1} \end{aligned}$$

Se puede aplicar **CR** pues $k + 1 \geq 3$ al ser $k \geq 2$

- **Ejercicio 1.58:** Dada la siguiente sucesión definida recursivamente:

$$\begin{cases} s_0 = 2 & \textbf{(CB}_1\textbf{)} \\ s_1 = 1 & \textbf{(CB}_2\textbf{)} \\ s_n = s_{n-1} + 2s_{n-2} \quad \text{si} \quad n \geq 2 & \textbf{(CR)} \end{cases}$$

Demostrar que se verifica $s_n = 2^n + (-1)^n$ para todo $n \in \mathbb{N}$.

Razonamos por **inducción completa** sobre $n \geq 0$:

- **Casos base:** $n = 0$ y $n = 1$

$$s_0 =^{\mathbf{CB_1}} 2 = 1 + 1 = 2^0 + (-1)^2$$
$$s_1 =^{\mathbf{CB_2}} 1 = 2 - 1 = 2^1 + (-1)^1$$

- **Paso inductivo:** $n \geq 2$

(HIC) Para cada $k \geq 2$ se verifica: $s_l = 2^l + (-1)^l$ para todo $0 \leq l < k$.

Demostramos que se verifica $s_k = 2^k + (-1)^k$ para $k \geq 2$:

$$s_k =^{\mathbf{CR}} s_{k-1} + 2s_{k-2}$$
$$=^{\mathbf{HI}} \left(2^{k-1} + (-1)^{k-1}\right) + 2 \cdot \left(2^{k-2} + (-1)^{k-2}\right)$$

Se puede aplicar **CR** pues $k \geq 2$

Se puede aplicar **HIC** pues $0 \leq k - 1 < k$ y $0 \leq k - 2 < k$ ya que $k \geq 2$

$$s_k =^{\mathbf{CR}} s_{k-1} + 2s_{k-2}$$
$$=^{\mathbf{HI}} \left(2^{k-1} + (-1)^{k-1}\right) + 2 \cdot \left(2^{k-2} + (-1)^{k-2}\right)$$

Se puede aplicar **CR** pues $k \geq 2$

Se puede aplicar **HIC** pues $0 \leq k-1 < k$ y $0 \leq k-2 < k$ ya que $k \geq 2$

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

- **Ejercicio 1.59:** Dada la siguiente sucesión definida recursivamente:

$$\begin{cases} s_1 = 3 & \textbf{(CB}_1\textbf{)} \\ s_2 = 5 & \textbf{(CB}_2\textbf{)} \\ s_n = 3s_{n-1} - 2s_{n-2} \quad \text{si} \quad n \geq 3 & \textbf{(CR)} \end{cases}$$

Demostrar que se verifica $s_n = 2^n + 1$, para todo $n \geq 1$.

Razonamos por **inducción completa** sobre $n \geq 1$:

- **Casos base:** $n = 1$ y $n = 2$

$$s_1 =^{\mathbf{CB_1}} 3 = 2 + 1 = 2^1 + 1$$
$$s_2 =^{\mathbf{CB_2}} 5 = 4 + 1 = 2^2 + 1$$

- **Paso inductivo:** $n \geq 3$

(HIC) Para cada $k \geq 3$ se verifica: $s_l = 2^l + 1$ para todo $1 \leq l < k$.

Demostramos que se verifica $s_k = 2^k + 1$ para $k \geq 3$:

$$\begin{aligned} s_k &=^{\mathbf{CR}} 3s_{k-1} - 2s_{k-2} \\ &=^{\mathbf{HI}} 3\left(2^{k-1} + 1\right) - 2\left(2^{k-2} + 1\right) \end{aligned}$$

Se puede aplicar **CR** pues $k \geq 3$
Se puede aplicar **HIC** pues $1 \leq k - 1 < k$ y $1 \leq k - 2 < k$ ya que $k \geq 3$

$s_k =^{\mathbf{CR}} 3s_{k-1} - 2s_{k-2}$ Se puede aplicar **CR** pues $k \geq 3$

$=^{\mathbf{HI}} 3\left(2^{k-1}+1\right) - 2\left(2^{k-2}+1\right)$ Se puede aplicar **HIC** pues $1 \leq k-1 < k$ y $1 \leq k-2 < k$ ya que $k \geq 3$

$= 3 \cdot 2^{k-1} + 3 - 2 \cdot 2^{k-2} - 2$
$= 3 \cdot 2^{k-1} - 2^{k-1} + 1$
$= (3-1) \cdot 2^{k-1} + 1$
$= 2 \cdot 2^{k-1} + 1$
$= 2^k + 1$

- La **Teoría de Números** es la **rama de las matemáticas** que estudia las propiedades de los números, en particular de los **números enteros**

$$\mathbb{Z} = \{\cdots -\mathbf{3}, -\mathbf{2}, -\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3} \cdots\}$$

- En este tema estudiaremos aquellos conceptos de la **Teoría de Números** más relacionados con la **informática**:
  - **División entera. Múltiplos y divisores.**
  - **Máximo común divisor y mínimo común múltiplo.**
  - **Algoritmo de Euclides y Teorema de Bézout.**
  - **Números primos.**
  - **Congruencias y aritmética modular.**

- **Teorema de la División Entera**

  Dados $a, b \in \mathbb{Z}$ con $a \geq 0$ y $b > 0$, existen dos únicos números enteros $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$.

  Demostración

  Comenzamos demostrando la **existencia**:

  Existen $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$, para todo $a \geq 0$ y $b > 0$.

  Razonamos por **inducción completa** sobre $a \geq 0$:

  - **Caso base:** $a \leq b$
    - Si $a < b$: $a = b \cdot 0 + a$ y $0 \leq a < b$. Luego $c = 0$ y $r = a$.
    - Si $a = b$: $a = b \cdot 1 + 0$ y $0 \leq 0 < b$. Luego $c = 1$ y $r = 0$.
  - **Paso inductivo:** $a > b$

    (HIC) Para todo $a > b$ se verifica:
    Existen $c', r' \in \mathbb{Z}$ tales que $l = b \cdot c' + r'$ y $0 \leq r' < b$, para todo $0 \leq l < a$.

    ¿ Existen $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$?

¿ Existen $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$?

Comenzamos observando que

$$a - b =^{\mathbf{HIC}} b \cdot c' + r' \text{ con } 0 \leq r' < b$$

Se puede aplicar la **HIC** pues $a > b$ y $b > 0$, luego $0 < a - b < a$ (tomamos $l = a - b$ en la **HIC**): Existen $c', r' \in \mathbb{Z}$ tales que $a - b = b \cdot c' + r'$ y $0 \leq r' < b$.

Operando $a - b = b \cdot c' + r'$ tenemos que

$$a = b \cdot c' + b + r'$$

que es lo mismo que decir

$$a = b \cdot (c' + 1) + r'$$

$$\begin{cases} div(a,b) = (0,a) & \text{si } a < b \\ div(a,b) = (1,0) & \text{si } a = b \\ div(a,b) = (c'+1, r') & \text{si } a > b \text{ siendo } div(a-b,b) = (c', r') \end{cases}$$

Con lo cual

$$a = b \cdot c + r$$

donde $c = c' + 1 \in \mathbb{Z}$, pues $c' \in \mathbb{Z}$ por **HIC**, y $r = r' \in \mathbb{Z}$, pues $r' \in \mathbb{Z}$ también por **HIC**.
Además: $0 \leq r < b$ pues $r = r'$ y se verifica $0 \leq r' < b$ también por **HIC**.

División Entera

$$\begin{cases} div(a,b) = (0,a) & \text{si } a < b \\ div(a,b) = (1,0) & \text{si } a = b \\ div(a,b) = (c'+1, r') & \text{si } a > b \text{ siendo } div(a-b,b) = (c',r') \end{cases}$$

```
( int, int ) div ( int a, int b ) {  // a >= b, b > 0

        int c, r ;

        if ( a < b ) {   // Caso base 1
                    c = 0 ;
                    r = a ;
        }
        else if ( a == b ) {   Caso base 2
                    c = 1 ;
                    r = 0 ;
        }
        else if ( a > b ) {   Caso recursivo
                    (c, r) = div(a – b, b) ;
                    c = c + 1 ;
        }
        return c, r ;
}
```

Por ejemplo, calculamos $div(7,4)$:

$$div(7-4,4) = div(3,4) = (0,3)$$

Luego

$$div(7,4) = (0+1,3) = (1,3)$$

Demostramos ahora la **unicidad**:

Los enteros $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$, para todo $a \geq 0$ y $b > 0$, son únicos.

Razonamos por **reducción al absurdo**: supongamos que no son únicos, es decir

$$a = b \cdot c_1 + r_1 \quad \text{con} \quad 0 \leq r_1 < b$$
$$a = b \cdot c_2 + r_2 \quad \text{con} \quad 0 \leq r_2 < b$$

y $c_1 \neq c_2$. **Distinguimos casos**: $c_1 > c_2$ y $c_1 < c_2$

- **Caso 1**: $c_1 > c_2$

$$a = b \cdot c_1 + r_1 = b \cdot c_1 + r_1 + (b \cdot c_2 - b \cdot c_2) =$$
$$b \cdot c_2 + b \cdot c_1 - b \cdot c_2 + r_1 = b \cdot c_2 + (c_1 - c_2) \cdot b + r_1$$

Como $a = b \cdot c_2 + r_2$ despejando r_2 se tiene $r_2 = a - b \cdot c_2$. Sustituyendo a por $a = b \cdot c_2 + (c_1 - c_2) \cdot b + r_1$ en $r_2 = a - b \cdot c_2$ se tiene:

$$r_2 = a - b \cdot c_2 = b \cdot c_2 + (c_1 - c_2) \cdot b + r_1 - b \cdot c_2 = \quad [\text{ Se elimina } b \cdot c_2 \text{ }]$$
$$(c_1 - c_2) \cdot b + r_1 \geq \quad [\text{ Como } c_1 > c_2 \text{ se tiene } c_1 - c_2 > 0, \text{ es decir, } c_1 - c_2 \geq 1 \text{ }]$$
$$1 \cdot b + r_1 \geq \quad [\text{ Como } 0 \leq r_1 \leq b \text{ se tiene } r_1 \geq 0 \text{ }]$$
$$b + 0 = b$$

Luego $r_2 \geq b$. Llegamos a **contradicción** pues $0 \leq r_2 < b$. Por tanto, este caso no puede darse.

- **Caso 2**: $c_1 < c_2$

  Razonando análogamente al **Caso 1**, llegamos a una nueva **contradicción**: $r_1 \geq b$, pero $0 \leq r_1 < b$. Luego este caso tampoco puede darse.

Luego, si suponemos que $c_1 \neq c_2$, llegamos a **contradicción**. Por tanto, $c_1 = c_2$. Pero entonces:

$$r_1 = a - b \cdot c_1 = a - b \cdot c_2 = r_2$$

Luego también $r_1 = r_2$. Así, $c_1 = c_2$ y $r_1 = r_2$, por lo que se tiene demostrada la unicidad. ■

- **Corolario 1**

Dados $a, b \in \mathbb{Z}$ con $b > 0$, existen únicos $c, r \in \mathbb{Z}$ con el mismo signo que a tales que $a = b \cdot c + r$ y $0 \leq |r| < b$.

Demostración

Si $a \geq 0$ se cumple directamente por el **Teorema de la División Entera**. Si $a < 0$ aplicamos el **Teorema de la División Entera** para $a' = -a$, pues $a' \geq 0$ y $b > 0$: existen únicos $c', r' \in \mathbb{Z}$ tales que $a' = b \cdot c' + r'$ con $0 \leq r' < b$. Ahora bien:

$$
\begin{aligned}
a' &= b \cdot c' + r' && \Longrightarrow && \text{[Por definición } a' = -a \text{]} \\
-a &= b \cdot c' + r' && \Longrightarrow \\
a &= -b \cdot c' - r' && \Longrightarrow \\
a &= b \cdot (-c') + (-r') && \Longrightarrow \\
a &= b \cdot c + r
\end{aligned}
$$

donde $c = -c' \in \mathbb{Z}$, pues $c' \in \mathbb{Z}$, y $r = -r' \in \mathbb{Z}$, pues $r' \in \mathbb{Z}$. Además:

$$
\begin{aligned}
0 \leq r' < b \quad &\Longrightarrow \quad \text{[Como } r' \geq 0 \text{ se verifica que } |-r'| = r' \text{]} \\
0 \leq |-r'| < b \quad &\Longrightarrow \quad \text{[Por definición } r = -r' \text{]} \\
0 \leq |r| < b
\end{aligned}
$$

Luego existen únicos $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq |r| < b$. ■

- **Ejemplo**

Para $a = -8$ y $b = 3$ se tiene que:

$-8 = 3 \cdot (-1) + (-5)$	pero no se verifica $0 \leq \|-5\| < 3$.
$-8 = 3 \cdot (-3) + 1$	pero no se verifica que $r = 1$ tenga el mismo signo que $a = -8$.
$-8 = 3 \cdot (-2) + (-2)$	se verifica que $0 \leq \|-2\| < 3$. Luego $c = -2$ y $r = -2$, con el mismo signo que $a = -8$.

- **Corolario 2**

  Dados $a, b \in \mathbb{Z}$ con $b > 0$, existen únicos $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$.

  Demostración

  Si $a \geq 0$ se cumple directamente por el **Teorema de la División Entera**. Si $a < 0$, por el **Corolario 1**: existen únicos $c', r' \in \mathbb{Z}$ tales que $a' = b \cdot c' + r'$ con $c' < 0$, $r' \leq 0$, y $0 \leq |r'| < b$.

  Distinguimos casos: $r' = 0$ y $r' < 0$

  - **Caso 1**: $r' = 0$

    $a = b \cdot c' + r' = b \cdot c' + 0 = b \cdot c'$. Luego $c = c'$ y $r = 0$.

  - **Caso 2**: $r' < 0$

    $$a = b \cdot c' + r' = b \cdot c' + r' - b + b = b \cdot c' - b + r' + b = b \cdot (c' - 1) + (r' + b) = b \cdot c + r$$

    donde $c = c' - 1 \in \mathbb{Z}$, pues $c' \in \mathbb{Z}$, y $r = r' + b \in \mathbb{Z}$, pues $r', b \in \mathbb{Z}$. Además $0 \leq r < b$:

    Como $0 \leq |r'| < b$ significa que $-b < r' < b$, y además $r' < 0$, se cumple que $-b < r' < 0$. Entonces $b - b < r' + b < 0 + b$, es decir, $0 < r < b$. Luego se cumple $0 \leq r < b$. ■

- Si $\boldsymbol{b < 0}$ entonces se cambiaría a de signo y se aplicaría el **Corolario 2** con $b > 0$.

- **Corolario 3**

  Dados $a, b \in \mathbb{Z}$ con $\boldsymbol{b \neq 0}$, existen únicos $c, r \in \mathbb{Z}$ tales que $a = b \cdot c + r$ y $0 \leq r < b$.

- **Notación**

  $c = a \ \boldsymbol{div}\ b$
  $r = a \ \boldsymbol{mód}\ b$

  - Si a es *par* entonces $a = (a\ div\ 2) \cdot 2$
  - Si a es *impar* entonces $a = (a\ div\ 2) \cdot 2 + 1$
  - Si $a\ mód\ b = 0$ entonces "a *es* ***divisible*** *por* b": $a = b \cdot (a\ div\ b)$ siendo $c = \frac{a}{b} \in \mathbb{Z}$ y $r = 0$.

- **Propiedades**

  1) $a \mid m$ y $a \mid n \Longrightarrow a \mid m + n$ y $a \mid m \cdot n$
  2) $a \mid m \implies a \mid m \cdot k$
  3) $a \mid m \implies a \cdot k \mid m \cdot k$
  4) $a \mid m \implies \frac{a}{k} \mid \frac{m}{k}$ para todo $k \in \mathbb{Z}^+$

- **Múltiplos y Divisores**

  $b \mid a \equiv$ "b *es* ***divisor*** *de* a" $\equiv \exists c \in \mathbb{Z} : a = b \cdot c$ (por ejemplo: $4 \mid 12$ pues $12 = 4 \cdot 3$)
  a es $\dot{b} \equiv$ "a *es* ***múltiplo*** *de* b" $\equiv \exists c \in \mathbb{Z} : a = b \cdot c$ (por ejemplo: 12 es $\dot{3}$ pues $12 = 3 \cdot 4$)
  Análogamente: $b \nmid a$ (por ejemplo: $2 \nmid 7$ y 7 no es $\dot{2}$)

- **Casos especiales**

  - $\frac{0}{0}$ **no está definido**.
  - $0 \mid 0$ pues $0 = 0 \cdot 0$
  - $0 \nmid a$ con $a \neq 0$ pues no se cumple $a = 0 \cdot c$ para ningún $c \in \mathbb{Z}$.
  - $\frac{a}{0}$ con $a \neq 0$ **no está definido**.

- El **máximo común divisor** de $a, b \in \mathbb{Z}$ (representado por $\boldsymbol{mcd(a, b)}$) es el mayor divisor común de a y de b, es decir, el mayor $d \in \mathbb{Z}$ tales que $d \mid a$ y $d \mid b$, en caso de que este exista.

$$mcd(a,b) = d \Leftrightarrow_{def} \begin{cases} d \mid a \wedge d \mid b & (d \text{ es divisor de } a \text{ y } b) \\ \forall d' \in \mathbb{Z} : \left((d' \mid a \wedge d' \mid b) \Longrightarrow d' \mid d\right) & (d \text{ es el mayor divisor de } a \text{ y } b) \end{cases}$$

- **Propiedades**

1) $mcd(0,0)$ **no existe** ($a \mid 0$ para todo $a \in \mathbb{Z}$, pues $0 = a \cdot 0$)
2) $mcd(a,b) = mcd(b,a)$
3) $mcd(a,b) = mcd(|a|,|b|)$
4) $mcd(a,0) = mcd(0,a) = |a|$, para todo $a \neq 0$.

- **Lema de Euclides**

$mcd(a,b) = mcd(b, a \text{ mód } b)$, para cada $a \geq b > 0$.

Demostración

Por el **Teorema de la División Entera** $a = b \cdot c + r$ con $0 \leq r < b$. Demostramos:

$$mcd(a,b) = mcd(b,r)$$

Lema de Euclides

Demostramos que $mcd(a,b) = mcd(b,r)$ por el **doble contenido**, es decir, veamos que tienen los mismos divisores comunes a y b que b y r:

⊆) Veamos que todo divisor común de a y b es también un divisor común de b y r. Sea $d \mid a$ y $d \mid b$:

$$a = d \cdot c_1 \text{ con } c_1 \in \mathbb{Z}$$
$$b = d \cdot c_2 \text{ con } c_2 \in \mathbb{Z}$$

$$r = a - b \cdot c = d \cdot c_1 - d \cdot c_2 \cdot c = d \cdot (c_1 - c_2 \cdot c) = d \cdot c' \text{ con } c' = c_1 - c_2 \cdot c \in \mathbb{Z}.$$

Luego $d \mid b$ y $d \mid r$.

⊇) Veamos que todo divisor común de b y r es también un divisor común de a y b. Sea $d \mid b$ y $d \mid r$:

$$b = d \cdot c_1 \text{ con } c_1 \in \mathbb{Z}$$
$$r = d \cdot c_2 \text{ con } c_2 \in \mathbb{Z}$$

$$a = b \cdot c + r = d \cdot c_1 \cdot c + d \cdot c_2 = d \cdot (c_1 \cdot c + c_2) = d \cdot c' \text{ con } c' = c_1 \cdot c + c_2 \in \mathbb{Z}.$$

Luego $d \mid a$ y $d \mid b$.

Como los divisores comunes de a y b son los mismos que los divisores comunes de b y r, también el mayor divisor común de a y b coincide con el mayor divisor común de b y r. Luego:

$$mcd(a,b) = mcd(b,r).$$ ■

- **Teorema de Euclides**

  Dados $a, b \in \mathbb{Z}$ tales que $a > b \geq 0$ **existe** y es **único** el $mcd(a, b)$.

  Demostración

  Demostramos la **existencia** razonando por **inducción completa** sobre $b \geq 0$:

  - **Caso base**: $b = 0$

    $$mcd(a, b) =^{b=0} mcd(a, 0) =^{4)} |a| =^{a>0} a$$

  - **Paso inductivo**: $b > 0$

    (HIC) Para todo $b > 0$: existe y es único el $mcd(a, l)$ para todo $0 \leq l < b$ y para todo $a > l \geq 0$.

    Veamos que existe el $mcd(a, b)$. Sabemos que:

    - $a = b \cdot c + r$ con $0 \leq r < b$ **(Teorema de la División Entera)**
    - $mcd(a, b) = mcd(b, r)$ **(Lema de Euclides)**

    Como se verifica $0 \leq r < b$, si tomamos $l = r$, se verifica la **HIC** para $a = b$. Luego existe $mcd(b, r)$. Aplicando el **Lema de Euclides**, $mcd(b, r) = mcd(a, b)$. Luego existe $mcd(a, b)$.

Demostramos ahora la **unicidad** razonando por **reducción al absurdo**:

Supongamos que

$$d_1 = mcd(a, b)$$
$$d_2 = mcd(a, b)$$

con $d_1 \neq d_2$. Como $a > b \geq 0$, se tiene que $d_1, d_2 > 0$.

Por definición de **máximo común divisor**:

$$d_1 \mid d_2 \equiv d_2 = c \cdot d_1 \quad \text{con} \quad c \in \mathbb{Z}$$
$$d_2 \mid d_1 \equiv d_1 = c' \cdot d_2 \quad \text{con} \quad c' \in \mathbb{Z}$$

$d_2 = c \cdot d_1 =^{d_1 = c' \cdot d_2} c \cdot c' \cdot d_2$. Como $d_2 > 0$ podemos simplificar la ecuación $d_2 = c \cdot c' \cdot d_2$, con lo cual:

$$c \cdot c' = 1 \Longrightarrow^{d_1, d_2 > 0} c = c' = 1$$

Luego $d_1 = c' \cdot d_2 = 1 \cdot d_2 = d_2$, es decir, $d_1 = d_2$. Llegamos a **contradicción**. Por tanto, $d_1 = d_2$. ■

- **Ejemplo:** $mcd(3258, 1164) =^{\mathbf{LE}} mcd(1164, 930) =^{\mathbf{LE}} mcd(930, 234) =^{\mathbf{LE}} mcd(234, 228) =^{\mathbf{LE}} mcd(228, 6) =^{\mathbf{LE}} mcd(6, 0) =^{4)} 6$

- **Algoritmo de Euclides**

Sean $a, b \in \mathbb{Z}$ tales que $a \geq b > 0$. Seguimos los siguientes pasos para obtener el $mcd(a, b)$:

Paso 1

Consideramos $a_0 = a$ y $b_0 = b$.

Paso 2

Paso 2.1

Si $b_i = 0$ entonces $mcd(a, b) = a_i$. El algoritmo termina su ejecución.

Paso 2.2

Si $b_i > 0$ entonces calculamos

$$c_i = a_i \; div \; b_i$$
$$r_i = a_i \; mód \; b_i$$

Se cumple entonces que $mcd(a_i, b_i) = mcd(b_i, r_i)$ por el **Lema de Euclides**.
Por tanto, consideramos $a_{i+1} = b_i$ y $b_{i+1} = r_i$. Volvemos al **Paso 2**.

Algoritmo de Euclides

- **Implementación iterativa en C del Algoritmo de Euclides**

```
int  mcd (int a, int b) {    // a ≥ b > 0

        int ai = a ;    // a_0 = a
        int bi = b;     // b_0 = b

        int ci ;
        int ri ;

        while ( bi > 0 ) {    // Si b_i > 0 entonces mcd(a_i, b_i) = mcd(b_i, r_i)

                ci = ai  / bi ;    // c_i = a_i div b_i
                ri = ai % bi ;     // r_i = a_i mód b_i

                ai = bi ;    // a_{i+1} = b_i
                bi = ri ;    // b_{i+1} = r_i

        }

        return ai ;    // Si b_i = 0 entonces mcd(a, b) = a_i

}
```

- **Implementación recursiva en C del Algoritmo de Euclides**

```
int  mcd (int a, int b) {    // a ≥ b > 0
        int resultado ;
        if ( b == 0 ) {    // Caso base (b = 0)
                resultado = a ;
        }
        else if ( b > 0 ) {    // Caso recursivo (b > 0)
                resultado = mcd(b, a % b) ;
        }
        return resultado ;
}
```

$$\begin{cases} mcd(a,b) = a & \text{si } b = 0 \ \textbf{(CB)} \\ mcd(a,b) = mcd(b, a \text{ mód } b) & \text{si } b > 0 \ \textbf{(CR)} \end{cases}$$

- **Ejercicio 2.40**: Calcular $mcd(2406, 654)$.

i	a_i	b_i	$r_i = a_i \text{ mód } b_i$	$c_i = a_i \text{ div } b_i$
0	2406	654	444	3
1	654	444	210	1
2	444	210	24	2
3	210	24	18	8
4	24	18	6	1
5	18	6	0	3
6	**6**	0	–	–

$$mcd(2406, 654) = mcd(654, 444) = mcd(444, 210) = mcd(210, 24) = mcd(24, 18)$$
$$= mcd(18, 6) = mcd(6, 0) = 6$$

Luego $mcd(2406, 654) = 6$.

- **Teorema de Bézout**

  Dados $a, b \in \mathbb{Z}$ tales que $d = mcd(a, b)$ existen $m, n \in \mathbb{Z}$ tales que $d = m \cdot a + n \cdot b$.

  (m y n no tienen por qué ser únicos. A la ecuación $d = m \cdot a + n \cdot b$ se le denomina **identidad de Bézout**)

  Demostración

  Es suficiente con probarlo para $a > b \geq 0$. En efecto:

  - Si no se verifica $a, b \geq 0$:

    $$d = mcd(a, b) =^{3)} mcd(|a|, |b|) = k \cdot |a| + l \cdot |b| = m \cdot a + n \cdot b$$

    donde $m = \pm k$ y $n = \pm l$.

  - Si $a = b = c$: no existe $d = mcd(0,0)$, así que este caso no puede darse.

  - Si $a = b > 0$: $d = mcd(a, b) =^{a=b} mcd(a, a) = mcd(a, 0) =^{4)} |a| =^{a>0} a$.

  Así pues, asumimos que $a > b \geq 0$ y razonamos por **inducción completa** sobre $b \geq 0$:

Así pues, asumimos que $a > b \geq 0$ y razonamos por **inducción completa** sobre $b \geq 0$:

- **Caso base**: $b = 0$

  $d = mcd(a,b) =^{b=0} mcd(a,0) =^{4)} |a| =^{a>0} a = 1 \cdot a + 0 \cdot b \implies m = 1$ y $n = 0$.

- **Paso inductivo**: $b > 0$

  (HIC) Para cada $b > 0$ se verifica que:

  Para cada $0 \leq l < b$ y cualquier entero $a' > l \geq 0$, si $d' = mcd(a', l)$ entonces existen $m', n' \in \mathbb{Z}$ tales que $d' = m' \cdot a' + n' \cdot l$.

  ¿ Existen $m, n \in \mathbb{Z}$ tales que $d = m \cdot a + n \cdot b$?

  Por el **Teorema de la División Entera**: $a = b \cdot c + r$ con $0 \leq r < b$.

  Por el **Lema de Euclides**:

  $$\begin{aligned} mcd(a,b) = mcd(b,r) &=^{\mathbf{HIC}} m' \cdot b + n' \cdot r \qquad [\text{ Se puede aplicar la } \mathbf{HIC} \text{ pues } 0 \leq r < b\ ] \\ &= m' \cdot b + n' \cdot (a - b \cdot c) \qquad [\text{ Como } a = b \cdot c + r, \text{ despejando } r = a - b \cdot c\ ] \\ &= n' \cdot a + m' \cdot b - n' \cdot b \cdot c \\ &= n' \cdot a + (m' - n' \cdot c) \cdot b = m \cdot a + n \cdot b \end{aligned}$$

  donde $m = n' \in \mathbb{Z}$ y $n = m' - n' \cdot c \in \mathbb{Z}$. ■

$$bezout(a,b) = (1,0) \quad \text{si } b = 0$$
$$bezout(a,b) = \big(n', m' - n' \cdot (a \; div \; b)\big) \quad \text{si } b > 0$$
siendo $bezout(b, a \; mód \; b) = (m', n')$

- **Algoritmo (iterativo) de Bézout**

Llamamos $\boldsymbol{k}$ al $\boldsymbol{i}$ con el que terminal el **algoritmo de Euclides** para el cálculo de $\boldsymbol{d = mcd(a,b)}$.

Paso 1

Consideramos $\boldsymbol{m_k = 1}$ y $\boldsymbol{n_k = 0}$. **(caso base de la inducción)**

Paso 2

Para todo $\boldsymbol{i}$ desde $\boldsymbol{k-1}$ hasta $\boldsymbol{0}$ tomamos: **(paso inductivo de la inducción)**

$$\boldsymbol{m_i = n_{i+1}}$$
$$\boldsymbol{n_i = m_{i+1} - n_{i+1} \cdot c_i}$$

Paso 3

Tomamos $\boldsymbol{m = m_0}$ y $\boldsymbol{n = n_0}$. Se verifica que $\boldsymbol{d = mcd(a,b) = m \cdot a + n \cdot b}$.

- **Ejemplo de aplicación del algoritmo de Bézout**

Dados $a = 15$ y $b = 10$, calcular el $mcd(a, b)$ y los coeficientes m y n de la **identidad de Bézout**.

i	a_i	b_i	r_i	c_i	m_i	n_i
0	15	10	5	1	1	$0 - 1 \cdot 1 = -1$
1	10	5	0	2	0	$1 - 0 \cdot 2 = 1$
2	**5**	0	–	–	1	0

$mcd(15, 10) = mcd(10, 5) = mcd(5, 0) = 5$, luego el $mcd(a, b) = 5$.

Los coeficientes de la identidad de Bézout son $m = 1$ y $n = -1$. En efecto:

$5 = m \cdot 15 + n \cdot 10 = 1 \cdot 15 + (-1) \cdot 10 = 15 - 10 = 5$

- **Ejercicio 2.41**: Calcular el $mcd(721, 448)$ aplicando el **algoritmo de Euclides**, así como enteros m y n tales que $mcd(721, 448) = 721 \cdot m + 448 \cdot n$ **(identidad de Bézout)**.

i	a_i	b_i	r_i	c_i	m_i	n_i
0	721	448	273	1	**23**	$-14 - 23 \cdot 1 = \mathbf{-37}$
1	448	273	175	1	-14	$9 - (-14) \cdot 1 = 23$
2	273	175	98	1	9	$-5 - 9 \cdot 1 = -14$
3	175	98	77	1	-5	$4 - (-5) \cdot 1 = 9$
4	98	77	21	1	4	$-1 - 4 \cdot 1 = -5$
5	77	21	14	3	-1	$1 - (-1) \cdot 3 = 4$
6	21	14	7	1	1	$0 - 1 \cdot 1 = -1$
7	14	7	0	2	0	$1 - 0 \cdot 2 = 1$
8	**7**	0	–	–	1	0

$mcd(721, 448) = \mathbf{7} = \mathbf{23} \cdot 721 + (\mathbf{-37}) \cdot 448$. Luego $m = 23$ y $n = -37$.

- **Mínimo común múltiplo**

  Dados $a, b \in \mathbb{Z}$, el **mínimo común múltiplo** de a y b, representado por $\boldsymbol{mcm(a, b)}$, es el menor $m \in \mathbb{N}$ tal que $a \mid m$ y $b \mid m$, si es que existe.

$$mcm(a,b) = m \Leftrightarrow_{def} \begin{cases} a \mid m \wedge b \mid m \\ \forall m' \in \mathbb{Z} : \big((a \mid m' \wedge b \mid m') \Longrightarrow m \mid m'\big) \end{cases}$$

(m es múltiplo de a y b)
(m es el menor múltiplo de a y b)

- **Propiedades**

1) $mcm(0,0) = 0$. En efecto, $0 \mid 0$ por lo que 0 es el menor múltiplo común.
2) $mcm(a,b) = mcm(|a|, |b|)$
3) $mcm(a,b) = mcm(b,a)$
4) $mcm(a,0) = mcm(0,a) = 0$ para todo $a \in \mathbb{Z}$. En efecto, $a \mid 0$ por lo que a es el menor múltiplo común.

5) $mcd(a,b) \cdot mcm(a,b) = a \cdot b$ para $a, b > 0$. Así

$$mcm(a,b) = \frac{a \cdot b}{mcd(a,b)}$$

El denominador nunca se anula, pues $mcd(a,b) \neq 0$ al tener que $a, b > 0$.

- Un número entero $p > 1$ es **primo** si los únicos divisores positivos de p son 1 y el propio p:

  p es **primo** $\Leftrightarrow_{def} \nexists\, d \in \mathbb{Z} : (d \mid p \wedge 1 < d < p) \equiv \forall\, d \in \mathbb{Z} : \big(d \mid p \Longrightarrow (d = 1 \vee d = p)\big)$

  Por ejemplo: $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

- Un número entero $x > 1$ es **compuesto** si no es primo:

  p es **compuesto** $\Leftrightarrow_{def} \exists\, d \in \mathbb{Z} : (d \mid x \wedge 1 < d < x)$

  Si x es compuesto entonces admite una descomposición $x = d \cdot k$, con $1 < d, k < x$.

  Por ejemplo: $12 = 3 \cdot 4$, $10 = 2 \cdot 5$, …

- $\mathbf{-1, 0, 1}$ **no son ni primos ni compuestos** (para los demás negativos es su opuesto el que determina si es primo o compuesto el número).

- **Propiedades**

  1) $n > 1$ es **compuesto** $\Leftrightarrow$ $\exists\, p$ **primo** tal que $p \mid n$ y $1 < p^2 \leq n$. **(Ejercicio 2.51)**

  $$\nexists\, d \in \mathbb{Z} : (d \mid n \wedge 1 < d^2 \leq n) \Longrightarrow n \text{ es } \textbf{primo} \equiv$$
  $$\nexists\, d \in \mathbb{Z} : \big(d \mid n \wedge 1 < d \leq \lfloor \sqrt{n} \rfloor\big) \Longrightarrow n \text{ es } \textbf{primo}$$

  2) p es **primo** y $p \mid x_1 \cdot x_2 \cdot \cdots \cdot x_n \Longrightarrow p \mid x_i$ para algún $1 \leq i \leq n$

- **Teorema Fundamental de la Aritmética**

  Cualquier número entero $x \geq 1$ se puede descomponer como producto de factores primos:

  $$x = p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_m^{n_m}$$

  donde p_i son **primos** diferentes $(p_i < p_{i+1})$ y $n_i \in \mathbb{N}$. La descomposición es única (salvo en el orden de los factores primos. Para que sea única imponemos que $p_i < p_{i+1}$, y si $p_i = p_j$ entonces $p_i \cdot p_j = p_i^2$).

  Demostración

  Comenzamos demostrando la **existencia**: para todo $n \geq 1$, n admite una descomposición en producto de números primos. Razonamos por **inducción completa** sobre $n \geq 1$:

  - **Caso base**: $n = 1$

    $1 = p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_m^{n_m}$ con $m = 0$ (1 admite un producto vacío de números primos)

  - **Paso inductivo**: $n > 1$

    (HIC) Para todo $1 \leq l < k$: l admite una descomposición en producto de números primos.

¿ Admite k una descomposición en producto de números primos ? Distinguimos casos:

- **Caso 1:** k es primo.

  En este caso, k admite un producto unitario de números primos con un solo factor, el propio k.

- **Caso 2:** k es compuesto.

  En este caso, $k = l_1 \cdot l_2$ con $1 < l_1, l_2 < k$. Por **(HIC)**:

$$l_1 = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_{m_{l_1}}^{n_{m_{l_1}}} \quad \text{con } p_i < p_{i+1}$$
$$l_2 = q_1^{n'_1} \cdot q_2^{n'_2} \cdot \dots \cdot q_{m_{l_2}}^{n'_{m_{l_2}}} \quad \text{con } q_j < q_{j+1}$$

  Luego

$$k = l_1 \cdot l_2 = p_1^{n_1} \cdot p_2^{n_2} \cdot \dots \cdot p_{m_{l_1}}^{n_{m_{l_1}}} \cdot q_1^{n'_1} \cdot q_2^{n'_2} \cdot \dots \cdot q_{m_{l_2}}^{n'_{m_{l_2}}}$$

  Podemos reordenar los p_i, q_j de menor a mayor. Si $p_i = q_j$ entonces $p_i^n \cdot q_j^m = p_i^{n+m}$. Con ello obtenemos la descomposición deseada de forma única.

Demostramos ahora la **unicidad**, es decir, la descomposición en factores primos de un entero $n \geq 1$ es **única** salvo el orden de los factores primos:

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k = p'_1 \cdot p'_2 \cdot \cdots \cdot p'_l$$

con $k, l \geq 1$ y p_i, p'_j primos (pueden repetirse). Razonamos por **inducción completa** sobre $n \geq 1$:

- **Caso base**: $n = 1$

  Se cumple trivialmente pues $k = 0$ y $l = 0$ (producto vacío).

- **Paso inductivo**: $n > 1$

  (HIC) La descomposición en factores primos de n' con $1 \leq n' < n$ es única salvo el orden de los factores primos.

  ¿ La descomposición en factores primos de $n \geq 1$ es única salvo el orden de los factores primos ?

  Como $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k = p'_1 \cdot p'_2 \cdot \cdots \cdot p'_l$ se cumple que $p_1 \mid p'_1 \cdot p'_2 \cdot \cdots \cdot p'_l$ (resulta sencillo comprobar que si $a \cdot b \mid n$ entonces $a \mid n$ y $b \mid n$). Aplicando la **propiedad 2)** de números primos: $p_1 \mid p'_i$ para algún $1 \leq i \leq l$.

  Podemos reordenar los p'_j para que $p'_i = p'_1$ y aparezca en primer lugar en la factorización. En ese caso $p_1 \mid p'_1$ y p'_1 es primo. Luego $p_1 = 1$ o bien $p_1 = p'_1$. Como p_1 es primo, $p_1 \neq 1$, luego $p_1 = p'_1$.

Distinguimos casos:

- **Caso 1**: $k = 1$

  $n = p_1 = p_1 \cdot p_2' \cdot \cdots \cdot p_l' \implies l = 1$. La descomposición es única para $n = p_1$ siendo p_1 primo.

- **Caso 2**: $k > 1$

  $$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k = p_1 \cdot p_2' \cdot \cdots \cdot p_l' \implies^{p_1 \neq 0} p_2 \cdot \cdots \cdot p_k = p_2' \cdot \cdots \cdot p_l'$$

  Si llamamos $n' = p_2 \cdot \cdots \cdot p_k = p_2' \cdot \cdots \cdot p_l'$, como $1 \leq n' < n$ (pues $k > 1$), por **(HIC)** la descomposición de n' en factores primos es única.

  Por tanto, para $n = p_1 \cdot n' = p_1 \cdot n'$, es decir, para $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k = p_1 \cdot p_2' \cdot \cdots \cdot p_l'$, se cumple también que la descomposición es única.

  ■

- **Descomposición en factores primos de un número $n \in \mathbb{N}$:**

  1) Obtener el menor número primo p tal que $p \mid n$.
  2) Como $n = p \cdot n'$, calcular $n' = \frac{n}{p} \in \mathbb{N}$.
  3) Volver a 1) cambiando n por n'.

- **Propiedad (Euclides, Siglo III a.C.)**

  Si p, q son números primos tales que $q \mid (1 + p!)$ entonces $q > p$.

  Demostración

  Razonamos por **reducción al absurdo**. Supongamos que $q \leq p$. Como:

  $$\begin{aligned} q \mid (1 + p!) \quad &\Leftrightarrow_{def} \quad 1 + p! = n \cdot q \quad \text{con} \quad n \in \mathbb{Z} \\ q \leq p \implies q \mid p! \quad &\Leftrightarrow_{def} \quad p! = n' \cdot q \quad \text{con} \quad n' \in \mathbb{Z} \end{aligned}$$

  Sustituyendo $p! = n' \cdot q$ en $1 + p! = n \cdot q$, obtenemos:

  $$1 + p! = 1 + n' \cdot q = n \cdot q$$

  Operando y sacando factor común a q:

  $$1 = (n - n') \cdot q$$

  Con lo cual: $q \mid 1 \implies q = 1$

  Pero entonces llegamos a una **contradicción**, pues q es un número primo. Luego $q > p$. ■

- **Corolario:** para cualquier número primo p siempre existe otro primo mayor q tal que $q \mid (1 + p!)$.

- **Teorema**

  Existe un número infinito de números primos.

  Demostración

  Razonamos por **reducción al absurdo**: supongamos que existe una cantidad finita de números primos $\{p_1, p_2, \dots, p_r\}$. Consideramos el número

  $$q = p_1 \cdot p_2 \cdot \dots \cdot p_r + 1$$

  Como este número no está en el conjunto $\{p_1, p_2, \dots, p_r\}$, se ha de tener que q no es primo. Por tanto, ha de existir un número primo p_i tal que $p_i \mid q$. Por definición:

  $$p_i \mid q \iff_{def} q = p_i \cdot c \text{ con } c \in \mathbb{Z}$$

  Igualando $q = p_1 \cdot p_2 \cdot \dots \cdot p_r + 1$ con $q = p_i \cdot c$ tenemos $1 + p_1 \cdot p_2 \cdot \dots \cdot p_i \cdot \dots \cdot p_r = p_i \cdot c$.

  Sacando factor común a p_i:

  $$1 = p_i \cdot (c - p_1 \cdot p_2 \cdot \dots \cdot p_{i-1} \cdot p_{i+1} \cdot \dots \cdot p_r)$$

  Luego

  $$p_i \mid 1 \implies p_i = 1$$

  Pero entonces llegamos a una **contradicción**, pues p_i es un número primo. Luego hay una cantidad infinita de números primos. ■

- **Algoritmo para determinar si un número n es primo**

  1) Calcular la raíz cuadrada aproximada (por defecto) del número n, es decir: $\lfloor \sqrt{n} \rfloor$.

  2) Indicar todos los números primos p menores o iguales a $\lfloor \sqrt{n} \rfloor$, es decir: $p^2 \leq n$.

  3) Se determina si el número n es o no divisible para cada uno de los números primos p anteriores:

     3.1) Si no resulta ser divisible por ninguno: $\boldsymbol{n}$ **es primo**.

     3.2) Si existe algún primo p que lo divide: $\boldsymbol{n}$ **es compuesto**.

- **Ejercicio 2.51:** ¿Es $n = 467$ primo?

  1) $\lfloor \sqrt{n} \rfloor = \lfloor \sqrt{467} \rfloor = 21$, pues $21^2 = 441$ pero $22^2 = 484$.

  2) Los números primos p menores o iguales a $\lfloor \sqrt{467} \rfloor = 21$ son:

  $$p = 2, 3, 5, 7, 11, 13, 17, 19$$

  3) Como ninguno de los números primos p anteriores divide a 467, el número 467 es primo.

- **Calcular todos los números primos menores o iguales que $n = 100$:**

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- **Implementación en C del método de la Criba de Eratóstenes para calcular todos los números primos menores o iguales que n:**

```
void criba ( bool tabla[ ] , int n ) {

        tabla[0] = false ;
        tabla[1] = false ;

        for ( int i = 2 ; i <= n ; ++ i ) {

              tabla[i] = true ;

        }

        for ( int i = 2 ; i * i <= n ; ++ i ) {

              if ( tabla[i] ) {

                    for ( int h = 2 ; i * h <= n ; ++ h ) {

                          tabla[ i * h ] = false ;

                    }
              }
        }
}
```

```
int esPrimo ( int n ) {

        for ( int i = 2 ; i * i <= n ; i ++ ) {

              if ( n % i == 0 ) {

                    return 0 ;

              }

        }

        return 1 ;

}
```

- Sea m un número entero positivo. Diremos que $a, b \in \mathbb{N}$ son **congruentes módulo m** (representado por $a \equiv_m b$) si se cumple cualquiera de las siguientes tres condiciones equivalentes:

  1) $a \; mód \; m = b \; mód \; m$
  2) $m \mid b - a$
  3) $\exists k \in \mathbb{Z} : b = a + k \cdot m$

- **Ejemplos:** $25 \equiv_7 32$

  1) $25 \; mód \; 7 = 32 \; mód \; 7 = 4$
  2) $7 \mid 32 - 25$, pues $7 \mid 7$
  3) $\exists k \in \mathbb{Z} : 32 = 25 + k \cdot 7$. En efecto, $k = 1$.

  $0 \equiv_2 0, 1 \equiv_2 1, 2 \equiv_2 0, 3 \equiv_2 1, 4 \equiv_2 0, 5 \equiv_2 1, \ldots$
  $13 \equiv_{12} 1, 14 \equiv_{12} 2, 15 \equiv_{12} 3, 17 \equiv_{12} 5, 19 \equiv_{12} 7, \ldots$

- Para cada $a \in \mathbb{Z}$, la **clase de congruencia de a módulo m** es:

  $[a]_m = \{ b \in \mathbb{Z} : a \equiv_m b \} = \{ a + k \cdot m : k \in \mathbb{Z} \} = \bar{a}$ (si m es conocido)

- **Ejemplos:** $m = 12$

  $[1]_{12} = \{ 1 + k \cdot 12 : k \in \mathbb{Z} \} = \{1, 13, -11, 25, -23, \ldots\} = \bar{1}$
  $[13]_{12} = \{ 13 + k \cdot 12 : k \in \mathbb{Z} \} = \{13, 25, 1, -11, \ldots\} = \bar{1}$

- El **conjunto cociente** $\mathbb{Z}/_{\equiv_m}$ (representado por $\mathbb{Z}/_{(m)}$) es el conjunto de todas las clases de equivalencia módulo m que son distintas entre sí:

$$\mathbb{Z}/_{(m)} = \{\, [0]_m, [1]_m, [2]_m, \dots, [m-1]_m \,\}$$

- **Ejemplo:** $m = 12$

$$\mathbb{Z}/_{(2)} = \{\, \bar{0}, \bar{1} \,\}$$
$$\mathbb{Z}/_{(3)} = \{\, \bar{0}, \bar{1}, \bar{2} \,\}$$
$$\mathbb{Z}/_{(12)} = \{\, \bar{0}, \bar{1}, \bar{2}, \dots, \overline{11} \,\}$$

- **Operaciones aritméticas módulo $m > 0$ en $\mathbb{Z}/_{(m)}$:**
  - **Suma:**

$$[a]_m +_m [b]_m = [c]_m \quad \text{siendo } c \in \mathbb{Z} \text{ tales que } a + b \equiv_m c.$$

  - **Multiplicación:**

$$[a]_m *_m [b]_m = [c]_m \quad \text{siendo } c \in \mathbb{Z} \text{ tales que } a \cdot b \equiv_m c.$$

- **Tablas de la suma y el producto en $\mathbb{Z}/_{(2)}$:**

$+_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$*_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	1

- **Tablas de la suma y el producto en $\mathbb{Z}/_{(6)}$:**

$+_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	4	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$*_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	4	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	2	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	2	$\bar{1}$

- **Ejercicio 2.66:** Resolver las siguientes ecuaciones

$*_5$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	4	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

1) $(\bar{3} *_5 x) +_5 \bar{2} = \bar{4}.$

Solución

$$(\bar{3} *_5 x) +_5 \bar{2} = \bar{4} \implies (\bar{3} *_5 x) = \bar{2} \implies \boldsymbol{x = 4}$$

2) $(\bar{2} +_6 x) *_6 \bar{4} = \bar{5}$ **No tiene solución en** $\mathbb{Z}/_{(6)}$:

x	$\bar{2} +_6 x$	$(\bar{2} +_6 x) *_6 \bar{4}$
$\bar{0}$	$\bar{2}$	$\bar{2}$
$\bar{1}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{4}$	$\bar{4}$
$\bar{3}$	$\bar{5}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{0}$
$\bar{5}$	$\bar{1}$	$\bar{4}$