Capítulo 1

Inducción

1.1. Los Postulados de Peano y la Inducción Matemática

Quien admita la existencia de al menos un conjunto (y ello ocurre tarde o temprano), deberá admitir la existencia del conjunto vacío $\varnothing$. A $\varnothing$ le ha sido dado el nombre de 0 y ha sido considerado un número natural.

Cuando se tiene un conjunto n, entonces n^+ queda definido por la siguiente igualdad:

$$n^+ = n \cup \{n\}$$

Otros nombres de números son los siguientes:

- $1 = 0^+ = 0 \cup \{0\} = \varnothing \cup \{0\} = \{0\}$
- $2 = 1^+ = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$
- $3 = 2^+ = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$

y así hasta los confines de la numeración, en general:

$$n^+ = \{0, 1, \ldots, n-1\}$$

Es admitido como axioma (*axioma del infinito*) que existe al menos un *conjunto inductivo*, es decir, un conjunto X tal que:

- $0 \in X$
- $n^+ \in X$ siempre que $n \in X$.

y el menor de todos ellos ha sido denominado conjunto de lo *números naturales* y ha sido representado por los símbolos ω ó $\mathbb{N}$, entre otros.

Puede que la función más conocida de las matemáticas sea la llamada *función sucesor de Peano*. GIUSEPPE PEANO fue un matemático italiano nacido en 1858 y fallecido en 1932. Dicha función, representada por s, asigna su siguiente a cada número natural. Puede ser considerada como "la función que cuenta".

Definición 1.1.1. La *función sucesor de Peano* es la función:

$$s\colon \omega \longrightarrow \omega$$

definida[1] como $s(n) = n^+$.

En términos de la función s existe una colección de "propiedades básicas" que caracterizan al "conjunto" de los números naturales ω. Estas propiedades se conocen con el nombre de *Postulados de Peano*, aunque para nosotros son teoremas.

Teorema 1.1.1. *Las siguientes afirmaciones, conocidas como postulados de Peano, son ciertas:*

P.1) $0 \in \omega$

P.2) Si $n \in \omega$, *entonces* $s(n) \in \omega$.

P.3) No existe $n \in \omega$ *tal que* $0 = s(n)$.

P.4) Si $s(n) = s(m)$, *entonces* $n = m$. s es inyectiva

P.5) Si $P \subseteq \omega$ *y cumple las siguientes condiciones:*

a) $0 \in P$

b) $s(n) \in P$ *siempre que* $n \in P$

entonces $P = \omega$.

El postulado P.5 se conoce como el *principio de inducción matemática*.

Observación 1.1.1. Hay subconjuntos de ω que aún teniendo a 0 entre sus elementos y no siendo "finitos" sin embargo no son todo ω, verbigracia el "conjunto de los números naturales pares" (el 1 es natural, pero no es par), que para colmo tiene el mismo "cardinal" que ω.

Teorema 1.1.2 (*Principio del Buen Orden*). *Todo conjunto de números naturales no vacío tiene un elemento mínimo.*

Teorema 1.1.3 (*Segundo Principio de Inducción*). *Sea* P *un conjunto cualquiera de números naturales. Si para todo número natural*[2] n *se cumple:*

$$n \in P \text{ siempre que } n \subseteq P \Longrightarrow \quad (1.1)$$

Entonces $P = \omega$.

$n = \{0, 1, \dots, n-1\}$ Claro porque $s(n-1) = n$ ↳ $s(n-1) = n-2$ ⋮

Observación 1.1.2. Obsérvese que si un subconjunto de números naturales P cumple la condición (1.1) necesariamente debe contar con 0 entre sus elementos. En efecto, sea cual sea P siempre se cumplirá $\emptyset \subseteq P$, por lo que en virtud de la condición (1.1) se debe cumplir $\emptyset \in P$, esto es, $0 \in P$.

Observación 1.1.3. Obsérvese que la demostración dada del Teorema 1.1.3 es una consecuencia del Principio del Buen Orden.-

[1] Siguiendo el desarrollo de la teoría de conjuntos, a la postre se comprueba que $s(n) = n + 1$.

[2] Según el modelo que tenemos de ω, también representado por algunos como $\mathbb{N}$, $0 = \emptyset$ y si $n \neq 0$ entonces $n = \{0, \dots, n-1\}$.

1.2. Equivalencia entre Principios

Hagamos una síntesis de los principios nombrados hasta ahora:

1. **Principio de Inducción Matemática**; Si $P \subseteq \omega$ y cumple las siguientes condiciones:

   a) $0 \in P$

   b) $s(n) \in P$ siempre que $n \in P$

   entonces $P = \omega$.

2. **Principio del Buen Orden**; Todo conjunto de números naturales no vacío tiene un elemento mínimo.

3. **Segundo Principio de Inducción**; Si $P \subseteq \omega$ y cumple que:

   $$\text{Para todo número natural } n,\ n \in P \text{ siempre que } n \subseteq P \tag{1.2}$$

   Entonces $P = \omega$.

Teorema 1.2.1. *Si es válido el principio del buen orden entonces es válido el principio de inducción matemática.*

Teorema 1.2.2. *Si es válido el segundo principio de inducción entonces es válido el principio del buen orden.*

Corolario 1.2.3. *Son equivalentes los siguientes principios:*

1. *El principio de inducción matemática.*
2. *El principio del buen orden.*
3. *El segundo principio de inducción.*

Esto es con lo que nos tenemos que quedar

El principio de inducción ha sido difundido enunciándolo sobre fórmulas de primer orden en el lenguaje de la aritmética y a veces no referidos a 0 como primer natural de validez. En lo que sigue nos referiremos con el nombre de *enunciados* o simplemente *fórmulas* a las fórmulas de primer orden en el lenguaje de la aritmética, $P(i)$, escritas con una única variable libre i en su única escritura. Partiendo de $P(i)$, el objeto de toda demostración según el método de inducción es evidenciar como cierta la fórmula $\forall i P(i)$.

Teorema 1.2.4. *Sea* $P(i)$ *una fórmula e* $i_0 \in \omega$. *Supongamos que:*

1. $P(i_0)$ *es cierto (paso base).*
2. *Para todo todo* $k \in \omega$ *tal que* $i_0 \leq k$, $P(k+1)$ *es cierto siempre que* $P(k)$ *sea cierto (hipótesis y paso de inducción).*

entonces $P(i)$ *es cierto para todo* $i \in \omega$ *tal que* $i_0 \leq i$.

Ejemplo 1.2.1. Para todo $n \in \omega$ es cierta la igualdad:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{1.3}$$

Solución. Es por inducción sobre n según el enunciado $P(k)$ del tenor

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

En el **caso base**, para $k = 0$, el miembro de la izquierda de la ecuación (1.3) es 0 y el de la derecha es $\frac{0(0+1)}{2} = 0/2 = 0$; por tanto $P(0)$ es cierta. Supongamos que para el número natural k, $P(k)$ es cierta (**hipótesis de inducción**) y deduzcamos de ello en el **paso de inducción** que $P(k+1)$ es cierta. Un razonamiento que sirve de demostración es el siguiente:

$$\begin{aligned}
\sum_{i=0}^{k+1} i &= (\sum_{i=0}^{k} i) + (k+1), && \text{por definición} \\
&= \frac{k(k+1)}{2} + (k+1), && \text{por hip. de inducción} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{(k+2)(k+1)}{2}
\end{aligned}$$

Por el *Principio de Inducción Matemática*, $P(n)$ es cierta para todo número natural n. □

Teorema 1.2.5. *Sea $P(i)$ una fórmula e $i_0 \in \omega$. Si para todo número natural n, $P(n)$ es cierto siempre que $P(i)$ sea cierto para todo $i \in \omega$ tal que $i_0 \leq i < n$, entonces $P(i)$ es cierto para todo $i \in \omega$ tal que $i_0 \leq i$.*

Ejemplo 1.2.2. Todo número natural mayor que 1 tiene al menos un factor primo.

Solución. Sea $P(i)$ el enunciado del tenor "el número natural i tiene al menos un factor primo". Supongamos que n es un número natural superior a 1 y supongamos que para todo $1 < k < n$, k tiene al menos un factor primo (**hip. de induc.**), es decir, suponemos que para todo $1 < k < n$, $P(k)$ es cierta. Demostraremos (en el **paso de inducción**) que $P(n)$ es cierta, esto es, que n tiene al menos un factor primo. Como n es natural, será primo o no lo será. Si n es primo, tiene un factor primo, a saber, él mismo; así pues la propiedad $P(n)$ resulta cierta cuando n es primo (por ahora no hemos usado la hipótesis de inducción). Si n no es primo, será producto de dos números naturales a y b, que cumplirán $1 < a \leq b < n$. Por la hipótesis de inducción a tiene al menos un factor primo (también se puede decir lo mismo de b y podría ser usado b con el mismo fin en lugar de a). Como todo factor de a lo es de cualquiera de sus múltiplos, sabemos ahora que n tiene al menos un factor primo: el conocido de a. Lo que se quería demostrar se deduce ahora por el *Segundo Principio de Inducción*. □

Definición 1.2.1. Sean $a, b \in \mathbb{Z}$ tales que $b \neq 0$. Un *par divisor de a por b* es un par de enteros $\langle q, r \rangle$ tales que:

1. $a = bq + r$.
2. $0 \leq r < |b|$.

Lema 1.2.6. *Supongamos que para todo $a, b \in \omega$ tales que $b \neq 0$ existe un par divisor de a por b. Entonces para todo $a, b \in \mathbb{Z}$ tales que $b \neq 0$ existe un par divisor de a por b y es el siguiente por casos, siempre que $\langle q, r \rangle$ sea un par divisor de $|a|$ por $|b|$:*

1. *Si $0 < a$ y $b < 0$, $\langle \operatorname{sgn}(a) \operatorname{sgn}(b) q, r \rangle$ es un par divisor de a por b.*

2. *En el resto de casos, si* $r = 0$ *entoces* $\langle \operatorname{sgn}(a)\operatorname{sgn}(b)(q + \operatorname{sgn}(r)), 0\rangle$ *es un par divisor de* a *por* b *y si* $r \neq 0$*, entonces* $\langle \operatorname{sgn}(a)\operatorname{sgn}(b)(q + \operatorname{sgn}(r)), |b| - r\rangle$ *es un par divisor de* a *por* b.

Demostración. Supongamos que $\langle q, r\rangle$ es un par divisor de $|a|$ por $|b|$. La casuística es la siguiente:

1. $0 < a$ y $b < 0$; entonces

$$\begin{aligned} a &= (-b)q + r \\ &= b(-q) + r \end{aligned}$$

   y $0 \leq r < |b|$. Así pues, $\langle -q, r\rangle = \langle \operatorname{sgn}(a)\operatorname{sgn}(b)q, r\rangle$.

2. $a < 0$ y $b < 0$; $-a = (-b)q + r$ y $0 \leq r < -b$. Entonces:

   - $r = 0$; como $-a = (-b)q$ se cumple $a = bq$ y así $\langle q, 0\rangle = \langle \operatorname{sgn}(a)\operatorname{sgn}(b)(q + \operatorname{sgn}(r)), 0\rangle$ es un par divisor de a por b.
   - $r > 0$; entonces:

$$\begin{aligned} a &= bq - r \\ &= bq + 0 - r \\ &= bq + b - b - r \\ &= b(q + 1) + (-b - r) \end{aligned}$$

     Las condiciones $0 \leq r < -b$ son equivalentes a $b < -r \leq 0$ o también a $0 < -b - r < |b|$. En definitiva, se tiene que $\langle q + 1, |b| - r\rangle = \langle \operatorname{sgn}(a)\operatorname{sgn}(b)(q + \operatorname{sgn}(r)), |b| - r\rangle$ es un par divisor de a por b.

3. Si $a < 0$ y $0 < b$; en este caso $-a = qb + r$ y $0 \leq r < b$.

   - $r = 0$; como $-a = bq$ se cumple $a = b(-q)$ y así $\langle -q, 0\rangle = \langle \operatorname{sgn}(a)\operatorname{sgn}(b)(q + \operatorname{sgn}(r)), 0\rangle$ es un par divisor de a por b.
   - $0 < r$; entonces:

$$\begin{aligned} a &= -bq - r \\ &= b(-q) - r \\ &= b(-q) + 0 - r) \\ &= b(-q) - b + b - r \\ &= b(-q - 1) + (b - r) \\ &= b(-q - 1) + (|b| - r) \end{aligned}$$

     y también $0 < b - r < b$. En definitiva, $\langle -q - 1, b - r\rangle = \langle \operatorname{sgn}(a)\operatorname{sgn}(b)(q + \operatorname{sgn}(r)), |b| - r\rangle$

□

Teorema 1.2.7 (teorema de la división). *Para todo* $a, b \in \mathbb{Z}$ *tales que* $b \neq 0$ *existe un único par divisor de* a *por* b.

Demostración. Supongamos que $a, b \in \omega$ y que $b \neq 0$. La demostración de la **existencia** es por inducción. Si $a = 0$, en tal caso $0 = b0 + 0$ y así $\langle 0, 0\rangle$ es un par divisor de a por b. Supongamos que $a \neq 0$ y que para todo $0 \leq c < a$ existen q_c y r_c tales que $c = q_c b + r_c$. Podemos distinguir dos casos:

1. Si $a < b$ entonces $a = 0b + a$, como $0 \leq a < b$ podemos tomar $q = 0$ y $r = a$.

2. Si $b \leq a$, sea $c = a - b$. En este caso $0 \leq c < a$. Por hipótesis de inducción, $c = q_c b + r_c$, para ciertos q_c y r_c tales que $0 \leq r_c < a$. Pero entonces:

$$\begin{aligned} a &= b + c \\ &= b + q_c b + r_c \\ &= b(q_c + 1) + r_c \end{aligned}$$

   y $0 \leq r_c < b$. Así pues, en este caso podemos tomar $q = q_c + 1$ y $r = r_c$.

Por el principio de inducción la existencia queda probada para todo $a, b \in \omega$ tal que $b \neq 0$. La existencia en los restantes casos está garantizada por lo establecido en el Lema 1.2.6. Para la **unidad**, supongamos que existen $q, q', r, r' \in \mathbb{Z}$ tales que $a = bq + r = bq' + r'$ y que $0 \leq r < |b|$ y que $0 \leq r' < |b|$. Supongamos, para fijar ideas, que $r \leq r'$ y consideremos $a - a$, o sea, $0 = b(q - q') + (r - r')$, o $b(q - q') = r' - r$. Se pueden dar dos casos:

1. $0 < b$. Como $0 \leq r' - r \leq r'$ y $r' < b$, se tiene $0 \leq b(q - q') < b$. De donde, $0 \leq q - q' < 1$ y por tanto $q - q' = 0$, o sea, $q = q'$. Entonces $r' - r = b(q - q') = 0$, de donde $r' = r$.

2. $b < 0$. Como $r' - r = b(q - q')$ y $0 \leq r' - r \leq r \leq -b$, entonces $0 \leq b(q - q') < -b$. Por tanto, $0 \leq q' - q < 1$. Así pues, $q' - q = 0$, o equivalentemente, $q' = q$. Como antes deducimos que $r = r'$.

□

1.3. Teorema de Recursión

La inducción se usa para demostrar resultados y también para definir, *definir por recursión*. A tal fin damos una versión particular del conocido como *teorema de recursión*.

Teorema 1.3.1 (de recursión). *Sea X un conjunto, $a \in X$ y $f\colon X \longrightarrow X$ una función. Existe una única función $u\colon \omega \longrightarrow X$ tal que $u(0) = a$ y que para todo $n \in \omega$, $u(n^+) = f\big(u(n)\big)$.*

Observación 1.3.1. Cada vez que se usa se usa el teorema 1.3.1, decimos que se ha hecho una definición recursiva.

En general es fácil de usar este teorema, aunque a veces puede parecer que las definiciones se complican. Veamos el ejemplo de la función factorial y de la *sucesión de Fibonacci*.

Ejemplo 1.3.1. Sea $x = \omega \times \omega$, $a = \langle 1, 1\rangle$ y $f : x \longrightarrow x$ definida como $f(n, m) = \langle nm, n^+\rangle$. El teorema afirma que existe una única función

$$u\colon \omega \longrightarrow \omega \times \omega$$

que cumple $u(0) = \langle 1, 1\rangle$ y $u\big(s(n)\big) = f\big(u(n)\big)$, para todo $n \in \omega$. Representemos por fac a la función $\pi_1 \circ f$, donde π_1 es la proyección de $\omega \times \omega$ en su primera coordenada. A fac se le denomina *función factorial*. Es fácil demostrar que $\mathrm{fac}(0) = 1$ y (por inducción) que para todo número natural n, $\mathrm{fac}(n + 1) = (n + 1)\,\mathrm{fac}(n)$.

Ejemplo 1.3.2. Sea $x = \omega \times \omega \times \omega$, $a = \langle 0, 1, 0\rangle$ y $f : x \longrightarrow x$ definida como $f(n, m, s) = \langle n + m, n, m\rangle$. El *teorema de recursión* afirma que existe una única función

$$u\colon \omega \longrightarrow \omega \times \omega \times \omega$$

que cumple $u(0) = \langle 0, 1, 0\rangle$ y $u\big(s(n)\big) = f\big(u(n)\big)$, para todo $n \in \omega$. Llamemos ν a la composición $\pi_1 \circ f$, donde π_1 es la proyección de $\omega \times \omega \times \omega$ sobre su primera coordenada. A ν se le denomina *sucesión de Fibonacci*. Es fácil demostrar que $\nu(0) = 0$, $\nu(1) = 1$ y (por inducción) que para todo $n \in \omega$, $\nu(n + 2) = \nu(n + 1) + \nu(n)$.

1.4. Ejemplos

Ejemplo 1.4.1. Demuestre que para todo número entero n y para todo número complejo no nulo z, que expresado en forma polar sea —digamos— $\cos\theta_z + i\sin\theta_z$, se cumple que:

$$z^n = \cos(n\theta_z) + i\sin(n\theta_z) \tag{1.4}$$

Concluya que para todo número complejo no nulo $z = r_z(\cos\theta_z + i\sin\theta_z)$ y todo número entero n se cumple (fórmula de *De Moivre*):[3]

$$z^n = r_z^n(\cos(n\theta_z) + i\sin(n\theta_z)) \tag{1.5}$$

Solución. En primer lugar haremos la demostración de la igualdad (1.4) cuando n es natural y será por medio del principio de inducción matemática. En el **caso base**, tenemos por una parte que:

$$\cos(0\theta_z) + i\sin(0\theta_z) = 1 + 0i = 1 = z^0$$

Supongamos que n es un número natural y que $z^n = \cos(n\theta_z) + i\sin(n\theta_z)$ **(hipótesis de inducción)** y demostremos, en el **paso de inducción**, que $z^{n+1} = \cos((n + 1)\theta_z) + i\sin((n + 1)\theta_z)$. En efecto:

$$\begin{aligned}
z^{n+1} &= (\cos\theta_z + i\sin\theta_z)^{n+1}\\
&= (\cos\theta_z + i\sin\theta_z)^n(\cos\theta_z + i\sin\theta_z)\\
&= (\cos(n\theta_z) + i\sin(n\theta_z))(\cos\theta_z + i\sin\theta_z)\\
&= \cos(n\theta_z)\cos\theta_z - \sin(n\theta_z)\sin(\theta_z) + i(\cos(n\theta_z)\sin\theta_z + \sin(n\theta_z)\cos(\theta_z))\\
&= \cos((n + 1)\theta_z) + i\sin((n + 1)\theta_z)
\end{aligned}$$

Por el principio de inducción matemática, la igualdad (1.4) vale para todo número natural n. Si $n < 0$, sea $m = |n| = -n$. Entonces:

$$\begin{aligned}
(\cos\theta_z + i\sin\theta_z)^n &= (\cos\theta_z + i\sin\theta_z)^{-m}\\
&= \frac{1}{(\cos\theta_z + i\sin\theta_z)^m}\\
&= \frac{1}{\cos(m\theta_z) + i\sin(m\theta_z)}\\
&= \cos(m\theta_z) - i\sin(m\theta_z)\\
&= \cos(-m\theta_z) + i\sin(-m\theta_z)\\
&= \cos(n\theta_z) + i\sin(n\theta_z)
\end{aligned}$$

[3] Recuerde que si $z = a + bi$ es cualquier número complejo no nulo, entonces $z^{-1} = \frac{a-bi}{a^2+b^2}$; es decir $z^{-1} = \frac{\overline{z}}{|z|^2}$ lo que es deducido sin más que observar que:

$$\frac{1}{z} = \frac{\overline{z}}{z\overline{z}}$$

Por lo que la igualdad (1.4) vale para todo número entero n. Supongamos ahora que $z = r_z(\cos\theta_z + i\sin\theta_z)$. Entonces:

$$\begin{aligned} z^n &= (r_z(\cos\theta_z + i\sin\theta_z))^n \\ &= r_z^n(\cos\theta_z + i\sin\theta_z)^n \\ &= r_z^n(\cos(n\theta_z) + i\sin(n\theta_z)) \end{aligned}$$

lo que demuestra la igualdad (1.5). □

Ejemplo 1.4.2. Considere la función f de variable natural y valores reales definida como:

$$f(n) = \begin{cases} 0, & \text{si } n = 0 \\ \sqrt{n + f(n-1)}, & \text{en otro caso.} \end{cases}$$

Demuestre que para todo número natural n se cumple que $f(n) < 1 + \sqrt{n}$.

Solución. Como primera aproximación al problema veamos **sin rigor** la idea intuitiva que nos permitirá su solución. Supongamos que estuviera resuelto, entonces tendríamos en particular que:

$$\sqrt{n + 1 + f(n)} < 1 + \sqrt{n+1}$$

dada la naturaleza del problema, valdrían las siguientes expresiones equivalentes:

$$\begin{aligned} \sqrt{n + 1 + f(n)} < 1 + \sqrt{n+1} \text{ sii } (\sqrt{n + 1 + f(n)})^2 &< (1 + \sqrt{n+1})^2 \\ \text{sii } n + 1 + f(n) &< 1 + (n+1) + 2\sqrt{n+1} \\ \text{sii } f(n) &< 1 + 2\sqrt{n+1} \end{aligned} \tag{1.6}$$

En definitiva, si fuésemos capaces de establecer (1.6), tendríamos lo que queremos sin más que "deslizarse" por la cadena de equivalencias. Como supuestamente (por hipótesis de inducción, ¡ahora vemos que un razonamiento por inducción será imprescindible!) $f(n) < 1 + \sqrt{n}$, bastaría con demostrar que $1 + \sqrt{n} \leq 1 + 2\sqrt{n+1}$. Nuevamente buscaremos una condición equivalente a ésta que, de ser cierta, indicaría que ésta lo es:

$$\begin{aligned} 1 + \sqrt{n} \leq 1 + 2\sqrt{n+1} \text{ sii } \sqrt{n} &\leq 2\sqrt{n+1} \\ \text{sii } n &\leq 4(n+1) \end{aligned} \tag{1.7}$$

No sólo que (1.7) es cierta, sino que vale con la desigualdad estricta, es decir, para todo número natural n:

$$n < 4(n+1) \tag{1.8}$$

No obstante, esta afirmación puede ser demostrada por inducción. Ahora sabemos que podremos hacer un razonamiento por inducción correcto, que resolverá el problema y que será fundado sobre (1.8). Sabemos que el problema es muy simple porque la acotación no es exigente ... y no lo es porque la desigualdad (1.8) es "muy holguera".

Ahora haremos el desarrollo **riguroso**.[4] El razonamiento es por medio del principio de inducción matemática razonando sobre n según el predicado $P(n)$ del tenor:

$$f(n) < 1 + \sqrt{n}$$

Así pues:

[4] Si a y b son números reales positivos, entonces

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

de donde $\sqrt{a+b} < \sqrt{a} + \sqrt{b}$. Sin embargo, este recurso no es productivo en este problema, como puede ser comprobado.

- en el **caso base** tenemos lo siguiente:

$$\begin{aligned} f(0) &= 0 \\ &< 1 \\ &= 1 + 0 \\ &= 1 + \sqrt{0} \end{aligned}$$

  por lo que $P(0)$ es cierta.

- Supongamos, como hipótesis de inducción, que n es un número natural y que $P(n)$ es cierta, es decir, que $f(n) < 1 + \sqrt{n}$

- En el **paso de inducción** comprobaremos que $P(n+1)$ es cierta. En efecto,

$$\begin{aligned} n < 4(n+1) &\Rightarrow \sqrt{n} < 2\sqrt{n+1} \\ &\Rightarrow 1 + \sqrt{n} < 1 + 2\sqrt{n+1} \\ &\Rightarrow f(n) < 1 + 2\sqrt{n+1} && \text{(hip. de inducción)} \\ &\Rightarrow (n+1) + f(n) < (n+1) + 1 + 2\sqrt{n+1} \\ &\Rightarrow (n+1) + f(n) < (1 + \sqrt{n+1})^2 \\ &\Rightarrow \sqrt{(n+1) + f(n)} < 1 + \sqrt{n+1} && (1.9) \end{aligned}$$

  En definitiva, por la validez de (1.8) y la hipótesis de inducción se tiene de (1.9) que

$$f(n+1) < 1 + \sqrt{n+1}$$

Por el *principio de inducción matemática* tenemos que para todo número natural n es cierta $P(n)$, como queríamos demostrar. □

Ejemplo 1.4.3. Demuestre que para todo número natural n tal que $1 < n$ se cumple:

$$\sqrt{n} < \sum_{k=1}^{n} \frac{1}{\sqrt{k}}$$

Solución. El razonamiento es mediante el *principio de inducción matemática* sobre n según el predicado $P(n)$ del tenor:

$$\sqrt{n} < \sum_{k=1}^{n} \frac{1}{\sqrt{k}}$$

y es como sigue:

- En el **caso base** $n = 2$; se tiene lo siguiente:

$$\begin{aligned} 1 < 2 &\Rightarrow 1 = \sqrt{1} < \sqrt{2} \\ &\Rightarrow 2 = 1 + 1 < 1 + \sqrt{2} \\ &\Rightarrow (\sqrt{2})^2 < 1 + \sqrt{2} \\ &\Rightarrow \sqrt{2} < \frac{1 + \sqrt{2}}{\sqrt{2}} = 1 + \frac{1}{\sqrt{2}} \end{aligned}$$

  Concluimos entonces que:

$$\sqrt{2} < 1 + \frac{1}{\sqrt{2}}$$

  y de ahí que $P(2)$ sea cierta.

- Supongamos que n es un número natural tal que $2 \leq n$ y como **hipótesis de inducción** que $P(n)$ es cierta, es decir, que:

$$\sqrt{n} < \sum_{k=1}^{n} \frac{1}{\sqrt{k}}$$

- En el **paso de inducción** demostraremos que $P(n+1)$ es cierta, es decir, que:

$$\sqrt{n+1} < \sum_{k=1}^{n+1} \frac{1}{\sqrt{k}}$$

El razonamiento es como sigue:

$$\begin{aligned} n &= \sqrt{n}^2 \\ &= \sqrt{n}\sqrt{n} \\ &< \sqrt{n}\sqrt{n+1} \\ &\Rightarrow n+1 < 1 + \sqrt{n}\sqrt{n+1} \\ &\Rightarrow \sqrt{n+1}^2 < 1 + \sqrt{n}\sqrt{n+1} \\ &\Rightarrow \sqrt{n+1} < \frac{1 + \sqrt{n}\sqrt{n+1}}{\sqrt{n+1}} \\ &\Rightarrow \sqrt{n+1} < \sqrt{n} + \frac{1}{\sqrt{n+1}} \end{aligned}$$

Así pues:

$$\begin{aligned} \sqrt{n+1} &< \sqrt{n} + \frac{1}{\sqrt{n+1}} \\ &< \left(\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \right) + \frac{1}{\sqrt{n+1}} && \text{(hip. de inducción)} \\ &= \sum_{k=1}^{n+1} \frac{1}{\sqrt{k}} \end{aligned}$$

y esto signifca que $P(n+1)$ es cierta.

Por el *principio de inducción matemática* concluimos que para todo número natural n mayor que 1, $P(n)$ es cierta. □

Ejemplo 1.4.4. Demuestre que para todo número natural n:

$$\left(\sum_{k=0}^{n} k \right)^2 = \left(\sum_{k=0}^{n-1} k \right)^2 + n^3$$

Solución. Se dan los siguientes casos:

- $n = 0$;

$$\begin{aligned}\left(\sum_{k=0}^{-1} k\right)^2 + n^3 &= 0 + 0^3 \\ &= 0 \\ &= 0^2 \\ &= \left(\sum_{k=0}^{0} k\right)^2\end{aligned}$$

- $n = 1$;

$$\begin{aligned}\left(\sum_{k=0}^{0} k\right)^2 + 1^3 &= 0^2 + 1^3 \\ &= 1 \\ &= \left(\sum_{k=0}^{1} k\right)^2\end{aligned}$$

- $n > 1$;

$$\begin{aligned}\left(\sum_{k=0}^{n} k\right)^2 &= \left(\sum_{k=0}^{n-1} k\right)^2 + n^2 + 2n\sum_{k=0}^{n-1} k \\ &= \left(\sum_{k=0}^{n-1} k\right)^2 + n^2 + 2n\frac{(n-1)n}{2} \\ &= \left(\sum_{k=0}^{n-1} k\right)^2 + n^2 + (n-1)n^2 \\ &= \left(\sum_{k=0}^{n-1} k\right)^2 + n^2(n-1+1) \\ &= \left(\sum_{k=0}^{n-1} k\right)^2 + n^3\end{aligned}$$

□

Ejemplo 1.4.5. Demuestre que para todo número natural n vale la siguiente igualdad (*Teorema de Nicomachus*):

$$\sum_{k=0}^{n} k^3 = \left(\sum_{k=0}^{n} k\right)^2$$

Solución. La demostración es por inducción sobre n según el predicado $P(n)$ del tenor:

$$\sum_{k=0}^{n} k^3 = \left(\sum_{k=0}^{n} k\right)^2$$

según el siguiente razonamiento:

- (**caso base**) $n = 0$;

$$\begin{aligned}\sum_{k=0}^{0} k^3 &= 0^3\\ &= 0\\ &= 0^2\\ &= \left(\sum_{k=0}^{0} k\right)^2\end{aligned}$$

  lo que significa que $P(0)$ es cierta

- (**hipótesis de inducción**) Supongamos que n es un número natural y que $P(n)$ vale.

- (**paso de inducción**) Demostremos que $P(n+1)$ vale; para ello consideremos la siguiente cadena de igualdades:

$$\begin{aligned}\sum_{k=0}^{n+1} k^3 &= \left(\sum_{k=0}^{n} k^3\right) + (n+1)^3 && \text{asociatividad}\\ &= \left(\sum_{k=0}^{n} k\right)^2 + (n+1)^3 && \text{hip. de inducción}\\ &= \left(\sum_{k=0}^{n+1} k\right)^2 && \text{Ejercicio 1.4.4}\end{aligned}$$

Por el *principio de inducción matemática* sabemos que para todo número natural n vale $P(n)$. □

Ejemplo 1.4.6. Pruebe que el producto de tres números naturales consecutivos cualesquiera es divisible por 6.

Solución. Sea p la aplicación entre números naturales que al número natural n cualquiera le asigna $p(n) = n(n+1)(n+2)$. El razonamiento es por inducción sobre n según el enunciado $P(i)$ del tenor "6 divide a $p(i)$". Como $p(0) = 0$ está claro que $P(0)$ es cierta (**caso base**). Supongamos que k es un número natural y que $P(k)$ es cierta (**hipótesis de inducción**), es decir, que existe un número natural k' tal que $p(k) = 6k'$; demostremos (en el **paso de inducción**) que como consecuencia $P(k+1)$ es cierta. Para ello consideremos:

$$\begin{aligned}p(k+1) - p(k) &= (k+1)(k+2)(k+3) - k(k+1)(k+2)\\ &= (k+3-k)(k+2)(k+3)\\ &= 3(k+1)(k+2)\end{aligned}$$

Al ser consecutivos los números $k+1$ y $k+2$, exactamente uno de los dos es par, por lo que $(k+1)(k+2)$ es par, o sea, existirá un número natural k'' tal que $(k+1)(k+2) = 2k''$. Recapitulando, tenemos que:

$$\begin{aligned}6k'' &= 3(2k'')\\ &= p(k+1) - p(k)\\ &= p(k+1) - 6k'\end{aligned}$$

y así pues $p(k+1) = 6k'' + 6k' = 6(k'' + k')$, o equivalentemente, $6 \mid p(k+1)$. Por el principio de inducción matemática sabemos que para todo número natural i, $P(i)$ es cierta y ello es lo que se quería demostrar. □

Ejemplo 1.4.7. Cualesquiera dos números naturales a y b tienen un mínimo común múltiplo, esto es, un número m que es múltiplo común a a y b y es divisor de cualquier otro múltiplo común a ambos.[5]

Solución. La **primera** solución que damos es **vía** el **Principio del Buen Orden**. Si $a = 0$ ó $b = 0$, entonces el único múltiplo común a ambos es 0, de hecho, el mínimo común múltiplo de a y b. Supongamos ahora que ninguno de ellos es nulo y llamemos M_{ab} al conjunto de los naturales múltiplos comunes a a y b y $V_{ab} = M_{ab} \setminus \{0\}$. El conjunto V_{ab} es no vacío pues al menos contiene a ab. Por el *Principio de Buen Orden*, deberá contener un elemento mínimo m y éste será mínimo común múltiplo de a y de b. En efecto:

- $a \mid m$ y $b \mid m$, pues $m \in V_{ab}$.
- Supongamos que $n \in V_{ab}$. Por el **Teorema de la División**, existen números naturales q y r tales que $n = mq + r$ y $0 \leq r < m$. Se tiene que $r \in M_{ab}$, puesto que $m, n \in V_{ab}$; pero como $r < m$ y m es el mínimo de V_{ab} obligatoriamente estará en $M_{ab} \setminus V_{ab}$, es decir, $r = 0$. Así pues, $m \mid n$.

De lo anterior se deduce que m es un mínimo común múltiplo de a y b, de hecho, el único no negativo que es representado por $[a, b]$. La **segunda** solución es **vía** el concepto de máximo común divisor de números enteros a y b, esto es, un número m que es divisor común a a y b y es múltiplo de cualquier otro divisor común a ambos. Si, en un inocente abuso del lenguaje, la frase "m es máximo común divisor de a y b" es abreviada por $(a, b) = m$, hemos de destacar dos propiedades:

- $(a, 0) = a$ (razone la verdad de esta afirmación)
- $(a, b) = (b, a \mod b)$ (demuestre, como sencillo ejercicio aritmético, la verdad de esta afirmación)

Razonemos ahora por el **Segundo Principio de Inducción** según el enunciado $P(k)$ del tenor "para todo número natural m, existe (a, k)". Supongamos, como **hipótesis de inducción**, que n es un número natural y que el resultado es cierto para todo número natural k que cumpla $k < n$. Razonamos por casos:

- $n = 0$; sea cual sea el número natural m se tiene $(m, 0) = m$, es decir, existe un máximo común divisor de m y 0 por cumplir m las propiedades necesarias al efecto.
- $n \neq 0$; por el Teorema de la División, existen números q, r tales que $m = nq + r$ y $0 \leq r < n$ (r el valor que hemos nombrado como $m \mod n$). Como $m \mod n < n$, de la hipótesis de inducción se deduce que existe un máximo común divisor de n y m que, según sabemos, es un máximo común divisor de m y n.

Concluimos que $P(k)$ vale para todo número natural k. Para cualesquiera números enteros m y n, (m, n) representará al único entero no negativo que cumple las propiedades de máximo común divisor. Ahora bien, es fácil entender que:

- para cualesquiera números naturales m y n, $(m, n) \mid m$, por lo que existirá un natural u tal que $(m, n)u = mn$.

[5] Cuídese de sustituir la expresión "es divisor de" con la de "es menor o igual que". Si así fuera, 15 no podría ser mínimo común múltiplo de 3 y 5, ya que no es menor o igual que -15, cuando 15 y $(-1)15$ cumplen lo necesario para serlo y, por convenio, se ha elegido en el caso de los números enteros al positivo entre los dos asociados como "el" mínimo común múltiplo. Sin salir del ámbito de los número naturales, más doloroso sería razonar con 0, que es múltiplo de cualquier entero; nuestro error lo convertiría en el mínimo común múltiplo de cualquier pareja de números naturales.

- u es un mínimo común múltiplo de m y n, por lo que la existencia de máximo común divisor es garantía suficiente de la existencia de mínimo común múltiplo.

□

Ejemplo 1.4.8 (Multiplicación por el *Método del Campesino Ruso*). Sea p la función dada por:

$$\begin{aligned} &p(a,0) = 0, \\ &p(a,b) = \begin{cases} p\left(2a, \frac{b}{2}\right) & \text{si } b \text{ es par,} \\ p\left(2a, \frac{b-1}{2}\right) + a & \text{si } b \text{ es impar.} \end{cases} \end{aligned}$$

Demuestre por inducción que para cualesquiera números naturales a y b, $p(a,b) = ab$.

Solución. La demostración es por el **segundo principio de inducción** según el enunciado $P(i)$ del tenor:

$$\text{Para todo número natural } m, \; p(m,i) = mi$$

Supongamos que n es un número natural y que para todo número natural $k < n$ es cierta $P(k)$ **(hip. de inducción)**. En el **paso de inducción** demostraremos que $P(n)$ es cierta. En efecto, son posibles dos casos, que distinguiremos por tener cada uno un tratamiento distinto:

- n par; en este caso, a su vez, hay dos posibilidades:
  - $n = 0$; sea cual sea el número natural m, $p(m,0) = 0 = m0$. Así pues vale $P(0)$. Obsérvese que en este caso no es necesario hacer uso de la hipótesis de inducción.
  - $n \neq 0$ y n es par; sea cual sea el número natural m,

$$\begin{aligned} p(m,n) &= p\left(2m, \frac{n}{2}\right) && \text{por definición de } p \\ &= 2m\frac{n}{2} && \text{de la hip. de inducción, ya que } \frac{n}{2} < n \\ &= mn \end{aligned}$$

- n es impar; sea cual sea el número natural m,

$$\begin{aligned} p(m,n) &= p\left(2m, \frac{n-1}{2}\right) + m && \text{por definición de } p \\ &= 2m\frac{n-1}{2} + m && \text{de la hip. de inducción, ya que } \frac{n-1}{2} < n \\ &= m(n-1) + m \\ &= mn \end{aligned}$$

Así pues, en aplicación del *Segundo Principio de Inducción*, $P(i)$ es cierta para todo número natural i y ello es lo que se pedía. □

Ejemplo 1.4.9. Sea $\{f_n\}$ una sucesión de números enteros tal que:

- $f_0 = 0$ y
- para cualesquiera números naturales m y n $f_n \equiv f_{n-m} \pmod{f_m}$ siempre que $m < n$.

Demuestre que:

1. $(f_n, f_m) = (f_{n-m}, f_m)$ siempre que m y n sean números naturales tales que $m < n$.
2. Para cualesquiera números naturales m y n, $(f_m, f_n) = f_{(m,n)}$.
3. Para cualesquiera números naturales a, m y n demuestre que:

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$$

Demostración.

1. Sean m y n números naturales tales que $m < n$. Por la definición de $\{f_n\}_n$ se tiene que existe un número entero k tal que $f_n = f_{n-m} + kf_m$. Así pues,

$$\begin{aligned}(f_n, f_m) &= (f_n - kf_m, f_m)\\ &= (f_{n-m}, f_m)\end{aligned}$$

2. La demostración es por inducción según el predicado $P(u)$ del tenor:

   para cualesquiera números naturales m y n, si $m + n = u$ entonces $(f_m, f_n) = f_{(m,n)}$

   Supongamos como hipótesis de inducción que u es un número natural sin otro condicionante aparte de que para todo $0 \leq k < u$, $P(k)$ es cierto. Tenemos los siguientes casos:

   - $u = m + n$ y $n = 0$;

$$\begin{aligned}(f_m, f_0) &= (f_m, 0)\\ &= f_m\\ &= f_{(m,0)}\\ &= f_{(m,n)}\end{aligned}$$

   - $u = m + n$ y $m = 0$; mismo esquema de razonamiento.
   - $u = m + n$ y $m = n$; $(f_n, f_n) = f_n = f_{(n,n)}$.
   - $u = m + n$ y $0 < m < n$; entonces:

$$\begin{aligned}(f_n, f_m) &= (f_{n-m}, f_m) && (1)\\ &= f_{(n-m,m)} && (n-m) + m = n < u \text{ y hip. induc.}\\ &= f_{(n,m)}\end{aligned}$$

   - $u = m + n$ y $0 < n < m$; mismo esquema de razonamiento.

   Hemos demostrado que para todo número natural u, si para todo $0 \leq k < u$ se tiene que $P(u)$ es cierto, entonces $P(u)$ es cierto. Por el segundo principio de inducción tenemos que para todo número natural u, $P(u)$ es cierto y eso es lo que queríamos demostrar.

3. Consideremos $f_n = a^n - 1$. Claro está que $f_0 = 0$. Por otra parte, dado que:

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

   entonces lo que se tiene es que $f_n = f_{n-m} + kf_m$ y según lo que establece (2) debe cumplirse que para cualesquiera números naturales m y n, $(f_m, f_n) = f_{(m,n)}$, esto es, que para cualesquiera números naturales m y n, $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

□

Ejemplo 1.4.10. Sean a, b, m y n números naturales. Demuestre que:

$$a^n - b^n = (a-b)\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right) \tag{1.10}$$

y que si m es un divisor de n entonces $a^m - b^m$ es un divisor de $a^n - b^n$. Seguidamente suponga que $1 \leq a < b$, que $(a,b) = 1$ y que tanto m como n son números naturales no nulos para demostrar que:

1. $(a^{(m,n)} - b^{(m,n)})|(a^n - b^n, a^m - b^m)$

2. $(a^n - b^n, a^m - b^m)|(a^{(m,n)} - b^{(m,n)})$

3. $(a^n - b^n, a^m - b^m) = a^{(m,n)} - b^{(m,n)}$

Demostración. Demostremos en primer lugar (1.10) mediante un razonamiento inductivo según el predicado $P(n)$ del tenor:

$$a^n - b^n = (a-b)\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right)$$

donde n es número natural. Para ello:

- $n = 0$ **(caso base)**; en efecto,

$$\begin{aligned} a^0 - b^0 &= 1 - 1 \\ &= 0 \\ &= (a-b)0 \\ &(a-b)\left(\sum_{k=1}^{0} a^{n-k}b^{k-1}\right) \end{aligned}$$

  lo que demuestra que vale $P(0)$.

- Supongamos, como **hipótesis de inducción,** que n es un número natural al que no se le exige nada aparte de que $P(n)$ es cierto, o sea, que $a^n - b^n = (a-b)\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right)$.

En el **paso de inducción** demostraremos que entonces $P(n+1)$ es cierto, esto es, que:

$$a^{n+1} - b^{n+1} = (a-b)\left(\sum_{k=1}^{n+1} a^{(n+1)-k}b^{k-1}\right)$$

En efecto:

$$\begin{aligned}
a^{n+1} - b^{n+1} &= a^{n+1} - ab^n + ab^n - b^{n+1} \\
&= (a^n - b^n)a + ab^n - b^{n+1} \\
&= (a-b)\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right)a + ab^n - b^{n+1} && \text{(hip. induc.)} \\
&= (a-b)\left(\sum_{k=1}^{n} a^{(n+1)-k}b^{k-1}\right) + ab^n - b^{n+1} \\
&= (a-b)\left(\sum_{k=1}^{n} a^{(n+1)-k}b^{k-1}\right) + (a-b)b^n \\
&= (a-b)\left(\left(\sum_{k=1}^{n} a^{(n+1)-k}b^{k-1}\right) + b^n\right) \\
&= (a-b)\left(\sum_{k=1}^{n+1} a^{(n+1)-k}b^{k-1}\right)
\end{aligned}$$

Hemos demostrado que $P(0)$ vale y que para todo número natural n, $P(n+1)$ vale siempre que $P(n)$ valga. El *principio de inducción matemática* permite asegurar que para todo número natural n, $P(n)$ vale y eso es lo que se quería demostrar. Supongamos ahora que m y n son números naturales y que $m \mid n$, es decir, que existe otro número natural s tal $ms = n$; se tiene entonces:

$$\begin{aligned}
a^n - b^n &= a^{ms} - b^{ms} \\
&= (a^m)^s - (b^m)^s \\
&= (a^m - b^m)\left(\sum_{k=1}^{s} a^{s-k}b^{k-1}\right)
\end{aligned}$$

de donde $a^m - b^m$ es un divisor de $a^n - b^n$. Supongamos seguidamente que $1 \leq a < b$, que $(a,b) = 1$ y que tanto m como n son números naturales no nulos. Entonces:

1. Dado que $(m,n) \mid m$ y $(m,n) \mid n$, se tiene entonces que $(a^{(m,n)} - b^{(m,n)}) \mid (a^n - b^n)$ y $(a^{(m,n)} - b^{(m,n)}) \mid (a^m - b^m)$, por lo que:

$$(a^{(m,n)} - b^{(m,n)}) \mid (a^n - b^n, a^m - b^m) \tag{1.11}$$

2. Para abreviar, llamaremos d a $(a^n - b^n, a^m - b^m)$. Sabemos que existen números enteros x e y tales que $mx + ny = (m,n)$. Por otra parte $(a,b) = 1$ es equivalente a que $(a,d) = 1$ y $(b,d) = 1$. Así pues, a^{mx} mód d y a^{ny} mód d existen (observe que tanto x como y pueden ser negativos). Es claro que $d \mid (a^n - b^n)$ y que $d \mid (a^m - b^m)$ o equivalentemente $a^n \equiv b^n \pmod{d}$ y $a^m \equiv b^m \pmod{d}$. Se tiene que $a^{mx} \equiv b^{mx} \pmod{d}$ y que $a^{ny} \equiv b^{ny} \pmod{d}$, por lo que:

$$a^{mx}a^{ny} \equiv b^{mx}b^{ny} \pmod{d}$$

   y esto significa que $a^{(m,n)} \equiv b^{(m,n)} \pmod{d}$ o equivalentemente:

$$(a^n - b^n, a^m - b^m) \mid (a^{(m,n)} - b^{(m,n)}) \tag{1.12}$$

3. Por lo que afirma (1.11) y (1.12) concluimos que:

$$(a^n - b^n, a^m - b^m) = a^{(m,n)} - b^{(m,n)}$$

□

Ejemplo 1.4.11. La *sucesión de los número de Fermat* es la sucesión $\{F_n\}_n$, donde para todo número natural n:

$$F_n = 2^{2^n} + 1$$

Demuestre que:

- Para todo número natural n no nulo, $\prod_{k=0}^{n-1} F_k = F_n - 2$.
- Para cualesquiera números naturales m y n, $(F_m, F_n) = 1$ siempre que se cumpla $m \neq n$.
- Los números primos no pueden estar en cantidad finita.

Demostración.

1. El razomamiento es por inducción sobre el número natural no nulo n según el predicado $P(n)$ del tenor:

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

según los siguientes:

- $n = 1$ (**caso base**); se tiene que $F_0 = 3$ y $F_1 = 5$

$$\begin{aligned}\prod_{k=0}^{0} F_k &= F_0 \\ &= 3 \\ &= 5 - 2 \\ &= F_1 - 2\end{aligned}$$

- Supongamos que n es un número natural no nulo sin otro particular salvo el de cumplir que $P(n)$ vale, es decir, que $\prod_{k=0}^{n-1} F_k = F_n - 2$ (**hip. de inducción**).
- En el **paso de inducción** debemos demostrar que:

$$\prod_{k=0}^{n} F_k = F_{n+1} - 2$$

y efectivamente así es ya que:

$$\begin{aligned}\prod_{k=0}^{n} F_k &= \left(\prod_{k=0}^{n-1} F_k\right) F_n \\ &= (F_n - 2)F_n \\ &= (2^{2^n} + 1 - 2)(2^{2^n} + 1) \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= 2^{2^{n+1}} - 1 \\ &= F_{n+1} - 2\end{aligned}$$

Hemos demostrado que para todo número natural no nulo n, $P(n+1)$ es cierta siempre que lo sea $P(n)$. El principio de inducción matemática permite establecer que para todo número natural no nulo n, $P(n)$ es cierta, y eso es lo que queríamos demostrar.

2. Supongamos que m y n son números naturales tales que $m < n$ y que t es un divisor común a F_n y F_m. Sabemos que:
$$F_n = \left(\prod_{k=0}^{n-1} F_k\right) + 2$$
así que t divide a F_n y $\prod_{k=0}^{n-1} F_k$, por lo que debe ser un divisor de 2; si t fuese igual a 2, F_n sería un número par lo cual es absurdo. Al no tener 2 más factores naturales que 1 y 2, t debe ser igual a 1 y ello es prueba de lo que se quería.

3. Cada número F_n tiene al menos un factor primo que no es compartido con el resto de números de la sucesión, así que los números primos no pueden estar en cantidad finita.

□

Ejemplo 1.4.12. Si n es un número natural cualquiera, sea $f(n) = 2^{2^{n+1}} + 2^{2^n} + 1$. Demuestre que para todo número natural n:

1. $(n^2 - n + 1, n^2 + n + 1) = 1$
2. $f(n)$ tiene al menos $n + 1$ factores primos distintos.

Solución.

1. Si p fuese un factor primo de (m^2-m+1, m^2+m+1), entonces dividiría a $m^2+m+1-(m^2-m+1) = 2m$; pero como tanto $m^2 - m + 1$ como $m^2 + m + 1$ son impares, p debe ser impar. Se deduce entonces que p sería un divisor de m y, por tanto, de $m^2 + m$ y $m^2 + m + 1$; como consecuencia el primo p sería un divisor de 1, lo cual es absurdo. Como consecuencia $(m^2 - m + 1, m^2 + m + 1) = 1$.

2. El razonamiento es por inducción sobre n. El valor de $f(0)$ es 7, por lo que $f(0)$ tiene $0 + 1$, es decir 1, factores. Supongamos, como hipótesis de inducción, que $0 \leq n$ y que el resultado es cierto para n; demostremos que también lo será para $n + 1$, que será un número natural no nulo. Sea $g(x) = x^4+x^2+1$; si $0 < n$ entonces $f(n) = g(2^{2^{n-1}})$ y dado que $x^4+x^2+1 = (x^2-x+1)(x^2+x+1)$ entonces:
$$\begin{aligned} g(2^{2^{n-1}}) &= (2^{2^n} + 2^{2^{n-1}} + 1)(2^{2^n} - 2^{2^{n-1}} + 1) \\ &= ((2^{2^{n-1}})^2 + 2^{2^{n-1}} + 1)((2^{2^{n-1}})^2 - 2^{2^{n-1}} + 1) \\ &= (m^2 - m + 1)(m^2 + m + 1) \qquad (m = 2^{2^{n-1}}) \end{aligned}$$
Así pues:
$$\begin{aligned} f(n+1) &= 2^{2^{n+2}} + 2^{2^{n+1}} + 1 \\ &= (2^{2^{n+1}} + 2^{2^n} + 1)(2^{2^{n+1}} - 2^{2^n} + 1) \\ &= f(n)(2^{2^{n+1}} - 2^{2^n} + 1) \end{aligned}$$
Por la hipótesis de inducción, $f(n)$ tiene al menos $n+1$ factores primos distintos; dado que el número $2^{2^{n+1}} - 2^{2^n} + 1$ es mayor o igual que 3 y $(f(n), 2^{2^{n+1}} - 2^{2^n} + 1) = 1$, entonces $2^{2^{n+1}} - 2^{2^n} + 1$ tiene todos sus factores primos —y al menos hay uno— distintos a los de $f(n)$, es decir, $f(n+1)$ tiene al menos $n + 2$ factores primos.

□

Ejemplo 1.4.13. Demuestre que para todo número natural n vale la siguiente igualdad:

$$\overbrace{11\ldots1}^{2n)} - \overbrace{22\ldots2}^{n)} = (\overbrace{33\ldots3}^{n)})^2$$

Demostración. Definamos las siguientes funciones:

$$\begin{array}{lll} f(0) = 0 & g(0) = 0 & h(0) = 0 \\ f(n+1) = f(n)10^2 + 11 & g(n+1) = g(n)10 + 2 & h(n+1) = h(n)10 + 3 \end{array}$$

En primer lugar demostremos por el *principio de inducción matemática* que para todo número natural n, $3g(n) = 2h(n)$; ello puede ser sirviéndonos del enunciado $Q(k)$ del tenor:

$$3g(k) = 2h(k) \tag{1.13}$$

En efecto, si $n = 0$ entonces $3g(0) = 3 \cdot 0 = 0 = 2 \cdot 0 = 2 \cdot h(0)$, es decir, vale $Q(0)$. Supongamos que para el número natural n vale $Q(n)$; entonces:

$$\begin{aligned} 3g(n+1) &= 3(g(n)10 + 2) \\ &= 3g(n)10 + 6 \\ &= 2h(n)10 + 6 \\ &= 2(h(n)10 + 3) \\ &= 2h(n+1) \end{aligned}$$

de lo que deducimos que para todo número natural k, vale $Q(k)$. Multiplicando ahora la igualdad (1.13) por 30 obtenemos que para todo número natural n, $9g(n)10 = 60h(n)$ y por tanto:

$$\begin{aligned} 60h(n) &= (10-1)g(n)10 \\ &= g(n)10^2 - g(n)10 \end{aligned}$$

Se tiene, en definitiva, que para todo número natural n,

$$60h(n) - g(n)10^2 = -g(n)10 \tag{1.14}$$

Seguidamente demostremos lo que se pide usando el *principio de inducción matemática* según el enunciado $P(k)$ del tenor:

$$f(k) - g(k) = h(k)^2$$

En el **caso base** demostremos que vale $P(0)$. En efecto:

$$f(0) - g(0) = 0 - 0 = 0 = 0^2 = h(0)^2$$

Supongamos que n es un número natural y que para él es cierto $P(n)$ (**hipótesis de inducción**) y demostremos que en consecuencia es cierto $P(n+1)$. En efecto,

$$\begin{aligned} f(n+1) - g(n+1) &= f(n)10^2 + 11 - (10g(n) + 3) \\ &= f(n)10^2 + 11 - 10g(n) - 3 \\ &= f(n)10^2 - g(n)10 + 9 \\ &= f(n)10^2 + 9 + 60h(n) - g(n)10^2 && \text{por (1.14)} \\ &= (f(n) - g(n))10^2 + 9 + 60h(n) \\ &= h(n)^2 10^2 + 3^2 + 2 \cdot 3h(n)10 && \text{por h.i.} \\ &= (h(n)10 + 3)^2 \\ &= h(n+1)^2 \end{aligned}$$

lo que significa que para todo número natural n, vale $P(n)$.[6] □

Ejemplo 1.4.14. Los *números de Fibonacci* son los números de la sucesión:

$$f(n) = \begin{cases} 0, & \text{si } n = 0; \\ 1, & \text{si } n = 1; \\ f(n-1) + f(n-2), & \text{si } 1 < n; \end{cases}$$

Demuestre que para todo número natural n se cumple:

$$f(n) < \left(\frac{5}{3}\right)^n$$

Solución. El razonamiento es por el Segundo Principio de Inducción según el enunciado $P(k)$ del tenor:

$$f(k) < \left(\frac{5}{3}\right)^k$$

Supongamos, como hipótesis de inducción, que n es un número natural y que para todo número natural k tal que $k < n$, vale $P(k)$. El razonamiento es por casos:

- $n = 0$; $f(0) = 0 < 1 = \left(\frac{5}{3}\right)^0$, de donde sabemos que $P(0)$ vale.
- $n = 1$; $f(1) = 1 < \frac{5}{3} = \left(\frac{5}{3}\right)^1$, de donde sabemos que $P(1)$ vale.
- $n > 1$; considere las siguientes realciones:

$$\begin{aligned} f(n) &= f(n-1) + f(n-2) && \text{(por definición)} \\ &< \left(\frac{5}{3}\right)^{n-1} + \left(\frac{5}{3}\right)^{n-2} && \text{(por hip. induc.)} \\ &= \left(\frac{5}{3}\right)^{n-2} \left(\frac{5}{3} + 1\right) \\ &= \left(\frac{5}{3}\right)^{n-2} \frac{8}{3} \\ &< \left(\frac{5}{3}\right)^{n-2} \left(\frac{5}{3}\right)^2 && \text{(pues } 72 < 75\text{)} \\ &= \left(\frac{5}{3}\right)^n \end{aligned}$$

Por el *Segundo Principio de Inducción* sabemos que para todo número natural n, vale $P(n)$. □

Ejemplo 1.4.15. Demuestre que para todo número natural n tal que $6 \leq n$ se cumple $n^3 < n!$

[6] En internet ha circulado la siguiente demostración:

$$\begin{aligned} \frac{10^{2n} - 1}{9} - \frac{2(10^n - 1)}{9} &= \frac{10^{2n} - 2 \cdot 10^n + 1}{9} \\ &= \frac{(10^n - 1)^2}{3^2} \\ &= \left(\frac{10^n - 1}{3}\right)^2. \end{aligned}$$

Ejemplo 1.4.16. Sea $A = \begin{pmatrix} 0 & -1 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{R})$.

1. Demuestre que para cualquier $n \geq 1$ se verifica que $A^n = \begin{pmatrix} -2^n + 2 & -2^n + 1 \\ 2^{n+1} - 2 & 2^{n+1} - 1 \end{pmatrix}$.
2. Particularice la expresión encontrada en el apartado anterior para $n = 0$ y $n = -1$ e identifique esas matrices.

Solución. Para todo número entero n, sea

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

Llamemos $P(n)$ a la igualdad:

$$A^n = B(n)$$

donde n es un número natural cualquiera. Razonaremos por inducción sobre n; para ello:

- $P(1)$ es cierta (*caso base*); en efecto,

$$B(1) = \begin{pmatrix} -2^1 + 2 & -2^1 + 1 \\ 2^{1+1} - 2 & 2^{1+1} - 1 \end{pmatrix} = \begin{pmatrix} -2 + 2 & -2 + 1 \\ 2^2 - 2 & 2^2 - 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 2 & 3 \end{pmatrix} = A = A^1$$

- Sea n un número natural n tal que $1 \leq n$ y supongamos que $B(n) = A^n$, es decir, que es cierta $P(n)$ (*hipótesis de inducción*).
- En el *paso de inducción* el objetivo es demostrar que $B(n+1) = A^{n+1}$, es decir que vale $P(n+1)$, lo cual efectivamente es cierto; en efecto:

$$\begin{aligned}
A^{n+1} &= A^n A && \text{(def. de potencia)} \\
&= B(n)A && \text{(hip. de inducción)} \\
&= \begin{pmatrix} -2^n + 2 & -2^n + 1 \\ 2^{n+1} - 2 & 2^{n+1} - 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 2 & 3 \end{pmatrix} && \text{(valor de } B(n)\text{)} \\
&= \begin{pmatrix} 2(-2^n + 1) & -(-2^n + 2) + 3(-2^n + 1) \\ 2(2^{n+1} - 1) & -(2^{n+1} - 2) + 3(2^{n+1} - 1) \end{pmatrix} && \text{(producto matricial)} \\
&= \begin{pmatrix} -2^{n+1} + 2 & 2^n - 2 - 3 \cdot 2^n + 3 \\ 2^{n+2} - 2 & -2^{n+1} + 2 + 3 \cdot 2^{n+1} - 3 \end{pmatrix} && \text{(desarrollo)} \\
&= \begin{pmatrix} -2^{n+1} + 2 & -2 \cdot 2^n - 2 + 3 \\ 2^{n+2} - 2 & -2 \cdot 2^{n+1} + 2 - 3 \end{pmatrix} && \text{(agrupación)} \\
&= \begin{pmatrix} -2^{n+1} + 2 & -2^{n+1} + 1 \\ 2^{n+2} - 2 & -2^{n+2} - 1 \end{pmatrix} && \text{(simplificación)} \\
&= B(n+1) && \text{(identificación)}
\end{aligned}$$

Por el *principio de inducción matemática* sabemos entonces que para todo número natural n tal que $1 \leq n$ se cumple:

$$A^n = B(n)$$

Por otra parte,

- para $n = 0$:

$$B(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A^0$$

- para $n = -1$:

$$\begin{aligned} B(-1) &= \begin{pmatrix} -2^{-1} + 2 & -2^{-1} + 1 \\ 2^{-1+1} - 2 & 2^{-1+1} - 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 - \frac{1}{2} & 1 - \frac{1}{2} \\ 2^0 - 2 & 2^0 - 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 - \frac{1}{2} & 1 - \frac{1}{2} \\ 1 - 2 & 1 - 1 \end{pmatrix} \\ &= \begin{pmatrix} \frac{3}{2} & \frac{1}{2} \\ -1 & 0 \end{pmatrix} \end{aligned}$$

y como quiera que:

$$AB(-1) = I = B(-1)A$$

se cumple:

$$B(-1) = A^{-1}$$

□

1.5. Ejercicios

1. Demuestre que para todo número natural no nulo n se cumple:

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

2. Demuestre que para cualquier número natural n el número $n^2 - n$ es par. Utilice lo anterior para demostrar que para todo número natural n, $n^3 - 3n^2 - 4n$ es un múltiplo de 6.

3. Demuestre por inducción que para todo número natural n

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

4. Use el teorema de inducción para demostrar que:

$$2^{n-1} \leq n!$$

para todo $n > 0$.

5. Demuestre mediante el teorema de inducción que:

$$\prod_{i=1}^{n} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{n+1}}$$

para todo $n \geq 1$.