Inducción

Fco. M. García Olmedo
Universidad de Granada
España

7 de noviembre de 2018

Resumen

Contiene una introducción general a los contenidos sucintos para poder usar la inducción como herramienta de demostración en matemáticas y aspectos teóricos de las ciencias de la computación.

Índice

Índice de figuras

1. Los Postulados de Peano y la inducción finita

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

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

definida[1] como $s(n) = n^+$, donde $n^+ = n \cup \{n\}$.

En términos de la función s existe una colección de "propiedades básicas" que caracterizan al "conjunto" de los números naturales ω que, como sabemos, es el conjunto de sucesores que está incluido en cualquier otro conjunto de sucesores. Estas propiedades se conocen con el nombre de *Postulados de Peano*.

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

Teorema 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* $n = m$*.*

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 finita.*

Teorema 1.2 (*Principio del Buen Orden*)**.** *Todo conjunto de números naturales no vacío tiene un elemento mínimo.*

Teorema 1.3 (*Segundo Principio de Inducción Finita*)**.** *Sea* P *un conjunto cualquiera de números naturales. Si para todo número natural*[2] n *se cumple:*

$$n \in P \text{ siempre que } n \subseteq P \tag{1}$$

Entonces $P = \omega$*.*

Observación 1.1. Obsérvese que si un subconjunto de números naturales P cumple la condición (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) se debe cumplir $\emptyset \in P$, esto es, $0 \in P$.

Observación 1.2. Obsérvese que la demostración dada del Teorema 1.3 es una consecuencia del Principio del Buen Orden.-

2. Equivalencia entre Principios

Hagamos una síntesis de los principios nombrados hasta ahora:

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

   $$\text{Para todo número natural } n,\ n \in P \text{ siempre que } n \subseteq P \tag{2}$$

   Entonces $P = \omega$.

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

Teorema 2.1. *Si es válido el principio del buen orden entonces es válido el principio de inducción finita.*

Teorema 2.2. *Si es válido el segundo principio de inducción finita entonces es válido el principio del buen orden.*

Corolario 2.3. *Son equivalentes los siguientes principios:*

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

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

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{3}$$

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 **paso base**, para $i = 0$, el miembro de la izquierda de la ecuación (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 Finita*, $P(n)$ es cierta para todo número natural n. □

Teorema 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 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 puede ser expresado como un producto de números primos. 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 $P(i)$ resulta cierta cuando i 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 tanto 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 Finita.* □

3. Ejemplos

Definición 3.1. 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 3.1. *Supongamos que para todo $a, b \in \mathbb{N}$ 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 3.2 (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 $a, b \in \mathbb{N}$ 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 $a, b \in \mathbb{N}$ tal que $b \neq 0$. La existencia en los restantes casos está garantizada por lo establecido en el Lema 3.1. 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 $r = r'$.

□

Ejercicio 3.1. 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:

$$z^n = \cos(n\theta_z) + i\sin(n\theta_z) \tag{4}$$

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]

$$z^n = r_z^n(\cos(n\theta_z) + i\sin(n\theta_z)) \tag{5}$$

Solución. En primer lugar haremos la demostración de la igualdad (4) cuando n es natural y será por medio del principio de inducción finita. 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 Finita, la igualdad (4) vale para todo número natural n. Si $n < 0$, sea $m = |n| = -n$. Entonces:

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

Por lo que la igualdad (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 demustra la igualdad (5). □

[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 $z^{-1} = \frac{\bar{z}}{|z|^2}$ lo que es deducido sin más que observar que:

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

Ejercicio 3.2. 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 finita sabemos que para todo número natural i, $P(i)$ es cierta y ello es lo que se quería demostrar. □

Ejercicio 3.3. 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.[4]

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)

[4] 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.

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

Razonemos ahora por el **Segundo Principio de Inducción Finita** 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 $(m, n)u = mn$.
- 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.

□

Ejercicio 3.4 (Multiplicación por el *Método del Campesino Ruso*). Sea p la función dada por:

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

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 finita** 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 Finita*, $P(i)$ es cierta para todo número natural i y ello es lo que se pedía. □

Ejercicio 3.5. 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:

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

   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.

□

Ejercicio 3.6. 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 Finita* que para todo número natural n, $3g(n) = 2h(n)$; ello puede ser sirviéndonos del enunciado $Q(k)$ del tenor:

$$3g(k) = 2h(k) \tag{6}$$

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 (6) 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,

$$60h(n) - g(n)10^2 = -g(n)10 \tag{7}$$

Seguidamente demostremos lo que se pide usando el *Principio de Inducción Finita* 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,

$$\begin{aligned} f(n+1) - g(n+1) &= f(n)10^2 + 11 - (10g(n) + 3) \\ &= f(n)10^2 + 11 - 10g(n) - 3 \\ &= f(n)10^2 - g(n)10 + 9 \\ &= f(n)10^2 + 9 + 60h(n) - g(n)10^2 && \text{por (7)} \\ &= (f(n) - g(n))10^2 + 9 + 60h(n) \\ &= h(n)^2 10^2 + 3^2 + 2 \cdot 3h(n)10 && \text{por h.i.} \\ &= (h(n)10 + 3)^2 \\ &= h(n+1)^2 \end{aligned}$$

lo que significa que para todo número natural n, vale $P(n)$.[5] □

Ejercicio 3.7. 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 Finita 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:

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

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

[5] En internet ha circulado la siguiente demostración:

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

4. Ejercicios de Inducción

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. Usar el teorema de inducción para demostrar que:

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

para todo $n>0$.

4. Utilizar el teorema de inducción para demostrar que:

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

para todo $n\geq 2$.

5. Demuestre mediante el teorema de inducción que:

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

para todo $n\geq 1$.

6. Todo número natural mayor que 1 puede ser expresado como producto de números primos.

7. Usar el teorema de inducción para demostrar que 3^n+7^n-2 es divisible por 8, para $n\geq 1$.

8. Usar el teorema de inducción para demostrar que para todo número natural n, n^3+2n es divisible por 3.

9. Es cierto que de un número n_0 en adelante se tiene que $100^n<n!$; encuéntrelo y demuestre por inducción lo dicho a partir de ese número n_0.

10. Deduzca del Ejercicio 3.5 que para cualquier conjunto finito de primos, existe uno que no pertenece al mismo (la cantidad de primos no es finita).

11. Se ha dado una demostración falaz del enunciado falso siguiente: "Todos los niños tienen el mismo color de ojos". La demostración es como sigue. Si el grupo de niños es de 1 está claro que todos los del grupo tienen el mismo color de ojos. Supongamos el resultado cierto para todo grupo de tamaño n (con $n\geq 1$) y veamos que es cierto para $n+1$. Si nos dan un grupo de $n+1$ niños y los ordenamos por edad (digamos de menor a mayor), los n primeros tienen el mismo color de ojos al igual que los n últimos. Por tanto, todos los niños del grupo tienen el mismo color de ojos. Ahora bien, los niños forman un conjunto como los mencionados —de mayor o menor tamaño— por lo que el resultado está demostrado. Indique en el argumento dónde está el fallo.

12. Exhiba una solución del Ejercicio 3.3 que haga uso del *Segundo Principio de Inducción Finita* en lugar de su equivalente, el *Principio del Buen Orden*.

13. Sea n un número natural y sea S cualquier conjunto de números naturales menores que n. Demuestre que S es vacío o S tiene máximo.

14. Demuestre que para todo número natural n, 8^n-3^n es múltiplo de 5.

15. Demuestre que para todo número natural n, $3^{4n} - 1$ es múltiplo de 5.

16. Demuestre que para todo número impar n, 9 divide a $4^n + 5^n$.

17. Formalice una demostración no inductiva de lo afirmado en el Ejemplo 2.1.

18. Sea e la función dada por:

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

Demuestre por inducción que para cualesquiera números naturales a y b, $e(a,b) = a^b$. Este método de "elevar" es, con justicia, muy afamado y se le ha llamado *Métod de la Exponenciación Rápida* ... muy usado en el ámbito de la criptografía moderna.

19. Demuestre que para todo número natural n:

$$\sum_{i=0}^{n} i!i = (n+1)! - 1$$

20. Demuestre que para para todo número natural n se cumple:

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

21. Supongamos que disponemos en cantidad suficiente de sellos de 3 y 8 céntimos sólo. Demuestre que con esos sellos, una carta podría ser franqueada con una cántidad de céntimos superior a 13.

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

    a) Demuestre que para cualquier $n \geq 1$ se verifica que $A^n = \begin{pmatrix} -2^n + 2 & -2^n + 1 \\ 2^{n+1} - 2 & 2^{n+1} - 1 \end{pmatrix}$.

    b) Particularice la expresión encontrada en el apartado anterior para $n = 0$ y $n = -1$ e identifique esas matrices.

23. Los *números de Lucas* son los números de la sucesión:

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

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

$$L_n < \left(\frac{7}{4}\right)^n$$

24. Sean $n_0, \ldots, n_d$ puntos distintos de un dominio de integridad $\mathbf{A}$ en cantidad igual a $d+1$ y sea el polinomio $g(x)$ en una variable definido por la siguiente igualdad:

$$g(x) = \prod_{i=0}^{d} (x - n_i)$$

Demuestre que:

$$g'(x) = \sum_{i=0}^{d} \prod_{\substack{j=0 \\ j \neq i}}^{d} (x - n_j)$$

25. Demuestre que para todo número natural superior a 5, $n^3 < n!$.

26. Demuestre que para todo número natural n, el dígito menos significativo de n^5 es igual al dígito menos significativo de n.

27. La sucesión finita de números enteros $e_0, e_1, \cdots e_{n-1}, e_n$ es una `expresión ternaria equilibrada` del número entero b sii, por definición, cumple las siguientes condiciones:

    a) Para todo $0 \leq i \leq n$, $e_i \in \{-1, 0, 1\}$

    b) $b = \sum_{i=0}^{n} e_i 3^i$

    c) $e_n \neq 0$

    El hecho de que se cumplan estas condiciones es abreviado escribiendo:

    $$b = (e_n e_{n-1} \cdots e_1 e_0)_{te}$$

    Demuestre que para todo número entero no nulo b existe una representación ternaria equilibrada. Demuestre también que dicha representación ternaria equilibrada es única.

Ejercicios señalados: 1, 5, 6, 7, 9, 27, 11, 12, 13, 16, 18, 18, 22, 23, 24 y 25.