CAPITULO III

INDUCCION MATEMATICA

Introducción .-

Se denomina inducción todo razonamiento que comprende el paso de proposiciones particulares a generales con la particularidad de que la validez de los últimos se deduce de la validez de los primeros. El método de inducción matemática es un método especial de demostración matemática que permite, a base de observaciones particulares, juzgar de las regularidades generales correspondientes. Para aclarar la idea consideramos el ejemplo siguiente :
Determínese la suma de los n-primeros números impares :

$$1 + 3 + 5 + \ldots + (2n - 1)$$

Sea $S(n)$ la suma de éstos n-números. Tomemos $n = 1, 2, 3, 4$ y 5 ; tenemos :

$$S(1) = 1,$$
$$S(2) = 1 + 3 = 4$$
$$S(3) = 1 + 3 + 5 = 9$$
$$S(4) = 1 + 3 + 5 + 7 = 16 \quad y$$
$$S(5) = 1 + 3 + 5 + 7 + 9 = 25$$

Como se ve para $n = 1, 2, 3, 4$ y 5 la suma de n números impares sucesivos es igual a n^2 . ¿Podemos sacar de aquí inmediatamente la conclusión de que esto tiene lugar para todo n ? No, pues semejante conclusión "por analogía" puede resultar a veces errónea .

Veamos algunos ejemplos :

Consideremos los números de tipo $2^{2^n} + 1$. Para $n = 0, 1, 2, 3,$ y 4 los números $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$; $2^{2^4} + 1 = 65537$ son primos .

P.Fermat ilustre matemático francés del siglo XVII, aceptaba que todos los númemeros de este tipo son primos. Sin embargo, L.Euler eminente sabio y académico de San Petersburgo, encontró en el siglo XVII que $2^{2^5} + 1 = 4294967297 = 641 \times 6700417$ es un número compuesto .

He aquí otro ejemplo del mismo género G.W. Leibniz famoso matemático alemán del siglo XVII y uno de los fundadores de las "Matemáticas Superiores", demostró que cualquiera que sea el entero positivo n, el número n^3-n es divisible por 3, el número n^5-n es divisible por 5 y el número n^7-n es divisible por 7. De aquí supuso que para todo k impar y cualquier número natural n el número n^k-n es divisible por k ; pero pronto observó que $2^9-2=510$ no es divisible por 9 .

Un error del mismo carácter cometió D.A. Grave, conocido matemático soviético, al suponer que para todo primo p el número $2^{p-1}-1$ no es divisible por p^2 .

El cálculo directo confirmaba esta hipótesis para todos los números p menores que mil. Sin embargo, pronto se comprobó que $2^{1092}-1$ es divisible por 1093^2 (1093 es un número primo); o sea , la hipótesis de Grave resultó errónea.

Veamos otro ejemplo muy instructivo. Sustituyendo n en la expresión $991n^2+1$ por los número enteros sucesivos 1,2,3,..., jamás obtendremos el cuadrado de un número por muchos días ó inclusive por años que dediquemos a ello.

Sin embargo, sería erróneo deducir de aquí que ningún número de este tipo es un cuadrado, pues, en realidad, entre los números de tipo $991n^2+1$ también hay cuadrados; pero es muy grande el valor mínimo de n para el cual es un cuadrado el número $991n^2+1$. He aquí este número :

$n = 12055735790331359447442538767$

Todos estos ejemplos deben prevenir al lector contra las deducciones por analogía no argumentadas .

Volvamos ahora al problema sobre la suma de los n primeros números impares . Está claro de lo anterior que por muchos que sean los primeros valores de n para los cuales hayamos comprobado la fórmula $S(n) = n^2$ (1) , no podemos darla por demostrada pues siempre quedará el temor de que deje de ser válida en algunos de los casos no analizados .

Para convencerse de que la fórmula (1) es válida para todos los n, es preciso demostrar que, por mucho que avancemos en la serie numérica natural, jamás podremos pasar de valores de n que aún verifican la fórmula (1) a valores de n que ya no la verifican .

Supongamos, pues, que nuestra fórmula es válida para un número n y tratemos de demostrar que también será válida para el número siguiente $n + 1$. Es decir, aceptamos que

$$S(n) = 1 + 3 + 5 + \ldots + (2n-1) = n^2 \text{ ; calculemos}$$

$$S(n+1) = 1 + 3 + 5 + \ldots + (2n-1) + (\underbrace{2(n+1)-1}_{2n+1})$$

Según nuestra hipótesis la suma de los n primeros términos del segundo miembro de la última igualdad es n^2 , y , por consiguiente :

$$S(n + 1) = n^2 + (2n + 1) = (n + 1)^2 .$$

O sea, suponiendo que la fórmula $S(n) = n^2$ es válida para cierto número natural n, hemos logrado demostrar su validez para el número siguiente inmediato $n + 1$. Pero hemos visto que esta fórmula es válida para $n = 1, 2, 3, 4$ y 5. Luego, también será válida para el número $n = 6$ que sigue a 5, así como para los números $n = 7$, $n = 8$, $n = 9$, etc. Nuestra fórmula puede considerarse ahora demostrada cualquiera que sea el número de sumandos.

Este método de demostración se denomina método de inducción matemática.

PRINCIPIO DE INDUCCION MATEMATICA .-

Si S es un conjunto de enteros positivos que tiene las dos propiedades siguientes:

i) $1 \in S$, y

ii) Si un entero $k \in S$ ($k \geq 1$) implica que $k + 1 \in S$.

Entonces todo entero positivo pertenece a S, es decir, $S = Z^+$.

En efecto, las condiciones i) y ii) dicen que S es inductivo, y como Z^+ es el más pequeño conjunto inductivo, $Z^+ \subseteq S$.

Por hipótesis S es un conjunto de enteros positivos, así que $S \subseteq Z^+$. Luego $S = Z^+$, es decir, todo entero positivo pertenece a S.

METODOS DE DEMOSTRACION POR INDUCCION .-

Frecuentemente aparecen propiedades referentes a los enteros positivos, que son satisfechas por todos estos números o parte de ellos, cuando estamos interesados en la justificación de éstos, utilizamos los llamados métodos de demostración por inducción. Se conocen tres de estos métodos:

Primer Método .-
Sea A(n) una afirmación referida a $n \in Z^+$.
Si i) A(1) es cierta y
ii) Supuesta A(k) cierta (siendo $k \in Z^+$ arbitrario, pero fijo) entonces A (k +1) es cierta .
Concluimos que A(n) es cierta para todo $n \in Z^+$.

Demost.- Sea $S = \{ n \in Z^+ / A(n) \text{ es cierta} \}$
$S \subseteq Z^+$ por construcción .
$1 \in S$, pues por i) A(1) es cierta .

Sea $k \in S$, es decir, $k \in Z^+$ y A(k) es cierta. Entonces por ii) A(k + 1) es cierta ($k + 1 \in Z^+$); así que $k + 1 \in S$. Por el principio de inducción matemática, entonces $S = Z^+$; es decir para todo $n \in Z^+$, A(n) es cierta .

Segundo Método .-
Sea A(n) una afirmación correspondiente a $n \in Z^+$ y n_1 un entero positivo fijo.

Si i) $A(n_1)$ es cierta y

ii) Supuesta $A(k)$ cierta, siendo $k \in Z^+$ arbitrario, pero fijo, $k \geq n_1$, entonces $A(k+1)$ es cierta .

Se concluye que $A(n)$ es cierta para todo $n \in Z^+$, $n \geq n_1$.

Demostr.- Sea $S = \{n \in Z^+ / A(n + n_1 - 1) \text{ es cierta}\}$. También se puede hacer la demostración llamando $Q(n) = A(n + n_1 - 1)$ y utilizando el método de demostración por inducción anterior .

$S \subseteq Z^+$ por construcción de S.

Ahora $1 \in S$, pues $1 \in Z^+$ y $A(1 + n_1 - 1) = A(n_1)$ es cierta, por i) .

Sea $k \in S$, es decir $k \in Z^+$ y $A(k+n_1-1)$ es cierta .

Como $k + n_1 - 1 \geq n_1$, pues $k \geq 1$ entonces por ii) $A(k+n_1-1)+1)$ que es igual a $A((k+1) + n_1 - 1)$ es cierta; así que $k + 1 \in S$. Entonces por el principio de inducción matemática $S = Z^+$.

Así que $A(n + n_1 - 1)$ es cierta para todo $n \in Z^+$.

Si $m = n + n_1 - 1$ entonces $m \geq n_1$, por tanto hemos probado que $A(m)$ es cierta para todo $m \geq n_1$.

Nota :

Este segundo método de demostración es más general que el primero, el primero es un caso particular del segundo, cuando $n_1 = 1$.

Tercer Método :.-

Sea $A(n)$ una afirmación relativa a $n \in Z^+$, y sea $m \in Z^+$ fijo. Si la verdad de $A(k)$ para todo $k < m$ $(k \in Z^+)$ implica la verdad de $A(m)$, entonces concluimos que $A(n)$ es cierta para todo $n \in Z^+$.

Demostr.- Si $m = 1$, la afirmación se tiene vacíamente.

Supongamos $m \in Z^+$, $m > 1$, es decir $m \geq 2$.

Sea $S = \{n \in Z^+ / A(n) \text{ es falsa}\}$. Supongamos que $S \neq \emptyset$, entonces por el principio de buena ordenación existe $m = \text{Mín } S$.

Como $m = \text{Mín } S$ entonces para todo $k < m$, $A(k)$ es verdadera, pues de lo contrario m dejaría de ser el mínimo de S. Pero como por hipótesis si $A(k)$ es verdadera para todo $k < m$, entonces $A(m)$ es verdadera, concluimos que $m \notin S$. Absurdo ! pues $\text{Mín } S \in S$. Por tanto $S = \emptyset$ y así $A(n)$ es cierta para todo $n \in Z^+$.

Veamos ahora algunos ejemplos de aplicación de estos métodos :

Ejemplo 1.-

Demostrar por inducción la siguiente afirmación acerca de $n \in Z^+$

$$A(n) : 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \quad (*)$$

Demostr.- Es claro que para la prueba de esta afirmación debemos utilizar el primer método de demostración por inducción .

i) $A(1)$ es cierta, pues $1 = \frac{1(1+1)}{2}$ ($n = 1$ en la fórmula (*))

ii) Supongamos que $A(k)$ es cierta $k \in Z^+$, es decir, $1+2+\ldots+k = \frac{k(k+1)}{2}$

y veamos que $A(k+1)$ es cierta, esto es que $1+2+\ldots+k+(k+1) = \frac{(k+1)(k+2)}{2}$

(Obsérvese que $A(k)$ se obtiene cambiando n por k en la fórmula (*) , y lo mismo se hace para obtener $A(k+1)$.

Como $1+2+\ldots+k = \frac{k(k+1)}{2}$, hipótesis, entonces sumando a ambos lados de la igualdad $k+1$, obtenemos :

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

Ahora el lado izquierdo de esta igualdad coincide con la parte izquierda de la igualdad correspondiente a $A(k+1)$. Veamos que los lados derechos también coinciden . Para esto desarrollamos la suma :

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

que era lo que se quería .

Así queda demostrada que la fórmula (*) es válida para $k+1$.
Entonces, por el primer método de demostración por inducción concluimos que $A(n)$ es cierta para todo $n \in Z^+$, es decir:

$$1+2+3+\ldots+n = \frac{n(n+1)}{2} \quad \text{para todo } n \in Z^+$$

Ejemplo 2.-

Pruebe que $2^n \geq 2n$ para todo $n \in Z^+$

Demostr.- Nuevamente es claro que en este caso debemos utilizar el primer método de demostración por inducción. Sea $A(n)$ la afirmación $2^n \geqslant 2n$.

i) Como $2^1 = 2 = 2.1$, entonces $A(1)$ es cierta
ii) Supongamos que se tiene $A(k)$, es decir $2^k \geqslant 2k$, $k \in Z^+$, y veamos que se tiene $A(k+1)$, e.d que $2^{k+1} \geqslant 2(k+1)$.

Como $2^k \geqslant 2k$, multiplicando a ambos lados de esta desigualdad por 2 obtenemos : $2 \times 2^k \geqslant 2(2k)$, es decir, $2^{k+1} \geqslant 4k$.
Ahora $4k = 2k + 2k \geqslant 2k + 2$, pues $k \geqslant 1$, así que $2^{k+1} \geqslant 4k \geqslant 2(k+1)$ de donde $2^{k+1} \geqslant 2(k+1)$. Lo que significa que $A(k+1)$ es cierta.

De la conclusión del primer método de demostración por inducción, se tiene que $A(n)$ es cierta para todo $n \in Z^+$, e.d. $2^n \geqslant 2n$ para todo $n \in Z^+$.

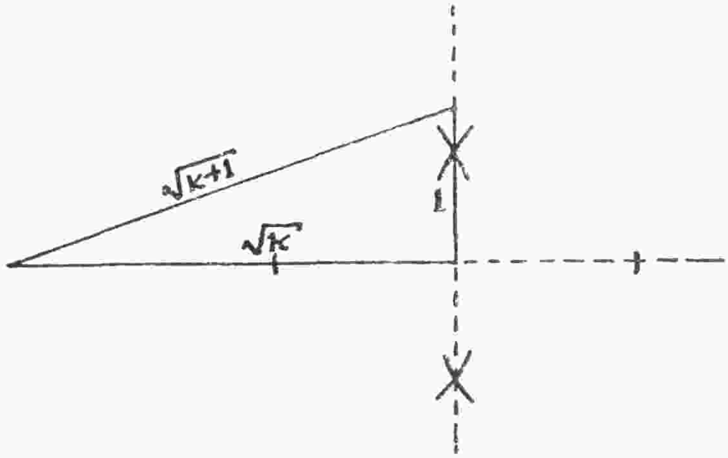
Ejemplo 3.-

Demuestre por inducción la proposición siguiente : Dado un segmento de longitud unidad, el segmento de longitud $\sqrt{n}$ se puede construir con regla y compás para cada entero positivo n.

Demostr.- Dado un segmento de longitud unidad, el segmento de longitud $\sqrt{1}=1$ se puede construir con regla y compás (Tómese el segmento dado).

Supongamos pues que el segmento de longitud $\sqrt{k}$, $k \in Z^+$, se puede construir con regla y compás.

Trácese con regla y compás un segmento de longitud $\sqrt{k}$, levántese en un extremo de este segmento una perpendicular, y sobre esta perpendicular márquese (utilizando el compás) una longitud de una unidad. De esta forma queda construido un triángulo rectángulo con catetos $\sqrt{k}$ y 1. Por el teorema de Pitágoras, la hipotenusa de este triángulo rectángulo tiene longitud $\sqrt{(\sqrt{k})^2 + 1^2} = \sqrt{k+1}$, es decir, hemos construido de esta forma un segmento de longitud $\sqrt{k+1}$ (con regla y compás), con lo que podemos concluir que el segmento de longitud $\sqrt{n}$ se puede construir con regla y compás para cada entero positivo n.



Ejemplo 4.-

Sea b un entero positivo (e.d. $b \in Z$, $b > 0$) Demostrar por inducción la proposición siguiente: Para cada entero $n \geq 0$ existen enteros no-negativos q y r, únicos, tales que $n = q.b + r$, $0 \leq r < b$.

Demostr.- El primer método de demostración nos permite demostrar que una afirmación es válida para todos los enteros positivos; como aquí necesitamos demostrar que la proposición es cierta para $n \geq 0$, $n \in Z$, el caso $n = 0$, debemos considerarlo por separado . Si $n = 0$ entonces $0 = 0.b + 0$, donde $q = 0$, $r = 0 < b$.

i) Si $n = 1$, como $b \in Z^+$, $b \geq 1$, así que para b hay dos posibilidades $b = 1$ ó $b > 1$.
Si $b = 1$, entonces $1 = 1.1 + 0$ donde $q = 1$, $r = 0 < 1 = b$.
Si $b > 1$, entonces $1 = 0.b + 1$ donde $q = 0$, $r = 1 < b$.

ii) Supongamos que la proposición es cierta para $k \in Z^+$, es decir, $k = q.b + r$ con $0 \leq r < b$, y veamos que es cierta para $k + 1$, es decir, existen q_1, r_1 en Z^+ tales que $k + 1 = q_1.b + r_1$, $0 \leq r_1 < b$.

En efecto : de $k = q.b + r$ donde $0 \leq r < b$, entonces $k + 1 = q.b + (r + 1)$. Como $0 \leq r < b$ entonces $0 \leq r + 1 \leq b$, pues r,b son enteros .

Si $0 \leq r + 1 < b$ entonces $k + 1 = q.b + r_1$ donde $r_1 = r + 1$ y $0 \leq r_1 < b$.
Si $0 \leq r + 1 = b$, entonces $k + 1 = q.b + b = (q + 1)b$ así que $q_1 = q + 1$ y $r_1 = 0 < b$ son tales que $k + 1 = q_1.b + r_1$ con $0 \leq r_1 < b$.

Luego en cualquier caso $k + 1 = q_1.b + r_1$ con $0 \leq r_1 < b$.

Por el primer método de demostración por inducción concluimos que para todo $n \in Z^+$, existen q, r enteros no-negativos tales que $n = q.b+r$, con $0 \leq r < b$.

De todo lo anterior concluimos que la proposición es cierta para todo $n \geq 0$, $n \in Z$.

Veamos la unicidad de los enteros no-negativos q y r. En efecto: supongamos que $n = q_1 b + r_1$ con $0 \leq r_1 < b$ y

$n = q_2 b + r_2$ con $0 \leq r_2 < b$. Entonces :

$$0 = q_1 . b + r_1 - q_2 . b - r_2 = (q_1 - q_2) b + (r_1 - r_2) \text{ de donde}$$

$$(q_1 - q_2) b = r_2 - r_1$$

Para q_1, q_2 hay tres posibilidades (Ley de Tricotomía): $q_1 = q_2$; $q_1 < q_2$; $q_2 < q_1$.

Supongamos que $q_1 < q_2$, entonces $q_1 + 1 \leq q_2$, pues $q_1, q_2 \in Z$, entonces $q_1 - q_2 \leq -1$ y así $b(q_1 - q_2) \leq -b$, esto es $b \leq -b(q_1 - q_2) = r_1 - r_2$.

Pero $r_1 - r_2 \leq r_1$ pues $r_2 \geq 0$, así que $b \leq r_1$. absurdo ! pues $r_1 < b$. Luego no puede ser $q_1 < q_2$.

Supongamos que $q_2 < q_1$, entonces $q_2 + 1 \leq q_1$, esto es $q_1 - q_2 \geq 1$, y entonces $b(q_1 - q_2) \geq b$; pero $r_2 - r_1 = b(q_1 - q_2)$ y $r_2 - r_1 \leq r_2$, pues $r_1 \geq 0$. Luego: $r_2 \geq r_2 - r_1 = b(q_1 - q_2) \geq b$, entonces $r_2 \geq b$, absurdo ! pues $r_2 < b$. Por tanto no puede ser $q_2 < q_1$.

Luego la única posibilidad es $q_1 = q_2$ y así $r_1 = r_2$.

Por tanto la escritura $n = b.q + r$ con $0 \leq r < b$ es única .

Veamos ahora algunos ejemplos de aplicación del segundo método de demostración por inducción .

Ejemplo 5.-

Demostrar por inducción la siguiente afirmación :

$A(n): (1-1/2)(1-1/3)(1-1/4)\ldots(1-1/n) = 1/n$ válida para todo $n \geq 2$, $n \in Z$.

Demostr.- En este caso $n_1 = 2$ .Veamos que $A(n_1) = A(2)$ es cierta .
En efecto : $(1-1/2) = 1/2$ que es el valor que se obtiene del lado derecho de la igualdad, haciendo $n = 2$.

Supongamos que la afirmación es cierta para k, $k \in Z^+$, $k \geq 2$. Es decir, $A(k) : (1-1/2)(1-1/3)\ldots(1-1/k)= 1/k$ y veamos que $A(k+1)$ es cierta.
Esto es :

$$A(k+1) : (1-1/2)(1-1/3)\ldots(1-1/k)(1-1/(k+1))= 1/(k+1)$$

Como por hipótesis $(1-1/2)(1-1/3)\ldots(1-1/k) = 1/k$, multiplicando a ambos lados de esta igualdad por $(1-1/(k+1))$obtenemos:

$$(1-1/2)(1-1/3)\ldots(1-1/k)(1-1/(k+1))= 1/k(1-1/(k+1)).$$

El lado izquierdo de esta igualdad es el mismo que el lado izquierdo en la expresión correspondiente a $A(k+1)$, luego solo resta ver que la parte derecha son las mismas.

$1/k(1-1/(k+1))= 1/k((k+1-1)/k+1) = 1/(k+1)$. Luego la fórmula es válida para $k+1$.
Por tanto por el segundo método de demostración por inducción :
$A(n) : (1-1/2)(1-1/3)\ldots(1-1/n) = 1/n$ es válida para todo $n \geq 2$, $n \in Z$.

Ejemplo 6.-

Sea n_1 el menor entero positivo n para el que la desigualdad $(1+x)^n > 1+nx+nx^2$ es cierta para todo $x > 0$. Calcular n_1 y demostrar que la desigualdad es cierta para todos los enteros $n \geq n_1$.

Solución : Si $n = 1$, $(1+x)^1 = 1+x \not> 1+1.x+1.x^2$, pues $x^2 > 0$.
Si $n = 2$, $(1+x)^2 = 1+2x+x^2 \not> 1+2.x+2x^2$. pues $x^2 < 2x^2$.
Si $n = 3$, $(1+x)^3 = 1+3x+3x^2+x^3 > 1+3x+3.x^2$ pues $x^3 > 0$ ya que $x > 0$.

Luego el menor entero positivo n para el cual la desigualdad

$$A(n): (1+x)^n > 1+nx+n.x^2 \text{ es válida, es } n = 3$$

Sea $n_1 = 3$, veamos si $(1+x)^n > 1+nx+nx^2$ es válida para todo $n \geq n_1$, $n \in Z$.

i) $A(n_1) = A(3)$ es cierta .

ii) Supongamos que la proposición es cierta para $k \in Z^+$, $k \geq n_1$, es decir $(1+x)^k > 1+kx+kx^2$ y veamos que es cierta para $k+1$, esto es, $A(k+1)$: $(1+x)^{k+1} > 1+(k+1)x+(k+1)x^2$.
$(1+x)^{k+1} = (1+x)^k(1+x)$. Ahora, como $1+x > 0$, pues $x > 0$ y como $(1+x)^k > 1+kx+kx^2$, por hipótesis, entonces multiplicando a ambos lados de la última desigualdad por $1+x$, obtenemos :
$(1+x)^{k+1} = (1+x)(1+x)^k > (1+x)(1+kx+kx^2) = 1+kx+kx^2+x+kx^2+kx^3$.
Pero $1+kx+kx^2+x+kx^2+kx^3 = 1+(k+1)x+2kx^2+kx^3 \geq 1+(k+1)x+(k+1)x^2$,
pues $2kx^2 \geq (k+1)x^2$ y $kx^3 > 0$.

Luego $(1+x)^{k+1} \geq 1+(k+1)x+(k+1)x^2$, que significa que $A(k+1)$ es cierta .

Por el segundo método de demostración por inducción concluimos que:

$A(n)$: $(1+x)^n > 1+nx+nx^2$ es válida para todo $n \geq 3$, $n \in Z$.

Ejemplo 7.-

Dados números reales positivos $a_1, a_2, a_3, \ldots$, tales que $(*) a_n \leq Ca_{n-1}$ para todo $n \geq 2$, donde C es un número positivo fijo, aplíquese el método de demostración por inducción para demostrar que: $a_n \leq a_1 C^{n-1}$ para cada $n \geq 1$

Demost.- Obsérvese que la propiedad dada en $(*)$ es válida para todo $n \geq 2$, sin embargo, lo que se trata de demostrar es válida para todo $n \in Z^+$.

i) Si $n = 1$, $a_1 = a_1 1 = a_1 C^0 = a_1 C^{1-1}$. Así que $a_1 \leq a_1 C^{1-1}$, lo que significa que la afirmación es cierta para $n = 1$.

ii) Supongamos que la afirmación es cierta para $k \in Z^+$, e.d. $a_k \leq a_1 C^{k-1}$ y veamos que se tiene para $k+1$, esto es :

$$a_{k+1} \leq a_1 C^{(k+1)-1} = a_1 C^k$$

De $a_k \leq a_1 C^{k-1}$ (hip. de inducción) y de la hipótesis de que $a_n \leq Ca_{n-1}$, entonces para $n = k+1$ tenemos :

$$a_{k+1} \leq Ca_{(k+1)-1} = C a_k \leq C a_1 C^{k-1} = a_1 C^{k-1+1} = a_1 C^k, \text{ pues } c > 0.$$

Luego $a_{k+1} \leq a_1 C^k$, que significa que la afirmación es válida para k+1 .

Por el primer método de demostración por inducción concluimos que $a_n \leq a_1 C^{n-1}$ para cada $n \geq 1$, $n \in Z$.

Veamos ahora unos ejemplos de aplicación del tercer método de la demostración por inducción..

Ejemplo 8.-

Sean n y d enteros. Se dice que d es un divisor de n si $n = c.d$ para algún entero c.

Un entero n se denomina primo si $n > 1$ y los únicos divisores de n son 1 y n. Demostrar por inducción que cada entero $n > 1$ es ó primo o producto de primos.

Demost.- Sea $m \in Z^+$ fijo, y supongamos que la proposición es cierta para todo $k < m$, $k \in Z^+$, es decir k es primo o producto de primos .

Para m hay dos posibilidades : m es primo o m no es primo.
Si m es primo, la afirmación es verdadera. Luego consideremos el caso en que m no es primo .
Si m no es primo, existen a,b en Z^+ (sin pérdida de generalidad) tales que $m = ab$. Afirmamos que $a \neq 1$ y $b \neq 1$, pues si $a = 1$, entonces $b = m$ ó si $b = 1$ entonces $a = m$, con lo cual m sería primo, absurdo ! Luego $a < m$ y $b < m$.

Como por hipótesis, la proposición es cierta para todos los enteros positivos menores que m, entonces lo es para a y b, por ser ambos menores que m. Así pues, a es primo ó producto de primos y b es primo ó producto de primos. Lo cual nos da, en cualquier caso que $m = a b$ es producto de primos .

Luego la proposición es válida para m y así por el tercer método de demostración por inducción, concluimos que la proposición es cierta para todo entero $n > 1$.

Ejemplo 9.-

Sea k un cuerpo (por ejemplo, el conjunto de los números reales R) y sean

$f(x)$ y $g(x)$ polinomios en $K[x]$, con $g(x) \neq 0$.

Entonces existen polinomios $q(x)$, $r(x)$ en $K[x]$ únicos que satisfacen :

$$f(x) = q(x)\, g(x) + r(x)$$

donde $r(x) = 0$ ó grado $(r(x)) <$ grado $(g(x))$.

Demostr.- Se demostrará usando inducción sobre el grado del polinomio $f(x)$.

Obsérvese primero que si :

i) $f(x) = 0$ entonces : $0 = f(x) = 0.g(x) + 0$ donde $q(x) = 0$ y $r(x) = 0$,ó

ii) $f(x) \neq 0$ y grado $(f(x)) <$ grado $(g(x))$, entonces :
$f(x) = 0.g(x) + f(x)$ donde $q(x) = 0$ y $r(x) = f(x)$, grado $(r(x))$ es menor que grado $(g(x))$.

iii) Si grado $(f(x))$ = grado $(g(x)) = 0$, entonces $f(x) = a$, $g(x) = b$, $a, b \in K$. Como $g(x) \neq 0$, entonces $b \neq 0$, y así :
$a = f(x) = (\, f(x)/ g(x))\, g(x) + 0$ donde $q(x) = f(x)/ g(x) = a / b$ y $r(x) = 0$.

Supongamos entonces que la proposición es verdadera para todos los polinomios $f(x)$ de grado menor que n (hipótesis de inducción) y Sean $f(x)$ y $g(x)$ polinomios tales que grado $(f(x)) = n$, grado $(g(x)) = m$, donde $n \geq m \geq 1$. Esto es :

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \,,\quad a_n \neq 0,\ a_i \in K,\quad i = 0, 1, 2, \ldots , n.$$

$$g(x) = b_0 + b_1 x + \ldots + b_m x^m,\quad b_m \neq 0,\ b_i \in K,\quad i = 0, 1, 2, \ldots , m .$$

Consideremos el polinomio :

(*) $f_1(x) = f(x) - (\, a_n / b_m) x^{n-m}\, g(x)$ que pertenece a $k[x]$.

$$\begin{aligned} f_1(x) &= a_0 + a_1 x + \ldots + a_n x^n - (\, a_n / b_m)\, x^{n-m}(b_0 + b_1 x + \ldots + b_m x^m) \\ &= a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} - (a_n / b_m)\, x^{n-m}\, (b_0 + b_1 x + \ldots + b_{m-1} x^{m-1}) \\ &\quad + a_n x^n - (\, a_n / b_m\,)\, x^{n-m}\, b_m x^m \\ &= a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} - (\, a_n / b_m)\, x^{n-m}(b_0 + b_1 x + \ldots + b_{m-1} x^{m-1}) \end{aligned}$$

Como se ve claramente, este polinomio $f_1(x)$ tiene grado menor que n, entonces existen polinomios $q_1(x)$ y $r(x)$ en $K[x]$ tales que:

$$f_1(x) = q_1(x)\, g(x) + r(x) \quad \text{donde} \quad r(x) = 0 \text{ ó grado } (r(x)) < \text{grado } (g(x)).$$

Sustituyendo en $(_*)$ obtenemos :

$$f(x) = f_1(x) + a_n/b_m\, x^{n-m}\, g(x)$$

$$f(x) = q_1(x)\, g(x) + r(x) + a_n/b_m\, x^{n-m}\, g(x)$$

$$f(x) = (\, q_1(x) + (a_n/b_m) x^{n-m})\, g(x) + r(x)$$

$$f(x) = q(x)\, g(x) + r(x)$$

Lo cual muestra que la representación deseada existe cuando grado $(f(x)) = n$. Por el tercer método de demostración por inducción concluimos que la proposición es cierta para todos los polinomios $f(x)$ en $K[x]$ tales que grado $(f(x)) = n$, donde $n \in Z^+$.

Para la unicidad , supongamos que :

$f(x) = q_1(x)\, g(x) + r_1(x)$ y $f(x) = q_2(x)\, g(x) + r_2(x)$ donde $r_1(x)$ y $r_2(x)$ satisfacen las condiciones de la proposición . De aquí tenemos :

$$(\, q_1(x) - q_2(x)\,)\, g(x) = r_2(x) - r_1(x) .$$

Como $g(x) \neq 0$, se tiene que $q_1(x) - q_2(x) = 0$ si y solo sí $r_2(x) - r_1(x) = 0$

Supongamos que $q_1(x) - q_2(x) \neq 0$. Como $g(x) \neq 0$, entonces :

$$\text{grado } (\, q_1(x) - q_2(x)\,)\, g(x) = \text{grado } (\, q_1(x) - q_2(x)\,) + \text{grado } (\, g(x)\,)$$

$$\geq \text{grado } (\, g(x)) > \text{grado } (\, r_2(x) - r_1(x)\,),$$

Pues grado $(\, g(x)\,) >$ grado $(\, r_1(x)\,)$

y grado $(\, g(x)\,) >$ grado $(\, r_2(x))$

Lo cual es una contradicción, ya que $(\, q_1(x) - q_2(x))\, g(x) = r_2(x) - r_1(x)$.

Luego tiene que ser $q_1(x) - q_2(x) = 0$, lo que da $q_1(x) = q_2(x)$ y así $r_1(x) = r_2(x)$, que era lo que se quería probar .