Resumen EX (materia nueva)

Ignacio Méndez

Principio de inducción simple:

Para una afirmación $P(x)$ sobre los naturales, si $P(x)$ cumple que:

1. $P(0)$ es verdadero.
2. Si $P(n)$ es verdadero, entonces $P(n+1)$ es verdadero.

Entonces para todo $n \in \mathbb{N}$ se tiene que $P(n)$ es verdadero.

Notación:

- $P(0)$ se llama el **caso base**.
- En la afirmación 2.
  - $P(n)$ se llama la **hipótesis de inducción**.
  - $P(n+1)$ se llama la **tesis de inducción** o paso inductivo.

$$\boxed{\Big(P(0) \wedge \big(\forall n.\, P(n) \to P(n+1)\big)\Big) \to \forall n.\, P(n)}$$

Principio de inducción fuerte:

Para una afirmación P sobre los naturales y un $k \in \mathbb{N}$, si P cumple que:

1. $P(k)$ es verdadero.
2. Para todo $n \geq k$, si $P(n)$ es verdadero, entonces $P(n+1)$ es verdadero, entonces $P(n)$ es verdadero para todo $n \geq k$.

$$\boxed{\Big(\forall n.\, \big(\forall k < n.\, P(k)\big) \to P(n)\Big) \to \forall n.\, P(n)}$$

Definiciones recursivas:

Una definición se dice **recursiva** si puede ser definida a partir de:

1. Casos **bases** sencillos.
2. Una **serie de reglas** que reducen la definición a casos anteriores.

Ejemplo

Caso **base**: $F(0) = 0$
$F(1) = 1$

Regla **recursiva**: $F(n) = F(n-1) + F(n-2)$ para $n \geq 2$

Definición recursiva de conjuntos:

Una definición recursiva de un conjunto $\mathbb{S}$ consta de:

1. Un conjunto **base** $B = \{b_1, \dots, b_n\}$ tal que $b_i \in \mathbb{S}$ para todo $i \leq N$.
2. **Reglas** recursivas R de la forma:

$$\text{Si} \quad s_1, \dots, s_n \in \mathbb{S} \quad \text{entonces} \quad R(s_1, \dots, s_n) \in \mathbb{S}$$

3. Una afirmación de **exclusión** de la forma:

"*El conjunto $\mathbb{S}$ son todos los elementos que se construyen solamente a partir de B y las reglas R*".

Ejemplos

- Se define el conjunto $\mathbb{N}$ tal que:

  Caso **base**: $0 \in \mathbb{N}$

  Regla **recursiva**: Si $a \in \mathbb{N}$, entonces $a + 1 \in \mathbb{N}$.

  $\mathbb{N}$ es el conjunto que se construye solo a partir de las reglas anteriores.

En general se omitirán las reglas de exclusión

Inducción estructural:

Sea $\mathbb{S}$ un conjunto definido a partir de:

- Un conjunto **base** B.
- Un conjunto de **reglas recursivas** $\mathcal{R}$.

Definimos la **capa** $\mathbb{S}[n]$ de $\mathbb{S}$ para todo $n \geq 0$ como:

$$\mathbb{S}[0] = B$$
$$\mathbb{S}[n+1] = \mathbb{S}[n] \cup \{T(s_1, \dots, s_k) \mid T \in \mathcal{R} \wedge s_1, \dots, s_k \in \mathbb{S}[n]\}$$

Para todo predicado $P(\cdot)$ sobre $\mathbb{S}$, la siguiente fórmula es siempre verdadera:

$$\boxed{\left[\left(\forall s\, n\, \mathbb{S}[0].\, P(s)\right) \wedge \forall n.\left(\forall s. \in \mathbb{S}[n].\, P(s)\right) \rightarrow \left(\forall s' \in \mathbb{S}[n+1].\, P(s')\right)\right] \rightarrow \forall s \in \mathbb{S}.\, P(s)}$$

División:

Sea $\mathbb{Z}$ el conjunto con $a \neq 0$, diremos que a divide b si $\exists q \in \mathbb{Z}$ tal que $a \cdot q = b$.

$$\boxed{a \mid b} \quad \text{si, y solo si,} \quad \exists q \in \mathbb{Z}.\ \boxed{a \cdot q = b}$$

Proposición:

Para $a, b, c \in \mathbb{Z}$ con $a \neq 0$:

1. Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.
2. Si $a \mid b$, entonces $a \mid (b \cdot c)$ para todo $c \in \mathbb{Z}$.
3. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
4. Si $a \mid b$ y $a \mid c$, entonces $a \mid (n \cdot b + m \cdot c)$ para todo $n, m \in \mathbb{Z}$.

División con resto:

Sea $a, b \in \mathbb{Z}$ con $a > 0$.
Entonces existen un único par $q, r \in \mathbb{Z}$ con $0 \leq r < a$ tal que:

$$\boxed{a \cdot q + r = b}$$

Definición:

Desde ahora, si $a \cdot q + r = b$ entonces anotaremos:

$$b \ \boldsymbol{div} \ a = q$$
$$b \ \boldsymbol{mod} \ a = r$$

Congruencia modular:

Sea $m \in \mathbb{Z}$ con $m > 0$.
Para todo $a, b \in \mathbb{Z}$ diremos que a es **congruente** con b **módulo** m si:

$$a \equiv b \pmod{m} \quad \text{si, y solo si,} \quad m \mid (a - b)$$

Proposición:

Para todo $a, b, m \in \mathbb{Z}$ con $m > 0$, las siguientes condiciones son equivalentes:

1. $a \equiv b \pmod{m}$.
2. $a = b + m \cdot s$ para algún $s \in \mathbb{Z}$.
3. $(a \ \boldsymbol{mod} \ m) = (b \ \boldsymbol{mod} \ m)$.

Proposición

Para todo $m > 0$, si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces:

$$a + c \equiv b + d$$
$$a \cdot c \equiv b \cdot d$$

Corolario

Para todo $a, b, m \in \mathbb{Z}$ con $m > 0$, se tiene que:

$$(a + b) \boldsymbol{mod}\ m = \big((a \boldsymbol{mod}\ m) + (b \boldsymbol{mod}\ m)\big) \boldsymbol{mod}\ m$$
$$(a \cdot b) \boldsymbol{mod}\ m = \big((a \boldsymbol{mod}\ m) \cdot (b \boldsymbol{mod}\ m)\big) \boldsymbol{mod}\ m$$

Definición

Para $m > 0$, sea $\mathbb{Z}_m = \{0, \dots, m-1\}$.
Para todo $a, b \in \mathbb{Z}_m$, definimos las operaciones $+_m$ y $\cdot_m$ como:

$$a +_m b = (a + b) \boldsymbol{mod}\ m$$
$$a \cdot_m b = (a \cdot b) \boldsymbol{mod}\ m$$

Propiedades

Para todo $a, b, c \in \mathbb{Z}_m$, se cumple que:

Clausura:	$a +_m b \in \mathbb{Z}_m$ y $a \cdot_m b \in \mathbb{Z}_m$.
Conmutatividad:	$a +_m b = b +_m a$ $a \cdot_m b = b \cdot_m a$
Asociatividad:	$a +_m (b +_m c) = (a +_m b) +_m c$ $a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c$
Identidad:	$a +_m 0 = a$ $a \cdot_m 1 = 1$
Inverso (aditivo):	Si $a \neq 0$, entonces existe $a' \in \mathbb{Z}_m$ tal que $a +_m a' = 0$
Distributividad:	$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$

Representación de números:

Sea $b > 1$. Si $n \in \mathbb{N} - \{0\}$, entonces se puede escribir de forma única como:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b^1 + a_0 b^0 = \sum_{i=0}^{k-1} a_i b^i$$

- $k \geq 1$.
- $a_0, \dots, a_{k_1}$ menor que b $(a_i < b)$.
- $a_{k-1} \neq 0$.

Desde ahora, decimos que la representación n **en base** b es la secuencia:

$$(n)_b = a_{k-1} \dots a_1 a_0$$

Ejemplo

$(123)_{10} = 123$ $(123)_2 = 1111011$ $(123)_8 = 173$

Para encontrar la representación de n en base b:

Para un $n \in \mathbb{N} - \{0\}$ y $b > 1$, si $(n)_b = a_{k-1} \dots a_1 a_0$ y $n = q \cdot b + r$, entonces:

$$r = a_0$$
$$(q)_b = a_{k-1} \dots a_1$$

Ejemplo

Para escribir 39 en base 2:

$$\begin{aligned} 39 &= 19 \cdot 2 + \mathbf{1} \\ 19 &= 9 \cdot 2 + \mathbf{1} \\ 9 &= 4 \cdot 2 + \mathbf{1} \\ 4 &= 2 \cdot 2 + \mathbf{0} \\ 2 &= 1 \cdot 2 + \mathbf{0} \\ 1 &= 0 \cdot 2 + \mathbf{1} \end{aligned}$$

Por lo tanto, $(39)_2 = 100111$.

Para escribir 39 en base 5:

$$\begin{aligned} 39 &= 7 \cdot 5 + \mathbf{4} \\ 7 &= 1 \cdot 5 + \mathbf{2} \\ 1 &= 0 \cdot 5 + \mathbf{1} \end{aligned}$$

Por lo tanto, $(39)_5 = 124$.

Teorema

Para todo $n \in \mathbb{N}$ y $b \geq 2$, se cumple que $|(n)_b| = \lceil \log_b(n+1) \rceil$.

Por lo tanto, $|(n)_b| \in \mathcal{O}(\log(n))$.

Máximo común divisor

Sea $a, b \in \mathbb{Z} - \{0\}$.
Se define el **máximo común divisor** $\gcd(a, b)$ de a, b como el mayor número d tal que $d \mid a$ y $d \mid b$.

Ejemplos

$$\gcd(8, 12) = 4 \qquad \gcd(24, 36) = 12 \qquad \gcd(54, 24) = 6$$

Teorema

Para todo $a, b \in \mathbb{Z} - \{0\}$, $\gcd(a, b) = \gcd\big(b, (a \bmod b)\big)$.

Ejemplo

$$\begin{array}{rcl@{\qquad}rcl} 287 & = & 91 \cdot 3 + 14 & \gcd(287, 91) & = & \gcd(91, 14) \\ 91 & = & 14 \cdot 6 + 7 & \gcd(91, 14) & = & \gcd(14, 7) \\ 14 & = & 7 \cdot 2 & \gcd(14, 7) & = & 7 \end{array}$$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

Este algoritmo se conoce como el algoritmo de Euclides, y está en $\mathcal{O}(\log(b))$.

Conjuntos generadores

Sea $a, b \in \mathbb{Z} - \{0\}$.
Se define el conjunto $\langle a, b \rangle$ **generado** por a y b como:

$$\boxed{\langle a, b \rangle = \{c \in \mathbb{Z} \mid \exists s, t \in \mathbb{Z}.\ \ c = sa + tb\}}$$

Se define el conjunto $\langle a_1, \dots, a_n \rangle$ **generado** por $a_1, \dots, a_n$ como:

$$\boxed{\langle a, b \rangle = \{c \in \mathbb{Z} \mid \exists s_1, \dots, s_n \in \mathbb{Z}.\ \ c = s_1 a_1 + \cdots + s_n a_n\}}$$

Menor elemento de un conjunto generador

Sea $a, b \in \mathbb{Z} - \{0\}$.
Defina g como el menor número positivo en $\langle a, b \rangle$:

$$g = \min\{\, c \in \langle a, b \rangle \mid c > 0 \,\}$$

Como se cumple que $\langle g \rangle \subseteq \langle a, b \rangle$ y $\langle a, b \rangle \subseteq \langle g \rangle$, entonces

$$\langle g \rangle = \langle a, b \rangle$$

Y g será el máximo común divisor de a y b.

Identidad de Bézout

Para todo $a, b \in \mathbb{Z} - \{0\}$:

1. $\gcd(a, b)$ es el **menor número positivo** tal que existe $s, t \in \mathbb{Z}$:

$$\gcd(a, b) = sa + tb$$

2. $\langle a, b \rangle = \langle \gcd(a, b) \rangle$

Ecuaciones de congruencias

Una **congruencia lineal** es una ecuación de la forma:

$$ax \equiv b \pmod{m}$$

Donde $m \in \mathbb{N} - \{0\}$, $a, b \in \mathbb{Z}$ y x es una variable.

¿Cómo se resuelven?

$$x \equiv a^{-1} \cdot b$$

Definición

Decimos que a y b son **primos relativos** si $\gcd(a, b) = 1$.

Teorema

Sea $a \in \mathbb{Z}$ y $m \in \mathbb{N}$ con $m > 1$.
Si a y m son primos relativos, entonces existe un único $a^{-1} \in \mathbb{Z}_m$ tal que:

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Corolario

1. Si a y m son primos relativos, entonces $ax \equiv b$ (**mod** m) tiene solución en $\mathbb{Z}_m$.
2. Si m es primo entonces, todo $a \in \mathbb{Z}_m - \{0\}$ tiene un **inverso multiplicativo**.