

Tarea 1

(1) Enuncia el Principio de Inducción, Principio de Inducción Modificada y El Principio de Buen Orden

- P.I.

Si $S \subseteq \mathbb{N}$ tal que satisface

$$\rightarrow 1 \in S \quad \circ \quad 0 \in S$$

$$\rightarrow n \in S \Rightarrow n+1 \in S$$

podemos concluir que $S = \mathbb{N}$

- P.I.M.

Si $S \subseteq \mathbb{N}$ tal que satisface

$$\rightarrow 1 \in S \quad \circ \quad 0 \in S$$

$$\rightarrow m \in S \quad \forall m < n \Rightarrow n \in S$$

entonces concluimos que $S = \mathbb{N}$

- P.B.O.

Si $S \subseteq \mathbb{N}$ y $S \neq \emptyset$

existe un $m \in S$ tal que para todo $n \in S$, $m \leq n$

Es decir S tiene un mínimo

(2) Demuestre que si $n, m, p \in \mathbb{N}$ y $n+p = m+p$, entonces $n=m$

Sean $n, m, p \in \mathbb{N}$ cualesquier. Demostración usando inducción sobre p

- Caso Base

Sea $p=1$, supongamos que $n+1 = m+1$ PD $n=m$

tenemos que $n+1 = m+1$, por definición de suma tenemos que

$s(n) = s(m)$ y por def de sucesor concluimos que $n=m$

= Hip de inducción

Supongamos que tenemos que $n+p = m+p$ entonces $n=m$

- Paso Inductivo

Supongamos que $n+s(p) = m+s(p)$ PD $n=m$

Por def de suma tenemos que $n+p+1 = n+s(p) = m+s(p) = m+p+1$

Por la hip tenemos que $1+n = m+1$, por def de suma tenemos

que $s(n) = s(m)$ y por def de sucesor concluimos que $n=m$

Por PI concluimos que si $n+p = m+p \Rightarrow n=m$

□

(3) Sean $n, m \in \mathbb{N}$, definimos que si $n \leq m$ si y solo si existe

$a \in \mathbb{N}$ tal que $na = m$. Demostremos lo siguiente

(a) Si $n < m$ y $m < s$, entonces $n < s$.

Supongamos que $n < m$ y $m < s$, por definición tenemos que

existen $a, b \in \mathbb{N}$ tales que $na = m$ y $mb = s$.

Ahora veamos que $(na) + b = s$ ya que $na = m$ por lo

tanto $n + (ab) = s$ y como $a, b \in \mathbb{N}$ entonces $ab \in \mathbb{N}$.

y con esto cumpliendo la definición de $<$ por lo tanto

$n < s$ \square

(b) Si $n < m$ y $a \in \mathbb{N}$, entonces $na < ma$.

Supongamos que $n < m$, por def. de $<$ tenemos que existe $b \in \mathbb{N}$

tal que $nb = m$, ahora veamos que $na + b = m + a$

entonces se cumple la definición de $<$ ya que existe $b \in \mathbb{N}$

tal que $na + b = ma + a$ por lo tanto $na < ma$ \square

(c) Si $n < m$ y $a \in \mathbb{N}$, entonces $n \cdot a < m \cdot a$.

Supongamos que $n < m$, por def. de $<$ tenemos que existe $b \in \mathbb{N}$

tal q.e. $n+b=m$, ahora veamos q.e. $(n+b) \cdot a = m \cdot a$

y por distributividad tenemos q.e. $n \cdot a + b \cdot a = m \cdot a$

ya q.e. como $b, a \in \mathbb{N}$ entonces $a \cdot b \in \mathbb{N}$, por lo tanto

se cumple la definición de $<$ con $b \cdot a$ ya q.e. $n \cdot a + b \cdot a = m \cdot a$

entonces $n \cdot a < m \cdot a$

□

(4) Demuestra que si $n, m \in \mathbb{N}$, entonces se cumple uno y solo uno de los siguientes

- (a) $n=m$ (b) $n < m$ (c) $n > m$

Casos:

-caso 1) supongamos q.e. $n=m$ PD q.e. $n < m$ no se cumple

Supongam. q.e. $n < m$ se cumple

Por def de $<$ tenemos q.e. existe $b \in \mathbb{N}$ tal q.e. $n+b=m$

y al ser $b \in \mathbb{N}$ entonces $0 < b$, pero tenemos q.e. $n=m$

entonces $n+b > m$ llegando a una contradicción al suponer q.e. $n < m$

-caso 2) supongamos q.e. $n=m$ PD q.e. $n > m$ no se cumple

Supongamos que $n \geq m$ se cumple

Por def. de $<$ tenemos que existe $b \in \mathbb{N}$ tal que $n+b = m$

y al ser $b \in \mathbb{N}$ entonces $0 < b$, pero tenemos que $n \geq m$ entonces

$n+b > n$ llegando a una contradiccion al suponer que $n \geq m$

-Caso 3) Supongamos que $n \leq m$ PD que $n=m$ no se cumple

Supongamos que $n=m$ se cumple

Por def de $<$ tenemos que existe $b \in \mathbb{N}$ tal que $n+b = m$

y como $b \in \mathbb{N}$ entonces $0 < b$ y por lo tanto al suponer $n=m$

se genera una contradiccion ya que $n+b = m$

-Caso 4) supongamos que $n \leq m$ PD que $n > m$ no se cumple

Supongamos que $n > m$ se cumple

Por def de $<$ tenemos que existe $b \in \mathbb{N}$ tal que $n+b = m$

y tambien que existe $a \in \mathbb{N}$ tal que $m+a = n$ y como

$b, a \in \mathbb{N}$ no pueden ser 0 por lo tanto generamos una contradiccion

-Caso 5) supongamos que $m > n$ PD que $m=n$ no se cumple

Supongamos que $n=m$ se cumple

Por def de < tenemos que exist $b \in \mathbb{N}$ tal que $m+b=n$ y

como $b \in \mathbb{N}$ entonces $b \geq 1$ y por lo tanto al suponer $m=n$ generamos una contradiccion ya que $m+b=n$

-caso 6) Supongamos que $m < n$ PD que $m > n$ no se cumple

Supongamos que $m > n$ se cumple

Por def de < tenemos que exist $b \in \mathbb{N}$ tal que $m+b=n$ y

existe $a \in \mathbb{N}$ tal que $n+a=m$, y como $a, b \in \mathbb{N}$ no pueden ser 0, por lo tanto generan una contradiccion ya que tenemos que $m+b=n$ y $n+a=m$

(5) Se define el conjunto de enteros como $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$

Donde \sim es de equivalencia sobre $\mathbb{N} \times \mathbb{N}$ de esta manera $(a, b) \sim (c, d)$

si $a+d=c+b$. Demostremos lo siguiente

(a) Demuestra que $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $[(a, b)] + [(c, d)] =$

$[(a+c, b+d)]$ estan bien definida.

Supongamos que $(a, b) \sim (a', b')$ y $(c, d) \sim (c', d')$

PD $[(a, b)] + [(c, d)] \sim [(a', b')] + [(c', d')]$

$$(a+c) + (b'+d') = (a'+b') + (c+d)$$

$$[(a+c), (b+d)] \sim [(a'+c'), (b'+d')]$$

Por def de \sim tenemos que $a+b' = a'+b$ y $c+d' = c'+d$

y si sumas los resultados tenes que $a+b'+c+d' = a'+b+c'+d$

y ahora por la comutatividad de la suma tenes que

$$(a+c) + (b'+d') = (a'+c') + (b+d) \quad \text{y por def de } \sim$$

tenemos que $[(a+c), (b+d)] \sim [(a'+c'), (b'+d')]$ y por def de

$$+ [(a,b)] + [(c,d)] \sim [(a'+b')] + [(c',d')] \quad \square$$

(b) Demostrar que $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $[(a,b)] \cdot [(c,d)] =$

$[(ac+bd, ad+bc)]$ esta bien definida.

Suponemos que $(a,b) \sim (a',b')$ y $(c,d) \sim (c',d')$

$$\text{PD } [(a,b)] \cdot [(c,d)] \sim [(a',b')] \cdot [(c',d')] = [(ac+bd, ad+bc)] \sim$$

$$[(a'c'+b'd', a'd'+b'c')] \Rightarrow (ac+bd) + (a'd'+b'c') = (a'c'+b'd') + (ad+bc)$$

Por def de \sim tenemos que $a+b' = a'+b$ y $c+d' = c'+d$

Veamos que $(ac+bd+a'c'+b'd') + (a'c'+b'c+a'd'+b'd) \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark \quad \checkmark$

permutatividad

$$= (a+b')c + (b+a')d + a'(c+d') + b'(d+c')$$

$$\text{y asociatividad} \quad = (a'+b)c + (a+b')d + a'(c'+d') + b'(c+d')$$

por def \sim

lo que queríamos

$$(a,b) \cdot (c,d) \sim (a',b') \cdot (c',d')$$

$$atd = c+d$$

$$(a,b) \sim (c,d)$$

$$\begin{aligned} &= a'c + bc + b'd + ad + a'd + a'c' + b'c + b'd' \\ &= (ad + bc + a'c' + b'd') + (a'c + b'c + a'd + b'd') \end{aligned}$$

entonces tenemos que

$$\begin{aligned} &\star (ad' + b'c' + ac + bd) + (a'c + b'c + a'd + b'd) \\ &\quad \equiv \\ &(ad + bc + a'c' + b'd') + (a'c + b'c + a'd + b'd) \end{aligned}$$

(*)

entonces

$$(a'd' + b'c' + ac + bd) = (ad + bc + a'c' + b'd')$$

y por def de \sim tenemos que

$$\star (ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$$

y por def de

$$(a,b) \cdot (c,d) \sim (a',b') \cdot (c',d')$$

□

(C) Demuestra que el orden definido como $(a,b) < (c,d)$ si $atd < ctb$

esta bien definido

Supongamos que $(a,b) \sim (a',b')$ y $(c,d) \sim (c',d')$ y $(a,b) K (c,d)$

PD si $(a,b) < (c,d) \Leftrightarrow (a',b') < (c',d')$

• Teoría $a < b \Leftrightarrow a+c < b+c$

Por def de \sim tenemos que $a+b' = a'+b$, $c+d' = c'+d$

por def de $<$ tenemos que $a+d < c+b$

entonces

$$a+d < c+b \Leftrightarrow a+b' + d < c+b+b'$$

$$\Leftrightarrow a'+b+d < c+b+b'$$

$$\Leftrightarrow a'+b+d+c' < c+b+b'+c'$$

$$\Leftrightarrow a'+b+c+d' < c+b+b'+c'$$

$$\Leftrightarrow a'+d' + (b+c) < a'+b' + (b+c)$$

por teorema ?

$$\Leftrightarrow a'+d' < c'+b' \quad \square$$

(6) La función $\varphi: \mathbb{N} \rightarrow \mathbb{Z}$ definida por $\varphi(n) = (n+1, 1)$. Demuestra lo siguiente

(a) φ es inyectiva.

Sean $n, m \in \mathbb{N}$ tales que $\varphi(n) = \varphi(m)$

PD $n = m$

Por def de φ tenemos que $\varphi(n) = (n+1, 1) = (m+1, 1) = \varphi(m)$

y como $(n+1, 1), (m+1, 1) \in \mathbb{Z}$ y al ser iguales enton

$(n+1, 1) \sim (m+1, 1)$ y por def de \sim , entonces

$(n+1) + 1 = (m+1) + 1 \Rightarrow n+2 = m+2$ y por la tcr

$\in \mathbb{N}$ tenemos que $n = m$ ya que $2 = 2$ \square

(b) Si $n, m \in \mathbb{N}$ entonces $\varphi(n+m) = \varphi(n) + \varphi(m)$

Sean $n, m \in \mathbb{N}$, supongamos que $\varphi(n+m)$

$\varphi(n+m) = (n+m+1, 1)$ por def de φ , ahora veamos que

$\varphi(n) = (n+1, 1)$, $\varphi(m) = (m+1, 1)$, que $\varphi(n) + \varphi(m) =$

$(n+1+m+1, 1+1) = (n+m+2, 2)$

veamos que $\varphi(n+m) \sim \varphi(n)+\varphi(m)$ ya que

$$(n+m+1, 1) \sim (n+m+2, 2) \stackrel{\text{def}}{\sim}$$

$$n+m+1+2 = n+m+2+1$$

$$\Rightarrow n+m+3 = n+m+3$$

por lo tanto $\varphi(n+m) = \varphi(n)+\varphi(m)$ \square

(C) Si $n, m \in \mathbb{N}$ entonces $\varphi(nm) = \varphi(n)\varphi(m)$

Sean $n, m \in \mathbb{N}$ $\sup_{a, b} \varphi(a, b) = \varphi(nm)$,

$\varphi(nm) = ((nm)+1, 1)$ por def de φ , entonces

$$\begin{aligned} \varphi(n)\varphi(m) &= ((n+1)(m+1)+(1)(1), (n+1)1+(m+1)1) = \\ &= ((nm+n+m+1+1), (n+1+m+1)) \end{aligned}$$

PD $\varphi(nm) \sim \varphi(n)\varphi(m)$

$\sup \varphi(nm) \sim \varphi(n)\varphi(m)$, veamos que por def \sim

$$nm+1+n+1+m+1 = nm+n+m+1+1+1$$

$$\Rightarrow nm+n+m+3 = nm+n+m+3$$



(1) Si $n, m \in \mathbb{N}$ tales que $n < m$ entonces $\varphi(n) < \varphi(m)$

Sea $n, m \in \mathbb{N}$ tales que $n < m$

Veamos que $\varphi(n) = (n+1, 1)$ y $\varphi(m) = (m+1, 1)$ por def de φ

Veamos que $n+1+1 < m+1+1 \Rightarrow n < m$ y al sumar

bonito se mantiene la desigualdad \Rightarrow ya que $n+1+1 < m+1+1$

por def de $<$ en \mathbb{Z} tenemos que $(n+1, 1) < (m+1, 1)$

$\Rightarrow \varphi(n) < \varphi(m)$ \square

(2) Demuestra que en \mathbb{Z} la ecuación $3x=1$ no tiene solución

Supongamos, para obtener una contradicción, que sí tiene solución

Por lo tanto existe $x \in \mathbb{Z}$ tal que $3x=1$

por lo tanto 3 sería una unidad en \mathbb{Z} , pero ya demostramos

que en \mathbb{Z} las únicas unidades son 1, -1 por lo tanto $x \notin \mathbb{Z}$

generando una contradicción por lo tanto $3x=1$ no

tiene solución en \mathbb{Z}

\square

(8) Sea A un anillo conmutativo con 1 , decimos que $a \in A$

es una unidad si existe $b \in A$ tal que $ab = 1 = ba$

Determine cuales son las unidades de \mathbb{Z} y cuales son las unidades

del anillo que asociamos al reloj de 12 horas

• Unidades en \mathbb{Z}

$$1 \text{ ya que } 1 \cdot 1 = 1$$

$$-1 \text{ ya que } -1 \cdot -1 = 1$$

• Unidades en Reloj de 12 horas

$$5 \text{ ya que } 5 \cdot 5 = 1$$

$$7 \text{ ya que } 7 \cdot 7 = 1$$

$$1 \text{ ya que } 1 \cdot 1 = 1$$

$$11 \text{ ya que } 11 \cdot 11 = 1$$

(9) Determina un algoritmo para sumar y multiplicar en el reloj de 12 horas

O Suma

```
1 Input n, m (dos numeros entre 1 y 12)
2 Output z (un numero entre 1 y 12)
3 z = n + m
4 if z > 12
5     z = z - 12
6 return z
```

O Multiplicar

```
1 Input n, m (dos numeros entre 1 y 12)
2 Output z (un numero entre 1, 12)
3 z = n * m
4 if z > 12
5     aux = z % 12      (modulo, el residuo de la division sobre 12)
6     if aux = 0
7         z = 12
8     else
9         z = aux
10 return z
```

(10) Escribe las tablas de sumar y multiplicar del reloj de 12 horas

+	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

X	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	2	4	6	8	10
3	3	6	9	12	3	6	9	12	3	6	9	12
4	4	8	12	4	8	12	4	8	12	4	8	12
5	5	10	3	8	1	6	11	4	9	2	7	12
6	6	12	6	12	6	12	6	12	6	12	6	12
7	7	2	9	4	11	6	1	8	3	10	5	12
8	8	4	12	8	4	12	8	4	12	8	4	12
9	9	6	3	12	9	6	3	12	9	6	3	12
10	10	8	6	4	2	12	10	8	6	4	2	12
11	11	10	9	8	7	6	5	4	3	2	1	12
12	12	12	12	12	12	12	12	12	12	12	12	12

(II) Demuestra que hay una infinidad de primos de la forma

$3n+2$ con $n \in \mathbb{N}$

Supongamos que hay finitos, que existen m primos de la

forma $3n+2$ con $n \in \mathbb{N}$ los cuales son $p_1, p_2, \dots, p_m = p_i$

Sea

$$N = 3(p_1 p_2 \dots p_m) + 2$$

P.D que N tiene un factor primo que no está en p_1, p_2, \dots, p_m

Veamos que N es impar ya que

si 2 es un factor de N , entonces no habría primos de la forma

$3n+2$. Y ya que 3 > cada p_1, p_2, \dots, p_m son impares

entonces $3(p_1 \dots p_m)$ también lo es por lo tanto

N es impar (un número impar es un número)

Ahora veamos que si 3 o alguno p_1, p_2, \dots, p_m fuese divisor

de N entonces también sería divisor de $N - 3(p_1 \dots p_m) = 2$

lo cual no se permite. Entonces N no es divisible por

$$2, 3, p_1, \dots, p_m$$

Como N es un producto de primos entonces podemos escribir

$$N = q_1 q_2 \cdots q_r \text{ , } \forall \text{ cada divisor primo } q_j \quad 1 \leq j \leq r$$

es de la forma $3n+1$ o $3n+2$, si todos fueran de la

forma $3k+1$ entonces

$$N = q_1 q_2 \cdots q_r = (3h_1 + 1)(3h_2 + 1) \cdots (3h_r + 1) = 3k + 1$$

donde k es de expandir el producto y agrupando los divisibles por 3

pero esto no sucede ya que N tiene un residuo de 2 al ser

dividido por 3

Por lo tanto hay un q en $q_1 q_2 \cdots q_r$ que es de la forma $3k+2$

lo llamaremos b y como N no es primo ni p_i entonces

$b \neq p_i$ con $1 \leq i \leq n$ la cual contradice que p_i son

todos los primos de la forma $3n+2$,

por lo tanto hay infinitos primos de la forma $3n+2$.