Axiomas de **PEANO**

a	$0 \in \mathbf{nat}$	// 0 es un elemento de **nat**
b	$(\forall n:\mathbf{nat}|: S.n \in \mathbf{nat})$	// si n está en **nat**, su sucesor también lo está
c	$(\forall n:\mathbf{nat}|: S.n \neq 0)$	// el 0 no es sucesor de ningún número natural
d	$(\forall n:\mathbf{nat}| S.n = S.m: n=m)$	// S es 1-1
e	$(\forall A:2^{\mathbf{nat}}| 0\in A \wedge (\forall n:A|: S.n\in A) : A = \mathbf{nat})$	

Principio del buen orden: Todo subconjunto no vacío de los naturales tiene un primer elemento o elemento mínimo, con respecto al orden estricto (**nat**,<).

Teo B (*Formas normales para* **nat**)

$n\in\mathbf{nat} \equiv n=0 \vee (\exists m:\mathbf{nat}|: n=S.m)$

a *divide* b $\equiv$ a|b
$\equiv (\exists c|: a*c = b)$

a *divisor de* b $\equiv$ a|b

b *multiplo de* a $\equiv$ a|b

Teorema A:
$n,d:\mathbf{int},\ d>0 \Rightarrow (\exists q,r|\ 0\le r<d : n = q*d+r)$
Además:
- si $n = q*d+r$, con $0\le r<d$, q y r son únicos
- si $\neg(d|n)$, existen q, r con $n = q*d+r$, $0<r<d$.

Nótese que la definición anterior permite afirmar que:
- x|0
- $0|x \equiv x=0$.

Además, se pueden establecer otros conceptos como, por ejemplo:
par.n $\equiv$ 2|n
impar.n $\equiv \neg$par.n

Teorema A:
1. $a|b \Rightarrow a|b*c$
2. $a|b \wedge b|c \Rightarrow a|c$
3. $a|b \wedge a|c \Rightarrow a|(m*b + n*c)$
4. $c\neq 0 \Rightarrow (c*a|c*b \equiv a|b)$
5. $a|b \wedge b|a \Rightarrow a = \pm b$
6. $a|b \wedge a>0 \wedge b>0 \Rightarrow a\le b$

```
// Pre: n≥0 ∧ d>0
q= 0;
r= n;
// Inv: n = q*d+r ∧ 0≤r
// Cota: r-d
while (r≥d) {
   q= q+1;
   r= r-d;
}
// Pos: n = q*d+r ∧ 0≤r<d
```

Definición B:
p *primo* $\equiv$ $p>1 \wedge (\forall d:\mathbf{nat}|\ d>0 \wedge d|p : d=1 \vee d=p)$

Definición A

Se definen las funciones
mcd: **int** × **int** → **nat** // *máximo común divisor*
mcm: **int** × **int** → **nat** // *mínimo común múltiplo*

así:
mcd(0,0) = 0
mcd(b,c) = (max d:**nat**| d|b ∧ d|c : d) , en otro caso

mcm(0,0) = 0
mcm(b,c) = (min m:**nat** | b|m ∧ c|m : m) , en otro caso

1 $mcd(b,c) = mcd(c,b)$

2 $(b,c)\neq(0,0) \Rightarrow mcd(b,c) = (\min x,y \mid b*x+c*y>0 : b*x+c*y)$

3 $mcd(b,c) = d \Rightarrow (\exists x,y \mid : d=bx+cy)$
Es un corolario del resultado anterior.

4 $mcd(b,mcd(c,d)) = mcd(mcd(b,c),d)$

5 $d|c \wedge d|b \Rightarrow d|mcd(b,c)$

6 $mcd(b,b) = |b|$

7 $mcd(b,1) = 1$

8 $mcd(b,0) = |b|$

9 $mcd(b,c) = mcd(|b|,|c|)$

10 $mcd(b,c) = mcd(b,b+c) = mcd(b,b-c)$

11 $d>0 \Rightarrow d*mcd(b,c) = mcd(d*b,d*c)$

12 $d|b \wedge d|c \wedge d>0 \Rightarrow mcd(b/d,c/d) = mcd(b,c)/d$
Si $g = mcd(b,c)$: $mcd(b/g,c/g) = 1$.

13 $d|b*c \wedge mcd(d,c)=1 \Rightarrow d|b$

14 $b|m \wedge c|m \Rightarrow mcm(b,c)|m$

15 $m>0 \Rightarrow mcm(m*b,m*c) = m*mcm(b,c)$

16 $mcm(b,c)*mcd(b,c)= b*c$

Si a l b y b l a, entonces si ambos son positivos, a = b

Algoritmo de Euclides

Versión 1: restas

```
// Pre: b>0 ∧ c>0

x = b;
y = c;

// Inv: x>0 ∧ y>0 ∧ mcd(x,y) = mcd(b,c)
// Cota: x+y

while (x!=y){
   if (x>y){
      x = x-y;
   }
   else y = y-x;
}

// Pos: x = mcd(b,c)
```

Versión 2: divisiones

```
// Pre: b≥0 ∧ c≥0

x = b;
y = c;

// Inv: x≥0 ∧ y≥0 ∧ mcd(x,y) = mcd(b,c)
// Cota: y

while (y!=0){
   int x1 = x;
   x = y;
   y = x1 % x;
}
// Pos: x = mcd(b,c)
```

Teorema fundamental de la Aritmética: todo número natural se puede expresar como producto de primos.

$n = (*p|\ p \text{ primo}: p^e)$

$$220 = 2^2 * 3^0 * 5^1 * 7^0 * 11^1 \quad \overline{n}$$

$$\overline{220} = \langle 2,0,1,0,1 \rangle$$

Teo C:

a $\overline{m*n}_k = \overline{m}_k + \overline{n}_k$

b $m|n \equiv (\forall k|: \overline{m}_k \le \overline{n}_k.$ $\overline{220*126} = \langle 2+1,0+2,1+0,0+1,1+0 \rangle = \langle 3,2,1,1,1 \rangle$

c $\overline{mcd(b,c)}_k = min(\overline{m}_k, \overline{n}_k)$

d $\overline{mcm(b,c)}_k = max(\overline{m}_k, \overline{n}_k)$

Teorema A

$p \text{ primo},\ p|a*b \Rightarrow p|a \lor p|b$

Teorema C

Hay infinitos primos.

CONGRUENCIAS

Sean a,b,m:**int**, m≠0.

$a =_m b \equiv m|(b-a)$

Teorema A

Sean a,b,c,d,m:**int**, m≠0.

1 $a =_m b \equiv res(a,m)=res(b,m)$

2 $a =_m a$

3 $a =_m b \quad \Rightarrow \quad b =_m a$

4 $a =_m b \;\wedge\; b =_m c \;\Rightarrow\; a =_m c$

5 $a =_m b \;\Rightarrow\; a+c =_m b+c$

6 $a =_m b \;\Rightarrow\; a*c =_m b*c$

7 $a =_m b \;\wedge\; c =_m d \;\Rightarrow\; a+c =_m b+d$

8 $a =_m b \;\wedge\; c =_m d \;\Rightarrow\; a*c =_m b*d$

Teorema B

Sean `a,x,y,d,m,n:`**`int`**; $d,n\neq 0$; $a,m>0$

1 $a*x =_m a*y \;\equiv\; x =_{m/mcd(a,m)} y$

2 $a*x =_m a*y \;\wedge\; mcd(a,m)=1 \;\Rightarrow\; x =_m y$

3 $x =_m y \wedge d|m \;\Rightarrow\; x =_d y$

4 $x =_m y \wedge x =_n y \;\equiv\; x =_{mcm(m,n)} y$

Divisibilidad:

Teorema A

1 $n =_3 (+k|\; 0\leq k<r : d_k)$

Dem:

Nótese que $10 =_3 1$. Usando repetidamente propiedades de las congruencias, se llega a $10^k =_3 1$, para cualquier k, $0\leq k<r$. También: $d_k*10^k =_3 d_k$, $0\leq k<r$. Por tanto:

$$
\begin{aligned}
& n \\
= \;& \\
& (+k|\; 0\leq k<r : d_k*10^k) \\
=_3 \;& \\
& (+k|\; 0\leq k<r : d_k)
\end{aligned}
$$

2 $n =_9 (+k|\; 0\leq k<r : d_k)$

3 $n =_{11} (+k|\; 0\leq k<r : (-1)^k*d_k)$

Teorema A (*de Fermat*)

p primo, $\neg(p|a) \;\Rightarrow\; a^{p-1} =_p 1$

Primos relativos:

$m,n>0: \quad m \perp n \;\equiv\; mcd(m,n)=1$ // m, n son *primos relativos*

$\varphi(n) = (+k \mid 0<k\leq n \wedge k\perp n : 1)$ // *función* φ *de Euler*
// No. de primos relativos a n, menores o iguales que n

$\varphi(n) = n * (*p \mid p|n \wedge primo.p : (1-1/p))$

$\varphi(p) = p * (1-1/p) = p-1.$

$a*x =_m b \quad x =_m a^{\varphi(m)-1}*b \qquad x =_m r^{\varphi(m)-1}*s. \qquad r = a \bmod m,\ s = b \bmod m.$

Teorema D (*de Euler*)
$a \perp m \;\Rightarrow\; a^{\varphi(m)} =_m 1$

INDUCCIÓN

Teo : $(\forall n \mid : p.n)$
Dem:
Inducción sobre **nat**.
Predicado de inducción: $p.n \equiv \ldots$

Caso base: $p.0$
⟨Demostración de $p.0$⟩

Caso Inductivo: $p(n+1)$
HI: $p.n,\ n\geq 0$
⟨Demostración de $p(n+1)$⟩

Teo: $(\forall n \mid : n^3-n =_3 0)$
Dem:
Inducción sobre **nat**.
Predicado de inducción: $d.n \equiv n^3-n =_3 0,\ n\geq 0$

Caso Base: $d.0$
0^3-0
$=$ ⟨Aritmética⟩
0
$=_3$ ⟨$=_m$ reflexiva⟩
0

Caso Inductivo: $d(n+1)$
HI: $d.n,\ n\geq 0$
$(n+1)^3-(n+1)$
$=$ ⟨Aritmética⟩
$n^3+3n^2+3n+1-n-1$
$=$ ⟨Aritmética⟩
$n^3-n + 3*(n^2+n)$
$=_3$ ⟨HI: $n^3-n =_3 0$⟩
$3*(n^2+n)$
$=_3$ ⟨$m*x =_m 0$⟩
0

Definiciones recursivas:

(1) Definir $f.0,\ldots,f.n_0$, para un $n_0\in$**nat**.
(2) Definir $f.k$, usando valores anteriores $f.0,\ldots,f(k-1))$, para $n_0<k$.

Ejemplo A

1 Dado un número natural $a>0$, considérese la función g definida así:

g: **nat** $\rightarrow$ **nat**
$g.0 = 1$
$g(2*n) = (g.n)*(g.n) \quad , n\geq 0$
$g(2*n+1) = g(2*n)*a \quad , n\geq 0$

La definición de g es buena: se define en 0 y, para $n\geq 0$ está bien definida, considerando el caso en que n sea par o impar. Cuando n es par la definición se apoya en la de $g(n/2)$; cuando es impar, en la de $g(n-1)$.

Se puede mostrar que $g.n = a^n$, $n\geq 0$. Nótese que se necesita una inducción fuerte que, además, sigue el esquema de casos que está presente en la definición de g. Como ya se dijo, esto no es casual.

EJEMPLOS DE EJERCICIOS:

3a El residuo de la división entera $(13*4^{713} + 5) \div 11$

AYUDA: Use el Teorema de Fermat y aritmética modular.

Para aplicar aritmética modular, se pueden calcular residuos módulo 11 de los operandos de la expresión.
Así, si

$13 =_{11} r$

$4^{713} =_{11} s$

$5 =_{11} t$

3a mcd(19288544,19288550)

$$
\begin{aligned}
& \quad \text{mcd}(19288544,19288550) \\
= & \quad \langle \text{mcd}(a,b) = \text{mcd}(a-b,b) \rangle \\
& \quad \text{mcd}(19288544,6) \\
= & \quad \langle \text{mcd}(p*a,p*b) = p*\text{mcd}(a,b) \rangle \\
& \quad 2*\text{mcd}(9644272,3) \\
= & \quad \langle \neg(3 \mid 9644272),\ \text{primo}.3 \rangle \\
& \quad 2*1 \\
= & \quad \langle \text{aritmética} \rangle \\
& \quad 2
\end{aligned}
$$

se tendrá que

$\text{res}(13*4^{713} + 5,\ 11) =_{11} r*s+t$

Claramente:

$13 =_{11} r = 2$

$5 =_{11} t = 5$

Para calcular t tal que $4^{713} =_{11} s,\ 0 \le s < 11$.

Por el Teorema de Fermat, ya que $\text{mcd}(4,11)=1, \text{primo}.11$:

$$
\begin{aligned}
& 4^{11-1} =_{11} 1 \\
= & \\
& 4^{10} =_{11} 1
\end{aligned}
$$

Por tanto (multiplicando miembro a miembro 71 veces):

$$
\begin{aligned}
& (4^{10})^{71} =_{11} 1^{71} \\
= & \\
& 4^{710} =_{11} 1 \\
= & \quad \langle\ a =_m b \Rightarrow a*p =_m b*p\ \rangle \\
& 4^{713} =_{11} 4^3 \\
= & \quad \langle 64 = 4^3 \rangle \\
& 4^{713} =_{11} 64 \\
= & \quad \langle 64 = 11*5 + 9 \rangle \\
& 4^{713} =_{11} 9
\end{aligned}
$$

Es decir, $s=9$.

Resumiendo:

$$
\begin{aligned}
& \text{res}(13*4^{713} + 5,\ 11) \\
=_{11} & \\
& 2*9+5 \\
=_{11} & \\
& 23 \\
=_{11} & \\
& 1.
\end{aligned}
$$

Sistemas de congruencia:

1 **[25/100]**

Encuentre todas las soluciones para el sistema de congruencias (x, y: **int**):

(1) $5*x + 6*y \equiv_3 12$

(2) $4*x + 2*y \equiv_3 1$

Sumando miembro a miembro las congruencias se llega a

(3) $9*x + 8*y \equiv_3 13$

Por tanto, ya que $9*x \equiv_3 0$, $8*y \equiv_3 -y$, $13 \equiv_3 1$:

$0 - y \equiv_3 1$

≡

$y \equiv_3 -1$

≡

$y \equiv_3 2$

Ahora, remplazando en la congruencia (2) el valor $y \equiv_3 -1$

$4*x - 2 \equiv_3 1$

≡

$4*x \equiv_3 3$

≡ $\langle\ 4*x \equiv_3 x;\ 3 \equiv_3 0\ \rangle$

$x \equiv_3 0$

Resumiendo, las soluciones son de la forma

$x \equiv_3 0,\ y \equiv_3 2$

O, equivalentemente:

$x = 3*u,\ y = 2+3*v$, u,v∈**int**.

Como demostrar que un número es divisible:

3 **[25/100]**

Pruebe que, para todo $n \in \mathbf{nat}$: $n*(n+1)*(2*n+1)$ es divisible por 3.

Dem: Inducción sobre $n \in \mathbf{nat}$.

Predicado de Inducción: $Q.n \equiv n*(n+1)*(2*n+1) =_3 0 \quad , \quad n \geq 0$

Caso Base: $Q.0$

$0*(0+1)*(2*0+1)$

$=$ ⟨Aritmética⟩

0

$=_3$

0

Caso Inductivo: $Q(n+1)$

HI: $Q.n$, $n \geq 0$

$(n+1)*(n+1+1)*(2*(n+1)+1)$

$=$ ⟨Aritmética⟩

$(n+1)*(n+2)*(2*n+3)$

$=_3$ ⟨ $3 =_3 0$ ⟩

$(n+1)*(n+2)*2*n$

$=$ ⟨Aritmética⟩

$n*(n+1)*(2n+4)$

$=_3$ ⟨ $4 =_3 1$ ⟩

$n*(n+1)*(2*n+1)$

$=_3$ ⟨HI⟩

0

$=_3$ ⟨Caso: $n =_3 1$⟩

$1*(1+1)*(2*1+1)$

$=_3$

$1*2*3$

$=_3$

0

Caso: $n =_3 2$

$n*(n+1)*(2*n+1)$

$=_3$ ⟨Caso: $n =_3 1$⟩

$2*(2+1)*(2*2+1)$

$=_3$

$2*3*5$

$=_3$

0