ISIS 1104 Matemática Estructural y Lógica
Semestre 2018-10
Parcial 3 – Mayo 10, 2018
Prof. Rodrigo Cardoso

****

1 **[25/100]**

Para `X⊆nat`, sea `DC.X` el conjunto de divisores comunes de todos los elementos de `X`.
El "." en la notación se omite si no hay posibilidad de confusión.
Note, por ejemplo, que

- `DC{a} = {d:nat| d|a}`
- `mcd(a,b) = (max d| d∈DC{a,b}: d)`

Demuestre las siguientes afirmaciones:

1a (4/25) `DC{b,c} = DC{b} ∩ DC{c}`

```
Dem:
   d ∈ DC{b,c}
=      〈Def DC〉
   d|b ∧ d|c
=      〈Def DC, 2 veces〉
   d∈DC{b} ∧ d∈DC{c}
=      〈Def ∩〉
   d ∈ DC{b} ∩ DC{c}
```

[4/4]

1b (7/25) `DC{mcd(b,c)} = DC{b} ∩ DC{c}`

```
Dem:
Lema 1b1: DC{mcd(b,c)} ⊆ DC{b} ∩ DC{c}
      Dem:
         d ∈ DC{mcd(b,c)}
      =       〈Def DC〉
         d|mcd(b,c)
      ⇒       〈mcd(b,c)|b, mcd(b,c)|c; transitividad de .|.〉
         d|b ∧ d|c
      =       〈def DC, 2 veces〉
         d∈DC{b} ∧ d∈DC{c}
      =       〈Def ∩〉
         d ∈ DC{b} ∩ DC{c}

Lema 1b2: DC{mcd(b,c)} ⊇ DC{b} ∩ DC{c}
      Dem:
         d ∈ DC{b} ∩ DC{c}
      =       〈Def ∩〉
         d∈DC{b} ∧ d∈DC{c}
      =       〈def DC, 2 veces〉
         d|b ∧ d|c
      ⇒       〈d|b ∧ d|c   ⇒   d|mcd(b,c)〉
         d|mcd(b,c)
      =       〈Def DC〉
         d ∈ DC{mcd(b,c)}
```

Ahora:

```
   DC{mcd(b,c)} = DC{b} ∩ DC{c}
=     ⟨Lema 1a1, 1a2⟩
   true
```

[7/7]

Variante (prueba ecuacional):

(Esta demostración requiere conocer el teorema: `d|mcd(b,c) ≡ d|b ∧ d|c`)

Dem:

```
        d ∈ DC{mcd(b,c)}
   =          ⟨Def DC⟩
        d|mcd(b,c)
   =          ⟨ d|mcd(b,c) ≡  d|b ∧ d|c ⟩
        d|b ∧ d|c
   =          ⟨Def DC, 2 veces⟩
        d∈DC{b} ∧ d∈DC{c}
   =          ⟨Def ∩⟩
        d ∈ DC{b} ∩ DC{c})
```

[7/7]

1c (7/25) `DC{a,mcd(b,c)} = DC{mcd(a,b),c}`

Dem:

```
   DC{a,mcd(b,c)}
=     ⟨1a⟩
   DC{a} ∩ DC{mcd(b,c)}
=     ⟨1b⟩
   DC{a} ∩ DC{b} ∩ DC{c}
=     ⟨1b⟩
   DC{mcd(a,b)} ∩ DC{c}
=     ⟨1a⟩
   DC{mcd(a,b),c}
```

[7/7]

1d (7/25) Muestre que `mcd` es una operación asociativa

```
   mcd(a,mcd(b,c))
=     ⟨Def mcd⟩
   max(d| d∈DC{a,mcd(b,c)} : d)
=     ⟨1c⟩
   max(d| d∈DC{mcd(a,b),c} : d)
=     ⟨Def mcd⟩
   mcd(mcd(a,b),c)
```

[7/7]

.

2 **[25/100]**

Un joyero quiere repartir su herencia entre sus 5 hijos, equitativamente. En total tiene r rubíes y d diamantes. Si reparte todas las piedras en 5 grupos, le quedan 2 piedras por repartir. Entonces, decide darle un valor de \$3 a cada rubí y un valor de \$2 a cada diamante, pero al repartir en 5 grupos iguales le queda \$1 por repartir. Por otra parte, si valora en \$2 cada rubí y en \$3 cada diamante le sobran \$4 para repartir. Pruebe que d, el número de diamantes, es divisible por 5.

Las condiciones del problema se pueden modelar así:

[1] $r + d =_5 2$

[2] $3r + 2d =_5 1$

[3] $2r + 3d =_5 4$

[9/25]

Restando [3] de [2]:

[4] $r - d =_5 -3$

Sumando [1] y [4]:

[5] $2r =_5 -1$

o bien

[6] $2r =_5 4$

Como mcd(2,5)=1, de [6] se puede inferir:

[7] $r =_5 2$

Y, remplazando en [1]:

[8] $2 + d =_5 2$

de donde

[9] $d =_5 0$

[16/25]

Variante:

Multiplicando [1] por -2:

[2'] $-2r -2d =_5 -4$

Sumando con [3]

[3'] $d =_5 0$

OJO: Solo usa 2 restricciones. Si en la primera parte no plantea la restricción no usada: bono +3.

[16/25]

3 **[25/100]**

Pruebe que, para todo $n \in$ **nat**: $8^{n+2} + 9^{2n+1}$ es divisible por 73.

Dem: Inducción sobre **nat**.

[2/25]

Predicado de inducción: $p.n \equiv (8^{n+2} =_{73} (-9)^{2n+1}),\ n\geq 0$

[8/25]

Caso base: $p.0$

$8^{0+2} =_{73} (-9)^{2*0+1}$

$=$ ⟨ aritmética ⟩

$64 =_{73} -9$

$=$ ⟨ aritmética ⟩

true

[5/25]

Caso inductivo: $p(n+1)$

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

$8^{n+1+2} =_{73} (-9)^{2(n+1)+1}$

$=$ ⟨ aritmética ⟩

$8*8^{n+2} =_{73} (-9)^{2}(-9)^{2n+1}$

$=$ ⟨ HI, aritmética modular ⟩

$8*8^{n+2} =_{73} (-9)^{2}8^{n+2}$

$=$ ⟨ $mcd(8^{n+2},73) = 1$ ⟩

$8 =_{73} (-9)^{2}$

$=$ ⟨ aritmética ⟩

$8 =_{73} 81$

$=$ ⟨ aritmética ⟩

true

[10/25]

Variante (Inducción usando directamente divisibilidad)

Dem: Inducción sobre **nat**.

[2/25]

Predicado de inducción: $q.n \equiv 73|(8^{n+2}+9^{2n+1}),\ n\geq 0$

[8/25]

Caso base: $q.0$

$73|(8^{0+2}+9^{0+1})$

$=$ ⟨ aritmética ⟩

$73|(64+9)$

$=$ ⟨ aritmética ⟩

true

[5/25]

Caso inductivo: $q(n+1)$

HI: $8^{n+2} + 9^{2n+1} = 73*k,\ n\geq 0$ // $k = (8^{n+2}+9^{2n+1})\div 73$

$8^{(n+1)+2} + 9^{2(n+1)+1}$

$=$ ⟨ aritmética ⟩

$8*8^{n+2} + 81*9^{2n+1}$

$=$ ⟨ HI: $8^{n+2} = 73*k - 9^{2n+1}$ ⟩

```
   8*(73*k - 9^(2n+1))  + 81*9^(2n+1)
=     ⟨ aritmética ⟩
   8*73*k - 8*9^(2n+1)  + 81*9^(2n+1)
=     ⟨ aritmética ⟩
   8*73*k + 73*9^(2n+1)
=     ⟨ aritmética ⟩
   73*(8*k + 9^(2n+1))
```

Es decir:

$73 \mid (8^{(n+1)+2} + 9^{2(n+1)+1})$

[10/25]

4 **[25/100]**

Considere el

```
TAD Lista[nat]
 * vac   :                → Lista
 * ins   : Lista × nat    → Lista
   prim  : Lista          → nat
   resto : Lista          → Lista
   esv   : Lista          → bool
   tam   : Lista          → nat
Axiomas
   …
DAT
```

con los axiomas que se discuten en las notas del curso.

4a (10/25) Enriquezca el `TAD Lista[nat]` con una función

`sumal : Lista → nat`

definiendo axiomas para que su semántica sea

`sumal(ln)` ≈ "suma de los elementos de la lista `ln`"

```
[s1] sumal(vac) = 0
[s2] sumal(ins(ln,n)) = sumal(ln)+n
```

[10/10]

4b (15/25) Use su definición para probar que la suma de los elementos de una lista que consta de solo `1`'s es igual al tamaño de la lista.

Sea `s` una lista que consta de solo `1`'s. Entonces `s` es igual a `vac` (la lista vacía de `1`'s) o es de la forma `ins(s1,1)`, donde `s1` es una lista que consta solo de `1`'s.

Se probará por inducción estructural el resultado.

[2/2]

Predicado de inducción: `P.s ≡ sumal.s = tam.s, s` consta solo de `1`'s.

[3/3]

Caso base: `P.vac`

```
   sumal(vac)
=     ⟨s1⟩
   0
```

```
=      ⟨t1⟩
   tam(vac)
```

[5/5]

Caso inductivo: `P(ins(s1,1))`

HI: `P.s1`

```
   suma1(ins(s1,1))
=      ⟨s2⟩
   suma1(s1)+1
=      ⟨HI⟩
   tam(s1)+1
=      ⟨t2⟩
   tam(ins(s1),1)
```

[5/5]