ISIS 1104 Matemática Estructural y Lógica
Semestre 2015-10
Parcial 3 – Mayo 7, 2015
Prof. Rodrigo Cardoso

****

1 **[30/100]**

1a (20/30) Demuestre que $2^j =_3 (-1)^j$, para $j \geq 0$.

Dem: Inducción sobre $j \geq 0$.

[2/2]

Predicado de inducción: $P.j \equiv 2^j =_3 (-1)^j,\ j \geq 0$.

[3/3]

Caso base: $P.0$

$$
\begin{array}{ll}
 & 2^0 \\
= & \langle \text{aritmética} \rangle \\
 & 1 \\
= & \langle \text{aritmética} \rangle \\
 & (-1)^0 \\
=_3 & \langle =_m \text{ - reflexividad} \rangle \\
 & (-1)^0
\end{array}
$$

[5/5]

Caso inductivo: $P(j+1)$
HI: $P.j,\ j \geq 0$

$$
\begin{array}{ll}
 & 2^{j+1} \\
= & \langle \text{aritmética} \rangle \\
 & 2 * 2^j \\
= & \langle 2 =_3 -1 \rangle \\
 & (-1) * 2^j \\
=_3 & \langle HI \rangle \\
 & (-1) * (-1)^j \\
= & \langle \text{aritmética} \rangle \\
 & (-1)^{j+1}
\end{array}
$$

[10/10]

[]

1b (10/30) Sea $(b_n b_{n-1} \ldots b_0)_2$ una expresión binaria para un número natural N, i.e.,

(i) $b_j \in \{0,1\},\ 0 \leq j \leq n$;

(ii) $N = (+j \mid 0 \leq j \leq n : 2^j\, b_j)$.

Pruebe que $N =_3 (+j \mid 0 \leq j \leq n : (-1)^j\, b_j)$.

Dem:

$$
\begin{array}{ll}
 & N \\
= & \langle (ii) \rangle \\
 & (+j \mid 0 \leq j \leq n : 2^j\, b_j)
\end{array}
$$

$=_3$ ⟨1a⟩

$(+j|\ 0\leq j\leq n : (-1)^j\ b_j)$

[10/10]

Variante:

Dem: Inducción sobre $n\geq 0$.

[1/10]

PI: $P.n \equiv (+j|\ 0\leq j\leq n : 2^j\ b_j) =_3 (+j|\ 0\leq j\leq n : (-1)^j\ b_j),\ n\geq 0.$

[2/10]

Caso Base: P.0

$(+j|\ 0\leq j\leq 0 : 2^j\ b_j)$

$=$ ⟨Un punto⟩

$2^0\ b_0$

$=$ ⟨aritmética⟩

b_0

$=_3$ ⟨$=_3$ -reflexividad⟩

b0

[2/10]

Caso Inductivo: P(n+1)

HI: $(+j|\ 0\leq j\leq n : 2^j\ b_j) =_3 (+j|\ 0\leq j\leq n : 2^j\ b_j),\ n\geq 0$

$(+j|\ 0\leq j\leq n+1 : 2^j\ b_j)$

$=$ ⟨Partir rango a la derecha⟩

$(+j|\ 0\leq j\leq n : 2^j\ b_j) + 2^{n+1}\ b_{n+1}$

$=$ ⟨HI⟩

$(+j|\ 0\leq j\leq n : (-1)^j\ b_j) + 2^{n+1}\ b_{n+1}$

$=$ ⟨1a⟩

$(+j|\ 0\leq j\leq n : (-1)^j\ b_j) + (-1)^{n+1}\ b_{n+1}$

$=$ ⟨Partir rango a la derecha⟩

$(+j|\ 0\leq j\leq n+1 : (-1)^j\ b_j)$

[5/10]

2 **[10/100]** Encuentre qué está mal en la siguiente argumentación, en la que se prueba que todo número de Fibonacci F_n es par, o bien, $F_n =_2 0$, para $n\geq 3$.

"Se probará por inducción fuerte sobre $n\geq 3$.

Para n=3 , claramente $F_3 = F_2 + F_1 = F_1 + F_0 + F_1 = 1 + 0 + 1 = 2 =_2 0$.

Supóngase ahora que $n\geq 4$ y que F_m es par, para $m<n$. Ahora,

F_n

$=$ ⟨Def F⟩

$F_{n-1} + F_{n-2}$

$=_2$ ⟨Hip Ind. en valores anteriores⟩

$0 + 0$

$=$ ⟨aritmética⟩

0

Es decir, $F_n =_2 0$ "

El caso F_4 se apoya en que el resultado valga para n=3 (caso base) y n=2 (no demostrado).

[5/10]

De hecho, $F_2 = F_1 + F_0 = 1 + 0 =_2 1$. Es decir, el resultado es falso en n=2. La prueba de F_4 no es correcta y, por tanto, tampoco son correctas las pruebas para F_n, con n>4.

[5/10]

3 **[30/100]** Explicando sus respuestas, determine valores para

3a mcd(19288544,19288550)

```
  mcd(19288544,19288550)
=    ⟨mcd(a,b) = mcd(a-b,b)⟩
  mcd(19288544,6)
=    ⟨mcd(p*a,p*b) = p*mcd(a,b)⟩
  2*mcd(9644272,3)
=    ⟨¬(3|9644272), primo.3⟩
  2*1
=    ⟨aritmética⟩
  2
```

[10/10]

3b mcd(19288544,mcd(2224,19288550))

```
  mcd(19288544,mcd(2224,19288550))
=    ⟨mcd conmutatividad⟩
  mcd(19288544,mcd(19288550,2224))
=    ⟨mcd asociatividad⟩
  mcd(mcd(19288544,19288550),2224))
=    ⟨3a⟩
  mcd(2, 2224))
=    ⟨mcd(p*a,p*b) = p*mcd(a,b)⟩
  2*mcd(1, 1112)
=    ⟨mcd(1,x) = 1⟩
  2*1
=    ⟨aritmética⟩
  2
```

[10/10]

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

$13 =_{11} r$

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

$5 =_{11} t$

se tendrá que

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

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 mcd(4,11)=1, primo.11:

$\quad 4^{11-1} =_{11} 1$

=

$\quad 4^{10} =_{11} 1$

Por tanto (multiplicando miembro a miembro 71 veces):

$\quad (4^{10})^{71} =_{11} 1^{71}$

=

$\quad 4^{710} =_{11} 1$

= $\quad \langle\ a =_m b \Rightarrow a*p =_m b*p\ \rangle$

$\quad 4^{713} =_{11} 4^3$

= $\quad \langle 64 = 4^3 \rangle$

$\quad 4^{713} =_{11} 64$

= $\quad \langle 64 = 11*5 + 9 \rangle$

$\quad 4^{713} =_{11} 9$

Es decir, s=9.

Resumiendo:

$\quad res(13*4^{713} + 5,\ 11)$

$=_{11}$

$\quad 2*9+5$

$=_{11}$

$\quad 23$

$=_{11}$

$\quad 1.$

[10/10]

4 **[30/100]** Defina las siguientes funciones

d: **nat** × **nat**$^+$→ **nat**

[d1] d(a,b) = 0 , si a<b

[d2] d(a,b) = 1+d(a-b,b) , si a≥b

r: **nat** × **nat**$^+$→ **nat**

[r1] r(a,b) = a , si a<b

[r2] r(a,b) = r(a-b,b) , si a≥b

Demuestre que d(a,b) = a÷b y que r(a,b) = a **mod** b.

Dem: Inducción fuerte sobre a≥0.

Predicado de inducción: `P.a ≡ d(a,b) = a÷b ∧ r(a,b) = a` **mod** `b`, a≥0.

[5/5]

Caso base: `P.0`

```
   P.0
=      ⟨Def P⟩
   d(0,b) = 0÷b    ∧    r(0,b) = 0 mod b
=      ⟨0<b, [d1], [r1]⟩
   0 = 0÷b   ∧   0 = 0 mod b
=      ⟨ 0÷b = 0; 0 mod b = 0⟩
   0 = 0 ∧ 0 = 0
=
   true
```

[5/5]

Caso inductivo: `P.a`

`HI: P.x, para 0≤x<a.`

[5/5]

```
   P.a
=      ⟨Def P⟩
   d(a,b) = a÷b    ∧    r(a,b) = a mod b
```

Casos: `a<b, a≥b.`

[5/5]

Caso a<b:

```
   d(a,b) = a÷b    ∧    r(a,b) = a mod b
=        ⟨a<b, [d1], [r1]⟩
   0 = a÷b    ∧    a = a mod b
=        ⟨a<b, a÷b = 0; a mod b = a⟩
   0 = 0    ∧    a = a
=
   true
```

[5/5]

Caso a≥b:

```
   d(a,b) = a÷b    ∧    r(a,b) = a mod b
=        ⟨a≥b, [d2], [r2]⟩
   1+d(a-b,b) = a÷b    ∧    r(a-b,b) = a mod b
=        ⟨0≤a-b<a, HI⟩
   1+(a-b)÷b = a÷b    ∧    (a-b) mod b = a mod b
=        ⟨a-b≥0, (a-b)÷b = a÷b - 1; (a-b) mod b = a mod b ⟩
   1+ a÷b - 1  = a÷b    ∧    a mod b = a mod b
=        ⟨ aritmética ⟩
   true    ∧    true
=
   true
```

[5/5]

[]

Variante:

Se busca probar que las funciones `d` y `r` cumplen las condiciones del algoritmo de la división. Como el cociente y el residuo son únicos, se cumpliría el resultado deseado.

Dem: Inducción fuerte sobre a≥0.

Predicado de inducción: `Q.a ≡ a = d(a,b)*b + r(a,b) ∧ 0≤r(a,b)<b` , a≥0

[5/5]

Caso base: `Q.0`

```
   Q.0
=     ⟨Def Q⟩
   0 = d(0,b)*b + r(0,b) ∧  0≤r(0,b)<b
=     ⟨0<b, [d1], r[1]⟩
   0 = 0*b + 0 ∧ 0≤0<b
=     ⟨0<b; aritmética⟩
   true
```

[5/5]

Caso inductivo: `Q.a`

```
HI: Q.x, para 0≤x<a.
   Q.a
=     ⟨Def Q⟩
   a = d(a,b)*b + r(a,b) ∧  0≤r(a,b)<b
```

Casos: `a<b,  a≥b`.

[5/5]

Caso a<b:

```
      a = d(a,b)*b + r(a,b) ∧  0≤r(a,b)<b
   =        ⟨a<b, [d1], [r1]⟩
      a = 0*b + a ∧  0≤a<b
   =        ⟨a<b; aritmética⟩
      true
```

[5/5]

Caso a≥b:

```
      a = d(a,b)*b + r(a,b) ∧  0≤r(a,b)<b
   =        ⟨a≥b, [d2], [r2]⟩
      a = (1+d(a-b,b))*b + r(a-b,b) ∧  0≤r(a-b,b)<b
   =        ⟨aritmética⟩
      a-b = d(a-b,b)*b + r(a-b,b) ∧  0≤r(a-b,b)<b
   =        ⟨0≤a-b<a, HI⟩
      true
```

[5/5]

[]