UNIVERSIDAD SIMÓN BOLÍVAR
Dept. Computación y Tecnología de la Información
Estructuras Discretas II
CI 2526
Mayo-Julio 2021

Práctica 9
Soluciones
Gustavo Lau
2021-07-18

Comentario acerca de la clase pasada:

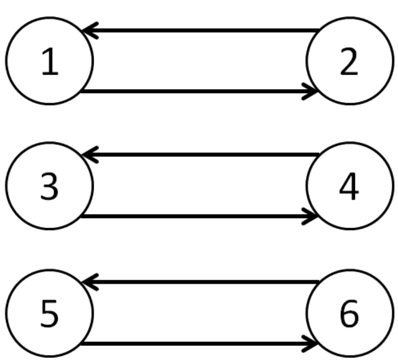
En la respuesta 7 usé erróneamente $=_{\mathbb{Z}}$ en vez de $=$. $=_{\mathbb{Z}}$ es una relación entre pares ordenados (a, b) de números naturales, en esas respuestas hay que usar la igualdad pues se está comparando clases de equivalencia $[(a, b)]$.

Pregunta de hora de consulta:

Estoy revisando la práctica 7 y tengo una duda en la pregunta 8: cuando dice que se busquen las potencias de R_1, ¿hay que buscarlas hasta que coincidan las matrices potencia, en el caso de ese ejercicio dejó de buscar las potencias cuando $M^3 = M^4$, y así poder encontrar la clausura transitiva?

Respuesta

Si el conjunto base tiene n elementos el teorema 5.6 del libro del prof. Yriarte nos dice que con $n-1$ potencias será suficiente. Pero nos podemos ahorrar trabajo parando cuando la matriz que obtienes sea igual a una de las potencias anteriores. Por ejemplo:



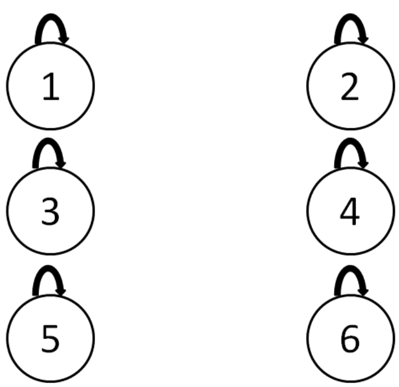
Si $A = \{1, 2, 3, 4, 5, 6\}$ y $R = \{(1, 2), (2, 1), (3, 4), (4, 3), (5, 6), (6, 5)\}$ entonces la matriz de adyacencia de R es:

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

y su cuadrado es:

$$M^2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = I \text{ (la matriz identidad)}$$

El grafo de R^2 representa los caminos de longitud 2 en el grafo de R:



$$M^3 = M$$

Las potencias pares son I y las impares son M.

1. **Definiciones:**

   Sea f una función de A en B, $f : A \to B$:

$$f \text{ es inyectiva } \equiv f(a) = f(b) \implies a = b$$

$$f \text{ es sobreyectiva } \equiv \forall b \in B \ (\exists a \in A \ (f(a) = b))$$

$$f \text{ es biyectiva } \equiv f \text{ es inyectiva y sobreyectiva}$$

   Demuestre que la siguiente función es biyectiva:

$$f : \mathbb{N} \to 2\mathbb{N}$$

$$f(n) = 2n$$

   donde $2\mathbb{N} = \{x \in \mathbb{N} | (\exists k \in \mathbb{N})(x = 2k)\}$.

$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \dots \\ 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & \dots \end{array}$$

Respuesta

Demostrar que f es una biyección es demostrar que $\mathbb{N}$ y $2\mathbb{N}$ tienen la misma cardinalidad. Intuitivamente:

f es inyectiva:

$$\begin{aligned} & f(a) = f(b) \\ \implies & \quad \langle \text{Definición de } f \rangle \\ & 2a = 2b \\ \equiv & \\ & a = b \\ \therefore\ & f(a) = f(b) \implies a = b \end{aligned}$$

f es sobreyectiva:

$$\begin{aligned} & b \in \{x \in \mathbb{N} | (\exists k \in \mathbb{N})(x = 2k)\} \\ \implies & \\ & \exists k \in \mathbb{N}(b = 2k) \\ \equiv & \quad \langle \text{Definición de } f \rangle \\ & \exists k \in \mathbb{N}(b = f(k)) \\ \therefore\ & \forall b \in 2\mathbb{N}\ (\exists a \in \mathbb{N}\ (f(a) = b)) \end{aligned}$$

$\therefore f$ es biyectiva

2. Demuestre que la siguiente función es biyectiva:

$$f : \mathbb{Z}^+ \to \mathbb{Z}$$

$$f(n) = \begin{cases} \frac{n-1}{2} & si \quad n\ es\ impar \\ \\ -\frac{n}{2} & si \quad n\ es\ par \end{cases}$$

$\mathbb{Z}^+$ son los enteros positivos (mayores a cero).

Respuesta

f es inyectiva:

Si $f(a) = f(b)$, dado que:

$$n \text{ es impar} \implies f(n) \geq 0$$

$$n \text{ es par} \implies f(n) < 0$$

a y b tienen que tener la misma paridad, es decir o ambos son pares o ambos son impares. Si ambos son impares:

$$\begin{aligned} f(a) &= f(b) \\ \frac{a-1}{2} &= \frac{b-1}{2} \\ a-1 &= b-1 \\ a &= b \end{aligned}$$

Si ambos son pares:

$$\begin{aligned} f(a) &= f(b) \\ -\frac{a}{2} &= -\frac{b}{2} \\ a &= b \end{aligned}$$

$\therefore f(a) = f(b) \implies a = b$

f es sobreyectiva:

Para preparar la demostración calculamos las funciones inversas:

$$\begin{aligned} f(n) &= \frac{n-1}{2} \\ 2f(n) &= n-1 \\ n &= 2f(n)+1 \end{aligned}$$

$$\begin{aligned} f(n) &= -\frac{n}{2} \\ 2f(n) &= -n \\ n &= -2f(n) \end{aligned}$$

Demostración de que f es sobreyectiva:

Sea $b \in \mathbb{Z}$. Si $b \geq 0$, sea $a = 2b+1$, entonces $a \in \mathbb{Z}^+$, a es impar y

$$f(a) = f(2b+1) = \frac{2b+1-1}{2} = \frac{2b}{2} = b$$

Si $b < 0$, sea $a = -2b$, entonces $a \in \mathbb{Z}^+$, a es par y

$$f(a) = f(-2b) = -\frac{-2b}{2} = b$$

$\therefore \forall b \in \mathbb{Z}\ (\exists a \in \mathbb{Z}^+\ (f(a) = b))$

$\therefore f$ es biyectiva

3. Dado $n \in \mathbb{N}$, $n > 1$, se define la relación de equivalencia $\equiv_n$ en $\mathbb{Z}$ como

$$a \equiv_n b \iff (\exists z \in \mathbb{Z})(a = b + nz)$$

y se define el conjunto $\mathbb{Z}_n := \mathbb{Z}/\equiv_n$.

Definiciones equivalentes:

$$a \equiv_n b \iff (\exists z \in \mathbb{Z})(a = b + nz)$$
$$a \equiv_n b \iff a - b \text{ es múltiplo de } n$$
$$a \equiv_n b \iff a \text{ y } b \text{ dan el mismo resto al dividirlos entre } n$$

$a \equiv_n b$ se lee "a es congruente con b módulo n", otra notación que se usa es $a \equiv b \pmod{n}$.

Por ejemplo, si a y b dan el mismo resto al dividirlos entre n entonces existen enteros q_1, q_2 y r tales que:

$$a = q_1 n + r$$

$$b = q_2 n + r$$

Restando la segunda igualdad de la primera:

$$a - b = (q_1 - q_2)n$$

Entonces $a - b$ es múltiplo de n y

$$a = b + n(q_1 - q_2)$$

Nota: en programación se llama módulo a la operación que da el resto de la división entera de un número entre otro. Ver https://en.wikipedia.org/wiki/Modulo_operation

Si las operaciones $+_n$ y $*_n$ estan definidas en $\mathbb{Z}_n$ como

$$[r] +_n [s] = [r + s]$$

$$[r] *_n [s] = [r * s]$$

donde $+$ y $*$ son la suma y multiplicación usual en $\mathbb{Z}$, entonces demuestre las siguientes propiedades para $[r], [s], [t] \in \mathbb{Z}_n$:

a) $[0] +_n [r] = [r]$

b) $[r] +_n [n - r] = [0]$

c) $[r] +_n [s] = [s] +_n [r]$

d) $[r] +_n ([s] +_n [t]) = ([r] +_n [s]) +_n [t]$

e) $[1] *_n [r] = [r]$

f) $[r] *_n [s] = [s] *_n [r]$

g) $[r] *_n ([s] *_n [t]) = ([r] *_n [s]) *_n [t]$

h) $[r] *_n ([s] +_n [t]) = [r] *_n [s] +_n [r] *_n [t]$

Respuestas

Todas estas propiedades, excepto la b), se deducen directamente de las propiedades análogas de la suma y multiplicación usuales en $\mathbb{Z}$:

a)
$$[0] +_n [r] = [0 + r] = [r]$$

b)
$$[r] +_n [n - r] = [r + n - r] = [n]$$

Como $n = 0 + n * 1$ tenemos que $n \equiv_n 0$ y $[n] = [0]$. Por tanto:
$$[r] +_n [n - r] = [0]$$

c)
$$[r] +_n [s] = [r + s] = [s + r] = [s] +_n [r]$$

d)
$$[r]+_n([s]+_n[t]) = [r]+_n[s+t] = [r+(s+t)] = [(r+s)+t)] = ([r+s]+_n[t] = ([r]+_n[s])+_n[t]$$

e)
$$[1] *_n [r] = [1 * r] = [r]$$

f)
$$[r] *_n [s] = [r * s] = [s * r] = [s] *_n [r]$$

g)
$$[r]*_n([s]*_n[t]) = [r]*_n[s*t] = [r*(s*t)] = [(r*s)*t)] = ([r*s]*_n[t] = ([r]*_n[s])*_n[t]$$

h)
$$[r]*_n([s]+_n[t]) = [r]*_n[s+t] = [r*(s+t)] = [r*s+r*t] = [r*s]+_n[r*t] = [r]*_n[s]+_n[r]*_n[t]$$

4. Carlos dijo: "Hoy es domingo, entonces será domingo de nuevo en 7 días
   y en 770 días
   y en 140 días
   y en 35035 días
   y en 14000000007 días."
   Isabel dijo: "y será martes en 2 días...
   y en 72 días
   y en 702 días
   y en 779 días
   y en 14777002 días."

¿Estás de acuerdo con todo lo que dijeron Carlos e Isabel? ¿Por qué?

Respuestas

Sí.

Los números de Carlos son múltiplos de 7 (son 0 módulo 7).

Los de Isabel son (múltiplos of 7) + 2 (son 2 módulo 7).

5. Si hoy es domingo

   ¿qué día de la semana será en 15 días?

   ¿En 26 días?

   ¿En 234 días?

   ¿En 1000 días?

   Respuestas

   Como hay 7 días en una semana, necesitamos encontrar los restos de 15, 26, 234 y 1000 al dividirlos entre 7. Como no necesitamos el cociente no necesitamos realizar la división. Podemos encontrar los restos de esta manera:

   En 15=14+1 días será lunes.

   En 26=21+5 días será viernes.

   En 234=210+24=210+21+3 días será miércoles.

   En 1000=700+300=700+280+20=700+280+14+6 días será sábado.

6. Actualmente en el hemisferio sur es invierno, ¿qué estación será allá en 100 estaciones?

   Respuesta

   Invierno pues hay cuatro estaciones y 100 es un múltiplo of 4.

7. Si ahora es las 8 pm, ¿qué hora será en 500 horas?

   Respuesta

   Como hay 24 horas en el día, necesitamos encontrar el resto de 500 al dividirlo entre 24.

   Nuevamente como no necesitamos el cociente no necesitamos realizar la división.

   Podemos encontrar el resto de esta manera:

   500 = 480 + 20

   Por lo tanto el resto es 20 y

   8 pm + 20 horas = 4 pm

   También pueden pensar que $20 \equiv_{24} -4$, restarle 4 a 8 pm y da 4pm.

8. Ahora estamos en el mes de julio, ¿qué mes será en 500 meses?

   Respuesta

   Como hay 12 meses en el año, hay que calcular el resto de 500 al dividirlo entre 12:

   500 = 480 + 20 = 480 + 12 + 8

   Basta sumar 8 meses.

   Julio es el mes 7

   7 + 8 = 15

   $15 \equiv_{12} 3$

   La respuesta es marzo.

9. ¿Cuáles de las siguientes congruencias son verdaderas?

   a) $177 \equiv_2 17$

   b) $181 \equiv_3 432$

   c) $1322 \equiv_{12} 5294$

   Respuestas

   a) Sí, ambos son pares.

   b) Recordemos que para todo $n \in \mathbb{N}$:

   $n \equiv_3$ suma de los dígitos de n

   Sumado los dígitos 1+8+1=10 vemos que 181 da resto 2 al dividirlo entre 3.

   Sumado los dígitos 4+3+2=9 vemos que 432 da resto 0 al dividirlo entre 3.

   Entonces 181 y 432 no son congruentes módulo 3.

   c) $5294 - 1322 = 3972$

   $3972 = 3600 + 360 + 12$

   Dado que $3600 \equiv_{12} 360 \equiv_{12} 12 \equiv_{12} 0$ tenemos:

   $3972 \equiv_{12} 0$

   Por tanto $1322 \equiv_{12} 5294$

10. ¿Cuáles son las tablas de sumar y multiplicar módulo 4 y módulo 7? Cuando trabajamos módulo n reemplazamos los números por sus restos módulo n: $0, 1, 2, \ldots, n-1$. Formalmente: esos son los elementos representantes de las clases de equivalencia $[0], [1], [2], \ldots, [n-1]$. Por ejemplo, en las tablas módulo 4 no deben tener el número 4, lo deben reemplazar por 0.

    Respuestas

Tabla de sumar módulo 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla de multiplicar módulo 4

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla de sumar módulo 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabla de multiplicar módulo 7

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

11. Dado que la tabla de multiplicar módulo 10 es:

x	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

¿Cuáles de los siguientes números son cuadrados de números naturales?

a) 6312

b) 4553

c) 9538

Respuesta

Ninguno. Viendo en la tabla los números en la diagonal que va de la esquina superior izquierda a la esquina inferior derecha, vemos que los números cuadrados sólo pueden tener 0, 1, 4, 5, 6 o 9 como último dígito. Los números dados no terminan en ninguno de esos dígitos.

12. ¿Cuál es el último dígito de los siguientes números?

a) 12345^3

b) 250^{13}

c) 4^{51}

d) 9^{57}

e) 9^{72}

f) 32^{10}

Respuestas

a) 5, como el último dígito es 5 todas sus potencias tienen 5 en el último dígito.

b) 0, como el último dígito es 0 todas sus potencias tienen 0 en el último dígito.

c) 4 (51 es impar, sería 6 para una potencia par)

d) 9 (57 es impar)

e) 1 (72 es par)

f) Es suficiente mirar el último dígito de 32: 2.
Para $n > 0$, el último dígito de 2^n es:
2 si $n \equiv_4 1$
4 si $n \equiv_4 2$
8 si $n \equiv_4 3$
6 si $n \equiv_4 0$
$10 \equiv_4 2$, por lo tanto la respuesta es 4.