Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC1253 — Matemáticas Discretas — 1' 2017

PAUTA INTERROGACION 3

Pregunta 1

La solución consistía en demostrar el ejercicio visto en clases, sobre poder representar cualquier número natural mayor a 0 en representación en base $b > 1$ y es única. Consideramos realizarlo por induccion sobre $n > 0$, la propiedad "n se puede tiene una representacion en base b y es unica", asi mostramos ambas propiedades al mismo tiempo. Se muestra el caso base con representacion trivial y argumentar por que es la unica. Luego, asumiendo que se cumple para todo $n' < n$, falta demostrarlo para n. Notamos que por teorema del resto se puede establecer que $n = qb + r$ con q y r unicos y $0 \leq r < b$. Es imporante notar (y por lo tanto, explicar) por que $q < n$ (por contradiccion por ejemplo). Luego es posible aplicar la hipotesis de induccion sobre q y por lo tanto incluyendo r se obtiene una representacion valida para n. Ademas, por hipotesis de induccion, la representacion de q es unica, y por lo tanto, tambien la de n.

Dado lo anterior, el puntaje asignado es el siguiente:

- **(1 punto)** Por mostrar el caso base $n = 1$.
- **(1 puntos)** Por relacionar el teorema del resto sobre n con unicos q, r.
- **(1 punto)** Por explicar por que q debe ser menor que n, (ya que teorema solo establece que es entero) y luego aplicar hipotesis de induccion sobre q.
- **(1 puntos)** Utilizando lo anterior, establecer los coeficientes de la representacion par n en base a los de q y r.
- **(2 puntos)** Se otorgan por incluir unicidad en la induccion o una explicacion aparte.

Otras demostraciones se admitieron, como por ejemplo por construccion o aplicando teorema del resto utilizando b^{k-1}, para un k apropiado, y aplicando hipotesis sobre r. En este caso el corrector aplica segun su criterio el puntaje.

Pregunta 2

Pregunta 2.1

La solución consistía en realizar inducción estructural. En primer lugar se debía poner atención en ser claro con la estructura de la inducción. La demostración en sí era sencilla, utilizando correctamente la hipótesis inductiva y las reglas recursivas de P_Σ (en particular, la tercera), la demostración salía fácilmente.

Dado lo anterior, el puntaje asignado es el siguiente:

- **(1 punto)** Por reconocer y mostrar correctamente los casos bases.
- **(2 puntos)** Por establecer y hacer uso de la hipótesis inductiva y luego, conectar esta con la formación de una nueva palabra del tipo $a \cdot w \cdot a$ con $a \in \Sigma$ y w en la capa anterior.

Pregunta 2.2

La solución consistía en hacer inducción sobre el largo de la palabra. La dificultad estaba en usar una buena estructura para la inducción y luego reconocer y justificar la forma que debe tener la palabra para que sea igual a su reversa.
Dado lo anterior, el puntaje asignado es el siguiente:

- **(1 punto)** Por reconocer y mostrar correctamente los casos bases.
- **(2 puntos)** Por establecer correctamente la hipótesis inductiva, reconocer la forma de las palabras que son iguales a su reversa (justificar) y concluir utilizando lo anterior.

Pregunta 3

Se debe demostrar que $\log(n!) \in \mathcal{O}(n\log(n))$ y $n\log(n) \in \mathcal{O}(\log(n!))$. Cada una de las partes valía 3 puntos.

Para la primera parte $\log(n!) \in \mathcal{O}(n\log(n))$ basta notar que:

$$\begin{aligned} n! &= 1 \cdot 2 \cdot \ldots \cdot n \\ &\leq n \cdot n \cdot \ldots \cdot n \\ &= n^n \end{aligned}$$

Luego aplicando logaritmo se obtiene lo pedido con $c = 1$ y $n_0 = 1$.
Dado lo anterior, el puntaje asignado es el siguiente:

- **(1 punto)** Por mostrar que $n! < n^n$.
- **(1 punto)** Por aplicar logaritmo.
- **(1 punto)** Por concluir lo pedido explicitando c y n_0 .

Para la segunda parte $n\log(n) \in \mathcal{O}(\log(n!))$ usando la fórmula de Stirling y aplicando logaritmo obtenemos:

$$\exists c \exists n_0 . \forall n \geq n_0 .\ \log(c\sqrt{2\pi n\left(\frac{n}{e}\right)^n}) \leq \log(n!)$$

Usando propiedades del logaritmo y quitando términos positivos al lado izquierdo obtenemos:

$$\log(n^n) - \log(e^n) \leq \log(n!)$$

Ahora usando que $e^n \in \mathcal{O}(n!)$, podemos llegar a que $\log(e^n) \leq 2\log(n!)$ para algún n_0. Reemplazando en la expresión anterior llegamos a lo buscado:

$$n\log(n) \leq 3\log(n!)$$

Luego con $c = 3$ y n_0 el máximo de los n_0 utilizados en la demostración se tiene que $n\log(n) \in \mathcal{O}(\log(n!))$.
Dado lo anterior, el puntaje asignado es el siguiente:

- **(0.5 puntos)** Por usar correctamente el hint.
- **(0.5 puntos)** Por aplicar logaritmo correctamente.
- **(1.5 puntos)** Por reducir la expresión para poder concluir lo pedido.
- **(0.5 puntos)** Por definir correctamente c y n_0.

Pregunta 4

Pregunta 4.1

Una posible solución es la siguiente. Primero que todo había que demostrar que todo divisor que divide a m y a a al mismo tiempo también divide a b, con lo cual el $gcd(a, m)$ divide a b. Lo anterior no es suficiente, ya que todavía podría existir un valor que divide a b y a m al mismo tiempo que sea mayor que $gcd(a, m)$, por eso también había que demostrar que todos los divisores que dividen al mismo tiempo a b y a m también dividen a a. Esta última demostración junto con la anterior concluyen que los divisores comunes entre a y m son los mismos que entre b y m lo que implica que $gcd(a, m) = gcd(b, m)$.

En forma algebraica es de la siguiente manera. Como tenemos lo siguiente:

$$a \equiv b \mod m$$

Ocurre lo siguiente:

$$mk = a - b$$

Luego si usamos c como cualquier divisor común entre a y m:

$$cpk = cq - b$$

Reordenando:

$$b = c(q - pk)$$

Como c y $(q - pk)$ son enteros entonces c divide a b, para todo c que divide a a y a m al mismo tiempo. Podemos escribir loo siguiente:

$$\{c \mid c/a \wedge c/m\} \subseteq \{d \mid d/b \wedge d/m\}$$

Otra forma de verlo es tomando c como $gcd(a, m)$, lo que implica que $gcd(a, m)/b$, entonces $gcd(a, m) \leq gcd(b, m)$. Ahora solo faltaría demostrar que los conjuntos de divisores comunes son iguales o que los máximos común divisor son iguales. Lo único que hay que hacer un procedimiento análogo al anterior con un c que divida a b y a m al mismo tiempo, para concluir que también divide a a:

$$cpk = a - cq$$

Reordenando:

$$a = c(pk + q)$$

Entonces, dado esto y con lo demostrado anteriormente se llega a que:

$$\{c \mid c/a \wedge c/m\} = \{d \mid d/b \wedge d/m\}$$

Si se hubiera asumido que c es el $gcd(b, m)$, entonces se llegaría a que $gcd(b, m)/a$, lo que implica que $gcd(b, m) \leq gcd(a, m)$, pero tomando lo demostrado anteriomente se concluye que no queda otra más que $gcd(b, m) = gcd(a, m)$. Con lo que queda demostrado.

Otra forma mucho más simple es la siguiente. Tenemos como hipótesis que:

$$a \mod m \;=\; b \mod m$$

Luego por propiedad vista en clases, la cual proviene del algoritmo de euclides:

$$gcd(a, m) = gcd(m, a \mod m)$$

Luego usando la hipotesis:

$$gcd(m, a \mod m) = gcd(m, b \mod m)$$

Finalmente reusando la propiedad mencionada:

$$gcd(m, b \text{ mód } m) = gcd(b, m)$$

Con lo que queda demostrado.

Dado lo anterior, el puntaje asignado es el siguiente:

- **(2 puntos)** Por demostrar que $\{c \mid c/a \wedge c/m\} \subseteq \{d \mid d/b \wedge d/m\}$ o que $gcd(a, m) \leq gcd(b, m)$ que para efectos de este problema tienen la misma importancia y dificultad.
- **(1 punto)** Por demostrar el otro lado, es decir, que $\{c \mid c/a \wedge c/m\} = \{d \mid d/b \wedge d/m\}$ o que $gcd(a, m) = gcd(b, m)$

  Con esta base de asignación, el puntaje puede variar dependiendo de que tan preciso y acertado fue en la descripción de cada paso y que tan acertado fue en las conclusiones de su desarrollo.

Pregunta 2.2

Una posible solución es la siguiente. Si consideramos que $gcd(c, m) = g$, entonces podemos establecer lo siguiente:

$$c = gs$$

$$m = gt$$

Luego usando la hipótesis y reemplazando lo anterior, tenemos que:

$$asg - bsg = ktg$$

Simplificando:

$$as - bs = qt$$

Lo que nos dice que:

$$as \equiv bs \mod t$$

Luego solo faltaría simplificar el s, pero no se puede hacer así de simple, ya que debe tener inverso multiplicativo en módulo t, lo que hay que demostrar algebraicamente o con palabras. La siguiente es la forma algebraica. Sabemos, usando los mismos símbolos anteriores, que se cumple lo siguiente para algun p y q enteros:

$$pc + qm = g$$

Luego reemplazando:

$$psg + qtg = g$$

Simplificando:

$$ps + qt = 1$$

Entonces se concluye que s y t son primos relativos, lo que implica que s tiene inverso en módulo t. También se podía argumentar que s y t son primos relativos porque corresponden a todos los factores no comunes entre c y m, por lo que s y t no podían tener ningun factor primo en común, lo que los hace primos relativos. Ahora dado lo anterior podemos decir que:

$$a \equiv b \mod t$$

con $t = \frac{m}{gcd(m,c)}$.

Dado lo anterior, el puntaje asignado es el siguiente:

- **(1.5 puntos)** Por llegar a que $as \equiv bs \mod t$.
- **(1.5 puntos)** Por mostrar o demostrar correctamente que s y t son primos relativos y por lo tanto $a \equiv b \mod t$.

Cabe recalcar que muy pocos hicieron exactamente esta demostración y la asignación de puntaje fue acorde a desarrollos equivalentes en proximidad al resultado final y en la dificultad de lo demostrado.