NOMBRE: Luis Felipe Silva De Vidts NOTA:

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

IIC1253 — Matemáticas Discretas

Tarea 7 – Respuesta Pregunta 1

Pregunta 1

Demuestre o de un contra ejemplo para las siguientes afirmaciones:

1. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ con $a, b, c, d, m \in \mathbb{Z}$ y $m \geq 2$, entonces $(a - c) \equiv (b - d) \pmod{m}$.

   Para demostrar esto probaremos que

   $$(a-c) \mod m = (b-d) \mod m$$

   entonces tenemos que el modulo distibuye sobre la suma, por lo tanto se cumple que

   $$(a-c) \mod m = (a \mod m - c \mod m) \mod m$$

   por enunciado $a \mod m = b \mod m$ y $c \mod m = d \mod m$, por lo que nos queda:

   $$(a-c) \mod m = (b \mod m - d \mod m) \mod m$$

   ahora aplicamos distributividad del modulo, entonces nos queda

   $$(a-c) \mod m = (b-d) \mod m$$

   Por lo tanto

   $$(a-c) \equiv (b-d) \mod m$$

2. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ con $a, b, c, d, m \in \mathbb{Z}$, $m \geq 2$ y $c, d \geq 0$, entonces $a^c \equiv b^d \pmod{m}$.

   Para este caso tomamos el contra-ejemplo en que $m = 7$, $a = 2$, $b = 9$, $c = 4$ y $d = 11$, donde se cumple

   $$(2 \mod 7) = (9 \mod 7) = 2$$

   $$(4 \mod 7) = (11 \mod 7) = 4$$

   luego tenemos que

   $$(2^4 \mod 7) = (16 \mod 7) = 2 \neq 4 = (31381059609 \mod 7) = (9^{11} \mod 7)$$

   Por lo que no se cumple $a^c \equiv b^d \mod m$

NOMBRE: Luis Felipe Silva De Vidts NOTA:

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC1253 — Matemáticas Discretas

Tarea 7 – Respuesta Pregunta 2

Pregunta 2

Una expansión factorial de un número n es una sumatoria de la forma:

$$n = a_k \cdot k! + a_{k-1} \cdot (k-1)! + \ldots + a_2 \cdot 2! + a_1 \cdot 1! = \sum_{i=1}^{k} a_i \cdot i!$$

tal que $a_i \in \mathbb{N}$, $0 \leq a_i \leq i$ para $i = 1, \ldots, k$ y $a_k \neq 0$.

1. Demuestre que todo número entero $n \geq 1$ se puede escribir en alguna expansión factorial.

   Primero tenemos que para $n = 1$ se cumple que tiene una expansión factorial

   $$1 = 1 \cdot 1!$$

   ### Lema

   Antes de probar para el caso general, probaremos que $\sum_{i=1}^{k} i \cdot i!$ tiene como sucesor a $(k+1)!$

   Primero evaluamos el caso base $k = 1$ se tiene

   $$2! = 1 \cdot 1! + 1 = 1 + 1 = 2 = 2!$$

   Ahora para el caso general probamos que se cumple para $k+1$ suponiendo que se cumple para todos los valores anteriores a $k+1$

   $$(k+1)! = (k+1) \cdot k! = k \cdot k! + k!$$

   como $k < k+1$ entonces se cumple la hipotesis y podemos reescribir lo anterior como

   $$(k+1)! = k \cdot k! + \sum_{i=1}^{k-1} i \cdot i! + 1 = \sum_{i=1}^{k} i \cdot i! + 1$$

   Por lo tanto por inducción fuerte, $(k+1)!$ es el sucesor de $\sum_{i=1}^{k} i \cdot i!$ para todo k natural.

Colorario

Un colorario de lo anterior es que

$$k! > \sum_{i=1}^{k-1} i \cdot i! > \sum_{i=1}^{k-1} a_i \cdot i!$$

con $0 \leq a_i \leq i$.

Ahora probamos que $n+1$ tiene una expansión factorial dado que todos los valores anteriores tienen una descomposición factorial, $n < n+1$ por lo que tendrá una expansión factorial

$$n+1 = \sum_{i=1}^{k} a_i \cdot i! + 1$$

notamos que el valor máximo que puede tomar n es cuando $a_i = i$ para todo i, y sigue cumpliendo que tiene una expansion factorial, cualquier otra forma de escribir n sería menor a esta forma y por hipotesis inductiva, tendría una expansión factorial. Entonces podemos cambiar la igualdad anterior y nos quedará

$$n+1 = \sum_{i=1}^{k} i \cdot i! + 1 = (k+1)!$$

por el lema anterior, por lo que $n+1$ tiene una expansión factorial, lo que significa que por inducción fuerte, todo número natural tiene una expansión factorial.

2. Demuestre que todo número entero $n \geq 1$ tiene una única expansión factorial.

Para esto suponemos que existen dos expansiones para un mismo número n

$$n = \sum_{i=1}^{k} a_i \cdot i! = a_k \cdot k! + \sum_{i=1}^{k-1} a_i \cdot i! = a_k \cdot k! + r_a$$

$$n = \sum_{i=1}^{k} b_i \cdot i! = b_k \cdot k! + \sum_{i=1}^{k-1} b_i \cdot i! = b_k \cdot k! + r_b$$

Lo que es equivalente a la división con resto de n en $k!$, ya que r_a y r_b son menores que $k!$ por el colorario anterior y $k! \leq n$, ya que n tiene expansión factorial, y como sabemos esta expresión nos da valores únicos de resto y parte entera, por lo tanto $a_k = b_k$ y $r_a = r_b$, pero eso es una contradicción, ya que los supusimos distintos, por lo tanto la expansión factorial es única.