Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Ayudantía 11

3 de julio de 2020

Profesores C. Riveros - J. Salas

Tamara Cucumides y Bernardo Barías

Video de la ayudantia:
`https://drive.google.com/file/d/1xr9nUigHJkzskOBRiz4XkVi5GrC26lyf/view?usp=sharing`

Pregunta 1 - Complejidad algoritmo de Euclides

Recuerde el algoritmo de Euclides visto en clases.

Input : Números a, b con $a \geq b \geq 0$
Output: $\gcd(a, b)$
$x \leftarrow a$
$y \leftarrow b$
while $y \neq 0$ **do**
  $r \leftarrow x \pmod{y}$
  $x \leftarrow y$
  $y \leftarrow r$
return x

Demuestre que el tiempo del algoritmo es $\mathcal{O}(\log(b))$

Hint: Demuestre y use el siguiente resultado (Lema de Fibonacci).
Para $n \geq 3$ se cumple que

$$f_n > \left(\frac{1+\sqrt{5}}{2}\right)^{n-2}$$

con $f_0 = 0$, $f_1 = 1$ y $f_n = f_{n-1} + f_{n-2}$

Pregunta 2 - Pequeño teorema de Fermat

Teorema 1 *Sea p un número primo y $a \in \mathbb{Z}$ tal que p no divide a. Luego*

$$a^p \equiv a \pmod{p}$$

Demuestre el teorema.

Pregunta 3

1. Para $m > 1$ demuestre que si $a \equiv b \pmod{m}$, entonces $\gcd(a, m) = \gcd(b, m)$
2. Para $m > 1$ demuestre que si $ac \equiv bc \pmod{m}$, entonces $a \equiv b \pmod{\frac{m}{\gcd(m,c)}}$