UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exáctas y Naturales
Departamento de Matemáticas

ÁLGEBRA I

Este es un modesto aporte para los alumnos de la fácultad de Ciencias Exactas y Naturales de la UBA de las carreras de licenciatura en Matemática y Computación. De ninguna manéra pretende ser una guía de estudio, ni remplaza las clases presenciales, el material oficial de la catedra esta disponible en el web site de la máteria.
http://cms.dm.uba.ar/

Autor: Isaac Edgar Camacho Ocampo
Carrera: Licenciatura en Ciencias de la Computación

Buenos Aires, 2020

Si se encuentra algún error u omisión en este resúmen por favor colaborar en
`https://github.com/IsaacEdgarCamacho/Apuntes/tree/master/Algebra/`
o escribirme a
`isaac.edgar.camacho@gmail.com`

Índice general

Índice general

Capítulo 1

Introducción

1.1. Conocimientos previos

1.2. Estado del arte

Capítulo 2

Conjuntos, Relaciones y Funciones.

2.1. Conjuntos.

2.1.1. Conjuntos y subconjuntos, pertenencia e inclusión.

Definición 1.1.1. (informal de conjunto y elementos.)

Un conjunto es una colección de objetos, llamados elementos, que tiene la propiedad que dado un objeto cualquiera, se puede decidir si ese objeto es un elemento del conjunto o no.

Ejemplos:

- $A = \{1, 2, 3\}, \quad B = \{\triangle, \square, \lozenge\}, \quad C = \{1, \{1\}, \{2, 3\}\}.$
- $N = \{1, 2, 3, 4, \ldots\}$ el conjunto de los números naturales.

2.1.2. Operaciones entre conjuntos

Teorema :si un conjunto A esta incluido en otro conjunto B, entonces el complemento de B esta incluido en el complemento de A

$$A \subseteq B \Rightarrow B^c \subseteq A^c$$

Demostracion:

$$Hitpotesis: \quad A \subseteq B \longleftrightarrow \quad \forall x \epsilon A \Rightarrow x \epsilon B$$

$$\equiv \quad def(a) \wedge def(i) \wedge \ (0 \leq i < |a|) \wedge (0 \leq i + 1 < |a|) \quad \wedge_L \ True$$

$$wp(S,\ Post) \equiv \quad (0 \leq i < |a|) \wedge (0 \leq i + 1 < |a|)$$

$$
\begin{aligned}
wp(S,\ Post) \ &\equiv\ wp(\ result := a[i] + a[i+1]\ ,\ Post^{result}_{a[i]+a[i+1]}\ ) \\
&\equiv\ def(a[i] + a[i+1]) \quad \wedge_L \quad \underbrace{a[i] + a[i+1] = a[i] + a[i+1]}_{\text{es siempre True}} \\
&\equiv\ def(a) \wedge def(i) \wedge\ (0 \leq i < |a|) \wedge (0 \leq i+1 < |a|) \quad \wedge_L\ True
\end{aligned}
$$

$$
wp(S,\ Post) \ \equiv\ (0 \leq i < |a|) \wedge (0 \leq i+1 < |a|)
$$

El Teorema de Pitágoras lleva este nombre porque su descubrimiento recae sobre la escuela pitagórica. (Fuente: Wikipedia)

Ejercicio: Probar usando el principio de inducción que 7 divide a $15^n + 7$ para todo $n \in \mathbb{N}$

$$
7 \mid (15^n + 7) \ \equiv\ wp(\ result := a[i] + a[i+1]\ ,\ Post^{result}_{a[i]+a[i+1]}\ )
$$

Ejercicio: Probar usando el principio de inducción que 7 divide a $15^n + 7$ para todo $n \in \mathbb{N}$

$$
\begin{aligned}
&\equiv\ def(a[i] + a[i+1]) \quad \wedge_L \quad \underbrace{a[i] + a[i+1] = a[i] + a[i+1]}_{\text{es siempre True}} \\
&\equiv\ def(a) \wedge def(i) \wedge\ (0 \leq i < |a|) \wedge (0 \leq i+1 < |a|) \quad \wedge_L\ True
\end{aligned}
$$

$$
wp(S,\ Post) \ \equiv\ (0 \leq i < |a|) \wedge (0 \leq i+1 < |a|)
$$

2.2. Ejercicios

Ejercicio: Probar usando el principio de inducción que 7 divide a $15^n + 7$ para todo $n \in \mathbb{N}$

Capítulo 3

Divisibilidad.

Divisibilidad Cuando hablamos de divisibilidad en el conjunto de los números enteros nos referimos a la división entera podemos señalar que tanto la suma el producto y la resta son operaciones cerradas dentro del conjunto de los enteros es decir como resultado obtenemos otro entero pero no ocurre esto en el caso de la división excepto para algunos casos

Dados a y b enteros diremos que a divide a b si podemos escribir a a como múltiplo de b

3.1. Cociente y resto

Cuando somos chicos aprendemos que 6 “cabe” cuatro veces en 27 y el resto es 3, o sea

$$27 = 6 \cdot 4 + 3.$$

Un punto importante es que el resto debe ser menor que 6. Aunque, también es verdadero que, por ejemplo

$$27 = 6 \cdot 3 + 9$$

debemos tomar el menor valor para el resto, de forma que “lo que queda” sea la más chico posible.

3.1.1. Suposiciones

3.1.2. Modelos

3.2. Resultados preliminares

3.3. Resultados postprocesados

3.3.1. Valores atípicos

3.3.2. Correlaciones

Capítulo 4

Conclusiones

Ejercicio: Probar usando el principio de inducción que 7 divide a $15^n + 6$ para todo $n \in \mathbb{N}_0$

Cuando trabajamos con inducción debemos definir cual es la afirmacion que vale para cada n y no se pone para todo n, porque eso es lo que queremos probar.

$$P(n) : 7 \mid 15^n + 6$$

Caso base $P(0) : n = 0$ Queremos ver si el primer numero del conjunto cumpler P(n)

$$(n = 0) \Rightarrow 7 \; divide \; a \; (15^0 + 6)$$

$$15^0 + 6 = 7, \; 7 = 1 \cdot 7 \; \Rightarrow 7 \mid 7$$

Por lo tanto la afirmación para $P(0)$ es verdadera ya que 7 divide a 7.

Paso inductivo Suponemos que $P(n)$ es verdadera y probamos la veracidad de $P(n + 1)$

$$\text{Hipótesis Inductíva} \; (HI) \equiv \; (15^n + 6 = k \cdot 7), \; con \; k \in \mathbb{Z}$$

Lo que queremos hacer es que suponiendo que $P(n)$ es verdad probamos la verdad de $P(n+1)$

$$\begin{aligned}
15^{n+1} + 6 &\equiv 15^{n+1} + 6 \\
&\equiv 15^n \cdot 15 + 6 \\
&\equiv 15^n \cdot (1 + 14) + 6 \\
&\equiv 15^n \cdot 1 + 15^n \cdot 14 + 6 \\
&\equiv (15^n \cdot 1 + 6) + 15^n \cdot 14 \\
HI &\equiv k \cdot 7 + 15^n \cdot 14 \\
&\equiv k \cdot 7 + 15^n \cdot (2 \cdot 7) \\
15^{n+1} + 6 &\equiv 7 \cdot \underbrace{(k + 15^n \cdot 2)}_{esto \; \in \mathbb{Z}}
\end{aligned}$$

Podemos ver que $15^{n+1} + 6$ se expresa como multiplo de 7, por lo tanto queda demostrado nuestro ejercicio

Ejercicio: Probar usando el principio de inducción que 10 divide a $16^n - 6^n$ para todo $n \in \mathbb{N}$

$$10 \mid 16^n - 6^n \quad \forall n \in \mathbb{Z}$$

$$\begin{array}{rcl}
\textbf{Caso Base P(1)} & & n = 1 \\
16^1 - 6^1 & \equiv & 16 - 6 = 10 \\
 & \equiv & 10 = 1 \cdot 10 \quad \text{(con esto vemos que cumple)}
\end{array}$$

$$\begin{array}{rcl}
\textbf{Paso inductivo P(n)} & & P(n) \text{ es verdad y pruebo para } P(n+1) \\
\text{Hipótesis inductiva} & \Rightarrow & (16^n - 6^n = k \cdot 10) \text{ con } k \in \mathbb{Z}
\end{array}$$

$$\begin{array}{rcl}
16^{n+1} - 6^{n+1} & \equiv & 16^n \cdot 16 - 6^n \cdot 6 \\
 & \equiv & 16^n \cdot (6 + 10) - 6^n \cdot 6 \\
 & \equiv & (16^n \cdot 6 + 16^n \cdot 10) - 6^n \cdot 6 \\
 & \equiv & 16^n \cdot 6 - 6^n \cdot 6 + 16^n \cdot 10 \\
 & \equiv & 6 \cdot \underbrace{(16^n - 6^n)}_{HI} + 16^n \cdot 10 \\
HI & \equiv & 6 \cdot k \cdot 10 + 16^n \cdot 10 \\
16^{n+1} - 6^{n+1} & \equiv & 10 \cdot (\underbrace{k \cdot 6 + 16^n}_{esto\ \in \mathbb{Z}})
\end{array}$$

Podemos ver que $16^{n+1} - 6^{n+1}$ se expresa como multiplo de 10, por lo tanto queda demostrado nuestro ejercicio

Capítulo 5

Congruencia

De manera informal dos números $a, b \in \mathbb{Z}$ son congruentes cuando tienen el mismo resto al dividirlo por un tercero m que vamos a llamar módulo.

$$a \equiv b(m) \quad \Leftrightarrow \quad r_m(a) = r_m(b) \quad \Leftrightarrow \quad m|(a-b)$$

es equivalente decir que la resta de esos dos números que llamamos congruentes es un múltiplo de ese tercer número que llamamos módulo