Bases matemáticas de la criptografía de clave asimétrica: la aritmética modular y la clave RSA

Barco G., Carlos*

Resumen

El presente artículo tiene un propósito didáctico, a saber, mostrar los fundamentos matemáticos de la criptografía en lo que se refiere a la aritmética modular y sus aplicaciones: por un lado, el cálculo del dígito de verificación en los números de identificación; y por el otro, la aritmética modular aplicada a la criptografía de clave pública RSA. Para lograr este propósito, se desarrollarán los siguientes temas: relaciones de congruencia módulo **n**, aritmética modular y propiedades de las congruencias módulo **n** y las aplicaciones ya mencionadas.

Palabras clave: criptografía, asimétrica, RSA, clave pública, aritmética modular.

Mathematical bases of cryptography of the asymmetric key: modular arithmetic and the RSA key

Abstract

The didactic purpose of this paper is centered on showing the mathematical foundations of cryptography, in regards to modular arithmetic and its applications. On one side, the calculation of the verification digit in identification numbers, and on the other side, modular arithmetic applied to the public key RSA cryptography. To achieve said purpose, the following subjects will be developed: congruence n-modular relations, modular arithmetic and the properties of n-modular relations and the above-mentioned applications.

Key words: cryptography, asymmetric, RSA, public clue, modular arithmetic.

* Departamento de Matemática, Universidad de Caldas. AA275 Manizales, Colombia. e-mail: carlosbarco@ucaldas.edu.co

Vector, Volumen 2, Enero - Diciembre 2007, págs 59 - 69
Recibido 12 Septiembre 2007, Aprobado 16 Noviembre 2007

Relaciones de congruencia módulo n.

Sea **Z** el conjunto de números enteros y **R** la relación sobre **Z** definida por la siguiente expresión:

$$\mathbf{R} = \{(x, y) \in \mathbf{X} \times \mathbf{X} / x - y \text{ es múltiplo de } 2\}$$

La relación entre x *y* y, x **R** y se escribe con el símbolo:

$$x \equiv y \pmod 2$$

Que se lee "x es congruente con y módulo 2". La relación así definida es una relación de equivalencia sobre el conjunto de los números enteros porque:

a) Para todo $x \in X$, se cumple que $x \equiv x \pmod 2$, ya que $a - a = 0 = 2 \times 0$ que es múltiplo de 2 y por tanto, la relación es reflexiva.
b) Sea $x \equiv y \pmod 2$, entonces $x - y = 2k$, $\forall k \in Z$, entonces, $y - x = 2(-k)$ y por lo tanto, $y - x$ también es un múltiplo de 2, es decir: $y \equiv x \pmod 2$ y por tanto, la relación es simétrica.
c) Si $x \equiv y \pmod 2$ *y* $y \equiv z \pmod 2$, entonces:

$$x - y = 2k_1$$
$$y - z = 2k_2$$

Donde k_1 y k_2 son números enteros. Sumando miembro a miembro las dos ecuaciones anteriores se obtiene: $x - z = 2(k_1 + k_2)$, lo que significa que $x \equiv z \pmod 2$ y por tanto, $x \equiv y \pmod 2 \wedge y \equiv z \pmod 2$, entonces, $x \equiv z \pmod 2$ y la relación es transitiva.

Esta relación de congruencia módulo 2 determina una partición del conjunto de los enteros **Z** en dos clases de equivalencia: la clase de equivalencia con representante cero (0), la clase del Cl (0), o también [0] constituida por los números cuya diferencia sea par (los números pares) y la clase de equivalencia con representante uno (1), la clase del uno Cl (1), o también [1] constituida por los números impares, simbólicamente se expresa:

$$Cl\ (0) = [0] = \{x \in Z / (x, 0) \in R\}$$
donde R: $= x - 0 = 2k$ (pares)
$$Cl\ (1) = [1] = \{x \in Z / (x, 1) \in R\}$$
donde R: $= x - 1 = 2k$ (impares)

El conjunto cociente de los enteros por la relación **Z** / **R** tiene dos elementos: la clase de los pares y la clase de los impares.

La partición o conjunto cociente se escribe:

$$\mathbf{Z} / \mathbf{R} = \{[0], [1]\}$$

La relación de congruencia módulo 3 se puede definir de la siguiente forma: dado un elemento $x \in \mathbf{Z}$, se determina una partición de números enteros así:

[0] = {x ∈ **Z** /xI3 tiene residuo 0}
[1] = {x ∈ **Z** /x I3 tiene residuo 1}
[2] = {x ∈ **Z** /x I 3 tiene residuo 2}

El conjunto cociente o partición de los enteros por la relación de congruencia módulo 3 es:

$$\mathbf{Z} / \mathbf{R} = \{[0], [1], [2]\}$$

Lo anterior se cumple cualquiera que sea n ∈ **N**, si **Z** es el conjunto de números enteros, en general la relación **R** de congruencia módulo n se puede escribir:

$$\mathbf{R} = \{(x, y) \in \mathbf{Z}^2 / x - y \text{ es múltiplo de } n\}$$

y la relación x **R** y se escribe:

$$x \equiv y \pmod{n}$$

Aritmética modular

Dos números a y b son congruentes módulo m, cuando los residuos de su división por el número m son iguales.

Simbólicamente:

$$a \equiv b \pmod{m}$$

que se lee: "a es congruente con b, módulo m"

De la definición anterior se derivan las dos consecuencias siguientes:

1) Si r es el residuo de la división de a por b se tiene la relación de congruencia

$$a \equiv r \pmod{b}$$

2) Si a es divisible por b, el residuo es cero y por tanto, la divisibilidad de a por b se escribe:

$$a \equiv 0 \pmod{b}$$

Propiedades de las congruencias del mismo módulo.

Estas propiedades son las consecuencias inmediatas de las igualdades de la división:

1) Dos números congruentes con un tercero, respecto de un mismo módulo, son congruentes entre si respecto de dicho módulo.

$$\text{Si } a \equiv b \pmod{d} \wedge b \equiv c \pmod{d},$$
$$\text{Entonces, } a \equiv c \pmod{d}$$

Demostración

a- b = Km.
a- c = k'm restando miembro a miembro se obtiene:
-b-(-c) = km-k'm
c – b = (k-k') m
∴cLb (mod m)

2) Sumando miembro a miembro dos congruencias, respecto del mismo módulo, resulta otra congruencia respecto de ese mismo módulo.

$$\text{Si } a \equiv b \pmod{m} \wedge c \equiv d \pmod{m},$$
$$\text{Entonces, } a + c \text{ L } b + d \pmod{m}$$

Demostración

a- b = km
a- c = k'm sumando miembro a miembro se obtiene:
(a-b)+(c-d) = (k+k') m
(a+c)- (b+d) = (k+k') m
∴ (a+b) L (b+d) (mod m)

3) Restando miembro a miembro dos congruencias del mismo módulo, resulta otra congruencia de dicho módulo.

Si a ≡ b (mod m) ∧ c ≡ d (mod. m),
Entonces, a – c L b – d (mod. m)

Demostración

a- b = km
a- c = k'm restando miembro a miembro se obtiene:
(a-b)-(c-d)= (k-k') m
(a-c)-(b-d)= (k-k') m
∴(a-c) L (b-d) (mod m)

Esta última igualdad supone que las substracciones son posibles: En las aplicaciones prácticas se añade, si fuera necesario, múltiplos del módulo. La consecuencia de esta última igualdad es que en una congruencia puede cambiarse un término de miembro, cambiando de signo. Las dos congruencias a ≡ b (mod m) y a – b ≡ 0 (mod. m) son consecuencias una de la otra. Esto se enuncia en el siguiente teorema.

Teorema: La condición necesaria y suficiente para que dos números a y b den el mismo residuo al dividirlos por un mismo número **m,** es que su diferencia sea divisible por **m.**

Demostración:

aL b (mod m)
a-b L (b-b) (mod m)
∴a-bL 0(mod m)

4) Multiplicando miembro a miembro dos congruencias de un mismo módulo, se obtiene otra congruencia de dicho módulo.

Si a ≡ b (mod. m) ∧ c ≡ d (mod.m)
Entonces, a × c ≡ b × d (mod. m)

Demostración

a-b = km ∴a=km+b
c-d=k'm ∴c=k'm+d multiplicando miembro a miembro se obtiene:
a×c= (km+b) (k'm+d)
a×c= (kk'm^2+kmd+k'mb+bd)
a×c- b×d=m (kk'm+kd+k'b)
∴ a×c≡ b×d (mod m)

Esta propiedad se extiende al producto de un número finito cualquiera de congruencias del mismo módulo.

Demostración

a≡ b (mod m)
c≡ d (mod m)
e≡ f (mod m)
∴ a×c×e≡ b×d×f (mod m)
Se deduce de lo anterior que, dada una congruencia, si se elevan los dos miembros de ella a la misma potencia resulta otra congruencia del mismo módulo.
Si $[a \equiv b \text{ (mod. m)}]^n \Rightarrow [a^n \equiv b^n \text{ (mod. m)}]$

Teorema: si en un producto de varios factores, uno de ellos es divisible por un número, su producto también lo es.

Sea el producto a × b × c en donde b es, por hipótesis, divisible por **m**; esto es b ≡ 0 (mod. m); entonces se puede escribir:
Si a ≡ a (mod. m), b ≡ 0 (mod. m) c ≡ c (mod. m)
Entonces a×b×c = a×0×c (mod. m). De donde se deduce que a×b×c = 0 (mod. m)
Esto demuestra que el producto a×b×c es divisible por **m**.

Aplicaciones de la aritmética modular: los números de identificación, los códigos de barras y la transmisión de la información.

Los números de identificación tienen dos funciones principales:

a) identificar inequívocamente a la persona o cosa
b) autocontrol del número

La transmisión libre de errores, garantiza la eficiencia de los sistemas de información de los bancos, de los hipermercados, del correo postal, de los tiquetes aéreos, de las tarjetas de crédito, etc. Por esta razón, se utiliza el último dígito (Low Significant Digit: LSD) como un código detector de error. El último dígito es un dígito de verificación que es congruente módulo **n** con cierta suma ponderada de las cifras del número que se quiere verificar o controlar la ausencia de errores. En los impresos se utilizan códigos de barras que traducen las cifras decimales en números binarios. En estos impresos también aparecen las letras (CK) (que simbolizan "check" encima del último dígito del número de identificación.

Por ejemplo, el servicio postal de E. U. utiliza números de identificación de 10 cifras más en dígito de verificación que se obtiene del residuo de dividir el número entre 9, es decir:

$$n \equiv CK \text{ (mod. 9)}$$

El número es congruente con el residuo CK módulo 9. Si el número es 18384459312-CK, el check se calcula realizando la división del número por 9, esto es: 1838459312 ÷9= 204273256 y tiene un residuo de 8.

Este residuo es el código de detección de error de tal manera que el número de identificación es 18384593128, también lo escriben: 1838459312-8.

Los cheques viajeros American Express utilizan números de identificación de 9 cifras más el "check". El dígito de control CK se obtiene así: se efectúa la suma de sus cifras y se suma el CK, de tal manera que la suma total sea divisible por 9. Esto se expresa simbólicamente así:

$$\sum_{i=1}^{i=9} a_i + CK \equiv 0 \pmod 9$$

Así, si el número es 452835227-CK, la suma: 4+5+2+8+3+5+2+2+7 = 38, más el dígito de control CK = 7 (38+7=45≡0 (mod. 9)). El número de identificación completo será 452835227-7.

Los servicios postales privados como FedEx y UPS y los tiquetes aéreos utilizan una congruencia módulo 7 con números de identificación de 10 cifras.

$$n \equiv CK \pmod 7$$

Así, para el número 1148253694-CK, el CK se calcula: 1148253697÷7 = 164036242 con un residuo de 3, de tal manera que el CK = 3.

El código universal de productos UPC es un número de identificación de 11 cifras cuyo "check" se calcula con la siguiente expresión:

$$3 \times \sum_{i=1}^{i=6} a_{2i-1} + \sum_{i=1}^{i=5} a_{2i} + CK \equiv 0 \pmod{10}$$

Por ejemplo para el número 45283598235 –CK se calcula:

$$3(4+2+3+9+2+5) + (5+8+5+8+3) = 3\times25+29 = 104,$$

Entonces, 104 + CK = 104+6 = 110 ≡ 0 (mod. 10), de donde CK = 6.

El sistema bancario de los E.U. usa una variante del sistema UPC asignando diferentes pesos a las cifras del número de identificación así:

$7a_1+3a_2+9a_3+7a_4+3a_5+9a_6+7a_7+3a_8 \equiv CK \pmod{10}$

Para el número de identificación de 8 cifras siguiente: 45283894 – CK se calcula:

7×4+3×5+9×2+7×8+3×3+9×8+7×9+3×4 =

28 + 15 +18+56+9+72+63+12 = 273 ≡ 3 (mod. 10)

por lo tanto, el número de identificación se escribe: 45283894-3.

Los bancos alemanes, tarjetas de crédito, bibliotecas, bancos de sangre, compañías fotográficas, permisos de conducir, utilizan una manera más compleja de calcular el dígito de control. Utilizan números de 13 cifras: 7 de orden impar y 6 de orden par.

Al duplo de la suma de las cifras de orden impar se le agrega el número de cifras que sean mayores que 4, y luego se agrega la suma de las cifras de orden par.

A esta suma se le debe agregar el CK para que sea divisible por 10, es decir simbólicamente:

$$2 \times \sum a_{2i-1} + n(\{a_{2i-1} \Big|_1^7 / a_{2i-1} \rangle a\}) + \sum_{i=1}^{i=6} a_{2i} + CK \equiv 0 \pmod{10}$$

El método usado en todo el mundo para calcular el dígito de control del Internacional Standard Book Number, ISBN, número de identificación de todos los libros que se imprimen en la actualidad se calcula ponderando cada una de las 9 cifras por su propio número de orden. La suma de esos productos es congruente con el CK módulo 11. Simbólicamente:

$$\sum ia_i \equiv CK \pmod{11}$$

Por ejemplo, el libro Matemática Digital tiene por ISBN el número 958-600-821-CK. El dígito de control CK se calcula así:
9×1+5×2+8×3+6×4+0×5+0×6+8×7+2×8+1×9 = 148
148÷11 = 13 y residuo 5; por lo tanto CK = 5 por que 148≡5 (mod. 11) y el ISBN de este libro es escribirá: 958-600-821-5.

Aplicaciones de la aritmética modular: la criptografía de clave pública.

En 1975, Rivest, Shamir y Adelman (RSA) diseñaron un ingenioso método que permite a cualquier persona que desee recibir un mensaje secreto, hacer pública la forma de codificar los mensajes que se envían. Y a pesar de que el método usado para codificar el mensaje es del dominio público, solamente la persona a la que se envía el mensaje es capaz de descifrarlo. La criptografía de clave pública RSA se basa en que existen métodos eficientes para encontrar números primos de alrededor de 100 dígitos y de multiplicarlos; pero no existen métodos para factorizarlos. Por tanto, la persona que desea recibir el mensaje encuentra un par de números primos grandes **p** y **q** y elige un entero **r** de tal manera que el único m.c.m (p-1. q-1) = r, la persona calcula n = pq y anuncia públicamente que el mensaje M se le debe enviar como M (mod. n). A pesar de que r, n y M están al alcance de cualquier persona, solamente quien conoce la factorización de n como pq es capaz de descifrar el mensaje.

Sin conocer los factores de n = pq no se puede encontrar el mínimo común múltiplo de p-1 y q-1 (en nuestro caso 16), y en consecuencia, tampoco se puede encontrar el número **s** que es necesario para descifrar el mensaje. En la práctica, los mensajes no se envían letra a letra. En cambio, se convierten a su notación decimal sustituyendo A por 01, B por 02,…, y un espacio por 00. A continuación, se divide el mensaje en bloques de tamaño uniforme y se envían estos bloques.

Véase el paso 2 en el párrafo encabezado "Remitente", que se describe más abajo.

Destinatario

1) Elija números primos muy grandes p y q y calcule n = pq
2) Calcule el mínimo común múltiplo de p – 1 y q – 1; llámele **m**
3) Elija **r** de manera que no tenga más divisores en común con **m** que el 1 (cualquier r, primo relativo de m, funcionará)
4) Encuentre **s** de manera que r×s ≡ 1 (mod. m) (solamente hay un número s que satisfaga esta igualdad y que esté entre 1 y m)
5) Olvídese de p y q
6) Anuncie públicamente los números n y r, pero mantenga en secreto el número s.

Remitente

1) Convierta el mensaje en una secuencia de dígitos. (en la práctica, se usan el código ASCII)
2) Separe el mensaje en bloques de dígitos de tamaño uniforme añadiendo ceros al último bloque si es necesario; llame a estos bloques M_1, M_2,… M_k.
Por ejemplo, para una secuencia tal como 2105092315 podríamos utilizar M_1=2105, M_2 = 0923, M_3 = 1500
3) Compruebe que el máximo común divisor de cada M_i y n es 1. En caso contrario, **n** puede factorizarse y el código se puede romper. (En la práctica, los números primos p y q son tan grandes que superan a todos los M_i y, por tanto, este paso puede ser omitido.

4) Calcule y envié $R_i = M_i^r \pmod{n}$

Destinatario

1) Para cada uno de los mensajes recibidos R_i, calcule $R_i^s \pmod{n}$

2) Convierta la secuencia de dígitos en una secuencia de caracteres.
Este método funciona debido a una propiedad básica de la aritmética modular y a la elección de r. Sucede que el número **m** tiene la propiedad de que para cada número x que no tiene con **n** más divisores comunes que el 1, siempre tenemos $x^m = 1 \pmod{n}$. Por tanto, como cada mensaje M_i no tiene divisores comunes con **n** excepto el 1, y r se ha elegido de manera que r×s = 1 +mt para algún t, tenemos, módulo n:

$$R_i^s = (M_i^t)^s = M_i^{r\times s} = M_i^{1+tm}$$
$$R_i^s = M_i(M_i^m)^t = M_i \times 1^t = M_i$$

Ejemplo:

Utilice el esquema RSA con p = 5, q = 17 y r = 3 para determinar los números enviados para el mensaje VIP.
RSA: p = 5, q = 17, r = 3
"VIP" mensaje

Destinatario

1) n = p×q = 5×17 = 85
2) mcm(4,16) = 16 = m
3) r = 3 / MCD (3,16) = 1
4) Hallar s / 3×s ≡ 1(mod 16) ∴s=11
5) Olvidar p y q
6) Publicar: n = 85 y r = 3

Remitente

1) "VIP" ≈ 86, 73, 80
2) Dividir mensaje en: $M_1 = 86$, $M_2 = 73$, $M_3 = 80$
3) Comprobar MCD (86,85) = 1
   MCD (73,85) = 1
   MCD (80,85) = 5?

4) Calcular y enviar: $R_i \equiv M_i^r \pmod{n}$

$$R_1 \equiv M_1^3 \pmod{85} \equiv 86^3 \pmod{85} \equiv 1 \pmod{85}$$

$$R_2 \equiv M_2^3 \pmod{85} \equiv 73^3 \pmod{85} \equiv 57 \pmod{85}$$

$$R_3 \equiv M_3^3 \pmod{85} = 80^3 \pmod{85} \equiv 45 \pmod{85}$$

Enviar: 1, 57, 45

Destinatario:

1) Calcular $R_i^s \pmod n$

$R_1^1 \pmod{85} \equiv 1^{11} \pmod{85} \equiv 1 \pmod{85}$

$R_2^1 \pmod{85} \equiv 57^{11} \pmod{85} \equiv 86 \pmod{85}$
$\equiv 57 \pmod{85} \equiv 57$
$\equiv 57^2 \pmod{85} \equiv 19$
$\equiv 57^4 \pmod{85} \equiv 57^2 \times 57^2 \pmod{85}$
$\equiv 19\times19 \pmod{(85)} = 361 \pmod{85} \equiv 21 \pmod{85}$
$\equiv 57^8 \pmod{85} = 21\times21 \pmod{85} = 441 \pmod{85} = 16 \pmod{85}$
$= 57\times 57^2 \times 57^8 \pmod{85}$
$= 57\times 19 \times 16 \pmod{85} = 73 \pmod{85}$

$R_3^1 \pmod{85} \equiv 45^{11} \pmod{85}$
$\equiv 45 \pmod{85} \equiv 45 \pmod{85}$
$\equiv 45^2 \pmod{85} \equiv 70 \pmod{85}$
$\equiv 45^4 \pmod{85} \equiv 45^2\times45^2 \pmod{85} = 70\times70 \pmod{85}$
$\equiv 4900 \pmod{85} \equiv 55 \pmod{85}$
$\equiv 45^8 \pmod{85} \equiv 45^4\times 45^4 \pmod{85} = 55\times55 \pmod{85}$
$\equiv 3025 \pmod{85} \equiv 50 \pmod{85}$
$45^{11} \pmod{85} = 45\times45^2\times45^8 \pmod{85}$
$\equiv 45\times70\times50 \pmod{85}$
$\equiv 157500 \pmod{85} = 80 \pmod{85}$

2) 86, 73, 80 ≈ "VIP"

Ejemplo

Utilice el esquema RSA con p = 5, q = 17 y R = 3 para decodificar los números recibidos: 52, 72.
RSA: p = 5, q = 17, r = 3

Decodificar: 52, 72
$R_i^s \pmod n$
$M_1 = 52^{11} \pmod{85} \equiv ?$
$52 \pmod{85} \equiv 52 \pmod{85}$
$52^2 \pmod{85} \equiv 52\times52 \pmod{85}$
$\equiv 69 \pmod{85}$
$52^4 \pmod{85} \equiv 52^2\times52^2 \pmod{85} = 69\times69 \pmod{85}$
$\equiv 1 \pmod{85}$
$52^8 \pmod{85} \equiv 52^4\times52^4 \pmod{85}$
$\equiv 1\times1 \pmod{85}$
$52^{11} \pmod{85} \equiv 52\times52^2\times52^8 \pmod{85}$
$\equiv 52\times69\times1 \pmod{85}$
$\equiv 18 \pmod{85}$

$M_2 = 72^{11} \pmod{85} \equiv ?$
$72 \pmod{85} \equiv 72 \pmod{85}$
$72^2 \pmod{85} \equiv 84 \pmod{85}$
$72^4 \pmod{85} \equiv 84\times84 \pmod{85} \equiv 1 \pmod{85}$
$72^8 \pmod{85} \equiv 1\times1 \pmod{85} \equiv 1\times1 \pmod{85} \equiv 1 \pmod{85}$
$72^{11} \pmod{85} \equiv 72\times72^2\times72^8 \pmod{85} \equiv 72\times84 \pmod{85}$
$\equiv 13 \pmod{85}$
luego el mensaje RSA: 52, 72 se decodifica en: 18, 13.

Ejemplo

En el esquema RSA con p = 5, q = 17 y r = 5, determine el valor de s.

RSA: p = 5, q = 17 y r = 5,

1) $n = p \times q = 5 \times 17 = 85$
2) $mcm(4,16) = 16 = m$
3) $r = 5 / MCD(5, 16) = 1$
4) $s / 5 \times s \equiv 1 \pmod{16} \ \therefore \ s = 13$

Bibliografía

Aristizábal y S. (2000). "Teoría de las relaciones en la plataforma Mathematica". En: . *Academos*, No.2., APUC. Año 5 julio-diciembre..

Ayres, Frank Jr. (1991). *Algebra Moderna*. México: McGraw-Hill...

Bourbaki, Nicolás. (1970). *Elements de Mathematique, Algebre I*. Hermann.

Casanova, Gastón. (1995). *El Algebra de Boole.* Madrid: Edit. Técnicos.

Frege, Gottlob. (1972). *Los Fundamentos de la aritmética*. México: Universidad Nacional Autónoma de México.

Grassmann, Winfried K., and Tremblay, Jean-Paul. (1997). *Matemática Discreta y lógica*. Madrid. Edit, Prentice may..

Gómez, Wills., Guarín y Londoño. (1976). *Matemática moderna estructurada.* Editorial.

Gillie, Angelo C. (1965). *Binary Arithmetic and Boolean Algebra*. New York: Edit. Mc Graw Hill.

Gregory, Arthur. (1973). *Conceptos Fundamentales de Algebra Booleana* México:. Edit. Trillas.

Heim, Klaus. (1973). *Algebra de los circuitos lógicos*. Berlín: Edit. Dossat.

Jhonson Baugh, Richard. (1997). *Matemáticas discretas*. México: Prentice-Hall.

Kostrikin, A. I. (1983). *Introducción al Algebra.* Moscú: Editorial MIR.

Lidl y Pilz. (1984). *Applied Abstract Algebra.* New York: Springer Verlag.

Lipschutz, Seymour. (1992). *Algebra Lineal.* 2ª ed. Madrid: Editorial McGraw-Hill.

Luque, C., Mora, L., Páez, S. (2002). *Actividades matemáticas para el desarrollo procesos lógicos: los procesos de contar e inducir.* Bogotá: Universidad Pedagógica Nacional.

Mendelson, Elliot. (1970). *Boolean algebra and sustching circuits*. New York: Edit Mc Graw Hill.

Muñoz, J. (2002). *Introducción a la teoría de conjuntos*. 4ª ed. Bogotá:. Universidad Nacional de Colombia.

Nachbin, Leopoldo. (1986). *Algebra Elemental* Washington: Editorial Departamento de asuntos científicos y tecnológicos de la secretaría general de la OEA.

Ross, Kenneth A. and Wright, Charles R.B. (1991). *Matemáticas Discretas.* 2ª ed. México: Edit. Prentice-Hall..

Sánchez y Velasco. (1978). *Curso Básico de Algebra Lineal.* 2ª ed. Colombia: Editorial COMEX S.A.

Silberschatz, Abraham., Korth Henry F., S. Sudarshan (1998). *Fundamentos de Bases de Datos.* 3ª ed Madrid:. Editorial McGraw-Hill.

Steen, L. A., y Cols. (1999). *Las matemáticas en la vida cotidiana*. Madrid: Addison-Wesley.

Suppes, Patrick. (1968). *Teoría axiomática de conjuntos.* Edit. Norma.

Whitesitt, J., Eldon. (1961). *Boolean algebra and its applications*. Estados Unidos: Editorial Addison-Wesley Publishing Co.

Wiederhold, Gio. (!985). *Diseño de bases de datos.* 2ª ed. (1ª ed. en español). México: McGraw-Hill.

Whitesitt, Eldon. (1972). *Boolean algebra and its Applications* México: Edit. Continental.

http://es.tldp.org/tutoriales/NOTAS-CURSO-BBDD/notas-curso-BD/node25.html