MATEMÁTICA

Cambio de base

Tecnicatura Universitaria en Programación

Enteros y División

Bibiliografía: Matemática Discreta y sus Aplicaciones (5ta ed), Rosen Kenneth. Mcgraw-Hill, Interamericana de España, S.A.

Capítulo 2. Sección 4

Capítulo 2. Sección 5

ENTEROS Y DIVISIÓN

Definición 1

Teoría de números: es la parte de la matemática discreta que estudia los enteros y sus propiedades.

La división de un entero por un entero positivo da como resultado un cociente y un resto. Trabajar con estos restos conduce a la aritmética modular.

Tres aplicaciones de la aritmética modular:

- Generación de números pseudoaleatorios
- Asignación de posiciones de memoria a ficheros en una PC
- Cifrado y descifrado de mensajes

ENTEROS Y DIVISIÓN

Definición 2

Si a y b son enteros, $a \neq b$, decimos que a divide a b si existe un entero c tal que $b = ac$. Cuando a divide a b decimos que a es un factor (o divisor) de b y que b es un múltiplo de a. Se denota con $a|b$ (a divide a b). Si a no divide a b se denota con $a \nmid b$

Proposición:

- Si a divide a b, entonces a divide a $-b$; $-a$ divide a $-b$ y $-a$ divide a b
- Si a divide a dos números b y c, entonces a divide a la suma de ellos. Es decir: $a|b$ y $a|c \Rightarrow a|(b+c)$
- Si a divide a b, entonces a divide a a cualquier múltiplo de b. Es decir; $a|b.c$ para cualquier entero c
- La relación de divisibilidad es transitiva: Si a divide a b, y b divide a c; entonces a divide a c. Es decir; $a|b$ y $b|c \Rightarrow a|c$
- Si a divide a b y a c, entonces a divide a la suma de multiplos de ellos. Es decir; $a|b$ y $a|c \Rightarrow a|(m.b+n.c)$

ENTEROS Y DIVISIÓN

Teorema 1

Sean a, b y c enteros, entonces:

1. Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$
2. Si $a \mid b$, entonces $a \mid bc, \forall$ entero c
3. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$

Corolario:

Si a, b y c son enteros tales que $a \mid b$ y $a \mid c$, entonces $a \mid mb + nc$ para m y n cualesquiera

Definición 3

Un entero positivo p mayor que 1 se llama primo si los únicos divisores positivos de p son 1 y p. Un entero positivo mayor que 1 que no es primo se denomina compuesto

NÚMEROS PRIMOS

Teorema 2

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

Todo entero positivo mayor que 1 se puede escribir de una única forma como un primo o como el producto de dos o mas primos en el que los factores primos se escriben en orden no decreciente

Teorema 3

Si n es un entero compuesto, entonces n tiene un divisor primo menor o igual que $\sqrt{n}$

Teorema 4

Hay infinitos números primos

ALGORITMO DE LA DIVISIÓN

Teorema 5

ALGORITMO DE LA DIVISIÓN

Sean a un número entero y d un entero positivo. Existen dos únicos enteros q y r, $0 \leq r < d$, tales que $a = d.q + r$

Definición 4

En la igualdad dada por el algoritmo de la división, d se llama divisor, a se llama dividendo, q es el cociente y r se conoce como resto.

La siguiente notación se usa para expresar el cociente y el resto:

$q = a$ **div** d $\quad r = a$ **mod** d

MÁXIMO COMÚN DIVISOR – MÍNIMO COMÚN MÚLTIPLO

Definición 5

Sean a y b enteros no nulos. El mayor entero d talque $d \mid a$ y $d \mid b$ se denomina máximo común divisor de a y b. el máximo común divisor de a y de b se denota como $\boldsymbol{MCD}\ (a, b)$

Definición 6

Los números enteros a y b son primos relativos o primos entre sí, si su máximo común divisor es 1

Definición 7

Los números enteros $a_1, a_2, \ldots, a_n$ son primos relativos dos a dos si su $\boldsymbol{MCD}\ (a_i, a_j) = 1$, para $1 \leq i < j \leq n$

MÁXIMO COMÚN DIVISOR – MÍNIMO COMÚN MÚLTIPLO

Definición 8

El mínimo común múltiplo de los enteros positivos a y b es el menor enteros positivo que es divisible tanto por a como por b. El mínimo común múltiplo de a y b se denota por $\boldsymbol{mcm}\ (a, b)$

Teorema 6

Sean a y b enteros positivos, entonces

$ab = \boldsymbol{MCD}\ (a, b)\ .\ \boldsymbol{mcm}\ (a, b)$

PRÁCTICA

Página 171 del PDF

- Ejercicio 1
- Ejercicio 9 a, b
- Ejercicio 11 a, b
- Ejercicio 28 a, b - MCD
- Ejercicio 29 a, b - mcm

ENTEROS Y ALGORITMOS

Teorema 10

Sea b un entero positivo mayor que 1. Entonces, si n es un entero positivo, se puede expresar como:

$$n = a_k\, b^k + a_{k-1}\, b^{k-1} + \ldots + a_1\, b^0 + a_0$$

De una única forma, donde k es un entero no negativo, $a_o, a_1, \ldots, a_k$ son enteros no negativos menores que b y $a_k \neq 0$

Ejercicios:

Cual es la expresión decimal de:

- la expresión binaria $(1\ 0101\ 1111)_2$
- la expresión hexadecimal $(2AE0B)_{16}$

Cual es la expresión en base 8 de $(12345)_{10}$

Cual es la expresión hexadecimal de $(11\ 1110\ 1011\ 1100)_2$

ALGORITMO DE EUCLIDES

Un algoritmo es una secuencia de pasos para conseguir un resultado.

Para calcular **MCD** entre dos números n_1 y n_2, con $n_1 > n_2$

Se divide n_1 / n_2

- Si: La división es exacta → MCD es n_2
- Si no: dividimos n_2 con el resto y se continúa hasta obtener una división exacta, siendo el último divisor el MCD

Para hallar el **mcm** $(n_1, n_2) = (n1 \,.\, n2)$ / MCD $(n1, n2)$

Lema 1

Sea $a = b.q + r$, donde a, b, q y r son enteros. Entonces:

$$MCD(a, b) = MCD(b, r)$$

PRÁCTICA

- Hallar el MCD (250, 110) y el mcm (250, 110). Comprueba el teorema 7

Hallar el MCD entre 250 y 110
250 : 110→ Cociente: 2, Resto: 30
110 : 30 → Cociente: 3, Resto: 20
30 : 20 → Cociente 1, Resto 10
20 : 10 → Cociente 2, Resto 0
Por lo tanto, MCD(250, 110) = **10**

Hallar el mcm entre 250 y 110
mcm (250, 110) = (250 . 110) /MCD (250 , 110)
mcm (250, 110) = 27.500/10 = **2.750**

Teorema 7:
250.110 = MCD (250, 110). mcm (250, 110)
27.500 = 10 . 2750
27.500 = 27.500

PRÁCTICA

Página 184 del PDF

- Ejercicio 1 - 3 - 4 – 5 – 9 – 10 – 21 - 22

Álgebra de Boole

Bibiliografía: Matemática Discreta y sus Aplicaciones (5ta ed), Rosen Kenneth. Mcgraw-Hill, Interamericana de España, S.A.

Capítulo 10

FUNCIONES BOOLEANAS

Definición 1

El álgebra de Boole proporciona las operaciones y las leyes para trabajar en el conjunto {0, 1}.

Las tres operaciones de un álgebra de Boole más utilizados son:

- Complemento:
- Suma:
- Producto Booleano

Las reglas de precedencia de los operadores son: complementos, producto y suma

COMPLEMENTO: NOT		SUMA: OR +			PRODUCTO: AND .		
1	0	1	1	1	1	1	1
0	1	1	0	1	1	0	0
		0	1	1	0	1	0
		0	0	0	0	0	0

EXPRESIONES Y FUNCIONES BOOLEANAS

Definición 2

Sea $B = \{0, 1\}$, entonces $B^n = \{(x_1, x_2, \ldots, x_n) / x_i \in B, 1 \leq i < n\}$ es el conjunto de todas las posibles *n-tuplas* de ceros y unos. La variable x se llama variable booleana si toma valores en el conjunto B. Una función B^n en B se llama función booleana de grado n.

Las funciones booleanas se pueden representar utilizando expresiones construidas con variables y operadores booleanos. Las expresiones booleanas en las variables $x_1, x_2, \ldots, x_n$ se definen recursivamente como:

$0, 1, x_1, x_2, \ldots, x_n$ Son expresiones booleanas;

Si E_1 y E_2 son expresiones booleanas, entonces E_1, (E_1E_2) y $(E_1 + E_2)$ son expresiones booleanas

EXPRESIONES Y FUNCIONES BOOLEANAS

Definición 3

Dos funciones booleanas de n variables F y G son iguales si, y sol si, $F(b_1, b_2, \ldots, b_n) = G(b_1, b_2, \ldots, b_n)$ para cualesquiera $b_1, b_2, \ldots, b_n$ de B. se dice que dos expresiones booleanas diferentes son equivalentes si representan la misma función.

Definición 4

El dual de una expresión booleana se obtiene intercambiando entre sí la suma y el producto booleano, así como los ceros y los unos.

El dual de una función boolena F representada por una expresión booleana es la función representada por el dual de dicha expresión.

Una igualdad entre funciones booleanas sigue siendo válida cuando se toman duales a ambos lados de la igualdad, a esto se lo conoce como Principio de Dualidad

PROPIEDADES

Propiedad	Nombre
$x = x$	Prop. del doble complemento
$x + x = x$ $x \cdot x = x$	Prop.de idempotencia
$x + 0 = x$ $x \cdot 1 = x$	Prop. del elem. neutro
$x + 1 = 1$ $x \cdot 0 = 0$	Prop. de acotación
$x + y = y + x$ $x.y = y.x$	Prop. conmutativas

Propiedad	Nombre
$x + (y + z) = (x + y) + z$ $x.(y.z) = (x.y).z$	Prop. asociativas
$x + yz = (x + y) (x + z)$ $x (y + z) = xy + xz$	Prop. distributivas
$\overline{(x.y)} = \overline{x} + \overline{y}$ $\overline{(x + y)} = \overline{x}.\overline{y}$	Prop. de De Morgan
$x + x.y = x$ $x.(x + y) = x$	Prop. de absorción
$x + \overline{x} = 1$	Prop. del inverso para el 1
$x.\overline{x} = 0$	Prop. del inverso para el 0

PRÁCTICA

Página 678 del PDF

- Ejercicio 1
- Ejercicio 2
- Ejercicio 3
- Ejercicio 26

REPRESENTACIÓN DE FUNCIONES BOOLEANAS

Definición 6

Un literal es una variable booleana complementada. Un minitermino en las variables booleanas $x_1, x_2, \ldots, x_n$ es un producto booleano $y_1.y_2 \ldots, y_n$ donde o $y_i = x_i$ o $y_i = x_i$.

Por lo tanto, un minitermino es un producto de n literales con un literal por cada variable.

Definición 7

A la suma de minitérminos que representa a la función se le llama desarrollo en suma de productos o bien forma normal disyuntiva de la función booleana

La forma normal conjuntiva o desarrollo en producto de sumas se puede obtener desde la forma normal disyuntiva tomando el dual y añadiendo los maximtérminos al producto por cada combinación de las variables para la que la función vale 0

PRÁCTICA

Página 682 del PDF

- Resolver los problemas del 1, 2 y 3

PUERTAS LÓGICAS

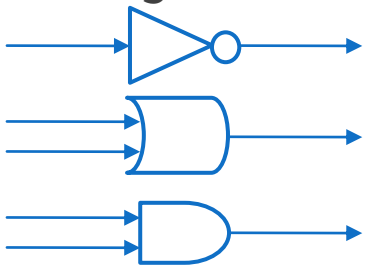
Definición 9

El álgebra de Boole se usa para modelar los circuitos de dispositivos electrónicos. Los elementos básicos de los circuitos se llaman puertas lógicas. Cada tipo de puerta implementa una operación booleana.

Los circuitos a estudiar producen una salida dependiente de la entrada y no del estado actual del circuito, es decir, no tienen memoria. Estos circuitos se llaman redes lógicas o circuitos combinacionales.

Veremos la construcción de una red lógica utilizando 3 tipos de elementos:

- Inversor o puerta NOT
- Puerta OR
- Puerta AND



PRÁCTICA

Página 688 del PDF

- Resolver los problemas del 1, 3 y 5
- Ejercicio 6 b y d

MINIMIZACIÓN DE CIRCUITOS

Definición 11

Minimización de la función booleana: describiremos dos procedimientos que simplifican formas normales disyuntivas.

El objetivo de ambos procedimientos es producir de entre todas las sumas booleanas de productos booleanos que representan a una función booleana, aquellas sumas de productos que contengan el menor numero posible de sumandos, de modo que estos sumandos sean productos del menor numero posible de literales.

Los procedimientos son:

- K – Diagramas o diagramas de Karnaugh
- Quine Mc Cluskey

PRÁCTICA

Página 701 del PDF

- Resolver los problemas del 2, 3 y 4