Capítulo 1: INTRODUCCIÓN A LA TEORÍA DE NÚMEROS

1.1 Introducción

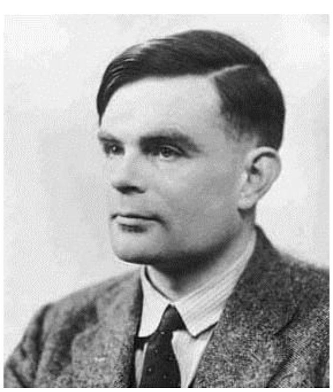
Desde hace cientos de años antes de Cristo los matemáticos ya habían realizado actividades de investigación con los números; es por ello que la teoría de números es una de las ramas de la matemática más antigua.

La teoría de números es la rama de matemáticas puras que estudia las propiedades de los números, de manera particular, los enteros, pero más en general, estudia las propiedades de los elementos de Dominios Enteros así como diversos problemas derivados de su estudio. Contiene una cantidad considerable de problemas que podrían ser comprendidos por "no matemáticos".

Las necesidades humanas han exigido también avance la capacidad técnica, lo que va contribuyendo, por consiguiente, al desarrollo de la ciencia y la tecnología, en particular la evolución de la electrónica que por ende ha implicado la creación de nuevos computadores y mejoramiento de otros.

En este capítulo se estudiarán algunos conceptos básicos de la teoría de números y algunas aplicaciones de la criptografía y los sistemas numéricos para la computación. Se desarrollarán técnicas para la creación de otros sistemas numéricos diferentes a los que él utiliza (como los el decimal): el binario, el octal y el hexadecimal. Además de los sistemas anotados existen algunos sistemas utilizados para codificar en computación, entre otros: los sistemas BCD, EBCDIC y ASCII.

Similarmente, se estudiará el sistema hexadecimal, porque algunos lenguajes de programación y en general los sistemas operativos utilizan este sistema para localizar archivos en un dispositivo de almacenamiento.


Alan Turing (1912-1954)

Alan Turing (1912-1954) puede ser considerado el padre de la Inteligencia Artificial (IA), aunque este nombre no se usase hasta después de 1956. Pero hablando de recursión y computación se tendrá que considerar Turing, quien a la edad de 24 años, realizó una gran contribución demostrando que el problema de la decisión de Hilbert que tenía solución negativa, no tiene un procedimiento automático que permita obtener la solución a cualquier cuestión matemática. Para ello recurrió a su famosa noción de "máquina de Turing", mostrando que el problema de la parada de cualquier máquina de Turing, es indecidible. Turing continuó realizando contribuciones muy importantes a la lógica, la computación, la inteligencia artificial y la biología matemática, al tiempo que participaba en las actividades de guerra como "rompe-códigos". En la Segunda Guerra Mundial ofreció un insospechado marco de aplicación práctica de sus teorías, al surgir la necesidad de descifrar los mensajes codificados que la Marina alemana empleaba para enviar instrucciones a los submarinos que hostigaban los convoyes de ayuda material enviados desde Estados Unidos. Turing, al mando de una división de la Inteligencia británica, diseñó tanto los procesos como las máquinas que, capaces de efectuar cálculos combinatorios mucho más rápido que cualquier ser humano, fueron decisivos en la ruptura final del código.

Pero su vida terminó muy pronto y trágicamente: a consecuencia de un robo en su casa, el inició de una serie de peripecias, cuando fue acusado de prácticas homosexuales en su propia casa con un "menor" de 19 años. Juzgado y condenado a recibir inyecciones de estrógeno, ésto acabó con su buena forma física (forjada en carreras de maratón). Puso fin a sus actividades de criptografía y se convirtió en objeto de vigilancia policial. De tal manera terminó llevándole a pensar que la vida ya no valía la pena; en efecto, el 8 de junio de 1954 decidió quitarse la vida, tomando cianuro potásico.

1.2 División

Sean a, b $\in \mathbb{Z}$ y b>0. Existen sólo un par de enteros q (cociente) y r (residuo) tales que a=qb+r con 0≤r<b, la cual denominaremos expresión de Euclides.

Ejemplo 1.1: calcule q y r, utilizando la expresión de Euclides, conocidos los valores de a y de b en cada uno de los siguientes casos:

1. a=715 y b=19
2. a=29 y b=4
3. a=146 y b=37
4. a=331, b=45
5. a=235 y b=16
6. a=-331 y b=45
7. a=-715 y b=19
8. a=-1237 y b=65

Solución:

1. 715=37*19+12 $\Rightarrow$ q=37 y r=12
2. 29=7*4+1$\Rightarrow$q=7 y r=1
3. 146=3*37+35$\Rightarrow$q=3 y r=35
4. 331=7*45+16$\Rightarrow$q=7 y r=16
5. 235=14*16+11$\Rightarrow$q=14 y r=11
6. 331= -8*45+29$\Rightarrow$q=-8 y r=29
7. -715= -38*19+7$\Rightarrow$ q=-38 y r=7
8. -1237= -65*21+7$\Rightarrow$ q=-38 y r=7

1.3 Div y Mod

Sean a, b$\in \mathbb{Z}$ y b>0. Según la expresión de Euclides, Div y Mod se definirán como

a Div b=q y **a Mod b=r**

Ejemplo 1.2: El cálculo de

41 Mod 7 = 6
41 Div 7 = 5
-37 Div 5 = -8
-37 Mod 5 = 3
-104 Div 431= -1
-104 Mod 431= 327

1.4 Divisor común

Sean a, b $\in \mathbb{Z}$. Se dice que un entero d es divisor común de a y de b si d|a y d|b.

Ejemplo 1.3: los divisores comunes de 24 y 18 son: 2, 3, 6

1.5 Máximo Común Divisor

Sean a, b $\in \mathbb{Z}$. Se dice que d$\in \mathbb{Z}$ es el **Máximo Común Divisor** y lo denotaremos mcd de a y b si y solo si

i) d es divisor común de a y b
ii) si e es divisor común de a y b, entonces e≤d

Ejemplo 1.4: mcd(18, 24)=6; mcd(2748, 213)=3 y mcd(-18, -24)=6

Teorema 1: sean a, b$\in \mathbb{Z}$ diferentes de cero. El entero positivo más pequeño de la forma ax+by, denominado "min(ax+by)" donde x,y$\in \mathbb{Z}$, es el mcd(a, b). Simbólicamente, mcd(a, b)=min(ax+by)$\in \mathbb{Z}^+$.

Ejemplo 1.6: calcule: 1. mcd(86;46), 2. mcd(45, 60) y mcd(120;)

Solución:
1. Proceda así:

		y										
		-5	**-4**	**-3**	**-2**	**-1**	**0**	**1**	**2**	**3**	**4**	**5**
x	**-5**	-660	-614	-568	-522	-476	-430	-384	-338	-292	-246	-200
	-4	-574	-528	-482	-436	-390	-344	-298	-252	-206	-160	-114
	-3	-488	-442	-396	-350	-304	-258	-212	-166	-120	-74	-28
	-2	-402	-356	-310	-264	-218	-172	-126	-80	-34	12	58
	-1	-316	-270	-224	-178	-132	-86	-40	6	52	98	144
	0	-230	-184	-138	-92	-46	0	46	92	138	184	230
	1	-144	-98	-52	-6	40	86	132	178	224	270	316
	2	-58	-12	34	80	126	172	218	264	310	356	402
	3	28	74	120	166	212	258	304	350	396	442	488
	4	114	160	206	252	298	344	390	436	482	528	574
	5	200	246	292	338	384	430	476	522	568	614	660

Tabla 1.1: entero más pequeño de la forma ax+by con MS-Excel

pasos	a	b	c
1	86	46	40
2	46	40	6
3	40	6	4
4	6	4	**2**
5	4	**2**	0

Tabla 8.2: Cálculo de mcd

En tal caso a=86 y b=46; construyamos una tabla en Microsoft Excel para estos valores y tomemos un intervalo para x e y entre -5 y 5.

Observe en la tabla 8.1 que 6 es el menor entero positivo y en consecuencia como 86*(-1)+46*2=6 y, el menor divisor de 6 es 2. Por lo tanto, el mcd(86,46)=2.

Verifiquemos ahora las iteraciones que se realizarían en el procedimiento para calcular el mcd:

1. 86 Mod 46=40
2. 46 Mod 40= 6
3. 40 Mod 6 = 4
4. 6 Mod 4 = 2
5. 4 Mod 2 = 0

$\Rightarrow$ mcd(86,46)=**2**

¿De qué tamaño son los números a y b después de 2t pasadas utilizando el "Algoritmo de Euclides"? Cada 2t pasos los números son menores que ($2^{-t}a$, $2^{-t}b$). Debido a que el algoritmo para su funcionamiento cuando el segundo número es menor que 1 se puede modelar este proceso así:

$$\mathbf{2^{-t}\,b \leq 1}$$

$2^{-t}\,b\leq 1 \Leftrightarrow \log_2(2^{-t}b) \leq \log_2 1 \Leftrightarrow -t+\log_2 b\leq 0 \Leftrightarrow \log_2 b\leq t$ (en este momento se detiene).

Por lo tanto, después de $2\log_2 b$ pasadas el algoritmo ha completado su trabajo.

2. mcd(45, 60)=60x+45y, Si x=2 y y=-3, entonces 60(2)+45(-3)=-15 (descartado!)

Si x=2 y y=-2, entonces 60(2)+45(-2)=30 (válido!)

60(1)+45(-1)=15 (el menor valor obtenido)

Por lo tanto, el mcd(45, 60)=**15**

3. mcd(120;48)= 120x+48y=120(1)+48(-2)=24 (el menor valor obtenido). Por lo tanto, el mcd(120, 48)=**24**

1.6 Números Primos relativos

Sean a, b $\in \mathbb{Z}$ diferentes de cero. Se dice que a, b son primos relativos si y solo si hay una solución entera de ax+by=1; es decir, mcd(a, b)=1.

Ejemplo 1.5: determine cuáles ternas dadas son primos relativos:

4, 6 y 9 son primos relativos, porque mcd(4, 6, 9)=1
5, 10 y 14 son primos relativos, porque mcd(5, 10, 14)=1
64,38 y 76 no son primos relativos, porque mcd(64,38, 76)=2

1.7 Algoritmo de Euclides

Hasta el momento se puede determinar el mcd de dos enteros positivos de manera correcta, pero para lograrlo se tienen que realizar muchas divisiones. Evitando hacer tantas operaciones el matemático griego Euclides (s. III a. C.) desarrollo un ingenioso algoritmo denominado **"Algoritmo de Euclides"** que reduce de manera notable la realización de tantas divisiones. Este algoritmo cada dos pasos disminuye a menos de la mitad sus valores actuales.

Utilizando la definición dada en la sección 8.2, se puede dar lograr el teorema que corresponderá al algoritmo de Euclides. En efecto veamos.

1.7.1 Teorema "Algoritmo de Euclides"

Sean a, b $\in \mathbb{Z}^+$ entonces el proceso repetido
$a=q.b+ r_1$ con $0\leq r_1<b$
$b=q_1.r_1+ r_2$ con $0\leq r_2< r_1$
$r_1=q_2.r_2+ r_3$ con $0\leq r_3< r_2$
$r_2=q_3.r_3+ r_4$ con $0\leq r_4< r_3$
.
.
.
$r_{K-3}=q_{K-2}.r_{K-2}+ r_{K-1}$ con $0\leq r_{k-1}< r_{k-2}$
$r_{K-2}=q_{K-1}.r_{K-1}+ r_K$ con $0\leq r_k< r_{k-1}$

Este proceso es útil para verificar si dos números tienen un divisor común. En efecto, si r_k es 0 y asumiendo que $r_{k-1}\neq 0$ entonces, r_{k-1} es el divisor común de a y b. Pero si r_k es 1, entonces es el único divisor común de a y b es 1, lo cual implica que los números son primos relativos.

Ejemplo 1.6: verifique utilizando el Algoritmo de Euclides si 1275 y 270 tienen un divisor común.
1275=4*270+195
270=1*195+75
195=2*75+45
75=1*45+30
45=1*30+15
30=2***15**+0

Por lo tanto, 15 es el máximo común divisor de 1275 y 270

1.7.2 El mcd y el algoritmo de Euclides

Sean a, b $\in \mathbb{Z}$ y sea c= a Mod b, entonces

$$\text{mcd}(a,b)= \text{mcd}(b,c)$$

o de otra manera

$$mcd(a,b)= mcd(b, a \text{ Mod } b)$$

donde mcd es el máximo común divisor.

Según el teorema anterior, si r_k es 0 y asumiendo que $r_{k-1} \neq 0$ entonces, r_{k-1} es el mcd(a,b). Por lo tanto, dicho teorema es de gran utilidad para el cálculo del mcd entre 2 ó más números.

Ejemplo 1.8: calcule el mcd(1275,270) utilizando el Algoritmo de Euclides con módulo.
1275 Mod 270= 195
270 Mod 195= 75
195 Mod 75= 45
75 Mod 45=30
45 Mod 30= 15
30 Mod 15= 0

Por lo tanto, mcd(1275,270)= **15**

1.7.3 Pasos del algoritmo de Euclides

Los pasos que se realizan en el Algoritmo de Euclides son:

Datos de entrada: a y b (enteros positivos)

Datos de salida: mcd(a,b)

Proceso:
- Sea c =a Mod b
- Si c=0 entonces muestre resultado (último divisor) y termine
  si no calcule mcd(b,c) y muestre su resultado

Tal como está planteado el proceso, el algoritmo es recursiva y se detiene en el momento en que el segundo número es menor que 1. También se puede realizar de manera iterativa.

Tal algoritmo es el siguiente:
- Entrar dos números enteros positivos
- Definir como menor el menor dato entre a y b
- Para todo entero positivo k desde 1 hasta el menor entre a y b, verifique si k|a y k|b. Si se cumple esto se pone este valor de k en la lista de divisores
- Escoger el menor valor de la lista y ese será el mcd(a,b)

Ejemplo 1.9: utilice el módulo para calcular el mcd(12375, 3270). Desde luego, si se llega a que dicho módulo es 0, entonces, el anterior Módulo será el mcd.

12375 mod 3270=2565
3270 Mod 2565=705
2565 Mod 705=450
705 Mod 450=255
450 Mod 255=195
255 Mod 195=60
195 Mod 60=15
60 Mod 15= 0

Por lo tanto, el mcd(12375, 3270)=15.

Algoritmo iterativo

```
Lea(a,b)
x←a
y←b
Mientras (y≠0)
{
    r← x Mod y
    x←y
    y←r
}
Muestre(x, “es  el mcd entre” a, “ y ”, b)
```

El mismo algoritmo puede realizarse con restas sucesivas; lo cual podría ser útil en caso de no tener en su compilador al operador Mod. Dicho algoritmo es el siguiente:

```
Lea(a,b)
x←a
y←b
 Mientras x≠y)
    Si  (x>y) entonces
            y←x - y
    Si no
            y=y – x
    Fin si
 Fin mientras
 Muestre (x, “es  el mcd entre”, a, “ y ”, b)
```

Ejercicio 1.1: haga un programa recursivo y otro iterativo, en cualquier lenguaje, que calcule el mcd de

a) dos números a y b.
b) tres números a, b, c

1.8 Definición del conjunto Zn

Sea $n \in \mathbb{Z}^+$; el conjunto de los enteros no negativos menores que n, se denota $\mathbb{Z}n$ y se escribe,

$$\mathbf{\mathbb{Z}n = \{0, 1, 2, 3, \ldots n\text{-}1\}}$$

Ejemplo 1.10: determine $\mathbb{Z}_9$ y $\mathbb{Z}_{41}$

$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\mathbb{Z}_{41} = \{0,1, 2,3, 4, 5, 6, 7, 8, 9, 10, \ldots, 39, 40\}$

Teorema 1.2:

Sean a, $b \in \mathbb{Z}$. Si a, $b \notin \mathbb{Z}n$ haga a=a(Mod n) y b=b(Mod n) y en efecto, a, $b \in \mathbb{Z}n$.

1.9 Operaciones modulares

Sean $n \in \mathbb{Z}^+$ y a, $b \in \mathbb{Z}n$. Las operaciones modulares $\oplus$ y $\otimes$ se conocen como suma modular y multiplicación modular respectivamente; son diferentes de las que no tienen círculo (+ y *) y corresponden a las operaciones ordinarias, pero con módulo, así:

$$a \oplus b = (a+b) \text{ Mod } n$$
$$a \otimes b = (a*b) \text{ Mod } n$$

Ejemplo 1.11: Calcule para $\mathbb{Z}_{10}$ las operaciones indicadas

$5 \oplus 5 = (5+5)$ Mod 10=0
$9 \oplus 8 = (9+8)$ Mod 10=7
$3 \oplus 6 = (3+6)$ Mod 10=9
$5 \otimes 4 = (5*4)$ Mod 10=0
$6 \otimes 8 = (6*8)$ Mod 10=8
$7 \otimes 6 = (7*6)$ Mod 10=2

La división modular que se simboliza $\oslash$ tiene un tratamiento especial ya que su cálculo se realiza $a \otimes b^{-1}$, siendo b^{-1} el inverso modular (vea la definición inverso modular)

1.9.1 Inverso modular

Sea $n \in \mathbb{Z}^+$ y $a \in \mathbb{Z}n$. El inverso multiplicativo de a definido en $\mathbb{Z}n$ denotado por a^{-1} es un elemento $b \in \mathbb{Z}n$ tal que $a \otimes b = 1$, es decir, son todos aquellos elementos de $\mathbb{Z}n$ que son invertibles.

$\otimes$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8
2	0	2	4	6	8	**1**	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	5	**1**	5
5	0	5	**1**	6	2	7	3	8	4
6	0	6	3	0	5	3	0	6	3
7	0	7	5	3	**1**	8	6	4	2
8	0	8	7	6	5	4	3	2	**1**

Tabla 1.10: inversos modulares en $\mathbb{Z}_9$

Ejemplo 1.12: halle los inversos modulares a^{-1} en $\mathbb{Z}_9$, es decir, los elementos invertibles en $\mathbb{Z}_9$

Los valores de la tabla multiplicación modular se pueden ver en la tabla 8.10; ellos se calcularon aplicando las operaciones, así:

$$1\otimes 1=(1*1)\text{Mod } 9=1$$
$$2\otimes 5=(2*5)\text{Mod } 9=1$$
$$5\otimes 2=(5*2)\text{Mod } 9=1$$
$$7\otimes 4=(7*4)\text{Mod } 9=1$$
$$8\otimes 8=(8*8)\text{Mod } 9=1$$

$\Rightarrow$ En $\mathbb{Z}_9$, 1, 2, 4, 5, 7, 8 tienen respectivamente como inversos, a 1, 5, 7, 2, 4, 8 (vea en la tabla 1.10 los que tienen 1).

1.9.2 Técnicas para calcular invertibles en $\mathbb{Z}n$

Para calcular el invertible de $a\in\mathbb{Z}n$ debe determinarse primero si este existe. En efecto, puede utilizarse el algoritmo de Euclides definiendo que mcd(n,a)=1. Posteriormente se pasa a calcular dicho invertible, utilizando una de las siguientes técnicas:

Técnica 1 (por inspección): Sean $a\in\mathbb{Z}n$, $n\in\mathbb{Z}^+$ y supongamos que mcd(a,n)=1. Entonces hay dos enteros x e y tales que n**.**x+a**.**y=1.

Este enunciado indica que un número $a\in\mathbb{Z}n$ tiene inverso multiplicativo en $\mathbb{Z}n$, si es primo relativo con n. Entonces para hallar $a^{-1}\in\mathbb{Z}n$ proceda así:

Paso 1: determine la existencia de $a^{-1}\in\mathbb{Z}n$ verificando que mcd(n,a)=1. En caso contrario $a^{-1}\in\mathbb{Z}n$ no existe y ahí termina el proceso.

Paso 2: encuentre 2 números x, $y\in\mathbb{Z}$ tales que nx+ay=1

Paso 3: tome el menor entero entre x e y que llamaremos m; es decir, min(x,y)=m.

Paso 4: si $m\in\mathbb{Z}n$, entonces calcule $m\otimes a$ en $\mathbb{Z}n$. Si $m\otimes a=1$ entonces $m=a^{-1}$ en $\mathbb{Z}n$; en caso contrario, vuelva al paso 2.

Ejemplo 1.13: halle el invertible de 8 en Z_{45} con la técnica 1

Verifiquemos primero si 8^{-1} existe. En efecto, si mcd(45,8)=1 Veamos
45(-3)+8(17)=1,
Como $-3\notin\mathbb{Z}_{45}\Leftrightarrow -3+45\in Z_{45}=42\in Z_{45}$. Pero $42\otimes 8=1$? No, porque $42\neq 8^{-1}$
Calculemos otro par de enteros:
45(5)+8(-28)=1, $-28\notin\mathbb{Z}_{45}\Leftrightarrow -28+45\in Z_{45}=17\in Z_{45}$. Pero $17\otimes 8=1$? Si. Entonces, 8^{-1} existe y es igual a 17, porque 8*17(Mod45)=1.

Técnica 2: algoritmo de Euclides y la expresión de la forma n**.**x+a**.**y=1 con x, y$\in\mathbb{Z}$ y a$\in\mathbb{Z}$n. Entonces para hallar a$^{-1}\in\mathbb{Z}$n proceda así:

Paso 1: aplique el algoritmo de Euclides como en la sección 1.7.1, hasta que r_i =1

Si r_i =1 entonces a^{-1} existe en $\mathbb{Z}$n (sigue al paso 2); en caso contrario, a^{-1} no existe en $\mathbb{Z}$n y ahí terminará el proceso.

Paso 2: Haga sustituciones reiteradas de los valores r_i obtenidos al lado derecho de la implicación (en el paso anterior).

$1= r_{K-2} – q_{k-1}.r_{k-1}$
$= r_{K-2} – q_{k-1}.(r_{K-3} – q_{k-2}.r_{k-2})$ reduzca los términos semejantes (no efectúe los productos)
.
.
.
$= r_2 – q_3.r_3$
$= r_2 – q_3.(r_1 - q_2.r_2)$
$= -q_3.r_1 + q_3.(q_2.r_2+ r_2)$
$= -q_3.r_1 + q_3.(q_2+ 1).r_2$

Realice las sustituciones sucesivas hasta obtener una expresión de la forma n**.**x+a**.**y=1 con x, y$\in\mathbb{Z}$ que multiplican a los valores originales de n y a. Por consiguiente, el valor entero positivo de “x” o de “y” corresponderá a^{-1}.

Ejemplo 1.14: halle el invertible de 8 en Z_{45} con la técnica 2

45=5*8+5	$\Rightarrow$**5**=**45**-5***8**
8=1*5+3	$\Rightarrow$**3**=**8**-1***5**
5=1*3+2	$\Rightarrow$**2**=**5**-1***3**
3=1*2+1 **(observe 8^{-1} existe)**	$\Rightarrow$**1=3-1*2**

Entonces, puede expresarse 45x+8y=1. Ahora, reiteremos las sustituciones (dadas en negrita) en la última expresión obtenida al lado derecho de la implicación, para determinar que el valor entero positivo de x o de y, será el invertible. Veamos,

1=3-1***2**	
=3-1*(5-1*3)	ley de sustitución
=-1*5+2***3**	por ley distributiva y reducción de términos semejantes
=-1*5+2*(8-1*5)	ley de sustitución
=2*8-3***5**	por ley distributiva y reducción de términos semejantes
=2*8-3*(45-5*8)	ley de sustitución
=45*(-3)+8*17	por ley distributiva y reducción de términos semejantes

Puede notarse que esta expresión es de la forma 45**.**x+8**.**y=1, donde y=17. Por lo tanto, $17=8^{-1}$ en Z_{45}.

Ejemplo 1.15: determine si los números dados tienen invertible en la correspondiente base

a) 29 en Z_{431}
b) 4027 en Z_{146}
c) 17 en Z_{121} (como ejercicio)

Solución:
Primero deberá verificar si los 2 números (la base y el número) son primos relativos; efectivamente, podemos utilizar el algoritmo de Euclides de la sección 8.7. En efecto,

a) 431 Mod 29=25
29 Mod 25=4
25 Mod 4=1
4 Mod 1=0

$\Rightarrow$ 431 y 29 son números primos relativos, porque el mcd(431, 29)=1. Por lo tanto, existe el invertible de 29. Cuál es 29^{-1}?

b) 4027 Mod 146= 85
146 Mod 85= 61
85 Mod 61= 24
61 Mod 24= 13
24 Mod 13= 11
13 Mod 11= 2
11 Mod 2=1
2 Mod 1=0

$\Rightarrow$ 4027 y 146 son números primos relativos, porque el mcd(4027,146)=1. Por lo tanto, existe el invertible de 146. Cuál es 146^{-1}?

1.9.3 División modular

Sea $n \in Z^{+}$ y $b \in \mathrm{Zn}$ un elemento invertible. Sea $a \in \mathrm{Zn}$. Se define la división modular como $a \otimes b^{-1}$ y se denota $\oslash$**.** Por lo tanto, la división modular existe en Zn siempre que exista b^{-1} en Zn.

$$a \oslash b = a \otimes b^{-1} = (a * b^{-1}) \text{ Mod } n$$

Ejemplo 1.16: Calcule la división modular en Z_9 de:

$6 \oslash 5 = 6 \otimes 5^{-1} = (6*2)$ Mod 9= 3
$5 \oslash 8 = 5 \otimes 8^{-1} = (5*8)$ Mod 9= 4
$7 \oslash 4 = 7 \otimes 4^{-1} = (7*7)$ Mod 9= 4
$8 \oslash 6 = 8 \otimes 6^{-1} =$ no existe

Ejemplo 1.17: calcule a) $18 \oslash 5^{-1}$ en $\mathbb{Z}_{21}$ y b) $30 \oslash 8^{-1}$ en $\mathbb{Z}_{45}$

Para desarrollar este problema debemos verificar primero si tanto los números 21 y 5 como 45 y 8 son números primos relativos y, en efecto lo son.

Ahora, busquemos los dos enteros x e y tales que:

a) 21x+5y=1
En efecto, 21(1)+5(-4)=1, pero $-4 \notin \mathbb{Z}_{21}$. Sin embargo, calculando -4 Mod 21=17 determinaremos el inverso. Por lo tanto, 5^{-1}= 17 en $\mathbb{Z}_{21}$; así que 18*17(Mod 21)=**12**

b) 45x+8y=1
45(5)+8(-28)=1, pero como $-28 \notin \mathbb{Z}_{45}$ entonces calculamos -28 Mod 45 que es igual a 17 y corresponderá 8^{-1} en $\mathbb{Z}_{45}$ y por lo tanto, 8*17(Mod 45)=**1.** Por lo tanto**,** $30 \oslash 8^{-1}$=30*17(Mod45)=**15**

1.9.4 Raíz cuadrada en $\mathbb{Z}n$

Sea $a \in$ Zn; se dice que raíz cuadrada de a existe en Zn, si existe un numero $x \in Zn$ tal que $x^2 = x \otimes x = a$

En los números enteros ($\mathbb{Z}$), calcular la raíz cuadrada es supremamente fácil, solo basta con tener una calculadora de bolsillo para obtener el resultado. Pero si la raíz cuadrada que se quiere calcular es $\mathbb{Z}n$, cualquier calculadora no lo podría lograr. Es por tal razón que se requiere de un tratamiento especial para hacer ese cálculo, ya que si el número es de muchos dígitos de longitud, en la práctica sería bastante dispendioso su cálculo.

Existe una herramienta informática llamada Microsoft Excel que le podrá servir para hacer estos cálculos. En efecto, utilice la función "Residuo" (que es la operación módulo en Microsoft Excel) con los parámetros correspondientes como los presentados en la figura 8.1; de tal manera hallará las raíces del número (hasta el conjunto $\mathbb{Z}_{256}$). Basta con tomar fijo el valor de la columna ($Columna) y multiplicarlo por el valor fijo de la fila ($Fila) y la formula quedará así:

$Columna#Fila*#Columna$Fila

El divisor corresponderá a la base con la se trabajará. Para localizar esos números busque la intersección entre la fila x y la columna x (diagonal principal) en la cual $x^2 = x \otimes x =$ raíz del número. Observe en la tabla 8.10 que en $\mathbb{Z}_9$ $\sqrt{4}$ es 7 y que $\sqrt{7}$ son 5 y 4

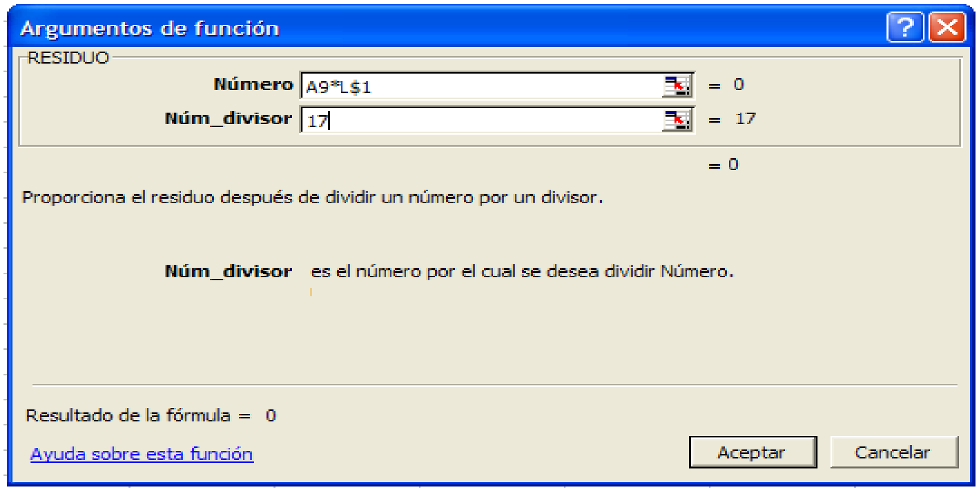


Figura 1.1: estructura de la función residuo en MS-Excel

Ejemplo 1.18: en $\mathbb{Z}_{12}$, $\sqrt{9}$ son: 3 y 9, similarmente $\sqrt{4}$ son 2, 4, 8 y 10.

El siguiente algoritmo permite determinar los divisores de un número entero. En efecto, utiliza un ciclo en el que su índice (que va desde mitad de n hasta 2) será un posible divisor, siempre que divida exactamente a n. Cada que halle un divisor lo muestra y guarda el cociente, que será un nuevo número para hallarle los divisores. La lista de divisores encontrados serán los divisores del número dado.

```
Print("ENTRE UN NUMERO ENTRE Y 65534 ")
read(n)
for i = n / 2 To 2, con incremento –1
{
    resto = n Mod i
    If resto = 0
    {
       aux = n / i
       if aux = 2 o (aux Mod 2 <> 0 y aux <> n y aux <> 1)
       {
            Print(aux)
       }
     }
}
```

1.9.5 Potencia en $\mathbb{Z}_n$

Realizar esta operación se tendrían que realizar muchas operaciones lo cual es un proceso demasiado tedioso. Sin embargo, aplicando la operación:

ab Mod n=((a Mod n)*(b Mod n))Mod n

se reduce el cálculo de manera notable.

Ejemplo 1.19: calcule 697^{31} en Z_{765}

En efecto, descomponga 31 en forma de sumas de potencias de 2, así: 31=16+8+4+2+1; ahora, calcule 479 elevada a esas potencias Mod 765. Por lo tanto, eleve al cuadrado esos resultados y multiplíquelos aplicando Mod 765.

697^2 Mod 765=485809 Mod 765=**34**
697^4 Mod 765=(697^2 Mod 765)*(697^2 Mod 765) Mod 765=34*34 Mod 765
=1156 Mod 765=**391**

697^8 Mod 765=(697^4 Mod 765)*(697^4 Mod 765) Mod 765
=391*391 Mod 765=152881 Mod 765=**646**

697^{16} Mod 765=(697^8 Mod 765)*(697^8 Mod 765) Mod 765
=646*646 Mod 765=417316 Mod 765=**391**
Por lo tanto,

697^{31} Mod 765= 697^{16}*697^8*697^4*697^2*697^1 Mod 765
= ((697* 34 Mod 765) * (391*646 Mod 765) * 391) Mod 765
= (748 *136 *391) Mod 765 =**238**

Ejemplo 1.20: diseñe un procedimiento que calcule a^n Mod z, con n un número entero grande arbitrario.
Variables de entrada: a, n, z
Variables de salida: exp= a^n Mod z

```
Procedimiento PotenciaModular (a, n, z)
{
        exp=1
        x= a Mod z
        Mientras (n>0) haga
        {
                Si (n Mod 2≠0) entonces
                        exp=exp*x Mod z
                Fin Si
                x=x*x Mod z
                n=n/2           //parte entera del cociente
        }
}
return (exp)
```

1.10 Congruencia de números

Johann Carl Friedrich Gauss (30 de abril de 1777 – 23 de febrero de 1855), fue un matemático, astrónomo y físico alemán, de alto reconocimiento universal por sus grandes aportes a las matemáticas y a la ciencia, particularmente a la teoría de números. Fue él quien dio la notación para describir que un número es residuo de la división de otros dos. Los trabajos de Gauss son muchísimos y han tenido y tienen una influencia muy grande prácticamente en casi la totalidad de las ramas de la Física y las Matemáticas (entre otros, Teoría de Números, Geometría Diferencial, Astronomía, Estadística, Magnetismo).

Después de 20 años en los que a penas había salido de Göttingen, en junio de 1854 salió para visitar la construcción del ferrocarril entre su ciudad. Los caballos se desbocaron y fue despedido fuera del carruaje sin tener daño alguno, pero si sufrió un fuerte "shock". A principios de 1855 comenzaron a aparecer los síntomas de su última enfermedad. Con dificultades, siguió trabajando hasta que murió el 23 de febrero de 1855.

Sean a, b $\in \mathbb{Z}$ y n>0. Entonces

$$a \equiv b(\text{Mod } n) \Leftrightarrow a \text{ Mod } n = b \text{ Mod } n$$

y se lee: "a es congruente con b módulo n sí y sólo sí a módulo n es igual b módulo n".

En efecto, $a \equiv b(\text{Mod } n)$ significa que a-b es divisible por n.

Ejemplo 1.21: $25 \equiv 16(\text{Mod } 9)$, porque 25(Mod 9)=16(Mod 9)=7. Por lo tanto, 25 y 16 son congruentes. Ahora, 149(Mod 15)=29(Mod 15)=14. En efecto, 149 y 29 son congruentes.

Observe si n es primo y $x \in \mathbb{Z}n$, entonces x tiene a los sumo dos raíces cuadradas en $\mathbb{Z}n$. Su demostración se puede ver en [Scheinerman].

Ejemplo 1.22: $\sqrt{12}$ en $\mathbb{Z}_{17}$ es ± 8. Para verificarlo, busque aquellos elementos $x \in \mathbb{Z}_{17}$ tales que $x^2 = x \otimes x = 12$. Observe, en este caso que $\sqrt{12}$ es ± 8, mas no es ± 3.4641...Como $-8 \notin \mathbb{Z}_{17}$ entonces se complementa a 12, es decir, 12-8=4. Por lo tanto la otra raíz es 4. Así que $\sqrt{12}$ en $\mathbb{Z}_{17}$ es 4 y 8.

De manera similar, ¿se puede hallar $\sqrt{10}$ en $\mathbb{Z}_{17}$? No, porque no existe un valor en $\mathbb{Z}_{17}$ que multiplicado por si mismo resulte 10. Compruébelo.

Teorema 1.3: raíces cuadradas en Zn

Sea n un número primo tal que $n \equiv 3(\text{Mod } 4)$. Si $x \in \mathbb{Z}n$ es un residuo cuadrático, entonces las raíces cuadradas de x en $\mathbb{Z}n$ son

$$(\pm x^{(n+1)/4}) \text{Mod } n$$

Vea su demostración en [Scheinerman]

Ejemplo 1.23: Como n=11 es primo y $11 \equiv 3(\text{Mod } 4)$; es decir, (11-3) es múltiplo de 4; entonces, en $\mathbb{Z}_{11}$ se tiene que:

$$\pm(9^{(11+1)/4} (\text{Mod } 11) = \pm 9^3 (\text{Mod } 11) = \pm 3.$$

Por lo tanto, las raíces cuadradas de 9 en $\mathbb{Z}_{11}$ son +3 y –3 (únicamente). Pero como $-3 \notin \mathbb{Z}_{11}$, entonces se complementa a 11; es decir, -3+11=8. Por consiguiente, las raíces cuadradas de 9 en $\mathbb{Z}_{11}$ son 3 y 8.

Si n no es número primo en $\mathbb{Z}_n$, entonces se puede proceder así:

- Factorice el número (el paso más complejo).
- Calcule las raíces cuadradas de cada factor primo del número en $\mathbb{Z}_p$ (con p como el respectivo factor primo y luego utilice en teorema 3).
- Aplique cuantas veces sea necesario el teorema del residuo a cada factor primo. Dichos resultados corresponderán a las raíces cuadradas de $x \in \mathbb{Z}_n$.

1.11 Teorema de Fermat

Sea a un número entero y p un número primo. Entonces

$$a^p \equiv a(\text{Mod } p)$$

Ejemplo 1.24: $32^{13} \equiv 32(\text{Mod } 13) = 6$

Teorema 1.4

Sean a y n enteros positivos. Si no es cierto que $a^n \equiv a(\text{Mod } n)$, entonces n no es primo.

Este teorema es una poderosa y excelente herramienta para demostrar que un número entero no es primo, sin tener que probar la factorización del número; es decir, demuestra la no primalidad de un número. Sin embargo, es importante tener en cuenta que este teorema no demuestra que un número dado sea primo.

Ejemplo 1.25: compruebe si 27, 29 y 4399 son números primos
$2^{27} \equiv 2 \text{ (Mod } 27) \Leftrightarrow 2^{27} \text{ (Mod } 27) \neq 2 \text{ (Mod } 27) \Rightarrow$ 27 no es número primo

Ahora, 29 es número primo, porque $2^{29} \equiv 2(\text{Mod } 29) \Leftrightarrow 2^{29}(\text{Mod } 29) = 2(\text{Mod } 29) = 2$

Sea n=4399, entonces, $2^{4399} \equiv 2(\text{Mod } 4399) \Leftrightarrow 2^{4399}(\text{Mod } 4399) \neq 2(\text{Mod } 4399) = 2$

En efecto, $4399 = 53 \text{x} 83 \Rightarrow$ 4399 no es número primo

1.12 Concepto de criptografía

La **criptografía** es un ejemplo de comunicación en la que se estudia mensajes secretos. La criptografía de clave pública mensajes consiste en crear una función de cifrado o encriptado y de descifrado o desencriptado para mensajes privados enviados entre dos personas, que no se ven entre y el medio de comunicación es inseguro. En el proceso de comunicación hay varios elementos: emisor, receptor, mensaje, código, clave y retroalimentación (respuesta).

Antiguamente, por ejemplo el militar y político Julio Cesar (Roma, 100 - 44 a. C.) enviaba mensajes secretos con clave en los que se cambiaban las letras por otra equivalente tres letras después, así: “a” por “d”, “b por “e”, “c” por “f” y así sucesivamente, “x” por “a”, “y” por “b”, “z” por “c”.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Figura 1.2: matriz de caracteres que codifica o encripta

Este proceso de cambio se conoce con el nombre de ***encriptación***.

Se conocen otros métodos de encriptación que consisten en mensajes matemáticos basados en el reemplazo por números enteros del 0 al 25, según la posición que ocupen en la lista de las letras de nuestro alfabeto, así:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figura 1.3: matriz de caracteres que encripta numéricamente

La ***desencriptación*** consiste en desarrollar un procedimiento que tenga como propiedad revelar el mensaje de quienes han establecido la comunicación con código secreto.

La encriptación de Julio Cesar estaba representada por la función f que asignaba un entero no negativo x menor o igual que 25, es decir, el entero

$$f(x)=(x+3) \text{ Mod } 26$$

Ahora, la idea es desarrollar un procedimiento secreto que tenga como propiedad, revelar un procedimiento, relativamente fácil de ejecutar, pero difícil de deshacerlo. En efecto, la función, que descifra un mensaje con a encriptación Julio Cesar es:

$$f^{-1}(x)=(x-3) \text{ Mod } 26$$

En general un mensaje escrito con solamente letras se encripta con la función

$$f(x)=(x+a) \text{ Mod } 26$$

y se desencripta o descifra con la función

$$f(x)=(x-a) \text{ Mod } 26$$

Ejemplo 1.26: el mensaje “bdu” equivale a “zar” y el mensaje “hv krud eyhqd” equivale a “es hora buena”.

Teorema 1.5
Sea $f(x)=(ax+b)$ Mod n con mcd(n,a)=1. Entonces, $g(y)=a^{-1}(y-b)$ Mod n, donde a^{-1} es el invertible de a Mod n.

Ejemplo 1.27: Dos interlocutores dialogan usando algunas letras del alfabeto, que ellos utilizan para cifrar y descifrar sus mensajes; si las letras que utilizan en su orden son: m, i, n, o, s, e, a, r, u (vea tabla 1.11) y los mensajes han sido cifrados mediante la función y=(7x+10) Mod 9, donde x corresponde a la posición de la letra, entonces la palabra correspondiente al mensaje “RISN” es ¿“AMOR” o “AMOS”?

En efecto es AMOS; basta con hallar la función que descifra y que en este caso es x=4(y-10) Mod 9 según el teorema 5 y la tabla 1.10 de la sección 1.14.1 (que calcula los invertibles).

Con la función dada, la palabra que encripta a “MINERO” es “IUAMOS”.

0	1	2	3	4	5	6	7	8
M	I	N	O	S	E	A	R	U

Tabla 1.12 ejemplo 1.27

AUTOEVALUACION 1

SELECCIÓN MÚLTIPLE DE MÚLTIPLE RESPUESTA

Resuelva el siguiente problema seleccionando la respuesta correcta según las siguientes situaciones:

A) Si 1 y 2 son correctas
B) Si 2 y 3 son correctas
C) Si 3 y 4 son correctas
D) Si 2 y 4 son correctas
E) Si 1 y 3 son correctas

$25 \equiv b(\text{Mod } n)$, si

1. n = 9 y b = 16 Respuesta: ____
2. n = 21 y b = 23
3. n = 13 y b =12
4. n = 9 y b = 12

2. Calcule (si existe) una de las raíces de: $\sqrt{(-13) \oplus 697^{31}}$ en Z_{765}

A) 35 B) 45 C) 28 D) 39

3. calcule el valor de $2 \otimes (5 \oslash 8)$ en Z_{45}

A) 25 B) 22 C) 15 D) 20

4. $(7 \oplus 39 \otimes (-108))^{-1}$ en Z_{84}

A) 34 B) 45 C) 56 D) 67

TALLER 1

b) Dado que a, b, q, r son enteros con b, c números positivos, se tiene que $a=bq+r$, con $0\leq r<b$, calcule los valores de x e y, dado que los valores de a y b son:

1.1 a=228, b=177
1.2 a= -228, b=177
1.3 a= 77, b=5
1.4 a=-77, b=5
1.5 a=23, b=10
1.6 a= -23, b=10

2 Dados los valores de a y b del numeral 1, calcule a Div b, a Mod b

3 Halle el mcd de los siguientes números, determinando cuáles son primos relativos:

1.1 34, 51,68
1.2 45, 64, 72
1.3 124, 98, 218
1.4 45, 64, 78, 234

4 Demuestre o refute que para valores a, b, c que el

$$mcd(a,b,c)=mcd(a, mcd(b,c))$$

5 Siendo d un entero positivo y mcd(a,b,c)=d es el número más pequeño de la forma $ax+by+cz$ con x, y, z número entero.

6 Haga un programa en cualquier lenguaje de programación que muestre de una tabla los valores de $ax+by$ con x e y entre -4 y 4 con a =30 y b =24. Se sabe que el menor valor de la tabla es el mcd(a,b) con a y b diferentes de cero. El programa debe mostrar el mcd.

7 Determine los enteros x, y, z tales que $6x+10y+15z=1$

8 Implemente el algoritmo que calcule el mcd para 3 números enteros.

9 Implemente el algoritmo que calcule el mcd para cualquier cantidad de números enteros.

10 Dados los números con gran cantidad de cifras, digamos de 1000 dígitos, ¿cuántas divisiones tendrían que realizarse para hallar el mcd?

11 Implemente un programa en cualquier lenguaje de programación para el Algoritmo de Euclides.

12 Implemente el algoritmo de Euclides recursivo para hallar mcd en cualquier lenguaje elegido por el lector.

13 Haga un programa que determine si un número es o no primo

14 Haga un programa que dado una lista de números, verifique si los números son o no primos relativos

15 Implemente un programa en cualquier lenguaje de programación para que determine los inversos multiplicativos de un número en Z_n, con n definido por el usuario.

16 Para Z_{10}, Z_9, Z_8 calcule lo siguiente:

8.1 $4 \oplus 4$
8.2 $7 \oplus 3$
8.3 $4 \otimes 3$
8.4 $7 \oslash 8$
8.5 $8 \oslash 7$

17 Escriba el proceso para calcular el valor de las operaciones indicadas (si existen) o ponga el mensaje de no existencia:

1. Calcule en Z_{72} las raíces cuadradas de: 0, 1, 4, 9, 16, 25, 36, 49, 64, 28, 40, 52, 53 y 70.
2. Calcule: $\sqrt{121}$ en Z_{1411} y $\sqrt{900}$ en Z_{2717} (si existen).
3. 29^{-1} en Z_{431}
4. 146^{-1} en Z_{4027}
5. $2 \otimes (5 \oslash 8)$ en Z_{45} R/. 35
6. $\sqrt{(-13) \oplus 697^{31}}$ en Z_{765} R/. 15
7. $2 \oslash 13^{-1}$ en Z_{45} R/. 26
8. $(-1238) \oslash 13^{-1}$ en Z_{145} R/. 139
9. $97^{15} \oslash \sqrt{-152}$ en Z_{72} R/. no existe
10. Para Z_{10}, Z_9, Z_8 calcule lo siguiente:
a. $(4 \oplus 4) \otimes (5 \oplus 4)$
b. $(7 \oplus 3) \otimes 72$
c. $(8 \otimes 3) \oslash (35)$
d. $11 \otimes (7 \oslash 8)$
e. $(8 \oslash 7) \oplus (27)$

c) Calcule el valor de x en los siguientes casos:
1. Si $\sqrt{x} = 9$ en Z_{12}
2. Si $\sqrt{x} = 23$ en Z_{31}

d) Calcule el valor de n en los siguientes casos:
1. Si $\sqrt{3} = 4$ en Z_n
2. Si $\sqrt{36} = 66$ en Z_n

Nota: utilice la definición de congruencia $\sqrt{x} = a$ en $Z_n \Leftrightarrow a^2$(Mod n)=x donde $x=a^2 - n$.

e) ANALISIS DE RELACIÓN

En los numerales 20.1 hasta 20.5, seleccione la opción correcta, así:

1. Si la afirmación y la razón son VERDADERAS y la razón es una explicación CORRECTA de la afirmación
2. Si la afirmación y la razón son VERDADERAS, pero la razón NO es una explicación CORRECTA de la afirmación
3. Si la afirmación es VERDADERA, pero la razón es una proposición FALSA
4. Si la afirmación es FALSA, pero la razón es una proposición VERDADERA
5. Si tanto la afirmación como la razón son proposiciones FALSAS

18.1 Si a= -89 y b= -98, entonces a y b son primos relativos PORQUE el mcd(-89, -98) =1 Respuesta: ____

18.2 En Z_5, $a \otimes b^{-1}=2$ con a = 3 y b = 4 PORQUE $3 \otimes 4=2$ Respuesta: B

18.3 En Z_9, $a \oslash b^{-1}=1$ con a = 3 y b = 4 PORQUE 7 es el invertible de 4 en $\mathbf{Z}_9$ y, $4 \otimes 7=1$ Respuesta: A

18.4 $17 \equiv b$ (Mod n) $\Leftrightarrow$ 17 (Mod n)= b (Mod n) PORQUE (17-b) es múltiplo de n. Respuesta: A

18.5 $\sqrt{4}$ en $\mathbb{Z}_9$ es 2 PORQUE $x^2=x \otimes x=2$ en $\mathbb{Z}_9$ Respuesta: E

19. Utilizando la tabla 1.12 del ejemplo 1.45, se quiere enviar un mensaje con las palabras: SERRANA, MARRANO, RAMONA, entonces ¿cuales deben ser las palabras encriptadas, respectivamente?

20. Utilizando las letras de la Tabla 1.13, para cifrar la frase “EL ROTA A ROMA”. Utilice el teorema 5

0	1	2	3	4	5	6	7	8
R	O	M	A	Y	T	E	L	U

Tabla 1.13 ejercicio 21

21. Con las letras: D, E, I, L, N, O, R, utilice el teorema 5 para encriptar las siguientes expresiones:
    - RINDELO
    - NO DE EL DINERO

22. Dos personas A y B establecen una comunicación con clave que consiste en cambiar las letras incluyendo el espacio en blanco. La clave entre estas personas es: "cambiar una letra del alfabeto por otra ubicada en las 5 siguientes, teniendo en cuenta que el espacio en blanco es un carácter que está en la última posición de la lista", Encripte los siguientes mensajes, utilizando la función f(x)=(7x+10) Mod 27 y las letras de nuestro alfabeto
   f) un zar
   g) es un buen momento
   h) en hora buena supo partir

Aplicación en computación

23. Haga un programa en un lenguaje de programación cualquiera que presente lo siguiente:
    23.1 Un menú con las distintas opciones para el usuario
    23.2 Los pantallazos para entrar los datos tales como la base modular, el número para calcular la raíz cuadrada modular, los cuadrados perfectos modulares y el exponente del número para la potencia modular.

a	b	c	d	e	f	g	h	i	j
k	l	m	n	o	p	q	r	s	t
u	v	w	x	y	z	á	é	í	ó
ú	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	Á	É	Í
Ó	Ú	1	2	3	4	5	6	7	8
9	0	+	-	*	/	^	%	#	$
@	SP	,	;	.	:	¿	?	¡	!
_	(	)	[	]	{	}	ü	Ü	ñ
Ñ									

Tabla 1.14: matriz de caracteres con "SP" carácter en blanco

    23.3 El programa debe mostrar los siguientes listados: los inversos multiplicativos modulares (si existen), las raíces cuadradas modulares y el listado de los cuadrados perfectos modulares (si existen) y el valor de la potencia modular.

    23.4 Según la tabla 1.14 que contiene los caracteres básicos para escribir un texto común y corriente los cuales van enumerados del 0 al 100 y que respectivamente van desde "a" hasta "Ü".

Resuelva lo anterior, dado que la función de cifrado es una de las siguientes:

a) f(x)=(5x -10) Mod n
b) f(x)=(17x -14) Mod n
c) f(x)=(7x $\oplus$ 13) Mod n
d) f(x)=(7x +10) Mod n
e) f(x)=(17x $\oplus$ 14) Mod n
f) f(x)=(17x $\oplus$ (-14)) Mod n
g) f(x)=(53x $\oplus$ (-37)) Mod n
h) f(x)=(23x $\oplus$ 30)) Mod n

23.5 Tome una de las funciones dadas y halle la función que descifra el mensaje enviado con esa función.

23.6 Cifre y descifre un mensaje enviado por un interlocutor usando una función de la forma ax+b donde a y b se generen aleatoriamente, siendo x la posición de uno de los caracteres dados en la tabla 1.14.

23.7 Haga un programa que establezca una comunicación inalámbrica o por puerto serial entre dos PC y almacene los mensajes en una base de datos (por ejemplo, en Microsoft Access). Intente proceder así:

- Conecte dos computadores por el puerto serial mediante un NULL MODEM.
- Envíe de un computador a otro, un mensaje cifrado o encriptado en binario. El computador receptor del mensaje debe recibirlo encriptado y debe descifrarlo; pero además, debe mostrar tanto el mensaje cifrado como el descifrado.
- Para al almacenar el mensaje en la base de datos utilice un campo que almacene el mensaje cifrado y otro campo para el mensaje descifrado.