ESCUELA SUPERIOR
POLITECNICA DEL LITORAL

INSTITUTO DE CIENCIAS MATEMATICAS

TUTORIAL DE ARITMETICA MODULAR
CICLO DIVERSIFICADO

MONOGRAFIA PREVIA A LA OBTENCION DEL TITULO DE:

MAGISTER EN EDUCACION MATEMATICA APLICADA AL NIVEL MEDIO

POR: TERESA L COSTALES PESANTES

GUAYAQUIL, Marzo - 1994

DECLARACION EXPRESA

La responsabilidad por los hechos, ideas y doctrinas expuestos en esta monografía, me corresponden exclusivamente; y el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".

(Reglamento de Exámenes y Títulos profesionales de la ESPOL).

....

Nombre y firma del autor

AGRADECIMIENTO

Expreso mi profundo agradecimiento al Lic. Mauro Ordóñez Bravo, Rector del Colegio Nacional "Hipatia Cárdenas", a los distiguidos profesores del INSTITUTO DE CIENCIAS MATEMATICAS de la ESPOL y, en forma especial a la Ing. Margarita Martínez en su calidad de directora de esta monografía.

Dedicado a

mi sobrino Diego Paul

INDICE DE ABREVIATURAS

gebra abstracta	
illo	<R,+,.>
ıpo	<G,+>
eración binaria	*
ase de equivalencia b	[b]
njuntos	
njunto vacío	{ }
njunto de números enteros	Z
njunto de números naturales	N
njunto de números no negativos	Z+
njunto de números racionales	Q
njunto de números reales	R
njunto {0, 1, 2 ,..., n-1}, n∈N	Z_n
nciones y relaciones	
nción	Φ
lación de equivalencia	Γ
gica	
es divisible entre c	c|b
ra todo	∀
rtenece a	∈
... entonces	⟹

INDICE GENERAL

INTRODUCCION

interés en realizar un programa tutorial radica en las
uientes consideraciones:

instrucción que utiliza recursos tecnológicos microelec-
nicos puede ensayarse y revisarse muchas veces, con
ativa facilidad, antes de ser "aplicada" en un proceso
enseñanza, y aún entonces, según sean los recursos, se
de realizar ajustes. Esta oportunidad de someter a
eba una serie didáctica, hasta que la <u>respuesta de los
mnos</u> garantice su validez, es una manera vigorosa de
jar una teoría de la instrucción que posteriormente
ere un autentico paradigma educativo.

un sistema con instrucción programada, los maestros
pliremos dos papeles fundamentales, uno nuevo, y otro ya
ocido, pero a veces mal llevado en la práctica. El nuevo
sistirá en preparar materiales para las máquinas:
gramas, lecciones televisadas, exhibiciones filmadas,
eriales ilustrativos audiovisuales, demostraciones e
trumentos de evaluación. El otro papel del maestro será
er lo que una máquina nunca podrá realizar, aconsejar,
entar a los alumnos hacia aquellas funciones intelectua-
de orden superior, analizar, criticar, sintetizar,
orar, crear, que son las metas primarias de la educa-
n. El maestro ya no necesitará seguir siendo el provee-

r de información, ni siquiera de desarrollar destrezas y mprensiones fundamentales. Cuando se encuentre con los umnos en los cursos formales, estarán preparados juntos ra tratar los aspectos más complejos, intrincados y safiantes de una materia y el número de tales reuniones rmales necesarias se reducirá grandemente. Así, tendrá empo para las reuniones informales con los estudiantes e lo "requieran" y para sus "propias investigaciones".

cuanto al tema ARITMETICA MODULAR, considero que debería r incluído en el contenido programático del nivel medio, que constituye un aporte fundamental en la teoría de meros. Su estudio permite un importante entrenamiento en s demostraciones matemáticas que, siendo un campo de perimentación de la imaginación, garantizan el desarrollo facultades intelectuales como ser la abstracción y la eatividad, que en todos los tiempos han sido las genera-ras de grandes realizaciones individuales y sociales.

nalmente, para ubicar en forma adecuada a este programa, continuación describo brevemente los tres niveles de teracción **alumno-computador** desarrollados en el campo de enseñanza asistida por computador:

vel 1: **"ejercicios y práctica"**. La noción correspondiente debe haber sido explicada por el profesor y el alumno ya realizado en clase algunos ejercicios. Se plantean ferentes problemas para diferentes alumnos según resulta-s previos.

ivel 2: **"programas tutoriales"**. Tienen la finalidad rincipal de entrenar a los alumnos en las "primeras ategorías" del area cognoscitiva, en base a una unidad idáctica. El profesor conocerá oportunamente del avance de odos los estudiantes mediante un registro de las respues- as a los cuestionarios propuestos para el alumno en el esarrollo del programa tutorial y, seguirá siendo el esponsable de ayudar en forma "individual" o en pequeños rupos a los estudiantes que no avancen suficientemente con l programa. Posteriormente, con el grupo que haya desarro- lado las destrezas y comprensiones fundamentales continua- á en etapas más avanzadas de su formación.

ivel 3: **"diálogo y autoprogramación"**. Sistemas que ermiten un auténtico diálogo entre los estudiantes y el rograma, así como el automejoramiento del programa. Ya xisten prototipos muy aceptables de estos sistemas, la ptimización depende tanto de la tecnología como de la ntroducción de técnicas de inteligencia artificial.

e las descripciones anteriores puedo ubicar a este rograma en el nivel 2 de la enseñanza asistida por omputador.

n los tres primeros capítulos se presenta el material eórico que se pretende enseñar con el programa tutorial, as no el desarrollo metodológico del mismo y finalmente, Capítulo 4 describe las instrucciones para el usuario.

CAPITULO 1

LECCIONES DE ARITMETICA MODULAR

ta es la primera opción del MENU PRINCIPAL del programa torial, consta de cinco subopciones numeradas aquí como 1., 1.2., 1.3., 1.4., 1.5.

s palabras señaladas con un símbolo #, constan en el ccionario del programa y por tanto pueden ser consultadas r el alumno desde la pantalla correspondiente o desde el NU PRINCIPAL. Ejemplos: Grupo#, primo#.

s preguntas dentro de un recuadro, son dirigidas al ctor.

1. NOCIONES PRELIMINARES

aritmética modular es un sistema con características rticulares muy interesantes, es aplicable cuando los ontecimientos se repiten de manera cíclica:

s horas del día, los días de la semana, la medida de los gulos, etc.

USTRACION 1: (El ciclo 0-6 de 7 días)

pongamos numerados los días de la semana de 0 a 6, comenndo por el Domingo. Si se continúa numerando, el día 7 es ningo otra vez, Lunes el 8, Martes el 9,...

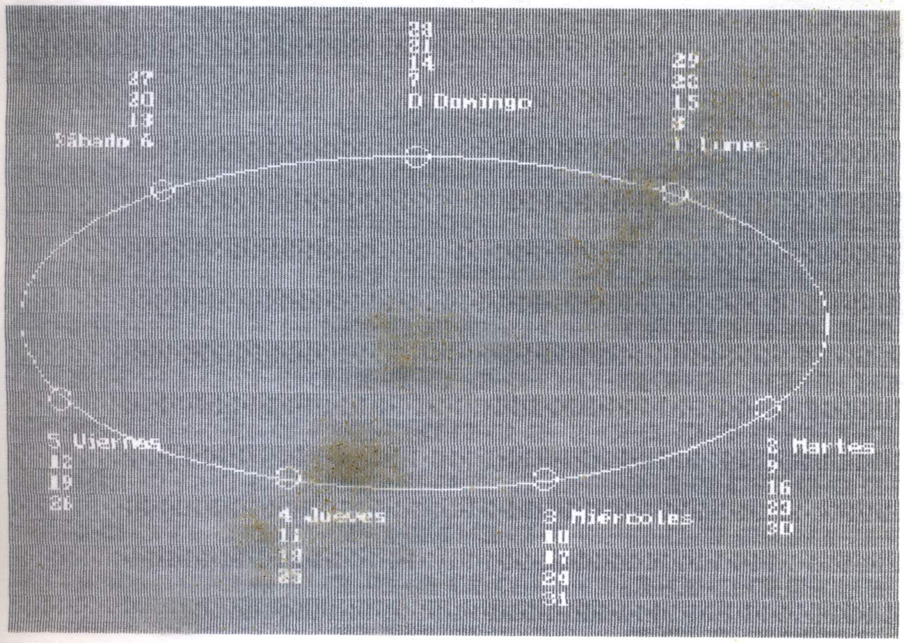


figura 1.1

cierto sentido se puede decir que 7=0, 8=1, 9=2,... don- por cierto, "=" no tiene el mismo significado usual.

bién se puede retroceder, así, el día -1 es el día erior al Domingo, que es el Sábado, luego -1=6; de igual era, -2=5. (ver figura 1.1.)

el sistema de los números enteros se enrolla entonces orno al círculo de los días, más o menos como se puede ervar en la figura 1.2.

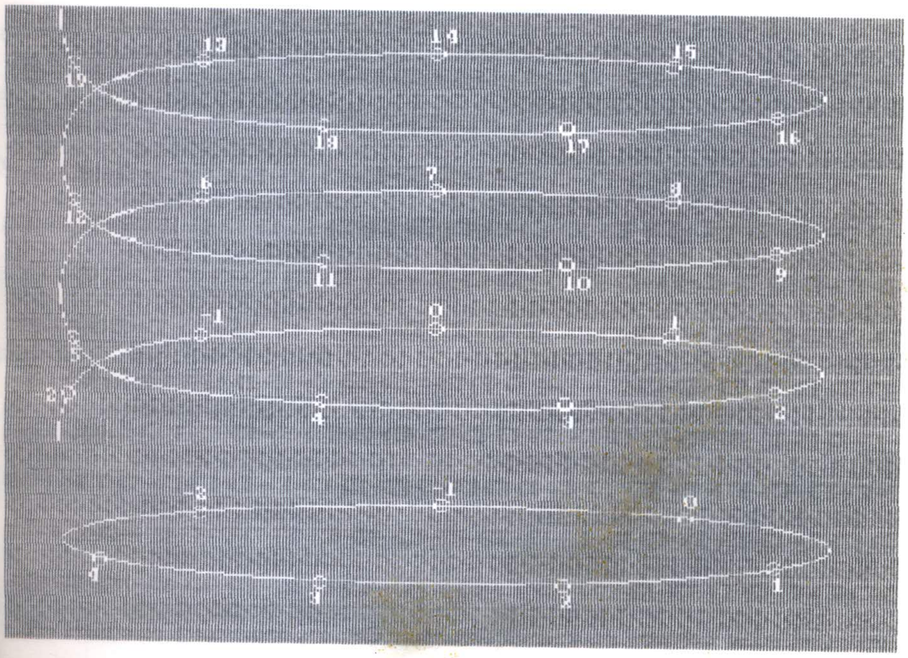


figura 1.2.

nces, se puede establecer un criterio general para iguar qué números caen en qué días de la semana:

mingo:

.,-14, -7, 0, 7, 14,...es decir los días de la forma 7n

nes :

.,-13, -6, 1, 8, 15,...es decir los días de la forma 7n+1

rtes :

.,-12, -5, 2, 9, 16,...es decir los días de la forma 7n+2

ércoles:

.,-11, -4, 3, 10, 17,..es decir los días de la forma 7n+3

eves :

.,-10, -3, 4, 11, 18,..es decir los días de la forma 7n+4

ernes :

.,-9, -2, 5, 12, 19,...es decir los días de la forma 7n+5

bado :

.,-8, -1, 6, 13, 20,...es decir los días de la forma 7n+6

s números de la forma 7n+7 son, naturalmente, iguales a 1 + 1) y, por consiguiente, de la forma 7n.

día correspondiente a un número dado está determinado el resto de dividir dicho número por 7. Los restos de es divisiones son siempre 0, 1, 2, 3, 4, 5, 6.

a referirnos a este conjunto de restos usaremos la ación Z_7, de modo que

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

realizamos un cierto tipo de "aritmética de restos" y venimos que una afirmación tal como

$$4 + 5 = 2$$

ebe interpretarse como "el cuarto día de la semana más 5 ías es el segundo día de la semana", lo que es completa- ente natural.

demos construir una tabla de sumar para los "números" 6, así:

Tabla I

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

ESTA TABLA COMPRENDE LA ESENCIA DEL CICLO DE 7 DIAS

nos preguntamos ¿ Cuál es el día 751 después del eves?, podríamos replantear la pregunta así:

$$4 + 751 = ?$$

1 no está en la Tabla I pero puede ser expresado así,

$$751 = 7x107 + 2$$

e es de la forma 7n + 2, luego,

$$751 = 2$$

ora lo que debemos determinar es

$$4 + 2 = ?$$

irando la Tabla I, la respuesta es ?=6, que es sábado.

?ara el lector:
¿Qué día de la semana será 440 días después de un Sá -
bado?

ervemos, algunos propiedades muy importantes que se
plen en esta Tabla I:

Al sumar un elememto a de Z_7 con cualquier elemento b de Z_7, el resultado es **siempre** algún elemento c de Z_7.

Ejemplos:

$3 + 4 = 0, \qquad 0 \in Z_7$

$6 + 5 = 4, \qquad 4 \in Z_7$

$2 + 6 = 1, \qquad 1 \in Z_7$

Esto es, se cumple la propiedad de cerradura, por tanto, la suma en Z_7 es una operación binaria[#].

Si se suma 3 elementos a, b, c, cualesquiera de Z_7, se cumple que:

$$a + (b + c) = (a + b) + c$$

Ejemplo:

$$3 + (4 + 2) = (3 + 4) + 2$$

$$3 + 6 = 7 + 2$$

$$9 = 9$$

Esto es, se cumple la propiedad asociativa.

Si se suma el número 0 con cualquier elemento b de Z_7, el resultado es **siempre** b.

Ejemplos: $\qquad 0 + 5 = 5$

$\qquad 0 + 1 = 1$

Por tanto, <u>0 es elemento neutro</u> de la suma en Z_7.

Para cada elemento b de Z_7, hay algún elemento b'

de Z_7 tal que,

$$b + b' = 0$$

Ejemplos:

$$3 + 4 = 0$$

$$2 + 5 = 0$$

$$6 + 1 = 0$$

<u>El elemento b' es el inverso aditivo de b.</u>

las propiedades (1), (2), (3) y (4) que acabamos de lizar podemos concluir que Z_7 junto con la operación aria suma es un Grupo‡. Expresamos este hecho con la ación $<Z_7,+>$.

Observemos también que al sumar cualquier elemento **a** de Z_7 con cualquier otro elemento **b** de Z_7 se cumple que:

$$a + b = b + a$$

Ejemplos:

$$3 + 4 = 4 + 3 = 7$$

$$6 + 4 = 4 + 6 = 3$$

Entonces, la suma en Z_7 es conmutativa y por tanto $<Z_7, +>$ es Grupo Abeliano‡.

Si se suma al menos 7 veces consigo mismo algunos elementos de Z_7 (excepto el cero), se obtienen TODOS los elementos de Z_7

Ejemplo:

$$3 + 3 = 6$$

$$6 + 3 = 2$$

$$2 + 3 = 5$$

$$5 + 3 = 1$$

$$1 + 3 = 4$$

$$4 + 3 = 0$$

$$0 + 3 = 3$$

onces, $<Z_7, +>$ es un GRUPO CICLICO#.

los los elementos de Z_7, excepto el 0 son ELEMENTO IERADOR# de Z_7.

ora, definamos <u>una multiplicación</u> para este sistema, ique, la interpretación de esta operación en los días de semana no tiene mayor sentido, podríamos aplicar para os casos en Z_7.

sentido adecuado a la operación 3 x 6 debería ser 6 + 6 5 y para la operación 6x3 debería ser 3+3+3+3+3+3 si amos en la Tabla I, en el primer caso la respuesta es 4 n el segundo caso la respuesta también es 4, de esta era se define 3 x 6 = 4.

o 3=10=-4 por ser de la forma 7n+3, entonces, 3x6 ería ser igual a: 10x6=-4x6, lo cual en efecto, es cierto que 60=-24=4 y 4, 60 y -24 son de la forma 7n+4. Por to los resultados son consistentes.

iante el uso repetido de la adición podemos construir la uiente tabla de multiplicar.

Tabla II

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

alicemos qué propiedades se cumplen en esta Tabla II:

) Al multiplicar un elememto a de Z_7 con cualquier elemento c de Z_7, el resultado es **siempre** algún elemento c de Z_7.

Ejemplos:

$3 \times 4 = 5, \qquad 5 \in Z_7$

$6 \times 5 = 2, \qquad 2 \in Z_7$

$2 \times 6 = 5, \qquad 5 \in Z_7$

Esto es, se cumple la propiedad de cerradura, por tanto, la multiplicación en Z_7 es una operación binaria‡.

) Si se multiplica 3 elementos a, b, c, cualesquiera de Z_7, se cumple que:

$$a \times (b \times c) = (a \times b) \times c$$

Ejemplo:

$$3 \times (4 \times 2) = (3 \times 4) \times 2$$

$$3 \times 1 = 5 \times 2$$

$$3 = 3$$

Esto es, se cumple la propiedad asociativa.

) Si se multiplica el número 1 con cualquier elemento b de Z_7, el resultado es **siempre** b.

Ejemplos: $1 \times 5 = 5$

$1 \times 1 = 1$

Por tanto, <u>1 es elemento neutro</u> de la multiplicación en Z_7.

Para cada elemento b de Z_7, hay algún elemento b' de Z_7 tal que,

$$b \times b' = 1$$

Ejemplos: $3 \times 5 = 1$

$2 \times 4 = 1$

$6 \times 6 = 1$

<u>El elemento b' es el inverso multiplicativo de b.</u>

las propiedades (1), (2), (3) y (4) que acabamos de lizar podemos concluir que Z_7 junto con la operación aria multiplicación es un Grupo[#]. Expresamos este hecho la notación $<Z_7, .>$.

Observemos también que al multiplicar cualquier elemento **a** de Z_7 con cualquier otro elemento **b** de Z_7 se cumple que:

$$a \times b = b \times a$$

Ejemplos:

$$3 \times 4 = 4 \times 3 = 5$$

$$6 \times 4 = 4 \times 6 = 3$$

Entonces, la multiplicación en Z_7 es conmutativa y por tanto $<Z_7, .>$ es Grupo Abeliano[#].

No existe algún elemento de Z_7 que al ser multiplicado por sí mismo al menos 7 veces, se obtenga TODOS los elementos de Z_7.

Ejemplos

(a) con 3:

$$3 \times 3 = 2$$
$$2 \times 3 = 6$$
$$6 \times 3 = 4$$
$$4 \times 3 = 5$$
$$5 \times 3 = 1$$
$$1 \times 3 = 3$$
$$3 \times 3 = 2$$

En ningún caso se generó el 0.

(b) Con 1:

$$1 \times 1 = 1$$
$$1 \times 1 = 1$$
$$\ldots$$
$$1 \times 1 = 1$$

Sólo se genera el 1.

gún elemento de Z_7, es un ELEMENTO GENERADOR# de Z_7.

onces, <Z_7, .> NO es un GRUPO CICLICO#.

No existen en Z_7 2 elementos a y b diferentes de 0, tales que,

$$a \times b = 0$$

RECUERDE esta propiedad, es muy importante cuando analicemos la estructura de anillo#. ∎

<u>números en el conjunto Z_7, junto con las dos tablas struidas, que definen dos operaciones binarias en Z_7, es</u>

l sistema de enteros módulo 7.

n general, cualquier número natural puede servir de ódulo, por ejemplo, en la siguiente Ilustración como el iclo es 0-23, el módulo es 24 que lo notaremos con Z_{24}.

$$Z_{24}=\{0,\ 1,\ 2,\ldots,\ 23\}$$

LUSTRACION 2. (Aritmética del reloj, EL CICLO 0-23)

n un reloj de 24 horas, supongamos que son las 09h00, he- os desayunado hace 2 horas y dentro de 4 horas tendremos na reunión en el Club ABC. Que podemos también decirlo sí: - hemos desayunado a las 07h00,

- a las 13h00 tendremos una reunión en el Club ABC

n realidad lo que hemos realizado es una suma y una resta horas, así:

$$9 - 2 = 7$$

$$9 + 4 = 13$$

ero, si los valores obtenidos están fuera del ciclo 0-23 oras, entonces la hora obtenida corresponde a próximas uelta(s) del reloj o a vuelta(s) anteriores, en estos asos, debemos expresar las horas como el residuo de ividir dicha hora para 24. Por ejemplo, 34 horas equivale las 10h00 porque 34 = 24 + 10.

Si son las 10h00, ¿qué hora será luego de 34 horas?

, al igual que en la Ilustración I se puede elaborar las
ablas de sumar y de multiplicar para Z_{24}.
n la suma se cumplen todas las propiedades analizadas para
, por lo tanto, <Z_{24}, +> SI ES GRUPO CICLICO#

Dejamos al lector verificar si <Z_{24}, .> es GRUPO CICLICO

a propiedad (7) analizada en Z_7, si se cumple en Z_{24}.

7) Si existen en Z_{24} 2 elementos a y b diferentes de 0, tales que,

$$a \times b = 0$$

jemplos

$$2 \times 12 = 0$$

$$3 \times 8 = 0$$

os números en el conjunto Z_{24}, junto con las tablas de
umar y de multiplicar, que definen 2 operaciones binarias
n Z_{24}, es **el sistema de enteros módulo 24.**

n general, <u>los números en el conjunto Z_m, junto con las
ablas de sumar y de multiplicar, que definen 2 operaciones
inarias en Z_m, es el sistema de enteros módulo m. Siendo
un número natural.</u>

*¿Podríamos aplicar los procedimientos utilizados en la aritmética del reloj, **en la medida de los ángulos**?*

DEFINICIONES Y PROPIEDADES BASICAS

1801, el matemático **GAUSS**, reconocido como uno de los s matemáticos más grandes en la Historia de la Matemáti- introdujo en su publicación DISQUISITIONES ARITHMETICAE revolucionaria noción, la de **CONGRUENCIA**.

sección que abre el tratado de Gauss, comienza así:

la diferencia (a-b) o (b-a) de dos números enteros a,b exáctamente divisible por el número m, decimos que a,b congruentes en relación al módulo m, o simplemente con- entes módulo m y lo simbolizamos escribiendo

$$a \equiv b (\mathrm{mod}\ m)."$$

INICION 1.1.

n h,k,s ∈ Z y, m ∈ N. Se define h congruente con k ulo m, lo cual se denota h ≡ k (mod m), si y solo si h-k divisible entre m, es decir, h-k=sm para alguna s ∈ Z.∎

relación de congruencia expresada en la definición 1.1. equivalente a $h = k + sm$

, 100 ≡ 2 (mod 7) porque 100-2=98 que es divisible entre ambién -2 ≡ 7(mod 9) porque -2-7 = -9 que es divisible re 9 5315 ≡ 315 (mod 100) porque 5315-315 = 5000 que es isible entre 100.

a enlazar esta definición con lo que acabamos de udiar, consideremos la congruencia módulo 7. Si h y k congruentes módulo 7, existe entonces un entero s tal e h-k = 7s o bien h = 7s + k.

 pues los números congruentes con un número dado k son, ecisamente, los de la forma 7s + k. Los números congruens con 1 mod 7 son los de la forma 7s + 1.

lo un número cualquiera se le puede dividir entre 7 y contrar su resto r, de manera que

$$h = 7q + r$$

 lo que se sigue que h es congruente con r (mod 7). Como chos restos sólo pueden tomar valores comprendidos entre s números 0 y 6, se llega a que todo número es congruente od 7) con alguno de los números 0, 1, 2, 3, 4, 5, 6.

 la figura 1.1. los números que están en la columna del a 0, domingo, son aquellos cuya forma es 7n;esto es, los e son congruentes con 0, los números que están en la lumna del lunes son aquellos que son congruentes con 1. general, los números que están en la columna del día d n todos los números congruentes con d.

FINICION 1.2.

an C un subconjunto[#] de Z y, m∈N. C es un sistema completo residuos módulo m si y sólo si cada entero es congruente uno y sólo uno de los elementos del conjunto C. ∎

emplos:

El conjunto {0, 1,2, ..., m-1} es un sistema completo de residuos módulo m para cualquier m∈N.

{0, 1, 2, 3, 4} es un sistema completo de residuos módulo 5

{0, 1, 12, -2, 4} es un sistema completo de residuos módulo 5, ya que 12 ≡ 2 (mod 5) y -2 ≡ 3 *(mod 5)*.

sten otros sistemas completos de residuo módulo 5.

ra ya podemos decir que la ARITMETICA MODULAR es un tema matemático definido sobre el conjunto de los eros enteros mediante la congruencia módulo m. Es por lo to, el sistema de enteros módulo m.

ventaja de este sistema es que recuerda la manera como ribimos las ecuaciones algebraicas, encierra la noción divisibilidad aritmética en una notación más compacta, ugiere trasladar a esta aritmética las operaciones de a y producto que en álgebra conducen a resultados eresantes como podremos comprender en los próximos remas.

rema 1.1. Dos enteros a,b dejan el mismo resto cuando divididos por un entero positivo m si y sólo si a≡b d m).

OSTRACION: Si a ≡ b (mod m), entonces existe un entero al que

$$a = b + sm$$

y b∈Z por definición de congruencia, entonces, por el oritmo# de la división en Z, existen enteros únicos q y ales que

$$b=qm + r, \text{ y } 0 \le r < m$$

e que r es el resto cuando b es dividido por m. Entonces

$$a=(qm + r) + sm$$

$$a=(q + s)m + r$$

o (q+s) es entero, r es también el resto de la división
a entre m .

ra, sea

$$a=q''m + r \quad y \quad b=qm + r,$$

de $0 \le r < m$; esto es, supongamos que a y b dejan el
mo resto cuando son divididos por m. Entonces

$$a - b = (q'' - q)m$$

o q" - q es un entero, m es un divisor de a-b; es decir,
(mod m). ∎

inición 1.3. El conjunto de números enteros b que dejan
mismo resto cuando son divididos para un número natural
constituyen una clase residual módulo m. **La notación**
al es [b]. ∎

ordemos el criterio general para averiguar qué números
n en qué días de la semana:

ingo: ...,-21,-14, -7, 0, 7, 14, 21,...

es : ...,-20, -13, -6, 1, 8, 15, 22,...

tes : ...,-19, -12, -5, 2, 9, 16, 23,...

rcoles: ...,-18, -11, -4, 3, 10, 17, 24,...

ves : ...,-17, -10, -3, 4, 11, 18, 25,...

rnes : ...,-16, -9, -2, 5, 12, 19, 26,...

ado : ...,-15, -8, -1, 6, 13, 20, 27,...

, observemos que cualquier número en alguna fila tiene
mismo residuo que cualquier otro número en la misma fila
ndo se divide entre 7. Estas 7 filas donde los puntos
ican una secuencia infinita de enteros, son las "clases

esiduales, módulo 7", del conjunto de enteros.

ada clase residual módulo m puede ser representada por no cualquiera de sus miembros; pero es usual representar cada clase por el menor entero no negativo que pertenezca esa clase.

or lo tanto: $[0] = [-7] = [7] = [14] = \ldots = [7n]$

$[1] = [8] = [-6] = [15] = \ldots = [7n+1]$

...

$[6] = [13] = [-8] = \ldots = [7n+6]$

eorema 1.2. La relación de congruencia módulo m, cuando es un número natural es una RELACION DE EQUIVALENCIA# en conjunto de los enteros; esto es, la relación de ongruencia módulo m es

Reflexiva: $a \equiv a \pmod{m}$ para todo entero a;

) Simétrica: si $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$,

i) Transitiva: si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$ para todo $a,b,c \in Z$.

EMOSTRACION:

$a-a=0$ y 0 es divisible entre m

) $a \equiv b \pmod{m} \Longrightarrow a-b=km$, para algún $k \in Z$, (definición 1.1.)

$\Longrightarrow b-a=(-k)m$ también es un múltiplo de m

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

i) $a \equiv b \pmod{m} \Longrightarrow a-b=km$, para algún $k \in Z$

$b \equiv c \pmod{m} \Longrightarrow b-c=jm$, para algún $j \in Z$

sumar se tiene $(a-b)+(b-c) = km + jm$

$a - c = (k + j)m$

ro (k+j) $\in$ Z, luego, a-c es múltiplo de m. Por lo tanto

$$a\equiv b(\text{mod } m) \text{ y } b\equiv c(\text{mod } m) \Longrightarrow a\equiv c(\text{mod } m). \blacksquare$$

mo la congruencia módulo **n** es una RELACIÓN DE EQUIVALEN-A[#], particiona al conjunto Z en subconjuntos disjuntos amados clases de equivalencia, esto sucede con cada $n\in N$. to significa que $Z=[0]\cup[1]\cup\ldots\cup[n-1]$.

propiedad **iii)** del teorema 1.2. es la que caracteriza a congruencia, y dice que la congruencia módulo **m** clasifi- a los enteros por su resto en la división por **m**; dos teros son congruentes módulo **m** si y sólo si poseen el smo resto en la división por **m**, por ejemplo, si m=2, la asificación de Z es de **pares** e **impares**.

FINICION 1.4.

s clases de equivalencia para la congruencia módulo n son s **CLASES RESIDUALES MODULO n.** $\blacksquare$

da una de estas clases residuales contiene un número finito de elementos.

amos de qué manera "la relación de congruencia módulo 12" rticiona al conjunto Z.

s 12 clases residuales constan de los enteros de la forma +12k, 1+12k, 2+12k, 3+12k, 4+12k, 5+12k, 6+12k, 7+12k, 12k, 9+12k, 10+12k, y 11+12k, respectivamente, siendo ın número natural, esto es las 12 clases residuales son:

[0] [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]

Este es **EL CONJUNTO DE CLASES RESIDUALES MODULO k.**

3. ALGUNOS TEOREMAS SOBRE CONGRUENCIAS

orema 1.3. Si $a \equiv b (\mathrm{mod}\ m)$ y $c \in Z$, entonces $a+c \equiv b+c\ (\mathrm{mod}\ m)$.

MOSTRACION:

a≡b (mod m), entonces existe un entero k tal que

$$a = b + km$$

$$\Longrightarrow \quad a+c = b + km + c$$

$$\Longrightarrow \quad (a+c) = (b+c) + km$$

por la definición de congruencia,

$$(a+c) \equiv (b+c)\ (\mathrm{mod}\ m). \blacksquare$$

ıstración: Consideremos la congruencia $12 \equiv 5\ (\mathrm{mod}\ 7)$ y c

3,

$$12 + 3 \equiv 5 + 3\ (\mathrm{mod}\ 7)$$

decir $15 \equiv 8\ (\mathrm{mod}\ 7)$ que es una proposición verdadera.

orema 1.4. Si $a \equiv b\ (\mathrm{mod}\ m)$ y c es un entero, entonces iste un entero k tal que $ac \equiv bc\ (\mathrm{mod}\ m)$.

MOSTRACION:

a≡b (mod m), entonces existe un entero primo k tal que

$$a = b + km$$

onces $\qquad ac = (b + km)c;$

o es, $\qquad ac = bc + (kc)m.$

o kc es un entero, por la definición de la relación de gruencia, tenemos $ac \equiv bc\ (\mathrm{mod}\ m)$. ∎

lustración:

onsideremos nuevamente la congruencia $12 \equiv 5 \pmod 7$ y $c = 3$,

$$12 \times 3 \equiv 5 \times 3 \pmod 7$$

s decir $$36 \equiv 15 \pmod 7$$

ue es una proposición verdadera.

os teoremas 1.3 y 1.4. expresan la compatibilidad de la uma y el producto de enteros con respecto a esta relación e congruencia. Esto es muy importante, pues permite trasladar" las operaciones de suma y producto al conjunto e clases de congruencia. Esto da lugar a los anillos[&] de nteros módulo m y así a la "aritmética módulo m".

eorema 1.5. Si $a \equiv b \pmod m$ y $c \equiv d \pmod m$, entonces

$$a \pm c \equiv b \pm d \pmod m$$

EMOSTRACION:

i $a \equiv b \pmod m$, entonces existe un entero k tal que

$$a = b + km$$

i $c \equiv d \pmod m$, entonces existe un entero j tal que

$$c = d + jm$$

sando propiedades de los números reales, tenemos que

$$a \pm c = b \pm d + (k + j)m$$

mo $k \pm j$ es un entero, entonces, por la definición de relación de, congruencia, $a \pm c \equiv b \pm d \pmod m$. ∎

ustración: Consideremos las congruencias $30 \equiv 8 \pmod{11}$ y $\equiv 2 \pmod{11}$.

licando el Teorema 1.5.,

30 ± 13 ≡ 8 ± 2 (mod 11)

=> 43 ≡ 10 (mod 11) es una proposición verdadera.

^ 17 ≡ 6 (mod 11) es también una proposición verdadera

eorema 1.6. Si a ≡ b (mod m) y c ≡ d (mod m), entonces

$$ac \equiv bd \pmod{m}$$

EMOSTRACION:

i a ≡ b (mod m) y c ≡ d (mod m), entonces existen enteros y j tales que

$$a = b + km$$

$$c = d + jm \qquad \text{respectivamente.}$$

sando propiedades de los números reales, tenemos que

$$ac = (b + km)(d + jm)$$

$$= bd + (bj + kd + kjm)m$$

omo bj+kd+kjm es un entero, por la definición de relación e congruencia

$$ac \equiv bd \pmod{m}. \blacksquare$$

lustración : Consideremos las congruencias 30≡8 (mod 11) 13≡2 (mod 11).

plicando el Teorema 1.6.,

$$30 \times 13 \equiv 8 \times 2 \pmod{11}$$

390 ≡ 16 (mod 11) es una proposición erdadera.

eorema 1.7. Si a ≡ b (mod m), m∈N y, n ∈ Z+, entonces

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

EMOSTRACION:

a demostración es por inducción matemática. Está dado ya ue $a \equiv b \pmod{m}$

upongamos ahora que

$$a^k \equiv b^k \pmod{m},\ k \in Z+$$

Entonces, por el Teorema 1.7.

$$a^k a \equiv b^k b \pmod{m};$$

esto es,

$$a^{k+1} \equiv b^{k+1} \pmod{m}.$$

Por lo tanto, por el principio de inducción matemática,

$$a^n \equiv b^n \pmod{m}. \blacksquare$$

lustración: Encontrar el resto de dividir 2^{30} entre 15. El roblema es equivalente a encontrar cual de las quince lases residuales módulo 15, que contiene a 0, 1, 2, 3, . ., 14, respectivamene, contiene a 2^{30}.

otemos primeramente que $2^4 \equiv 1 \pmod{15}$.

ntonces, por el teorema 1.8.

$$(2^4)^7 \equiv 1^7 \pmod{15};$$

esto es, $2^{28} \equiv 1^7 \pmod{15}$.

Por el Teorema 1.4. con $c = 2^2$, tenemos

$$2^{30} \equiv 4 \pmod{15}.$$

or tanto, según el Teorema 1.3., el resto de dividir 2^{30} ntre 15 es 4.

plicando el procedimiento usual tendríamos que dividir 2^{30} ntre 15, esto es, 1073741824 entre 15.

1.3.1. OPERACIONES CON CLASES RESIDUALES

La relación de congruencia módulo 2 particiona al conjunto Z en las clases residuales [0] y [1], consideradas ya desde la lejana antigüedad como [pares] e [impares], para las cuales se conocen las siguientes tablas de suma y de multiplicación:

Tabla III

+	[par]	[impar]
[par]	[par]	[impar]
[impar]	[impar]	[par]

Tabla IV

.	[par]	[impar]
[par]	[par]	[par]
[impar]	[par]	[impar]

Estas tablas pueden ser consideradas como la definición de operaciones de suma y multiplicación en el conjunto de clases residuales módulo 2 así:

Tabla V

+	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Tabla VI

+	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Las tablas V y VI podrían ser consideradas como la definición de operaciones de "suma" y de "multiplicación" en una álgebra de las dos clases residuales [0] y [1].

Por los teoremas 1.3 y 1.4, podemos trasladar las operaciones definidas en las tablas V y VI a los representante de las clases [0] y [1] esto es, a sus respectivos restos 0 y 1 respecto del módulo 2, las tablas anteriores se convierten en:

Tabla VII

+	0	1
0	0	0
1	0	1

Tabla VIII

+	0	1
0	0	0
1	0	1

En forma análoga obtenemos una álgebra Z_m de **m** elementos, mediante el sistema de clases residuales módulo **m**, llamado también sistema de enteros módulo **m**.

Las operaciones de suma y multiplicación entre los elementos de Z_m, es decir, entre las clases residuales módulo m, se definirán por las operaciones ya conocidas del mismo nombre con sus respectivos restos representantes. Por los teoremas 1.5 y 1.6, estas operaciones son efectivamente operaciones entre las clase residuales.

Estas operaciones cumplen en Z_m los siguientes axiomas

$$\forall\ a, a', b, c \in Z_m,$$

SUMA	MULTIPLICACION
(1) Asociativa:	
$(a+b)+c \equiv a+(b+c) \pmod{m}$	$(a.b).c \equiv a(b.c) \pmod{m}$
(2) Elemento Identidad:	
$a+0 \equiv a \pmod{m}$	$a.1 \equiv a \pmod{m}$
(3) Conmutativa:	
$a + b \equiv b + a \pmod{m}$	$a.b \equiv b.a \pmod{m}$

(4) Distributiva:

$$c.(a + b) \equiv c.a + c.b$$

(5) Inverso aditivo:	No siempre existe
$a + a' \equiv 0 \pmod{m}$	en la multiplicación

Como se cumplen los axiomas (1), (2), (3) (4) y (5) que acabamos de enunciar, podemos afirmar que:

$\langle Z_m, +\rangle$ es un grupo#

$\langle Z_m, +\rangle$ es un grupo abeliano#

$<Z_m, +, .>$ es un anillo$^{\#}$

$<Z_m, +, .>$ es un anillo$^{\#}$ conmutativo

El Elemento unitario$^{\#}$ en $<Z_m, +, .>$ es el 1, por lo tanto, $<Z_m, +, .>$ es un anillo$^{\#}$ conmutativo con unitario.

El axioma (5) se cumple en la multiplicación sólo cuando m es número primo$^{\#}$, lo notaremos con Z_p, entonces:

i) en $<Z_m, +, .>$, donde m NO es primo, NO todos los elemento son unidades$^{\#}$

i) en $<Z_p, +, .>$, donde p SI es primo, TODOS los elementos son unidades$^{\#}$

En consecuencia,

$<Z_p, +, .>$, donde p es número primo$_{\#}$, es un SEMICAMPO$^{\#}$

Ejemplo: $<Z_7, +, .>$ es un semicampo

pero, $<Z_m, +, .>$, donde m no es primo$_{\#}$, no es un SEMICAMPO$^{\#}$

Ejemplo: $<Z_6, +, .>$ no es un semicampo.

Los anillos $<Z_m, +, .>$, donde m no es número primo, si tienen divisores$^{\#}$ de cero, ejemplo, en $<Z_6, +, .>$ 3 y 2 son divisores de 0 porque 3.2=0, pero, en $<Z_p, +, .>$, siendo p primo, no pueden haber divisores de 0$^{\#}$. En consecuencia,

$<Z_p, +, .>$, donde p es número primo$_{\#}$, es un DOMINO ENTERO$^{\#}$

Ejemplo: $<Z_7, +, .>$ es un domino entero

pero, $<Z_m,+,.>$, donde m no es primo$_{\#}$, no es DOMINIO ENTERO$^{\#}$

Ejemplo: $<Z_6, +, .>$ no es un dominio entero

FINALMENTE, $<Z_p, +, .>$, siendo p primo, es un semicampo conmutativo, por lo tanto es un CAMPO$^{\#}$.

.4. UNA APLICACION DE LA RELACION DE CONGRUENCIA

estudio de las condiciones bajo las cuales un entero ado es divisible por otro entero ha fascinado a los tudiosos de la matemática por muchos años, y aún continúa endo de interés.

esta sección analizaremos el criterio bajo el cual un tero es divisible entre 9.

eorema 1.8. Un entero expresado en notación decimal es visible entre 9 si y sólo si la suma de sus dígitos es visible entre 9.

MOSTRACION

odo entero positivo n puede ser expresado en numeración cimal en la forma

$$n = a_0+a_1.10+a_2.10^2+a_3.10^3+...+a_k.10^k,$$

nde cada a_i es un entero tal que $0 \leq a_i < 10$ y k es un entero sitivo. Como

$$10 \equiv 1 \pmod 9),$$

r el teorema 1.7,

$$10^2 \equiv 1^2 \pmod 9$$

$$10^3 \equiv 1^3 \pmod 9$$

$$...$$

$$10^k \equiv 1^k \pmod 9$$

por los teoremas 1.2. y 1.4.,

$$a_0 \equiv a_0 \pmod 9$$

$$a_1 . 10 \equiv a_1 \pmod{9}$$

$$a_2 . 10^2 \equiv a_2 \pmod{9}$$

$$a_3 . 10^3 \equiv a_3 \pmod{9}$$

$$\ldots$$

$$a_k . 10^k \equiv a_k \pmod{9}$$

r el teorema 1.5.

$$n \equiv a_0 + a_1 + a_3 + \ldots + a_k \pmod{9},$$

nde

$$a_0 + a_1 + a_3 + \ldots + a_k$$

presenta la suma de los dígitos de **n**. Por lo tanto, según teorema 1.1., ambos, el entero positivo **n** y la suma de s dígitos, dejan el mismo resto cuando son divididos por De aquí que un entero expresado en numeración decimal es visible entre 9 si y sólo si, la suma de sus dígitos es visible entre 9.

ustración. ¿es el número 26356734 divisible entre 9?

suma de los dígitos es

$$2+6+3+5+6+7+3+4 = 36$$

mo 36 es divisible entre 9, entonces 263567734 si es ivisible entre 9.

ra verificar, notemos que 26356734 ÷ 9 = 2928526.

Para el lector: *¿Cuál sería el criterio para la divisibilidad de un entero entre 11?*

1.5. UN TEOREMA FAMOSO

En una carta del 18 de Octubre de 1640, el matemático Francés Pierre de Fermat comunicó al matemático Bernard Frénicle (1605-1675) el siguiente teorema: si **p** es un primo y a es cualquier entero primo[#] relativo con **p**, entonces p divide a $a^{p-1} - 1$. Fermat no dio ninguna demostración y fue el gran matemático suizo Leonhard Euler (1707-1783) quién, en 1736, publicó la **primera** demostración y obtuvo años más tarde, en 1760, una importante generalización.

El resultado enunciado por Fermat constituye el famoso "pequeño Teorema de Fermat (P.T.F)", resultado importante y fundamental en muchos aspectos de la teoría de números.

1.3.1. Teorema de Fermat: Si $a \in Z$ y p es un primo que no divide a, entonces divide $a^{p-1} -1$, esto es, $a^{p-1} \equiv 1 \pmod p$. ∎

Por ejemplo: $2^4 \equiv 1 \pmod 5$; $3^{10} \equiv 1 \pmod{11}$

La siguiente es una **demostración** conceptual del teorema de Fermat debida a Euler, que aparece en *Disquisitions Arithmeticae Nº 49.*

"Sea **a** un entero primo[#] relativo con **p**, o sea **p** no es divisible entre **a**. Formemos los p-1 números

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1).a \qquad (1)$$

los resto de la división de esos números entre p son exactamente

$$1, 2,\ \ldots,\ p-1$$

vo una permutación (o sea son los mismos restos, pero respectivamente). Es decir (1) constituye un sistema pleto de restos módulo p. Por ejemplo, si $p=5$ y $a=8$ se nen los números 8, 16, 24, 32 y los restos en la isión por 5 son, respectivamente, 3, 1, 4, 2.

a probar la afirmación anterior, nótese que el resto 0 puede aparecer en la sucesión (1) dado que si p es isor de i.a, $1\leq i\leq p-1$, entonces p es divisor de i o p es isor de a, pero ninguna de las dos cosas puede ocurrir. más, dos elementos distintos de (1) producen restos tintos. En efecto, si i.a y j.a producen el mismo resto, $1\leq i\leq j\leq p-1$, entonces $(j-i).a$ es divisible entre **p** y, por ntico razonamiento al precedente, se llega a que $j-i$ e ser 0 o sea $j=i$.

claro ahora que el producto

$$a.2a.3a\ldots(p-1)a \equiv 1.2.3\ldots(p-1) \pmod p$$

decir

$$a^{p-1}.1.2.3\ldots(p-1) \equiv 1.2.3\ldots(p-1) \pmod p$$

por ser $1.2.3\ldots(p-1)$ primo relativo con p, se puede icar la ley cancelativa en ambos miembros de la con- iencia para obtener el Pequeño Teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod p)." \blacksquare$$

Teorema de Fermat proporciona un criterio bastante ectivo para analizar la no primalidad de un entero itivo n.

Fermat se sabe que

$$a^2 \equiv 1 \pmod 3),$$

o sea $$a^{560} \equiv 1 \pmod 3$$

es decir $$a^{561} \equiv a \pmod 3$$

$$a^{16} \equiv 1 \pmod{17},$$

o sea $$a^{560} \equiv 1 \pmod{17}$$

es decir $$a^{561} \equiv a \pmod{17}.$$

Si hay valores $0<a<n$ tales que a^{n-1} no es congruente con 1 (mod n), entonces **n** no es primo. Precisamente este criterio sirve para probar la no primalidad del número $2^{32} + 1$, (el número de Fermat). Fue el matemático Euler quien probó la no primalidad de $2^{32}+1$ al descubrir que 641 era divisor de este número.

Una formulación equivalente al teorema de Fermat es la siguiente:

Sea p primo positivo a entero. Entonces

$$\mathbf{a^p \equiv a \pmod p}. \blacksquare$$

En efecto, si p divide a **a**, el enunciado precedente reduce a $0 \equiv 0 \pmod p$.

Si p no es divisor de **a** puede cancelarse una **a**: $a^{p-1} \equiv 1$ (mod p). Por ejemplo, $2^5 \equiv 2 \pmod 5$.

Ilustración: Determinar el residuo de dividir 8^{103} entre 13.

Usando el Teorema de Fermat, tenemos

$$8^{103} \equiv (8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv 8^7 \equiv (-5)^7$$

$$\equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \pmod{13}.$$

CAPITULO 2

DEFINICIONES COMPLEMENTARIAS

Estas definiciones corresponden a la **opción 2 Diccionario** del Menu principal del programa. El alumno puede accesar de dos formas:

a) Por la opción 2 del MENU PRINCIPAL

b) Desde las pantallas que desplieguen el mensaje

[? diccionario]

CONJUNTO

En matemática hay conceptos sin definición o, primitivos. CONJUNTO es un concepto primitivo, pero, las siguientes ideas sobre el mismo, permiten lograr una adecuada comunicación:

I] Un conjunto S está formado por elementos y, si "a" es uno de estos elementos la notación es:

$$a \in S$$

que se lee "a pertenece al conjunto S"

II] Existe sólo un conjunto sin elementos. Es el conjunto VACIO la notación usual es

$$\{\ \}$$

III] Se puede describir un conjunto mediante una propiedad que caracterice a los elementos o, encerrando en llaves las designaciones de los elementos, separados por comas. También es común usar la notación $\{x|Px\}$, donde Px caracteriza los elementos del conjunto. Para nombrarles se utiliza letras Mayúsculas del alfabeto latino.

Ejemplos:

$A=\{1,a,2\}$

$B=\{x|x$ es un número entero positivo$\}$

IV] Se dice que un conjunto S está bien definido, si para todo objeto "a", se sabe con seguridad que: a pertenece a S o que, a no pertenece a S.

Usualmente se utiliza la siguiente notación para algunos conjuntos numéricos conocidos:

N= {x|x es número entero positivo}

Z= {x|x es número entero}

Z+={x|x es número entero no negativo}

Q= {x|x es número racional}

Q+={x|x es número racional positivo}

R= {x|x es número real}

R+={x|x es número real positivo}

C= {x|x es número complejo}

Zn= {0, 1, 2, ... , n-1} Z6= {0, 1, 2, ... , 5}

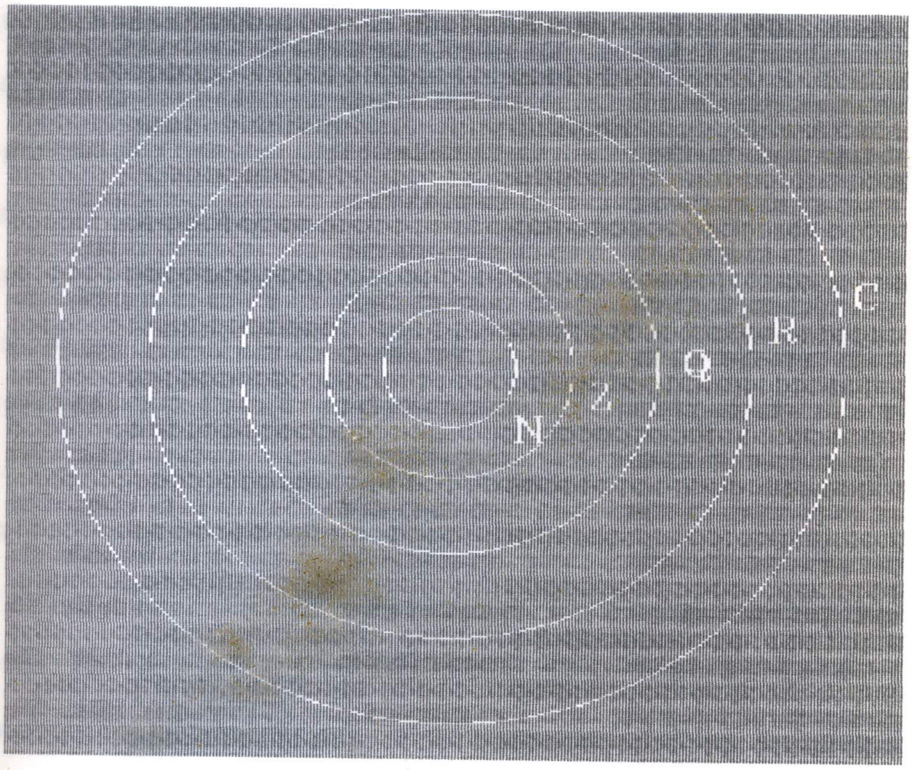


figura d.1

SUBCONJUNTO

Sean S y T dos conjuntos cualesquiera. T es "subconjunto" de S si y solo si, $(\forall a)$ $(a \in S \Rightarrow a \in T)$. ∎

Ejemplos:

N "es subconjunto" de R

Zn "es subconjunto" de Z

RELACION DE EQUIVALENCIA

Una relación Γ en un conjunto S, que satisface las propiedades reflexiva, simétrica y transitiva descritas en el Teorema 2.1, de la definición de partición, es una "relación de equivalencia en S". Cada celda [a] en la partición natural dada por una relación de equivalencia es una "clase de equivalencia". ∎

PARTICION DE UN CONJUNTO

"Una partición de un conjunto S no vacío" es una descomposición del conjunto en n celdas [a], tales que todo elemento del conjunto está en exactamente una de las celdas. ∎

La notación formal es P(S)

$P(S) = [a_1] \cup [a_2] \cup [a_3] \cup \ldots \cup [a_n]$

$[a_1] \cap [a_2] \cap [a_3] \cap \ldots \cap [a_n] = \{\ \}$

Cada celda [a] en la partición natural dada por una relación de equivalencia es una "clase de equivalencia".

Teorema 2.1. **Sea S un conjunto no vacío y sea Γ una relación entre elementos de S que satisface las propiedades siguientes:**

1 REFLEXIVIDAD.- $a \Gamma a$ para todas las $a \in S$.

2 SIMETRIA.- Si $a \Gamma b$, entonces $b \Gamma a$.

3 TRANSITIVIDAD.- Si $a \Gamma b$ y $b \Gamma c$, entonces $a \Gamma c$.

Entonces, Γ produce una partición natural de S, donde

$$(\text{celda})a=[a]=\{x \in S \mid x \Gamma a\}$$

es la celda que contiene a "a" para todas las $a \in S$. Recíprocamente, cada partición de S da lugar a una relación natural Γ que satisface las propiedades reflexiva, simétrica y transitiva si se define $a \Gamma b$ como $a \in [b]$. ∎

Ejemplo:

La relación de congruencia módulo m , $m \in N$, determina una partición en el conjunto de los enteros.

PRODUCTO CARTESIANO

El "producto cartesiano de conjuntos" S1, S2,...,Sn es el conjunto de todas las n-adas ordenadas (a1, a2, ...an), donde $a_i \in S_i$.

La notación es S1 x S2 x ... x Sn. ∎

FUNCION

Una función Φ de un conjunto A en un conjunto B es una regla de correspondencia que asigna a cada elemento de A exactamente un elemento de $b \in B$. Se dice que Φ lleva a en b y que Φ lleva A en B. La notación clásica es $\Phi(a)=b$. El elemento b es la imagen de a bajo Φ. El hecho que Φ lleva A en B se representará simbólicamente por $\Phi : A \longrightarrow B$ donde A es el dominio de Φ; B es el codominio de Φ y el conjunto $A\Phi=\{a\Phi | a \in A\}$ es la imagen de A bajo Φ. ∎

OPERACION BINARIA

Sean S un conjunto cualquiera, $s_1, s_2, s_3 \in Z$ y, * una función. Una "operación binaria" en S es la función * de S x S en S. La notación es $s_1 * s_2 = s_3$. ∎

Una operación binaria * en un conjunto S es **CONMUTATIVA** si y solo si a*b = b*a para toda a,b ∈ S. ∎

Una operación binaria * en un conjunto S es **ASOCIATIVA** si y solo si (a*b)*c = a*(b*c) para todo a,b,c ∈ Z. ∎

ALGORITMO DE LA DIVISION EN Z (TEOREMA)

Sea p ∈ N. Para cada entero n existen enteros únicos q y r tales que se satisface

$$n = pq + r \quad y \quad 0 \leq r < p.$$ ∎ '

Los números q y r se llaman **cociente** y **residuo**, respectivamente, **cuando se divide** n **por** p.

Por ejemplo. Por ejemplo, si p=7 y n=33 entonces 33=7x4 + 5 por lo que q=4 y r=5.

NUMERO PRIMO

Se denomina " número primo " a todo número entero que posee exactamente cuatro divisores. ∎

Ejemplos:

1) Si p es un número primo, sus únicos divisores son: 1, -1, p, y -p.

2) 3 es primo pues tiene exactamente 4 divisores: 1, -1, 3, -3

3) 0 no es primo, tiene más de 4 divisores ya que, cualquier entero diferente de cero divide a 0.

NUMEROS PRIMOS RELATIVOS

Dos números enteros a y b se dirán primos relativos si satisfacen:

d es divisor de a

d es divisor de b

$\Longrightarrow$ d=1 o d=-1

Ejemplos:

1) Si p y q son primos positivos distintos, p y q son primos relativos.

2) 6 y 15 no son primos relativos, pues 3 es divisor común de 6 y 15.

CONGRUENCIA MODULO m

Sean $h,k,s \in Z$ y, $m \in N$. Se define h congruente con k módulo m, lo cual se denota $h \equiv k \pmod{m}$, si y solo si h-k es divisible entre m, es decir, h-k=sm para alguna $s \in Z$.∎

GRUPO

Un grupo <G,*> es un conjunto G, junto con una operación binaria * en G, tal que se satisface los siguientes axiomas:

G1 La operación binaria es asociativa.

G2 Existe un elemento e en G tal que e*x = x*e=x para todas las $x \in G$. Este elemento e es un "elemento identidad" para * en G.'

G3 Para cada $b \in G$ existe un elemento $b'' \in G$ con la propiedad de que b"*b=b*b"=e. El elemento b" es un inverso de b respecto a *. ∎

GRUPO ABELIANO

Un grupo G es abeliano si su operación binaria * es conmutativa.∎

ELEMENTO GENERADOR

Un elemento a de un grupo G "genera" G y es un generador de G si $\langle a \rangle = G$. ∎

GRUPO CICLICO

Un grupo G es CICLICO si existe algún elemento a en G que genere G. ∎

ANILLO

Un anillo $\langle R,+,.\rangle$ es un conjunto R junto con dos operaciones binarias + y ., que llamamos suma y multiplicación, definidas en R tales que se satisfacen los siguientes axiomas:

R_1 $\langle R,+\rangle$ es un grupo abeliano.

R_2 La multiplicación es asociativa.

R_3 Para todas la $a,b,c \in R$, se cumple la ley distributiva izquierda $a(b+c)=(ab)+(ac)$ y la ley distributiva derecha $(a+b)c = (ac)+(bc)$. ∎

ANILLO CONMUTATIVO

Un anillo en donde la multiplicación es conmutativa es un anillo conmutativo. ∎

ANILLO CON UNITARIO

Un anillo R con identidad multiplicativa 1 tal que $1x=x=x$ para todas las $x \in R$ es un anillo con unitario. ∎

LEMENTO UNITARIO en un anillo

Jna identidad multiplicativa en un anillo es un elemento ınitario. ∎

NIDAD DE UN ANILLO

ea R un anillo con unitario. Un elemento u en R es una nidad de R si tiene un inverso multiplicativo en R. ∎

EMICAMPO o anillo con división

i todo elemento distinto de cero en un anillo R con nitario es una unidad, entonces R es un semicampo o anillo on división. ∎

AMPO

n campo es un anillo conmutativo con división. ∎

IVISORES DE CERO

i a y b son dos elementos distintos de cero de un anillo tal que ab=0, entonces a y b "son divisores de 0". En articular, a es un divisor izquierdo de 0 y b es un ivisor derecho de 0. ∎

OMINIO ENTERO

n dominio entero D es un anillo conmutativo unitario que o contiene divisores de 0. ∎

CAPITULO 3

BIOGRAFIAS

4.1. GAUSS, EL PRINCIPE DE LOS MATEMATICOS

El linaje de Gauss, Príncipe de los Matemáticos, lo fue todo menos real. Hijo de padres pobres, nació en una miserable cabaña de Brunsvic, Alemania, el 30 de Abril de 1777. Su nombre bautismal fue Johann Friedrich Carl Gauss. La imagen que la historia tiene del padre de Gauss es la de un hombre justo, escrupulosamente honesto y rudo hasta casi llegar a la brutalidad con sus hijos. Hizo todo lo que estaba a su alcance para frustrar a su hijo y privarle de adquirir una educación adecuada a sus facultades.

Por el lado de su madre Dorothea, Gauss fue verdaderamente afortunado. El padre de Dorothea fue un cantero que murió de tuberculosis a los 30 años de edad; dejó dos hijos: Dorothea y su hermano menor Friedrich.

Aquí se evidencia la ascendencia del genio de Gauss. Condenado por necesidad económica al oficio de tejedor, Friedrich fue un hombre genial, altamente inteligente, cuya mente aguda e inquieta se desarrolló por sí misma en campos muy alejados de sus medios subsistenciales. Friedrich hizo gran reputación como tejedor de finos damascos. Encontrando una mente afín en la del hijo de su hermana, agudizó su ingenio en el del joven genio e hizo lo que pudo para estimular la vida lógica del muchacho con su propia filosofía de la vida.

La madre de Gauss fue una honrada mujer de fuerte carácter, aguda inteligencia. Su hijo fue su orgullo desde el día de su nacimiento hasta su muerte a los 96 años. Pasó los últimos 20 años en la casa de su hijo. Gauss recompensó la valerosa protección de sus primeros años, dándole una serena vejez. Cuando se volvió ciega, él la cuidó y atendió en su larga y última enfermedad.

En toda la historia de las Matemáticas nada hay que se cerque a la precocidad de Gauss cuando niño.

stando aún en el colegio Gauss había empezado las investi-aciones en las matemáticas superiores que habían de acerle inmortal. Sus prodigiosos poderes de cálculo ntraron entonces en juego. Fue directamente a los mismos úmeros con que experimentaba, descubriendo por inducción ecónditos teoremas generales, cuya demostración le habían e costar incluso a él un esfuerzo. De esta forma redescu-rió "la joya de la aritmética", theorema aureum, al cual abía llegado también Euler inductivamente, que es onocido como la " LEY DE LA RECIPROCIDAD CUADRATICA" y ue él había de ser el primero en demostrar.

a formulación de Gauss de la Ley de la Reciprocidad uadrática es la siguiente:

> "Sean p y q primos positivos impares. Si p es de la forma 4m + 1, entonces la ecuación $X^2 \equiv q \pmod{p}$ admite solución si, y sólo si, la ecuación $X^2 \equiv p \pmod{q}$ admite solución. Si p es de la forma 4m + 3, entonces la ecuación $X^2 \equiv q \pmod{p}$ admite solución, si y sólo si, la ecuación $X^2 \equiv -p \pmod{q}$ admite solución".

a investigación se originó en una simple pregunta: Cuántos dígitos hay en el período de un decimal que se epite? Para esclarecer un poco el problema, Gauss calculó as representaciones decimales de todas las fracciones 1/n ara n=1 hasta 1000, siendo n un entero. Así ...

desde 1/1

1.000000000000000000	0.500000000000000000	0.333333333333333333
0.250000000000000000	0.200000000000000000	0.166666666666666667
0.142857142857142857	0.125000000000000000	0.111111111111111111
0.100000000000000000	0.090909090909090909	0.083333333333333333
0.076923076923076923	0.071428571428571429	0.066666666666666667
0.062500000000000000	0.058823529411764706	0.055555555555555556
0.052631578947368421	0.050000000000000000	0.047619047619047619
0.045454545454545455	0.043478260869565217	0.041666666666666667
0.040000000000000000	0.038461538461538462	0.037037037037037037
0.035714285714285714	0.034482758620689655	0.033333333333333333
0.032258064516129032	0.031250000000000000	0.030303030303030303
0.029411764705882353	0.028571428571428571	0.027777777777777778
0.027027027027027027	0.026315789473684211	0.025641025641025641
0.025000000000000000	0.024390243902439024	0.023809523809523810
0.023255813953488372	0.022727272727272727	0.022222222222222222
0.021739130434782609	0.021276595744680851	0.020833333333333333
0.020408163265306122	0.020000000000000000	0.019607843137254902
0.019230769230769231	0.018867924528301887	0.018518518518518519
0.018181818181818182	0.017857142857142857	0.017543859649122807
0.017241379310344828	0.016949152542372881	0.016666666666666667
0.016393442622950820	0.016129032258064516	0.015873015873015873
0.015625000000000000	0.015384615384615385	0.015151515151515152
0.014925373134328358	0.014705882352941177	0.014492753623188406
0.014285714285714286	0.014084507042253521	0.013888888888888889
0.013698630136986301	0.013513513513513514	0.013333333333333333
0.013157894736842105	0.012987012987012987	0.012820512820512821
0.012658227848101266	0.012500000000000000	0.012345679012345679
0.012195121951219512	0.012048192771084337	0.011904761904761905
0.011764705882352941	0.011627906976744186	0.011494252873563218
0.011363636363636364	0.011235955056179775	0.011111111111111111
0.010989010989010989	0.010869565217391304	0.010752688172043011
0.010638297872340426	0.010526315789473684	0.010416666666666667
0.010309278350515464	0.010204081632653061	0.010101010101010101
0.010000000000000000	0.009900990099009901	0.009803921568627451
0.009708737864077670	0.009615384615384615	0.009523809523809524
0.009433962264150943	0.009345794392523364	0.009259259259259259
0.009174311926605505	0.009090909090909091	0.009009009009009009
0.008928571428571429	0.008849557522123894	0.008771929824561404
0.008695652173913043	0.008620689655172414	0.008547008547008547
0.008474576271186441	0.008403361344537815	0.008333333333333333

hasta 1/120

desde 1/121

0.008264462809917355	0.008196721311475410	0.008130081300813008
0.008064516129032258	0.008000000000000000	0.007936507936507937
0.007874015748031496	0.007812500000000000	0.007751937984496124
0.007692307692307692	0.007633587786259542	0.007575757575757576
0.007518796992481203	0.007462686567164179	0.007407407407407407
0.007352941176470588	0.007299270072992701	0.007246376811594203
0.007194244604316547	0.007142857142857143	0.007092198581560284
0.007042253521126761	0.006993006993006993	0.006944444444444444
0.006896551724137931	0.006849315068493151	0.006802721088435374
0.006756756756756757	0.006711409395973154	0.006666666666666667
0.006622516556291391	0.006578947368421053	0.006535947712418301
0.006493506493506494	0.006451612903225806	0.006410256410256410
0.006369426751592357	0.006329113924050633	0.006289308176100629
0.006250000000000000	0.006211180124223602	0.006172839506172840
0.006134969325153374	0.006097560975609756	0.006060606060606061
0.006024096385542169	0.005988023952095808	0.005952380952380952
0.005917159763313609	0.005882352941176471	0.005847953216374269
0.005813953488372093	0.005780346820809249	0.005747126436781609
0.005714285714285714	0.005681818181818182	0.005649717514124294
0.005617977528089888	0.005586592178770950	0.005555555555555556
0.005524861878453039	0.005494505494505495	0.005464480874316940
0.005434782608695652	0.005405405405405405	0.005376344086021505
0.005347593582887701	0.005319148936170213	0.005291005291005291
0.005263157894736842	0.005235602094240838	0.005208333333333333
0.005181347150259067	0.005154639175257732	0.005128205128205128
0.005102040816326531	0.005076142131979695	0.005050505050505051
0.005025125628140704	0.005000000000000000	0.004975124378109453
0.004950495049504951	0.004926108374384236	0.004901960784313725
0.004878048780487805	0.004854368932038835	0.004830917874396135
0.004807692307692308	0.004784688995215311	0.004761904761904762
0.004739336492890995	0.004716981132075472	0.004694835680751174
0.004672897196261682	0.004651162790697674	0.004629629629629630
0.004608294930875576	0.004587155963302752	0.004566210045662100
0.004545454545454545	0.004524886877828054	0.004504504504504505
0.004484304932735426	0.004464285714285714	0.004444444444444444
0.004424778761061947	0.004405286343612335	0.004385964912280702
0.004366812227074236	0.004347826086956522	0.004329004329004329
0.004310344827586207	0.004291845493562232	0.004273504273504274
0.004255319148936170	0.004237288135593220	0.004219409282700422
0.004201680672268908	0.004184100418410042	0.004166666666666667

hasta 1/240

Y ASI SUCESIVAMENTE ....

desde 1/881

0.001135073779795687	0.001133786848072562	0.001132502831257078
0.001131221719457014	0.001129943502824859	0.001128668171557562
0.001127395715896280	0.001126126126126126	0.001124859392575928
0.001123595505617978	0.001122334455667789	0.001121076233183857
0.001119820828667413	0.001118568232662192	0.001117318435754190
0.001116071428571429	0.001114827201783724	0.001113585746102450
0.001112347052280311	0.001111111111111111	0.001109877913429523
0.001108647450110865	0.001107419712070875	0.001106194690265487
0.001104972375690608	0.001103752759381898	0.001102535832414553
0.001101321585903084	0.001100110011001100	0.001098901098901099
0.001097694840834248	0.001096491228070175	0.001095290251916758
0.001094091903719912	0.001092896174863388	0.001091703056768559
0.001090512540894220	0.001089324618736383	0.001088139281828074
0.001086956521739130	0.001085776330076004	0.001084598698481562
0.001083423618634886	0.001082251082251082	0.001081081081081081
0.001079913606911447	0.001078748651564186	0.001077586206896552
0.001076426264800861	0.001075268817204301	0.001074113856068743
0.001072961373390558	0.001071811361200429	0.001070663811563169
0.001069518716577540	0.001068376068376068	0.001067235859124867
0.001066098081023454	0.001064962726304579	0.001063829787234043
0.001062699256110521	0.001061571125265393	0.001060445387062566
0.001059322033898305	0.001058201058201058	0.001057082452431290
0.001055966209081309	0.001054852320675105	0.001053740779768177
0.001052631578947368	0.001051524710830705	0.001050420168067227
0.001049317943336831	0.001048218029350105	0.001047120418848168
0.001046025104602510	0.001044932079414838	0.001043841336116910
0.001042752867570386	0.001041666666666667	0.001040582726326743
0.001039501039501040	0.001038421599169263	0.001037344398340249
0.001036269430051813	0.001035196687370600	0.001034126163391934
0.001033057851239669	0.001031991744066047	0.001030927835051546
0.001029866117404737	0.001028806584362140	0.001027749229188078
0.001026694045174538	0.001025641025641026	0.001024590163934426
0.001023541453428864	0.001022494887525562	0.001021450459652707
0.001020408163265306	0.001019367991845056	0.001018329938900204
0.001017293997965412	0.001016260162601626	0.001015228426395939
0.001014198782961460	0.001013171225937183	0.001012145748987854
0.001011122345803842	0.001010101010101010	0.001009081735620585
0.001008064516129032	0.001007049345417925	0.001006036217303823
0.001005025125628141	0.001004016064257028	0.001003009027081244
0.001002004008016032	0.001001001001001001	0.001000000000000000

hasta 1/1000

ODOS esos cálculos realizó Gauss en su época SIN calcula-
ora ni computadora. No encontró, GAUSS, el tesoro que
staba buscando, sino algo infinitamente mayor, la "ley de
a reciprocidad cuadrática", al mismo tiempo introdujo una
e las revolucionarias nociones que adoptó en la nomencla-
ura aritmética y en la notación, la de CONGRUENCIA.

a ideas que asaltaban a Gauss desde sus diecisiete años
abían reducidas al orden. Desde 1795 había estado meditan-
o una gran obra sobre la teoría de los números . Esta tomó
ntonces una forma definitiva y en 1798 las *Disquisitiones*
rithmeticae estaban prácticamente acabadas.

espués de Gauss las matemáticas se convirtieron en algo
otalmente distinto de las matemáticas de Newton, Euler y
agrange.

.2. FERMAT

ierre de Fermat (1601-1665), nació cerca de Toulouse y
asó toda su vida en el sur de Francia, lejos de los
entros europeos importantes. Fermat fue el primer matemá-
icos en aceptar el desafío en teoría de números que
resentaba la *Aritmética de Diofanto de Alejandría* (325-
09), obra editada por primera vez en Europa, en 1621, por
laudio Bachet (1587-1638) en su texto original griego y
na traducción al latín.

ermat trabajó como abogado y juez y tal vez buscó en la abstracción y la creación matemática refugio a sus funciones de jurista. Muchos de los resultados de su labor Fermat los comunicaba epistolarmente a sus amigos o los redactaba en notas personales o, los escribía en las márgenes de su copia del libro de Bachet. Su hijo Samuel publicó, después de la muerte de Fermat, acaecida en 1665, una segunda edición de la *Aritmética* y agregó las notas marginales (Toulouse, 1670). De estas notas marginales la más famosa es la denominada "conjetura de Fermat: $x^n + y^n = z^n$", que considera imposible de resolverla para números enteros mayores que 2.

4.3. EULER

Leonard Euler (1707-1783) fue hijo de un clérigo, que vivía en los alrededores de Basilea. Su talento natural para las matemáticas se evidenció pronto por el afán y la facilidad con que dominaba los elementos, bajo la tutela de su padre. A una temprana edad fue enviado a la Universidad de Basilea, donde trajo la atención de Jean Bernouilli. Inspirado por un maestro así, maduró rápidamente, y a los 17 años de edad, cuando se graduó de Doctor, provocó grandes aplausos con un discurso probatorio, el tema del cual era una comparación entre los sistemas cartesiano y newtoniano. Su último y principal objetivo fue el perfeccionamiento del cálculo y del análisis matemático.

CAPITULO 4

MANUAL DEL USUARIO

Este programa junto con todos los programas complementarios y el sistema de inicialización, requiere de un medio de almacenamiento (diskette), de al menos 720 kb.

Para su mantenimiento, obtenga una copia de respaldo de todo el diskette, mediante el comando diskcopy, desde el sistema operativo.

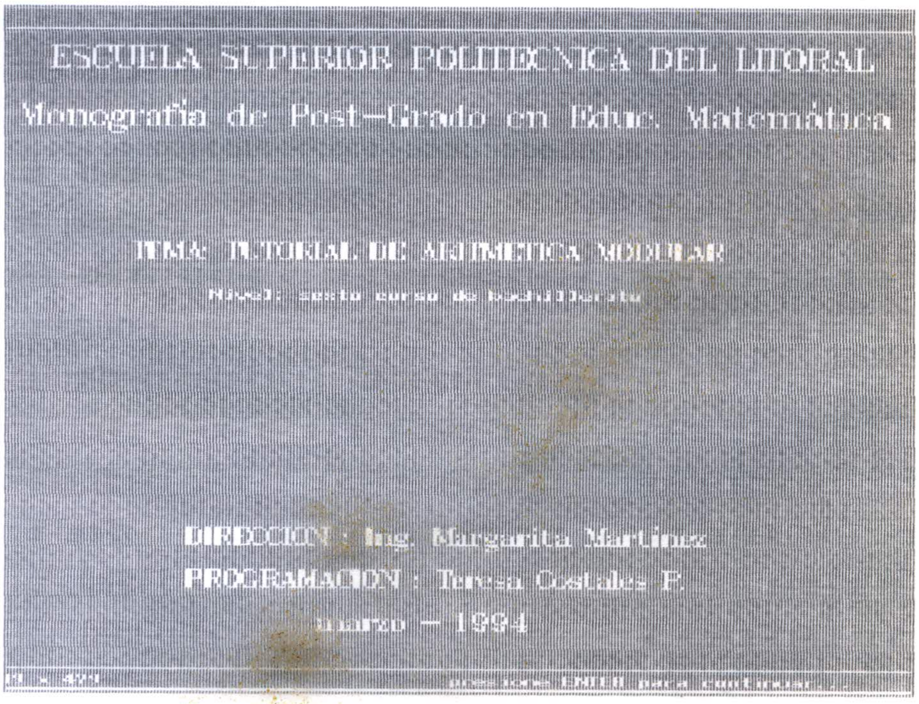
Para su ejecución siga las siguientes instrucciones:

1. Coloque el diskette "protegido contra escritura"

en el drive que corresponda e inicialice el sistema operativo.

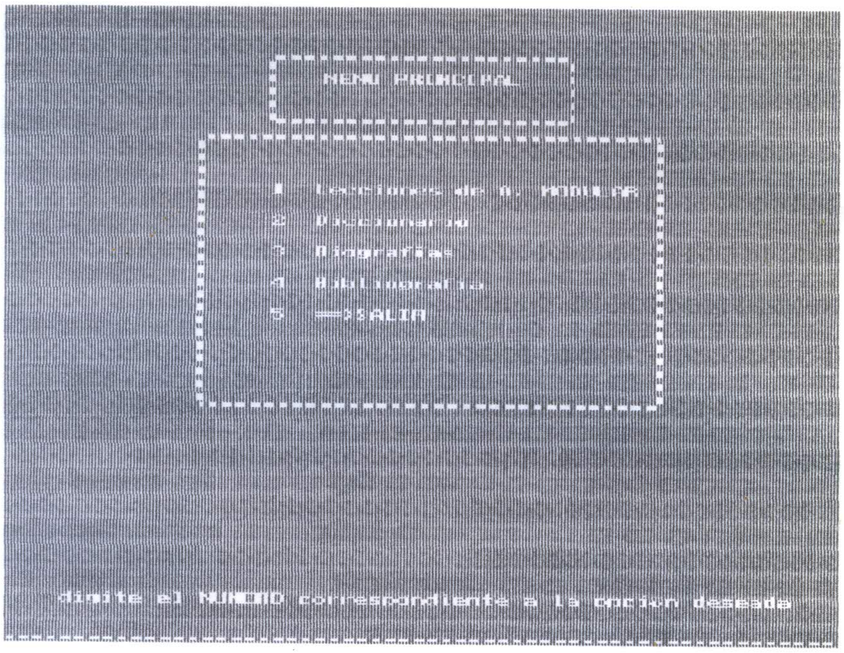
2. Desde el mismo drive digite MODULAR, pulse la tecla Enter y espere un momento.

3. Primero se despliega la pantalla de presentación del TEMA,



pulse la tecla Enter para continuar.

4. Se desplegará el MENU PRINCIPAL que luce así



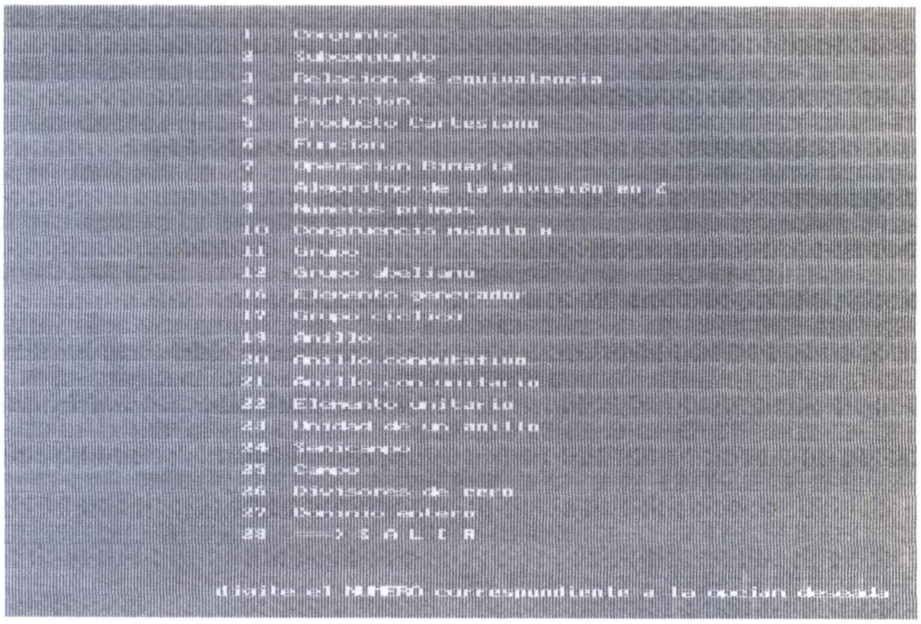
pulse la tecla Enter para continuar ...

Pulse el número que coresponde a la opción que usted desea seleccionar. Si es la primera vez que usa este programa, es recomendable que siga en orden las opciones porque los temas se explican de forma secuencial.

4. Preste la debida atención durante el desarrollo de este Tutorial, lea todos los mensajes que se despliegan en pantalla, si existen preguntas que no pueden ser contestadas con la ayuda del programa, <u>anótelas</u> para que sean consultadas al profesor.

5. La opción 2 Diccionario, le permite ingresar a la consulta de definiciones matemáticas relacionadas

con el tema tratado. El MENU correspondiente es



Pulse el número correspondiente a la definición que desee consultar.También puede ingresar a esta opción desde las pantallas donde se despliega el mensaje [? para ingresar a diccionario].

6. Cuando concluya una lección deberá contestar un cuestionario y sus respuestas serán almacenadas en el diskette para que el profesor pueda enterarse de su avance. Cumpla con este requisito cuando esté seguro de <u>haberse esforzado lo suficiente</u> para comprender todo lo explicado en la lección correspondiente.

7. La opción 5 ==>SALIR le permite salir del programa y regresar al sistema operativo, desde donde podrá apagar el computador.

CONCLUSIONES

. La definición de la relación de congruencia enunciada por Gauss, establece una estrecha analogía con la relación de igualdad.

. Los criterios de divisibilidad de los números, así como la determinación de la primalidad son aplicaciones muy importantes de la relación de congruencia módulo **m**.

. Es muy importante el aporte de las congruencias en el análisis del comportamiento de las potencias numéricas. Por ejemplo, si calculamos las potencias sucesivas de los números módulo 7, encontraremos que se repite la misma secuencia una y otra vez. Así, las potencias de 2 son

$2^0 \equiv 1$	$2^3 \equiv 1$	$2^6 \equiv 1$
$2^1 \equiv 2$	$2^4 \equiv 2$	$2^7 \equiv 2$
$2^2 \equiv 4$	$2^5 \equiv 4$	$2^8 \equiv 3$

la serie 1, 2, 4, 1, 2, 4, 1, 2, 4 se repite indefinidamente. Para las potencias de 3, la serie es 1,3,2,6,4,5 una y otra vez; y, como puede comprobarse, hay series semejantes para los demás números. Es fácil ver que cuando se alcanza una potencia cuyo valor sea 1, la secuencia se repite.

. En general, la congruencia módulo m es particularmente importante para la Teoría de números.

BIBLIOGRAFIA

BORLAND INTERNACIONAL, (1988), Turbo Pascal Reference Guide, Borland Inc., California.

FRALEIGH-JOHN, (1987), Algebra Abstracta, Adison Wesley Iberoamericana, México.

HASHISAKI-JOSEPH, (1964), Theory of Arithmetic, Wiley & Sons Inc., New York.

PETTOFREZO-ANTHONY, (1972), Introducción a la Teoría de los Números, Editorial Prentice Hall I., Madrid.

ROSS-KENNETH, (1987), Matemáticas discretas, Editorial Prentice Hall I., Segunda Edición, México.

STEWART-IAN, (1975), Conceptos de matemática moderna, Editorial Alianza, Madrid.