UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
FACULTAD DE CIENCIAS

"Notas de Clase para el Curso de Algebra Superior II para la Facultad de Ciencias"

TESIS

QUE PARA OBTENER EL TITULO DE

MATEMATICO

PRESENTA

ROSA MARIA HERNANDEZ TREJO

1986

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

CONTENIDO:

I DIVISIBILIDAD Y TEORIA DE NUMEROS

El origen del estudio de las propiedades de los números - retrocede probablemente tan lejos como contar y hacer operaciones aritméticas. No toma mucho tiempo, después de tener un cierto dominio sobre las operaciones con los números enteros - positivos y con los quebrados, descubrir que muchos números se comportan en forma diferente a otros; por ejemplo, algunos números pueden ser divididos en partes más pequeñas y otros no, las operaciones con fracciones conducen inmediatamente al estudio de la divisibilidad de números, al máximo común divisor y al mínimo común múltiplo.

El paso de saber operar al de establecer el estudio de las propiedades generales de los números se atribuye a los griegos. Este interés de los griegos está muy relacionado con el hecho de que en doctrinas filosóficas importantes como la - de los Pitagóricos, los números juegan un papel central, ellos eran particularmente devotos a las especulaciones de símbolos numéricos en la filosofía y la naturaleza. El hecho de establecer una correspondencia simbólica entre los números y conceptos filosóficos e ideas era común a muchas de las culturas antiguas. A manera de ejemplo, mostramos lo que dijo San Agustín sobre el número 6 que tiene la propiedad de ser igual a la - suma de sus divisores propios $6 = 1 + 2 + 3$. (A los números con esta propiedad se les llaman perfectos)

> "6 es un número perfecto en sí mismo y no porque - Dios haya creado todas las cosas en seis días; mas bien es al revés: Dios creó todas las cosas en seis días porque este número es perfecto. Y seguirá siendo perfecto aún cuando el trabajo de los seis días no hubiera existido". -

La tendencia a atribuirles propiedades místicas a los nú-

meros fué poco a poco quedando en el olvido, y fué cobrando cada vez mayor interés el estudio de las características "no místicas" de los números. Este estudio del aspecto científico de las propiedades "íntimas" de los números, tanto en los griegos como en el desarrollo posterior de la humanidad, va conformando lo que en la actualidad conocemos como Teoría de los Números.

Para dar una idea de lo que abarca la Teoría de Números citamos a Beiler.[1]

> "Uno entra al terreno de la Teoría de Números y vagabundea tímidamente entre los enteros, los divisores y los primos, nombres que recuerdan la aritmética de los grados elementales. Pronto nos encontramos los números perfectos y los números amigables, es decir el número de divisores de un número y su suma. El camino se dirige dentro de lo nuevo y de ahí a la insospechada tierra de las congruencias; luego a través de la maleza de los Teoremas de Fermat y Wilson. Raíces primitivas, residuos cuadráticos, análisis Diofantino, exponentes de Haupt y reciprocidad cuadrática se revelan ante nosotros. Adelante hay dominios escabrozos donde el andar será lento y difícil: formas cuadráticas y particiones, ideales, ecuaciones de Pell, fracciones continuas, automorfismos, teoría de primos y teoría analítica de números".

En este curso, nuestro objetivo es introducirnos a la parte elemental de la Teoría de Números, conocer sus métodos y resultados más importantes.

---

1) RECREATIONS IN THE THEORY OF NUMBERS, the queen of mathematics entertains. Albert H. Beiler.

DIVISIBILIDAD. ALGORITMO DE LA DIVISION

Siguiendo el plan de estudiar las propiedades de los números enteros, lo primero que notamos son cuestiones del siguiente tipo: hay números pares, es decir, números que son exactamente divisibles entre dos; también hay números que son exactamente divisibles entre tres, etc. Esta clasificación de los números nos habla de una noción que está en la base del estudio de los números: la noción de divisibilidad. En forma general, ésta se refiere a aquellos casos en que un entero "cabe" un número exacto de veces en otro.

Euclides definió esto como sigue: "Un número es parte de un número, el menor del mayor, cuando mide al mayor" (Euclides en su definición, sólo se refiere a enteros positivos).

En términos modernos y precisos tenemos la siguiente

DEFINICION 1. Sean a y b enteros. Decimos que a divide a b si existe un entero c tal que $b = ac$.

La notación usual para indicar que a divide a b es $a \mid b$.

También es común decir, "a es factor de b", "a es divisor de b", o bien "b es múltiplo de a" o "b es divisible entre a".

Notemos que todo entero a tiene al menos a 1, -1, a y $-a$ como divisores.

Entre las primeras consecuencias importantes de la definición anterior están las siguientes propiedades:

PROPIEDADES:

i) $a \mid 0$ para todo entero a.

ii) $0 \mid a$ si y solo si, $a = 0$.

iii) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
iv) Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.
v) Si $a \mid b$, entonces $a \mid bc$ para todo entero c.
vi) Si $a \mid b$ y $a \mid c$, entonces $a \mid b + c$.
vii) Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$

La demostración de las primeras seis propiedades es inmediata a partir de la definición. A manera de ilustración, demostraremos las propiedades v) y vi)

v) Supongamos que $a \mid b$.
Entonces, por definición, existe un entero r tal que
$$b = ra$$
multiplicando en ambos lados de la igualdad por un entero c cualquiera, tenemos
$$bc = rac ;$$
asociando, resulta que:
$$bc = (rc)a,$$
de donde concluimos que
$$a \mid bc.$$

vi) Supongamos que $a \mid b$ y $a \mid c$.
Entonces, por definición, existen enteros m y n tales que
$$b = ma \quad y \quad c = na$$
sumando, obtenemos: $b + c = (m + n)a$,
de donde concluimos que $a \; b + c$.

Un concepto ampliamente utilizado es el de combinación lineal de dos (o más) enteros:

DEFINICION 2. Una combinación lineal de a y b es un entero de la forma $\lambda a + \gamma b$ donde λ y γ son enteros.[2]

---

2) Una combinación lineal de n enteros $a_1, a_2, \ldots, a_n$, es un entero de la forma $\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n$, donde $\lambda_1, \lambda_2, \ldots, \lambda_n$ son, a su vez, enteros.

Así por ejemplo, 13 y 56 son combinaciones lineales, respectivamente, de 5 y 3 y de 4 y 7, ya que

$$13 = (2)5 + (1)3 \qquad \text{y} \qquad 56 = (0)4 + (8)7.$$

Poco a poco vamos a darnos cuenta que la noción de combinación lineal es de suma importancia. Por lo pronto, un corolario importante que se obtiene de combinar las propiedades v) y vi) es el siguiente:

COROLARIO 1. Si $a \mid b$ y $a \mid c$, entonces
a divide a cualquier combinación lineal de b y c.

En forma simbólica:
$a \mid b$ y $a \mid c$, entonces
$a \mid \lambda b + \gamma c$ para todo λ y γ enteros.

Dem.
En virtud de v), como $a \mid b$ y $a \mid c$, entonces
$a \mid \lambda b$ y $a \mid \gamma c$, λ y γ enteros.
por lo tanto, de vi) se sigue que
$a \mid \lambda b + \gamma c$ para todo λ y γ enteros.

Después de este corolario, una pregunta que se ocurre es la siguiente: ¿la implicación recíproca se valdrá?, es decir, ¿si un número a divide a cualquier combinación lineal de b y c, entonces $a \mid b$ y $a \mid c$?

La respuesta es sí; pero es importante hacer notar que lo que garantiza su validez es el hecho de que a divide a cualquier combinación lineal de b y c. En efecto, como a divide a cualquier combinación lineal de b y c, en particular divide a las combinaciones lineales

$$b(0) + c(1) = c \qquad \text{y} \qquad b(1) + c(0) = b.$$

EJEMPLO. $b = 2$, $c = 6$ y $a = 4$
28 es combinación lineal de 2 y 6, ya que
$28 = 2(5) + 6(3)$

4 28 , es decir, a b(5) + c(3)
y sin embargo
a no divide a b y a no divide a c

¿Este ejemplo contradice lo anteriormente?
No, lo que ocurre aquí, es que a = 4 no divide a toda combinación lineal de 2 y 6 .

Quedan como ejercicio las demostraciones de las demás propiedades enunciadas.

Es evidente que en los enteros no siempre es posible dividir de tal suerte que el resultado sea de nuevo un número entero (esto sólo sucede cuando el dividendo es múltiplo del divisor). Sin embargo, lo que si es cierto es que al dividir cualesquiera dos enteros siempre obtenemos, en forma única, un cociente y un residuo, que sí son enteros. Por ejemplo:

$$13\overline{)28}\quad 2$$

2

En este caso el cociente es 2 y el residuo es 2. Otra forma de expresar la división anterior es a través de la siguiente igualdad

$$28 = 13 \cdot 2 + 2$$

Es evidente que el residuo en cualquier división, siempre es menor que el divisor, puesto que en caso contrario seguiríamos dividiendo. Basándonos en este ejemplo y en estas observaciones, el hecho de que siempre es posible dividir dos enteros positivos cualesquiera para obtener un cociente y un residuo únicos, lo podemos enunciar en forma general como sigue:

ALGORITMO DE LA DIVISION PARA ENTEROS POSITIVOS
Sean a y b enteros positivos con $a \neq 0$
Entonces existen enteros q y r únicos tales que

$$b = aq + r \quad y \quad 0 \leq r < a$$

(Obsérvese que en este enunciado, b es el dividendo,

a el divisor, q el cociente y r el residuo).

Por supuesto que esta afirmación, a pesar de ser tan evidente, requiere demostración. Antes de proceder a ella, conviene ver algunos ejemplos.

Consideremos a=13 y b=28 en este caso q=2 y r=2, es decir,

$$28 = 13.2 + 2$$

Sin embargo, también sucede que $28 = 13.1 + 15$, más aún:

$$\begin{aligned} 28 &= 13.0 + 28 \\ 28 &= 13.1 + 15 \\ 28 &= 13.2 + 2 \\ 28 &= 13.3 + (-11) \\ 28 &= 13.4 + (-24) \end{aligned}$$

.
.
.

Nótese que los "residuos" (los sumandos de la derecha) siempre difieren consecutivamente en 13 y que el <u>único</u> que es nonegativo y menor que el divisor es el <u>menor</u> de todos los residuos nonegativos, que en este caso es 2. Veamos otro ejemplo.

Sean a=35 y b=8 entonces $35 = 8.4 + 3$ de donde q=4 y r=3

Sin embargo:

.
.
.

$$\begin{aligned} 35 &= 8.2 + 19 \\ 35 &= 8.3 + 11 \\ 35 &= 8.4 + 3 \\ 35 &= 8.5 + (-5) \\ 35 &= 8.6 + (-13) \end{aligned}$$

.
.
.

Aquí volvemos a observar el mismo fenómeno. En particular,

de nuevo sucede que el menor de los números nonegativos que aparecen hasta la derecha es el único "residuo" que simultaneamente es nonegativo y menor que el divisor. Modificando ligeramente las listas anteriores, podemos escribir los residuos de la siguiente manera:

.	.
.	.
.	.
$28 - 13.0 = 28$	$35 - 8.2 = 19$
$28 - 13.1 = 15$	$35 - 8.3 = 11$
$28 - 13.2 = 2$	$35 - 8.4 = 3$
$28 - 13.3 = -11$	$35 - 8.5 = -5$
$28 - 13.4 = -24$	$35 - 8.6 = -13$
.	.
.	.
.	.

Con lo que hemos visto ya podemos conjeturar lo siguiente sobre el caso general: Que dados los enteros a y b,

1) Hay una multitud de enteros q y r tales que
$$b = aq + r.$$
2) todos los residuos son de la forma
$$b - ax \quad ,$$
donde x es algún entero. Ademas, la diferencia entre cualesquiera dos residuos siempre es multiplo de a.
3) El menor de todos los "residuos"
$$b - ax \geq 0$$
es un número r que satisface
$$0 \leq r < a.$$

De estas conjeturas, la que nos va a servir para la demostración es la tercera. Requerimos tambien del Principio del Buen Orden, que simplemente enunciamos a continuación.

PRINCIPIO DEL BUEN ORDEN

Sea A un subconjunto no vacío de números naturales entonces A tiene un elemento m mínimo; es decir,

$\exists\ m \in A$ tal que $m \leq n$ para todo $n \in A$.

Ahora si, la demostración del ALGORITMO DE LA DIVISION para enteros positivos:

Dem.

Sean a y b enteros positivos. Lo primero que vamos a demostrar es la existencia de números enteros q y r tales que

$$b = aq + r \quad y \quad 0 \leq r < a$$

Para esto, consideremos al conjunto

$$A = \{ b - ax \geq 0 \mid x \in Z \}$$

(Obsérvese que este es el conjunto de "residuos" nonegativos)

evidentemente, $A \neq \emptyset$ ya que

$$0 \leq b = b - a.0 \in A$$

Entonces, por el P. del B.O., A tiene un elemento mínimo r.

Como $r \in A$, entonces r es de la forma $b - aq$, donde q es algún entero; es decir $b - aq = r$, y por -- tanto, $b = aq + r$.

Además $r \geq 0$. Ahora hay que probar que $r < a$; para esto, supongamos que $r \geq a$, entonces

$$0 \leq r - a = (b - aq) - a$$
$$= b - a(q + 1) \in A$$

y además $r - a < r$, lo cual es imposible ya que r es el elemento mínimo de A.

Por lo tanto: $r < a$.

En resumen, hemos probado que existen q y r tales que

$$b = aq + r, \qquad 0 \leq r < a \quad ...(1).$$

Para probar la unicidad, supongamos que existen q_1 y r_1 tales que

$$b = aq_1 + r_1, \qquad 0 \leq r_1 < a \quad ...(2).$$

De (1) y (2) tenemos que

$$aq + r = aq_1 + r_1$$

sin pérdida de generalidad podemos suponer que $q \geq q_1$ entonces

$$a(q - q_1) = r_1 - r \quad ...(3).$$

Por otra parte, de las desigualdades (1) y (2) tenemos que

$$r_1 - r < a$$

combinando todo esto llegamos a que

$$0 \leq a(q - q_1) = r_1 - r < a$$

puesto que todos los valores son positivos, cancelamos y obtenemos

$$0 \leq q - q_1 < 1$$

de donde se sigue que $q - q_1 = 0$ y por ende $q = q_1$.

Sustituyendo en (3), tenemos $r = r_1$, y el resultado queda demostrado.

Conviene notar que aunque hemos establecido el algoritmo de la división para enteros positivos, éste se puede generalizar a todos los enteros. En efecto, en este caso tenemos:

Algoritmo de la División en Z.

Sean a y b enteros con $a \neq 0$ entonces existen enteros q y r únicos tales que

$$b = aq + r \qquad 0 \leq r < |a|$$

Una vez que se conoce la demostración para a y b positivos, la demostración para el caso general no ofrece dificultades esenciales adicionales. Todo el problema es "separar en casos". Es conveniente que el lector haga algunos ejemplos con los números $a > 0$ y $b < 0$, $a < 0$ y $b > 0$ y $a < 0$ y $b < 0$ antes de hacer la demostración para el caso general.

MAXIMO COMUN DIVISOR

Para introducir este concepto planteamos el siguiente problema: ¿ Como le hacemos para obtener 4l de agua si sólo tenemos dos jarras, una de 3l de capacidad y otra de 5l de capacidad? (Por supuesto no estan graduadas las jarras).

La idea es combinar el uso de estas jarras para obtener los 4 litros de agua. Para empezar, con una notación adecuada se puede simplificar la forma de resolver el problema. Por ejemplo, podemos usar parejas ordenadas (a,b); la componente a corresponde a la jarra de 3 litros y b a la de 5 litros. Así si escribimos (0,0) significa que ambas jarras están vacías; la pareja (3,0) que la jarra de 3 litros esta llena y la de 5 vacía,etc..Si escribimos una lista de parejas como la siguiente:

(0,0)
(3,0)
(0,3)
(3,3) ——→ 6l

Lo que queremos indicar es un proceso de vaciar y llenar ambas jarras de esta manera: Partimos de que ambas jarras están vacías (escribimos la pareja (0,0)); luego, llenamos la de 3 l (escribimos (3,0)); luego, vaciamos estos 3l en la jarra de 5l (escribimos(0,3)) y por último, volvemos a llenar la de 3l(escribimos(3,3)). En total, hemos obtenido 6l (como lo indica la flecha "——→6l").

Cada lista de parejas que escribamos significará un proceso de este estilo.

La idea es encontrar una lista que nos lleve finalmente a obtener 4l (se sobreentiende, por ejemplo, que ninguna lista puede empezar con la pareja (2,0) puesto que nuestras jarras, no graduadas, son solo de 3l y 5l respectivamente).

La siguiente es una forma de obtener 2l :

(0,0)
(0,5)

(3,2)
(0,2) ⟶ 2l

(El lector debe asegurarse que entiende todos los pasos). continuando el mismo procedimiento

(2,0)
(2,5) ⟶ 7l

obtenemos 7l.

Procediendo al tanteo es fácil obtener 4l .

Habiendonos puesto de acuerdo en una notación, vamos a resolver el problema planteado.

(0,0)
(3,0)
(0,3)
(3,3) ⟶ 6l
(1,5)
(1,0) ⟶ 1l
(0,1)
(3,1)
(0,4) ⟶ 4l

Observemos que también puedo obtener un 1l y 6l.

¿Con estas 2 jarras cuáles son <u>todos</u> los números n de litros que podemos obtener?

Revisando las listas vemos que podemos obtener 1,2,3,4, 5,6,7,8l y con ellos, cualquier número n de litros.

Se plantea otra vez la misma situación, pero las jarras son de 12l y 14l de capacidad y la pregunta es ¿Cómo obtener 5l y 6l?

(0,0)
(12,0)
(0,12)
(12,12)
(10,14)
(10,0)
(0,10)
(12,10)
(8,14)
↓
(12,8)
(6,14)
(6,0) ⟶ 6l

(8,0)
(0,8)

Hasta aqui, hemos obtenido 6l pero no ha aparecido 5l, sigamos buscando.

(0,0)	(12,8)
(12,0)	(6,14)
(0,12)	(6,0) ⟶ 6l
(12,12)	(0,6)
(10,14)	(12,6)
(10,0)	(4,14)
(0,10)	(4,0)
(12,10)	(0,4)
(8,14)	(12,4)
(8,0)	(2,14)
(0,8)	(2,0)

No es posible obtener 5l, ya que nunca aparece el 5 en la lista y de cóntinuar vaciando y llenando, solo estaría repitiendo los pasos que ya están aquí.

Entonces ¿que números n de litros podemos obtener de estas 2 jarras?

De la lista se desprende que es posible obtener 2,4,6, 8,10,12,14,16,18,20,22,24,26 litros y con estos podemos también obtener.

28,30,32,..., n = 2k, ...

¿Por qué no podemos obtener 5l con las jarras de 12l y 14l ? En el primer problema fué posible encontrar nl para cualquier n, ¿ cuándo es posible esto ?.

Observemos que lo que hicimos en los dos problemas fué llenar uno de los recipientes y pasarlo al otro; volver a llenarlo, pasar litros al otro y cuando el segundo el segundo recipiente se llena, tiramos esos litros,etc. hasta encontrar los litros deseados, es decir, estamos llenando un recipiente cierto número de veces y tirando (cuando está lleno) cierto número de veces los litros del segundo recipiente. Revisemos por ejemplo, el problema anterior en el que se obtuvieron los 6l.

	(0,0)	
llenamos el de 12l	(12,0)	
	(0,12)	
llenamos el de 12l	(12,12)	
	(10,14)	
	(10,0)	tiramos los 14l
	(0,10)	
llenamos el de 12l	(12,10)	
	(8,14)	
	(8,0)	tiramos los 14l
	(0,8)	
llenamos el de 12l	(12,8)	
	(6,14)	
	(6,0)	tiramos los 14l

$\longrightarrow$ 6l

En total, llenamos 4 veces el recipiente de 12l y tirámos 3 veces el de 14l algebraicamente esto lo podemos escribir como

$$4\ (12) - 3\ (14) = 48 - 42 = 6.$$

Preguntar que otras cantidades de litros podemos obtener con ricipientes dc 12l y 14l es preguntar qué números podemos obtener al llenar de agua m veces un recipiente y tirarla n veces del otro, es decir, qué números enteros obtenemos, al variar m y n en los enteros, con

$$12\ m - 14\ n,$$

o bien,

$$14\ m - 12\ n;$$

en cualquiera de los dos casos lo que sabemos es que el resultado tendra la forma de un múltiplo de dos:

$$12\ m - 14\ n = 2\ (6\ m - 7\ n) = 2x \qquad \text{para algún } x \text{ natural}$$

$$14\ m - 12\ n = 2\ (7\ m - 6\ n) = 2y \qquad \text{para algún } y \text{ natural}$$

Así que en este problema no podemos obtener 5l porque 5 no es par.

Puesto así el problema, es facil responder la pregunta

de las posibles cantidades de litros que obtengo con recipientes de 15l y 24l.

Con estos 15 y 24 sólo obtengo números de la forma

$$15\,m - 24\,n = 3\,(5\,m - 8\,n) = 3x$$

para x natural.

Así que con recipientes de 24l y 40l ¿cuáles obtengo? bueno, pues los de la forma:

$$24\,m - 40\,n = 2\,(12\,m - 20\,n) = 2x$$

para algún x natural.

Es cierto que con estos recipientes obtengo pares, pero no obtengo todos los pares, sólo los pares que tienenla forma 4y para alguna y natural:

$$\begin{aligned} 24\,m - 40\,n &= 2\,(12\,m - 20\,n) \\ &= 2\,.\,2\,(6\,m - 10\,n) \\ &= 4\,(6\,m - 10\,n) \\ &= 4y \end{aligned}$$

Pero no, nosontodos los de esta forma tampoco, todavía puedo factorizar en $6\,m - 10\,n$:

$$\begin{aligned} 24\,m - 40\,n &= 4\,(6\,m - 10\,n) \\ &= 4\,.\,2\,(3\,m - 5\,n) \\ &= 8\,(3\,m - 5\,n) \\ &= 8z \qquad \text{para z natural} \end{aligned}$$

Ahora sí, obtenemos los que tienen la forma 8z, es decir,múltiplos de 8 ¿ Ycómo sé que aparte de ser múltiplos de 8 no son múltiplos de otro número mayor ? Bueno, pues porque ya no puedo factorizar ningún otro número de $3\,m - 5\,n$, dado que 3 y 5 no tienen factores comunes, exepto el uno claro, pero este al factorizarlo me deja todo igual.

Así que la forma que tienen los números que puedo obtener en este caso es la de ser múltiplos del factor común más grande de 24 y 40.

Y este factor común más grande es el máximo común divisor de 24 y 40, que es 8.

Lo que podemos observar y conjeturar es lo siguiente:

En general, dados dos enteros a y b , los únicos valo-

res es que podemos obtener con

$$ax + by \quad \text{para} \quad x, \ y \ \text{enteros}$$

son los múltiplos del m.c.d. de a y b.

Si llamamos d a este m.c.d. de a y b entonces,

$$ax + by = dr \quad \text{para} \quad x, y, r \ \text{enteros}$$

Esta expresión nos muestra que cada dr_0 es una combinación lineal de a y b, $(dr_0 = ax_0 + by_0)$, en particular $d \cdot 1 = d$ es combinación lineal de a y b, pero además, d es el número positivo más chico que podemos obtener de todos los múltiplos de d. En otras palabras,

d es la mínima combinación lineal positiva de a y b

Los ejemplos que vimos nos llevan a la pregunta:

Dado c entero, ¿Cuándo c es combinación lineal de a y b?

La respuesta es: cuando c es múltiplo del máximo común divisor de a y b. En otras palabras c es combinación lineal de a y b si el m.c.d. de a y b es divisor de c.

Esta misma pregunta podemos expresarla en términos de ecuaciones.

¿Cuándo $ax + by = c$ tiene solución entera?

A las ecuaciones de este tipo, en las que se trata de encontrar soluciones enteras se les llama ecuaciones Diofantinas (donde a, b y c son enteros).

Lo que estamos conjeturando es que:

una ecuación Diofantina tiene solución si y solo si

c es múltiplo del m.c.d. de a y b.

Pasemos a formalizar estos resultados.

Todo entero , que divide simultaneamente a los enteros a y b , se llama divisor común de los mismos.

DEFINICION 1. Al mayor de los divisores comunes de los enteros a y b se le llama máximo común divisor y se designa con la notación (a,b)

También utilizaremos las iniciales m.c.d. de a y b para referirnos al (a,b).

Dados dos números enteros a y b distintos de cero ¿siempre existe el m.c.d. de ellos?

Sí. Por un lado el conjunto de divisores comunes es distinto del vacio ya que, el 1 pertenece a dicho conjunto. Por otro lado, para cada número entero distinto de cero, tenemos un número finito de divisores, luego, el conjunto de divisores comunes es finito. Por lo tanto existe el m.c.d. de a y b .

Si los números son a = 0 , b = 0 , no tiene sentido hablar de su m.c.d. ya que los divisores de 0 son todos los enteros.

Si a = 0 y b un entero distinto de cero, sus divisores comunes son los divisores de b y por tanto (0,b) = b .

Notemos que dada la definición del m.c.d. de a y b , éste resulta ser positivo, es decir, (a,b) > 0

Pasemos ahora al siguiente problema: Dados a y b enteros distintos de cero ¿cómo encontrar su m.c.d.?

EJEMPLO 1. Si a = 8 y b = 14
Encontrar (a,b)

los divisores de a son: $\pm 1, \pm 2, \pm 4, \pm 8$
los de b : $\pm 1, \pm 2, \pm 7, \pm 14$
los divisores comunes : $\pm 1, \pm 2$

por tanto (a,b) = 2

Si los números a y b son los siguientes

$$a = 2,784 \qquad y \qquad b = 4,988$$

se nota que aplicar el procedimiento anterior para encontrar su m.c.d. resultaría muy latoso.

Busquemos otro procedimiento para encontrar (a,b)

Sean a , b enteros distintos de cero

TEOREMA 1. Si $a \mid b$ entonces $(a,b) = |a|$

Dem.

Todo divisor común de a y b es un divisor de a.

Reciprocamente:

Todo divisor de a es un divisor común de a y b, ya que todo divisor de a es divisor de b.

En efecto, si d_1 es divisor de a, entonces

$$a = d_1 q_1,$$

y como $b = a\,q$,

entonces $b = d_1(q_1 q)$;

luego, d_1 es divisor de b.

Por lo tanto, el conjunto de divisores comunes de a y b coincide con el conjunto de divisores de a y como el máximo de éste último conjunto es $|a|$ resulta que:

$$(a,b) = |a|$$

TEOREMA 2. Si $b = aq + r \qquad 0 \leq r < |a|$
entonces $(b,a) = (a,r)$

Dem.

Vamos aprobar que el conjunto de divisores comunes de a y b coincide con el conjunto de divisores comunes de a y r.

Todo divisor de a y b es divisor de r:

En efecto, si d_1 es divisor de a y b, esto es, si $d_1 \mid a$ y $d_1 \mid b$

entonces

$$d_1 \mid b - aq = r$$

es decir,

$$d_1 \text{ es divisor de } r .$$

Por consiguiente, todo divisor de a y b es divisor de a y r .

Reciprocamente:

Todo divisor de a y r es divisor de a y b .

En efecto, si

$$d_1 \mid a \quad y \quad d_1 \mid r$$

entonces

$$d_1 \mid aq + r = b,$$

luego, todo divisor de a y r es divisor de a y b.

Por lo tanto los divisores comunes de a y b coinciden con los de a y r ; en particular, tiene que coincidir el mayor de estos divisores, es decir:

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

Así, encontrar el m.c.d. de a y b se reduce a encontrar el de a y r, que son números menores que b ; de este modo, si a es múltiplo de r , entonces;

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

en caso contrario

$$a = rq_1 + r_1 \qquad 0 \leq r_1 < |r| ,$$

y entonces

$$(a,b) = (a,r) = (r,r_1) \quad ;$$

continuamos el mismo procedimiento hasta que para alguna i , r_i sea múltiplo de r_{i+1} , en cuyo caso

$$(a,b) = (a,r) = \ldots = (r_i,r_{i+1}) = r_{i+1} .$$

A este procedimiento se le llama Algoritmo de Euclides y lo vamos a reescribir de la siguiente manera:

Sean a y b enteros. El proceso de aplicar iteradamente el Algoritmo de la División, como sigue, es llamado el Algoritmo de Euclides:

$$
\left.
\begin{aligned}
b &= aq + r & 0 &\leq r < |a| \\
a &= rq_1 + r_1 & 0 &\leq r_1 < r \\
r &= r_1q_2 + r_2 & 0 &\leq r_2 < r_1 \\
&\vdots & &\vdots \\
r_{n-1} &= r_nq_{n+1} + r_{n+1} & 0 &\leq r_{n+1} < r_n \\
r_n &= r_{n+1}q_{n+2}
\end{aligned}
\right\} \quad (1)
$$

Este proceso termina cuando se obtiene un residuo cero. - Puesto que la sucesión $|a|$, r , r_1 , ... , de enteros decrecientes es finita (no puede contener más de a enteros positivos) , se garantiza que el proceso termina.

Ahora si, nuestro nuevo procedimiento para encontrar el m.c.d. de a y b es: efectuar sobre a y b el Algoritmo de Euclides y por los Teoremas 1 y 2

$$(a,b) = r_{n+1}$$

es decir, el m.c.d. de a y b es el último resto distinto de cero del Algoritmo de Euclides.

EJEMPLO 2.

Aplicando el Algoritmo de Euclides, encontrar el m.c.d. de $a = 2,784$ y $b = 4,988$

$$
\begin{aligned}
4,988 &= 2,784(1) + 2,204 \\
2,784 &= 2,204(1) + 580 \\
2,204 &= 580(3) + 464 \\
580 &= 464(1) + 116 \\
464 &= 116(4)
\end{aligned}
$$

por lo tanto $(4,988,2,784) = 116$.

Habíamos conjeturado que (a,b) es combinación lineal de a y b ¿Cómo demostrar esto?.

Una manera de hacerlo es exhibiendo una combinación lineal de a y b que de (a,b).

El mismo algoritmo de Euclides nos da un procedimiento para encontrar dicha combinación lineal.

Sean a y b dos enteros. Aplicamos el algoritmo de Euclides, (1), entonces:

$$(a,b)=r_{n+1}$$

directamente de la serie de igualdades (1) obtenemos que:

$$r_{n+1} = r_{n-1} - r_n q_{n+1} \cdots\cdots (2)$$

es decir obtengo r_{n+1} como combinación lineal de r_{n-1} y r_n, pero a su vez r_n y r_{n-1} son combinaciones lineales de residuos anteriores, que sustituyendolas en (2) queda r_{n+1} como combinación lineal de r_{n-2} y de r_{n-3}, así sucesivamente vamos sustituyendo los residuos por su combinación lineal de residuos índices menores hasta llegar a que

r_{n+1} es combinación lineal de a y b.

Así con este procedimiento descrito se obtiene una combinacion lineal de a y b que resulta ser el m.c.d. de esos dos números. Para fijar ideas, encontremos los valores x_0 y y_0 tales que

$$ax_0 + by_0 = (a,b)$$

con los valores a y b del ejemplo 2

EJEMPLO 3.

a = 2784 y b = 4988 , (a,b) = 116.

Buscamos x_0, y_0 enteros tales que

$2784x_0 + 4988y_0 = 116$

escribamos el Algoritmo de Euclides

$4988 = 2784(1) + 2204$

$2784 = 2204(1) + 580$

$2204 = 580(3) + 464$

$580 = 464(1) + 116$

$464 = 116(4)$,

lo podemos reescribir como:

$4988 - 2784(1) = 2204$

$2784 - 2204(1) = 580$

$2204 - 580(3) = 464$

$580 - 464(1) = 116$,

de estas igualdades tenemos:

116 = 580 464

sustituyendo 464 por su combinación lineal tenemos

$116 = 580 - [2204 - 580(3)]$;

agrupando,

$116 = 580(4) - 2204$,

sustituyendo 580,

$116 = [2784 - 2204]4 - 2204$

$= 2784(4) - 2204(5)$;

por último, sustituyendo 2204,

$116 = 2784(4) - [4984 - 2784](5)$,

de donde:

$116 = 2784(9) - 4988(5)$.

Por lo tanto 116 queda expresado como combinación lineal de 2784 y 4988.

Mencionamos también que (a,b) es la mínima combinación lineal positiva de a y b. Veamos.

TEOREMA 3.

Sean a,b enteros distintos de cero $(a,b) = d \Leftrightarrow d$ es la mínima combinación lineal positiva de a y b

PRIMERA PARTE: Sea $d = ka + lb$, k,l enteros, d entero positivo la mínima combinación lineal positiva de a y b

P.D. $d = (a,b)$

Dividiendo a entre d tenemos que

$$a = dq + r \quad \text{con} \quad 0 \leq r < d,$$

de donde

$$r = a - dq;$$

sustituyendo d:

$$r = a - (ka + lb)q,$$

reagrupando resulta que

$$r = (1 - kq)a + (-lq)b,$$

es decir, r es combinación lineal de a y b; pero $0 \leq r < d$ esto implica que $r = 0$ ya que d es la com

binación lineal positiva de a y b mínima.

Por lo tanto

$a = dq$; es decir, $d|a$.

Lo mismo ocurre si dividimos b entre d: llegamos a que;

$b = dq'$, es decir, $d|b$;

De donde, d es divisor comùn de a y b.

Falta probar que d es el máximo divisor común.

Si c es otro divisor común, entonces

$a = ct$ y $b = ct'$

como $d = ka + lb$,

sustituyendo a y b obtenemos que

$d = c(kt + lt')$,

es decir, $c|d$,

de donde $c \leq d$

∴ d es el máximo común divisor de a y b.

SEGUNDA PARTE: Si $d = (a,b)$,

P.D. $d = la + kb$ es la mínima combinación lineal positiva .

Supongamos que $h = \alpha a + \beta b > 0$ es cualquier combinación lineal positiva de a y b.

Como $d|a$ y $d|b$

entonces $d|\alpha a + \beta b$,

es decir, $d|h$, donde $d \leq h$,

y por lo tanto d es la mínima combinación lineal positiva, quedando así demostrado el teorema 3.

ALGUNAS PROPIEDADES DEL (a,b)

Sean a y b enteros distintos de cero

1) $(am,bm) = (a,b)m$, donde m es un entero positivo
2) Si d' es un divisor común de a y b, entonces

$(a/d', b/d') = (a,b)/|d'|$ y en particular se tiene que

$(a/(a,b),\ b/(a,b)) = (a,b)/(a,b) = 1$

3) Si $(a,b) = 1$ $\quad (ac,b) = (c,b)$

4) Si $(a,b) = 1$ y $a|bc \quad a|c$.

DEMOSTRACION DE LAS PROPIEDADES DE (a,b)

1) $(am,bm) = (a,b)m$, donde m es un entero positivo.

DEM. Utilizando el algoritmo de Euclides :

$$\left.\begin{array}{ll} b = aq + r \ , & 0 \leq r < |a| \\ a = rq_1 + r_1 \ , & 0 \leq r_1 < r \\ \vdots & \vdots \\ r_{n-1} = r_n q_{n+1} + r_{n+1} \ , & 0 \leq r_{n+1} < r_n \end{array}\right\} \ldots(1)$$

$$r_n = r_{n+1} q_{n+2}$$

tenemos que $(a,b) = r_{n+1}$.

Multiplicando las relaciones (1) término a término por m. Obtendremos las nuevas relaciones

$$\begin{array}{ll} bm = amq + rm \ , & 0 \leq rm < |a|m \\ am = rmq_1 + r_1 m \ , & 0 \leq r_1 m < rm \\ \vdots & \vdots \\ r_{n-1} m = r_n m q_{n+1} + r_{n+1} m \ , & 0 \leq r_{n+1} m < r_n m \end{array}$$

$$r_n m = r_{n+1} m q_{n+2} \ ,$$

de las cuales tenemos que ,

$$(bm,am) = r_{n+1} m \ .$$

Por lo tanto $(bm,am) = (a,b)m$. (Notemos que esta propiedad se cumple para m entero con la siguiente modificación :

$(am,bm) = (a,b)|m|$

queda probar esta modificaciòn como ejercicio)

2) Si d' es un divisor comùn de a y b , entonces $\left(\frac{a}{d'} ; \frac{b}{d'}\right) = \frac{(a,b)}{|d'|}$.

DEM:

$(a,b) = \left(\frac{ad'}{d'} , \frac{bd'}{d'}\right)$,

aplicando la propiedad 1 tenemos que

$(a,b) = \left(\frac{ad'}{d'} , \frac{bd'}{d'}\right) = \left(\frac{a}{d'} , \frac{b}{d'}\right)|d'|$,

de donde $\frac{(a,b)}{|d'|} = \left(\frac{a}{d'} , \frac{b}{d'}\right)$.

En particular, como (a,b) es divisor comùn de a y b, tenemos que:

$$\left(\frac{a}{(a,b)} , \frac{b}{(a,b)}\right) = \frac{(a,b)}{(a,b)} = 1$$

3) Si $(a,b) = 1$ entonces $(ac,b) = (c,b)$

DEM:

$(ac,b)|ac$ y $(ac,b)|b$,

luego, $(ac,b)|ac$ y $(ac,b)|bc$.

Entonces, (ac,b) divide a cualquier combinaciòn lineal de ac y bc, en particular, a (ac,bc);

es decir, $(ac,b)|(ac,bc)$,

pero $(ac,bc) = c(a,b)$ ... (propiedad 1)

y como por hipótesis $(a,b) = 1$ entonces tenemos que $(ac,b)|c$.

Luego, como $(ac,b)|b$ y $(ac,b)|c$

entonces $(ac,b)|(b,c)$

y por lo tanto $(ac,b) \leq (b,c)$ . . . . (*)

Por otro lado $(b,c)|b$ y $(b,c)|c$

luego $(b,c)|b$ y $(b,c)|ac$

entonces (b,c) divide a cualquier combinaciòn lineal de b y ac, en particular a (ac,b);

es decir, $(b,c)|(ac,b)$

y por lo tanto $(b,c) \leq (ac,b)$ . . . . (**)

Por (*) y (**) tenemos que $(ac,b) = (b,c)$

4) Si $(a,b) = 1$ y $a|bc$ entonces $a|c$

DEM:

Como $(a,b) = 1$ entonces existen α, β enteros tales que $1 = \alpha a + \beta b$; multiplicando por c tenemos que $c = \alpha ca + \beta cb$, pero por hipótesis $bc = aq$ con q entero, entonces $c = \alpha ca + \beta qa$ luego $c = a(\alpha c + \beta q)$ y por lo tanto $c|a$.

EJERCICIOS

1. Demostrar que si $a \neq 0$ el conjunto de divisores de a es finito.

2. Aplicando el algoritmo de Euclides hallar
   i) (6188, 4709)
   ii) (34 121, 452)

3. Encontrar (a,b) y expresarlo como combinación lineal de a y b cuando:
   i) a = 56 b = 72
   ii) a = 2184 b = 1764
   iii) a = 1901 b = 601

4. Poisson (181-1840) siendo un jovencito le fue planteado un problema. Interesado en él posteriormente quedó absorto por la matemática y le dedicó toda su vida. He aquí el problema:

   Se tienen 12 pintas de vino y se quiere vaciar la mitad en otro recipiente, pero se cuenta sólo con recipientes de capacidades de 8 y 5 pintas. Se pregunta de qué manera vaciar 6 pintas de vino en el recipiente de 8 pintas.

5. Sea un número de tres cifras. Si le agregamos 6 a dicho número, éste resulta divisible entre 7. Si al número original le agregamos 7, éste resulta divisible entre 8. Si al número original le agregamos 8, éste es divisible entre 9. ¿Cuál es el número?

6. Los números 4373 y 826 al dividirlos entre un mismo número se obtuvieron respectivamente los residuos 8 y 7. ¿Entre qué número se dividió?

7. Pruebe que si a y b son enteros impares, entonces $a^2 - b^2$ es divisible entre 8.

8. Sea $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ con a_i enteros $i = 1, 2, \ldots, n$ y $a_n \neq 0$. Demostrar que si $\frac{r}{s} \in Q$ (con $(r,s) = 1$) es raíz del polinomio p(x), entonces r a_0 y s a_n ¿Es cierto el recíproco de esta proposición?

9. Demostrar que $3 \mid n^{13} - n \quad n \in \mathbb{N}$.

10. Demostrar que $13 \mid n^{12} - a^{12}$ si $(n,13) = (a,13) = 1$

11. Los siguientes son criterios "usuales" de divisibilidad. Probar que:
i) Un número es divisible entre 2 si y sólo si su último dígito (de izquierda a derecha) es divisible entre 2.
ii) Un número es divisible entre 3 si y sólo si la suma de sus dígitos es divisible entre 3.
iii) Un número es divisible entre 8 si y solo si el entero formado por sus 3 últimos dígitos es divisible entre 8.

12. Sean a, b y m enteros. Demostrar que si $(a,m) = (b,m) = 1$ entonces $(ab,m) = 1$.

13. Sean b, c y r enteros. Demostrar que si $(b,c) = 1$ y $r \mid b$ entonces $(r,c) = 1$

14. Sean a, b y c enteros $c \neq 0$. Demostrar que
$|c|(a,b) = (ca,cb)$

15. Sean $a_1, a_2, \ldots, a_n$ enteros. Formemos la sucesión de números $(a_1,a_2) = d_2$, $(d_2,a_3) = d_3$, $\ldots$, $(d_{n-1},a_n) = d_n$.
i) Probar que el número d_n obtenido de este modo será el m.c.d. de todos los números dados.
ii) Encontrar (81719,52003,33649,30107).

ECUACIONES DIOFANTINAS

TEOREMA 1. Dados a, b, c enteros, a y b distintos de cero, la ecuación $ax + by = c$ tiene solución en los enteros si y solo si $(a,b)|c$.

DEM:

Supongamos que la ecuación

$$ax + by = c \qquad (1)$$

tiene solución.

P.D. $(a,b)|c$.

Como (1) tiene solución existen x_o, y_o enteros tales que

$$ax_o + by_o = c$$

Como $(a,b)|a$ y $(a,b)|b$

entonces $(a,b)|ax_o + by_o = c$

es decir $(a,b)|c$

Reciprocamente supongamos que $(a,b)|c$

P.D. existen x_o, y_o enteros tales que $ax_o + by_o = c$

Sabemos que $(a,b) = \alpha a + \beta b$ para α y β enteros y por hipótesis $c = (a,b)r$ para r entero

entonces $c = (\alpha a + \beta b)r$

de donde $c = a(\alpha r) + b(\beta r)$

Sea $\alpha r = x_o$ y $\beta r = y_o$

Por lo tanto existe $x_o = \alpha r$ y $y_o = \beta r$ enteros tales que

$$ax_o + by_o = c$$

Quedando así demostrado el teorema.

Este teorema establece una condición necesaria y suficiente para que una ecuación diofantina tenga solución. Y la demostración nos da una manera de encontrar una solución para dichas ecuaciones.

Repitamos, con un ejemplo el procedimiento para encontrar la solución.

EJEMPLO 1.

$$114x + 312y = 30$$

Buscamos el m.c.d. de 114 y 312 por el algoritmo de de Euclides.

$$
\left.\begin{aligned}
312 &= 114(2) + 84\\
114 &= 84(1) + 30\\
84 &= 30(2) + 24\\
30 &= 24(1) + 6\\
24 &= 6(4)
\end{aligned}\right\} \qquad (2)
$$

Por lo tanto $(114,312) = 6$

como $(114,312) \mid 30$

la ecuación $114x + 312y = 30$ tiene solución, para encontrarla (según el procedimiento de la demostración), necesitamos x y y enteros tales que:

$$x\,114 + y\,312 = 6$$

Para esto utilizamos nuevamente el algoritmo de Euclides. Despejando los residuos de (2) tenemos:

$84 = 312 - 114(2)$

$30 = 114 - 84$

$24 = 84 - 30\ (2)$

$6 = 30 - 24$

Sustituyendo los valores de los residuos y agrupando obtenemos

$$
\begin{aligned}
6 &= 30 - 24\\
&= 30 - (84 - 30(2))\\
&= 30(3) - 84(4)\\
&= (114 - 84)(3) - 84\\
&= 114(3) - 84(4)\\
&= 114(3) - (312 - 114(2))(4)\\
&= 114(11) - 312(4),
\end{aligned}
$$

es decir, $6 = 114(11) + 312(-4)$

y como $30 = 6 \cdot 5 = 114(55) + 312(-20)$

tenemos que la solución de la ecuación

$$114x + 312y = 30$$

es $x_0 = 55$ y $y_0 = -20$

Así hemos obtenido <u>una</u> solución para la ecuación. La pregunta que inmediatamente surge es ¿será la única? Si hay más ¿cuántas son? y ¿cómo encontrarlas?

Para responder a esto veamos el caso de la ecuación diofantina más sencilla.

Sean a, b y c enteros; a y b distintos de cero.

$$ax + by = 0 \qquad (3)$$

es llamada ecuación homogénea.

Observemos que esta ecuación siempre tiene al menos una solución.

$x = 0$, $y = 0$ ya que $a0 + b0 = 0$

Pero muy facilmente puede encontrarse otra solución $x = b$, $y = -a$ ya que $ab + b(-a) = 0$ y otra $x = 2b$, $y = -2a$ ya que $a2b + b(-2a) = 0$.

En general $x = tb$, $y = -ta$ para t entero es solución de (3) ya que $a(tb) + b(-ta) = 0$.

Por lo pronto ya sabemos que (3) tiene tantas soluciones como valores enteros puedan darse a t, es decir, tiene una infinidad de soluciones.

Pero la pregunta natural que se ocurre es: ¿por medio de $x = tb$, $y = -ta$ obtenemos <u>todas</u> las soluciones de $ax + by = 0$? ¿no se nos escapará alguna otra solución?

La respuesta a la primera pregunta es, en general, negativa. Veamos el siguiente ejemplo.

$$8x + 12y = 0$$

tenemos que $x = 12t$, $y = -8t$ para t entero son soluciones ya que $8(12t) + 12(-8t) = 0$.

Sin embargo $x = 3$, $y = -2$ también es solución de la ecuación ya que $8(3) + 12(-2) = 0$ y

$x = 3$ no es múltiplo de 12; $12 \nmid 3$ y

$y = -2$ no es múltiplo de -8; $8 \nmid -2$

Por tanto, en general, <u>no todas</u> las soluciones de $ax + by = 0$ se obtienen por medio de $x = tb$, $y = -ta$.

Tratemos de ver bajo qué restricciones de a y b, <u>toda</u> solución de $ax + by = 0$ tiene la forma $x = tb$, $y = -ta$.

Partamos de $ax + by = 0$

$$ax = -by$$

de aquí se sigue que

$$b \mid ax \quad y \quad a \mid by$$

pero de aquí no podemos garantizar en general que

$$b \mid x \quad y \quad a \mid y$$

($6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$)

Sin embargo, sabemos que si

$$b \mid ax,\ a \mid by \text{ y } (b,a) = 1 \text{ entonces } b \mid x \text{ y } a \mid y.$$

De modo que la restricciòn para que $x = tb$, $y = \mp ta$ nos de todas las soluciones de (3) es que $(a,b) = 1$. Enunciémoslo como un teorema y hagamos su demostración.

TEOREMA 2. Si $(a,b) = 1$ todas las soluciones de $ax + by = 0$ son de la forma $x = bt$, $y = \mp ta$ con t entero.

DEM.

$x = bt$, $y = \mp ta$ es solución de (3) ya que $a(bt)+b(\mp ta)=0$ $a(bt) + b(\mp ta) = 0$. Reciprocamente si x_0, y_0 es solución de (3) entonces

$$ax_0 + by_0 = 0$$

de donde $ax_0 = \mp by_0$

entonces $a \mid \mp by_0$ y $b \mid ax_0$

y como $(a,b) = 1$

entonces $a \mid \mp y_0$ y $b \mid x_0$

y por tanto $y_0 = \mp at_0$, $x_0 = bt_0$ para algùn t_0 entero.

¿Què pasa si $(a,b) \neq 1$?

Regresemos al ejemplo

$$8x + 12y = 0 \qquad (a)$$

aquí $(8,12) = 4$. Y nótese que la ecuación (a) podemos reescribir la como

$$4(2x + 3y) = 0$$

y las soluciones de (a) son exactamente las mismas que las soluciones de

$$2x + 3y = 0 \qquad (b)$$

Como $(2,3) = 1$ entonces todas las soluciones de (b) están dadas por

$$x = 3t, \quad y = \mp 2t \text{ con t entero}$$

y por ende, también las de (a).

En general tenemos que si $d = (a,b)$ las soluciones de $ax + by = 0$ y las de $\frac{a}{d}x + \frac{b}{d}y = 0$ son las mismas, donde $(\frac{a}{d}, \frac{b}{d}) = 1$. Así que las soluciones de $ax + by = 0$ están dadas por $x = \frac{b}{d}t$ $y = \mp \frac{a}{d}t$, con t entero.

Regresemos al caso de la ecuación no homogenea

$$ax + by = c$$

Teníamos ya un método para encontrar una solución. Sea x_0, y_0 una solución, entonces

$$ax_o + by_o = c \qquad (4)$$

por otro lado, si $d = (a,b)$, sabemos que

$$x = \frac{b}{d}t, \quad y = -\frac{a}{d}t \quad \text{con } t \text{ entero}$$

son todas las soluciones de (3)

por lo tanto $a(\frac{b}{d}t) + b(-\frac{a}{d}t) = 0 \qquad (5)$

si sumamos (4) y (5) tenemos

$$a(x_o + \frac{b}{d}t) + b(y_o - \frac{a}{d}t) = c$$

es decir, obtenemos una infinidad de soluciones para

$$ax + by = c$$

y no solo esto sino que además aseguramos que son todas las soluciones de la ecuación puesto que si x_1, y_1 son otras soluciones de (1) entonces

$$ax_1 + by_1 = c$$

si a esta ecuación le restamos $ax_o + by_o = c$ tenemos

$$a(x_1 - x_o) + b(y_1 - y_o) = 0$$

o sea que $x_1 - x_o$, $y_1 - y_o$ es solución de la ecuación homogenea, y por tanto, es de la forma:

$$x_1 - x_o = \frac{b}{d}t, \quad y_1 - y_o = -\frac{a}{d}t \ ;$$

es decir, $x_1 = x_o + \frac{b}{d}t$, $y_1 = y_o - \frac{a}{d}t$.

Lo anterior da lugar al siguiente:

TEOREMA 3. Sean a, b y c enteros dados; a, b distintos de cero. Sea $d = (a,b)$. Las soluciones de la ecuación

$$ax + by = c$$

están dadas por

$$x = x_o + \frac{b}{d}t, \quad y = y_o - \frac{a}{d}t$$

donde x_o, y_o es una solución particular de la ecuación.

En resumen, sea

$$ax + by = c$$

una ecuación diofantina.

Para resolverla se procede de la siguiente manera:

1.- Se calcula el m.c.d. de a y b. Sea $d = (a,b)$.

2.- a) Si $d \nmid c$ la ecuación no tiene solución.

b) Si $d|c$ la ecuación tiene solución.

3.- Para encontrar la solución hay que buscar una pareja de enteros x_o, y_o tales que

$$ax_o + by_o = c$$

4.- Se calculan todas las soluciones de

$$ax + by = 0\ ,$$

que vienen dadas por

$$x = \frac{b}{d}\,t, \quad y = -\frac{a}{d}\,t\ ; \text{ con } t \text{ entero}$$

5.- Las soluciones de $ax + by = c$ están dadas, por

$$x = x_o + \frac{b}{d}\,t, \quad y = y_o - \frac{a}{d}\,t.$$

EJERCICIOS

1. Resolver las siguientes ecuaciones diofantinas (dar todas las soluciones):

i) $2x + 3y = 6$

ii) $4x + 7y = 3$

iii) $8x - 6y = 97$

2. Se tienen ladrillos de 2 y 3 decímetros. En una barda de 4.9 metros se tiende una hilada de ladrillos. ¿Cuántos ladrillos de 2 y 3 decímetros se pusieron sabiendo que el número de cada uno de ellos es primo?

3. Al intercambiar las cifras de pesos y centavos de un cheque se obtiene una cantidad que es 20 pesos mayor que el doble del valor original del cheque. ¿de cuánto era el cheque?

4. Probar que si c es impar, entonces c no es combinación lineal de 98 y 102.

5. i) Probar que no existen x, y enteros tales que $x + y = 100$ y $(x,y) = 3$.

ii) Probar que existe una <u>infinidad</u> de enteros que satisfacen $x + y = 100$ y $(x,y) = 5$.

MINIMO COMUN MULTIPLO

El Calendario Maya

El Calendario Maya lleva la cuenta de dos tipos de años: el año sagrado y el año civil.

Año Sagrado

Para llevar la cuenta del año sagrado se utilizan los números 1,2,3,...,12,13 y veinte jeroglíficos Ik,Akbal,Kan,..,Imix.

El primer día del año sagrado empieza con 1Ik y cada día se va aumentando en uno el número y se va pasando al jeroglífico siguiente. Así los primeros dias del año son: 1 Ik, 2 Akbal, 3 Kan,.... Cuando se acaban los números o los jeroglíficos se vuelve a empezar por el primero. El nuevo año sagrado empezará cuando se vuelve a formar la combinación 1 Ik.

¿ De cuántos días es el año sagrado ?

¿ A lo largo del año aparecen todas las combinaciones de números con jeroglíficos ?

Para saber cuántos días tiene el año sagrado tenemos que ver cuándo vuelve a coincidir 1 con Ik, para esto, tenemos que agotar cierto número de veces los números y cierto número de veces los jeroglíficos, de tal suerte que nos den el mismo resultado, es decir, que m veces los números sea igual a n veces los jeroglíficos: $13m = 20n$

De hecho lo que buscamos es : de los múltiplos de 13 y 20 los que son comunes (siempre que esto suceda habrá terminado otro año sagrado), más precisamente el que necesitamos es el más chico, esto es, buscamos el mínimo múltiplo común de 13 y 20 (ya que buscamos los dias de un año sagrado).

Un múltiplo común muy sencillo de obtener es el producto de ambos:

$$13 \cdot 20$$

Ahora hay que ver si hay otro múltiplo común menor (positivo) o este es el mínimo.

El problema entonces es saber si hay alguna $n < 13$ y $m < 20$, tales que $13m = 20n$

Supongamos entonces que

$$20n = 13m ,$$

esto significa, en particular, que $13 \mid 20n$ y como 13 y 20 son primos relativos entonces $13 \mid n$, lo cual nos lleva a que la n positiva con valor mínimo es $n=13$ y por lo tanto $m=20$.

Así el mínimo común múltiplo de 13 y 20 es precisamente el producto de ambos números $13 \cdot 20 = 260$.

De manera que si cada número representa un día tenemos que repetir 20 veces todos los números, para empezar el año sagrado, habrán transcurrido 260 dias.

Por lo tanto el año sagrado tiene 260 días.

A lo largo del año aparecen todas las combinaciones de números con geroglíficos ya que dichas combinaciones son 13 números $\times$ 20 jeroglíficos = 260 combinaciones que coinciden con el número de días del año sagrado.

Observemos algunas cosas de lo hecho anteriormente. Lo que buscamos fué el mínimo común múltiplo de 13 y 20, rápidamente - obtuvimos un múltiplo común: el producto de los dos numeros - $(13 \cdot 20)$ y comprobamos también rápidamente que ese era el más chico. Algo que nos facilitó probar esto último fué el hecho de que $(13,20)=1$ ¿Qué pasa si los números que se dan no son primos relativos? Veamos el siguiente problema.

Dos ruedas engranadas tienen 32 y 28 dientes respectivamente. Partiendo de una posición ¿ cuántas vueltas tiene que dar cada rueda antes de llegar por primera vez las dos ruedas a la posición original ?

Este problema es completamente equivalente al del año sagrado. Lo que buscamos aquí es el menor múltiplo común de 32 y 28.

Como lo hicimos anteriormente, un múltiplo común es $32 \cdot 28$, ahora vamos a ver si es el mínimo (positivo) o no.

Según el procedimiento anterior queremos saber si hay

$$n < 32 \quad y \quad m < 28 \quad \text{tales que}$$

$$28\,n = 32\,m.$$

Ahora, si $28\,n = 32\,m$,

entonces $32 \mid 28n$, pero de aquí ya no podemos concluir que 32 divide a n, ya que 32 y 28 no son primos entre si (recordemos que un número puede dividir a un producto sin que necesariamente divida a alguno de los factores. Por ejemplo

$6 \mid 3 \times 4$ pero $6 \nmid 3$ y $6 \nmid 4$).

Busquemos otro camino para encontrar los valores mínimos m y n tales que

$$28n = 32m \qquad (1)$$

n = 32 y m = 28 satisfacen (1) pero también

$n_1 = \frac{32}{2}$ y $m_2 = \frac{28}{2}$ la satisfacen y son tales

que $n_1 < n$ y $m_1 < m$

¿ serán estas n_1 y m_1 los valores más chicos que satisfacen (1)?

Si $n = \frac{32}{3}$ y $m = \frac{28}{3}$ también serán solución de (1)

pero, ¡cuidado! recordemos que según el contexto del problema, m y n deben ser enteros, de modo que sólo podemos dividir entre números que sean divisores de 28 y de 32. Como 4 es divisor de ambos entonces

$n_2 = \frac{32}{4}$ y $m_2 = \frac{28}{4}$ son tales que

$$28n_2 = 32m_2$$

los valores de n_2 y m_2 son menores que n_1 y m_1 respectivamente, es más, estos valores son los valores mínimos (positivos) que puede tomar m y n , ya que 4 es el máximo común divisor de 28 y 32.

Entonces los enteros positivos menores, que satisfacen (1) son n = 8 y m = 7

O como lo habíamos planteado al principio el menor múltiplo común de 32 y 28 es

$$28n_2 = 28 \cdot \frac{32}{4} = 32 \cdot \frac{28}{4} = 32 \cdot m_2$$

es decir, el menor múltiplo común de 32 y 28 es

$\frac{28 \cdot 32}{4}$ donde $4 = (32,28)$

Por lo tanto la rueda que tiene 32 dientes tiene que dar 7 vueltas y la de 28 dientes tiene que dar 8 vueltas para llegar por primera vez ambas ruedas a la posición original.

Estos dos ejemplos nos muestran que el mínimo común multiplo de dos números a y b no necesariamente es el producto ab de éstos (aunque ab es un múltiplo común). Sólo si ocurre, como en el ejemplo 1, que (a,b) = 1, tenemos que ab es el mínimo

común múltiplo. Si (a,b)=d entonces el mínimo común múltiplo es el producto ab dividido entre el m.c.d. de a y b, es decir es $\frac{ab}{(a,b)}$. Esto naturalmente, hay que demostrarlo. Pero antes, conviene definir en forma precisa el mínimo común múltiplo de-- dos números.

Los múltiplos de a entero, son todos los números

.... -3a, -2a, -a, 0, a, 2a, 3a, ...,

es decir, todo número de la forma ka , k entero.

Todo entero que es múltiplo de a y b enteros, se llama múltiplo común de los mismos.

DEFINICION 1. Al menor múltiplo común positivo de los enteros a y b se le llama mínimo común múltiplo y se designa con la notación $[a,b]$

También utilizamos las iniciales m.c.m. de a y b para referirnos al $[a,b]$.

Ejemplo 1. Encontrar el m.c.m. de 4 y 9

múltiplos de 4: $0, \pm 4, \pm 8, \pm 12, \pm 16, \pm 20, \pm 24 \pm 28, \pm 32, \pm 36$ .....

múltiplos de 9: $0, \pm 9, \pm 18, \pm 27, \pm 36$.....

m.c.m. de 4 y 9 : 36

TEOREMA 1. Sean a y b enteros distintos de cero.

$$[a,b] = \frac{ab}{(a,b)}$$

DEM: Sea M algún múltiplo común de dos números a y b.
Como M es múltiplo de a,
se tiene que $M = a\,k$ con k entero.
Pero M también es múltiplo de b,
es decir, $M = b\,k_1$ con k_1 entero
entonces $a\,k = b\,k_1$
de donde $\frac{a\,k}{b} = k_1$,
es decir, $\frac{a\,k}{b}$ es un entero
esto quiere decir que $b \mid ak$.

Si $d = (a,b)$, entonces también se cumple que $\frac{b}{d} \mid \frac{a}{d} k$

y como $\left(\frac{b}{d}, \frac{a}{d}\right) = 1$ (propiedad 2 sec. m.c.d.)

entonces $\frac{b}{d} \mid k$

es decir, existe un entero t tal que $k = \frac{b}{d} t$.

De aquí que $M = a k = a \frac{b}{d} t$

esto es, $M = \frac{a b}{d} t$.

Reciprocamente, es evidente que cualquier M de esta forma es múltiplo tanto de a, como de b, y por consiguiente, esta forma proporciona todos los múltiplos comunes de a y b.

El menor positivo de estos múltiplos, es decir, el mínimo común múltiplo, se obtiene para $t = 1$ esto es, $[a,b] = \frac{ab}{d}$ donde $d = (a,b)$.

De este teorema se obtiene el siguiente.

COROLARIO 1. Sean a y b enteros distintos de cero. El conjunto de múltiplos comunes de dos números a y b, coincide con el conjunto de los múltiplos de su m.c.m.

En efecto, en el teorema se demuestra que todos los múltiplos comunes M de a y b son de la forma $M = \frac{ab}{d} t$ con t entero

es decir, $M = [a,b] t$, t entero.

COROLARIO 2. Sean a y b enteros distintos de cero tales que $(a,b) = 1$. Entonces $[a,b] = a \cdot b$.

Directo de sustituir $d = 1$.

Ejemplo 2 . Encontrar el m.c.m. de 2784 y 4988

En el ejemplo 2 de la sec. m.c.d. calculamos el m.c.d. de éstos números . $(2784, 4988) = 116$

Aplicando el Teorema 1 tenemos que

$[2784, 4988] = \frac{2784 \cdot 4988}{116}$

por lo tanto $[2784, 4988] = 119,712$

EJERCICIOS

Encontrar el m.c.m. de las siguientes parejas :

1.- a = 56 , b = 72

2.- a = 2184, b = 1764

3.- a = 1901, b = 601

4.- Año Civil (del Calendario Maya)

el año civil consta de 365 dias y se cuenta por meses y dias de forma similar al nuestro. Bástenos saber que el primer día del año se llama 0 Pop.

Si un año coincide el 0 Pop con el primer día del año sagrado 1 Ik.

¿ Al cabo de cuántos años volveran a coincidir ?

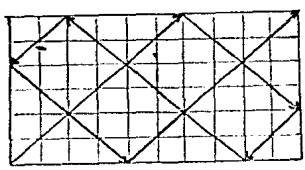
¿ Cuántos dias representa esto ?

5.- Mientras Elena y Tony paseaban por el parque se cruzaron con la banda municipal, que ensayaba un desfile. La banda pasó desfilando de cuatro en fondo, salvo uno de los músicos, el pobre Pánfilo que cerraba la marcha. El director de la banda estaba molesto. Para encajar al músico en la formación, el director mando formar en columna de a tres. Pero Pánfilo seguía estando solo en la última fila. Incluso cuando la banda desfila de dos en dos, Panfilo sigue solo, de farolillo rojo. Aunque no era asunto suyo, Elena se acercó al director de la banda y le dijo: fórmelos usted de cinco en fondo. El director respondió: jovencita, eso precisamente iba a ordenar ahora. Cuando la banda formó de cinco en fondo, todas las filas quedaron completas y Pánfilo quedó perfectamente encuadrado.

¿Cuántos músicos componen la banda ?

6.- Una mesa de billar mide n unidades en su lado menor y m en el mayor. A partir de una esquina se lanza una bola formando un ángulo de 45° con los lados, la que va rebotando en los lados de la mesa hasta llegar por primera vez a otra esquina, donde se le detiene.

Por ejemplo si n = 6 y m = 10 la trayectoria es la siguiente



a) Hacer ver que la bola llega a pegar efectivamente en algún momento en alguna esquina.

b) Dar un procedimiento para determinar (dados n y m) cuántas veces choca la bola con los lados mayores de la mesa y cuántas con los lados menores y en qué esquina va a terminar.

c) Describir la distribución de los puntos sobre el parámetro de la mesa donde choca la bola.

d) ¿Qué puede decirse de los incisos a, b y c en el caso de que los lados de la mesa sean inconmensurables?

7.- Los enteros del 1 al 1000 se escriben a lo largo de una circunferencia. Empezando con el 1 señalamos los números saltandonos de 15 en 15, esto es, 1,16,31,46,.. Este proceso se continúa hasta que luego de tantas vueltas como sea necesario se regrese al 1. Se pregunta ¿Cuántos números quedan sin señalar?

8.- La dueña de una huertita de manzanos levanta su cosecha y la lleva directamente al mercado. Lo único que se sabe por el tamaño estandar de la manzana y las cajas donde las colocan es que son menores de 500. En el puesto del mercado la marchanta las dispone de 2 en 2 pero le sobra 1, por lo que decide ponerlas en pilas de 3,4,5 y 6 pero siempre le sobra 1. Finalmente prueba ponerlas en montones de 7 y no le sobra ninguna. ¿Cuántas manzanas tenía ?

9.- Sean a, b y c enteros. Demostrar que

$|c|\,[a,b] = [ca,cb]$

10.- Sean $a_1, a_2, \ldots, a_n$ enteros. Formemos la sucesión de números:

$[a_1,a_2] = m_2,\ [m_2,a_3] = m_3, \ldots,\ [m_{n-1},a_n] = m_n$

Probar que el número m_n obtenido de este modo será el m.c.m. de todos los números dados.

NUMEROS PRIMOS

Al estudiar las propiedades de los enteros, quizá el hecho más notorio es que existen números que pueden ser divididos por otros números y otros que no, es decir, números que tienen divisores (positivos) distintos de el mismo y la unidad (los "números compuestos") y otros que solo tienen como divisor (positivo) distinto de él a la unidad. Estos son los conocidos números primos. Todo número entero positivo a excepción del 1 tiene al menos dos divisores positivos y pertenecen a la clase de los primos o bien a la de los compuestos. El número 1 solo tiene un divisor positivo, precisamente el 1. En este sentido el número 1 en la sucesión de los números enteros positivos, es particular y no se considera primo ni compuesto.

De importancia fundamental en Teoría de números es la clase de los números primos. La importancia se debe al hecho de que cualquier entero puede expresarse como producto de números primos (Teorema Fundamental de la Aritmética), este resultado es intuitivamente muy claro ya que un número si no es primo, se puede descomponer sucesivamente hasta que todos sus factores lo sean.

DEFINICION 1. Un entero $p \neq \pm 1$ es llamado es llamado primo cuando tiene como únicos divisores a 1 y p.

Ejemplos de primos son ... 11, 7, 5, 3, 2, 2, 3, 5, 7, 11

Nótese que 2 y −2 son los unicos primos pares. Cualquier otro par tiene además de los divisores triviales al 2 como divisor.

DEFINICION 2. Un número entero $m \neq \pm 1$ que no es primo es llamado compuesto.

Ejemplos de números compuestos: ...−9, −8, −6, −4, 0, 4, 6, 8

En los siguientes resultados, por comodidad, se considerarán solo los factores positivos y se enunciarán estos resultados para enteros positivos, aunque los mismos resultados se cumplan para los enteros negativos y las demostraciones sean equivalentes.

El trabajar con enteros positivos simplifica el lenguaje y la notación y ayuda a fijar mas las ideas y resultados.

En relación a la divisibilidad los primos tienen propiedades simples.

1. El m.c.d. de un número primo p y un entero cualquiera n es 1 o bien p. Esto es, $(p,n) = 1$ o $(p,n) = p$. Veamos.

Como $d = (p,n)$ entonces $d|p$ y como p es primo sus únicos divisores son p o 1.

Antes de continuar con las propiedades de los primos establezcamos la siguiente:

DEFINICION 3. Decimos que a y b son primos relativos si y solo si $(a,b) = 1$

2. Si el producto de varios factores es divisible por p al menos uno de los factores es divisible por p, es decir, si

$$p|n_1n_2\cdots n_r \quad \text{entonces} \quad p|n_i \text{ para alguna } i=1, 2,\ldots, r$$

dem.:

Cada factor n_i es primo relativo a p o es divisible por p.

Si suponemos que todos los factores fuesen primos relativos a p entonces por ser $(n_1,p) = 1$ (prop. 3 secc. divisibilidad)

$$\begin{aligned}(n_1n_2\cdots n_r,p) &= (n_2\ n_3\ \cdots n_r,p)\\ &= (n_3n_4\cdots n_r,p) \qquad \text{porque } (n_2,p) = 1\\ &\ \ \vdots\\ &= (n_r,p) \quad 1 \qquad \text{porque } (n_{r-1},p) = 1\end{aligned}$$

es decir, llegaríamos a que

$(n_1n_2\cdots n_r,p) = 1$ lo que contradice la hipótesis.

Por tanto <u>no todos</u> los factores pueden ser primos relativos a p, esto quiere decir que existe algun n_i para $i = 1, 2,\ldots,r$ tal que $p|n_i$.

3. El divisor menor (distinto de la unidad) de un entero $n > 1$, es un numero primo.

dem.:

Sea $q > 1$ el divisor menor de $n > 1$.

Entonces $n = n_1q$.

Si q fuese compuesto tendría un divisor q_1 tal que $1 < q_1 < q$.

Haciendo $q = q_1 1$, tenemos $n = n_1(q_1 1)$, lo que llevaría a que q_1 es divisor de n y es menor que q, lo cual contradice la hipótesis de que q es el menor divisor de n.

Por lo tanto q no puede ser compuesto y entoces q es primo.

4. El divisor menor (distinto de la unidad) de un número compuesto n (que según la propiedad anterior tiene que ser primo) no es mayor que $\sqrt{n}$.

dem.:

Sea $q > 1$ el divisor menor de $n > 1$,

entonces $n = n_1 q$

por ser q el menor divisor de n tenemos que

$$q \leq n_1$$

multiplicando en ambos lados por q obtenemos

$$q^2 \leq n_1 q,$$

es decir, $q^2 \leq n$

de donde $q \leq \sqrt{n}$

TEOREMA 1. Todo entero $n > 1$ puede descomponerse en un producto de factores primos y además de modo único, si no se tiene en cuenta el orden de los factores.

DEM:

Sea $n > 1$. Si n es primo no hay nada que hacer, su descomposición es el número mismo.

Si n es compuesto, n tiene un divisor menor distinto de 1 que es un primo. Llamémosle p_1

$$n = n_1 p_1 \qquad \text{donde } n > n_1 > 1$$

Si n_1 es primo ya hemos acabado, la descomposición de n es

$$n = p_1 n_1$$

Si n_1 es compuesto, este tiene un divisor p_2 menor distinto de 1 que es primo, es decir,

$$n_1 = p_2 n_2 \qquad \text{con } n_1 > n_2 > 1$$

obteniendo que

$$n = p_1 p_2 n_2 \qquad \text{con } n > n_1 > n_2 > 1$$

siguiendo este procedimiento llegamos (en a lo más n pasos) a la descomposición de n

$$n = p_1 p_2 \cdots p_r$$

Demostremos ahora la unicidad de la descomposición.

Supongamos que para n existe una segunda descomposición en factores primos

$$n = q_1 q_2 \cdots q_s$$

entonces

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

de donde

$$q_1 \mid p_1 p_2 \cdots p_r$$

entonces q_1 divide a alguno de los factores p_i.

Supongamos, por ejemplo, que

$$q_1 \mid p_1$$

(el orden de la numeración de los factores es arbitrario) entonces como p_1 sólo es divisible por 1 y p_1 tenemos que

$$q_1 = p_1$$

Simplificando ambos términos de la igualdad se tiene que

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Repitiendo el razonamiento anterior para esta nueva igualdad obtenemos que

$$p_3 \cdots p_r = q_3 \cdots q_s \qquad \text{pues } p_2 = q_2$$

Continuamos así hasta que en un lado de la igualdad se simplifiquen todos los factores, supongamos que es en el primero, entonces quedaría

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

lo cual es una contradiccion ya que

$q_{r+1}, q_{r+2}, \ldots, q_s$ son mayores que 1 siendo imposible que su producto sea igual a 1.

Por lo tanto la segunda descomposicion en factores primos es idéntica a la primera.

Por cierto, aquí hay una de las razones por las cuales no conviene que 1 sea primo: la descomposición en primos no será unica (le agregamos unos).

En la descomposición del número n en factores primos algunos de ellos pueden repetirse. Si designamos con las letras $p_1, p_2, \ldots, p_k$ los primos distintos de dicha descomposicion y con $\alpha_1, \alpha_2, \ldots, \alpha_k$ las veces que aparecen obtenemos la llamada descompo-

sición canónica del número n:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Ejemplos:

$$180 = 2^2 \cdot 3^2 \cdot 5$$

$$3087 = 3^2 \cdot 7^3$$

$$15 = 3 \cdot 5$$

$$1575 = 3^2 \cdot 5^2 \cdot 7$$

Se han visto algunos resultados teóricos sobre los números primos. Ahora entremos a otro tipo de problemas.

Se mencionaron como ejemplos de primos a

2, 3, 5, 7, 11, ...

¿Qué otros primos conocemos?

13, 17, 19, 23, 29, 31, 37, ..., 91,93, 97, ...

al ir recordando números primos nos planteamos dos preguntas:

¿Como encontrar los números primos?

¿Como saber si un número dado es primo o no? por ejemplo 217 ¿es primo? o 6728042130721 ¿es primo?

Existe un método muy antiguo para encontrar primos conocido como la Criba de Eratóstenes. Para formar la tabla de números primos menores o iguales a un numero dado N, digamos, por ejemplo N = 100, el método consiste en lo siguiente:

Escribimos los números del 1 al 100 en la siguiente forma:

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	26	27	
28	29	30	31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	51	52	53	
54	55	56	57	58	59	60	61	62	63	64	65	66	
67	68	69	70	71	72	73	74	75	76	77	78	79	
80	81	82	83	84	85	86	87	88	89	90	91	92	
93	94	95	96	97	98	99	100						

TABLA 1

El primer número primo es el 2. Tachamos de la tabla todos los múltiplos de 2, a excepción del 2 mismo.

El siguiente número no tachado que sucede al 2 es el 3; tachamos de la tabla todos los números que son múltiplos del 3, a ex-

cepción del 3 mismo.

El primer número no tachado que sigue al 3 es el 5 ... seguimos el procedimiento descrito. Nótese que los números que necesariamente van quedando sin tachar son precisamente los primos. Además obrservemos que para encontrar todos los primos que hay entre 1 y 100 basta con tachar los múltiplos de los primos menores que 100 (recordar prop. 4), porque cualquier número no tachado $m_o \leq 100$ es primo, ya que si fuera compuesto tendría un factor primo menor o igual a $\sqrt{m_o} \leq \sqrt{100}$ y como tachamos todos los múltiplos de los primos menores o iguales que $\sqrt{100}$ entonces m_o esta tachado. Por la misma razón (prop. 4), en la Criba de eratóstenes, al comenzar a tachar los múltiplos de un número primo p hay que empezar a tachar desde p^2.

Con el método de la Criba de Eratóstenes podemos conocer todos los primos menores o iguales a N para cierta N dada. También nos sirve para saber si un número es primo o no, siempre y cuando este número no sea demasiado grande, por ejemplo, para saber si

217 es primo o no

bastaría con aplicar el método de la tabla formada por los números del 1 al 217 y checar si quedó tachado o no el número 217.

En realidad no es necesario hacer todo este procedimiento, dado que sólo interesa saber sobre el 217; apliquemos las observaciones que hemos hecho al método de la Criba.

$217 < 225 = 15^2$

(elegimos 225 porque es un cuadrado perfecto y facilita el cálculo, en realidad necesitamos solo 217).

De modo que por fuerza si 217 no es primo debe tener un factor primo menor que $\sqrt{15^2} = 15$, es decir, si 217 no es primo algún número primo de los siguientes tendría que ser un divisor de él: 2, 3, 5, 7, 11, 13. Entonces basta checar si alguno de estos 6 números es divisor de 217.

Como $7 \mid 217$ entonces 217 no es primo.

(Nótese que este es el contenido de la propiedad 4. Esta propiedad es también, en cierta forma, la esencia de la Criba de Eratóstenes).

Pero ¿qué pasa cuando el numero que queremos saber si es pri-

mo o no es muy grande? por ejemplo, si el número mencionado anteriormente 07280421310721, que tiene 14 dígitos, es primo. Teoricamente siguiendo el mismo procedimiento descrito arriba podría mos, después de muchísimas cuentas, saber si es primo o no. Se nota que este camino tiene sus limitaciones. Bueno, el número de los 14 digitos si es primo. En realidad no se ha descubierto un metodo general para determinar si un número es o no primo, para números como el de arriba, a menos que tenga una forma especial, puede requerirse mucho trabajo para resolverlo.

Podemos decir algunas cosas más sobre esto de saber si un número es primo o no.

Sabemos que si un número es divisible entre 5 termina en 0 o en 5.

Y si es divisible entre 2 termina en 0, 2, 4, 6 u 8.

Esto nos lleva a lo siguiente: un número para ser primo necesita terminar en 1, 3, 7 o 9 (excepto los primos 2 y 5). Ojo: esto no quiere decir que si termina en 1, 3, 7 o 9 ya es primo.

Contraejemplos:

$21 = 3 \cdot 7$

$39 = 3 \cdot 13$

$27 = 3^3$

$33 = 3 \cdot 11$

Lo que quiere decir es que si es primo (y no es el 2 ni el 5) entonces termina en 1, 3, 7 o 9.

(Es importante tener presentes las reglas para los divisibles entre 3, 4, 6, 7, 8, etc.)

Para ir conociendo cómo estan distribuidos los primos entre los naturales contestemos lo siguiente:

¿Podemos dar dos números consecutivos que no sean primos?

Es fácil, 8 y 9.

¿Tres consecutivos que no sean primos? 14, 15 y 16.

¿Cinco consecutivos que no sean primos? Recurriendo a la tabla 1 es facil exhibir cinco

62, 63, 64, 65 y 66.

¿Habra veinte consecutivos no primos? Aqui el problema no es tan fácil de contestar, tendríamos que tener tablas mas grandes de primos. Para responder, nos servirá conocer los siguientes da-

tos sobre la frecuencia de aparición de los números primos.

Cada centena del 1 al 1000 contiene respectivamente

25, 21, 16, 16, 17, 14, 16, 14, 15, 14

números primos.

Cada centena del 1 000 000 al 1 001 000 la correspondiente frecuencia es

6, 10, 8, 8, 7, 7, 10, 5, 6, 8

y de 10 000 000 a 10 001 000

2, 6, 6, 6, 5, 4, 7, 10, 9, 6

y de 10^{12} a 10^{12}+ 1 000

4, 6, 2, 4, 2, 4, 3, 5, 1, 6

Regresando a la pregunta de si habrá veinte consecutivos no primos, según los datos arriba mencionados entre el número 10 000 000 y el 10 000 100 hay sólo dos número primos, esto quiere decir que entre esos números podemos elegir los 20 consecutivos no primos.

¿Podrían haber 1 000 o 100 000 consecutivos no primos?

Se nota que el metodo usado anteriormente de recordar numeros o recurrir a tablas o datos ya no funciona para estos numeros tan grandes.

La respuesta es que sí podemos encontrar esos consecutivos no primos, es más, uno puede encontrar primos consecutivos cuya distancia entre si sea tan grande como uno quiera. En otras palabras, existen sucesiones arbitrariamente largas de números compuestos. Para probar esto basta con darnos cuenta que los n-1 números

n!+2, n!+3, n!+4, ..., n!+n son compuestos ya que como

$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n$

entonces

$2 \mid n!+2$, $3 \mid n!+3$, $4 \mid n!+4$, ... $n \mid n!+n$

Asi que si queremos 1000 consecutivos no primos, los números que sirven son

1001!+2, 1001!+3, 1001!+4, ..., 1001!+1001

Este hecho muestra la gran irregularidad en la frecuencia de los primos.

Ahora se ocurre preguntar:

¿Cuántos primos hay en los naturales?

¿No ocurrirá que los primos empiezan a espaciarse tanto que a partir de un cierto número ya no hay primos?

Pues resulta que no, que hay una infinidad de primos. La demostracion de este resultado se conoce desde Euclides.

TEOREMA 2. Hay una infinidad de primos en los naturales.

DEM:

Supongamos que hay un número finito de primos.

Indiquemos dichos números por

$$p_1, p_2, \cdots, p_n$$

Vamos a ver que esta suposición nos lleva a una contradicción.

Construyamos el número

$$p = p_1 p_2 \cdots p_n + 1$$

Es claro que $p \neq p_i$ para cada $i = 1, 2, \ldots, n$.

Sabemos que el divisor menor distinto de 1 de p es un primo (prop. 3), entonces algún p_i tiene que dividir a p lo cual es falso ya que al dividir cada p_i entre p siempre queda 1 como residuo.

Esto quiere decir que o

p es primo o

el primo que divide a p es uno distinto de

$$p_1, p_2, \cdots, p_n$$

Por lo tanto no hay un número finito de primos. Estos son infinitos.

De hecho esta demostración nos da un método para encontrar primos. Cualesquiera que sean los números primos distintos $p_1, p_2, \ldots, p_n$ obtenemos otro primo nuevo que es o bien $p = p_1 p_2 \cdots p_n + 1$ o el divisor menor del mismo p.

Se ilustra la construcción de primos por el metodo llamado de Euclides con los siguientes ejemplos:

$2 \cdot 3 + 1 = 7$ primo

$2 \cdot 3 \cdot 5 + 1 = 31$ primo

$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ primo

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ primo

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509$

$$2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17 + 1 = 510\ 511 = 19\cdot97\cdot277$$

$$2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19 + 1 = 9\ 699\ 691 = 347\cdot27\ 953$$

Hemos visto que hay una infinidad de primos en la sucesión de números naturales.

Otro resultado importante sobre la distribución de primos es que también hay una infinidad de primos en la sucesión de números

$$3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ \ldots$$

es decir, en la sucesión $4n-1$ con $n = 1, 2, 3, \ldots$

Para demostrar esto, sólo hay que hacer una generalización de la demostración hecha para el teorema 2.

Supongamos que existe un número finito de primos en la sucesión 3, 7, 11, 15, 19, ..., 4n 1, ... Sean estos primos

$$p_1,\ p_2,\ \cdots p_k$$

Construímos el número $N = 4p_1p_2\cdots p_k - 1 = 4p-1$.

Entonces, o bien N es primo o puede ser descompuesto en factores primos, ninguno de los cuales puede ser $p_1, p_2, \ldots, p_k$ puesto que N no es divisible por p_i para i 1, 2, ..., k.

Observemos que todo primo mayor que 2 es impar y por lo tanto será de la forma 4n+1 o 4n−1 (ya que los números de la sucesión son o bien de la forma 4n−1, 4n, 4n+1 o 4n+2, y 4n y 4n+2 son pares)

Otra cosa a observar es que el producto de dos números de la forma 4n+1 es también de esta forma ya que

$$(4l+1)(4m+1) = 414m + 4l + 4m + 1$$

$$= 4(4lm + l + m) + 1$$

Entonces según estas observaciones, no puede ocurrir que todos los factores de N sean de la forma 4n+1 ya que N tendría que ser de esa misma forma, luego, N tiene al menos un factor primo p de la forma 4n−1. Pero este primo no puede ser cualquiera de los p_i's dado que ellos no dividen a N; entonces p es un nuevo primo de la sucesión 3, 7, 11, 15, ...

Con los mismos argumentos puede probarse que la sucesión aritmética de término general 6n−1, es decir,

$$5,\ 11,\ 17,\ 23,\ 29,\ 35,\ \ldots$$

o la 6n+5 o la 4n+3 contienen una infinidad de primos.

En general una sucesión aritmética consiste de términos

$an + b \qquad n = 1, 2, 3, \ldots$

donde a y b son números fijos.

Si a y b tienen como m.c.d. a d, todo número de la sucesión es divisible por d, entonces no contiene nigún primo dicha sucesión.

Pero si suponemos que a y b son primos relativos, se puede probar que la sucesión contiene un número infinito de primos.

Este resultado es conocido como el Teorema de Lejeune-Dirichlet. No haremos la demostración de este teorema. (la demostración requiere de herramienta matemática complicada y resultados de otros campos).

Uno de los problemas que ha interesado a los matemáticos es el de encontrar fórmulas que den primos (aunque no den todos). Esto ha interesado poque como se ha mencionado es difícil determinar si un número es primo.

Fermat conjeturó que todos los números de la forma

$$F(n) = 2^{2^n} + 1$$

son primos.

A los números de esta forma se les llamó números de Fermat para $n = 0, 1, 2, 3, 4$ se obtiene que $F(n)$ es primo

$$F(0) = 2^0 + 1 = 3$$

$$F(1) = 2^2 + 1 = 5$$

$$F(2) = 2^4 + 1 = 17$$

$$F(3) = 2^8 + 1 = 257$$

$$F(4) = 2^{16} + 1 = 65\ 537$$

pero posteriormente Euler obtuvo una descomposición de $F(5) = 2^{32} + 1 = 641 \cdot 6700417$, es decir, Euler demostró que para $n = 5$, la fórmula propuesta por Fermat no da un primo. Ya se ha probado que otros números de Fermat son compuestos. Más aún, a la fecha no se ha probado que sea primo ninguno de los números $F(n)$ para $n > 4$.

Euler desarrollo otra fórmula para encontrar primos

$$f(n) = n^2 + n + 41$$

esta fórmula no sólo da primos, pero para n desde 0 hasta 40,

f(n) es primo. Sin embargo para n = 41,

$$f(41) = 41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \cdot 43$$

que es compuesto.

Lo mismo ocurre para la fórmula

$$f(n) = n^2 - 79n + 1601$$

que da 80 primos con los naturales desde 0 hasta 79.

Y para

$$f(n) = n^2 + 81n + 1681$$

obtenemos una buena cantidad de primos, pero tambien falla.

De hecho lo que se puede deostrar esque ningún polinomio en n con coeficientes enteros toma solamente valores primos.

En los últimos resultados de los primos, notamos que estos números se van espaciando en la sucesión de naturales, que podemos encontrar huecos tan grandes como se quiera de números consecutivos compuestos; que no se ha encontrado hasta la fecha fórmula algebraica que dé todos los primos, ni siquiera fórmulas que den solo primos. Esto nos podría llevar a suponer que definitivamente no hay "ley que gobierne" a los primos. Sin embargo estudiando la distribución media de los números primos dada por la razón

$$\frac{A(n)}{n}$$

donde A(n) es el numero de primos que hay entre 1 y n (por ejemplo A(1) = 0, A(2) = 1, A(3) = 2, A(4) = 2, ..., A(19) = 8, ..., A(1000) = 168, ...) Gauss descubrió una ley que rige el comportamiento de dicho cociente y conjeturó que dicha razón es "asintóticamente igual" a $\frac{1}{\log n}$, (donde log n es el logaritmo natural de n), es decir, que si tomamos una sucesión creciente de valores de n:

$$\lim_{n\to\infty} \frac{A(n)/n}{1/\log n} = 1$$

Esta conjetura logra describir mediante la función logaritmo la distribución de los primos. Se necesitó, cien años antes de que el análisis se desarrollara lo suficiente para poder dar una demostración de este teorema conocido como Teorema de los Números Primos.

EJERCICIOS

1. Exprese los siguientes números en su descomposición canónica:

i) 100 ii) 1300 iii) 1986

2. Encuentre lafactorización en primos de los números:

i) 2468 ii) 262144 iii) 99999 iv) 100001

3. Mersenne determinó la factorización del número 51 001 180 160. Encuentre los factores primos de este número.

4. Use el teorema fundamental de la aritmética para determinar las raíces cuadradas de los siguientes números con tres decimales de aproximación:

i) 392 ii) 5780

5. Sea m un entero positivo cuya factorización en primos es

$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ (con p_i primo y $\alpha_i \geq 1$ $i = 1, 2, \ldots, n$)

i) Demostrar que todo divisor (positivo) de m es de la forma

$p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$

ii) Demostrar que el número dedivisores (positivos) de m es

$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_n + 1)$.

6. Encontrar un número con

i) 14 divisores (positivos)

ii) 12 divisores (positivos)

7. Encontrar el <u>menor</u> entero positivo con

i) 14 divisores (positivos)

ii) 12 divisores (positivos)

8. Sean a y b enteros positivos cuya factorización en primos es

$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ $\quad b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$

Demostrar que

$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n}$ donde $\gamma_i = \min\{\alpha_i, \beta_i\}$

$[a,b] = p_1^{\delta_1} p_2^{\delta_2} \ldots p_n^{\delta_n}$ donde $\delta_i = \max\{\alpha_i, \beta_i\}$

9. Utilizando el teorema fundamental de la aritmética demuestre que $(a,b)[a,b] = ab$ donde a y b son enteros positivos.

10. i) Pruébese que el producto de números naturales de la forma $3k + 1$ es un número que es de nuevo de esa misma forma.

ii) Utilizando i) demostrar que hay una infinidad de primos de la forma $3k + 2$. En otras palabras, se trata de demostrar que la sucesión 2, 5, 8, 11, 14, 17, ... contiene una infinidad de primos.

11. ¿Por qué sucede que

$$7 \cdot 15873 = 111\ 111$$
$$14 \cdot 15873 = 222\ 222$$
$$21 \cdot 15873 = 333\ 333$$
$$28 \cdot 15873 = 444\ 444$$
$$\vdots \qquad\qquad ?$$

CONGRUENCIAS

Normalmente nunca oye uno decir a alguien "son las 33- horas del lunes", incluso no es usual que al preguntar al-- guien la hora se le conteste "son las 15 horas.

Sin embargo, si yo dijera "son las 33 horas del lunes" casi todos sabrían de inmediato que son las 9 de la mañana- del martes, pordría a partir del lunes y pasado unos días - insistir en que "son las 107 horas del lunes. Más adelante en que son las 323 horas del lunes" y seguramente conforme pasara el tiempo y continuara con mi empecinamiento, ya nadie me preguntará la hora. Pero aquellos inocentes que se - toparon conmigo a las 107 o a las 323 horas del lunes, ha-- ciendo cuentas, llegarán a la conclusión de que son las 11 de la mañana del viernes siguiente a ese lunes y las 11 de- la mañana del segundo domingo después de ese lunes ¿Cuáles fueron las operaciones que estas personas utilizaron ?.

Como el día tiene 24 horas, dividieron 107 y 323 entre 24 para saber cuántas veces "cabe 24" y como no les intesaba el día puesto que lo conocían se fijaron en lo que sobró es decir, en el residuo de la división que en ambos casos resultó ser 11. Por tanto la hora era 11 de la mañana.

Haciendo a un lado los días, las horas y mis empecinamientos, lo que podemos observar es que los números 107 y - 323 dejan el mismo residuo, el 11, al dividirlos ente 24; y que las horas del día se miden, no tanto acumulándolas, sino "volviendoa empezar" con el 1, 2, 3, etc. cada que alcanzamos un múltiplo de 24, es decir, se mide con los residuos que dejan los números al dividirse entre 24.

Pensando en estos residuos y hablando en términos in-- formales, podemos decir que 11, 107 y 323 representan "lo - mismo" para el número 24, o dicho de otra forma, si nuestra "unidad de medida" es el 24, a los números 11, 107 y 323 -- les sobra lo mismo al "medirlos" con el 24. Cuando esto sucede se dice que los números 11, 107 y 323 son "congruentes para el 24 y a la "unidad de medida" se le llama módulo. Se

dice entonces que 11, 107 y 323 son "congruentes módulo 24".

En este nuevo lenguaje ¿qué otros números son congurentes con 11, 107 y 323 módulo 24?. Todos aquellos que al dividirlo entre 24 dejen residuo 11. A saber:

..., -51, -37, -13, 11, 35, 59, 83, ..., 323, ...

Si en lugar de 11 tomamos el 3, los números congruentes -- con 3 módulo 24 son:

..., -21, 3, 27, 51, 75,...

Para expresar que cierto número entero a es congruente con algún otro entero b módulo 24, se escribe

$a \equiv b \mod 24$

y se lee "a es congruente con b módulo 24".

Así por ejemplo;

$11 \equiv 107 \mod 24$

$3 \equiv 27 \mod 24$

y también, como puede comprobarse fácilmente:

$2 \equiv 26 \mod 24$

$5 \equiv 125 \mod 24$

$7 \equiv 31 \mod 24$

Otra situación en la que en el fondo medimos el tiempo con congruencias son los días del año. El módulo en este caso es, obviamente 365 (los años bisiestos los exclímos por ahora). - Si tomamos como punto de partida el 1º de enero de 1985 y le-llamamos el "día 1º", entonces el "día 369" es el 4 de enero - de 1986 (369 deja residuo 4 al dividirlo entre 365). El 4 de-enero de 1987 viene a ser el "dia 734" (o lo que es lo mismo 734 deja también residuo 4 al dividirlo entre 365). Usando la notación de congruencia, tenemos:

$369 \equiv 734$ módulo 365

Y el 4 de enero de 1984, ¿qué "día" es? Admitiendo días con número negativo - recordando el punto de partida-viene a ser el "día - 361". Es decir:

$-361 \equiv 4 \mod 365$

Con base en los días de la semana se podrían desarrollar ejemplos de números congruentes módulo 7 (lo dejamos al lector). Hay otras situaciones donde aparecen congruencias de una u otra manera.

La idea de manejar los residuos en lugar de los números (dado cierto entero como módulo, claro está) fué introducido por Gauss, y desde entonces ha sido de la máxima importancia en la Teoría de los Números. Las congruencias o "aritmética residual" como suele llamarse a esto de manejar los residuos- abren un panorama nuevo en la Teoría de números y aunque en este trabajo nos limitaremos a exponer una breve introcción al tema, esperamos mostrar algo de este panorama nuevo.

El hecho básico en el cual descansan las congruencias es en el Algoritmo de la División. En efecto, supongamos que hemos escogido como módulo a cierto entero $m > 0$. Dado cualquier entero a, el algoritmo de la división nos asegura la existencia de un único residúo r tal que

$$a = mq + r \quad \text{donde} \quad 0 \leq r < m$$

la escencia de las congruencias consiste en "identificar" a con r. A partir de ahí. las operaciones con a se traducirán en operaciones con el residuo r.

Pasemos a precisar esto.

DEFINICION 1. Decimos que dos entero a y b son <u>congruentes módulo m</u> para $m > 0$ si ambos dejan el mismo residuo al dividirlos entre m.

Como ya dijimos, la notación usual (introducida por Gauss) para expresar que a es congruente con b módulo m es la siguiente:

$$a = b \bmod m$$

Simbolicamente la definición anterior la expresamos como

$a = b \bmod m$ si y solo si $a = km + r$ y $b = lm + r$ con $0 \leq r < m$ y k y l enteros.

Si escribimos el residuo r como $r = b - lm$ y lo sustituímos en la igualdad $a = km + r$ obtenemos $a = km + b - lm$, es de

cir, $a = (k - 1)m + b$. Así otra manera equivalente de definir la congruencia de a y b módulo m es la siguiente:

DEFINICION 2. $a = b \bmod m$ si y sólo si algún t entero tal que
$a = mt + b$

(nótese que la expresión $a = mt + b$ no necesariamente es el residúo del Algoritmo de la división).

Reescribiendo $a = mt + b$ como $a - b = mt$ resulta $m \mid a - b$ entonces, de manera equivalente podemos dar otra definición. Esta fué dada por Gauss.

DEFINICION 3. $a \equiv b \bmod m$ si y sólo si $m \mid a - b$

Probemos ahora la equivalencia entre estas tres definiciones

TEOREMA 1. Las definiciones 1, 2 y 3 de congruencias son equivalentes.

DEM:

- P.D. Def. 1 $\Rightarrow$ Def. 2
- Por la def. 1, $a \equiv b \bmod m$ implica que $a = km + r$ y $b = lm + r$ donde $0 \leq r < m$ y k y l enteros. Entonces, despejando r obtenemos $r = b - lm$, de donde $a = km + b - lm$. Agrupando tenemos $a = (k - l)m + b$. Por lo tanto $a = mt + b$, donde t es un entero.
  P.D. Def. 2 $\Rightarrow$ Def. 3
  Por la def. 2, $a \equiv b \bmod m$ implica $a = mt + b$ con t entero. Entonces $a - b = mt$, es decir, $m \mid a - b$.
  P.D. Def. 3 $\Rightarrow$ Def. 1
  Por la def. 3, $a \equiv b \bmod m$ implica que $a - b = mt$ con t entero, es decir, $a = mt + b$. Dividiendo b entre m obtenemos $b = m q_1 + r$ con $0 \leq r < m$. Entonces $a = mt + mq_1 + r$ y agrupando obtenemos que $a = m(t + q_1) + r$ con $0 \leq r < m$. Por lo tanto a y b dejan el mismo residuo al ser divididos entre m.

La notación $\equiv$ se basa en el hecho de que la congruencia respecto a un módulo fijo tiene varias de las propiedades de la - -

igualdad.

PROPIEDADES DE LAS CONGRUENCIAS

Sea m un natural y sean a, b, c y d números enteros.

1) $a \equiv a \bmod m$
2) Si $a \equiv b \bmod m$, entonces $b \equiv a \bmod m$
3) Si $a \equiv b \bmod m$ y $b \equiv c \bmod m$, entonces $a \equiv c \bmod m$

Demostración de las propiedades anteriores.

1) $a \equiv a \bmod m$

La demostración es directa de la definición de congruencia, ya que como son el mismo número al dividirlos entre m dejan el mismo residuo.

2) Si $a \equiv b \bmod m$ entonces $b \equiv a \bmod m$

DEM:

Como $a \equiv b \bmod m$, entonces $a = mt + b$, con t entero, de donde $b = a - mt$ es decir $b = m(-t) + a$ con $-t$ entero y por lo tanto $b \equiv a \bmod m$.

3) Si $a \equiv b \bmod m$ y $b \equiv c \bmod m$ entonces $a \equiv c \bmod m$

DEM.

Como $a \equiv b \bmod m$ y $b \equiv c \bmod m$ entonces $a = mt + b$ y $b = mt_1 + c$ con t, t_1 enteros, de donde $a = mt + (mt_1 + c)$ es decir, $a = m(t + t_1) + c$, $t + t_1$ entero.
Por lo tanto $a = c \bmod m$

Estas tres propiedades hacen de la relación de "ser congruentes" módulo m, una relación de equivalencia en el conjunto de los enteros. Las correspondientes clases de equivalencia se comprenden fácilmente como sigue: Tomemos otra vez el modulo 24. ada entero a es congruente con sólo uno de los números 0, 1, 2, 3,...,23.

Los multiplos de 24 son todos congruentes con cero (y congruentes entre si, por la propiedad 3). El conjunto de estos múltiplos son la clase de equivalencia del cero.

Los que dejan residuo 1 vienen a ser la clase de equivalencia del 1; los múltiplos listados en la pag. son la clase de equivalencias del 11, etc...

Como se puede apreciar, hay 24 clase de equivalencias distintas (módulo 24, naturalmente).

Esto obedece a que cada entero a lo hemos identificado con su residuo al dividirlo entre 24 y el residuo es necesariamente un número entre 0 y 23 (en otras palabras hemos "clasificado"a los enteros según el residuo que dejan).

En general, para elmódulo $m > 0$ cada entero a es de la -- forma $a = mq + r$ con $0 \leq r < m$ (*) por consiguiente, los m números 0, 1, 2, ..., m - 1 son todos los posibles residúos al dividir entre m. Cada entero es congruente con uno y sólo uno de estos m residúos.

Los múltiplos de m son congruentes con cero; esta es la -- clase de equivalencia del 0. La clase de equivalencia de r, con $0 \leq r < m - 1$, son todos los enteros de la forma (*). En virtud de todo esto, a los números 0, 1, 2, ..., m - 2, m - 1 se les llama un sistema completo de residuos módulo m.

Regresando a las propiedades de las congruencias respecto del mismo mod, es fácil verificar que estas pueden sumarse, restarse y multiplicarse.

OTRAS PROPIEDADES DE LAS CONGRUENCIAS

Si $a \equiv b \bmod m$ y $c \equiv d \bmod m$, entonces

4) $a + c \equiv b + d \bmod m$
5) $a - c \equiv b - d \bmod m$
6) $ac \equiv bd \bmod m$
7) Si $a \equiv b \bmod m$ entonces $a^n \equiv b^n \bmod m$ para toda n natural
8) Si $a \equiv b \bmod m$ entonces $ca \equiv cb \bmod m$ para todo c entero

DEMOSTRACION DE LAS PROPIEDADES ANTERIORES

4.- Si $a \equiv b \bmod m$ y $c \equiv d \bmod m$ entonces $a + c \equiv b + d \bmod m$

DEM:

Como $a \equiv b \bmod m$ y $c \equiv d \bmod m$, entonces $a = mt + b$ y $c = mt_1 + d$ con t, t_1 enteros, de donde $a+c=mt+b+mt_1+d$ es decir, $a + c = m(t + t_1) + (b + d)$ con $t + t_1$ entero. Por lo tanto $a + c \equiv b + d \bmod m$.

5.- Si $a \equiv b \bmod m$ y $c \equiv d \bmod m$, entonces $a - c \equiv b - d \bmod m$
La demostración es completamente análoga a la anterior. (Conviene que el lector la escriba).

6.- Si $a \equiv b \bmod m$ y $c \equiv d \bmod m$, entonces $ac \equiv bd \bmod m$
DEM:

Como $a \equiv b \bmod m$ y $c \equiv d \bmod m$, entonces $a = mt + b$ y $c = mt_1 + d$ con t, t_1 enteros, de donde $ac=(mt+b)(mt_1+d)$ esto es $ac = m(mtt_1 + t_1b + td) + bd$. Y por lo tanto $ac \equiv bd \bmod m$

7.- Si $a \equiv b \bmod m$ entonces $a^n \equiv b^n \bmod m$ para todo n natural.
DEM:

La demostración se hará por inducción. Queremos probar que la propiedad $P_n : a^n \equiv b^n \bmod m$ es verdadera $\forall n \in \mathbb{N}$
La propiedad se cumple para n=1 por hipótesis.
Supongamos que P_n se cumple para n=k, es decir, $a^k \equiv b^k \bmod m$. Vamos a demostrar que es válida para n=k+1. Como $a \equiv b \bmod m$ y $a^k \equiv b^k \bmod m$ entonces $aa^k \equiv bb^k \bmod m$ (prop. 6). Y por tanto $a^{k+1} \equiv b^{k+1} \bmod m$. Y por lo tanto $a^n \equiv b^n \bmod m$ para todo n natural.

8.- Si $a \equiv b \bmod m$ entonces $ca \equiv cb \bmod m$.
DEM:

Como $a \equiv b \bmod m$ entonces $a = mt + b$, t entero; multiplicando por c entero tenemos que $ac = m(tc) + bc$. tc entero por lo tanto $ac \equiv bc \bmod m$.

Como se vé sumar y multiplicar congruencias del mismo módulo siempre es válido, Una pregunta que se ocurre es si valdrá el recíproco de la propiedad 8, es decir, si vale la ley de la cancelación en congruencias :

Si $ca \equiv cb \bmod m$ ¿ocurrirá que $a \equiv b \bmod m$?
No siempre ocurre esto, por ejemplo:
$22 \equiv 8 \bmod 7$ y $11 \equiv 4 \bmod 7$ pero
$14 \equiv 2 \bmod 12$ y $7 \not\equiv 1 \bmod 12$

Y es que en general si $ca \equiv cb \bmod m$ (suponemos $c \not\equiv 0 \bmod m$), entonces $m \mid ca - cb$ o equivalentemente $m \mid c(a-b)$. De aquí no

puede desprenderse que $m|(b-a)$ y por lo mismo no necesariamente $a \equiv b \bmod m$, así que no siempre vale la ley de la cancelación. Sin embargo, este razonamiento nos muestra que bajo ciertas condiciones, sí es posible cancelar; de esta manera agregamos una novena propiedad.

9.- Si $ca \equiv cb \bmod m$ y $(c,m)=1$ entonces $a \equiv b \bmod m$

DEM:

Como $ca \equiv cb \bmod m$ entonces $m|c(a-b)$

y como $(c,m)=1$ entonces $m|a-b$

y porlo tanto $a \equiv b \bmod m$.

Una última propiedad:

10.- Si $a \equiv b \bmod m_1$, $a \equiv b \bmod m_2$, ..., $a \equiv b \bmod m_k$ entonces

$a \equiv b \bmod [m_1, m_2, \ldots, m_k]$

DEM:

Como $a \equiv b \bmod m_1$, $a \equiv b \bmod m_2$, ..., $a \equiv b \bmod m_k$ entonces $a-b=m_1t_1$, $a-b=m_2t_2$, ..., $a-b=m_kt_k$ $t_1, t_2, \ldots t_k$ enteros.

Esto es, a-b es multiplo común de $m_1, m_2, \ldots, m_k$ entonces (corolario 1 secc. m.c.m.) a-b es múltiplo del m.c.m. de $m_1, m_2, \ldots, m_k$

es decir, $a-b = [m_1, m_2, \ldots, m_k]t$ t entero

por lo tanto $a \equiv b \bmod [m_1, m_2, \ldots, m_k]$

EJEMPLOS

1.- Cuál es el último dígito de 2^{40}?

Aquí se trata de buscar un procedimiento para encontrar el último dígito de 2^{40} sin tener que multiplicar a 2 por sí mismo 40 veces.

Para poder resolver este problema observemos lo siguiente:

Tomemos un número cualquiera, por ejemplo 342.

342 lo podemos expresar como $342=34 \cdot 10+2$.

5421 lo podemos escribir como $5421 = 542 \cdot 10 + 1$.

Estos números al dividirlos entre 10 dejan como residuo al último dígito del número.

En general si tengo un número N formado por los dígitos $a_n, a_{n-1}, \ldots, a_1, a_0$, N lo podemos expresar como

$N = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$, es decir,

$N = 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_1) + a_0$.

Si llamamos t a lo que está dentro del paréntesis tenemos que:

$N = 10t + a_0$, es decir,

$N \equiv a_0 \mod 10$

Ahora sí, ayudados con esto y las propiedades de las congruencias podemos resolver nuestro problema.

Para encontrar el último dígito de 2^{40} basta con encontrar $0 \leq x < 10$ tal que $2^{40} \equiv x \mod 10$.

Para empezar: $2^{40} = (2^5)^8 = 32^8$ (a)

por la propiedad 7 tenemos que $32^8 \equiv 2^8 \mod 10$. (b)

Ahora bien, $2^8 = (2^4)^2 = 16^2$ y $16 \equiv 6 \mod 10$. En consecuencia $16^2 \equiv 6^2 \equiv 6 \mod 10$.

Por lo tanto $2^8 \equiv 6 \mod 10$.

Regresando a (b) resulta que $32^8 \equiv 2^8 \equiv 6 \mod 10$ y por tanto, de (a) $2^{40} \equiv 6 \mod 10$, es decir, el último dígito de 2^{40} es 6.

2.- Demostrar que $1^5 + 2^5 + 3^5 + \ldots + 11^5$ es múltiplo de 3.

Basta con demostrar que $1^5 + 2^5 + \ldots + 11^5 \equiv 0 \mod 3$.

$1 \equiv 1 \mod 3$	$4 \equiv 1 \mod 3$	$7 \equiv 1 \mod 3$	$10 \equiv 1 \mod 3$
$2 \equiv 2 \mod 3$	$5 \equiv 2 \mod 3$	$8 \equiv 2 \mod 3$	$11 \equiv 2 \mod 3$
$3 \equiv 0 \mod 3$	$6 \equiv 0 \mod 3$	$9 \equiv 0 \mod 3$	

por la propiedad 7 tenemos que

$1^5 \equiv 1 \mod 3$	$4^5 \equiv 1 \mod 3$	$7^5 \equiv 1 \mod 3$	$10^5 \equiv 1 \mod 3$
$2^5 \equiv 2 \mod 3$	$5^5 \equiv 2 \mod 3$	$8^5 \equiv 2 \mod 3$	$11^5 \equiv 2 \mod 3$
$3^5 \equiv 0 \mod 3$	$6^5 \equiv 0 \mod 3$	$9^5 \equiv 0 \mod 3$	

sumando de ambos lados de la congruencia (propiedad 4) tenemos que

$$1^5 + 2^5 + 3^5 + \ldots + 11^5 \equiv 12 \equiv 0 \mod 3$$

por lo tanto $1^5 + 2^5 + 3^5 + \ldots + 11^5$ es múltiplo de 3.

3.- Los hombres de cierto ejército no podían se divididos en grupos de 2, 3, 4, ..., 12 ya que en cada caso sobraba un hombre, sin embargo, si era posible acomodarlos en grupos de 13 ¿cuál era el menor número de hombres en el ejército?

Si llamamos x al número de hombres en el ejército, lo que buscamos es la menor x tal que

$$\left.\begin{array}{l} x \equiv 1 \bmod 2 \\ x \equiv 1 \bmod 3 \\ \vdots \\ x \equiv 1 \bmod 12 \end{array}\right\} (*) \qquad \text{y} \quad x \equiv 0 \bmod 13$$

Pero por la propiedad 10 podemos expresar las congruencias (*) como la congruencia $x \equiv 1 \bmod [2, 3, \ldots, 12]$. Entonces lo que buscamos es la x menor tal que

$$x \equiv 1 \bmod 27720 \qquad \text{y} \qquad x \equiv 0 \bmod 13.$$

Las que satisfacen la primera congruencia son de la forma $x = 27720m + 1$ con m entero; de éstas hay que escoger aquella que cumpla con la segunda congruencia, es decir, encontrar la menor m tal que

$$27720m + 1 \equiv 0 \bmod 13$$

Pero como $27720 \equiv 4 \bmod 13$

entonces $27720m + 1 \equiv 4m + 1 \bmod 13$

esto es, buscamos la menor m tal que

$$4m + 1 \equiv 0 \bmod 13.$$

Por inspección es fácil encontrarla. La solución es m=3. Y por lo tanto $x = 27720\ 3 + 1 = 83161$.

Notemos que si por inspección no se ocurre la solución de la congrunecia $4m + 1 \equiv 0 \bmod 13$, podemos resolverla de la siguiente manera:

$4m + 1 \equiv 0 \bmod 13$ si y solo si $4m + 1 = 13t$ $t \in Z$

es decir, la congruencia podemos transformarla en la ecuación diofantina $4m - 13t = -1$ para la cual ya tenemos un método para resolverla.

$m_0 = 3$, $t_0 = 1$ son una solución particular y por lo tanto las soluciones de la ecuación son $m = 3 + 13k$, $t = 1 + 4k$ con k entero. Así que la menor m se obtiene con $k = 0$ y la x puede ser cualquier número de la forma $x = 27720(13k + 3) + 1 =$

$= 360360k + 83161$.

Así para k = 0 tenemos la solución buscada x = 83161.

Esto último nos permite establecer en general que resolver la ecuación en x entero $ax \equiv b \bmod m$ donde a, b y m son enteros y $m > 0$ es equivalente a resolver la ecuación diofantina $ax - mt = b$.

En efecto, las x, si las hay, que satisfacen $ax \equiv b \bmod m$ son aquellas para las que $m \mid ax - b$, es decir, $ax - b = mt$, t entero, y por lo tanto las que satisfacen $ax - mt = b$.

4.- Una pila de ladrillos es tal que si la dividimos en 2 sobra 1; si la dividimos en 3 sobran 2; en 4 sobran 3; vidimos en 12 sobran 11. Sin embargo se puede dividir en 13. ¿Cuál es el menor número de ladrillos en la pila?

Si x es el número de ladrillos, lo que tenemos planteado es el siguiente sistema de congruencias:

$$\left.\begin{array}{l} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 4 \\ \quad \vdots \\ x \equiv 11 \bmod 12 \end{array}\right\} \quad (**) \qquad \text{y} \quad x \equiv 0 \bmod 13$$

Este sistema da la impresión de ser distinto al del ejemplo anterior, sin embargo, lo podemos transformar en uno equivalente

$$\left.\begin{array}{l} x \equiv -1 \bmod 2 \\ x \equiv -1 \bmod 3 \\ x \equiv -1 \bmod 4 \\ \quad \vdots \\ x \equiv -1 \bmod 12 \end{array}\right\} \quad (***) \qquad \text{y} \quad x \equiv 0 \bmod 13$$

que se resuelve de forma análoga al anterior.

(***) se transforma en $x \equiv -1 \bmod 27720$ y por lo tanto $x = 27720k - 1$ con k entero. Como $x \equiv 4k-1 \bmod 13$, tenemos, por inspección, que k=10 satisface $x \equiv 0 \bmod 13$ y por lo tanto $x = 277199$. Así el número de ladrillos en la pila es 277199.

Obsérvese que $k = 13m + 10$ y que $x = 27720(13m + 10) - 1 = 360360m + 277199$ es solución.

EJERCICIOS

1. Encuentre la menor x positiva en cada una de las congruencias siguientes:

i) $572^{24} \equiv x \bmod 4$

ii) $321^{210} \equiv x \bmod 5$

iii) $232^{15} \equiv x \bmod 10$

iv) $3^{100} \equiv x \bmod 5$

v) $2^{21} \equiv x \bmod 11$

2. Qué residuo deja $1^{10} + 2^{10} + \ldots + 100^{10}$ al dividirlo entre 7?

3. ¿Cuáles de las siguientes congruencias son válidas?

i) $12\,345\,678\,987\,654\,321 \equiv 0 \bmod 12\,345\,678$

ii) $12\,345\,678\,987\,654\,321 \equiv 0 \bmod 12\,345\,679$

iii) $57 \equiv 208 \bmod 4$

iv) $531 \equiv 1236 \bmod 7561$

v) $12345 \equiv 111 \bmod 3$

4. Pruebe que si $bd \equiv bd' \bmod p$ donde p es primo y $p \nmid b$ entonces $d \equiv d' \bmod p$.

5. Enuncie y demuestre un resultado que establezca una condición necesaria y suficiente para que la congruencia $ax \equiv b \bmod m$ tenga solución.

6. Diga cómo encontrar <u>todas</u> las soluciones de la congruencia $ax \equiv b \bmod m$.

7. Encontrar todas las soluciones de las siguientes congruencias lineales:

i) $362x \equiv 236 \bmod 24$ ii) $55x \equiv 5 \bmod 31$ iii) $84x \equiv 96 \bmod 7$

8. Demostrar que la congruencia $ax \equiv 1 \bmod m$ tiene solución si y sólo si $(a,m) = 1$.

9. ¿Cuál es el menor entero positivo que deja residuo 1 al dividir entre 1000 y residuo 8 cuando dividimos entre 761?

10. Utilizando congruencias demuestre que un número es divisible entre 4 <u>si y sólo si</u> el entero formado por sus dos últimas cifras es divisible entre 4.

II TEORIA DE ECUACIONES ALGEBRAICAS

Uno de los problemas que fue ocupando un lugar central en el algebra a finales del siglo XVIII y comienzos del siglo XIX era la teoría de la resolución de ecuaciones algebraicas de -- grado n con una incógnita,

La ecuación de segundo grado fué resuelta en la Antigüe-- dad. Su solución general es muy sencilla. Los algebristas - italianos del siglo XVI (durante el Renacimiento en Italia) en contraron reglas generales análogas, aunque más complicadas pa ra la solución de ecuaciones de tercero y cuarto grados. Las investigaciones que se hicieron para encontrar soluciones de - las ecuaciones de grado superior tropezaron con dificultades - insalvables.

Iniciamos este capítulo presentando las soluciones genera les o "fórmulas" para las ecuaciones de primero, segundo, ter- cero y cuarto grados.

El método para resolver estas ecuaciones fué el de las ma nipulaciones algebraicas, recurriendo en las ecuaciones de ter cero y cuarto grados a soluciones de ecuaciones auxiliares.

SOLUCION ALGEBRAICA DE UNA ECUACION

Una ecuación algebraica de grado n en una incógnita es una ecuación de la forma

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = 0 \qquad (1)$$

en la que $a_1, a_2, \ldots, a_n$ son coeficientes conocidos.

Resolver una ecuación quiere decir encontrar todos los valores de x tales que al sustituirlos en (1) satisfagan la igualdad.

El método para resolver las ecuaciones algebraicas fue el de encontrar ciertas fórmulas que expresaran las soluciones de la ecuación en términos de sus coeficientes y que dichas fórmulas sólo involucraran las operaciones suma, resta, multiplicación, división y radicación con exponentes enteros positivos.

ECUACIONES DE PRIMERO Y SEGUNDO GRADO

La solución para la ecuación de primer grado

$$x + a = 0$$

es inmediata. Se obtiene sumando a ambos lados el inverso aditivo de a. Teniendo como solución $x = -a$.

La ecuación de segundo grado también se resuelve de manera sencilla. Desde tiempos de los griegos se sabia resolver por el método de completar cuadrados, que consiste en lo siguiente:

Sea

$$x^2 + px + q = 0$$

la ecuación de segundo grado.

Entonces

$$x^2 + px = -q$$

completamos el cuadrado perfecto

$$x^2 + px + \left(\frac{p}{2}\right)^2 = -q + \left(\frac{p}{2}\right)^2$$

y lo expresamos como binomio al cuadrado

$$\left(x + \frac{p}{2}\right)^2 = -q + \frac{p^2}{4}$$

$$x + \frac{p}{2} = \pm\sqrt{-q + \frac{p^2}{4}}$$

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2 - 4q}{4}}.$$

$$x = -\frac{p}{2} \pm \frac{\sqrt{p^2 - 4q}}{2}$$

obteniendo como solución general

$$x = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

LA ECUACION DE TERCER GRADO

Sobre la ecuación de tercer grado se habían resuelto algunos casos particulares pero no se había encontrado un método general que pudiera utilizarse para resolver cualquier cúbica. Fue hasta el siglo XVI cuando los matemáticos italianos Tartaglia (1500-1557), Cardano (1501-1576), Del Ferro (1465-1526) descubren un procedimiento para resolver ecuaciones del tipo

$$x^3 + px + q = 0$$

Sea

$$x^3 + bx^2 + cx + d = 0 \qquad (2)$$

la ecuación de tercer grado. La solución de esta puede reducirse a la solución de una ecuación cúbica de la forma

$$x^3 + px + q = 0 \qquad (3)$$

Supongamos que $x = z$ es solucion de (2) entonces

$$z^3 + bz^2 + cz + d = 0$$

ahora si $z = w - \frac{b}{3}$

sustituyendo obtenemos

$$(w - \frac{b}{3})^3 + b(w - \frac{b}{3})^2 + c(w - \frac{b}{3}) + d = 0$$

$$w^3 - 3w^2\frac{b}{3} + 3w\frac{b^2}{9} - \frac{b^3}{27} + bw^2 - 2w\frac{b^2}{3} + \frac{b^3}{9} + cw - c\frac{b}{3} + d = 0$$

$$w^3 + w\frac{b^2}{3} - w\frac{2b^2}{3} + cw + \frac{b^3}{9} - \frac{b^3}{27} - \frac{cb}{3} + d = 0$$

si $p = c - \frac{b^2}{3}$ y $q = d - \frac{cb}{3} + \frac{2b^3}{27}$

tenemos que

$$w^3 + pw + q = 0$$

Es decir si z es solución de (2) y $z = w - \frac{b}{3}$

entonces w es solución de (3).

Inversamente si w es solución de (3) con p y q como se mencionó arriba y $w = z + \frac{b}{3}$ entonces z es solución de (2)

De esta manera el problema de resolver la ecuación de tercer grado se reduce a resolver la que tiene la forma

$$x^3 + px + q = 0$$

Esta ecuación se resuelve de la siguiente manera:

Sea $x = u + v$

sustituyendo en (3)

$$(u + v)^3 + p(u + v) + q = 0$$

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u + v) + q = 0$$

$$u^3 + v^3 + p(u + v) + 3uv(u + v) + q = 0$$

$$u^3 + v^3 + (u + v)(p + 3uv) + q = 0 \qquad (4)$$

Aquí se utiliza el siguiente hecho: cualquiera que sea la suma de dos números, siempre es posible exigir que su producto tenga un valor fijado de antemano, obteniendo un sistema

$$\left.\begin{aligned} m + n &= A \\ mn &= B \end{aligned}\right\} \qquad (a)$$

que siempre tiene solución. Así que si pedimos que el segundo sumando de (4) sea cero, es decir, que $p + 3uv = 0$ obtenemos el sistema

$$\left.\begin{aligned} u^3 + v^3 + q &= 0 \\ p + 3uv &= 0 \end{aligned}\right\} .$$

que puede escribirse como

$$\left.\begin{aligned} u^3 + v^3 &= -q \\ u^3v^3 &= -\frac{p^3}{27} \end{aligned}\right\} \qquad (b)$$

Nótese que tiene la forma del sistema (a)

Por tanto si encontramos los numeros u y v que satisfagan este sistema de ecuaciones, el número $x = u + v$ será raíz de la ecuación (3)

El sistema (b) siempre tiene solución y se obtiene como vere

mos. Despejamos v^3 de la primera ecuación del sistema (b)

$$v^3 = -q - u^3$$

sustituyendo en la segunda ecuación tenemos que

$$u^3(-q - u^3) = -\frac{p^3}{27}$$

$$-u^3q - (u^3)^2 = -\frac{p^3}{27}$$

$$(u^3)^2 + q(u^3) - \frac{p^3}{27} = 0$$

por tanto para resolver el sistema (b) es suficiente con que u^3 sea solución de la ecuación de segundo grado

$$z^2 + qz + \frac{p^3}{27} = 0$$

Como ya conocemos la fórmula general para dichas ecuaciones obtenemos que

$$u^3 = \frac{-q \pm \sqrt{q^2 + 4(p^3/27)}}{2}$$

es decir,

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

y como

$$v^3 = -q - u^3$$

obtenemos los valores siguientes:

Si $u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, $v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$

o bien si $u^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, $v^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$

en ambos casos obtenemos como solución general de (3)

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad [1]$$

conocida como la formula de Cardano

---

1) Recordemos que para obtener esta solución general se pidió en el desarrollo que $3uv + p = 0$; es decir, que $uv = -\frac{p}{3}$, esto va a ser necesario contemplarlo cuando estemos resolviendo los casos particulares de ecuaciones de tercer grado con esta fórmula.

LA ECUACION DE CUARTO GRADO

Poco después de la resolución de la ecuación cúbica, Ferrari (1522-1565) resolvió la ecuación general de cuarto grado. Para la solución de la ecuación de tercer grado hemos visto que se necesita la solución de la ecuación auxiliar de segundo grado

$$z^2 + qz - \frac{p^3}{27} = 0$$

donde $z = u^3$ o v^3; análogamente, la solución de una ecuación de cuarto grado se basa en la solución de una ecuación cúbica auxiliar.

El método de Ferrari consiste en lo siguiente:

Sea $x^4 + ax^3 + bx^2 + cx + d = 0$ (1)

la ecuación general de cuarto grado.

Escribámosla en la forma

$$x^4 + ax^3 = -bx^2 - cx - d$$

completamos en el primer miembro de la igualdad un cuadrado perfecto

$$x^4 + ax^3 + \frac{a^2x^2}{4} = -bx^2 - cx - d + \frac{a^2x^2}{4}$$

$$\left(x^2 + \frac{ax}{2}\right)^2 = \left(\frac{a^2}{4} - b\right)x^2 - cx - d$$

formamos nuevamente en el primer miembro un cuadrado perfecto, introduciendo una nueva variable y. Para esto sumamos a ambos miembros

$$\left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4}$$

(mas adelante se le impondrá una condición necesaria a la variable y)

$$\left(x^2 + \frac{ax}{2}\right)^2 + \left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4} = \left(\frac{a^2}{4} - b\right)x^2 - cx - d + \left(x^2 + \frac{ax}{2}\right)y + \frac{y^2}{4}$$

$$\left(x^2 + \frac{ax}{2} + \frac{y^2}{4}\right)^2 = \left(\frac{a^2}{4} - b + y\right)x^2 + \left(\frac{ay}{2} - c\right)x + \left(\frac{y^2}{4} - d\right) \qquad (2)$$

El problema ha quedado reducido a otro con dos incógnitas. El segundo miembro de la ecuación (2) es un trinomio de segun

EJERCICIOS

Encuentre las raíces de las siguientes ecuaciones

1) $x^4 = -16i$

2) $x^4 = 1 + i$

3) $x^3 = -2i$

4) $x^3 = 1-i$

5) $x^4 = -1/2 + i\sqrt{3}/2$

6) $x^6 = 1 + \sqrt{3} + (1-\sqrt{3})i$

7) $x^5 = 1$

8) $z^4 = i$

9) Usando la fórmula de De Moivre obtener expresiones para $\cos 5\theta$ y $\operatorname{sen} 5\theta$ en términos de $\cos\theta$ y $\operatorname{sen}\theta$

10) Sea $\rho = \cos(2\pi/3) + i\operatorname{sen}(2\pi/3)$

a) Pruebe que $z=1$, $z=\rho$, $z=\rho^2$ son las diferentes soluciones de la ecuación $z^3=1$

b) Pruebe que si $z = u$ es una solución de $z^3 = w$, entonces las otras soluciones son de la forma $u\rho^j$ donde $j = 1,2$

Antes de pasar a la siguiente sección demostraremos un resultado que nos va a ser de gran utilidad en la resolución de las ecuaciones de tercer grado por la fórmula

TEOREMA. Sea $w,z \in \mathbb{C}$

Si w es raíz n-ésima de z, entonces $\bar{w}$ es raíz n-ésima de $\bar{z}$

DEM.

Si w es raíz n-ésima de z, entonces $w^n = z$ y como $\overline{w^n}=\bar{w}^n$ entonces $\bar{w}^n = \bar{z}$

por lo que $\bar{w}$ es raíz n-ésima de $\bar{z}$.

do grado en x cuyos coeficientes dependen de y. Elijamos y de modo que este trinomio sea el cuadrado de un binomio de primer grado $\alpha x + \beta$.

Para que el binomio de segundo grado

$$Ax^2 + Bx + C$$

sea el cuadrado del binomio $\alpha x + \beta$ es suficiente con que el trinomio sea cuadrado perfecto, es decir, que

$$B = 2\sqrt{A}\sqrt{C}$$

esto es $B^2 = 2AC$

de donde $B^2 - 4AC = 0$

En efecto, si $B^2 - 4AC = 0$ entonces

$$Ax^2 + Bx + C = (\sqrt{A}x + \sqrt{C})^2$$

es decir $Ax^2 + Bx + C = (\alpha x + \beta)^2$

donde $\alpha = \sqrt{A}$ y $\beta = \sqrt{C}$

por tanto si se elige y tal que

$$(\frac{ay}{2} - c)^2 - 4(\frac{a^2}{4} - b - y)(\frac{y^2}{4} - d) = 0 \qquad (3)$$

la primera parte de la ecuacion (2) será el cuadrado perfecto $(\alpha x + \beta)^2$.

desarrollando (3) obtenemos

$$\frac{a^2y^2}{4} - acy + c^2 + (-a^2 + 4b - 4y)(\frac{y^2}{4} - d) = 0$$

$$\frac{a^2y^2}{4} - acy + c^2 - \frac{a^2y^2}{4} + a^2d + by^2 - 4bd - y^3 + 4dy = 0$$

$$y^3 - by^2 + (ac - 4d)y - (d(a^2 - 4b) + c^2) = 0 \qquad (4)$$

De modo que elegir y tal que satisfaga (3) es lo mismo que encontrar una solución y_o de la ecuación cúbica auxiliar (4) (recuérdese que siempre es posible).

Con esta solución y_o se calculan α y β y (2) queda

$$(x^2 + \frac{ax}{2} + \frac{y_o}{2})^2 = (\alpha x + \beta)^2$$

de donde

$$x^2 + \frac{ax}{2} + \frac{y_o}{2} = \pm(\alpha x + \beta)$$

A partir de estas dos ecuaciones de segundo grado se pueden encontrar las cuatro raíces de la ecuación de cuarto grado. dada.

De esta manera los matemáticos italianos del siglo XVI -- llegan a la resolución de las ecuaciones algebraicas de tercero y cuarto grado . Después de estos logros, no hubo matemático de la época que no intentara por el mismo procedimiento resolver las ecuaciones de quinto grado y de grados superiores. En esa época era natural pensar que, por ejemplo, para la ecuación de quinto grado era posible encontrar una fórmula. En sus intentos por obtenerla, los matemáticos llegaban como en el caso de la ecuación de tercero y cuarto grado a la necesidad de resolver ecuaciones auxiliares, sólo que estas siempre resultaban ser de grado mayor que cinco.

Así transcurrieron más de dos siglos y medio, desde el tiempo de Del Ferro sin que nadie, durante este largo periodo hubiese podido encontrar soluciones generales para las ecuaciones de grado n para $n \geq 5$, pero tampoco nadie dudaba que el problema tuviera solución. Sobre lo que empiezan a dudar -- años más tarde, es sobre si el método seguido hasta entonces era el adecuado para obtener las soluciones, se dan cuenta que en cierta forma las transformaciones, sustituciones e introducción de variables auxiliares que utilizan en la búsqueda de soluciones son muy especiales y en cierta forma accidentales. El trabajo de Lagrange "Reflexiones sobre la resolución de ecuaciones algebraicas" publicado en 1770-1771 es representativo de esto. Lagrange dice "por nuestro razonamiento vemos que es muy dudoso que los métodos que hemos considerado puedan dar -- una solución completa de las ecuaciones de quinto grado". En su trabajo él examina críticamente las soluciones de las ecuaciones de segundo, tercero y cuarto grado que se conocían hasta entonces y demuestra que dichas soluciones se basan siempre en propiedades que no se verifican para las ecuaciones de grado $n \geq 5$ y desarrolló otros métodos para la resolución de -- las mismas. Los métodos de Lagrange estaban completamente ordenados y desarrollados a partir de una idea general en la que intervenía la teoría de los polinomios simétricos, la teoría -

de las permutaciones (que según expresó Lagrange es la "verdadera filosofía de toda la cuestión" en lo cual acertó plenamente, como lo demostraron las investigaciones posteriores de Galois) y la teoría de resolventes.

Sin embargo, aún cuando Lagrange con sus nuevos métodos logra dar un giro a cómo abordar el problema de las soluciones de una ecuación y, que de hecho es la base para resolverlo, no se llega en esos tiempos a su solución e incluso se sigue pensando que es posible resolver por radicales las ecuaciones de grado $n \geq 5$. En su memoria Lagrange dice: "El problema de resolver (por radicales) ecuaciones de grado mayor que cuatro es uno de quellos problemas que no han sido resueltos, aunque nada demuestra la imposibilidad de su resolución".

Es hasta el año de 1824 que Abel (1802-1829) publica la demostración de que, si los coeficientes a_1, a_2, ..., a_n de una ecuación

$$x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

se consideran unicamente como letras, no existe entonces ninguna expresión radical de estos coeficientes que sea raiz de la ecuación correspondiente, si su grado es mayor o igual a cinco.

Galois va más adelante respecto a esta problemática. Si bien la ecuación general de grado superior a cuatro no puede resolverse por radicales, sí hay muchas ecuaciones especiales de grado arbitrario que pueden resolverse. Galois determina exactamente qué ecuaciones pueden ser resueltas por radicales, en otras palabras, determina las condiciones necesarias y suficientes para la resolución de una ecuación por radicales.

Esto es en resumen los intentos y logros que durante siglos se llevaron a cabo para resolver por radicales una ecuación de n-ésimo grado. El problema resultó muy difícil y profundo y condujo a la aparición de nuevos conceptos, importantes no solo para el álgebra, sino para toda la matemática.

Después de este breve esbozo de cómo fué resuelta la problemática, regresemos a analizar cómo son las soluciones de ciertas ecuaciones particulares.

RAICES DE NUMEROS NEGATIVOS

Para la ecuación de segundo grado $x^2 + px + q = 0$ la solución general esta dada por

$$x = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

observemos que si $p^2 - 4q < 0$ ya no podemos con sólo los reales, obtener la solución, aún cuando dicha solución esté indicada por la fórmula. Es el caso de la ecuación

$$x^2 - 2x + 2 = 0$$

cuya solución es

$$x = \frac{2 \pm \sqrt{-4}}{2}$$

esta "solución" para nosotros no tiene sentido pues en el sistema de números que hasta el momento hemos trabajado, que es el de los reales, no es posible extraer la raíz cuadrada de un número negativo, (no existen números reales tales que su cuadrado sea negativo).

Pero esto de encontrarse con raíces negativas no solo ocurre con la fórmula para la ecuación de segundo grado. Observemos la de tercer grado.

La ecuación $x^3 + px + q = 0$ tiene como solución

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

si $\frac{q^2}{4} + \frac{p^3}{27} < 0$ otra vez aparece una raíz negativa y ya no podemos calcular la solución. Veamos el siguiente ejemplo:

$$x^3 - 15x - 4 = 0$$

es fácil encontrar por inspección, la solución $x = 4$

$$(4)^3 - 15(4) - 4 = 0$$

pero aplicando la fórmula, la solución nos queda

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

¡qué pasa aquí! Por un lado sabemos que la solución es un número real y por otro nos resulta con raíces negativas; pero además, admitimos los dos caminos para encontrar la solución como válidos. Estando así el asunto, no nos queda otra que admitir

como "números" con los que podemos "operar" lo que aparece dentro de la raíz cúbica. Así pues,"operemos" con estos "números" y veamos que sucede. Por supuesto que operamos como si fuesen numeros reales.

Queremos calcular

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

para ello tenemos que saber a que es igual

$$\sqrt[3]{2 + \sqrt{-121}} \quad y \quad \sqrt[3]{2 - \sqrt{-121}}$$

pero

$$\sqrt[3]{2 \pm \sqrt{-121}} = (2 \pm \sqrt{-1})$$

ya que

$$\begin{aligned}(2 \pm \sqrt{-1})^3 &= 8 + 12(\pm\sqrt{-1}) + 6(\sqrt{-1})^2 \pm (\sqrt{-1})^3 \\ &= 8 + 12(\pm\sqrt{-1}) + 6(\sqrt{-1})^2 \mp \sqrt{-1} \\ &= 2 \pm 11\sqrt{-1} \\ &= 2 \pm \sqrt{-121}\end{aligned}$$

ahora si

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = 2 + \sqrt{-1} + 2 - \sqrt{-1} = 4.$$

Sucede que obtenemos la raíz real $x = 4$

En realidad, durante mucho tiempo, cuando al tratar de resolver una ecuación aparecían raíces negativas, se descartaban éstas, diciendo que la ecuación no tenía solución. Posteriormente los matemáticos se dan cuenta que aunque aparecían raíces negativas la ecuación podia tener solución, aunque esta resultara un "ente desconocido". A las raíces de números negativos les llamaron numeros "imaginarios" o "imposibles". Después, como dijo Cardano, "haciendo a un lado las torturas mentales" empiezan a operar con las raíces negativas como si fueran numeros reales, obteniendo, como en el ejemplo que acabamos de ver, incluso soluciones reales.

De lo anterior podemos sacar dos conclusiones

1) Que no basta con los números reales para obtener las soluciones de muchas ecuaciones, así que es necesario extender el sistema de los números reales de modo tal que ecuaciones tan simples como $x^2 + 1 = 0$ tengan solución.

2) Que la manera natural de extenderlos es admitiendo las raíces negativas y operandolas como números reales.

NUMEROS COMPLEJOS

De hecho la necesidad de los números complejos, esto es, números de la forma $a + b\sqrt{-1}$, aparece en relación a la resolución de ecuaciones algebraicas. Pero lo cierto es que para que pudieran ser aceptados y comprendidos en su totalidad tuvieron que aparecer en multitud de problemas, como por ejemplo en problemas de calcular integrales por el método de fracciones parciales.

Para calcular la integral.

$$\int \frac{dx}{x^2 + 1}$$

necesitaban calcular la integral.

$$\int \frac{dx}{x + \sqrt{-1}}$$

ya que

$$\int \frac{dx}{x^2 + 1} = \frac{1}{2\sqrt{-1}} \int \left(\frac{1}{x + \sqrt{-1}} - \frac{1}{x - \sqrt{-1}} \right) dx$$

Leibniz y Bernoulli no vacilaron en resolver este tipo de integrales. Bernoulli transforma la integral

$$\int \frac{a\,dz}{b^2 + z^2} \quad \text{en} \quad \int \frac{-a\,dt}{2\,bt\sqrt{-1}}$$

haciendo $$z = \frac{(t - 1)\, b\sqrt{-1}}{t + 1}$$

y la resuelve mediante logaritmos. De paso muestra la relación entre el logaritmo de un imaginario y la función arcotangente.

Dicho esto, pasamos directamente a definir los números complejos y sus operaciones. Estas definiciones, remarcamos, se dan a partir de que son manejados como números reales.

Los números complejos son de la forma.

$$a + b\sqrt{-1}$$

simplemente por notación llamaremos i a $\sqrt{-1}$. La i se debe a aquello de imaginarios. Entonces formalmente los números complejos son de la forma.

$a + bi$ donde a y b son números reales y $i^2 = -1$

Denotaremos al conjunto de los números complejos por $\mathbb{C}$.

DEFINICION 1. Igualdad de complejos

$$a + bi = c + di \iff a = c \quad y \quad b = d$$

DEFINICION 2. Suma y Producto de Complejos

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

Apartir de estas definiciones facilmente puede demostrarse el siguiente teorema

TEOREMA 1. El conjunto de los núemros complejos es un campo, es decir, satisface las siguientes propiedades:

Si z_0, z_1, y z_2 son números complejos arbitrarios, entonces

1) $z_0 + z_1 = z_1 + z_0$

2) $z_0 + (z_1 + z_2) = (z_0 + z_1) + z_2$

3) Existe el neutro bajo la suma: $0 + 0i$

4) Para todo complejo existe un inverso bajo la suma que denotaremos por $-z$. Si $z = a + bi$ entonces $-z = -a + (-b)i$

5) $z_0 z_1 = z_1 z_0$

6) $z_0(z_1 z_2) = (z_0 z_1) z_2$

7) Existe el neutro bajo el producto: $1 + 0i$

8) Para todo complejo $z \neq 0 + 0i$ existe su inverso bajo el producto que denotaremos por z^{-1}. Si $z = a + bi$ entonces $z^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i$

9) $z_0(z_1 + z_2) = z_0 z_1 + z_0 z_2$

La demostración se deja como ejercicio.

El hecho de que $\mathbb{C}$ sea un campo nos permite definir las operaciones de resta y división para los complejos.

DEFINICION 3. Si z y w son complejos arbitrarios entonces

$$z - w = z + (-w) \quad \text{y}$$
$$\frac{z}{w} = z w^{-1}$$

PARTE REAL, PARTE IMAGINARIA Y CONJUGADO DE UN COMPLEJO

En un número complejo $z = a + bi$, a es llamada la parte real y se denota $a = \mathrm{Re}(z)$ y b la parte imaginaria denotada por $b = \mathrm{Im}(z)$.

Los números complejos a con parte imaginaria 0 son llamados números reales y a los números de la forma bi con la parte real igual a 0 se les llama imaginarios puros.

Al complejo $a - bi$ se le llama el conjugado del complejo $z = a + bi$ y se denota como $\overline{z} = a - bi$.

El producto de dos números conjugados $z = a + bi$, $\overline{z} = a - bi$ es un número real $z\overline{z} = (a + bi)(a - bi) = a^2 + b^2$

Los números reales coinciden con sus conjugados, e inversamente, un número que es igual a su conjugado es real. En

efecto, la igualdad $a + bi = a - bi$ nos lleva a que $b = -b$ y esto solo ocurre si $b = 0$.

Unos cuantos ejemplos muestran la sencillez con la que se operan los complejos.

EJEMPLOS

1. Encontrar $(1 + i)^3$; $(1 + i)^2 = 1 + 2i + i^2 = 2i$

entonces $(1 + i)^3 = (1 + i)^2(1 + i) = 2i(1 + i) = 2i + 2i^2$

$\therefore \quad (1 + i)^3 = -2 + 2i$

el mismo ejemplo puede resolverse así:

$$(1 + i)^3 = 1 + 3i + 3i^2 + i^3$$

pero

$$i^2 = -1 , \quad i^3 = i^2 \cdot i = -i$$

entonces

$$(1 + i)^3 = 1 + 3i - 3 - i = -2 + 2i$$

2. Reduzca el número complejo $\frac{1 + i}{1 - i}$

$$\frac{1 + i}{1 - i} = (1 + i)(1 - i)^{-1} = (1 + i)\left(\frac{1}{2} + \frac{1}{2}i\right) = 0 + 1i = i$$

3. Calcule el cociente $\frac{(2 + i)(1 - 2i)}{3 - i}$

$$\frac{(2 + i)(1 - 2i)}{3 - i} = \frac{4 - 3i}{3 - i} = \frac{(4 - 3i)(3 + i)}{(3 - i)(3 + i)} = \frac{15 - 5i}{10} = \frac{3}{2} - \frac{1}{2}i$$

EJERCICIOS

Reduzca los siguientes complejos a la forma $a + bi$

1) $7 - i + (-6 + 3i) - (4 + 3i)$

2) $(2 + i)(1 + 2i)$

3) $(2 - 3i)i$

4) $\frac{1}{i}$

5) $\frac{1 + i}{-i}$

6) $\frac{1 + i}{i} + \frac{i}{1 - i}$

7) $\frac{(4 + 3i)(1 - 2i)}{7 - i}$

8) $\frac{(1 + i)^5}{1 - i}$

9) $\left(\frac{1 + i}{\sqrt{2}}\right)^4$

10) $\frac{i}{1 + i} + \frac{i}{1 + i} + \frac{i}{1 + i}$

11) Demostrar el teorema 1

12) Demostrar que si z_0 y z_1 son complejos

$$z_0 \cdot z_1 = 0 \Leftrightarrow z_0 = 0 \text{ ó } z_1 = 0$$

13) Encontrar valores reales de x y y tales que

$$(1 + i)(x + 2y) - (3 - 2i)(x - y) = 5 + 3i$$

14) Encontrar soluciones reales de

$$(1 + i)x^3 + (1 + 2i)x^2 - (1 + 4i)x - 1 + i = 0$$

Si z y w son complejos arbitrarios demostrar que

15) $\overline{z + w} = \overline{z} + \overline{w}$

16) $\overline{(-z)} = -\overline{z}$

17) $\overline{\overline{z}} = z$

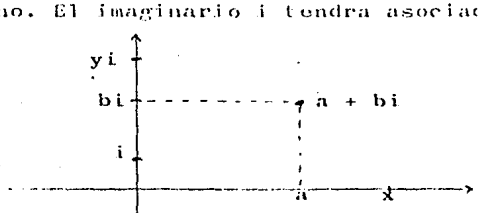
18) $\overline{z\,w} = \overline{z}\ \overline{w}$

19) $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$ para $w \neq 0$

20) $z + \overline{z} = 2\,\mathrm{Re}(z)$.

REPRESENTACION GEOMETRICA DE LOS NUMEROS COMPLEJOS

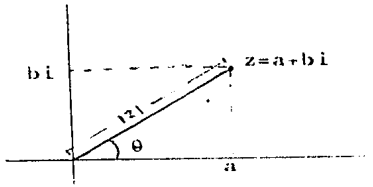
Basándose en el hecho de que cada número complejo a + bi está completamente determinado por dos reales a y b, la representación geométrica consiste en asociarle a cada número de estos la pareja ordenada (a,b) la cual tiene asociado un punto en el plano. El imaginario i tendra asociada la pareja (0,1) -



Los puntos sobre el eje de las abcisas, que llamaremos -- eje real, corresponde a los números reales que son de la forma x + 0i ; y los puntos sobre el eje de las ordenadas, que llamaremos eje imaginario, correponde a los números imaginarios - que son de la forma 0 + yi

FORMA POLAR DE UN COMPLEJO

Observemos que el número complejo z = a + bi



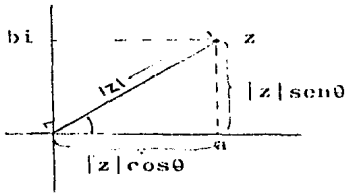
puede determinarse por la distancia que hay del origen al punto (a,b) y el angulo θ que va del eje real positivo al segmento que une el origen con (a,b) . A la distancia del origen al complejo z le llamaremos magnitud de z o módulo de z y al ángulo θ le llamaremos argumento de z. Antes de determinar la forma del complejo a + bi en términos de su módulo y argumento escribamos bien estas definiciones.

DEFINICION 4. Llamamos módulo de un complejo z = a + bi y lo denotaremos por |z|, al número real positivo $|z| = a^2 + b^2$

DEFINICION 5. Al ángulo θ determinado por la parte positiva del eje real y un complejo $z \neq 0$ le llamaremos argumento de z y lo denotaremos como Arg(z) = θ

OBSERVACION: El argumento de cualquier número complejo puede tomar una infinidad de valores ya que Arg z = θ + 2kπ , para cualquier k entero. El argumento de cualquier real mayor que cero es -- cero. El argumento del complejo cero no está definido.

Ahora si, escribamos al complejo z = a + bi en términos de su módulo y su argumento



Si z = a + bi

tenemos que $\cos\theta = \frac{a}{|z|}$ donde $\theta = Arg(z)$

y $\operatorname{sen}\theta = \frac{b}{|z|}$

De donde

$a = |z| \cos\theta$

y $b = |z| \operatorname{sen}\theta$

obteniedo que

$z = a + bi \quad |z| \cos\theta + |z| \operatorname{sen}\theta\, i$

es decir

$z = |z| (\cos\theta + i \operatorname{sen}\theta)$

Esta expresión se conoce como forma polar del complejo z

Dado que el argumento de un complejo puede tomar una infinidad de valores, la forma polar no es única.

Esta forma polar de los complejos nos va a servir mucho para calcular potencias y sacar raíces de números complejos.

EJEMPLOS Encontrar la forma polar de:

a) $z = -4$

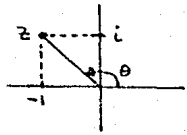
$|z| = 4 \quad Arg(z) = 180° = \pi$

$z = 4(\cos\pi + i \operatorname{sen}\pi)$

b) $z = -1 + i$

$|z| = \sqrt{1+1} = \sqrt{2} \qquad Arg(z) = \frac{3\pi}{4}$

$z = \sqrt{2}\left(\cos\frac{3\pi}{4} + i \operatorname{sen}\frac{3\pi}{4}\right)$



En general va a ser necesario usar tablas trigonométricas para calcular la forma polar de los números complejos y siempre es más ventajoso determinar el ángulo por su tangente. Así si $z = a + bi$ es tal que $\frac{b}{a} > 0$ determinar el ángulo agudo w por su tangente

$$\tan w = \frac{b}{a}$$

y tomar $\theta = w$ si $a > 0$

y $\theta = w - \pi$ si $a < 0$.

En el caso en que $\frac{b}{a} < 0$ entonces el ángulo agudo w está determinado por

$$\tan w = -\frac{b}{a}$$

y $\theta = -w$ si $a > 0$

y $\theta = \pi - w$ si $a < 0$

EJERCICIOS

Encontrar la forma polar de los siguientes números complejos:

1) $-6i$

2) i

3) $\frac{1}{2} - i\sqrt{\frac{3}{2}}$

4) $-\frac{1}{2} + i\sqrt{\frac{3}{2}}$

5) $\sqrt{3} - i$

6) $1 - \sqrt{3} - i(1 + \sqrt{3})$

7) $-4 - 3i$

8) $-2 + i$

9) Demuestre que $z \cdot \overline{z} = |z|^2$ donde z es un complejo

10) Demuestre que $|\overline{z}| = |z|$ donde z es un complejo.

11) Probar que si z y w son complejos entonces $|z + w| \leq |z| + |w|$

MULTIPLICACION Y DIVISION DE NUMEROS COMPLEJOS EN SU FORMA POLAR. FORMULA DE DE MOIVRE.

Sea $z = a + bi$ y $w = c + di$

supongamos que la forma polar de estos complejos es

$$z = r(\cos\theta + i \operatorname{sen}\theta) \quad y \quad w = r'(\cos\theta' + i \operatorname{sen}\theta')$$

multiplicando y reagrupando factores tenemos

$$z\,w = r\,r'(\cos\theta + i \operatorname{sen}\theta)(\cos\theta' + i \operatorname{sen}\theta')$$

$$= r\,r'[(\cos\theta\cos\theta' - \operatorname{sen}\theta \operatorname{sen}\theta') + i(\operatorname{sen}\theta\cos\theta' + \operatorname{sen}\theta'\cos\theta)]$$

pero sabemos que

$$\cos\theta\cos\theta' - \operatorname{sen}\theta\operatorname{sen}\theta' = \cos(\theta+\theta')$$
$$\operatorname{sen}\theta\cos\theta + \operatorname{sen}\theta'\cos\theta = \operatorname{sen}(\theta+\theta')$$

por tanto

$$zw = rr'\left[\cos(\theta+\theta') + i\operatorname{sen}(\theta+\theta')\right]$$

es decir, el módulo del producto es el producto de los módulos de los factores y el argumento es la suma de sus argumentos.

Podemos repetir esta regla para cualquier número de factores.

Así el producto de n factores

$$\cos\theta_1 + i\operatorname{sen}\theta_1\ ,\ \cos\theta_2 + \operatorname{sen}\theta_2,\ldots,\cos\theta_n + i\operatorname{sen}\theta_n$$

cuyo módulo de cada uno es 1 es

$$(\cos\theta_1 + i\operatorname{sen}\theta_1)(\cos\theta_2 + i\operatorname{sen}\theta_2)\ldots(\cos\theta_n + i\operatorname{sen}\theta_n) =$$
$$= \cos(\theta_1+\theta_2+\ldots+\theta_n) + i\operatorname{sen}(\theta_1+\theta_2+\ldots+\theta_n)$$

en particular cuando $\theta_1 = \theta_2 = \ldots = \theta_n = \theta$

esta fórmula da la identidad

$$(\cos\theta + i\operatorname{sen}\theta)^n = \cos n\theta + i\operatorname{sen} n\theta$$

conocida como la fórmula de De Moivre. Por supuesto aquí n es un entero positivo.

notemos que

$$(\cos\theta + i\operatorname{sen}\theta)^{-1} = \frac{1}{\cos\theta + i\operatorname{sen}\theta} = \frac{\cos\theta - i\operatorname{sen}\theta}{\cos^2\theta + \operatorname{sen}^2\theta} =$$
$$= \cos\theta - i\operatorname{sen}\theta = \cos(-\theta)+i\operatorname{sen}(-\theta).$$

De modo que

$$(\cos\theta + i\operatorname{sen}\theta)^{-n} = \cos(-n\theta) + i\operatorname{sen}(-n\theta)$$

que es la fórmula de De Moivre para exponentes enteros negativos.

Si z y w son complejos y su forma polar es

$$z = r(\cos\theta + i\operatorname{sen}\theta)\ ,\ w = r'(\cos\theta' + i\operatorname{sen}\theta')$$

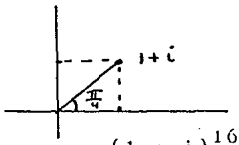
su cociente lo podemos representar como

$$\frac{z}{w} = \frac{r(\cos\theta + i\operatorname{sen}\theta)}{r'(\cos\theta' + \operatorname{sen}\theta')} = (r\cos\theta + i\operatorname{sen}\theta)(r'\cos\theta' + i\operatorname{sen}\theta')$$
$$= r(\cos\theta + i\operatorname{sen}\theta)\frac{1}{r'}(\cos(-\theta) + i\operatorname{sen}(-\theta'))$$
$$= \frac{r}{r'}(\cos(\theta-\theta') + i\operatorname{sen}(\theta-\theta'))$$

de donde el módulo del cociente es igual al cociente de los módulos y el argumento es la diferencia de argumentos del dividendo y divisor.

EJEMPLOS

1. Calcular $(1 + i)^{16}$



$$1 + i = \sqrt{2}\left(\cos\frac{\pi}{4} + i \operatorname{sen}\frac{\pi}{4}\right)$$

$$(1 + i)^{16} = \sqrt{2}^{16}\left(\cos\frac{\pi}{4} + i \operatorname{sen}\frac{\pi}{4}\right)^{16}$$

$$= \sqrt{2}^{16}\left(\cos 16\frac{\pi}{4} + i \operatorname{sen} 16\frac{\pi}{4}\right)$$

$$= \sqrt{2}^{16}(\cos 4\pi + i \operatorname{sen} 4\pi)$$

$$= 256 .$$

2. Calcular i^{12}

$$i^{12} = \left(\cos\frac{\pi}{2} + i \operatorname{sen}\frac{\pi}{2}\right)^{12}$$

$$= \cos 6\pi + i \operatorname{sen} 6\pi$$

$$= 1$$

RAICES N-ESIMAS DE UN COMPLEJO

Las raices n-ésimas de un complejo z son las soluciones de la ecuación

$$w^n = z$$

para encontrarlas escribamos a z y w en su forma polar

$$z = r(\cos\theta + i \operatorname{sen}\theta)$$

$$w = R(\cos\Theta + i \operatorname{sen}\Theta)$$

(recordemos que R y Θ son desconocidas)

entonces

$$w^n = R^n(\cos n\Theta + i \operatorname{sen} n\Theta) = r(\cos\theta + i \operatorname{sen}\theta)$$

Dado que números complejos iguales tienen igual módulo, tenemos que

$$R^n = r$$

donde R está determinada sin ambigüedad como

$$R = \sqrt[n]{r}$$

por otra parte, argumentos de números complejos iguales pueden diferir solo por múltiplos de 2

teniendo así que

$$n\Theta = \theta + 2k \quad , \quad \Theta = \frac{\theta + 2k}{n}$$

donde k es un entero.

Obteniendo la expresión para las raíces w

$$w = \sqrt[n]{r}\left(\cos\ \frac{\theta + 2k\pi}{n} + i\ \text{sen}\ \frac{\theta + 2k\pi}{n}\right)$$

donde k es un entero, pero el número de raíces distintas es solamente n. Para obtener todas las raíces distintas es suficiente con tomar en la fórmula k = 0,1,2, ...,n-1 ya que si k es un entero arbitrario, por el algoritmo de la división tenemos que

$$k = nq + r \qquad 0 \leq r < n$$

entonces

$$\text{Arg } w_k = \frac{\theta}{n} + \frac{2k\pi}{n}$$

$$= \frac{\theta}{n} + \frac{2(nq + r)\pi}{n}$$

$$= \frac{\theta}{n} + \frac{2\pi r}{n} + 2\pi k$$

$$= \text{Arg } w_r + 2\pi q$$

lo cual implica que $w_k = w_r$ para algún valor de r entre 0 y n-1 inclusive. Ahora demostraremos que si $w_s = w_t$ donde $0 \leq s, t < n-1$, necesariamente $s=t$

Tomemos dos valores enteros tales que

$$0 \leq s, t < n$$

y supongamos que $w_s = w_t$ Entonces

$\text{Arg } w_s = \text{Arg } w_t = 2m\pi$ para alguna m entera, esto es

$$\frac{\theta}{n} + \frac{2s\pi}{n} = \frac{\theta}{n} + \frac{2t\pi}{n} + 2m\pi$$

lo cual implica que

$$s - t = nm \text{ para algún valor entero } m$$

pero esto quiere decir que s-t es múltiplo de n o m = 0. Pero como $0 \leq s,t < n$, entonces $|s-t| < n$ entonces s-t no puede ser múltiplo de n, por lo tanto m = 0 de donde s = t.

Resumiendo el resultado tenemos.

Todo número complejo $z \neq 0$ tiene exactamente n raíces n-ésimas distintas y vienen dadas por la siguiente expresión.

$$w_k = \sqrt[n]{|z|}\left[\cos\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right) + i\ \text{sen}\left(\frac{\theta}{n} + \frac{2k\pi}{n}\right)\right]$$

para $k = 0,1,\ldots,n-1$ y donde $\text{Arg } z = \theta$

EJEMPLOS

1 Resolver la ecuación

$$x^4 = -4$$

dado que

$$-4 = 4(\cos\pi + i \operatorname{sen}\pi)$$

la fórmula de la raíz es

$$x = \sqrt[4]{4}\left(\cos\left(\frac{\pi}{4} + \frac{2k\pi}{4}\right) + i \operatorname{sen}\left(\frac{\pi}{4} + \frac{2k\pi}{4}\right)\right)$$

tomando k = 0, 1, 2, 3 encontramos que las cuatro raíces son

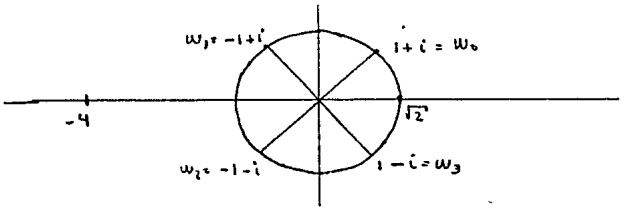
$$W_0 = \sqrt{2}\left(\cos\frac{\pi}{4} + i \operatorname{sen}\frac{\pi}{4}\right) = 1 + i$$

$$W_1 = \sqrt{2}\left(\cos\frac{3\pi}{4} + i \operatorname{sen}\frac{3\pi}{4}\right) = -1 + i$$

$$W_2 = \sqrt{2}\left(\cos\frac{5\pi}{4} + i \operatorname{sen}\frac{5\pi}{4}\right) = -1 - i$$

$$W_3 = \sqrt{2}\left(\cos\frac{7\pi}{4} + i \operatorname{sen}\frac{7\pi}{4}\right) = 1 - i$$

geométricamente las raíces quedan



2 Resolver la ecuación

$$x^3 = -8\,i$$

la forma polar de

$$-8i = 8\left[\cos\left(\frac{-\pi}{2}\right) + i \operatorname{sen}\left(-\frac{\pi}{2}\right)\right]$$

de donde

$$x = 2\left[\cos\left(-\frac{\pi}{6} + \frac{2k\pi}{3}\right) + i \operatorname{sen}\left(-\frac{\pi}{6} + \frac{2k\pi}{3}\right)\right]$$

$$= 2\left[\cos\frac{(4k-1)\pi}{6} + i \operatorname{sen}\frac{(4k-1)\pi}{6}\right]$$

tomando k = 0, 1, 2 tenemos raíces

$$W_0 = 2\left(\cos\frac{\pi}{6} - i \operatorname{sen}\frac{\pi}{6}\right) = \sqrt{3} - i$$

$$W_1 = 2\left(\cos\frac{\pi}{2} + i \operatorname{sen}\frac{\pi}{2}\right) = 2i$$

$$W_2 = 2\left(\cos\frac{7\pi}{6} + i \operatorname{sen}\frac{7\pi}{6}\right) = -\sqrt{3} - i$$

EJEMPLOS

Resolver las siguientes ecuaciones.

1. $x^2-(4-i)x+(5-5i)=0$

$$x = \frac{(4-i) \quad (4-i)^2-4(5-5i)}{2} = \frac{(4-i) \quad -5+12i}{2}$$

como $-5+12i = (2+3i)$ entonces

$$x = \frac{(4-i) \quad (2+3i)}{2}$$

por lo tanto $x_1 = 3+i \quad x_2 = 1-2i$

2. $x^3-9x^2+36x-80=0 \qquad (a)$

haciendo la sustitución $x=y+3$

$(y+3)^3-9(y+3)^2+36(y+3)-80=0$

$y^3+9y^2+27y+27-9y^2-54y-81+36y+108-80=0$

de donde obtenemos la ecuación equivalente

$y^3+9y-26=0 \qquad (b)$

Aplicamos la fórmula de Cardano

$y= \sqrt[3]{13+\sqrt{169+27}} + \sqrt[3]{13-\sqrt{169+27}}$

$y= \sqrt[3]{13+14} + \sqrt[3]{13-14}$

$y = \sqrt[3]{27} + \sqrt[3]{-1}$

Calculamos las raíces cúbicas de 27 y de -1

Una de las raíces de 27 es 3, entonces 3ρ y $3\rho^2$ son las otras dos raíces donde

$\rho = -\frac{1}{2}+\frac{\sqrt{3}}{2}i$ y por tanto $\rho^2 = -\frac{1}{2}-\frac{\sqrt{3}}{2}i$

Así las raíces de 27 son

$u_0 = 3 \quad ; \quad u_1 = 3(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) \quad ; \quad u_2 = 3(-\frac{1}{2} - \frac{\sqrt{3}}{2}i)$

y las del -1 son

$v_0 = -1 \quad ; \quad v_1 = \frac{1}{2} - \frac{\sqrt{3}}{2}i \quad ; \quad v_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$

Recordemos que para encontrar la solución $y=u+v$ u y v deben satisfacer la igualdad $uv = -\frac{p}{3}$ es decir $uv = -3$

Las soluciones que satisfacen la condición son las parejas u_0 y v_0 ; u_1 y v_2 ; u_2 y v_1.
De modo que las soluciones de (b) son
$y_1 = 2$; $y_2 = -1 + 2\sqrt{3}i$; $y_3 = -1 - 2\sqrt{3}i$
haciendo la sustitución $x = y+3$
Obtenemos las soluciones de (a) que era lo que buscábamos
$x_1 = 5$; $x_2 = 2 + 2\sqrt{3}i$; $x_3 = 2 - 2\sqrt{3}i$

3. $x^3-18x-30=0$

La fórmula de Cardano da $x = \sqrt[3]{18} + \sqrt[3]{12}$
Tomando las raíces reales verificamos que $uv=(-p/3)$, es decir, $uv=6$. Por lo tanto las raíces de la ecuación son:
$x_1 = \sqrt[3]{18} + \sqrt[3]{12}$; $x_2 = \rho\sqrt[3]{18} + \rho^2\sqrt[3]{12}$; $x_3 = \rho^2\sqrt[3]{18} + \rho\sqrt[3]{12}$

EJERCICIOS

Resuelva las siguientes ecuaciones

1. $x^3-9x-12=0$
2. $x^3-18x+30=0$
3. $x^4-4x^2-8x-4=0$
4. $x^4-4x^3-5x^2+12x+6=0$

TEOREMA FUNDAMENTAL DEL ALGEBRA

Las fórmulas para las ecuaciones de tercero y cuarto grado, como lo muestran los ejemplos anteriores son de poco valor práctico. incluso el hecho de que no exitan fíomulas para resolver las ecuaciones de n-ésimo grado cuando $n \geq 5$ no provoca dificultades serias en lo que respecta a la búsqueda práctica de las raíces de las ecuaciones. Esto se compensa totalmente por otros métodos que se han desarrollado para la resolución de las ecuaciones y que incluso en el caso de las ecuaciones de tercero y cuarto grado conducen al objetivo con mayor rapidez que utilizando las fórmulas. Más adelante estudiaremos esto.

No obstante que tienen poco valor práctico, la existencia de fórmulas para las ecuaciones de segundo, tercero y cuarto grado, permitió demostrar que estas ecuaciones poseen a lo más, respectivamente, dos, tres y cuatro raíces distintas.

Ahora bien, cómo estarán las cosas respecto a la existencia de raíces para las ecuaciones de n-ésimo grado para n arbitrario?

Para las ecuaciones de grado mayor que cuatro no existe una fórmula (una solución por radicales) que exhiba al menos una solución; esto lleva, y llevó a los matemáticos del renacimiento, a preguntarse si existen siquiera esas soluciones. La respuesta a esta pregunta se encuentra en el Teorema Fundamental del Algebra que nos garantiza la existencia de al menos una raíz en cualquier ecuación.

Antes de enunciar este terorema conviene trabajar el primer miembro de la ecuación como una función.

Dada la ecuación

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \qquad (1)$$

donde a_1, a_2, $\ldots$, a_{n-1}, a_n son números reales o complejos, podemos considerar el primer miembro de la ecuación como función de la variable x, es decir, considerar la ecuación (1) como

$$f(x) = 0$$

donde $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$

Esta función también es llamada polinomio en x de grado n.

TEOREMA FUNDAMENTAL DEL ALGEBRA.

Cualquier polinomio

$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ de grado n 0 cuyos coeficientes a_1, a_2, ..., a_{n-1}, a_n son números reales o complejosdados, tiene al menos una raíz real o compleja.

Este teorema es uno de los más importantes de toda la matemática. Fué demostrado en el siglo XVIII por D'Alembert y Gauss; en sus demostraciones utilizaron resultados que estaban intimamente relacionados con el análisis, las demostraciones de dichos resultados se dan hasta la segunda mitad del siglo XIX.

La demostración delTeorema Fundamental del Algebra no es sencilla y requiere deciertos elementos y resultados que todavía no son familiares a los estudiantes del nivel correspondiente a losprimeros semestres. Por esta razón nodaremos aquí su demostración.

Partiendo de que tenemos garantizada la existencia de al menos una raíz en una ecuación de grado n, la pregunta que se ocurre inmediatamente es ¿cuál será el número máximo de raíces? El siguiente teorema nos ayudará a resolver la pregunta.

TEOREMA DEL FACTOR. Sea

$f(x) = x^n + a_1x^{n-1} + \ldots + a_1x + a_n$ un polinomio de grado n, cuyos coeficientes a_1, a_2, ..., a_{n-1}, a_n son reales o complejos.

es raíz de f(x) si y sólo si $f(x) = g(x)(x -)$ donde g(x) es un polinomio de grado n-1.

DEM:

Supongamos que α es raíz de f(x). Dividiendo* f(x) entre $(x - \alpha)$ obtenemos

$$f(x) = (x - \alpha)g(x) + r(x) \qquad (2)$$

como el grado de r(x) es menor que el grado del polinomio divisor, podemos reescribir (2) como:

$$f(x) = (x - \alpha)g(x) + r \qquad (3)$$

el grado de g(x) es entonces (n - 1)

sustituyendo $x = \alpha$ en (3) tenemos que

$$f(\alpha) = (\alpha - \alpha)g(\alpha) + r$$

es decir

$$f(\alpha) = r$$

por otro lado

$$f(\alpha) = 0 \quad \text{por ser } \alpha \text{ raíz de } f(x)$$

de donde $r = 0$

y por tanto

$$f(x) = (x - \alpha)g(x)$$

Ahora supongamos que

$$f(x) = (x - \alpha)g(x)$$

sustituyendo $x = \alpha$ obtenemos

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0$$

por lo tanto α es raíz de f(x) quedando así demostrado el teorema.

Apliquemos este resultado para saber cuántas raíces puede tener un polinomio de grado n.

Si f(x) es un polinomio de grado n sabemos que f(x) tiene al menos una raíz (real o compleja), llamémosle α_1, entonces porel teorema del factor

$$f(x) = (x - \alpha_1)f_1(x) \qquad (4)$$

donde el grado de $f_1(x)$ es n-1

pero $f_1(x)$ tiene al menos una raíz α_2, entonces

$$f_1(x) = (x - \alpha_2)f_2(x) \qquad (5)$$

donde el grado de $f_2(x)$ es n-2.

*Recuérdese que el proceso usual para la división de polinomios es igual que el de la división de números.

sustituyendo (5) en (4) obtenemos

$$f(x) = (x - \alpha_1)(x - \alpha_2)f_2(x)$$

repitiendo el mismo argumento llegamos a que

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \qquad (6)$$

donde las raíces $\alpha_1, \alpha_2 \ldots\ldots, \alpha_n$ pueden ser todas distintas entre sí o puede suceder que algunas de ellas sean iguales.

Establezcamos este resultado como un teorema.

TEOREMA 1. Si $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ es un polinomio de grado $n > 0$, donde los coeficientes son números reales o complejos entonces $f(x)$ tiene a lo más n raíces reales o complejas distintas.

La demostración es directa a partir del teorema del factor y ha quedado ya esbozada. Queda como ejercicio el formalizarla.

Hemos mencionado que puedesuceder que en la factorización (6) de $f(x)$ algunas de las 's sean iguales, daremos una definición respecto a esto.

DEFINICION. Si en la factorización de

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$$

m raíces son iguales con $1 < m \leq n$, es decir, sin pérdida de generalidad, si $\alpha_1 = \alpha_2 = \ldots = \alpha_m = \alpha$ se dice que la raíz α es de multiplicidad m.

Nótese que si α es de multiplicidad m, $f(x)$ puede escribirse como

$$f(x) = (x - \alpha)^m (x - \alpha_{m+1}) \ldots (x - \alpha_n)$$

A las raícesque no se repiten en la factorización se les llama raíces simples.

Ejemplo 1

El polinomio $f(x) = x^3$ lo podemos factorizar como

$$f(x) = x^3 = (x - 0)(x - 0)(x - 0)$$

observamos que tiene tres raíces iguales, dicho en otros términos, tiene una raíz $\alpha = 0$ de multiplicidad 3.

Ejemplo 2

En el polinomio $f(x) = x^7 + 2x^6 + 3x^5 + 2x^4 + x^3$ cuya factorización es

$$f(x) = x^3[x - (-\tfrac{1}{2} + \tfrac{3}{2}i)]^2[x - (-\tfrac{1}{2} + \tfrac{3}{2}i)]^2$$

$\alpha_1 = 0$ es una raíz de multiplicidad 3, también llamada triple $\alpha_2 = -\frac{1}{2} + \frac{3}{2}i$, $\alpha_3 = -\frac{1}{2} - \frac{3}{2}i$, son raíces de multiplicidad 2, también llamadas raíces dobles.

Si bien el teorema del factor nos ha servido para establecer que una ecuación de grado n tiene alo más n raíces distintas, vamos a ver que también es muy útil para facilitar la búsqueda práctica de raícesde un polinomio. Ilustraremos esto con algunos ejemplos.

Ejemplo 3.

Sea $f(x) = x^4 - 5x^2 - 10x - 6$. Encontrar todas las raíces de f(x).

Por inspección encontramos que -1 es raíz de f(x); entonces

$x - (-1)$ es factor de f(x)

haciendo ladivisión de f(x) entre x + 1

$$\begin{array}{r|l} & x^3 - x^2 - 4x - 6 \\ \hline x + 1 & x^4 - 5x^2 - 10x - 6 \\ -(x^4 + x^3) & \\ \hline & -x^3 - 5x^2 \\ & -(-x^3 - x^2) \\ \hline & -4x^2 - 10x \\ & -(-4x^2 - 4x) \\ \hline & -6x - 6 \\ & -(-6x - 6) \\ \hline & 0 \end{array}$$

obtenemos que

$$f(x) = (x + 1)(x^3 - x^2 - 4x - 6)$$

Nuevamente por inspección encontramos que 3 es raíz de

$x^3 - x^2 - 4x - 6 = g(x)$

dividiendo g(x) entre x - 3

$$
\begin{array}{r|l}
x - 3 & x^2 + 2x + 2 \\
\hline
 & x^3 - x^2 - 4x - 6 \\
 & -x^3 + 3x^2 \\
 & \hline
 & 2x^2 - 4x \\
 & -2x^2 + 6x \\
 & \hline
 & 2x - 6 \\
 & -2x + 6 \\
 & \hline
 & 0
\end{array}
$$

obtenemos que

$$g(x) = (x - 3)(x^2 + 2x + 2)$$

de donde

$$f(x) = (x + 1)(x - 3)(x^2 + 2x + 2)$$

Ahora resolviendo laecuación de segundo grado encontramos que

$$x_1 = \frac{-2 + \sqrt{4 - 8}}{2} = \frac{-2 + \sqrt{-4}}{2} = -1 + i$$

$$x_2 = \frac{-2 + \sqrt{-4}}{2} = -1 - i$$

son las otras dos raíces de f(x).

Podemos escribir la factorización completa de f(x)

$$f(x) = (x + 1)(x - 3)(x - (-1 + i)(x -(-1 - i))$$

$$f(x) = (x + 1)(x - 3)(x +1 - i)(x + 1 + i)$$

Para notar que esto facilita el encontrar las raíces de un polinomio, intente encontrarlas con la fórmula para la ecuación de cuarto grado.

Ejemplo 4

Sea $f(x) = x^3 - 19x + 30$. Encontrar las raíces de f(x).

Es fácil encontrar que $\alpha_1 = 2$ es raíz de f(x). Al dividir entre x - 2

$$
\begin{array}{r|l}
x - 2 & x^2 + 2x - 15 \\
\hline
 & x^3 - 19x + 30 \\
 & -x^3 + 2x^2 \\
 & \hline
 & 2x^2 - 19x \\
 & -2x^2 + 4x \\
 & \hline
 & -15x + 30 \\
 & -15x + 30 \\
 & \hline
 & 0
\end{array}
$$

obtenemos que

$$f(x) = (x - 2)(x^2 + 2x - 15)$$

pero $x^2 + 2x - 15$ es fácil defactorizar

$$x^2 + 2x - 15 = (x - 3)(x + 5)$$

de donde obtenemos las otras dos raíces de f(x) que son $_2 = 3$ y $_3 = -5$.

La factorización completa de f(x) es

$$f(x) = (x - 2)(x - 3)(x + 5)$$

En los dos últimos ejemplos el procedimiento ha sido encontrar una raíz del polinomio f(x) en cuestión y hacer la correspondiente factorización de f(x). A continuación damos un método que simplifica la división de f(x) entre $x - \alpha$ y un resultado que va a servir para guiar la búsqueda por inspección de raíces de un polinomio.

DIVISION SINTETICA

La división sintética es un método que hace más sencillo el problema de encontrar el cociente y el residuo de la división de dos polinomios f(x) y g(x) con

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \quad \text{con } a_0 \neq 0$$

y $a_0, a_1, \ldots, a_n$ números reales o complejos

y $$g(x) = (x - \alpha)$$

Encontrar este cociente y residuo se reduce a encontrar $f_1(x)$ y r tal que

$$f(x) = (x - \alpha)f_1(x) + r \qquad (1)$$

donde el grado de $f_1(x)$ es n - 1

Para encontrar $f_1(x)$ y r en función de f(x) y α supongamos que

$$f_1(x) = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}$$

sustituyendo esta expresión en (1) obtenemos

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n =$$

$$= (x - \alpha)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-2}x + b_{n-1}) + r$$

$$= b_0x^n - \alpha b_0x^{n-1} + b_1x^{n-1} - \alpha b_1x^{n-2} + \ldots + b_{n-2}x^2 - \alpha b_{n-2}x +$$

$$+ b_{n-1}x - \alpha b_{n-1} + r$$

$$= b_0x^n + (b_1 - \alpha b_0)x^{n-1} + (b_2 - \alpha b_1)x^{n-2} + \ldots$$
$$\ldots + (b_{n-1} - \alpha b_{n-2})x + r - \alpha b_{n-1}$$

y como dos polinomios son iguales si sus coeficientes respectivos son los mismos, tenemos que:

$a_0 = b_0$; $a_1 = b_1 - b_0$; $a_2 = b_2 - b_1$; ...

$$\ldots; \ a_{n-1} = b_{n-1} - b_{n-2}; \ a_n = r - b_{n-1}$$

o sea

$b_0 = a_0$; $b_1 = a_1 + \alpha b_0$; $b_2 = a_2 + \alpha b_1$; ...

$$\ldots; \ b_{n-1} = a_{n-1} + \alpha b_{n-2} \text{ y } r = a_n + \alpha b_{n-1}$$

estas relaciones las podemos poner en una sola así:

a_0	a_1	a_2	...	a_{n-1}	a_n
	αb_0	αb_1	...	αb_{n-2}	αb_{n-1}
b_0	b_1	b_2	...	b_{n-1}	r

Por lo tanto para calcular el polinomio cociente $f_1(x)$ y el residuo r, sólo necesitamos calcular las b_i que vienen dadas por la fórmula de recurrencia

$$b_i = a_i + \alpha b_{i-1} \quad \text{donde } b_0 = a_0$$

y siendo $r = a_n + \alpha b_{n-1}$

obteniendo así el método llamado División Sintética.

Ilustramos el método con un ejemplo.

Ejemplo 5

Dividir $f(x) = x^2 - 6x + 5$ entre $x-3$

los coeficientes del polinomio f(x) se escriben en un renglón

1	-6	5	

al final de los coeficientes en una , se acostumbra escribir el número que integra el divisor con signo contrario

1	-6	5	3

dejando un renglón de espacio se traza una línea y se baja el primer coeficiente, luego se multiplica por 3 y

el resultado se coloca debajo del segundo coeficiente y se suman

el resultado de esta suma se multiplica por tres y se coloca debajo del siguiente coeficiente y se suman

esta última suma da el residuo de la división y los números anteriores son los coeficientes del cociente, cuyo grado será menor en uno que el grado del dividendo

1	-6	5	3
	3		
1	-3		

1	-6	5	3
	3	-9	
1	-3	-4	

cociente: $x - 3$
residuo: -4

TEOREMA 2. Si $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ es un polinomio de grado n, con coeficientes enteros y es una raíz entera de f(x) entonces $\alpha | a_n$

DEM:

Sea $x = \alpha$ entonces

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$$

de donde $a_n = -a_0\alpha^n - a_1\alpha^{n-1} - \ldots - a_{n-1}\alpha$

factorizando α tenemos que

$$a_n = \alpha(-a_0^{\,n} - a_1^{\,n-1} - \ldots - a_{n-1})$$

y por tanto $\alpha | a_n$

Ejemplo 6

Factorizar el polinomio $f(x) = x^3 - 6x^2 + 11x - 6$

Si f(x) tiene una raíz entera, ésta debe dividir a -6, entonces de tenerla ésta tendría que ser uno de los divisores de -6. Los divisores de -6 son ±1, ±2, ±3, ±6.

$f(2) = 8 - 24 + 22 - 6 = 0$ 2 es raíz de f(x)

$f(1) = 1 - 6 + 11 - 6 = 0$ 1 es raíz de f(x)

$f(3) = 27 - 54 + 33 - 6 = 0$ 3 es raíz de f(x)

por lo tanto la factorización de f(x) es

$$f(x) = x^3 + 11x - 6 = (x - 2)(x - 3)(x - 1)$$

Ejemplo 7

Factorizar el polinomio $f(x) = x^3 + x^2 - 3x + 9$

Los divisores de 9 son ± 1, ± 3 y ± 9

$$f(-3) = -27 + 9 + 9 + 9 = 0$$

así que -3 es raíz. Como ningún otro divisor de 9 satisface $f(x) = 0$ entonces -3 es la <u>única</u> raíz entera de $f(x)$. Es más, como es psible demostrar que toda raíz racional de un polinomio con oceficientes enteros <u>es</u> entera (la demostración se <u>de</u>ja como ejercicio) podemos asegurar que las otras raíces de $f(x)$ son irracionales o bien complejas.

Dividamos $x^3 + x^2 - 3x + 9$ entre $x + 3$

1	1	-3	9	|-3
	-3	6	-9	
1	-2	3	0	

por lo tanto

$$x^3 + x^2 - 3x + 9 = (x + 3)(x^2 - 2x + 3)$$

resolviendo $x^2 - 2x + 3 = 0$ con la fórmula obtenemos las otras dos raíces que son

$x_{1,2} = \frac{2 \pm \sqrt{4 - 12}}{2}$ es decir,

$x_1 = 1 + \sqrt{2}i$ y $x_2 = 1 - \sqrt{2}i$

así $f(x) = (x+ 3)(x - (1 + \sqrt{2}i))(x - (1 - \sqrt{2}i))$

Observemosque las dos últimas raíces que obtuvimos $x_1 = 1 + \sqrt{2}i$ y $x_2 = 1 - \sqrt{2}i$ son números conjugados, es decir, $x_1 = \overline{x_2}$. No es casualidad que siendo x_1 raíz de $f(x)$ su conjugado también lo sea. Este resultado que enunciaremos como teorema puede serútil también para la solución práctica de las ecuaciones algebraicas.

TEOREMA 3. Sea

$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ un polinomio de grado n con coeficientes reales.

Si $\alpha = a + bi \in \mathbb{C}$ es una raíz de $f(x)$ entonces el conjugado de α, $\overline{\alpha} = a - bi$ también es raíz de $f(x)$.

DEM:

Como α es raíz de f(x) se tiene que

$$f(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$$

de donde

$$\overline{a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n} = \overline{0}$$

utilizando las propiedades del conjugado tenemos que

$$\overline{a_0\alpha^n} + \overline{a_1\alpha^{n-1}} + \ldots + \overline{a_{n-1}\alpha} + \overline{a_n} = 0$$

$$\overline{a_0}\,\overline{\alpha^n} + \overline{a_1}\,\overline{\alpha^{n-1}} + \ldots + \overline{a_{n-1}}\,\overline{\alpha} + \overline{a_n} = 0$$

como $a_0, a_1, \ldots, a_n$ son reales

$$a_0\overline{\alpha^n} + a_1\overline{\alpha^{n-1}} + \ldots + a_{n-1}\overline{\alpha} + a_n = 0$$

nuevamente utilizando las propiedades del conjugado tenemos

$$a_0(\bar{\alpha})^n + a_1(\bar{\alpha})^{n-1} + \ldots + a_{n-1}(\bar{\alpha}) + a_n = 0$$

es decir

$$f(\bar{\alpha}) = 0$$

y porlo tanto $\bar{\alpha}$ es raíz de f(x)

Ejemplo 8

El conocimiento de una raíz de f(x) simplifica encontrar las otras. Si nos dicen que 1 + i es raíz de

$$f(x) = x^4 - 4x^3 + 5x^2 - 2x - 2$$

y queremos encontrar todas las raíces de f(x), lo que hacemos es lo siguiente:

Como 1 + i es raíz su conjugado también lo será y

$$f(x) = (x - (1 + i))(x - (1 - i))g(x)$$

para obtener g(x) basta con dividir f(x) entre

$(x - (1 + i))(x - (1 - i)) = x^2 - 2x + 2$

resulta entonces que

$$g(x) = x^2 - 2x - 1$$

así

$$f(x) = (x - (1 + i))(x - (1 - i))(x^2 - 2x - 1)$$

y al resolver la ecuación encontramos las raíces restantes

$$x_{1,2} = \frac{2 \pm \sqrt{8}}{2}, \quad \text{es decir}$$

$$x_1 = 1 + \sqrt{2} \qquad x_2 = 1 - \sqrt{2}$$

la factorización completa de f(x) resulta ser

$$f(x) = (x - (1 + i))(x - (1 - i))(x - 1 - \sqrt{2})(x - 1 + \sqrt{2})$$

Para finalizar esta sección mencionaremos larelación que existe entre las raíces de un polinomio y los coeficientes de éste y la relación entre las derivadas del polinomio y la multiplicidad de sus raíces.

RELACION ENTRE LOS COEFICIENTES DE UN POLINOMIO Y LAS RAICES DE ESTE.

Sea $f(x) = x^3 + a_1x^2 + a_2x + a_3$ un polinomio de tercer grado.

f(x) puede escribirse como

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

donde α_1, α_2, α_3 son las raíces de f(x).

Desarrollando el segundo miembro obtenemos

$$f(x) = x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3$$

por lo tanto

$$-a_1 = \alpha_1 + \alpha_2 + \alpha_3$$
$$a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$$
$$-a_3 = \alpha_1\alpha_2\alpha_3$$

Para polinomios

$$f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$$ obtenemos

$$-a_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$$
$$a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4$$
$$-a_3 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4$$
$$a_4 = \alpha_1\alpha_2\alpha_3\alpha_4$$

donde α_1, α_2, α_3, α_4 son las raíces de f(x).

En general para

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

obtendremos que

$-a_1$ es la suma de las n raíces de f(x)

a_2 es la suma de losproductos de las raíces tomados de dos en dos

$-a_3$ es la suma de los productos de las raíces tomados de tres en tres

$\vdots$

$(-1)^n a_n$ es el producto de las n raíces.

Así pues podemos enunciar el siguiente resultado.

TEOREMA 4. Sea $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ un polinomio de grado n con coeficientes reales o complejos entonces los coeficientes $a_0, a_1, \ldots, a_n$ podemos expresarlos como:

$$-a_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n$$

$$a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_i\alpha_j + \ldots + \alpha_{n-1}\alpha_n$$

$$\vdots$$

$$(-1)^n a_n = \alpha_1\alpha_2 \ldots \alpha_n$$

donde $\alpha_1, \alpha_2, \ldots, \alpha_n$ son las raíces de f(x)

Ejemplo 9

Encontrar las raíces de $f(x) = x^4 + 6x^3 + 12x^2 + 10x + 3$ sabiendo que tiene una raíz de multiplicidad 3.

Como una raíz es de multiplicidad 3, podemos hacer $\alpha_1 = \alpha_2 = \alpha_3$ y por el resultado anterior

$$-6 = \alpha_1 + \alpha_1 + \alpha_1 + \alpha_4 = 3\alpha_1 + \alpha_4$$

$$12 = \alpha_1\alpha_1 + \alpha_1\alpha_1 + \alpha_1\alpha_1 + \alpha_1\alpha_4 + \alpha_1\alpha_1 + \alpha_1\alpha_4 + \alpha_1\alpha_4 =$$

$$= 3\alpha_1^2 + 3\alpha_1\alpha_4$$

$$-10 = \alpha_1\alpha_1\alpha_1 + \alpha_1\alpha_1\alpha_4 + \alpha_1\alpha_1\alpha_4 + \alpha_1\alpha_1\alpha_4 =$$

$$= \alpha_1^3 + 3\alpha_1\alpha_1\alpha_4$$

$$3 = \alpha_1\alpha_1\alpha_1\alpha_4 = \alpha_1^3\alpha_4$$

nos queda el sistema

$$-6 = 3\alpha_1 + \alpha_4$$
$$12 = 3\alpha_1^2 + 3\alpha_1\alpha_4$$
$$-10 = \alpha_1^3 + 3\alpha_1^2\alpha_4$$
$$3 = \alpha_1^3\alpha_4$$

resolviendo obtenemos

$$\alpha_1 = -1 \quad \text{y} \quad \alpha_4 = -3$$

de donde

$$\alpha_1 = -1, \quad \alpha_2 = -1, \quad \alpha_3 = -1 \quad \text{y} \quad \alpha_4 = -3$$

RELACION QUE HAY ENTRE LAS DERIVADAS DE UN POLINOMIO Y LA MULTIPLICIDAD DE SUS RAICES

Sea f(x) un polinomio de grado n y supongamos que tiene una raíz de multiplicidad dos, entonces

$$f(x) = (x - \alpha_i)^2 g(x) \quad \text{donde } g(\alpha_i) \neq 0$$

derivando f(x) obtenemos

$$f'(x) = 2(x - \alpha_i)g(x) + g'(x)(x - \alpha_i)^2$$

evaluando f'(x) en α_i resulta que

$$f'(\alpha_i) = 0$$

es decir, resulta que α_i también es raíz de f'(x).

Derivamos f'(x), es decir, calculamos f''(x)

$$f''(x) = 2g(x) + g'(x)2(x - \alpha_i) + g''(x)(x - \alpha_i) + 2(x - \alpha_i)g'(x)$$

evaluando la segunda derivada en α_i tenemos que

$$f''(\alpha_i) = 2g(\alpha_i) \neq 0$$

es decir, α_i ya no es raíz de f''(x).

Generalizando podemos establecer el siguiente resultado

TEOREMA 5. Sea $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ un polinomio de grado n con coeficientes reales o complejos. α_i es una raíz de f(x) de multiplicidad k si y sólo

si las (k - 1) primeras derivadas son cero y la k-ésima derivada es distinta de cero, evaluadas en α_i.

EJERCICIOS

1. Factorice los siguientes polinomios en factores lineales

   i) $x^3 - 1$

   ii) $x^3 - i$

   iii) $x^4 - x^2 + 1$

   iv) $x^4 + 3x^3 + x^2 - 3x - 2$

   v) $2x^5 - 3x^4 - 2x^3 + 4x^2 - 1$

2. Utilizando el método de división sintética encuentre el cociente y el residuo en la división de

   i) $2x^4-6x^3+7x^2-5x+1$ entre $x+1$

   ii) $-x^4+7x^3-4x^2$ entre $x-3$

3. Este ejercicio nos da un método para escribir un polinomio como suma de potencias de $x-a$, donde aes un complejo.

   Sea $p(x)$ un polinomio de grado n y a un número complejo. Efectuamos las siguientes divisiones

   $$p(x)=(x-a)p_1(x)+b_0$$

   $$p_1(x)=(x-a)p_2(x)+b_1$$

   $$\vdots$$

   $$p_{n-1}(x)=(x-a)p_n(x)+b_{n-1}$$

   i) Demostrar que $p_n(x)$ es de grado cero

   ii) Sea $b_n=p_n(x)$. Demostrar que $p(x)$ se puede escribir como

   $$p(x)=b_0+b_1(x-a)+\ldots+b_n(x-a)^n$$

   iii) Mostrar que

   $$2x^4+3x^3-x^2+x-2=2(x-2)^4+19(x-2)^3+65(x-2)^2+97(x-2)+52$$

   iv) Expresar x^9-1 como la suma de potencias de $x-1$

   Sugerencia: Usese división sintética en iii) y iv)

4. Demostrar que si $p(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ es un polinomio de grado n con coeficientes enteros, entonces toda raíz racional de $p(x)$ es raíz entera.

5. Encuentre el polinomio de menor grado

   i) que se hace cero para $x=-1$, o, 1 y toma el valor 1 para $x=2$

ii) que se hace cero para $x= 0, 2+i, 2-i$ y toma el valor 1 y -1 para $x=-1$ y $x=1$ respectivamente.

6. Escriba un polinomio de menor grado tal que en $x=0$ toma el valor 1 y tiene las siguientes raíces: 1 y -1 como raíces simples; 2 como raíz doble y -3 como una raíz triple.

7. Resuelva

i) $x^3-2(1+i)x^2-(1-2i)x+2(1+2i)=0$ dada la raíz $1+2i$

ii) $x^4-(1+2i)x^3+(-4+i)x^2+(3+6i)x+3-3i=0$ dadas las raíces i y $\sqrt{3}$

8. Resuelve las ecuaciones

i) $20x^3-30x^2+12x-1=0$ sabiendo que $1/2$ es una raíz

ii) $2x^4-x^3-17x^2+15x+9=0$ si $1+\sqrt{2}$ y $1-\sqrt{2}$ son raíces.

9. Sea $f(x)$ un polinomio de grado n. Probar que es raíz doble de $f(x)$ si y solo si es raíz de $f(x)$ y $f'(x)$.

10. ¿Cuándo $f(x)=ax^2+bx+c$ $(a\neq 0)$ tiene una raíz doble? ¿Qué quiere decir geométricamente esa condición?

RAICES REALES

Hasta aquí hemos notado que resolver las ecuaciones por medio de las fórmulas no es nada práctico, excepto para el caso de las ecuaciónes de segundo grado; también hemos visto que hay otros caminos que facilitan en muchos casos la solución de la ecuación.

Otra problemática que desde hace tiempo han trabajado los matemáticos, y que en esta sección nos proponemos abordar, es la relacionada con lo siguiente:

Sin resolver una ecuación dada con coeficientes reales, obtener información sobre si tiene o no raíces reales; en caso afirmativo, cuantas raíces positivas y cuantas negativas tiene.

UN METODO PARA ANALIZAR LA CUBICA

Sea $f(x) = x^3 + px + q$ un polinomio de tercer grado con coeficientes reales.

Sabemos que la función $f(x)$ es continua y está definida para todos los números reales. Además para valores de x muy grandes en valor absoluto, el comportamiento de la función está determinado por el termino x^3, es decir cuando

x tiende a ∞ ; $f(x)$ tiende a ∞ y cuando

x tiende a $-\infty$; $f(x)$ tiende a $-\infty$

Por ser $f(x)$ una función continua, toma todos los valores entre $-\infty$ e ∞

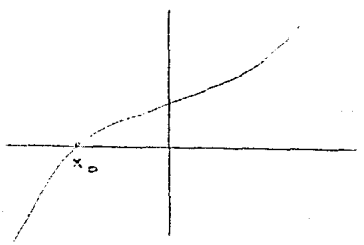
Esto nos asegura que la gráfica de la función corta al eje x en algún punto, es decir, existe al menos un número real x_0 tal que $f(x_0) = 0$.

Dicho número real es solución de la ecuación $f(x) = 0$

Así queda establecido que la ecuación

$$x^3 + px + q = 0$$

siempre tiene al menos una raiz real



Por otro lado sabemos que la ecuación de tercer grado a lo

más tiene tres raíces distintas.

Resuelto lo anterior, el problema consiste en saber bajo qué condiciones sucede que la ecuación $f(x) = 0$ tiene exactamente una raíz, dos raíces o tres raíces reales.

Buscaremos las condiciones para que la cúbica tenga exactamente tres raíces reales.

Los polinomios son funciones que tienen derivadas continuas de todos los órdenes.

Sea $f'(x) = 3x^2 + p$ la derivada de $f(x)$, $f'(x)$ a lo más tiene dos raíces reales distintas.

Una condición necesaria (mas no suficiente fig. 1b) para que la cúbica tenga más de una raíz es que su gráfica sea como la figura 1a,

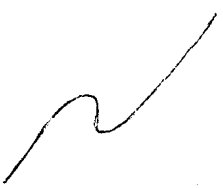


fig. 1a

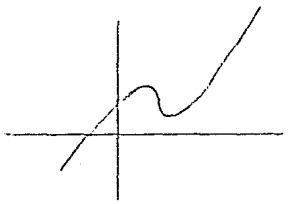


fig. 1b

es decir, la función debe tener un máximo y un mínimo relativo.

En términos de la derivada de $f(x)$ esto quiere decir, que hay dos valores distintos para los cuales $f'(x) = 0$, esto es, la derivada debe tener dos raíces distintas.

Si $f'(x) = 3x^2 + p$.

entonces $3x^2 + p = 0$ implica que $x = \pm\sqrt{-\frac{p}{3}}$

Para que sean dos raíces reales distintas necesariamente $p < 0$. Las raíces son $x_1 = \sqrt{-p/3}$ y $x_2 = -\sqrt{-p/3}$

Evaluando en la segunda derivada

$f''(x) = 6x$

los puntos x_1 y x_2 nos damos cuenta que en x_1 hay un valor mínimo relativo $(f''(x_1) > 0)$ y en x_2 hay un valor máximo relativo $(f''(x_2) < 0)$.

Ahora bien, la cúbica tiene exactamente tres raíces reales si y solo si el valor máximo y el valor mínimo son de dife

rente signo (fig. 2)

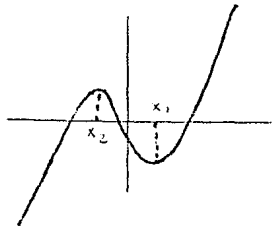


fig. 2

Es decir, sucede si y solo si

$f(\sqrt{-p/3})f(-\sqrt{-p/3}) \quad 0$

Haciendo cálculos tenemos:

$$f(\sqrt{-p/3})f(-\sqrt{-p/3}) = \left[(\sqrt{-p/3})^3+p(\sqrt{-p/3})+q\right]\left[(-\sqrt{-p/3})^3-p(\sqrt{-p/3})+q\right]$$

$$= (p/3)^3 - (2p^3/9) + p^3/3 + q^2$$

$$= (p/3)^3 - (6p^3/27) + (9p^3/27) + q^2$$

$$= (4p^3/27) + q^2$$

$$= 4\left[\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2\right]$$

Así que la ecuación $f(x) = 0$ tiene <u>exactamente</u> <u>tres raíces reales</u> si y solo si

$$\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 < 0$$

De igual manera se puede concluir que la ecuación $f(x) = 0$ tiene exactamente dos raíces reales si y solo si

$$\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = 0$$

(ver fig. 3)

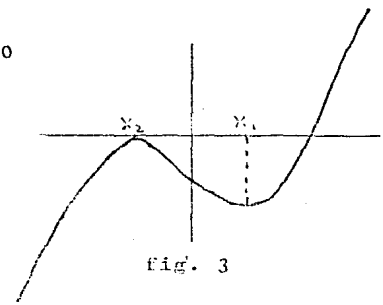


fig. 3

Y tiene exactamente una raíz real si y solo si

$$\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 > 0$$

o bien $p = 0$

(ver fig. 4a y 4b)

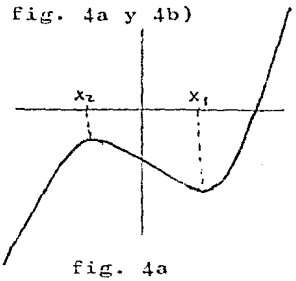


fig. 4a

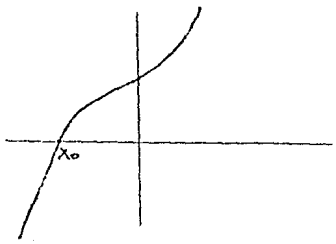


fig. 4b

Observación:

Recordemos que el término $\left[\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right]$ aparece en la fórmula para la ecuación $x^3 + px + q = 0$

$$x \quad x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Cuando en la fórmula aparecen números complejos, la cúbica tiene exactamente tres raíces reales.

EJEMPLOS

1) ¿Cuántas raíces reales tiene la cúbica $x^3 - 3x + \sqrt{2}$?

Como $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = \frac{1}{2} - 1 = -\frac{1}{2} < 0$

la ecuación cúbica tiene exactamente tres raíces reales

2) La ecuación cúbica $x^3 - 9x - 12 = 0$ tiene exactamente una solución real ya que

$$\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = 9 > 0$$

El argumento utilizado en la cúbica para garantizar la existencia de al menos una raíz real, lo podemos generalizar para todo polinomio de grado impar.

Sea

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

un polinomio de grado impar con coeficientes reales.

Para valores muy grandes de x, $f(x)$ y x^n toman "casi" los mismos valores $\left[\lim_{n\to\infty} \frac{f(x)}{x^n} = \lim_{n\to\infty} \left(\frac{x^n}{x^n} + \frac{a_1x^{n-1}}{x^n} + \ldots + \frac{a_n}{x^n}\right) = 1\right]$ lo mismo ocurre para valores muy pequeños de x. Esto es lo mismo que decir que el comportamiento de la función está determinado por el término x^n, de modo que cuando

$x \longrightarrow \infty$, $f(x) \longrightarrow \infty$ y cuando

$x \longrightarrow -\infty$, $f(x) \longrightarrow -\infty$ (recuerde que n es impar).

Como $f(x)$ es una función continua, $f(x)$ toma todos los valores intermedios entre $-\infty$ e ∞, en particular $f(x)$ toma el valor cero, es decir, existe al menos un real α tal que $f(\alpha) = 0$. Cumpliéndose así el siguiente Teorema

TEOREMA 1. Todo polinomio de grado impar con coeficientes reales tiene por lo menos una raíz real.

De manera semejante podemos demostrar el

TEOREMA 2. Si en un polinomio con coeficientes reales, el coeficiente principal a_0 (de x^n) y el término independiente tienen signos diferentes, entonces el polinomio tiene por lo menos una raíz positiva. Si además el polinomio es de grado par, entonces también posee por lo menos una raíz negativa.

DEM:

Sea $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$

un polinomio de grado n con coeficientes reales donde a_0 y a_n tienen signos diferentes.

Tenemos que $f(0) = a_n$ y cuando $x \longrightarrow \infty$, $f(x) \longrightarrow \pm\infty$ según sea el signo de a_0. Sin pérdida de generalidad podemos suponer que $a_0 > 0$ y $a_n < 0$. Entonces tenemos que $f(0) < 0$ y $f(x) \longrightarrow \infty$ cuando $x \longrightarrow \infty$.
Y como $f(x)$ es una función continua, ésta, toma todos los valores entre $f(0)$ e ∞. Por lo tanto existe al menos un α_1 real positivo tal que $f(\alpha_1) = 0$. (Ver fig. 5)

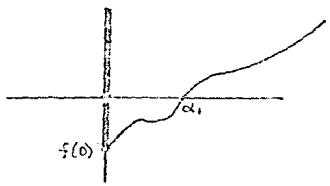


fig. 5

Si además $f(x)$ es de grado par, tenemos que
$f(x) \longrightarrow \infty$ cuando $x \longrightarrow -\infty$
y por tanto, existe un α_2 real negativo tal que
$f(\alpha_2) = 0$ (ver fig. 6)

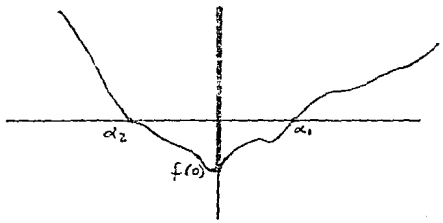


fig. 6

EJEMPLOS

1) La ecuación $x^7 - 8x^3 + x - 2 = 0$
tiene al menos una raíz real.

2) La ecuación $x^6 + 2x^5 - x^2 + 7x - 1 = 0$
tiene al menos una raíz positiva y otra negativa.

EJERCICIOS

1. Sea a, b y c números reales, con $c \neq 0$. Probar que la ecuación $ax^2+bx+c=0$
   i) tiene dos (diferentes) soluciones reales si $b^2 > 4ac$
   ii) tiene una solución real si $b^2=4ac$
   iii) tiene dos soluciones complejas conjugadas si $b^2 < 4ac$

2. i) Demostrar que si $p \geq 0$, la ecuación $x^3+px+q=0$ tiene una única solución real.
   ii) Dar un ejemplo de una ecuación que tenga una única solución y que $p < 0$ ¿Contradice esto al inciso i)?

3. La ecuación $x^3+px+q=0$ con p y q no simultaneamente cero tiene dos soluciones reales si y solo si $(q/2)^2+(p/3)^3=0$. Demostrar que dichas soluciones son $2\sqrt[3]{-q/2}$ y $\sqrt[3]{q/2}$
   Sugerencia: Una de las raíces la da la fórmula de Cardano. La otra se puede obtener recurriendo a la primera derivada de $f(x)=x^3+px+q$

4. Demostrar que $x^3+px+q=0$ tiene una única raíz real si y solo si $(q/2)^2+(p/3)^3 > 0$ o $p=q=0$

5. Una raíz de la cúbica $x^3-(2a+1)x^2+a(a+2)x-a(a+1)=0$ es $a+1$ Encuentre las otras raíces.

6. Escribe una ecuación cúbica con
   i) raíces 0, 1, 2
   ii) raíces 1, 1+i, 1-i

7. Encontrar el polinomio p(x) de grado 3, si sabemos que su gráfica es como en la figura 1. Nota:la gráfica es tangente al eje X en x=1.

8. Pruebe que el polinomio $p(x)=x^4+7x^3-9$ tiene a lo menos dos raíces reales.

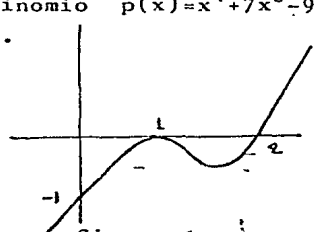


figura 1

9. Pruebe que la ecuación $x^5-5x+m=0$ no puede tener más de una raíz en el intervalo $[-1,1]$

10. Encuentre los valores reales de x los cuales son soluciones de las siguientes ecuaciones.

i) $x^2-4x-20$

ii) $3x^3-10$

iii) $x^2+x+1=0$

APROXIMACION DE RAICES REALES

Sea

$$f(x) = x^3 - 9x - 12$$

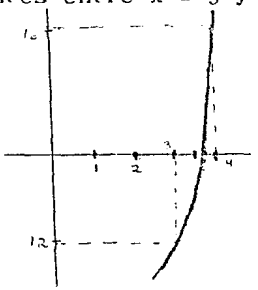
Este polinomio (según los resultados vistos en la sección anterior) tiene al menos una raíz positiva.

Evaluando

$$f(0) = -12;\ f(1) = -20;\ f(2) = -22;\ f(3) = -12,$$

$$f(4) = 16$$

nos damos cuenta que de f(3) a f(4) hay un cambio de signo, entonces entre x = 3 y x = 4 hay una raíz.



Si evaluamos en el punto 3.5 sabremos si la raíz esta en el intervalo $(3,3.5]$ o en $[3.5,4)$

Como f(3.5) = -.625 la raíz está entre 3.5 y 4.

Repitiendo este procedimiento tenemos que como f(3.75) = 6.98... la raíz está entre 3.5 y 3.75, etc.

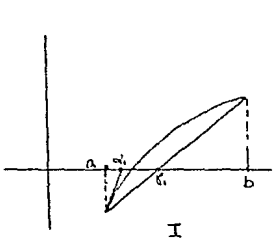
Así nos vamos aproximando (teoricamente), a la raíz tanto como queramos. Pero este camino puede requerir calculos muy voluminosos que se vuelven muy pronto prácticamente irrealizables.

En esto de encontrar las raíces por metodos de aproximación, la idea es encontrar aquellos que permitan calcular más rápidamente los valores aproximados de las raíces reales de las ecuaciones.

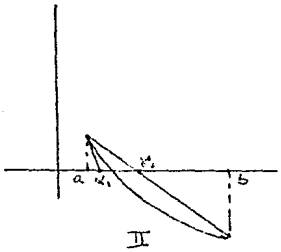
EL METODO DE LA TANGENTE Y EL METODO DE LA CUERDA

Supongamos que entre a y b sólo hay una raíz del polinomio f(x), por lo que f(a) y f(b) tienen signos opuestos, y supongamos que entre a y b la segunda derivada f''(x) es de signo constante.

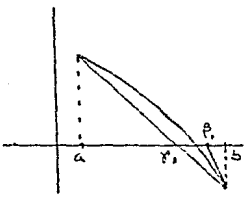
En este caso la gráfica de f(x) entre a y b tiene una de las cuatro formas siguientes:



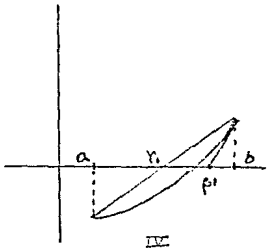
I



II



III



IV

Cuando la figura es como I y II la tangente a la gráfica en el punto a corta al eje x en el punto α_1 que queda situado entre a y la raíz buscada.

Si ahora consideramos la tangente a la gráfica en α_1 obtenemos el punto α_2 situado entre el punto α_1 y la raíz buscada y así sucesivamente. De este modo nos aproximamos a la raíz buscada .

En casos como III y IV debemos empezar por el punto b y obtener demanera análoga los β_1, β_2,... para aproximarnos a la raíz.

Para determinar en que caso se está, hay que ver como son los signos de f(a), f(b) y f''(x) para $a < x < b$.

Como la ecuación de la recta tangente a la curva $y = f(x)$ en el punto a es

$$y - f(a) = f'(a)\ (x - a)$$

la abscisa α_1 del punto de interseccion con el eje x se obtiene al sustituir en la igualdad anterior $x = \alpha_1$, $y = 0$ y despejarla, tenemos entonces

$$0 - f(a) = f'(a)\ (\alpha_1 - a)$$

es decir,

I =

$$\alpha_1 = a - f(a)/f'(a)$$

entonces

$$\alpha_2 = \alpha_1 - f(\alpha_1)/f'(\alpha_1), \quad \alpha_3 = \alpha_2 - f(\alpha_2)/f'(\alpha_2)$$

y así sucesivamente.

Analogamente obtenemos que

$$\beta_1 = b - f(b)/f'(b), \quad \beta_2 = \beta_1 - f(\beta_1)/f'(\beta_1)$$

$$\beta_3 = \beta_2 - f(\beta_2)/f'(\beta_2)$$

y así sucesivamente.

El Método de la cuerda consiste en lo siguiente. La ecuación de la cuerda, tiene la forma

$$(x - a)/(b - a) = (y - f(a))/[f(b) - f(a)]$$

y la abscisa γ_1 del punto de su intersección con el eje x, obtenida de la ecuación

$$(\gamma_1 - a)/(b - a) = (0 - f(a))/[f(b) - f(a)]$$

es

$$\gamma_1 = -(b - a)f(a)/[f(b) - f(a)] + a =$$

$$= [af(b) - bf(a)]/[f(b) - f(a)]$$

tomando γ_1 como nuevo b en los casos I y II obtenemos

$$\gamma_2 = [af(\gamma_1) - \gamma_1 f(a)]/[f(\gamma_1) - f(a)],$$

$$\gamma_3 = [af(\gamma_2) - \gamma_2 f(a)]/[f(\gamma_2) - f(a)]$$

y así sucesivamente y tomando γ_1 como nueva a en los casos III y IV obtenemos

$$\gamma_2 = [\gamma_1 f(b) - bf(\gamma_1)]/[f(b) - f(\gamma_1)],$$

$$\gamma_3 = [\gamma_2 f(b) - bf(\gamma_2)]/[f(b) - f(\gamma_2)]$$

Aplicando estos dos métodos tenemos una rápida aproximación por ambos lados a la raíz buscada de la ecuación.

EJERCICIOS

Resuelva las siguientes ecuaciones por aproximación

1. $x^3-5x^2+2x+1=0$
2. $x^7-8x^3+x-2=0$
3. $x^6+2x^5-x^2+7x-1=0$
4. $x^5-4x-2=0$
5. $x^4+7x^3-9=0$

BIBLIOGRAFIA:

Aleksandrov, A.D., Kolmogorov, A.N. y otros. La Matemática: su contenido, método y significado. Tomo I.

Aragón, Jorge. Notas de Números Complejos.

Beaumont, R.A. y Pierce, R.S. The algebraic foundations of mathematics.

Beiler, A.H. Recreations in the theory of numbers.

Courant, R. y Robins, H. ¿Qué es la matemática?

King Dávalos, Jefferson. Introducción a la teoría elemental de los números. (Notas).

Kúrosch, A.G. Ecuaciones algebraicas de grados arbitrarios.

Ore, O. Number theory and its history.

Uspensky, J.V. Theory Equations.

Vinogradov, I. Fundamentos de la teoría de números.