UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

"TOPICOS EN LA TEORIA DE LOS NUMEROS"

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A

MARIO PINEDA RUELAS

MÉXICO, D.F. 1984.

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

C O N T E N I D O

INTRODUCCION

Creo que es obligación de todos influir, de acuerdo a las reglas de juego establecidas, en la evolución del mundo que nos rodea. La Matemática no podría ser la excepción y por ello, según mi experiencia, he pensado que en aras de un mejor aprovechamiento podría sugerir algunas ideas para complementar la educación en una dirección específica.

Los programas señalan al maestro una guía, que dentro de los estatutos universitarios, no lo obligan sino a ubicarse dentro de una linea de acción. Estimo que lo periférico es también importante.

El presente trabajo tiene como finalidad mostrar lo - que deseablemente debe ser periférico en un curso tradicional - de la Teoría de los Números. El orden no es sino mi apreciación de los mismos en grados crecientes de dificultad.

En el Capitulo I, se presentan los números enteros (ordinarios) Z y algunos conceptos fundamentales en la Teoría de - los números. Asimismo tratamos algunos aspectos sobre los números perfectos sin pasar por alto a los "primos gemelos" y la Conjetura de Goldbach.

En el Capitulo II, III, extendemos el concepto de número entero en estructuras menos simples (Dominios enteros sobre Z)

CAPITULO I

LOS NUMEROS ENTEROS

Informalmente el conjunto de los números enteros consiste de:

a) el conjunto de los números naturales

b) un objeto llamado cero y denotado por 0

c) para cada número natural n, un objeto -n, el cual es diferente de todos los números naturales y el cero.

Entonces si m y n son números naturales distintos, -m y -n son objetos distintos. Al conjunto {-n/n es natural} lo llamaremos el conjunto de enteros negativos.

Existen varias formas para construir el conjunto de los números enteros a partir de los números naturales y podríamos preguntarnos ¿Qué son los objetos específicos llamados enteros? Lo que queremos decir con esto, es que todas las construcciones de los enteros nos llevan a sistemas que esencialmente son los mismos.

Cuando los números naturales son definidos a partir de un número ordinal finito en el sentido de Von Newman, entonces una elección conveniente para el cero es el conjunto vacío y podriamos definir a los números negativos como $-n = \{n\}$ $n = 1,2,3...$ Ahora definimos el conjunto de los números enteros como:

$$[\ \{n\}/\ n \text{ es natural}\ ] \cup \{\phi\} \cup N$$

Con esta definición ya podemos abordar la manera clásica de identificar al conjunto de los números enteros como $...-n,...,-2,-1,0,1,2,...,n,...$ y denotaremos a este conjunto como Z.

y se clasifican a los elementos irreducibles.

No podriamos pasar por alto, al menos una presentación breve del Teorema de los Números Primos y a ésto por consecuencia dedicamos el cuarto capitulo. Es claro que no hay una demostración simple del Teorema pero buscamos algunos acercamientos elementales a la misma, sin recurrir a la Teoría de Funciones de Variable Compleja.

Una vez definido al conjunto de los enteros, lo dotaremos de dos operaciones llamadas suma y producto respectivamente que son sencillamente las operaciones usuales que todos conocemos. Ahora dirigiremos nuestra atención a una de las propiedades más importantes de los números enteros y en general de cualquier dominio entero (un dominio entero es un anillo comnutativo el cual no tiene divisores de cero, Z es un ejemplo de dominio entero).

La ecuación $ax=b$ con $a,b \in Z$ no siempre tiene solución entera. Si existe una solución entera para ésta ecuación entonces diremos que "a" divide a "b" ó que "b" es múltiplo de "a". Un concepto análogo se puede dar en cualquier dominio entero D, diremos que "a" divide a "b" en D, si $b = ax$ para alguna $x \in D$. Frecuentemente los divisores de 1 en D son llamados unidades de D, en Z son 1 y -1.

Es importante hacer notar que la noción de divisibilidad depende no solamente de los elementos a,b que se elijan, sino también depende del dominio entero en el cual se trabaje. Por ejemplo, 7 divide a 6 en los racionales pero 7 no divide a 6 en Z.

Notación: escribiremos $a|b$ si "a" divide a "b"

$a \nmid b$ en otro caso.

TEOREMA 1: Sean $a,b,c \in Z$ entonces

I.- Si $a|b$ y $b|c$ entonces $a|c$

II.- Si $a|x_1, \ldots, a|x_n$ entonces $a| \sum_{i=1}^{n} \alpha_i x_i$

III.- Si $a|0$, $-1|a$, $a|a$

IV.- Si $b \neq 0$ y $a|b$ entonces $|a| \leq |b|$

V.- Si $a|b$ y $b|a$ entonces $|a| = |b|$. ▲

Admitiremos éste teorema sin demostración por considerarlo elelemental, simplemente justificaremos la propiedad IV, es decïr, si $b \neq 0$ y $a|b$ entonces $b = aq$, por lo tanto $|b| = |a||b|$, pero $b \neq 0$ entonces $|q| \geq 1$ lo cual quiere decir que $|a| \leq |a||q| = |b|$, dicho de otra manera cualquier número entero tiene solamente un número finito de divisiores.

TEOREMA 2: (Algorítmo de la división)

Sean $a, b, \in Z$ con $a \neq 0$. Entonces existen enteros únicos q y r tal que $b = aq + r$ donde $0 \leq r < |a|$.

El algorítmo de la división puede usado para obtener un importan re resultado sobre la representación de los números naturales.

TEOREMA 3: Sea $a > 1$, entonces cualquier número $x > 0$ puede -- ser expresado en forma única como:

$x = b_0 + b_1 a + \ldots + b_n a^n$ con $n \geq 0$, $b_n > 0$ y

$0 \leq b_m < a$ para $0 \leq m \leq n$.

Dem. La prueba de existencia de tal expresión se hará por supues to haciendo inducción sobre el entero x.

Si $x = 1$ no hay nada que demostrar.

Supongamos que cualquier número natural $m < x$ puede ser re presentado de manera única en la forma

$r_k a^k + r_{k-1} a^{k-1} + \ldots + r_1 a + r_0$ donde $0 \leq r_i < a$ para -- $0 \leq i \leq k$.

Por el algorítmo de la división, existen enteros únicos - q, r tal que $x = qa + r$, $0 \leq r < |a| = a$,

es claro que $x \geq q > 0$. Si $q = 0$ entonces $n = r$ es la representación requerida ($n = 0$, $b_0 = r$). es decir, éste es el caso cuando $x = 1$.

Supongamos ahora que $q > 0$, esto es, $n \geq a$. Entonces $q \leq x$, así que apliquemos la hipótesis de inducción a q, es decir, - existe una única representación para q de la forma:

$$q = r_k a^k + r_{k-1} a^{k-1} + \ldots + r_1 a + r_0 \qquad 0 \leq r_i < a.$$

Ahora usando esta representación de q tenemos que:

$$x = aq + r = r_k a^{k+1} + r_{k-1} a^k + \ldots + r_1 a^2 + r_0 a + r$$

y con un cambio de notación obtenemos

$$x = b_0 + b_1 a + \ldots + b_n a^n .$$

Ahora demostraremos la unicidad de ésta representación.

Supongamos que $x = b_0 + b_1 a + \ldots + b_n a^n = C_0 + C_1 a + \ldots + C_j a^j$ afirmamos que $n = j$ y $b_n = C_m$ para $0 \leq m \leq n$.

Veamos porque; supongamos que nuestra afirmación es falsa,- entonces $0 = h_0 + h_1 a + \ldots + h_s a^s$, $h_s \neq 0$, $s > 0$,

$-a < h_i < a$ para $0 \leq i \leq s$ y $h_i = C_i - b_i$

como $h_i < a$ entonces $h_i \leq a-1$.

Por lo tanto

$a^s \leq |h_s a^s| = |h_0 + h_1 a + \ldots + h_{s-1} a^{s-1}| \leq |h_0| + |h_1| a + \ldots + |h_{s-1}| a^{s-1} \leq (a-1) + (a-1)a + \ldots + (a-1)a^{s-1} = (a-1)(1 + a + \ldots + a^{s-1}) = a^s - 1$ lo cual es absurdo. ▲

Sea x un número real, definimos $[x]$ como el mayor entero menor ó igual a x, esto es, el entero d tal que $d \leq x < d+1$, - observemos que $d \leq x < d+1$ implica que $d-1 \leq x-1 < d \leq x$ es decir $x - 1 < [x] \leq x$.

TEOREMA 4: Sean a,b,c,r enteros, $a \neq 0$ tal que $b = aq + r$ - con $0 \leq r < |a|$ entonces $q = [\frac{b}{a}]$

Dem. Como $a \neq 0$ entonces tenemos dos casos $a \geq 1$ y $a \leq -1$

Si $a \geq 1$ entonces $qa \leq qa + r = b < qa + a = (q+1)\,a$

es decir $qa \leq b < (q+1)a$ por lo tanto $q \leq \frac{b}{a} < q+1$. ▲

Si a y b son enteros no nulos entonces el conjunto de sus divisores comunes es finito, en efecto, sean $a,b,c \in Z$ tal que $c|a$ y $c|b$ si $a \neq 0$ entonces $a = yc$ para algún entero y, por lo tanto $|a|=|y||c| \geq |c|$, es decir $-|a| \leq c \leq |a|$, claramente existe un número finito de enteros c que satisfacen $-|a| \leq c \leq |a|$.

Ahora, sean $a,b \in Z$ ($a \neq 0$ ó $b \neq 0$) definimos el máximo común divisor de a y b como:

$\max\{ c \in Z / c > 0 , c|a , c|b \}$ y lo denotamos como

(a,b)

Puesto que $1 \in \{ c \in Z / c|a \text{ y } c|b \}$ entonces claramente $\max \{ c \in Z / a|c \text{ y } c|b\} \geq 1$, es decir, el máximo común divisor de a y b es un número entero positivo mayor ó igual a 1. Si $(a,b)=1$ diremos que a y b son primos relativos. Veamos que los divisores comunes de 18 y -42 son $\pm 1, \pm 2, \pm 3$ y ± 6. Por lo tanto $(18,-42) + 6$.

Observemos que los divisores comunes de 18 y -42 dividen a $6=(18,-42)$. Demostraremos que esto no es una simple casualidad, es decir, que este hecho es la propiedad que lo caracteriza.

TEOREMA 5: Sean a y b enteros no nulos entonces:

I.- Existen enteros x_0, y_0 tal que $(a,b)= ax_0 + by_0$

II.- Si $c \in Z$ y $c|a$, $c|b$ entonces $c|(a,b)$

Dem. Sea $g=(a,b)$, consideremos $S=\{ax + by / x,y \in Z\}$

observemos que $x = \pm 1$, $y = 0$ implica

a) $S \neq \phi$, b) $S \cap N \neq \phi$.

Sean x_0, y_0 enteros de tal manera que $d = ax_0 + by_0$ es el menor entero positivo en S. MOstraremos que $d|a$ y $d|b$.

"$d|a$" supongamos que $d \nmid a$ entonces por el teorema 2 existen q,r en Z tal que $a = dq + r \qquad 0 < r < d$, entonces

$r=a-dq = a-q(ax_0 + by_0) = a-qax_0 -qby_0 = a(1-qx_0) + b(-qy_0)$ lo cual contradice la elección de d. De manera similar $d|b$.

Hasta ahora hemos demostrado que d es divisor común de a y b, - es decir $d \leq g$ .....(1)

por otro lado tenemos que $a = gr$ y $b= gr_1$ por lo tanto $g|d$ y por (1), tenemos que $g = d$.

II. Si $c|a$ y $c|b$ entonces $c|ax$, $c|by$ para todo $x,y \in Z$ consecuentemente $c|g$.

A continuación enunciaremos algunas de las propiedades más importantes del máximo común divisor:

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

II) Si $c \neq 0$ entonces $(ca,cb) = |c|(a,b)$

III) Si $(a_1,m) = (a_2,m) = \ldots = (a_s,m)=1$ entonces $(\prod_{i=1}^{s} a_i, m)=1$

IV) $(a_1,a_2,\ldots a_s) = ((a_1,a_2,\ldots,a_{s-1}), a_s)$ ▲

TEOREMA 6: Sean a,b enteros no nulos, sea $d \in Z$ que satisface:

I. $d|a$ y $d|b$

II. $c|a$ y $c|b$ implica $c|d$

Entonces $d = \pm (a,b)$ ▲

Como observación aclaremos que las condiciones I y II del teorema anterior junto con el requerimiento de que $d > 0$ pueden ser - tomados como la definición de máximo común divisor en un dominio entero arbitrario, sin embargo la primera definición de máximo -

común divisor en Z depende no solamente del orden en Z sino también de que cualquier entero distinto de cero, tiene sólo un número finito de divisores. Con la aclaración anterior demos una nueva definición.

Sea D un dominio entero y sean $a,b \in D$ no ambos cero, entonces un elemento $d \in D$ es llamado máximo común divisor de a y b si:

I. $d|a$, $d|b$

II Si $c \in D$ tal que $c|a$ y $c|b$ entonces $c|d$.

En Z es fácil probar que el máximo común divisor es único, cosa que no sucede en cualquier dominio entero. Por ejemplo, en los racionales si a y b son distintos de cero entonces cualquier racional satisface las condiciones de nuestra nueva definición. El siguiente teorema justifica la existencia del máximo común divisor en Z.

TEOREMA 7: Sean a,b enteros no nulos. Entonces existe un único entero g tal que $g = (a,b)$.

Dem. Si $a = 0$ y $b \neq 0$ entonces $(0,b) = |b|$ y por lo tanto el teorema es válido.

supongamos que $a \neq 0 \neq b$

apliquemos el algorítmo de la división de la siguiente manera:

$a = bq_1 + r_1$ $\quad 0 < r_1 < |b|$

$b = r_1 q_2 + r_2$ $\quad 0 < r_1 < r_2$

$r_1 = r_2 q_3 + r_3$ $\quad 0 < r_3 < r_2$

$r_{k-2} = r_{k-1} q + r_k$ $\quad 0 < r_k < r_{k-1}$

$r_{k-1} = r_k q_{k+1}$

Observemos que éste proceso es finito puesto que siempre obtenemos una sucesión decreciente de enteros positivos ----

$0 < r_k < r_{k-1} < \ldots < r_2 < r_1 < |b|$ definimos $g = r_k$

Para asegurar que $g = (a,b)$ debemos mostrar lo siguiente:

I. $g > 0$

II. $g|a$ y $g|b$

III. Si $c|a$, $c|b$ entonces $c|g$

Por la forma en que construimos a g es obvio que satisface - I y II.

Sea c entero tal que $c|a$ y $c|b$, entonces claramente $c|r_1$ y por consiguiente $c|r_2$, $c|r_3$, ... $c|r_k$, es decir $c|g$.

Por lo tanto, haciendo uso del teorema 6, $g = (a,b)$. ▲

Por otro lado, en algunos dominios enteros no cualquier par de elementos tiene máximo común divisor, veamos por ejemplo;

Sea $A = \{ m + n\sqrt{10} / \ m,n \in Z \}$, entonces:

a) A es dominio entero con la suma y producto usual de números reales, en efecto, sean $a + b\sqrt{10}$ y $c + d\sqrt{10} \in A$ supongamos que $(a + b\sqrt{10})(c + d\sqrt{10}) = 0$, entonces - --

$$ac + 10bd = 0 \quad y \quad ad + bc = 0$$

por lo tanto $d(ac + 10bd) = 0$ y $c(ad + bc) = 0$

es decir $dac + 10bd^2 - cad - bc^2 = 0$

$10bd^2 - bc^2 = b(10d^2 - c^2) = 0$ $\therefore$ $b = 0$ impli

ca A dominio entero y lo mismo se puede concluir si ---

$10d^2 - c^2 = 0$.

b) Si $a + b\sqrt{10} | c + d\sqrt{10}$ en A, entonces $a^2 - 10b^2 | c^2 - 10d^2$ en Z.

c) 2 y $4+\sqrt{10}$ son divisores comunes de 6 y $8+2\sqrt{10}$ en A, es decir $2|6$ y $2|8+2\sqrt{10}$ porque $6 = 2(3)$ y $8+2\sqrt{10} = 2(4+\sqrt{10})$

$4+\sqrt{10} \mid 6$ y $4+\sqrt{10} \mid 8+2\sqrt{10}$ porque $6=(4+\sqrt{10})(4-\sqrt{10})$ Y

$$8+2\sqrt{10} = 2(4+\sqrt{10})$$

d) Si $2 \mid a+b\sqrt{10}$ en A, entonces $2 \mid a$ y $2 \mid b$ en Z.

e) Si $4+\sqrt{10} \mid 2c+2d\sqrt{10}$ en A, entonces $3 \mid c^2 - 10d^2$ en Z, en efecto, aplicando el inciso b) tenemos que si $4+\sqrt{10} \mid 2c+2d\sqrt{10}$ en A entonces $6 \mid 4(c^2-10d^2)$ en Z, por lo tanto $3 \mid c^2-10d^2$ en Z.

f) Si $2c + 2d\sqrt{10} \mid 6$ en A entonces $c^2-10d^2 \mid 9$ en Z.

g) Si $2c+2d\sqrt{10} \mid 8+2\sqrt{10}$ en A, entonces $c^2-10d^2 \mid 6$ en Z.

h) Por último demostraremos que no existe un elemento en A el cual es divisor común de 6 y $8+2\sqrt{10}$ y que sea divisible por 2 y $4+\sqrt{10}$ en A. Supongamos que existe $a+b\sqrt{10}$ en A, tal que $a+b\sqrt{10} \mid 6$ y $a+b\sqrt{10} \mid 8+2\sqrt{10}$ de tal manera que

$$2 \mid a+b\sqrt{10} \quad y \quad 4+\sqrt{10} \mid a+b\sqrt{10} \quad en \ A.$$

Si $2 \mid a+b\sqrt{10}$ entonces $2 \mid a$ y $2 \mid b$, es decir, $a+b\sqrt{10}=2c+2d\sqrt{10}$. Como $4+\sqrt{10} \mid 2c+2d\sqrt{10}$ en A, entonces $3 \mid c^2-10d^2$ en Z , esto implica que $c^2-10d^2 \neq \pm 1$.

Por otro lado tenemos que $2c+2d\sqrt{10} \mid 6$ en A, entonces ----

$$c^2-10d^2 \mid 9 \quad en \ Z.$$

Por lo tanto tenemos que:

$$c^2-10d^2 \mid 9 \qquad y \qquad c^2-10d^2 \mid 6 \quad en \ Z$$

entonces $c^2-10d^2 \mid 9-6$, es decir, $c^2-10d^2 \mid \pm 3$

pero $3 \mid c^2-10d^2$ en Z

consecuentemente $c^2-10d^2 = \pm 3$ es una ecuación insoluble en Z.

Por último concluimos diciendo que los números 6 y $8+2\sqrt{10}$ no tienen máximo común divisor en A.

En suma, hemos visto que existen estructuras algebraicas (Dominios enteros) en los cuales podemos encontrar elementos

que no tienen máximo común divisor. Ahora trataremos con rigor - algunos resultados que son poco manejados dentro de los cursos - tradicionales de teoria de los números.

TEOREMA 8: Sean $a,b,c \in Z$ tal que $a|bc$ y $(a,b)=1$, entonces $a|c$, omitimos la demostración por ser elemental, - simplemente mencionaremos que éste teorema algunas veces es llamado "Teorema fundamental de la Aritmética".

Corolario 1; Sean a,b,c enteros tal que $a|c$, $b|c$ y $(a,b)=1$ --- entonces $ab|c$.

Dem. $a|c$ entonces $c=ax$ para alguna $x \in Z$,

$b|c$ y $c=ax$ entonces $b|ax$, pero $(a,b)=1$, por el teorema 8 $b|x$, es decir, $x=by$

por lo tanto $c=ax=aby$ entonces $ab|c$. ▲

Observemos que el teorema 8 se puede generalizar como sigue:

TEOREMA 9: Si a,b,c son enteros tal que $b|ac$ entonces $b|(a,b)(b,c)$

Dem.; $b|ac$ implica que $ac=bt$ para algún $t \in Z$

Sea $d=(a,b)$, $d_1=(b,c)$, entonces existen $x,y,z,w \in Z$ tal - que $d=ax+by$, $d_1=bz+cw$

ahora tenemos que

$$dd_1 = (ax+by)(bz+cw) = b(axz+txw+byz+cyw)$$

y por lo tanto $b|(a,b)(b,c)$. ▲

TEOREMA 10: Sean a,b,c enteros tal que $(a,b)=(a,c)=1$, entonces - $(a,bc)=1$. ▲

Como consecuencia del Teorema 10 se puede demostrar inductivamente el siguiente

TEOREMA 11: para $k \geq 2$ y $a_1, a_2, \ldots, a_k, a \in Z$ tal que $(a_\nu, a)=1$ -

entonces $(a_1 a_2 \ldots a_k, a)=1$

Corolario 1; Si $(a,b)=1$ y k es natural, entonces $(a^k, b^k)=1$. ▲

Corolario 2; Sean a,b,k números naturales tal que $a^k \mid b^k$, entonces $a \mid b$.

Dem.; Sea $(a,b)=d$. Entonces tenemos que $a=da_1$, $b=db_1$ con $(a_1, b_1)=1$. Por el corolario 1, $(a_1^k, b_1^k)=1$. $a^k \mid b^k$ equivale a decir que $a_1^k d^k \mid b_1^k d^k$, así, $a_1^k \mid b_1^k$ y por lo tanto :

$$a_1 = 1, \quad a = d \quad y \quad b = ab_1 \quad \blacktriangle$$

Observemos que para dos números naturales s,k, la relación $s^s \mid k^k$ no necesariamente implica que $s \mid k$, por ejemplo, es fácil checar que $4^4 \mid 10^{10}$ pero $4 \nmid 10$ similarmente $9^9 \mid 21^{21}$ pero $9 \nmid 21$. En general hay una infinidad de enteros a,b con esta propiedad.

La noción de divisibilidad puede ser extendida a los números reales. Sean α, β reales, decimos que α divide a β $(\alpha \mid \beta)$, si existe un entero k tal que $\beta = k\alpha$. En el caso de ésta noción generalizada de divisibilidad, la relación $\alpha^2 \mid \beta^2$ no necesariamente implica que $\alpha \mid \beta$. Por ejemplo $(\sqrt{3})^2 \mid (\sqrt{9})^2$ pero $\sqrt{3} \nmid 3$, suponga-mos que $\sqrt{3} \mid 3$, entonces existe k entero tal que $3 = k\sqrt{3}$, es decir, $k=\sqrt{3}$, dicho de otra manera, $k^2=3$ indica que $k > 1$, $k \geq 2$ y por lo tanto $k^2 \geq 4$. Esto último claramente es falso.

Coroloario 3: Para enteros positivos a,b y $k > 1$, la relación $a^k \mid 2b^k$ implica que $a \mid b$.

Dem.; Sea $d = (a,b)$, entonces $a=da_1$, $b=db_1$ con $(a_1, b_1)=1$, Por el corolario 1 $(a_1^k, b_1^k)=1$. $a^k \mid 2b^k$ equivale a $d^k a_1^k \mid 2d^k b_1^k$ es decir. $a_1^k \mid 2b_1^k$. Entonces $a_1^k \mid 2$, pero $k > 1$, consecuentemente $a_1 = 1$, $a=d$ y por lo tanto $b=ab_1$. ▲

TEOREMA 12; Si a,b,d son enteros tal que (a,b)=1 y d|a+b, entonces (a,d)=1 y (b,d)=1

Dem.: Sea (a,d)= δ , entonces $\delta|a$, $\delta|d$.Por lo tanto $\delta|a+b$ y $\delta|b$. Concluimos diciendo que $\delta|(a,b)$, es decir $\delta|1$, dicho de otra manera $\delta=1$.

La igualdad (b,d)=1 se demuestra similarmente.▲

TEOREMA 13: Sean a,b,m enteros positivos tal que (a,b)=1

Entonces la progresión aritmética a+bk(k=0,1,2...) contiene un número infinito de números primos relativos con m, para cualquier $m \in N$.

Dem.: Supongamos (a,b)=1 y sea m entero positivo.

Consideremos el siguiente conjunto:

$$A = \{ x \in N/(x,a)=1 \ , \ x|m \}$$

Es claro que $A \neq \phi$; por otro lado, como $m \neq 0$, entonces sólo tiene un número finito de divisores y por lo tanto A es finito.

Por las razones anteriores tiene sentido definir el siguiente número: $c = \sup A$.

Ahora demostraremos que (a+bc,m)=1.

Supongamos que (a+bc,m)=d, entonces d|a+bc con (a,bc)= 1 haciendo uso del teorema 12 obtenemos (a,d)=1, (bc,d)=1 y obviamente (c,d)=1. Como (a,d)=(a,c)=1 entonces (a,dc)=1 Además c|m, d|m y (d,c)=1 entonces dc|m y por lo tanto d=1.

Sea l entero positivo arbitrario. Definimos k=c+lm. Demostraremos que (a+bk,m)=1.

Supongamos (a+bk,m)=(a+bc+blm,m)=d, es decir, d|m y ----

$d|a+bc+blm$, como $d|blm$, entonces $d|a+bc$ con $(a,bc)=1$, aplicando el teorema 12 tenemos $(a,d)=1=(d,bc)$ y también $(d,c)=1$. Además $d|m$, $c|m$ y $(d,c)=1$, por el corolario 1 del teorema 8 sabemos que $dc|m$ y por lo tanto $d=1$.▲

Por último generalizaremos nuestra definición de máximo común divisor en los enteros.

Definición: Sean $a_1, a_2, \ldots, a_k \in Z$. Un entero d es llamado máximo común divisor de los números $a_1, a_2, \ldots, a_k$ si satisface:

I) $d > 0$

II) $d|a_s \quad s=1,2,\ldots,k$

III) Si $c|a_s$ con $s=1,2,\ldots,k$, entonces $c|d$.

TEOREMA 14: Sea $k>2$ y $a_1, a_2, \ldots, a_{k+1}$ enteros, entonces

$$(a_1, a_2, \ldots a_{k+1}) = ((a_1, a_2, \ldots, a_k), a_{k+1})$$

Dem.: Sea $d = ((a_1, a_2, \ldots, a_k), a_{k+1})$. Sabemos que d es divisor común de los números $(a_1, a_2, \ldots, a_k)$ y a_{k+1}. Como $d|(a_1, a_2, \ldots, a_k)$ y $(a_1, a_2, \ldots, a_k)|a_s$ $(s=1,2,\ldots k)$, entonces $d|a_s$ para $s=1,2,\ldots k+1$. Sea d' cualquier divisor común de $a_1, a_2, \ldots, a_{k+1}$. En virtud de la condición 3 de la última definición tenemos que $d'|(a_1, \ldots a_k)$. Puesto que $d'|a_{k+1}$ entonces se tiene $d'|((a_1, a_2, \ldots, a_k), a_{k+1})$, es decir, $d'|d$. Pero $d|a_s$ -- $(s=1,\ldots k+1)$, por lo tanto d es divisor común de a_s con $s=1,\ldots k+1$ el cual es divisible por cualquier divisor común de estos números. Consecuentemente $d=(a_1, a_2, \ldots, a_{k+1})$.▲

Para encontrar el número $(a_1, a_2, \ldots, a_k)$ podemos calcular sucesivamente los siguientes números: $d_2=(a_1, a_2)$, $d_3=(d_2, a_3)$ $\ldots, d_{k-1}=(d_{k-2}, a_{k-1})$ y $(a_1, \ldots a_k)=(d_{k-1}, a_k)$.

NOCIONES DE MINIMO COMUN MULTIPLO

Sean $a_1, a_2, \ldots, a_K$ enteros. Cualquier entero x tal que $a_s | x$ $(s=1,2,\ldots,k)$, es llamado múltiplo común de los enteros $a_1, a_2, \ldots, a_K$. Por ejemplo $\prod_{s=1}^{k} a_s$ es múltiplo común de los a_s con $s=1,\ldots,k$.

Consideremos el siguiente conjunto:

$$S = \{x \in Z / a_s | x \ (s=1,\ldots,k),\ x > 0\}$$

Puesto que $|\prod_{s=1}^{k} a_s| \in S$, entonces $S \neq \Phi$ y por el principio del buen orden existe N en S tal que para todo $x \in S$, $N \leq x$. N es llamado el mínimo común múltiplo de los enteros $a_1, a_2, \ldots a_K$ y es denotado $[a_1, a_2, \ldots, a_K]$.

TEOREMA 15: Sean $a_1, a_2, \ldots, a_K$ enteros. Sea $N = [a_1, a_2, \ldots, a_K]$. Si c es entero tal que $a_s | c$ $(s=1,\ldots,k)$ entonces $N | c$.

Dem.: supongamos que existe un múltiplo común M de los a_s tal que $N \nmid M$, entonces por el algorítmo de la división tenemos

$$M = Nq + r \qquad 0 < r < N$$

es decir $r = M - Nq$

Como M,N son múltiplos comunes de los a_s, entonces existen enteros x_s, y_s tal que $M = x_s a_s$, $N = y_s a_s$.

Por lo tanto $r = M - Nq = a_s(x_s - y_s q)$, es decir $a_s | r$ $(s=1,\ldots,k)$, de esta manera r es múltiplo común de los a_s, pero además $0 < r < N$. Esto claramente es imposible puesto que N es el menor múltiplo común positivo de los a_s. Por lo tanto $N | M$ ▲

Por último veremos la relación que existe entre el mínimo común múltiplo y el máximo común divisor.

TEOREMA 16: Sean a_1, a_2 enteros no nulos, entonces el número $\frac{|a_1 a_2|}{(a_1, a_2)}$ satisface las siguientes condiciones:

I) $\frac{|a_1 a_2|}{(a_1, a_2)}$ es un entero mayor ó igual a cero.

II) $a_1 \left| \frac{|a_1 a_2|}{(a_1, a_2)} \right.$ y $a_2 \left| \frac{|a_1 a_2|}{(a_1, a_2)} \right.$

dicho en palabras, el número $\frac{|a_1 a_2|}{(a_1, a_2)}$ es un múltiplo común de los enteros a_1 y a_2.

III) Si x es entero tal que $a_1 | x$ y $a_2 | x$, entonces $\frac{|a_1 a_2|}{(a_1, a_2)} \left| x \right.$. En efecto, $a_1 | x$ y $a_2 | x$ implica

$x = a_1 r = a_2 t$. Sea $d = (a_1, a_2)$, es decir, $a_1 = dq_1$; $a_2 = dq_2$ con $(q_1, q_2) = 1$, entonces $a_1 r = dq_1 r = a_2 t = dq_2 t$, es decir $q_1 \left| q_2 t \right.$, aplicando el teorema 8 tenemos que $t = q_1 s$.

Ahora $x = a_2 t = dq_2 t = s(dq_1 q_2) = s(\frac{a_1 a_2}{d})$

de la última igualdad tenemos que $\frac{a_1 a_2}{(a_1, a_2)} \left| x \right.$,

por lo tanto $\frac{|a_1 a_2|}{(a_1, a_2)} \left| x \right.$ ▲

TEOREMA 17: Sean $a_1, a_2 \in Z$. Sea $N = [a_1, a_2]$ entonces $N = \frac{|a_1 a_2|}{(a_1, a_2)}$.

Dem.; Como N es múltiplo común de a_1 y a_2, entonces aplicando la parte III) del teorema 16, tenemos que $\frac{|a_1 a_2|}{(a_1, a_2)} \left| N \right.$

Por la parte II) del teorema 16, $\frac{|a_1 a_2|}{(a_1, a_2)}$ es multiplo común de a_1 y a_2, entonces aplicando el teorema 15 tenemos ----- $N \left| \frac{|a_1 a_2|}{(a_1, a_2)} \right.$, como N y $\frac{|a_1 a_2|}{(a_1, a_2)}$ son enteros positivos entonces $N = \frac{|a_1 a_2|}{(a_1, a_2)}$ ▲

Veamos un contraejemplo en el cual para $k \geq 3$, la colección de enteros $a_1, a_2, \ldots, a_K$ no satisface el teorema 17:

$$[4,4,-12](4,4,-12) \neq |(4)(4)(-12)|.$$

NUMEROS PRIMOS

Un número entero p es primo si satisface:

1° $p > 1$

2° $\{x \in Z / x > 0,\ x|p\} = \{1, p\}$

Un entero positivo que no es primo es llamado compuesto. En el año 1968 el Almanaque Mundial enlista al número 1 como primo. Como podremos ver más adelante, no es conveniente hacer ésto porque entonces el teorema fundamental de la aritmética sería falso.

TEOREMA 18: (Euclides). Cualquier entero positivo $a > 1$ es producto de números primos, es decir, $a = \prod_{s=1}^{r} p_s$ $r \geq 1$ ▲

TEOREMA 19: Si p es primo y $p | a_1 a_2 \ldots a_K$ entonces $p | a_s$ para alguna $s = 1, \ldots, k$ ▲

TEOREMA 20: Todo entero compuesto a, se puede factorizar en forma única como producto de primos. ▲

Observación; en el teorema 18 los números primos no necesariamente son distintos, ni estan colocados en algún orden particular, - por ejemplo; $288=2(3)(3)(4)(4)=2(3^2)(4^2)$, Si los colocamos en orden creciente y cambiamos la notación por una más apropiada tenemos que $a=p_1^{\nu_1} p_2^{\nu_2}...p_k^{\nu_k}$ con $\nu_s > 0$ y $1 < p_1 < p_2 <...<p_K$

Además veamos que los números p_s (s=1,...,k) tanto como el número de ellos, están determinados en forma única por el número a. --- Asimismo, los exponentes ν_s también estan determinados en forma - única por el entero a. En particular, el número ν_s puede ser definido como el mayor número natural para el cual $p_s^{\nu_s} | a$. Es fácil observar que si n es compuesto entonces n tiene un divisor primo p tal que $p \leq \sqrt{n}$, o sea si un número natural $n > 1$ no tiene divisores primos menores o iguales que $\sqrt{n}$, entonces n es primo.

TEOREMA 21: Sea $n > 2$, entonces existe al menos un número primo p que satisface $n < p < n!$

Dem: Puesto que $n > 2$, el número $z= n!-1 > 1$ y por lo tanto z - tiene un divisor primo p.

Si $p \leq n$, claramente $p|1$ lo cual es imposible. Por lo tanto $p > n$. Como $p \leq z$ y p es un divisor de z , entonces

$$n < p \leq n!-1 < n!$$ ▲

El teorema 21 no indica que dado n entero positivo siempre existe un primo p tal que $p > n$. Por lo tanto podemos inferir que existe un número infinito de números primos.

Dado m entero positivo, para obtener todos los números primos que aparecen en la sucesión 1,2,...,m es suficiente quitar

de ésta, todos los múltiplos de la forma kp, $k > 1$ donde p es primo tal que $p \leq \sqrt{m}$. En particular, para obtener todos los primos que aparecen en la sucesión 2,3,...,521 es suficiente quitar todos los números mayores que 2,3,5,7,11,13,17 y 19 que son divisibles por al menos uno de éstos.

Un método fácil para encontrar números primos consecutivos fué dado por ERATOSTENES. Consideremos la sucesión 2,3,4,... Denotaremos por p_1 al primer primo que aparece en ésta sucesión, es decir, $p_1=2$. Quitemos de la sucesión todos los números mayores que p_1 y que son divisibles por 2. El primero de los números restantes es $3=p_2$. Nuevamente quitemos de la sucesión todos los números mayores que p_2 y divisibles por p_2. El primero de los números restantes es $5=p_3$. Supongamos que después del k-ésimo paso encontramos el k-ésimo primo p_k. Quitemos de la sucesión todos los números mayores que p_k y divisibles por p_k. El siguiente número de los que restan en la sucesión es el k+1-ésimo primo. En particular $p_{6,000,000} = 104,395,301$. El método descrito anteriormente es conocido como la criba de ERATOSTENES. A continuación daremos una sencilla interpretación geométrica de la misma:

Consideremos en el plano cartesiano los siguientes conjuntos;

$$A=\{(0,\tfrac{1}{m})/m=1,2,...\} \quad , \quad B=\{(n+1,0)/n=1,2,...\}$$

donde cada punto del conjunto A esta conectado por una recta con cada punto del conjunto B. La ecuación de la recta que pasa por los puntos $(0,\frac{1}{m})$ y $(n+1,0)$ esta descrita como $y=-\frac{1}{m(n+1)}x+\frac{1}{m}$.

Las intersecciones de $y=-\frac{1}{m(n+1)}x+\frac{1}{m}$ con la recta $y=-1$ son de la forma $((m+1)(n+1),-1)$, es decir, las abscisas de

de estos puntos son precisamente números compuestos.

Recíprocamente, si x es entero positivo compuesto, entonces, $x=(m+1)(n+1)$ $n=1,2...,$ y $m=1,2,...,$ de donde claramente el punto $(x,1)$ satisface las ecuaciones

$$y= -\frac{1}{m(n+1)}x + \frac{1}{m}, \qquad y= -1$$

Dicho de otra manera, si z es entero positivo, claramente el punto $(z,-1)$ se encuentra en la recta $y=-1$. Denotaremos por L_1 la recta $y= -\frac{1}{m(n+1)}x + \frac{1}{m}$, L_2 la recta $y= -1$.

Si $(z,-1) \notin L_1 \cap L_2$ entonces z es primo ▲

Sea p_n el n-ésimo primo. Consideremos el número $d_n= p_{n+1} - p_n$, $n=1,2,....$, los primeros cien terminos de la sucesión infinita $d_1, d_2, ..., d_n....$ se muestran en la tabla 1.

Observemos que si $n > 1$ entonces p_n es un primo impar y por lo tanto el número d_n es par. También notemos que los números d_n pueden ser suficientemente grandes, en efecto, sea $m > 1$ entero positivo arbitrario. Sea p_n el mayor primo tal que $p_n \leq m!+1$. Los números $m!+k$ $(k=2,...,m)$ son compuestos ya que $k \mid m!+k$. Por lo tanto, tenemos que $p_{n+1} \geq m! + m + 1$ y consecuentemente $d_n= p_{n+1} - p_n \geq m$. También observemos que no es posible demostrar en general que los números d_n tienden a infinito porque por ejemplo existen enteros positivos n tal que $d_n= d_{n+1}$ $(n=2,15,36,39,46)$. También existen enteros positivos n para los cuales $d_n=d_{n+1}=d_{n+2}$ $(n=54,464,682,709,821,829)$. Sin embargo, no se sabe si dado un entero positivo k existe un entero positivo n tal -

TABLA 1.

p_{n+1}	p_n	d_n	p_{n+1}	p_n	d_n	p_{n+1}	p_n	d_n	p_{n+1}	p_n	d_n
3	2	1	103	101	2	239	233	6	389	383	6
5	3	2	107	103	4	241	239	2	397	389	8
7	5	2	109	107	2	251	241	10	401	397	4
11	7	4	113	109	4	257	251	6	409	401	8
13	11	2	127	113	14	263	257	6	419	409	10
17	13	4	131	127	4	269	263	6	421	419	2
19	17	2	137	131	6	271	269	2	431	421	10
23	19	4	139	137	2	277	271	6	433	431	2
29	23	6	149	139	10	281	277	4	439	433	6
31	29	2	151	149	2	283	281	2	443	439	4
37	31	6	157	151	6	293	283	10	449	443	6
41	37	4	163	157	6	307	293	14	457	449	8
43	41	2	167	163	4	311	307	4	461	457	4
47	43	4	173	167	6	313	311	2	463	461	2
53	47	6	179	173	6	317	313	4	467	463	4
59	53	6	181	179	2	331	317	14	479	467	12
61	59	2	191	181	10	337	331	6	487	479	8
67	61	6	193	191	2	347	337	10	491	487	4
71	67	4	197	193	4	349	347	2	449	491	8
73	71	2	199	197	2	353	349	4	503	449	4
79	73	6	211	199	12	359	353	6	509	503	6
83	79	4	223	211	12	367	359	8	521	509	12
89	83	6	227	223	4	373	367	6	523	521	2
97	89	8	229	227	2	379	373	6	541	523	18
101	97	4	233	229	4	383	379	4	547	541	6

que $d_n=d_{n+1}=\ldots=d_{n+k}$.

NUMEROS PRIMOS EN UNA PROGRESION ARITMETICA

Son conocidas algunas progresiones aritméticas que contienen un número finito de primos distintos; por ejemplo, 199+210k, para k=0,1,2,...,9. También se ha encontrado que los números -- 60060k + 4943 (k=0,1,2,...,12) forman una progresión aritmética - que contiene 13 primos diferentes. Sin embargo, existe un problema más general que queda enunciado como sigue: ¿Para qué enteros positivos a,b, la progresión aritmética ak + b (k=1,2,...) contiene un número infinito de primos?

Es claro que si (a,b)= d > 1, entonces no existen números - primos en la progresión ak + b, k=1,2,...

En el año 1837 L. Dirichlet demostró que esta condición también es suficiente. Para ver una demostración elemental de éste hecho remitimos al lector a:

Selberg, A., "An elementary Proof of Dirichlet's theorem aboot - primes in an arithmetic progression". An. of Math., 50(1949), pp.297-304,

Los siguientes teoremas son equivalentes;

T_1 = Sean a,b enteros positivos tal que (a,b)=1. Entonces existe un número infinito de números primos de la forma ak + b, k entero positivo.

T_2 = Sean a,b, enteros positivos tal que (a,b)=1. Entonces existe al menos un número primo de la forma ak+b, k entero positivo.

Dem.: Claramente T_1 implica T_2 . Demostraremos que T_2 implica T_1. Si a=1 entonces obviamente T_1 es válido. Supongamos que --

$a > 1$. Sea b entero positivo tal que $(a,b)=1$. Entonces -- $(a^s,b)=1$. Por T_2 existe un primo p de la forma $p=a^s k + b$ para algún k entero positivo. Como $a>1$ tenemos que: $a^s k+b > a^s \geq 2^s > s$. Entonces $p > s$. Así hemos demostrado que para cualquier entero positivo s existe un primo p de la forma ak+b y tal que $p > s$. Esto muestra que existe un número infinito de primos de esta forma ▲

Observemos que si:

D_1: Si $(a,b)=1$ entonces la progresión $a+bk$ $(b=1,2,...)$ contiene un número infinito de primos.

D_2: Si $(a,b)=1$ entonces existe p primo de la forma $p=a+bk$ $(a,b,\ k \in N)$.

D_3: Sean a,b,m enteros positivos tal que $(a,b)=1$. Entonces la progresión aritmética $a+bk$ $(k=1,2,...)$ contiene un número infinito de terminos que son primos relativos -- con m.

D_4: Sean a,b,m enteros positivos tal que $(a,b)=1$. Entonces existe $p=a+bk$ tal que $p \nmid m$.

Entonces las siguientes relaciones se cumplen:

$D_1 \leftrightarrow D_2$

$D_1 \Rightarrow D_3$

$D_1 \Rightarrow D_4$

$D_2 \Rightarrow D_3$

$D_2 \Rightarrow D_4$

Conjetura de Goldbach

Si n es entero positivo par mayor que 2, entonces siem-

pre se puede expresar como suma de dos números primos impares. - Esta afirmación es conocida como la Conjetura de Goldbach. Se conocen tablas numéricas donde ésta ha sido verificada directamente para números pares menores ó iguales a $33(10^6)$. Sin embargo, la - prueba final no existe.

TEOREMA 22: La Conjetura de Goldbach implica que cualquier número impar mayor que 7 es expresable como suma de tres números primos impares ▲

TEOREMA 23: La Conjetura de Goldbach es equivalente a afirmar - que cualquier número $x=2n > 4$ se puede expresar como suma de tres números primos ▲

TEOREMA 24: Todo entero $n > 11$ puede ser expresado como suma de dos números compuestos.

Dem.: Si $n=2k$, entonces $k \geq 6$, por lo tanto $n-6=2k-6=2(k-3)$ es - un número compuesto, dicho de otra manera $n=2(k-3)+6$ es suma de dos números compuestos. ▲

Si $n=2k+1$, entonces $k \geq 6$, por lo tanto $n-9=2k-8=2(k-4)$ es un número compuesto, dicho de otra manera $n=2(k-4)+9$ es suma de dos números compuestos

Definición: Sea n entero positivo, decimos que n es libre de cuadrados si no existe p primo tal que $p^2 | n$, es decir, $n= p_1 p_2 \ldots p_s$. $(p_i \neq p_j \text{ si } i \neq j)$

TEOREMA 25: Todo entero positivo n puede ser expresado en forma única como $n=k^2\ell$ con $k,\ell \in N$, ℓ libre de cuadrados ▲

NUMEROS PERFECTOS

Sea n entero positivo,

Si $\sum_{d|n} d < n$ $(0 < d < n)$, entonces diremos que n es deficiente.

(8 es deficiente).

Si $\sum_{d|n} d > n$ $(0 < d < n)$, entonces diremos que n es abundante.

(12 es abundante)

Si $\sum_{d|n} d = n$ $(0 < d < n)$, entonces diremos que n es perfecto.

Observemos que existe una infinidad de números deficientes, por ejemplo, los números de la forma $x=p^5$ con p primo. También notemos que existe un número infinito de números abundantes, por ejemplo los números de la forma $x=2(3^2)(k+1)$ con $k=1,2,\ldots$ Con respecto a los números perfectos podemos decir muy poco, ya que en la actualidad sólo se conocen 23 y todos ellos son pares. Si existe un número perfecto N impar (Descartes-Euler) éste debe ser de la forma $N=p^{4a+1}q^2$ con p primo de la forma $p=4k+1$, $a \geq 0$ y q impar tal que $(q,p)=1$. Recientemente se demostró que si N es perfecto impar entonces $N > 10^{20}$ y debe tener al menos 6 factores primos diferentes. El mayor de los números perfectos que se conoce en la actualidad es $2^{11212}(2^{11213}-1)$ el cual tiene 6751 dígitos.

Sea n entero positivo tal que $n=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_K^{\alpha_K}$. Sea $d>0$ divisor de n, Puesto que cualquier divisor de d es un divisor de n, entonces en la factorización del número d en primos sólo pueden aparecer los números $p_s^{\gamma_s}$ $0 \leq \gamma_s \leq \alpha_s$ $(s=1,2,\ldots,k)$, es decir, $d=p_1^{\gamma_1}\ldots p_K^{\gamma_K}$ con $0 \leq \gamma_i \leq \alpha_i$ $i=1,\ldots,k$. Consideremos la función:

$$\sigma: N \to N$$

$$n \to \sigma(n) = \sum_{d|n} d \qquad (d > 0)$$

Notemos que si consideramos a "n" como divisor de él mismo tenemos que $\sigma(1)=1$, $\sigma(4)=7$, $\sigma(5)=6$, $\sigma(10)=18$. Claramente si n es un número perfecto entonces $\sigma(n)=2n$. Asi si $n=p_1^{\alpha_1}\ldots p_K^{\alpha_K}$ entonces $\sigma(n) = \Sigma p_1^{\gamma_1}\ldots p_K^{\gamma_K}$, $0 \leq \gamma_i \leq \alpha_i$ $(i=1,2,\ldots,k)$ donde la sumatoria se extiende sobre los conjuntos de k-enteros que satisfacen $0 \leq \gamma_i \leq \alpha_i$. Claramente los números $p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_K^{\gamma_K}$ $(0 \leq \gamma_i \leq \alpha_i)$ están contenidos en la expansión del producto;

$$(1+p_1+p_1^2+\ldots+p_1^{\alpha_1})\,(1+p_2+p_2^2+\ldots+p_2^{\alpha_2})\ldots(1+p_K+p_K^2+\ldots+p_K^{\alpha_K}).$$

Inversamente, cada uno de los sumandos de éste último producto aparece como sumando en $\Sigma p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_K^{\gamma_K}$, $0 \leq \gamma_i \leq \alpha_i$ $(i=1,2,\ldots,k)$.

Así, tenemos el siguiente resultado:

TEOREMA 26: Sea n entero positivo tal que $n=p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_K^{\alpha_K}$, entonces

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_K^{\alpha_K+1}-1}{p_K-1} \quad \blacktriangle$$

Como ejemplo $\sigma(200)=17(31)=465$.

Observemos que si p es primo entonces $\sigma(p)=p+1$.

TEOREMA 27: Para que un número par positivo n sea perfecto, es necesario y suficiente que $n=2^{s-1}(2^s-1)$, donde $s > 1$ y 2^s-1 es primo.

Dem.: Sea n número perfecto par. Entonces $n=2^{s-1}\mathbb{L}$, $s > 1$ y $\mathbb{L}=2k+1$. Por lo tanto $\sigma(n)=\sigma(2^{s-1})\sigma(\mathbb{L})=(2^s-1)\sigma(\mathbb{L})$. Puesto que n es perfecto, entonces $(2^s-1)\sigma(\mathbb{L})=2n=2^s\mathbb{L}$. Además $(2^s-1, 2^s)=1$ y $2^s \mid (2^s-1)\sigma(\mathbb{L})$, por lo tanto $2^s \mid \sigma(\mathbb{L})$ y en consecuencia $\sigma(\mathbb{L})=2^s q$ con $q \in N$. $(2^s-1)q=\mathbb{L}$ implica que $\sigma(\mathbb{L})=\mathbb{L}+q$ ya que $\sigma(\mathbb{L})=2^s q$. Como $(2^s-1)q=\mathbb{L}$ entonces $q \mid \mathbb{L}$ y $q < \mathbb{L}$ $(s>1)$. Por lo tanto $\mathbb{L}$ tiene al menos dos divisores distintos que

son q, L. Pero la formula $\sigma(L)=1+q$ nos indica que L, q son los únicos divisores. Consecuentemente q=1 y L es primo. Pero ------ $L=(2^s-1)q=2^s-1$. Entonces $n=2^{s-1}L=2^{s-1}(2^s-1)$. Así tenemos demostrada la condición necesaria. Para probar la suficiencia, supongamos que 2^s-1 es un número primo. Sea $n=2^{s-1}(2^s-1)$. Entonces;

$$\sigma(n)=\sigma(2^{s-1})\sigma(2^s-1)=(2^s-1)2^s=2n.$$

Esta última igualdad afirma que n es un número perfecto, con lo -- cual terminamos la demostración del teorema ▲

Es fácil demostrar que si 2^s-1 es un número primo, entonces p debe ser también un número primo. El teorema anterior se resume como:

Todos los números perfectos pares son de la forma $2^{k-1}(2^k-1)$, donde k y 2^k-1 son números primos ▲

Los números perfectos fueron investigados por Euclides - quien descubrió el siguiente método para calcularlos. "Consideremos las sumas $1+2+2^2+2^3+\ldots 2^k$. Si en una de éstas obtenemos un número primo, entonces la multiplicamos por su último sumando y así obtenemos un número perfecto".

Con ayuda del teorema (27), observamos que el método de Euclides nos proporciona todos los números perfectos pares.

Ahora vamos a calcular, por el método de Euclides, algunos números perfectos pares. Consideremos la sucesión de los números primos. Observemos cuando ó no el número 2^k-1 es primo. Vemos que para k=2,3,5,7 los números $2^k-1=3,7,31,127$ son primos. Con esto obtenemos los primeros cuatro números perfectos, los cuales ya eran conocidos en la antiguedad. Ellos son $2(2^2-1)=6$, $2^2(2^3-1)=28$, $2^4(2^5-1)=496$; $2^6(2^7-1)=8128$. Para k=11 el número $2^{11}-1=23(89)$ es

compuesto y por lo tanto $2^{10}(2^{11}-1)$ no es un número perfecto. Todo esto muestra que la tarea de encontrar números perfectos pares, es la misma que encontrar números de Mersenne definidos como números primos de la forma 2^s-1. Sin embargo, aun quedan dos preguntas que contestar ¿Existe un número infinito de números perfectos? ¿Existe un número perfecto impar?.

Por último analizemos el problema de caracterizar todos los enteros $n > 1$ tal que $\prod_{d|n} d = n^2$. Los enteros positivos que satisfacen la igualdad anterior son conocidos como números perfectos multiplicativos.

TEOREMA 28: Sea $n > 1$. Si $d(n)$ es el número de divisores positivos de n, entonces

$$d(n)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_s+1) \quad , \quad n=p_1^{\alpha_1}\ldots p_s^{\alpha_s} \quad \blacktriangle$$

TEOREMA 29: $\prod_{d|n} d = n^2$ si y sólo si $n=p^3$ ó $n=p_1p_2$, $p_1 \neq p_2$.

Dem.: esclaro que $\prod_{d|n} d = \prod \frac{n}{d}$

Por lo tanto

$$n^4=n^2n^2=\prod d \cdot \prod \frac{n}{d} = \prod n = n^{d(n)} \quad , \quad (d|n)$$

haciendo uso del teorema 28 tenemos que:

$$d(n)=4=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_s+1)=4$$

Asi es que $s=1$ y $\alpha_1=3$ ó $s=2$ y $\alpha_1=\alpha_2=1$ $\blacktriangle$

Como una simple observación notemos que existe un número infinito de números perfectos multiplicativos.

CAPITULO II

ENTEROS GAUSSIANOS

Los enteros complejos ó enteros gaussianos son números complejos de la forma a+bi donde a,b son enteros. Este conjunto es denotado por $Z[i]=\{a+bi/a,b \in Z,\ i^2=-1\}$.

La Teoría de los enteros gaussianos es importante por dos razones, primeramente resulta interesante ver hasta que punto las propiedades de los enteros ordinarios son suceptibles a generalizaciones, segundo; porque algunas propiedades de los enteros ordinarios son consecuencia directa de las propiedades de los enteros gaussianos.

Observemos que los gaussianos forman un dominio entero con la suma y producto usuales. Si $\alpha= a+bi \in Z[i]$ denotaremos $\bar{\alpha} = a-bi$ y $N(\alpha)= \alpha\bar{\alpha}$. Llamaremos a $N(\alpha)$ la norma de α.

Notemos que α y $\bar{\alpha}$ tienen la misma norma, es decir, $N(\alpha)= N(\bar{\alpha})$. Si $\alpha=a+bi$ $(a,b \in Z)$, tenemos que $N(\alpha)=a^2+b^2$. Por lo tanto, la norma de un gaussiano es un entero positivo, es cero si y sólo si $\alpha=0$.

Sean $\alpha_1, \alpha_2 \in Z[i]$. Decimos que α_2 divide a $\alpha_1 \in Z[i]$ si existe α_3 en $Z[i]$ tal que $\alpha_1=\alpha_2\alpha_3$. Si α_2 divide a α_1 en $Z[i]$ escribiremos $\alpha_2 \mid \alpha_1$ y $\alpha_2 \nmid \alpha_1$ en caso contrario. Notemos que un entero ordinario puede verse como un entero gaussiano. Es importante observar que esta definición de divisibilidad en $Z[i]$ es consistente con la que dimos para los enteros ordinarios.

TEOREMA 1: Sean a,b enteros ordinarios tal que $b \mid a$ en $Z[i]$. Entonces $b \mid a$ en Z.▲

Dem.: Para establecer cuando $c+di \mid a+bi$ es útil el siguiente resultado

TEOREMA 2: $c+di \mid a+bi$ si y sólo si $c^2+d^2 \mid ac+bd$ y $c^2+d^2 \mid bc-ad$ en Z. ▲

Ejemplos:

$1+i \mid 2$ porque $2 \mid 2$ y $2 \mid -2$

$1+i \nmid 1+2i$ porque $2 \nmid 3$

TEOREMA 3: Sean α_1, α_2 enteros gaussianos. Entonces

I) si $\alpha_1 \mid \alpha_2$ entonces $\overline{\alpha_1} \mid \overline{\alpha_2}$

II) $N(\alpha_1 \alpha_2) = N(\alpha_1) N(\alpha_2)$

III) Si $\alpha_1 \mid \alpha_2$ entonces $N(\alpha_1) \mid N(\alpha_2)$ ▲

La propiedad II se puede expresar diciendo que la norma es una -- función multiplicativa.

Ciertos enteros gaussianos dividen a cualquier elemento de $Z[i]$, - ellos son llamados unidades. En particular, una unidad divide a 1. Inversamente si $u \mid 1$ entonces u es unidad, en efecto, tenemos que $1=u\alpha$, entonces para todo β en $Z[i]$, $\beta=\beta(1)=(\beta\alpha)u$. Por lo tanto $u \mid \beta$.

Podemos encontrar las unidades en $Z[i]$ simplemente localizando los divisores de 1. Las únicas soluciones de la ecuación $a^2+b^2=1$ en Z son $\pm 1, 0$ y $0, \pm 1$, y por lo tanto las únicas unidades de $Z[i]$ son $\pm 1, \pm i$.

TEOREMA 4: $N(\alpha)=0$ si y sólo si $\alpha=0$.

$N(\alpha)=1$ si y sólo si $\alpha \mid 1$

$N(\alpha) > 1$ en otro caso ▲

Sean $\alpha, \beta \in Z[i]$. Si $\alpha \mid \beta$ y $\beta \mid \alpha$ entonces decimos que α y β son asociados.

TEOREMA 5: Sean α, β asociados, entonces $N(\alpha)=N(\beta)$ ▲

El inverso del teorema anterior no siempre es válido, por ejemplo: $N(1-2i)=N(1+2i)$ pero $1-2i \nmid 1+2i$

TEOREMA 6: Sea $\alpha \in Z[i]$, $\alpha \neq 0$. Entonces α tiene exactamente cuatro asociados. ▲

TEOREMA 7: (Algorítmo de la División). Si $\alpha, \beta \neq 0$ son enteros gaussianos, entonces existen κ, δ tal que;

$$\alpha = \beta\kappa + \delta \quad \text{con } N(\delta) < N(\beta).$$

Dem.: $$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = A+Bi \qquad (A, B \in \mathbb{Q})$$

Sean x, y los enteros más próximos a A y B respectivamente, es decir $|A-x| \leq \frac{1}{2}$ y $|B-y| \leq \frac{1}{2}$,

Entonces;

$$N\left(\frac{\alpha}{\beta} - (x+yi)\right) = N(A+Bi-(x+yi)) = N((A-x)+(B-y)i) = (A-x)^2+(B-y)^2 < 1.$$

Sea $\kappa = x+yi$, $\delta = \alpha - \beta(x+yi)$

Finalmente tenemos que

$$N(\delta) = N(\alpha-\beta(x+yi)) = N(\beta)N\left(\frac{\alpha}{\beta} - (x+yi)\right) < N(\beta) \text{ ▲}$$

TEOREMA 8: Sean $\alpha, \beta \in Z$. Entonces existe $\delta \in Z[i]$ tal que;

I. $\delta \mid \alpha$ y $\delta \mid \beta$

II. Si $\delta' \mid \alpha$, $\delta' \mid \beta \rightarrow \delta' \mid \delta$

III. Existen $\xi, \eta \in Z[i]$ tal que $\delta = \alpha\xi + \beta\eta$.

Dem.: En base al Teorema 7, el algorítmo euclideano puede ser generalizado para los enteros gaussianos como sigue:

$$\alpha = \beta\kappa_1 + \rho_1 \qquad N(\rho_1) < N(\beta)$$

$$\beta = \rho_1\kappa_2 + \rho_2 \qquad N(\rho_2) < N(\rho_1)$$

$$\vdots$$

$$\rho_{k-2} = \rho_{k-1}\kappa_k + \rho_k \qquad N(\rho_k) < N(\rho_{k-1})$$

$$\rho_{k-1} = \rho_k\kappa_{k+1}$$

esta sucesión de ecuaciones debe terminar porque $N(\beta)$, $N(\rho_1)$ $N(\rho_2)$,... es una sucesión decreciente de enteros positivos.

Sea $\delta=\rho_k$. Es fácil observar que ρ_k es un divisor común de α y β. También ρ_k puede ser escrito como combinación lineal de ρ_{k-1} y ρ_{k-2}, del mismo modo ρ_{k-1} es combinación lineal de ρ_{k-3} y ρ_{k-2} y así sucesivamente obtenemos que ρ_k es combinación lineal de α y β, es decir $\rho_k = \alpha\xi+\beta\eta$.

Por otro lado, si δ' satisface I y II entonces como $\delta \mid \alpha$ y $\delta \mid \alpha$, $\delta \mid \delta'$. Pero $\delta_1 \mid \alpha$ y $\delta_1 \mid \beta$, por lo tanto $\delta_1 \mid \delta$.

En conclusión, δ y δ' son asociados.▲

Cualquier entero gaussiano δ que satisface I y II es llamado el máximo común divisor de α y β, escribimos $(\alpha,\beta)=\delta$.

Corolario: Cualquier par de enteros gaussianos tiene exactamente cuatro máximos comunes divisores. Todos ellos son asociados.▲

Realmente, los enteros ordinarios tienen 2 máximos comunes divisores los cuales difieren en el signo. Ellos son de tal forma que cada uno de ellos es dividido por cualquier divisor común de los números dados. En el caso de los enteros gaussianos podemos considerar sólo un máximo común divisor simplemente identificando divisores asociados.

Como una aplicación del teorema 8 citamos el siguiente par de ejemplos:

1) Encuentre el máximo común divisor de $6-17i$ y $18+i$

$$\frac{6-17i}{18+i} = \frac{(6-17i)(18-i)}{325} = \frac{91-312i}{325} = -i+\frac{91+13i}{325}$$

$$6-17i=-i(18+i) + (5+i)$$

$$\frac{18+i}{5+i} = \frac{(18+i)(5-i)}{26} = \frac{91-13i}{26} = 3 + \frac{1-i}{2}$$

$$18+i=3(5+i)+(3-2i)$$

$$5+i=1+i$$

Por lo tanto $(6-17i,18+i)=3-2i$ y los números asociados con éste, es decir, $-3+2i$, $2+3i$, $-3-2i$.

2) Encuentre el máximo común divisor de $7+11i$ y $3+5i$

$$\frac{7+11i}{3+5i} = \frac{76-2i}{34} = 2 + \frac{8-2i}{34}$$

$$7+11i=2(3+5i)+(1+i)$$

$$\frac{3+5i}{1+i} = 4+i \quad , \qquad 3+5i=(4+i)(1+i)$$

Por lo tanto $(7+11i,3+5i)=1+i$ y los números asociados a éste, es decir, $-1-i$, $i-1$, $-i+1$.

Es fácil notar que entre los divisores comunes de α y β, el máximo común divisor tiene norma máxima. El inverso también es cierto. Así el máximo común divisor también puede ser definido como el divisor común que tiene norma mayor.

La teoría de el máximo común divisor de dos o más enteros gaussianos se puede establecer fácilmente considerando formas lineales, justamente como se hizo para los enteros ordinarios.

TEOREMA 9: Sean $\alpha_1, \alpha_2, \ldots, \alpha_k$ enteros gaussianos distintos de cero. Entonces existe $\rho \in Z[i]$ tal que

I. $\rho \mid a_i \quad (i=1,2,\ldots,k)$

II. Si $\mu \mid a_i$ con $i=1,2,\ldots,k$, entonces $\mu \mid \rho$.

Dem.: Sea $\mathcal{B} = \{a_1x_1+a_2x_2+\ldots+a_kx_k / \ x_i \in Z[i]\}$

y $M = \{N(x) / \ x \in Z\}$

Como M es un subconjunto de los enteros positivos, enton-

ces existe $\rho \in \mathbb{A}$ de norma mínima y $\rho=a_1\rho_1+a_2\rho_2+\ldots+a_K\rho_K$.

Ahora vamos a demostrar que para toda x en $\mathbb{A}$, $\rho \mid x$.

Sea x en $\mathbb{A}$, entonces existen $x_1, x_2, \ldots, x_K$ en $Z[i]$ tal que

$$x= a_1x_1+a_2x_2+\ldots a_Kx_K .$$

Aplicando el teorema 7 tenemos que existen q,r en $Z[i]$ tal que $x=\rho q+r$ $\quad N(r) < N(\rho)$

pero $r=x-\rho q=a_1(x_1-q\rho_1)+\ldots+a_K(x_K-q\rho_K)$.

Si $N(r) \neq 0$ entonces $r \neq 0$ y por lo tanto $r \in \mathbb{A}$. Además r es entero gaussiano que satisface $N(r) < N(\rho)$.

Esta última contradicción implica que $N(r)=0$, es decir, $r=0$.

Por consiguiente $x=\rho q$ y $\rho \mid x$ para toda x en $\mathbb{A}$.

Por último, sea μ cualquier divisor común de a_i,

$$a_i=\mu\tau_i$$

como $\rho=a_1\rho_1+\ldots+a_K\rho_K=\mu(\tau_1\rho_1+\ldots+\tau_K\rho_K)$

entonces $\mu \mid \rho$. ▲

Cualquier par de enteros gaussianos α,β tienen por lo menos 4 divisores en común, a saber: $1,-1,i,-i$. Si α,β sólo tienen éstos números como divisores comunes, entonces decimos que α,β son primos relativos. En este caso escribimos $(\alpha,\beta)=1$.

Como una aplicación del teorema 9 tenemos el siguiente resultado:

TEOREMA 10: Sean $\alpha,\beta \in Z[i]$. Entonces α,β son primos relativos si existen x,y en $Z[i]$ tal que $\alpha x+\beta y=1$. ▲

TEOREMA 11: Sean $\alpha,\beta,\delta \in Z[i]$ tal que $\alpha \mid \beta\delta$ y $(\alpha,\beta)=1$. Entonces $\alpha \mid \delta$. ▲

TEOREMA 12: Si $(\alpha,\beta)=1=(\alpha,\delta)$, entonces $(\alpha,\beta\delta)=1$. ▲

Sean $a_1, a_2, \ldots, a_K$ enteros gaussianos distintos de cero. Conside-

remos el siguiente conjunto $M=\{x \in Z[i] / a_i \mid x,\ i=1,\ldots,k\}$.

Claramente $M \neq \Phi$ puesto que el número Πa_i $(i=1,\ldots,k)$ pertenece a M. Con ésto, tenemos justificado que al menos existe un multiplo común de los enteros $a_1, a_2, \ldots a_k$.

TEOREMA 13: Sean $a_1, a_2, \ldots, a_k$ enteros gaussianos distintos de cero. Existe μ en $Z[i]$ con las siguientes propiedades:

I. $a_i \mid \mu$ para $i=1,2,\ldots k$

II. Si $\mu' \in M$ entonces $\mu \mid \mu'$.

Dem.: Sea $M=\{x \in Z[i] / a_i \mid x,\ i=1,2,\ldots,k\}$

Consideremos $H=\{N(x)/x \in M\}$,

Observemos que $H \neq \Phi$ puesto que $M \neq \Phi$.

Como H es subconjunto de los enteros positivos, entonces existe m en H tal que $m \leq h$ para todo h en H,

Por lo tanto, existe μ en M tal que $N(\mu)=m$.

Obviamente μ satisface I.

Por último, sólo resta checar que μ satisface II.

Sea μ' en M. Sabemos que existen q,r, en $Z[i]$ tal que

$$\mu' = c\mu + r \qquad N(r) < N(\mu).$$

Si $r \neq 0$, entonces resulta ser multiplo común de $a_1, \ldots a_k$ y además r satisface $N(r) < N(\mu)$ lo cual es una contradicción.

Por lo tanto $r = 0$ y consecuentemente $\mu \mid \mu'$. ▲

La norma de cualquier entero gaussiano que satisface I y II es menor ó igual que la norma de cualquier multiplo común de los números $a_1, a_2, \ldots, a_k$.

Es fácil ver que todos los enteros gaussianos que satisfacen las dos propiedades del teorema anterior son asociados.

PRIMOS en Z[i]

Es claro que todo $\alpha \in Z[i]$ tiene al menos cuatro divisores: $1,-1,i,-i$. Si α es asociado con 1 entonces α también tiene como divisores a $\alpha,-\alpha,i\alpha,-i\alpha$, Dicho de otra manera, todo entero gaussiano α al menos tiene como divisores a $1,-1,i,-i,\alpha,-\alpha,i\alpha,-i\alpha$.

Un entero gaussiano π será llamado primo en Z[i] si sus únicos divisores son $1,-1,i,-1,\pi,-\pi,i\pi,-i\pi$. Para distinguir entre un primo en Z de un primo en Z[i] llamaremos primos ordinarios a los de Z y simplemente primos a los de Z[i].

Resumiendo, tenemos que un entero gaussiano es primo si no tiene divisores excepto sus asociados y las unidades. Es claro que esta definición es equivalente a la siguiente:

> Un entero gaussiano α es primo si su norma es mayor que 1 y si no es representable como producto de enteros gaussianos con norma mayor que 1.

En efecto, si α esta en Z[i], $N(\alpha) > 1$ y $\alpha=\mu\beta$, donde $N(\mu) > 1$, $N(\beta) > 1$, entonces μ no es asociado de 1 puesto que $N(\mu) > 1$. También μ no es asociado de α puesto que entonces β resultaría asociado con 1. Por lo tanto, α tiene un divisor μ el cual no es asociado con 1 ni con α, es decir α no es primo.

TEOREMA 14: Sea $\alpha \in Z[i]$ tal que $N(\alpha)$ es primo ordinario. Entonces α es primo.

Dem.: Supongamos que $N(\alpha)=p$, y $\alpha=\mu\beta$ con p primo ordinario. $p=N(\alpha)=N(\mu)N(\beta)$. $N(\mu)=1$ ó $N(\beta)=1$, es decir, μ ó β es unidad. Por lo tanto α es primo. ▲

El inverso del teorema 14 es falso puesto que;

7 es primo en Z[i] y $N(7)=49$ no es primo ordinario.

En general si p es un primo ordinario no necesariamente p es un - primo en $Z[i]$.

TEOREMA 15: Sea n entero positivo tal que n es primo en $Z[i]$. Entonces n es primo en Z.

Dem.: Si n es primo en $Z[i]$ entonces sus únicos divisores son -- $1,-1,i,-i,n,-n,in,-in$.

Entonces claramente n es primo en Z ▲

TEOREMA 16: Cualquier entero gaussiano α con $N(\alpha) > 1$ puede ser representado como un producto finito de primos.

Dem.: Sea $\alpha \in Z[i]$, $N(\alpha) > 1$. La demostración la haremos por inducción sobre $N(\alpha)$.

El primer caso a considerar es $N(\alpha)=2$: los 4 enteros gaussianos de norma 2 son asociados del primo $1+i$, en éste -- caso el teorema queda demostrado.

Supongamos que α es tal que para todo μ en $Z[i]$ con $N(\mu) < N(\alpha)$, μ es representable como producto finito de - primos. Si α es primo, terminamos. Si α no es primo entonces $\alpha=\beta\gamma$, con $1 < N(\beta) < N(\alpha)$, $1 < N(\gamma) < N(\alpha)$. Haciendo uso de la hipótesis de inducción tenemos que

$$\beta = \pi_1 \pi_2 \ldots \pi_\mu \quad , \quad \gamma = \pi'_1 \pi'_2 \ldots \pi'_\tau$$

donde π_s, π'_k son primos

por lo tanto

$$\alpha = \pi_1 \pi_2 \ldots \pi_s \pi'_1 \pi'_2 \ldots \pi'_\tau \quad ▲$$

Por definición, cualquier primo π tiene por divisores a

$$1,-1,i,-i,\pi,-\pi,i\pi,-i\pi.$$

De ésto último inferimos que, si un entero gaussiano α no es dividido por un primo π, entonces $(\alpha,\pi)=1$.

TEOREMA 17: Si $\pi, \pi_1, \pi_2, \ldots, \pi_k$ son primos y $\pi \mid \pi_1 \pi_2 \ldots \pi_k$, entonces π es asociado de algún π_s con $1 \leq s \leq k$. ▲

TEOREMA 18: (Teorema de Factorización única para Z[i]).

La representación de un entero gaussiano como un producto finito de primos es única salvo el orden de los primos y asociados.

Dem.: Sea α en Z[i], $N(\alpha) > 1$. Supongamos que α tiene dos factorizaciones $\alpha = \pi_1 \pi_2 \ldots \pi_k = \pi'_1 \pi'_2 \ldots \pi'_s$, $k < s$.

Entonces $\pi_1 \mid \pi'_1 \pi'_2 \ldots \pi'_s$. Por el teorema 17, π es asociado con algún π_T, supongamos que es π'_1. Entonces

$$\mu_1 \pi_2 \pi_3 \ldots \pi_k = \pi'_2 \pi'_3 \ldots \pi'_s \text{ donde } \mu_1 \text{ es una unidad.}$$

El argumento puede ser repetido k veces para obtener

$$\mu_1 \mu_2 \ldots \mu_k = \pi'_{k+1} \pi'_{k+2} \ldots \pi'_s$$

Por lo tanto, $1 = N(\mu_1) N(\mu_2) \ldots N(\mu_k) = N(\pi'_{k+1}) N(\pi'_{k+2}) \ldots N(\pi'_s)$

lo cual es falso puesto que $N(\pi_{k+i}) > 1$

$1 \leq i \leq s-k$. Por lo tanto $s=k$ ▲

A continuación damos la demostración de algunos resultados básicos que nos serviran posteriormente para caracterizar los números primos en Z[i].

El principio de la caja de Dirichlet nos dice que si tenemos n cajas y m > n objetos para colocarlos en ellas, entonces al menos una caja contiene más de un objeto. El siguiente resultado es una simple aplicación de éste principio.

TEOREMA 19: (Axel Thue) Sea n > 1, y se k el menor entero tal que $k > \sqrt{n}$. Entonces para cualquier entero a, tal que $p \nmid a$, podemos encontrar $x, y \in \{0,1,2,\ldots k-1\}$ de tal manera que $ay \equiv \pm x \pmod{n}$.

Dem.: Sea $S=\{ay+x\}$ con $x,y \in \{0,1,\ldots,k-1\}$

Es claro que la cardinalidad de S es k^2.

Por lo tanto, como $k^2 > n$ entonces existen

ay_1+x_1 , $ay_2+x_2 \in S$ tal que $ay_1+x_1 \equiv ay_2+x_2 \pmod n$

(principio de la caja de Dirichlet).

Podemos escribir $a(y_1-y_2) \equiv x_1-x_2 \pmod n$

Además $0 < |y_1-y_2| \leq k-1$, $0 < |x_1-x_2| < k-1$

Si $y_1-y_2=0$ entonces $x_1-x_2=0$

Sea $y=y_1-y_2$, $x=x_1-x_2$ ▲

TEOREMA 20: Sea p primo ordinario. Entonces $x^2 \equiv -1 \pmod p$ tiene solución si y sólo si $p \equiv 1 \pmod 4$ ▲

TEOREMA 21: Cualquier primo de la forma 4n+1 puede ser representado de manera única como suma de dos cuadrados.(Fermat)

Dem.: Sea p primo de la forma 4n+1.

Sea a solución de la congruencia $x^2+1 \equiv 0 \pmod p$, es decir, $a^2+1 \equiv 0 \pmod p$. Es claro que $p \nmid a$. Por el teorema 19 existen z,w enteros positivos tal que $az \equiv \pm w \pmod p$ con $0 \leq z \leq k-1$, $0 \leq w \leq k-1$ y k el menor entero tal que $k > \sqrt{p}$.

Por lo tanto $a^2z^2 \equiv w^2 \pmod p$

es decir $a^2z^2+z^2 = w^2+z^2 \pmod p$

así que $w^2+z^2=pt$ para algun $t \in N$.

Pero $w^2 \leq (k-1)^2 < p$, $z^2 \leq (k-1)^2 < p$

entonces $w^2+z^2=pt < 2p$

por lo tanto t=1.

Por último veremos que ésta representación es única.

En efecto, supongamos que $p= x^2+y^2=w^2+z^2$

entonces $p(y^2-z^2)=w^2y^2-z^2x^2=(wy+zx)(wy-zx)$

por lo tanto $wy \equiv \pm zx \pmod{p}$ 1

por otro lado tenemos que

$$p^2=(xw\pm yz)^2 + (wy+zx)^2 \quad .....2$$

si $wy=zx$. Como $(w,z)=(x,y)=1$ entonces $x=w$, $y=z$

Si $wy \neq zx$ entonces de 1 y 2 tenemos que

$|wy \mp zx|=p$ y $xw \pm yz=0$

Por lo tanto $xw=yz$

y entonces $y=z$, $y=w$.▲

Observemos lo siguiente: un entero ordinario de la forma 4k+3 no puede ser suma de dos cuadrados. El argumento es que, puesto que el cuadrado de un entero es congruente a 0 ó 1 (mod 4), la suma de cualesquiera dos cuadrados debe ser congruente a 0,1 ó 2 pero nunca a 3. Dicho de otra manera, los números primos de la forma 4k+1 y 2 son suma de 2 cuadrados.

TEOREMA 22: Los primos en $Z[i]$ son

I. 1+i y sus asociados

II. los factores a+bi de primos racionales de la forma 4n+1 y sus asociados

III. los primos racionales de la forma 4n+3 y sus asociados.

Dem.: Basta demostrar que 1+i es primo puesto que por definición resulta claro que los asociados de 1+i son primos.

Supongamos que $1+i=\alpha\beta$, entonces $N(\alpha)N(\beta)=N(1+i)=2$.

Por lo tanto, $N(\alpha)=1$ ó $N(\beta)=1$, consecuentemente α ó β, es asociado con 1, es decir, 1+i es primo.

II. Continuaremos determinando los enteros positivos los

cuales, vistos como enteros gaussianos son primos en $Z[i]$. Claramente deben ser primos racionales y deben ser impares puesto que $2=(1+i)(1-i)$. Así que tenemos que considerar -- los primos de la forma $4n+1$ y $4n+3$.

Sea p primo racional de la forma $4n+1$. Por el teorema 19 - existen a,b enteros positivos tales que $p=a^2+b^2$, entonces - $p=(a+bi)(a-bi)$ y $N(a\pm bi)=a^2+b^2=p > 1$. Por lo tanto p no es un primo en $Z[i]$.

Sin embargo, los factores $a+bi$ y $a-bi$ son primos.

En efecto, si $a+bi=\alpha\beta$, donde $N(\alpha) > 1$, $N(\beta) > 1$ entonces - $p=N(a+bi)=N(\alpha)N(\beta)$, lo cual es falso puesto que p es primo racional.

Por lo tanto, concluimos afirmando que los factores complejos de primos de la forma $4n+1$ $(n \geq 1)$, son primos.

III. Por último demostraremos que los primos racionales de la forma $4k+3$, vistos como enteros gaussianos, son primos - en $Z[i]$. En efecto, sea p primo racional tal que $p=4k+3$. Si p fuera producto de dos enteros gaussianos de norma ma-- yor que 1, entonces $p=(a+bi)(c+di)$

por lo tanto $N(p)=p^2=(a^2+b^2)(c^2+d^2)$, con $a^2+b^2 > 1$, $c^2+d^2 > 1$. Como p es primo entonces $p= a^2+b^2$. Esto último es falso para cualquier primo de la forma $4k+3$.

Así, hemos mostrado que los primos racionales de la forma - $4k+3$ son primos en $Z[i]$.

Es claro que no pueden existir otros primos complejos, porque si π fuera tal primo, entonces, en virtud de la unicidad de la descomposición de un entero gaussiano en primos,

π no debería ser un divisor primo de cualquier número racional. Pero $\pi\bar{\pi}=N(\pi)$ lo cual es falso.

FACTORIZACION DE UN ENTERO GAUSSIANO

Ahora vamos a mostrar un método por medio del cual, un entero gaussiano puede ser representado como el producto de primos.

Sea $N(z)=n$. Cualquier factor primo del número z es un factor primo de su norma $n=z\bar{z}$. Los factores primos gaussianos del entero positivo n, pueden encontrarse fácilmente obteniendo sus factores primos ordinarios.

$$\text{Sea } n=2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s} \quad \ldots\ldots\ldots\ldots (1)$$

donde los p_i's son primos de la forma $4t+1$[1] y los q_j's son primos de la forma $4t+3$. Sea π_j y $\bar{\pi}_j$, $j=1,\ldots,k$ los factores primos complejos conjugados del número p_j. Sea $\pi_j=a+bi$ y $\bar{\pi}_j=a-bi$; entonces $p_j=a^2+b^2$. Entonces la factorización de n en factores primos complejos es:

$$n=(-i)^{\alpha}(1+i)^{\alpha}\ \pi_1^{\alpha_1}\bar{\pi}_1^{\alpha_1}\pi_2^{\alpha_2}\bar{\pi}_2^{\alpha_2}\ldots\pi_k^{\alpha_k}\bar{\pi}_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2}\ldots q_s^{\beta_s} \quad \ldots\ldots (2)$$

puesto que $n=z\bar{z}$, entonces

$$z= i^{\delta}(1+i)^{\lambda}\pi_1^{\lambda_1}\bar{\pi}_1^{\lambda_1'}\bar{\pi}_2^{\lambda_2}\pi_2^{\lambda_2'}\ldots\pi_k^{\lambda_k}\bar{\pi}_k^{\lambda_k'} q_1^{\mu_1} q_2^{\mu_2}\ldots q_s^{\mu_s} \quad \ldots\ldots\ldots (3)$$

donde δ puede ser 1, 2, 3 ó 4 y $\lambda, \lambda_1, \lambda_1', \ldots, \lambda_k, \lambda_k', \mu_1, \ldots, \mu_s$ son enteros positivos.

Puesto que $N(\pi_j)=p_j$ y $N(q_j)=q_j^2$, tomando normas en (3)

$$N(z)=2^{\lambda} p_1^{\lambda_1+\lambda_1'} p_2^{\lambda_2+\lambda_2'}\ldots p_k^{\lambda_k+\lambda_k'} q_1^{2\mu_1} q_2^{2\mu_2}\ldots q_s^{2\mu_s}$$

comparando los exponentes de ésta última expresión y (1) obtenemos

$$\lambda=\alpha,\ \lambda_1+\lambda_1'=\alpha_1,\quad \lambda_2+\lambda_2'=\alpha_2,\ \ldots,\ \lambda_k+\lambda_k'=\alpha_k$$

(1) aquí p_k no denota el k-ésimo primo.

$2\mu_1=\beta_1$, $\mu_2=\beta_2$, . . . , $2\mu_s=\beta_s$

Esta última expresión muestra que los exponentes β_i deben ser pares. Por lo tanto, $\lambda=\alpha, \mu_1=\frac{1}{2}\beta_1$, $\mu_2=\frac{1}{2}\beta_2$, . . . , $\mu_s=\frac{1}{2}\beta_s$. Así los exponentes están determinados de forma única.

De lo anterior podemos concluir el siguiente resultado:

TEOREMA 21: Si un entero positivo n es la norma de un entero gaussiano, entonces en la factorización de n en primos racionales, los primos de la forma 4k+3 tienen exponentes pares.

Hasta ahora, hemos determinado los exponentes de los primos de la forma 4k+3. Sin embargo, para tener la factorización completa de z, aún debemos encontrar los exponentes con los cuales deberan aparecer en la factorización, los primos de la forma 4k+1, es decir, tenemos que determinar los números λ_j, λ'_j.

Para determinar los exponentes λ_j, λ'_j, donde j=1, . . . , k, usaremos otra regla que puede ser deducida como sigue:

Sea k_j el mayor exponente positivo para el cual $p_j^{k_j} | z$, entonces afirmamos que

$$\left.\begin{array}{l}\lambda_j=\alpha_j-k_j \\ \lambda'_j=k_j\end{array}\right\} \text{Si } p_j^{k_j}\pi_j | z \quad , \quad \left.\begin{array}{l}\lambda'_j=\alpha_j-k_j \\ \lambda_j=k_j\end{array}\right\} \text{Si } p_j^{k_j}\pi_j \nmid z$$

Demostraremos ésta última afirmación:

Por definición del exponente k_j tenemos que $\frac{z}{p_j^{k_j}}$ no puede ser dividido simultaneamente por π_j y $\bar{\pi}_j$, porque si ésto sucediera, como $(\pi_j, \bar{\pi}_j)=1$, entonces $p_j=\pi_j\bar{\pi}_j$ debe dividir a $\frac{z}{p_j^{k_j}}$, es decir, $p_j^{k_j+1} | z$, lo cual es falso puesto que k_j es el mayor entero positivo tal que $p_j^{k_j} | z$.

Consecuentemente si $\pi_j \mid \frac{z}{p_j^{k_j}}$, entonces $\bar{\pi}_j \nmid \frac{z}{p_j^{k_j}}$.

Como $p_j^{k_j} = \pi_j^{k_j}\,\bar{\pi}_j^{k_j}$, haciendo uso de que

$$z = i^{\delta}(1+i)^{\lambda}\pi_1^{\lambda_1}\bar{\pi}_1^{\lambda'_1}\cdots\pi_K^{\lambda_K}\bar{\pi}_K^{\lambda'_K}q_1^{\mu_1}\cdots q_s^{\mu_s}$$

Concluimos que $\lambda'_j = k_j$, entonces $\lambda_j = \alpha_j - k_j$. Si el número $\frac{z}{p_j^{k_j}}$ no es dividido por π_j, entonces $\lambda_j = k_j$ y $\lambda'_j = \alpha_j - k_j$.

Por último, el exponente δ se puede encontrar fácilmente haciendo una simple división de z y el producto de los factores primos los cuales sus exponentes ya han sido determinados.▲

Para finalizar, veamos algunos ejemplos:

1.- Sea $z=22+7i$. Entonces tenemos que:

$N(z) = 484 + 49 = 533 = 13(41)$, $p_1 = 13 = 2^2+3^2$, $p_2 = 41 = 4^2+5^2$

Por lo tanto $z = i^{\delta}\pi_1^{\lambda_1}\bar{\pi}_1^{\lambda'_1}\pi_2^{\lambda_2}\bar{\pi}_2^{\lambda'_2}$ $\quad \alpha_1 = 1 \quad \alpha_2 = 1$

donde $\pi_1 = 2+3i$, $\quad \bar{\pi}_1 = 2-3i$, $\quad \pi_2 = 4+5i$, $\quad \bar{\pi}_2 = 4-5i$.

sólo nos falta encontrar los exponentes $\lambda_1, \lambda'_1, \lambda_2, \lambda'_2$

Como $p_1 \nmid z$ y $p_2 \nmid z$ entonces $k_1 = k_2 = 0$

Ahora veamos si $\pi_1 \mid z$ ó $\bar{\pi}_1 \mid z$

$\frac{z}{\pi_1} = \frac{22+7i}{2+3i} = 5-4i$ así que $\bar{\pi}_1 \nmid z$ y por lo tanto

$\lambda_1 = 1$, $\lambda'_1 = 0$

Similarmente para calcular los números λ_2, λ'_2

$\frac{z}{\pi_2} = \frac{22+7i}{4+5i} = 3-2i$, así que $\bar{\pi}_2 \nmid z$ y por lo tanto

$\lambda_2 = 1-0 = 1$, $\quad \lambda'_2 = 0$

Por lo tanto $z = i^{\lambda}(2+3i)(4+5i)$

por un cálculo elemental obtenemos que $\lambda=3$, es decir,

$$z=i^3(2+3i)(4+5i)$$

2.- Sea $z=19+17i$ entonces tenemos que:

$N(z)=361+289=650=2(5^2)(13)=2p_1^2 p_2$

$p_1=1^2+2^2$, $p_2=2^2+3^2$, consecuentemente $z=i^{\lambda}(1+i)\pi_1^{\lambda_1}\bar{\pi}_1^{\lambda'_1}\pi_2^{\lambda_2}\bar{\pi}_2^{\lambda'_2}$

donde $\pi_1=1+2i$, $\bar{\pi}_1=1-2i$, $\pi_2=2+3i$, $\bar{\pi}_2=2-3i$

puesto que $5 \not| z$ y $13 \not| z$ entonces $k_1=k_2=0$

Además $\pi_1 \not| 19+17i$, es decir, $\lambda_1=0$ $\lambda'_1=2$

también $\pi_2 \not| 19+17i$, es decir, $\lambda_2=0$ $\lambda'_2=1$

por lo tanto $z=i^{\lambda}(1-2i)^2(2-3i)(1+i)$

Por un cálculo elemental tenemos $\lambda=2$, es decir,

$$z=i^2(1+i)(1-2i)^2(2-3i)$$

3.- Sea $z=10+100i$, podemos escribir $z=10(1+10i)$

como $10=-i(1+i)^2(1+2i)(1-2i)$ entonces es suficiente encontrar la factorización de $1+10i$; pero $N(1+10i)=101$ es primo racional, entonces por el teorema 14 tenemos que $1+10i$ es primo en $Z[i]$.

Por lo tanto $z=-i(1+i)^2(1+2i)(1-2i)(1+10i)$.

CAPITULO III

$Z[\rho]$

Sea $\rho \in \mathbb{C}$ y $\rho^2+\rho+1=0$

Entonces $\rho = e^{\frac{2}{3}\pi i} = \frac{1}{2}(-1+i\sqrt{3})$ y $\rho^2 = \frac{1}{2}(-1-i\sqrt{3}) = e$

Definimos $Z[\rho]=\{a+b\rho / a,b \in Z,\ \rho^2+\rho+1=0\}$

Si $\alpha=a+b\rho$, es inmediato de $\rho^2+\rho+1=0$ que:

$$a+b\rho=a-b-b\rho^2 \quad \text{ó} \quad a+b\rho^2=a-b-b\rho$$

Por lo tanto, los enteros de $Z[\rho]$ son de la forma $a+b\rho$ ó $a+b\rho^2$, con $a,b \in Z$.

Si $\alpha=a+b\rho$, definimos la norma de α como

$$N(\alpha)=(a+b\rho)(a+b\rho^2)=a^2-ab+b^2$$

Notemos que $N(\alpha)$ es un entero positivo, puesto que $a^2-ab+b^2=(a-\frac{1}{2}b)^2+\frac{3}{4}b^2$, entonces $N(\alpha)=0$ si y sólo si $\alpha=0$.

Es fácil checar que $N(\alpha\beta)=N(\alpha)N(\beta)$ y más generalmente

$$N(\Pi\alpha_i)=\Pi N(\alpha_i) \qquad (i=1,\ldots,n)$$

Definición: Sean $\alpha,\beta \in Z[\rho]$. Decimos que $\alpha \mid \beta$ si existe $\gamma \in Z[\rho]$ tal que $\beta=\alpha\gamma$.

TEOREMA 1: Sean $\alpha,\beta \in Z[\rho]$. Si $\alpha \mid \beta$ entonces $N(\alpha) \mid N(\beta)$ ▲

Definición: Sea $\alpha=a+b\rho$. Diremos que α es unidad si $\alpha \mid 1$.

TEOREMA 2: Si α es unidad entonces $N(\alpha)=1$ ▲

TEOREMA 3: Sea $\alpha \in Z[\rho]$. Si $N(\alpha)=1$ entonces α es unidad ▲

El Teorema 3 nos indica que las únicas unidades de $Z[\rho]$ son

$$\pm 1,\ \pm\rho,\ \pm(1+\rho).$$

Sea $\alpha \in Z[\rho]$. Diremos α y β son asociados si $\alpha \mid \beta$ y $\beta \mid \alpha$.

TEOREMA 4: Si α y β son asociados, entonces $N(\alpha)=N(\beta)$ ▲

Ahora estamos en posibilidades de afirmar cuantos asociados tiene α.

TEOREMA 5: Sea $\alpha \in Z[\rho]$, $\alpha \neq 0$. Entonces α tiene exactamente 6 asociados.▲

TEOREMA 6: Sea $\alpha \in Z[\rho]$ tal que $N(\alpha)$ es un primo ordinario. Entonces α es primo en $Z[\rho]$.

Dem.: Supongamos que $N(\alpha)=p$, $\alpha=\mu\beta$ con p primo ordinario.

Entonces $p=N(\alpha)=N(\mu)N(\beta)$.

Por lo tanto $N(\mu)=1$ ó $N(\beta)=1$, es decir, α es primo en $Z[\rho]$.▲

Claramente $1-\rho$ es primo en $Z[\rho]$ puesto que $N(1-\rho)=3$.

El inverso del Teorema 6 es falso, por ejemplo; 7 es primo racional, pero no es primo en $Z[\rho]$.

TEOREMA 7: Sean $\alpha, \beta \in Z[\rho]$, $\beta \neq 0$. Existen $k, \alpha_1 \in Z[\rho]$ tal que

$$\alpha=k\beta+\alpha_1 \qquad N(\alpha_1) < N(\beta).$$

Dem.: Sea $\alpha=a+b\rho$, $\beta=c+d\rho$

$$\frac{\alpha}{\beta} = \frac{a+b\rho}{c+d\rho} = \frac{(a+b\rho)(c+d\rho^2)}{(c+d\rho)(c+d\rho^2)} = \frac{ac+bd-ad+(bc-ad)\rho}{c^2-cd+d^2} = R + S$$

$R, S \in \mathbb{Q}$

Sean x,y enteros ordinarios tal que

$$|R-x| \leq \frac{1}{2} \quad , \quad |S-y| \leq \frac{1}{2} \quad \text{entonces}$$

$$N\left(\frac{\alpha}{\beta} - (x+y\rho)\right) = N(R+S\rho-(x+y\rho)) = N(R-x+(S-y)\rho) =$$

$$(R-x)^2-(R-x)(S-y)+(S-y)^2 \leq \frac{3}{4}$$

Sea $k=x+y\rho$, $\alpha_1=\alpha-k\beta$

$$N(\alpha_1)=N(\alpha-k\beta)=N(\beta)N\left(\frac{\alpha}{\beta}-k\right) \leq \frac{3}{4} N(\beta) < N(\beta).$$▲

El Teorema Fundamental de la Aritmética también es válido en $Z[\rho]$

TEOREMA 8: (Teorema Fundamental de la Aritmética).

La expresión de un entero de $Z[\rho]$ como un producto

de primos es única.

Los primos de $Z[\rho]$

TEOREMA 9: Sea $p=3n+1$ primo ordinario. Entonces existen a,b - enteros positivos tal que $p=a^2-ab+b^2$.

Observemos que para todo $a,b \in Z$ $\quad a^2-ab+b^2 \equiv 0,1 \pmod 3$.

Por lo tanto todo entero positivo de la forma $3n+2$ no se puede - expresar de la forma a^2-ab+b^2, puesto que $3n+2 \equiv 2 \pmod 3$.

TEOREMA 10: Los primos de $Z[\rho]$ son

I. $1-\rho$ y sus asociados,

II. Los primos racionales de la forma $3n+2$ y sus asociados.

III. Los factores $a+b\rho$ de los primos racionales de la forma $3n+1$,

Dem.: I. Aplicando el Teorema 6 obtenemos que $N(1-\rho)=3$. Por lo tanto $1-\rho$ es primo de $Z[\rho]$,

II. Sea $p=3n+2$ primo ordinario. Si p fuera producto de -- dos enteros de $Z[\rho]$ con norma mayor que 1 tendriamos que

$p=(a+b\rho)(c+d\rho)$ con $N(a+b\rho) > 1$, $N(c+d\rho) > 1$

Por lo tanto $N(p)=p^2=(a^2-ab+b^2)(c^2-cd+d^2)$

Como p es primo racional y $a^2-ab+b^2 > 1$, $c^2-cd+d^2 > 1$ entonces $p=a^2-ab+b^2$ lo cual es falso.

III. Sea $p=3n+1$ primo ordinario. Entonces por el Teorema 9 tenemos que

$$p=(a+b\rho)(a+b\rho^2)$$

Debemos mostrar que los factores $a+b\rho$ y $a+b\rho^2$ son pri

primos de $Z[\rho]$.

En efecto, puesto que $p=N(a+b\rho)=N(a+b\rho^2)$. Entonces aplicando el Teorema 6 obtenemos que $a+b\rho$ y $a+b\rho^2$ - son primos de $Z[\rho]$.▲

Ahora dirigiremos nuestra atención a los primos de $Z[\rho]$ que son primos ordinarios de la forma $3n+1$.

Por el Teorema 9 sabemos que existen $a,b \in Z$ tal que

$$a^2-ab+b^2 = p = 3n+1 \qquad .....(1)$$

Si a y b son impares, podemos introducir b' definida por $b=a-b'$ donde claramente b' es par.

Sustituyendo en 1 obtenemos que

$$p=3n+1=a^2-ab+b^2 \mp a^2-ab'+b'^2$$

Como en los dos casos obtenemos números de la misma forma entonces podemos escoger libremente b par, es decir

$$b=2\beta \quad (\beta \in Z)$$

Por lo tanto de (1) obtenemos

$$a^2-ab+b^2=(a-\frac{b}{2})^2+\frac{3}{4}b^2=(a-\beta)^2+3\beta^2$$

Si $c=a-\beta$ entonces

$$a^2-ab+b^2=c^2+3\beta^2=3n+1=p \qquad .....(2)$$

De la igualdad (2) se sigue que $3 \nmid c$, es decir

$$c=3k+1 \text{ ó } c=3k+2$$

También podemos afirmar que en (2), n no puede ser impar porque si lo fuera, entonces p es par.

Por lo tanto podemos escribir $n=2m$. Así que (2) se convierte en

$$c^2+3\beta^2=p=6m+1 \qquad .....(3)$$

Regresando a la forma $a+b\rho$ tenemos que

$$a+b\rho=a+b\left(-\frac{1}{2}+\frac{i\sqrt{3}}{2}\right)=a-\frac{b}{2}+\frac{ib}{2}\sqrt{3}=a-\beta+i\beta\sqrt{3}=c+i\beta\sqrt{3}.$$

y por lo tanto $c+i\beta\sqrt{3}$ es primo en $Z[\rho]$ cuando $c^2+3\beta^2=6m+1=p$.

Por ejemplo: $1^2+3(2^2)=13=6(2)+1$ donde $c=1$, $\beta=2$ y $1+2i\sqrt{3}$ es un primo en $Z[\rho]$ junto con sus asociados.

Considerando la expresión $3(1\cdot 2\cdot \ldots \cdot p)^2+1$ (p primo ordinario de la forma 6m+1) se puede demostrar que existe un número infinito de primos de la forma 6m+1. (Véase el Teorema de Dirichlet).

Existen ecuaciones cuadráticas que representan una sucesión finita de primos de la forma 6m+1, por ejemplo,

$$y=6x^2+6x+31$$

la cual, para $x=0,1,\ldots,28$ representa 29 primos de la forma 6m+1 comprendidos entre 31 y 4909; remplazando x por x-29 obtenemos la siguiente ecuación:

$$y_1=6x^2-342x+4903$$

la cual representa 58 primos de la forma 6m+1.

Entre 1 y 10^4 existen 1229 primos de los cuales 611 son de la forma 6m+1.

El propósito de ésta sección es descomponer los primos de la forma 6m+1 en la forma $c^2+3\beta^2$ y representarlos en el plano complejo (c,β).

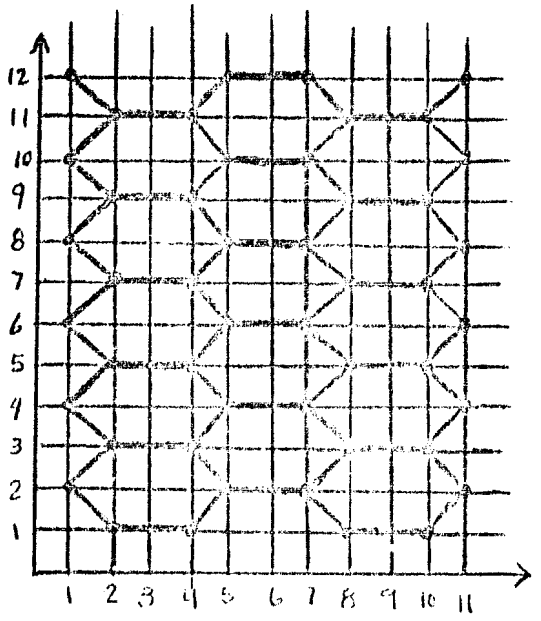
La relación $6m+1=c^2+3\beta^2$ nos indica que

1) $3 \nmid c$

2) Si c es par, entonces β es impar

3) Si c es impar, entonces β es par.

Ahora grafiquemos en el plano (c,β) todos los números de la forma 6m+1, primos ó no, que satisfacen 1),2) y 3) y observemos que están situados sobre los vértices de exágonos.



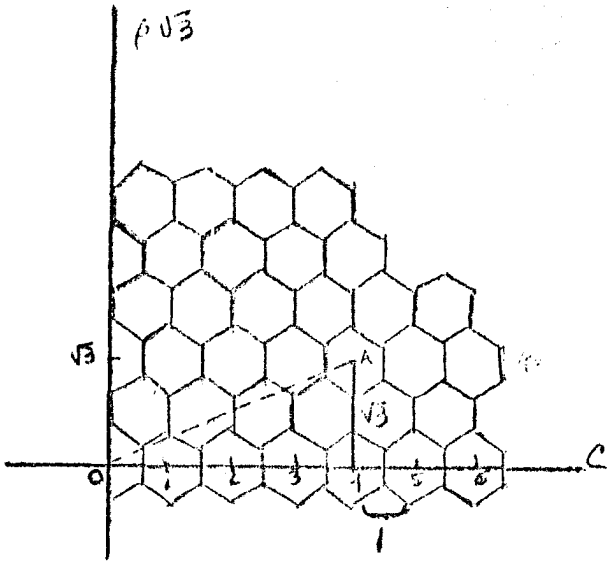
Al final , damos una tabla de las descomposiciones de los primos de la forma 6m+1 en la forma $c^2+3\beta^2$.

La primera columna proporciona los primos p y la segunda proporciona los valores c y β.

La representación de los primos $c+i\beta\sqrt{3}$ de $Z[\rho]$ en el plano complejo es efectuada de manera más natural, primero tapizando todo el plano con una red de exágonos regulares adyacentes donde la distancia de dos centros de exágonos situados horizontalmente es 1 y la distancia más corta entre dos centros de dos exágonos situados verticalmente es $\sqrt{3}$. Es fácil ver que los lados de cada exágono miden $\frac{1}{\sqrt{3}}$.

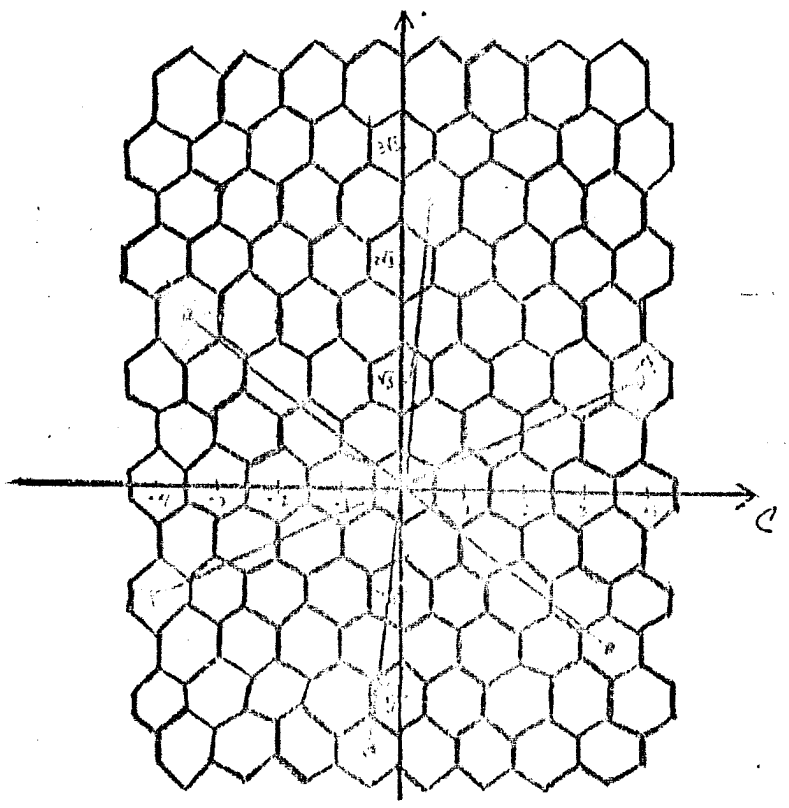
En la siguiente figura el punto A representa el primo complejo $4+i\sqrt{3}$, su norma $N(4+i\sqrt{3})=(4+i\sqrt{3})(4-i\sqrt{3})=19$ es un primo ordina-

rio de la forma 6m+1.



Observemos que la norma definida en Z[ρ] coincide con la norma - definida en Z[i] .

El exágono que tiene como centro al punto A ha sido sombreado -- junto con sus asociados $\pm(4+\sqrt{3})$, $\pm\rho(4+i\sqrt{3})$, $\pm\rho^2(4+i\sqrt{3})$. Estos - asociados también pueden ser encontrados rotando al punto $4+i\sqrt{3}$ ángulos de 60°, 120°, 180°, 240°, 300°

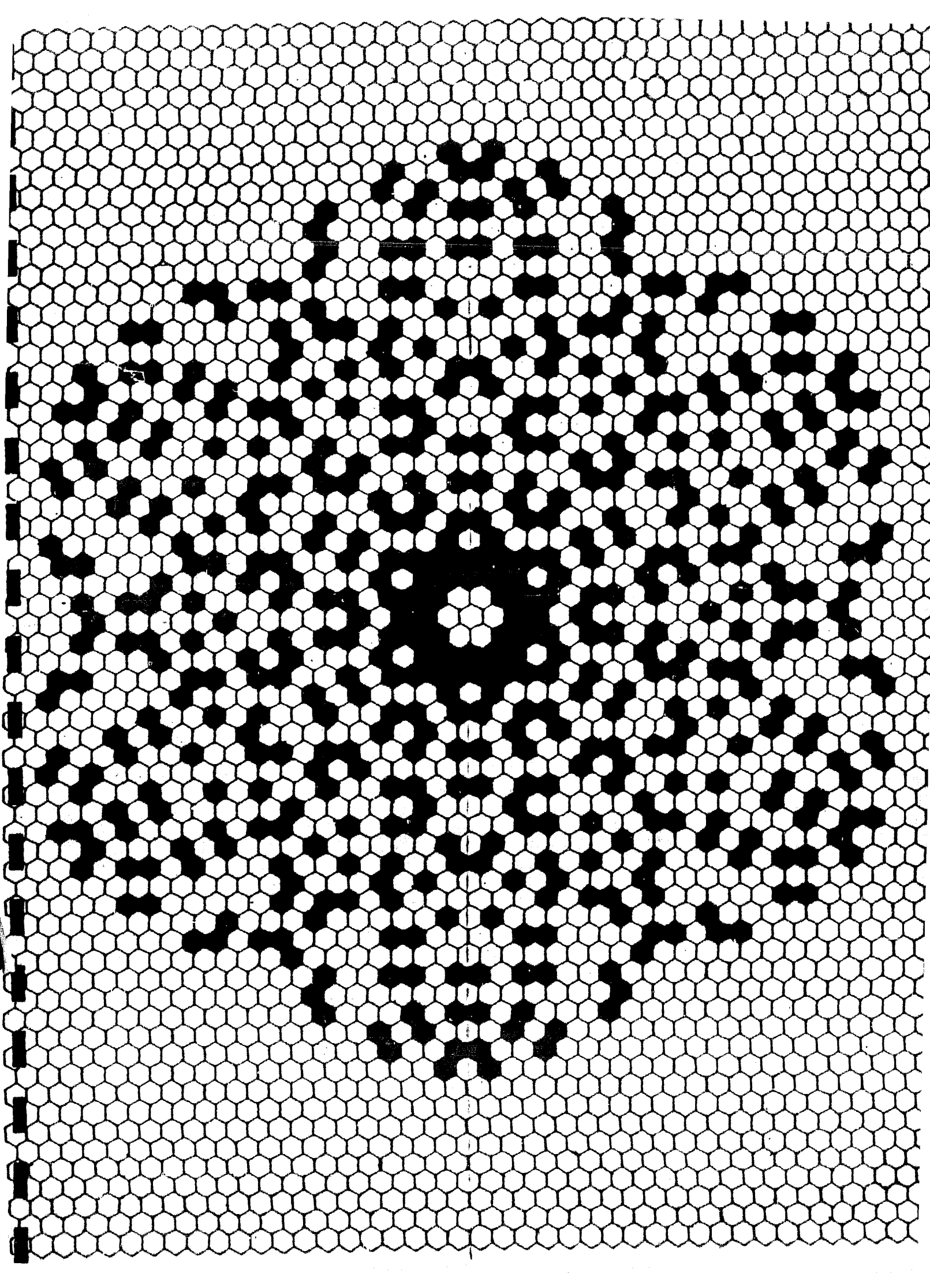


De ésta manera construimos el Diagrama 1 el cual muestra clara-- mente las simetrías de puntos rotados 60°,120°, 180°,240°, 300°. El centro de éste diagrama es ilustrado en la siguiente hoja.

Descomposición de primos de la forma $6m+1$ en la forma $c^2+3\beta^2$

p	c,β	p	c,β	p	c,β	p	c,β	p	c,β	p	c,β
7	2,1	571	8,13	1231	34,5	1951	38,13	2713	19,28	3517	7,34
13	1,2	577	23,4	1237	35,2	1987	20,32	2710	14,29	3529	59.4
19	4,1	601	13,12	1249	7,20	1993	35,16	2731	52,3	3541	29,30
31	2,3	607	10,13	1279	14,19	1999	26,21	2749	7,30	3547	32,29
37	5,2	613	5,14	1291	28,13	2011	44,5	2767	38,21	3559	26,31
43	4,3	619	16,11	1297	23,16	2017	17,24	2791	46,15	3571	52,17
61	7,2	631	22,7	1303	34,7	2029	1,26	2797	47,14	3583	50,19
67	8,1	643	20,9	1321	11,20	2053	5,26	2803	44,17	3607	58,9
73	5,4	661	19,10	1327	2,21	2083	44,7	2833	49,12	3613	55,14
79	2,5	673	25,4	1381	87,2	2089	19,24	2851	52,7	3631	38,27
97	7,4	691	4,15	1399	34,9	2113	41,12	2857	53,4	3637	13,34
103	10,1	709	11,14	1423	10,21	2131	16,25	2887	2,31	3643	56,13
109	1,6	727	22,9	1429	29,14	2137	37,16	2917	53,6	3673	59,8
127	10,3	733	25,6	1447	38,1	2143	46,3	2953	35,24	3691	4,35
139	8,5	739	8,15	1453	1,22	2161	31,20	2971	28,27	3697	25,32
151	2,7	751	26,5	1459	28,15	2179	44,9	3001	53,8	3709	41,26
157	7,6	757	13,14	1471	38,3	2203	4,27	3019	44,19	3727	58,11
163	4,7	769	1,16	1483	20,19	2221	47,2	3037	55,2	3733	61,2
181	13,2	787	28,1	1489	17,20	2239	34,19	3049	43,20	3739	8,35
193	1,8	811	28,3	1531	32,13	2251	8,27	1061	19,30	3769	61,4
100	14,1	823	26,7	1543	26,17	2269	41,14	3067	52,11	3793	55,16
211	8,7	829	23,10	1559	31,14	2281	43,12	3079	14,31	3823	50,21
223	14,3	853	29,2	1567	22,19	2287	10,27	3109	53,10	3847	62,1
229	11,6	859	28,5	1579	16,21	2293	29,22	3121	7,32	3853	49,22
241	7,8	877	17,14	1597	25,18	2311	38,17	3163	57,3	3877	43,27
271	14,5	883	4,17	1609	29,16	2341	37,18	3169	49,16	3889	1,36
277	13,6	907	20,13	1621	13,22	2347	32,21	3181	47,18	3907	32,31
283	16,3	919	26,9	1627	40,3	2371	28,23	3187	40,23	3919	32,5
307	8,9	937	13,16	1657	35,12	2377	5,28	3217	55,8	3931	16,35
313	11,8	967	10,17	1663	34,13	2383	14,27	3229	23,30	3943	26,33
331	16,5	991	22,13	1669	37,10	2389	19,26	3253	35,26	3967	38,29
337	17,4	997	5,18	1693	41,2	2437	43,14	3259	44,21	4003	56,17
349	7,10	1009	31,4	1699	32,15	2467	40,17	3271	2,33	4021	61,10
367	2,11	1021	7,18	1723	20,21	2473	11,28	3301	43,22	4027	52,21
373	19,2	1033	29,8	1741	17,22	2503	50,1	3307	28,29	4051	28,33
379	4,11	1039	26,11	1747	40,7	2521	13,28	3313	31,28	4057	13,36
397	17,6	1051	32,3	1753	5,24	2539	4,29	3319	38,25	4093	25,34
409	19,4	1063	14,17	1759	26,19	2551	26,25	3331	8,33	4099	64,1
421	11,10	1069	31,6	1777	7,24	2557	23,26	3343	34,27	4111	2,37
433	1,12	1087	2,19	1783	14,23	2593	49,8	3361	17,32	4129	49,24
439	14,9	1093	11,18	1789	41,6	2617	43,16	3373	49,18	4253	61,12
457	5,12	1117	23,14	1801	37,12	2647	50,7	3391	58,3	4159	22,35
463	10,11	1123	16,17	1831	34,15	2659	28,25	3433	19,32	4177	17,36
487	22,1	1129	19,16	1861	43,2	2671	22,27	3457	55,12	4201	43,28
499	16,9	1153	31,8	1867	28,19	2677	35,22	3463	14,33	4219	56,19
523	4,13	1171	32,7	1873	41,8	2683	40,19	3469	1,34	4231	58,17
541	23.2	1201	1,20	1879	2,25	2689	31,24	3499	56,11	4243	64,7
547	20,7	1213	25,14	1933	31,18	2707	52,1	3511	58,7	4261	53,22

p	c,β	p	c,β	p	c,β	p	c,β	p	c,β	p	c,β
4273	65,4	5227	52,29	6211	68,23	7177	37,44	8191	46,45	9091	4,55
4297	35,32	5233	71,8	6217	67,24	7207	2,49	8209	49,44	9103	26,53
4327	38,31	5281	47,32	6229	77,10	7213	79,18	8221	89,10	9109	19,54
4339	64,9	5323	56,27	6247	58,31	7219	4,49	8233	11,52	9127	50,47
4357	5,38	5347	28,39	6271	14,45	7237	85,2	8263	86,17	9133	95,6
4363	16,37	4507	70,13	6277	53,34	7243	56,37	8269	79,26	9151	74,35
4423	34,33	5413	11,42	6301	73,18	7297	65,32	8287	22,51	9157	53,46
4441	37,32	5419	64,21	6337	23,44	7309	31,46	3293	91,2	9181	41,50
4447	58,19	5431	62,23	6343	74,17	7321	83,12	8311	82,23	9187	68,39
4483	40,31	5437	73,6	6361	77,12	7333	85,6	8317	55,42	9199	94,11
4507	20,37	5443	20,41	6367	62,29	7351	74,25	8329	91,4	9241	83,28
4513	25,36	5449	61,24	6373	5,46	7369	59,36	8353	89,12	9277	23,54
4519	62,15	5479	74,1	6379	52,35	7393	71,28	8377	67,36	9293	80,31
4549	43,30	5503	74,3	6379	7,46	7411	28,47	8389	91,6	9319	46,49
4561	47,28	5521	73,8	6421	61,30	7417	85,9	8419	88,15	9337	35,52
4567	2,39	5527	22,41	6427	80,3	7459	16,49	8431	2,53	9343	94,13
4591	22,37	5557	35,38	6451	76,15	7477	83,14	8443	4,53	9349	43,50
4597	67,6	5563	4,43	6469	11,46	7489	41,44	8461	31,50	9391	62,43
4603	64,13	5569	41,36	6481	41,40	7507	68,31	8467	92,1	9397	77,34
4621	17,38	5581	17,42	6529	73,20	7537	25,48	8521	61,40	9403	40,51
4639	46,29	5623	74,7	6547	80,7	7459	7,50	8527	10,53	9421	97,2
4651	68,3	5641	29,40	6553	59,32	7561	67,32	8539	92,5	9433	5,56
4657	65,12	5647	10,43	6571	32,43	7573	35,46	8563	44,47	9439	58,45
4663	10,39	5653	19,42	6577	65,28	7591	82,17	8581	91,10	9463	70,39
4723	56,23	5659	56,29	6607	50,37	7603	20,49	8599	82,25	9511	94,15
4729	29,36	5683	64,23	6619	64,29	7621	11,50	8623	14,53	9547	92,19
4759	14,39	5689	67,20	6637	17,46	7639	86,9	3629	77,30	9601	97,3
4783	26,37	5701	37,38	6661	37,42	7669	13,50	8641	23,52	9613	95,14
4789	61,10	5737	43,36	6673	79,12	7681	73,28	8647	38,49	9619	88,25
4801	1,40	5743	14,43	6679	46,39	7687	22,49	8677	85,22	9631	98,3
4813	65,14	5749	61,26	6691	9,47	7699	56,39	8689	89,16	9643	64,43
4831	34,35	5779	76,1	6703	34,43	7717	37,46	8707	92,9	9649	89,24
4861	23,38	5791	46,35	6709	19,46	7723	30,21	8713	91,12	9661	73,38
4903	70,1	5821	23,42	6733	49,38	7741	71,30	8719	86,21	9679	98,5
4909	47,30	5827	28,41	6763	80,11	7753	29,48	8731	68,37	9697	17,56
4933	59,22	5839	74,11	6781	73,22	7759	86,11	8737	25,52	9721	53,48
4951	58,23	5851	76,5	6793	61,32	7789	17,50	8761	43,48	9733	91,22
4957	25,38	5857	/,44	6823	14,47	7867	8,51	8779	52,45	9739	44,51
4969	13,40	5869	49,34	6829	79,14	7873	31,48	8803	40,49	9769	19,56
4987	68,11	5881	53,32	6841	67,38	7879	26,49	8821	67,38	9781	67,42
4993	65,16	5923	76,7	6871	82,7	7927	58,39	8839	94,1	9787	92,21
4999	46,31	5953	65,24	6883	16,47	7933	89,2	8863	94,3	9811	8,57
5011	56,25	6007	38,39	6907	80,13	7951	62,37	8887	64,41	9817	77,36
5023	50,29	6037	77,6	6949	59,34	7963	76,27	8893	89,18	9829	59,46
5059	4,41	6043	44,37	6961	7,48	7993	85,16	8923	80,29	9859	28,55
5077	67,14	6067	32,41	6967	82,9	8011	44,45	8929	71,36	9871	38,53
5101	49,30	6073	61,28	6991	38,43	8017	47,44	8941	79,30	9883	76,37
5107	8,41	6079	2,45	6997	83,6	8053	61,38	8971	92,13	9901	49,50
5113	35,36	6091	4,45	7027	20,47	8059	16,51	9001	77,32	9907	52,49
5119	38,35	6121	77,8	7039	58,35	8069	83,20	9007	70,37	9931	88,27
5167	62,21	6133	29,42	7057	73,24	8101	53,42	9013	61,42	9949	89,26
5179	64,19	6151	74,15	7069	71,26	8161	7,52	9043	76,33	9967	98,11
5197	56,18	6163	40,39	7129	77,20	8167	70,33	9049	91,16	9973	35,54
5209	59,24	6199	34,41	7159	46,41	8179	56,41	9067	88,21		



CAPITULO IV

PRESENTACION DEL TEOREMA DE LOS NUMEROS PRIMOS

Examinando detenidamente una tabla de números primos encontramos que están distribuidos de manera muy irregular. Las tablas muestran grandes separaciones entre ellos. Por ejemplo, el primo 370,261 tiene 111 números compuestos a su derecha. No existen primos entre 20,831,323 y 20,831,533.

Es fácil demostrar que existen grandes hoyos entre los primos. Sin embargo existen primos consecutivos p_n y p_{n+1} tal que $p_{n+1}-p_n=2$. Este tipo de primos son conocidos como primos gemelos. Existen aproximadamente 1,000 pares de éstos primos menores que 100,000 y 8,000 aproximadamente menores que 1,000,000. Los más grandes conocidos en la actualidad son $76(3^{139})-1$ y $76(3^{139})+1$. Muchos matemáticos piensan que existe un número infinito de ellos, sin embargo, ésta afirmación aún no ha sido demostrada.

Una de las razones de la irregularidad en la distribución de primos es que no existe una fórmula simple que los reproduzca en su totalidad. J.P.Jones y otros autores en su artículo "Diophantine Representation of the set of Prime Number", American Mathematical Montnly 83,1976, dicen que: el conjunto de los primos coincide con el conjunto de valores positivos que toma el polinomio:

$$(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2-[2n+p+q+z-e]^2$$
$$-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)$$
$$y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2$$
$$+1-(x+cu)^2]^2-[n+1+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p$$
$$+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2-[q+y(a-p-1)+s(2ap-2a-p^2-$$
$$2p-2)-x]^2-[z+pl(a-p)+r(2ap-p^2-1)-pm]^2\}.$$

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

Algunas ecuaciones simples reproducen una infinidad de primos, recordemos que el Teorema de Dirichlet el cual fue tratado en el cap. I. Dirichlet mostró que si a,2b,c no tienen un factor primo en común, entonces el polinomio cuadrático en dos variables $ax^2+2bxy+cy^2$ representa un número infinito de primos cuando x,y - son enteros positivos. En 1947 el matemático W. H. Mill demostró que existe algún número A mayor que 1 pero no entero tal que;

$[A^{3^x}]$ es primo para toda x=1,2,3,...

Entendiendo que $[A^{3^x}]$ es el mayor entero menor ó igual que A^{3^x}. - Desafortunadamente sólo demostró que A existe.

Los comentarios anteriores ilustran la irregularidad de la distribución de los primos.

En el siglo pasado la frecuencia de disminución de pri-- mos fué objeto de muchas especulaciones. Para estudiar ésta distribución consideremos la función $\pi(x)$ definida como;

$\pi(x)$=número de primos p que satisfacen $2 \leq p \leq x$.

En la siguiente hoja proporcionamos una tabla de $\pi(x)$ - comparada con $\frac{x}{\log x}$ donde log x es el logaritmo natural de x.

Gauss y Legendre propusieron independientemente que para x muy grande la razón $\frac{\pi(x)\log x}{x}$ se aproxima a 1 y conjetura- ron que éste cociente debe ser 1 cuando $x \to \infty$. El problema de decidir la validez o falsedad de ésta conjetura atrajo la atención de eminentes matemáticos por más de 100 años.

En 1851 Chébyshev logra demostrar que existen números positivos c_1 y c_2 tal que

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} \quad \text{para toda } x \geq 2.$$

Por fin en el año 1896 J. Hadamard y C.J. de la Vallée Poussin demuestran independientemente que

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$$

Este resultado es conocido como "Teorema de los números primos".

x	$\pi(x)$	$\frac{x}{\log x}$	$\pi(x) \div \frac{x}{\log x}$
10	4	4.3	0.93
10	25	21.7	1.15
10	168	144.9	1.16
10	1,229	1,086	1.11
10	9,552	8,666	1.10
10	78,498	72,464	1.08
10	664,579	621,618	1.07
10	5,761,455	5,434,780	1.06
10	50,847,534	48,309,180	1.05
10^{10}	455,052,512	434,294,482	1.048

PROPIEDADES ELEMENTALES DE $\pi(x)$

Admitamos sin demostración el siguiente resultado:

TEOREMA 1: $\lim_{x \to \infty} \pi(x) = +\infty$.

El Teorema 1 nos indica que existe un número infinito de números primos.

TEOREMA 2: $\pi(x) \geq \dfrac{\log x}{2 \log x}$, $x=1,2,\ldots$

Dem.: Por el Teorema 25 del cap. I sabemos que $x=k^2\ell$, donde --- k y ℓ son enteros positivos determinados en forma única y ℓ libre de cuadrados. Para cada uno de los números ---- $1,2,\ldots,x$, $k^2\ell \leq x$ implica que $k^2 \leq x$.

Por lo tanto $k \leq \sqrt{x}$. Consecuentemente el número k puede - formar a lo más $\sqrt{x}$ valores diferentes.

El número ℓ, por ser libre de cuadrados y menor que x, pue de ser representado como producto de primos de tal forma - que cada uno de ellos no exceda a x, es decir, ℓ se puede expresar como producto de primos distintos de la sucesión $p_1, p_2, \ldots p_{\pi(x)}$. El número de tales productos (incluyendo al 1) es $2^{\pi(x)}$. Consecuentemente el número ℓ puede tomar a lo más $2^{\pi(x)}$ valores diferentes. Por lo tanto, el número de -- productos $k^2\ell \leq x$ es a lo más $\sqrt{x}2^{\pi(x)}$. Puesto que cualquier número menor ó igual que x es representable como tal producto, tenemos que $x \leq \sqrt{x}2^{\pi(x)}$, entonces $\sqrt{x} \leq 2^{\pi(x)}$, es decir, $\log \sqrt{x} \leq \pi(x) \log 2$, por lo tanto

$$\frac{\log x}{2\log 2} \leq \pi(x) \blacktriangle$$

Corolario: Sea p_n el n-ésimo primo. Entonces $p_n < 2^{2n}$.

Dem.: Puesto que $\pi(p_n)=n \geq \dfrac{\log p_n}{2\log 2}$ entonces

$$2n\log 2 \geq \log p_n \text{ , es decir, } 2^{2n} \geq p_n$$

pero 2^{2n} es un número compuesto, por lo tanto

$$2^{2n} > p_n \blacktriangle$$

TEOREMA 3: Si $M > 1$ y $p_1, p_2, \ldots, p_s$ son todos los primos en $\{1,2,\ldots,M\}$, entonces

$$\frac{1}{n} < \frac{1}{\prod(1-\frac{1}{p_i})}$$

Dem.: Es claro que

$$\frac{1}{1-\frac{1}{p}} = 1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\ldots$$

por lo tanto

$$\frac{1}{(1-\frac{1}{p_i})} = \frac{1}{p_i} = \frac{1}{n} > \frac{1}{n}$$

donde C_m es el conjunto de enteros los cuales son producto de primos menores ó iguales a M.▲

TEOREMA 4: Si $1 \geq a_n > 0$ entonces $\prod(1-a_n)$ y $\sum a_n$ son ambas convergentes ó ambas divergentes.

Admitiremos el Teorema 4 sin demostración▲

TEOREMA 5: $\sum_{i=1}^{\infty} \frac{1}{p_i}$ diverge.

Dem.: Si en el Teorema 3 hacemos $M \to \infty$ entonces

$$\prod_{i=1}^{\infty} (1 - \frac{1}{p_i}) = 0$$

Consecuentemente $\prod(1 - \frac{1}{p_i})$ diverge

por el Teorema 4 concluimos que $\sum_{i=1} \frac{1}{p_i}$ diverge.▲

Lema 1: Si k es cualquier entero positivo entonces

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$$

Dem.: Dividamos los enteros $\{1,2,\ldots,x\}$ en los conjuntos de k enteros consecutivos más un resto de r-enteros

$k\ell+1, k\ell+2, \ldots, k\ell+r$.

Entre los enteros $1, 2, \ldots, k$ existen a lo más k primos. Puesto que cualquier entero que no es primo relativo con k tiene un factor primo en común con k que es menor ó igual a k, entonces entre los enteros $k+1, k+2, \ldots, 2k$ existen a lo más $\phi(k)$ primos. Similarmente en cada uno de los restantes conjuntos de k enteros consecutivos existen a los más $\phi(k)$ primos. Finalmente, en el conjunto restante de r enteros existen a lo más r primos. Por lo tanto

$$\pi(x) \leq k + (\ell-1)\phi(k) + r \leq 2k + \frac{x}{k}\phi(k)$$

entonces

$$\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x} \quad \blacktriangle$$

El siguiente Teorema muestra que $\pi(x)$ es a largo plazo mucho menor que x.

TEOREMA 6: $\lim_{x \to \infty} \frac{\pi(x)}{x} = 0$

Dem.: La idea es mostrar que $\frac{\pi(x)}{x}$ es arbitrariamente pequeño cuando x es muy grande.

Por el Lema 1 sabemos que para toda k entero positivo se cumple que $\frac{\pi(x)}{x} \leq \frac{\phi(k)}{k} + \frac{2k}{x}$

Sea M entero muy grande. Elijamos $k = p_1 p_2 \ldots p_s$ donde $p_i \in \{1, 2, \ldots, M\}$.

Entonces

$$\frac{\phi(k)}{k} = \frac{k(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_s})}{k} = \prod_{i=1}^{s}(1-\frac{1}{p_i}) < \left(\sum_{n=1}^{m}\frac{1}{n}\right)^{-1}$$

Así tenemos que

$$\frac{\pi(x)}{x} < \left(\sum_{n=1}^{m}\frac{1}{n}\right)^{-1} + \frac{2p_1 p_2 \cdots p_s}{x}$$

Puesto que $\sum_{n=1}^{\infty} \frac{1}{n}$ diverge, podemos escoger M tan grande que $\sum_{n=1}^{m} \frac{1}{n} > \frac{2}{\varepsilon}$ para todo $\varepsilon > 0$. Entonces $x > \frac{4p_1 p_2 \cdots p_s}{\varepsilon}$.

$$\frac{\pi(x)}{x} < \frac{\varepsilon}{2} + \frac{2p\ p_i \cdots p_s \varepsilon}{4p_1 p_2 \cdots p_s} = \varepsilon \quad \blacktriangle$$

Lema 2: Si $[x]$ denota el mayor entero menor ó igual a x entonces

$$0 \leq [2x] - 2[x] \leq 1$$

Dem.: La conclusión se puede deducir de las siguientes desigualdades

$$2x-1 < [2x] \leq 2x$$

$$2x-2 < 2[x] \leq x \quad \blacktriangle$$

TEOREMA 7: Si p es un primo, entonces $\sum_{k=1}^{\infty} \frac{n}{p^k}$ $(k=1,2,\ldots)$ es el exponente con el cual p aparece en la factorización de n! .

Dem.: Sean n,s enteros positivos. Sea p primo $\leq$ n.

Los números de la sucesión $\{1,2,\ldots,n\}$ los cuales son divisibles por p^s son de la forma ℓp^s, donde ℓ es entero positivo tal que $\ell p^s \leq n$, esto es $\ell \leq \frac{n}{p^s}$. El número de ℓ's es por supuesto $\left[\frac{n}{p^s}\right]$. Consecuentemente es claro que el exponente del primo p en la factorización en números primos del número n! . Se obtienen sumando al número de los terminos de la sucesión $\{1,2,\ldots,n\}$ los cuales son divisibles por p, el número de terminos divisibles por p^2 y también sumando el número de terminos los cuales son divisibles por p^3 y así sucesivamente. ▲

Por último estableceremos el Teorema de Chébyshev pero antes examinaremos algunas de las propiedades de la función $\frac{x}{\log x}$.

TEOREMA 8: Si $f(x)=\frac{x}{\log x}$, entonces

I. $f(x)$ es creciente si $x > e$

II. $f(x-2) > \frac{1}{2}f(x)$ si $x \geq 4$

III. $f(\frac{x+2}{x}) < \frac{15}{16} f(x)$ si $x \geq 8$

Dem.: I. Puesto que $f'(x)=\frac{\log x-1}{(\log x)^2}$

es claro que $f(x)$ es creciente si $x > e$.

II. Notemos que si $x \geq 4$ entonces $x-2 \geq \frac{x}{2}$

por lo tanto

$$f(x-2)=\frac{x-2}{\log x-2} \geq \frac{x}{2\log(x-2)} > \frac{x}{2\log x} = \frac{1}{2} f(x)$$

III. Si $x \geq 8$ entonces $\frac{x}{2} \geq x^{2/3}$ y $x+2 \leq \frac{5x}{4}$

por lo tanto

$$f\left(\frac{x+3}{2}\right)=\frac{x+2}{2\log\frac{x+2}{2}} \leq \frac{x+2}{2\log\frac{x}{2}} \leq \frac{x+2}{2\log x^{2/3}} \leq \frac{\frac{5x}{4}}{\frac{4}{3}\log x} = \frac{15}{16}f(x)$$ ▲

TEOREMA 9: (Chébyshev). Si $x \geq 8$ entonces

$$\frac{\log 2}{4} \cdot \frac{x}{\log x} < \pi(x) < 30(\log 2) \frac{x}{\log x}.$$

Dem.: Examinemos el coeficiente binomial $\binom{2n}{n}$

Es claro que $\binom{2n}{n}=\frac{(2n!)}{n!\,n!}=\frac{2n(2n-1)\ldots(n+1)}{n!}$

Cualquier primo en el intervalo $(n,2n]$ debe aparecer como factor en el numerador de $\binom{2n}{n}$ puesto que $n< p < 2n$.

Sea $P_n = \Pi p_i$ $(n < p_i < 2n)$, entonces claramente $P_n \mid \binom{2n}{n}$.

Como $p_i > n$ y P_n tiene $\pi(2n)-\pi(n)$ factores, entonces

$$n^{\pi(2n)-\pi(n)} < p_n < \binom{2n}{n} \qquad \ldots\ldots\ldots(1)$$

Sea p primo. Definimos r_p como

$$p^{\gamma_p} \leq 2n < p^{r_p+1}$$

Usando el Teorema 7 determinamos la potencia de p con la cual aparece en la factorización prima de $\binom{2n}{n}$, observemos que el exponente de p con el que figura en $\binom{2n}{n}$ debe ser la potencia de p con la cual aparece en (2n)! menos la potencia de p con la cual aparece en n! n! , es decir, el exponente debe ser

$$\sum_{j=1}^{\gamma_p} \left(\left[\frac{2n}{p^j} \right] - 2 \left[\frac{n}{p^j} \right] \right)$$

Por el Lema 2 obtenemos

$$0 \leq \sum_{j=1}^{\gamma_p} \left(\left[\frac{2n}{p^j} \right] - 2 \left[\frac{n}{p^j} \right] \right) \leq \sum_{j=1}^{\gamma_p} 1 = r_p$$

Sea $Q_n = \Pi p^{\gamma_p}$ $(p^{\gamma_p} \leq 2n)$. Es claro que $\binom{2n}{n} \Big| Q_n$.

Puesto que $p^{\gamma_p} \leq n$ y como Q_n tiene $\pi(2n)$ factores de la forma p^{γ_p} entonces

$$\binom{2n}{n} \leq Q_n \leq (2n)^{\pi(2n)} \qquad \ldots\ldots\ldots(2)$$

Ahora demostraremos que el Teorema de Chébyshev puede ser deducido de (1) y (2).

Observemos las siguientes desigualdades:

$$2 = 1 + \binom{2n}{1} + \ldots + \binom{2n}{n} + \ldots + 1 > \binom{2n}{n} \qquad \ldots\ldots(3)$$

$$\binom{2n}{n} = \frac{2n(2n-1)(2n-2)\ldots(n+1)}{n(n-1)(n-2)\ldots\ldots} \geq 2^n \qquad \ldots\ldots(4)$$

de (2) y (4) obtenemos que

$$2^n \leq (2n)^{\pi(2n)} \qquad \ldots\ldots(5)$$

Por lo tanto

$$n\log 2 \leq \pi(2n)\ \log 2n \quad \ldots\ldots\ldots(6)$$

Consecuentemente, si $x \geq 5$ y $f(x)=\dfrac{x}{\log x}$, entonces por (6) y Teorema 8 tenemos,

$$\pi(x) \geq \pi\left(2\left[\frac{x}{2}\right]\right) \geq \frac{\left[\frac{x}{2}\right]\log 2}{\log\ 2\left[\frac{x}{2}\right]} = \frac{\log 2}{2}\cdot\frac{2\left[\frac{x}{2}\right]}{\log\ 2\left[\frac{x}{2}\right]}$$

$$= \frac{\log 2}{2}\ f\left(2\left[\frac{x}{2}\right]\right) > \frac{\log 2}{2}\ f(x-2) > \frac{\log 2}{4}\ f(x) \quad \ldots.(7)$$

Finalmente usemos (1) y (3) para obtener

$$n^{\pi(2n)-\pi(n)} < 2^{2n}$$

Entonces

$$(\pi(2n)-\pi(n))\log n < 2n\log 2$$

o sea

$$\pi(2n) < 2\log 2\ \frac{n}{\log n} + \pi(n) \quad \ldots\ldots\ldots(8)$$

Vamos a establecer por inducción matemática que

$$\pi(2n) < 32(\log 2)\ \frac{n}{\log n}\ , \quad n > 1 \quad \ldots\ldots\ldots(9)$$

Es claro que (9) es válido para $2 \leq n \leq 8$.

En efecto, $\pi(4)=2 < \pi(6)=3 < \pi(8)=4=\pi(10)=4 < \pi(12)=$

$$5 < \pi(14)=6=\pi(16)=6 < 64=32(\log 2)\frac{2}{\log 2}$$

Supongamos que (9) es válido para toda $n \leq k$, $k \geq 8$. Entonces

$$\pi(2k+2) < 2\log 2\ f(k+1) + \pi(k+1) \quad \text{por 8}$$

$$\leq 2\log 2\ f(k+1)+\pi\left(2\left[\frac{k+2}{2}\right]\right) \quad \text{puesto que } \frac{k+1}{2} \leq \left[\frac{k+2}{2}\right]$$

$$< 2\log 2\ f(k+1)+32\log 2\ f\left(\left[\frac{k+2}{2}\right]\right) \quad \text{por hipótesis de}$$

inducción

$$\leq 2\log 2\ f(k+1)+32\log 2\ f\left(\frac{k+2}{2}\right) \quad \text{ya que } \left[\frac{k+2}{2}\right] \leq \frac{k+2}{2}$$

$$\leq 2\log 2\ f(k+1)+32\log 2\ f(k)\ \frac{15}{16} \quad \text{por Teorema 8}$$

$< 2\log 2\ f(k+1) + 32\log 2\ \frac{15}{16}\ f(k+1)$.

$= 32 \log 2\ f(k+1)$

Por lo tanto $\pi(2n) < 32(\log 2)\frac{n}{\log n}$

En general para cada real $x \geq 8$ tenemos que $\frac{x-2}{2} < \left[\frac{x}{2}\right]$

entonces $\pi(x) < \pi\left(2\left[\frac{x}{2}\right] + 2\right)$ puesto que $\frac{x-2}{2} < \left[\frac{x}{2}\right]$

$< 32 \log 2\ f\left(\left[\frac{x}{2}\right] + 1\right)$ por (9)

$\leq 32 \log 2\ f\left(\frac{x}{2} + 1\right)$ ya que $\left[\frac{x}{2}\right] \leq \frac{x}{2}$

$= 32 \log 2\ f\left(\frac{x+2}{2}\right)$

$< 32(\log 2)\ \frac{15}{16}\ f(x)$ por Teorema 8

$= 30(\log 2)\ \frac{x}{\log x}$ .....(10)

juntando (7) y (10) tenemos

$$\frac{\log 2}{4}\ \frac{x}{\log x} < \pi(x) < 30(\log 2)\ \frac{x}{\log x}$$ ▲

BIBLIOGRAFIA

Apostol, T.M.: Introduction to Analitic Number theory. Undergraduate texts in Mathematics: Springer-Verlag. 1976

Birkhoff, G.: Modern Algebra (a Survey of). 3a. edición. MacMilan Co.

Blanusa, D.: Une interprétation géométrique du crible d'Erathosténe. Glasnik Mat. Fiz. Astronom. Drustvo Mat. Fiz. - Hrvatske.

Griffin, H.: Elementary theory of Numbers. McGraw-Hill. 1954

Hardy, G.H. and Wright, E.M.: An Introduction to the theory of - Numbers. Oxford University Press. Oxford. 1938.

Landau, E.: Elementary Number theory. Chelsea Publishing. 2a. -- edición. New York.

LeVeque, W.J.; Topic in Number theory. Vol.I. Readin Mass: Adi-- son-Wesley Publishing Co. 1956.

LeVeque, W.J.; Elementary theory of Numbers. Adison-Wesley Publi_ shing Co. 1962.

Nagell, T.; Introduction to Number theory. John Wiley & Sons,Inc. New York. 1951.

Ore, O.: Number Theory and its History. McGraw-Hill Book Co.Inc. New York. 1948.

Shanks, D.: Solved and Unsolved problems in Number theory. 2a. - edición. Chelsea Publishing.

Selberg, A.: An elementary proof of the prime-number theorem. -- Ann. of Math. (2) 50, 1949.

Sierspiński, W.: Elementary theory of Numbers. Monografie Matematyczne. Warsaw: Palistwowe Wzdawnictwo Naukowe. (42). - 1964.

Vinogradov, I.M.: Elements of Number theory. Dover Publications. 1954.

Tietze, H.: Famous Problems of Mathematics. Graylock Press. Baltimor. 1965.