UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

LA TEORIA DE LOS NUMEROS Y ALGUNOS RESULTADOS CLASICOS.

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

LUIS NÚÑEZ RODRIGUEZ

MÉXICO, D.F. 1988.

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

CONTENIDO

I

DIVISIBILIDAD

La ecuación $ax = b$ con coeficientes enteros no siempre tiene solución entera x. En el caso que x sea un entero nos conduce al concepto llamado divisibilidad que es uno de los fundamentos principales de la Teoría de los números. Antes de dar la definición de éste y sus aplicaciones, escribimos a continuación un hecho más general.

Teorema 1: Si m es un entero positivo y n es un entero arbitrario, entonces existe exactamente un par de enteros q y r tales que las condiciones (1) $n = qm + r$ y $0 \leq r < m$ se cumplen.

Demostración:

Primero, mostraremos que (1) tiene al menos una solución.

Consideremos al conjunto $D = \{\alpha \in \mathbb{Z} \mid \alpha = n - sm, s \in \mathbb{Z}\}$,

para la elección particular siguiente de

$$S = \begin{cases} -1 & \text{si } n \geq 0 \\ n & \text{si } n < 0 \end{cases}$$

el número $n - sm$ es no negativo, así D tiene elementos positivos. El subconjunto de elementos no negativos de D, por el Principio del Buen Orden, tiene un elemento mínimo. Llamaremos r a éste elemento y q al valor correspondiente de S para él. Entonces $r = n - qm \geq 0$, $r - m = n - (q+1)m < 0$, de esta manera (1) se satisface.

Para mostrar la unicidad, suponemos que n lo podemos escribir como $n = q'm + r'$, $0 \leq r' < m$ para $q', r' \in \mathbb{Z}$. Entonces si $q' < q$, $n - q'm = r' \geq n - (q-1)m = r + m \geq m$, de la misma manera si $q < q'$ obtenemos $r \geq m$. Por lo tanto $q' = q$ y $r' = r$.

Cuando r toma el valor cero en el teorema 1 tenemos:

Definición 1. Si m y n están en $\mathbb{Z}$, con $m \neq 0$. Decimos que m divide a n si existe $q \in \mathbb{Z}$ tal que $n = qm$. En caso contrario diremos que m no divide a n.

Usaremos las notaciones $m \mid n$ y $m \nmid n$ para indicar que m divide a n y m no divide a n respectivamente. El siguiente teorema se demuestra directamente de la definición 1, por lo que no haremos la prueba.

Teorema 2: Sean m, n, l, x e y enteros.

a) i) Para cualquier $m \neq 0$, $m \mid 0$ y $m \mid m$

ii) Para cualquier n, $\pm 1 \mid n$

b) Si $m \mid n$ y $n \mid l$ entonces $m \mid l$

c) Si $m \mid n$ y $n \mid m$ entonces $m = \pm n$

d) Si $m \mid n$ y $m \mid l$ entonces $m \mid (nx + ly)$

e) Si $m \mid n$ entonces $|m| \leq |n|$

f) Si $m \mid n$ entonces $ml \mid nl$

g) Si $lm \mid ln$ y $l \neq 0$ entonces $m \mid n$

h) Si $m \mid n$ y $m \neq 0$ entonces $\left(\frac{n}{m}\right) \mid m$

Las siguientes dos definiciones son muy útiles:

Definición 2.

i) Si $n = gm$ y $l = g'm$, entonces m se llama común divisor de n y l

ii) Dados m y n enteros, si existe un entero positivo d tal que:

1) d es común divisor de m y n.

2) Cualquier común divisor de m y n es también divisor de d. Entonces d es llamado el Máximo Común Divisor de m y n, y es designado por $d = (m, n)$.

Quizás ya sean familiares estas ideas; puesto que sin mucho esfuerzo podemos reconocer que $(15, 21) = 3$, pero no que $(4147, 10672) = 29$; tal vez porque 4147 y 10672 son mayores que 15 y 21 respectivamente. Sin embargo, hay un algoritmo mediante el cual podemos encontrar el máximo común divisor de dos números dados no importando que tan grandes sean estos. Este mecanismo es conocido como:

El algoritmo de Euclides. Dados m y n enteros positivos tales que $m \leq n$, entonces podemos obtener la siguiente sucesión finita de ecuaciones

$$
\begin{aligned}
n &= q\,m + r_1 && , \quad 0 < r_1 < m \\
m &= q_1 r_1 + r_2 && , \quad 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 && , \quad 0 < r_3 < r_2 \\
&\vdots && \vdots \\
r_{k-2} &= q_k r_{k-1} + r_k && , \quad 0 < r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k + 0 && , \quad r_{k+1} = 0
\end{aligned}
$$

Demostración.

Por el teorema 1, podemos escribir $n = qm + r$ donde $0 \leq r < m$, si $r = 0$, terminamos con la ecuación $n = qm$. El caso más importante es cuando $r \neq 0$, pues aplicando, nuevamente el teorema 1 a m y r obtenemos la ecuación $m = q_1 r + r_1$ donde $0 \leq r_1 < r$. De nuevo si $r_1 \neq 0$, aplicamos el teorema 1 a r y r_1, obteniendo $r = q_2 r_1 + r_2$ donde $0 \leq r_2 < r_1$. Ahora supongamos que podemos aplicar repetidamente el algoritmo de la división, digamos $K+1$ veces, entonces obtenemos $r_{k-2} = q_k r_{k-1} + r_k$ donde $0 \leq r_k < r_{k-1}$. Puesto que los residuos forman una sucesión decreciente de enteros positivos $m > r > r_1 > \cdots > r_k > 0$, se sigue que en un número finito de pasos el proceso termina, digamos en $K+2$ pasos, es decir, que si $r_k \neq 0$, obtenemos $r_{k-1} = q_{k+1} r_k + r_{k+1}$

donde $r_{k+1} = 0$.

Trabajamos con m y n enteros positivos pero también El Algoritmo de Euclides es verdadero para todo par de enteros. El teorema que sigue nos asegura la existencia, la unicidad del máximo común divisor, y además cómo puede ser encontrado mediante el Algoritmo de Euclides.

Teorema 3.

Para cualquier par de enteros positivos n y m, el máximo común divisor $d = (n, m)$

i) Existe

ii) Es único

iii) Es tal que existen enteros x e y para los cuales $d = nx + my$

iv) Es tal que los enteros d, x, y pueden ser encontrados en un número finito de pasos por el Algoritmo de Euclides.

Demostración: i) Consideremos el Algoritmo de Euclides descrito anteriormente. Si $r = 0$, el algoritmo consiste de una sola ecuación $n = qm$, y es claro que m satisface los requerimientos de la definición 2(ii), así que $d = m$. Si $r \neq 0$, mostraremos que r_k es el máximo común divisor de n y m, si es el último residuo no cero en el Algoritmo de Euclides (en el caso $r_1 = 0$ convenimos definir $r_0 = r$). Debemos mostrar que r_k posee las propiedades (1) y (2) de la definición 2(ii).

Prueba de (1):

de $r_{K-1} = q_{K+1} r_K$ se sigue que r_K divide a r_{K-1}, de

$$r_{K-2} = q_K r_{K-1} + r_K = (q_K q_{K+1} + 1) r_K$$

se sigue que r_K divide a r_{K-2}.
De manera similar, retrocediendo ecuación por ecuación en el algoritmo encontramos que r_K divide a m y finalmente que r_K divide a n.
Así que r_K es un divisor común de n y m.

Prueba de (2):

Sea d' cualquier común divisor de n y m, así que $n = Pd'$ y $m = Qd'$. Reacreglemos la primera ecuación del algoritmo para ver que $(r = n - qm = (P - qQ)d')$ d' divide a r.
Entonces reacreglando la segunda ecuación $(r_1 = m - q_1 r)$, mostramos que d' divide a r_1. Haciéndolo ecuación por ecuación en el algoritmo, finalmente encontramos que $(r_K = r_{K-2} - q_K r_{K-1})$ d' divide a r_K.

Puesto que hemos mostrado que r_K posee las propiedades (1) y (2), se sigue de la definición de d que $r_K = d$. Por lo tanto, almenos un entero $d = (n, m)$ existe.

ii) Sean d y d' dos máximos comunes divisores de n y m. Por la propiedad (2) se sigue que por un lado $d = Kd'$ y por otro lado que $d' = Sd$, entonces $d = \pm d$ por el teorema 2.

Inversamente, si $S = \pm 1$ y d es un máximo común divisor de n y m, entonces $d' = Sd$, también es un máximo común divisor de n y m

De esta manera el máximo común divisor de n y m es único.

Las demostraciones de (iii) y (iv) se dan directamente por eliminaciones sucesivas (aun cuando es muy largo) de $r_{k-1}, r_{k-2}, \ldots r_1$ y r del sistema de ecuaciones del algoritmo, comenzando con

$$r_k = r_{k-2} - q_k r_{k-1} = \left(r_{k-4} - q_{k-2} r_{k-3}\right) - q_k \left(r_{k-3} - q_{k-1} r_{k-2}\right),$$

descubrimos en un número finito de pasos, los enteros x e y convenientes tales que $r_k = nx + my$. En el caso $r = 0$, tenemos que $d = m$ y así podemos tomar $x = 0$ e $y = 1$, para tener $d = nx + my$

Ejemplo: Si $n = 2210$ y $m = 493$, el Algoritmo de Euclides se puede escribir como sigue:

$$\begin{array}{rl|l}
 & & 4 = q \\
m = 493 & 2210 = n & \\
 & 1972 & \\
\hline
 & & 2 = q_1 \\
r = 238 & 493 & \\
 & 476 & \\
\hline
 & & 14 = q_2 \\
r_1 = 17 & 238 & \\
 & 238 & \\
\hline
 & & 1 = q_3 \\
 & r_2 = 0 &
\end{array}$$

Puesto que $r_2 = 0$, tenemos que $r_1 = 17 = (2210, 493)$. Para encontrar x e y unicamente hay que eliminar a r de las ecuaciones, como sigue:

$17 = m - 2r = m - 2(n - 4m) = -2n + 9m$, por lo tanto obtenemos que $x = -2$ e $y = 9$. Para efectuar tal eliminación es conveniente conservar las letras r_i, n y m y substituir unicamente los números q_i en cada paso.

Si $n \neq 0$, entonces $n = (n, 0)$, por lo tanto el simbolo (n, m) tiene sentido en cualquier caso excepto para $(0, 0)$ donde ciertamente no tiene sentido, puesto que cualquier entero es un divisor de cero.

Observar que el teorema 3 vale para cualquier par de enteros no ambos cero.

Damos una lista de propiedades del máximo común divisor.

Teorema 4.

El máximo común divisor tiene las siguientes propiedades:

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

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

c) $(ac, bc) = |c|(a, b)$

d) Sean $a_1, a_2, \ldots, a_n$ enteros definimos $D_1 = (a_1, a_2)$, $D_2 = (D_1, a_3)$, $\ldots$, $D_{n-1} = (D_{n-2}, a_n)$ entonces $(a_1, a_2, \ldots, a_n) = D_{n-1}$

Una de las aplicaciones directas del teorema 3 es la solución de ecuaciones de la forma $nx + my = c$, tal que sus soluciones sean enteras, estas ecuaciones reciben el nombre de Ecuaciones Lineales Diofantinas. Para ello es fácil pensar en un esquema

para encontrar un número infinito de soluciones en caso de que existan, el esquema puede ser mejor explicado por medio de un ejemplo numérico, digamos $5n + 22m = 18$. Puesto que n es un entero, $\frac{1}{5}(18 - 22m)$ debe ser un entero. Escribiendo $n = \frac{18 - 22m}{5} = 3 - 4m + \frac{3 - 2m}{5}$ vemos que $\frac{1}{5}(3 - 2m)$ debe ser también un entero digamos z.

Esto da $z = \frac{3 - 2m}{5}$, $2m + 5z = 3$

Ahora repitamos el mismo argumento para $2m + 5z = 3$, resolviendo como antes para la variable que tenga el coeficiente más pequeño:

$$m = \frac{3 - 5z}{2} = 1 - 2z + \frac{1 - z}{2}, \text{ de donde}$$

$t = \frac{1 - z}{2} \in \mathbb{Z}$, entonces $z = 1 - 2t$. Claramente z será un entero para cualquier entero t, tenemos que $m = \frac{3 - 5(1 - 2t)}{2} = -1 + 5t$ y

$$n = \frac{18 - 22(-1 + 5t)}{5} = 8 - 22t$$

Más aún, es fácil ver que cualquier solución $\{n, m\}$ de la ecuación original debe ser de esta forma, de esta manera tenemos una solución general de la ecuación.

La misma idea se aplica al caso general, que enunciamos en lo siguiente:

Proposición 1. Una condición necesaria y suficiente para que la ecuación $nx+my=c$ (2), tenga una solución $\{n, m\}$ en los enteros es que $d|c$, donde $d=(n, m)$. Si existe una solución, existen una infinidad de soluciones; ellas son exactamente números de la forma

$$n=n_0+\frac{m}{d}t\ ,\ m=m_0+\frac{n}{d}t \quad \text{donde } t\in\mathbb{Z} \text{ y}$$

$\{n_0, m_0\}$ es una solución particular.

Demostración:

Notemos que (2) no tiene solución a menos que $d|c$ donde $d=(n, m)$ y que si este requerimiento se satisface, podemos dividir completamente a (2) por d y obtenemos una nueva ecuación $n'x+m'y=c'$ (3) donde $(n'; m')=1$. Por el teorema 3 podemos afirmar que existen $n'_0\ ,\ m'_0\in\mathbb{Z}$ tales que $n'n'_0+m'm'_0=1$, así que $\{c'n'_0, c'm'_0\}$ es una solución de (3). Haciendo $n_0=c'n'_0$, $m_0=c'm'_0$ y si t es cualquier entero, tenemos:

$$n'(n_0+m't)+m'(m_0-n't)=n'n_0+m'm_0=c',$$

de esta manera

$\{n_0+m't\ ,\ m_0-n't\}$ es una solución para cada $t\in\mathbb{Z}$.

Finalmente, si $\{n_1, m_1\}$ es cualquier solución de (3), tenemos $n'n_0+m'm_0=c'$, $n'n_1+m'm_1=c'$ y restándolas, $n'(n_0-n_1)+m'(m_0-m_1)=0$.

Así $n' \mid (m_0 - m_1)$, $m_0 - m_1 = n' t_1$ y $m' \mid (n_0 - n_1)$, $n_0 - n_1 = m' t_2$.

Esto da $n_1 = n_0 - m' t_2$, $m_1 = m_0 - n' t_1$ y como estos números satisfacen (3), tenemos $t_2 = -t_1$. Por lo tanto cualquier solución de (3) es de la forma

$$\{n_0 + m' t, m_0 - n' t\} \text{ donde } t \in \mathbb{Z}$$

Si un par de números no tiene como máximo común divisor o un número $d > 1$, tenemos:

Definición 3.

Si el máximo común divisor de los enteros n y m es el número uno, entonces diremos que n y m son primos relativos.

Ejemplos:

$(8, 15) = 1$ y $(21, 32) = 1$

Teorema 5.

a) Los enteros n y m son primos relativos si y solo si existen enteros x e y tales que $nx + my = 1$

b) Si $(n, m) = d$ y $n = td$, $m = sd$ entonces $(t, s) = 1$

c) Si $(m, n) = 1$ y $(m, l) = 1$ entonces $(m, nl) = 1$

d) Si $(n, m) = 1$ y $n \mid ml$ entonces $n \mid l$

Demostración:

a) Si x e y existen tales que $nx+my=1$ y d' es cualquier común divisor de n y m, es decir, $n=td'$ y $m=sd'$, entonces $(tx+sy)d'=1$, de donde $d'=\pm 1$.
Por lo tanto $d=(n,m)=1$. Inversamente, si $(n,m)=1$ entonces el teorema 3 garantiza la existencia de los enteros x, y tales que $nx+my=1$.

b) Por el teorema 3 existen enteros x, y tales que $d=nx+my$
Entonces de $d=nx+my=(tx+sy)d$ obtenemos $tx+sy=1$, de (a) se sigue que $(t,s)=1$

c) De (a) existen $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ tales que $mx_1+ny_1=1$, $mx_2+ly_2=1$, multiplicándolos obtenemos $1=(mx_1+ny_1)(mx_2+ly_2)$ $=m(x_1mx_2+x_1ly_2+ny_1x_2)+nl(y_1y_2)$, haciendo $x_3=x_1mx_2+x_1ly_2+ny_1x_2$ y $y_3=y_1y_2$, tenemos que $mx_3+nly_3=1$. Por lo tanto de (a) tenemos $(m,nl)=1$.

d) Puesto que $(n,m)=1$, existen enteros x e y tales que $1=nx+my$.
Por lo tanto $l=l(nx+my)=nlx+mly$, pero por hipótesis $n \mid ml$, es decir, $ml=ng$ de donde $l=n(lx+gy)$. Por lo tanto $n \mid l$.

Cuando escribimos $m \mid n$, queremos decir también que n es múltiplo de m, sin embargo m tiene una infinidad de múltiplos, por ejemplo si $m=25$, entonces 25, 50, 75, 100, son algunos de sus múltiplos. Pero es más interesante, pensar en los múltiplos comunes de dos o más números y encontrar el más pequeño de ellos, para esto damos lo siguiente:

Definición 4.

a) Si: $l = qn = rm$, entonces decimos que l es un múltiplo común de n y m

b) Si: l satisface las siguientes propiedades:

i) l es un múltiplo común de n y m

ii) Cualquier múltiplo común de n y m es un múltiplo de l.

Entonces a l lo llamamos el mínimo común múltiplo de n y m y lo denotaremos por $l = [n, m]$.

La manera para encontrar el mínimo común múltiplo (m.c.m) de dos números enteros positivos arbitrarios, sin ninguna dificultad es sugerido por:

Teorema 6. Si: $d = (n, m)$ y $l = [n, m]$ entonces $dl = nm$,

Demostración

Si: $n = qd$, y $m = rd$, entonces $nm = qdrd$, demostrando que $l' = qdr$ es igual a $[n, m]$., el teorema quedo establecido.

1) Puesto que $l' = qdr = nr = mq$, es claro que l' es múltiplo común de n y m.

2) Sea M cualquier múltiplo común de n y m, es decir, $M = ns = mt$. Entonces $qds = rdt$, de donde $qs = rt$.
Además $(q, r) = 1$, entonces $r \mid s$, es decir, $s = rv$. Por lo tanto $M = ns = nrv = l'v$, de donde M es un múltiplo de l'.

Ahora podemos concluir de (1) y (2) que $l' = [n, m]$ y esto termina la demostración.

Podemos calcular el mínimo común múltiplo encontrando primero el m.c.d. y después utilizar el teorema anterior. Por ejemplo, calculemos el $[2625, 2205]$. Encontramos primero el $(2625, 2205)$ que es igual a 105, de donde

$$[2625, 2205] = \frac{2625\ 2205}{(2625, 2205)} = \frac{2625 \cdot 2205}{105} = 55125$$

Corolario 1.

Si $m > 0$ entonces $[ma, mb] = m[a, b]$

La noción de divisibilidad induce a definir a dos clases de enteros, la de los divisibles por ± 1 y por él mismo, y la de los que sus divisores no son únicamente ± 1 y él mismo; Euclides fue el primero en definirlos, enseguida formalizamos a éstos con lo siguiente:

Definición 5.

Un entero n es llamado primo si $n > 1$ y si los únicos divisores positivos de n son 1 y n.

Si $n > 1$ y si n no es primo, entonces n es llamado compuesto.

Los primeros 6 números compuestos positivos son 4, 6, 8, 9, 10 y 12 y los primeros 6 números primos son 2, 3, 5, 7, 11, y 13.

Las propiedades de los números primos las enunciamos por medio de los siguientes teoremas:

Teorema 7.

a) Si un número primo p, divide a $n.m$, entonces debe dividir al menos a uno de los enteros n ó m.

b) Si un primo p divide a un producto $\prod_{i=1}^{k} n_i$ entonces p debe dividir al menos a uno de los factores n_i, $i=1, 2, \ldots, k$.

Demostración.

Haremos sólo la prueba de (a) porque (b) es una consecuencia de ésta.

Supongamos que $p \mid n$, entonces hemos terminado. Supongamos ahora que $p \nmid n$, entonces $(p, n) = 1$, porque los únicos divisores de p son ± 1 y $\pm p$, por lo tanto existen x e y enteros tales que $nx + py = 1$. Multiplicando por m a la igualdad, obtenemos $m = nmx + pmy$. Como $p \mid nm$ y $p \mid pm$ entonces $p \mid m$.

Teorema 8.

a) El divisor menor distinto de uno, de un entero $m > 1$, es un número primo.

b) El divisor menor distinto de uno de un número compuesto m no es mayor que $\sqrt{m}$

Demostración.

a) Sea q el divisor menor de m tal que $q \neq 1$ Si q fuese compuesto tendría un divisor q_1, con la condición

$1 < q_1 < q$, pero q es divisor de m entonces q_1 divide a m y esto contradice al hecho de que q es el divisor menor de m.

b) Sea q este divisor, entonces $m = q m_1$, $m_1 \geq q$, de donde multiplicando por q y simplificando; obtenemos $m \geq q^2$.

Por lo tanto $q \leq \sqrt{m}$

Teorema 9.

Cualquier entero $n > 1$ o' es un primo o' un producto de primo.

Demostracion:

Usaremos induccion sobre n. El teorema claramente es verdadero para $n = 2$. Supongamos que es verdadero para cualquier entero menor que n. Entonces si n no es primo tiene un divisor positivo $1 < d < n$. Por lo tanto $n = cd$, donde $c \neq n$. Pero c y d son menores que n y mayores que 1, asi que c y d se pueden escribir como productos de primos, por lo tanto n se puede escribir como un producto de primos.

Teorema 10.

El Teorema Fundamental De La Aritmética.

Cualquier entero positivo $n \neq 1$, se puede escribir de manera unica como sigue:

$$n = \prod_{i=1}^{k} P_K^{\alpha_K}$$

donde k es un entero positivo y cada p_i es un primo, α_i también es un entero positivo y $1 < p_1 < p_2 < \ldots < p_k$

Demostración

A) La existencia de la representación es una consecuencia inmediata del Teorema 9.

B) Supongamos que existen dos representaciones para un entero n dado, digamos $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m}$ donde por supuesto p_i y q_i son primos y $1 < p_1 < p_2 < \ldots < p_k$; $1 < q_1 < q_2 < \ldots < q_m$. No es necesario suponer que $m \geq k$.

Por el teorema 7 se sigue que el primo p_1 debe dividir a algún factor q_i y puesto que q_i es un primo, entonces $p_1 = q_i$; pero $q_i \geq q_1$ entonces $p_1 \geq q_1$. Pero de manera similar se puede mostrar que el primo q_1 debe dividir a algún factor p_j y puesto que p_j es un primo, se sigue que $q_1 = p_j$; sin embargo $p_j \geq p_1$, por lo tanto $q_1 \geq p_1$. Así obtenemos que $p_1 = q_1$. Ahora supongamos que $\beta_1 \geq \alpha_1$ entonces $p_1^{\alpha_1} = q_1^{\beta_1}$. Al dividir a la ecuación por $p_1^{\alpha_1}$ obtenemos que

$$p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1 - \alpha_1} q_2^{\beta_2} \ldots q_m^{\beta_m}.$$

Si $\beta_1 > \alpha_1$, el primo q_1 por el mismo argumento anterior debe ser igual a algún p_j, $j \geq 2$, pero puesto que $q_1 = p_1 < p_j$, $j \geq 2$. Tenemos una contradicción. Por lo tanto $\beta_1 = \alpha_1$. Un argumento similar es suficiente, si suponemos que $\alpha_1 \geq \beta_1$.

Repitiendo este argumento paso por paso, nos conduce a las siguientes conclusiones:

$$p_1 = q_1,\ \alpha_1 = \beta_1;\ p_2 = q_2,\ \alpha_2 = \beta_2;\ \ldots\ p_K = q_K,\ \alpha_K = \beta_K$$

En este momento la igualdad estudiado se reduce (en el caso $m > K$) a la siguiente $1 = q_{K+1}^{\beta_{K+1}} \cdots q_m^{\beta_m}$, pero éste es una contradicción, puesto que un primo q no es divisor de 1. Por lo tanto $m = K$ y la demostración de la unicidad de la representación está completa.

En muchos textos El Teorema Fundamental De La Aritmética se establece de esta manera "Cualquier entero positivo, excepto el 1, puede ser representado de manera única como productos de primos, excepto por el orden." Pero arreglando la colección de primos en orden ascendente la última frase puede ser reemplazada por la condición $1 < p_1 < p_2 < \ldots < p_K$.

Teorema 11. Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, el conjunto de divisores positivos de n es el conjunto de los números de la forma $\prod_{i=1}^{r} p_i^{\beta_i}$ donde

$0 \leq \beta_i \leq \alpha_i$ para $i = 1, 2, \ldots, r$

Teorema 12. Si dos enteros n y m tienen la factorización:

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \quad , \quad m = \prod_{i=1}^{s} p_i^{\beta_i}$$

entonces su m.c.d. tiene la factorización

$$(n,m) = \prod_{i=1}^{t} p_i^{\mu_i} \qquad \text{donde cada } \mu_i =$$

$$\min \{\alpha_i, \beta_i\}$$

Demostración

Sea $d = \prod_{i=1}^{t} p_i^{\mu_i}$, puesto que $\mu_i \leq \alpha_i$ y $\mu_i \leq \beta_i$,

tenemos que $d|n$ y $d|m$, de esta manera d es un común divisor de n y m. Sea d' cualquier común divisor de n y m, lo podemos escribir como

$$d' = \prod_{i=1}^{t} p_i^{\alpha_i} \quad \text{entonces } \alpha_i \leq \alpha_i \text{ y } \alpha_i \leq \beta_i,$$

por lo que $\alpha_i \leq \mu_i$.

Por lo tanto $d'|d$, lo que quiere decir que d es el máximo común divisor.

Hasta el momento hemos hablado de algunas propiedades de los números primos y compuestos, pero hay preguntas que podemos formular aún como las siguientes:

1.- ¿Cómo podemos determinar una lista de primos y números compuestos los cuales son menores

que n, donde n es un entero dado?

2.. ¿Cómo podemos determinar cuando un entero n dado es primo ó es compuesto?

3.. ¿Existen una infinidad de números primos distintos?

4.. ¿Es posible dar una fórmula para el n-ésimo primo?

5.. ¿Es posible encontrar un polinomio $f(x)$ el cual represente primos únicamente para todos los valores de x?

6.. ¿Existen sucesiones arbitrariamente largas de enteros consecutivos, donde todos son números compuestos?

Dar alguna respuesta a las preguntas 1 y 2 nos conduce al procedimiento que describió Eratóstenes (276-194 a.c), el cual recibe el nombre de "Criba de Eratóstenes", que consiste en: Dar un número entero positivo n y escribir a todos los enteros positivos menores o iguales que n y eliminar sistemáticamente a todos los enteros compuestos.

En general, para la pregunta 1; la respuesta que se da a continuación no es muy práctica y para la pregunta 2 realmente no es satisfactoria la respuesta que damos, porque hay varios criterios los cuales dan una respuesta completa.

Para entender mejor el procedimiento de la criba demos un ejemplo, sea $n = 100$, enlistamos a los enteros desde 2 hasta 100. Reconocemos que 2 es un primo, pero todos los múltiplos propios de 2 son compuestos, eliminamos a $4, 6, 8, \ldots, 100$. El siguiente número no eliminado es 3, el cual debe ser primo porque su único factor propio posible es 2 y 3

no es multiplo de 2 porque si lo fuese hubiese sido eliminado.

Reconociendo ahora que todos los multiplos propios de 3 son compuestos, eliminamos a 6, 9, 12, ... 99, (aunque no es necesario eliminar a 6, 12, 18, ..., 96, otra vez, puesto que ellos ya han sido eliminados por ser multiplos propios de 2). El siguiente número eliminado de la lista es el 5, éste número debe ser primo, porque si fuera compuesto tendria como factores propios a los primos menores que él, es decir, 2 ó 3, por lo cual 5 no es multiplo de 2 ó 3. Eliminamos a todos los multiplos de 5, que aún no han sido eliminados previamente, es decir, 25, 35, 55, 65, 85, 95. Encontramos por el mismo razonamiento, que el siguiente número no eliminado debe ser un primo; es el 7. Los multiplos de 7 aún no eliminados son 49, 77, 91, y a éstos los cancelamos. Ahora si no ser que no hayamos sido cuidadosos analizando el proceso de la criba estaremos sorprendidos. ¡Todos los números sobrantes los cuales han sobrevivido a la criba son primos!

La criba aparece como sigue:

(2) (3) ~~4~~ (5) ~~6~~ (7) ~~8~~ ~~9~~ ~~10~~ (11) ~~12~~ (13)
~~14~~ ~~15~~ ~~16~~ (17) ~~18~~ (19) ~~20~~ ~~21~~ ~~22~~ (23) ~~24~~
~~25~~ ~~26~~ ~~27~~ ~~28~~ (29) ~~30~~ (31) ~~32~~ ~~33~~ ~~34~~ ~~35~~
~~36~~ (37) ~~38~~ ~~39~~ ~~40~~ (41) ~~42~~ (43) ~~44~~ ~~45~~ ~~46~~
(47) ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ (53) ~~54~~ ~~55~~ ~~56~~ ~~57~~
~~58~~ (59) ~~60~~ (61) ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ (67) ~~68~~
~~69~~ ~~70~~ (71) ~~72~~ (73) ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ (79)
~~80~~ ~~81~~ ~~82~~ (83) ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ (89) ~~90~~
~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ (97) ~~98~~ ~~99~~ ~~100~~

Estamos en posición de alcanzar el fin en el proceso de la criba cuando tengamos eliminados a los múltiplos propios de p, donde p es el primo más grande tal que $p \leq \sqrt{n}$, donde n es el número dado. Esto se sigue del hecho de que si $s = ab$ es compuesto al menos uno (y de hecho exactamente uno) de los factores a y b debe ser $\leq \sqrt{s}$, porque si $a > \sqrt{s}$ y $b > \sqrt{s}$ encontramos que $s = ab > (\sqrt{s})^2 = s$, que es una contradicción. Por lo tanto si s no es eliminado cuando los múltiplos propios de p (y de todos los primos menores) han sido eliminados, entonces s debe ser un primo. Porque no habiendo sido eliminado en este o cualquiera de los pasos previos, s no puede tener un factor que no es $\leq \sqrt{n}$; y puesto que $s \leq n$, s no puede tener un factor distinto de uno $\leq \sqrt{s}$, por lo que s no puede ser compuesto

Daremos la respuesta a la pregunta 3 de dos maneras.

1.. Usaremos $P_! + 1$. Si recordamos la definición de $n!$, entonces es especialmente fácil describir la prueba de Euclides de que existe una infinidad de primos distintos. Suponemos que existen un número finito de primos y que el primo p es el más grande. Mostraremos que esta suposición es falsa, estudiando el número $M = P_! + 1 = (1 \cdot 2 \cdot 3 \cdots P) + 1$. Evidentemente M no es divisible por cualquiera de los números $2, 3, 4, \ldots, P$, porque existe el residuo 1 en cada uno de estos casos. Si suponemos que $n \mid M$ donde $2 \leq n \leq P$, entonces existe $q \in \mathbb{Z}^+$ tal que $M = qn$, de donde $P_! + 1 = qn$. Por lo tanto existe $Q \in \mathbb{Z}$ tal que $qn + (-1)P_! = 1$, lo que significa que n y $P_!$ son primos relativos, lo que es una contradicción.

Por lo tanto $n \nmid M$, entonces M no es divisible por ningún primo $\leq P$.

Sin embargo por el Teorema Fundamental De La Aritmética, M ó es un primo ó es un producto de primos. En cualquiera de los 2 casos vemos que debe existir un primo más grande que P, lo que quiere decir que no existe un primo p más grande. Por lo tanto deben de existir una infinidad de primos.

2.- Usando a los enteros de la forma $6x-1$. Podemos mostrar que existen una infinidad de números primos mezclados con los enteros de la progresión aritmética A: 5, 11, 17, 23, 29, 35, ..., siendo la forma general $6n-1$ para cada entero de la sucesión. Porque si suponemos que $P_1, P_2, \ldots, P_K$ son los primeros K primos que pertenecen a A, arreglados en el orden natural, entonces podemos probar la existencia de un primo todavía más grande que pertenece a A. Consideremos el entero $M = 6 P_1 P_2 \ldots P_K - 1$. Expresamos a M como un producto de primos, es decir,

$$\prod_{i=1}^{r} q_i^{\alpha_i} = M \quad \text{donde } 1 < q_1 < q_2 < \cdots < q_r$$

Puesto que M es impar y no es múltiplo de 3, se sigue que todos los factores primos de M son de la forma $6x+1$ ó $6x-1$, porque no existen primos impares > 3 de la forma $6x \pm 3$, todos los números de ésta forma (excepto 3) son compuestos. Sin embargo, el producto de cualquier número de primos de la forma $6x+1$ es otra vez un número de la forma $6x+1$, M debe tener al menos un factor primo P de la forma $6x-1$.

Sin embargo, el primo p debe ser más grande que P_K, porque ninguno de los $P_1, P_2, \ldots, P_K$ es un factor de M, puesto que cada uno de éstos deja residuo -1, si los ensayamos como factores. Por lo tanto P_K no es el primo más grande en A y A debe contener una infinidad de primos.

Para dar una respuesta a la pregunta 6, basta considerar a un entero n, ver que entre $(n+1)!+2$ y $(n+1)!+n+1$ hay n números compuestos sucesivos.

Cuando estudiamos la función $f(x) = x^2 - x + 41$, nos excitamos cuando empezamos a substituir a x por 1, 2, 3, ... 40, porque encontramos 40 primos y pensamos que hemos encontrado una fórmula para hallar a cualquier número primo, pero nos llevamos una gran desilusión al substituir $x = 41$, y vemos que $f(41)$ no es un primo. De manera similar sucede con la función $f(x) = x^2 - 79x + 1601$

Ahora para probar que un polinomio $f(x)$ el cual no es una constante y tiene coeficientes enteros no puede ser primo para todos los valores enteros de x y es compuesto para una infinidad de valores enteros de x, necesitamos estar un poco familiarizados con las propiedades de los polinomios.

Puesto que $f(x)$ no es una constante $|f(K)| > 1$, para algún entero K.

Hagamos $y = f(K)$ y consideremos $f(ty + K)$. Hay varias maneras de mostrar que $f(ty + K) = y Q + f(K)$, donde Q es un polinomio en t, y, K con coeficientes enteros. Por lo tanto $f(ty + K) = y(Q + 1)$ es divisible por $y = f(K)$ para todos los valores t. Puesto que $f(x)$ no es una constante, $f(ty + K)$ se incrementa en valor absoluto para t, suficientemente grande. Por lo tanto

para tales valores suficientemente grandes de t, el factor complementario $Q+1$ no es una unidad y por lo tanto $f(ty+K)$ es compuesto. Puesto que $ty+K$ llega a ser arbitrariamente grande con t, teniendo éste, digamos el mismo signo que y, se sigue que $f(x)$ fracasa para representar exactamente primos en una infinidad de casos y de hecho para todo $x = ty+K$ cuando t es suficientemente grande. Con esto damos una respuesta negativa a la pregunta 5.

Más adelante daremos la respuesta para la pregunta 4.

En lo que sigue nos dedicaremos a estudiar los números Perfectos, los cuales fueron investigados por los griegos y son interesantes.

Definición 6.

Un número Perfecto es aquel que es igual a la suma de todos sus divisores propios positivos.

Los primeros números perfectos, los cuales fueron conocidos por los griegos, son: $P_1 = 6$, $P_2 = 28$, $P_3 = 496$, $P_4 = 8\,128$, $P_5 = 33\,550\,336$, $P_6 = 8\,589\,869\,056$.

Primero probaremos un teorema que será útil para demostrar algunas afirmaciones sobre los números perfectos.

Teorema 13.

(Cataldi-Fermat). Si $2^n - 1$ es un primo entonces n también es prima

Demostración

Notemos que $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$. Supongamos que n no es primo, entonces lo podemos escribir como $n = rs$ con $r > 1$ y $s > 1$. De donde

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)\left((2^r)^{s-1} + (2^r)^{s-2} + \ldots + 2^r + 1\right)$$

Por lo tanto $2^n - 1$ es divisible por $2^r - 1$ el cual es mayor que 1 porque r también lo es. Esto significa que $2^n - 1$ no es primo.

Teorema 14.

El número $2^{n-1}(2^n - 1)$ es perfecto, si $2^n - 1$ es un primo.

Demostración

Los siguientes enteros positivos dividen a $N = 2^{n-1}(2^n - 1)$:

$$\begin{array}{ccc} 1 & y & 2^n - 1 \\ 2 & y & 2(2^n - 1) \\ 2^2 & y & 2^2(2^n - 1) \\ \vdots & & \vdots \\ 2^{n-1} & y & 2^{n-1}(2^n - 1) \end{array}$$

Así la suma de estos divisores es igual a:

$$\begin{aligned} \Sigma &= 1 + 2 + 2^2 + \ldots + 2^{n-1} + (2^n - 1) + 2(2^n - 1) + \ldots + 2^{n-1}(2^n - 1) \\ &= (1 + 2 + 2^2 + \ldots + 2^{n-1})[1 + (2^n - 1)] \\ &= (2^n - 1)2^n = 2N \end{aligned}$$

Pero como $2^n - 1 = P$ es un primo, los únicos divisores positivos de $N = 2^{n-1} P$ son todos los enlistados anteriormente.

Como en la suma incluimos a N entonces $\Sigma - N = N$, por lo tanto N es perfecto.

Teorema 15.

Cualquier número perfecto par es de la forma $2^{n-1}(2^n - 1)$, con $2^n - 1$ primo

Demostración.

Sea $N = 2^{n-1} F$ un número perfecto, donde F es un número impar. Sea Σ la suma de los divisores positivos de F. Los divisores positivos de N, incluyen a los divisores impares de F, sus duplicados, sus múltiplos de $4, \ldots,$ sus múltiplos de 2^{n-1}. No hay otros divisores positivos, puesto que N es perfecto tenemos

$$N = 2^{n-1} F = (1 + 2 + \ldots + 2^{n-1}) \Sigma - N$$

ó

$$2N = 2^n F = (2^n - 1) \Sigma$$

y puesto que Σ y F son enteros, debe ser $\frac{F}{2^n - 1}$ un entero. Así que $(2^n - 1) \mid F$ y $\frac{F}{2^n - 1}$ debe ser uno de los divisores de F.

Puesto que Σ es la suma de todos los divisores de F, vemos de la última igualdad, que los divisores de F pueden ser únicamente dos, es decir, F y $\frac{F}{2^n - 1}$. Pero 1 es un divisor de F. Por lo tanto

$\frac{F}{2^n - 1} = 1$, de donde $F = 2^n - 1$, y como $2^n - 1$ no tiene

otros divisores positivos, $2^n - 1$ es primo.

Teorema 16.

Cualquier número perfecto termina en 6 ó en 8.

Demostración

Si N es un número perfecto par entonces $N = 2^{p-1}(2^p - 1)$ con p primo. Cualquier primo mayor que 2 es de la forma $4m+1$ ó $4m+3$, puesto que de otra manera sería divisible por 2. Supongamos el primer caso, entonces

$$N = 2^{4m}\,(2^{4m+1} - 1) = 16^m(2 \cdot 16^m - 1) \text{ con } m \geq 1$$

Pero por inducción, es claro que 16^m siempre termina en 6. Por lo tanto $2 \cdot 16^m$ termina en 2, de donde $2 \cdot 16^m - 1$ termina siempre en 1 y en consecuencia N termina en 6. Similarmente, si $p = 4m+3$, tenemos que $N = 4 \cdot 16^m (8 \cdot 16^m - 1)$ y como $4 \cdot 16^m$ termina en 4 entonces $8 \cdot 16^m$ termina en 8, por lo tanto $8 \cdot 16^m - 1$ termina en 7. Asigue N termina en 8. Finalmente si $p = 2$, tenemos $N = P_1 = 6$, de esta manera podemos concluir que todos los perfectos pares deben terminar en 6 ó en 8.

II

Funciones Aritméticas

Las funciones que se presentan frecuentemente en la Teoría de los Números son $[x]$, $\varphi(n)$, $\tau(n)$, $\sigma_k(n)$, $\mu(n)$, $\Lambda(n)$, $\psi(x)$, $\Psi(x)$, etc. Algunas de ellas reciben el nombre de Funciones Aritméticas de acuerdo a la siguiente:

Definición 1.

Una función $f : \mathbb{Z}^+ \to \mathbb{Q}$ es llamada función Aritmética.

Son de particular interes aquellas funciones aritméticas que toman valores enteros como los primeros cinco que se definen a continuación.

Definición 2.

a) Para un número $x \in \mathbb{R}$, el símbolo $[x]$ denotará el máximo entero menor o igual a x, y recibe el nombre de función parte entera de x.

b) La función $\varphi(n)$ denota al número de enteros positivos menores o iguales a n y que además son primos relativos con n. A esta función se le conoce como la función φ de Euler.

c) La función $\tau(n)$ denotará al número de divisores positivos de n.

d) La función $\sigma_k(n)$, se encuentra definida por $\sigma_k = \sum_{d|n} d^k$, es decir, la suma de todas las k-ésimas potencias de los divisores de n. El caso particular cuando $k=1$ se denota

por $\sigma(n)$, que es únicamente la suma de los divisores positivos de n.

e) La función μ llamada la Función de Möbius está definida como:

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ es el producto de } r \text{ números primos distintos.} \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

f) La función $\Lambda(n)$ está definida por:

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m, \text{ para algún primo } p \text{ y algún } m \in \mathbb{Z}^+ \\ 0 & \text{en cualquier otro caso} \end{cases}$$

g) La función $\vartheta(x)$ denota a la suma

$$\vartheta(x) = \sum_{p \leq x} \log p$$

extendida sobre todos los primos $p \leq x$. Notemos que $\vartheta(x) = 0$ si $x < 2$.

h) La función ψ denota a la suma

$$\psi(x) = \sum_{p^m \leq x} \log p = \sum_{p \leq x} \left[\frac{\log x}{\log p} \right] \log p$$

y la suma termina para el primer entero positivo m tal que $x^{1/m+1} < 2$. Observemos que $\psi(x) = 0$ si $x < 2$. También la podemos definir como

$$\psi(x) = \sum_{1 \leq m \leq \log_2 x} \vartheta(x^{1/m})$$

puesto que

$$\psi(x) = \sum_{p^m \leq x} \log p = \sum_{m \geq 1} \sum_{p \leq x^{1/m}} \log p = \sum_{m \geq 1} \vartheta(x^{1/m})$$

$$= \sum_{1 \leq m \leq \log_2 x} \vartheta(x^{1/m})$$

Daremos sus propiedades y relaciones más conocidas, de las cuales haremos algunas demostraciones a continuación.

Teorema 1.

Sean $x, y \in \mathbb{R}$, entonces

i) $[x] \leq x < [x]+1$, $x-1 < [x] \leq x$, $0 \leq x-[x] < 1$

ii) $[x] = \sum_{1 \leq n \leq x} 1$ si $x \geq 0$

iii) $[x+m] = [x] + m$ si $m \in \mathbb{Z}$

iv) $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$

v)

$$[x] + [-x] = \begin{cases} 0 & \text{si } x \in \mathbb{Z} \\ 1 & \text{en cualquier otro caso} \end{cases}$$

vi) $\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right]$ si $m \in \mathbb{Z}^+$

vii) $x - [x]$ es la parte fraccionaria de x

viii) $-[-x]$ es el menor entero $\geq x$

ix) $\left[x + \frac{1}{2}\right]$ es el entero más próximo a x.

Si 2 enteros son igualmente próximos a x, es el mayor de los dos.

x) $-\left[-x + \frac{1}{2}\right]$ es el entero más próximo a x. Si dos enteros igualmente próximos a x, es el menor de los dos.

Demostración.

Solamente haremos las pruebas de (iv) y (vi) porque las demás se deducen de la definición de $[x]$.

iv) Escribamos $y = m + \alpha$ y $x = n + \beta$, donde $m, n \in \mathbb{Z}$ y $0 \leq \alpha, \beta < 1$, entonces $[x] + [y] = n + m \leq [n + \beta + m + \alpha] = n + m + [\beta + \alpha] \leq n + m + 1 = [x] + [y] + 1$

vi) Escribamos $x = n + \alpha$ y $n = qm + r$, donde $0 \leq \alpha < 1$ y $0 \leq r \leq m-1$, por lo que

$$\frac{x}{m} = \left[\frac{qm + r + \alpha}{m}\right] = q + \left[\frac{r+\alpha}{m}\right] = q$$

puesto que $0 \leq r + \alpha < m$. Por otro lado

$$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right] = \left[q + \frac{r}{m}\right] = q$$

Teorema 2.

Sea p un número primo, entonces el mayor exponente K tal que $p^K \mid n!$ esta dado por

$$K = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

Demostración

La suma realmente es finita porque si $p^i > n$, entonces $\left[\frac{n}{p^i}\right] = 0$. Haremos la prueba por inducción matemática. Es verdadero para $1!$, ya que $\frac{1}{p} < 1$ para todo primo p, de donde $\left[\frac{1}{p}\right] = 0$ y como $p^0 = 1$, $p^0 \mid 1!$.

Por lo tanto $0 = \sum_{i=1}^{\infty} \left[\frac{1}{p^i}\right]$. Supongamos que es

verdadero para $(n-1)!$ y denotemos por j el mayor entero tal que $p^j \mid n$. Dado que $n! = n(n-1)!$, basta probar que

$$\sum \left[\frac{n}{p^i}\right] - \sum \left[\frac{n-1}{p^i}\right] = j$$

como $\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right] = \begin{cases} 1 & \text{si } p^i \mid n \\ 0 & \text{si } p^i \nmid n \end{cases}$

Por lo tanto $\sum \left[\frac{n}{p^i}\right] - \sum \left[\frac{n-1}{p^i}\right] = j$

Teorema 3.

Si a y b son dos números irracionales positivos tales que $\frac{1}{a} + \frac{1}{b} = 1$, entonces las sucesiones $[an]$ y $[bn]$, donde n recorre a todos los enteros positivos, representan a Todos los enteros positivos sin repetición.

Demostración

Puesto que a y b son positivos tales que $\frac{1}{a} + \frac{1}{b} = 1$, se sigue que $a > 1$, y $b > 1$.

Haremos la demostración en dos partes

A. Mostraremos que no existen repeticiones en

las sucesiones $[an]$ y $[bn]$

i) En la sucesión $[an]$ no hay repeticiones porque $[an] < an < a(n+1) - 1 < [a(n+1)]$, por lo tanto $[an] < [a(n+1)]$ la primera desigualdad se sigue puesto que a y an son irracionales, la segunda desigualdad la obtenemos de $a > 1$. Similarmente no existen repeticiones en la sucesión $[bn]$.

ii) Para todos los enteros positivos n y m, podemos mostrar que $[an] \neq [bm]$. Porque si suponemos que

$$x = [an] = [bm], \text{ entonces}$$

$$an - 1 < x < an \text{ ó } n - \frac{1}{a} < \frac{x}{a} < n \text{ y}$$

$$bm - 1 < x < bm \text{ ó } m - \frac{1}{b} < \frac{x}{b} < n,$$

sumando las anteriores desigualdades y usando que $\frac{1}{a} + \frac{1}{b} = 1$, obtenemos $n+m-1 < x < n+m$. Así que el entero x se encuentra entre dos enteros sucesivos, lo cuales una contradicción.

B. Mostraremos que ningún entero x es omitido en ambas sucesiones. Porque si suponemos que x es tal entero, entonces deben existir m y n enteros tales que

$$an < [an] + 1 \leq x \leq [a(n+1)] < a(n+1) - 1 \text{ ó}$$

$$n < \frac{x}{a} < n + 1 - \frac{1}{a} \text{ y}$$

$$bm < [bm] + 1 \leq x \leq [b(m+1)] - 1 < b(m+1) - 1 \text{ ó}$$

$$m < \frac{x}{b} < m + 1 - \frac{1}{b}$$

sumando las desigualdades anteriores y usando $\frac{1}{a} + \frac{1}{b} = 1$, encontramos que $n+m < r < n+m+1$, lo cual es una contradicción.

Habiendo establecido las partes A y B terminamos la demostración del teorema.

Teorema 4.

Para cada número primo p, tenemos $\varphi(p^m) = p^m\left(1 - \frac{1}{p}\right)$, donde $m \in \mathbb{Z}^+$

Demostración.

Procedemos contando a los números enteros positivos menores que p^m que no son primos relativos a p^m. Claramente un entero n tiene un factor más grande que 1 en común con p^m si y solo si: $p \mid n$. Por lo tanto, los enteros positivos menores o iguales a p^m que no son primos relativos con p^m, son los p^{m-1} múltiplos de p, es decir, $p, 2p, 3p, \ldots, p^m$. En consecuencia hay $p^m - p^{m-1}$ enteros positivos menores que p^m y primos relativos con p^m, lo que significa $\varphi(p^m) = p^m - p^{m-1} = p^m\left(1 - \frac{1}{p}\right) = p^{m-1}(p-1)\, p^m$. Una consecuencia inmediata es:

Corolario 1. i) $\varphi(p) = p - 1$ para todo primo p

ii) $1 + \sum_{K=1}^{n} \varphi(p^K) = p^n$

Teorema 5. $\sum_{d|n} \varphi(d) = n$, donde $\sum_{d|n} \varphi(d)$ denota la suma de los valores de la función φ que toma para todos los divisores de n.

Demostración.

Consideremos el conjunto $S = \{1, 2, 3, 4, \ldots n\}$

Distribuimos a los enteros de S en conjuntos ajenos como sigue: Para cada divisor d de n, sea

$$A(d) = \{ K \mid (K, n) = d, \quad 1 \leq K \leq n \}$$

es decir, $A(d)$ contiene aquellos elementos de S los cuales tienen como m.c.d. a d con n. Los conjuntos $A(d)$ forman una colección disjunta cuya unión es S. Por lo tanto si $f(d)$ denota el número de enteros en $A(d)$ tenemos $\sum_{d|n} f(d) = n$

Pero $(K, n) = d$ si y solo si $\left(\frac{K}{d}, \frac{n}{d}\right) = 1$ y

$0 < K \leq n$ si y solo si $0 < \frac{K}{d} \leq \frac{n}{d}$

Por lo tanto, si consideramos a $q = \frac{K}{d}$, existe una correspondencia uno a uno entre los elementos de $A(d)$

y aquellos enteros q que satisfacen

$$0 \leq q \leq \frac{n}{d}\,,\ \left(q, \frac{n}{d}\right) = 1$$

El número de tales q es $\varphi\left(\frac{n}{d}\right)$. Por lo tanto $f(d) = \varphi\left(\frac{n}{d}\right)$, de donde

$$\sum_{d|n} f(n) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$$

Pero esto es equivalente a la afirmación $\sum_{d|n} \varphi(d) = n$,

porque cuando d recorre a todos los divisores de n también lo hace $\frac{n}{d}$.

Teorema 6.

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, entonces

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1) \quad y$$

$$\tau(1) = 1$$

Demostración.

Sea $n \in \mathbb{Z}^+$ y consideremos $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, entonces todos los divisores positivos de n, son de la forma $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$, donde

$$0 \leq \beta_i \leq \alpha_i \quad y \quad i = 1, 2, 3, \ldots, r$$

Ahora por un principio de combinatoria, se sigue que β_1 puede ser elegido en $\alpha_1 + 1$ maneras, β_2 puede ser escogido de $\alpha_2 + 1$ formas, ..., y β_r puede ser elegido en $\alpha_r + 1$ maneras, entonces $\beta_1, \beta_2, \ldots \beta_r$ pueden ser seleccionados todos juntos de $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1)$ maneras. Por lo tanto encontramos que el número $\tau(n)$ de divisores positivos de n está dado exactamente por

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

Teorema 7.

$\tau(n)$ es impar si y sólo si n es cuadrado.

Teorema 8.

Si $(m,n) = 1$, entonces $\tau(mn) = \tau(m)\tau(n)$

Demostración

Consideremos a m y n en su forma estandar, es decir, $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ y $n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_k^{\beta_k}$

Como $(m,n) = 1$, entonces $p_i^{\alpha_i} \neq q_j^{\beta_j}$, $\forall \alpha_i, \beta_j$

además $mn = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} q_1^{\beta_1} \ldots q_k^{\beta_k}$ y si denotamos a $p_{r+j}^{\alpha_{r+j}} = q_j^{\beta_j}$ donde $\alpha_{r+j} = \beta_j$, para

$j = 1, \dots k$) obtenemos $mn = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} \dots$

$p_{r+k}^{\alpha_{r+k}}$ entonces

$$\sigma(mn) = \prod_{i=1}^{r+k} (\alpha_i + 1) = \prod_{i=1}^{r} (\alpha_i + 1) \prod_{j=r+1}^{k} (\alpha_j + 1)$$

$$= \sigma(m)\sigma(n)$$

Teorema 9.

Si: $(n, m) = 1$ entonces $\tau(mn) = \tau(n)\tau(m)$

Demostración.

$$\tau(nm) = \sum_{d \mid nm} d = \sum_{\substack{d_1 \mid n \\ d_2 \mid m}} d_1 d_2$$

$$\tau(nm) = \left(\sum_{d_1 \mid n} d_1 \right) \left(\sum_{d_2 \mid m} d_2 \right) = \tau(n)\tau(m)$$

Las igualdades anteriores se cumplen por la hipótesis $(n, m) = 1$.

Teorema 10.

Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ entonces

$$\tau(n) = \prod_{i=1}^{r} \frac{p^{\alpha_i+1} - 1}{p_i - 1}$$

Demostración.

Por definición tenemos:

$\tau(p_i^{\alpha_i}) = 1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}$ de donde

$$\tau(p_i^{\alpha_i}) = \frac{p^{\alpha_i+1} - 1}{p_i - 1}, \text{ aplicando reiteradamente}$$

el teorema anterior obtenemos

$$\tau(n) = \prod_{i=1}^{r} \tau(p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p^{\alpha_i+1} - 1}{p_i - 1}$$

Teorema 11.

Si $n \in \mathbb{Z}^+$ entonces:

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Demostración.

La fórmula es verdadera para $n = 1$.

Supongamos que $n > 1$ y escribimos a $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

En la suma $\sum_{d|n} \mu(d)$ los únicos términos distintos de cero provienen cuando $d=1$ y de aquellos divisores de n los cuales son productos de primos distintos. Así:

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(P_1) + \ldots + \mu(P_K) + \mu(P_1 P_2) + \ldots \mu(P_{K-1} P_K) +$$

$$+ \ldots + \mu(P_1 P_2 \ldots P_K) = 1 + \binom{K}{1}(-1) + \binom{K}{2}(-1)^2 +$$

$$\ldots + \binom{K}{K}(-1)^K = (1-1)^K = 0$$

Teorema 12.

Si $(n,m)=1$ entonces $\mu(nm) = \mu(n)\mu(m)$

Demostración.

Si m ó n tienen un factor primo cuadrado entonces mn también lo tiene, de donde $\mu(nm)$ y $\mu(n)\mu(m)$ son cero. Si ninguno de ellos tiene un factor primo cuadrado podemos escribirlos en la forma $m = P_1 P_2 \ldots P_s$ y $n = q_1 q_2 \ldots q_t$, donde P_i y q_j son primos distintos. Entonces $\mu(m) = (-1)^s$, $\mu(n) = (-1)^t$ y $\mu(nm) = (-1)^{s+t}$, por lo tanto $\mu(nm) = \mu(n)\mu(m)$

Teorema 13.

Si $n \in \mathbb{Z}^+$ entonces $\log n = \sum_{d|n} \Lambda(d)$

Demostración.

Para $n=1$ se cumple la igualdad, pues ambos miembros son iguales a cero. Ahora supon-

gamos que $n > 1$ y escribimos $n = \prod_{K=1}^{r} p_K^{\alpha_K}$, tomando

logaritmos obtenemos

$$\log n = \sum_{K=1}^{r} \alpha_K \log p_K$$

Consideremos

$$\sum_{d|n} \Lambda(d) = \sum_{K=1}^{r} \sum_{m=1}^{d_K} \Lambda(p_K^m) = \sum_{K=1}^{r} \sum_{m=1}^{\alpha_K} \log p_K =$$

$$= \sum_{K=1}^{r} \alpha_K \log p_K = \log n$$

puesto que los únicos términos no cero en la suma son los divisores $d = p_K^m$ para $m = 1, 2, \ldots, \alpha_K$

Teorema 14.

Fórmula de inversión de Möbius.

Si dos funciones aritméticas $f(n)$ y $g(n)$ satisfacen una de las 2 condiciones:

1) $f(n) = \sum_{d|n} g(d)$

o'

2) $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$

para cada n, entonces satisfacen ambas condiciones.

Demostración.

Supongamos que $f(n) = \sum_{d|n} g(d)$

entonces:

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{dd'=n} \mu(d) f(d') = \sum_{dd'=n} \mu(d) \sum_{e|d'} g(e) =$$

$$= \sum_{de\,h=n} \mu(d)\, g(e) = \sum_{eh'=n} g(e) \sum_{d|h'} \mu(d)$$

pero $\sum_{d|h'} \mu(d) = \begin{cases} 1 & \text{si } h'=1 \\ 0 & \text{si } h'>1 \end{cases}$

Por lo tanto $\sum_{d|h} \mu(d) f\left(\frac{n}{d}\right) = g(n)$

Ahora supongamos que $g(n) = \sum_{d|h} \mu(d) f\left(\frac{n}{d}\right)$

$$\sum_{d|n} g(d) = \sum_{d|n} \sum_{d'|d} \mu(d') f\left(\frac{d}{d'}\right) = \sum_{d'ef=n} \mu(d') f(e) =$$

$$= \sum_{eh'=n} f(e) \sum_{d'|h'} \mu(d') = f(n)$$

Teorema 15.

Si $n \in \mathbb{Z}^+$ entonces $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Demostracion.

Sean $f(n)=n$, $g(n)=\varphi(n)$

Por el teorema 5, $f(n)=n=\sum_{d|n}\varphi(d)=\sum_{d|n}g(d)$

entonces por el teorema 14, $\varphi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$

Demostraremos ahora que $\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})$

Para $n=1$, el producto es vacio puesto que no hay primos que dividan a 1. En este caso entenderemos que al producto le asignamos el valor 1.

Supongamos entonces que $n>1$ y sean $p_1, p_2, \ldots, p_r$ los divisores primos distintos de n. El producto puede ser escrito como

$$\prod_{p|n}(1-\frac{1}{p})=\prod_{i=1}^{r}(1-\frac{1}{p_i})=1-\sum\frac{1}{p_i}+\sum\frac{1}{p_i p_j}-$$

$$\sum\frac{1}{p_i p_j p_k}+\cdots+\frac{(-1)^r}{p_1 p_2 \ldots p_r}$$

En el lado derecho, en cada termino como $\sum\frac{1}{p_i p_j p_k}$ entenderemos que considerando a todos los posibles productos $p_i p_j p_k$ de factores primos distintos de n tomados de 3 a la vez. Notemos que cada termino del lado derecho de la igualdad es la forma $\pm\frac{1}{d}$ donde d es un divisor de n el

cual es 1 o producto de primos distintos. El numerador ± 1 es exactamente $\mu(d)$. Puesto que $\mu(d)=0$ si d es divisible por el cuadrado de cualquier p_i, vemos que la suma es exactamente $\sum_{d|n} \frac{\mu(d)}{d}$

Como $\prod_{p|n} \left(1-\frac{1}{p}\right) = \sum_{d|n} \frac{\mu(d)}{d}$ entonces

$$n \prod_{p|n} \left(1-\frac{1}{p}\right) = \sum_{d|n} \mu(d)\,\frac{n}{d}$$

por lo tanto $\varphi(n) = n \prod_{p|n} \left(1-\frac{1}{p}\right)$

Teorema 16.

Si $n \in \mathbb{Z}^+$ entonces $\Lambda(n) =$

$$\sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(n) \log d$$

Demostración.

Invirtiendo la fórmula del teorema 13, usando el teorema 14 obtenemos

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d$$

$$= \left[\frac{1}{n}\right] \log n - \sum_{d|n} \mu(d) \log d$$

Puesto que

$\left[\frac{1}{n}\right] \log n = 0$ para toda n, obtenemos

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d$$

Teorema 17.

$$\sum_{K=1}^{[x]} \psi\left(\frac{x}{K}\right) =$$

$$= \sum_{p \le x} \left(\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \dots \right) \log p =$$

$$= \log [x]!$$

y

$$\sum_{K=1}^{[x]} (-1)^{K-1} \psi\left(\frac{x}{K}\right) =$$

$$= \log [x]! - 2 \log \left[\tfrac{1}{2} x\right]!$$

Las funciones ψ, Σ, ∇_K, μ tienen otra característica que ya hemos encontrado en Σ y en μ, que queda enmarcada en la siguiente:

Definición 3.

Una función aritmética f se dice que es multiplicativa si y sólo si:

1) $f(n) f(m) = f(nm)$ cuando $(n,m)=1$
2) $f \neq 0$

Algunas propiedades de las funciones multiplicativas son:

Teorema 18.

Si $f(n)$ es multiplicativa entonces $g(n) = \sum_{d|n} f(d)$ es también multiplicativa.

Teorema 19.

Si f es multiplicativa entonces $f(1) = 1$.

Teorema 20.

f es multiplicativa si y sólo si

$$f(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}) =$$

$$= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_r^{\alpha_r})$$

para todos los primos p_i y todos los enteros $\alpha_i \geq 1$.

Teorema 21.

Si f es multiplicativa entonces

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p))$$

III

CONGRUENCIAS

Gauss introduce una noción la cual simplifica muchos problemas concernientes a la divisibilidad en los enteros. Así él creó una nueva área de la Teoría de los Números llamada Teoría de Congruencias. La esencia de esta noción es su notación.
Empezamos a desarrollar esta idea con su definición.

Definición 1.

Dados los enteros a, b, m con $m>0$. Decimos que a es congruente con b módulo m y lo escribimos $a \equiv b \pmod{m}$, si m divide a la diferencia $a-b$. El número m es llamado el módulo de la congruencia.

En otras palabras la congruencia $a \equiv b \pmod{m}$ es equivalente a la relación de divisibilidad $m \mid (a-b)$.

En particular, $a \equiv 0 \pmod{m}$ si y sólo si $m \mid a$. Por lo tanto $a \equiv b \pmod{m}$ si y solo si $a - b \equiv 0 \pmod{m}$.
Si $m \nmid (a-b)$ escribimos $a \not\equiv b \pmod{m}$ y decimos que a y b son incongruentes módulo m.

Ejemplos

1) $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $3^2 \equiv 1 \pmod{5}$.

2) n es par si y sólo si $n \equiv 0 \pmod{2}$

3) n es impar si y sólo si $n \equiv 1 \pmod 2$.

4) $a \equiv b \pmod 1$ para cualquiera a y b.

5) Si: $a \equiv b \pmod m$ entonces $a \equiv b \pmod d$ cuando $d \mid m$, $d > 0$.

El símbolo de congruencia $\equiv$ fue elegido por Gauss para sugerir una analogía con el signo de igualdad. Los dos teoremas siguientes muestran que las congruencias realmente poseen muchas de las propiedades formales de las ecuaciones.

Teorema 1.

Si: $a \equiv b \pmod m$ y $\alpha \equiv \beta \pmod m$ entonces

1) $ax + \alpha y \equiv bx + \beta y \pmod m \quad \forall x, y \in \mathbb{Z}$

2) $a\alpha \equiv b\beta \pmod m$

3) $a^n \equiv b^n \pmod m \quad \forall n \in \mathbb{Z}^+$

4) $f(a) \equiv f(b) \pmod m$ para cualquier polinomio f con coeficientes enteros.

Demostración.

Haremos la prueba sólo de (1) y (2)

1) Puesto que $m \mid (a-b)$ y $m \mid (\alpha - \beta)$ tenemos

$$m \mid x(a-b) + y(\alpha - \beta) = (ax + \alpha y) - (bx + \beta y)$$

2) Notemos que $a\alpha - b\beta = \alpha(a-b) + b(\alpha - \beta) \equiv 0 \pmod{m}$

Habiendo investigado el comportamiento de las congruencias bajo la adición y la multiplicación, es natural considerar qué podemos hacer con respecto a la división. Un simple ejemplo muestra que en general

$ac \equiv bc \pmod{m}$ no implica $a \equiv b \pmod{m}$, por ejemplo

$6 \equiv 3 \pmod{3}$ pero $2 \not\equiv 1 \pmod{3}$

sin embargo podemos considerar otras situaciones.

Teorema 2.

1) Si $c > 0$ entonces $a \equiv b \pmod{m}$ si y sólo si $ac \equiv bc \pmod{m}$.
2) Si: $ac \equiv bc \pmod{m}$ y $d = (c, m)$ entonces $a \equiv b \pmod{\frac{m}{d}}$.
3) Supongamos que $a \equiv b \pmod{m}$. Si: $d \mid m$ y $d \mid a$ entonces $d \mid b$.
4) Si: $a \equiv b \pmod{m}$ entonces $(a, m) = (b, m)$.
5) Si: $a \equiv b \pmod{m}$ y $0 \leq |b - a| < m$ entonces $a = b$.
6) $a \equiv b \pmod{m}$ si y sólo si a y b tienen el mismo residuo cuando son divididos por m.
7) Si: $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$ donde $(n, m) = 1$ entonces $a \equiv b \pmod{mn}$.

La noción de congruencias módulo un entero m fijo es una relación de equivalencia natural en el siguiente sentido:

1) Propiedad reflexiva: $a \equiv a \pmod{m}$
2) Propiedad simétrica: Si $a \equiv b \pmod{m}$ entonces $b \equiv a \pmod{m}$
3) Propiedad transitiva: Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ entonces $a \equiv c \pmod{m}$.

Como una relación de equivalencia la idea de congruencia módulo m separa a los enteros en clases de equivalencia, donde los enteros de una clase son aquellos enteros que son congruentes módulo m.

Dado cualquier entero a y aplicando el algoritmo de la división obtenemos $a = qm + r$, $0 \leq r < m$ ó $a - r = qm$. Así $a \equiv r \pmod{m}$, donde r es uno de los enteros $0, 1, 2, 3, \ldots, m-1$, es decir, cualquier entero es congruente módulo m exactamente con uno de estos residuos. Denotamos a la clase de congruencia módulo m que contiene a r por $\bar{r}$, vemos que los m conjuntos mutuamente ajenos $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$ incluyen a todos los enteros.

Definición 2.

> Las clases $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$ son llamadas las clases de residuo módulo m. Cualquier conjunto de representantes, uno de cada uno de estas clases, es llamado un sistema completo de residuos módulo m.

Así, por ejemplo, los enteros $0, 1, 2, \ldots, m-1$ constituyen un sistema completo de residuos módulo m.

Claramente los conjuntos

$$\{1, m+2, 2m+3, 3m+4, \ldots, m^2\}$$

y

$$\{m, 2m+1, 3m+2, \ldots, (m-2)m+(m-1)\}$$

también constituyen sistemas completos de residuos módulo m.

Damos a continuación algunas de las propiedades que son consecuencias inmediatas de la definición de clases residuales.

Teorema 3.

1) $\bar{a} = \bar{b}$ si y sólo si $a \equiv b \pmod{m}$.

2) Dos enteros x e y están en la misma clase residual si y sólo si $x \equiv y \pmod{m}$.

3) Las m clases residuales $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$ son disjuntas y su unión es el conjunto de los enteros.

Teorema 4.

Supongamos que $(K, m) = 1$.

Si $\{a_1, a_2, \ldots, a_m\}$ es un sistema completo de residuos módulo m entonces $\{Ka_1, Ka_2, \ldots Ka_m\}$ también lo es.

Hasta el momento hemos estudiado congruencias numéricas, sin embargo también existen congruencias polinomiales que ya hemos mencionado en el teorema 1, de las cuales haremos un breve análisis.

Empezemos considerando únicamente a los polinomios $f(x)$ con coeficientes enteros, así que de esta manera cuando evaluamos en un entero x, $f(x)$ también es entero y podemos aplicar a estos la noción de congruencia. Un entero x que satisface una congruencia polinomial $f(x) \equiv 0 \pmod{m}$ es llamado una solución de la congruencia. Por supuesto si $x \equiv y \pmod{m}$ entonces $f(x) \equiv f(y) \pmod{m}$, así cualquier congruencia que tiene una solución, tiene también una infinidad. Por lo tanto hacemos la convención de que las soluciones que pertenecen a la misma clase residual no serán pensadas como distintas, y cuando hablamos de el número de soluciones de la congruencia $f(x) \equiv 0 \pmod{m}$ pensamos en el número de soluciones contenidas en el conjunto $\{1, 2, \ldots, m\}$ o en cualquier otro sistema completo de residuos módulo m. Por lo tanto cualquier congruencia polinomial módulo m, tiene a lo más m soluciones.

Ejemplos:

1) La congruencia lineal $2x \equiv 3 \pmod{4}$ no tiene soluciones, puesto $2x - 3$ es impar para cualquier x y por lo tanto no puede ser divisible por 4.

2) La congruencia cuadrática $x^2 \equiv 1 \pmod{8}$ tiene exactamente 4 soluciones dadas por $x \equiv 1, 3, 5, 7 \pmod{8}$

La teoría de las congruencias lineales está completamente descrito por los siguientes tres teoremas.

Teorema 5.

Supongamos que $(a, m) = 1$. Entonces la congruencia lineal $ax \equiv b \pmod{m}$ tiene exactamente una solución.

Demostración.

Unicamente necesitamos probar con los números $1, 2, 3, \ldots, m$, puesto que ellos constituyen un sistema completo de residuos. Por lo tanto formamos los productos $a, 2a, \ldots, am$. Puesto que $(a, m) = 1$ estos números también constituyen un sistema completo de residuos. Por lo tanto exactamente uno de estos productos es congruente con b módulo m, es decir, existe exactamente un x que satisface $ax \equiv b \pmod{m}$.

Si $(a, m) = 1$ la única solución de la congruencia $ax \equiv 1 \pmod{m}$ es llamada el recíproco de a módulo m. Si a' es el recíproco de a entonces ba' es solución de $ax \equiv b \pmod{m}$.

Teorema 6.

Supongamos que $(a, m) = d$. Entonces la congruencia lineal $ax \equiv b \pmod{m}$ tiene soluciones si y sólo si $d \mid b$.

Demostración

Si una solución existe entonces $d \mid b$ puesto que $d \mid a$ y $d \mid m$. Inversamente, si $d \mid b$ la congruencia

$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, tiene una solución puesto que

$\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ y esta solución también es solución de

$ax \equiv b \pmod{m}$.

Teorema 7.

Supongamos que $(a,m)=d$ y $d|b$. Entonces la congruencia lineal $ax \equiv b \pmod{m}$ tiene exactamente d soluciones módulo m. Estas están dadas por

$$t,\ t+\frac{m}{d},\ t+2\frac{m}{d},\ \ldots,\ t+(d-1)\frac{m}{d},$$

donde t es la solución única módulo $\frac{m}{d}$ de la congruencia lineal

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Demostración.

Cualquier solución de $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ también es solución de $ax \equiv b \pmod{m}$. Inversamente, cualquier solución de $ax \equiv b \pmod{m}$ satisface

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Ahora los d números enlistados son soluciones de

$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$, por lo tanto de $ax \equiv b \pmod{m}$.

Dos o dos no son congruentes módulo m puesto que las relaciones

$$t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{\frac{m}{d}} \quad \text{con } 0 \leq r < d,\ 0 \leq s < d$$

implican $r\frac{m}{d} \equiv s\frac{m}{d} \pmod{m}$ y por lo tanto

$r \equiv s \pmod{m}$ pero $0 \leq |r-s| < d$, así que $r = s$.

Mostremos que $ax \equiv b \pmod{m}$ no tiene más soluciones que las que hay en la lista. Si y es una solución de $ax \equiv b \pmod{m}$ entonces $ay \equiv at \pmod{m}$, así que

$y \equiv t \left(\mod \frac{m}{d}\right)$. Por lo tanto $y = t + K\frac{m}{d}$ para alguna K.

Pero $K \equiv r \pmod{d}$ para alguna r que satisface $0 \leq r < d$. Por lo tanto

$$K\frac{m}{d} \equiv r\frac{m}{d} \pmod{m} \quad \text{así que}$$

$$y \equiv t + r\frac{m}{d} \pmod{m}$$

Por lo tanto y es congruente módulo m con uno de los números de la lista.

Corolario 1.

Si $(a,b) = d$, existen x e y enteros tales que $ax + by = d$

Definición 3.

Por un sistema reducido de residuos módulo m pensaremos en cualquier conjunto de $\varphi(m)$ enteros incongruentes módulo m, cada uno de los cuales es primo relativo con m.

Teorema 8.

Si $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ es un sistema reducido de residuos módulo m y si $(K, m) = 1$, entonces $\{Ka_1, Ka_2, \ldots, Ka_{\varphi(m)}\}$ también es un sistema reducido de residuos módulo m.

Teorema 9.

(Euler - Fermat). Supongamos que $(a, m) = 1$.
Entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demostración.

Sea $\{b_1, b_2, \ldots, b_{\varphi(m)}\}$ un sistema reducido de residuos módulo m. Entonces $\{ab_1, ab_2, \ldots, ab_{\varphi(m)}\}$ es también un sistema reducido de residuos. Por lo tanto el producto de todos los enteros en el primer conjunto, es decir, $b_1 b_2 \cdots b_{\varphi(m)} \equiv a^{\varphi(m)} b_1 b_2 \cdots b_{\varphi(m)} \pmod{m}$

cada b_i tiene la propiedad $(b_i, m) = 1 \ \forall \ i = 1, 2, \ldots, \varphi(m)$, por lo que podemos cancelar a cada b_i y obtener

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Teorema 10.

Si: $p \nmid a$, p un primo, entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

Teorema 11.

Para cualquier entero a y cualquier primo p tenemos

$$a^p \equiv a \pmod{p}$$

El teorema 9 puede ser usado para calcular las soluciones de las congruencias lineales.

Teorema 12.

Si: $(a, m) = 1$, la solución (única módulo m) de la congruencia lineal $ax \equiv b \pmod{m}$ esta dada por

$$x \equiv ba^{\varphi(m)-1} \pmod{m}$$

Ejemplos.

1) La solución de $5x \equiv 3 \pmod{24}$ es $x \equiv 15 \pmod{24}$ puesto que $(5, 24) = 1$ existe una única solución, utilizando

el teorema 12 tenemos $x \equiv 3 \cdot 5^{\varphi(24)-1} \equiv 3 \cdot 5^{7} \pmod{24}$, puesto que $\varphi(24) = \varphi(3)\,\varphi(8) = 24$, módulo 24 tenemos $5^2 \equiv 1$ y $5^7 \equiv 5^6 \equiv 1$, $5^7 \equiv 5$ así que $x \equiv 15 \pmod{24}$

2) Las soluciones de

$25x \equiv 15 \pmod{120}$ son $x \equiv 15, 39, 63, 87, 111 \pmod{120}$.
Puesto que

$d = (25, 120) = 5$ y $d \mid 15$, la congruencia

tiene exactamente 5 soluciones módulo 120.
Para encontrar estas dividimos por 5 y resolvemos la congruencia $5x \equiv 3 \pmod{24}$ de acuerdo al ejemplo 1 y el teorema 7, encontramos que las cinco soluciones están dadas por $x = 15 + 24K$, $K = 0, 1, 2, 3, 4$.

Trataremos ahora congruencias polinomiales módulo un primo que son interesantes para hablar de las soluciones de ellas.

Teorema 13.
(Lagrange). Dado un primo p, sea

$f(x) = C_0 + C_1 x + C_2 x^2 + \dots + C_n x^n$ un polinomio de grado n con coeficientes enteros tal que $C_n \not\equiv 0 \pmod{p}$. Entonces la congruencia polinomial $f(x) \equiv 0 \pmod{p}$ tiene a lo más n soluciones.

Observamos que este resultado no es verdadero para módulos compuestos. Por ejemplo, la congruencia cuadrática $x^2 \equiv 1 \pmod 8$ tiene 4 soluciones.

Demostración.

Usamos inducción sobre n, el grado de f. Cuando $n=1$ la congruencia es lineal $c_1 x + c_0 \equiv 0 \pmod p$. Puesto que $c_1 \not\equiv 0 \pmod p$, tenemos $(c_1, p) = 1$ y existe exactamente una solución. Supongamos, entonces que el teorema es verdadero para polinomios de grado $n-1$, también supongamos que la congruencia $f(x) \equiv 0 \pmod p$ tiene $n+1$ soluciones incongruentes módulo p, digamos $x_0, x_1, x_2, \ldots, x_n$, donde $f(x_k) \equiv 0 \pmod p$ para cada $k = 0, 1, \ldots, n$. Obtendremos una contradicción. Tenemos la identidad algebraica

$$f(x) - f(x_0) = \sum_{r=1}^{n} c_r (x^r - x_0^r) = (x - x_0)\, g(x), \text{ donde}$$

$g(x)$ es un polinomio de grado $n-1$ con coeficientes enteros y entre ellos a c_n. Así $f(x_k) - f(x_0) = (x_k - x_0) g(x_k) \equiv 0 \pmod p$ puesto que $f(x_k) \equiv f(x_0) \equiv 0 \pmod p$. Pero $x_k - x_0 \not\equiv 0 \pmod p$. Si $k \neq 0$, por lo que debemos tener $g(x_k) \equiv 0 \pmod p$ para cada $k \neq 0$. Pero esto significa que la congruencia $g(x) \equiv 0 \pmod p$ tiene n soluciones incongruentes módulo p, contradiciendo a nuestra hipótesis de inducción.

Teorema 14.

Si $f(x) = c_0 + c_1 x + \ldots + c_n x^n$ es un polinomio de grado n con coeficientes enteros y si la congruencia $f(x) \equiv 0 \pmod p$ tiene más de n soluciones, donde p es primo entonces

cualquier coeficiente de f es divisible por p.

Teorema 15.

Para cualquier primo p, todos los coeficientes de el polinomio $f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$ son divisibles por p.

Teorema 16.

(Wilson). Para cualquier primo p tenemos $(p-1)! \equiv -1 \pmod{p}$

Teorema 17.

Para cualquier primo $p \geq 5$ tenemos

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$$

Un sistema de dos o más congruencias lineales no necesariamente tiene una solución, aun cuando cada congruencia individual tengan una solución.

Por ejemplo no existe x la cual satisfaga simultáneamente a $x \equiv 1 \pmod 2$ y $x \equiv 0 \pmod 4$, aun cuando cada una por separado tienen soluciones, En este ejemplo los módulos 2 y 4 no son primos relativos. Probaremos que cualquier sistema de dos o más congruencias lineales las cuales se pueden resolver separadamente con soluciones únicas se pueden también resolver simultáneamente si los módulos son primos relativos en pares.

Comenzamos con un caso especial.

Teorema 18.

(Teorema Chino del Residuo). Supongamos que $m_1, m_2, \dots, m_r$ son enteros positivos y primos relativos en pares, es decir,

$(m_j, m_k) = 1$ si $j \neq k$.

Sean $b_1, b_2, \dots, b_r$ enteros arbitrarios.

Entonces el sistema de congruencias

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

tiene exactamente una solución módulo el producto $m_1 m_2 \cdots m_r$.

Demostración.

Sean $M = m_1 m_2 \cdots m_k$ y $M_k = \frac{M}{m_k}$. Entonces $(M_k, m_k) = 1$. Así cada M_k tiene un único recíproco M'_k módulo m_k. Ahora sea $x = b_1 M_1 M'_1 + \dots + b_r M_r M'_r$. Consideramos cada término en esta suma módulo m_k. Puesto que $M_i \equiv 0 \pmod{m_k}$ si $i \neq k$, tenemos

$$x \equiv b_k M_k M'_k \equiv b_k \pmod{m_k}.$$

Por lo tanto x satisface cualquier congruencia del sistema.

Es fácil mostrar que el sistema tiene una única solución mod M, de hecho, si x e y son dos soluciones de el sistema tenemos $x \equiv y \pmod{m_K}$ para cada K, puesto que los m_K son primos relativos en pares, por lo tanto tenemos $x \equiv y \pmod{M}$.

Teorema 19.

Supongamos que $m_1, m_2, \dots, m_r$ son primos relativos en pares. Sean $b_1, \dots, b_r$ enteros arbitrarios y $a_1, a_2, \dots, a_r$ que satisfacen $(a_K, m_K) = 1$ para $K = 1, 2, \dots, r$. Entonces el sistema lineal de congruencias

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \quad\quad \vdots \\ a_r x \equiv b_r \pmod{m_r} \end{cases}$$

tiene exactamente una solución módulo $m_1 m_2 \dots m_K$.

Teorema 20.

Sea f un polinomio con coeficientes enteros, sean $m_1, m_2, \dots, m_r$ enteros positivos primos relativos por pares y sea $m = m_1 m_2 \dots m_r$. Entonces la congruencia $f(x) \equiv 0 \pmod{m}$ tiene una solución si y sólo si cada una de las congruencias:

$f(x) \equiv 0 \pmod{m_i}$ $(i = 1, 2, \cdots, r)$
tiene una solución. Más aún,
si $v(m)$ y $v(m_i)$ denotan el
número de soluciones de
$f(x) \equiv 0 \pmod{m}$ y $f(x) \equiv 0 \pmod{m_i}$
respectivamente; entonces
$v(m) = v(m_1)\, v(m_2) \cdots v(m_r)$.

IV

El Teorema De Dirichlet Y El Teorema De Los Números Primos

En esta parte desarrollamos dos afirmaciones que conciernen a la infinidad de primos en una progresión aritmética y a la manera en la cual están distribuidos los primos, que son conocidos como El Teorema de Dirichlet y El Teorema de los Números Primos, respectivamente.

Legendre formulo en 1808, la primera afirmación que dice: Sean K y l enteros tales que $(K, l) = 1$, entonces existe un número infinito de primos de la forma $l + Kn$, $(n = 0, 1, 2, \ldots)$. La demostración de esta fue dada por Dirichlet en 1837, por lo que lleva su nombre. En esta demostración desarrollo dos ideas radicalmente nuevas, la primera fue introducir las funciones aritméticas llamadas Caracteres y denotadas como $X : \mathbb{Z}^{+} \longrightarrow \mathbb{C}$, la segunda fue asociar a cada carácter y cada número real $s > 1$, por medio de las series infinitas

$$L(S, X) = \sum_{n=1}^{\infty} \frac{X(n)}{n^s}$$

También Legendre publicó una afirmación cercana al Teorema de los Números Primos en 1798, él afirmo que $\pi(x)$ es de la forma $x/(A \log x + B)$, donde $\pi(x)$ = número de primos p que satisfacen $2 \leq p \leq x$ y A, B son constantes, que es bastante parecida a la

afirmación que $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$, que es el enunciado del Teorema de los Números Primos. Legendre después refinó su conjetura en 1808, para afirmar que

$$\widetilde{\pi}(x) = \frac{x}{\log x + A(x)}$$

donde $A(x)$ es "aproximadamente $1.08366\ldots$", es decir, $\lim_{x\to\infty} A(x) = 1.08366\ldots$.

Aunque Legendre fue la primera persona en publicar en forma conjetural El Teorema de los Números Primos, Gauss poseía ya un extenso trabajo sobre la teoría de primos en 1792-93 y sospechó que la densidad con la cual ocurren los primos en una vecindad del entero n es de $1/\log n$, así que el número de primos en el intervalo $[a,b]$ será aproximadamente igual a

$$\int_a^b \frac{dx}{\log x}$$

, aunque él nunca publicó sus investigaciones sobre la distribución de los primos.

La demostración hecha por Dirichlet a la afirmación de Legendre representó un paso más hacia la demostración del Teorema de los Números Primos. Tchebycheff, un matemático ruso, fue el que logró el primer gran progreso después de Dirichlet rumbo a la

demostración de dicho teorema, introduciendo las dos funciones de variable real siguientes, $\varphi(x) = \sum_{p \leq x} \log p$ y $\chi(x) = \sum_{p^m \leq x} \log p$; él prueba que el Teorema de los Números Primos es equivalente a cualquiera de las dos afirmaciones siguientes:

a) y b)

$$\lim_{x \to \infty} \frac{\varphi(x)}{x} = 1 \qquad \lim_{x \to \infty} \frac{\chi(x)}{x} = 1$$

Reimann introduce la función de variable compleja $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, la cual se conoce con el nombre de Función Zeta de Riemann, con esta función se logra un avance bastante significativo hacia la demostración del Teorema de los Números Primos, pues prueba que $\zeta(s)$ puede ser extendida analíticamente a una función la cual es meromorfa en todo el s-plano. Con esto Riemann logra establecer una íntima conexión entre la función $\chi(x)$ y la función $\zeta(s)$ en 1860.

La más famosa conjetura de Riemann, es la casi

llamada Hipótesis de Riemann, la cual afirma que todos los ceros no triviales de $\zeta(s)$ se encuentran en la recta $Re(s) = \frac{1}{2}$, que es el eje de simetría de la ecuación funcional $R(s) = R(1-s)$, donde

$$R(s) = s(s-1)\,\pi^{-\frac{s}{2}}\,\Gamma\left(\tfrac{s}{2}\right)\,\zeta(s)$$

es una función entera.

El suponer verdadera la Hipótesis de Riemann, conduce a afirmar que $\psi(x) = x + O(x^{1/2+\varepsilon})$ para cualquier $\varepsilon > 0$, donde

$O(x^{1/2+\varepsilon})$ denota a la función

$f(x)$ tal que $\dfrac{f(x)}{x^{1/2+\varepsilon}}$ esta acotada para todos

los x grandes, que es equivalente a El Teorema de los Números Primos.

En 1896, Hadamard y de la Vallée Poussin, independientemente establecen la existencia de una región libre de ceros para $\zeta(s)$, que admite la demostración de

$$\psi(x) = x + O\left(x\,e^{-c(\log x)^{1/14}}\right)$$

que es equivalente al Teorema de los Números Primos, con lo que después de un siglo de arduo trabajo de muchos de los mejores matemáticos del mundo, se logra la demostración del teorema de los Números Primos.

1

El Teorema de Dirichlet

La progresión de números impares $1, 3, 5, 2n+1, \cdots$, contiene una infinidad de números primos.
Es natural preguntar cuándo otra progresión aritmética tiene esta propiedad. Una progresión aritmética con el primer término h y una diferencia común K consiste de todos los números de la forma $Kn+h$, $n=0,1,2,\ldots$. Si h y K tienen un factor común d, cada elemento de la progresión es divisible por d y no hay ningún primo en la progresión si $d>1$. En otras palabras, una condición necesaria para la existencia de una infinidad de primos en $Kn+h$ es que $(h,K)=1$. Dirichlet fue el primero en probar que esta condición es también suficiente. Es decir, si $(h,K)=1$ la progresión aritmética $Kn+h$ contiene una infinidad de primos. Esta afirmación es conocido como El Teorema de Dirichlet, lo cual probaremos en esta sección. Empezamos con algunos teoremas de congruencias.

Definición 1.

Sean $m>0$ y $a\in\mathbb{Z}$, tales que $(a,m)=1$. Decimos que a "pertenece al exponente f módulo m", si a^f es la primera de todas las potencias de a con un exponente positivo para el cual
$$a^f \equiv 1 \pmod{m}.$$

El exponente f existe, puesto que por el Teorema de Euler-Fermat, tenemos que

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$ y lo denotamos como $f = exp_m(a)$.

Teorema 1.

Dados $m > 1$, $a \in \mathbb{Z}$ tales que $(a, m) = 1$ y $f = exp_m(a)$. Entonces

1) $a^k \equiv a^h \pmod{m} \iff k \equiv h \pmod{f}$
2) $a^k \equiv 1 \pmod{m} \iff k \equiv 0 \pmod{f}$
   en particular $f \mid \varphi(m)$.
3) Los números $a^0, a, a^2, \ldots, a^{f-1}$ son incongruentes módulo m.

Demostración.

Basta con probar (1), pues (2) y (3) son consecuencias directas de (1).

Sin pérdida de generalidad, podemos suponer que $k \geq h \geq 0$. Como $a^k \equiv a^h \pmod{m}$ entonces $a^{k-h} \equiv 1 \pmod{m}$. Utilizando el algoritmo de la división obtenemos

$k - h = qf + r$, $q \geq 0$ y $0 \leq r < f$. Por lo tanto

$1 \equiv a^{k-h} \equiv a^{qf+r} \equiv (a^f)^q a^r \equiv a^r \pmod{m}$, por la definición de f, $r = 0$ y en consecuencia $f \mid k - h$. Es decir, $k \equiv h \pmod{f}$.

Recíprocamente, de $k-h=qf$, se sigue
$a^k \equiv a^{h+qf} \equiv a^h (a^f)^q \equiv a^h \pmod m$. De donde $a^k \equiv a^h \pmod m$.

Teorema 2.

Sean q un número primo y $l \in \mathbb{Z}^+ - \{0\}$ tales que $q^l \mid (p-1)$.

Entonces existe un número a tal que $\exp_p(a) = q^l$ donde p es primo.

Demostración

La congruencia polinomial $x^{\frac{p-1}{q}} \equiv 1 \pmod p$ tiene a lo más

$$\frac{p-1}{q} \leq \frac{p-1}{2} \leq p-2 \text{ soluciones (puesto que}$$

$$p \geq 3 \text{ y } \frac{p-1}{q} \in \mathbb{Z} \text{ ya que } p-1 = Q q^l)$$

Por lo tanto existe al menos un $c \in \mathbb{Z}$ el cual $1 \leq c \leq p-1$ tal que

$$c^{\frac{p-1}{q}} \not\equiv 1 \pmod p$$

Hagamos $a = c^{\frac{p-1}{q^l}}$ y veamos que $\exp_p(a) = q^l$. Sea $\exp_p(a) = f$, entonces $f \mid q^l$, si no tuviéramos que $f = q^l$, tendríamos que $f = q^i$ para alguna i, $1 \leq i \leq l-1$ de donde $f \mid q^{l-1}$, de modo que $a^{q^{l-1}} \equiv c^{\frac{p-1}{q}} \equiv 1 \pmod p$, lo cual es una contradicción. Por lo tanto $f = q^l$ ya que $a^{q^l} \equiv c^{p-1} \equiv 1 \pmod p$

Teorema 3.

Existe $g \in \mathbb{Z}$ tal que $\exp_p(g) = p-1$

Demostración.

Si $p = 2$ entonces $g = 2K+1$, $K \in \mathbb{Z}$ satisface la condición del teorema.

Si $p > 2$, sea la descomposición canónica de

$$p-1,\ p-1 = \prod_{n=1}^{r} p_n^{l_n}.$$ Si $r = 1$ se satisfacen los condiciones del teorema 2 y por lo tanto existe talg.

Supongamos que $r > 1$, podemos elegir un número a_n con $\exp_p(a_n) = p_n^{l_n}$ para cada $n = 1, 2, \ldots, r$. Definimos

$$g = \prod_{n=1}^{r} a_n, \text{ entonces } g^{p-1} = \left(\prod_{n=1}^{r} a_n\right)^{p-1} =$$

$$\prod_{n=1}^{r} a_n^{p-1}$$

De donde $$g^{p-1} \equiv \prod_{n=1}^{r} a_n^{p-1} \equiv \prod_{n=1}^{r} a_n^{p_n^{l_n}} \equiv 1 \pmod{p}.$$

Supongamos que $\exp_p(g) = f$, entonces $f \mid p-1$. Si no sucediera que $f = p-1$, sin perdida de generalidad, tendriamos que

$$f \mid \left(\frac{p-1}{p_1}\right), \text{ puesto que } p_n^{l_n} \mid \left(\frac{p-1}{p_1}\right) \ \forall n = 2, 3, \ldots, r,$$

ya que $$\frac{p-1}{p_1} = p_1^{l_1 - 1} \prod_{n=2}^{r} p_n^{l_n}.$$ Así que

$$1 \equiv g^{\frac{p-1}{p_1}} \equiv a_1^{\frac{p-1}{p_1}} \prod_{n=2}^{r} a_n^{\frac{p-1}{p_1}} \equiv a_1^{\frac{p-1}{p_1}} \pmod{p}$$

y en consecuencia $p_1^{l_1} \mid \frac{p-1}{p_1}$. Esto es una contradicción. Por lo tanto $exp_p(g) = p-1$.

Definición 2.

Cualquier $a \in \mathbb{Z}$ tal que $exp_m(a) = \varphi(m)$, recibe el nombre de raíz primitiva módulo m.

Teorema 4.

Sean $a, m \in \mathbb{Z}$ tales que $(a,m)=1$. Entonces a es una raíz primitiva módulo $m \iff a, a^2, \ldots, a^{\varphi(m)}$, forman un sistema reducido de residuos módulo m.

Demostración.

Si a es una raíz primitiva entonces $exp_m(a) = \varphi(m)$. Por lo tanto $a, a^2, \ldots a^{\varphi(m)}$ son incongruentes módulo por el teorema 1. Puesto que hay $\varphi(m)$ de tales números, entonces ellos forman un sistema reducido de residuos módulo m.

Recíprocamente, si $a, a^2, \ldots, a^{\varphi(m)}$ forman un sistema reducido de residuos, entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$, pero una potencia más pequeña no es congruente con 1 módulo m, por lo tanto a es una raíz primitiva módulo m.

La importancia de las raíces primitivas es explicada por el teorema 4. Si m tiene una raíz primitiva entonces cada sistema reducido de residuos módulo m

puede ser expresado como una progresión geométrica.

Este teorema da una herramienta poderosa que puede ser usada en problemas que envuelven sistemas reducidos de residuos. Desafortunadamente, no todos los módulos tienen raíces primitivas. Unicamente los siguientes módulos: $m = 1, 2, 4, p^\alpha$ y $2p^\alpha$ donde p es un primo impar y $\alpha \geq 1$. Usamos este hecho para demostrar el siguiente teorema.

Teorema 5.

Si $p > 2$ y $l > 0$ entonces existe un número g que pertenece a $\varphi(p^l) \pmod{p^l}$.

Del teorema 1, se sigue que para $p \nmid a$ $a \equiv g^b \pmod{p^l}$, $b \geq 0$ es siempre soluble para b y en particular para las clases de residuo módulo $\varphi(p^l)$.

Demostración.

Para $l = 1$ se probó en el teorema 3. Por lo tanto sea $l > 1$. Sea g una raíz primitiva módulo p. Podemos elegir a g tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Cuando g es una raíz primitiva módulo p, también lo es $g + p$, y si $g^{p-1} \equiv 1 \pmod{p^2}$, entonces $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2} p \equiv 1 + (p-1)g^{p-2}p \pmod{p^2}$, así que $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$.

Probaremos que la g determinada por $g^{p-1} \not\equiv 1 \pmod{p}$ satisface la condición del teorema (la cual es incidentalmente una raíz primitiva módulo p).

Primero probamos por inducción matemática, que para todo $l \geq 1$, tenemos

$$g^{p^{l-2}(p-1)} = 1 + h_l p^{l-1}, \quad p \nmid h_l .$$

Para $l = 2$ esto es cierto por el teorema de Fermat, junto con $g^{p-1} \not\equiv 1 \pmod{p^2}$. Si $g^{p^{l-2}(p-1)} = 1 + h_l p^{l-1}$, $p \nmid h_l$ se cumple para l, entonces se sigue para $l+1$ así:

$$g^{p^{l-1}(p-1)} = (1 + h_l p^{l-1})^p = 1 + h_l p^l + h_l^2 p \left(\frac{p-1}{2}\right) p^{2(l-1)} +$$

$$n p^{3(l-1)} \quad \text{donde}$$

$$n = \frac{p(p-1)(p-2)}{3!} h_l^3 + \frac{p(p-1)(p-2)(p-3)}{4!} h_l^4 p^{l-1} + \ldots +$$

$$+ h_l^p p^{(p-3)(l-1)} .$$

De esta igualdad, el tercer y el cuarto término del lado derecho son divisibles por p^{l+1} puesto que $2(l-1) \geq l+1$ y $3l-3 \geq l+1$, respectivamente.
Por lo tanto el lado derecho es igual a $1 + h_{l+1} p^l$, donde $p \nmid h_{l+1}$.

Supongamos que $\exp_{p^l}(g) = f$; por el teorema 1, tenemos $f \mid p^{l-1}(p-1)$; puesto que g pertenece a $p-1$ módulo p, se sigue que $p-1 \mid f$, así que $f = p^m (p-1)$ $0 \leq m \leq l-1$.

Si no fuera verdadero (como se afirma) que $f = p^{l-1}(p-1)$ entonces tendríamos $f \mid p^{l-2}(p-1)$, así que $g^{p^{l-2}(p-1)} \equiv 1 \pmod{p^l}$ que es una contradicción.

Teorema 6.

Si: $l > 2$, entonces $exp_{2^l}(5) = 2^{l-2}$

Demostración

Probamos por inducción que para $l > 2$, $5^{2^{l-3}} = 1 + h_l 2^{l-1}$, $2 \nmid h_l$. Para $l = 3$, esto es verdadero, es decir, $5^1 = 1 + 1 \cdot 4$. De suponer que la igualdad es verdadera para $l \geq 3$, podemos concluir que también es verdadera para $l+1$, porque $5^{2^{l-2}} = (1 + h_l 2^{l-1})^2 = 1 + h_l 2^l + h_l^2 2^{2l-2} = 1 + h_{l+1} 2^l$, $2 \nmid h_{l+1}$. De las dos igualdades anteriores se sigue que $5^{2^{l-3}} \not\equiv 1 \pmod{2^l}$ y $5^{2^{l-2}} \equiv 1 \pmod{2^l}$. Supongamos que $exp_{2^l}(5) = f$, entonces $f \nmid 2^{l-3}$ y $f \mid 2^{l-2}$, de donde $f = 2^{l-2}$.

Teorema 7.

Para $l > 2$, cualquier número impar a satisface la relación $a \equiv (-1)^{\frac{a-1}{2}} 5^b \pmod{2^l}$, $b \geq 0$, precisamente para aquellos números $b \geq 0$, pertenecientes a una particular clase de residuos módulo 2^{l-2}.

Demostración.

1) Sea $a \equiv 1 \pmod 4$. Para $0 \leq b < 2^{l-2}$, 5^b representa 2^{l-2} números incongruentes módulo 2^l, por el

Teorema 6, todos son $\equiv 1 \pmod 4$, sin embargo cualquier conjunto reducido de residuos módulos 2^l contiene exactamente 2^{l-2} números que son $\equiv 1 \pmod 4$; por lo tanto se sigue que $a \equiv 5^b \pmod{2^l}$, $b \geq 0$ es soluble para b. Puesto que, si $b \geq 0$, 5^b es periódico con periodo 2^{l-2} módulo 2^l, se sigue la afirmación.

2) Sea $a \equiv 3 \pmod 4$, entonces aplicamos (1) al número $-a$.

Caracteres

La letra i representa al número complejo $\sqrt{-1}$, todas las demás letras minúsculas excepto e, como antes representan enteros.

Sea $K > 0$ fijo, consideremos $\varphi(K) = h$

Definición 3.

Una función aritmética χ es llamado un carácter módulo K, si satisface:

1) $\chi(a) = 0$ para $(a, K) > 1$.
2) $\chi(1) \neq 0$
3) $\chi(a_1 a_2) = \chi(a_1)\chi(a_2)$ para $(a_1, K) = 1$ y $(a_2, K) = 1$.
4) $\chi(a_1) = \chi(a_2)$ para $a_1 \equiv a_2 \pmod K$ y $(a_1, K) = 1$ (y por lo tanto por (1) siempre que $a_1 \equiv a_2 \pmod K$)

Ejemplo.

Si $K = 4$, $\chi(a) = 0, 1, 0$ y -1 para $a \equiv 0, 1, 2$ y $3 \pmod 4$ respectivamente.

Teorema 8.

Para cualquier carácter tenemos $\chi(1) = 1$

Demostración

Por (3), $\chi(1) = \chi(1 \cdot 1) = \chi(1)\ \chi(1)$ y por (2) $\chi(1) = 1$.

Teorema 9.

Si: $(a, k) = 1$, entonces $(\chi(a))^h = 1$, así $\chi(a)$ es una raíz h-ésima de la unidad y $|\chi(a)| = 1$

Demostración

Como $a^h \equiv 1 \pmod{k}$ y por (3) y (4),

$$(\chi(a))^h = \chi(a^h) = \chi(1) = 1$$

Teorema 10.

1) Para cualquier k existen un número finito de caracteres y además al menos uno. (De esta manera serán dos caracteres distintos sino coinciden para todo a).

Demostración

Para cualquier a en el intervalo $1 \leq a \leq k$ se sigue de (1) y el teorema 9 que $\chi(a)$ debe elegirse de una colección finita de valores posibles (0 ó una raíz h-ésima de la unidad); De (4) se sigue que el valor de $\chi(a)$ para

$1 \leq a \leq K$, determina el valor para toda a. Por lo tanto no puede haber un número infinito de caracteres módulo K.

2) La función

$$\chi(a) = \begin{cases} 0 & \text{para } (a, K) > 1 \\ 1 & \text{para } (a, K) = 1 \end{cases}$$

es claramente un carácter, puesto que satisface la definición 3.

Definición 4.

El carácter definido en la parte (2) de la anterior demostración es llamado el Carácter Principal y es denotado por χ_0.

Teorema 11.

Si χ es un caracter, entonces su función conjugado $\overline{\chi}$ también lo es (Si χ es real entonces no difiere de $\overline{\chi}$).

Teorema 12.

Si a recorre a un conjunto completo de residuos módulo K, entonces

$$\sum_a \chi(a) = \begin{cases} h & \text{para } \chi_0 \\ 0 & \text{en cualquier otro caso} \end{cases}$$

Demostración.

El valor de la suma es en cualquier caso, independiente de la elección del conjunto de residuos, por la definición 3.

1) Para el carácter $\chi = \chi_0$, la suma tiene h términos iguales a 1 y $K-h$ términos iguales a 0.

2) Por otro lado, elijamos (podemos) un número $b>0$, para el cual $(b,K)=1$, $\chi(b) \neq 1$. Puesto que ba recorre a un conjunto completo de residuos módulo K cuando a lo hace también, se sigue que $\xi = \sum \chi(a) =$

$$\sum \chi(ba) = \sum \chi(b) \sum \chi(a) = \chi(b) \sum_{a} \chi(a) =$$

$$= \chi(b)\,\xi, \text{ de donde } (\chi(b) - 1)\,\xi = 0 \therefore \xi = 0,$$

puesto que $\chi(b) - 1 \neq 0$

Teorema 13.

Si χ_1 y χ_2 son caracteres, entonces $\chi_1 \chi_2$ también lo es; En particular si χ es un carácter entonces χ^2 es un carácter.

Teorema 14.

Si χ_1 es un carácter, entonces si χ recorre a los c caracteres; también los recorre $\chi_1 \chi$.

Demostración

Si $\chi_2(a)\,\chi_1(a) = \chi_3(a)\,\chi_1(a)$, entonces se sigue para $(a,k)=1$ que $\chi_2(a) = \chi_3(a)$, puesto que $\chi_1(a) \neq 0$. y por la definición 3(1), esto se satisface para $(a,k)>1$ también. Las φ funciones $\chi\chi_1$ son por lo tanto los φ caracteres distintos

Teorema 15.

Si $d>0$, $(d,k)=1$ y $d \not\equiv 1 \pmod{k}$ entonces existe un carácter el cual $\chi(d)\neq 1$.

Demostración.

Puesto que $\chi(a)=0$ debe cumplirse siempre para $(a,k)>1$, necesitamos definir adecuadamente a $\chi(a)$, únicamente para $(a,k)=1$

Puesto que $d \not\equiv 1 \pmod{k}$, existe un número $p^l \mid k$, donde $p>2$ y $l>0$ para el cual $d \not\equiv 1 \pmod{p^l}$, o de otra manera, un número $2^l \mid k$, donde $l>0$ para el cual $d \not\equiv 1 \pmod{2^l}$.

A) Sea $d \not\equiv 1 \pmod{p^l}$, $p>2$, $l>0$ y $p^l \mid k$; Por lo tanto $p \nmid d$, puesto que $(d,k)=1$. Sea g que pertenece a $\varphi(p^l)$ módulo p^l.

Para $(a,k)=1$, tenemos $p \nmid a$ y por lo tanto $a \equiv g^b \pmod{p^l}$, $\varphi(p^l) > b \geq 0$, hagamos $\rho = e^{\frac{2\pi i}{\varphi(p^l)}}$, $\chi(a) = \rho^b$, entonces $\chi(a)$ está completamente determinada por a (la elección anterior está hecha para un número fijo g) puesto que

ρ^b tiene periodo $\varphi(p^l)$ y b está unívocamente determinado módulo $\varphi(p^l)$.

$X(a)$ es un carácter, porque:

2) $X(1) = \rho^0 = 1$

3) Para $(a_1, K) = 1 = (a_2, K)$, $a_1 \equiv g^{b_1}$, $a_2 \equiv g^{b_2} \pmod{p^l}$, tenemos $a_1 a_2 \equiv g^{b_1+b_2} \pmod{p^l}$, $X(a_1 a_2) = \rho^{b_1+b_2} = \rho^{b_1}\rho^{b_2} = X(a_1)X(a_2)$.

4) Para $a_1 \equiv a_2 \pmod{K}$ tenemos $a_1 \equiv a_2 \pmod{p^l}$, lo que implica que $X(a_1) = X(a_2)$.

Finalmente, se sigue de $d \not\equiv 1 \pmod{p^l}$ y $p \nmid d$ que $d \equiv g^r \pmod{p^l}$, $\varphi(p^l) \nmid r$, $X(d) = \rho^r \neq 1$

B) Sea $d \not\equiv 1 \pmod{2^l}$, $l > 0$ y $2^l \mid K$ y por lo tanto $l > 1$ (puesto que K es par, así que $d \equiv 1 \pmod 2$).

B.1) Sea $d \equiv 1 \pmod 4$, así que $l > 2$. Entonces para $(a, K) = 1$ tenemos por el teorema 7; ya que $(a, 2) = 1$, $a \equiv (-1)^{\frac{a-1}{2}} 5^b \pmod{2^l}$, $b \geq 0$, haciendo $\rho = e^{\frac{2\pi i}{2^{l-2}}}$, $X(a) = \rho^b$. Entonces $X(a)$ está bien definido y puesto que ρ^b tiene periodo 2^{l-2} y b está determinado módulo 2^{l-2}.

$X(a)$ es un carácter, porque:

2) $X(1) = \rho^0 = 1$

3) Para $(a_1, K) = 1 = (a_2, K)$, $a_1 \equiv (-1)^{\frac{a_1-1}{2}} 5^{b_1}$, $a_2 \equiv (-1)^{\frac{a_2-1}{2}} 5^{b_2} \pmod{2^l}$ por lo que

$$a_1 a_2 \equiv (-1)^{\frac{a_1-1}{2} + \frac{a_2-1}{2}} 5^{b_1+b_2} \equiv (-1)^{\frac{a_1 a_2 - 1}{2}} 5^{b_1+b_2} \pmod{2^l}$$

(Como a_1 y a_2 son impares tenemos que $(a_1-1)(a_2-1) \equiv 0 \pmod 4$ esto implica que

$\frac{a_1 a_2 - 1}{2} \equiv \frac{a_1 - 1}{2} + \frac{a_2 - 1}{2} \pmod 2$, por lo tanto

$(-1)^{\frac{a_1 a_2 - 1}{2}} = (-1)^{\frac{a_1 - 1}{2} + \frac{a_1 - 1}{2}}$. Es decir,

$$\chi(a_1 a_2) = \rho^{b_1 + b_2} = \rho^{b_1} \rho^{b_2} = \chi(a_1)\chi(a_2)$$

4) Para $a_1 \equiv a_2 \pmod K$, nos da $a_1 \equiv a_2 \pmod{2^l}$. Finalmente, se sigue de $d \not\equiv 1 \pmod{2^l}$ y $d \equiv 1 \pmod 4$ que $d \equiv 5^r \pmod{2^l}$, $2^{l-2} \nmid r$, por lo tanto $\chi(d) = \rho^r \neq 1$

B. 2) Sea $d \equiv -1 \pmod 4$. Entonces para $(a, K) = 1$ (donde a es impar), haciendo $\chi(a) = (-1)^{\frac{a-1}{2}}$, $\chi(a)$ es un carácter porque:

2) $\chi(1) = 1$

3) Para $(a_1, K) = 1 = (a_2, K)$, tenemos $\chi(a_1 a_2) =$

$$(-1)^{\frac{a_1 a_2 - 1}{2}} = (-1)^{\frac{a_1 - 1}{2}} (-1)^{\frac{a_2 - 1}{2}} = \chi(a_1)\chi(a_2)$$

4) Es claro porque $4 \mid K$. Finalmente $\chi(d) = -1 \neq 1$

Teorema 16.

Para $a > 0$ fijo

$$\sum_{\chi} \chi(a) = \begin{cases} \varphi(K) \text{ para } a \equiv 1 \pmod K \\ 0 \text{ para } a \not\equiv 1 \pmod K \end{cases}$$

donde la suma es tomada sobre

los c caracteres.

Demostración

1) Para $a \equiv 1 \pmod{K}$, la suma (se sigue del teorema 8), tiene c términos los cuales son iguales a 1.

2) Para $(a,K) > 1$, todos los términos se anulan.

3) Para $(a,K) = 1$ y $a \not\equiv 1 \pmod{K}$, podemos elegir un carácter χ_1, el cual $\chi_1(a) \neq 1$ por el teorema 15, y por el teorema 14, tenemos $n = \sum_{\chi} \chi(a) = \sum_{\chi} \chi(a)\chi_1(a) = \chi_1(a) \sum_{\chi} \chi(a)$

$= \chi_1(a)\, n$. Por lo tanto $(\chi_1(a) - 1)\, n = 0$, en consecuencia $n = 0$.

Teorema 17.

$C = h$ (es decir, existen exactamente $\varphi(K)$ caracteres mod K)

Demostración.

Si a recorre un conjunto completo de residuos módulo K y χ recorre todos los caracteres entonces por los teoremas 16 y 12, tenemos

$$\sum_{a,\chi} \chi(a) = \begin{cases} \sum_{a} \sum_{\chi} \chi(a) = c + 0 + \ldots + 0 = c \\ \sum_{\chi} \sum_{a} \chi(a) = h + 0 + \ldots + 0 = h \end{cases}$$

Teorema 18.

Sean $(l, K) = 1$, $l > 0$ y $a > 0$, entonces

$$\sum_{\chi} \frac{1}{\chi(l)} \chi(a) = \begin{cases} h & \text{para } a \equiv l \pmod K \\ 0 & \text{para } a \not\equiv l \pmod K \end{cases}$$

Observación.

En el lado izquierdo, podemos escribir $\overline{\chi}(l)$ en lugar de $1/\chi(l)$.

Demostración

Elijamos $j > 0$ de tal manera que $jl \equiv 1 \pmod K$. Puesto que $\chi(j)\chi(l) = \chi(jl) = 1$, se sigue que

$$\sum_{\chi} \frac{1}{\chi(l)} \chi(a) = \sum_{\chi} \chi(j)\chi(a) = \sum_{\chi} \chi(ja), \text{ así que}$$

por los teoremas 16 y 17

$$\sum_{\chi} \frac{1}{\chi(l)} \chi(a) = \begin{cases} h & \text{para } ja \equiv 1,\ a \equiv l \pmod K \\ 0 & \text{en cualquier otro caso} \end{cases}$$

Definición 5.

χ es llamado carácter de primer género si es el carácter principal, de segundo género si es real pero no es un carácter principal y de tercer género si no siempre es real.

Ejemplos:

1) El carácter dado en el ejemplo anterior es un carácter de segundo género directamente de la definición.

2) Para $K = 5$, $\chi(a) = 0, 1, i, -i, -1$, para $a \equiv 0, 1, 2, 3, 4 \pmod 5$, es un carácter de tercer género.

3) El símbolo de Kronecker $\left(\frac{K}{a}\right)$ es un carácter de segundo género $(\mathrm{mod}\ K)$. Pero no es un carácter principal, éste hecho es importante.

L - Series

Las $L(s, \chi)$ series las introdujo y definió Dirichlet con el propósito expreso de demostrar, el teorema que lleva su nombre.

Teorema 19.

Para cada uno de los h caracteres módulo K, las series

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s} = L(s, \chi) \text{ son}$$

absolutamente convergentes para $s > 1$.

Demostración.

Por la definición 3 y el teorema 9, tenemos

$$|\chi(a)| \leq 1, \quad \left|\frac{\chi(a)}{a^s}\right| \leq \frac{1}{a^s}. \text{ Como } \sum_{a=1}^{\infty} \frac{1}{a^s}$$

converge entonces $\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$ converge absolutamente.

Teorema 20.

Si χ no es el carácter principal entonces

$$\left| \sum_{a=M}^{N} \chi(a) \right| \leq \frac{h}{2} \quad \text{para} \quad N \geq M \geq 1$$

Demostración.

Por el teorema 12 $\sum \chi(a)$ se anula tomando a a sobre un conjunto completo de residuos por lo que podemos suponer que el número de términos de nuestra suma $N - M + 1 \leq K - 1$.

En un conjunto completo de residuos exactamente h valores de $|\chi(a)|$ son iguales a 1 y el resto igual a cero. Si en nuestro conjunto de residuos parcial ocurre que en a lo más $\frac{h}{2}$ términos, $|\chi(a)| = 1$, entonces

$$\left| \sum_{a=M}^{N} \chi(a) \right| \leq \sum_{a=M}^{N} |\chi(a)| \leq \frac{h}{2} .$$ Si ocurren más

de $\frac{h}{2}$ de tales términos, entonces

$$\left| \sum_{a=M}^{N} \chi(a) \right| = \left| \sum_{a=M}^{N+K-1} \chi(a) - \sum_{a=N+1}^{N+K-1} \chi(a) \right| =$$

$$= \left| \sum_{a=N+1}^{M+K-1} \chi(a) \right| \leq \sum_{a=N+1}^{M+K-1} |\chi(a)| < \frac{h}{2}$$

Teorema 21.

Sean $v \geq \mu$, γ_a un número complejo arbitrario y para cada a que satisface $\mu \leq a \leq v$, sean

$$\sum_{a=\mu}^{w} \gamma_a = R(w) \quad \text{para } \mu \leq w \leq v,$$

$$\operatorname{Max}_{\mu \leq w \leq v} |R(w)| = \nu, \quad \varepsilon_\mu \geq \varepsilon_{\mu+1} \geq \dots \geq \varepsilon_v \geq 0,$$

entonces tenemos $\left| \sum_{a=\mu}^{v} \varepsilon_a \gamma_a \right| \leq \varepsilon_\mu \nu$

Demostración

Sea $R(\mu-1) = 0$. Entonces tenemos

$$\sum_{a=\mu}^{v} \varepsilon_a \gamma_a = \sum_{a=\mu}^{v} \varepsilon_a (R(a) - R(a-1)) = \sum_{a=\mu}^{v-1} R(a)(\varepsilon_a - \varepsilon_{a+1}) +$$

$$+ R(v)\varepsilon_v, \text{ de donde}$$

$$\left| \sum_{a=\mu}^{v} \varepsilon_a \gamma_a \right| \leq \nu \left[\sum_{a=\mu}^{v-1} (\varepsilon_a - \varepsilon_{a+1}) + \varepsilon_v \right] = \nu \varepsilon_\mu$$

Teorema 22.

Si χ no es el carácter principal, entonces la serie

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s} = L(s, \chi) \text{ converge}$$

uniformemente para $s \geq 1$.

Teorema 21.

Sean $\nu \geq \mu$, γ_a un número complejo arbitrario y para cada a que satisface $\mu \leq a \leq \nu$, sean

$$\sum_{a=\mu}^{w} \gamma_a = R(w) \quad \text{para } \mu \leq w \leq \nu,$$

$$\max_{\mu \leq w \leq \nu} |R(w)| = \mu, \quad \varepsilon_\mu \geq \varepsilon_{\mu+1} \geq \dots \geq \varepsilon_\nu \geq 0,$$

entonces tenemos $\left| \sum_{a=\mu}^{\nu} \varepsilon_a \gamma_a \right| \leq \varepsilon_\mu \mu$

Demostración

Sea $R(\mu-1) = 0$. Entonces tenemos

$$\sum_{a=\mu}^{\nu} \varepsilon_a \gamma_a = \sum_{a=\mu}^{\nu} \varepsilon_a (R(a) - R(a-1)) = \sum_{a=\mu}^{\nu-1} R(a)(\varepsilon_a - \varepsilon_{a+1}) +$$

$$+ R(\nu)\varepsilon\nu, \text{ de donde}$$

$$\left| \sum_{a=\mu}^{\nu} \varepsilon_a \gamma_a \right| \leq \mu \left[\sum_{a=\mu}^{\nu-1} (\varepsilon_a - \varepsilon_{a+1}) + \varepsilon_\nu \right] = \mu \varepsilon_\mu$$

Teorema 22.

Si χ no es el carácter principal, entonces las series

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s} = L(s,\chi) \text{ convergen}$$

uniformemente para $s \geq 1$.

Demostración.

Para $U \geq u \geq 1$, se sigue de los teoremas 21 y 20 (con $\varepsilon_a = \frac{1}{a^s}$) que

$$\left| \sum_{a=u}^{U} \frac{\chi(a)}{a^s} \right| \leq \frac{h}{2} \frac{1}{u^s} \leq \frac{h}{2u}, \quad \text{asi que dada}$$

$$\delta > 0, \quad \left| \sum_{a=u}^{U} \frac{\chi(a)}{a^s} \right| < \delta \quad \text{para } U \geq u \geq u_0(\delta)$$

donde u_0 no depende de s.

Teorema 23.

1) Las series $\sum_{a=1}^{\infty} \frac{\chi(a) \log a}{a^s}$ convergen absolutamente para $s > 1$ y convergen uniformemente para $s > 1+\varepsilon$, si fijamos $\varepsilon > 0$.

2) Si $s > 1$ entonces

$$L'(s,\chi) = -\sum_{a=1}^{\infty} \frac{\chi(a) \log a}{a^s}$$

Demostración

1) Para $s > 1+\varepsilon$ tenemos $\left| \frac{\chi(a) \log a}{a^s} \right| \leq \frac{\log a}{a^{1+\varepsilon}}$

y $\sum_{a=1}^{\infty} \frac{\log}{a^{1+\varepsilon}}$ converge. Por lo tanto tambien $\sum_{a=1}^{\infty} \frac{\chi(a) \log a}{a^s}$

converge.

2) Como $s>1$ y $L(s,\chi)=\sum_{a=1}^{\infty}\frac{\chi(a)}{a^s}$ tenemos que $\frac{\chi(a)}{a^s}=\chi(a)a^{-s}$, por lo tanto $(\chi(a)a^{-s})'=(-1)\chi(a)a^{-s}\log a$

$=\frac{-\chi(a)\log a}{a^s}$, por lo tanto $L'(s,\chi)=-\sum_{a=1}^{\infty}\frac{\chi(a)\log a}{a^s}$

Teorema 24.

Si χ no es el carácter principal, entonces las series

$\sum_{a=1}^{\infty}\frac{\chi(a)\log a}{a^s}$ convergen uniformemente para $s\geq 1$ y para estos valores de s su suma es menor que h en valor absoluto.

Demostración.

1) Sea $s\geq 1$, puesto que $\frac{d}{d\xi}\left(\frac{\log\xi}{\xi^s}\right)=$

$=\frac{1}{\xi}\xi^{-s}+(-s)\xi^{-s-1}\log\xi=\frac{1-s\log\xi}{\xi^{s+1}}$, se sigue

que $\frac{\log\xi}{\xi^s}$ es una función decreciente para $\xi>e^{1/s}$,

ya que su derivada es negativa y decreciente.

Como $3 > e \geq e^{1/3}$, por los teoremas 20 y 21 tenemos, para $v \geq u \geq 3$,

$$\left| \sum_{a=u}^{v} \frac{\chi(a) \log a}{a^s} \right| \leq \frac{h}{2} \frac{\log u}{u^s} \leq \frac{h}{2} \frac{\log u}{u}, \text{ de lo}$$

cual se sigue la convergencia uniforme.

2) Para $s \geq 1$, se sigue de la desigualdad anterior haciendo $u = 3$ y $v \to \infty$ que

$$\left| \sum_{a=1}^{\infty} \frac{\chi(a)\, \mu(a)}{a^s} \right| \leq \frac{\log 2}{2} + \frac{h}{2} \frac{\log 3}{3} < \frac{1}{2} + \frac{h}{2} \leq h$$

Teorema 25.

Las series $\sum_{a=1}^{\infty} \frac{\chi(a)\, \mu(a)}{a^s}$ convergen absolutamente para $s > 1$.

Demostración.

$$\left| \frac{\chi(a)\mu(a)}{a^s} \right| = \frac{|\chi(a)|\,|\mu(a)|}{a^s} \leq \frac{1}{a^s}$$

Teorema 26.

Para $s > 1$, tenemos

$$L(s,\chi) \sum_{a=1}^{\infty} \frac{\chi(a)\, \mu(a)}{a^s} = 1, \text{ asique } L(s,\chi) \neq 0.$$

Demostración

De la convergencia absoluta de ambas series en el lado izquierdo de la siguiente fórmula junto con el teorema 11 capítulo III, tenemos

$$\sum_{b=1}^{\infty} \frac{\chi(b)}{b^s} \sum_{a=1}^{\infty} \frac{\chi(a)\mu(a)}{a^s} = \sum_{l=1}^{\infty} \sum_{ba=l} \frac{\chi(b)\chi(a)\mu(a)}{b^s a^s} =$$

$$\sum_{l=1}^{\infty} \left(\frac{\chi(l)}{l^s} \sum_{a|l} \mu(a) \right) = 1$$

Teorema 27.

Para $s>1$, tenemos

$$\prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right) = \frac{1}{L(s,\chi)}$$

El producto está ordenado para valores crecientes de p.

Demostración.

Para $\xi > 1$, tenemos

$$\prod_{p \le \xi} \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{a=1}' \frac{\chi(a)\mu(a)}{a^s}$$

donde a recorre aquellos naturales que no son divisibles por cualquier $p > \xi$. Entre ellos ocurren todos los números $a \le \xi$.

Por lo tanto

$$\prod_{p \le \xi} \left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{1 \le a \le \xi} \frac{\chi(a)\,\mu(a)}{a^s} + \sum_{a > \xi}' \frac{\chi(a)\mu(a)}{a^s},$$

cuando $\xi \to \infty$, la primer suma de la derecha se aproxima a

$$\sum_{a=1}^{\infty} \frac{\chi(a)\mu(a)}{a^s} = \frac{1}{L(s,\chi)} \quad ;$$

por el teorema 26; la segunda se aproxima a 0 puesto que es menor o igual a $\sum_{a > \xi} \frac{1}{a^s}$ en valor absoluto.

Teorema 28.

Para $s > 1$, tenemos

$$\sum_{a=1}^{\infty} \frac{\chi(a)\,\Lambda(a)}{a^s} = -\frac{L'(s,\chi)}{L(s,\chi)},$$

donde para $n \ge 1$

$$\Lambda(n) = \begin{cases} \log p \text{ si } n = p^m \text{ para} \\ \quad \text{algún primo } p \\ \text{y } m \ge 1 \\ 0 \text{ en cualquier otro} \\ \quad \text{caso.} \end{cases}$$

La serie de la izquierda converge absolutamente para $s > 1$.

Demostración:

1) $\left|\chi(a)\Lambda(a)\right| \leq \log a$, nos conduce a la convergencia absoluta de las series de la izquierda para $s>1$.

2) Por el teorema 13 capítulo III, sabemos que

$$\sum_{a|l}\Lambda(a) = \log l,$$ así que para $s>1$, tenemos

$$L(s,\chi)\sum_{a=1}^{\infty}\frac{\chi(a)\Lambda(a)}{a^s} = \sum_{b=1}^{\infty}\frac{\chi(b)}{b^s}\sum_{a=1}^{\infty}\frac{\chi(a)\Lambda(a)}{a^s}$$

$$= \sum_{l=1}^{\infty}\left[\frac{\chi(l)}{l^s}\sum_{a|l}\Lambda(a)\right] = \sum_{l=1}^{\infty}\frac{\chi(l)\log l}{l^s} = -L'(s,\chi)$$

Teorema 29.

Cuando $s\to 1$ por la derecha,

$$-\frac{L'(s,\chi_0)}{L(s,\chi_0)} \to \infty$$

Demostración

Por el teorema 28, tenemos

$$-\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \sum_{\substack{a=1\\(a,K)=1}}^{\infty}\frac{\Lambda(a)}{a^s} = \sum_{a=1}^{\infty}\frac{\Lambda(a)}{a^s} - \sum_{p|K}\log p\sum_{m=1}^{\infty}\frac{1}{p^{ms}} =$$

$$= \sum_{a=1}^{\infty} \frac{\Lambda(a)}{a^s} - \sum_{p|K} \frac{\log p}{p^s - 1}$$

cuando $s \to 1$, el segundo término se aproxima a un valor finito, así que tenemos que mostrar simplemente que el primer término se aproxima a infinito. Daremos dos demostraciones.

1) Si aplicamos el teorema 28 con $K = 1$, se sigue que el primer término es igual a

$$\frac{\sum_{a=1}^{\infty} \frac{\log a}{a^s}}{\sum_{a=1}^{\infty} \frac{1}{a^s}}$$

En esta fórmula, el denominador se aproxima a infinito cuando $s \to 1$, puesto que

$$\sum_{a=1}^{\infty} \frac{1}{a^s} > \int_1^{\infty} \frac{dx}{x^s} = \frac{1}{s-1}$$

Sea $g > 1$, para $s > 1$, tenemos

$$\sum_{a=1}^{\infty} \frac{\log a}{a^s} \geq \sum_{a=g}^{\infty} \frac{\log a}{a^s} >$$

$$> \log g \sum_{a=g}^{\infty} \frac{1}{a^s} = \log g \left[\sum_{a=1}^{\infty} \frac{1}{a^s} - \sum_{a=1}^{g-1} \frac{1}{a^s} \right], \text{ el lado}$$

derecho es mayor que $\frac{1}{2} \log g$ para $1 < s < 1 + \varepsilon(g)$.

2) Usemos la siguiente afirmación : La serie $\sum_p \frac{1}{p}$, la suma sobre todos los primos en orden crecien-

te, diverge.

Entonces podemos asegurar que $\sum_p \frac{\log p}{p}$ diverge y en consecuencia también la serie $\sum_{a=1}^{\infty} \frac{\Lambda(a)}{a}$. Por lo

tanto, para cualquier $w > 0$ existe el correspondiente $b(w)$ para el cual $\sum_{a=1}^{b} \frac{\Lambda(a)}{a} > w$.

Por lo tanto $\sum_{a=1}^{b} \frac{\Lambda(a)}{a^s} > w$ para $1 < s < 1 + \varepsilon(w)$, así que $\sum_{a=1}^{\infty} \frac{\Lambda(a)}{a^s} > w$.

Teorema 30.

Para $0 < n < 1$ y $r \geq 0$, $r < 0$ tenemos

$$(1-n)^3 \left|1 - n e^{ri}\right|^4 \left|1 - n e^{2ri}\right|^2 < 1$$

Demostración

El significado geométrico de estos tres números es que a lo más el producto es igual a su media geométrica.

Como $2\cos N + \cos 2N = 2\cos^2 N + 2\cos^2 N - 1 =$
$-\frac{3}{2} + 2\left(\cos N + \frac{1}{2}\right)^2 \geq -\frac{3}{2}$, tenemos

$$\left|1 - n e^{Ni}\right|^4 \left|1 - n e^{2Ni}\right|^2 = \left|1 - n e^{Ni}\right|^2 \left|1 - n e^{Ni}\right|^2$$

$$\left|1 - n e^{2Ni}\right|^2 =$$

$$= (1 - 2n\cos N + n^2)(1 - 2n\cos N + n^2)$$
$$(1 - 2n\cos 2N + n^2) \leq$$

$$\leq \left[1 - \frac{2}{3}n\,(2\cos N + \cos 2N) + n^2\right]^3 \leq (1 + n + n^2)^3 < \left(\frac{1}{1-n}\right)^3$$

Teorema 31.

Para $s > 1$, tenemos

$$\left(L(s, \chi_0)\right)^3 \left|L(s,\chi)\right|^4 \left|L(s,\chi^2)\right|^2 \geq 1$$

Demostracion

Hagamos $\chi(p) = e^{Ni}$ y $\frac{1}{p^s} = n$, para $p \nmid K$ y apliquemos el teorema 30, esto nos conduce a

$$\left(1 - \frac{\chi_0(p)}{p^s}\right)^3 \left|1 - \frac{\chi(p)}{p^s}\right|^4 \left|1 - \frac{\chi^2(p)}{p^s}\right|^2 \leq 1$$

esto tambien se cumple para $p \mid K$. Multiplicando con respecto a p, el teorema 27 nos da el resultado del teorema.

Teorema 32.

Para cualquier carácter de los de tercer género, tenemos $L(1,\chi) \neq 0$

Demostración

Puesto que χ^2 no es el carácter principal (porque de otro modo χ sería real), se sigue de

$$\left| \sum_{q=M}^{N} \frac{\chi(q)}{q^s} \right| \leq \frac{h}{2M} \quad (\text{con } M=1 \text{ y } N \to \infty) \quad \text{que}$$

$$\left| L(s,\chi^2) \right| < h \quad \text{para} \quad s > 1. \quad \text{O de otra manera,}$$

para $1 < s < 2$ tenemos

$$L(s,\chi_0) = \sum_{\substack{q=1 \\ (q,k)=1}}^{\infty} \frac{1}{q^s} \leq \sum_{q=1}^{\infty} \frac{1}{q^s} < 1 + \int_1^{\infty} \frac{dx}{x^s} =$$

$$1 + \frac{1}{s-1} = \frac{s}{s-1} < \frac{2}{s-1}$$

Por lo tanto, por el teorema 31, tenemos

$$L(s,\chi) \geq \frac{1}{(L(s,\chi_0))^{3/4}} \frac{1}{|L(s,\chi^2)|^{1/2}} > \frac{(s-1)^{3/4}}{2^{3/4}} \frac{1}{\sqrt{h}} >$$

$$> \frac{(s-1)^{3/4}}{2\sqrt{h}}$$

Si tuvieramos $L(1,\chi)=0$ entonces se sigue del teorema 24 (puesto que $L'(\xi,\chi)$ es continua para $\xi \geq 1$) que para $s>1$,

$$\left|L(s,\chi)\right| = \left|L(s,\chi) - L(1,\chi)\right| =$$

$$= \left|\int_1^s L'(\xi,\chi)\,d\xi\right| < h(s-1).$$

Por lo tanto, para $1 < s < 2$ tenemos $(s-1)^{1/4} > \frac{1}{2h^{3/2}}$.

Esto por supuesto, es falso para $s = 1 + \frac{1}{16h^6}$

Teorema 33.

Para cualquier carácter de segundo género tenemos

$$L(1,\chi) \neq 0$$

Este es el más profundo de todos los lemas que son necesarios para la prueba del Teorema de Dirichlet. Dirichlet lo probó únicamente por el importante método indirecto, usando la así llamada Teoría de las Clases de números de las formas cuadráticas. Incidentalmente $L(1,\chi) \geq 0$ es trivial, porque de los teoremas 26 y 27 obtenemos que $L(s,\chi) > 0$ para $s > 1$ y por el teorema 22 las series son continuas para $s \geq 1$.

Demostración.

Consideremos la función aritmética $f(a)=\sum_{d|a} \chi(d)$

entonces para $l \geq 0$, tenemos

$$f(p^l) = 1 + \chi(p) + \ldots + \chi(p^l) = \begin{cases} 1+0+\ldots+0 & \text{para } \chi(p)=0 \\ 1+1+\ldots+1 \geq 1 & \text{para } \chi(p)=1 \\ 1-1+\ldots+(-1)^l = \begin{cases} 1 & \text{para } \chi(p) = -1, 2 \mid l \\ 0 & \text{para } \chi(p) = -1, 2 \nmid l \end{cases} \end{cases}$$

Por lo tanto tenemos

$$f(p^l) \geq \begin{cases} 1 & \text{si } 2 \mid l \\ 0 & \text{en cualquier otro caso} \end{cases}$$

Sean $a_1 > 0$, $a_2 > 0$ y $(a_1, a_2) = 1$. Existe una correspondencia uno a uno entre todos los números positivos $d \mid a_1 a_2$ y todos los productos de números positivos $d_1 \mid a_1$ por los números positivos $d_2 \mid a_2$. Por lo tanto

$$f(a_1 a_2) = \sum_{d \mid a_1 a_2} \chi(d) = \sum_{\substack{d_1 \mid a_1 \\ d_2 \mid a_2}} \chi(d_1 d_2) = \sum_{d_1 \mid a_1} \chi(d_1) \sum_{d_2 \mid a_2} \chi(d_2) = f(a_1) f(a_2)$$

Se sigue que

$$f(a) \geq \begin{cases} 1 & \text{si } a \text{ es igual a un cuadrado perfecto} \\ 0 & \text{en cualquier otro caso} \end{cases}$$

Hagamos

$$m = (4h)^6 \quad y \quad Z = \sum_{n=1}^{m} 2(m-n) f(n) = \sum_{n=1}^{m} 2(m-n) \left(\sum_{d|n} \chi(d) \right) =$$

$$= \sum_{n=1}^{m} 2 \sum_{d|n} (m-n) \chi(d) = \sum_{n=1}^{m} 2 \sum_{\substack{ab=n \\ a>0, b>0}} (m-ab) \chi(b) = \sum_{\substack{ab \leq m \\ a>0, b>0}} 2(m-ab) \chi(b)$$

Entonces

$$Z \geq \sum_{b=1}^{\sqrt{m}} 2(m-b^2) \geq \sum_{b=1}^{1/2\sqrt{m}} 2(m-b^2) \geq \sum_{b=1}^{1/2\sqrt{m}} 2\left(m - \frac{m}{4}\right) =$$

$$= \frac{3}{4} m^{3/2} = \frac{3}{4} (4h)^9.$$

Por otro lado (el lector dibujará el triángulo curvilíneo en el plano ab acotado por la rama positiva de la hipérbola $ab = m$ y las rectas $a = 1$, $b = 1$ y además por la recta auxiliar $b = m^{2/3}$) se sigue de $ab \leq m$, $a > 0$, $b > 0$ que $a \leq \sqrt[3]{m}$, $b > m^{2/3}$ ó $b \leq m^{2/3}$. Así tenemos $Z = Z_1 + Z_2$,

haciendo

$$Z_1 = \sum_{a=1}^{\sqrt[3]{m}} \sum_{m^{2/3} < b \le \frac{m}{a}} 2\,(m-ab)\,\chi(b)$$

$$Z_2 = \sum_{b=1}^{m^{2/3}} \sum_{0 < a \le \frac{m}{b}} 2\,(m-ab)\,\chi(b)$$

De los teoremas 20 y 21 (con b en lugar de a, $\sigma_b = \chi(b)$ y $\varepsilon_b = 2(m-ab)$ para $m^{2/3} < b \le \frac{m}{a}$) se sigue que

$$Z_1 \le \sum_{a=1}^{\sqrt[3]{m}} \left| \sum_{m^{2/3} < b < \frac{m}{a}} 2\,(m-ab)\,\chi(b) \right| \le \sum_{a=1}^{\sqrt[3]{m}} \cdot 2m\frac{h}{2} = m^{1/3}\,h$$

Mientras que

$$Z_2 = \sum_{b=1}^{m^{2/3}} \chi(b) \sum_{0 < a \le \frac{m}{b}} (2m - 2ab)$$

En esta fórmula, si hacemos $u = u(m,b) = \frac{m}{b} - \left[\frac{m}{b}\right]$,

entonces $0 \le u < 1$, y obtenemos

$$\sum_a (2m - 2ab) = 2m \sum_a 1 - b \sum_a 2a = 2m\left[\frac{m}{b}\right] - b\left[\frac{m}{b}\right]\left(\left[\frac{m}{b}\right] + 1\right)$$

$$= 2m\left(\frac{m}{b} - u\right) - b\left(\left(\frac{m}{b} - u\right)^2 + \frac{m}{b} - u\right) =$$

$$= \frac{2m^2}{b} - 2m\,u - b\left(\frac{m^2}{b^2} - 2u\,\frac{m}{b} + v^2 + \frac{m}{b} - u\right) =$$

$$= \frac{m^2}{b} - m + b\,(u - v^2)$$

Por lo tanto (observando que $|u - v^2| \leq 1$) tenemos:

$$Z_2 = m^2 \sum_{b=1}^{m^{2/3}} \frac{\chi(b)}{b} - m \sum_{b=1}^{m^{2/3}} \chi(b) + \sum_{b=1}^{m^{2/3}} \chi(b)\, b\,(u - v^2) \leq$$

$$\leq m^2 \left(L(1,\chi) - \sum_{b=m^{2/3}+1}^{\infty} \frac{\chi(b)}{b} \right) + m\,\frac{h}{2} + m^{2/3} \sum_{b=1}^{m^{2/3}} 1$$

Asigue por $\left| \sum_{a=M}^{u} \frac{\chi(a)}{a} \right| \leq \frac{h}{2M}$ (haciendo $M = m^{2/3}+1$, $u \to \infty$)

$$Z_2 < m^2 L(1,\chi) + m^2 \frac{h}{2}\,\frac{1}{m^{2/3}} + m^{4/3}\,\frac{h}{2} + m^{4/3}\,h = m^2 L(1,\chi) +$$

$$+ m^{4/3}\,h\,\left(\frac{1}{2} + \frac{1}{2} + 1\right) = m^2 L(1,\chi) + 2\,m^{4/3}\,h$$

Por todo lo anterior podemos afirmar que

$$\frac{3}{4}(4h)^4 \leq Z < m^2 L(1,\chi) + 3m^{4/3}\,h = m^2 L(1,\chi) + 3(4h)^{8}\,h =$$

$$= m^2 L(1,\chi) + \frac{3}{4}(4h)^4 \;;\; 0 < m^2 L(1,\chi),\, 0 < L(1,\chi).$$

Teorema 34.

Para cualquier carácter de segundo o tercer género $\frac{L'(s,\chi)}{L(s,\chi)}$ está acotado para $s > 1$.

La cota puede depender de K y χ. Sin embargo χ no se necesita mencionar aquí, puesto que para cualquier K existen únicamente $\varphi(K)$ valores posibles para χ.

Demostración

Por el teorema 22, $L(s,\chi)$ es continua para $s \geq 1$, por el teorema 26 nunca es cero para $1 \leq s \leq 2$ y por los teoremas 32 y 33 nunca es cero para $s = 1$. Entonces $\frac{1}{L(s,\chi)}$ está acotado para $1 \leq s \leq 2$ y para $s > 2$, por los teoremas 25 y 26. Finalmente por el teorema 24, $L'(s,\chi)$ está acotada para $s \geq 1$.

Ahora estamos en posición de dar la demostración del teorema de Dirichlet.

Teorema 35.

Sea $(l,K) = 1$ y $l > 0$. Entonces para $s > 1$

$$-\frac{1}{h}\sum_{\chi}\frac{1}{\chi(l)}\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{a \equiv l}\frac{\Lambda(a)}{a^s}$$

El término de la derecha es la

suma sobre todos los números $a \equiv l \pmod{k}$ crecientes-0, por supuesto en forma arbitraria. El hecho de que no todos los términos se anulen se seguirá del teorema 36, por el momento esto es irrelevante.

Demostración.

Por los teoremas 28 y 18

$$-\sum_{\chi} \frac{1}{\chi(1)} \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\chi} \frac{1}{\chi(l)} \sum_{a=1}^{\infty} \frac{\chi(a)\Lambda(a)}{a^s}$$

$$= \sum_{a=1}^{\infty} \left(\frac{\Lambda(a)}{a^s} \sum_{\chi} \frac{1}{\chi(l)} \chi(a) \right)$$

Por el teorema 15, Si $a \not\equiv l \pmod{k}$, como sabemos que existe $y \in \mathbb{Z}$ tal que $ly = 1 \pmod{k}$, entonces $ay \not\equiv 1 \pmod{k}$ Sea χ_1 tal que $\chi_1(ay) \neq 1$, entonces

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \sum_{\chi} \frac{\chi(a)\chi(y)}{\chi(l)\chi(l)} \quad \text{entonces}$$

$$\left(\frac{\chi_1(a)}{\chi_1(l)} - 1 \right) \sum_{\chi} \frac{\chi(a)}{\chi(l)} = 0 \qquad (*)$$

Pero $\chi_1(1y) = \chi_1(1) = 1$ y $\chi_1(\ell y) = \chi_1(\ell)\,\chi_1(y)$

entonces $\chi_1(y) = \frac{1}{\chi_1(\ell)}$

Ahora: Si $(a, K) = 1$, entonces $\sum_{\chi} \frac{\chi(a)}{\chi(1)} = 0$

Si $(a, K) = 1$, entonces $\chi_1(ay) = \chi_1(a)\,\chi_1(y)$

Por lo tanto $\frac{\chi_1(a)}{\chi_1(1)} \neq 1$, entonces por (*)

$$\sum_{\chi} \frac{\chi(a)}{\chi(\ell)} = 0$$

Por lo anterior tenemos que

$$\sum_{a=1}^{\infty} \left(\frac{\Lambda(a)}{a^s} \sum_{\chi} \frac{1}{\chi(\ell)}\ \chi(a) \right) \sum_{a \equiv 1} \frac{\Lambda(a)}{a^s}\ h$$

Por lo tanto

$$-\frac{1}{h} \sum_{\chi} \frac{1}{\chi(\ell)}\ \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{a \equiv \ell} \frac{\Lambda(a)}{a^s}$$

Teorema 36.

Sea $(l, k) = 1$. Entonces existe una infinidad de números primos $p \equiv l \pmod{k}$

Demostración.

Sin pérdida de generalidad, sea $l > 0$.

Cuando $s \to 1$, $-\frac{1}{h} \sum_{\chi} \frac{1}{\chi(l)} \frac{L'(s,\chi)}{L(s,\chi)} \to \infty$;

el término de la suma que involucra a χ_0 se aproxima a ∞, por el teorema 29. los otros $h-1$ términos restantes se encuentran acotados, por el teorema 34, por lo tanto.

$$\sum_{p \equiv l} \frac{\log p}{p^s} + \sum_{\substack{p,m \\ m>1 \\ p^m \equiv l}} \frac{\log p}{p^{ms}} = \sum_{a \equiv l} \frac{\Lambda(a)}{a^s} \to \infty$$

La suma permanece acotada para $m > 1$, puesto que

$$\sum_{a=2}^{\infty} \frac{2 \log a}{a^2} > \sum_{a=2}^{\infty} \frac{\log a}{a(a-1)} \geq \sum_{p} \frac{\log p}{p(p-1)} \geq \sum_{\substack{p,m \\ m>1}} \frac{\log p}{p^m} >$$

$$> \sum_{\substack{p,m \\ m>1}} \frac{\log p}{p^{ms}} \geq \sum_{\substack{p,m \\ m>1 \\ p^m \equiv l}} \frac{\log p}{p^{ms}} \quad (s > 1);$$

Por lo tanto tenemos que $\sum_{p \equiv l} \frac{\log p}{p^s} \to \infty$

De esto se sigue que la suma no es vacía, ni contiene un número finito de términos.

El Teorema De Los Numeros Primos

En lo que sigue presentamos una demostración del teorema de los números primos que establece que $\pi(x)$ es asuntótica a $x/\log x$, es decir, $\lim_{x\to\infty} \frac{\log x\, \pi(x)}{x} = 1$

donde $\pi(x)$ denota el número de primos que no exceden de x con $x>0$, y algunas de sus equivalencias. El comportamiento de $\pi(x)$ como función de x ha sido objeto de intenso estudio por muchos matemáticos famosos entre ellos se encuentran Gauss, Legendre, Hadamand y de la Vallée Poussin, estos dos últimos demostraron el teorema de los Numeros Primos en 1896, aquí lo haremos sin usar la Teoria de Funciones de variable compleja y las propiedades de la función zeta de Riemann, basándonos en la prueba de Selberg y Erdös.

Primero probamos dos fórmulas que relacionan a las funciones $\vartheta(x)$ y $\pi(x)$, que usaremos para mostrar que el teorema de los numeros primos es equivalente al $\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$. Las funciones $\pi(x)$ y $\vartheta(x)$

son funciones escalonadas que saltan en los primos, π tiene saltos de 1 en cada primo, y $\vartheta(x)$ tiene saltos de $\log p$ en cada primo p. Sumas que envuelven funciones escalonadas de este tipo pueden ser expresados como integrales, como vemos en el siguiente:

Teorema 1.

Para cualquier función aritmética $a(n)$, sea

$$A(x) = \sum_{n \le x} a(n) \quad \text{donde} \quad A(x) = 0 \text{ si } x < 1$$

Supongamos que f tiene derivada continua en el intervalo $[y, x]$ donde $0 < y < x$.

Entonces

$$(1) \quad \sum_{y < n \le x} a(n) f(x) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t)\, dt$$

Demostración

Sea $K = [x]$ y $m = [y]$ así que $A(x) = A(K)$ y $A(y) = A(m)$, entonces

$$\sum_{y < n \le x} a(n) f(n) = \sum_{n=m+1}^{K} a(n) f(n) = \sum_{n=m+1}^{K} \{A(n) - A(n-1)\} f(n) =$$

$$= \sum_{n=m+1}^{K} A(n) f(n) - \sum_{n=m}^{K-1} A(n) f(n+1) = \sum_{n=m+1}^{K-1} A(n) \{f(n) - f(n+1)\} +$$

$$+ A(K) f(K) - A(m) f(m+1)$$

$$= -\sum_{n=m+1}^{K-1} A(n) \int_n^{n+1} f'(t)\, dt + A(K) f(K) - A(m) f(m+1)$$

$$= -\sum_{n=m+1}^{K-1} \int_n^{n+1} A(t) f'(t)\, dt + A(K) f(K) - A(m) f(m+1)$$

$$= -\int_{m+1}^{K} A(t) f'(t)\,dt + A(x) f(x) - \int_{K}^{x} A(t) f'(t)\,dt -$$

$$A(y) f(y) - \int_{y}^{m+1} A(t) f'(t)\,dt$$

$$= A(x) f(x) - A(y) f(y) - \int_{y}^{x} A(t) f'(t)\,dt$$

Teorema 2.

Para $x \geq 2$ tenemos

$$(2)\quad \psi(x) = \pi(x) \log x - \int_{2}^{x} \frac{\pi(t)}{t}\,dt$$

y

$$(3)\quad \tilde{\pi}(x) = \frac{\psi(x)}{\log x} + \int_{2}^{x} \frac{\psi(t)}{t \log^2 t}\,dt$$

Demostración

Sea $a(n) = \begin{cases} 1 & \text{si } n \text{ es primo} \\ 0 & \text{en cualquier otro caso} \end{cases}$

La función característica de los primos, entonces

$$\tilde{\pi}(x) = \sum_{p \leq x} 1 = \sum_{1 < n \leq x} a(n) \qquad y$$

$$\psi(x) = \sum_{p \leq x} \log p = \sum_{1 < n \leq x} a(n) \log n.$$

Tomando $f(x) = \log x$ en (1) con $y = 1$, obtenemos

$$\psi(x) = \sum_{1<n\leq x} a(n) \log n = \widetilde{\pi}(x) \log x - \widetilde{\pi}(1) \log(1) -$$

$$- \int_1^x \frac{\widetilde{\pi}(t)}{t} \, dt$$

$$= \widetilde{\pi}(x) \log x - \int_1^x \frac{\widetilde{\pi}(t)}{t} \, dt = \widetilde{\pi}(x) \log x - \int_2^x \frac{\widetilde{\pi}(t)}{t}$$

porque $\widetilde{\pi}(x) = 0$ para $x < 2$

Ahora sea $b(n) = a(n) \log n$ y escribimos

$$\widetilde{\pi}(x) = \sum_{3/2 < n \leq x} b(n) \frac{1}{\log n} \; ; \; \psi(x) = \sum_{n \leq x} b(n)$$

haciendo $f(x) = \frac{1}{\log x}$ en (1) con $y = \frac{3}{2}$ obtenemos

$$\widetilde{\pi}(x) = \frac{\psi(x)}{\log x} - \frac{\psi(3/2)}{\log 3/2} + \int_{3/2}^t \frac{\psi(t)}{t \log^2 t} \, dt$$

lo cual prueba (3) puesto que $\psi(t) = 0$ si $t < 2$

Sea x una variable entera o continua la cual tiende a infinito. Si $g(x)$ es una función positiva de x denotamos por

$$O(g(x))$$

a cualquier función de x la cual tiene la propiedad

$$\frac{O(g(x))}{g(x)} \longrightarrow 0 \quad \text{cuando} \quad x \longrightarrow \infty$$

Así $x = O(x^2)$, pero $x = O(\sqrt{x})$. Además también denotamos por

$$O(g(x))$$

a cualquier función de x que tiene la propiedad

$$\frac{|O(g(x))|}{g(x)} < M, \; M > 0 \quad \text{cuando} \quad x \longrightarrow \infty$$

Por ejemplo $O(x) = 2x + \sqrt{x}$, $O(1) = \operatorname{sen} x$, $O(\sqrt{x}) = \log x$

El teorema de los números primos puede ser formulado como sigue:

$$\widetilde{\pi}(x) = \frac{x}{\log x} + O\left(\frac{x}{\log x}\right)$$

y la fórmula

$$\sum_{p \leq n} \frac{\log p}{p} = \log x + \Theta$$

donde Θ es una función de x tal que $|\Theta| < N$ con $N > 0$, puede ser escrita como

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$$

Ahora consideremos algunas formas equivalentes del Teorema de los Números Primos.

Teorema 3.

Las siguientes relaciones son equivalentes:

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

5) $\lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1$.

6) $\lim_{x \to \infty} \frac{\psi(x)}{x} = 1$

Demostración

De (2) y (3) obtenemos respectivamente

$$\frac{\vartheta(x)}{x} = \frac{\pi(x) \log x}{x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t}\, dt$$

y $$\frac{\pi(x) \log x}{x} = \frac{\vartheta(x)}{x} + \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t \log^2 t}\, dt$$

Para que (4) implique (5) necesitamos únicamente demostrar que (4) implica

$$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\tilde{\pi}(t)}{t}\,dt = 0$$

Pero (4) implica $\dfrac{\tilde{\pi}(t)}{t} = O\left(\dfrac{1}{\log t}\right)$ para $t \geq 2$

asi $\dfrac{1}{x}\displaystyle\int_2^x \frac{\tilde{\pi}(t)}{t}\,dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\,dt\right)$

Ahora

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}$$

Asi $\dfrac{1}{x}\displaystyle\int_2^x \frac{dt}{\log t} \longrightarrow 0$ cuando $x\to\infty$

Esto muestra que (4) implica (5).

Para mostrar que (5) implica (4) necesitamos probar que (5) implica

$$\lim_{x\to\infty} \frac{\log x}{x}\int_2^x \frac{\psi(t)}{t\log^2 t} = 0$$

Pero (5) implica

$$\psi(t) = O(t)$$

Asi $\dfrac{\log x}{x}\displaystyle\int_2^x \frac{\psi(t)}{t\log^2 t}\,dt = O\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right)$

Ahora

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2 \sqrt{x}}$$

Por lo tanto

$$\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t} \longrightarrow 0 \text{ cuando } x \longrightarrow \infty$$

Esto prueba que (5) implica (4), así (4) y (5) son equivalentes.

Para demostrar que (5) y (6) son equivalentes es necesario mostrar la desigualdad

$$0 \leq \frac{\psi(x)}{x} - \frac{\theta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2} \quad \text{para } x > 0$$

Sabemos que

$$\psi(x) = \sum_{m \leq \log_2 x} \theta(x^{1/m})$$

entonces

$$0 \leq \psi(x) - \theta(x) = \sum_{2 \leq m \leq \log_2 x} \theta(x^{1/m})$$

Pero de la definición de $\theta(x)$ tenemos

$$\theta(x) = \sum_{p \leq x} \log p \leq x \log x$$

Así:

$$0 \leq \psi(x) - \vartheta(x) \leq \sum_{2 \leq m \leq \log_2 x} x^{1/m} \log(x^{1/m}) \leq (\log x)\sqrt{x} \log \sqrt{x}$$

$$= \frac{\log x}{\log 2} \cdot \frac{\sqrt{x}}{2} \log x = \frac{\sqrt{x}\,(\log x)^2}{2 \log 2}$$

dividiendo entre x obtenemos la desigualdad deseada. Ahora la desigualdad implica que

$$\lim_{x \to \infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0$$

Por lo tanto (5) y (6) son equivalentes y también (4) y (6) lo son.

Empezamos la demostración del Teorema de los Números primos con lemas que preparan la prueba.

Lema 1.

Existe una constante $\gamma > 0$ tal que

$$(7) \quad \sum_{n \leq y} \frac{1}{n} = \log y + \gamma + O\left(\frac{1}{y}\right)$$

donde la suma se extiende sobre todos los enteros positivos $n \leq y$ (El número γ es conocido como la constante de Euler).

Demostración.

Sea z el menor entero $> y$. Si hacemos

$\delta_n = \frac{1}{n} \log\left(1 + \frac{1}{n}\right)$ tenemos

$$\log z = \log\left\{(1+1)\left(1+\tfrac{1}{2}\right)\left(1+\tfrac{1}{3}\right)\cdots\left(1+\tfrac{1}{z-1}\right)\right\} =$$

$$= \sum_{n=1}^{z-1} \log\left(1+\frac{1}{n}\right)$$

$$= \sum_{n=1}^{z-1} \frac{1}{n} - \sum_{n=1}^{z-1} \delta_n \qquad (8)$$

Sabemos que

$$0 < \delta_n < \frac{1}{2n^2} \qquad (9)$$

por lo cual la serie

$$\sum_{n=1}^{\infty} \delta_n$$

es convergente y tiene un valor positivo γ. Por lo tanto

$$\sum_{n=z}^{\infty} \delta_n < \frac{1}{2} \sum_{n=z}^{\infty} \frac{1}{n^2} < \frac{1}{2} \sum_{n=z}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \frac{1}{2(z-1)}$$

De (8) concluimos

$$\sum_{n=1}^{z-1} \frac{1}{n} = \log z + \sum_{n=1}^{z-1} \delta_n = \log z + \sum_{n=1}^{\infty} \delta_n - \sum_{n=1}^{\infty} \delta_n$$

$$= \log z + \gamma + \frac{\theta}{z}$$

donde θ es una función de z tal que $|\theta| < N$ con $N > 0$.

Esta fórmula nos conduce a (7)

Lema 2.

Existe una constante absoluto c tal que

$$(10) \quad \sum_{n \le y} \frac{\log n}{n} = \frac{1}{2} (\log y)^2 + c + O\left(\frac{\log y}{y}\right)$$

donde la suma se extiende sobre todos los enteros positivos $n \le y$.

Demostración

Sea z el menor entero $> y$. Claramente

$$(\log z)^2 = \sum_{n=1}^{z-1} \left[(\log (n+1))^2 - (\log z)^2 \right]$$

y como $\log (n+1) = \log n + \frac{1}{n} - \delta n$,

tenemos que

$$\frac{1}{2} (\log z)^2 = \sum_{n=1}^{z-1} \frac{\log n}{n} - \sum_{n=1}^{z-1} \left(\delta n \log n + \frac{1}{n} \delta n - \frac{1}{2n^2} - \frac{1}{2} \delta n^2 \right)$$

por (9) vemos que la anterior suma en el lado derecho tiende a un límite finito cuando $z \to \infty$. Por lo tanto

$$\left| \sum_{n=z}^{\infty} \left(\delta_n \log n + \frac{1}{n}\delta_n - \frac{1}{2n^2} - \frac{1}{2}\delta_n^2 \right) \right| < \sum_{n=z}^{\infty} \frac{\log n}{n^2} < \frac{\log z}{z^2} +$$

$$+ \int_z^{\infty} \frac{\log x}{x^2}\, dx$$

$$= \frac{\log z}{z^2} + \frac{1}{z^2} + \frac{\log z}{z}$$

(integrando por partes)

Así concluimos que

$$\sum_{n=1}^{z-1} \frac{\log n}{n} = \frac{1}{2}(\log z)^2 + C + O\left(\frac{\log z}{z}\right)$$

donde C es una constante absoluta. Esta fórmula nos conduce a (10).

Lema 3.

Si $z(n)$ denota el número de divisores positivos de n, entonces

$$\sum_{n \le y} \frac{z(n)}{n} = \frac{1}{2}(\log y)^2 + 2\gamma \log y + \gamma^2 - 2C + O\left(\frac{\log y}{\sqrt{y}}\right)$$

donde la suma se extiende sobre todos los enteros positivos $n \le y$, γ y C son las mismas constantes absolutas de los lemas (1) y (2).

Demostración

Puesto que $z(n)$ es igual a el número de parejas de números naturales a y b tales que $ab = n$, tenemos

$$\sum_{n \le y} \frac{z(n)}{n} = \sum_{ab < y} \frac{1}{ab}$$

denotemos por S_1 la parte de esta suma en la cual

$a \le \sqrt{y}$, por S_2 denotemos la

parte de la suma

en la cual $b \le \sqrt{y}$ y por S_3 denotamos la parte en la cual $a \le \sqrt{y}$ y $b \le \sqrt{y}$.
Entonces el valor de la suma es

$$S_1 + S_2 - S_3$$

Haciendo $z = \sqrt{y}$ y $t = \frac{y}{a}$ obtenemos por los lemas 1 y 2

$$S_1 = \sum_{a \le z} \frac{1}{a} \sum_{b \le t} \frac{1}{b} = \sum_{a \le z} \frac{1}{a} \left[\log \frac{y}{a} + \gamma + O\left(\frac{a}{y}\right) \right]$$

$$= \log y \sum_{a \le z} \frac{1}{a} - \sum_{a \le z} \frac{\log a}{a} + \gamma \sum_{a \le z} \frac{1}{a} + O\left(\frac{1}{y}\right) \sum_{a \le z} 1$$

$$= \left[\log y + \gamma \right] \left\{ \log z + \gamma + O\left(\frac{1}{z}\right) \right\} - \frac{1}{2} \left(\log z \right)^2 - C + O\left(\frac{\log z}{z}\right)$$

$$+ O\left(\frac{1}{z}\right) = \frac{3}{8} \left(\log y \right)^2 + \frac{3}{2} \log y + \gamma^2 - C + O\left(\frac{\log y}{y}\right)$$

Por el mismo procedimiento vemos que $S_2 = S_1$.
Por lo tanto por los lemas 1 y 2

$$S_3 = \left(\sum_{a \le z} \frac{1}{a} \right)^2 = \left(\log z + \gamma + O\left(\frac{1}{z}\right) \right)^2$$

$$= \frac{1}{4} \left(\log y \right)^2 + \gamma \log y + \gamma^2 + O\left(\frac{\log y}{y}\right)$$

En consecuencia

$$\sum \frac{1}{ab} = S_1 + S_2 - S_3 = \frac{3}{4}(\log y)^2 + 3\gamma \log y + 2\gamma^2$$

$$- 2C - \frac{1}{4}(\log y)^2 - \gamma \log y +$$

$$+ O\left(\frac{\log y}{\sqrt{y}}\right) + \gamma^2$$

$$= \frac{1}{2}(\log y)^2 + 2\gamma \log y + \gamma^2 - 2C + O\left(\frac{\log y}{y}\right)$$

lo cual prueba el lema 3.

Para cualquier entero $h \geq 0$ definimos una función aritmética por la ecuación

$$\varphi_h(n) = \sum_d \mu(d) (\log d)^h$$

donde la suma se extiende sobre todos los divisores positivos d de n y μ es la función de Möbius definida en el capítulo II.

Lema 4.

Si un número natural n es divisible por más de h primos distintos entonces $\varphi_h(n) = 0$

Demostración

Para $h=0$ la afirmación es verdadera.

Podemos suponer que $h \geq 1$, usamos inducción sobre h. Suponemos el lema 4 verdadero para todas las funciones $\varphi_\ell(n)$ con $\ell \leq h-1$. Sea $n = p^\alpha m$ donde $\alpha \geq 1$ y m no es divisible por el primo p, entonces.

$$\varphi_h(n) = \sum_d \mu(d) (\log d)^h = \sum_{d_1} \sum_{d_2} \mu(d_1 d_2) (\log d_1 + \log d_2)^h$$

donde la suma exterior del lado derecho se extiende sobre todos los divisores positivos d_1 de m y la suma interna sobre todos los divisores d_2 de p^α, entonces

$$\varphi_h(n) = \sum_{s=0}^{h} \binom{h}{s} \sum_{d_1} \mu(d_1) (\log d_1)^s \sum_{d_2} \mu(d_2) (\log d_2)^{h-s}$$

$$= \sum_{s=0}^{h} \binom{h}{s} \varphi_s(m) \varphi_{h-s}(p^\alpha)$$

Puesto que n tiene más de h factores primos diferentes, m tiene más de $h-1$ factores primos diferentes. Por lo tanto por hipótesis $\varphi_s(m) = 0$ para $s = 0, 1, \ldots, h-1$, el término restante $\varphi_h(m) \varphi_0(p^\alpha)$ es también igual a cero puesto que $\varphi_0(p^\alpha) = 0$

Lema 5.

Cuando x es un número positivo, haciendo

$$\lambda(d) = \mu(d)\left(\log \frac{x}{d}\right)^2 \quad y$$

$$f(n) = \sum_d \lambda(d)$$

donde la suma se extiende sobre todos los divisores positivos d de el número positivo n, entonces

$$f(1) = (\log x)^2$$

y

$$f(p^\alpha) = -(\log p)^2 + 2(\log x)(\log p)$$

donde p es un primo y α un entero ≥ 1.

$$f(p^\alpha q^\beta) = 2(\log p)(\log q)$$

donde p y q son primos diferentes, α y β son enteros ≥ 1; $f(n) = 0$ cuando n es divisible por tres o más primos diferentes.

Demostración

$$f(1) = \sum_d \lambda(d) = \lambda(1) = \mu(1)\left(\log\left(\frac{x}{1}\right)\right)^2 = (\log x)^2$$

$$f(p^\alpha) = \sum_{d} \lambda(d) = \sum_{d} \mu(d) \left(\log \frac{x}{p}\right)^2 = \mu(1)(\log x)^2 + \mu(p)\left(\log \frac{x}{p}\right)^2$$

$$+ \ldots + \mu(p^\alpha)\left(\log \frac{x}{p^\alpha}\right)^2 = (\log x)^2 - \left(\log \frac{x}{p}\right)^2$$

$$= -(\log p)^2 + 2(\log x)(\log p)$$

$$f(p^\alpha q^\beta) = \sum_{d} \lambda(d) = \sum_{d} \mu(d)\left(\log \frac{x}{d}\right)^2.$$

$$= \mu(1)(\log x)^2 + \mu(p)\left(\log \frac{x}{p}\right)^2 + \mu(q)\left(\log \frac{x}{q}\right)^2 +$$

$$+ \mu(pq)\left(\log \frac{x}{pq}\right)^2$$

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

$$= 2(\log p)(\log q)$$

Con esto termino la demostración.

Lema 6.

Para cualquier número natural x, tenemos

$$\left| \sum_{d=1}^{x} \frac{\mu(d)}{d} \right| \leq 1$$

Demostración

Como

$$\sum_{n=1}^{x} \sum_{d} \mu(d) = 1 ,$$

donde la suma interior se extiende sobre todos los divisores d de entero positivo x. Por tanto, puesto que el número de multiplos de $d \geq 1$ y $\leq x$ es igual a $[x/d]$,

$$\sum_{d=1}^{x} \mu(d) \left[\frac{x}{d}\right] = 1$$

En consecuencia

$$\left| x \sum_{d=1}^{x} \frac{\mu(d)}{d} - 1 \right| = \left| \sum_{d=1}^{x} \mu(d) \left(\frac{x}{d} - \left[\frac{x}{d}\right] \right) \right| \leq$$

$$\leq \sum_{d=1}^{x} \left(\frac{x}{d} - \left[\frac{x}{d}\right] \right) \leq x - 1$$

Asi que

$$\left| x \sum_{d=1}^{x} \frac{\mu(d)}{d} \right| \leq 1 + x - 1 = x$$

Lema 7.

Para cualquier entero positivo x tenemos

$$(11) \quad \sum_{d \le x} \frac{\mu(d)}{d} \log \frac{x}{d} = O(1)$$

donde la suma se extiende sobre todos los enteros positivos $d \le x$.

Demostración

Aplicando el lema 1, encontramos que el lado izquierdo de la afirmación es igual a

$$\sum_{d \le x} \frac{\mu(d)}{d} \left(\sum_{n \le t} \frac{1}{n} - \gamma + \theta_1 \frac{d}{x} \right)$$

donde $t = \frac{x}{d}$ y $|\theta_1|$ es menor que un entero positivo C_1 constante. Para $dn = m$, esto se convierte en

$$\sum_{m \le x} \frac{1}{m} \sum_{\delta} M(\delta) - \gamma \sum_{d \le x} \frac{\mu(d)}{d} + \sum_{d \le x} M(d) \frac{\theta_1}{x}$$

donde δ recorre a todos los divisores positivos de m; la primera suma tiene el valor 1 y por el lema 6, la segunda suma tiene un valor absoluto $\le \gamma$. El valor absoluto de la tercera suma es a lo más

$$\frac{C_1}{x} \sum_{d \le x} 1 = C_1$$

Lema 8.

Para cualquier número natural n tenemos

$$(12)\quad \sum_{d} \mu(d)\, Z\left(\frac{n}{d}\right) = 1$$

la suma extendida sobre todos los divisores positivos d de n.

Demostración

Puesto que $Z(n) = \sum_{\delta} 1$, la suma extendida sobre todos los divisores positivos δ de n/d, el lado izquierdo de (12) se convierte en

$$\sum_{d} \mu(d) \sum_{\delta} 1 = \sum_{\delta} \sum_{\delta_1} \mu(\delta_1)$$

donde la suma interior del lado derecho se extiende sobre todos los divisores positivos δ_1 de n/δ, esta suma es igual a cero cuando $\delta \neq n$ y igual a 1 cuando $\delta = n$, así el lado derecho es igual a 1.

Lema 9.

Para cualquier entero positivo x tenemos

$$(13)\quad \sum_{d \leq x} \frac{\mu(d)}{d} \left(\log \frac{x}{d}\right)^2 = 2 \log x + O(1)$$

donde la suma se extiende sobre todos los enteros positivos $d \leq x$.

Demostración

Aplicando el lema 3 para $y = x/d$, el lado izquierdo de la fórmula (13) puede ser escrito como

$$2 \sum_{d \le x} \frac{\mu(d)}{d} \left[\sum_{n \le x} \frac{Z(n)}{n} - 2\gamma \log \frac{x}{d} + \gamma^2 + 2C \right] +$$

$$+ \sum_{d \le x} \frac{\mu(d)}{d} \left(\theta \left(\frac{d}{x}\right)^{1/2} \log \frac{x}{d} \right)$$

donde $|\theta|$ es menor que una constante positiva C_2. Para todos los x suficientemente grandes el valor absoluto de lo anterior suma es más pequeño que

$$4 C_1 \sum_{d \le x} \frac{1}{d} \left(\frac{d}{x}\right)^{1/2} \left(\frac{x}{d}\right)^{1/4} = x^{-1/4} O\left(\sum_{d \le x} d^{-3/4}\right) =$$

$$= x^{-1/4} O\left(\int_1^x z^{3/4} \, dz\right) = O(1)$$

Por lo tanto, haciendo $K = nd$, tenemos

$$S = 2 \sum_{d \le x} \frac{\mu(d)}{d} \sum_{K \le n} \frac{Z(n)}{n} = 2 \sum_{K = x} \frac{1}{K} \sum_{d} \mu(d) Z\left(\frac{K}{d}\right)$$

donde la suma interior del lado derecho se extiende sobre todos los divisores positivos d de K. Por el significado de los lemas 8 y 1,

$$S = 2 \log x + O(1)$$

Finalmente aplicando los lema 7 y 6 el lado izquierdo de (13) es igual a

$$2 \log x + O(1)$$

Lema 10.

La suma extendido sobre todos los primos $p \le x$, tenemos

$$(14) \quad \sum_{p \le x} (\log p)\left(\log \frac{x}{p}\right) = O(x \log x)$$

Demostración.

Si $y = x/\log x$ la suma del lado izquierdo es igual a

$$\sum_{p \le y} (\log p)\left(\log \frac{x}{p}\right) + \sum_{p > y}^{p \le x} (\log p)\left(\log \frac{x}{p}\right) \le (\log x) \sum_{p \le y} \log p +$$

$$+ (\log \log x) \sum_{p \le x} \log p$$

$$= (\log x)\, \theta\left(\frac{x}{\log x}\right) + (\log \log x)\, \theta(x)$$

Observamos que esta función tiene el orden de magnitud $O(x \log \log x)$ el cual es un poco superior que (14).

Lema 11.

La suma extendida sobre las potencias de los primos $p^{\alpha} \leq x$, donde x es un número natural

$$\sum{}' \log p = O(x)$$

Demostración
La suma del lado izquierdo es igual a

$$\theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \ldots + \theta(\sqrt[k]{x})$$

donde k es el entero mas grande tal que $2^k \leq x$.
Por lo tanto

$$k \leq \frac{\log x}{\log 2}$$

. Esta suma es a lo más

igual a

$$\theta(x) + k\,\theta(\sqrt{x})$$

y tiene un orden de magnitud

$$O(x) + \frac{\log x}{\log 2}\, O(\sqrt{x}) = O(x)$$

Lema 12.

Si $f(n)$ es la función definida en el lema 5 tenemos que

$$\sum_{n \leq x} f(n) = (\log x)\,\theta(x) + 2\sum_{p \leq y} \theta\left(\frac{x}{p}\right) \log p + O(x \log x)$$

donde la suma del lado izquierdo se extiende sobre todos los enteros positivos $n \leq x$ y la suma del lado derecho se extiende sobre todos los primos $p \leq y = \sqrt{x}$.

Demostración.

Del lema 5 tenemos

$$(15) \quad \sum_{n \leq x} f(n) = (\log x)^2 + \sum \left(2 \log x (\log p) - (\log p)^2 \right) +$$

$$+ 2 \sum (\log p)(\log q)$$

donde la primera suma en el lado derecho se extiende sobre todas las potencias de primos $p^\alpha \leq x$, α es un número natural; la segunda suma del lado derecho se extiende sobre todas las potencias de primos p^α y q^β tales que $p^\alpha q^\beta \leq x$ y $p < q$, donde α y β son naturales.

En la primera suma del lado derecho primero consideramos los términos $\alpha \geq 2$. Si denotamos por $g(x)$ el número de las potencias de primos $p^\alpha \leq x$ con $\alpha \geq 2$, vemos que la contribución de estos términos o la suma es a lo más igual a

$$2 (\log x)^2 g(x) \leq 2 (\log x)^2 \left(\sqrt{x} + \sqrt[3]{x} + \ldots + \sqrt[k]{x} \right)$$

donde k es el entero más grande tal que $2^k \leq x$. Así la contribución no excede a

$$2(\log x)^2 K\sqrt{x} \le 2(\log x)^2 \frac{\log x}{\log 2}\sqrt{x} = O(x\sqrt{x})$$

Consideremos los siguientes términos con $\alpha = 1$ en la primera suma del lado derecho. La contribución de estos términos es igual a

$$\sum_{p \le x}\left[2\log x(\log p) - (\log p)^2\right] = (\log x)\sum_{p\le x}\log p +$$

$$+ \sum_{p\le x}(\log p)\left(\log \frac{x}{p}\right)$$

$$= (\log x)\,\theta(x) + O(x\log x)$$

de acuerdo al lema 10. Así la primera suma del lado derecho de la fórmula (15) es igual a

$$(16)\quad (\log x)\,\theta(x) + O(x\log x)$$

Finalmente consideremos la segunda suma del lado derecho. Aplicando el lema 11 para x/q^β en lugar de x vemos que la contribución de los términos para $\beta \ge 2$ y $\alpha \ge 1$ tiene orden de magnitud.

$$\sum (\log q)\, O\left(\frac{x}{q^\beta}\right) = O(x)\sum \frac{\log q}{q^\beta} = O(x)$$

para las series infinitas $\sum_2^\infty \frac{\log q}{q^\beta}$ que se extienden sobre todos los primos q son claramente

convergente, puesto que $\beta \geq 2$. Así que la segunda suma del lado derecho es igual a

$$(17) \qquad 2 \sum (\log p)(\log q) + O(x)$$

la suma que se extiende sobre todos los primos p y q tales que $pq \leq x$ y $p < q$. Si hacemos $y = \sqrt{x}$ la suma anterior es igual a

$$\sum_{pq \leq x} (\log p)(\log q) - \sum_{p \leq y} (\log p)^2 =$$

$$= \sum_{\substack{p \leq y \\ pq \leq x}} (\log p)(\log q) + \sum_{\substack{q \leq y \\ pq \leq x}} (\log p)(\log q) -$$

$$- \sum_{\substack{p \leq y \\ q \leq y}} (\log p)(\log q) - \sum_{p \leq y} (\log p)^2$$

Las 2 sumas anteriores tienen a lo más orden de magnitud

$$\left(\theta(\sqrt{x})\right)^2 = O(x)$$

y

$$(\log \sqrt{x})\, \theta(x) = O(x \log x)$$

respectivamente por lo que concluimos que (17) es igual a

$$\sum_{p \le y} (\log p)\, \psi\left(\frac{x}{p}\right) + \sum_{q \le y} (\log q)\, \psi\left(\frac{x}{q}\right) + O(x)$$

$$= 2 \sum_{p \le y} (\log p)\, \psi\left(\frac{x}{p}\right) + O(x)$$

Introducimos las expresiones (16) y (17) en la fórmula (15) y obtenemos finalmente el lema 12

Finalizamos con la demostración de la fórmula básica de Selberg.

Teorema 4.

Haciendo $y = \sqrt{x}$ tenemos

$$\psi(x) \log x + 2 \sum_{p \le y} \psi\left(\frac{x}{p}\right) \log p - 2x \log x =$$

$$= O(x \log x)$$

Demostración.

Por el lema 12 el lado izquierdo es igual a

$$\sum_{n \le x} f(n) - 2x \log x + O(x \log x)$$

de acuerdo a la definición de $f(n)$ tenemos

$$S = \sum_{n \le x} f(n) = \sum_{n \le x} \sum_{d} \lambda(d)$$

de donde la suma interior se extiende sobre

todos los divisores positivos d de n. Por lo tanto

$$S = \sum_{d \le x} \lambda(d) \left[\frac{x}{d}\right] = \sum_{d \le x} \lambda(d) \left(\frac{x}{d} - \varepsilon_d\right) \quad \text{donde } 0 \le \varepsilon_d < 1$$

haciendo $z = \dfrac{x}{(\log x)^2}$, tenemos

$$\sum_{d \le x} |\lambda(d)| \le \sum_{d \le x} \left(\log \frac{x}{d}\right)^2 = \sum_{d \le z} \left(\log \frac{x}{d}\right)^2 +$$

$$+ \sum_{d > z} \left(\log \frac{x}{d}\right)^2 \le z (\log x)^2 + 4x \left(\log(\log x)\right)^2 = O(x)$$

$$+ O\left(x (\log(\log x))^2\right) = o(x \log x)$$

y por el lema 9

$$S = 2x \log x + o(x \log x)$$

En el teorema 3 establecimos que el Teorema de Los Números Primos es equivalente a la proposición

$$\lim_{x \to \infty} \frac{Q(x)}{x} = 1$$

aquí demostraremos esta proposición de una manera elemental.

Para x creciente el cociente

$$\frac{Q(x)}{x}$$

tiene un límite inferior a y un límite superior A, entonces $0 < a \leq A$. Así que para probar (5) Tenemos que mostrar que

$$(18) \quad a = A = 1$$

La demostración está basada principalmente en la fórmula de Selberg

$$(19) \quad \frac{\varphi(x)}{x} + \frac{2}{x \log x} \sum_{p \leq x} \varphi\left(\frac{x}{p}\right) \log p - 2 = O(1)$$

La suma es extendida sobre los primos $p \leq y \leq \sqrt{x}$ también necesitamos

$$(20) \quad \sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$$

donde la suma es extendida sobre todos los primos $\leq x$.

Lema 13.

Si $\limsup_{x \to \infty} \frac{\varphi(x)}{x} = A$ y

$\liminf_{x \to \infty} \frac{\varphi(x)}{x} = a$

entonces

$$(21) \quad a + A = 1$$

Demostración.

Es posible dejar a x tender a infinito de tal manera que $\frac{\varphi(x)}{x}$ tiende a A. Si ε es un número positivo dado, tenemos

$$\varphi\left(\frac{x}{p}\right) > \left(a-\varepsilon\right)\frac{x}{p}$$

para cualquier x suficientemente grande y cualquier primo $p \le y = \sqrt{x}$, y por tanto

$$\frac{2}{x \log x} \sum_{p \le y} \varphi\left(\frac{x}{p}\right) \log p \ge \frac{2(a-\varepsilon)}{\log x} \sum_{p \le y} \frac{\log p}{p}$$

Se sigue de (20) que el lado derecho de esta desigualdad $\longrightarrow (a-\varepsilon)$ cuando $x \to \infty$. Así aplicando (19) obtenemos $2 - A \ge a - \varepsilon$. Puesto que esto se cumple para cualquier ε positivo tenemos

$$(22) \quad A + a \le 2$$

Por otro lado, es posible dejar a x tender a infinito de tal manera que $\frac{\varphi(x)}{x}$ tienda a a.

Dado $\varepsilon > 0$, tenemos

$$\varphi\left(\frac{x}{p}\right) < \left(A+\varepsilon\right)\frac{x}{p}$$

para cualquier x suficientemente grande y cualquier primo $p \le y = \sqrt{x}$, por lo tanto

$$\frac{2}{x \log x} \sum_{p \le y} \varphi\left(\frac{x}{p}\right) \log p \le \frac{2(A+\varepsilon)}{\log x} \sum_{p \le y} \frac{\log p}{p}$$

Se sigue de (20) que el lado derecho de esta desigualdad tiende a $A+\varepsilon$ cuando $x \to \infty$. Así aplicando (19) obtenemos $2-\alpha \leq A+\varepsilon$. Puesto que esto se cumple para cualquier $\varepsilon > 0$, concluimos que

$$(23) \quad A + \alpha \geq 2$$

Por lo tanto de (22) y (23)

$$A + \alpha = 2$$

En lo que sigue siempre dejaremos a la variable x tender a infinito de tal manera que

$$\frac{\psi(x)}{x} \quad \text{tiendo a } 1$$

Lema 14.

Si λ es un número dado $> \alpha$ y si la suma

$$S(x) = \sum{}' \frac{\log p}{p}$$

se extiende sobre todos los primos $p \leq x$ y tal que $\psi\left(\frac{x}{p}\right) \geq \frac{\lambda x}{p}$, entonces el cociente

$$\frac{S(x)}{\log x} \quad \text{tiende a cero cuando } x \to \infty.$$

Demostración.
Haciendo $y = \sqrt{x}$ obtenemos

$$\sum_{p \le x} Q\left(\frac{x}{p}\right) \log p = \sum_{p \le x} \log p \sum_{pq \le x} \log p =$$

$$= \sum_{p \le y} Q\left(\frac{x}{p}\right) \log p + \sum_{q \le y} Q\left(\frac{x}{q}\right) \log q -$$

$$- \left(\sum_{p \le y} \log p\right)^2 = 2 \sum_{p \le y} Q\left(\frac{x}{p}\right) \log p - \left(Q(\sqrt{x})\right)^2$$

Puesto que, el último término tiene orden $O(x)$, vemos que la fórmula de Selberg (19) también puede ser escrito como

$$\frac{Q(x)}{x} + \frac{1}{x \log x} \sum_{p \le x} Q\left(\frac{x}{p}\right) \log p - 2 = O(1)$$

Sea $\varepsilon > 0$, para cualquier x/p que exceda a un cierto número u el cual depende de ε tenemos que

$$Q\left(\frac{x}{p}\right) > (a - \varepsilon)\frac{x}{p}$$

existe un número positivo b que depende de u y también de ε, tal que

$$(24) \qquad Q\left(\frac{x}{p}\right) > (a - \varepsilon)\frac{x}{p} - b$$

para todos los primos p tales que $\frac{x}{p} \leq M$.
Así la última desigualdad se cumple para cualquier $p \leq x$. Si las sumas $\sum'$ se extienden sobre todos los primos $p \leq x$ tales que

$$\ell\left(\frac{x}{p}\right) \geq \frac{\lambda x}{p}, \text{ tenemos}$$

$$(25) \quad \sum{}' \ell\left(\frac{x}{p}\right) \log p \geq \lambda x \sum{}' \frac{\log p}{p} >$$

$$> (\lambda - a)\, x \sum{}' \frac{\log p}{p} + (a - \varepsilon)\, x \sum{}' \frac{\log p}{p}$$

Si las sumas $\sum''$ se extienden sobre todos los primos $p \leq x$ tales que

$$\ell\left(\frac{x}{p}\right) < \frac{\lambda x}{p} \quad \text{tenemos por (24),}$$

$$(26) \quad \sum{}'' \ell\left(\frac{x}{p}\right) \log p > (a - \varepsilon) x \sum{}'' \frac{\log p}{p} - b\ell(x)$$

de (25) y (26) deducimos que

$$\sum_{p \leq x} \ell\left(\frac{x}{p}\right) \log p = \sum{}' \ell\left(\frac{x}{p}\right) \log p +$$

$$+ \sum{}'' \ell\left(\frac{x}{p}\right) \log p$$

$$> (a - \varepsilon)\, x \sum_{p \leq x} \frac{\log p}{p} + (\lambda - a)\, x \sum{}' \frac{\log p}{p} - b\ell(x)$$

Sustituyendo este resultado en la fórmula (14), haciendo que x tienda a infinito de tal manera que $\frac{\varphi(x)}{x}$ tienda a A obtenemos

$$A + a - \varepsilon + (\lambda - a) \lim_{x \to \infty} \sup \frac{\sum' \frac{\log p}{p}}{\log x} \leq 2$$

Por lo tanto, recordando que $A + a = 2$

$$\lim_{x \to \infty} \sup \frac{\sum' \frac{\log p}{p}}{\log x} \leq \frac{\varepsilon}{\lambda - a}$$

Puesto que $\lambda - a > 0$ y ε puede elegirse arbitrariamente pequeño esto da el teorema deseado

Lema 15.

Si μ es un número positivo dado $< A$ y si la suma

$$R(x) = \sum' \left(\frac{\log p}{p}\right)\left(\frac{\log q}{q}\right)$$

se extiende sobre todos los primos p y q los cuales satisfacen los siguientes condiciones:

$$p \leq \sqrt{x}, \quad q \leq \sqrt{\tfrac{x}{p}} \quad y \quad \psi\left(\frac{x}{pq}\right) \leq \frac{\mu x}{pq}$$

entonces el cociente

$$\frac{R(x)}{(\log x)^2} \longrightarrow 0 \quad \text{cuando } x \longrightarrow \infty$$

Demostración.

Reemplazando a x por $\frac{x}{p}$ en la fórmula de Selberg obtenemos, haciendo $z = \sqrt{x/p}$

$$\theta(x) = \frac{2x}{p} + O\left(\frac{x}{p}\right) - \frac{2}{\log \frac{x}{p}} \sum_{q \le z} \theta\left(\frac{x}{pq}\right) \log q$$

Introduciendo esta expresión para $\theta\left(\frac{x}{p}\right)$ en la misma fórmula tenemos, haciendo $y = \sqrt{x}$

$$\theta(x) = 2x + O(x) - \frac{2x}{\log x} \sum \frac{\log p}{p} \left(2 + O(1)\right) + \frac{4V}{\log x}$$

donde

$$V = \sum_{p,q} \theta\left(\frac{x}{pq}\right) \frac{(\log p)(\log q)}{\log x/p}$$

es la suma extendida sobre todos los primos p y q tales que $p \le \sqrt{x}$, $q \le \sqrt{x/p}$. Puesto que por la fórmula (20)

$$\sum_{p \le x} \frac{\log p}{p} = \frac{1}{2} \log x + O(1)$$

se sigue que

$$\theta(x) = \frac{4V}{\log x} + O(x)$$

En cualquier término de la suma V tenemos que $p \le \sqrt{x}$ y $q \le \sqrt{x/p}$, y, por lo tanto

$$pq = p^{1/2} (pq^2)^{1/2} \le x^{3/4}$$

Así, si δ es cualquier número positivo tenemos,

$$\mathcal{U}\left(\frac{x}{pq}\right) < \left(A + \delta\right)\frac{x}{pq}$$

para x suficientemente grande

Escribimos

$$V = \sum' + \sum''$$

donde la primera suma se extiende sobre p y q, primos tales que

$$p \le \sqrt{x},\ q \le \sqrt{x/p} \quad \text{y} \quad \mathcal{U}\left(\frac{x}{pq}\right) \le \frac{\mu x}{pq}$$

y la segunda suma sobre los primos p y q tales que

$$p \le \sqrt{x},\ q \le \sqrt{x/p} \text{ y } \mathcal{U}\left(\frac{x}{pq}\right) > \frac{\mu x}{pq}$$

Entonces

$$V \le \mu x \sum' \frac{1}{\log \frac{x}{p}} \frac{\log p}{p} \frac{\log q}{q} + (A+\delta)x \sum'' \frac{1}{\log \frac{x}{p}} \frac{\log p}{p} \frac{\log q}{q}$$

donde las sumas están tomadas como antes.

Además obtenemos

$$V \leq (A+\delta) \times W - (A+\delta-\mu) \times \sum{}' \frac{1}{\log \frac{x}{p}} \frac{\log p}{p} \frac{\log q}{q}$$

donde

$$W = \sum_{p,q} \frac{1}{\log \frac{x}{p}} \frac{\log p}{p} \frac{\log q}{q} = \sum_{p \leq y} \frac{1}{\log \frac{x}{p}} \frac{\log p}{p} \sum_{q \leq z} \frac{\log q}{q}$$

son las sumas extendidas sobre todos los primos $p \leq y = \sqrt{x}$ y sobre todos los primos $q \leq z = \sqrt{x/p}$.

Aplicando la fórmula (20) obtenemos

$$W = \sum_{p \leq y} \frac{\log p}{p} \left(\frac{1}{2} + O(1) \right) = \frac{1}{4} \log x + O(\log x)$$

Por lo tanto

$$U(x) \leq (A+\delta) x - \frac{4}{\log x} (A+\delta-\mu) x \sum{}' \frac{1}{\log \frac{x}{p}} \frac{\log p}{p} \frac{\log q}{q} +$$

$$+ \eta x$$

donde $\eta \to 0$ cuando $x \to \infty$. De esto deducimos que

$$\frac{4}{(\log x)^2}\,(A+\delta-\mu)\sum{}' \frac{\log p}{p}\,\frac{\log q}{q} \le A+\delta-\frac{\theta(x)}{x}+n$$

donde la suma es la misma del lema 15.
Por lo tanto, para $x \to \infty$ de tal manera

$$\frac{\theta(x)}{x} \longrightarrow A$$

$$\lim_{x\to\infty} \sup \frac{1}{(\log x)^2} \sum{}' \frac{\log p}{p}\,\frac{\log q}{q} \le \frac{\delta}{4(A-\mu)}$$

Puesto que $A-\mu>0$ y δ es un número arbitrario positivo esto prueba el lema.

Por los significados de los lemas 13, 14 y 15 podemos ahora probar la relación

(18) $\quad \alpha = A = 1$

Supongamos que $A>\alpha$. Sean $\tau>1$ tal que $\tau\alpha<A$ y δ un número positivo pequeño tal que

(27) $\quad A-\alpha\tau \ge \delta\tau + 2\delta$

Denotamos por N a un número natural

Consideremos la suma

$$S=\sum{}_2 \frac{\log p}{p}\,\frac{\log q}{q}\sum{}_3 \frac{\log r}{r}$$

donde Σ_2 se extiende sobre todos los primos p y q tales que $p \le \sqrt{x}$, $q \le \sqrt{x/p}$, $pq \ge N$, $Q\left(\frac{x}{pq}\right) \ge (A-\delta)\frac{x}{pq}$

y Σ_3 se extiende sobre todos los primos r tales que

$$\frac{pq}{T} < r \le T\, pq$$

si no existen primos r, la suma $\Sigma_3 = 0$. Para cualquier término de Σ_3 tenemos que

$$r \le T\, pq = T\, p^{1/2} (pq^2)^{1/2} \le T\, x^{1/4} x^{1/2} = T\, x^{3/4} \le x$$

cuando x es suficientemente grande. Para los mismos términos probemos la desigualdad

$$(28) \quad Q\left(\frac{x}{r}\right) > (a+\delta)\frac{x}{r}$$

cuando x es suficientemente grande. Esta desigualdad es verdadera para todos los $r \le pq$ puesto que

$$Q\left(\frac{x}{r}\right) \ge Q\left(\frac{x}{pq}\right) \ge (A-\delta)\frac{x}{pq} > (A-\delta)\frac{x}{Tr} \ge (a+\delta)\frac{x}{r}$$

en virtud de (27). Ahora consideremos los términos con $r > qp$, si hacemos $\frac{x}{r} = u$ y $\frac{x}{pq} = v$ obtenemos $u < v \le Tu$. Si en la fórmula de Selberg

$$(\log x)\, Q(x) + 2 \sum_{p \le y} Q\left(\frac{x}{p}\right) \log p = 2x \log x + O(x \log x)$$

donde $y = \sqrt{x}$, primero reemplazamos x por v y

luego x por u, obtenemos restando

$$(\log v)\,\ell(v)-(\log u)\,\ell(u)\le 2v\log v-2u\log u+O(u\log u)$$

o

$$\ell(u)\ge\frac{\log v}{\log u}\,\ell(u)-2(v-u)-2v\,\frac{\log v-\log u}{\log u}+O(u)$$

o,

$$\ell(u)>(A-\delta)v-2(v-u)+O(u)=2u-(2-A+\delta)v+O(u)$$

y puesto que

$$a+A=2 \quad y \quad A-a\delta\ge 2-\delta+2\delta$$

$$\ell(u)>(a+2\delta)u+O(u)$$

Si x es suficientemente grande,

$$\ell\left(\frac{x}{r}\right)=\ell(u)>(a+\delta)u=(a+\delta)\frac{x}{r}$$

Esto prueba la desigualdad (28) para toda r.
Consecuentemente

$$S\le\sum_r\frac{\log r}{r}\sum_q\frac{\log p}{p}\quad\frac{\log q}{q}$$

donde la primera suma se extiende sobre todos los primos $r\le x$ tales que

$$\ell\left(\frac{x}{r}\right)\ge(a+\delta)\frac{x}{r}$$

y la suma $\sum_4$ se extiende sobre todos los primos p y q tales que

$$p \le \sqrt{x}, \quad q \le \sqrt{x}/p, \quad \frac{r}{\sqrt{r}} \le pq < \sqrt{r}$$

Así tenemos haciendo $y = \sqrt{x}$ y $t = \frac{\sqrt{r}}{p}$,

$$\sum_4 \frac{\log p}{p} \frac{\log q}{q} \le \frac{\sqrt{r}}{r} \sum_{p \le y} \log p \sum_{q \le t} \log q =$$

$$= \frac{\sqrt{r}}{r} \sum_{p \le y} (\log p)\, Q\left(\frac{\sqrt{r}}{p}\right) < C_1 \sum_{p \le y} \frac{\log p}{p} < C_2 \log r$$

donde C_1 y C_2 son constantes positivas. En consecuencia

$$S \le C_2 \log x \sum_r \frac{\log r}{r}$$

donde la suma se extiende sobre todos los primos $r \le x$ tales que

$$Q\left(\frac{x}{r}\right) \ge (a+\delta)\frac{x}{r}$$

Entonces por el lema 14

$$(24) \quad S = n_1 (\log x)^2$$

donde $n_1 \to 0$ cuando $n \to \infty$

Ahora consideremos la suma

$$T = \sum \frac{\log p}{p} \frac{\log q}{q}$$

que se extiende sobre todos los primos p y q tales que $p \le \sqrt{x}$, $q \le \sqrt{x/p}$, $pq \ge N$. Haciendo

$$y = \sqrt{x}, \quad z = \sqrt[3]{x} \quad y \quad n = \sqrt{N}$$ se tiene

$$T \ge \left(\sum_{p \ge n}^{p \le y} \frac{\log p}{p} \right) \left(\sum_{q \ge n}^{q \le z} \frac{\log q}{q} \right)$$

Por lo tanto por (29)

$$(30) \qquad T > C_3 (\log x)^2$$

siendo C_3 una constante positiva, hagamos

$$T = \sum\nolimits_2 \frac{\log p}{p} \frac{\log q}{q} + \sum\nolimits_2{}' \frac{\log p}{p} \frac{\log q}{q}$$

donde la última suma se extiende sobre todos los primos p y q que satisfacen las condiciones

$$p \le \sqrt{x}, \quad q \le \sqrt{x/p}, \quad \text{ó} \quad \left(\frac{x}{pq}\right) < (A - \delta) \frac{x}{pq}$$

Esta última suma, en virtud del lema 15 es igual a

$$n_2 (\log x)^2$$

donde $n_2 \to 0$ cuando $x \to \infty$. Por lo tanto

$$\sum\nolimits_2 \frac{\log p}{p} \frac{\log q}{q} = T - n_2 (\log x)^2$$

y en virtud de (30)

$$(31)\quad \sum \frac{\log p}{p}\,\frac{\log q}{q} > \tfrac{1}{2} C_2 (\log x)^2$$

para x suficientemente grande.

En la suma $\sum_2$ ahora consideramos para un valor fijo de x los primos los cuales tienen la propiedad que la suma

$$\sum_3 \frac{\log r}{r}$$

toma su valor mínimo μ. μ depende únicamente de x. Entonces por (31)

$$S \geq \mu \sum_2 \frac{\log p}{p}\,\frac{\log q}{q} > \tfrac{1}{2}\mu C_3 (\log x)^2$$

Si comparamos este resultado con (29) obtenemos cuando $x \to \infty$ que

$$\mu = \sum_3 \frac{\log r}{r} \to 0$$

Consecuentemente para cualquier número positivo ε y para cualquier número natural N le corresponde un número $t = pq \geq N$ tal que

$$\sum_{r \leq \tau t}^{r\tau > t} \frac{\log r}{r} < \varepsilon$$

La suma se extiende sobre todos los primos r los cuales son $> \frac{t}{\tau}$ y $\leq \tau t$. Por lotanto

$$\sum_{r \leq \tau t}^{r\tau > t} \log r < \varepsilon \tau t \quad y$$

$$(32)\quad \vartheta(\tau t) - \vartheta\left(\frac{t}{\tau}\right) < \varepsilon \tau t$$

Si N y por lo tanto también t, son suficientemente grandes, tenemos

$$Q(Tt) > (a-\varepsilon)Tt$$

y $$Q\left(\frac{t}{T}\right) < (A+\varepsilon)\frac{t}{T}$$

En consecuencia, se sigue de (32) que

$$(a-\varepsilon)T - \frac{A+\varepsilon}{T} < \varepsilon T$$

Esta desigualdad se cumple para cualquier número positivo ε. Por lo tanto obtenemos

$$aT^2 - A \leq 0$$

O de otra manera, tenemos

$$aT < A \quad y \quad a > 0$$

Así cualquier número

$$T < \frac{A}{a}$$

tiene la propiedad que

$$T^2 < \frac{A}{a}$$

Si T tiende a $\frac{A}{a}$, obtenemos

$$\frac{A^2}{a^2} \leq \frac{A}{a}$$

que implica $\frac{A}{a} \leq 1$

Puesto que

$$a \leq A \quad y \quad A + a = 2$$

Claramente tenemos que

$$A = a = 1$$

Con esto hemos demostrado que

$$\lim_{x \to \infty} \frac{\ell(x)}{x} = 1$$

y como es equivalente al

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

que es el enunciado del Teorema de los Números Primos, hemos terminado la demostración de este Teorema.

B I B L I O G R A F I A

Andrews, G.E. : Number Theory
W.B. Lauders Company 1971

Apostol, T.M. : Introduction to Analitic Number Theory
Undergraduate texto in Mathematics
Springer-Verlang 1976

Birkhoff, G : Modern Algebra (a surveyof) 3ª edición
Macmilan Co.

Dickson, L.E. : History of the theory of Numbers
Vol. I, II, III
Chelsea Publishing Co. 1971.

Goldstein, L.J : A History of the Prime Number
Theorem.
American Mathematical Monthly
Vol. 80 1973.

Griffin, H. : Elementary theory of Numbers
McGrow-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. Co. 2ª edición

LeVeque, W. J. : Topics in Number Theory Vol. I
Addison - Wesley Publishing Co. 1965

Nagell, T. : Introduction to Number Theory
John Wiley & Sons, Inc. 1951

Pineda, M. : Topicos en la Teoria de los números
Tesis, México, D.F. 1984

Shanks, D. : Solved and Unsolved problems in
Number Theory 2ª edición
Chelsea Publishing Co. 1978

Shapiro, H.N. : Introduction to the Theory of
Numbers.
John Wiley & Sons, 1983

Vinogradov, I.N. : Fundamentos de la Teoría
de los Números
Editorial Mir 1977