Numeros son simbolos para contar

1, 2, 3, 4, ...

o oo ooo oooo

~~a++~~ $3+1=4$

$a+b=b+a$

defino $a+0=0+a=a$

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

defino $a+(-a)=0$

Ahorrar tiempo $\underbrace{a+\dots+a}_{b} = ab$

$ab=ba$

$a(bc)=(ab)c$

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

~~a<0~~ $a>b$ si $a=b+c$ si $a>0 \Rightarrow$

$1>0 \dots$ $-a<0$


relacion nos geometrica

~~los numeros representan un segmento~~ ?

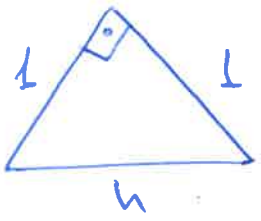
claramente

~~$n<1 \Rightarrow n-1<0$~~

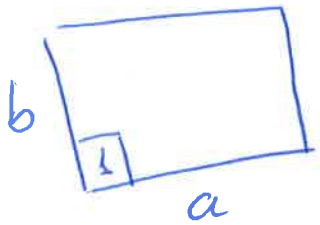
no representan el segmento


$2X=1 \quad X=\frac{1}{2}$

aparecen los racionales pueden estos representar todos los números ⑥

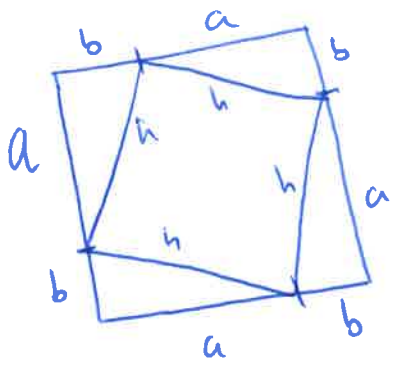



El área, así como la distancia es fácil de definir en cuadrados




¿cuánto cabe

ab




$(a+b)^2 = a^2+2ab+b^2$

$h^2 + 2ab$ luego

$$\boxed{h^2 = a^2+b^2}$$

$h^2 = 2$ $\quad \boxed{h = \sqrt{2}}$

Veremos que no puede ser $h = \frac{p}{q}$

En general es difícil reconocer cuando un número es irracional

Representamos los números ~~en dos dimensiones~~ con objetos geométricos bidimensionales. El más sencillo es

Sucesión $n^2 = S_n = S_{n-1} + 2(n-1) + 1$

$$(n+1)^2 = S_{n+1} = S_n + 2n + 1$$

$$(n+1)^2 = (2n+1) + (2n-1) + \cdots + 1$$

Binomio de Newton

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j$$

$$\boxed{\binom{n+1}{j} = \binom{n}{j} + \binom{n}{j-1}} \qquad \binom{n}{0} = \binom{n}{n} = 1$$

Números triangulares

$$t_n = t_{n-1} + n = n + n-1 + \cdots + 1$$

$$t_n = \frac{n(n+1)}{2}$$

El 5 no es cuadrado ni triangular

En general

Gauss 1796

Lagrange 1798

Cauchy 1813 todo numero se escribe

como $m$ $n$-gonales todos o ó 1 salvo 4.

Inducción para los binomiales

$$P_{N,n} = P_{N-1,n} + (N-2)(n-1) + 1$$

$$\sum_{j=0}^{n-1} (a\,y + b) = a\frac{(n-1)n}{2} + bn$$

$$= (N-2)\frac{n(n-1)}{2} + n$$

Son todos los numeros poligonales por algun $K$

$$M = (K-2)\frac{n(n-1)}{2} + n$$

Trivialmente, si quito este caso trivial

supongo que si $M = \frac{n}{2}\left[(N-2)(n-1) + 2\right]$

luego es un producto de numeros y sabemos que lo primo por definicion no lo son

si permitimos no regulares rectangulares

$a \cdot b$

Es primo $\Leftrightarrow$ no es rectangular.

Fermat, 1636, Gauss 1796, Lagrange, 1798 Cauchy 1815

Induccion

$P(1)$ cierta

$P(n-1) \Rightarrow P(n)$ $\Rightarrow$ $P(n)$ es cierta $\forall n$.

Aplicacion

$$(a+b)^n = \sum \binom{n}{j} a^{n-j} b^j$$

si ~~(n+1)² = n²~~

$1+3+\dots+2n-1 = n^2+3$

Antes de

$(n+1)^2+3$

Summary

Numero de Fibonacci

1 1

Numero de Lucas

1 3

$U_{n-1}+U_{n+1} = V_n$

Ejercicio

Equivalencia con P(1) cierta

P(1) .. P(n-1) ciertas

Principio de Inclusión exclusión

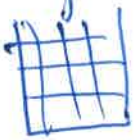
$N - N_1 - N_2 - \dots - N_k + [N_{12}] + \dots$

$(1-1)^n = 0$ i si no.

ni cubos ni cuadrados hasta $2^{64}$

Principio del palomar

Amigos



palomar completo

Cerdos $n+1$ manzanas de $n$

Asignatura..... Grupo .....
Apellidos..... Nombre .....
Ejercicio del día .....

(10)

# Divisibilidad

objetivo Teorema fundamental de la aritmetica

Definicion a divide a b $a|b$ si $ad=b$
en ese caso $a|b$ a es divisor de b

Propiedades $\forall a|0, 1|a, a|a$ (divisores propios)

Propiedades: 1) $a|b \Rightarrow a|bc \quad \forall c$
2) $a|b \quad a \leq b \quad b \neq 0$
3) $ac|bc \ (c\neq 0) \iff a|b$
4) $a|b \quad b|c \Rightarrow a|c$
5) $a|b \quad a|c \Rightarrow a|$ suma
6) $a|b \quad b|a \Rightarrow a=b$

Una forma de ver si b divide es m.c.d.

Def: $(a,b)$ maximo divisor comun de a y b
$[a,b]$ minimo comun multiplo

Teorema si $a|b \Rightarrow$ $a=(a,b)$
$b=[a,b]$

- Sea P.a. Cualesquiera $n^2+1$ numeros hacen una sucesion monotona de $n+1$ elementos.

Divisibilidad: Objetivo TFA que clasifica los numeros enteros respecto a la operacion division

Def: $a|b$ si $ad=b$ en caso contrario $a \nmid b$

Es claro $a|0$ $1|a$ $a|a$.

si $a|b$ a es un divisor de b $a \neq 1, b$ entonces es un divisor propio.

Propiedades: 1) $a|b \Rightarrow a|bc \ \forall c$

2) $a|b \Rightarrow a \leq b$ $(b \neq 0)$ $(a, b \geq 0)$

3) $c \neq 0$ $ac|bc \Leftrightarrow a|b$

4) $a|b$ $b|c \Rightarrow a|c$

5) $a|b$ y $a|c \Rightarrow a|mb+nc$

6) $a|b$ y $b|a \Rightarrow a=b$

Definicion m.c.d $(a,b)$

m.c.m $[a,b]$

Asignatura..... Grupo .....
Apellidos..... Nombre .....
Ejercicio del día .....

(11)

Una forma de calcular el m.c.d. es gracias a la ordenación de los elementos

Teorema (Algoritmo de división)

$\forall\, a, (b>0)$ existen $q, r$ únicos tal que

$$a = qb + r \qquad 0 \le r < b$$

$\{a - qb\}$ $\quad a+b \quad a \quad a+b \quad a+2b$

el menor entero $\ge 0$

$$0 \le r = a - qb$$

si $r > b$ $\quad r = b + s$

$$a = qb + b + s = (q+1)b + s$$

$0 \le s < r$ contradiciendo que es el menor

son únicos $\quad q_1 b + r_1 = q_2 b + r_2$

$$(q_2 - q_1)b = r_2 - r_1 \qquad q_2 = q_1 \qquad r_2 = r_1$$

Es de $\left[\frac{a}{b}\right] = q$

repitiendo el proceso

$a = r_0$

$b = r_1$

$a = q_1 b + r_2$

$b = q_2 r_2 + r_3$

$\vdots$

$r_j = r_{j+1} q_{j+1} + r_{j+2}$

$(a,b) \mid (r_2, b) \mid \cdots \mid r_j \ \forall j$

luego $(a,b) \mid r_N$

por otro lado $r_N \mid (r_N, r_{N-1}) \mid \cdots \mid (a,b)$ luego

$r_N \leq (a,b)$ y $r_N = (a,b)$

Corolario

Todo divisor divide al m.c.d

Ejemplo $(154, 275)$

Volviendo hacia atrás hemos resuelto una ecuación diofántica $ax+by=d$

Teorema $ax+by=d$ tiene sol $\Leftrightarrow (a,b) \mid d$

$0<l$ el menor $ax+by=l$ $\forall a$ $a = q l + r$

a tiene y d tiene luego $l \leq a$

$a - ql = r$ y tiene rep. $l \mid a$ y $l \mid b$

$l \mid (a,b)$ pero $(a,b) \mid a$ y $b \Rightarrow (a,b) \mid l \Rightarrow \boxed{l = (a,b)}$

$ax+by = D = r(a,b) + s$ s tiene rep $< (a,b)$

no puede ser luego $s=0$ y $(a,b) \mid D$

teorema Si $a|b \Rightarrow (a,b)=a$
$[a,b]=b$

Algoritmo de división Sea $b>0$ a entero $\exists\, q\ r$ únicos

$$a = qb + r \qquad 0 \le r < b$$

$$q = \left[\frac{a}{b}\right]$$

[Si nido como de lejos está b de dividir a a
tiene que tener una estrecha relación con el m.c.d.]

$$a = r_0$$
$$b = r_1$$

$$r_j = q_{j+1} r_{j+1} + r_{j+2}$$

$$0 \le r_i \le r_{i-1} < b$$

en algún punto $r_{N+1} = 0$ $r_N$ es el m.c.d.

$(a,b) \mid r_k$ por dos lados $r_N \mid (r_N, r_{N-1})$

pues $r_{N-1} = q_N r_N$

luego $r_N \mid (r_{N-1}, r_{N-2}) \Rightarrow r_N \mid (a,b) \Rightarrow$

$(a,b) \le r_N \le (a,b) \Rightarrow r_N = (a,b)$

Corolario si $d|a$ y $b \Rightarrow d|(a,b)$

Ejemplo $(154, 275)$ ⟶

Es mucho mas fuerte

$(a,b) = ax+by$

Teorema $ax+by=n \iff (a,b)/n$

Hemos visto que $(a,b) = ax_0+by_0$.

si $n = k(a,b) \Rightarrow a(kx_0)+b(ky_0)=n$

Supongamos $ax+by=n$ ~~$(a,b)/n \Rightarrow n = q(a,b)+r$~~

Sea $\ell$ el menor nº representable $\ell = (a,b)$

Supongamos que no lo divide $\Rightarrow r=0$.

De hecho podemos ~~resolver~~ encontrar todas las soluciones gracias al siguiente lema

Lema: Si $p/ab$ y $p \nmid a \Rightarrow p/b$

Si $d/ab$ y $(d,a)=1 \Rightarrow d/b$

se llaman coprimos

Teorema Toda solución de $ax+by=n$

~~$x$~~ $x = x_0 + t\frac{b}{(a,b)}$

$y = y_0 - t\frac{a}{(a,b)}$

Ejemplo $154x+275y=-22$

Teorema todas soluciones $x = x_0 + t\frac{a}{(a,b)}$

$y = y_0 - t\frac{b}{(a,b)}$

Lema: si $p \mid ab$ y $p \nmid x \Rightarrow p \mid b$

$xp + ya = 1$

$xpb + yab = b \Rightarrow p \mid b$

en general si $d \mid ab$ y $(d,a) = 1 \Rightarrow d \mid b$ □

prueba $-(x - x_0)\frac{a}{(a,b)} = \frac{b}{(a,b)}(y - y_0)$

Encontrar todas las soluciones de

$154x + 275y = -22$

Ya podemos probar varios teoremas

Def: Un número es primo si no tiene divisores propios

Teorema todo nº es producto de primos

el menor divisor es primo $n = p_1 \cdots p_r$

$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la descomposición normal

Teorema es única

$p_1^{\alpha_1} \cdots p_s^{\alpha_r} = q_1^{\beta_1} \cdots q_r^{\beta_r}$

Inducción

~~Teorema~~

**Teorema** Todo nº es producto de primos

el menor debe ser primo ∎

descomposicion normal

**Teorema** (TFA) La descomposicion normal es única

1 no es primo

no es evidente!!

$(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$

A pesar de su importancia no da ni siquiera los primos

**Teorema** (Euclides)

$N = P_1 \cdots P_n + 1$ no es primo ni divisible por primo

Algo mas

$$P_{n+1} \leq (P_1 \cdots P_n) \leq (P_1 \cdots P_{n-1})^2 \leq (P_1 \cdots P_{n-2})^4$$

$$P_{n+1} \leq 2^{2^{n-1}}$$

$P_0 = 2$ $\quad P_n \leq 2^{2^n}$

$$P_{n+1} \leq (P_1 \cdots P_n) + 1 = 2^2 2^{2^2} 2^{2^3} \cdots 2^{2^n} + 1$$

$$= 2^{2+2^2+\cdots+2^n} + 1 = 2^{2^{n+1}-2} + 1 < 2^{2^{n+1}}$$

$\#_{n+1} < \#_n$

$$V_{2^{n+1}} = V_{2^n}^2 - 2$$

$$V_{2^m} = \left(V_{2^{m-1}}\right)^2 - 2 = \left(k V_{2^n} + 2\right)^2 - 2$$

$$= \tilde{k} V_{2^n} + 2$$

$$P_n < V_{2^n} = 2^{2^n} + 0^{2^n} < 2^{2^n} + 1$$

$$\frac{V_{2^n}}{2^{2^n}} \longrightarrow 0 \quad \text{mejor cota}$$

$3, 5, 17, 257, 65537$

$P_0 = 3 < P_1 = 5 <$

A la vista de los primeros casos Fermat conjetura

1736 Euler $641 \mid F_5$ !!

Se sabe $F_{23}$ todos son compuesto y p. ejemplo

$F_{3310}$ $10^{990}$ cifras es compuesto

$P(n)$ no es siempre primo

por otra parte $2^n + 1$ primo $\Rightarrow n = 2^k$

$2^n - 1$ radicalmente distinta

$2^n - 1$ primo $\Rightarrow$ $n$ primo

$(x^n - 1) = (x-1)(x^{n-1} + \cdots + 1)$

primos de Mersenne

$2^{6972593} - 1$ 2098960 cifras

No se sabe si hay infinitos A pesar de que

Test Lucas - Lehmer

$$M_p / F_{p-1} \iff M_p \text{ primo}$$

La mejor forma de probar la infinitud de los primos se debe a Euler

$$\zeta(s) = \sum \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

consecuencia del T.F.A.

$$\infty = \lim_{s \to 1} \sum \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p}\right)^{-1} < \infty$$

la serie $\sum \frac{1}{p}$ diverge !! ver Chandra pag 105 siguiente página (51)

La fórmula producto no es particular de $\zeta(s)$

$$L(s) = \sum_{n \geq 1} \frac{a_n}{n^s} \qquad a_n a_m = a_{nm}$$

$$\Rightarrow \prod_p \left(1 - \frac{a_p}{p^s}\right)^{-1} = L(s)$$

Chandra pag 105



$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

$$\lg \zeta(s) = -\sum_p \lg\left(1 - \frac{1}{p^s}\right)$$

$$\lg(1-x) = -\sum_{n \geq 1} \frac{x^n}{n} \Rightarrow -\lg(1-x) < \sum_{n \geq 1} x^n$$

$$= \frac{x}{1-x} < 2x \quad \text{si } x < \frac{1}{2}$$

Si $p$, primo $s > 1 \Rightarrow \frac{1}{p^s} < \frac{1}{2}$ luego

$$\lg \zeta(s) < 2 \sum_p \frac{1}{p^s}$$

Si $\sum_p \frac{1}{p}$ fuese convergente $\sum_p \frac{1}{p^s} < \sum_p \frac{1}{p}$

Luego $\lg \zeta(s) < 2 \sum \frac{1}{p} = K$ para todo $s > 1$

Sin embargo $\lim_{s \to 1} \sum_{n \geq 1} \frac{1}{n^s} = \infty$

luego $\exists\, s$ tal que $\sum_{n \geq 1} \frac{1}{n^s} > e^{2k}$

para cualquier $k$ luego

$2k < \lg \zeta(s) < 2k$ que no

puede ser.

# funciones aritméticas

**Def:** Si tienen dominio en $\mathbb{N}$

**Def:** $f(n)$ es multiplicativa si

$$f(nm) = f(n)\cdot f(m) \quad \forall (n,m)=1$$

completamente multiplicativa,

$$\forall (n,m)$$

Ejemplos $1$, $n$, $\Pi(n)$ no mult.

**Teorema:** Si $f$ es mult $\Rightarrow \sum_{d|n} f(d) =$ también

$$d(n) = \prod_{i=1}^{r} (1+\alpha_i) \qquad n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$$

caracterizar $d(n) = 2$ $\quad \prod_{i=1}^{r}(1+\alpha_i) = 2 \quad \alpha_i \geq 1$

los primos !! Ejercicio $d(n)=6$.

Si tomamos $f(n)=n$ $\quad \sigma(n) = \sum_{d|n} d = \prod \frac{p^{\alpha}-1}{p-1}$

$\sigma(n) = 6$ no tiene sentido.

pero y lineal en $n$

$1+2+3+6 = 2\cdot 6$

$1+2+4+7+14+28 = 2\cdot 28$

¿Existen algún número más tal que $\sigma(n) = 2n$ ?

Se les llama perfectos

- no se sabe si hay $\infty$
- no se sabe si hay impares

$n$ perfecto par $\Leftrightarrow$ $n = 2^{p-1}(2^p - 1)$ primo de Mersenne

En contraposición con el [illegible] que mide en cuántos [illegible]

$\phi(n) = \#\{ N \leq n \mid (N, n) = 1 \}$.

I-E $(N, n) = 1 \Leftrightarrow (N, p) = 1 \ \forall\, p \mid n$

$p_i$ si $p_i \mid n$

$$n - \sum \frac{n}{p_i} + \sum \frac{n}{p_i p_j} - \dots$$

$$1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k}$$

$$P(X) = \prod_{i=1}^{r} \left(X - \frac{1}{p_i}\right) \qquad P(1) \qquad (X-\alpha)(X-\beta) = X^2 - (\alpha+\beta)X + \alpha\beta$$

$$\boxed{\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)}$$

Conviene en este contexto definir una función aritmética a I-E.

$$\mu(n) = \begin{cases} 0 & \text{si } p^2 \mid n \\ (-1)^N & n = p_1 \cdots p_N \\ 1 & n = 1 \end{cases}$$

es claramente multiplicativa.

Hecho más destacado es la fórmula de inversión

Si $F(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$

Consecuencia de la ortogonalidad de $\mu$ — en un post sobre ejercicios del recreo

Lema: $\sum_{d|(n)} \mu(d) = \begin{cases} 0 & n \neq 1 \\ 1, & n = 1 \end{cases}$

Demo:

del teor.

$$\sum_{d|n} \mu(d) \sum_{N|\frac{n}{d}} f(N) \qquad N|\tfrac{n}{d} \Leftrightarrow d|\tfrac{n}{N}$$

$$= \sum_{N|n} f(N) \sum_{d|\frac{n}{N}} \mu(d) = f(n) \quad \boxtimes$$

Corolario si $\sum_{d|n} f(d)$ mult $\Rightarrow f$ mult

$n = \sum \phi(d)$ es multiplicativa.

La relacion entre $\mu(n)$ y las sumas trigonometricas es en realidad mas estrecha de hecho podemos definir $\mu$ en terminos de estas

Sea $$c_n(m) = \sum_{\substack{1 \le h \le n \\ (h,n)=1}} e\left(\frac{hm}{n}\right)$$

donde $e(z) = e^{2\pi i z}$. Estas sumas ~~son~~ han sido muy estudiadas en primer lugar por ~~Ramanujan y esto muy relacionado~~ y aparecen en diferentes partes de la teoria analitica

Teorema: $$c_n(m) = \sum_{d \mid (n,m)} \mu\left(\frac{n}{d}\right) d$$

Lema: Cada fraccion $1 \le h \le n$ $\frac{h}{n} = \frac{a}{d}$ con $(a,d)=1$ $a \le d$ y todas aparecen

$d \mid n$

luego $$\sum_{1 \le h \le n} e\left(\frac{hm}{n}\right) = \sum_{d \mid n} \sum_{\substack{1 \le a \le d \\ (a,d)=1}} e\left(\frac{am}{d}\right)$$

$$\sigma_m(n) = \sum_{d \mid n} c_d(m)$$

$$\sigma_m(n) = \begin{cases} 0 & n \nmid m \\ n & n \mid m \end{cases}$$

el teorema de inversión

$$c_n(m) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \sigma_m(d) = \sum_{d \mid (n,m)} \mu\left(\frac{n}{d}\right) \cdot d$$

$c_n(m)$ es $c_n(m)$ con $(n,m)=1$

con lo cual $\boxed{c_n(1) = \mu(n)}$

Hemos introducido las f. ant en relación con $\zeta(s)$ y ~~en realidad ésta~~ la serie asociada de esta relación podemos deducir propiedades para la función aritmética

## Funciones generatrices

Dada $f(n)$ llamamos serie de Dirichlet asociada a

$$L_f = \sum_{n \geq 1} \frac{f(n)}{n^s}$$

$(n)^s (m)^s = (nm)^s$

Primer ejemplo $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ y comprobar que es por cierto un cierto entero

~~A pesar de que~~ ads converge para $s > 1$

$\zeta(2) = \frac{\pi^2}{6}$ $\boxed{\zeta(2n) = \frac{(-1)^{n+1} 2^{2n-1} B_{2n} \pi^{2n}}{(2n)!}}$

Cuando que no sabe $\zeta(2n+1)$ ni siquiera si es racional

otros ejemplos $\sum_{n\geq 1} \frac{d(n)}{n^s}$, $\sum_{n\geq 1} \frac{\mu(n)}{n^s}$, $\sum \frac{\phi(n)}{n^s}$

¿Como evaluarlos?

$|f(n)|$ abs convergente

Si $f(n)$ es multiplicativa $\Rightarrow$

$$\sum \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right)$$

$$\sum_{n\geq 1} \frac{\mu(n)}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)} \qquad \blacksquare$$

$$\boxed{\sum_{n\geq 1} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}} \qquad \lim_{s\to 0} = 0$$

$$\sum_{n\geq 1} \frac{d(n)}{n^s} = \prod_p \left(1 + \frac{2}{p^s} + \frac{3}{p^{2s}} + \cdots\right)$$

no es manejable

multiplicación

$$F(s) = \sum_{n\geq 1} \frac{d(n)}{n^s} \qquad \sum_{n\geq 1} \frac{g(n)}{n^s} = G(s)$$

entonces $F(s)\cdot G(s) = \sum \frac{\sum_{d\mid n} d(d)\, g\left(\frac{n}{d}\right)}{n^s}$

se puede probar convergencia por función formal

$$\zeta^2(s) = \sum_{n\geq 1} \frac{\phi(n)}{n^s} \quad \text{luego}$$

$$\boxed{\sum_{n\geq 1} \frac{\phi(n)}{n^2} = \frac{\pi^4}{36}}$$

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n\geq 1} \frac{\phi(n)}{n^s}$$

**Teorema:** $$\frac{\sigma_{s-1}(n)}{n^{s-1}\zeta(s)} = \sum_{n\geq 1} \frac{c_n(n)}{n^s}$$

$$\sum_{n\geq 1} \sum_{d|(n,m)} \frac{\mu\left(\frac{n}{d}\right) d}{n^s} \qquad n, d \to \frac{p}{n}$$

$$= \sum_{D\geq 1} \sum_{\substack{d|m \\ Dp=m}} \frac{\mu(D)\, d}{D^s d^s}$$

$$\sum_{D\geq 1} \frac{\mu(D)}{D^s} \sum_{d|m} \frac{1}{d^{s-1}} = \frac{\sigma_{1-s}(m)}{m^{s-1}\zeta(s)}$$

$$\boxed{\sum_{n\geq 1} \frac{c_n(m)}{n^2} = \frac{\sigma(m)\, 6}{m \cdot \pi^2}}$$

nos de fórmulas para manejar la serie

ahora el producto de funciones (★★)

Teorema: $\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$

A partir de cálculo de serie hacer aplicaciones en ostentos de identidades así

$$1 = \zeta(s)\frac{1}{\zeta(s)} = \sum \frac{\sum_{d|n} \mu(d)}{n^s}$$

o bien

Si $F(s)\zeta(s) = G(s)$

es claro que $F(s) = \frac{1}{\zeta(s)} G(s)$

la fórmula de inversión

Estas funciones generadoras que hemos visto son un caso particular de

$$\sum f(n) \frac{U_n(s)}{\lambda_n} \qquad e^{-\lambda_n s}$$

$\lambda_n = \log n$

$\lambda_n = n$

$U_n(s) = n^{-s}$ mul. aditiva

$\sum f(n) x^n$ aditiva

encontre el nº de soluções de $2x+3y=n$

$x \geq 0, y \geq 0$

$$\frac{1}{1-x^2} = \sum_{n \geq 0} x^{2n}$$

$$\frac{1}{1-x^3} = \sum_{n \geq 0} x^{3n}$$

$$\frac{1}{(1-x^2)(1-x^3)} = \sum_{n \geq 0} \Gamma(n)\, x^n$$

deriva 3 vezes

$$v_n(s) = \frac{e^{-ns}}{1-e^{-ns}}$$

$$\sum f(n) \frac{x^n}{1-x^n}$$ série de Lambert

$$F(x) = \sum_{n \geq 1} f(n) \sum_{m \geq 1} x^{mn} =$$

$$= \sum_{D \geq 1} \left( \sum_{d \mid D} f(d) \right) x^D$$

$$F(x) = \sum b(n) x^n$$

$\Leftrightarrow$

$$F(x) = \sum_{n \geq 1} f(n) \frac{x^n}{1-x^n}$$

$$= \sum_{n \geq 1} f(n) \sum_{N \geq 1} x^{nN}$$

$$= \sum_{D \geq 1} \left( \sum_{n \mid D} f(n) \right) x^D = \sum_{D \geq 1} F(D)\, x^D$$

**Teorema** Sea $L_f(s) = \sum \frac{f(n)}{n^s}$ $L_g(s) = \sum \frac{g(n)}{n^s}$

$$F(x) = \sum_{D \geq 1} g(D)\, x^D$$

si y solo si

$$L_f(s)\, \zeta(s) = L_g(s)$$

Como $\frac{1}{\zeta(s)} \cdot \zeta(s) = 1$

$\zeta(s)$

$\zeta(s-1) \cdot \zeta(s)$

$$\sum \mu(n) \frac{x^n}{1-x^n} = x$$

$$\zeta(s) \cdot \zeta(s) = \sum \frac{d(n)}{n^s}$$

$$\boxed{\sum \frac{x^n}{1-x^n} = \sum d(n)\, x^n}$$

Dejamos las funciones generadoras y vamos a volver al estudio de las funciones aritméticas

$d(p) = 2$ $\quad$ $\lim d(n) = 2$

$d(2^n) = n+1$ $\quad$ $\lim d(n) = \infty$

$d(n) >$ hay infinitos veces

Aunque irregularidad sin embargo se conoce que la media es una medida de regularización de G funciones esto va a ser el caso de las aritméticas

Buscamos fórmulas ~~que puedan~~ con las que estimar $\sum_{n \le x} f(n)$

Notación $f$ una función cualquiera y $g$ una función positiva $n \to \infty$ o $x \to a$

$f = O(g)$ si $|f| \le C g$ para $n \gg 0$ $|x-a| < \delta$

$f = o(g)$ si $\frac{f}{g} \to 0$

$f \sim g$ $\quad \frac{f}{g} \to 1$

$f > g$ $\quad \frac{f}{g} \to \infty$

$f < g$

$f \asymp g$ $\quad c g \le |f| \le C g$

& usar cosas como $O(1)+O(1)=O(1)$

$$\sum_{i=1}^{n} O(1) = O(n)$$

Si: $P(x) = o(x)$ casi todos los números no

pueden $P$ $\frac{P(x)}{x} \to 0$

Teorema

$$A(x) = \sum_{n \le x} a(n)$$

$f \in C^1[1,\infty)$

$$\sum_{n \le x} a(n) f(n) = A(x) f(x) - \int_1^x A(t) f'(t)\, dt$$

Prop

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

$$1 + \int_1^x [t] \frac{1}{t^2}\, dt = 1 + \log x - \int_1^x \frac{1}{t^2}\, dt$$

$$c + \log x + O\left(\frac{1}{x}\right)$$

Teorema integración por partes

$$\int u\, dv = uv - \int v\, du$$

Vamos completando la suma en una tabla

Si $F(n) = \sum_{d|n} f(d)$ fácil

$$\sum_{n\le x} F(n) = \sum_{n\le x} \left[\frac{x}{n}\right] f(n)$$

fácil

y completamos a variable real

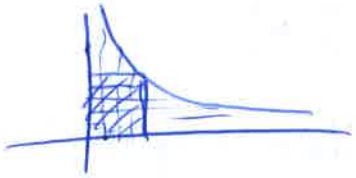
Segundo $d(n) = \sum_{d|n} 1 \Rightarrow \sum_{n\le x} d(n) = x \sum_{n\le x} \frac{1}{n} + O(x)$

Segundo lema $\sum_{n\le x} f(n)\, a(n)$ discreta de integral

Abel es integrar por partes

Prop $\sum \frac{1}{n} = \ln x + \gamma + O\left(\frac{1}{x}\right)$

se hace mejor



$u^2 = \cancel{x}$

$[\sqrt{x}]$

$$\sum_{i=1}^{u} r_i = \#\{(a,b) \; ab \le x\} =$$

$$\sum_{i=1}^{u} \left[\frac{x}{i}\right] + \sum_{i=1}^{u} \left[\frac{x}{i}\right] - u^2$$

Si nos interesa sólo acotar una suma con decrec.

$$\sum_{N+1}^{M} < \int_N^M f(t)\,dt < \sum_{N}^{M-1}$$

Este método es muy útil cualquiera que sea el problema del retículo

$$\Gamma(n) = \{ a^2 + b^2 = n \}$$

de modo es muy irregular sin embargo

$$\sum_{n \le X} \Gamma(n) = \text{Área}\left(\sqrt{X} + \sqrt{\ }\right)$$

No sólo nos permite resolver problemas geométricos, sino también ~~medir la densidad~~ de los estamos preguntando por la densidad de los números con cierta característica

$$\sum_{n \le N} f(n)$$ f(n) cuánto vale en n

Luego $\sum_{n \le N}$ f(n) cuánto vale hasta N

problema hecho en (1775)

$$\prod_p \left(1 - \frac{1}{p}\right)^2 \qquad \prod_p \left(1 - \frac{1}{p^2}\right)^2 = \frac{6}{\pi^2}$$

$$\left(\frac{1}{2}\right)^2$$

$$\sum_{n \le X} n \sum_{d \mid n} \frac{\mu(d)}{d} = \sum_{n \le X} \mu(n) \sum_{n \le \frac{X}{n}} n$$

$$= \frac{1}{2} \sum_{n \le X} \mu(n) \left( \left[\frac{X}{n}\right]^2 + \left[\frac{X}{n}\right] \right)$$

$$\frac{1}{2}\sum_{n\le x}\mu(n)\frac{x^2}{n^2}+\frac{1}{2}\sum_{n\le x}\mu(n)\left(\left\{\frac{x}{n}\right\}^2+\left\{\frac{x}{n}\right\}\right)$$

(2T)

$$+\frac{1}{2}\sum_{n\le x}\mu(n)\left\{\frac{x}{n}\right\}^2+\frac{1}{2}\sum_{n\le x}\mu(n)\frac{x}{n}\left\{\frac{x}{n}\right\}+$$

## Congruencias:

Anotaciones previo a cualquier problema aritmético

algoritmo de división $a=bq+r \quad 0\le r\le m-1$

divide en $m-1$ clases distintas así como

pares e impares

Def: $a\equiv r \pmod m$ si $m\mid a-r$

$a\ \overline{r}=\{a : a\equiv r(m)\}$

$\{0,-,m-1\}$

$r_1,-,r_{m1}$ es un sistema completo de residuos $\pmod m$ debajo $m-1$

~~Teorema: $f(x)\equiv f(a) \pmod m$~~

~~Corolario~~

Este conjunto hereda la operación de suma y producto Teor: $f(x)\equiv f(a) \pmod m$

$\mathbb{Z}/m\mathbb{Z}$ es un grupo anillo

$\mathbb{Z}/p\mathbb{Z}$ es un cuerpo

Por t … e e … $(y)$ … $y^2$. Teniend … cuent …

$$= \int_{-} \; = 1,$$

ol…

$$\sum_{n}$$

p…ra … lta… … e…

T…o…

$$= \frac{1}{\sqrt{}} \; (1/t).$$

*Dem…*

P… …e l … …) … cumple $\hat{g}_t(\nu) =$ $t^{-1/2}$ … l… … … de Poisso… … d… el …

*N…t…* … válid… para … > 0, s… …ra cualquier … en el se… …ció… …lid… …ide…ales.

**Fun…**

… …o… … conocidas como fu… …p… … … … este… el … … a … … tam… f… … … fun… p… … gene…lo p… … …ros complej… ne… … tal … … … … Observemos … A … … … … era $w_1', w_2'$ tales que …

$$=$$

p… … …

**I**… … … … … …nio $f$ … …

*D…*

resolver una ecuación en congruencias, es resolver una ec. diofántica. Sin embargo la importancia de G congruencias es que se da un grupo

$x^n + y^n = z^n \quad p \mid 0 \qquad x^n + y^n - z^n \equiv 0 \ (p)$ tiene sol. es cond. necesaria $\Leftrightarrow$ un conjunto de condiciones

$4N+3$ no tiene sol.

Vamos a centrarnos en resolver ec diofánticas en aritmética modular.

Lineales: Sea $(a,m) = d$ entonces

$ax \equiv b \pmod m$ tiene sol $\Leftrightarrow d \mid b$ y

en ese caso tiene $d$ soluciones

$$ax = b + hm$$

$$x_0,\ x_0 + \frac{m}{d},\ \dots,\ x_0 + \frac{(d-1)m}{d}$$

No son congruentes

Corolario $\left| \mathbb{Z}/m\mathbb{Z}^{*} \right| = \varphi(m)$

$ax \equiv 1 \ (m)$

Si Lema: el orden de un elemento divide al orden del grupo $a^{\varphi(m)} \equiv 1 \ (m)$ de hecho si $a^d \equiv 1$

Teorema (Euler-Fermat) $a^d \equiv 1 \pmod m$ y $d$ es el orden de $a$

Aplicación $ax \equiv b \pmod m$

$$x = a^{\varphi(m)-1} b$$

distinguir primos

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

$\varphi(6) = 2$

$5^5 = -1 \not\equiv 1 \pmod 6$ no es primo

¿Hay un inverso si $a^{p-1} \not\equiv 1 \pmod p$ → p no es primo

Euler

no $a^{560} \equiv 1 \pmod{561}$ $\forall a, \gcd(a,561)=1$ y no es primo.

- pseudo primes
- Carmichael ∞

Teorema

si ahora aplicamos $\prod g = e$

Wilson

$\rightarrow (p-1)! \equiv -1 \pmod p$ / $g \neq 1$ $g^2 \neq 1$ $g \neq -1$

$x^2 - 1 \equiv 0 \pmod p$

$(x-1)(x+1)$

$x = 1 + p^2$

$x = -1 + pk$

Una ec → sistema de ecuaciones

Teo: $x_i \equiv a_i \ (m_i) \quad \exists \ 1 \pmod m$

son independientes por eso no da mas condiciones

¿ grado superior?

$x^3 - x \mod 6$ tiene 6 soluciones

Teo: Si $(m_i, m_j) = 1$ entonces sea $p(d) : P(m) \equiv 0 \ (d)$ p es multiplo

$$f(x) \equiv 0 \ (m) \iff f(x) \equiv 0 \ (m_i)$$

y tiene $\pi \nu_{m_i}$ soluciones

~~Lema~~ ~~Si $f(a) \equiv 0 \ (m)$ entonces $x-a \mid f(x)$~~

~~$f(x) = (x-a) q(x) \pmod m$~~

~~$f(x) = \sum_{i=1}^{r} a_i (x-a)^i + k \qquad k = 0$~~

$f(a_i) \equiv 0 \ (m_i) \qquad a \equiv a_i \ (m_i)$

$f(a) \equiv f(a_i)(m_i) \equiv 0 \ (m_i) \equiv 0 \ (m)$

se reduce a potencia de un primo

Si nos quedamos con $\alpha = 1$

```
-0.148 0 (p)A
0.361 0 (r)A
-0.148 0 (o)A
0.852 0 (p)A
-0.426 0 (i)A
-0.148 0 (o)A
0.500 0 (s)A
8.000 0 32 -0.074 0 (. )D
0.074 0 (D)A
-0.426 0 (i)A
0.852 0 (a)A
-0.148 0 (go)A
0.852 0 (n)A
-0.148 0 (a)A
0.574 0 (li)A
-0.500 0 (z)A
-0.426 0 (i)A
-0.148 0 (a)A
1.500 0 (c)A
-0.426 0 (i)A
9.074 0 32 -0.148 0 (\363n )D
9.426 0 32 -1.500 0 (y )D
-0.148 0 (ap)A
0.574 0 (l)A
-0.426 0 (i)A
0.500 0 (c)A
-0.148 0 (a)A
0.500 0 (c)A
-0.426 0 (i)A
-0.148 0 (o)A
0.852 0 (n)A
-0.148 0 (e)A
7.426 0 32 0.500 0 (s )D
-0.426 0 (li)A
0.852 0 (n)A
-0.148 0 (e)A
0.852 0 (a)A
-0.426 0 (l)A
-0.148 0 (e)A
0.500 0 (s)A
7.000 0 32 -0.074 0 (. )D
0.287 0 (F)A
-0.148 0 (o)A
0.361 0 (r)A
1.861 0 (m)A
-0.148 0 (a)A
7.426 0 32 0.500 0 (s )D
8.074 0 32 -0.148 0 (de )D
0.500 0 (J)A
-0.148 0 (o)A
0.361 0 (r)A
-0.148 0 (dan)A
7.000 0 32 0.926 0 (. )D
-0.361 0 (E)A
0.500 0 (s)A
-0.148 0 (pa)A
1.500 0 (c)A
-0.426 0 (i)A
-0.148 0 (o)A
7.426 0 32 0.500 0 (s )D
0.852 0 (e)A
-0.148 0 (u)A
0.500 0 (c)A
-0.426 0 (l)A
-0.074 0 (\355)A
0.852 0 (d)A
-0.148 0 (eo)A
8.426 0 32 0.500 0 (s )D
-1.500 0 (y)A
; : 0 0 4725 6800 rc 0 0 0 sco F5_83
Ji
357 3664 M
-0.148 0 (e)A
0.500 0 (s)A
-0.148 0 (pa)A
0.500 0 (c)A
-0.426 0 (i)A
-0.148 0 (o)A
1.426 0 32 0.500 0 (s )D
0.852 0 (h)A
```

Una vez tenemos resuelta una ec. sistema de ecuaciones

Teo $x_i \equiv a_i \pmod{m_i}$ $\exists$ 1 mód m

son independientes, por eso se mantiene no de más condiciones

resolver el ccn lineal. ¿Qué pasa en grado superior? (es diferente al caso global $x^3 - x \pmod 6$)

Teo si $(m_i, m_j) = 1$

$f(x) \equiv 0 \pmod{m_i} \iff f(x) \equiv 0 \pmod{m_i}$ $\forall i$

además tiene $\prod m_i$ soluciones

$f(a_i) \equiv 0 \pmod{m_i}$

$a \equiv a_i \pmod{m_i}$ $\exists$ 1.

$f(a) \equiv f(a_i) \pmod{m_i} \equiv 0$ $\forall i$

reducimos a potencias de primos

si nos restringimos a $\alpha = 1$ entonces "ITFAO/Hz"

Teo $f(x) \equiv 0 \pmod p$ tiene a lo sumo $p$ sol.

tiene $f(a) \equiv 0 \pmod p \iff (x-a) \mid f(x)$

en general si

$f(x) = g(x)\,h(x)$ y $f(\alpha) \equiv 0 \pmod p$

$\Rightarrow g \circ h \equiv 0 \pmod p$

Inducción $|x - a \equiv 0 \pmod p$ tiene $\leq A+B$

grado $\leq n-1$

$(x-a)\,|\,f(x)$

$f(x) = (x-a)\,h(x)$

$\deg h = n-1$

Aplicación $\mathbb{Z}_p$ es cuerpo

Lema $x^d - 1 \equiv 0 \pmod p$ tiene $d$ soluciones

si $d \mid p-1$

$x^{p-1} - 1 = (x^d - 1)\left(x^{de-d} + x^{de-2d} + \cdots + 1\right)$

$de = p-1$

Demo: $\nu_d$ es $x^d - 1 \equiv 0 \pmod p$

$\nu_d$ el nº de elementos de orden $d$

$$\sum_{c \mid d} \nu_c = d$$

$$\sum_{c \mid p-1} \nu_c = p-1$$

$$\nu_d = \sum_{c \mid d} \mu\left(\frac{d}{c}\right) c$$

$$\varphi(p-1) = \sum_{c \mid p-1} \mu\left(\frac{p-1}{c}\right) c$$

$\geq 1$

MS INCLUIDO HASTA Números

Corolario: Si hay una sol. $\Rightarrow c_i \equiv 0 \pmod p$

$$f(x) = (x-1)\cdots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod p$$

Wilson $\boxed{(p-1)! \equiv -1 \pmod p}$

Además es un s. y solo si

El caso de potencia general, de hecho se puede resolver de manera inductiva

Claramente $f(a) \equiv 0 \pmod{p^\alpha} \Rightarrow f(a) \equiv 0 \pmod{p^{\alpha-1}}$

Teorema

Sea $f(a) \equiv 0 \pmod{p^{\alpha-1}}$ s.

1) $f'(a) \not\equiv 0 \pmod p \Rightarrow$ $\exists$ 1 sol. $x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$

2) $f'(a) \equiv 0 \pmod p$ y $f(a) \not\equiv 0 \pmod{p^\alpha}$ no sol

$f'(a) \equiv 0 \pmod p$ y $f(a) \equiv 0 \pmod{p^\alpha}$ $p$ sol.

$$a \quad a + p^{\alpha-1} \quad \cdots \quad a + (p-1)p^{\alpha-1}$$

Ejemplo $x^3 - 2x^2 + 3x + 9 \pmod{27}$

~~$ax^2+bx+c$~~

Modulo um primo $f(x) \equiv 0 \ (p)$.

$f(x)=0$ muy difícil. Más fácil, pero muy difícil

$$ax^2+bx+c \equiv 0 \ (p) \qquad p \neq 2$$

$$\Updownarrow$$

$$(4ax)^2 + 4abx + 4ac \equiv 0 (p)$$

$$(2ax+b)^2 + 4ac - b^2 \equiv 0 (p)$$

$$\Updownarrow$$

$y = 2ax+b \qquad y^2 \equiv \Delta \ (p)$

$\Delta = b^2-4ac$

Ejemplo $x^2+x+1 \equiv 0 \ (3)$

$$y^2 \equiv 0 \ (3)$$

$y=0 \Rightarrow \quad 2x+1 \equiv 0 (3) \iff$ $\boxed{x = \text{[illegible]}}$

Si $p = 2$

$ax^2 + bx + c \equiv 0 \ (2)$ es

$x^2 \equiv c \ (2)$ Exacta

$x^2 + x + c \equiv 0 \ (2)$

$x^2 + x \equiv 0 \ (2)$ siempre luego

$x^2 + x + 1 \equiv 0 \ (2^l)$ no tiene sol $\forall\, l$

$2x + 1 \neq 0$ luego tiene la solución única 0 ~~pues $2 \neq 0 \ (4)$~~ y 1

$$\dot{a} = a - \frac{f(a)}{f'(a)} = 1 - \frac{2}{3} \ (4)$$

$$= -1 \ (4)$$

$0, -1$

$0, -1 \ \forall\, l$. pues solo tiene dos pues sobre de manera única

Hemos reducido las ecuaciones cuadráticas a entender si

$x^2 \equiv N \ (p)$ tiene solución

**Def:** Decimos que $N$ es residuo cuadrático $N \mathrel{R} p$ si tiene y si no $N \mathrel{N} p$

Es una condición binaria que nos sabe cuáles son que mejor

$$\left(\frac{N}{p}\right) = \begin{cases} 1 & N \mathrel{R} p \\ -1 & N \mathrel{N} p \\ 0 & p \mid N \end{cases}$$

Símbolo de Legendre es ~~multiplicativo~~ completamente mult

↳ Hay $\frac{p-1}{2}$ Lemc ¿Hay algún?

**Lema** $\frac{p-1}{2} \mathrel{R} p$ y $\frac{p-1}{2} \mathrel{N} p$

$-\frac{p-1}{2}, \dots, -1, 1, \dots, \frac{p-1}{2}$ son todos

$x^2 \equiv N^2 \quad x = N$
$x = -N$

y los cuadrados son $N^2$ $n = 1 \dots \frac{p-1}{2}$

Hay $X = N_0 N^2$ $\{N_0 N^2\}$ hay $\frac{p-1}{2}$ y no son cong.

Es car multiplicativo

$$\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right) = \left(\frac{n_1 n_2}{p}\right)$$

Si $n_1 RP \; n_2 RP \Rightarrow n_1 n_2 = n^2 \; RP$

$n_1 RP \; n_2 NP \Rightarrow (n_1 n_2)^2 n \; NP$

$n_1 NP \; n_2 NP \Rightarrow n_1^2 n_2^2 \; RP$

Criterio de Euler $x^2 \equiv n \; (p) \iff n^{\frac{p-1}{2}} \equiv 1 \; (p)$

$x^2 \equiv n \; (p)$ tiene $\frac{p-1}{2}$ sol. que son los cuadrados

ejercicio

Teorema $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$

$x^2 + 1 \equiv 0 \; (p)$

$\iff p \equiv 1 \; (4)$

Euler

$(p-1)! \equiv -1$

$1 \; 2 \cdots \frac{p-1}{2}$

$-2 \leq \left(\frac{-1}{p}\right) + (-1)^{\frac{p-1}{2}} \leq 2$ pX

Teorema $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

$p - \frac{p+1}{2}$

$\frac{p-1}{2}! \equiv 1 \; 2 \; 3 \cdots \frac{p-1}{2} = 1$

$2 \; 4 \cdots p-1 = 2^{\frac{p-1}{2}} \left(1 \; 2 \cdots \frac{p-1}{2}\right)!$

$(-1)(-1)^2 2 (-1)^3 3 (-1)^4 4 \cdots (-1)^{\frac{p-1}{2}} \frac{p-1}{2}$

$\frac{p-1}{2} + \cdots + 1 \quad \frac{p-1}{2} \frac{p+1}{2} = \frac{p^2-1}{8}$

Se puede extender gracias al

## Lema (Gauss)

Sea $n$ el nº de soluciones de

$kn \equiv r \pmod p$ con $r < \frac{p-1}{2}$ $\quad n = 1, \dots, \frac{p-1}{2}$ entonces

$$\left(\frac{n}{p}\right) = (-1)^m$$

$$n \cdot 2n \cdots k\tfrac{p-1}{2} = n^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)!$$

$$(-1)^m \; a_1 \cdots a_\ell \, b_1 \cdots b_m \quad (-1)^m \left(\tfrac{p-1}{2}\right)!$$

$r \neq -s$

Ejemplo

$\left(\frac{3}{7}\right)$ $\quad 3 \; 6 \; 9 \; \frac{1}{2}$ $\quad (-1)^2 = 1$

0 1 2 3 4 5 6

1 1 4 2 2 4 1

$\left(\frac{6}{73}\right)$

Es demasiado costoso nos gustaría encontrar un método (Gauss 3) = fácil

$4 ; 7 \; (9) \quad -2 \; (5)$
$1 \; (3)$

$\left(\frac{3}{\;\;}\right)$ no da/ra

¿Existe alguna relación? $x^2 \equiv 3 \pmod 7$ :
$x^2 \equiv 7 \pmod 3$

En principio no parece evidente

Se puede extender gracias al (32)

Lema (Gauss)

Sea $n$ el nº de soluciones de

$kn \equiv r \pmod p$ con $r < \frac{p-1}{2}$ $\quad n = 1, \dots, \frac{p-1}{2}$ entonces

$$\left(\frac{n}{p}\right) = (-1)^m$$

$$n \cdot 2n \cdots k\tfrac{p-1}{2} = n^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)!$$

$$(-1)^m \; a_1 \cdots a_\ell \, b_1 \cdots b_m \quad (-1)^m \left(\tfrac{p-1}{2}\right)!$$

$r \neq -s$

Ejemplo

$\left(\frac{3}{7}\right)$ $\quad 3 \; 6 \; 9 \; \frac{1}{2}$ $\quad (-1)^2 = 1$

0 1 2 3 4 5 6

1 1 4 2 2 4 1

$\left(\frac{6}{73}\right)$

Es demasiado costoso nos gustaría encontrar un método (Gauss 3) = fácil

$4 ; 7 \; (9) \quad -2 \; (5)$
$1 \; (3)$

$\left(\frac{3}{\;\;}\right)$ no da/ra

¿Existe alguna relación? $x^2 \equiv 3 \pmod 7$ :
$x^2 \equiv 7 \pmod 3$

En principio no parece evidente

3 (7) $\quad 4^2 = 3 + 13$

$\left(\frac{3}{7}\right) = -1 \qquad \left(\frac{3}{13}\right) = 1.$

$\left(\frac{7}{3}\right) = 1 \qquad \left(\frac{13}{3}\right) = 1$

Teve tan explicito nos permite concluir uno de la relación mas bonitas de los matemáticos Euler y Legendre

LRC $\quad \frac{p}{q}$

Sean $p, q$ primos impares $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$

Ejemplo $\quad -1457 = 31 \cdot 47$ . 2389 es primo

resolver $\quad x^2 \equiv -1457 \pmod{2389}$

$\left(\frac{-1457}{2389}\right) = \left(\frac{-1}{2389}\right)\left(\frac{31}{2389}\right)\left(\frac{47}{2389}\right)$

$= \left(\frac{-6}{73}\right) = \left(\frac{-1}{73}\right)\left(\frac{3}{73}\right)\left(\frac{2}{73}\right) = \left(\frac{3}{73}\right)$

$\frac{73^2-1}{8} = 72 \cdot 74$

$\left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$

Tiene solución (encontrarla?)

Ejemplo $\left(\frac{-6}{73}\right)$

¿Cual es?

$x^2 \equiv -6 \pmod{73}$

Demostración de LRC

# Demostración

$\left(\frac{q}{p}\right)$

$M = \begin{cases} kq \equiv -j \pmod{p} \\ 1 \le M \le \frac{p-1}{2} \end{cases}$

$1 \le M \le \frac{p-1}{2}$

$\frac{p-1}{2} \le r \le p-1$

$1 \le Mq - pp \le \frac{p-1}{2}$

$1 \le M \le \frac{p-1}{2}$

$1 \le p \le \frac{q-1}{2}$

$N \begin{cases} 1 \le \\ \le \frac{q-1}{2} \end{cases}$

$1 \le Xq - Yp \le \frac{q-1}{2}$

$1 \le Y \le \frac{q-1}{2}$

$1 \le X \le \frac{p-1}{2}$

$qX \equiv -j \pmod{p}$

$qX + j = Yp$

$yp \equiv -j \pmod{q}$

$1 \le yp - qx \le \frac{p-1}{2}$

$1 \le X \le \frac{p-1}{2}$

$1 \le y \le \frac{q-1}{2}$

$yp = qx$

El símbolo de Legendre tiene generalización inmediata en el símbolo de Jacobi. Sea $m$ entero positivo impar

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\cdots\left(\frac{n}{p_r}\right)$$

está relacionado con la congruencia $x^2 \equiv n \pmod m$ pero a diferencia del símbolo de Legendre no resume la información de esta. Así

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right) = (-1)(-1) = 1$$

pero $x^2 \equiv 2 \pmod{15}$ no tiene sol. pues $x^2 \equiv 2 \pmod 3$ sin embargo si $\left(\frac{a}{3}\right)\left(\frac{a}{5}\right) = -1$ no tiene sol. que haya algún $-1$

Tiene las mismas propiedades en completamente mult. en $a$ y $b$ y $b$ periodico

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} \quad ; \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} \qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{b-1}{2}\frac{a-1}{2}}$$

Lema $\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \pmod 2$ impar

$$\frac{(rs)^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \pmod 2$$

$$\frac{\prod p_i - 1}{2} \equiv \sum \frac{p_i - 1}{2} \pmod 2$$

$$\frac{\prod p_i^2 - 1}{8} \equiv \sum \frac{p_i^2 - 1}{8} \pmod 2$$

por inducción

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{p_1-1}{2}}\cdots(-1)^{\frac{p_r-1}{2}} = (-1)^{\sum \frac{p_i-1}{2}} = (-1)^{\frac{n-1}{2}}$$

Ejercicio Teo. 6.5 del HWA visto pag 67 de Rose

$$\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)$$

Ejemplo Calcular $\left(\frac{383}{443}\right)$

$$\left(\frac{383}{443}\right)=\left(\frac{443}{383}\right)(-1)^{\frac{443-1}{2}\cdot\frac{383-1}{2}}=\left(\frac{60}{383}\right)=\left(\frac{383}{60}\right)$$

$$=-\left(\frac{4}{383}\right)\left(\frac{15}{383}\right)=-\left(\frac{15}{383}\right)=+\left(\frac{383}{15}\right)=\left(\frac{83}{15}\right)=\left(\frac{-7}{15}\right)=\left(\frac{8}{15}\right)=\left(\frac{2}{15}\right)$$

$$=(-1)\left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right)=1$$

La LRC fue una aplicación de E-F. De hecho detrás de la estructura del grupo

$\mathbb{Z}/p\mathbb{Z}^*$ es cíclico.

$x^d-1\equiv 0(p)$ $\psi(d)$ nº de veces de orden exactamente

Si $x$ tiene orden $c$ y $c|d$ entonces

$$x^d-1\equiv 0(p)$$

$$d=\sum_{c|d}\psi(c)$$

$$\psi(d)=\sum_{c|d}\mu(c)\frac{d}{c}=\phi(d) \quad \text{en general}$$

$$\psi(p-1)>1$$

A cada generador le llamamos raíz primitiva

**Def.** Si $g$ es tal que $\operatorname{ord} g = p-1$ se dice que "$g$ es una raíz primitiva módulo $p$.

~~No es cierto~~ se puede extender al caso compuesto

Se dice que $g$ es raíz primitiva módulo $m$ si

$$\operatorname{ord} g = \phi(m).$$

Lo clave característico de los grupos cíclicos es por tanto que podemos dar un sistema completo de restos

$$1, g, g^2, \dots g^{\phi(m)}$$

Si $g^i \equiv g^j \Rightarrow g^{i-j} \equiv 1 \pmod m$ no puede ser

Sea $g$ un generador de $\mathbb{Z}/m\mathbb{Z}^*$

**Def.** Llamamos índice de $a$ en el a $g$ si $g^a \equiv a \pmod m$

Índice es como el logaritmo discreto pero aditivo

Aplicación $x^N \equiv a \pmod p \iff (N, p-1) = d \mid \operatorname{Ind} a$

y en ese caso tiene $d$ soluciones

$$g^{gN} \equiv g^a \pmod p \iff Ny \equiv a \pmod{p-1}$$

por la vista

$y_0, y_0 + \frac{p-1}{d}, \dots y_0 + (d-1)\frac{p-1}{d}$

Ejemplo las soluciones son cuyo $d$ de $g^d, g^{2d}, \dots g^{\frac{p-1}{d}d}$

observación es calcular la raiz primitiva. pero Indice no es única

Cambio de base $\quad \text{Ind}_g u = (\text{Ind}_{g_1} g)(\text{Ind}_{g_1} u) \ (p-1)$

$u = g^a = g_1^{ba} \qquad (\text{Ind}_{g_1} g)(\text{Ind}_g u) \equiv \text{Ind}_{g_1}(u) \ (p-1)$

Incluso se pueden calcular soluciones. Supongamos que sabemos 3 raiz (17) y formamos la tabla

1 3 9 10 13 5 15 11 16 14 8 7 4 12 2 6 1

Calcular $x^3 + 6 \equiv 0 \ (17) \qquad (3,16) = 1$ una sol.

$3(\text{Ind } x) \equiv (\text{Ind } 11) \pmod{16}$

$3 \text{ Ind } x \equiv 7 \ (16)$

$\text{Ind } x \equiv 77 \ (16) = 13 \ (16)$

$\boxed{x = 12}$

Pasa por calcular una raiz primitiva, y despues una tabla.

¿Cuando se puede calcular una raiz primitiva?

ejemplo $\mathbb{Z}/8\mathbb{Z}$ $\qquad x^2 = 1$ $\qquad \varphi(8) = 4$

no tiene raices primitivas.

**Teorema** $\mathbb{Z}/m\mathbb{Z}^*$ es cíclico $\Leftrightarrow m = 2p^\alpha, p^\alpha, 4, 1, 2$

si tiene orden máximo $g^{\varphi(m)} \equiv 1 \ (p^\alpha)$

$m = 2^c p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $\quad \varphi(m) = 2^{c-1} \varphi(2^c)\varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$

$= 2^{c-1} p_1^{\alpha_1 - 1}(p_1 - 1) p_r^{\alpha_r - 1}(p_r - 1)$

**Lema 1** Si $\varphi(p_i^{\alpha_i}) \mid d \Rightarrow g^d \equiv 1 \ (m)$

$g^d \equiv 1 \ (\varphi(p_i^{\alpha_i})) \Leftarrow g^{\varphi(p_i^{\alpha_i})} \equiv 1 \ (p_i^{\alpha_i})$

T.Ch.r. $\quad g^d \equiv 1 \ (m)$.

**Corolario:** Si es cíclico $\varphi(m) = M = [\ , \ ]$ que $\varphi(p_i^{\alpha_i}) \mid M$

~~Demostración~~

~~Lema~~ cíclico $\Rightarrow m = 2^c p_1^{\alpha_1} \cdots$

~~Demostración~~: **Lema 2** Si $m \neq 2p^\alpha, p^\alpha, 2^c \Rightarrow M \mid \varphi(m)$

$m = 2^c p^\alpha q^\beta \Rightarrow \quad \varphi(p_i^{\alpha_i}) \mid \frac{\varphi(m)}{2} \quad \varphi(q^\beta) \mid \frac{\varphi(m)}{2} \quad \varphi(2^c) \mid \frac{\varphi(m)}{2}$

$\frac{\varphi(m)}{2} = \frac{1}{2} 2^{c-1} p^{\alpha-1}(p-1) q^{\beta-1}(q-1)$

~~$m = 2^c p_1^{\alpha_1} \cdots p_r^{\alpha_r}$~~ si $c \geq 2$ & hace igual

$m = 2^c p^\alpha \Rightarrow \varphi(m)$

**Demostración teorema**

Caso $m = p^\alpha$

**Lema 3** $(1+kp)^{p^\alpha} \equiv 1 + kp^{\alpha+1} \ (p^{\alpha+2})$

$$(1+kp)^p = \sum_{j=0}^{p} \binom{p}{j} (kp)^j = 1 + kp^2 + \frac{p(p-1)}{2} k^2 p^3$$

$$(1+kp)^{p^\alpha} = \left((1+kp)^{p^{\alpha-1}}\right)^p = \left(1 + kp^\alpha + sp^{\alpha+1}\right)^p$$

$$= 1 + \left(kp^{\alpha-1} + sp^\alpha\right) p^2 + \frac{p(p-1)}{2}\left(kp^{\alpha-1} + sp^\alpha\right)^2 p^3$$

$$= 1 + kp^{\alpha+1} \ (p^{\alpha+2})$$

**Lema 4** Si $g$ r.p $(p^2) \Rightarrow g$ r.p $(p)$

Sea $g^d \equiv 1 \ (p) \Rightarrow g^d = 1 + kp$

$$g^{d(p^{\alpha-1})} = (1+kp)^{p^{\alpha-1}} = 1 + kp^\alpha \ (p^{\alpha+1}) = 1 \ (p^\alpha)$$

**Lema** Debo buscar $g+kp$ de hecho vale con $k=0$ o $1$

**Lema 5** $g$ r.p $(p)$ sea $r = \begin{cases} g & g^{p-1} \not\equiv 1 \ (p^2) \\ g+p & g^{p-1} \equiv 1 \ p^2 \end{cases}$ r r.p $(p^\alpha)$ $\forall \alpha \geq 1$

**Ejercicio** basta probar que $r^{(p-1)p^{\alpha-2}} \not\equiv 1 \ (p^\alpha)$

$r^{p-1} - 1 = kp$ donde $p \nmid k$

$$(g+p)^{p-1} - 1 = \sum_{j=0}^{p-1} \binom{p-1}{j} g^{p-1-j} p^j - 1 = g^{p-1} - 1 + (p-1) g^{p-2} p + p^2 \ldots$$

$$\equiv -g^{p-2} p \ (p^2)$$

$(1+Np)^{p^{\alpha-1}} = 1 + Kp^{\alpha-1}(p^\alpha)$ ⊠

Caso $m = 2p^\alpha$ $\quad \varphi(2p^\alpha) = \varphi(p^\alpha)$

Si $g^d \equiv 1 (2p^\alpha) \Rightarrow g^d \equiv 1 (p^\alpha)$

g es impar ⊠ g es par $\notin \mathbb{Z}/m\mathbb{Z}$ pero $g+p^\alpha$ si ⊠

Caso $m = 2^c$ $\quad c=1$ y $2$ trivial

Lema 6 $a^{2^{c-2}} \equiv 1 (2^c)$ Inducción

Sin embargo es casi cíclico

Proposición Lema ⊠ $5^{2^{c-2}} \equiv 1 + 2^c (2^{c+1})$ $\quad c \geq 3$

no tenemos mas que multiplicar por un elemento de orden 2 para obtener todas las clases

Lema $\pm 5^b$ es un conjunto completo de residuos

si $a, b, c \leq 2^{c-2}$

$5^b \not\equiv -5^c (2^c)$ $\quad -5^b (5^{b-c} + 1) \equiv 0 (2^c)$

$\equiv 2 (4)$

De hecho $a \equiv (-1)^{\varepsilon} 5^b (2^c)$ para algún $\varepsilon$

Se puede generalizar ~~de forma que~~ a todo un multiplicando elemento de orden máximo

**Teorema:** Sea $m = 2^{\ell} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $(a,m)=1$

existen $a_0, b_0, a_1, \dots a_r$ tal que

entonces $a \equiv g_0^{a_0} \tilde{g}_0^{b_0} g_1^{a_1} \cdots g_r^{a_r} \ (m)$

donde $g_i$ son fijos

$g_0 = \tilde{g}_0 = 1$ si $\ell = 0$ ó $1$

$g_0 = 1 \quad \tilde{g}_0 = -1$ si $\ell = 2$

$g_0 = -1 \quad \tilde{g}_0 = 5$ si $\ell \geq 3$

$2 \leq g_i \leq p_i^{\alpha_i - 1}$ para $1 \leq i \leq r$

~~$a \leq \varphi(p_i^{\alpha_i})$~~

$(m_1, m_2) = 1$

Demost: Sean $a_1 \cdots a_{\varphi(m_1)}$ S.C.R mod. $m_1$

$b_1 \cdots b_{\varphi(m_2)}$ S.C.R mod $m_2$

$A_i \equiv a_i \ (m_1) \quad A_i \equiv 1 \ (m_2)$

$B_i \equiv b_i \ (m_2) \quad B_i \equiv 1 \ (m_1)$

entonces $A_i B_j$ lo es de $m$.

$A_i B_j \equiv A_s B_t \ (m) \Rightarrow$ 

$A_i B_j \equiv A_s B_t \ (m_1) \Rightarrow A_i \equiv A_s \ (m_1)$

$A_i B_j \equiv A_s B_t \ (m_2) \quad B_i \equiv B_s \ (m_2)$

2) Se deduce del teorema anterior $G \equiv g \ (p_i^{\alpha_i})$

$G \equiv 1 \ (\beta_j^{\alpha_j})$

# Distribución de los números primos

estamos en condiciones de un estudio + detallado

usar la definición. No puede tener factores
A mano encuentro los primeros hasta $z$
Quiero distinguir los primos $*$ en $[z, z^2]$

Tacho todos los multiplos de 2, 3 ... $p < z$

los que quedan son primos $\leq n < z^2$ no puede ser
$z^2 \leq ab$

eventualmente llego a cualquier lado es un teorema

¿Como aparece el método puede tener
teoría)

- Método de la criba ~~criba por~~ más general
$(q, 4) = 1 = (q, 3) = (q, p)$ $p < t$
$\{a \in \mathbb{N} : (a, P(t)) = 1\}$

$[z, z^2 - 2]$

dos columnas $n$ $n+2$

$z^2 - 1$, $z^2 - 2$

$n$ $n+2$ son primos primos gemelos

tercia de primos

& puedo entender como un único problema

$A = \{ n(n+2) \mid z < n \leq z^2 - 2$ cada uno son primos

Estimar por tanto el número de elementos que superan la criba, es dar una buena estimación de $|A_d|$

$$A = \{1 \le n \le x \mid |A_d| = \left[\frac{x}{d}\right] = x\frac{1}{d} + \theta\}$$

una aproximación continua a $\frac{x}{d}$ de forma que

$$|A_d| - \frac{x}{d} \ll 1 \quad \text{es pequeño}$$

En general buscamos $A_d = x\frac{\omega_d}{d} + r_d$

$\omega_d$ la mejor aproximación $r_d$ pequeño

Si $A$ es buena mult $\Rightarrow$ $\omega_d$ es mult. y queda

$$S(A, P(z)) = x \sum_{d \mid P(z)} \frac{\omega(d)}{d}\mu(d) + \sum_{d \mid P(z)} \mu(d) r(d)$$

término principal — pequeño

$$= x \prod_{p < z}\left(1 - \frac{\omega(p)}{p}\right) + O\left(\sum_{d \mid P(z)} r(d)\right)$$

$$S(A, P(z)) = \sum_{d \mid P(z)} \mu(d) |A_d|$$

Estimar $|A_d| = X \frac{\omega_d}{d} + r_d$

encontrar la mejor aprox. $\omega_d$ tal que $r_d$ es pequeño

$\omega_d = 1 \quad r_d = \left\{ \frac{X}{d} \right\} < 1$ pequeño.

Si en un prob. mult $\Rightarrow$ $\omega_d$ mult. en ese caso

A breve

$$\sum_{d \mid P(z)} \mu(d) |A_d| = X \sum_{d \mid P(z)} \mu(d) \frac{\omega(d)}{d} + \sum_{d \mid P(z)} \mu(d) r_d$$

$$= X \underbrace{\prod_{p < z} \left(1 - \frac{\omega(p)}{p}\right)}_{\text{grande}} + \underbrace{\sum_{d \mid P(z)} \mu(d) r_d}_{\text{pequeño.}}$$

Si $r_d \leq \omega_d$ y $\omega(p) < C$ como en el caso de Cribas

$$X \prod_{p < z} \left(1 - \frac{\omega(p)}{p}\right) + O\left(\sum_{d \mid P(z)} \omega_d\right)$$

$$X \prod_{p < z} \left(1 - \frac{\omega(p)}{p}\right) + O\left(\prod_{p < z} (1 + \omega_p)\right)$$

$$+ O\left((C+1)^z\right)$$

Cribas

Lema Teorema criba de Eratóstenes-Legendre — y si

En el caso de los primos

$$X \prod_{p < z} \left(1 - \frac{\omega(p)}{p}\right) + O(2^z)$$

no vale

pero y si $X^{1/2} > z^2 \Rightarrow$ casi primos

Si $|f(d)| \le \omega(d)$ y $\omega(3) \le C$

entonces

$$X \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right) + O\left(\sum \omega(d)\right)$$

$$O\left(\prod_{p\le z}\sum_{d|p}\omega(p)\right) + O(1+C)^z$$

exp.

Idea si $z$ es pequeño en comparación con $x$ son casi primos por ejemplo

$[z, z^3)$ quedan de dos factores en cualquier caso uno está seguro

$$\pi(x) \ge \pi(z) + S(A, P(z)) \quad \text{son los casi primos}$$

$$S(A, P(z)) > \pi(x) - \pi(z)$$

$$\pi(x) < z + S(A, P(z))$$

$$= z + X \prod_{p<z}\left(1-\frac{1}{p}\right) + O(2^z)$$

$$2^{\lg x} = e^{\lg x \left(\frac{z}{e}\right)^{\lg x}} = x \qquad \left(\frac{z}{e}\right)^{\lg x} = y \quad \lg y = \lg x$$

$$\lg y = \lg x \left(\frac{z}{e}\right)$$

$S(\mathcal{A}, P(z)) = \{ z \le n < z^3 : n \text{ primo ó } n = pq \text{ primos } p, q > z \}$



no hay muchos más y en este sentido

**Teorema:** $\pi(x) < \dfrac{x}{\lg \lg x}$

**Demo:** ~~Para $z \le x^{1/2}$~~ Para $z > 1$

$$\pi(x) \le z + S(\mathcal{A}, P(z))$$

$$\le z + x \prod_{p<z} \left(1 - \frac{1}{p}\right) + O(2^z)$$

$$\prod_{p<z} \left(1 - \frac{1}{p}\right)^{-1} > \sum_{n<z} \frac{1}{n} = \lg z + \gamma + O\left(\frac{1}{z}\right)$$

luego $$\ll z + \frac{x}{\lg z} + O(2^z)$$

$z = \lg x$ □

**Teorema** $\pi_2(x) = \#\{ n \le x : n, n+2 \text{ primos} \}$

$$\pi_2(x) \ll \frac{x}{\lg^2 \lg x}$$

Tenemos que encontrar $W_d$ ~~y comprobar~~

Sea $A = \{ n(n+2) : 1 \le n \le x \}$

$$\pi_2(x) < z + S(A, P(z))$$

$$= z + \#A_d R = \{ d \mid n(n+2) \}$$

$F(n) = n(n+2)$ !

Sea $\rho(d) : \#\{ n(n+2) \equiv 0 \pmod d \}$ es multiplicativa

~~Además~~ Sean $n_1, \dots, n_N$ sol.

en tanto $F(n) \equiv 0 \pmod d \iff n \equiv n_i \pmod d$


habrá N soluciones

tal que $nd \le x$ $\quad n \le \frac{x}{d}$

luego $|A_d| = \rho(d) \left[ \frac{x}{d} \right] = \# x \frac{\rho(d)}{d} + \theta \rho(d)$

$\rho(d)$ mult. $r_d < \rho d$ y ~~es~~ Además

$\rho(p) \le 2$ en este caso $\rho(p) = 2$ por Lagrange

luego por el teorema $\pi_2(x) < z + x \prod_{p < z} \left(1 - \frac{2}{z}\right) + O(3^z)$

$$\prod\left(1-\frac{2}{p}\right) < \prod\left(1-\frac{1}{p}\right)^2 = \prod\left(1+\frac{1}{p^2}-\frac{2}{p}\right)$$

luego $\pi_2(x) < 2 + \dfrac{x}{\lg^2 x} + O(3^{\frac{x}{2}})$

$$3^{\frac{x}{2}} = \frac{x}{\lg^2 x} \qquad x = \frac{1}{2}\lg x$$

$$\ll \frac{x}{\lg^2(\lg x)}$$

$$\lg^2\left(\tfrac{1}{2}\lg x\right) = \left(\lg 2 \lg x + \lg^2 2\right)^2 \geq \left(\lg 2 \lg x\right)^2 = \lg^2 2 \lg^2 x$$

A pesar de obtener resultados no triviales, todavía estan lejos de ser optimos. ~~Observar que solo utilizamos la definicion~~ solo cojo $x$ como $\lg x$ arbitrario cojiendo mucho con primos

Solo hemos usado la definicion lo que no hemos echo es entender la relacion entre los primos y los naturales 1850 Tchebychev dio una relacion que sera el primer paso hacia el correcto orden de magnitud

Considerando todos los enteros es como un especie de medio más facil de entender.

Sea $M = [1, \dots, n]$ el mcm o multiplo comun mas pequeño

Supongamos que hay $r$ primos hasta $n$. Entonces

$M = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ $\alpha_i$ maximo exponente

tal que $p_i^{\alpha_i} \mid j$ $(i \leq) \leq n$ luego en particular $p_i^{\alpha_i} < n$ es decir

$M \leq n^r$ luego

$\log M \leq r \log n \; \pi(n)$

La funcion $M = \prod_{p < n} p^{\left[\frac{\log n}{\log p}\right]}$

Def: $\psi(x) = \sum_{p < x} \left[\frac{\log x}{\log p}\right] \log p$

se puede expresar como suma sobre los enteros

Sean $\psi(x) = \sum_{n \le x} \Lambda(n)$

$\Lambda(n) = \begin{cases} \log p & n = p^\alpha \\ 0 & \text{resto} \end{cases}$ Von Mangoldt

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

$\Lambda(n) = \log p$ si $n = p, p^2, \dots p^m$ un vez

Así que ~~que resulta~~ estimar $\psi(x)$ sea como estimar $\pi(x)$. En vez de $\psi(x)$ se puede considerar

$$\theta(x) = \sum_{p \le x} \log p$$ teniendo en cuenta

que $\sum \frac{1}{p^2}$ es convergente y que hay pocos cuyo suma

es $p^2$ y demás

$$\theta(x^{1/2}\log^2 x) + \theta(x) = \psi(x)$$

**Teorema**

$$\theta(x) = \pi(x)\lg x + O\left(\frac{x}{\lg\lg x}\right)$$

Demostración

$\theta(x) < \lg x\, \pi(x)$ trivialmente.

por otra parte

$$\theta(x) = \sum_{2\le n\le x} \lg n \cdot a_n \qquad a_n = \begin{cases} 0 & n \neq p \\ \lg p & n = p \text{ primo} \end{cases}$$

Abel

$$= \lg x\, \pi(x) - \int_2^x \frac{\pi(t)}{t}\, dt$$

De $\pi(x) \ll \dfrac{x}{\lg\lg x}$ se deduce que

$$\pi(x) \le C \frac{x}{\lg\lg x} \quad \text{para todo } x > e^e$$

por tanto

~~$= \lg x\, \pi$~~

$$\theta(x) - \pi(x)\lg x = -\int_1^c \frac{\pi(t)}{t}\, dt - \int_c^x \frac{\pi(t)}{t}\, dt$$

$$\theta(x) - \pi(x)\log x > -K + \int_C^x \frac{1}{\log\log t}\,dt$$

$$f(x) = \frac{x}{\log\log x}$$

$$f'(x) = \frac{\log\log x - x\,\frac{1}{x\log x}}{(\log\log x)^2} = \frac{1}{\log\log x} - \frac{1}{\log x \log\log x}$$

por tanto

$$\int_C^x \frac{1}{\log\log t}\,dt = \frac{x}{\log\log x} + K + \int_C^x \frac{1}{\log t \log\log t}\,dt$$

$$= \frac{x}{\log\log x} + K + \int_C^{\sqrt{x}} \frac{1}{\log t \log\log t}\,dt + \int_{\sqrt{x}}^x \frac{1}{\log t(\log\log t)}\,dt$$

$$\ll \frac{x}{\log\log x} + \sqrt{x} + \frac{2x}{\log x}$$

$$\ll \frac{x}{\log\log x}$$

es decir $I \le K \dfrac{x}{\log\log x} \quad \forall\, x \ge C'$

luego $\theta(x) - \pi(x)\log x \ge -K\dfrac{x}{\log\log x}$

Teorema (Chebychev) ~~existen dos~~ constantes tal que $x \geq 2$

$$B_1 x < \theta(x) < A_1 x$$
$$B_2 x \leq \psi(x) < A_2 x$$

$$\theta(x) \asymp x$$
$$\psi(x) \asymp x$$

Basta probar ~~$\theta(x) < C_1 x$~~

$$\psi(x) > C_2 x$$

Lema: $\theta(x) < 2^{\lg 2} x \quad x \geq 2$

Sea $M = \binom{2m+1}{m+1}$ es el número que va a relacionar los primos con los naturales

$$\prod_{m < p \leq 2m+1} p \leq M$$

Luego $$\sum_{m+1 < p \leq 2m+1} \lg p \leq \lg M$$

ahora bien $\binom{2m+1}{m}$

$$2^{2m+1} = \sum_{j=0}^{2m+1} \binom{2m+1}{j}$$

$$= 2\binom{2m+1}{m} + 2\sum_{j=0}^{m-1} \binom{2m+1}{j}$$

$$> 2\binom{2m+1}{m}$$

$2 \lg_2 m$

$\theta(2m+1) \leq \theta(m+1) + 2\lg_2 m < 2\lg_2 m = 4\lg_2 m$

$\theta(2m) = \theta(2m-1)$ ☒

$M = \binom{2m}{m}$ A pese de Lagrange en 6 cuenta de Legendre

Lema:

$$n! = \prod_{p \leq n} p^{e(n,p)}$$

$$e(n,p) = \sum_{p^m \leq n} \left[\frac{n}{p^m}\right]$$

Demo: $p \quad 2p \cdots (p-1)p \quad p^2 \quad 2p^2 \cdots (p-1)p^m$

$\left[\frac{n}{p^m}\right]$ cuenta los multiplos de $p^m \leq n$

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots$$

Teo $\psi(x) > \frac{\lg 2}{2} x \quad x \geq 2$

$$N = \binom{2n}{n} = \frac{2n!}{n!^2}$$

~~$\lg N =$~~

$$\prod_p p^{N_p} \qquad N_p = \sum_{m \geq 1} \left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]$$

Claramente $[2x] - 2[x] = \begin{cases} 0 \\ 1 \end{cases}$

$$m < \left[\frac{\lg 2n}{\lg p}\right]$$

Si $x = [x] + \theta$

$$2x = 2[x] + 2\theta$$

$$[2x] = \begin{cases} 2[x] & 0 \leq \theta < \frac{1}{2} \\ 2[x]+1 & \frac{1}{2} < \theta < 1 \end{cases}$$

$$\lg 2\binom{2n}{n} \lg N \leq \sum_{p \leq 2n} \left[\frac{\lg 2n}{\lg p}\right] \lg p = \psi(2n)$$

$2n\ 2n-1 \cdots 1$

$n\ n-1 \cdots 1\ n-1 \cdots$

$$\psi(2n+1) \geq \psi(2n) > (n+1)\lg 2 > \frac{(2n+2)}{2}\lg 2$$

$$> \frac{2n+1}{2}\lg 2$$

Del teorema anterior deducimos

Corolario $\pi(x) \simeq \dfrac{x}{\log x}$

| $\limsup$ 1'0423 |
|---|
| $\liminf$ 0'96695 |

$$c > \frac{\theta(x)}{x} > \frac{\pi(x)}{x/\log x} + \frac{\log\log x}{\log\log x}$$

$$> \frac{\pi(x)}{x/\log x} - \varepsilon$$

Corolario ~~Bertrand~~

Corolario: Existe $c$ tal que en el intervalo $(x, cx)$ hay un primo

~~$\theta(cx) \Rightarrow Kcx$~~

$$\theta(cx) - \theta(x) > N_1 c_1 x - N_2 x = (N_1 c - N_2)\, x$$

$$c > \frac{N_2}{N_1} \quad \square \quad 2\log 2 \quad \frac{\log 2}{2} \quad 4.$$

Teorema: (Postulado de Bertrand) [$n \geq 1$]

existe un primo

$$\sum_{p^m \leq 2n} \left[\frac{\log 2n}{\log p}\right] - 2\left[\frac{\log n}{\log p}\right]$$

$\in M f \approx s o \in f e 2 \blacktriangleright \int \Pi \ddot{\imath} \# 100 \dashv p \# (1 \ddot{u} \circledcirc 8 o \eta \ddot{o} \dashv p \#) \ddot{A} \ddot{A} \ddot{A} \ddot{A} \ddot{A} \ddot{A} æ S Z \acute{e} \eta \; \S \dot{\imath} \dot{\imath} \dot{\imath} f \cdot < \$ \dot{\imath} æ$

$$\binom{2n}{n} = \prod_{p \le 2n} p^{w(p)} =$$

Si $w_p \ge 2$

$$\left[ \sum \right]$$

$$2 \le w_p \le \left[ \frac{\lg 2n}{\lg p} \right] < \frac{\lg 2n}{\lg p} \qquad p \le \sqrt{2n}$$

$$\le \prod_{p \le \sqrt{2n}} p^{w_p} \prod_{\sqrt{2n} < p < \frac{2}{3}n} p^{w_p}$$

$$\lg \binom{2n}{n} < \sum_{p \le \sqrt{2n}} \left[ \frac{\lg 2n}{\lg p} \right] \lg p + \sum_{\sqrt{2n} < p < \frac{2}{3}n} \lg p$$

$$2n \lg 2 - \lg(2n) < \lg(2n)\sqrt{2n} + \frac{2}{3} n \lg 2$$

$$\frac{2}{3} \lg 2n < \lg 2n(\sqrt{2n}+1)$$ no es cierto

$$n > 467$$

para $n \le 467$ se prueba a mano ∎

Hemos probado $A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x}$

todavía lejos de la conjetura de Gauss-Legendre

$$\pi(x) \sim \frac{x}{\log x}$$

En primer lugar porque $(A-B)\frac{x}{\log x}$ es grande

y porque no existe $\lim \pi(x)/x/\log x$

por métodos parecidos Sylvester obtuvo

$$\overline{\lim}\ \pi(x) < 1'0423$$

$$\underline{\lim}\ \pi(x) > 0'96695$$

Observar que $2\log 2 = 1'386294$

$$\log 2^{2x}/2 = 0'34657$$

Hacen falta métodos completamente distintos para probar el teorema

Probar $\pi(x) \sim \frac{x}{\lg x}$ es

$$\sum_{p \le x} 1 = \frac{x}{\lg x} + o\left(\frac{x}{\lg x}\right)$$

**Lema** $f(x) \sim g(x) \iff f(x) = g(x) + o(g(x))$

cuenta el desarrollo asintótico de una suma.

Si fuéramos capaces de calcular

$A(x) = \sum_{p \le x} f(p)$, entonces por Abel

$$\sum_{p \le x} 1 = \sum \frac{1}{f(p)} f(p) = f(x) A(x) - \int_1^x A(t) f'(t)\, dt$$

podríamos aspirar a demostrar el teorema

## Fórmula de Mertens

$$\sum_{p \le x} \frac{\lg p}{p} = \lg x + O(1)$$

$$\sum_{p \le x} \frac{1}{p} = \lg\lg x + B + O\left(\frac{1}{\lg x}\right)$$

Demostración:

$$\lg m! = \sum_{p \le m} e(m,p) \lg p$$

$$= \sum_{p \le m} \left( \sum_{p^w \le m} \left[ \frac{m}{p^w} \right] \right) \lg p$$

$$= \sum_{p \le m} \left[ \frac{m}{p} \right] \lg p + \sum_{p \le m} \sum_{2 \le k \le \left[ \frac{\lg m}{\lg p} \right]} \left[ \frac{m}{p^k} \right] \lg p$$

$$m \sum_{p \le m} \frac{\lg p}{p} \sum_{2 \le w} \frac{1}{p^w} = m \sum_{p \le m} \frac{\lg p}{p(p-1)} \le m \sum_{p \le m}$$

$$\le m \sum_{p \le q} \frac{\lg p}{p(p-1)} + m \sum_{q < p} \frac{\lg p}{p(p-1)}$$

$$\le m K_1 + m \sum_{q < p} \frac{1}{p^{3/2}} = K m$$

$$= m \sum_{p \le m} \frac{\lg p}{p} + \sum_{p \le m} \lg p + O(m)$$

$$= m \sum_{p \le m} \frac{\lg p}{p} + O(m)$$

por otro lado

$$\sum_{j=1}^{m} \lg j = \lg m! = m \lg m - \int_1^m \frac{[t]}{t}\, dt$$

$$= m \lg m - m + O(\lg m) = m \lg m + O(m)$$

dividiendo por $m$

$$\sum_{p \le x} \frac{\lg p}{p} = \sum_{p \le m} \frac{\lg p}{p} = \lg m + O(1) = \lg x + r(x)$$

$$\sum_{2 \le p \le x} \frac{1}{p} = \sum_{2 \le p \le x} \frac{\lg p}{p} \frac{1}{\lg p} = \frac{1}{\lg x} \sum_{2 \le p \le x} \frac{\lg p}{p}$$

$$+ \int_2^x \frac{\sum_{p \le t} \frac{\lg p}{p}}{t \lg^2 t}\, dt =$$

$$= 1 + O\left(\frac{1}{\lg x}\right) + \int_2^x \frac{1}{t \lg t}\, dt + \int_2^x \frac{r(t)}{t \lg^2 t}\, dt$$

$$= 1 + O\left(\frac{1}{\lg x}\right) + \lg\lg x - \lg\lg 2 + \int_2^\infty \frac{r(t)}{t \lg^2 t}\, dt$$

$$+ \int_x^\infty \frac{r(t)}{t \lg^2 t}\, dt$$

$$= \lg\lg x + B + O\left(\frac{1}{\lg x}\right) \quad \blacksquare$$

Sin embargo no pasamos a el teorema del número primo

$$\sum 1 = \sum \frac{1}{p} p = x \lg\lg x \quad \text{muy grande}$$

$$\sum 1 = \sum_{\text{grande}} \frac{\lg p}{p} \frac{p}{\lg p} = \frac{x}{\lg x} \lg x \quad \text{luego el error es muy}$$

**Teorema** (del número primo) $\pi(x) \sim \frac{x}{\lg x}$.

Partimos de la identidad de Euler

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad \text{en } \mathrm{Res} > 1$$

queremos una identidad entre una función analítica y una suma

$$\lg \lg \zeta(s) = +\sum_p \sum_m \frac{1}{m p^{ms}}$$

$$= +\sum_p \sum_n \frac{1}{n} e^{-ms \lg p}$$

o tomando derivada

$$\frac{\zeta'(s)}{\zeta(s)} = +\sum_p \frac{\lg p}{p^{ms}} = -\sum_{n \geq 1} \frac{\Lambda(n)}{n^s}$$

Una ~~vez~~ suma "es" una integral a la cual es más facil aplicar el analisis

**Lema:** $$-\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(t)}{t^{s+1}}\,dt \quad \text{para } \operatorname{Re} s > 1$$

**Demostración**

$$\sum_{n\le x} \frac{\Lambda(n)}{n^s} = \frac{1}{x^s}\sum_{n\le x}\Lambda(n) + s\int_1^x \frac{\psi(t)}{t^{s+1}}\,dt$$

$\psi(x) = O(x)$ luego $\lim_{x\to\infty} \frac{\psi(x)}{x^{s+1}} = 0$

define una función analítica por convergencia dom. ~~uniforme~~. me da el ~~Teorema~~. Lema.

$-\frac{\zeta'(s)}{\zeta(s)}$

Este formula relaciona analisis complejo con aritmetica. ~~Ahora bien, cuando integre en $\psi$~~ ~~luego~~ Sin embargo no queremos calcular el desarrollo de $\psi$ sino de $\Pi$

**Lema:** $\lim_{x\to\infty} \frac{\Pi(x)}{x/\log x} = 1 \iff \lim_{x\to\infty} \frac{\psi(x)}{x} = 1$

Si existe $\lim \frac{\psi(x)}{x}$ entonces

Demostración $\frac{\psi(x)}{x} = \frac{\theta(x)}{x} + O\left(\frac{\log^2(x)}{x^{1/2}}\right)$

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = \lim_{x\to\infty} \frac{\theta(x)}{x}$$

por otra parte $\lim_{x\to\infty} \frac{\theta(x)}{x} = \lim_{x\to\infty} \frac{\pi(x)}{x/\log x}$ ⊠

Sin embargo nuestra incognita es $\psi(x)$.

Luego quisieramos encontrar esta formula.

$\int_1^\infty \psi(t)\, e^{-(s+1)\log t}\, dt$ la transformada de

Fourier luego basta con aplicar el teorema de inversión

para encontrar $\psi$ en función de $\zeta$.

Vamos a hacerlo clasicamente. ~~mecli~~

En primer lugar vamos a regularizar la función

$\psi$ para que los calculos sean más sencillos

Consideramos $\psi_1(x) = \int_1^x \psi(t)\, dt$ la media

**Lema:** Sea $f$ monotona creciente

$F(x) = \int_a^x f(t)\, dt$ tal que $F(x) \sim x^a$ $x\to\infty$ $a>0$

~~Veremos que dar entender la función~~

Es sabido que si uno sabe como se comporta la función ⇒ sabe como se comporta la medida o lo que se conoce como teoremas directos o Abelian

si $f(t) \sim a t^{a-1}$

$$F(x) = \int_0^x f(t)\,dt \Rightarrow F(x) \sim x^a$$

$$\int_0^x (f(t) - a t^{a-1})\,dt + x^a$$

$$\leq \int_0^M (f(t) - a t^{a-1})\,dt + \varepsilon (x^a - M^a)$$

$$\lim_{x \to \infty} \left| \frac{F(x) - x^a}{x^a} \right| < \varepsilon \quad \forall \varepsilon \qquad \blacksquare$$

Queremos dar un teorema inverso o tauberiano si conocemos la medida y algo más sabemos la función.

entonces $f(x) \sim a x^{a-1} \quad x \to \infty$.

Demostración:

$$\frac{F(cx) - F(x)}{x(c-1)} = \frac{1}{c-1} \int_x^{cx} f(t)\,dt \geq f(x) \geq \frac{F(x) - F(bx)}{x(1-b)}$$

$$\left(\frac{1}{c-1}\right)\left(\frac{F(cx)}{x^a} - \frac{F(x)}{x^a}\right) \geq \frac{f(x)}{x^{a-1}} \geq \left(\frac{F(x)}{x^a} - \frac{F(bx)}{x^a}\right)\left(\frac{1}{1-b}\right)$$

Si

$$\frac{c^a - 1}{c-1} \geq \overline{\lim} \frac{f(x)}{x^{a-1}} \geq \underline{\lim} \frac{f(x)}{x^{a-1}} \geq \left(\frac{1-b^a}{1-b}\right)$$

$$a \geq \overline{\lim} \frac{f(x)}{x^{a-1}} \geq \underline{\lim} \frac{f(x)}{x^{a-1}} \geq a$$

∎

Lema: $\dfrac{\psi_1(x)}{x} = \displaystyle\sum_{n \leq x} \left(1 - \frac{n}{x}\right) \Lambda(n)$ Tiene una interpretación aritmética

$$\sum_{n \leq x} n\,\Lambda(n) = x\,\psi(x) - \int_1^x \psi(t)\,dt$$

$$\Rightarrow \psi_1(x) = \sum_{n \leq x} (x - n)\,\Lambda(n)$$

**Proposición** $c>1$

$$\frac{\psi_1(x)}{x} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^s}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right) ds$$

**Lema** (Fórmula de Perron)

Para $c>0$ $y>0$ se tiene

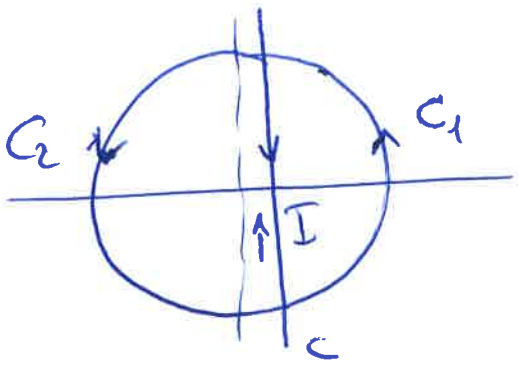
$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s(s+1)\cdots(s+N)} ds = \begin{cases} 0 & 0<y\le 1 \\ \frac{1}{N!}\left(1-\frac{1}{y}\right)^N & 1\le y \end{cases}$$

Por el teorema de los residuos

$$\frac{1}{2\pi i}\int_C f(s)\,ds = \sum_{P_i} \operatorname{Res} f(P_i)$$

$P_i$ polos interiores a $C$ camino simple cerrado

Consideramos




$$\Gamma_1 = C_1 \cup I$$

Supongamos $0 < y \leq 1$

$y^s$ es analítica en $\mathbb{C}$ no tiene polos

$$\int_{C_1} + \int_I = 0$$

$\int$ en $C_1$ $\quad |y^s| < y^c$ escogiendo $R > 2K$

$$|s+j| > |s| - j > R/2$$

$$|f(s)| < \frac{y^c}{(R/2)^N} \xrightarrow[R\to\infty]{} 0$$

Si $y \geq 1$ escojo $\Gamma_2 = I \cup C_2$

si $R > K$ entonces $\dfrac{y^s}{s(s+1)\cdots(s+N)}$ tiene

polos simples en $0, -1, \ldots -K$ el residuo es

$$\lim_{s\to -j} (s+j) f(s) = \frac{y^{-j}}{(-j)\cdots(N-j)\, j!} = \frac{(-y)^{-j}}{(N-j)!\, j!}$$

$$-j\ -j+1 \cdots -j+(j-1)\ (-j+j+1)\cdots(-j+N)$$

$$(-1)^j (N-j)!\, j!$$

Luego

$$\sum \operatorname{res} f(P_i) = \sum_{j=0}^{N} \frac{(-y)^{-j}}{j!(N-j)!} = \frac{1}{N!}\left(1-\frac{1}{y}\right)^N$$

Por otro lado en $C_2$ $R>2N$

$$\int_{C_2} |f(s)| < \frac{y^c}{(R_2)^N} \longrightarrow 0 \qquad \blacksquare$$

**Corolario** $c>1$ $x>1$

$$\frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \int_{c-i\infty}^{c+i\infty} \frac{x^{s-1}}{s(s+1)(s-1)}\,ds$$

$\blacksquare$

Observa que la función $\psi_1$ está definida como nos sirve que se corte en $x>n$ o lo que es lo mismo cuando $y=\frac{n}{x}<1$ que es justamente cuando la fórmula de Perron vale cero

Demostración

$$\frac{\psi_1(x)}{x} = \sum_{n\le x} \Delta_n\left(1-\frac{n}{x}\right) = \sum_{n\le x} \frac{\Delta(n)}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^s}{s(s+1)}\frac{1}{n^s}\,ds$$

$$\frac{1}{2\pi i}\sum_{n\ge 1}\int_{c-i\infty}^{c+i\infty} \frac{x^s}{s(s+1)}\frac{\Delta(n)}{n^s}\,ds$$

para $c>1$ $\quad \frac{x^s}{s(s+1)}\sum_{n\le T}\frac{\Delta(n)}{n^s} < \left|\frac{x^s}{s(s+1)} - \frac{\zeta'(s)}{\zeta(s)}\right| < x^c - \frac{\zeta'(c)}{\zeta(c)}\frac{1}{c+c^2}$

convergencia dominada

Contamos para $c>1$

$$\frac{\psi_1(x)}{x^2} - \frac{1}{2}\left(1-\frac{1}{x}\right)^2 = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}\right) ds$$

en para quitar el polo

Supongamos que puedo ~~quitar~~ trasladar la línea de integración a $c=1$ entonces queda

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} x^{it} h(t)\, dt \qquad h(t) = \left(-\frac{\zeta'(1+it)}{\zeta(1+it)} - \frac{1}{it}\right)$$

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} e^{it\log x} h(t)\, dt \longrightarrow 0 \quad (x\to\infty)$$

por el lema de Riemann-Lebesgue cuando

$h \in L^1(\mathbb{R})$

Tengo que probar $h \in L^1$, y que puedo pasar la línea de integración a $c=1$.

Necesito contar otro caso. Por un lado continuación analítica. Si quiero entender la función en strip. Segundo orden de magnitud que quiero que esté en $L^1$ y tercero la cero de $\zeta(s)$ no puede tener cero en $\sigma=1$. Concretamente veremos que es equivalente

- Continuación analítica

Teorema La función $\zeta(s)$ admite continuación analítica a $\sigma>0$ con un único polo simple en $s=1$ de residuo 1.

Demostración

$$F(s)=\sum_{n\geq 1}\frac{(-1)^{n+1}}{n^s}$$

para $\sigma>0$

Por el criterio de Leibnitz $F(s)$ converge para todo $s>0$.

**Proposición:** Si $F(s)$ converge para $\sigma_0$ entonces converge uniformemente en todo el semiplano $s > \sigma_0 + \varepsilon$

$$\sum_{n \le x} \frac{a_n}{n^s} = \sum_{n \le x} \frac{a_n}{n^{s-\sigma_0} n^{\sigma_0}} = \frac{1}{x^{s-\sigma_0}} \sum_{n \le x} \frac{a_n}{n^{\sigma_0}}$$

$$+ (s-\sigma_0) \int_1^x \frac{\sum_{n \le t} \frac{a_n}{n^{\sigma_0}}}{t^{s-\sigma_0+1}} dt = \frac{1}{x^{s-\sigma_0}} \sum_{n \le x} \frac{a_n}{n^{\sigma_0}}$$

$$+ (s-\sigma_0) \int_1^{\infty} \frac{\sum_{n \le t} \frac{a_n}{n^{\sigma_0}}}{t^{s-\sigma_0+1}} dt - (s-\sigma_0) \int_x^{\infty} \frac{\sum_{n \le t} \frac{a_n}{n^{\sigma_0}}}{t^{s-\sigma_0+1}} dt$$

$$F(s) + O\left(\frac{1}{x^{\varepsilon}}\right)$$

**Corolario** Si $F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$

$$G(s) = \sum_{n\geq 1} \frac{g(n)}{n^s}$$

y $F(\sigma) = G(\sigma) \Rightarrow f(n) = g(n)$

Por convergencia uniforme $\sigma \to \infty$ $f(1) = g(1)$

Supongamos que son todos $1, \dots, N-1$

$$f(N) = N^\sigma \sum_{N}^{\infty} f(n) n^{-\sigma} = N^\sigma \sum_{N}^{\infty} g(n) n^{-\sigma} = g(N)$$ ☒

para $\sigma > 1$

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \sum_{n\geq 1}$$

$$F(s) = \sum_{n\geq 1} \frac{1}{(2n)^s} - \sum_{n\geq 1} \frac{1}{(2n+1)^s}$$

$$= 2 \sum_{n\geq 1} \frac{1}{(2n)^s} - \sum_{n\geq 1} \frac{1}{n^s}$$

$$= -\left(2^{1-s} - 1\right) \zeta(s)$$ ☒

~~Por $(s-1) F(s)$~~

$$\lim_{s\to 1} \zeta(s)(s-1) = \frac{(s-1)F(s)}{(1-2^{1-s})}$$

$$F(1) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} = \lg 2$$

$$\lg(1-x) = -\sum_{n\geq 1} \frac{x^n}{n} \quad \to 1$$

por otro lado $\lim_{s\to 1} \frac{s-1}{1-2^{1-s}} = \frac{1}{\lg 2}$

**Observación** $\zeta(\sigma) < 0 \quad 0<\sigma<1$

**Corolario** $\zeta(s) + \frac{1}{s-1}$ es analítica en $s=1$

**Orden de magnitud** $\zeta(s) = \sum \frac{1}{n^s}$

$\sum_{n\leq x} \frac{1}{n^s}$ = Me interesa acotar

le hacemos en $\sigma = 1$ pero observar que cerca de 1

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \sum_{n\leq x} \frac{1}{n^s} + \sum_{n>x} \frac{1}{n^s}$$

pequeño

$\sim \lg x$ nos da una aproximación comparando con una suma finita

- $F(s) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n^s} =$

$$= \sum \frac{1}{(2n-1)^s}$$

$$F(s) = (1 - 2^{1-s})\,\zeta(s)$$

Lema $\zeta(s)$ es analítica en $\Re s > 0$ con un único polo simple en $s=1$ de Residuo 1. es decir $\zeta(s) = \frac{1}{s-1} + \sum_{n\geq 0} c_n (s-1)^n$

$$\zeta(s) = \frac{1}{(1-2^{1-s})} F(s)$$

$$\lim_{s\to 1} (s-1)\,\zeta(s) = \lim_{s\to 1} F(s) \cdot \frac{s-1}{(1-2^{1-s})} = 1$$

$$\lim_{s\to 1} \frac{2^{1-s} - 1}{1-s} = \frac{1}{\lg 2} \qquad \lim_{x\to 0} \frac{2^x - 2^0}{x}$$

Corolario: la función $\frac{\zeta'(s)}{\zeta(s)} + \frac{1}{s-1}$ es analítica en $s=1$

$$f(s) = (s-1)\,\zeta(s) \qquad f(1) \neq 0$$

$$\sum_{n\geq 0} (n+1) c_n (s-1)^n = \frac{f'(s)}{f(s)} = \frac{1}{s-1} + \frac{\zeta'(s)}{\zeta(s)}$$

**Lema:** $\zeta(s) = \sum_{n \le x} \frac{1}{n^s} + \frac{1}{(s-1)x^{s-1}} + \frac{\{x\}}{x^s} - s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt$ (68)

para $\sigma \ge 0$ $t \ge 1$, $x \ge 1$

**Corolario** $|\zeta(s)| < \sum_{n \le x} \frac{1}{n^\sigma} + \frac{1}{|s-1|x^{\sigma-1}} + \frac{1}{x^\sigma} + \frac{|s|}{\sigma}\frac{1}{x^\sigma}$ para $\sigma \ge 0$

**Demostración**

$$\sum_{n \le x} \frac{1}{n^s} = \frac{1}{x^s}[x] + s\int_1^x \frac{[t]}{t^{s+1}}dt$$

$$= \frac{1}{x^{s-1}} - \frac{\{x\}}{x^s} + s\int_1^x \frac{1}{t^s}dt - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt + s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt$$

si $\sigma > 1$

$$\zeta(s) = \frac{-s}{1-s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt$$

cont. analítica y remuevo 1

Además

$$\sum_{n \le x} \frac{1}{n^s} = \frac{1}{x^{s-1}} - \frac{\{x\}}{x^s} + \zeta(s) + \frac{s}{(1-s)x^{s-1}} + s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt$$

$$= \frac{1}{(1-s)x^{s-1}} - \frac{\{x\}}{x^s} + s\int_x^\infty \frac{\{t\}}{t^{s+1}}dt$$

Con esta comparación podemos probar

**Teorema:** 1) $|\zeta(s)| < A \lg t \quad \sigma \geq 1 \quad t \geq 1$

2) $|\zeta(s)| < A(\delta)\, t^{1-\delta} \quad 1 > \sigma > \delta \quad t \geq 1$, $0 < \delta < 1$

3) $|\zeta'(s)| < A \lg^2(t) \quad \sigma \geq 1 \quad t \geq 2$

Basta probar 1) para $\sigma \leq 2$ pues en el resto está acotada

en ese caso ~~$\sigma + |s-1| > 1$~~

$|s-1| > t \qquad |s| < t+1 \qquad |\sigma + it| = \sqrt{\sigma^2 + t^2} < (t^2+4)$

$$|\zeta(s)| < \sum_{n \leq x} \frac{1}{n^\sigma} + \frac{1}{t x^{\sigma-1}} + \left(\frac{t+2}{x^\sigma}\right)$$

$$\leq \lg x + \gamma + O\left(\frac{1}{x}\right) + \frac{1}{t x^{\sigma-1}} + \frac{t+2}{x^\sigma}$$

$x > t \qquad \ll \lg t$

2)

$$\int_0^x \frac{1}{t^\delta}\,dt + \frac{1}{t x^{\delta-1}} + \frac{1}{x^\delta} + \frac{t}{\delta x^\delta}$$

$$\frac{x^{1-\delta}}{1-\delta} + \frac{1}{t x^{\delta-1}} + \frac{1}{x^\delta} + \frac{t}{\delta x^\delta}$$

$$< x^{1-\delta}\left(\frac{1}{1-\delta} + 1\right) + \frac{2t}{\delta x^\delta}$$

$$x^{1-\delta} = \frac{t}{x^\delta} \qquad x = t$$

$$= t^{1-\delta}\left(\frac{1}{1-\delta} + 1 + \frac{2}{\delta}\right)$$

Formule de Cauchy

3) $$f'(w) = \frac{1}{2\pi i}\int_\zeta \frac{f(s)}{(s-w)^2}\,ds$$

$$\sum_{n\geq 0} a_n (s-w)^n = \frac{1}{2\pi i}\sum_{n\geq 0}\int_{\zeta'} (s-w)^{n-2}\,ds$$

$$= \frac{1}{2\pi i}\sum_{n\geq 0} a_n \int_0^{2\pi} e^{i(n-1)\theta}\,d\theta \to 0 \text{ si } n \neq 1$$

$n=1 \quad a_1 = f'(w)$

$$\zeta'(s) = \frac{1}{2\pi i}\int_C \frac{\zeta(w)}{(w-s)^2}\,dw$$

$$|\zeta'(s)| < \frac{M}{\rho} = \left(\frac{1}{\rho} + 1 + \frac{2}{1-\rho}\right)\frac{t^\rho}{\rho}$$

$$< \frac{4t^\rho}{\rho^2} \qquad f(\rho) \text{ el mínimo en } \rho = \frac{2}{\log t}$$

$$< 4\log^2 t.$$

**Teorema:** $\zeta(s) \neq 0$ en $\sigma \geq 1$ y $\frac{1}{\zeta(s)} = O(\log^7 t)$ en $\sigma = 1$ uniformemente en $\sigma \geq 1$.

$$0 \leq 2(1+\cos\theta)^2 = 2 + 2\cos^2\theta + 4\cos\theta$$

$$= 2 + 2\cos 2\theta + 4\cos\theta$$

$$3 + \cos 2\theta - \operatorname{sen}^2\theta + 4\cos\theta$$

$$= 3 + \cos 2\theta + 4\cos\theta$$

en $\sigma > 1$ se tiene

$$\zeta(\sigma+it)\sum \frac{n^{-it}}{n^\sigma} = \sum_{n\geq 1} \frac{1}{n^\sigma}\cos(t\log n) - i\operatorname{sen}(t\log n)$$

~~$\sum_{n\geq 1} \frac{\cos(t\lg n)}{n^\sigma} + i \sum_{n\geq 1} \frac{\sin(t\lg n)}{n^\sigma}$~~

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

$$\lg \zeta(s) = -\sum_p \lg\left(1 - \frac{1}{p^s}\right) =$$

$$= \sum_p \sum_m \frac{1}{m p^{ms}} = \sum_{n\geq 1} \frac{c(n)}{n^s}$$

$$= \sum_n \frac{c(n)}{n^s}$$

$$c(n) = \begin{cases} 0 & \text{si } n \neq p^m \\ \frac{1}{m} & \text{si } n = p^m \end{cases} \quad \text{reales}$$

$$= \sum_{n\geq 1} \frac{c(n)}{n^\sigma} e^{-it\lg n} = \sum_{n\geq 1} \frac{c(n)}{n^\sigma} \cos(t\lg n) + i \sum \frac{c(n)}{n^\sigma} \sin(t\lg n)$$

$$\lg|\zeta(\sigma)| = \sum \frac{c(n)}{n^\sigma} \cos(t\lg n)$$

$$3\lg|\zeta(\sigma)| + 4\lg|\zeta(\sigma+it)| + \lg|\zeta(\sigma+2it)| =$$

$$= \sum \frac{c_n}{n^\sigma} (3 + 4\cos(t\lg n) + \cos(2t\lg n))$$

$$\geq 0$$

es decir

$$|\zeta(\sigma)|^3 |\zeta(\sigma+it)|^4 |\zeta(\sigma+2it)| \geq 1$$

$$(\sigma-1)|\zeta(\sigma)|^3 \left|\frac{\zeta(\sigma+it)}{(\sigma-1)}\right|^4 |\zeta(\sigma+2it)| \geq \frac{1}{\sigma-1}$$

finito e infinito que no puede ser

Multiplicando por $(\sigma-1)^4$ queda

$$(\sigma-1)|\zeta(\sigma)|^3 |\zeta(\sigma+it)|^4 |\zeta(\sigma+2it)| \geq (\sigma-1)^3$$

De nuevo basta probarlo para $\sigma \leq 2$

si $\sigma > 2$ $\left|\frac{1}{\zeta(s)}\right| = \left|\sum_{n\geq 1} \frac{\mu(n)}{n^s}\right| < |\zeta(2)|$. ∎

Por un lado tenemos para $\sigma \geq 1$ $t \geq 1$

$|\zeta(s)| < C \lg t$. Además si $1 < \sigma \leq 2$

$$(\sigma-1)\zeta(\sigma) = \sum_{n\geq 1} \frac{\mu(n)}{n^\sigma} \left(\frac{n}{n^\sigma}\right)$$

$|\sigma-1| < \varepsilon$ $\quad |(\sigma-1)\zeta(\sigma)| < 1+\varepsilon$

$1 \geq \sigma-1 > \varepsilon$ $\quad |(\sigma-1)\zeta(\sigma)| < \zeta(\varepsilon+1)$

luego en $1 \le \sigma \le 2$ si $t \ge 2$

$$|\zeta(\sigma+it)|^4 \ge \frac{(\sigma-1)^3}{C \lg t}$$

Sea $\eta$ fijo $1 < \eta \le 2$ y $1 \le \sigma < \eta$ $t \ge 3$

$$|\zeta(\eta+it)| - |\zeta(\sigma+it)| = \int_\sigma^\eta \zeta'(s)\, ds < C_2 |\eta - \sigma| \lg^2 t$$

$$|\zeta(\sigma+it)| > |\zeta(\eta+it)| - C_2(\eta-\sigma)\lg^2 t$$

$$> \frac{(\eta-1)^{3/4}}{C \lg^{3/4} t} - C_2(\eta-\sigma)\lg^2 t$$

cierto si $\eta \le \sigma \le 2$ por la desigualdad

luego para todo $1 \le \sigma \le 2$ basta escoger $\eta$ de forma que sea lo mas grande posible

$$(\eta-1)\lg^2 t < \frac{(\eta-1)^{3/4}}{\lg^{3/4} t}$$

$$\Rightarrow (\eta-1)^{1/4} \le \frac{1}{\lg^{9/4} t}$$

$$\eta = 1 + \frac{1}{\lg^9 t}$$

**Resumen** - $\zeta(s)$ analítica en $\sigma > 0$

Con un único polo simple en $s = 1$

- $|\zeta(s)| \le A_1 \log t \quad \sigma \ge 1, \ t \ge 2$

$|\zeta'(s)| < A(\delta)\, t^{1-\delta} \quad 1 > \sigma > \delta \ \ 0 < \delta < 1 \quad t \ge 2$

$|\zeta'(s)| < A_2 \log^2 t \quad 1 \le \sigma \quad t \ge 3$

$\zeta(s) \neq 0$ en $s = 1 + it$ $\quad \frac{1}{\zeta(s)} = O(\log^7(t)) \quad \sigma \ge 1.$

$$h(s) = -\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$$

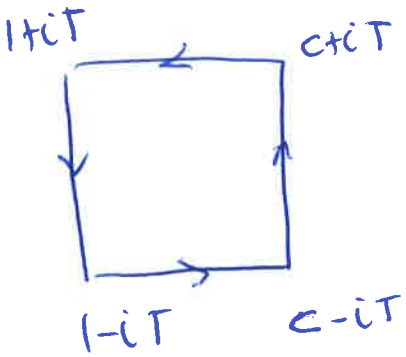
Es analítica en $\sigma \ge 1$. el único problema es en $s = 1$

pero $\quad (s-1)\zeta(s) = f(s)$ anal. $\neq 0$ en $\sigma \ge 1$

$$\log(s-1) + \log \zeta(s) = \log f(s)$$

$$\frac{1}{s-1} + \frac{\zeta'(s)}{\zeta(s)} = \frac{f'(s)}{f(s)} \text{ analítica}$$

$$\frac{1}{2\pi i} \int_R x^{s-1} h(s)\, ds = 0$$



$$\int_{c-iT}^{c+iT} + \int_{1+iT}^{1+iT} + \int_{1-iT}^{c-iT} + \int_{c+iT}^{1+iT}$$

$$|x^{s-1}| < x^{c-1}$$

T>>to

$$|h(s)| < \frac{1}{T^2}\left(\lg^{q} T + \frac{1}{T}\right) \longrightarrow 0 \quad T \to \infty$$

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} = -\frac{1}{2\pi i}\int_{1+i\infty}^{1-i\infty} x^{s-1} h(s)\,ds \qquad s = 1+it \qquad ds = i\,dt$$

$$= \frac{1}{2\pi}\int_{-\infty}^{\infty} x^{it} h(1+it)\,dt$$

$$\int_{-\infty}^{\infty} h(1+it)\,dt < \int_{-t_0}^{t_0} h(1+it)\,dt + \int_{\mathbb{R}-[-t_0,t_0]} h(1+it)\,dt$$

$$< \frac{\lg^{q}(t)}{t^2} \text{ integrable}$$

Lema de Riemann Lebesgue ejerc. 26 pag 452 Spivak capitulo 15.

El teorema del nº primo tiene diferentes interpretaciones equivalentes

Teorema: $\pi(x) \sim \frac{x}{\lg x} \iff p_n \sim n \lg n$

$\Rightarrow$ $n = \pi(p_n) \sim \frac{p_n}{\lg p_n} \Rightarrow p_n \sim n \lg p_n \sim n \lg n$

$\Rightarrow \lg p_n \sim \lg n + \lg\lg p_n \qquad 1 \sim \frac{\lg n}{\lg p_n}$

$\Leftarrow$ $p_n \sim n \lg n$ ~~$\Rightarrow \pi(x) = \sum_{p \le x}$~~

~~$n = \pi(p_n)$~~

$p_n \le x < p_{n+1}$

$n = \pi(y)$

$\pi(y) \sim \frac{y}{\lg y}$

$x \sim n \lg n$

$x \sim \pi(x) \lg \pi(x)$

~~$\lg x \sim \lg \pi(x)$~~

Para cada $x$ definimos $n$ tal que

$p_n \le x < p_{n+1}$ si $x \sim n \lg n$

$n = \pi(x)$ $\qquad x \sim \pi(x) \lg \pi(x)$

$$\boxed{\pi(x) \sim \frac{x}{\lg x}}$$

La segunda equivalencia tiene que ver con la función zeta. Efectivamente, demostrar el teorema del número primo es en realidad equivalente a $\pi(x) \sim \frac{x}{\log x}$.

Teorema: $\zeta(1+it) \neq 0 \iff \psi(x) \sim x$.

$$\psi(x) = x + o(x) \qquad \sigma > 1$$

$$\psi(x) = -\frac{\zeta'(s)}{\zeta(s)} = s \int_1^\infty \frac{\psi(t)}{t^{s+1}}\, dt \quad \text{luego}$$

$$-\frac{\zeta'(s)}{s\,\zeta(s)} = \int_1^\infty \frac{\psi(t)-t}{t^{s+1}}\, dt + \int_1^\infty \frac{1}{t^s}\, dt$$

$$= \frac{1}{s-1} + \int_1^\infty \frac{\psi(t)-t}{t^{s+1}}\, dt$$

$t > t_0 \quad \psi(t)-t < \varepsilon t$

$$-\frac{\zeta'(s)}{s\,\zeta(s)} = \int_1^{t_0} \frac{\psi(t)-t}{t^{s+1}}\, dt$$


$$\frac{\varepsilon}{1-\sigma}\, t_0^{1-\sigma}\Big|_{t_0}^{\infty}$$

$\lim_{\sigma \to 1} |(\sigma-1)\zeta(s)| < \varepsilon$ luego $= 0$

y $\zeta$ analítica en $1+it$ luego no tiene ceros ahí

Esto equivalencia es un paso más general en el sentido de que

Teorema: $\zeta(\sigma+it) \neq 0 \quad \sigma > \alpha \geq \frac{1}{2} \iff$ porque se sabe que si $\sigma = \frac{1}{2}$ hay ceros

$$\psi(x) - x = O(x^{\alpha+\varepsilon}) \quad \forall \varepsilon > 0$$

$$\left| -\frac{\zeta'(s)}{s\zeta(s)} \right| \leq K + \varepsilon \int_{\eta}^{\infty} \frac{1}{t^{\sigma-\alpha-\varepsilon+1}}\, dt$$

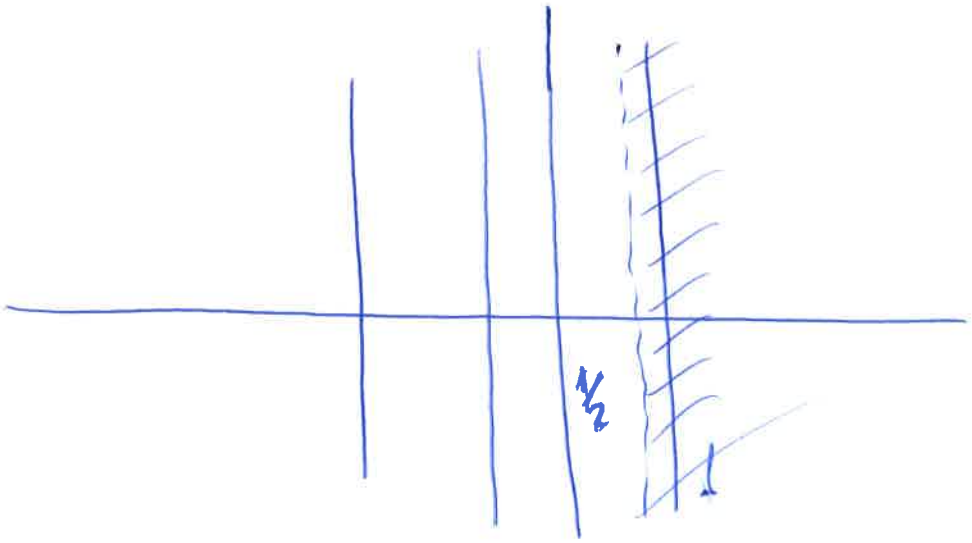
$$K + \varepsilon \frac{t_0^{\sigma-\alpha-\varepsilon}}{(\sigma-\alpha-\varepsilon)} + \varepsilon + M$$

$\sigma = \alpha + \delta$ y sea $\varepsilon = \frac{\delta}{2}$

$$\psi(x) - x = O(x^{\alpha+\delta})$$

$$\left| -\frac{\zeta'(s)}{s\zeta(s)} \right| < K + \varepsilon \int_{\eta}^{\infty} t^{\alpha+\delta-\sigma-1}\, dt$$

$$\varepsilon + M + \varepsilon \frac{t_0^{\alpha+\delta-\sigma}}{|\alpha+\delta-\sigma|}$$




Conjetura: $\psi(x) \sim x + O(x^{1/2+\varepsilon}) \quad \forall\, \varepsilon > 0$

por ejemplo $x^{1/2} \log x = O(x^{1/2+\varepsilon}) \; \forall\, \varepsilon$

Se sabe Levinson: $\frac{1}{3}$ cero están en $\mathrm{Re}\, s = \frac{1}{2}$

lo primero $10^9$ Hardy 1915 y cero

Actualmente 1 doble. (Conrey-Ghosh-Gonek)

La otra parte del teorema es

$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^\infty \frac{\psi(t)}{t^{s+1}}\, dt \quad \text{mmt}$$

$$\psi(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{s\,\zeta(s)}\, x^s\, ds$$

# La función Gamma

Teorema: $\pi^{-s}\zeta(2s)\Gamma(s) = \pi^{s-\frac{1}{2}}\zeta(1-2s)\Gamma(\frac{1}{2}-s)$

donde $\Gamma(s)$ es la función gamma

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dx \qquad \Re s > 0$$

Integrando por partes

$$\Gamma(s+1) = s\,\Gamma(s) \quad \Rightarrow \Gamma(1) = 1 \Rightarrow \Gamma(n+1) = n!$$

$$\Gamma(s+n+1) = (s+n)\cdots s\,\Gamma(s)$$ analítica con polos en los enteros negativos y 0

Además $\Gamma(s)\Gamma(1-s) = \int_0^\infty \frac{t^{s-1}}{1+t}dt = \frac{\pi}{\operatorname{sen}\pi s}$

cambio de variable

$$\int_0^\infty e^{-x} x^{-s} e^{-y} y^{s-1}\, dy\, dx \qquad \begin{matrix} x+y = u \\ \frac{y}{x} = v \end{matrix}$$

se tiene entonces

$$x = \pi n^2 y$$

$$e^{(s-1)\log(-1)} \quad (-1)^{s-1} \quad e^{(s-1)\log(-1)(i\pi)}$$

$$\Gamma(s) = \int_0^\infty e^{-\pi n^2 y} (\pi n^2 y)^{s-1} \pi n^2 dy$$

$$\frac{\pi^s \Gamma(s)}{\pi^s n^{2s}} = \int_0^\infty e^{-\pi n^2 y} y^{s-1} dy$$

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty \theta^*(y)\, y^{s/2}\, \frac{dy}{y}$$

$$\theta(y) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 y} \quad \text{comp} \quad \theta(y) = \frac{1}{\sqrt{y}}\theta\left(\frac{1}{y}\right)$$

$$2\theta^*(y) + 1 = \theta(y) = \frac{1}{\sqrt{y}}\left(2\theta\left(\frac{1}{y}\right)+1\right)$$

$$= \int_0^1 + \int_1^\infty$$

$$\psi(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds$$

$$\psi(x) = x - \frac{\zeta'(0)}{\zeta(0)} - \sum \frac{x^{-2n}}{-2n} - \sum \frac{x^\rho}{\rho}$$

$$x - \frac{\zeta'(0)}{\zeta(0)} - \log(1-x^{-2}) - \sum \frac{x^\rho}{\rho}$$

$$x - \frac{\zeta'(0)}{\zeta(0)} - \log(1-x^{-2}) - \sum_{|\rho|<x} \frac{x^\rho}{\rho} + \text{Error}$$

$x \neq \pi$

# Primos en progresiones aritméticas

Sabemos que $\pi(x) \sim \frac{x}{\lg x}$.

Ahora bien $p = 2n+1$. Una pregunta natural es ¿$4n+1$ ó $4n+3$? Son todos de uno o de otro.

Teorema: Existen infinitos primos de la forma $4n+3 = p$

Demostración: $4P_1 \cdots P_r + 1 = N \quad p \mid N \Rightarrow p \equiv 1 (4)$

$\Rightarrow$ producto de $\equiv 1 (4) \Rightarrow \equiv (4)$ abs.

No vale para $4n+1$ pues $(-1)(-1) = 1$.

Sin embargo Buscamos algo propio de los $p \equiv 1 (4)$

$\exists \infty$ $4n+1$. Supongamos que hay finitos

$$4(P_1 \cdots P_r)^2 + 1 = N \mid p$$

$$4(P_1 \cdots P_r)^2 + 1 \equiv 0 (p)$$

$-1 R p \Rightarrow p \equiv 1 (4) \neq P_i$

De la misma forma no es mult de 3

$3n+1 \quad 3n-1 \rightarrow 6n-1 \rightarrow$ sigue funcionando

$6n+1 \quad 6n+4$

porque hay solo dos que pasa en general

$p = an+b$ ya no funciona

$7u+1 \quad 7(p_1 \cdots p_r) - 1 \equiv +1$

$7 - 7^{-1}$

Propósito a probar Para $(a,b)=1$ existen infinitos primos de 6 forma $p=an+b$.

Idea previa Hacer como Euler.

$$\sum_{n\geq 1} \frac{1}{n^s} = \zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \longrightarrow \sum \frac{1}{p} \text{ diverge.}$$

$\chi(n)$ una función comp. mult. y tal que

$$\chi(n) = \begin{cases} 1 & n \equiv a \ (b) \\ 0 & \text{resto} \end{cases}$$

$$L(\chi, s) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} = \prod_{p \equiv a(b)} \left(1 - \frac{\chi(p)}{p^s}\right)$$ tomando log

$$\log L(\chi,s) = \sum_{p \equiv a(b)} \frac{\chi(p)}{p^s} + \sum_p \sum_{m\geq 2} \frac{\chi(p^m)}{p^{ms}}$$

acotado

$\log L(\chi,s)$ diverge

diverge

Necesito una función completamente multiplicativa y periódica tal que $\chi(n)=1 \iff n \equiv a \pmod{5}$

Es imposible pues para $(c,5)=1$

$cx \equiv a \pmod 5$ tiene solución y

$$0 = \chi(c)\chi(x) = \chi(cx) = \chi(a) = 1$$

Sin embargo $\log L(\chi,s)$ es lineal en $\chi$

$$\sum_\chi \log L(\chi,s) = \sum_\chi \sum_p \sum_{m\geq 1} \frac{\chi(p^m)}{p^{ms}} = \sum_p \sum_m \frac{1}{p^{ms}} \sum_\chi \chi(p^m)$$

una combinación lineal de funciones de $\chi$

Recordar que $\displaystyle\sum_{k=0}^{m-1} e^{2\pi i \frac{ak}{m}} = \begin{cases} 0 & \text{si } m \nmid a \\ m & \text{si } m \mid a \end{cases}$

## Raíz de 6 unidad Pequeña idea y Caracteres

Definición Un carácter módulo $m$ es una función aritmética, completamente multiplicativa y $m$-periódica tal que $\chi(1) \neq 0$ tal que $\chi(n)=0$ $(n,m)>1$

Ejemplo: $\chi(n) = \begin{cases} 1 & (n,m)=1 \\ 0 & \text{resto} \end{cases}$ lo es

Este definido en cualquier módulo $m$

$\chi(an+b) = \chi(b)$

$\chi(0)=0 \quad \chi(1)=1 \quad \chi(-1)=(-1)$

$\chi(n) = \left(\frac{n}{p}\right)$ es un carácter módulo $p$ Símbolo de Jacobi. Dado cualquier entero impar tenemos un carácter. ¿Es el único?

Teorema: Los caracteres forman un grupo Abeliano finito.

Lema: $\chi$ un carácter módulo $m$

entonces

i) $\chi(1)=1$

ii) $\chi(a)$ es una raíz $\varphi(m)$-ésima de la unidad

iii) $\bar{\chi}$ es un carácter módulo $m$ de ecuación $\bar{\chi}(a) = \chi(a^{-1})$ $(a,m)=1$

Demos $\chi(1)^2 = \chi(1\cdot 1) = \chi(1) \Rightarrow \chi(1)=1$ ∎

$1 = \chi(a^{\varphi(m)}) = (\chi(a))^{\varphi(m)}$ ∎

$\bar{\chi}(a)\cdot\chi(a) = 1 = \chi(a)\chi(a^{-1})$

$\bar{\chi}(ab) = \frac{1}{\chi(a)\chi(b)} = \bar{\chi}(a)\cdot\bar{\chi}(b)$

$\bar{\chi}(a) = \chi(a^{-1})$

Lema: $\chi = \chi_1 \cdot \chi_2 (a) = \chi_1(a) \cdot \chi_2(a)$ es un caracter.

Tengo operación elemento

Teo: Es un grupo $\chi_0(a) = 1 \quad (a,m)=1$ resto

$1 = \chi \bar{\chi} \quad (a,m)=1$

$0 \quad (a,m) > 1$ en el resto

conmutativo y asociativo es pues son números complejos

Es finito pues $\chi(a)$ es una $\phi(m)$-raíz de 6 unidad a cada a mod m puedo tener $\phi(m)$ valor $\phi(m)^2$ posibilidades

Ejemplo: módulo 5

raíz 4 de C a 2 raíz primitiva $2 \cdot 2 = 4$ $a^4 = 1$

$a = \pm 1, \pm i$

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $\chi_0$ | 0 | 1 | 1 | 1 | 1 |
| $\chi_1$ | 0 | 1 | -1 | -1 | 1 |
| | 0 | 1 | i | -i | -1 |
| | 0 | 1 | -i | i | -1 |

$= \left(\frac{a}{5}\right) = (-1)$

$\left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1$

$\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$

$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = -1$

~~Podemos existirlo todos y~~ Basta existir este, pues es porque 2 es raíz primitiva

$\chi(g^a) = \chi(g)^a$ basta ahora

Tesis Proposición Sea $X = \{\chi \text{ caracter mod } m\}$

$$|X| \geq \phi(m)$$

1) Si $m = p$ ~~$\chi(a)$~~ $\exists$ raíz primitiva

$$a \equiv g^b \ (p) \qquad \chi(a) = (\chi(g))^b$$

$$\chi(g) = e^{2\pi i \frac{h}{p-1}} \qquad 1 \leq h \leq p-1 \quad \text{Son distintos}$$

$$\chi(g) = \tilde{\chi}(g) \Rightarrow e^{2\pi i \frac{(h-h_1)}{p-1}} = 1 \quad \text{no puede ser}$$

$\chi(g) \neq 1$ si $\chi \neq \chi_0$ $\qquad \chi(a) = e^{2\pi i \frac{hb}{(p-1)}}$

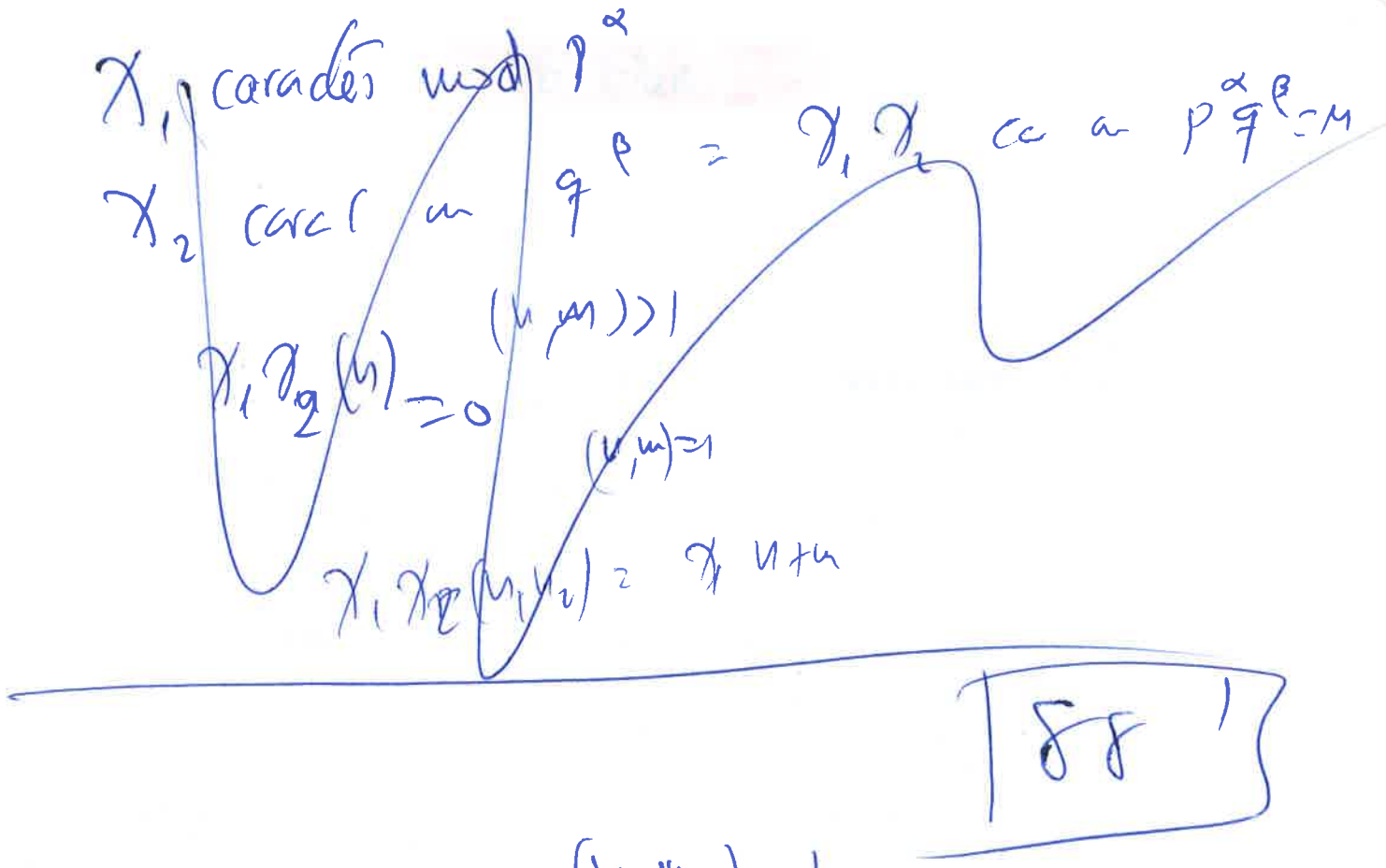
2) Si $m = p^2$ igual

3) Si $m = 2^e p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$$a = g_0^{a_0} \tilde{g}_0^{b_0} g_1^{a_1} \cdots g_r^{a_r} \ (m)$$

$$\chi(a) = e\left(\frac{a_0 n_0}{2} + \frac{b_0 n_0'}{2^{e-2}} + \frac{a_1 n_1}{\phi(p_1^{\alpha_1})} + \cdots \frac{a_r n_r}{\phi(p_r^{\alpha_r})}\right)$$

es un caracter, pues




88 |

$(n_1, n_2) = 1$

Lema: Si $\chi_1$ caracter mod $m_1$

$\chi_2$ " " $m_2$

$\chi_1\chi_2(n) = \chi_1(n)\chi_2(n)$ es un caracter mod $m_1 m_2$

3) ...

$\chi_1\chi_2(n_1 n_2) = \chi_1(n_1)\chi_2(n_2)$

$= \chi_1(n_1)\chi(n_2)$ —

y son distintos que algún $u_i \neq u_i'$ $\quad a \equiv g_i (p_i^{\alpha_i}) \quad$ 89

$$a \equiv \phi(p_j^{\alpha_j})$$

$$a \equiv \chi(a) = e^{2\pi i \frac{u_i}{\phi(p_i^{\alpha_i})}}$$

$$\chi_1(a) = e^{2\pi i \frac{u_i'}{\phi(p_i^{\alpha_i})}}$$

$\exists$ a t.q. $\chi(a) \neq 1 \ (m)$

---

De 6 simetría en $u_i$ y $a$ deducimos

Ejemplo 12

**Teorema:** Si $u \not\equiv 1 (m)$ $\exists \chi$ tal que $\chi(u) \neq 1$

$u_i \neq 0$ para algún $i$ sea $\chi(u) = e\left(\frac{q_i u_i}{\varphi p_i^{\alpha_i}}\right)$

Nuestro objetivo es probar ortogonalidad

**Teorema.**

$$\sum_u \chi(u) = \begin{cases} \varphi(m) & \text{si } \chi = \chi_0 \\ 0 & \text{resto} \end{cases}$$

$$\sum_\chi \chi(u) = \begin{cases} c & \text{si } u \equiv 1 (m) \\ 0 & \text{resto} \end{cases}$$

$(a,m)=1$

$\chi(a)\cdot S$

$$\chi(a)\sum_n \chi(n) = \sum_n \chi(an) = S \Rightarrow S=0$$

$$\chi_1(n)\sum_\chi \chi(n) = \sum_\chi \chi_1\chi(n) = \sum_\chi \chi(n) \quad \boxtimes$$

Corolario $|X| = \phi(m)$

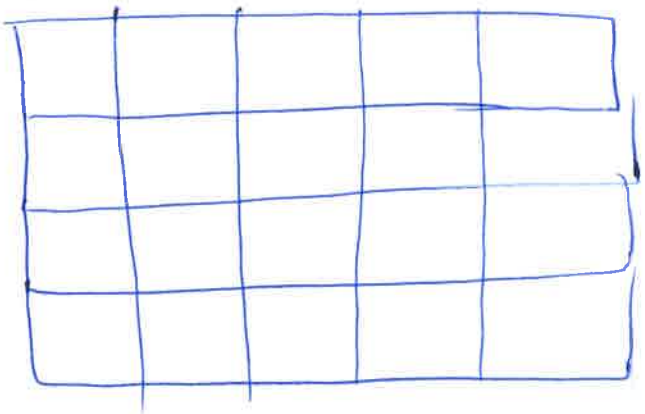
$$\sum_\chi \sum_n \chi(n) = \sum_n \sum_\chi \chi(n)$$

$$\| \qquad\qquad = c \quad \boxtimes$$

$$\phi(m)$$

~~De entre los caracteres hay que distinguir~~

Hay dos tipos de caracteres. En la tabla del 12 vimos



pensados modulo un numero menor y los que no

Corolario: $\sum_{N \le n \le M} \chi(n) \le K$

Lo probamos para $N = 0$

$$\sum_{n \le M} \chi(n) = \sum_{k=0}^{[\frac{M}{m}]-1} \sum_{km+1}^{(k+1)m} \chi(n) + \sum_{[\frac{M}{m}]m+1}^{M} \chi(n)$$

$$\le$$

Ejercicio en general

Corolario: ~~Todo carácter puede factorizarse como~~

~~$\chi(n) = \prod \chi_i(n; p_i^{\alpha_i})$~~

Sea $\chi_1(n; 2^\ell) = (-1)^{\frac{n-1}{2}}$

$\chi_2(n; 2^\ell) = e^{\frac{2\pi i b_0}{2^{\ell-2}}}$

$\chi(n; p^\ell) = e^{\frac{2\pi i b_i}{\phi(p^\ell)}}$

Entonces si $n = 2^\ell p_1^{\alpha_1} \cdots p_s^{\alpha_s}$

$$\chi(n) = \begin{cases} \prod \chi(n, p_i)^{k_i} & \ell = 0, 1 \\ \chi_1(n, 2^\ell)^{k_0} \prod \chi(n, p_i)^{k_i} & \ell = 2 \\ \chi_1(n; 2^\ell)^{k_0} \chi_2(n; 2^\ell)^{k_0} \prod \chi(n, p_i)^{k_i} & \ell \ge 3 \end{cases}$$

**Definición:** Un carácter $\chi$ mod $m$ es impropio si es periódico módulo $d|m$. para todo $(n,m)=1$ en caso contrario es propio

módulo 8 $\chi(1)=1$ $\chi(3)=-1$

$\chi(5)=1$ $\chi(7)=-1$

~~no es primo~~ es impropio

$\chi(1)=1$ $\chi(3)=-1$

$\chi(5)=-1$ $\chi(7)=1$

~~**Lema:** Todos los caracteres mod p son primitivos~~ Si

$d \neq$

**Lema** Si $\chi$ es impropio existe $\chi_1$ tal que $\chi(n) = \chi_1(n)$ $\forall (n,m)=1$

$(n+td, m)=1$

$\chi_1(n) = \chi(n+td)$

$\chi_1$ es el carácter inducido

Siguiente página

**Lema** $\chi(n) = \prod_i \chi(n; p_i^{\alpha_i})$

es primitivo $\Leftrightarrow$ lo son cada uno de los $\chi(n; p_i^{\alpha_i})$

Si $\chi(n; p_j^{\alpha_j})$ es impropio entonces está inducido por $\tilde{\chi}(n; p_j^{\beta_j})$ luego $\tilde{\chi}(n) = \prod_{(i \neq j)} \chi(n; p_i^{\alpha_i}) \tilde{\chi}(n; p_j^{\beta_j})$

induce a $\chi$

**Lema:** Es $\chi \bmod p \geq 3$ impropio $\Leftrightarrow p \mid n_i$ ~~para algún $n_i$~~

$\Leftarrow \chi(n, p_i^{\alpha_i}) = e^{2\pi i \frac{n_i b_i}{\phi(p_i^{\alpha_i})}} = e^{2\pi i \frac{n_i b_i}{\phi(p_i^{\alpha_i - 1})}}$ cuando $\bmod p_i$

$\Rightarrow$ ~~$\chi(n; p_i^{\alpha_i}) = \chi(n + p_i^{\beta_i}) = e^{2\pi i \frac{n_i b_i}{\phi(p_i^{\alpha_i})}} e^{2\pi i \frac{b_i}{p_i^{\alpha_i - 1}}}$~~

~~$n = g^a (p_i^{\alpha_i})$~~

~~$n + p_i^{\beta_i} = g^a + p_i^{\beta_i} + \cdots + p_i^{\alpha_i}$~~

$\chi(n; p_i^{\alpha_i}) = \chi(n; p_i^{\beta_i}) = e^{2\pi i \frac{k_i b_i}{\phi(p_i^{\beta_i})}}$

$= e^{2\pi i \frac{n_i p^s b_i}{\phi(p_i^{\alpha_i})}}$

**Лемма:** $\chi \bmod p^l$ $p \geq 3$ — примитивный $\Leftrightarrow p \nmid N$.

$\Leftarrow$ $\chi(n; p^l) = e^{2\pi i \left(\frac{Nb}{\phi(p^l)}\right)} = e^{2\pi i \frac{N/p\, b}{\phi(p^{l-1})}}$ — в самом деле.

$\Rightarrow \chi(n; p^l) = \chi_1(n; p^{l-1}) = e^{2\pi i \frac{Nb}{\phi(p^{l-1})}} =$

$e^{2\pi i \frac{Nb}{\phi(p^l)}} = e^{2\pi i \frac{pKb}{\phi(p^l)}}$ $\quad pN = \bar{N}$ кратно $\phi(p^l)$

**Лемма** $\chi \bmod 2^l$ $l \geq 3$ — примитивный $\Leftrightarrow 2 \nmid K_0'$

$$\chi = e^{2\pi i \left(\frac{N_0 a}{2} + \frac{N_0' b_0}{2^{l-2}}\right)}$$

$\Leftarrow$ ясно

$\Rightarrow$ $\chi(n) = \chi(n + 2^{l-1})$ $\quad n \equiv n + 2^{l-1}\,(4)$, $a = a'$

$$e^{2\pi i \left(\frac{N_0 a}{2} + \frac{N_0' b_0}{2^{l-2}}\right)} = e^{2\pi i \left(\frac{N_0 a}{2} + \frac{N_0' b_0'}{2^{l-2}}\right)}$$

$$N_0'(b_0 - b_0') \equiv 0 \,(2^{l-2})$$

$$n + 2^{l-1} \equiv n + n 2^{l-1} \,(2^l) = n 5^{2^{l-3}} 5_0 + 2^{l-3}$$

**Corolario** Sea $m$ entero impar. El único carácter real primitivo es $\chi(n) = \left(\frac{n}{m}\right)$ el símbolo de Jacobi cuando $m = p_1 \cdots p_r$ y no hay si $m$ no es libre de cuadrados

$$\chi(n, p^\alpha) = e^{2\pi i K \frac{b}{\phi(p^\alpha)}} \quad \text{real} \Rightarrow \frac{\phi(p^\alpha)}{2} \mid K$$

pero si $p \mid K \Rightarrow$ no es dos $\alpha = 1$. en ese caso

$$\chi(n, p) = e^{\pi i b} = \begin{cases} -1 & \text{si } b \text{ impar} \\ 1 & \text{si } b \text{ par} \end{cases}$$

si $b$ es par $n = g^{2a} \Rightarrow n \, R \, p \Rightarrow \left(\frac{n}{p}\right) = +1$

$b$ impar $n = g^{2a+1} \Rightarrow n \, N \, p \Rightarrow \left(\frac{n}{p}\right) = -1$ ∎

Es producto de primitivos. $\chi(n) = \chi\left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{m}\right)$ ∎

Conclusión: $\chi(n) = \prod \chi(n_i, p^{\alpha_i})$ es impropio

si y sólo si $p \mid n_i$ o $2 \mid n_i$ para algún $i$

es primitivo si el producto de primitivos

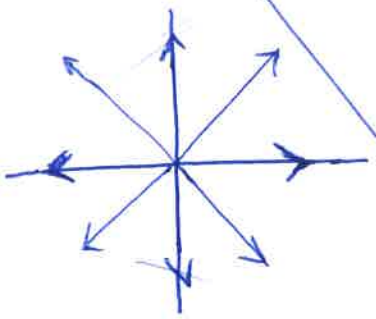
## Sumas de Caracteres

## Sumas de Gauss

Geométricamente

$$\sum_{b=1}^{m} \chi(n) = 0 \qquad e^{\frac{2\pi i k b}{\phi(p^\alpha)}}$$

$m = 4$



$$\sum_{n=1}^{\phi(p^\alpha)/m} e^{2\pi i \frac{m n}{\phi(p^\alpha)}}$$

Todos dan cero. Incluso si me quedo con las clases primas con el módulo dan cero.

Hay más sumas

$$C_m(n) = \sum_{(h,m)=1} e^{2\pi i \frac{h n}{m}}$$

$$= \sum_{d \mid (n,m)} \mu\left(\frac{m}{d}\right) d$$

$$C_m(1) = \mu(m)$$

$$\chi(n) = e^{\pi i b} = \begin{cases} 1 & n \, R \, p \\ -1 & n \, N \, p \end{cases}$$

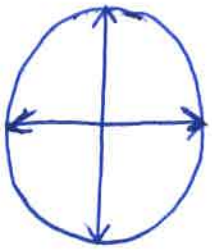
94

$$= \left(\frac{n}{p}\right)$$

en general $m = p_1 \cdots p_r$

$$\chi(n) = \left(\frac{n}{p_1}\right) \cdots \left(\frac{n}{p_r}\right) = \left(\frac{n}{m}\right)$$

## Sumas de caracteres



$$\sum_{n=1}^{m} e^{2\pi i \frac{nk}{m}} = \begin{cases} 0 & m \nmid k \\ m & m \mid k \end{cases}$$

si nos restringimos $\sum_{n} \chi(n) = \begin{cases} 0 & n \not\equiv 1 \ (m) \\ \phi(m) & n \equiv 1 \ (m) \end{cases}$

quedamos con los $(n,m)=1$

¿Existen más?

$$c_m(n) = \sum_{\substack{1 \le h \le m \\ (h,m)=1}} e^{2\pi i \frac{nh}{m}} = \sum_{d \mid (m,n)} \mu\left(\frac{m}{d}\right) d$$

los $h$ primos con $m$ no es lo mismo que antes!!

$$c_m(1) = \mu(m)$$

Gauss considera las sumas sobre residuos cuadráticos

**Def** La suma de Gauss $S(n,m) = \sum_{x=1}^{m} e^{2\pi i \frac{x^2 n}{m}}$

$(n,m)=1$

$(m_1,m_2)=1$

**Lema:** $S(n,m_1m_2) = S(m_1 n, m_2)\cdot S(m_2 n, m_1)$

$a m_1 + b m_2 = x$

$$\sum_{a=1}^{m_2}\sum_{b=1}^{m_1} e^{2\pi i \frac{a^2 m_1^2 + b^2 m_2^2 + 2 m_1 m_2 ab\, n}{m_1 m_2}}$$

$$= \sum_{a=1}^{m_2} e^{2\pi i a^2 \frac{m_1^2 n}{m_2}} \sum_{b=1}^{m_1} e^{2\pi i b^2 \frac{m_2 n}{m_1}}$$

Basta estudiar $S(n, p^\ell)$

**Proposición.** $p \geq 3$

i) $S(n;p^\ell) = p\, S(n;p^{\ell-2})$ $\quad \ell \geq 2$

ii) $S(n;2^\ell) = 2\, S(n;2^{\ell-2})$ $\quad \ell \geq 4$

Demostración

$n = x + y p^{l-1}$ $\quad 1 \le x \le p^{l-1}$

$0 \le y \le p-1$

$$S(n, p^l) = \sum_{y=0}^{p-1} \sum_{x=1}^{p^{l-1}} e^{2\pi i (x+yp^{l-1})^2 \frac{n}{p^l}}$$

$$= \sum_{y=0}^{p-1} \sum_{x=1}^{p^{l-1}} e^{2\pi i (x^2 + 2xy p^{l-1}) \frac{n}{p^l}}$$

$$= \sum_{x=0}^{p^{l-1}-1} e^{2\pi i \frac{x^2 n}{p^l}} \sum_{y=0}^{p-1} \left( e^{4\pi i \frac{xn}{p^2}} \right)^y$$

$$= p \sum_{x=1}^{p^{l-2}} e^{2\pi i \frac{x^2 y}{p^{l-2}}}$$

en el caso de $2^l$ se hace igual

Ejercicio

Me restringe a entender

$S(n,2)$ $S(n,4)$ $S(n,8)$ $S(n,p)$

Evaluar también en $S(n,27)$ $S(n,17)$ $S(n,25)$

**Teorema:** $S(n,p) = \left(\frac{n}{p}\right) S(1,p)$

$$\sum_{k=1}^{p} e^{2\pi i \frac{k^2 n}{p}} = \sum_{k=1}^{p} \left(1+\left(\frac{k}{p}\right)\right) e^{2\pi i \frac{kn}{p}}$$

$$= \sum_{k=1}^{p} \left(\frac{k}{p}\right) e^{2\pi i \frac{kn}{p}}$$

$$= \left(\frac{n}{p}\right) \sum_{k=1}^{p} \left(\frac{kn}{p}\right) e^{2\pi i \frac{kn}{p}} = \left(\frac{n}{p}\right) S(1,p) \quad \blacksquare$$

Basta entender $S(1,p)$. Caso particular de sumas de caracteres

**Def:** Sea $\chi$ caracter mod $m$

$$S(\chi,m) = \sum_{k=1}^{m} \chi(n)\, e^{2\pi i \frac{na}{m}} \quad (a,m)=1$$

**Proposición** $\chi(a)S(a,\chi) = S(1,\chi) = S(\chi)$

$(a,m)=1$

Ya que

De la misma forma que antes se tiene

**Proposición** Sea $\chi$ carácter mod $(m_1,m_2)$

$\chi = \chi_1 \cdot \chi_2$ $\chi_1$ mod $m_1$ $\chi_2$ mod $m_2$

entonces $S(a,\chi) = \chi_1(m_2)\chi_2(m_1) S(a,\chi_1) S(a,\chi_2)$

$$\sum_{n=1}^{m_1 m_2} \chi(n) e^{\frac{2\pi i n a}{m}} = \chi_1(m_2)\chi_2(m_1) \sum_{n_1=1}^{m_1} \sum_{n_2=1}^{m_2} \chi_1(n_2)\chi_2(n_1) e^{\frac{2\pi i n_1 a}{m_2}} e^{\frac{2\pi i n_2 a}{m_1}}$$

$n = n_1 m_1 + n_2 m_2$

Debemos entender $S(\chi)$ mod $p^l$

Queremos ~~saber~~ asegurar que cierta suma de caracteres no es cero. Aquí se ve la importancia de ser primitivo

**Teorema** Sea $\chi$ mod $p^l$ primitivo y $q \nmid a$

entonces

$$S(a,\chi) = 0$$

primitivo y $p \mid a \Rightarrow S(a,\chi) = 0$

$$\chi(x+y p^{l-1}) = \chi(x)$$

$$S(a,\chi) = \sum_{x=1}^{p^{l-1}} \sum_{y=0}^{p-1} \chi(x+y p^{l-1})\, e^{\frac{2\pi i a (x+y p^{l-1})}{p^l}}$$

$$= \sum_{x=1}^{p^{l-1}} \chi(x)\, e^{\frac{2\pi i a x}{p^l}} \sum_{y=0}^{p-1} e^{\frac{2\pi i a y}{p}} = 0 \quad p \nmid a$$

Si $\chi$ es primitivo $\quad a = pa'$

$$\sum_{p \nmid x} e^{\frac{2\pi i a x}{p^{l-1}}} \sum_{y=0}^{p-1} \chi(x+y p^{l-1})$$

$$= \sum_{p \nmid x} e^{\frac{2\pi i a' x}{p^{l-1}}} \chi(x) \sum_{y=0}^{p-1} \chi(1+x^{-1} y p^{l-1})\, \chi(1+y' p^{l-1})$$

$$\chi(1+y_0 p^{l-1}) \neq 1 \Rightarrow$$

$$\chi(1+y_0 p^{l-1})\, S = \sum \chi(1+y_0 p^{l-1}+y' p^{l-1})$$

$$\equiv S \quad \blacksquare$$

$$S = 0$$

por tanto es cero

Caracteres primitivos y tal que ~~$\chi(a) \neq 0$~~ $P \nmid a$.

Proposición: $\chi(a)\, S(a,\chi) = S(1,\chi)$ ⊣

Falta encontrar el valor de $S(1,\chi)$

$S(1,\bar{\chi}) = S(1,\chi)$ donde $\chi = \left(\frac{n}{p}\right)$.

Podemos asegurar que es $\neq 0$ mediante

Teorema ~~$S(\chi)$~~ Sea $\chi$ un caracter primitivo. entonces $|S(\chi)| = \sqrt{m}$.

~~i) $m = p^l$~~ Basta probarlo para $m = p^l$

$$|S(\chi)|^2 = S(\chi)\,\overline{S(\chi)} = \sum_{\substack{m=1 \\ (m,p)=1}}^{p^l} \sum_{\substack{n=1 \\ (n,p)=1}}^{p^l} \chi(m)\,\overline{\chi}(n)\, e^{2\pi i \frac{(m-n)}{p^l}}$$

$$\overline{\chi}(m) = \chi(n^{-1})$$

$$= \sum_{\substack{n=1 \\ (n,p)=1}}^{p^l} \sum_{\substack{m=1 \\ (m,p)=1}}^{p^l} \chi(mn^{-1})\, e^{2\pi i \frac{n(mn^{-1}-1)}{p^l}}$$

$$= \sum_{(n,p)=1} \sum_{(m,p)=1} \chi(m)\, e^{2\pi i \frac{n(m-1)}{p^l}}$$

$$= \sum_{(m,p)=1} \chi(m) \sum_{(n,p)=1} e^{2\pi i \frac{n(m-1)}{p^l}} =$$

$m = 1 + y p^{l-1}$

$$= \sum_{(m,p)=1} \chi(m)\, C_{p^l}(m-1)$$

$$= \sum_{(m,p)=1} \chi(m)\, C_{p^l}(m-1)$$

$$p^l - p^{l-1} - p^{l-1} \sum_{y=1}^{p-1} \chi(1 + y p^{l-1}) = p^l$$

$$\sum_{y=1}^{p-1} \chi(1 + y p^{l-1}) = -1$$

∎

Si además el carácter es real todavía podemos decir un poco más

Sumas Caracteres reales

**Teorema:** Sea $\chi$ un carácter primitivo real mod $p$ impar. Entonces

$$S^2(\chi) = (-1)^{\frac{p-1}{2}} p$$

$$\sum_{n=1}^{p} \sum_{m=1}^{p} \chi(n)\chi(m)\, e^{\frac{2\pi i (n+m)}{p}} = \sum_{n=1}^{p-1} \sum_{m=1}^{p-1} \chi(m)\, e^{\frac{2\pi i m(n+1)}{p}}$$

de 6 manera que antes

$$S^2(\chi) = \sum_{(m,p)=1} \chi(m)\, C_p^{(m+1)}$$

$$= -\sum_{m=2}^{p-2} \chi(m) + (p-1)\chi(-1)$$

$$= p\,\chi(-1) \quad \blacksquare$$

el resultado general es por $\tilde{S}(\chi_1, \chi_2) = \chi_1(a)\chi_2(a)$

contar el signo de G sume es mucho más delicado. Le costó 4 años a Gauss el probarlo.

Teorema: $$S(p) = \begin{cases} \sqrt{p} & p \equiv 1 \ (4) \\ i\sqrt{p} & p \equiv 3 \ (4) \end{cases}$$

La demostración ~~requiere~~ Existen diferentes pruebas de este hecho. Vamos a dar una de Kronecker que relaciona la suma de Gauss con la teoría de ciclotomia. Polinomio ciclotómico

Lema $x^{p-1} + \dots + 1 = f(x)$ es irreducible en $\mathbb{Q}[x]$

Lema de Gauss
Criterio de Eisenstein $F(x) = (x^p - 1)$

$$f(x+1) \cdot x = F(x+1) = (x+1)^p - 1 = \sum_{j \geq 1}^{p} \binom{p}{j} x^j$$

∎

**Lema:** $\prod_{w=1}^{\frac{p-1}{2}} \left(\zeta^{2w-1} - \zeta^{-(2w-1)}\right)^2 = (-1)^{\frac{p-1}{2}} p$

Demostración. $\zeta = e^{\frac{2\pi i}{p}}$ $\qquad 1 + x + \cdots + x^{p-1} = \prod_{w=1}^{p-1}(x - \zeta^w)$

$$\prod_{w=1}^{p-1}(1 - \zeta^w) = p$$

$$\| \qquad 2w+1 = x \text{ es un sistema completo de residuos y por tanto}$$

también lo es $4w+2$

$$p = \prod_{w=1}^{p-1}\left(1 - \zeta^{4w+2}\right) = \prod_{w=1}^{p-1} \zeta^{2w+1} \prod_{w=1}^{p-1}\left(\zeta^{-(2w+1)} - \zeta^{(2w+1)}\right)$$

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

$$1 \quad 3 \quad \cdots \quad p-2 \quad = \quad 2w+1 \qquad w = 1, \ldots, \tfrac{p-1}{2}$$

$$-1 \qquad -(p-2) \qquad -(2w-1)$$

**Lema** $\prod_{h=1}^{\frac{p-1}{2}} \left(\zeta^{2h-1} - \zeta^{-(2h-1)}\right)^2 = (-1)^{\frac{p-1}{2}} p$

$$X^p - 1 = (X-1) \prod_{h=1}^{p-1} (X - \zeta^h)$$

$1, 2, \dots, p-1 \qquad 1 \quad 3 \quad \dots \quad p-2$

$\qquad\qquad\qquad\qquad -1 \quad -3 \quad \dots \quad -(p-2)$

$$p = \prod_{h=1}^{p-1} (X - \zeta^h) = \prod_{h=1}^{\frac{p-1}{2}} (X - \zeta^{4h+2}) \prod_{h=1}^{\frac{p-1}{2}} (X - \zeta^{-(4h-2)})$$

$$= \prod_{h=1}^{\frac{p-1}{2}} \zeta^{2h-1} \prod_{h=1}^{\frac{p-1}{2}} \left(\zeta^{-(2h-1)} - \zeta^{2h-1}\right) \prod_{h=1}^{\frac{p-1}{2}} \left(\zeta^{2h-1} - \zeta^{-(2h-1)}\right)$$

$$= \prod_{h=1}^{\frac{p-1}{2}} \left(\zeta^{\frac{2h-1}{2}} - \zeta^{-(2h-1)}\right)^2 (-1)^{\frac{p-1}{2}} \qquad \blacksquare$$

**Corolario** $S(1,p) = \varepsilon \prod_{h=1}^{\frac{p-1}{2}} \left(\zeta^{\frac{2h-1}{2}} - \zeta^{-(2h-1)}\right)$

**Lema** $\prod_{h=1}^{\frac{p-1}{2}} \left(\zeta^{\frac{2h-1}{2}} - \zeta^{-(2h-1)}\right) = \begin{cases} \sqrt{p} & p \equiv 1 \ (4) \\ i\sqrt{p} & p \equiv 3 \ (4) \end{cases}$

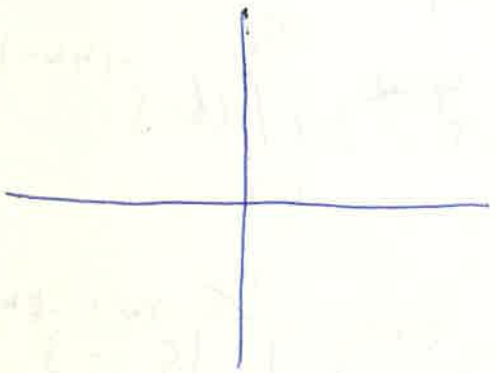
Baste ver el signo del producto

$$e^{2\pi i \frac{2N-1}{p}} - e^{-2\pi i \frac{(2N-1)}{p}} = 2i \operatorname{Sen}\left(2\pi \frac{4N-2}{p}\right)$$

$$= i^{\frac{p-1}{2}} \, 2^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \operatorname{Sen}\left(\frac{4N-2}{p}\pi\right)$$

$p \equiv 1 \ (4)$

$p \equiv 3 (4)$



$$\frac{4N-2}{p} < 1$$

$$4N < p+2 \qquad p \equiv 1(4)$$

$$N < \frac{p+2}{4}$$

$$N \leq \frac{p-1}{4} \qquad p \equiv 3(4)$$

$$N \leq \frac{p+1}{4} + 1$$

$$\prod_{N=\frac{p+1}{4}+1}^{\frac{p-1}{2}}$$

$$\frac{p+1}{4} + \frac{p-3}{4}$$

$$(-1)^{\frac{p-3}{4}}$$

$$(-1)^{\frac{p-1}{4}+1^{\frac{p-3}{4}}} = 1$$

$$\frac{p-1}{4} n \quad \frac{p-1}{4} + \frac{p-1}{4} \quad (-1)^{\frac{p-1}{2}} \qquad p \equiv 1(4)$$

$(-1)$

Bank ver el signo del producto

$$\prod_{N=1}^{\frac{p-1}{2}} \left(\zeta^{2N-1} - \zeta^{-(2N-1)}\right) = i^{\frac{p-1}{2}} 2^{\frac{p-1}{2}} \prod_{N=1}^{\frac{p-1}{2}} \operatorname{Sen}\left(\frac{4N-2}{p}\pi\right)$$

$p \equiv 1 (4)$ $\quad = (-1)^{\frac{p-1}{4}}$ pasa hace siempre que

$$\frac{4N-2}{p} \leq 1 \qquad N \leq \frac{p+2}{4}$$

$p \equiv 1\ 4 \qquad 1 \leq N \leq \frac{p-1}{4}$

$p \equiv 3(4) \qquad 1 \leq N \leq \frac{p+1}{4}$

Si $p \equiv 1 \ 4$

$(-1)^{\frac{p-1}{4}} = 1$

Si $p \equiv 1(4)$ queda $(-1)^{\frac{p-1}{4}} 2^{\frac{p-1}{2}} \prod_{1}^{\frac{p-1}{4}}(\ ) \prod_{\frac{p-1}{4}+1}^{\frac{p-1}{2}} \operatorname{Sen}(\ )$

$= (-1)^{\frac{p-1}{2}} C \qquad C \geq 0 \qquad = C' \geq 0$

Si $p \equiv 3(4)$ queda $i\, i^{\frac{p-3}{2}} 2^{\frac{p-1}{2}} \prod_{1}^{\frac{p+1}{4}} \operatorname{Sen}$

$i\ (-1)^{\frac{p-3}{4}} (-1)^{\frac{p-3}{4}} = i\, C' \qquad C \geq 0$

Demostrar el teorema en probar $\varepsilon = 1$

Consideramos

$$f(x) = \sum_{j=1}^{p-1} x(j)\, x^j - \varepsilon \prod_{j=1}^{\frac{p-1}{2}} (x^{2j-1} - x^{p-(2j-1)})$$

$f(1) = 0 \quad f(3) = 0$ luego $x^p - 1 \mid f(x)$

existe $h(x) \in \mathbb{Z}[x]$ tal que

$$f(x) = (x^p - 1)\, h(x)$$

pues $f$ es impar

Sea $x = e^z$

entender $\varepsilon$ es hacerlo mod $p$ y la pide en 0 mod $p$

$$(e^{zp} - 1)\, h(e^z) = f(e^z)$$

desarrollo en serie de potencias

$$\sum_{n \geq 1} \frac{(pz)^n}{n!} \sum \frac{a_n z^n}{n!} \quad ; \quad \sum c_n x^n$$

entra $p$ $\frac{A}{B}$ $\quad pXB$ para $n \leq p-1$

pues es $\sum \frac{a_{n-w}\, b_w}{(n-w)!\, w!}$

Entender $\varepsilon$ es lo mismo que hacerlo mod $p$ !! y la derecha es 0 mod $p$ !!



**Lema:** Si $f(z) = \sum_{n\geq 0} \frac{a_n}{n!} z^n$ $\quad g(z) = \sum_{n\geq 0} \frac{b_n}{n!} z^n$

y $p \mid (a_0, \dots, a_{p-1}) \Rightarrow$ $\quad f(z)g(z) = \sum C_n z^n$

es tal que $C_n = p\frac{A_n}{B_n}$ $\quad p \nmid B_n$ $\quad n = 0, \dots, p-1$.

**Demostración** $\quad \sum_{n\geq 0} \left( \sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} \right) z^n$ $\quad$ si $n \leq p-1$

$p \nmid k!$, $p \nmid (n-k)!$

$\Rightarrow p\frac{A}{B}$

$$\sum_{n\geq 0} \frac{p a_n}{n!} x^n \qquad \sum_{n\geq 0} \frac{b_n}{n!} x^n$$

$$\sum \left( \sum_{n\leq N} \frac{a_n}{n!} \frac{b_{N-n}}{(N-n)!} \right) x^N \qquad N \leq p-1$$

$$p \nmid n! \; (N-n)!$$

$$\varepsilon = 1 \qquad S(1,p) = \sum \left(\frac{N}{p}\right) e^{2\pi i \frac{N}{p}}$$

$$S(x) = \sum_{N=1}^{p-1} \chi(N) e^{\frac{2\pi i N}{p}} x^N - \varepsilon \prod_{j=1}^{\frac{p-1}{2}} \left( x^{(2j-1)} - x^{-(2j-1)} \right)$$

$$f(x) = \sum_{j=1}^{p-1} \chi(j) x^j - \varepsilon \prod_{j=1}^{\frac{p-1}{2}} \left( x^{(2j-1)} - x^{p-(2j-1)} \right)$$

$$f(1) = 0 \qquad f(\zeta) = 0 \qquad x^p - 1 \mid f(x)$$

$f(x)$ es primitivo luego $(x^p-1) h(x) = f(x) \quad h(x) \in \mathbb{Z}[x]$

$$\sum \chi(j) e^{zj} - \varepsilon \prod_{j=1}^{\frac{p-1}{2}} \left( e^{(2j-1)z} - e^{(p-(2j-1))z} \right) = (e^{zp}-1) h(e^z)$$

Por otro lado

$$\sum_{j=1}^{p-1} \chi(j) \sum_{N=0}^{\infty} \frac{(jz)^N}{N!}$$

y $e^{(2j-1)z} - e^{(p-(2j-1))z} = \sum_{n\geq 1} a_{n,j} z^n = a_{1,j} z + a_{2,j} z^2 + \cdots$

luego $\prod_{j=1}^{\frac{p-1}{2}} \left( e^{(2j-1)z} - e^{(p-(2j-1))z} \right) = A_{\frac{p-1}{2}} z^{\frac{p-1}{2}} + \cdots$

$$a_{1,j} = (2j-1) - (p-(2j-1)) = 4j - 2 - p$$

Por tanto mod $p$

$$\frac{1}{\left(\frac{p-1}{2}\right)!} \sum_{j=1}^{p-1} \chi(j)\, j^{\frac{p-1}{2}} - \varepsilon \prod_{j=1}^{\frac{p-1}{2}} (4j-2-p) = p\,\frac{A}{B}$$

$$\sum_{j=1}^{p-1} \chi(j)\, j^{\frac{p-1}{2}} \equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{j=1}^{\frac{p-1}{2}} (4j-2) \qquad (p)$$

$$\sum_{j=1}^{p-1} \chi(j)^2 = p-1 \qquad = \varepsilon \,(1\,2\,3 \cdots \tfrac{p-1}{2})\, 2^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} (2j-1)$$

$$= \varepsilon\,(p-1)! \equiv -\varepsilon \qquad (p)$$

$\square$

La relación entre las sumas de Gauss y los polinomios ciclotómicos se hace más evidente cuando en vez de todo el polinomio, consideramos solo aquel que corresponde a residuos cuadráticos.

Ciclotómica

Se puede hacer al revés una vez que tenemos información sobre las sumas de Gauss podemos deducir información sobre polin. ciclot. observar que la relación entre $S(1,p)$ y $\zeta^{R}, \zeta^{N}$

$f(x) = 1 + \cdots + x^{p-1}$ es el polin. ciclot.

Sea $\zeta = e^{\frac{2\pi i}{p}}$. Entonces $1 + \cdots + \zeta^{p-1} = 0$

De ambos hechos deducimos que si

$$F(\zeta) = \sum_{n \geq 0} a_n \zeta^n \qquad a_n \in \mathbb{Z},$$ entonces

$$F(\zeta) = \sum_{i=1}^{p-1} A_i \zeta^i \quad \text{de manera única}$$

por ejemplo si $\zeta = e^{2\pi i/3}$

$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$

$\zeta^2 + \zeta^3 + \cdots + \zeta^6 = 0$

$\zeta^6 = -\zeta^2 - \zeta^3 - \zeta^4 - \zeta^5$

$1 = -\zeta^4 - \zeta^3 - \zeta^2 - \zeta$

$1 + \zeta^{46} = -\zeta - 2\zeta^2 - 2\zeta^3 - 2\zeta^4 - \zeta^5$

Por ejemplo $\zeta = e^{2\pi i/3}$ $\quad 1+\zeta^4$

$1+\zeta+\zeta^2=0$ $\quad -\zeta-\zeta^2=1$

$\zeta^2+\zeta^3+\zeta^4=0$ $\quad -\zeta^2-\zeta^3=\zeta^4$ $\Rightarrow$ $\boxed{-\zeta-2\zeta^2-\zeta^3=1+\zeta^4}$

$1+\zeta^4=-\zeta^2$

$\zeta^3=-\zeta-\zeta^2 \Rightarrow -\zeta^2$

$1+\zeta^2+\zeta^4=0$

Es única pues si

$$F(\zeta)=\sum_{i=1}^{p-1} A_i\zeta^i=\sum_{i=1}^{p-1} B_i\zeta^i \quad \text{entonces}$$

$$\sum_{i=1}^{p-1}(A_i-B_i)\zeta^i=0 \quad \text{y } \zeta \text{ satisface}$$

un polinomio de grado menor que $p-1$ lo cual no es posible que $f$ es irred. (polinomio mínimo divide a $f$). es el mismo polinomio si cambio $\zeta$ por $\zeta^g$

Teorema: Ejemplos de dichos polinomios

son $\eta_1=F(\zeta)=\sum_R \zeta^R$, $G(\zeta)=\sum_N \zeta^N=\eta_0$

se puede calcular explícitamente su valor gracias a $S(1,p)$. Efectivamente $\eta_1=\frac{-1+\varepsilon p^{1/2}}{2}$

$$\eta_0=\frac{-1-\varepsilon p^{1/2}}{2}$$

Dichos polinomios tienen la prop de que $F(\zeta) = F(\zeta^R)$ y en realidad definen cualquier polinomio con esa prop en el siguiente sentido para todo $R$.

Proposición: Si $F(\zeta) = F(\zeta^R)$ entonces

$$F(\zeta) = A_1 \eta_1 + A_0 \eta_0$$

donde $A_1, A_0$ son enteros.

$$\sum A_i \zeta^i = \sum A_j \zeta^{Rj}$$

$$Rj \equiv i \bmod p \Rightarrow A_j = A_i$$

para cada $jRp$ $\exists\ j^{-1} R p$ tal que $jj^{-1} \equiv 1\ p$

Luego $A_j = A_1$ Para todo $jRp$.

Además Si $j_0 N p$ $\exists$ ~~$R$~~ $R$ tal que

$$Rj_0 = j_0^{\cdot}$$ $j_0 j^{-1}$ luego.

$$A_j = A_{j_0}$$ ⊠

Es importante observar que si cambio $\zeta$ por $\zeta^q$ el polinomio la exigencia no varían $A_0, A_1$

*

Un primer ejemplo. Consideraremos

Corolario: Sea $F(x,y)$ tal que $F(x,y^R) = F(x,y)$

entonces $F(x,y) = A_1(x)\eta_1 + A_0(x)\eta_0$

$$F(0,y) = A_1(0)\eta_1 + A_0(0)\eta_0$$

$$F(d,y) = A_1(d)\eta_1 + A_0(d)\eta_0$$

$A_1(x) = A_{10}$, etc

$A_0(x) = A_{00}$, etc

luego el Polin $F(x) = A_1(x)\eta_1 + A_0\eta_0$

para dos puntos luego son iguales.

Teorema: $F(x,y) = \Pi(x-y^R) = \frac{1}{2}\left(Y(x) - \varepsilon\rho^{1/2}Z(x)\right)$

$G(x,y) = \Pi(x-y^N) = \frac{1}{2}\left(Y(x) + \varepsilon\rho^{1/2}Z(x)\right)$

$\eta_1(y^g) = \eta_0(y)$ luego $F(x,y^g) =$

$\eta_0(y^g) = \eta_1(y)$ $\quad = A_1(x)\eta_0(y^g) + A_0(x)\eta_0(y^g)$

$\quad \| \quad = A_1(x)\eta_0(y) + A_0(x)\eta_1(y)$

$G(x,y) =$

Cambia $\eta_0$ por $\eta_1$ es $\varepsilon$ por $-\varepsilon$

Sabemos $4p = Y(1)^2 - \varepsilon^2 p Z(1)^2$ $\quad \varepsilon = i$

$$4 = pY(1)^2 + Z(1)^2$$

y $Z(1) \neq 0$ pues $p$ no es un cuadrado

ejemplo $\zeta = e^{2\pi i/3}$

Ya podemos probar el teorema de Dirichlet

Teorema: $an+b$ representa infinitos primos $\Leftrightarrow (a,b)=1$

i) $a = q$ primo.

Sabemos que $\sum_{\chi} \chi(n) = \begin{cases} 0 & n \not\equiv 1 \ (q) \\ q-1 & n \equiv 1 \ (q) \end{cases}$

Sea $L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$

Analítica y $\neq 0$ en $\sigma > 1$. Por tanto

$$\lg L(\chi, s) = \sum_{p^m} \frac{\chi(p^m)}{p^{ms}}$$

Multiplico por $\chi(b)$ y sumo en $\chi$

$$\frac{1}{\varphi-1}\sum_{\chi}\chi(b^{-1})\log L(\chi,s)=\sum_{p^m}\frac{1}{p^{ms}}\sum_{\chi}\chi(b^{-1}p^m)$$

$$=\sum_{p^m\equiv b(q)}\frac{1}{p^{ms}}=\sum_{p\equiv b(q)}\frac{1}{p^s}+\underbrace{\sum_{m\geq 2}\frac{1}{p^{ms}}}_{\text{convergente}}$$

Tenemos que probar que la izda tiene a infinito cuando $s\to 1$

Si $\chi=\chi_0$ entonces

$$L(\chi_0,s)=\sum_{q\nmid n}\frac{1}{n^s}=\prod_{p\neq q}\left(1-\frac{1}{p^s}\right)^{-1}$$

$$=\left(1-\frac{1}{q^s}\right)\zeta(s)\longrightarrow_{s\to 1}\infty$$

Por otra parte $L(\chi,s)=\sum_{n\geq 1}\frac{\chi(n)}{n^s}$

es convergente en $s>0$ luego es analítica en $s>0$ Por tanto $\lim_{s\to 1} L(\chi,s)=L(\chi,1)$

Si no quiero que sea $\infty$ tengo que probar

$L(\chi,1) = \sum_n \frac{\chi(n)}{n}$ no es cero cuando

$\chi \neq \chi_0$. ~~Ahora bien Consideramos~~

$$\prod \sum \log L(\chi,s) = \log \prod L(\chi,s)$$

Supongamos que $L(\chi,1)=0$ y $\chi$ es complejo

Entonces $L(\bar{\chi},1) = \overline{L(\chi,1)} = 0$ Pero si $s>1$

$$\log L(\chi,s) = \sum_{p^m s} \frac{\chi(p^m)}{p^{ms}}$$

$$= \sum_{p^m \equiv 1 (q)} \frac{1}{p^{ms}} \geq 0$$

$$\prod_{\chi} L(\chi,s) \geq 1$$

$$L(\chi_0,s)\, L(\chi,s)\, L(\bar{\chi},s) \geq 1$$

$$L(\chi,s) = (s-1)\sum_{n\geq 0} a_n (s-1)^n$$

$$L(\bar{\chi},s) = (s-1)\sum_{n\geq 0} b_n (s-1)^n$$

$$L(\chi_0,s) = \frac{c}{s-1} + \sum_{n\geq 0} c_n (s-1)^n$$

luego ~~$\lim L(\chi,s)\,L(\bar{\chi},s)\,L(\chi_0,s)$~~

$$\prod L(\chi,s) \xrightarrow[s\to 1]{} 0$$

pero $$\sum \log L(\chi,s) = \sum_{p^m \equiv 1 (q)} \frac{1}{p^{ms}} \geq 0$$

luego $$\prod L(\chi,s) \geq 1$$ ⊠

Falta por demostrar que $L(\chi,1)\neq 0$

si $\chi$ es el caracter real $\chi(n) = \left(\frac{n}{q}\right)$

(Los caracteres reales y primitivos eran símbolo de Legendre)

$$L(\chi,1) = \sum_{n\geq 1} \frac{\chi(n)\left(\frac{n}{q}\right)}{n}$$

~~$S(N,q) = \left(\frac{N}{q}\right) S(N,q)$~~

luego $\left(\frac{N}{q}\right) S(\chi) = \left(\frac{N}{q}\right) S(N,\chi)$ luego

$$L(\chi,1) = \frac{1}{S(\chi)} \sum_{n \geq 1} \frac{\sum_{N=1}^{q-1} \left(\frac{N}{q}\right) e^{2\pi i \frac{kn}{q}}}{n}$$

$$= \frac{1}{S(\chi)} \sum_{N=1}^{q-1} \left(\frac{N}{q}\right) \sum_{n \geq 1} \frac{e^{2\pi i \frac{Nn}{q}}}{n}$$

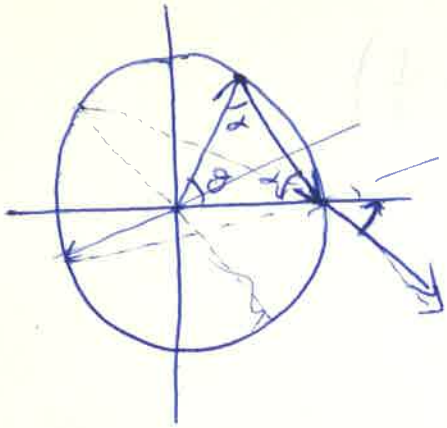
$$= \frac{-1}{S(\chi)} \sum_{N=1}^{q-1} \left(\frac{N}{q}\right) \log\left|1 - e^{2\pi i \frac{N}{q}}\right)$$

¿Que logaritmo es $N \to i\infty \to 0$

$$\log 1 = 0$$

$$\log|1| + i \arg 1 \qquad -\pi < \theta < \pi$$

$$= \frac{1}{S(\chi)} \sum_{N=1}^{q-1} \left(\frac{N}{q}\right) \log\left(1 - \cos\frac{2\pi N}{q} + i \operatorname{sen}\frac{2\pi N}{q}\right)$$



$\theta = \frac{2\pi N}{q}$

$\theta < \frac{\pi}{2}$

$\theta > \pi/2$

$2\alpha + \theta = \pi$

$\alpha = \frac{\pi - \theta}{2}$

$\alpha =$

Si $\theta < \pi$ angulo negativo

Si $\theta > \pi$ angulo positivo

luego a $\frac{\theta}{2} - \frac{\pi}{2}$.

$$\sqrt{\left(1 - \cos\frac{2\pi N}{q}\right)^2 + \operatorname{sen}^2\frac{2\pi N}{q}} =$$

$\cos^2\alpha + \operatorname{sen}^2\alpha = 1$

$\cos^2\alpha - \operatorname{sen}^2\alpha = \cos 2\alpha$

$$= \sqrt{2 - 2\cos\frac{2\pi N}{q}}$$

$$= \sqrt{4\operatorname{sen}^2\frac{\pi N}{q}} = 2\operatorname{sen}\frac{\pi N}{q} \text{ positivo}$$

luego queda

$$-\frac{1}{S(\chi)} \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \lg\left(2 \operatorname{sen} \frac{\pi n}{q}\right) + i\left(\frac{\pi n}{q} - \frac{\pi}{2}\right)$$

es una suma finita !!

$q \equiv 3 (4)$ entonces $S(\chi)$ es imaginario puro luego

$$L(\chi, 1) = \frac{-\pi i}{q S(\chi)} \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) n$$

$$= \frac{-\pi}{q^{3/2}} \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) n$$

Hay que probar que $\neq 0$ $\quad q = 7$

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 1 | 4 | 2 | 2 | 4 | 1 |

$$\frac{\pi}{7^{3/2}} (1 + 2 - 3 + 4 - 5 - 6)$$

$$= \frac{\pi}{7^{3/2}} (-7) = + \frac{\pi}{7^{1/2}} \quad \blacksquare \; !!$$

$e_1 \neq 0$ ~~pues $q \equiv 3 \ (4)$ luego~~

$q \equiv 3 \ (4)$ luego $(-1)^N q$

$$\sum_{N=1}^{q-1} \left(\frac{N}{q}\right) N = \sum_{N=1}^{\frac{q-1}{2}} \left(\frac{N}{q}\right) N + \sum_{\frac{q+1}{2}}^{q-1} \left(\frac{N}{q}\right) N$$

$$= \sum_{N=1}^{\frac{q-1}{2}} \left(\frac{N}{q}\right) N + \sum_{\frac{q+1}{2}}^{q-1} \left(\frac{N}{q}\right) (q-N)$$

$$= 2 \sum_{N=1}^{\frac{q-1}{2}} \left(\frac{N}{q}\right) - q \sum_{1}^{\frac{q-1}{2}} \left(\frac{N}{q}\right)$$

---

Si $q$ es un entero impar

pues $-1 \equiv 1 \ (2)$ luego

$$\equiv \sum_{N=1}^{q-1} N = \frac{(q-1)q}{2} \text{ impar} \neq 0 \ !!$$

$q \equiv 1 \ (4)$

$$L(\chi, 1) = \frac{-1}{S(\chi)} \sum_{N=1}^{q-1} \left(\frac{N}{q}\right) \lg \left(2 \operatorname{Sen} \frac{\pi N}{q}\right)$$

$$= \frac{-1}{S(\chi)} \lg \prod_{N} \frac{\operatorname{Sen}(\pi R/q)}{\operatorname{Sen} \pi N/q}$$

$$= \frac{-1}{S(\chi)}$$

$$\frac{\prod_R \left(e^{\frac{i\pi R}{q}} - e^{-\frac{i\pi R}{q}}\right)}{\prod_N \left(e^{\frac{i\pi N}{q}} - e^{-\frac{i\pi N}{q}}\right)} = \frac{\prod_R e^{-\frac{i\pi R}{q}} \prod_R \left(e^{\frac{2\pi i R}{q}} - 1\right)}{\prod_N e^{-\frac{i\pi N}{q}} \prod_N \left(e^{\frac{2\pi i N}{q}} - 1\right)}$$

$$F(X,Y) = \Pi(X - \zeta^R) \qquad F(1,1) \neq 0$$
$$G(X,Y) = \Pi(X - \zeta^N) \qquad G(1,1)$$

$$\sum \left(\frac{R}{q}\right) R = 0 \quad !!$$

$m$ = compuesto  De la misma forma tenemos

que prueba $L(\chi, 1) \neq 0$ para $\chi$ real.

Sea $\psi(s) = \dfrac{L(\chi, s)\, L(\chi_0, s)}{L(\chi_0, 2s)}$ analítica en $s > \frac{1}{2}$

$s > 1$

$$\prod \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \prod \left(1 - \frac{1}{p^s}\right)^{-1}$$
$$\left(1 - \frac{1}{p^{2s}}\right)^{-1}$$

$\chi(p) = -1$

$$= \prod_{\chi(p)=1} \frac{\left(1 + \frac{1}{p^s}\right)}{\left(1 - \frac{1}{p^s}\right)} = \prod_{\chi(p)=1} \left(1 + \frac{1}{p^s}\right)\left(1 + \frac{1}{p^{2s}} + \cdots\right)$$

si no hay $p$ tal que $\chi_p \neq 1$ entonces vale 1 pero $\lim_{s \to 1/2}$ $\to 0$ no puede ser

$$\psi(s) = \sum_{n \geq 0} \frac{b_n}{n!} (s-2)^n \qquad \text{radio } r = 3/2$$

~~$a_n = \psi^{(n)}(2)$~~ $\qquad \psi(s) = \sum_n \frac{a_n}{n^s} \qquad a_n \geq 0$

$a_1 = 1$

$$\psi^{(k)}(s) = \sum_n a_n e^{-s \log n}$$

$$(-1)^k (\log n)^k a_n e^{-s \log n}$$

$$\sum \frac{\log n^k a_n}{n!} (2-s)^n \geq 1 \quad \text{no puede ser}$$

# Aproximación diofántica

- Cambiamos de tema. Y volvemos un poco al principio. Aritmética trata de entender las propiedades de los números enteros y racionales en clear definidos sin necesidad del paso al límite y por tanto "discretos"

¿Pero es necesario pasar al límite? es clear existe algún ℚ que no sea racional?

**Teorema:** $\forall$ sea $K \in \mathbb{Q}$. $\sqrt{N}$ es racional $\Leftrightarrow$ $N \in \mathbb{Q}^2$. $N = \left(\frac{M}{n}\right)^2$

$\sqrt{N} = \frac{a}{b} \Rightarrow Pb^2 = qa^2$ $\quad (a,b)=(p,q)=1$

luego $a^2/p$ $\quad b^2/q$ $\quad p = a^2 r$ $\quad q = b^2 s$ $\quad$ igualando $r=s$

y $\frac{p}{q} = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2$

Definición $\left(\frac{a}{b}\right)^2 = K$

Corolario $\sqrt{2}$ es irracional

$$2 = \frac{p^2}{q^2}$$

Teorema $\sqrt{N} \in \mathbb{Q} \Leftrightarrow N \in \mathbb{Q}^2$

$\sqrt{N} = \frac{a}{b}$ por def $\left(\frac{a}{b}\right)^2 = K$

Corolario $\sqrt{2}$ es irracional

$2 = \frac{p^2}{q^2}$ $\quad (p,q) = 1 \Rightarrow 2q^2 = p^2$

$2 | p \Rightarrow 4 | p^2 \Rightarrow 2 | q$ que no puede ser

La pregunte es ¿Como distinguirlos?

La primera forma de distinguir un numero irracional es mediante su representación decimal.

**Teorema** Todo $\alpha \in \mathbb{R}$ se puede representar de manera única como $\alpha = \sum_{i \leq N} a_i 10^i$

con $0 \leq a_i \leq 9$. ~~$a_i = $ todos tal que~~

Demostración $10^N \leq \alpha < 10^{N+1}$

$$1 \leq \left[\frac{\alpha}{10^N}\right] < 10 = a_N$$

$$\alpha = a_N 10^N + r \qquad r < 10^N$$

$$\alpha = \sum_{M=0}^{N} a_M 10^M + r \qquad 0 < r < 1$$

$$0 \leq [10r] \leq 9 \qquad 10r = b_1 + r_1 \qquad 0 < r_0 < 1$$

$$r = \frac{b_1}{10} + \frac{r_1}{10}$$

$$r = \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{r_2}{10^2} \qquad 10 r_0 = b_2 + r_2$$

$$r = \sum_{i=1}^{N} b_i 10^{-i} +$$

La serie es convergente y como

$$\sum_{i=M}^{\infty} b_i 10^{-i} < \varepsilon \quad \text{converge a } \alpha$$

$$\left| \alpha - \sum_{i=1}^{N} b_i 10^{-i} \right| < \varepsilon \qquad \blacksquare$$

**Teorema:** ~~$b_i$ no puede ser $9 \ \forall \ i > I$~~

$\forall\ I$ existe $b_i \neq 9 \quad i > I$

Si todos son 9 en todos

$$\frac{r_N}{10^{N+1}} = \sum_{i>N} b_i 10^{-i} = 9 \frac{1}{10^{N+1}} \left( \frac{1}{1-\frac{1}{10}} \right) = \frac{1}{10^N}$$

y $r_N = 1$ que no puede ser. $\blacksquare$

**Teorema:** La expresión es única. $b_j \neq a_i$

$$\sum_{i \geq j} a_i 10^{-i} = \sum_{i \geq j} b_i 10^{-i}$$

$$\sum_{i \geq j} (a_i - b_i) 10^{-i} = 0$$

$$(a_j - b_j)10^{-j} + \sum_{i \geq j+1} (a_i - b_i)10^{-i} = 0$$

$$\Longleftrightarrow \qquad |a_i - b_i| \leq 9$$

$$(a_j - b_j)10^{-j} - \sum_{i \geq j+1} |a_i - b_i|10^{-i} \geq$$

$$(a_j - b_j)10^{-j} - \frac{1}{10^j} \geq 0 \quad \text{igualdad si todos}$$

son $-9$ $a_j - b_j$ es decir $b_j = 9 \ \forall j$ no puede ser.

Teor Definición: Decimos que $\alpha$ tiene una expresión periódica pura si

$b_{n+j} = b_j$ para todo $j \geq 1$

mixta si $b_{n+j} = b_j$ para todo $j \geq m$

Teorema $\alpha$ es racional $\Leftrightarrow$ $\alpha$ es periódico ó $b_j = 0 \ \forall j > 1$

Si el dato es claramente racional

Si es periódico $10^{m+n}\alpha - 10^m\alpha = M \in \mathbb{Z}$

luego $\alpha = \dfrac{M}{10^m(10^n-1)}$ ☒

Supongamos que es racional

$$\alpha = \frac{p}{q}$$

y sea $(q,10)=1$. Entonces $10^{\varphi(q)} - 1 \equiv 0 \,(q)$

luego $(10^{\varphi(q)}-1)\alpha = \dfrac{10^{\varphi(q)}-1}{q}\cdot p \in \mathbb{Z} \quad 1 \le M < 10^{\varphi(q)}$


$$10^{\varphi(q)}\alpha = M + \alpha$$

$$\alpha = \frac{M}{10^{\varphi(q)}} + \frac{\alpha}{10^{\varphi(q)}} = \frac{M}{10^{\varphi(q)}} + \frac{M}{10^{2\varphi(q)}} + \cdots$$

$$= M \sum_{r\ge 1} \frac{1}{10^{\varphi(q)r}} = \sum_{r\ge 1}$$

$$M = \sum_{i=0}^{\varphi(q)-1} a_i 10^i$$

$$\sum_{i=0}^{\varphi(q)-1} \frac{a_i}{10^{\varphi(q)-i}} = \sum_{1}^{\varphi(q)} \frac{a_{\varphi(q)-i}}{10^{i}} + \sum_{i=1}^{\varphi(q)} \frac{a_{\varphi(q)-i}}{10^{\varphi(q)+i}}$$

Si $(q,10)>1$ entonces $\alpha = \frac{p}{10^m q}$ $(q,10)=1$

~~$\alpha 10^m = \beta = [\beta] + \{\beta\}$~~ $p = kq + r$

$\beta = N + \frac{r}{q}$

Sin embargo, no todos los numeros aparecen de manera natural con su expresión decimal. De hecho nunca sabremos toda la expresión decimal de un irracional. Luego no es muy útil! ~~Sin~~ El metodo que seguiremos es ver como de lejos esta un numero de ser racional es decir $|\alpha - \frac{n}{q}|$

Sorprendentemente, cuanto mejor es la aproximación más lejos está de ser racional. Vamos a ver la "discreción" de $\mathbb{Q}$ en $\mathbb{R}$, por ser discreto, está lejos de otro, por ser discreto, está lejos

$$\left|\frac{a}{b} - \frac{m}{n}\right| = \frac{|an - bm|}{bn} > \frac{1}{bn}$$

mientras que hemos visto que los racionales llenan $\mathbb{R}$ luego de un irracional estará cerca como queramos. La definición de lejos y cerca es en realidad la misma

$$|\alpha - \sum_{i=1}^{N\alpha} \frac{q_i}{10^i}| < \frac{1}{10^{N\alpha}} \qquad 10^n \sum_{i=1}^{N\alpha} \frac{q_i}{10^i} \in \mathbb{N}$$

luego $\sum \frac{q_i}{10^i} = \frac{P}{10^N}$

Para todo real existe $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{q_n}$

no es suficiente, para distinguir

hemos usado unas pocas fracciones, las de denominador 10. Si usamos todas obtendremos mejor aproximación.

## Fracciones de Farey

Definimos $F_N = \left\{ \frac{a}{b} , (a,b)=1 \; 1 \le b \le N \right\}$ $a<b$

Todas las fracciones irreducibles de denominador $\le N$ y ~~con tu~~ ordenadas según tamaño

$\frac{1}{2}$

$\frac{1}{3}\ \frac{1}{2}\ \frac{2}{3}$

$\frac{1}{4}\ \frac{1}{3}\ \frac{1}{2}\ \frac{2}{3}\ \frac{3}{4}$

$\frac{1}{5}\ \frac{1}{4}\ \frac{1}{3}\ \frac{2}{5}\ \frac{1}{2}\ \frac{3}{5}\ \frac{2}{3}\ \frac{3}{4}\ \frac{4}{5}$

Ya hemos visto en 6 desde que hay $\sim \frac{3}{\pi^2} N^2$ de estas fracciones luego


la distancia entre ellas es $\ll \frac{1}{N^2}$ $\left|\alpha - \frac{p_n}{q_n}\right| \ge \frac{1}{N^2}$

Para demostrarlo vemos propiedades de $F(N)$

**Lema:** Sean $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}} \in F(N)$ consec. entonces

$q_n \neq q_{n+1}$

$$\frac{p_n}{q_n} < \frac{p_n}{q_n - 1} < \frac{p_{n+1}}{q_n} \leq \frac{p_{n+1}}{q_n}$$

$$p_n q_n < p_n q_n - p_n + q_n - 1$$

$$q_n - p_n \quad 1 < q_n - p_n$$

**Teorema Lema:** $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ consec. $\Rightarrow q_n + q_{n+1} > N$

$$\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}} \Rightarrow p_{n+1} q_n - p_n q_{n+1} = 1$$

Sea $-y p_n + x q_n = 1$

$$x = x_0 + t p_n$$
$$y = y_0 + t q_n$$

Sea $N - q_n < y \leq N$

suponganos que $\frac{x}{y}$ no es lo siguiente a $\frac{p_n}{q_n}$

$$\frac{1}{y q_n} = \frac{x}{y} - \frac{p_n}{q_n} = \frac{x}{y} - \frac{p_{n+1}}{q_{n+1}} + \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \geq \frac{1}{y q_{n+1}} + \frac{1}{q_n q_{n+1}} = \frac{q_n + y}{y q_n q_{n+1}}$$

$> \frac{1}{y q_n}$

lo más ~~que~~ pequeño posible a distancia

Teorema: si $\frac{P_n}{q_n}$ $\frac{P_{n+1}}{q_{n+1}}$ $\frac{P_{n+2}}{q_{n+2}}$ cerca

$$\Rightarrow \frac{P_{n+1}}{q_{n+1}} = \frac{P_n + P_{n+2}}{q_n + q_{n+2}}$$

Consecuencia del anterior.

Obtener son equiv. ~~Cierto~~ $\Leftarrow$ Cierto para

$F_{N-1}$ $\frac{P_n}{q_n}$ $\frac{q}{N}$ $\frac{P_{n+1}}{q_{n+1}}$

$$P_n + P_{n+1} = \lambda a \qquad \text{pero } q_n \text{ y } q_{n+1} < N$$

$$q_n + q_{n+1} = \lambda N$$

luego $\lambda = 1$ de donde se deduce el resultado (*)

Teorema $\alpha$ es irracional $\Leftrightarrow$ existen infinitas fracciones tal que $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{q_n^2}$

Si $\alpha = \frac{a}{b}$ $\quad \left|\frac{a}{b} - \frac{p_n}{q_n}\right| > \frac{1}{b q_n} > \frac{1}{q_n^2}$

si $q_n > b$ luego como mucho hay $F(b)$.

Si es irracional $\quad \frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$

luego $\quad \alpha - \frac{p_n}{q_n} < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$ ⊠

Para cada $N$ hay una fracción distinta y siempre hay una entre medias $\frac{p_n + p_{n+1}}{q_n + q_{n+1}}$ ⊠

Tenemos así el primer método para distinguir irracionales. De la forma

Teorema: Existe una sucesión tal que $|b_n \alpha - a_n| \xrightarrow[n\to\infty]{} 0$ $\Leftrightarrow$ $\alpha$ es irracional.

Si $\alpha = \frac{a}{b}$ entonces

$$\left|b_n \frac{a}{b} - a_n\right| \geq \frac{1}{b} > 0$$

en caso contrario el resultado se deduce del teorema anterior pues $q_n \longrightarrow \infty$.

Ejemplo: $e$ es irracional

$$e = \sum_{n\geq 0} \frac{1}{n!}$$

$$\left| N!\, e - K! \sum_{n\leq N} \frac{1}{n!} \right| = N! \sum_{n>K} \frac{1}{n!}$$

si $n \geq N+2$ entonces ~~$\frac{N!}{n!} \leq \frac{1}{N(N-1)}$~~

$$n! \geq n(n-1)\,N! \quad \text{luego}$$

$$\leq \frac{1}{N+1} + \sum_{n\geq N+2} \frac{1}{n(n-1)} = \frac{1}{N+1} + \frac{1}{N+2} \longrightarrow 0.$$

El método es útil cuando el nº se aproxima por una serie de rapido decrecimiento. $\sum_{n\geq 0} \frac{a_n}{b_n} = \alpha$

$$a_n b_1 \cdots b_{n-1} = o(b_n)$$

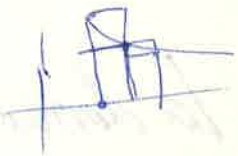
entonces $$b_1 \cdots b_{N-1}\,\alpha - b_1 \cdots b_{N-1} \sum_{1}^{N-1} \frac{a_n}{b_n} = \sum_{n\geq N} \frac{a_n}{b_n} (b_1 \cdots b_{N-1})$$

$$\frac{b_1 \cdots b_{N-1} a_n}{b_n} \leq b_1 \cdots b_{n-1} \frac{a_n}{b_N \cdots b_{n-1} b_n} < \frac{\varepsilon\, b_n}{b_N \cdots b_{n-1}} < \varepsilon \sum_{n\geq N} \frac{1}{b_{n-1}} \longrightarrow 0$$

Sin embargo con todo los nº irrac. se aproximan de esta forma

$$\zeta(2) = \sum_{n\geq 1} \frac{1}{n^2}$$

$$(N!)^2 \zeta(2) - (N!)^2 \sum_{n\leq N} \frac{1}{n^2} = (N!)^2 \sum_{n>N} \frac{1}{n^2} > \frac{(N!)^2}{N+1} \not\to 0$$



$$\sum_{n\geq N+1} \frac{1}{n^2} > \int_{N+1}^{\infty} \frac{1}{t^2} dt = \frac{1}{N+1}$$

De hecho probar que $\zeta(2)$ es irracional fue uno de los problemas de preocupación de todo el siglo 17. Ahora En realidad se sabía el interés era incluso el hecho de saber cual era su suma $\zeta(2) = \frac{\pi^2}{6}$. Queremos probar que $\pi$ es irrac en mas debil. Fijaros que si $\pi = \frac{a}{b} \Rightarrow \zeta(2) = \frac{c}{d}$ pero no al revés $(\sqrt{2})^2$.

$\pi$ es irracional: Vamos a usar la definición
- el menor número
En concreto usaremos que $\text{Sen}(\pi) = 0$ y tal que

$$\text{Sen}'(x) = \cos x \qquad \text{Sen}''x = -\text{Sen}\,x$$

$$\text{Sen}'' + \text{Sen} = 0$$

$\int_0^{\pi} f(x) \operatorname{Sen} x$ entero en $0, \pi$ será entero si Además $f(x)$ es muy pequeño no puede ser un entero $< 1$. Que funcion tiene Valores enteros en $\pi := \frac{a}{b}$. $(x(a-bx))^n$ entera en $0, \pi$

La derivada de una función así es del mismo estilo

$$f(x) = \sum_{j}^{n} \binom{n}{j} a^{n-j} (-1)^j b^j x^{n+j}$$

$$= \sum_{n}^{2n} \binom{n}{j-n} a^{2n-j} (-1)^{j-n} b^{j-n} x^j$$

$$f^{(k)}(0) = k! \binom{n}{k-n} a^{2n-k} (-1)^{k-n} b^{k-n}$$

$$= \binom{k}{n} \frac{n!^2}{(2n-k)!}$$

Luego $\frac{1}{n!} f^{(k)}(0)$ es entero !!

$$g(y) = f\left(\frac{a-y}{b}\right) = \frac{1}{b^n} y^n (a-y)^n$$

$$= \frac{1}{b^n} \sum_{n}^{2n} \binom{n}{j-n} a^{2n-j} (-1)^{j-n} x^j$$

$$\frac{1}{n!} g^{(k)}(0) = \frac{M}{b^n} \qquad \frac{b^n}{n!} g^{(k)}(0) = M$$

Buscar una función que ella y sus derivadas sean cuales en el 0 es fácil $x^n$ en $\pi$ es fácil $(a-bx)^n$ luego el producto $x^n(a-bx)^n$ también que serán sumas de derivadas pero tiene un problema que no es pequeño

pero $g^{(n)}(y) = \frac{(-1)^n}{b^n} f^{(n)}\left(\frac{a-y}{b}\right)$ luego

$(-1)^n b^n \frac{g^{(n)}(0)}{n!} = \frac{f^{(n)}(\pi)}{n!}$ es entero

luego $f(x) = \frac{x^n (a-bx)^n}{n!}$ $f^{(n)}(0)$ y $f^{(n)}(\pi)$ entero !!

Truco $F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) \cdots (-1)^n f^{(2n)}(x)$

$F''(x) = f^{(2)} - f^{(4)} \cdots - (-1)^n f^{(2n+2)}(x)$

$F + F'' = f$

Por tanto $(F' \operatorname{sen} - F \cos)' = F'' \operatorname{sen} + F' \cos - F' \cos + F \operatorname{sen}$

$= f \operatorname{sen}$

$\int f \operatorname{sen} = F(\pi) + F(0)$ entero

$0 < \int < 1$

pues $f < \frac{(a\pi)^n}{n!} \to 0$

el método se puede extender para probar $\pi^2$ es irrac. no obvio.

Cada número ~~es casi~~ necesita casi un nuevo método. Sin embargo hay muy pocos racionales $\mathbb{Q}$ es contable.

$\exists\, A \to \mathbb{N}$ ~~biyec~~ ~~inyec~~ inyec

Teorema:

Unión contable de conj. contables es contable

$\alpha_{11}\ \alpha_{12}\ \cdots$

$\alpha_{21}\ \alpha_{22}\ \cdots$

$\vdots$

Corolario $\mathbb{Q}$ es contable $\quad \mathbb{Q} \to \mathbb{Z}^2$

$r \to (a,b)$

~~biyect~~ inyect

$\mathbb{Z}^2 = (1,1), (1,2) \cdots$

$(2,1)\ (2,2) \cdots$

$\blacksquare$

Teorema

$\mathbb{R}$ no es contable

Supongamos que sí sea $\alpha_1, \alpha_2, \ldots$ la biyección

$$0' a_{11} a_{12} \ldots$$
$$0' a_{21} a_{22} \ldots$$
$$\vdots$$

$\alpha = 0' b_1 b_2 \ldots$ $\quad b_i \neq a_{ii} \Rightarrow \alpha$ no está en la enumeración. ⊠

De hecho es mucho más radical. Se puede extender la definición de racional mucho y todavía se pueden contar los números que engloba

un rac es una raíz de $a + bx = 0$

Definición: Un $\alpha$ es algebraico si $P(\alpha) = 0$.

Teorema: Los algebraicos son contables cogiendo los polinomios definidos por $P(x) = \sum_{i=0}^{n} a_i x^i$ tal que

$n + |a_1| + \ldots + |a_n| \leq N$ finito luego

$E_1 \cup E_2 \cup \ldots$ unión contable de contables

$\Rightarrow$ contable

a decir $P[\alpha] \in \mathbb{Q}[a]$ cons!!

Es cierto que en una extensión en el sentido de que esos números no son los racionales por ejemplo $x^2-2=0$. De hecho son todos irracionales

Teorema: $F(\alpha)=0$ $\deg F > 1$, $F$ irred. y mónico $\Rightarrow$ $\alpha$ irracional o entero tal que $p \mid a_0$.

$$q^d F\left(\frac{p}{q}\right) = \sum a_i p^i q^{d-i} = a_d p^d + q \sum_{i \le d-1} a_i q^{d-i-1} p^i$$

luego $q \mid a_d \Rightarrow q=1$ y $\frac{p}{q} \in \mathbb{Z}$ ☒ además

p/ $F(p) = \sum_{i=0}^{d} a_i p^i = p \sum_{i=1}^{d} a_i p^{i-1} + a_0$ ☒

---

De menos el hecho de ser algebraicos nos permite aproximar el nº lo mejor posible. Los trascendentes van a ser los que mejor se aproximen Ser raíz de un polinomio da una cierta dependencia con los racionales que los hace ser más difíciles de aproximar

Si son independientes no hay pegas en la aproximación

irred (si no podría ser raíz de un polinomio entero de grado menor)

**Teorema** (Liouville) Sea $F(\alpha)=0$ $\deg \alpha = d > 1$

existe $c$ tal que entonces $\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^d}$ para todo $\frac{p}{q} \in \mathbb{Q}$

Si $p/q \notin [\alpha-1, \alpha+1]$

$$F(x) = \sum_{i=1}^{n} a_i x^i$$

$$\left|F\left(\frac{p}{q}\right) - F(\alpha)\right| = \left|\frac{p}{q} - \alpha\right| |F'(\beta)| \quad \text{con} \quad \beta \in \left(\alpha, \frac{p}{q}\right)$$

$\left[\frac{p}{q}, \alpha\right] \subset (\alpha_1, \alpha_n)$

$\left[\alpha, \frac{p}{q}\right] \subset (\alpha-1, \alpha_n)$

alcanza el máximo

$$\leq \left|\frac{p}{q} - \alpha\right| M$$

$$\left|\frac{p}{q} - \alpha\right| \geq \sum_{i=0}^{d} a_i \frac{p^i}{q^i} = \frac{c}{q^d} \sum_{i=0}^{d} a_i p^i q^{d-i}$$

$$\geq \frac{c}{q^d}$$

# metodo de trascendencia

**Teorema:** Si Para todo $k$ existen infinitos $\frac{p_n}{q_n}$ tal que $\quad 0 < q_n^k \left|\alpha - \frac{p_n}{q_n}\right| \longrightarrow 0$

entonces $\alpha$ es trascendente.

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d} \Rightarrow \quad q^d \left|\alpha - \frac{p}{q}\right| > c'$$

**Corolario:** $\sum_{n\geq 0} \frac{1}{10^{n!}}$ es trascendente

Se sabe que $e$ es trascendente (Gelfond Hoc o Spiro

Lindemann probó $e^\alpha$ $\alpha$ alg $\neq 0$ $\quad e^\alpha$ trascendente

$e^{i\pi} = -1$ luego $\pi$ trascendente

Gelfond Schneider probó decimo de Hilbert

$\alpha^{\beta}$ $\alpha \neq 0,1$ alg $\beta$ irrac $\Rightarrow$ trasc $\quad i^{2i}$

$e^{\pi}$

$\pi^e$ no se sabe

El método, al igual que el que teníamos para decidir irracionalidad, se basa en la rapida aproximación por racionales y la definición de $\pi$ no tiene porque mostrar este hecho.

Así si lo aplicamos a $e$, ni siquiera vale para $e^2$

Teorema: $e$ es trascendente [Cille, Hua, Spivak].

Hermite $c_n e^n + \dots + c_0 = 0$ no tiene sol

Lindemann generaliza el resultado a

$$\alpha_1 e^{\beta_1} + \dots + \alpha_n e^{\beta_n} = 0$$

no tiene sol. si no todos $\alpha_i$ son cero y $\beta_i \neq \beta_j$ algebraicos. $n=2$ $\beta_2 = 0$ $\alpha_1 = 1$

Corolario: $\alpha e^{\beta_1} + \alpha_2 \neq 0$ es decir

$e^\beta$ es trascendente si $\beta \neq 0$ es algebraico.

(1882)

Teorema: $\pi$ es trascendente $e^{\pi i} = -1$ ☒

Este es un problema que venía entretuviendo desde la antigua grecia. En particular los griegos se preguntaron por un cuadrado que tuviese el área del círculo de radio 1 esto es $\sqrt{\pi}$ pero intersección de círculos y rectas es $+ - \cdot \sqrt{}$. en particular algebraico

Gelfond y Schneider generalizaron lo ec a $\alpha^\beta$ es trascendente si ambos son alg $\alpha \neq 0, 1$

↳ Irracional

Corolario: $e^\pi$ trascendente $i^{2i} = e^{-\pi}$ ☒

Si $\frac{1}{\alpha}$ es alg $\Rightarrow q(\frac{1}{\alpha}) = 0 \Rightarrow$ multiplico $\alpha^n$

lo es $\alpha$.

No se sabe si $\pi^e$ ó $\pi + e$ que son si $\pi e$.

La aproximación diofántica al cero y en general?

$$|q_n\alpha - p_n| \longrightarrow 0$$

es que $q_n\alpha = [q_n\alpha] + 0'0\ldots\ldots 0\delta_1$

y si ponemos $\delta' a_1 \ldots a_r$ podremos acercarnos

a ese nº

Teorema: Si $\alpha$ irrac. $\beta \in \mathbb{R}$ existen $\infty$

$x, y$ tal que $|x\alpha - y - \beta| < \frac{3}{x}$

Demos: Sabemos $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$

es decir $\alpha \approx \frac{p_n}{q_n}$

queremos ver $\beta \approx x\alpha - y \approx x\frac{p_n}{q_n} - y = \frac{xp_n - yq_n}{q_n}$

$$\beta = \frac{k_n}{q_n} + \frac{\delta}{2q_n}$$

La pregunta es $\exists\, x, y$ tal que $xp_n - yq_n = N_n$ ?
además quiero $x \approx q_n$ para tener una aprox
en términos de $x$ y no $y$.

Pero $xp_n - yq_n = N_n$ se exige $(p_n, q_n) = 1$

$$\frac{q_n}{2} \le x \le \frac{3}{2} q_n \quad \text{del mismo orden}$$

Si $\alpha = \frac{p_n}{q_n} + \frac{\delta}{q_n^2}$ ~~$|\delta| < 1$~~

$$\beta = \frac{N_n}{q_n} + \frac{\delta'}{2q_n} \qquad |\delta'| < 1$$

$$= \frac{p_n}{q_n} x - y + \frac{\delta'}{2q_n}$$

~~$\alpha x$~~

$$|\alpha x - \beta - y| = \left|\left(\alpha - \frac{p_n}{q_n}\right)x + \frac{\delta'}{2q_n}\right| \le \frac{x}{q_n^2} + \frac{1}{2q_n}$$

$$< \frac{2}{q_n} < \frac{3}{x} \qquad \square$$

hay infinitos pues $q_n \to \infty$ $\quad x \ge q_n/2$ $\quad \square$

Ejemplo probar que $\{n\pi\}$ tiene un 7 en el lugar 77 para infinitos $n$.

$\beta = 0'7$

$|x\pi - y - 0'7| < \frac{3}{x} \longrightarrow 0$

$|x\pi - y| - 0'7 < |x\pi - y - 0'7|$

$|x\pi - y| > 0'7 - \varepsilon_0$

$3 + \varepsilon_0 > \{x\pi\} > 3 + \varepsilon_0$

$2\varepsilon_0 > \{x\pi\} > 0$

Corolario: $\{n\alpha\}$ es denso en $(0,1)$



(Pero como se ~~aproxima~~; distribuye hay más en el centro?

Definición: $a_n \in (0,1)$ está uniformemente distribuida si

$$\lim_{N\to\infty} \frac{\#\{a_n \in I : n \le N\}}{N} = |I|$$

Si definimos $\chi_I(x) = \begin{cases} 0 & x \notin I \\ 1 & x \in I \end{cases}$

$$\sum_{n=1}^{N} \frac{\chi_I(a_n)}{N} = |I| = \int_0^1 \chi_I(x)\,dx$$

$\Rightarrow$ es cierto para funciones escalonadas

Toda función continua se puede aproximar por funciones escalonadas

~~$f_2 \le f \le f_1 + \varepsilon$~~ $f_2 \le f \le f_1$ $\int (f_1 - f_2) \le \varepsilon$

Proposición: $\forall f$ continua $\lim_{N\to\infty} \frac{\sum_{n=1}^{N} f(a_n)}{N} = \int_0^1 f(x)\,dx$

Las funciones continuas basta hacerlo para una base de funciones con por linealidad de la integral. Tal base es ~~por tener~~ las polinomios trigonométricos.

(sirve definición posible gracias)

$$f(x) = \sum_{n=-N}^{N} a_n e^{2\pi i n x}$$

uniformemente $\quad$ Teo (Weyl) $\frac{1}{N}\sum_{n=1}^{N} e^{2\pi i a_m m} \to 0 \quad \forall m \neq 0$ $\Leftrightarrow$ uniformemente

$$\int f(x) = a_0$$

$$\frac{1}{N}\sum_{n=1}^{N} P(x_n) = \sum_{n=-m}^{m} a_n \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i n x_n} \to a_0$$

$\to 0$

sabiendo que sea $\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f_m(x_n) = \int P_m = \int$

de nuevo las cont. aproximan a continuas a trozos

$f_2 \le f \le f_1 \quad \int f_1 - f_2 \le \varepsilon$.

Corolario $\alpha$ irrac $\Leftrightarrow$ $\{n\alpha\}$ está uniformemente distribuida

Si $\alpha$ racional $\alpha = \frac{p}{q}$ sea irreducible

$$\frac{1}{N}\sum_{n=1}^{N} e^{2\pi i n\alpha n} = \frac{e^{2\pi i N\alpha} - e^{2\pi i \alpha}}{N\left(e^{2\pi i \alpha} - 1\right)} \to 0$$

$N \to \infty$

En particular no permite calcular ~~el~~ el valor exacto de sumas, ~~o~~ promedios ~~de la integral~~ a través de integral

~~Calcular~~ Demostrar que $\sum \frac{1}{n^4}$ converge ~~Es lo mismo de medir~~

$\sum_{n=1} \{n\pi\}$ lo mismo

Conjetura: $\alpha$ irracional $\Leftrightarrow$ $\{n\alpha\}$ es en media $= \frac{1}{2}$

$\alpha = \frac{1}{4}$ $\quad \frac{1}{4} \quad \frac{3}{4}$

$\frac{1}{N} \sum_{n=1}^{4N} \{n\alpha\} = \frac{1}{N} \sum_{n=1}^{N} \frac{1}{4} + \frac{1}{N}\left[ N\left(\frac{1}{4} + \frac{1}{2} + \frac{3}{4}\right)\right] = \frac{6}{4}$

$q = 2a+1$ $(5)$ $\quad \sum \frac{(q-1)(q)}{2q} =$ $\quad N-1 \frac{N}{5}$

$\Rightarrow 5 \mid b+1$ $\quad \sum_{n=1}^{N} \{n \frac{q}{5}\} = \frac{N}{5}\left(\frac{1}{5} + \frac{2}{5} + \cdots \frac{5-1}{5}\right) = \frac{(b-1)}{2b} = \frac{1}{2}$

$(q,5)=1$

$b=2$

$\sum_{n=1}^{2r} \{\frac{n}{2}\} = \frac{1}{2} \cdot \frac{N}{2} \left(\frac{2n-1}{2}\right) = \frac{Nq}{2}$

$\sum_{n=1}^{bm+r} \{\frac{n}{b}\} = \frac{1}{N} \sum_{k=0}^{b-1} \sum_{n=1}^{m} \frac{bn+k}{b}$

$\frac{M}{N} \sum_{k=1}^{b} \{\frac{ak}{b}\} \Rightarrow 0$ $\quad \frac{N}{b}\left(\frac{b-1}{2}\right) \to \frac{b-1}{2b} = \frac{1}{2}$

Corolario $\alpha$ es irracional $\Leftrightarrow \{n\alpha\}$ es equidistribuida en media $\frac{1}{2}$.

$$\frac{1}{N}\sum_{n=1}^{N}\{n\alpha\} = \int_0^1 x\,dx = \frac{1}{2}$$

Si $\alpha$ racional $\alpha = \frac{a}{b}$ $\quad m = \left[\frac{N}{b}\right]$

$$\frac{1}{N}\sum_{h=1}^{N}\{n\alpha\} = \frac{1}{N}\sum_{h=1}^{b}\sum_{n=1}^{m}\left\{(mb+h)\frac{a}{b}\right\} + O\left(\frac{1}{N}\right)$$

$$= \frac{1}{N}\sum_{h=1}^{m}\sum_{h=1}^{b}\left\{\frac{ah}{b}\right\} + O\left(\frac{1}{N}\right) \qquad ah \equiv ah' \ (b) \Rightarrow h \equiv h'(b)$$

$$= \frac{m}{Nb}\frac{b(b-1)}{2} + O\left(\frac{1}{N}\right) = \frac{N-\left\{\frac{N}{b}\right\}}{N}\frac{b-1}{2b} + O\left(\frac{1}{N}\right)$$

$$\longrightarrow \frac{b-1}{2b} = \frac{1}{2} \Leftrightarrow b = b-1 \text{ imposible}$$

# Fracciones continuas

Los teoremas de irracionalidad aseguran la existencia de fracciones que aproximan muy bien a los irracionales. Sin embargo, de la definición del nº no tienen porque aparecer dichas fracciones por ejemplo $e^2 = \sum_{n\geq 1} \frac{2^n}{n!}$ pero no es la que mejor aproxima. Vamos a intentar encontrar aquella fracción con la mejor aprox en términos del denominador al nº

~~Si empezamos por~~

Empezemos por un nº racional $\frac{a}{b}$, $(a,b)=1$

suponjamos que $b$ $a<b$. $b = ka + r$. En este caso

$$\frac{a}{b} = \frac{1}{\frac{b}{a}} = \frac{1}{k + \frac{r}{a}} \approx \frac{1}{k}$$

Lema: $\left|\frac{c}{d} - \frac{a}{b}\right| \geq \left|\frac{1}{N} - \frac{a}{b}\right|$ para todo $\frac{c}{d} \in F(N)$

$$\frac{|cb-da|}{bd} = \frac{|a(cN-d)+cr|}{bd} \geq \frac{cr}{bd} \geq \frac{r}{bk}$$

$$\frac{a}{b} =$$

En general $\frac{a}{b} = a_0 + \frac{r_0}{d} = a_0 + \frac{1}{\frac{d}{r_0}} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_0}}$

$a = a_0 b + r_0$

$d = a_1 r_0 + r_1$

$r_0 = a_2 r_1 + r_2$

$= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_2}{r_1}}}$

$r_N = a_{N+2} r_{N+1} + 1$

$= a_0 + \frac{1}{a_1 + \frac{1}{\ddots \; a_n + \frac{1}{a_n}}}$

**Definición:** Se llama fracción continua finita a cada expresión $\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_{n2}]$. ejemplo $\frac{55}{48}$

**Prop:** Todo $r \in \mathbb{Q}$ tiene una única representación en fracción continua. tal que $a_n > 1$ $a_0 \in \mathbb{Z}$ $a_i \in \mathbb{N}$.

**Demos:** Algoritmo de euclides

Observar que $r_{n-2} = a_n r_{n-1} + 1 \Rightarrow \frac{1}{r_{n-1}} = \frac{1}{(r_{n-1}^{-1}) + \frac{1}{1}}$

$$\frac{55}{43} = 1 + \frac{12}{43}$$

$43 = 3 \cdot 12 + 7$
$12 = 7 + 5$
$7 = 5 + 2$
$5 = 2 \cdot 2 + 1$

$$\Rightarrow \quad \frac{55}{43} = 1 + \frac{1}{3 + \frac{7}{12}} = 1 + \frac{1}{3 + \frac{1}{1 + \frac{5}{7}}}$$

$$= 1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}} = [1; 3, 1, 1, 2, 2]$$

$\frac{55}{43}$, se aproxima por $1, \frac{4}{3}, \frac{5}{4}, \frac{9}{7}, \frac{23}{18}, \frac{55}{43}$

Queremos generalizarlo a irracionales. Vamos

$\sqrt{2}$

$$\sqrt{2} = 1 + \alpha = 1 + \frac{1}{\alpha + 2} = 1 + \frac{1}{2 + \frac{1}{2 + \ldots}}$$

$$2 = 1 + \alpha^2 + 2\alpha \qquad \alpha^2 + 2\alpha - 1 = 0$$

$$\alpha + 2 = \frac{1}{\alpha}$$

Así $\sqrt{2} = [1; 2, 2, 2, \ldots]$

Definición. Se llama fracción continua infinita a toda expresión $[a_0; a_1, a_2 \ldots]$

fracción continua de $\alpha = \alpha = [a_0; a_1, \ldots \alpha_j]$ $\quad \alpha_{j+1} = \frac{1}{\alpha_j - [a_j]}$

Queremos probar que de hecho el método sirve para representar a los números, y que además nos dirán las mejores aproximaciones ~~Suponemos $a_0 \in \mathbb{Z}$~~ $a_i \in \mathbb{N}$.

~~Definimos~~ $P_n$ Sea $\frac{P_n}{q_n}$ fracción continua $[a_0, a_1, a_2 \dots]$

decimos que $\frac{P_n}{q_n} = [a_0, a_1, \dots, a_n]$ es la $n$-ésima convergente.

$P_{-1} = 1 \quad q_{-1} = 0$

Proposición: $\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$

Cierto para orden $n$.

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_n & P_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} a_0 P_n + q_n & \\ P_n & \end{pmatrix}$$

$$\frac{P_{n+1}}{q_{n+1}} = a_0 + \frac{1}{a_1 + \frac{1}{\ddots}} = a_0 + \frac{1}{\frac{P_n}{q_n}} = \frac{q_n a_0 + P_n}{P_n}$$

$$P_{n+1} = q_n a_0 + P_n$$

$$q_{n+1} = P_n$$

$\boxtimes$

Corolario
Sean $\frac{P_n}{q_n}$, $\frac{P_{n+1}}{q_{n+1}}$ convergentes sucesivas de $\alpha$.

Entonces $P_n q_{n+1} - q_n P_{n+1} = (-1)^{n+1}$

Demostracion: Tomar determinantes.

Corolario: $P_n = a_n P_{n-1} + P_{n-2}$

$q_n = a_n q_{n-1} + q_{n-2}$

Demos:
$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} * \begin{pmatrix} P_{n-1} & P_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$ ∎

Si nos restringimos a $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$ se llaman fracción continua simple.

Corolario:
$$\frac{P_0}{q_0} < \frac{P_2}{q_2} < \cdots < \frac{P_3}{q_3} < \frac{P_1}{q_1}$$

para $n > 1$ $q_n > q_{n-1}$ ; $q_n \geq n$, y $\frac{P_n}{q_n}$ son reducidas

Demostración: $q_n = a_n q_{n-1} + q_{n-2}$ luego $q_n > 0$

luego $q_n \geq q_{n-1} + 1$

Además $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$

por tanto $\frac{p_{2n}}{q_{2n}} < \frac{p_{2n-1}}{q_{2n-1}}$ y

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{\frac{p_{n-2}}{q_{n-2}}}{\frac{a_n \frac{p_{n-1}}{p_{n-2}} + 1}{a_n \frac{q_{n-1}}{q_{n-2}} + 1}}$$

pero $\frac{p_n}{p_{n-1}} < \frac{q_n}{q_{n-1}}$ n par

$>$ n impar

luego $\frac{p_{2n}}{q_{2n}} > \frac{p_{2n-2}}{q_{2n-2}}$

$\frac{p_{2n+1}}{q_{2n-1}} < \frac{p_{2n-3}}{q_{2n-3}}$ ∎

**Teorema**: Toda fracción continua irracional es convergente $\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \to 0$ luego es de Cauchy $\left|\frac{p_{n+m}}{q_{n+m}} - \frac{p_n}{q_n}\right| < \sum_{N>n} \frac{1}{N^2} \to 0$ $n \to \infty$

**Teorema** Todo irracional se puede representar de manera única como fracción continua

$\alpha = \alpha_0 \quad \alpha_{j+1} = \frac{1}{\alpha_j - [\alpha_j]}$ $a_j = [\alpha_j]$ entonces

$\alpha = [a_0, a_1, \dots, a_n, \alpha_{n+1}]$ para todo $n$

inducción trivial

$$\alpha = \left|\frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n |\alpha_{n+1} q_n + q_{n+1}|}$$

$$< \frac{1}{q_n q_{n-1}} \to 0.$$

es única es trivial si hubiese dos serían iguales

Ejemplos: $\sqrt{2}$, $\frac{\sqrt{5}+1}{2}$, $\sqrt[3]{2}$

$\frac{\sqrt{5}+1}{2} = \alpha_1 = \frac{1}{\alpha - [\alpha]} = \frac{1}{\frac{\sqrt{5}+1}{2} - 1} = \frac{1}{\frac{\sqrt{5}-1}{2}} = \frac{\sqrt{5}+1}{2}$

$$\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

Sus convergentes son $\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$

Luego es $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1}$.

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ $\quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$

$$\begin{pmatrix} P_n & P_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ b_n & a_n - b_n \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_n + b_n & a_n \\ a_n & b_n \end{pmatrix} = \begin{pmatrix} a_{n+1} & b_{n+1} \\ b_{n+1} & a_{n+1} - b_{n+1} \end{pmatrix}$$

además $b_{n+1} = a_n$ luego $a_{n+1} = a_n + a_{n-1}$ Fibonacci

$a_{n+1} = a_n + b_n$

$\sqrt[3]{3} = 1 + \frac{1}{\alpha}$ $\quad \alpha_1 = \frac{1}{\sqrt{2} - [\sqrt{2}]} = \frac{1}{\sqrt[3]{2} - 1} = \frac{\sqrt[3]{4} + \sqrt[3]{2} + 1}{3}$ $\quad 1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5 + \cdots}}}$

$1, \frac{4}{3}, \frac{5}{4}, \frac{29}{23}$

se puede mejorar pues

$$\frac{p_0}{q_0} < \alpha < \frac{p_1}{q_1}$$

luego $\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$

Esta, por otro lado es la "~~mejor~~ cerca de ser la mejor" aproximación posible en el siguiente sentido

Teorema: $\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{q_{n+1}(q_n + q_{n+1})}$

Demostración:

Lema: Tengo que obtener fracciones entre medias si quiero no utilizar la aproximación para $n+1$ y mejorar lo que tengo. Al igual que Farey las mediadas

Lema: $\frac{p_n + j\,p_{n+1}}{q_n + j\,p_{n+1}}$ es no hubna. $0 \le j \le a_{n+2}$

$$\frac{P_n + jP_{n+1}}{q_n + jq_{n+1}} - \frac{P_n + (j-1)P_{n+1}}{q_n + (j-1)q_{n+1}} =$$

$$= \cancel{P_n q_n} + (j-1)P_n q_{n+1} + jP_{n+1}q_n + j(j-1)P_{n+1}q_{n+1}$$

$$\cancel{- P_n q_n} - jP_n q_{n+1} \cancel{+ (j-1)P_{n+1}q_n} - j(j-1)P_{n+1}q_{n+1}$$

$$= \frac{P_{n+1}q_n - P_n q_{n+1}}{(q_n + jq_{n+1})(q_n + (j-1)q_{n+1})} = \frac{(-1)^{n+2}}{(q_n + jq_{n+1})(q_n + (j-1)q_{n+1})}$$

siempre del mismo signo $\Leftrightarrow$ si $n$ par creciente

$$\frac{P_{2n}}{q_{2n}} < \cdots < \frac{P_{2n+2}}{q_{2n+2}}$$

Si $n$ impar decreciente $\frac{P_{2n+1}}{q_{2n+1}} < \cdots < \frac{P_{2n-1}}{q_{2n-1}}$

En particular

$$\left|\alpha - \frac{P_n}{q_n}\right| > \left|\alpha - \frac{P_n + P_{n+1}}{q_n + q_{n+1}} - \frac{P_n}{q_n}\right| = \frac{1}{q_n(q_n + q_{n+1})}$$

En realidad, se tiene un resultado más fuerte en el sentido de que toda fracción es combinación lineal de las dos

consecutivas

**Proposición:** Para toda fracción $a/b$ se hacen $x, y$ enteros tal que

$$x p_n + y p_{n-1} = a$$
$$x q_n + y q_{n-1} = b$$

**Demostración** $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$ determinante $\pm 1$ luego es invertible y $b$ inverso son enteros

Este orden de aproximación es de hecho lo mejor posible. Son la mejor.

**Teorema:** Sea $\frac{p_n}{q_n}$ una convergente de $\alpha$ irac y $\frac{p}{q} \in F(q_n)$ entonces $\left|\alpha - \frac{p}{q}\right| > \left|\alpha - \frac{p_n}{q_n}\right|$.

**Demostración:** Quiero comparar $\frac{p_n}{q_n}$ con $\frac{p}{q}$ luego

$x q \leq q_n$ $\quad p = x p_n + y p_{n-1}$ $\quad (x, y) \neq 0$ pues $(p, q) = 1$

$$q = x q_n + y q_{n-1}$$

$x, y$ son de distinto signo pues si no $q > q_n$

$$|q\alpha - p| = |(xq_n + yq_{n-1})\alpha - (xp_n + yp_{n-1})|$$

$$= |x(q_n\alpha - p_n) + y(q_{n-1}\alpha - p_{n-1})|$$

Si $\frac{p_n}{q_n} > \alpha \Rightarrow \frac{p_{n-1}}{q_{n-1}} < \alpha$ luego son del mismo signo por tanto $|q\alpha - p| > x|q_n\alpha - p_n|$

luego $|\alpha - \frac{p}{q}| > \frac{q_n}{q}|\alpha - \frac{p_n}{q_n}| \geq |\alpha - \frac{p_n}{q_n}|$ ☒

Son la mejor aproximación $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$

pero depende de encontrar la siguiente convergente. En este sentido tenemos una aproximación mejor que $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{q_n^2}$ y queremos saber exactamente el orden exacto que se puede conseguir

Teorema: de cada dos convergentes sucesivas $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{2q_n^2}$

Demos: $\left|\alpha - \frac{P_n}{q_n}\right| = \left|\alpha - \frac{P_{n+1}}{q_{n+1}} + \frac{P_{n+1}}{q_{n+1}} - \frac{P_n}{q_n}\right|$

$$\frac{1}{q_n q_{n+1}} = \left|\frac{P_{n+1}}{q_{n+1}} - \frac{P_n}{q_n}\right| = \left|\frac{P_{n+1}}{q_{n+1}} - \alpha + \alpha - \frac{P_n}{q_n}\right|$$

$$\geq \frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2} = \frac{q_{n+1}^2 + q_n^2}{2q_{n+1}^2 q_n^2}$$

No puede ser

no puede ser

Son la mejor aproximación $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$

pero depende de encontrar la siguiente convergente. En este sentido tenemos una aproximación mejor que $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{q_n^2}$ y queremos saber exactamente el orden exacto que se puede conseguir

Teorema: de cada dos convergentes sucesivas $\left|\alpha - \frac{P_n}{q_n}\right| < \frac{1}{2q_n^2}$

Demos: $\left|\alpha - \frac{P_n}{q_n}\right| = \left|\alpha - \frac{P_{n+1}}{q_{n+1}}\right| + \left|\frac{P_{n+1}}{q_{n+1}} - \frac{P_n}{q_n}\right|$

$$\frac{1}{q_n q_{n+1}} = \left|\frac{P_{n+1}}{q_{n+1}} - \frac{P_n}{q_n}\right| = \left|\frac{P_{n+1}}{q_{n+1}} - \alpha\right| + \left|\alpha - \frac{P_n}{q_n}\right|$$

$$\geq \frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2} = \frac{q_{n+1}^2 + q_n^2}{2q_{n+1}^2 q_n^2}$$

No puede ser

no puede ser

~~¿es la mejor constante?~~

Corolario: existen ∞ fracciones tal que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

¿la mejor constante?

Teo Hurwitz $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\,q^2}$ para una de cada 3 fracciones consecutivas

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| > \frac{1}{\sqrt{5}\,q_{n-1}^2} \quad y \quad \left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{\sqrt{5}\,q_n^2}$$

$$\alpha \in \frac{p_{n-1}}{q_{n-1}} + \frac{\alpha_n p_n + p_{n-1}}{\alpha_n q_n + q_{n-1}}$$

Suponhamos que $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \geq \frac{1}{q_{n-1}^2\sqrt{5}}$

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{q_n^2\sqrt{5}}$$

$$\left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| > \frac{1}{q_{n+1}^2\sqrt{5}}$$

então se $\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{1}{q_n^2(\alpha_{n+1}+\beta_n)}$

$\beta_{n+1} = \frac{q_{n-1}}{q_n} = \frac{1}{a_n + \beta_n}$ $\qquad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}$

por tanto $\frac{1}{\beta_n + \alpha_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}$

$$\frac{1}{\alpha_n} \leq \sqrt{5} - \frac{1}{\beta_n}$$

$$\alpha_n \leq \sqrt{5} - \beta_n$$

$$1 \leq 5 - \sqrt{5}\left(\frac{1}{\beta_n} + \beta_n\right) + 1$$

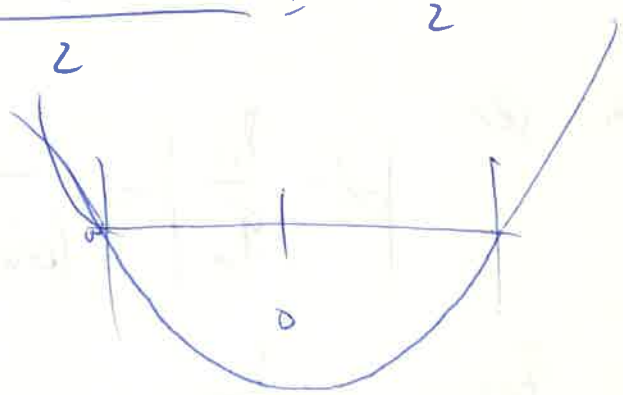
$$\frac{1}{\beta_n} + \beta_n \leq \frac{}{\sqrt{5}} \qquad \beta_n$$

$$\frac{1}{\beta_n} + \beta_n \leq \sqrt{5}$$

$$1 + \beta_n^2 - \frac{1}{\sqrt{5}}\beta_n = 0$$

$$1 + \beta_n^2 - \sqrt{5}\beta_n \geq 0 \qquad \frac{\sqrt{5}-1}{2} < \beta_n < 1$$

$$\frac{\sqrt{5} \pm \sqrt{5-4}}{2} = \frac{\sqrt{5} \pm 1}{2}$$



Luego $\beta_n > \frac{\sqrt{5}-1}{2}$ ; $\beta_{n+1} > \frac{\sqrt{5}-1}{2}$

$\beta_n$ y $\beta_{n+1}$ ↗

$$\frac{\sqrt{5}+1}{2} > \frac{1}{\beta_{n+1}} = \beta_n + a_n > \frac{\sqrt{5}-1}{2} + a_n \Rightarrow a_n < 1$$

Conclusión existen $\infty$ fracciones tal que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\,q^2}$$

Es lo mejor posible

Teorema. ~~Para~~ Sea $\alpha$ irracional. Para todo $A > \sqrt{5}$ la desigualdad $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$ tiene un número finito de soluciones

$$\alpha = \frac{p}{q} + \frac{\delta}{q^2}$$ En particular $\alpha = \frac{\sqrt{5}-1}{2}$

$$\frac{\sqrt{5}-1}{2} = \frac{p}{q} + \frac{\delta}{q^2}$$

$$\left(q\frac{\sqrt{5}}{2} - \frac{\delta}{q}\right)^2 = \left(p + \frac{q}{2}\right)^2 \qquad \therefore \delta \neq -\frac{1}{\sqrt{5}}$$

$$q^2\frac{5}{4} - 1 \neq q^2\frac{5}{4} + \frac{\delta^2}{q^2} + \delta\sqrt{5} = p^2 + \frac{q^2}{4} + pq$$

que $\to \infty$

$$-1 \neq p^2 + \frac{q^2}{4} + pq - q^2\frac{5}{4} \qquad |\delta\sqrt{5}| + \frac{1}{q^2}$$

$$|p^2 + pq - q^2| < \frac{\delta^2}{q^2} + \delta\sqrt{5} < 1$$

$= 0$ no puede ser

El teorema se basa en que $\frac{\sqrt{5}-1}{2} = [0, \overline{1}]$

este es un hecho que se repite en todas las cuadráticas. Si quitamos la razón aurea, la cantidad se aumenta hasta el siguiente periodico

Teorema: Una fracción continua es periodica si y solo si $\alpha$ es irracional cuadratica.

Si es periodica $\alpha = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} = \frac{\alpha_{n+1} \tilde{P}_n + \tilde{P}_{n-1}}{\alpha_{n+1} \tilde{q}_n + \tilde{q}_{n-1}}$

$$\alpha = [a_0, a_1 \dots, a_n, \overline{b_1 \dots b_m}] = [a_0, \overline{a_1, \dots, a_n, \alpha_{n+1}}]$$
$$= [a_0, a_1 \dots a_n, b_1 \dots b_m, \alpha_{n+1}]$$

luego cumple una ec. cuadratica y por tanto $\alpha$ tambien.

Al reves Supongamos que es irracional cuadratico

$$\alpha = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

$$A\alpha^2 + B\alpha + C = A\left(\frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}\right)^2 +$$

$$P(\alpha) = 0$$

$$+ B\left(\frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}\right) + C = 0$$

$$A\left(\alpha_{n+1} P_n + P_{n-1}\right)^2 + B\left(\alpha_{n+1} P_n + P_{n-1}\right)\left(\alpha_{n+1} q_n + q_{n-1}\right)$$

$$+ C\left(\alpha_{n+1} q_n + q_{n-1}\right)^2 = 0$$

$$\alpha_{n+1}^2\left(A P_n^2 + B P_n q_n + C q_n^2\right)$$

$$+ \alpha_{n+1}\left(2A P_n P_{n-1} + P_n q_{n-1} + q_n P_{n-1} + 2C q_n q_{n-1}\right)$$

$$+ \left(A P_{n-1}^2 + B P_{n-1} q_{n-1} + C q_{n-1}^2\right) = 0$$

$$\alpha_{n+1}^2 C_1 + \alpha_{n+1} C_2 + C_3 = 0$$

$$q_n^2\left|P\left(\frac{P_n}{q_n}\right) - P(\alpha)\right| = \left|\alpha - \frac{P_n}{q_n}\right| \left|P'(\xi)\right| \leq \frac{1}{q_n^2} q'$$

luego $C_1 \leq q'$

$$2A\frac{P_n^2}{q_n^2} + 2B\frac{P_n q_n}{q_n} + 2C q_n^2$$

$$-2A\frac{P_n P_{n-1}}{q_n q_{n-1}} - B\left(\frac{P_n q_{n-1}}{q_n} + \frac{q_n P_{n-1}}{q_{n-1}}\right) - 2C(q_n q_{n-1})$$

$$\frac{P_n}{q_n}\ \frac{1}{q_n q_{n-1}}\ \frac{C}{q_n q_{n-1}}\ +\ \frac{C}{q_{n-1}^2}$$

$$2A\frac{P_n^2}{q_n^2} + 2B\frac{P_n}{q_n} + 2C - 2A\frac{P_n}{q_n}\frac{P_{n-1}}{q_{n-1}} - B\left(\frac{P_n}{q_n} + \frac{P_{n-1}}{q_{n-1}}\right) - 2C$$

$$\leq \frac{K}{q_n q_{n-1}}$$

y la última es la misma que la primera ☒

luego tenemos infinitas raíces de un conjunto de polinomios luego se repiten

Al igual que en las fracciones decimales, ~~las fracciones continuas~~ los irracionales cuadráticos son como los racionales

Ejemplo: $\sqrt{3} = [1,\overline{1,2}]$, $\sqrt{2} = [1,\overline{2}]$, $\frac{\sqrt{5}-1}{2} = [0,\overline{1}]$, $\sqrt{6} = [2,\overline{2,4}]$

Lo que tienen fracciones periodicas puras son también distinguidas como

Teorema: $\alpha$ tiene fracción periódica pura

$\Leftrightarrow$ $\alpha > 1$ $0 > \bar{\alpha} > -1$

Demostración $\alpha = [\dot{a}_0, \ldots \dot{a}_n]$

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} =$$

$$\alpha = \frac{p_n \alpha + p_{n-1}}{q_n \alpha + q_{n-1}} \quad \text{es irracional cuadratico.} \quad a\alpha^2 + b\alpha + c = 0$$

$\gamma = [a_n, \ldots, a_0]$

$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} \text{ luego}$$

$$\gamma = \frac{p_n \gamma + q_n}{p_{n-1}\gamma + q_{n-1}} \quad \text{cumple la}$$

~~misma ecuación luego~~ $\gamma$ y por tanto $\gamma \geq a_n > 1$

$$a\left(-\frac{1}{\gamma}\right)^2 + b\left(-\frac{1}{\gamma}\right) + c = 0$$

luego $-\frac{1}{\gamma} < 0$ $-\frac{1}{\gamma} = \bar{\alpha}$

al revés sea $\alpha$ $-1 < \bar{\alpha} < 0$

$\alpha_{j+1} = \frac{1}{\alpha_j - [\alpha_j]}$ $\qquad$ $\alpha'_{j+1} = \frac{1}{\alpha_j - [\alpha_j]}$

~~$\alpha'_{j+1} < 0$~~

$$\alpha_j = a_j + \frac{1}{\alpha_{j+1}}$$

$$\overline{\alpha_j} = a_j + \frac{1}{\overline{\alpha_{j+1}}}$$

$-1 < \overline{\alpha_j} < 0$ luego $0 > \overline{\alpha_1} = \frac{1}{\bar{\alpha} - a_0} > \frac{1}{a_0} \geq -1$

$$\left[ -\frac{1}{\overline{\alpha_{j+1}}} \right] = a_j$$

~~Supongamos~~ Sabemos que es periódica

$$a_0, a_1 \ldots a_m \; b_1 \ldots b_n$$

$$a_{n+k} = a_k \quad \forall k \geq m+1$$

$$a_m = \left[ -\frac{1}{\overline{\alpha_{m+1}}} \right] = \left[ -\frac{1}{\overline{\alpha_{m+n+1}}} \right] = a_{n+m}$$

y repitiendo el mismo razonamiento

Conclamo

$$\sqrt{N} = [a_0; a_1 \cdots a_n \dot{2}a_0]$$

tal que $a_n = 2a_0$ $a_{n-1} = a_1$ $a_{n-j} = a_j$ $1 \leq j \leq \frac{n}{2}$

~~$\sqrt{N} = a_0 + \alpha$~~ $1 < \sqrt{N} + a_0$ y $-1 < a_0 - \sqrt{N} < 0$

luego $\sqrt{N} + a_0 = [\dot{2}a_0, a_1 \cdots, \dot{a}_n]$

$$\sqrt{N} = [a_0; \dot{a}_1, \cdots, \dot{a}_n, \dot{2}a_0]$$

$$-\frac{1}{a_0 - \sqrt{N}} = [\dot{a}_n, a_{n-1} \cdots, \dot{2}a_0]$$

$$\sqrt{N} = a_0 + \frac{1}{[\dot{a}_n; a_{n-1}, \cdots, \dot{2}a_0]} = [a_0; a_n, \cdots, \dot{2}a_0]$$

∎