Mètodes analítics en teoria de nombres

Bernat Esteve i Luis M. Villabón

2025

ÍNDEX

CAPÍTOL

1 FUNCIONS L

Fins ara hem estat tractant amb funcions $F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$; i hem vist un cas (teorema **??**) de com estendre aquestes funcions una mica més enllà del que permet la sèrie en si. En aquest capítol veurem més exemples d'aquestes extensions. Començarem primer per un costat més algebraic, que després ens servirà per estudiar les funcions que va estudiar Dirichlet; on prenia $f(n) = \chi(n)$ on χ és un caràcter de Dirichlet (definició **??**). Però primer fem un pas enrere, i considerem un grup G abelià i finit (durant el capítol, els grups seran abelians i finits).

Definició 1.1 Caràcter d'un grup

Sigui G un grup finit i abelià, aleshores un caràcter de G serà un morfisme $\psi\colon G \to \mathbb{C}^*$ (on $\mathbb{C}^*$ és el grup multiplicatiu de $\mathbb{C} \setminus \{0\}$)

I com que si tenim un objecte, el primer que ens hauríem de preguntar és quina estructura té:

Definició 1.2 El grup de caràcters

Denotem per $\widehat{G}$ al grup $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*) = \{\text{Caràcters de G}\}$, on la operació és:

$$\psi, \phi\colon G \to \mathbb{C}^* \qquad \text{aleshores } (\psi \cdot_{\widehat{G}} \phi)(g) \mapsto \psi(g) \cdot_{\mathbb{C}^*} \phi(g)$$

I anomenarem a $\widehat{G}$ el grup de caràcters de G.

I ara veurem alguna propietat d'aquests caràcters, sobretot com es comporten amb els grups abelians finits més bàsics: els grups cíclics.

Lema 1.1 El grup de caràcters d'un grup cíclic

Sigui $G = \langle s \rangle$ un grup cíclic d'ordre n i sigui μ_n el grup d'arrels n-èssimes de la unitat.

Aleshores

$$\begin{aligned} \widehat{G} &\longrightarrow \mu_n \\ \psi &\longmapsto \psi(s) \end{aligned}$$

és un isomorfisme.

Demostració. Com que $\psi(s)^n = \psi(s^n) = \psi(1) = 1$, $\psi(s)$ és arrel n-èssima de la unitat. D'altra banda, el morfisme és injectiu perquè si $\psi_1, \psi_2 \in \widehat{G}$ i $\psi_1(s) = \psi_2(s)$, llavors $\psi_1(s^k) = \psi_1(s)^k = \psi_2(s)^k = \psi_1(s^k)$ per tot $s^k \in \langle s \rangle = G$. Finalment, per veure l'exhaustivitat, si $\omega \in \mu_n$, podem definir $\psi(s^k) = \omega^k$. □

Resulta també natural preguntar-se ara sobre la relació entre els caràcters d'un grup i el dels seus subgrups.

Proposició 1.1 Extensió de caràcters de subgrups

Sigui $H \leq G$ subgrup. Tot caràcter de H estén a un caràcter de G.

Demostració. Si $H = G$, el resultat és tautològic. Suposem $H \neq G$, i sigui $x \in G \setminus H$. Com que G és finit, n'hi ha prou amb veure que un caràcter $\psi\colon H \to \mathbb{C}^\times$ estén a un de $H' := \langle H, x \rangle$. Atès que G és abelià, tot element de H' es pot escriure com hx^a on $h \in H$ i $a \in \mathbb{Z}$. A més $|G/H| < +\infty$, per tant $[x]$ és d'ordre finit i existeix $n \in \mathbb{Z}^+$ tal que $[x]^n = [1]$, equivalentment $x^n \in H$. Prenem el mínim dels n tals que això passi i fixem $\omega \in \mathbb{C}^\times$ tal que $\psi(x^n) = \omega^n$. Definim

$$\begin{aligned} \psi'\colon\ H' &\longrightarrow \mathbb{C}^\times \\ hx^a &\longmapsto \psi(h)\omega^a \end{aligned}$$

És clar que $\psi'|_H = \psi$. Cal veure que està ben definida i que és morfisme. Suposem que $h_1 x^{a_1} = h_2 x^{a_2}$. Aleshores $h_1 h_2^{-1} = x^{a_2 - a_1} = x^{na'}$ per algun $a' \in \mathbb{Z}^+$, per la minimalitat de n. Per tant

$$\psi(h_1)\psi(h_2)^{-1} = \psi(h_1 h_2^{-1}) = \psi((x^n)^{a'}) = \psi(x^n)^{a'} = \omega^{na'} = \omega^{a_2 - a_1},$$

d'on $\psi(h_1)\omega^{a_1} = \psi(h_2)\omega^{a_2}$. Finalment, comprovem que és morfisme:

$$\psi'(h_1 x^{a_1} h_2 x^{a_2}) = \psi'(h_1 h_2 x^{a_1 + a_2}) = \psi(h_1 h_2)\omega^{a_1 + a_2} = \psi(h_1)\omega^{a_1}\psi(h_2)\omega^{a_2} = \psi'(h_1 a_1)\psi'(h_2 a_2).$$

□

Podem refinar aquest últim resultat una mica més.

Proposició 1.2 Restricció de caràcters de subgrups

La restricció $\mathrm{Res}\colon \widehat{G} \to \widehat{H}$ que envia ψ a $\psi|_H$ és exhaustiva, i $\ker(\mathrm{Res}) \cong \widehat{G/H}$.

Demostració. Dir que aquesta aplicació és exhaustiva és equivalent a la proposició anterior. Per veure l'isomorfisme, tenim que $\psi \in \ker(\mathrm{Res})$ si i només si $\psi(H) = \{1\}$ o equivalentment $H \subseteq \ker(\psi)$. Però això últim es dona si i només si existeix $\psi'\colon G/H \to \mathbb{C}^\times$ tal que ψ factoritza a través de de ψ', és a dir, el diagrama commuta. L'isomorfisme, doncs, ve donat l'assignació $\psi \mapsto \psi'$, i té inversa $\psi' \mapsto \psi' \circ \pi$ on $\pi\colon G \to G/H$ és la projecció al quocient. □

Això ens dona, a més, l'ordre del grup de caràcters d'un determinat grup.

Corol·lari 1.1 Ordre del grup de caràcters

Si G és un grup abelià finit, $|G| = |\widehat{G}|$.

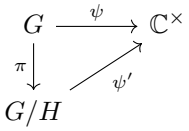

Figura 1.1: Aquest diagrama commuta.

Demostració. Procedim per inducció sobre l'ordre. Si $|G| = 1$, és trivial. Suposem $|G| > 1$. Pel teorema de Cauchy, existeix un subgrup $H \leq G$ d'ordre p, que és cíclic per ser d'ordre primer i per tant pel lema 1, $|\widehat{H}| = |\mu_p| = p = |H|$. D'altra banda, per la proposició anterior i pel primer teorema d'isomorfia, $|\widehat{H}| = |\widehat{G}|/|\ker(\mathrm{Res})| = |\widehat{G}|/|\widehat{G/H}|$. Ara, com que $|G/H| < |G|$, per la hipòtesi d'inducció $|G/H| = |\widehat{G/H}|$, i tot plegat deduïm

$$|\widehat{G}| = |\widehat{H}||\widehat{G/H}| = |H||G/H| = |G|.$$

□

La següent proposició és un anàleg de la relació entre un espai vectorial i el seu bidual en àlgebra lineal. Aquí tindrem també un isomorfisme canònic entre un grup i el grup de caràcters del seu grup de caràcters.

Proposició 1.3 Isomorfisme canònic entre G i $\widehat{\widehat{G}}$

Definim $\epsilon\colon G \to \widehat{\widehat{G}}$ per $g \mapsto (\mathrm{ev_g}\colon \widehat{G} \to \mathbb{C}^\times)$ on $\mathrm{ev_g}(\psi) := \psi(g)$. Llavors ϵ és un isomorfisme.

Demostració. Veure que és morfisme és directe: si $g, h \in G$ i $\psi \in \widehat{G}$, $\mathrm{ev}_{gh}(\psi) = \psi(gh) = \psi(g)\psi(h) = \mathrm{ev}_g(\psi)\mathrm{ev}_h(\psi)$, d'on $\mathrm{ev}_{gh} = \mathrm{ev}_g\mathrm{ev}_h$, és a dir, $\epsilon(gh) = \epsilon(g)\epsilon(h)$. A més, pel corol·lari anterior, $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, per tant, per provar que és un isomorfisme només cal provar la injectivitat. Sigui $g \in \ker(\epsilon)$, és a dir, $\psi(g) = 1$ per tot $\psi \in \widehat{G}$. Suposem per arribar a contradicció que $g \neq 1$. Llavors tenim un caràcter $\psi\colon \langle g \rangle \to \mathbb{C}^\times$ definit per $g \mapsto e^{\frac{2\pi i}{|\langle g \rangle|}} \neq 1$. Però llavors ψ' estén a un caràcter ψ de G, absurd ja que $\psi(g) = \psi'(g) \neq 1$. □

La suma de les arrels n-èssimes de la unitat dona 0. El següent resultat és una generalització d'això a caràcters de grups abelians finits.

Proposició 1.4 Relacions d'ortogonalitat

(i) Donat $\psi \in \widehat{G}$, tenim

$$\sum_{g\in G} \psi(g) = \begin{cases} |G| & \psi \text{ trivial} \\ 0 & \text{altrament} \end{cases}$$

(ii) Donat $g \in G$, tenim

$$\sum_{\psi\in\widehat{G}} \psi(g) = \begin{cases} |G| & g = 1 \\ 0 & \text{altrament} \end{cases}$$

Demostració. (i) Si $\psi = 1$, és directe. Suposem que existeix $h \in G$ tal que $\psi(h) \neq 1$. Aleshores

$$\psi(h)\sum_{g\in G}\psi(g) = \sum_{g\in G}\psi(hg) = \sum_{g\in G}\psi(g),$$

i aïllant,

$$(1-\psi(h))\sum_{g\in G}\psi(g) = 0.$$

i com que $\psi(h) \neq 1$ obtenim el resultat.

(ii) Si apliquem l'apartat (i) a $\widehat{\widehat{G}}$ i utilitzem que $G \cong \widehat{\widehat{G}}$, ho tindrem: donat $g \in G$,

$$\sum_{\psi\in\widehat{G}}\psi(g) = \sum_{\psi\in\widehat{G}}\mathrm{ev}_g(\psi) = \begin{cases} |G| & \mathrm{ev}_g = 1 \\ 0 & \text{altrament} \end{cases}$$

i $\mathrm{ev_g} = 1$ si i només si $g = 1$ (ja que $g \mapsto (\mathrm{ev_g}\colon \widehat{G} \to \mathbb{C}^\times)$ és un isomorfisme). □

Definirem ara els caràcters en els que estarem interessats per a provar el teorema de Dirichlet.

Definició 1.3 Caràcter mòdul m

Un caràcter mòdul m és un caràcter de $(\mathbb{Z}/m\mathbb{Z})^\times$.

Això encaixa amb la definició de caràcter de Dirichlet mòdul m que es va donar al principi: tot caràcter de Dirichlet mòdul m χ defineix un caràcter mòdul m ψ com $\psi([a]) = \chi(a)$ per $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$; i recíprocament, tot caràcter mòdul m ψ defineix un caràcter de Dirichlet mòdul m com

$$\chi(a) = \begin{cases} \psi([a]) & \gcd(a,m) = 1 \\ 0 & \gcd(a,m) \neq 1. \end{cases}$$

Notem que d'aritmètica, ja coneixíem un exemple de caràcter mòdul m: el símbol de Legendre.

Exemple. Sigui $m = p$ primer senar. Llavors $(\mathbb{Z}/m\mathbb{Z})^\times$ és cíclic d'ordre $p-1$, i llavors té un únic element d'ordre 2. Per tant,

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathbb{C}^\times \\ a &\longmapsto \left(\frac{a}{p}\right) \end{aligned}$$

és un caràcter mòdul p.

Ara distingirem un tipus de caràcter de Dirichlet que es comporta de manera diferent a la resta.

Definició 1.4 Caràcter principal mòdul m

El caràcter principal mòdul m és $\chi_0(a)\colon \mathbb{Z}^+ \to \mathbb{C}$ definit per

$$\chi_0(a) = \begin{cases} 1 & \gcd(a,m) = 1 \\ 0 & \text{altrament} \end{cases}$$

A partir d'ara, χ sempre denotarà un caràcter de Dirichlet mòdul m (és a dir, fixem la m). A continuació, associarem a cada caràcter de Dirichlet una certa funció que dona nom a aquest capítol.

Definició 1.5 Funció L associada a un caràcter de Dirichlet

La funció L associada al caràcter de Dirichlet mòdul m χ és la sèrie de Dirichlet

$$L(\chi, s) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}.$$

.

Demostrarem seguidament algunes propietats analítiques de les funcions L.

Lema 1.2 Convergència de les funcions L de caràcters no principals

Si $\chi \neq \chi_0$, llavors $L(\chi, s)$ té

(i) $\sigma_c = 0$, per tant $L(\chi, s)$ és holomorfa per $\sigma > 0$.

(ii) $\sigma_a > 1$, per tant té una factorització

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

atès que χ és completament multiplicativa. En particular, no s'anul·la per $\sigma > 1$.

Demostració. (i) Sigui $x \geq 1$ i sigui $k \in \mathbb{Z}^+$ tal que $km \leq x \leq (k+1)m$. Aleshores,

$$\left|\sum_{n\leq x} \chi(n)\right| = \left|\sum_{n\leq km} \chi(n) + \sum_{km<n\leq x} \chi(n)\right| = \left|\sum_{km<n\leq x} \chi(n)\right| \leq \sum_{km<n\leq x} |\chi(n)| \leq \varphi(m).$$

on la segona igualtat es dona per les relacions d'ortogonalitat; i la última desigualtat perquè $|\chi(n)| = 1$ si $\gcd(n,m) = 1$ per ser $\chi(n)$ arrel de la unitat, i $|\chi(n)| = 0$ altrament. Per tant, χ té sumes parcials fitades, i per l'exercici 1 del full de problemes 2, $L(\chi, s)$ convergeix per $\sigma > 0$. A més, no ho fa per $s = 0$ ja que el terme general no tendeix a 0.

(ii) Com que $|\chi(n)| \leq 1$, per l'exercici 1 del full de problemes 2, $L(\chi, s)$ convergeix absolutament per $\sigma > 1$. A més, no ho fa per $s = 1$: tenim

$$\sum_{n\geq 1} \frac{|\chi(n)|}{n^s} = \sum_{\gcd(n,m)=1} \frac{1}{n} > \sum_{k\geq 1} \frac{1}{mk+1},$$

que divergeix. □

Ara estem en procés de demostrar el teorema de les progressions aritmètiques de Dirichlet. I per fer-ho passarem per veure propietats de les funcions L. La primera, i poder de les més importants, és que $L(\chi_0, s)$ té un pol en $s = 1$.

Lema 1.3 Continuació meromorfa de $L(\chi_0, s)$

Si χ_0 és el caràcter principal, aleshores:

$$L(\chi_0, s) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \qquad \text{per } \sigma > 1.$$

En particular $L(\chi_0, s)$ té continuació meromorfa en el semiplà a la dreta del 0 amb un únic pol simple en $s = 1$.

Demostració. Com que $|\chi_0(m)| \leq 1$ (recordem que $\chi_0(m) \in \{0, 1\}$), aleshores per l'exercici 1 del full de problemes 1, sabem que $\sigma_a \leq 1$. Per tant, pel corol·lari **??**, tenim que:

$$L(\chi_0, s) = \prod_p \frac{1}{1 - \frac{\chi_0(p)}{p^s}} = \prod_{p \nmid m} \frac{1}{1 - \frac{1}{p^s}} = \underbrace{\left(\prod_p \frac{1}{1 - \frac{1}{p^s}}\right)}_{\zeta(s)} \left(\prod_{p|m} 1 - \frac{1}{p^s}\right)$$

Que és el que volíem veure. Ja que com que podem estendre la funció de la dreta a $\sigma > 0$, podem fer el mateix amb la funció de la esquerra (coincideixen en un conjunt amb com a mínim un punt d'acumulació). □

Notem també, que pel lema 1, tenim que $L(\chi, 1) \in \mathbb{C}$. I el punt clau de la demostració del teorema de la progressió aritmètica de Dirichlet consistirà en veure que $L(\chi, 1) \neq 0$ per cap caràcter de Dirichlet.

Lema 1.4 Un producte sobre tots els caràcters de Dirichlet

Sigui $m \in \mathbb{Z}/m\mathbb{Z}$, i p un primer tal que $p \nmid m$, sigui f l'ordre de p mòdul m. Aleshores tenim la següent igualtat sobre $\mathbb{C}[T]$:

$$\prod_\chi (1 - \chi(p)T) = (1 - T^f)^{\frac{\varphi(m)}{f}}$$

Exemple. Recordem que a amb $m = 4$ ja hem vist que hi havien 2 caràcters de Dirichlet:

$$\chi_0(a) = \begin{cases} 1 & \text{si } a \text{ és senar,} \\ 0 & \text{altrament.} \end{cases} \qquad \chi_1(a) = \begin{cases} 1 & \text{si } a \equiv 1 \pmod 4 \\ -1 & \text{si } a \equiv 3 \pmod 4 \\ 0 & \text{altrament.} \end{cases}$$

Per tant si prenem un $p \equiv 1 \pmod 4$ qualsevol, tenim que $\varphi(4) = 2$ i l'ordre de p és 1, aleshores:

$$(1 - \chi_0(p)T)(1 - \chi_1(p)T) = (1 - T^1)^{\frac{2}{1}}$$

I si prenem $p \equiv 3 \pmod 4$, aleshores té ordre 2:

$$(1-\chi_0(p)T)(1-\chi_1(p)T) = (1-T^2)^{\frac{2}{2}}$$

I ara que hem vist un exemple, comencem la demostració.

Demostració. Sigui $\psi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$, aleshores pel lema 1 tenim que $\psi(p)$ és una arrel p-èsima de la unitat, diguem-li $\psi(p) = \xi$. Definim ara

$$\eta : \langle p\rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$$

que envia $\eta(a) = \xi^a$. Ara volem contar quantes funcions $\chi \in \widehat{G}$ es restringeixen a $\langle p\rangle$ de la mateixa manera que ψ. O sigui, si recordem la funció restricció Res:

$$\mathrm{Res}\colon \widehat{(\mathbb{Z}/m\mathbb{Z})^\times} \to \widehat{\langle p\rangle}$$

Que envia θ a $\theta|_{\langle p\rangle}$; aleshores el que volem trobar és $\#\ker(\mathrm{Res})$. Però per la proposició 1 tenim:

$$\#\ker(\mathrm{Res}) = \#\frac{(\mathbb{Z}/m\mathbb{Z})^\times}{\langle p\rangle} = \frac{\varphi(m)}{f}$$

Per tant, sabem que hi ha $\frac{\varphi(m)}{f}$ caràcters que restringits al grup $\langle p\rangle$ són iguals, i envien $p \mapsto \xi$; per tant:

$$\prod_\chi 1-\chi(p)T = \prod_{\substack{\xi \text{ arrel } f\text{-èsima}\\ \text{de la unitat}}} (1-\xi T)^{\frac{\varphi(m)}{f}}$$

Però el producte de $1-\xi T$ sobre totes les f-èsimes arrels de la unitat és $1-T^f$, per tant:

$$\prod_\chi 1-\chi(p)T = \prod_{\substack{\xi \text{ arrel } f\text{-èsima}\\ \text{de la unitat}}} (1-\xi T)^{\frac{\varphi(m)}{f}} = (1-T^f)^{\frac{\varphi(m)}{f}}$$

Que és justament el que volíem veure. □

I ara definirem un objecte molt important en la demostració del teorema de Dirichlet: la funció m-èsima de Dirichlet:

Definició 1.6 Funció m-èsima de Dirichlet

Sigui $m \in \mathbb{Z}_{\geq 1}$, aleshores la funció m-èsima de Dirichlet es defineix com

$$\zeta_m(s) := \prod_\chi L(\chi, s)$$

On el producte recorre tots els caràcters de Dirichlet mòdul m.

Recordem que volem veure que $L(\chi, 1)$ no és zero; per tant, ens interessarà estudiar ζ_m en $s = 1$, i per fer-ho començarem veient com es comporta aquesta funció:

Proposició 1.5 Producte d'Euler, i sèrie de Dirichlet de ζ_m.
Es té:

1. $\zeta_m(s) = \prod_{p \nmid m}(1 - p^{-f_p s})^{-\frac{\varphi(m)}{f_p}}$ per $\sigma > 1$; i on f_p és l'ordre de p a $(\mathbb{Z}/m\mathbb{Z})^\times$.

2. $\zeta_m(s)$ admet una expressió com a sèrie de Dirichlet amb coeficients a $\mathbb{Z} \geq 0$ (en particular, $\mathbb{R}_{\geq 0}$) per a $\sigma > 1$.

Demostració. Per $\sigma > 1$ tenim que:

$$\zeta_m(s) = \prod_\chi \left(\prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \right) \overset{\text{conv. abs.}}{=} \prod_p \left(\prod_\chi \frac{1}{1 - \frac{\chi(p)}{p^s}} \right)$$

I com que $\chi(p|m) = 0$, podem ignorar els termes que siguin divisors de m:

$$\prod_p \left(\prod_\chi \frac{1}{1 - \frac{\chi(p)}{p^s}} \right) = \prod_{p \nmid m} \left(\prod_\chi \frac{1}{1 - \frac{\chi(p)}{p^s}} \right)$$

I pel lema 1, utilitzant $T = p^{-s}$:

$$\prod_{p \nmid m} \left(\prod_\chi \frac{1}{1 - \frac{\chi(p)}{p^s}} \right) = \prod_{p \nmid m} \left(1 - p^{-s f_p}\right)^{-\frac{\phi(m)}{f_p}} =$$

I amb això demostrem la primera part de la proposició. I ara per demostrar la segona part, passem això a sèries de potències:

$$\prod_{p \nmid m} \left(\prod_\chi \left(1 - p^{-s f_p}\right)^{\frac{\phi(m)}{f_p}} \right) = \prod_{p \nmid m} \left(\sum_{r \geq 0} p^{-s f_p r} \right)^{\frac{\varphi(m)}{f_p}}$$

Notem que per $\sigma > 1$, tenim que $\sum_{r \geq 0} p^{-s f_p r}$ és una sèrie de Dirichlet amb coeficients $\in \{0, 1\}$. A més, com que sabem que una sèrie de potències al quadrat es transforma a fer una convolució en els coeficients, sabem que ara passen a ser enters no negatius. I per tant, si considerem la funció multiplicativa que en els primers val l'enter no negatiu que hi ha al producte, (i 0 en els primers $p|m$), sabem que té tots els coeficients no negatius. Que és el que volíem veure. □

I ara finalment demostrem el que portem un temps volent demostrant: que $L(\chi, 1) \neq 0$. De fet, això que veurem ara és la base del teorema de Dirichlet, i tot i que no veurem la demostració original d'aquest fet, sí que en veurem 2: la que va fer l'Edmund Landau, al 1909; i la de'n Vallée-Poussin, del 1896.

Teorema 1.1 Les funcions $L(\chi, s)$ no s'anul·len en $s = 1$

1. La funció $\zeta_m(s)$ té un pol simple a $s = 1$.

2. $L(\chi, 1) \neq 0$ si $\chi \neq \chi_0$.

Demostració. Notem que si veiem el segon apartat, tindrem de regal el primer, ja que:

$$\zeta_m(s) = \underbrace{L(\chi_0, s)}_{\text{pol simple}} \prod_{\chi \neq \chi_0} \overbrace{\underbrace{L(\chi, s)}_{\text{no s'anul·la}}}^{\text{holomorfa per } \sigma > 0}$$

Per tant, ara procedirem a veure el segon apartat.

Suposem que hi ha alguna $\chi_1 \neq \chi_0$ tal que $L(\chi_1, 1) = 0$. Aleshores:

$$\zeta_m(s) = L(\chi_0, s)L(\chi_1, s) \prod_{\chi \neq \chi_0, \chi_1} L(\chi, s)$$

Com que sabem que el producte és una funció holomorfa per $\sigma > 0$, i que a més, el pol simple de $L(\chi_0, s)$ mor amb el zero de $L(\chi_1, s)$, ens queda que $\zeta_m(s)$ es pot estendre a una funció holomorfa a la dreta del 0. També sabem, però, que per la proposició 1 es pot expressar com una sèrie de Dirichlet amb coeficients reals no negatius. I per tant, podem aplicar el teorema de Landau (**??**), que ens diu que la sèrie de Dirichlet associada ha de convergir per $\sigma > 0$. Però:

Claim:

La sèrie de Dirichlet no convergeix per $\sigma = \frac{1}{\varphi(m)}$

Recordem que la sèrie era:

$$\prod_{p \nmid m} \frac{1}{\left(1 - p^{-sf_p}\right)^{\frac{\varphi(m)}{f_p}}} = \prod_{p \nmid m} \left(\sum_{r \geq 0} p^{-rsf_p} \right)^{\frac{\varphi(m)}{f_p}} \geq \prod_{p \nmid m} \sum_{r \geq 0} \left(p^{-rsf_p}\right)^{\frac{\varphi(m)}{f_p}} = \prod_{p \nmid m} \sum_{r \geq 0} p^{-rs\varphi(m)}$$

On la desigualtat es té ja que $rsf_p \in \mathbb{R}$, i per tant, $p^{-rsf_p} \in \mathbb{R}_{\geq 0}$. Per tant, com que si $a, b > 0$ tenim $(a+b)^k \geq a^k + b^k$. Que és bàsicament el que tenim a dalt.

$$\prod_{p \nmid m} \sum_{r \geq 0} p^{-rs\varphi(m)} = \prod_{p \nmid m} 1 + \frac{1}{p^{s\varphi(m)}} + \frac{1}{p^{2s\varphi(m)}} + \cdots = \sum_{\substack{n \geq 1 \\ (n,m)=1}} \frac{1}{n^{s\varphi(m)}}$$

I si prenem $s = \frac{1}{\varphi(m)}$ aleshores la sèrie és divergent. Però això contradiu el que havíem suposat: que ζ_m es pot estendre de manera holomorfa fins a $\sigma = 0$. □

Sigui $a \in \mathbb{Z}$, tal que $(m, a) = 1$, on m és un enter que hem fixat més a munt. Sigui ara $\mathbb{P}_a := \{p \equiv a \pmod m\}$, aleshores donat un caràcter de Dirichlet $\chi \colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$ definim la funció

$$f_\chi \colon \mathbb{R}_{\geq 1} \to \mathbb{C} \qquad \text{tal que} \qquad f_\chi(s) := \sum_{p \nmid m} \frac{\chi(p)}{p^s}$$

Que comparant-la amb ζ veiem que convergeix de manera absoluta per $\sigma > 1$.

Lema 1.5

El sumatori

$$\sum_{p\in\mathbb{P}_a}\frac{1}{p^s}=\frac{1}{\varphi(m)}\sum_{\chi}\frac{f_\chi(s)}{\chi(a)}$$

Demostració. Considerem el sumatori

$$\sum_{\chi}\frac{f_\chi(s)}{\chi(a)}=\sum_{\chi}\frac{\sum_{p\nmid m}\frac{\chi(p)}{p^s}}{\chi(a)}=\sum_{\chi}\sum_{p\nmid m}\frac{\chi(p)}{\chi(a)p^s}=\sum_{\chi}\sum_{p\nmid m}\frac{\chi(a^{-1}p)}{p^s}=$$

Com que per $\sigma>1$ estem sumant una quantitat finita de coses que convergeixen absolutament, i per tant no hi ha cap problema per canviar l'ordre del sumatori.

$$\sum_{p\nmid m}\sum_{\chi}\frac{\chi(a^{-1}p)}{p^s}=\sum_{p\nmid m}\frac{1}{p^s}\sum_{\chi}\chi(a^{-1}p)$$

Però notem que $\sum_\chi\chi(a^{-1}p)=\begin{cases}\varphi(m) & \text{si } a\equiv p \pmod m\\ 0 & \text{altrament.}\end{cases}$ degut a la proposició 1, utilitzant $G=(\mathbb{Z}/m\mathbb{Z})^\times$. Per tant:

$$\sum_{p\in\mathbb{P}_a}\frac{1}{p^s}=\frac{1}{\varphi(m)}\sum_{\chi}\frac{f_\chi(s)}{\chi(a)}$$

Que és el que volíem veure. □

Notem que si en algun moment veiem que $\frac{1}{\varphi(m)\chi(a)}\sum_\chi f_\chi(s)$ divergeix en alguna s, aleshores sabrem que el sumatori $\sum_{p\in\mathbb{P}_a}\frac{1}{p^s}$ també ho farà, i per tant, sabrem que n'hi haurà d'haver un nombre infinit. Per tant considerem el següent lema:

Lema 1.6 Estudi de convergència de les f_χ.

Tenim que per $\chi=\chi_0$

$$\lim_{\substack{s\to1\\ s\in\mathbb{R}_{>1}}}\frac{f_{\chi_0}(s)}{\log\left(\frac{1}{s-1}\right)}=1$$

I si $\chi\neq\chi_0$, aleshores:

$$\lim_{\substack{s\to1\\ s\in\mathbb{R}_{>1}}}\frac{f_{\chi}(s)}{\log\left(\frac{1}{s-1}\right)}=0$$

Demostració. Notem que la diferència entre $f_\chi(s)=\sum_{p\nmid m}p^{-s}$ i $\sum_p p^{-s}$ és només en els primers termes, per tant, el comportament asimptòtic serà igual, i pel corol·lari **??**, tenim:

$$\lim_{\substack{s\to1\\ s\in\mathbb{R}_{>1}}}\frac{\sum_p p^{-s}}{\log\left(\frac{1}{s-1}\right)}=1$$

Que és el que volíem veure per la primera part.

Per la segona part, hem de veure que si no és principal, el mateix límit és zero. Per fer-ho considerem:

$$F(s) := \sum_p \log\left(\frac{1}{1-\chi(p)p^{-s}}\right) = \sum_p \sum_{n\geq 1} \frac{\chi(p)^n}{np^{ns}} = f_\chi(s) + \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}$$

On la segona igualtat és la expansió del logaritme per $\sigma > 1$.

Però el sumatori que hi ha a la última expressió que tenim, el vam fitar en el corol·lari **??**:

$$\left|\sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}\right| \leq \sum_p \sum_{n\geq 2} \frac{1}{np^{ns}} \leq 1$$

Per tant, si veiem que F està fitada, aleshores tindrem que f_χ està fitada, i per tant, fent el límit del quocient amb el logaritme ens donarà 0. I si ara considerem la següent expressió:

$$e^{F(s)} = \prod_p \frac{1}{1-\chi(p)p^{-s}} = L(\chi, s) \xrightarrow{s\to 1^+} L(\chi, 1) \neq 0$$

Per tant, $F(s)$ roman fitada quan $s \to 1^+$. I per tant, $f_\chi(s)$ també ho fa: que és el que volíem veure. □

I ara ja podem demostrar el teorema de la progressió aritmètica de Dirichlet:

Teorema 1.2 **Teorema de la progressió aritmètica de Dirichlet (fort)**
Sigui $a \in \mathbb{Z}$ un enter tal que $(a, m) = 1$, aleshores

$$\lim_{\substack{s\to 1 \\ s\in\mathbb{R}_{>1}}} \frac{\sum_{p\in\mathbb{P}_a} p^{-s}}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{\varphi(m)}$$

Corol·lari 1.2 **Teorema de la progressió aritmètica de Dirichlet**
$\#P = \infty$

Notem que el teorema ens diu més que el corol·lari, ja que ens descriu la distribució dels primers en les classes mòdul m.

Demostració. Primer veurem la demostració del corol·lari, que és immediata del teorema. Ja que si suposem que $\mathbb{P}_a$ fos finit, aleshores $\sum_{p\in\mathbb{P}_a} p^{-s}$ seria finit, i dividit per alguna cosa que se'n va a l'infinit ens donaria 0, i no $\frac{1}{\varphi(m)}$ que és el que ens diu el teorema per $s \to 1$. □

I ara veurem la demostració del teorema important:

Demostració. Pel lema 1 sabem que

$$\lim_{\substack{s\to 1 \\ s\in\mathbb{R}_{>1}}} \frac{\sum_{p\in\mathbb{P}_a} p^{-s}}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{\varphi(m)} \sum_\chi \chi(a^{-1}) \lim_{\substack{s\to 1 \\ s\in\mathbb{R}_{>1}}} \frac{f_\chi(s)}{\log\left(\frac{1}{s-1}\right)}$$

Però pel lema 1 tenim que en el sumatori valdrà 0 per totes les $\chi \neq \chi_0$, i valdrà $\frac{\chi(a^{-1})}{\varphi(m)}$ si $\chi = \chi_0$, però aleshores, $\frac{\chi(a^{-1})}{\varphi(m)} = \frac{1}{\varphi(m)}$; que és el que volíem veure. □

Notem que en aquesta demostració incloent tots els lemes previs, hem utilitzat molt el teorema de Landau, en particular el teorema 1. Però Landau no va ser el primer en demostrar això el teorema de Dirichlet. En aquest curs segurament no veurem la demostració que va donar Dirichlet al 1837-1838; però sí que veurem la que va donar Vallée-Poussin al 1896, 20 anys [1] abans de la de Landau; i voldrà demostrar el mateix: que $L(\chi, 1) \neq 0$.

Definició 1.7 Caràcters reals i complexos.

Diem que $\chi\colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$ és un caràcter de Dirichlet real si $\mathrm{Im}(\chi) \subset \mathbb{R}$. És a dir $\mathrm{Im}(\chi) \subset \{-1, 0, 1\}$. I direm que és complex altrament.

Definició 1.8 Caràcter conjugat

Direm $\overline{X}$ al caràcter de Dirichlet conjugat

$$\overline{X}\colon \mathbb{Z}_{\geq 1} \to \mathbb{C} \qquad \text{que envia } a \in \mathbb{Z} \text{ a } \overline{\chi}(a) = \overline{\chi(a)}$$

I no és massa difícil de veure que aquesta funció és un caràcter de Dirichlet del mateix mòdul.

Valleé-Poussin va distingir 2 casos: si χ és real o si és complexa. Aleshores, nosaltres veurem primer:

Proposició 1.6 $L(\chi, 1)$ **no s'anul·la si** χ **és complex.**

Si χ és un caràcter complex, aleshores $L(\chi, 1) \neq 0$.

Demostració. Suposem que $L(\chi, 1) = 0$, aleshores, primer veurem que $L(\overline{\chi}, 1) = 0$.

Com que el caràcter χ no és principal, tenim que la sèrie convergeix per $\sigma > 0$. A més, si restringim $L(\chi, s)$ i $L(\overline{\chi}, s)$ als reals positius, aleshores les funcions $\overline{L(\overline{\chi}, s)} = L(\chi, s)$ són iguals:

$$L(\chi, s) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} \qquad \overline{L(\overline{\chi}, s)} = \overline{\sum_{n\geq 1} \frac{\overline{\chi}(n)}{n^s}} = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$$

I com que les 2 són analítiques, i iguals en un conjunt amb un punt d'acumulació (en aquest cas els reals positius); han de ser iguals a tot arreu. Per tant:

$$\zeta_m(s) = \prod_{\theta} L(\theta, s) = L(\chi_0, s)L(\chi, s)L(\overline{\chi}, s) \prod_{\theta \neq \chi_0, \chi, \overline{\chi}} L(\theta, s)$$

Però sabem que $L(\chi_0, s)$ és meromorfa amb un pol en $s = 1$; també sabem que $L(\chi, s)$ i la seva conjugada són funcions holomorfes que s'anul·len en el 1 (per hipòtesi). I com que el producte també és una funció holomorfa, sabem que $\zeta_m(1) = 0$. I per tant, tindríem que ζ_m seria una funció holomorfa en $\sigma > 0$.

[1] No he trobat enlloc aquesta data, però em sembla que està en algun lloc dels apunts (tampoc he buscat excessivament).

Però això no pot ser:

$$\zeta_m(s) \geq \sum_{\substack{n>1 \\ (n,m)=1}} \frac{1}{n^\varphi}$$

□