SATO-TATE, *avant la lettre*

•

Pilar Bayer

Universitat de Barcelona

•

STNB 2013, 27è any

Tema: Avenços en la conjetura de Sato-Tate

UB, 2013.01.30

Contingut

1. Caràcters de Hecke
2. Un teorema de Hecke de no anul·lació (1918)
3. Un teorema de Hecke de densitat (1918)
4. El teorema de Hecke d'equidistribució (1920)
5. El teorema de densitat de Txebotarev
6. Sato-Tate per a corbes el·líptiques amb CM
7. Teoremes de densitat de Txebotarev-Sato-Tate

1. Caràcters de Hecke (1918)

Un tipus nou de funcions zeta i la seva relació amb la distribució dels nombres primers, I

K cos quadràtic real, $h =$ nombre de classes, $\varepsilon =$ unitat fonamental

Definició. *Donat un ideal* $\mathfrak{a}$, *tal que* $\mathfrak{a}^h = (\alpha)$, $\alpha \in K^*$, *sigui*

$$\lambda(\mathfrak{a}) = e^{\left(\frac{\pi i}{\log|\varepsilon|} \log\left|\frac{\alpha}{\alpha'}\right|\right)},$$

on α' *denota el conjugat galoisià de* α.

Propietats.

(i) El valor $\lambda(\mathfrak{a})$ no depèn del generador α escollit.

(ii) $|\lambda(\mathfrak{a})| = 1$, per a tot ideal $\mathfrak{a}$.

(iii) $\lambda(\mathfrak{ab}) = \lambda(\mathfrak{a})\lambda(\mathfrak{b})$, per a tot $\mathfrak{a}, \mathfrak{b}$.

Cas general

$[K:\mathbb{Q}] = n = r_1 + 2r_2 \qquad (r_1 > 0)$

$K^{(i)}, 1 \leq i \leq r_1$, conjugats reals

$K^{(r_1+j)}$, $1 \leq j \leq r_2$, conjugats complexos no equivalents

$S = \{\varepsilon_i\}_{1 \leq i \leq r}$ un sistema d'unitats tal que

$$\begin{vmatrix} 1 & \log|\varepsilon_1^{(1)}| & \cdots & \log|\varepsilon_r^{(1)}| \\ 1 & \log|\varepsilon_1^{(2)}| & \cdots & \log|\varepsilon_r^{(2)}| \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \log|\varepsilon_1^{(r+1)}| & \cdots & \log|\varepsilon_r^{(r+1)}| \end{vmatrix} \neq 0.$$

A partir de les entrades de la matriu inversa,

$$\begin{pmatrix} 1 & \log|\varepsilon_1^{(1)}| & \cdots & \log|\varepsilon_r^{(1)}| \\ 1 & \log|\varepsilon_1^{(2)}| & \cdots & \log|\varepsilon_r^{(2)}| \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \log|\varepsilon_1^{(r+1)}| & \cdots & \log|\varepsilon_r^{(r+1)}| \end{pmatrix} \begin{pmatrix} \frac{e_1}{n} & \frac{e_2}{n} & \cdots & \frac{e_{r+1}}{n} \\ e_1^{(1)} & e_2^{(1)} & \cdots & e_{r+1}^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ e_1^{(r)} & e_2^{(r)} & \cdots & e_{r+1}^{(r)} \end{pmatrix} = 1,$$

i donats enters arbitraris m_i, $1 \leq i \leq r$, defineix

$$\lambda(\mu) = \exp\left(2\pi i \sum_{q=1}^{r} m_q \sum_{p=1}^{r+1} e_p^{(q)} \log|\mu^{(p)}|\right),\ \mu \in K^*.$$

• Per a cada elecció dels enters $\{m_q\}$, s'obté així un *caràcter* de K^* *respecte de les unitats* S.

En el cas quadràtic real, tenim que $r = 1$,

$$\begin{pmatrix} 1 & \log|\varepsilon| \\ 1 & \log|\varepsilon'| \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2\log|\varepsilon|} & \frac{-1}{2\log|\varepsilon|} \end{pmatrix} = 1,$$

i tots els caràcters anteriors de K^* són potències del caràcter definit per

$$\lambda(\mu) = \exp\left(\pi i \frac{\log|\mu| - \log|\mu'|}{\log\varepsilon}\right).$$

- Definició del *caràcter d'un ideal* segons les unitats

$\{\mathfrak{r}_1, \ldots, \mathfrak{r}_h\}$ representants de I_K/P_K, de norma potència d'un primer

$$\mathfrak{r}_i^{c_i} = (\rho_i), \;\; \tau_i^{(p)} = \left| \sqrt[c_i]{\rho_i^{(p)}} \right|, \; 1 \leq p \leq n; \; 1 \leq i \leq h$$

Definició. Donat un ideal $\mathfrak{a} \neq (0)$ de K tal que $\mathfrak{a}\mathfrak{r}_1^{a_1} \ldots \mathfrak{r}_h^{a_h} = (\alpha)$,

$$\lambda(\mathfrak{a}) := \exp\left(2\pi i \sum_{q=1}^{r} m_q \sum_{p=1}^{r+1} e_p^{(q)} \log \left| \frac{\alpha^{(p)}}{\tau_1^{(p)a_1} \ldots \tau_h^{(p)a_h}} \right| \right).$$

Propietats.

(i) El valor $\lambda(\mathfrak{a})$ no depèn del generador α escollit.

(ii) $|\lambda(\mathfrak{a})| = 1$, per a tot ideal $\mathfrak{a}$.

(iii) $\lambda(\mathfrak{a}\mathfrak{b}) = \lambda(\mathfrak{a})\lambda(\mathfrak{b})$, per a tot $\mathfrak{a}, \mathfrak{b} \in I_K$.

- Caràcters bàsics. S'obtenen en prendre $m_q = 1, m_i = 0$ per a $i \neq q$:

$$\lambda_q(\mathfrak{a}) := \exp\left(2\pi i \sum_{p=1}^{r+1} e_p^{(q)} \log \left| \frac{\alpha^{(p)}}{\tau_1^{(p)a_1} \dots \tau_h^{(p)a_h}} \right| \right), \ 1 \leq q \leq r.$$

Proposició. *Dos ideals de K són idèntics si, i només si, posseeixen la mateixa norma i els mateixos caràcters bàsics.*

- Classes radials d'ideals

Definició. Dos ideals enters $\mathfrak{m}_1, \mathfrak{m}_2$ coprimers amb un ideal enter $\mathfrak{f}$ s'anomenen *equivalents mòdul* $\mathfrak{f}$ si existeix un ideal enter $\mathfrak{a}$, coprimer amb $\mathfrak{f}$, tal que

$$\mathfrak{a}\mathfrak{m}_1 = (\alpha_1), \quad \mathfrak{a}\mathfrak{m}_2 = (\alpha_2),$$

i, a més, $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{f}}$. Representem aquest grup de classes com $I_K(\mathfrak{f})/\mathfrak{f}$.

$$h(\mathfrak{f}) := \sharp I_K(\mathfrak{f})/\mathfrak{f} = \frac{1}{w(\mathfrak{f})} h\varphi(\mathfrak{f}).$$

Funcions zeta i funcions L

$$\zeta(s;\lambda) := \sum_{\mathfrak{r}} \frac{\lambda(\mathfrak{r})}{N(\mathfrak{r})^s},\ \Re(s) > 1$$

$$L(s;\lambda,\chi) := \sum_{\mathfrak{r}} \frac{\lambda(\mathfrak{r})\chi(\mathfrak{r})}{N(\mathfrak{r})^s},\ \Re(s) > 1.$$

La suma s'estén a tots els ideals enters no nuls de K.
λ és un caràcter segons un sistema d'unitats, S.
$\chi : I_K(\mathfrak{f})/\mathfrak{f} \to \mathbb{C}^*$ és un caràcter mòdul $\mathfrak{f}$.

Teorema. *Per a $\lambda \neq 1$, $\mathfrak{f} \neq 1$, la funció $\xi(s;\lambda,\chi) := \gamma(\lambda)A^s\Gamma(s;\lambda)L(s;\lambda,\chi)$ s'estén a una funció transcendent entera de s i satisfà l'equació funcional*

$$\xi(1-s;\overline{\lambda},\overline{\chi}) = W(\overline{\chi})\xi(s;\lambda,\chi),$$

amb $|W(\overline{\chi})| = 1$ i $A = (d_K N(\mathfrak{f})\pi^{-n}2^{-2r_2})^{1/2}$.

2. El teorema de Hecke de no anul·lació (1918)

Teorema. *Per a* $\lambda \neq 1$, *les funcions* $\zeta(s;\lambda)$ *i* $L(s;\lambda,\chi)$ *no s'anul·len en la recta* $\Re(s) = 1$.

• Primer demostra l'afirmació en el punt $s = 1$; després ho fa en tota la recta.

• Extreu les idees de la demostració de *Herr de la Vallée Poussin* sobre la no anul·lació de la funció zeta de Riemann en la recta $\Re(s) = 1$ (necessària per a la demostració del teorema dels nombres primers).

Recordem que

$$\zeta(s;\lambda) = \prod_{\mathfrak{p}} [1 - \lambda(\mathfrak{p}) N(\mathfrak{p})^{-s}]^{-1},$$

$$L(s;\lambda) = \prod_{\mathfrak{p}} [1 - \lambda(\mathfrak{p})\chi(\mathfrak{p}) N(\mathfrak{p})^{-s}]^{-1},$$

per a $\Re(s) > 1$.

Demostració. Siguin $s = 1 + \varepsilon$, $\varepsilon > 0$.

$$\log|\zeta(1+\varepsilon;\lambda)| = \log|\prod_{\mathfrak{p}}[1-\lambda(\mathfrak{p})N(\mathfrak{p})^{-1-\varepsilon}]^{-1}| = \sum_{m=1}^{\infty}\frac{1}{m}\sum_{\mathfrak{p}}\frac{\Re(\lambda(\mathfrak{p})^m)}{N(\mathfrak{p})^{(1+\varepsilon)m}}.$$

Atès que els valors de λ són complexos de mòdul 1, tindrem que

$$3 + 4\Re(\lambda) + \Re(\lambda^2) \;= 3 + 4\cos\varphi + \cos 2\varphi \;= 2(1+\cos\varphi)^2 \geq 0.$$

Per tant,

$$3\log|\zeta(1+\varepsilon)| + 4\log|\zeta(1+\varepsilon;\lambda)| + \log|\zeta(1+\varepsilon;\lambda^2)| \geq 0.$$

És a dir,

$$|\zeta(1+\varepsilon)|^3|\zeta(1+\varepsilon;\lambda)|^4|\zeta(1+\varepsilon;\lambda^2)| \geq 1.$$

O bé,

$$|\varepsilon\zeta(1+\varepsilon)|^3\left|\frac{\zeta(1+\varepsilon;\lambda)}{\varepsilon}\right|^4\varepsilon|\zeta(1+\varepsilon;\lambda^2)| \geq 1.$$

Suposem que $\zeta(1;\lambda) = 0$, per a un cert $\lambda \neq 1$. Aleshores,

- $\lim_{\varepsilon\to 0} \frac{\zeta(1+\varepsilon;\lambda)}{\varepsilon} = \zeta'(1;\lambda) \neq \infty$, ja que $\zeta(s;\lambda)$ és holomorfa.

- $\lim_{\varepsilon\to 0} \varepsilon\zeta(1+\varepsilon) \neq 0, \infty$, atès que la funció ζ de Riemann té un pol simple quan $s = 1$.

Per tant, i ja que $\zeta(s;\lambda)$ és holomorfa,

$$\lim_{\varepsilon\to 0} |\varepsilon\zeta(1+\varepsilon)|^3 \left|\frac{\zeta(1+\varepsilon;\lambda)}{\varepsilon}\right|^4 \varepsilon|\zeta(1+\varepsilon;\lambda^2)| = 0.$$

la qual cosa contradiu la desigualtat obtinguda: ≥ 1.

Així, $\zeta(1;\lambda) \neq 0$, per a tot $\lambda \neq 1$.

Teorema. *Siguin* $\lambda \neq 1$, $\chi \neq 1$. *Aleshores,*

(i) $\zeta(1;\lambda) \neq 0$.

(ii) $L(1;\lambda,\chi) \neq 0$.

La demostració en el cas de la funció L segueix passos paral·lels a l'anterior. Cal, però, tenir en compte que

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

segons la generalització que havia fet el propi Hecke del teorema de Dirichlet.

Teorema. *Siguin* $\lambda \neq 1$, $\chi \neq 1$. *Aleshores,*

(i) $\zeta(s;\lambda) \neq 0$, *quan* $\Re(s) = 1$,

(ii) $L(s;\lambda,\chi) \neq 0$, *quan* $\Re(s) = 1$.

En aquest cas, cal només tenir en compte que, per a tot $t \in \mathbb{R}$,

$$|\zeta(1+\varepsilon)|^3 |\zeta(1+\varepsilon+ti;\lambda)|^4 |\zeta(1+\varepsilon+2ti;\lambda^2)| \geq 1.$$

3. Un teorema de Hecke de densitat (1918)

- Per a cada ideal $\mathfrak{a} \neq (0)$ de K, considerem els valors dels caràcters bàsics:

$$(\lambda_1(\mathfrak{a}), \ldots, \lambda_r(\mathfrak{a})) \in U(1)^r.$$

Quan ens restringim a una classe mòdul $\mathfrak{f}$ d'ideals primers, les seves "coordenades" estan equidistribuïdes en $U(1)^r$. Més feblement:

Teorema. (I) *Siguin* $(x_1, \ldots, x_r) \in U(1)^r$ *i* $\delta > 0$ *elements arbitraris. Aleshores, cada classe d'ideals mòdul un ideal enter* $\mathfrak{f}$ *conté infinits ideals primers* $\mathfrak{p}$, *de grau* 1, *per als quals*

$$|\lambda_q(\mathfrak{p}) - x_q| < \delta, \quad \textit{per a } 1 \leq q \leq r.$$

Teorema. (II) *Donats* r *parells de nombres reals positius* (a_p, b_p), *amb* $a_p < b_p$, *per a cada ideal* $\mathfrak{a}$ *coprimer amb* $\mathfrak{f}$, *existeixen infinits ideals primers* $\mathfrak{p}$ *tals que* $\mathfrak{a}\mathfrak{p} \sim 1 \pmod{\mathfrak{f}}, \mathfrak{a}\mathfrak{p} = (\alpha)$ *i*

$$a_p < \left| \frac{\alpha^{(p)}}{\sqrt[n]{N(\alpha)}} \right| < b_p, \qquad 1 \leq p \leq r.$$

Teorema. (III) *Si, donat un ideal* $\mathfrak{a}$*, primer amb* $\mathfrak{f}$*, considerem tots els ideals primers tals que* $\mathfrak{a}\mathfrak{p} \sim 1 \pmod{\mathfrak{f}}, \mathfrak{a}\mathfrak{p} = (\alpha)$*, aleshores el conjunt de punts de* $\mathbb{R}^r$ *de coordenades*

$$c_q(\mathfrak{p}\mathfrak{a}) = \sum_{p=1}^{r+1} e_p^{(q)} \log \alpha^{(p)}, \quad 1 \leq q \leq r,$$

és dens mòdul 1*.*

Demostració. Sigui $\lambda \neq 1$. Primer veurem que la funció

$$P(s; \lambda, \mathfrak{a}) := \sum_{\substack{\mathfrak{p} \\ \mathfrak{p}\mathfrak{a} \sim 1(\mathfrak{f})}} \frac{\lambda(\mathfrak{p}\mathfrak{a})}{N(\mathfrak{p})^s}$$

és regular en el punt $s = 1$ (fins i tot en $\Re(s) = 1$). Per a això, escrivim

$$\log L(s; \lambda, \chi) = \sum_{\mathfrak{p}} \frac{\lambda(\mathfrak{p})\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + g(s),$$

on $g(s)$ és regular per a $\Re(s) > \frac{1}{2}$.

Recordem que

$$\sum_{\chi} \chi(\mathfrak{m}) = \begin{cases} 0 & \text{si } \mathfrak{m} \not\sim 1 \pmod{\mathfrak{f}}, \\ h(\mathfrak{f}) & \text{altrament.} \end{cases}$$

En sumar per a tots els χ:

$$\begin{aligned} \lambda(\mathfrak{a}) \sum_{\chi} \chi(\mathfrak{a}) \log L(s; \lambda, \chi) &= h(\mathfrak{f}) \sum_{\substack{\mathfrak{p} \\ \mathfrak{p}\mathfrak{a} \sim 1(\mathfrak{f})}} \frac{\lambda(\mathfrak{p}\mathfrak{a})}{N(\mathfrak{p})^s} + g_1(s), \\ &= h(\mathfrak{f}) P(s; \lambda, \mathfrak{a}) + g_1(s) \end{aligned}$$

amb $g_1(s)$ regular per a $\Re(s) > \frac{1}{2}$.

Pel que hem provat abans, $P(s; \lambda, \mathfrak{a})$ serà regular per a $\Re(s) = 1$.

En canvi, $P(s; 1, \mathfrak{a}) \sim \dfrac{1}{h(\mathfrak{f})} \log(s-1), \quad$ quan $s \to 1$.

A fi de veure la densitat mòdul 1, construïm un polinomi trigonomètric:

$$\varphi(x_1,\ldots,x_r) = a_0 + \sum_{m_1,\ldots,m_r} a(m_1,\ldots,m_r)e^{2\pi i(m_1x_1+\cdots+m_rx_r)}$$

que satisfaci:

(i) $a_0 > 0$.

(ii) Si $J \subseteq W = [0,1]^r$ és un cub i $A := W \setminus J$, aleshores $\varphi(x_1,\ldots,x_r) < 0$, per a tot $(x_q) \in A$.

Ara considerem:

$\varphi(\mathfrak{p})$	valor del polinomi φ en el punt de coordenades $c_p(\mathfrak{ap})$,
$\varphi_J(\mathfrak{p})$	valor del polinomi φ en els punts que, mòdul 1, són de J,
$\varphi_A(\mathfrak{p})$	valor del polinomi φ en els punts que, mòdul 1, són de A.

Atès que

$$\sum_{\mathfrak{a}\mathfrak{p}\sim 1(\mathfrak{f})} \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})^s} \sim a_0 P(s;1,\mathfrak{a}) + \sum_{m_1,\ldots,m_r} a(m_1,\ldots,m_r) P(s;\lambda_1^{m_1},\lambda_2^{m_2}\ldots\lambda_r^{m_r},\mathfrak{a}) \tag{1}$$

i, a més,

$$\sum \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p}_J)^s} + \sum \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p}_A)^s} < \sum \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p}_J)^s},$$

la sèrie

$$\sum_{\mathfrak{p}_J} \frac{\varphi(\mathfrak{p})}{N(\mathfrak{p}_J)^s}$$

és divergent quan $s \to 1$. Per tant, aquesta sèrie ha de contenir infinits sumands i, en particular, la sèrie

$$\sum_{\mathfrak{p}_J} \frac{1}{N(\mathfrak{p}_J)}$$

serà, també, divergent. $\square$.

Conjectures (Hecke, 1918)

- $\displaystyle\sum_{\mathfrak{p}_J} \frac{1}{N(\mathfrak{p}_J)^s} = \frac{V_J}{h(\mathfrak{f})} \log \frac{1}{s-1} + g(s),$

- $\pi_J(x) \sim \dfrac{V_J}{h(\mathfrak{f})} \dfrac{x}{\log x}, \quad (x \to \infty)$

V_J denota el volum de J

$g(s)$ és una funció fitada quan $s \longrightarrow 1$

$\pi_J(x)$ denota el nombre d'ideals $\mathfrak{p}_J$ de norma $\leq x$.

Zum Beweise [...] hätte man an Stelle von φ diejenige *unendliche* Fourierreihe zu nehmen, die in A gleich 0, in J glecih 1 ist, und in der Identität (1) hätten wir auf der linken Seite dann eine Reihe, deren analytischer Character erst durch eine besondere Untersuchung festgestellt werden müste.

4. El teorema de Hecke d'equidistribució (1920)

Größencharakteren

- k quadràtic real, ε unitat fonamental, $\alpha \in k^*$:

$$\lambda(\alpha) = \exp\left(\frac{\pi i}{\log|\varepsilon|} \log\left|\frac{\alpha}{\alpha'}\right|\right)$$

- k quadràtic imaginari, $-d$ $(d > 4)$ discriminant, $\alpha \in k^*$:

$$\lambda(\alpha) = \left(\frac{\alpha}{|\alpha|}\right)^2$$

satisfan que estan ben definides sobre els ideals (α) i, a més,

$$\lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta).$$

$[k:\mathbb{Q}] = n = r_1 + 2r_2,\ r = r_1 + r_2 - 1$

$k^{(p)}$ els conjugats, $c_q(x)$ coordenades:

$$x \in k^*, \quad x_p > 0 \quad (1 \le p \le r_1), \quad x_{p+r_2} = \overline{x}_p \quad (r_1 + 1 \le p \le r + 1)$$

- Cerca les funcions contínues més generals tals que

(i) $F(x_1, \ldots, x_{r+1})F(y_1, \ldots, y_{r+1}) = F(x_1y_1, \ldots, x_{r+1}y_{r+1})$,

(ii) $F(\eta^{(1)}x_1, \ldots, \eta^{(r+1)}x_{r+1}) = F(x_1, x_2, \ldots, x_{r+1})$,

per a tota unitat η mòdul $\mathfrak{f}$.

La solució és donada per:

$$F(x) = N(x)^s \prod_{q=1}^{r} \exp(2\pi i m_q c_q(x)) \prod_{p=r_1+1}^{r} \left(\frac{x_p}{|x_p|} \exp\left(i \sum_{k=1}^{n} \vartheta_k^{(p)} c_k(x) \right) \right)^{a_p},$$

on

$\eta_k^{(p)} = |\eta_k^{(p)}| e^{i\vartheta_k^{(p)}}$, sistema fonamental d'unitats totalment positives,

$\eta_k^{(p)}$, $1 \le p \le r_1$; $\quad \eta_k^{(p)} = -\eta_k^{(p+r_2)}$, $r_1 + 1 \le p \le r + 1$; $\quad \eta_k^{(p)} \equiv 1$ (ƒ),

$s \in \mathbb{C}$, $\quad m_q \in \mathbb{Z}$ enters arbitraris,

$a_p \in \mathbb{Z}, a_p > 0, a_p a_{p+r_2} = 0$ satisfan certes condicions de congruència.

- $s = 0$, $\quad \lambda(x) := F(x)$ **Größencharakter** de x mòdul ƒ

Größencharakter d'ideals

$[k:\mathbb{Q}]=n, \quad \langle \mathfrak{b}_1,\dots,\mathfrak{b}_e\rangle = I_k/P_k; \quad \mathfrak{a}\in I_k$

$$\mathfrak{a}=(\rho)\mathfrak{b}_1^{a_1},\dots,\mathfrak{b}_e^{a_e}, \quad \rho\in k^*$$

$$\mathfrak{b}_i^{h_i}=(\beta_i), \quad \beta\in k; \quad h_i \text{ l'enter més petit}$$

Hecke considera *nombres ideals* $\widehat{\beta}_i$ (en el $HCF(k)$, per exemple)

$$\widehat{\beta}^{h_i}=\varepsilon_i\beta_i, \quad \varepsilon_i \text{ unitat de } k$$

Grups de nombres en el sentit de Weber:

$$\mathfrak{Z}=\langle \beta_i, \text{tots seus els associats}, k^*; 1\le i\le e\rangle$$

Grups de congruència de nombres mòdul $\mathfrak{f}=(\widehat{\varphi})$, $\mathfrak{f}$ ideal enter de k

$$\mathfrak{Z}(\mathfrak{f}): \qquad \widehat{\alpha}\equiv\widehat{\beta}\ (\mathrm{mod}\,\mathfrak{f})$$

$$\mathfrak{Z}_0(\mathfrak{f}): \qquad \widehat{\alpha}\equiv\widehat{\beta}\ (\mathrm{mod}\,\mathfrak{f}), \quad \frac{\widehat{\alpha}}{\widehat{\beta}} \text{ totalment positiu}$$

Grups de congruència d'ideals en el sentit de Weber:

$$\mathfrak{I}(\mathfrak{f}): \qquad \widehat{\alpha} \equiv \varepsilon\widehat{\beta} \pmod{\mathfrak{f}}$$

$$\mathfrak{I}_0(\mathfrak{f}): \qquad \widehat{\alpha} \equiv \varepsilon\widehat{\beta} \pmod{\mathfrak{f}}, \quad \frac{\widehat{\alpha}}{\varepsilon\widehat{\beta}} \text{ totalment positiu}$$

Größencharakter d'una classe de congruència d'ideals

$$\lambda((\widehat{a})) = \lambda(\widehat{a})\chi(\widehat{a})v(\widehat{a}).$$

Teorema. *Sigui $\lambda(\widehat{\alpha})$ un Größencharakter d'un ideal $(\widehat{\alpha})$ mòdul $\mathfrak{f}$. La funció zeta definida per*

$$\zeta(s;\lambda) := \sum_{\widehat{\alpha}} \frac{\lambda((\widehat{\alpha}))}{N(\widehat{\alpha})^s},\ \Re(s) > 1,$$

on el sumatori s'estén a tots els nombres ideals enters $\widehat{\alpha}$ no associats, és una funció analítica que admet el desenvolupament en producte infinit

$$\prod_{\widehat{\pi}} \frac{1}{1-\lambda((\widehat{\pi}))N(\widehat{\pi})^{-s}}.$$

Teorema. *La funció $\xi(s;\lambda) := \gamma(\lambda)A^s\Gamma(s;\lambda)\zeta(s;\lambda)$ és una funció entera per a tot character*

$$\lambda((\widehat{\mu})) = \lambda(\widehat{\mu})\chi(\widehat{\mu})v(\widehat{\mu})$$

que no satisfaci simultàniament les condicions

$$\lambda(\widehat{\mu})v(\widehat{\mu}) \equiv 1, \quad \chi \text{ el caràcter principal mòdul } \mathfrak{f}.$$

A més, satisfà l'equació funcional

$$\xi(1-s;\overline{\lambda}) = W(\overline{\lambda})\xi(s;\lambda).$$

La distribució asimptòtica dels caràcters dels ideals primers

Teorema. *Per a tot Großencharackter no trivial, és* $\zeta(1;\lambda) \neq 0$.

Demostració. Es fa con la que hem vist de l'article de l'any 1918. □

Teorema. *Sigui* $\lambda(\hat{\alpha})$ *un Großencharackter primitiu del nombre* $\hat{\alpha}$ *mòdul* $\mathfrak{f}$. *Suposem que* $(\hat{\pi})$ *recorre tots els ideals primers tals que* $\hat{\alpha} \equiv \hat{\pi} \pmod{\mathfrak{f}}$ *i el quocient* $\dfrac{\hat{\pi}}{\hat{\alpha}}$ *és totalment positiu. Aleshores,*

$$\sum_{|N(\hat{\pi})|<x} \lambda((\hat{\pi})) = O(xe^{-c\sqrt{\log x}}),$$

$$\pi(x) = \sum_{N(\hat{\pi})<x} 1 = \frac{1}{h_0(\mathfrak{f})} \int_2^x \frac{u}{\log u} + O(xe^{-c\sqrt{\log x}}).$$

La demostració dels resultats anteriors es fa seguint el mateix mètode emprat per Landau. Fent ús dels teoremes de no anul·lació en $s = 1$ en el cas de la funció zeta de Dedekind, $\zeta_K(s)$, i $L(s, \chi)$ associada a un caràcter del grup de classes, Landau havia obtingut que

Teorema. (Landau, 1918)

$$\sum_{N(\mathfrak{p})<x} \lambda((\mathfrak{p})) = O(xe^{-c\sqrt{\log x}}), \tag{2}$$

$$\pi(x) = \sum_{N(\mathfrak{p})<x} 1 = \int_2^x \frac{u}{\log u} + O(xe^{-c\sqrt{\log x}}). \tag{3}$$

Aquests teoremes es poden demostrar via els *teoremes tauberians* (que refinen el mètode de sumació d'Abel).

Teorema. **(Landau, 1918)**

$$\sum_{N(\mathfrak{p})<x} \lambda((\mathfrak{p})) = O(xe^{-c\sqrt{\log x}}), \tag{4}$$

$$\pi(x) = \sum_{N(\mathfrak{p})<x} 1 = \int_2^x \frac{u}{\log u} + O(xe^{-c\sqrt{\log x}}). \tag{5}$$

Aquests teoremes es poden demostrar via els *teoremes tauberians* (que refinen el mètode de sumació d'Abel).

Alfred Tauber (Bratislava 1866–Theresienstadt 1942)

Corol·lari. *De les fórmules asimptòtiques 4 i 5 es dedueix, en considerar la successió de sumes parcials:*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{h=1}^{N} \lambda(\widehat{\pi}_h) = 0, \tag{6}$$

on el sumatori s'estén a una successió d'elements ordenats per normes creixents i tals que la classe mòdul $\mathfrak{f}$ *dels ideals* $(\widehat{\pi}_h)$ *és fixada.*

Teorema. **(d'equidistribució, Hecke 1920)** *Sigui* $\mathfrak{I}$ *un domini contingut en* $[0,1]^n$. *Sigui* $\pi_{\mathfrak{I}}(x;\widehat{\rho},\mathfrak{f})$ *el nombre d'ideals primers* $(\widehat{\pi})$ *per als quals*

$$\widehat{\pi} \equiv \widehat{\rho} \pmod{\mathfrak{f}}, \quad \frac{\widehat{\pi}}{\widehat{\rho}} \text{ és totalment positiu}, \quad |N(\widehat{\pi})| \leq x$$

i tals que els punts de coordenades $x_q = w_q(\widehat{\pi})$ *mòdul* 1 *pertanyen a* $\mathfrak{I}$. *Aleshores*

$$\lim_{x\to\infty} \frac{\pi_{\mathfrak{I}}(x;\widehat{\rho},\mathfrak{f})}{\dfrac{x}{\log x}} = \frac{\mathrm{vol}(\mathfrak{I})}{h_0(\mathfrak{f})}.$$

Demostració del teorema d'equidistribució

Hecke reflexiona que cada Großencharkter primitiu mòdul $\mathfrak{f}$ es pot escriure en la forma

$$\lambda(\widehat{\alpha}) = e^{2\pi i \omega(\widehat{\alpha})},$$

on $\omega(\widehat{\alpha})$ denota una funció dels n conjugats $\widehat{\alpha}^{(p)}$ que és real mòdul 1, contínua, i unívocament determinada. En funció dels caràcters bàsics:

$$\lambda_k(\widehat{\alpha}) = e^{2\pi i \omega_k(\widehat{\alpha})}, \qquad 1 \leq k \leq n-1,$$

$$\lambda(\widehat{\alpha}) = \lambda_1^{m_1}(\widehat{\alpha}) \cdots \lambda_{n-1}^{m_{n-1}}(\widehat{\alpha}), \quad m_i \in \mathbb{Z}.$$

Per tant, el límit (6) es pot escriure com

$$\lim_{N\to\infty} \frac{1}{N} \sum_{h=1}^{N} e^{2\pi i [m_1\omega_1(\widehat{\pi}_h) + \cdots + m_{n-1}\omega_{n-1}(\widehat{\pi}_{n-1})]} = 0, \tag{7}$$

essent la igualtat vàlida per a totes les tries dels exponents m_i enters.

Però ara Herr Weyl ha demostrat (1916) que la condició (7) és necessària i suficient a fi que els infinits punts P_h mòdul 1 de coordenades

$$P_h : (\omega_1(\widehat{\pi}_h), \ldots, \omega_{n-1}(\widehat{\pi}_h))$$

estiguin equidistribuïts en el cub $[0,1]^{n-1}$.

Quan això és així, se satisfà que

$$\lim_{N\to\infty} \frac{z(N)}{N} = \text{vol}(\mathfrak{I}),$$

on $z(N)$ és el nombre de punts P_h, $1 \leq h \leq N$, de coordenades en $\mathfrak{I}$.

En tenir en compte la fórmula (5) per a N, s'obté l'afirmació del teorema d'equidistribució.

Una aplicació a les formes nòrmiques

Escrivim $\mathfrak{a} = (\widehat{\alpha})$. Considerem els n nombres

$$\left| \frac{\widehat{\alpha}^{(p)}}{\sqrt[n]{N(\widehat{\alpha})}} \right|, \quad 1 \leq p \leq n,$$

unívocament determinats llevat d'una unitat mòdul $\mathfrak{f}$ quan s'imposa que les r_1 primers coordenades són totalment positives. Per mitjà d'una base de l'ideal els podem escriure com

$$\mu = z_1\alpha_1 + \cdots + z_n\alpha_n.$$

Ara definim la forma primitiva en n variables, de coeficients enters:

$$F(z_1, \ldots, z_n) = \frac{1}{N(\mathfrak{a})} \prod_{p=1}^{n} (\alpha_1^{(p)} z_1 + \cdots + \alpha_n^{(p)} z_n).$$

Aleshores, la forma F representa infinits primers encara que les infinites coordenades enteres descriguin mòdul 1 un domini tan petit com es vulgui.

Una observació sobre el cub unitat

- $U(N) := \{A \in \mathrm{GL}(N,\mathbb{C}) : AA^* = 1\}$, és un grup de Lie compacte i $T := \{\mathrm{diag}(e^{i\theta_1},\ldots,e^{i\theta_N}),\ \theta_j \in [0,2\pi)\}$ n'és un tor maximal.

- Tota matriu de $U(N)$ és diagonalizable i els seus valors propis són nombres complexos de mòdul 1. Per tant, el conjunt $X(U(N))$ de les classes de conjugació de $U(N)$ s'identifica amb $[0,2\pi)^N$.

- Si $f = U(N) \to \mathbb{C}$ és una funció que és constant sobre les classes de conjugació, *la fórmula d'integració de Weyl* ens diu que

$$\int_{U(N)} f d\mu = \int_{[0,2\pi]^N} f(\theta_1,\ldots,\theta_N)\det(S_N(\theta_k-\theta_j))\frac{d\theta_1\cdots d\theta_N}{N!(2\pi)^N},$$

on $S_N(\theta) = \frac{\sin\frac{N\theta}{2}}{\sin\frac{\theta}{2}}$, amb la qual cosa podem apreciar la projecció de la mesura de Haar de $U(N)$ en el conjunt $X(U(N))$.

La fórmula d'integració de Weyl per a SU(2):

En aquest cas,

$$G = SU(2), \quad T = U(1)$$

$$\int_{U(2)} f d\mu = 2 \int_0^{2\pi} f(\theta) \sin^2(\theta) \frac{d\theta}{2\pi}$$

5. El teorema de densitat de Txebotarev

Sigui G el grup de Galois finit d'una extensió $L|k$ de cossos de nombres i sigui X el conjunt de classes de conjugació de X. En aquest cas, μ_* coincideix amb la mesura discreta de X. Sigui S el conjunt de primers que ramifiquen. Per a cada $\mathfrak{p} \notin S$, sigui $x_\mathfrak{p}$ l'element de Frobenius, $\mathrm{Frob}_\mathfrak{p} \in X$, en $\mathfrak{p}$.

Teorema. *Per a tota representació complexa ρ de* $\mathrm{Gal}(L|k)$*, la funció L d'Artin $L(\rho, s)$ satisfà que $L(\rho, 1) \neq 0$.*

Demostració. Pel teorema de Brauer, tot caràcter de G és combinació lineal amb coeficients enters dels caràcters induïts pels subgrups elementals. La funció L d'un caràcter induït coincideix amb la funció L del caràcter. En els grups elementals, tots els caràcters irreductibles són induïts per caràcters de dimensió 1. Per la teoria de cossos de classes, la funció L d'un caràcter de dimensió 1 coincideix amb la funció L d'un caràcter de Hecke. I sabem que aquestes no s'anul·en en $s = 1$.

Com que, a més, se satisfan els teoremes tauberians, tenim el teorema d'equidistribució:

Teorema. (Txebotarev) *Sigui c una classe de conjugació de* $\mathrm{Gal}(L|k)$. *La densitat dels primers $\mathfrak{p}$ per als quals* $\mathrm{Frob}_{\mathfrak{p}} = c$ *és* $\dfrac{|c|}{[L:k]}$.

6. Sato-Tate per a corbes el·líptiques amb CM

Sigui $E|k$ una corba el·líptica amb CM definida sobre un cos k de nombres. Aleshores, existeix un caràcter de Hecke per al qual

$$L(E,s) = L(\psi,s).$$

És a dir, $\psi(\mathfrak{p}) = \alpha(\mathfrak{p})$, per a tot $\mathfrak{p}$ que no divideix el conductor de E (Deuring).

Per tant, $L(\psi,s) \neq 1$ i, pel teorema d'equidistribució de Hecke:

Corol·lari. *Els valors* $x_{\mathfrak{p}} = \alpha(\mathfrak{p})/N\mathfrak{p}^{1/2}$ *estan* μ_**-equidistribuïts en* $U(1)$.

Corol·lari. *Els valors de les traces* $a(\mathfrak{p})/N\mathfrak{p}^{1/2}$ *estan* μ_**-equidistribuïts en* $[-2,2]$ *respecte de la mesura*

$$\mu_{cm} = \frac{1}{\pi}\frac{dx}{\sqrt{4-x^2}},$$

on dx *denota la mesura de Lebesgue en* $[-2,2]$.

Corol·lari. *Els valors de les traces* $a(\mathfrak{p})/N\mathfrak{p}^{1/2}$ *estan* μ_{cm}*-equidistribuïts en* $[-2,2]$ *respecte de la mesura*

$$\mu_{cm} = \frac{1}{\pi}\frac{dx}{\sqrt{4-x^2}},$$

on dx *denota la mesura de Lebesgue en* $[-2,2]$*.*

El resultat s'obté en projectar μ_* en $[-2,2]$ i tenier en compte que

$$a(\mathfrak{p}) = \alpha(\mathfrak{p}) + \overline{\alpha}(\mathfrak{p}).$$

En aquest cas, Sato-Tate = Davenport-Hasse-Deuring-Hecke.

7. Teoremes de densitat de Txebotarev-Sato-Tate

(Murty-Murty)

$E|\mathbb{Q}$, corba el·líptica sense CM; $L|\mathbb{Q}$

$G = \mathrm{SU}(2) \times \mathrm{Gal}(L|\mathbb{Q})$

S conjunt de primers de mala reducció de E o bé ramificats en L

μ_* mesura de Haar de G

$x_p = \rho_{E,\ell}(\mathrm{Frob}_p)/p^{(1/2)}$, per a $p \notin S$

Teorema. (i) *Per a tot $m > 0$ o bé ρ no trivial, la funció $L(Sym^m(\mathbb{C}^2) \otimes \rho, s)$ és holomorfa i no nul·la per a $\Re(s) \geq 1$.*

(ii) *Els x_p són μ_*-equidistribuïts.*

(iii) *Per a tota classe de conjugació de* $\mathrm{Gal}(L|\mathbb{Q})$, *la subsuccessió dels $a_p/p^{1/2}$ tals que* $\mathrm{Frob}_p = c$ *és μ_{ST}-equidistribuïda.*

$E|\mathbb{Q}$, corba el·líptica amb CM definida definida sobre k

$G = \mathrm{U}(1) \times \mathrm{Gal}(L|k)$

S conjunt de primers de mala reducció de E o bé ramificats en L

μ_* mesura de Haar de G

$x_p = \rho_{E,\ell}(\mathrm{Frob}_p)/p^{(1/2)}$, per a $p \notin S$

Teorema. (i) *Per a tot* $a \in \mathbb{Z}$, $a \neq 0$, *la funció* $L(\psi_a \otimes \rho, s)$ *és holomorfa i no nul·la per a* $\Re(s) \geq 1$.

(ii) *Els* x_p *són* μ_**-equidistribuïts.*

(iii) *Per a tota classe de conjugació de* $\mathrm{Gal}(L|\mathbb{Q})$, *la subsuccessió dels* $a_p/p^{1/2}$ *tals que* $\mathrm{Frob_p} = c$ *és* μ_{mc}*-equidistribuïda.*