(Don Zagier)

Sèries de Dirichlet

$\left(f(z) = \sum_{n\geq 0} a_n z^n \right.$. Sabem $\exists\, r \geq 0$ tq: $\begin{cases} |z|<r \Rightarrow f(z) \text{ convergència uniforme } (\Rightarrow f \text{ holomorfa}) \\ |z|>r \Rightarrow \sum a_n z^n \text{ divergeix} \end{cases}$ $\left.\right)$

$\varphi(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ on $\begin{cases} s_0 \in \mathbb{C} \\ a_n \in \mathbb{C} \\ \lambda_n \in \mathbb{R}, \quad \lambda_1 < \lambda_2 < \cdots \longrightarrow \infty \end{cases}$ (sèrie de Dirichlet generalitzada)

Ex: $\lambda_n = n$: $\varphi(s) = \sum a_n e^{-ns} = \sum a_n (e^{-s})^n = f(e^{-s})$

Per tant, la sèrie serà convergent a la dreta d'una certa abscissa s_0, i divergent a l'esquerra.

Ex 2 (s-Dir. ordinària): $\boxed{\lambda_n = \log n} \Rightarrow \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \varphi(s)$.

Prop: Si la sèrie convergeix per $s = s_1$ i si $\mathrm{Re}(s_2) > \mathrm{Re}(s_1)$, aleshores la sèrie convergeix en s_2. (a partir d'on, $s = \sigma + it$).
i $\varphi(s)$ és holomorfa.

Cor: $\exists\, \sigma_0 \in [-\infty, +\infty]$ tq. $\begin{cases} \sigma > \sigma_0 \Rightarrow \text{Convergència i } \varphi(s) \text{ holomorfa.} \\ \sigma < \sigma_0 \Rightarrow \text{divergència} \end{cases}$

Notació: $A(N) = \sum_{n=1}^{N} a_n$; $A(M,N) = \sum_{M}^{N} a_n \quad 1 \leq M \leq N$.

Prova: WLOG podem suposar $s_1 = 0$ $\left(\begin{matrix} s \to s+s_1 \\ a_n \to a_n e^{-\lambda_n s_1} \end{matrix} \right)$

$$\sum_{1}^{N} \frac{a_n}{n^s} = \sum_{1}^{N} \frac{A(n)-A(n-1)}{n^s} = \sum_{n=1}^{N-1} A(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + \frac{A(N)}{N^s}$$

Obs que $\left| \frac{1}{n^s} - \frac{1}{n+1^s} \right| = \left| s \int_{\lambda_n}^{\lambda_{n+1}} e^{-su}\, du \right| \leq |s| \int_{\lambda_n}^{\lambda_{n+1}} e^{-\sigma u}\, du =$

$$= \frac{|s|}{\sigma} \left(e^{-\lambda_n \sigma} - e^{-\lambda_{n+1}\sigma} \right)$$

Per tant, $\left| \sum_{M}^{N} \frac{a_n}{n^s} \right| = \left| \sum_{n=M}^{N-1} |A(M,N)| \left| e^{-\lambda_n s} - e^{-\lambda_{n+1} s} \right| + \frac{|A(M,N)|}{|e^{\lambda_N s}|} \right| \leq$

$$\leq \varepsilon \frac{|s|}{\sigma} \left(e^{-\lambda_M \sigma} - e^{-\lambda_N \sigma} \right) + \varepsilon e^{-\lambda_N \sigma} \longrightarrow 0$$

Prop: $\sigma_0 = \begin{cases} \limsup_{N\to\infty} \left(\dfrac{\log|A(N)|}{\lambda_N} \right) & \text{si } \sum_1^\infty a_n \text{ divergeix} \\ \limsup_{N\to\infty} \left(\dfrac{\log|\sum_n^\infty a_n|}{\lambda_N} \right) & \text{si } \sum_1^\infty a_n \text{ convergeix} \end{cases}$

En el cas ordinari correspon a $\inf\{\alpha \mid A(N) = \mathcal{O}(N^\alpha)\}$.

Dem: Exercici. (comparar $\sum a_n$ i $\sum \frac{a_n}{e^{\lambda_n s}}$)

A partir d'ara, considerem Dirichlet ordinàries.

σ_0 = abscissa de convergència, σ_A = abscissa de convergència absoluta. (σ_A abc. conv. de $\sum \frac{|a_n|}{n^s}$)

Corollari: $\sigma_0 \le \sigma_A \le \sigma_0 + 1$ (pot ser en general, p. ex. $\sum \frac{(-1)^n}{\sqrt{n}} (\log n)^{-s}$ té $\sigma_0 = -\infty$, $\sigma_A = +\infty$)

Exemple: $\zeta(s) = \sum_1^\infty \frac{1}{n^s}$ $\quad a_n = 1$, $A(N) = N = \mathcal{O}(N^\alpha) \Leftrightarrow \alpha \ge 1 \Rightarrow \sigma_0 = \sigma_A = 1$.

Exemple: $\zeta^-(s) = \sum_1^\infty \frac{(-1)^{n+1}}{n^s}$ $\quad a_n = (-1)^{n+1}$; $\sigma_0 = 0$, $\sigma_A = 1$

Podem escriure $\zeta^-(s) = \zeta(s) - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \dots\right) = \left(1 - \frac{2}{2^s}\right)\zeta(s)$

Això vol dir que $\zeta(s)$ és meromorfa per $\sigma > 0$, amb pols simples (com a molt)

pol com a molt quan $1 = 2^{1-s} \Leftrightarrow s - 1 = \frac{2\pi i n}{\log 2}$

Provem ara $(a_n) = \{1, 1, -2, 1, 1, -2, \dots\}$.

$A(N) = \{1, 2, 0, 1, 2, 0, 1, 2, 0, \dots\} = \mathcal{O}(N^0)$.

Es pot veure que $\left(1 - \frac{1}{3^{s-1}}\right)\zeta(s)$. Per tant $\sigma_0 = 0$, $\sigma_1 = 1$

i per tant és holomorfa; per tant $\zeta(s)$ tindria pols com a molt,

$$s \in \left(1 + \frac{2\pi i}{\log 2}\mathbb{Z}\right) \cap \left(1 + \frac{2\pi i}{\log 3}\mathbb{Z}\right) = \{1\}$$

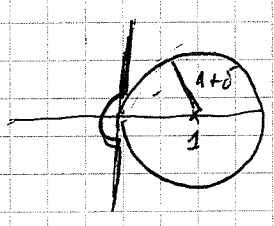
Per $s = 1$, $\sum_1^\infty \frac{1}{n} = \infty$, per tant té un pol

Th (Landau): Si $\varphi(s) = \sum \frac{a_n}{n^s}$ és Dirichlet ordinària amb $a_n \ge 0$ $(\forall n)$, el punt $s = \sigma_0 (= \sigma_A)$ és una singularitat de φ

Exemple: $\zeta^-(s)$ $\sigma_0 = 0$, però en canvi és una funció holomorfa a tot $\mathbb{C}$.
(no s'aplica Landau ja que $a_n \not\geq 0$.

Prova (de Landau):

Suposem que $\sigma_0 = 0$. Suposem que es pot prolongar.



Aleshores es pot prendre un cercle de radi $1+\delta$ amb δ prou petit (i centre 1) com perquè sigui contingut en la regió amplada de convergència.

(convergent, per tant, $\{|s-1| \leq 1+\delta\}$. Podem, per fer, calcular $\varphi(-\delta)$:

$$\varphi(-\delta) = \sum_{k=0}^{\infty} \frac{(-1-\delta)^k}{k!} \varphi^{(k)}(1) = \sum_{k=0}^{\infty} \frac{(1+\delta)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n}{n^s} (\log n)^k = \left(\text{podem intercanviar sumatoris, pq. a' abs. convergent}\right)$$

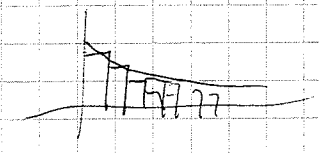
$$= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \sum_{k=0}^{\infty} \frac{(1+\delta)^k}{k!} (\log n)^k = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{(1+\delta)\log n} = \sum_{1}^{\infty} a_n n^{\delta} \to \infty !!$$ perquè

això significaria que la sèrie és convergent per $-\delta$, contradicció $\sigma_0 = 0$!!.

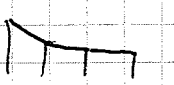
Podem substituir el pol a $\zeta(s)$ (podem veure que el seu residu és 1):

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{dt}{t^s} = \sum_{n=1}^{\infty} \int_n^{n+1} \underbrace{\left(\frac{1}{n^s} - \frac{1}{t^s}\right)}_{|\,| \leq \frac{|s|}{\sigma}\left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\right)} dt \leq \frac{|s|}{\sigma}$$

Si, en comptes de considerar

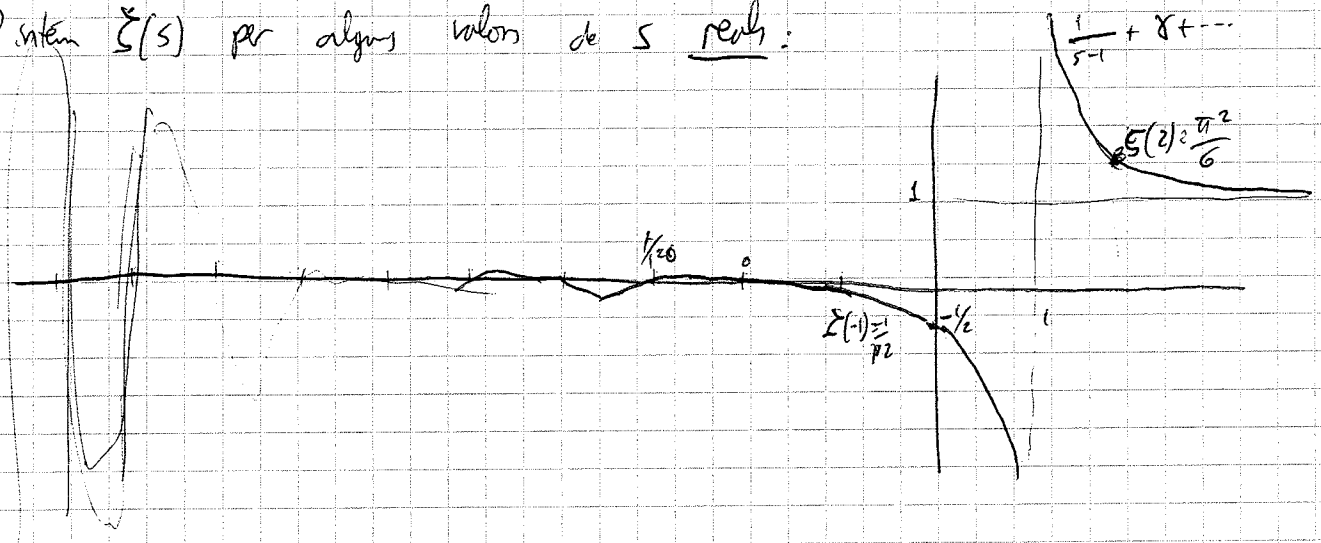


aproximem per considerem aproximar també



, obtenim que es pot prolongar cap a l'esquerra.

Pintem $\zeta(s)$ per alguns valors de s reals:



Th: (Prolongament analític a valors especials de sèries de Dirichlet ordinàries):

Sigui $\varphi(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ una sèrie de Dirichlet, convergent per $\sigma \gg 0$. ($\exists c : a_n \leq O(n^c)$)

Escrivim $f(t) := \sum_{n\geq 1} a_n e^{-nt}$, que convergirà per $t > 0$ (ja que a_n té creixement polinomial).

Si $f(t) \sim b_0 + b_1 t + b_2 t^2 + \cdots \quad (t \to 0)$

Aleshores

(a) $\varphi(s)$ és entera (holomorfa a tot $\mathbb{C}$).

(b) $\varphi(0) = b_0$, $\varphi(-1) = b_1$, ... $\varphi(-n) = (-1)^n n!\, b_n \quad (n \geq 0)$

Si: $f(t) \sim \frac{b_{-1}}{t} + b_0 + b_1 t + \cdots$

(a') $\varphi(s) - \frac{b_{-1}}{s-1}$ és entera

(b) $\varphi(-n) = (-1)^n n!\, b_n \quad (n \geq 0)$

Exemple: $\zeta(s) = \sum \frac{1}{n^s} \Rightarrow f(t) = \sum_{1}^{\infty} e^{-nt} = \frac{1}{e^t - 1} = \frac{1}{t + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots} =$

$$= \frac{1}{t} - \frac{1}{2} + \frac{1}{12} t + \cdots + \frac{B_n}{n!} t^{n-1}$$

on B_n són els nombres de Bernoulli.

n	0	1	2	4	6	8	10	12	14
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	$\frac{-1}{30}$	$\frac{1}{42}$	$\frac{-1}{30}$	$\frac{5}{66}$	$\frac{-691}{2730}$	$\frac{7}{6}$

$B_n = 0$ per n imparell $\neq 1$.

Per tant $\zeta(-n) = -\frac{B_{n+1}}{n+1} \quad (n \geq 1)$.

Exemple: $L(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \cdots = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$, $\chi(s) = \begin{cases} 1 & n \equiv 1 \ (4) \\ -1 & n \equiv 3 \ (4) \\ 0 & n \text{ parell} \end{cases}$

$$f(t) = e^{-t} - e^{-3t} + e^{-5t} - \cdots = \frac{1}{e^t + e^{-t}} = \frac{1}{2\cosh t} = \frac{1}{2} \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n$$

n	0	2	4	6	8
E_n	1	-1	5	-61	1385

$E_n = 0$ per n imparell.

Per tant $L(s)$ és entera i $L(-n) = \frac{1}{2} E_n$.

↑ nombres d'Euler.

Prova (del th. #)

$$\Gamma(s) := \int_0^\infty e^{-t} t^{s-1}\, dt \qquad (\sigma \geq 0) \qquad \text{func. gamma.}$$

1) $\Gamma(s+1) = s\,\Gamma(s)$

2) $\Gamma(1) = 1 \Rightarrow \Gamma(n+1) = n! \quad (n \geq 0)$

Per (1), es veu que $\Gamma(s)$ té pols simples en $0, -1, -2, -3, \ldots$, i és holomorfa al resta de $\mathbb{C}$.

Canviar $t \longmapsto nt$, obtenim

$$\int_0^\infty e^{-nt} t^{s-1}\, dt = \Gamma(s)\, n^{-s} \qquad (n > 0)$$

Per $\sigma > 0$,

$$\Gamma(s)\varphi(s) = \sum_1^\infty a_n \frac{\Gamma(s)}{n^s} = \sum_1^\infty a_n \int_0^\infty e^{-nt} t^{s-1}\, dt =$$

$$= \int_0^\infty f(t)\, t^{s-1}\, dt \qquad \left(\text{transformada de } \underline{\text{Mellin}}\right)$$

↑ la funció que defineix l'enunciat

Descomposem la integral entre $\left(\int_0^{t_0} + \underbrace{\int_{t_0}^\infty}_{\text{convergent } \forall s \in \mathbb{C}}\right)$ i recordem $f(t) = \frac{b_{-1}}{t} + b_0 + \ldots + b_N t^N + O(t^{N+1})$ $(t \to 0)$

a la integral queda

$$= \int_0^{t_0} \left[\frac{b_{-1}}{t} + b_0 + \ldots + b_N t^N + O(t^{N+1})\right] t^{s-1}\, dt = b_{-1}\frac{t_0^{s-1}}{s-1} + b_0 \frac{t_0^s}{s} + \frac{t_0^{s+1}}{s+1} + \ldots$$

$$+ \frac{b_N t^{s+N}}{s+N} + \left(\begin{array}{c}\text{conv. per}\\ \sigma > -N-1\end{array}\right)$$

Per tant,

$\Gamma(s)\varphi(s)$ es pot prolongar com a funció meromorfa a tot $\mathbb{C}$

excepte $\{1, 0, -1, -2, -3, \ldots\}$ on hi té (com a molt) pols simples,

i amb residus $\operatorname*{Res}_{s=-n} \left(\Gamma(s)\varphi(s)\right) = b_n \qquad (n \geq -1)$.

Es pot demostrar que $\Gamma(s)$ no s'anul·la mai, per tant $\frac{1}{\Gamma(s)}$ és holomorfa.

$s \to -n \Rightarrow \Gamma(s) \sim \frac{(-1)^n/n!}{s+n} \Rightarrow$ Res ⤵

Per tant, el

$s=1$ $\quad \Gamma(s)\varphi(s) = \frac{b_{-1}}{s-1} + \dots \sim \varphi(s) = \frac{b_{-1}}{s-1}$

$s=0$ $\quad \underbrace{\Gamma(s)}_{-1/s}\,\varphi(s) = \frac{b_0}{s} + O(1)$

$s=-n$ $\quad \operatorname*{Res}_{s=-n}\left(\Gamma(s)\,\varphi(s)\right) = b_n \Rightarrow \varphi(-n)\operatorname{Res}\left(\Gamma(s)\right) = \operatorname{Res}\left(\Gamma(s)\varphi(s)\right) = b_n \Rightarrow$

$\Rightarrow \varphi(-n) = \frac{b_n}{\operatorname{Res}\left(\Gamma(s)\right)}$ //

Series de Dirichlet formals.

$\varphi(s) = \sum \frac{a_n}{n^s}$ com a sèrie formal.

$\mathcal{D} := \{\text{series formals de Dirichlet}\}$ és un anell $\left(\sum \frac{a_n}{n^s}\sum \frac{b_n}{n^s} = \sum \frac{c_n}{n^s}, \; c_n = \sum_{n_1 n_2 = n} a_{n_1} b_{n_2}\right)$

és la convolució multiplicativa !! ↑ important.

Exercici:

$d(n) = \#$ divisors de n $\quad (d(6) = 4 \quad (\{1,2,3,6\})$

- $\sum_1^\infty \frac{d(n)}{n^s} = \zeta(s)^2$
- $\sum_1^\infty \frac{d(n)^2}{n^s} = \frac{\zeta(s)^4}{\zeta(2s)}$
- $\sum_1^\infty \frac{d(n^2)}{n^s} = \frac{\zeta(s)^3}{\zeta(2s)}$

demostrar-ho i donar les abscisses de convergència.

Siguin $\varphi(s)=\sum \frac{a_n}{n^s}$, $\psi(s)=\sum \frac{b_n}{n^s}$ $\rightsquigarrow \lambda\varphi(s)+\psi(s)=\sum \frac{\lambda a_n+b_n}{n^s}$

Per tant $\mathcal{D}=\{$ sèries (formals) de dirichlet $\}$ és un espai vectorial $/\mathbb{C}$, i també una algebra, ja que $\sum \frac{a_n}{n^s}\sum \frac{b_n}{n^s}=\sum \frac{c_n}{n^s}$ on $c_n=\sum_{d\mid n} a_d b_{n/d}$ (convolució / multiplicativa)

Sabem que les unitats de $\mathbb{C}[[X]]$ són les sèries $\sum_{n\geq 0} a_n X^n$ t.q. $a_0\neq 0$

Per tant, el mateix passa amb les sèries de Dirichlet: cal $a_1\neq 0$

Es pot veure fàcilment que:

$\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$, μ = funció de Möbius.

n	1	2	3	4	5	6	7	8	9
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0

$$\mu(p_1^{\nu_1}\cdots p_r^{\nu_r})=\begin{cases}0 & \text{si } \exists\, \nu_i\geq 2\\ (-1)^r & \text{si tots els } \nu_i=1\end{cases}$$

Def: Una funció $a:\mathbb{N}\to\mathbb{C}$ ($\mathbb{N}=\{1,2,3,\dots\}$) és multiplicativa sii $a(nm)=a(n)a(m)$ $\forall (n,m)=1$.

Si a és multiplicativa, $a(p_1^{\nu_1}\cdots p_r^{\nu_r})=a(p_1^{\nu_1})\cdots a(p_r^{\nu_r})$

Si $a\neq 0$, $a(1)=1$ (fàcil).

La funció a queda determinada pels valors $a(p^r)$ $p\in\mathbb{P}$, $r\geq 1$

La sèrie de Dirichlet associada a (a_n), $\varphi(s)=\sum \frac{a_n}{n^s}$ té un producte d'Euler:

$$\frac{a_1}{1^s}+\frac{a_2}{2^s}+\frac{a_3}{3^6}+\frac{a_{2^2}}{2^{2s}}+\frac{a_5}{5^6}+\frac{a_2a_3}{2^s3^s}+\cdots=\left(\frac{1}{1^s}+\frac{a_2}{2^s}+\frac{a_{2^2}}{2^{2s}}+\cdots\right)\left(\frac{1}{1^s}+\frac{a_3}{3^s}+\cdots\right)(\ )\cdots$$

$$=\prod_{p\in\mathbb{P}}\left(1+\frac{a_p}{p^s}+\frac{a_{p^2}}{p^{2s}}+\cdots\right)$$

Exercici: $\mathcal{M}:=\{\sum_1^{\infty}\frac{a_n}{n^s}$: a multiplicativa $\}\subset\mathcal{D}^{\times}$ (invertibles) és un subgrup.

Exemple: La funció de Möbius $\mu(n)$

- $\sum \frac{\mu(n)}{n^s}=\zeta(s)^{-1}$
- $\mu(p_1^{\nu_1}\cdots p_r^{\nu_r})=\begin{cases}(-1)^r & \text{si } \nu_i=1\ \forall i\\ 0 & \text{si } \exists\, \nu_i\geq 2\end{cases}$
- $\sum_{d\mid n}\mu(d)=\begin{cases}1 & n=1\\ 0 & n\geq 2\end{cases}$

$$\zeta(s) = \sum_{1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_{p} \frac{1}{1-p^{-s}} \qquad \left(\mathrm{Re}(s) > 1\right) \Rightarrow \zeta(s) \neq 0$$

$$\frac{1}{\zeta(s)} = \prod_{p} \left(1 - p^{-s}\right) = \sum \frac{\mu(n)}{n^s}, \quad \mu(p) = -1, \ \mu(p^2) = \mu(p^3) = \cdots = 0$$

Exemples:

- $$\sum \frac{\mu(n)^2}{n^s} \left(= \sum_{\substack{n \geq 1 \\ \text{sense factors} \\ \text{quadrats}}} \frac{1}{n^s} \right) = \prod_{p} \left(1 + \frac{1}{p^s} + \frac{0}{p^{2s}} + 0 + \cdots\right) = \prod_{p} \left(1 + \frac{1}{p^s}\right) = \left[1 + x = \frac{1-x^2}{1-x}\right]$$

$$= \prod \frac{1-p^{-2s}}{1-p^{-s}} = \frac{\zeta(s)}{\zeta(2s)} \sim \frac{6/\pi^2}{s-1} \simeq 61\% \Rightarrow$$ 61% dels naturals no tenen factors quadrats.

- $$d(n) = \sum_{d \mid n} 1 = \sigma_0(n), \qquad \sigma_k(n) = \sum_{d \mid n} d^k$$

$$\sigma_k(\underbrace{n' n''}_{n}) = \sum_{d \mid n' n''} d^k = \sum_{\substack{d' \mid n' \\ d'' \mid n''}} (d' d'')^k = \left(\sum d'^k\right)\left(\sum d''^k\right) = \sigma_k(n')\,\sigma_k(n'')$$

$$(n', n'') = 1$$

(b multiplicativa $\Leftrightarrow$ $a(n) = \sum_{d \mid n} b(d)$ és multiplicativa)

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2 \quad \text{ja que} \quad d(n) = \sum_{d \mid n} 1 \cdot 1$$

$$\sum_{1}^{\infty} \frac{\sigma_k(n)}{n^s} = \zeta(s)\,\zeta(s-k) \quad \text{ja que} \ \ldots \ \text{(exercici)}.$$

- $$\sum_{1}^{\infty} \frac{d(n^2)}{n^s} = \prod_{p} \left(1 + \frac{d(p^2)}{p^s} + \frac{d(p^4)}{p^{2s}} + \cdots\right) \overset{d(p^\nu) = \nu + 1 \ (\nu > 0)}{=} \frac{1-x^2}{(1-x)^3} = \frac{\zeta(s)^3}{\zeta(2s)}$$

$d(n^2)$ és multiplicativa

$x = p^{-s}$

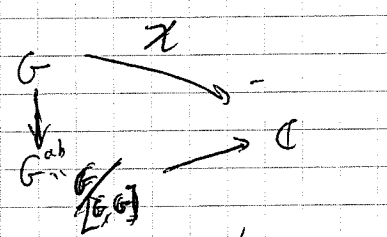
Series 6

• Caràcters de Dirichlet.

G grup finit. Un <u>caràcter</u> de G és un <u>homomorfisme</u> $\chi: G \to \mathbb{C}^*$

Com que $g^N = 1$ per cert N, $|\chi(g)| = 1$. Per tant, de fet $\chi(G) \subseteq \mu_\infty = \{z \in \mathbb{C} : z^N = 1 \text{ per cert } n\}$.

Obviament, tot caràcter és commutatiu $\chi(g_1 g_2) = \chi(g_2 g_1)$. Per tant,



cal considerar només G abelians.

$\hat{G} = \{\chi : G \to G \text{ caràcters}\}$ és el <u>grup dual</u> de G.

<u>Th</u>: $\hat{G} \cong G$ ← com a grups abstractes, però no és natural.

<u>Cor</u>: $|\hat{G}| = |G|$

Sabem que $G = C_{n_1} \times \cdots \times C_{n_r}$, on C_{n_i} és grup cíclic d'ordre n_i.
$C_{n_i} = \langle g_i \rangle$, $g_i^{n_i} = 1$

$\chi(g_1), \dots, \chi(g_r)$ determinen el caràcter.

A més, $\chi(g_i)$ és una arrel n_i-èssima de 1, pròpia.

Per tant, $\hat{G} \cong \mu_{n_1} \times \cdots \times \mu_{n_r}$
↑ però hem d'escollir abans els generadors de G!

<u>Def</u>: Sigui N un nombre natural ($N > 0$). Un <u>caràcter de Dirichlet</u> mòdul N és un caràcter del grup $\left(\mathbb{Z}/N\mathbb{Z}\right)^\times$.

Podem entendre un caràcter com definit a $\mathbb{Z}$, $\chi(n) = \begin{cases} \chi(n \bmod N) & (n,N)=1 \\ 0 & (n,N)>1 \end{cases}$

Així $\chi(\mathbb{Z}) \subseteq \mu_\infty \cup \{0\}$.

<u>Ex 1</u>: (caràcter principal): $\chi_0 \in \hat{G}$ $\left(G = (\mathbb{Z}/N\mathbb{Z})^\times\right)$ és tal que $\chi_0(n) = \begin{cases} 1 & (n,N)=1 \\ 0 & (n,N)>1 \end{cases}$

<u>Ex</u>: $p > 2$ $\rightsquigarrow$ $\left(\frac{\cdot}{p}\right)$ = Símbol de Legendre: $n \mapsto \left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n \\ +1 & \text{si } n \equiv x^2 \bmod (p) \\ -1 & \text{si no} \end{cases}$

$x \mapsto x^2$ és $1-a-2 \Rightarrow$ hi ha la meitat de quadrats i l'altra de no-quadrats.
i d'aquí es dedueix que el producte de dos no-residus és un residu.

Def: Sigui χ un caràcter $(\bmod N)$; sigui $N' \equiv 0 \pmod N$. Aleshores podem considerar un caràcter $(\bmod N')$, que és $\chi'(n) := \begin{cases} \chi(n) & (n,N')=1 \\ 0 & (n,n')>1 \end{cases}$

S'anomena el <u>caràcter induït</u> per χ.

$$\begin{array}{ccc} \left(\mathbb{Z}/N'\mathbb{Z}\right)^* & \xrightarrow{\chi' = \chi \circ \text{red.}} & \\ \downarrow \text{red} & & \\ \left(\mathbb{Z}/N\mathbb{Z}\right)^* & \xrightarrow{\chi} & \mathbb{C}^* \end{array}$$

Def: Un caràcter $\chi \pmod N$ és <u>primitiu</u> s.i. $\nexists N_1 \mid N$, $N_1 < N$ tq χ és induït per $\chi \pmod{N_1}$.

Def: Un caràcter χ té associats tres nombres:

- N: mòdul de definició.
- P: període
- C: conductor: el mòdul del caràcter mínimal que indueix χ (exercici: demostrar que existeix un únic C, χ' tq. for caràcter que indueix χ és induït per χ'.

Obs:

- $C \mid P \mid N$
- primitiu $\Leftrightarrow C = P = N$
- en general, $C < P \leq N$ ($\chi_0 \bmod 4$ té $N=4$, $P=2$, $C=1$ ← és el període "verdader").

Lema 1: (Relacions d'ortogonalitat).

a) χ caràcter $(\bmod N) \Rightarrow \sum_{n \,(\bmod N)} \chi(n) = \begin{cases} \varphi(N) & \chi = \chi_0 \\ 0 & \chi \neq \chi_0 \end{cases}$

a') χ_1, χ_2 caràcters $(\bmod N)$ $\Rightarrow \sum_{n \,(\bmod N)} \chi_1(n)\overline{\chi_2}(n) = \begin{cases} \varphi(N) & \chi_1 = \chi_2 \\ 0 & \chi_1 \neq \chi_2 \end{cases}$

b) $n \pmod N \Rightarrow \sum_{\chi \text{ car mod } N} \chi(n) = \begin{cases} \varphi(N) & \text{si } n \equiv 1 \pmod N \\ 0 & \text{si } n \not\equiv 1 \pmod N \end{cases}$

b') $n_1, n_2 \pmod N \Rightarrow \sum_{\chi \text{ car mod } N} \chi(n_1)\overline{\chi}(n_2) = \begin{cases} \varphi(N) & \text{si } n_1 \equiv n_2 \pmod N \\ 0 & \text{si } n_1 \not\equiv n_2 \pmod N \end{cases}$

Dem: a) $\chi \neq \chi_0 \Rightarrow \exists (n_0, N) = 1$ tq $\chi(n_0) \neq 1 \Rightarrow \chi(n_0) \sum_{n \,(\bmod N)} \chi(n) = \sum \chi(nn_0) = \sum \chi(n) \Rightarrow \sum \chi(n) = 0$.

(χ multiplicatiu)

b) Si $n \not\equiv 1 \bmod N \Rightarrow \exists \chi_1$ tq $\chi_1(n) \neq n \Rightarrow \chi_1(n) S = \sum \chi_1 \chi(n) = \sum \chi = S$ //

Def: La sèrie de Dirichlet associada a χ és $L(s,\chi) := \sum_{n\geq 1} \frac{\chi(n)}{n^s} =$

$$= \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \cdots\right) = \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}}$$

Obs: $\boxed{L(s,\chi_0) = \prod_p \frac{1}{1-\frac{\chi_0(p)}{p^s}} = \prod_{p\nmid N} \frac{1}{1-\frac{1}{p^s}} = \zeta(s) \prod_{p\mid N} \left(\frac{1}{1-\frac{1}{p^s}}\right)^{-1} =}$

$$\boxed{= \zeta(s) \prod_{p\mid N} \left(1-p^{-s}\right)}$$

- $\chi_1 \pmod N$ és induït per $\chi \pmod N$, aleshores $L(s,\chi_1) \prod_{p\mid N} \left(1-\frac{\chi(p)}{p^s}\right) = L(s,\chi)$

(per tant, ens podem reduir també als caràcters primitius).

Prop: $\chi \neq \chi_0 \Rightarrow$ • l'abscissa de convergència és 0 ($\Leftrightarrow L(s,\chi)$ holomorfa per $\sigma > 0$).

• $L(s,\chi)$ és <u>entera</u>.

Prova: Només cal observar que $\sum_{0<n<x} \chi(n) = O(1)$ (de fet, $\leq \varphi(N)\frac{N}{2}$).

Teorema (Dirichlet): $L(1,\chi) \neq 0$ (per $\chi = \chi_0$, val ∞ o sigui que...).

Prova: Definim $F(s) := \prod_{\chi \bmod N} L(s,\chi) = \prod_\chi \prod_p \frac{1}{1-\frac{\chi(p)}{p^s}} = \sum \frac{a_n}{n^s}$ ($\sigma > 1$).

(χ multiplicatiu)

$$\log F(s) = \sum_\chi \sum_p \sum_{r=1}^\infty \frac{\chi(p)^r}{r p^{rs}} = \sum_{\substack{r\geq 1\\ p^r \equiv 1 \bmod N}} \frac{1}{r p^{rs}} \sum_\chi \chi(p^r) = \sum_{\substack{r\geq 1\\ p^r \equiv 1 \bmod N}} \frac{\varphi(N)}{r p^{rs}}$$

$\log\left(\frac{1}{1-t}\right) = t + \frac{t^2}{2} + \frac{t^3}{3} + \cdots$

És tracta d'una sèrie de Dirichlet amb tots els coef's positius. Per tant exponencial, també es mantenen els exponents positius.

Ja sabem que $L(s,\chi)$ ($\chi \neq \chi_0$) és holomorfa per $\sigma > 0$, i $L(s,\chi_0)$ hol. $\sigma > 0$ excepte en $s=1$, on hi té un pol simple.

Per tant, si $\exists \chi$ tq $L(1,\chi) = 0$, aleshores es tindria $F(s)$ holomorfa en $s=1$, i per tant holomorfa per $\sigma > 0$. Però no pot ser, perquè pel petit teorema de Fermat, $\overbrace{L(\varphi(N)s,\chi_0)}^{\text{pol simple}}$ =

$$\varphi(N) \sum_{p^r \equiv 1 (N)} \frac{1}{r p^{rs}} \geq \varphi(N) \sum_{p\nmid N} \sum_{\substack{r\geq 1\\ \varphi(N)\mid r}} \frac{1}{r p^{rs}} = \sum_{p\nmid N} \sum_{k=1}^\infty \frac{1}{k p^{k\varphi(N)s}} = \sum_{p\nmid N} \log \frac{1}{1-p^{-\varphi(N)s}} \Rightarrow F(s) \geq \prod_{p\nmid N} \frac{1}{1-p^{-\varphi(N)s}}$$

Hem vist que $F(s) \geq L(\varphi(N)s, \chi_0)$.

Té un pol, per tant, en $s = \frac{1}{\varphi(N)} > 0$, però pel Th. de Landau, no es podria prolongar a l'esquerra de $\frac{1}{\varphi(N)}$, $\Rightarrow$!!

A més, si hi ha una excepció ha de ser única, perquè sinó amb dos 0's i un pol $\rightsquigarrow$ es tindria un zero i hem vist que no és 0 en $F(1)$.

Per tant, l'excepció ha de ser real (sinó $\overline{\chi}$ també ho seria). //

~~Considerem una~~

Th (Dirichlet): $N > 0$ i $(a, N) = 1 \Rightarrow \exists$ infinits p tq. $p \equiv a \pmod N$.

A més, $\sum_{p \equiv a (\mathrm{mod}\, N)} \frac{1}{p} = \infty$

Dem: $\sum_{\substack{p \text{ primer} \\ p^r \equiv a (\mathrm{mod}\, N)}} \sum_{r=1}^{\infty} \frac{1}{r p^{rs}} = \sum_{p \text{ primer}} \sum_{r \geq 1} \sum_{\chi \bmod N} \frac{\chi(p^r)\overline{\chi}(a)}{r p^{rs}} =$

$$= \sum_{\chi (N)} \overline{\chi}(a) \sum_{p} \sum_{r \geq 1} \frac{\chi(p)^r}{r p^{rs}} = \sum_{\chi (N)} \overline{\chi}(a) \log\left(L(s, \chi)\right) \qquad (\sigma > 1)$$

$$= \left(\log \frac{1}{s-1} + \mathcal{O}(1)\right) + \mathcal{O}(1) \longrightarrow \infty$$

($s \to 1$; $\chi \neq \chi_0$)

Observem que $\varphi(N) \sum_{\substack{p \\ p^r \equiv a (\mathrm{mod}\, N)}} \sum_{r \geq 1} \frac{1}{r p^{rs}} = \varphi(N) \sum_{p \equiv a (N)} \frac{1}{p^s} + \overbrace{\mathcal{O}(1)}^{s \geq 1}$

(perquè les altres sèries són convergents)

Per tant, $\sum_{\substack{p \\ p \equiv a \bmod N}} \frac{1}{p^s}$ és divergent per $s \to 1$, i

per tant hi ha infinits primers $\equiv a \pmod N$. //

Si volem trobar $L(s,\chi) = \varphi(s)$ en els valors $-n$, $n \geq 0$, hem d'escriure (pel teorema que haurien vist fa uns dies).

$$f(t) = \sum_{n=1}^{\infty} \chi(n) e^{-nt} = \sum_{n=1}^{N} \chi(n) \left(e^{-nt} + e^{-(n+N)t} + e^{-(n+2N)t} + \cdots \right) =$$

$$= \frac{\sum_{n=1}^{N} \chi(n) e^{-nt}}{1 - e^{-Nt}} = \frac{1}{Nt} \frac{\sum \chi(n) \left(1 - nt + \frac{n^2}{2} t^2 - \cdots\right)}{1 - \frac{N}{2!} t + \frac{N^2}{3!} t^2 - \cdots} = \left(\frac{1}{N} \sum_{n=1}^{N} \chi(n) \right) \frac{1}{t} + \left(\sum_{n=1}^{N} \chi(n) \left(\frac{1}{2} - \frac{n}{N} \right) \right) +$$

$$+ \frac{t}{2N} \sum_{n} \chi(n) \left(n^2 - nN + \frac{N^2}{6} \right) + \cdots$$

Per tant, $L(s,\chi)$ és holomorfa ($\chi \neq \chi_0$).

i $L(0,\chi) = -\frac{1}{N} \sum_{n=1}^{N} n \chi(n)$

$$L(-1,\chi) = -\frac{1}{2N} \sum_{n=1}^{N} \chi(n) \left(n^2 - nN + \frac{N^2}{6} \right)$$

Def: Un enter $D \neq 0, 1$ s'anomena **discriminant** si $D \equiv 0, 1 \pmod 4$.

És d'un **fonamental** si no es pot descomposar com $D = D_0 f^2$ amb $f \neq 1$ i D_0 disc.

Ex: $1, 5, 8, 12, 13, 17, 21, \ldots$; $-3, -4, -7, -11, -15, -19, -20, -23, \ldots$

Th (i) Si D és un discriminant fonamental, aleshores $\exists \chi_D$, un caràcter de Dirichlet que és primitiu $(\bmod D)$. S'anomena $\chi_D(p) = \left(\frac{D}{p}\right)$ $(p \neq 2)$.

$$\begin{cases} 0 & D \equiv 0 \ (4) \\ +1 & D \equiv 1 \ (8) \\ -1 & D \equiv 5 \ (8) \end{cases} \quad (\text{i } p = 2)$$

(i) A més, satisfà $\chi_D(-1) = \text{sign}(D)$

(ii) Aquests χ_D són els únics caràcters primitius reals.

Def: Un **discriminant primer** és aquell discriminant D tq és fonamental i conté exactament un nombre primer. (i.e. si és una potència d'un primer)

Obs: Tots els discriminants fonamentals es descomposen **únicament** com a producte de disc primers.

Prop: D és un discriminant primer $\iff$

$$\begin{cases} D = p, & p > 0, \ p \equiv 1 \ (4) \\ D = -p, & p > 0 \ \ p \equiv 3 \ (4) \\ D = -4, -8, +8 \end{cases}$$

Obs: $D = D' \cdot D''$, $(D', D'') = 1 \Rightarrow \text{Cor}(D) \cong \text{Cor}(D') \times \text{Cor}(D'')$ (T. restes xinesos)

Prova del Th:

Com que ja està definit, anem a veure que és periòdic $(\bmod D)$.

$D = q \equiv 1 \ (4)$: $\chi_q(p) = \left(\frac{q}{p}\right) \overset{\text{LRQ}}{=} \left(\frac{p}{q}\right)$ depèn només de $p \ (\bmod q)$

$$\chi_q(z) = \begin{cases} +1 & q \equiv 1 \ (8) \\ -1 & q \equiv 5 \ (8) \end{cases} = \left(\frac{2}{q}\right) \quad \text{pq } q \equiv 1 \ (4).$$

$$\Rightarrow \chi_q(m) = \left(\frac{m}{q}\right) \quad \forall m > 0$$

$D = -\ell$, $\ell \equiv 3 \ (4)$: $\chi_D(p) = \left(\frac{-\ell}{p}\right) \overset{\text{LRQ}}{=} (\ )$

$$p \equiv 1 \ (4) \to \left(\frac{-\ell}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)$$

$$p \equiv -1 \ (4) \Rightarrow \left(\frac{-\ell}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\ell}{p}\right) = -\left(\frac{\ell}{p}\right) = \left(\frac{\ell}{\ell}\right)$$

$$\chi_D(2) = \begin{cases} -1 & \ell \equiv 3 \ (8) \\ +1 & \ell \equiv 7 \ (8) \end{cases} = \left(\frac{2}{\ell}\right)$$

Per tant, hem vist que si $D = \pm$ primer, aleshores $\chi_D(n) = \begin{cases} \left(\frac{n}{|D|}\right) & n > 0 \\ \operatorname{sgn} D & n = -1 \end{cases}$; multiplicatiu

Observem que si tenim un caràcter χ mod N,

podem descomposar $N = p_1^{\nu_1} \cdots p_K^{\nu_K}$.

$N = p^\nu \wedge p \nmid \chi$,

$$\left\{\begin{matrix}\text{car. primitius reals}\\ \text{de } \mathbb{Q}\end{matrix}\right\} \overset{1:1}{\longleftrightarrow} \left\{ \text{disc} \neq \square \right\} / \sim \;\cong\; \left\{ \begin{matrix}\text{disc} \\ \text{fonamentals}\end{matrix} \right\} \;\cong\; \left\{ n \neq 0, 1 \right\} / \sim \;\cong\; \mathbb{Q}^* / \mathbb{Q}^{*2} \;\cong\; \left\{ K / \mathbb{Q} : [K:\mathbb{Q}] = 2 \right\} \cup \mathbb{Q} + \mathbb{Q}.$$

$D_1 \sim D_2 \Leftrightarrow D_1 D_2 = \square$

Per tant $\left\{ \begin{matrix}\text{caràcters} \\ \text{primitius reals}\end{matrix} \right\} \cong \left\{ K/\mathbb{Q} : [K:\mathbb{Q}] = 2 \right\} \cup \mathbb{Q} \oplus \mathbb{Q}$.

- **Formes (binàries) quadràtiques.**

$f(x,y) = ax^2 + bxy + cy^2$, assumim els coeficients $a, b, c \in \mathbb{Z}$. $\left(b \in \mathbb{Z} / \text{no a } \mathbb{Z}[\tfrac{1}{2}] !! \right)$.

Exemple: $t^2 - Du^2 = 4$, $D \overset{\neq \square}{\text{donat}}$, $D > 0$. Té solucions? (eq. de Pell).

$x^2 + y^2 = p$?

Sigui $f(x,y) = ax^2 + bxy + cy^2$. Prenem $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ $\left(\begin{matrix} \alpha, \beta, \gamma, \delta \in \mathbb{Z} \\ \alpha\delta - \beta\gamma = 1 \end{matrix} \right)$

aleshores $f'(x,y) = f(\alpha x + \beta y, \gamma x + \delta y) = (a\alpha^2 + b\alpha\gamma + c\gamma^2)x^2 +$

$+ (2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta)xy +$

$+ (a\beta^2 + b\beta\delta + c\delta^2)y^2$

Veiem que $f \sim f'$, és una relació d'equivalència.

A més, és obvi que f rep $n \Leftrightarrow f'$ rep n.

Qüestió 1: Quantes classes d'equivalència hi ha?

Qüestió 2: Descriure les solucions de $n = f(x,y)$ (on f és una classe d'equivalència).

- Classes d'equivalencia de formes quadràtiques.

Si $f=[a,b,c] \sim f'=[a',b',c']$,

aleshores $D:=b^2-4ac$; $D':=b'^2-4a'c'$

Es pot comprovar que $D=D'$ (càlcul estúpid).

Per tant, n'hi ha infinites (com a mínim una per cada $D \in \mathbb{Z}$):

D és un discriminant (def. del cap. anterior). Aleshores $\exists f$ t.q. $D(f)=D$:

Si $D \equiv 0\ (4)$: $f=[1, 0, -D/4]$

Si $D \equiv 1\ (4)$: $f=[1, 1, -\frac{D-1}{4}]$

Teorema: Suposem D no és un quadrat (i.e. la forma és irreductible sobre $\mathbb{Q}$).
Aleshores hi ha un nombre finit de classes d'equivalencia de formes quadràtiques de discriminant D.

Prova:

(1) $f=(a,b,c)$, $\mathrm{disc}(f)=D \Rightarrow f \sim g=(a',b',c')$ t.q. $|b'| \leq |a'| \leq |c'|$

(2) $\{(a,b,c) \mid b^2-4ac=D,\ |b| \leq |a| \leq |c|\}$ és finit (i ja acabem)

Pf (2): $|D|=|4ac-b^2| \geq 4|a||c|-|b|^2 \geq 4|a|^2-|a|^2=3a^2 \Rightarrow |a| \leq \sqrt{\frac{|D|}{3}}$

i $|b| \leq |a| \leq \sqrt{\frac{|D|}{3}}$ $\Rightarrow$ Tant a com b són acotats, i c depèn de a i b $\Rightarrow$ //.

Pf (1): Sigui a' el nombre de 1-1 mínimal representat per f

(obs que $a' \neq 0$ perquè altrament $D \neq \square$)

$a'=f(\alpha,\beta) \Rightarrow \exists \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ (assumim $(\alpha,\beta)=1$)

Aleshores $f'':=f\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \Rightarrow f'' \sim f$, i $f''=[a', b'', c'']$

Per tant ara aquesta forma pot ésser representada de forma que el coef. de x^2 sigui el mínimal representat.

$a'(x-ny)^2+b''(x-ny)y+c''y^2 = a'x^2+b'xy+cy^2 = a'x^2+\overbrace{(b''-2na')}^{b'}xy$

$+(a'n^2-b''n+c'')y^2$

i per tant podem escollir b' t.q. $|b'| \leq |a'|$

i a més $|b'| \leq |c'|$, altrament

//

Algorítmicament: $[a,b,c] \longmapsto [a, b-2na, c-nb+na]$ on $n \in \mathbb{Z}$

Fal que $-|a| < b-2na \leq |a|$.

Si aleshores $|c| \geq |a|$, ja estem.

Si no, canviem $(c,-b,-a)$ en compte, i tornem a començar.

Def: Sigui $D \neq 0$ un discriminant. El nombre de classes, $h(D)$, es defineix com el nombres de classes d'equivalència de formes binàries quadràtiques primitives de discriminant D, i definides positives si $D<0$.

Ex:

D	1	4	5	8	9	12	13	16	17	20	21	24	25	28	29
$h(D)$	1	1	1	1	2	2	1	2	1	3	2	2	4	2	1

D	-3	-4	-7	-8	-11	-12	-15	-16	-19	-20	-23	-24	-27
$h(D)$	1	1	1	1	1	1	2	1	1	2	3	2	1

A f, hi associem $U_f = \{M \in SL_2(\mathbb{Z}) : f \circ M = f\} \subset_{\text{sgp}} SL_2(\mathbb{Z})$.

Def: $R_f(n)$ = "nombre de representacions de n per f" $= \#\{(x,y) \in \mathbb{Z}^2 / U_f : f(x,y) = n\}$

- $R_D(n) = \sum_{i=1}^{h(D)} R_{f_i}(n)$ on f_i són les formes no-equivalents primitives de discriminant D, def pos si $D<0$.

  ↑ No és fer cap fórmula explícita. / No és fer cap fórmula explícita

També es fa amb fórmula pel valor mig de $R_f(-)$ quan $n \to \infty$.

Teorema: D fonamental:

$$R_D(n) = \sum_{d \mid n} \chi_D(d)$$

estructura de grup: $(t_1,u_1)(t_2,u_2) = \left(\frac{t_1 t_2 + D u_1 u_2}{2}, \frac{t_1 u_2 + t_2 u_1}{2}\right)$

Teorema:

1) $f = (a,b,c)$, $\operatorname{disc}(f) = D \rightsquigarrow \{(t,u) \in \mathbb{Z}^2 : t^2 - Du^2\} \longleftrightarrow U_f \subset SL_2(\mathbb{Z})$

$$(t,u) \longmapsto \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$$

(D primitiu!)

2) $D<0 \rightsquigarrow |U_f| = \begin{cases} 6 & D=-3 \\ 4 & D=-4 \\ 2 & D \neq -3,-4 \end{cases}$

$D>0 \rightsquigarrow U_f = \{\pm 1\} \times \mathbb{Z}$

Th:

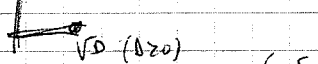
1) $\{(t,u)\in\mathbb{Z}^2 \mid t^2-Du^2=4\} \xleftrightarrow{1:1} U_f$ (via U_D)

2) $D<0 \Rightarrow |U_f| = w_D \in \{2,4,6\}$ si: $D\neq -3,-4$; $D=-4$; $D=-3$

$D\geq 0 \Rightarrow U_f = \{\pm 1\}\times\mathbb{Z}$

Prova

$U_D \ni (t,u) \rightsquigarrow \varepsilon = \varepsilon_D = \frac{t+u\sqrt{D}}{2} \in \mathbb{C}$



$\varepsilon' = \varepsilon'_D = \frac{t-u\sqrt{D}}{2}$ $\rightsquigarrow$ $\varepsilon^2 - t\varepsilon + 1 = 0$ $\left(\begin{array}{l}\varepsilon+\varepsilon' = t \in \mathbb{Z} \\ \varepsilon\varepsilon' = 1\end{array}\right.$

I observem que $\varepsilon_1 - \varepsilon_2 = \frac{t_1+u_1\sqrt{D}}{2} - \frac{t_2+u_2\sqrt{D}}{2} = \dots$

Si l'eq. de Pell té com solució $(t,u)\neq 0$, n'hi ha una de mínima de natural (t_0,u_0), que es correspon a un $\varepsilon_0 = \frac{t_0+u_0\sqrt{D}}{2}$

Podem identificar U_D com a subgrup de $\mathbb{C}^\times$, $U_D \sim \{\varepsilon = \frac{t+u\sqrt{D}}{2}\}$

$U_f = \{\pm \varepsilon_0^n \mid n\in\mathbb{Z}\}$

$R_f(n) = \#\{(x,y)\in\mathbb{Z}^2/U_f \mid f(x,y)=n\}$ $\left(\text{si } D<0,\ R_f(n) = \frac{1}{w_D}\#\{(x,y)\in\mathbb{Z}^2 : f(x,y)=n\}\right)$

$R_f^*(n)$ = nombre de solucions primitives ($\text{sol}(x,y)$ de $f(x,y)=n$ és primitiva si $\gcd(x,y)=1$).

Observem que $R_f(n) = \sum_{\substack{g\geq 1 \\ g^2\mid n}} R_f^*\left(\frac{n}{g^2}\right)$

$R_D(n) = \sum_{i=1}^{h(D)} R_{f_i}(n)$; $R_D^*(n) = \sum_{i=1}^{h(D)} R_{f_i}^*(n)$

(si D no és fonamental, es presenten moltes formes primitives)

Totes les formes quadràtiques de discr. D.

Th 1: D fonamental $\Rightarrow R_D(n) = \sum_{m|n} \chi_D(n)$.

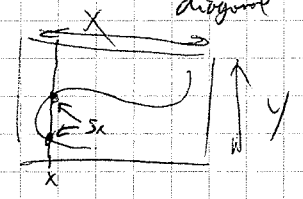
Th 2: D qualsevol, $n \geq 0$ $\Rightarrow R_D^*(n) = \{ b \pmod{2n} \mid b^2 \equiv D \pmod{4n} \}$

Prova 2

Primer, sigui G un grup, X, Y dos conjunts, i G actuï sobre els dos conjunts.

Sigui $S \subseteq X \times Y$ tal que $S^G = S$ (G actua sobre $X \times Y$ de manera diagonal)

Sigui, per cada $x \in X$, $S_x := (\{x\} \times Y) \cap S$



Recordem que Stabilitzador és $G_x = \{ g \in G : gx = x \}$

Aleshores $\sum_{x \in X/G} |S_x/G_x| = \sum_{y \in Y/G} |S_y/G_y|$ (perquè valen $|S/G|$).

Provem com a grup $G_x = U_\ell$; $X = \{ f : \text{form. quad.}, \operatorname{disc}(f) = D \}$

$Y = \{ (r,s) \in \mathbb{Z}^2 : \gcd(r,s) = 1 \}$

$S = \{ (f, (r,s)) : f(r,s) = n \}$

Observem que volem comptar $|S/G| = R_D^*(n)$:

$$|S/G| = \sum_{x \in X/G} |S_x/G_x| = \sum_{\substack{\{\text{rep. de les} \\ \text{classes prog. de disc } D\}}} \#\left(\{ \begin{bmatrix} r \\ s \end{bmatrix} : \begin{matrix} (r,s)=1 \\ f(r,s)=n \end{matrix} \} / U_\ell \right) = R_D^*(n).$$

No podem calcular també com $\sum_{y \in Y/G} |S_y/G_y|$

Anomenem un cert dels $y_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$S_{y_0} = \{ f = [a,b,c] : f(1,0) = n \} = \{ [n,b,c] : \begin{matrix} b, c \in \mathbb{Z} \\ b^2 - 4nc = D \end{matrix} \}$$

$\operatorname{disc} f = D$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_{y_0} \Leftrightarrow \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \Rightarrow G_{y_0} = \{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, r \in \mathbb{Z} \}$. i observem $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} [n,b,c] = (n, b+2rn, \ldots)$

Per tant, $S_{y_0} \cong \{ b \in \mathbb{Z} : b^2 \equiv D \pmod{4n} \}$

$G_{y_0} \cong \mathbb{Z}$

Prova de th 1:

D fonamental. $R_D(n) = \sum_{\substack{g \geq 1 \\ g^2 | n}} R_D^*\left(\frac{n}{g^2}\right)$.

Volem veure $R_D(n) = \sum_{m|n} \chi_D(m)$

Pel th. 1, $R_D^*(\cdot)$ és multiplicativa. I per la relació entre R_D i R_D^*, $R_D(\cdot)$ és també multiplicativa. $\chi_D(m)$ també ho és, i $\sum_{m|n} \chi_D(m)$ també ho és.

Per tant, n'hi ha prou amb demostrar-ho per una potència d'un primer arbitrari.

$n = p^r$, p primer, $r \geq 1$.

- Cas $p \geq 2$ (el cas $p=2$, exercici).

- Si $\chi_D(p) = +1$, $R_D^*(p^r) = \#\{ b \pmod{p^r} \mid b^2 \equiv D \pmod{p^r} \} = \begin{cases} 2 & r \geq 1 \\ 1 & r = 0 \end{cases}$

i per tant $R_D(p^r) = R_D^*(p^r) + R_D^*(p^{r-2}) + \cdots = \sum_{0 \leq s \leq \frac{r}{2}} 2 + \sum_{s = \frac{r}{2}} 1 \equiv r+1 = \sum_{m|p^r} \chi_D(m)$ //

- Si $\chi_D(p) = -1$, $R_D^*(p^r) = \begin{cases} 0 & r \geq 0 \\ 1 & r = 0 \end{cases} \Rightarrow R_D(p^r) = \sum_{0 \leq s < \frac{r}{2}} 0 + \sum_{s = \frac{r}{2}} 1 = \begin{cases} 1 & r \text{ parell} \\ 0 & r \text{ imparell} \end{cases} = \sum_{m|p^r} \chi_D(m)$

- Si $\chi_D(p) = 0$, $R_D^*(p^r) = \begin{cases} 1 & r = 0, 1 \\ 0 & r \geq 2 \end{cases} \Rightarrow R_D(p^r) = \sum_{0 \leq s \leq \frac{r-2}{2}} 0 + \sum_{\frac{r-1}{2} \leq s \leq \frac{r+1}{2}} 1 = \underbrace{1}_{r+1} = \underbrace{1+0+0+0}_{r+1} = \sum_{m|p^r} \chi_D(m)$ //

Corollari: $\langle R_D \rangle := \lim_{N \to \infty} \frac{\sum_{n=1}^{N} R_D(n)}{N}$. Aleshores si D és fonamental, $\langle R_D \rangle = L(1, \chi_D)$ ($\Leftarrow$ si $D \neq 1$)

Prova $\Leftarrow$

$$\sum_{n=1}^{N} R_D(n) = \sum_{1 \leq n \leq N} \sum_{m|n} \chi_D(m) = \sum_{\substack{k,m \geq 1 \\ km \leq N}} \chi_D(m) = \sum_{1 \leq m \leq \sqrt{N}} \chi_D(m) \left\lfloor \frac{N}{m} \right\rfloor + \sum_{1 \leq k \leq \sqrt{N}} \left(\sum_{\sqrt{N} < m \leq \frac{N}{k}} \chi_D(m) \right) =$$

$$= \sum_{1 \leq m \leq \sqrt{N}} \chi_D(m) \left(\frac{N}{m} + O(1) \right) + \sum_{1 \leq k \leq \sqrt{N}} O(1) = N \sum_{1 \leq m \leq \sqrt{N}} \frac{\chi_D(m)}{m} + O(\sqrt{N})$$

Per tant, $\frac{\sum_{n=1}^{N} R_D(n)}{N} = \sum_{1 \leq m \leq \sqrt{N}} \frac{\chi_D(m)}{m} + O\left(\frac{1}{\sqrt{N}}\right) \longrightarrow L(1, \chi_D)$ //

Però podem interpretar el corol·lari: $R_D(n) = \sum_{f \text{ l.q.h., disc}=D} R_f(n)$ $\Rightarrow \langle R_D \rangle = \sum_{i=1}^{h(D)} \langle R_{f_i} \rangle$ si existeixen

Th 3: $\operatorname{disc} f = D$; $\langle R_f \rangle$ existeix i val:

$$\langle R_f \rangle = \begin{cases} \frac{2\pi}{w\sqrt{|D|}} & \text{si } D<0 \\ \frac{\log \varepsilon_0}{\sqrt{D}} & \text{si } D \text{ no } \square \end{cases} \qquad \left(\text{on } w = w_f = \begin{cases} 2 & D<-4 \\ 4 & D=-4 \\ 6 & D=-3 \end{cases} \right.$$

$\left(\text{on } \varepsilon_0 = \frac{t_0 + u_0\sqrt{D}}{2} \right)$

($\langle R_f \rangle$ independent de f !).

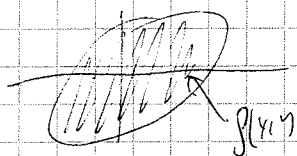
Per tant,

Corol·lari: $h(D) = \begin{cases} \frac{w\sqrt{|D|}}{2\pi} L(1, \chi_D) & \text{per } D<0 \\ \frac{\sqrt{D}}{\log \varepsilon_0} L(1, \chi_D) & \text{per } D>0 \end{cases}$

Prova Th 3:

$D<0$: $R_f(n) = \#\{(x,y) \in \mathbb{Z}^2/U_f \mid f(x,y) = n\} \Rightarrow \sum_{n=0}^{N} R_f(n) = \#\{(x,y) : \mathbb{Z}^2/U_f : f(x,y) \le N\}$

$= \frac{1}{w} \#\{(x,y) \in \mathbb{Z}^2 \mid f(x,y) \le N\}$

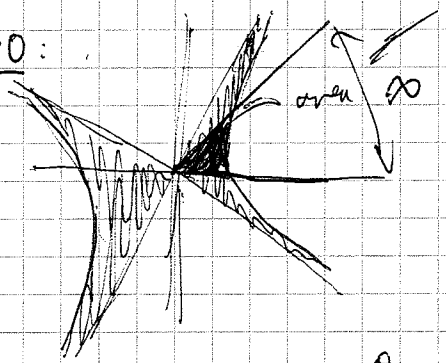


$\rightsquigarrow$ àrea $= \frac{\pi}{\sqrt{|D|}/4}$ $\Rightarrow$ $\{f(x,y) \le N\}$ té més $\frac{2\pi N}{\sqrt{|D|}}$

Per $N \to \infty$, el nombre de punts és justament l'àrea, i per tant:

el límit val $\frac{2\pi}{\sqrt{|D|}}$ //

$D>0$:



Observem que $\begin{pmatrix} x \\ y \end{pmatrix} \to M_0 \begin{pmatrix} x \\ y \end{pmatrix}$ (on $M_0 \leftrightarrow \varepsilon_0$)

$x - \theta y \mapsto \varepsilon_0 (\,)$

$x - \theta' y \to \varepsilon_0^{-1} (\,)$

Per tant podem suposar

$$1 \le \frac{x - \theta y}{x - \theta' y} \le \varepsilon_0^2$$

Qüestió: χ caràcter ($\neq \chi_0$). Com calcular $L(1,\chi)$?

- Sumes de Gauss:

χ caràcter ($\neq \chi_0$), mod N i primitiu ($N>1$).

$$G = G_\chi = \sum_{n \pmod N} \chi(n) e^{\frac{2\pi i n}{N}} = \sum_{n \pmod N} \chi(n)\, \zeta^n \quad \text{on } \zeta = \zeta_N = e^{2\pi i/N}$$

Prop: i) $\sum_{n \bmod N} \chi(n)\, \zeta^{kn} = \overline{\chi(k)}\, G$ ($\overline{\ }$ és el conjugat complex).

ii) $|G| = \sqrt{N}$ ($\neq 0$, en particular). (és a dir $G\overline{G} = \chi(-1) N = \pm N$)

Corol·lari: $\chi(k) = \frac{1}{G} \sum_{n (N)} \overline{\chi}(n)\, \zeta^{-kn}$ (i notem que aleshores $\chi(kk') = \ldots$

Prova

(1) $(k,N)=1 \Rightarrow \chi(k) \cdot \sum_{n (N)} \chi(n)\, \zeta^{kn} = \sum_{n (N)} \chi(kn)\, \zeta^{kn} = G$

$|\chi(k)| = 1 \Rightarrow \overline{\chi}(k) = \chi(k)^{-1} \Rightarrow //$

$(k,N) > 1 \Rightarrow \sum \chi(n)\, \zeta^{kn} = 0$? Sigui $N_1 := \frac{N}{(k,N)} < N$

$\zeta^{kn} = \left(\zeta_N^k\right)^n = \left(\zeta_{N_1}^1\right)^n$

Cal demostrar que $\sum_{n' \equiv n (N_1)} \chi(n') = 0$ (exercici)

(2) $|G|^2 = G\overline{G} = G \cdot \sum \overline{\chi}(n)\, \overline{\zeta^k} = \sum G \overline{\chi}(n)\, \zeta^{-k} = \sum \left(\sum \chi(n) \zeta^{kn}\right) \zeta^{-k} =$

$= \sum_n \chi(n) \sum_{k (N)} \zeta^{k(n-1)} = \chi(1) \cdot N = 1 \cdot N$ //

(la suma interna és 0 si $n \neq 1$, i val N si $n = 1$)

(3) igual que (2).

$$L(s,\chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} = \frac{1}{G} \sum_{n(N)} \bar{\chi}(n) \left(\sum_{k=1}^{\infty} \frac{\zeta^{-kn}}{k^s} \right)$$

$\Re(s) > 1$

Lemma: $0 < \theta < 2\pi$, $\sum \frac{e^{in\theta}}{n} = -\log\left(2\sin\frac{\theta}{2}\right) + i \cdot \frac{\pi - \theta}{2}$

Dem $|z| < 1 \Rightarrow \sum_{1}^{\infty} \frac{z^n}{n} = -\log(1-z)$

Pour $z = x e^{i\theta}$ (x désigne $x \to 1$). $\Big\} \sim -\log(1 - e^{i\theta})$

$$1 - e^{i\theta} = e^{\frac{i\theta}{2}} \left(e^{\frac{i\theta}{2}} - e^{-\frac{i\theta}{2}} \right) = e^{\frac{i\theta}{2} + \frac{-i\pi}{2}} \left(2\sin\frac{\theta}{2} \right) \quad //$$

$$L(1,\chi) = \frac{\chi(-1)}{G} \sum_{n(N)} \bar{\chi}(n) \cdot \sum_{k=1}^{\infty} \frac{\zeta^{kn}}{k} = \frac{\chi(-1)}{G} \sum_{0<n<N} \bar{\chi}(n) \left(-\log\left(2\sin\frac{\pi n}{N}\right) - \frac{n}{N} - \frac{1}{2} \right) i\pi$$

Th: Soit $\chi \pmod N$ un caractère primitif, $N > 1$.

Alors si χ est pair ($\chi(-1) = 1$), $L(1,\chi) = \sum_{n=1}^{N-1} \chi(n) \log\left(\sin\frac{\pi n}{N}\right) = \frac{-1}{G} \sum_{n=1}^{N-1} \chi(n) \log\left(\sin\frac{\pi n}{N}\right)$

si χ est impair ($\chi(-1) = -1$), $L(1,\chi) = \frac{+i\pi}{G \cdot N} \sum_{n=1}^{N-1} \chi(n) \cdot n$

Exemple: $D = -4$

n	1	2	3	4
$\chi_D(n)$	1	0	−1	0

$\zeta = e^{\frac{i\pi}{2}} = i$

$L(1,\chi) \overset{?}{=} \frac{\pi}{4}$ $\quad G = \sum \chi(n) i^n = i - i^{-1} = 2i$

$$L(1,\chi) = \frac{i\pi}{-8i} \left(1 - 3 \right) = \frac{\pi}{4}$$

$D = -3$

n	1	2	3
$\chi_D(n)$	1	−1	0

$G = \zeta - \zeta^2 = i\sqrt{3}$

$$L(1,\chi) = \frac{i\pi}{-3i\sqrt{3}} \left(1 - 2 \right) = \frac{\pi}{3\sqrt{3}}$$

$D = 5$

n	1	2	3	4	5
$\chi_D(n)$	1	−1	−1	1	0

$G = 2\cos\frac{2\pi}{5} - 2\cos\frac{4\pi}{5} = \sqrt{5}$

$$L(1,\chi) = \frac{-1}{\sqrt{5}} \log\left(\frac{2\sin\frac{\pi}{5} \sin\frac{4\pi}{5}}{2\sin\frac{2\pi}{5} \sin\frac{3\pi}{5}} \right) = \frac{1}{\sqrt{5}} \log\left(\frac{3+\sqrt{5}}{2} \right)$$

Soit $\chi = \chi_D$ (équivalent à dire que χ est réel).

$$G^2 = \begin{cases} +|D| & \chi_D(-1) = +1 \\ -|D| & \chi_D(-1) = -1 \end{cases} = D$$

Théorème (Gauss) : $G = \begin{cases} \sqrt{D} & \text{si } D > 0 \\ i\sqrt{|D|} & \text{si } D < 0 \end{cases}$

Corollaire (l'hem démontré, l'essentiel de la preuve) :

$$L(1, \chi_D) = \begin{cases} -\frac{\pi}{|D|^{3/2}} \sum_{0<n<|D|} \chi_D(n) \cdot n & (D<0) \\ -\frac{1}{\sqrt{D}} \sum \chi_D(n) \log\left(\sin \frac{\pi n}{D}\right) & (D>0) \end{cases}$$

Cor : $D < 0$, $h(D) = \begin{cases} 1 & \text{si } D = -3, -4 \\ \frac{1}{|D|} \sum \chi_D(n) n & \text{si } D < -4 \end{cases}$ où $K_D = \frac{\pi}{\sqrt{|D|}}$

$D > 0$: $h(D) \log \varepsilon_0 = -\sum_{0<n<D} \chi_D(n) \log\left(\sin \frac{\pi n}{D}\right)$

Théorème : $\sum_{0<n<\frac{|D|}{2}} \chi_D(n) = h(D)\,(2 - \chi_D(2))$ où $\begin{cases} D \equiv 1\ (8) & \lambda = 1 \\ D \equiv 5\ (8) & \lambda = \frac{1}{3} \\ D \equiv 0\ (4) & \lambda = \frac{1}{2} \end{cases}$

Dem (D impair, sinon exercice, considérer $\chi_D(n + \frac{|D|}{2}) = -\chi_D(n)$).

$D \equiv 1\ (4)$. $S = \sum_{0<n<|D|} \chi_D(n) \cdot n = \sum_{0<k<\frac{|D|}{2}} \chi_D(2k) \cdot 2k + \chi_D(|D|-2k)(|D|-2k) =$

$= \sum_{0<k<\frac{|D|}{2}} = \sum_{0<k<|D|} \chi_D(2k) \cdot \begin{cases} 2k & k < \frac{|D|}{2} \\ 2k - |D| & k > \frac{|D|}{2} \end{cases} =$

$= 2\chi_D(2) \sum_{0<k<|D|/2} \chi_D(k) \cdot k - |D| \sum_{0<k<|D|} \chi_D(k) = \frac{|D|}{1 - 2\chi_D(2)} \sum_{\frac{|D|}{2}<k<|D|} \chi_D(k)$

Sigui ara $D>0$

$$\prod_{0<n<D}\left(\sin\frac{\pi n}{D}\right)^{\chi_D(n)} \overset{?}{=} \frac{t+u\sqrt{D}}{2} \quad \text{on } t,u\in\mathbb{Z} \qquad \left(=\left(\frac{t_0+u_0\sqrt{D}}{2}\right)^{\text{enter}}\right)$$

$$t^2-Du^2=4 \quad (i\ u\neq 0)$$

Prenem $D=p\equiv 1\ (4)$ primer (el cas general és igual).

$$\left(\frac{n}{p}\right)=\begin{cases}+1 & n=\square \bmod p \quad (R)\\ -1 & n\neq\square \bmod p \quad (N)\end{cases}$$

$$A=\sum_{\left(\frac{n}{p}\right)=1}\zeta^n \qquad B=\sum_{\left(\frac{n}{p}\right)=-1}\zeta^n$$

$$A=\sum\zeta^R \quad , \quad B=\sum\zeta^N$$

$$A+B=-1$$

$$A-B=\sum\left(\frac{n}{p}\right)\zeta^n=G=\sqrt{p} \quad \Rightarrow \quad A=\frac{-1+\sqrt{p}}{2}, \quad B=\frac{-1-\sqrt{p}}{2}$$

$$\epsilon=\prod(1-\zeta^R) \qquad \delta=\prod(1-\zeta^N)$$

$$C=\prod(1-\zeta^R)=\sum_{l=0}^{p-1}c_l\zeta^l \qquad c_l\in\mathbb{Z} \text{ donen únics} \quad \left(\text{ja que } \zeta^{p-1}+\zeta^{p-2}+\cdots+\zeta^1+1=0\right)$$

$$D=\prod(1-\zeta^N)=\sum_{l=1}^{p-1}d_l\zeta^l$$

Si canviem $\zeta\mapsto\zeta^k$, $p\nmid k$,

$$\prod(1-\zeta^{kN})=\sum d_l\zeta^{kl} \quad ; \quad \prod(1-\zeta^{kR})=\sum c_l\zeta^{kl}$$

Si $k\in R$, $C=\sum c_l\zeta^{kl}\Rightarrow c_l=c_{kl}$ $\quad (;\ d_l=d_{kl})$.

Si $k\in N$ $\quad\Rightarrow c_l=-c_{kl}$ $\quad (;\ d_l=-d_{kl})$

Per tant, $\prod(1-\zeta^R)=c_1\sum_R\zeta^R+d_1\sum_N\zeta^N$ *

$$\prod(1-\zeta^N)=d_1\sum\zeta^R+c_1\sum\zeta^N$$

per certs c_1, d_1

$$c_1A+d_1B=\frac{-c_1-d_1+(c_1-d_1)\sqrt{D}}{2}$$

Per tant $\prod(1-\zeta^R)=\frac{r+s\sqrt{p}}{2}$; $\prod(1-\zeta^N)=\frac{r-s\sqrt{p}}{2}$

Prenent el producte, $\frac{r^2-s^2p}{4}=\prod_{0<n<p}(1-\zeta^n)=\left(\prod_1^{p-1}(X-\zeta^i)=(X^p-1)/(X-1)\right)=p \Rightarrow r^2$ //

Sigui K un cos de nombres quadràtic ($[K:\mathbb{Q}]=2$).

$K = \mathbb{Q}\cdot 1 + \mathbb{Q}\cdot\alpha \Rightarrow \alpha^2 \in K \Rightarrow \alpha^2 \in \mathbb{Q}\cdot\alpha + \mathbb{Q} \Rightarrow \alpha^2 - t\alpha + n = 0,\ t,n\in\mathbb{Q}$

$\alpha = \frac{t}{2} + \frac{1}{2}\sqrt{t^2-4n} \rightsquigarrow K = \mathbb{Q}\left(\sqrt{t^2-4n}\right)$

$d := t^2-4n \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$

Si $d = \frac{a}{b}$ $\Rightarrow \mathbb{Q}(\sqrt{d}) = \mathbb{Q}\left(\sqrt{\frac{a}{b}b^2}\right) = \mathbb{Q}(\sqrt{ab})$. Per tant podem suposar $d \in \mathbb{Z}$, $d \neq 1$ i sense factors quadrats.

$\mathcal{O} = \mathcal{O}_K$ és l'anell dels enters algebraics en K. $\therefore \mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ ($\overline{\mathbb{Q}}^{cc}$)

Portem càlculs explícits dels cossos més generals.

- **Càlcul de $\mathcal{O}_K$ per $K=\mathbb{Q}(\sqrt{d})$** ($d\in\mathbb{Z}$, $d\neq 1$, d lliure de quadrats).

$\alpha = r + s\sqrt{d} \in K$ $(r,s\in\mathbb{Q})$.

$\alpha' = r - s\sqrt{d}$ conjugat de α.

$\mathrm{tr}(\alpha) = \alpha + \alpha' = 2r \in \mathbb{Q}$, $N(\alpha) = \alpha\cdot\alpha' = r^2 - s^2 d \in \mathbb{Q}$

Es compleix $\alpha^2 - t\alpha + n = 0$ $\quad X^2 - tX + n = (X-\alpha)(X-\alpha')$.

Si $t, n \in \mathbb{Z}$, aleshores α és enter algebraic.

Recíprocament, si α és enter, α' també ho serà i aleshores $\alpha+\alpha'$ i $\alpha\alpha'$ també.

Com que són simètrics, són de $\mathbb{Q}$. $\mathbb{Q}\cap\overline{\mathbb{Z}} = \mathbb{Z} \Rightarrow //$.

$$\mathcal{O}_K = \left\{ \frac{a+b\sqrt{d}}{2} \mid a,b\in\mathbb{Z},\ a^2 \equiv b^2 d \pmod 4 \right\} \in \begin{cases} t = 2r \in \mathbb{Z} \\ n = r^2 - s^2 d \in \mathbb{Z} \end{cases} \Rightarrow$$

$\Rightarrow 4n = 4r^2 - (2s)^2 d \in \mathbb{Z}$

$(2s)^2 d \in \mathbb{Z}$

$2s \in \mathbb{Z}$

$r = a/2$

$s = b/2$

$d \equiv 1 \ (4) \Rightarrow a^2 \equiv b^2 \ (4) \Leftrightarrow a \equiv b \ (2)$

$d \equiv 2 \ (4) \Rightarrow a^2 \equiv 2b^2 \ (4) \Leftrightarrow a \equiv b \equiv 0 \pmod 2$

$d \equiv 3 \ (4) \Rightarrow a^2 \equiv 3b^2 \ (4) \Rightarrow a \equiv b \equiv 0 \pmod 2$

Per tant,

$\mathcal{O}_K = \mathbb{Z} + \sqrt{d}\,\mathbb{Z}$ si $d \equiv 2, 3 \ (4)$

$\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$ si $d \equiv 1 \ (4)$

Si $\mathcal{O}_K$ té una base $\langle \alpha, \beta \rangle$, es defineix el $\operatorname{disc} K = \operatorname{disc} \mathcal{O}_K$

com $D = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}^2$

Si fem un canvi de base $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto M \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $M \in GL_2(\mathbb{Z})$

Part de càlculs, obtenim:

$$\operatorname{disc}(\mathcal{O}_K) = \begin{cases} d & d \equiv 1 \ (4) \\ 4d & d \equiv 2,3 \ (4) \end{cases}$$

$\mathbb{Q}(\sqrt{d}) \longleftrightarrow d \longmapsto D$ (amb fletxes cap a {caràcters de Dirichlet} i {Reals primitius})

Corollari: Es té una bijecció: $\left\{ K \supset \mathbb{Q} \mid [K:\mathbb{Q}] = 2 \right\} \longleftrightarrow \left\{ D \neq 1 \text{ disc fonamental} \right\}$

Un ideal entre de K és un subgrup $\mathfrak{a} \subset \mathcal{O} = \mathcal{O}_K$ tq $\mathfrak{a}\mathcal{O} \subseteq \mathfrak{a}$ ($\Rightarrow$ índex finit).

La norma d'un ideal $\mathfrak{a}$ és $[\mathcal{O} : \mathfrak{a}]$

Un ideal $\mathfrak{a} \subseteq \mathcal{O}$ tindrà sempre una $\mathbb{Z}$-base, $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$, i:

es defineix el discriminant de $\mathfrak{a}$ com $\begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}^2 \in \mathbb{Z}$ $\left(\mathfrak{a} = \mathcal{O} \Rightarrow \begin{cases} N(\mathcal{O}) = 1 \\ \operatorname{disc}(\mathcal{O}) = D \end{cases} \right)$.

$$\boxed{\operatorname{disc}(\mathfrak{a}) = N(\mathfrak{a})^2 D_K}$$ (a partir de les definicions).

Lema: $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) N(\mathfrak{b})$

Un ideal principal és $\xi \mathcal{O}_K$ amb $\xi \in \mathcal{O}_K$.

Prop: $N((\xi)) = |N(\xi)| \left(= |\xi \cdot \xi'| \right)$

Dem: $(\xi) = \xi \mathcal{O}_K = \mathbb{Z}\xi\alpha + \mathbb{Z}\xi\beta$

$$N((\xi))^2 D_K = D((\xi)) = \begin{vmatrix} \xi\alpha & \xi\beta \\ \xi'\alpha' & \xi'\beta' \end{vmatrix} = \left(\xi\xi' (\alpha\beta' - \alpha'\beta) \right)^2 = N(\xi)^2 D_K$$

$K = \mathbb{Q}(\sqrt{6})$. $d = 6$, $D = 24$, $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{6}$.

$(4+\sqrt{6})(4-\sqrt{6}) = (2) \cdot (5)$

$\mathfrak{p}\mathfrak{q} \quad \mathfrak{p}\mathfrak{q}' \quad \mathfrak{p}^2 \quad \mathfrak{q}\mathfrak{q}'$

ideal d'índex 2 !!

$\mathfrak{p} = (2, 4+\sqrt{6}) = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot \sqrt{6}$

$\mathfrak{q} = (5, 4+\sqrt{6})$

Def $\mathcal{a} \subseteq K$ és un ideal (fraccionari) si $0 \neq \mathcal{a}$ és un grup abelià, $\mathcal{a}\mathcal{O} \subseteq \mathcal{O}$ finit generat.

La norma de $\mathcal{a}$ es defineix com: Si $\mathcal{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta$, $\exists\, m \in \mathbb{Z}^+$ tq $m\alpha, m\beta \in \mathbb{Z}$,

i aleshores $N(\mathcal{a}) := \frac{N(m\mathcal{a})}{m^2}$

Està, com $\mathcal{a}\cdot\mathcal{a}' = (N(\mathcal{a}))$, que $\mathcal{a}^{-1} = \frac{1}{N(\mathcal{a})}\mathcal{a}'$

Formen, per tant, un grup.

Hi ha un subgrup, que és el dels ideals fraccionaris principals.

Def: $\mathcal{Cl}(K) = \frac{\mathrm{Frac}(K)}{\mathrm{Princ}(K)}$ és el grup de classes d'ideals.

Per tant, $\mathcal{a} \sim \mathcal{b} \iff \mathcal{b} = \lambda\mathcal{a}$, $\lambda \in K^*$.

Direm que $\mathcal{a} \sim \mathcal{b}$ en sentit estricte $\iff \mathcal{b} = \lambda\mathcal{a}$ amb $N(\lambda) > 0$

Donin lloc al grup de classes en sentit estricte $\mathcal{C}_K^+$

$0 \to G \to \mathcal{C}_K^+ \to \mathcal{C}_K \to 0$ on $G = \{\xi(\xi)/\xi(\mathcal{z}),\ N(\xi) > 0\}$ $(\#G \leq 2)$.

Th: $K = \mathbb{Q}(\sqrt{D})$, aleshores $\mathcal{C}_K^+ \cong \{$classes d'equivalència (mod $S_L(\mathcal{O})$ de $\{$formes bilineals quad. de disc $D\}$ (def pos si $D<0$)$\}$

Cor: $|\mathcal{C}_K^+| < \infty$, $|\mathcal{C}_K^+| = \frac{L(1,\chi_D)}{\kappa_D}$.

Prop:

Volem associar a cada $\mathcal{a}$ ideal fracc. una f. quad. de disc D.

$\xi \in \mathcal{a} \iff \xi\mathcal{O}_K \subseteq \mathcal{a} \subseteq \mathcal{a} \mid (\xi) \Rightarrow N(\mathcal{a}) \mid N((\xi)) = |N(\xi)|$

(K^*, ideal fracc.)

$\mathcal{a} \ni \xi \longrightarrow \frac{N(\xi)}{N(\mathcal{a})} = \frac{\xi\xi'}{N(\mathcal{a})} \in \mathbb{Z}$ $\Rightarrow$ $f(x,y) = \frac{(x\alpha+y\beta)(x\alpha'+y\beta')}{N(\mathcal{a})} =$

($\mathcal{a} = \mathbb{Z}\alpha + \mathbb{Z}\beta$, $x\alpha+y\beta$)

$= \left[\frac{\alpha\alpha'}{N(\mathcal{a})}, \frac{\alpha\beta'+\alpha'\beta}{N(\mathcal{a})}, \frac{\beta\beta'}{N(\mathcal{a})}\right]$.

(a, b, c)

$a \in \mathbb{Z}$, $\mathcal{a} \in \mathbb{Z}$. Si, com, $a+b+c \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$.

$b^2 - 4ac \left(= \mathrm{disc}(f)\right) = \frac{(\alpha\beta'+\alpha'\beta)^2 - 4(\alpha\alpha')(\beta\beta')}{N(\mathcal{a})^2} = \frac{\mathrm{disc}(\mathcal{a})}{N(\mathcal{a})^2} = D$. ✗

Si canviem α, β per una altra base, obtindrem una forma equivalent. Cal, però, que la base sigui orientada: demanem $\frac{\alpha'\beta - \alpha\beta'}{\sqrt{D}} \in \mathcal{a}_{>0}$.