

ANÁLISIS DE FOURIER EN GRUPOS ABELIANOS FINITOS

N. SIROLLI
(UBA)

REF: • TERNAS,
FOURIER AN. ON
FINITE GROUPS AND
APPLICATIONS

• DEITMAR, A 1ST
COURSE ON HARM.
ANALYSIS

§1. INTRODUCCIÓN

CONSIDEREMOS $G = \mathbb{R}$ (NO ES FINITO, Y
TAMPOCO COMPACTO)

DADA $f: \mathbb{R} \rightarrow \mathbb{R}$ "CON RÁPIDO DECR.", $\rightarrow$ MÁS PRECIS,
SE DEFINE $\hat{f}: \mathbb{R} \rightarrow \mathbb{R}$ $f \in \mathcal{S}(\mathbb{R})$

$$\hat{f}(\gamma) = \int_{\mathbb{R}} f(x) e^{-2\pi i x \gamma} dx, \quad f \in \mathcal{S}(\mathbb{R})$$

¿? $\rightarrow$ A EXPLICAR

LA TRANSF. DE FOURIER DE f . SE DEFINIÓ PARA
RESOLVER LA EC. DEL CALOR

$$\begin{cases} u_t = u_{xx} \\ u(x, 0) = \phi(x) \end{cases}$$

$\rightarrow$ SOL: $u(x, t) =$
 $\frac{1}{\sqrt{4\pi t}} \int_{\mathbb{R}} e^{-\frac{(x-y)^2}{4t}} \phi(y) dy$

PARA LO QUE SON FUNDAMENTALES LAS SIGUIENTES PROP.

• $f(x) = \int_{\mathbb{R}} \hat{f}(\gamma) e^{2\pi i x \gamma} d\gamma = \hat{\hat{f}}(-x)$ "FÓRMULA DE
INVERSIÓN"

• $\widehat{f * g} = \hat{f} \hat{g}$, SIENDO $(f * g)(x) = \int_{\mathbb{R}} f(y) g(x-y) dy$

"CONVOLUCIÓN
ENTRE f Y g "

• S) $f(x) = e^{-\pi x^2}$, $\hat{f} = f$.

§ 2. EL GRUPO DUAL

SEA G UN GRUPO ABELIANO FINITO.

DEF: $\hat{G} = \text{Hom}(G, \mathbb{C}^\times) = \text{Hom}(G, S^1)$. (SERÁ EL DOMINIO DE LA TRANSF.)

LEMA: $\widehat{H \times K} \simeq \hat{H} \times \hat{K}$.

¡ES UN G.A.F.!

DEM: $H \rightarrow H \times K \leftarrow K$; $\chi \mapsto (\chi_H, \chi_K)$ ISO.

$\chi_H \searrow \downarrow \chi \swarrow \chi_K$
 S^1

PROP: $G \simeq \hat{\hat{G}}$ (NO NATURALMENTE)

"TODO G.A.F. ES AUTO DUAL"

DEM: BASTA CONSIDERAR $G = \mathbb{Z}/N$ (POR EL LEMA).

EL MAPA

$$G \rightarrow \hat{G}$$

$$x \mapsto (y \mapsto e^{2\pi i xy/N})$$

¡PUEDES IR COMO EL. TRAS LA DEF!

ES UN ISO.

- BD, MORFISMO ✓
- ISO: HAY UNA BIY

$$\hat{G} \rightarrow \{z \in S^1 : z^N = 1\}$$

$$\varphi \mapsto \varphi(1)$$

OBS: SE PUEDE CAMBIAR S^1 POR CUALQUIER GRUPO QUE TENGA UN ELEM. DE ORDEN N

☒

SEA $H \leq G$. DEFINIMOS

$$H^\# = \{ \chi \in \hat{G} : \underbrace{\chi|_H = 1} \} \simeq \widehat{G/H}$$

$$=: \text{Res}(\chi)$$

(ie, $H^\# = \ker \text{Res}$)

Prop:

$$0 \rightarrow \widehat{G/H} \rightarrow \widehat{G} \xrightarrow{\text{Res}} \widehat{H} \rightarrow 0$$

ES EXACTA (A DERECHA).

DEM: $\text{Im Res} \simeq \widehat{G} / \widehat{G/H}$ TIENE ORDEN $|H|$

$\leadsto$ ES IGUAL A $\widehat{H}$.

TEO (DUALIDAD DE PONTRYAGIN):

$$\begin{aligned} \text{ev}: G &\rightarrow \widehat{\widehat{G}} \\ x &\mapsto (x \mapsto \chi(x)) \end{aligned}$$

ES UN ISO (NATURAL). → TENÍAMOS UN ISO, NO NATURAL...

DEM: B.V. ES MONO, i.e. QUE SI $x \neq 0$,

$\exists \chi \in \widehat{G}$ CON $\chi(x) \neq 1$. "LOS CARACTERES SEPARAN PUNTOS"

Tomamos $H = \langle x \rangle$, $\psi \in \widehat{H} \setminus \{1\}$ y $\chi \in \widehat{G}$ con $\text{Res } \chi = \psi$ □

§ 3. LA TRANSF. DE FOURIER

DEF: $L^2(G) = \text{Fun}(G, \mathbb{C})$.

$\leadsto$ ES UN $\mathbb{C}$ -EV DE DIMENSIÓN $|G|$,
CON BASE $\{\delta_x\}_{x \in G}$.

NOTA: SI $G = \mathbb{Z}/N$, VALE CAMBIAR $\mathbb{C}$ POR K SIEMPRE
QUE $K^\times$ TENGA UNA RAÍZ N -ÉSIMA (PRIMITIVA). POR EJ.,
 $K = \mathbb{Z}/p$, CON p PRIMO TAL QUE $p \equiv 1 \pmod{N}$.

LEMA (ORTOGONALIDAD DE CARACTERES):

$$1) \sum_{x \in G} \chi(x) = |G| \cdot \delta_0(\chi)$$

$$2) \sum_{\chi \in \hat{G}} \chi(x) = |G| \delta_0(x) \\ = \text{ev}_x(\chi)$$

DEM:

1) SE SIGUE DE QUE SI DADO $\chi \in \hat{G}$ CONSIDERAMOS
 $S = \sum_{x \in G} \chi(x)$, ENTONCES

$$\chi(y) S = S \quad \forall y \in G$$

2) SE SIGUE DE (1) + CONTRADICCIÓN ($\text{ev}_\chi = 1$ SI $\chi = 0$) $\square$

PROP: $L(G) = \langle \hat{G} \rangle \rightsquigarrow$ LUEGO, $\hat{G}$ ES UNA BASE DE $L(G)$

DEM: $\sum_{\chi \in \hat{G}} \chi(x) \chi(y) = |G| \delta_0(x+y) = |G| \delta_{-x}(y)$

$$\Rightarrow \delta_{-x} \in \langle \hat{G} \rangle \quad \square$$

DEF: SEA $f \in L(G)$. LA TRANSF. DE FOURIER DE f
ES LA FUNCIÓN $\hat{f} \in L(\hat{G})$ DADA POR

$$\hat{f}(\chi) = \sum_{x \in G} f(x) \overline{\chi(x)}$$

(TENEMOS
 $L(G) \xrightarrow{\sim} L(\hat{G})$
 $f \mapsto \hat{f}$,
C-LINEAL)

OBJ: SI $G = \mathbb{Z}/N$ E IDENTIFICAMOS

$$G \rightarrow \hat{G}, \quad x \mapsto (x \mapsto e^{2\pi i xy/N}),$$

TENEMOS

$$\hat{\hat{f}}(y) = \sum_{x \in \mathbb{Z}/N} f(x) e^{-2\pi i xy/N}$$

"SIMILAR
A $G = \mathbb{R}$ "

EJEMPLOS

$$1) \hat{f}_x = \text{ev}_{-x} \quad \forall x \in G \quad \hat{\hat{G}} \subseteq L(\hat{G})$$

$\leadsto$ DEFINICIÓN

$$2) \hat{\chi} = |G| \delta_x \quad \forall \chi \in \hat{G}$$

$\leadsto$ ORTOGONALIDAD

TEO (FÓRMULA DE INVERSIÓN): si $f \in L(G)$,

$$f(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(x)$$

→ POR ESTO
LLAMAMOS A
LOS $\hat{f}(\chi)$
"COEF. DE FOURIER"
de f

(|G|: PUNTOS "MIDEN" 1)

DEM: BASTA CONSIDERAR $f = \psi \in \hat{G}$. EN ESTE CASO, EL RHS. ES

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} |G| \delta_\psi(\chi) \chi(x) = \psi(x)$$

□

OBS: PENSANDO $\chi(x) = \text{ev}_{-x}(\chi)$, (Y USANDO QUE $|\hat{G}| = |G|$)
LA FÓRMULA DICE QUE

$$f(x) = \frac{1}{|G|} \hat{\hat{f}}(\text{ev}_{-x})$$

$\leadsto$ "PONTYAGIN" $f(x) = \frac{1}{|G|} \hat{\hat{f}}(-x)$ //

PROP (PRIO. DE INCERTIDUMBRE, HEISENBERG): si $f \neq 0$,

$$|\text{supp } f| \cdot |\text{supp } \hat{f}| \geq |G|$$

$\leadsto$ VALE EL =
EN LOS EJEMPLOS

DEM: $|\hat{f}(\chi)| \leq \max |f| |\text{supp } f|$,

por DEF

$|f(x)| \leq \frac{1}{|G|} \max |\hat{f}| |\text{supp } \hat{f}|$, por F. INV.

5

Así,

$$\cancel{\max |f|} \leq \frac{1}{|G|} \cdot \cancel{\max |f|} \cdot \cancel{|\text{supp } f|} \cdot |\text{supp } \hat{f}|$$

si $f \neq 0$

□

§ 4. PROPIEDADES BÁSICAS

NOT: • Si $f \in L(G)$ y $x \in G$, $T_x f \in L(G)$ es
LA FUNCIÓN DADA POR

$$(T_x f)(y) = f(y-x)$$

• Si $G \in \mathbb{Z}/N$ y $a \in (\mathbb{Z}/N)^\times$, PARA $f \in L(G)$
PONEMOS $R_a f \in L(G)$,

$$(R_a f)(x) = f(ax)$$

PROP: 1) $\widehat{T_x f}(\chi) = \chi(-x) \hat{f}(\chi)$

2) $\widehat{R_a f}(\chi) = \hat{f}(R_{a^{-1}} \chi)$

DEM: 1) BASTA PROBARLO PARA $f = \psi \in \hat{G}$;

$$\widehat{T_x \psi}(\chi) = \sum_{y \in G} \psi(y-x) \overline{\chi(y)} = \sum_{y \in G} \psi(y-x) \overline{\chi(y-x+x)} = \sum_{y \in G} \psi(y-x) \overline{\chi(y-x)} \overline{\chi(x)} = \chi(-x) \sum_{y \in G} \psi(y-x) \overline{\chi(y-x)} = \chi(-x) \hat{\psi}(\chi)$$

2) $\widehat{R_a f}(\chi) = \sum_{x \in G} f(ax) \overline{\chi(x)}$

$$\stackrel{\substack{\downarrow \\ y=ax}}{=} \sum_{y \in G} f(y) \overline{\chi(a^{-1}y)} = \hat{f}(R_{a^{-1}} \chi)$$

□

NOT: Si $f, g \in L(G)$, $f * g \in L(G)$ es la
FUNCIÓN DADA POR

$$(f * g)(x) = \sum_{y \in G} f(y) g(x-y)$$

EJ: $\delta_x * \delta_y = \delta_{x+y}$

$\leadsto L(G) \simeq \mathbb{C}[G]$, como $\mathbb{C}$ -ÁLGEBRAS

PROP: $\widehat{f * g} = \widehat{f} \widehat{g}$ " $(L(G), *) \xrightarrow{\widehat{\cdot}} (L(\widehat{G}), \cdot)$ "
ES UN ISO DE ÁLG.

DEM: BASTA CONSIDERAR $f = \delta_x$, $g = \delta_y$. ASÍ:

$$\begin{aligned} \widehat{\delta_x * \delta_y} &= \widehat{\delta_{x+y}} = \text{ev}_{-(x+y)} = \text{ev}_{-x} \cdot \text{ev}_{-y} \\ &= \widehat{\delta_x} \cdot \widehat{\delta_y} \quad \square \end{aligned}$$

PROP: 1) $\delta_x * f = T_x f$
2) $\chi * f = \widehat{f}(\chi) \cdot \chi$

DEM: 1) POR DEF.

$$\begin{aligned} 2) \quad \widehat{\chi * f} &= \widehat{\chi} \widehat{f} = |G| \delta_\chi \widehat{f} \\ \widehat{f}(\chi) \chi &= \widehat{f}(\chi) \widehat{\chi} = \widehat{f}(\chi) |G| \delta_\chi, \end{aligned}$$

Y LISTO ☺

□

PARA CADA f ,
 $\widehat{G}$ ES UNA BASE
DE AVEC. DEL
OPERADOR
 $L(G) \xrightarrow{\widehat{\cdot}} L(G)$
 $g \mapsto g * f$

DEF: $\langle, \rangle$ P.I. EN $L(G)$,

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$$

OBS VARIAS:

1) $\{\delta_x\}$ ES UNA BASE ORTOG, $\|\delta_x\| = 1/\sqrt{|G|}$

2) $\hat{G}$ ES UNA BON $\leadsto$ ORTOGONALIDAD DE CARACTERES

3) $\hat{f}(x) = |G| \langle f, \chi \rangle \leadsto$ LOS COEF. DE FOURIER DE f SON PROD. INTERNOS

PROP (PLANCHEREL):

$$\langle f, g \rangle = \frac{1}{|G|} \langle \hat{f}, \hat{g} \rangle \quad "4G) \rightarrow L(\hat{G}) \text{ ES CASI UNA ISOMETRÍA}"$$

DEM: PODEMOS SUPONER

$f = \chi, g = \psi \in \hat{G}$. ASÍ,

$$\begin{aligned} \langle \hat{\chi}, \hat{\psi} \rangle &= |G|^2 \langle \delta_\chi, \delta_\psi \rangle = \begin{cases} |G|, & \chi = \psi \\ 0, & \text{SI NO} \end{cases} \\ &= |G| \langle \chi, \psi \rangle \quad \square \end{aligned}$$

CONO (PARSEVAL): SI $f \in L(G)$,

$$\sum_{x \in G} |f(x)|^2 = \frac{1}{|G|} \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2.$$

OBS (CONT): CONSIDEREMOS $C_f \in \text{End}(4G)$.

$$\bullet \text{Tr}(C_f) = |G| \sum_{x \in G} \langle C_f(\delta_x), \delta_x \rangle$$

$\hookrightarrow$ BASE $\{\delta_x\}$, ORT $\|\delta_x\|^2 = 1/|G|$

$$= |G| \sum_{x \in G} \langle T_x f, \delta_x \rangle = |G| f(0)$$

$$\bullet \text{Tr}(C_f) = \sum_{\chi \in \hat{G}} \langle C_f(\chi), \chi \rangle = \sum_{\chi \in \hat{G}} \hat{f}(\chi)$$

$\hookrightarrow$ BON $\hat{G}$

→ RECUPERAMOS LA FÓRMULA DE INV. EN 0:

$$f(0) = \frac{1}{|G|} \sum_{x \in \hat{G}} \hat{f}(x)$$

NOTA: ESTO IMPLICA LA F.I. EN GENERAL,
CAMBIANDO f POR $T_x f$.

§5. FÓRMULA DE SUMACIÓN DE POISSON

CUANDO $G = \mathbb{R}$, LA FÓRMULA DICE QUE

$$\sum_{m \in \mathbb{Z}} f(m) = \sum_{m \in \mathbb{Z}} \hat{f}(m) \quad (f \in \mathcal{S}(\mathbb{R})),$$

O MÁS GRALMENTE,

$$\sum_{m \in \mathbb{Z}} f(m+x) = \sum_{m \in \mathbb{Z}} \hat{f}(m) e^{2\pi i m x}$$

$f(x)$, FUNCIÓN EN
 $\mathbb{R}/\mathbb{Z} \cong S^1$

TRANSF.
EN $\mathbb{R}$

→ CONECTA EL ANÁLISIS DE FOURIER EN S^1 CON
EL DE $\mathbb{R}$; EL RHS ES EL DESARROLLO DE FOURIER DE f .

APLICACIÓN

SEA $f(x) = e^{-\pi x^2}$. PARA $z \in \mathbb{C}$, SEA $f_z(x) = e^{-\pi z x^2} = f(\sqrt{z}x)$. TENEMOS QUE

$$\hat{f}_z(y) = \frac{1}{\sqrt{z}} \hat{f}(y/z) = \frac{1}{\sqrt{z}} f(y/z) = \frac{1}{\sqrt{z}} f_z(y)$$

$$\therefore \underbrace{\sum_{m \in \mathbb{Z}} e^{-\pi i z m^2}}_{=: \theta(z)} = 1/\sqrt{z} \sum_{m \in \mathbb{Z}} e^{-\pi i \frac{1}{z} m^2},$$

ES DECIR: $\theta(1/z) = \sqrt{z} \theta(z)$

"MODULARIDAD" DE LA SERIE θ ; IMPLICA LA ECUACIÓN FUNCIONAL $\zeta(s) \leftrightarrow \zeta(1-s)$ PARA LA FUNCIÓN ζ DE RIEMANN

VOLVIENDO A G G.A.F. SEA $H \leq G$.
RECORDAMOS QUE $\widehat{G/H} \cong H^\# = \{ \chi \in \widehat{G} : \chi|_H = 1 \}$.

SEA $f \in L(G)$

TEO:
$$\sum_{y \in H} f(y) = \frac{1}{[G:H]} \sum_{\chi \in H^\#} \widehat{f}(\chi).$$

DEM: SEA $F(x) = \sum_{y \in H} f(y+x) \in L(G/H)$.

POR LA FÓRMULA DE INV. EN G/H ,

$$F(x) = \frac{1}{[G:H]} \sum_{\chi \in H^\#} \widehat{F}(\chi) \chi(x);$$

AHORA, SI $\chi \in H^\#$:

$$\widehat{F}(\chi) = \sum_{x \in G/H} F(x) \overline{\chi(x)} = \sum_{x \in G/H} \sum_{y \in H} f(x+y) \overline{\chi(x)}$$

$$= \widehat{f}(\chi). \quad \text{Y LISTO, PONIENDO } x=0 \quad \square \quad /10$$

§ 6. APLICACIONES A LA ARITMÉTICA

Tomamos p primo impar.

CONSIDERAMOS EL SÍMBOLO DE LEGENDRE

$$\left(\frac{x}{p}\right) = \begin{cases} 0, & p \mid x \\ 1, & x \text{ es un } \square \text{ en } (\mathbb{Z}/p)^\times \\ -1, & \text{si no} \end{cases}$$

PROP: 1) p -PERIÓDICO
2) MULTIP (EN x)

$$3) \left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p}$$

DEM: VALE SI
 $(\mathbb{Z}/p)^\times = \langle x \rangle$;
 EL LHS ES $-1 \dots$

TOMAMOS $G = \mathbb{Z}/p$, CONSIDERAMOS

$f_p(x) = \left(\frac{x}{p}\right) \in L(G)$, IDENTIFICAMOS

$$G \xrightarrow{\sim} \hat{G}$$

$$x \mapsto \left(\frac{x}{p}\right) \mapsto e^{2\pi i xy/p}$$

LEMA: $\hat{f}_p(x) = \hat{f}_p(1) \cdot f_p(x)$.

" f_p ES LA VERSIÓN DISCRETA DE LA GAUSSIANA $e^{-\pi x^2}$ "

DEM: • SI $x \neq 0$,

$$\hat{f}_p(x) = \sum_y \left(\frac{y}{p}\right) e^{-2\pi i xy/p} = \left(\frac{x}{p}\right) \sum_y \left(\frac{xy}{p}\right) e^{-2\pi i xy/p}$$

$$= f_p(x) \sum_z \left(\frac{z}{p}\right) e^{-2\pi i z/p} = f_p(x) \hat{f}_p(1)$$

• si $x=0$,

$$\hat{f}_p(0) = \sum_y \left(\frac{y}{p}\right) = 0$$

• ORTOGONALIDAD, δ
• MITAD $\square$, MITAD ∇

como: si $p \nmid x$, $\hat{f}_p(1) = f_p(x) \hat{f}_p(x)$.

DEF (SUMA DE GAUSS):

$$G_p = \hat{f}_p(-1) = \sum_y \left(\frac{y}{p}\right) e^{2\pi i y/p} \in \mathbb{Z}[e^{2\pi i/p}] =: \mathbb{R}$$

PROP: $G_p^2 = (-1)^{p-1/2} p =: p^*$ (o.a. $|G_p| = \sqrt{p}$)

DEM: $p f_p(-x) = \hat{\hat{f}}_p(x) = \hat{f}_p(1) \hat{f}_p(x)$
INV. LEMA

$\Rightarrow$ $x=-1$ $p = \hat{f}_p(1) \hat{f}_p(-1) = f_p(-1) (\hat{f}_p(-1))^2 = (-1)^{p-1/2} G_p^2$ $\square$

TEO (LEY DE RECIP. CUADRÁTICA, GAUSS):

p, q PRIMOS IMPARES. ENTONCES

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

LEMA: $(\hat{f}_p(x))^q \equiv \hat{f}_p(qx) \pmod{q\mathbb{R}}$

DEM: $\hat{f}_p(x)^q = \left(\sum_y \left(\frac{y}{p}\right) e^{-2\pi i xy/p}\right)^q$

CLAVE: DA CONGRUENCIAS mod q PARA $\left(\frac{y}{p}\right)$ (TRANSF.)

$\left(\frac{y}{p}\right)^q \equiv \left(\frac{y}{p}\right)$ $\equiv \sum_y \left(\frac{y}{p}\right) e^{-2\pi i xyq/p} = \hat{f}_p(qx) \pmod{q\mathbb{R}}$ $\square$

DEM (DE LA LRC.):

$G_p^q = (\hat{f}_p(-1))^q \equiv \hat{f}_p(-q) = \hat{f}_p(1) \hat{f}_p(-q)$

LEMA VIEJO LEMA

$$= \hat{f}_p(1) \hat{f}_p(-1) \hat{f}_p(q) = G_p\left(\frac{q}{p}\right) \pmod{qR}$$

$$\Rightarrow G_p^{q+1} \equiv p^* \left(\frac{q}{p}\right) \pmod{qR} \quad (1);$$

Por otra parte,

$$G_p^{q-1} = (G_p^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \stackrel{\text{PROP (3)}}{\equiv} \left(\frac{p^*}{q}\right) \pmod{q} \quad (2).$$

JUNTANDO TODO,

$$p^* \left(\frac{q}{p}\right) \equiv G_p^2 G_p^{q-1} \equiv p^* \left(\frac{p^*}{q}\right) \pmod{qR}$$

$$\Rightarrow \left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$$

→ SIENDO ENTEROS,
ES $\pmod{q}$

$$\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left((-1)^{\frac{p-1}{2}}\right) \left(\frac{p}{q}\right) = \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \quad \square$$

§ 7. FFT (COOLEY-TUKEY, 1965 ó
GAUSS, 1805)

TOMEMOS $G = \mathbb{Z}/m$

e.g. SIRVE
PARA MULTIPLIC.
POLINOMIOS

PROBLEMA: si $f, g \in L(G)$, CALCULAR $f * g$
LLEVA "MUCHAS" MULTIPLICACIONES:

$$(f * g)(x) = \sum_{y \in \mathbb{Z}/m} f(y) g(x-y) \quad \sim m^2 \text{ MULT (m POR CADA } x)$$

$$\text{PERO: } (f * g)(x) = \frac{1}{m} \widehat{\widehat{f * g}}(-x) = \frac{1}{m} \widehat{f} \widehat{g}(-x)$$

→ PODEMOS CALCULAR $f * g$ RÁPIDO SI PODEMOS
TRANSFORMAR RÁPIDO (CALCULAR $\widehat{f \cdot g}$: m MULTIP.)

OBS: $\hat{f}(x) = \frac{1}{m} \sum_{y \in \mathbb{Z}/m} f(y) \zeta_m^{yx}$ (NOT: $\zeta_m = e^{-2\pi i/m}$)

$\leadsto$ LLEVA m^2 MULTIPLICACIONES*, INGENUAMENTE.

(NOT: $\tilde{f}_m$, LA TRANSF. EN $\mathbb{Z}/m$)

DIVIDIR Y CONQUISTAR

SUPONGAMOS $m = 2m$ (EN PART, $\zeta_m^2 = \zeta_{m/2}$; $\zeta_m^m = -1$)

SEA $f \in L(\mathbb{Z}/m)$. ENTONCES $\forall 0 \leq x < m$:

$$(\tilde{f}_m f)(x) = \sum_{y=0}^{m-1} f(y) \zeta_m^{xy} = \sum_{y=0}^{m-1} f(2y) \zeta_m^{xy} + \zeta_m^x \sum_{y=0}^{m-1} f(2y+1) \zeta_m^{xy}$$

CONSIDEREMOS $f', f'' \in L(\mathbb{Z}/m)$ DADAS POR

$$f'(y) = f(2y), \quad f''(y) = f(2y+1). \quad \left(\begin{array}{l} \text{⊗ EL CÁLCULO} \\ \text{DE LAS POT.} \\ \text{DE } \zeta_m \text{ NO} \\ \text{CUENTA} \end{array} \right)$$

ASÍ, $\forall 0 \leq x < m$:

$$\bullet (\tilde{f}_m f)(x) = (\tilde{f}_m f')(x) + \zeta_m^x (\tilde{f}_m f'')(x)$$

$$\bullet (\tilde{f}_m f)(x+m) = (\tilde{f}_m f')(x) - \zeta_m^x (\tilde{f}_m f'')(x)$$

SI DENOTAMOS $T_m = \#$ MULT. NECESARIAS PARA CALCULAR $\tilde{f}_m$ (ASÍ)

$$T_m = \underbrace{2T_{m/2}}_{\tilde{f}_m f'', \tilde{f}_m f''} + m \rightarrow \zeta_m^x (\tilde{f}_m f'')(x), \quad 0 \leq x < m$$

ASÍ (INDUCCIÓN): $T_{2^k} = 2^{k-1} (k+2)$

$$\circ \circ T_m = O(m \log m) \leadsto \text{mucho mejor que } m^2$$

(Y EN PART, CÁLCULO $f \zeta$ CON $\approx m \log m + m = O(m \log m)$ MULT.
 TRANSF. MULT. PUNT.