Mètodes analítics en teoria de nombres

Bernat Esteve Sagarra

November 10, 2025

Exercici 1

Sigui K un cos, q un primer senar diferent de la carecterística de K i ω un arrel primitiva q-èsima de la unitat. Donat $a \in \mathbb{F}_q^\times$, definim la *suma de Gauss* relativa a a i ω com:

$$G_\omega(a) := G(a) := \sum_{m \in \mathbb{F}_q^\times} \left(\frac{m}{q}\right) \omega^{ma}.$$

Escrivim simplement G per denotar $G(1)$. Demostreu que:

1. $G(a) = \left(\frac{a}{q}\right) G$.
2. $G = 1 + \sum_{m \in \mathbb{F}_q^\times} \omega^{m^2}$.

Exercici 1.1

Primer, recordem que pels primers senars, el símbol de Legendre es defineix

$$\left(\frac{a}{q}\right) = \begin{cases} -1 & \text{si } a \text{ no és un quadrat mòdul } q. \\ 0 & \text{si } a = 0. \\ 1 & \text{si } a \text{ és un quadrat mòdul } q. \end{cases}$$

Per tant:

$$\left(\frac{a}{q}\right) G(1) = \left(\frac{a}{q}\right) \sum_{m \in \mathbb{F}_q^\times} \left(\frac{m}{q}\right) \omega^m = \sum_{m \in \mathbb{F}_q^\times} \left(\frac{ma}{q}\right) \omega^m =$$

I si $a = 0$, aleshores, $G(a) = \sum_{m \in \mathbb{F}_q^\times} \left(\frac{m}{q}\right) = 0$, ja que la meitat dels elements de $\mathbb{F}_q^\times$ són quadrats i la altra no (es pot veure veient que el símbol de Legendre és multiplicatiu, i que per tant, hi ha una bijecció entre els 2 conjunts que consisteix en multiplicar per un no-quadrat).
En el cas de que $a \neq 0$, aleshores $\left(\frac{ma^2}{q}\right) = \left(\frac{m}{q}\right)$. Per tant:

$$\sum_{m \in \mathbb{F}_q^\times} \left(\frac{ma}{q}\right) \omega^m = \sum_{am \in \mathbb{F}_q^\times} \left(\frac{ma^2}{q}\right) \omega^{am} = \sum_{m \in \mathbb{F}_q^\times} \left(\frac{m}{q}\right) \omega^{am} = G(a)$$

Que és el que volíem veure.

Exercici 1.2

Per veure la segona part, notem que

$$\sum_{m\in\mathbb{F}_q^\times}\left(\frac{m}{q}\right)\omega^m$$

Però, notem que si $m=n^2$, aleshores, $\left(\frac{m}{q}\right)\omega^m=\omega^{n^2}$; d'altra banda, si m no és un quadrat, aleshores

$$\sum_{\left(\frac{m}{q}\right)=-1}\left(\frac{m}{q}\right)\omega^m=\sum_{\left(\frac{m}{q}\right)=-1}-\omega^m=\sum_{\left(\frac{m}{q}\right)=1}\omega^m$$

On la última igualtat es deu a que la suma de les arrels és 0. Per tant

$$\sum_{m\in\mathbb{F}_q^\times}\left(\frac{m}{q}\right)\omega^m=2\sum_{\left(\frac{m}{q}\right)=1}\omega^m$$

Però notem que estem sumant 2 vegades sobre tots els quadrats, però com que cada quadrat és el quadrat de 2 enters mòdul q. Excepte que el 1 només el sumem una vegada (estem excluint el 1, ja que no és una arrel primitiva). Per tant:

$$\sum_{m\in\mathbb{F}_q^\times}\left(\frac{m}{q}\right)\omega^m=2\sum_{\left(\frac{m}{q}\right)=1}\omega^m=\sum_{m\in\mathbb{F}_q^\times}\omega^{m^2}$$

Que és el que volíem veure.

Exercici 2

Sigui K un cos, q un primer senar diferent de la carecterística de K i ω una arrel primitiva q-èsima de la unitat. Demostreu que:

1. Les arrels q-èsimes primitives de la unitat a la clausura algebràica $\overline{K}$ són les arrels de $\Phi_q(T) = T^{q-1} + \cdots + T + 1 \in K[T]$. En particular, la suma de totes elles és -1.
2. $G^2 = (-1)^{\frac{q-1}{2}} q$.

Exercici 2.1

Notem que $\Phi_q(T) = \frac{T^q-1}{T-1}$, per tant, $\Phi_q(\omega) = \frac{1-1}{\omega-1} = 0$. que és el que volia veure. I per les fòrmules de Vieta, tenim que la suma de les arrels és menys el coeficient de grau $[T^{q-2}]$, i per tant, la suma de les arrels és -1.

Exercici 2.2

Per veure què val G^2, seguirem la indicació:

$$\begin{aligned} G^2 &= \sum_{m\in\mathbb{F}_q^*}\sum_{n\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\left(\frac{n}{q}\right)\omega^m\omega^n = \\ &= \sum_{m\in\mathbb{F}_q^*}\sum_{n\in\mathbb{F}_q^*}\left(\frac{mn}{q}\right)\omega^{m+n} = \\ &= \sum_{m\in\mathbb{F}_q^*}\sum_{n\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\omega^{n(m+1)} = \\ &= \sum_{m\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\sum_{n\in\mathbb{F}_q^*}\omega^{n(m+1)} \end{aligned}$$

Però, sabem que si $m+1 \equiv 0 \pmod q$ aleshores, la suma dona $q-1$, i dona -1 altrament, per tant:

$$\sum_{m\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\sum_{n\in\mathbb{F}_q^*}\omega^{n(m+1)} = \left(\frac{-1}{q}\right)(q-1) - \sum_{m\in\mathbb{F}_q^*\setminus\{-1\}}\left(\frac{m}{q}\right)$$

Però sabem també, que la suma sobre $\sum_{m\in\mathbb{F}_q^*}\left(\frac{m}{q}\right) = 0$, per tant, si restem als 2 costats $\left(\frac{-1}{q}\right)$ obtenim:

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

On la última igualtat, és un resultat bastant conegut (i.e. que -1 és un quadrat mòdul q si i només si q és congruent amb 1 mòdul 4).

Exercici 3

Siguin q i p primers senars diferents. Demostreu que

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

Exercici 3

Sigui ω una arrel primitiva q-èsima. Aleshores mirem-nos G_ω sobre el cos $\mathbb{F}_p[\omega]$.

$$\left(\frac{p}{q}\right) G = G_\omega(p) = \sum_{m\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\omega^{pm}$$

però com que p és un primer senar, aleshores $\left(\frac{m}{q}\right)^p = \left(\frac{m}{q}\right)$. Per tant:

$$\sum_{m\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\omega^{pm} = \sum_{m\in\mathbb{F}_q^*}\left(\left(\frac{m}{q}\right)\omega^{m}\right)^p$$

I com que el cos té carecterística p, aleshores, $a^p + b^p = (a+b)^p$:

$$\sum_{m\in\mathbb{F}_q^*}\left(\left(\frac{m}{q}\right)\omega^{m}\right)^p = \left(\sum_{m\in\mathbb{F}_q^*}\left(\frac{m}{q}\right)\omega^{m}\right)^p = G^p$$

I com que p i q són primers senars, alehsores $p-1$ és parell.

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

Que és el que volíem veure.

Exercici 4

Sigui $G \in \mathbb{C}$ la suma de Gauss relativa a $\omega = e^{2\pi i/q}$. Demostreu que

$$G = \sqrt{q}\frac{1+i^{-q}}{1-i}.$$

Exercici 4

Recordem la fòrmula de sumació de Poisson: Si A i B són enters amb $A < B$, aleshores

$$\sum_{n=A}^{B} f(n) = \sum_{\nu\in\mathbb{Z}} \int_A^B f(u)e^{2\pi i\nu u}\mathrm{d}u$$

Per tant, aplicant això al nostre cas:

$$\sum_{n=0}^{q} \omega^{n^2} = \sum_{\nu\in\mathbb{Z}} \int_0^q e^{2\pi i\nu u+\frac{2\pi i u^2}{q}}\mathrm{d}u$$

I ara si fem el canvi de variable $u = q(y-\nu/2)$ $\mathrm{d}u = q\mathrm{d}y$.

$$\sum_{\nu\in\mathbb{Z}} \int_0^q e^{2\pi i\nu u+\frac{2\pi i u^2}{q}}\mathrm{d}y = \sum_{\nu\in\mathbb{Z}} \int_{\nu/2}^{1+\nu/2} e^{2\pi i\nu q(y-\nu/2)+2\pi iq(y^2-\nu y+\nu^2/4)}q\mathrm{d}y$$

I simplificant les coses, obtenim

$$\sum_{\nu\in\mathbb{Z}} \int_{\nu/2}^{1+\nu/2} e^{2\pi iq(-\nu^2/4+y^2)}q\mathrm{d}y = q\sum_{\nu\in\mathbb{Z}} e^{-\pi iq\nu^2/2}\int_{\nu/2}^{1+\nu/2} e^{2\pi iqy^2}\mathrm{d}y$$

Si ara separem la suma entre ν parell i senar:

$$q\sum_{2\nu\in\mathbb{Z}} e^{-2\pi iq\nu^2}\int_{\nu}^{1+\nu} e^{2\pi iqy^2}\mathrm{d}y + q\sum_{2\nu+1\in\mathbb{Z}} e^{2\pi iq\nu(-\nu^{-1})}e^{-\pi iq/2}\int_{\nu+1/2}^{\nu+3/2} e^{2\pi iqy^2}\mathrm{d}y$$

Però notem que com que ν són enters, aleshores per Euler $e^{2\pi ik} = 1$:

$$q\sum_{2\nu\in\mathbb{Z}} \int_{\nu}^{1+\nu} e^{2\pi iqy^2}\mathrm{d}y + q\sum_{2\nu+1\in\mathbb{Z}} e^{-\frac{\pi iq}{2}}\int_{\nu+1/2}^{\nu+3/2} e^{2\pi iqy^2}\mathrm{d}y$$

I si ajuntem tots els sumatoris:

$$q\int_{-\infty}^{\infty} e^{2\pi iqy^2}\mathrm{d}y + qe^{-\frac{\pi iq}{2}}\int_{-\infty}^{\infty} e^{2\pi iqy^2}\mathrm{d}y = q(1+e^{-\frac{\pi iq}{2}})\int_{-\infty}^{\infty} e^{2\pi iqy^2}\mathrm{d}y$$

Però $e^{-\frac{\pi iq}{2}} = i^{-q}$. Per tant:

$$q(1+i^{-q})\int_{-\infty}^{\infty} e^{2\pi iqy^2}\mathrm{d}y$$

I ara si fem el canvi de variable dins de la integral: $y = \frac{x}{\sqrt{q}}$:

$$q(1+i^{-q})\int_{-\infty}^{\infty}\frac{1}{\sqrt{q}}e^{2\pi ix^2}\mathrm{d}x = \sqrt{q}(1+i^{-q})\underbrace{\int_{-\infty}^{\infty} e^{2\pi ix^2}\mathrm{d}x}_{=C} = \sqrt{q}(1+i^{-q})C$$

Per determinar el valor de la constant, podem $q = 3$:

$$G_{\zeta_3}(1) = \left(\frac{1}{3}\right)\zeta_3 + \left(\frac{2}{3}\right)\zeta_3^2$$

On $\zeta_3 = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$, i $\zeta_3^2 = \overline{\zeta}_3$. Per tant

$$G_{\zeta_3}(1) = \zeta_3 - \zeta_3^2 = i\sqrt{3}$$

I segons la fòrmula

$$G = \sqrt{3}(1+i)C = i\sqrt{3}$$

Per tant

$$C = \frac{i}{1+i} = \frac{1}{1-i}$$

I ens dona justament la fòrmula que havíem de veure.