Raíces de la unidad

Egor Maximenko

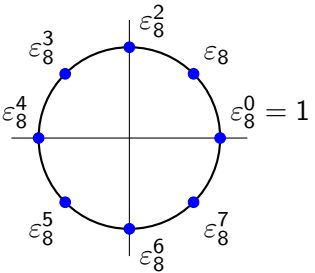
Instituto Politécnico Nacional
Escuela Superior de Física y Matemáticas
México

18 de julio de 2025

Objetivos

Estudiar los números de la forma ε_n^m, donde

$$\varepsilon_n := \mathrm{e}^{\frac{2\pi\,\mathrm{i}}{n}}\,.$$



Calcular la suma

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} \qquad (m \in \mathbb{Z}).$$

Prerrequisitos

Para entender bien este tema, se recomienda saber los siguientes temas.

- La función exp y sus propiedades.
- La función circular $\varphi \mapsto \mathrm{e}^{\mathrm{i}\,\varphi}$ y sus propiedades.
- Divisibilidad de números enteros.
- Opcional: el grupo $\mathbb{Z}_n \coloneqq \mathbb{Z}/(n\mathbb{Z})$.

Plan

La función exponencial $\exp\colon \mathbb{C} \to \mathbb{C}$

$$\exp(z) := \sum_{k=0}^{\infty} \frac{z^k}{k!}.$$

Esto es,

$$\exp(z) = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{z^k}{k!} = 1 + z + \frac{z^2}{2} + \frac{z^3}{6} + \cdots.$$

La serie converge de manera absoluta para cada z en $\mathbb{C}$:

$$\sum_{k=0}^{\infty} \frac{|z|^k}{k!} < +\infty.$$

Teorema (exp convierte sumas en productos)

$$\exp(z+w) = \exp(z)\exp(w).$$

Teorema (exp y la conjugación compleja)

$$\left(e^{z}\right)^{*} = e^{z^{*}}.$$

El número e

$$\mathrm{e} := \exp(1).$$

$$\mathrm{e} = \sum_{k=0}^{\infty} \frac{1}{k!} = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + \cdots .$$

La función exponencial de números reales

$$\mathrm{e} := \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Se puede demostrar que si $x \in \mathbb{R}$,

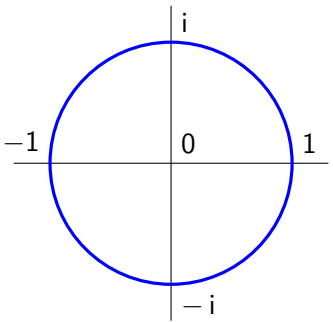
$$\exp(x) = \mathrm{e}^x, \qquad \text{esto es,} \qquad \exp(x) = \lim_{\frac{m}{n} \to x} \left(\sqrt[n]{\mathrm{e}}\right)^m.$$

Por eso se usa la notación

$$\mathrm{e}^z := \exp(z) \qquad (z \in \mathbb{C}).$$

El círculo unitario en el plano complejo

$$\mathbb{T} := \{z \in \mathbb{C} : \ |z| = 1\}.$$



Teorema

$\mathbb{T}$ es un grupo.

En particular,

$$\forall z \in \mathbb{T} \qquad z^{-1} = z^{*}.$$

La función circular

Vamos a repasar las propiedades principales de la función

$$u\colon \mathbb{R} \to \mathbb{T}, \qquad u(\varphi) := \mathrm{e}^{\mathrm{i}\,\varphi}\,.$$

Esta función importante se llama a veces “la exponencial imaginaria”.
Otro término adecuado sería “la función circular”.

Propiedades aritméticas de números de la forma $e^{i\varphi}$

$$e^{i(\varphi+\psi)} = e^{i\varphi}\, e^{i\psi}\,.$$

$$e^{i\varphi}\, e^{-i\varphi} = e^{0} = 1.$$

$$\left(e^{i\varphi}\right)^{*} = e^{(i\varphi)^{*}} = e^{-i\varphi}\,.$$

$$\left(e^{i\varphi}\right)^{-1} = \left(e^{i\varphi}\right)^{*}.$$

El lugar geométrico de números de la forma $e^{i\varphi}$

Teorema

Para cada φ en $\mathbb{R}$,

$$e^{i\varphi} \in \mathbb{T}.$$

Demostración.

$$\left| e^{i\varphi} \right|^2 = e^{i\varphi} \left(e^{i\varphi}\right)^* = e^{i\varphi} e^{-i\varphi} = e^0 = 1.$$

La función circular
(“la función exponencial imaginaria”)

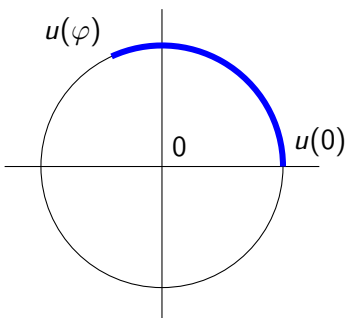
$$u\colon \mathbb{R} \to \mathbb{T}, \qquad u(\varphi) := \mathrm{e}^{\mathrm{i}\,\varphi}\,.$$

Teorema

La longitud del arco $u([0, \varphi])$ es φ.

Idea de demostración:

$$|u'(t)| = |\mathrm{i}\, \mathrm{e}^{\mathrm{i}\varphi}| = 1.$$



El número π

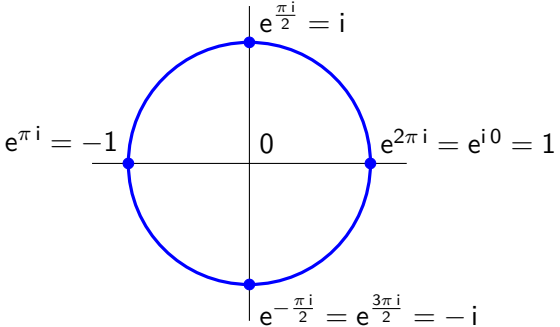
El número π se puede definir de varias maneras equivalentes.

En particular, el número π se determina por las siguientes propiedades:

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

$$\forall x \in \left(0, \frac{\pi}{2}\right) \qquad e^{ix} \neq i\,.$$

Algunos valores de $e^{i\varphi}$



Periodicidad de la función circular $u(\varphi) = e^{i\varphi}$

Lema

Para cada φ en $(0, 2\pi)$,

$$e^{i\varphi} \neq 1.$$

Teorema

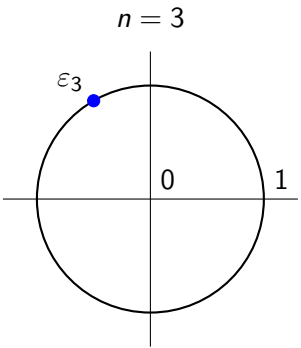
$\ker(u) = 2\pi\mathbb{Z}$, esto es,

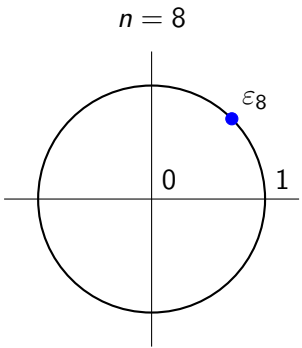
$$\forall \varphi \in \mathbb{R} \qquad e^{i\varphi} = 1 \qquad \Longleftrightarrow \qquad \varphi \in 2\pi\mathbb{Z}.$$

Plan

El número ε_n

$$\varepsilon_n := \mathrm{e}^{\frac{2\pi\,\mathrm{i}}{n}}\,.$$



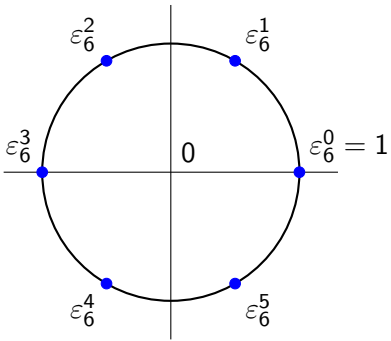


$$\varepsilon_n := \mathrm{e}^{\frac{2\pi\,\mathrm{i}}{n}}\ .$$

La propiedad básica de este número:

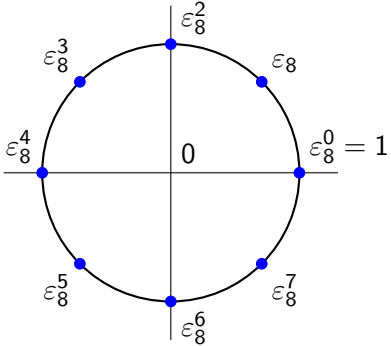
$$\varepsilon_n^n = \mathrm{e}^{2\pi\,\mathrm{i}} = 1.$$

Potencias del número ε_6



Ejercicio: calcular ε_6^k para $k = 6$, $k = 7$, $k = 8$, $k = -2$.

Potencias del número ε_8



Ejercicio: calcular ε_8^k para $k = 8$, $k = 9$, $k = 15$, $k = -3$.

Criterio para $\varepsilon_n^m = 1$

Teorema

Sean $m \in \mathbb{Z}$, $n \in \mathbb{N}$.

$$\varepsilon_n^m = 1 \iff m \in n\mathbb{Z}.$$

Demostración.

$$\varepsilon_n^m = 1 \iff \exp \frac{2\pi \,\mathrm{i}\, m}{n} = 1 \iff \frac{2\pi m}{n} \in 2\pi\mathbb{Z} \iff m \in n\mathbb{Z}.$$

Los números ε_n^p son n-ésimas raíces de 1

Para cada p en $\mathbb{Z}$,

$$\left(\varepsilon_n^p\right)^n = \varepsilon_n^{pn} \overset{pn \in n\mathbb{Z}}{=\!=\!=} 1.$$

Criterio de igualdad $\varepsilon_n^p = \varepsilon_n^q$

$$\varepsilon_n^p = \varepsilon_n^q \quad \Longleftrightarrow \quad \varepsilon_n^{p-q} = 1 \quad \Longleftrightarrow \quad p - q \in n\mathbb{Z}.$$

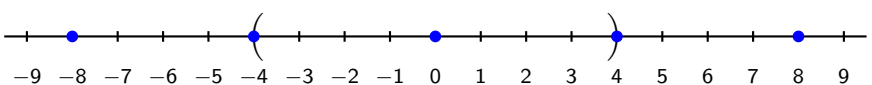
Un lema sobre la divisibilidad de números enteros

Lema

Sean n en $\mathbb{N}$, m en $n\mathbb{Z}$ tales que $|m| < n$.

Entonces, $m = 0$.

$n = 4$



Demostración

Supongamos que $m \in \mathbb{N}$, $m \in n\mathbb{Z}$, $|m| < n$.

Queremos mostrar que $m = 0$.

Demostración

Supongamos que $m \in \mathbb{N}$, $m \in n\mathbb{Z}$, $|m| < n$.

Queremos mostrar que $m = 0$.

Razonando por reducción al absurdo, supongamos que $m \neq 0$.

Demostración

Supongamos que $m \in \mathbb{N}$, $m \in n\mathbb{Z}$, $|m| < n$.

Queremos mostrar que $m = 0$.

Razonando por reducción al absurdo, supongamos que $m \neq 0$.

Como $m \in n\mathbb{Z}$, existe q en $\mathbb{Z}$ tal que $m = nq$.

Demostración

Supongamos que $m \in \mathbb{N}$, $m \in n\mathbb{Z}$, $|m| < n$.

Queremos mostrar que $m = 0$.

Razonando por reducción al absurdo, supongamos que $m \neq 0$.

Como $m \in n\mathbb{Z}$, existe q en $\mathbb{Z}$ tal que $m = nq$.

La suposición que $m \neq 0$ implica que $q \neq 0$.

Demostración

Supongamos que $m \in \mathbb{N}$, $m \in n\mathbb{Z}$, $|m| < n$.

Queremos mostrar que $m = 0$.

Razonando por reducción al absurdo, supongamos que $m \neq 0$.

Como $m \in n\mathbb{Z}$, existe q en $\mathbb{Z}$ tal que $m = nq$.

La suposición que $m \neq 0$ implica que $q \neq 0$.

Como $q \in \mathbb{Z}$ y $q \neq 0$, tenemos que $|q| \geq 1$.

Demostración

Supongamos que $m \in \mathbb{N}$, $m \in n\mathbb{Z}$, $|m| < n$.

Queremos mostrar que $m = 0$.

Razonando por reducción al absurdo, supongamos que $m \neq 0$.

Como $m \in n\mathbb{Z}$, existe q en $\mathbb{Z}$ tal que $m = nq$.

La suposición que $m \neq 0$ implica que $q \neq 0$.

Como $q \in \mathbb{Z}$ y $q \neq 0$, tenemos que $|q| \geq 1$.

Concluimos que $|m| = |nq| \geq n$. Contradicción.

Segundo lema sobre la divisibilidad de números enteros

Lema

Sean n en $\mathbb{N}$ y p, q en $\{0, \ldots, n-1\}$ tales que $p - q \in n\mathbb{Z}$.

Entonces, $p = q$.

Demostración

$0 \leq p < n$ $0 \leq q < n$ $p - q \in n\mathbb{Z}$

Demostración

$0 \leq p < n$

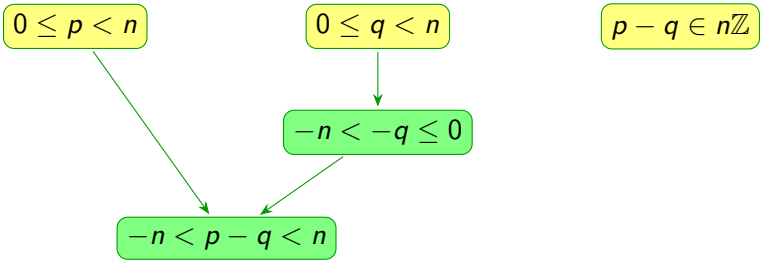
$0 \leq q < n$

$$\downarrow$$

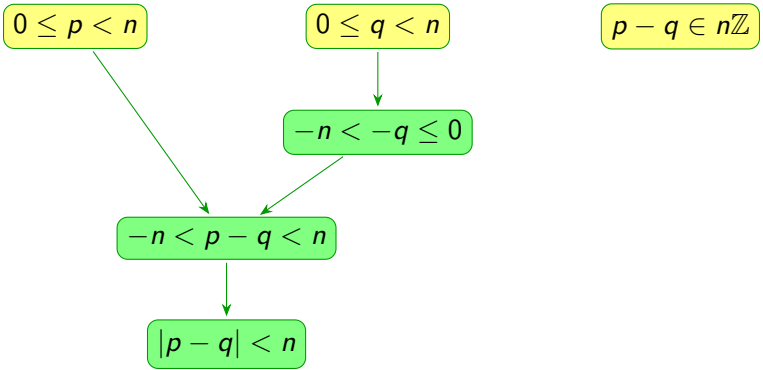
$-n < -q \leq 0$

$p - q \in n\mathbb{Z}$

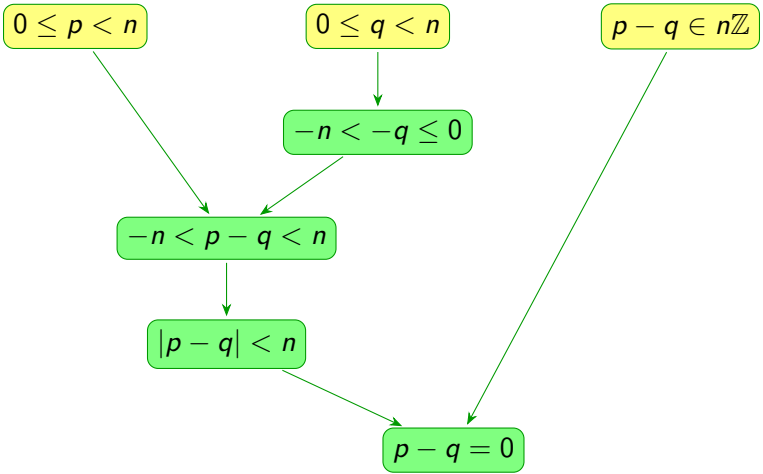
Demostración



Demostración



Demostración



Criterio de igualdad $\varepsilon_n^p = \varepsilon_n^q$

Teorema

Sean $p, q \in \{0, 1, \ldots, n-1\}$. Entonces,

$$\varepsilon_n^p = \varepsilon_n^q \quad \Longleftrightarrow \quad p = q.$$

El grupo de las n-ésimas raíces de unidad

$$G_n := \left\{ z \in \mathbb{C} : \ z^n = 1 \right\}.$$

Teorema

G_n es un grupo.

Teorema

$$G_n = \left\{ \varepsilon_n^p : \ p \in \{0, 1, \ldots, n-1\} \right\}.$$

Isomorfismo entre $\mathbb{Z}_n$ y G_n

$$f\colon \mathbb{Z} \to G_n, \qquad f(k) \coloneqq \varepsilon_n^k.$$

Proposición

f es un epimorfismo, y su núcleo es $\ker(f) = n\mathbb{Z}$.

Por lo tanto,

$$G_n \cong \mathbb{Z}/(n\mathbb{Z}) = \mathbb{Z}_n.$$

Factorización del polinomio $P_n(z) = z^n - 1$

Consideremos el siguiente polinomio:

$$P_n(z) := z^n - 1.$$

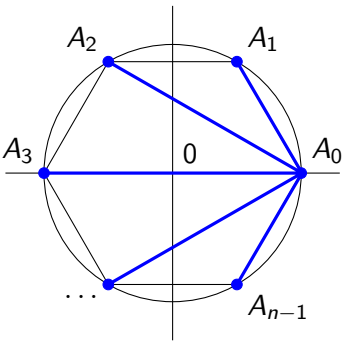
$$\Big\{z \in \mathbb{C}\colon\ P_n(z) = 0\Big\} = G_n = \Big\{\varepsilon_n^k \colon\ k \in \{0, 1, \ldots, n-1\}\Big\}.$$

$$P_n(z) = \prod_{k=0}^{n-1} (z - \varepsilon_n^k).$$

Ejercicio sobre un producto de distancias entre los vértices del polígono regular

Calcule el producto

$$\prod_{k=1}^{n-1} |\overrightarrow{A_0A_k}|.$$



Regla de simplificación para ε_{mq}^{mp}

Para cualesquiera p en $\mathbb{N}$, q en $\mathbb{Z}$, m en $\mathbb{N}$,

$$\varepsilon_{mq}^{mp} = \exp\left(\frac{2\pi\,\mathrm{i}\;mp}{mq}\right) = \exp\left(\frac{2\pi\,\mathrm{i}\,p}{q}\right) = \varepsilon_q^p.$$

Por ejemplo,

$$\varepsilon_8^2 = \varepsilon_4, \qquad \varepsilon_{16}^{12} = \varepsilon_4^3.$$

Plan

$$(z-1)\sum_{k=0}^{4} z^k$$

$$(z-1)\sum_{k=0}^{4} z^k =$$

$$(z-1)\sum_{k=0}^{4} z^k = (-1+z)(1+z+z^2+z^3+z^4)$$

$$(z-1)\sum_{k=0}^{4} z^k = (-1+z)(1+z+z^2+z^3+z^4)$$

$$=$$

$$(z-1)\sum_{k=0}^{4} z^k = (-1+z)(1+z+z^2+z^3+z^4)$$

$$= -1-z-z^2-z^3-z^4$$

$$(z-1)\sum_{k=0}^{4} z^k = (-1+z)(1+z+z^2+z^3+z^4)$$

$$\begin{aligned} &= -1-z-z^2-z^3-z^4 \\ &\quad +z+z^2+z^3+z^4+z^5 \end{aligned}$$

$$
\begin{aligned}
(z-1)\sum_{k=0}^{4} z^k &= (-1+z)\left(1+z+z^2+z^3+z^4\right) \\
&= -1-z-z^2-z^3-z^4 \\
&\qquad +z+z^2+z^3+z^4+z^5 \\
&= z^5-1.
\end{aligned}
$$

$$
\begin{aligned}
(z-1)\sum_{k=0}^{4} z^k &= (-1+z)(1+z+z^2+z^3+z^4) \\
&= -1-z-z^2-z^3-z^4 \\
&\qquad +z+z^2+z^3+z^4+z^5 \\
&= z^5-1.
\end{aligned}
$$

$$
(z-1)\sum_{k=0}^{n-1} z^k = z^n - 1.
$$

La suma de la progresión geométrica finita

$$(z-1)\sum_{k=0}^{n-1} z^k = z^n - 1.$$

Teorema

Sean $n \in \mathbb{N}$, $z \in \mathbb{C}$. Entonces,

$$\sum_{k=0}^{n-1} z^k$$

La suma de la progresión geométrica finita

$$(z-1)\sum_{k=0}^{n-1} z^k = z^n - 1.$$

Teorema

Sean $n \in \mathbb{N}$, $z \in \mathbb{C}$. Entonces,

$$\sum_{k=0}^{n-1} z^k =$$

La suma de la progresión geométrica finita

$$(z-1)\sum_{k=0}^{n-1} z^k = z^n - 1.$$

Teorema

Sean $n \in \mathbb{N}$, $z \in \mathbb{C}$. Entonces,

$$\sum_{k=0}^{n-1} z^k = \begin{cases} \dfrac{z^n - 1}{z - 1}, & z \neq 1; \\ n, & z = 1. \end{cases}$$

Plan

Sumas de potencias de las raíces de la unidad

Teorema

Sean $n \in \mathbb{N}$, $m \in \mathbb{Z}$. Entonces,

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \begin{cases} n, & m \in n\mathbb{Z}; \\ 0, & m \notin n\mathbb{Z}. \end{cases}$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m =$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk}$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} =$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \sum_{k=0}^{n-1} (\varepsilon_n^m)^k$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \sum_{k=0}^{n-1} (\varepsilon_n^m)^k =$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \sum_{k=0}^{n-1} (\varepsilon_n^m)^k = \sum_{k=0}^{n-1} 1$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \sum_{k=0}^{n-1} (\varepsilon_n^m)^k = \sum_{k=0}^{n-1} 1 =$$

Demostración, caso $m \in n\mathbb{Z}$

Si $m \in n\mathbb{Z}$, entonces

$$\varepsilon_n^m = 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \sum_{k=0}^{n-1} (\varepsilon_n^m)^k = \sum_{k=0}^{n-1} 1 = n.$$

Demostración, caso $m \notin n\mathbb{Z}$

Supongamos que $m \notin n\mathbb{Z}$. Entonces,

$$\varepsilon_n^m$$

Demostración, caso $m \notin n\mathbb{Z}$

Supongamos que $m \notin n\mathbb{Z}$. Entonces,

$$\varepsilon_n^m \neq$$

Demostración, caso $m \notin n\mathbb{Z}$

Supongamos que $m \notin n\mathbb{Z}$. Entonces,

$$\varepsilon_n^m \neq 1.$$

Demostración, caso $m \notin n\mathbb{Z}$

Supongamos que $m \notin n\mathbb{Z}$. Entonces,

$$\varepsilon_n^m \neq 1.$$

Luego

$$\sum_{k=0}^{n-1} \varepsilon_n^{mk} = \sum_{k=0}^{n-1} (\varepsilon_n^m)^k = \frac{\varepsilon_n^{mn} - 1}{\varepsilon_n^m - 1} = 0.$$

Otra forma de demostración, caso $m \notin n\mathbb{Z}$

(Gracias a Eliseo Sarmiento Rosales por mostrarme este razonamiento.)

Recordemos la descomposición del polinomio $P(z) = z^n - 1$:

$$\underbrace{z^n - 1}_{P(z)} = (z-1)\ \underbrace{(z^{n-1} + \cdots + z + 1)}_{Q(z)}.$$

Para $z = \varepsilon_n^m$, tenemos $P(z) = 0$, pero $z - 1 \neq 0$.

Luego $Q(z) = 0$.

Ejercicio: demostrar que la matriz de Fourier es unitaria

Sea $n \in \mathbb{N}$, $n \geq 2$.

Definimos

$$F_n := \frac{1}{\sqrt{n}} \left[\varepsilon_n^{jk} \right]_{j,k=0}^{n-1}.$$

Demostrar que

$$F_n^\dagger F_n = I_n.$$