Transformada rápida de Fourier

Parte I

Segundo semestre 2022

IIC2283

Prof. Nicolás Van Sint Jan

Outline

Multiplicación de polinomios

Transformada discreta de Fourier

Outline

Representación de un polinomio

Sea $p(x)$ un **polinomio no nulo de coeficientes racionales**.

La **representación canónica** de $p(x)$ es:

$$p(x) \quad = \quad \sum_{i=0}^{n-1} a_i x^i$$

donde $n \geq 1$, $a_{n-1} \neq 0$ y el grado de $p(x)$ es $n-1$.

- Utilizamos el grado $n-1$ para dar énfasis a que estos polinomios poseen n coeficientes.
- Si bien trabajaremos con polinomios de coeficientes racionales, vamos a evaluarlos usando números reales y complejos.

Representamos $p(x)$ a través de una **tupla** $(a_0, \ldots, a_{n-1})$ **de largo** n.

- También podemos representar $p(x)$ como una tupla $(a_0, \ldots, a_{n-1}, 0, \ldots, 0)$ de largo $m > n$ donde cada término x^i tiene coeficiente 0 si $i \geq n$.

Suma de polinomios

La **suma** de dos polinomios $(a_0, \ldots, a_{n-1})$ y $(b_0, \ldots, b_{n-1})$ es un polinomio $(c_0, \ldots, c_{n-1})$ tal que:

$$c_i \quad = \quad a_i + b_i \qquad \text{para } i \in \{0, \ldots, n-1\}$$

Consideramos a **la suma y multiplicación de números en** $\mathbb{C}$ como las operaciones básicas a contar.

¿ Cuál es la **complejidad** de este algoritmo ?

R: $O(n)$

Multiplicación de polinomios

La **multiplicación** de dos polinomios $(a_0, \ldots, a_{n-1})$ y $(b_0, \ldots, b_{n-1})$ es un polinomio $(c_0, \ldots, c_{2n-2})$ tal que:

$$c_i = \sum_{k,\ell \in \{0,\ldots,n-1\} \,:\, k+\ell=i} a_k \cdot b_\ell \qquad \text{para } i \in \{0, \ldots, 2n-2\}$$

¿ Cuál es la **complejidad** de realizar esta operación ?

R: $O(n^2)$

¿ Podemos realizar esta operación en un **orden menor** ?

Una representación alternativa de un polinomio

Un polinomio $p(x)$ de grado $n-1$ se puede representar de manera única a través de **un conjunto de n pares de puntos-valores**:

$$p(x) \;\mapsto\; \{(v_0, p(v_0)), (v_1, p(v_1)), \ldots, (v_{n-1}, p(v_{n-1}))\},$$

suponiendo que $v_i \neq v_j$ para $i \neq j$.

Ejemplo

El polinomio $p(x) = 1 + x + x^2$ es representado de manera única a través del conjunto de pares de puntos-valores:

$$\{(0,1), (1,3), (2,7)\}$$

y también a través del conjunto de pares de puntos-valores:

$$\{(-2,3), (0,1), (5,31)\}$$

¿ Por qué esto es cierto ?

R: Investigar matriz de Vandermonde

Una representación alternativa de un polinomio

Un polinomio $p(x)$ de grado $n-1$ también se puede representar de manera única a través de un conjunto de pares de puntos-valores con $m > n$ elementos:

$$p(x) \mapsto \{(v_0, p(v_0)), \ldots, (v_{n-1}, p(v_{n-1})), (v_n, p(v_n)), \ldots, (v_{m-1}, p(v_{m-1}))\},$$

suponiendo que $v_i \neq v_j$ para $i \neq j$.

Ejemplo

El polinomio $p(x) = 1 + 2x$ es representado de manera única a través del conjunto de pares de puntos-valores:

$$\{(0, 1), (1, 3), (2, 5)\}$$

y también a través del conjunto de pares de puntos-valores:

$$\{(-2, -3), (0, 1), (5, 11), (7, 15)\}$$

¿Por qué es útil la representación basada en puntos-valores?

Sean $p(x)$ y $q(x)$ dos polinomios de grado $n-1$ representados por

$$p(x) \mapsto \{(v_0, p(v_0)), \ldots, (v_{n-1}, p(v_{n-1}))\}$$
$$q(x) \mapsto \{(v_0, q(v_0)), \ldots, (v_{n-1}, q(v_{n-1}))\}.$$

¿ Cuál será la **representación** de $r(x) = p(x) + q(x)$?

R: $r(x) \mapsto \{(v_0, p(v_0) + q(v_0)), \ldots, (v_{n-1}, p(v_{n-1}) + q(v_{n-1}))\}$

¿ Cómo lo hacemos para $s(x) = p(x) \cdot q(x)$?

¿Por qué es útil la representación basada en puntos-valores?

Suponga que se agrega n puntos a las representaciones de $p(x)$ y $q(x)$:

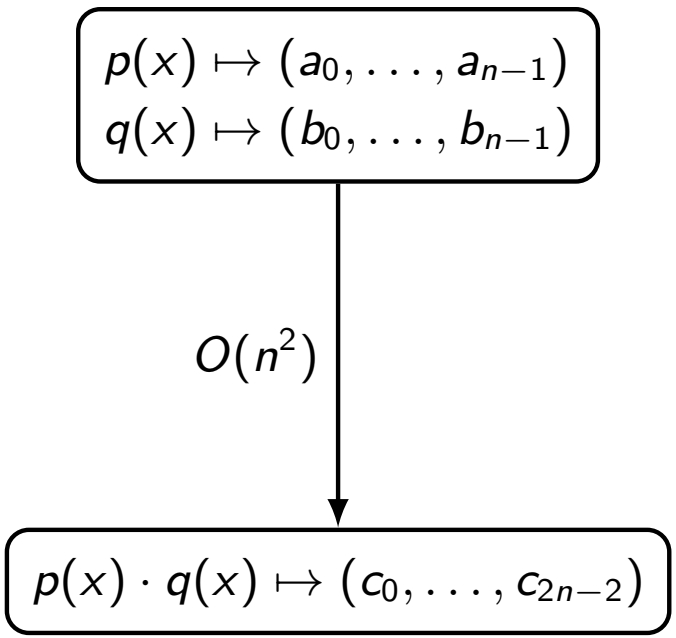
$$\{(v_0, p(v_0)), \ldots, (v_{n-1}, p(v_{n-1})), (v_n, p(v_n)), \ldots, (v_{2n-1}, p(v_{2n-1}))\}$$
$$\{(v_0, q(v_0)), \ldots, (v_{n-1}, q(v_{n-1})), (v_n, q(v_n)), \ldots, (v_{2n-1}, q(v_{2n-1}))\}$$

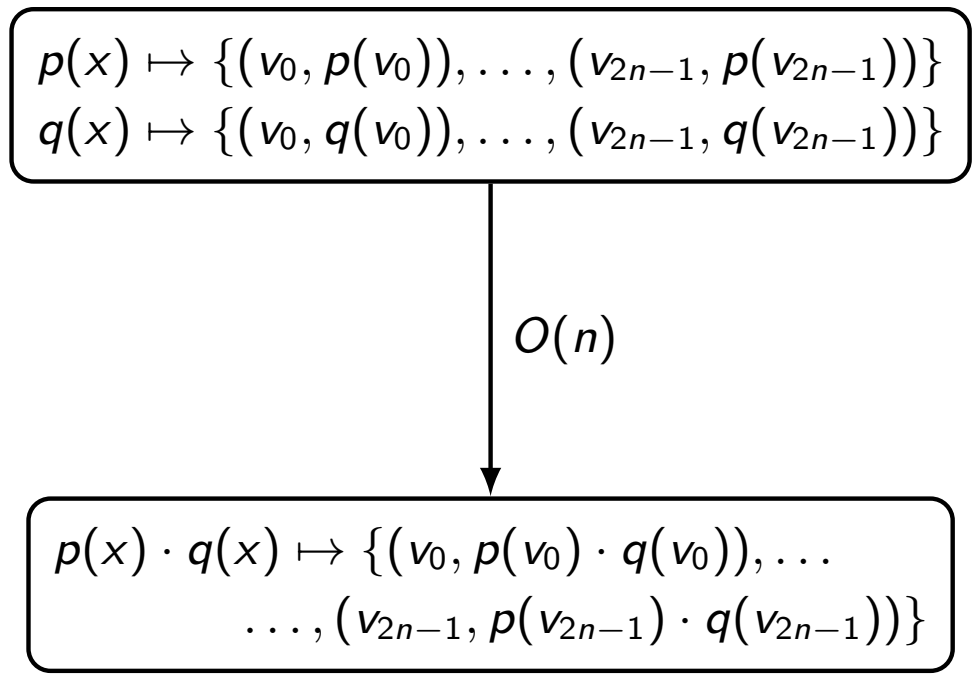
El polinomio $s(x) = p(x) \cdot q(x)$ es representado por:

$$\{(v_0, p(v_0) \cdot q(v_0)), \ldots, (v_{2n-1}, p(v_{2n-1}) \cdot q(v_{2n-1}))\}$$

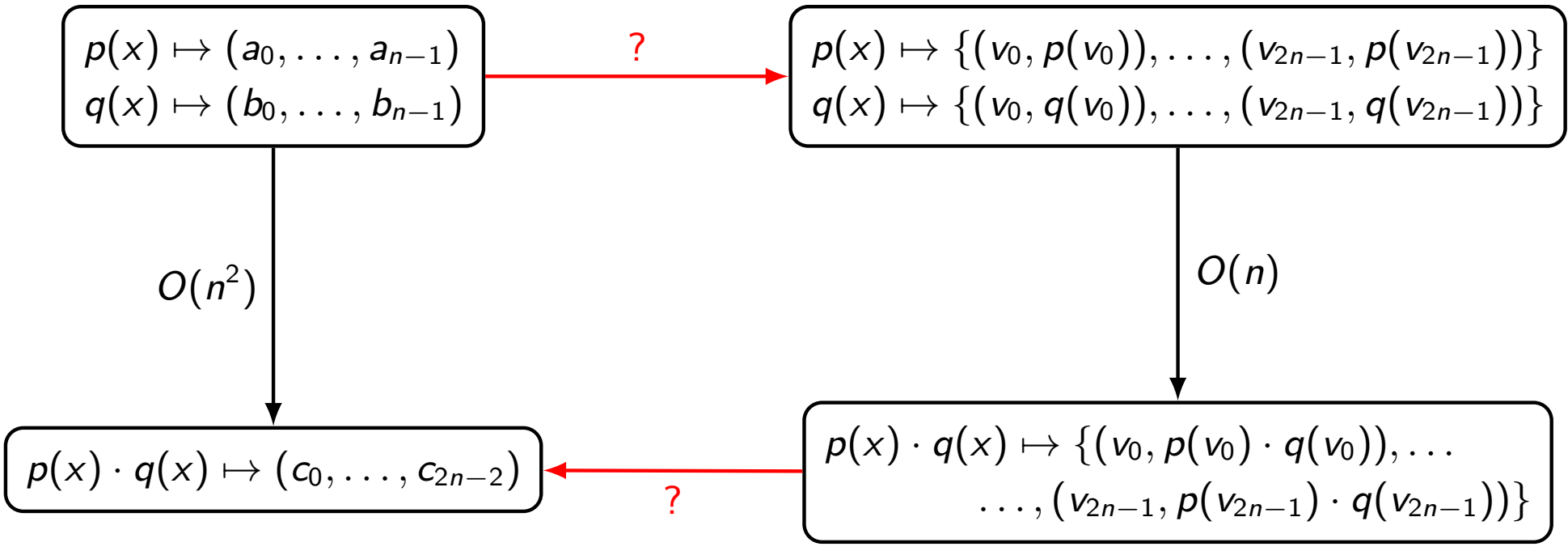
Podemos **sumar y multiplicar polinomios en tiempo** $O(n)$ si están representados por pares de puntos-valores (y por los mismos puntos).

La situación hasta ahora





La situación hasta ahora



De la representación canónica a la de puntos-valores

Ejercicio

Dado un polinomio $p(x)$ de grado n en su representación canónica y un punto v, de un algoritmo que calcule $p(v)$ en tiempo $O(n)$

- Podemos entonces pasar de la representación canónica a la de puntos-valores en tiempo $O(n^2)$.

¿ Cómo podemos pasar de la representación de puntos-valores a la **representación canónica** ?

De la representación puntos-valores a la canónica

Sea $p(x)$ un polinomio de grado $n-1$ dado por una representación punto-valores:

$$\{(v_0, p(v_0)), \ldots, (v_{n-1}, p(v_{n-1})), (v_n, p(v_n)), \ldots, (v_{m-1}, p(v_{m-1}))\},$$

donde $m \geq n$.

Podemos pasar a la representación canónica de $p(x)$ utilizando **fórmula de Lagrange**:

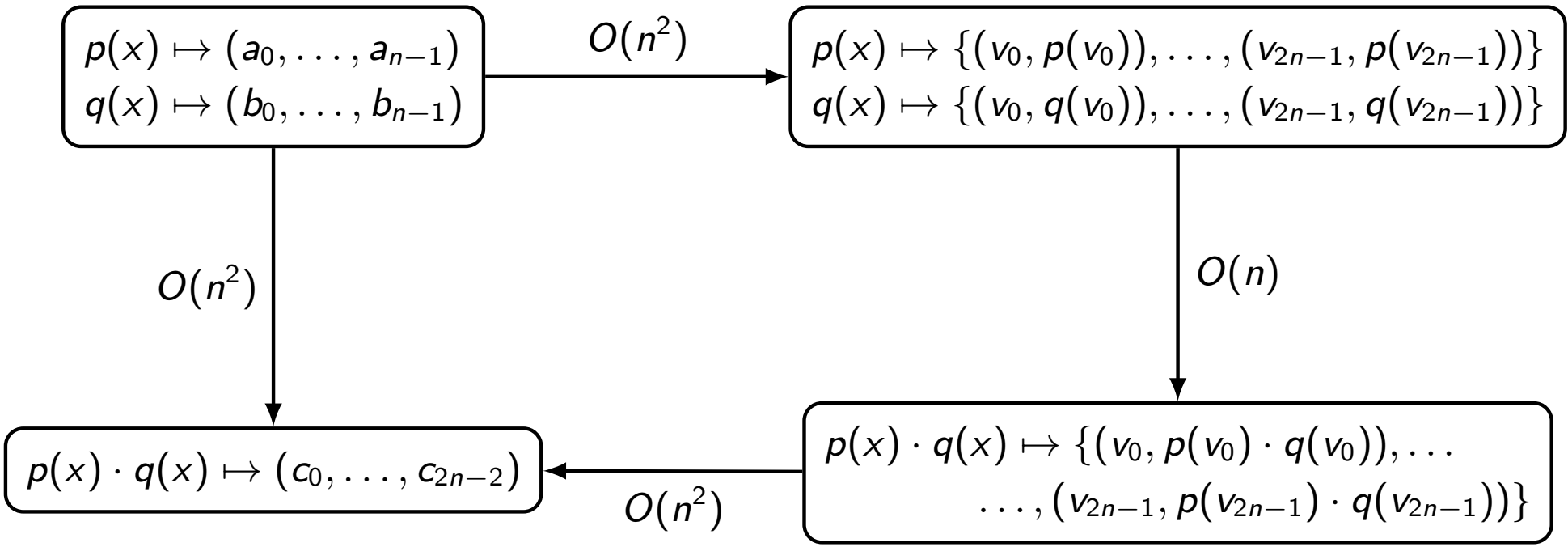
$$p(x) = \sum_{i=0}^{m-1} p(v_i) \cdot \left(\prod_{j \in \{0,\ldots,m-1\} : j \neq i} \frac{(x - v_j)}{(v_i - v_j)} \right)$$

De la representación puntos-valores a la canónica

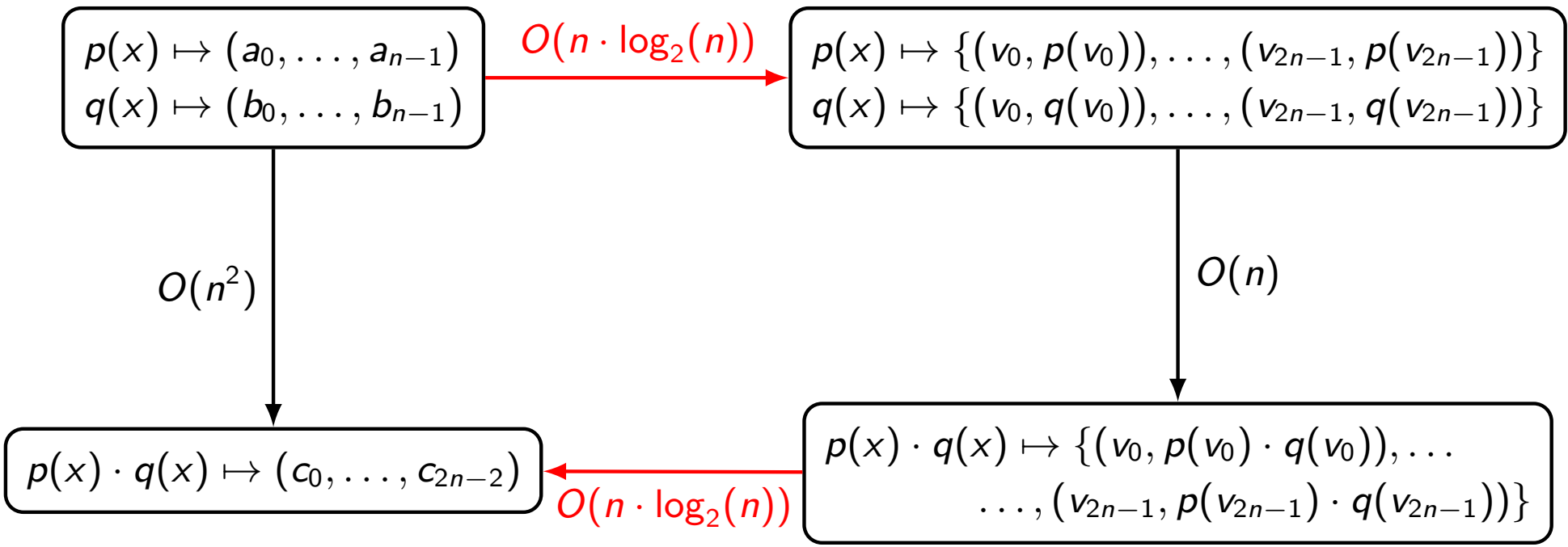
Ejercicio

Dado un polinomio $p(x)$ representando por el conjunto de punto-valores $\{(v_0, p(v_0)), \ldots, (v_{2n-1}, p(v_{2n-1}))\}$, muestre que la fórmula de Lagrange permite construir la forma canónica de $p(x)$ en tiempo $O(n^2)$

Todavía no tenemos un algoritmo más rápido para multiplicar polinomios



La solución: la transformada rápida de Fourier



Outline

La solución: la transformada rápida de Fourier

La **transformada rápida de Fourier** nos va a permitir entonces calcular la multiplicación de dos polinomios de grado $n-1$ en tiempo $O(n \cdot \log_2(n))$

- La idea clave es cómo elegir los puntos $v_0, \ldots, v_{2n-1}$ cuando se calcula la representación como punto-valores de un polinomio de grado $n-1$

Los **números complejos** y las **raíces de la unidad** juegan un papel fundamental en la definición de la transformada rápida de Fourier.

La fórmula de Euler

Teorema

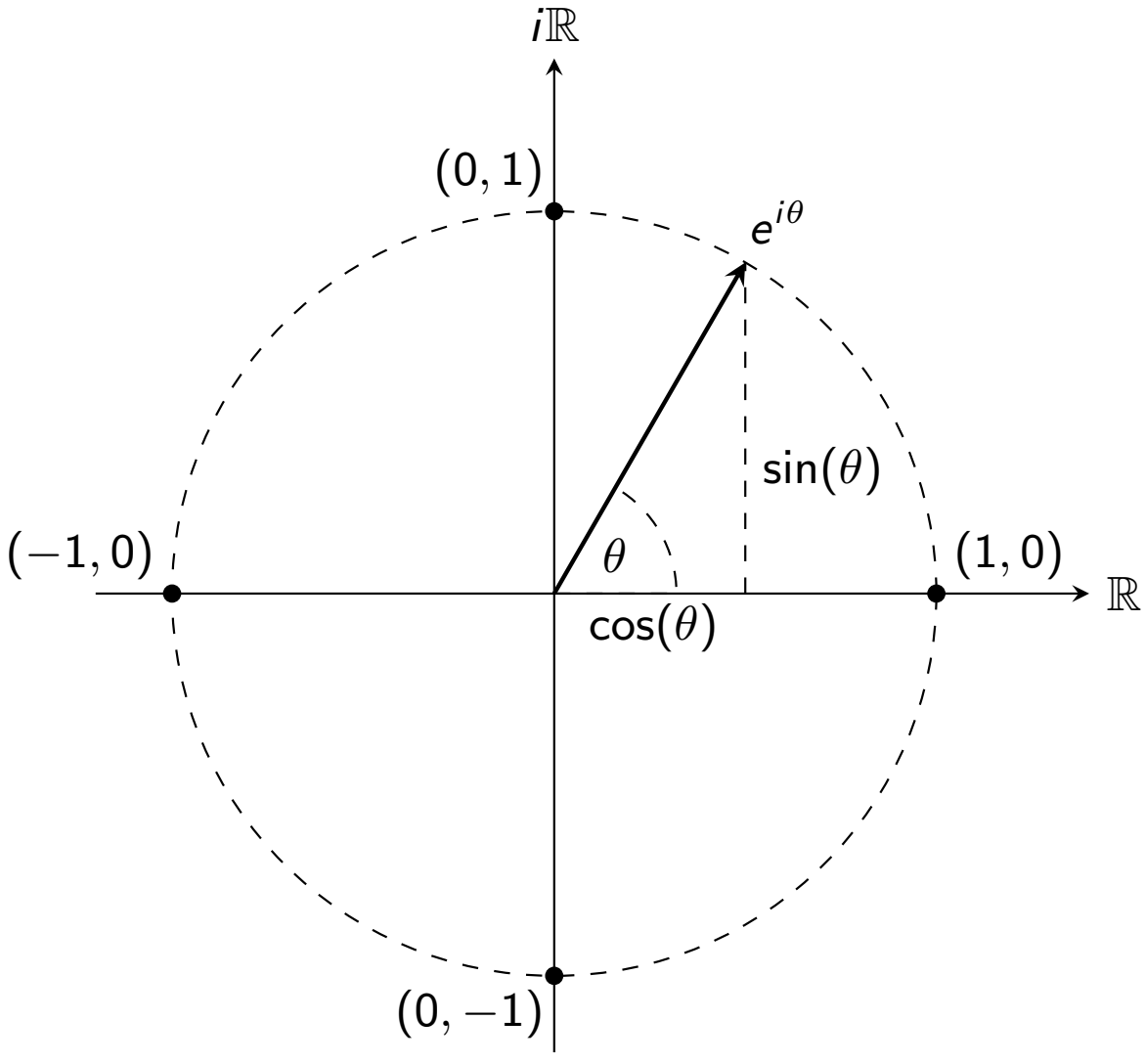
Para todo número real x:

$$e^{ix} = \cos(x) + i\sin(x)$$

Podemos representar entonces a $e^{i\theta}$ como un vector $(\cos(\theta), \sin(\theta))$ en el plano complejo.

- $e^{i\theta}$ es un vector unitario: $||e^{i\theta}|| = \cos^2(\theta) + \sin^2(\theta) = 1$

La fórmula de Euler: interpretación geométrica



La fórmula de Euler: las raíces de la unidad

Dado $n \geq 1$, queremos encontrar las n raíces del polinomio $p(x) = x^n - 1$

- Sabemos que este polinomio tiene n raíces en los números complejos.
- Llamamos a estos elementos las **n-raíces de la unidad**.

El componente básico para definir las n-raíces de la unidad:

$$\omega_n \quad = \quad e^{\frac{2\pi i}{n}}$$

La fórmula de Euler: las raíces de la unidad

Las n-raíces de la unidad son ω_n^0, ω_n^1, ω_n^2, $\ldots$, ω_n^{n-1}

Si $k \in \{0, \ldots, n-1\}$, tenemos que:

$$\begin{aligned}
(\omega_n^k)^n &= ((e^{\frac{2\pi i}{n}})^k)^n \\
&= ((e^{\frac{2\pi i}{n}})^n)^k \\
&= (e^{2\pi i})^k \\
&= (\cos(2\pi) + i\sin(2\pi))^k \\
&= 1^k \\
&= 1
\end{aligned}$$

La fórmula de Euler: las raíces de la unidad

Además, si $0 \leq k \leq \ell \leq n-1$, entonces:

$$
\begin{aligned}
\omega_n^k = \omega_n^\ell \quad &\Rightarrow \quad (e^{\frac{2\pi i}{n}})^k = (e^{\frac{2\pi i}{n}})^\ell \\
&\Rightarrow \quad (e^{\frac{2\pi i}{n}})^{\ell-k} = 1 \\
&\Rightarrow \quad (e^{\frac{2\pi(\ell-k)i}{n}}) = 1 \\
&\Rightarrow \quad \cos\left(\frac{2\pi(\ell-k)}{n}\right) + i\sin\left(\frac{2\pi(\ell-k)}{n}\right) = 1 \\
&\Rightarrow \quad \cos\left(\frac{2\pi(\ell-k)}{n}\right) = 1 \\
&\Rightarrow \quad \frac{\ell-k}{n} = 0 \qquad\qquad \text{puesto que } 0 \leq \frac{\ell-k}{n} \leq \frac{n-1}{n} \\
&\Rightarrow \quad \ell = k
\end{aligned}
$$

Por lo tanto: $\omega_n^0, \ldots, \omega_n^{n-1}$ son elementos distintos

Raíces de la unidad: ejemplos

Ejemplo

¿Cuáles son las raíces del polinomio $x^4 - 1$?

- Considerando $\omega_4 = e^{\frac{2\pi i}{4}} = e^{\frac{\pi}{2} i}$, tenemos que las 4-raíces de la unidad son:

$$\begin{aligned}
\omega_4^0 &= 1 \\
\omega_4^1 &= e^{\frac{\pi}{2} i} = \cos(\frac{\pi}{2}) + i \sin(\frac{\pi}{2}) = i \\
\omega_4^2 &= (e^{\frac{\pi}{2} i})^2 = e^{\pi i} = \cos(\pi) + i \sin(\pi) = -1 \\
\omega_4^3 &= (e^{\frac{\pi}{2} i})^3 = e^{\frac{3\pi}{2} i} = \cos(\frac{3\pi}{2}) + i \sin(\frac{3\pi}{2}) = -i
\end{aligned}$$

Raíces de la unidad: otro ejemplo

Ejemplo

¿Cuáles son las raíces del polinomio $x^5 - 1$? Considerando $\omega_5 = e^{\frac{2\pi i}{5}}$, tenemos que las 5-raíces de la unidad son 1, $e^{\frac{2\pi i}{5}}$, $e^{\frac{4\pi i}{5}}$, $e^{\frac{6\pi i}{5}}$ y $e^{\frac{8\pi i}{5}}$

Representación geométrica: