Computação Quântica
Aula 13

Murilo V. G. da Silva

DINF/UFPR

Trasformada quântica de Fourier

Assuntos da aula de hoje:

- Propriedades das raízes de $x^n = 1$ (útil nos assuntos abaixo)
- A transformada discreta de Fourier (DFT)
- A transformada quântica de Fourier (QFT)
- Propriedades da DFT/QFT

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$,

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$,

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

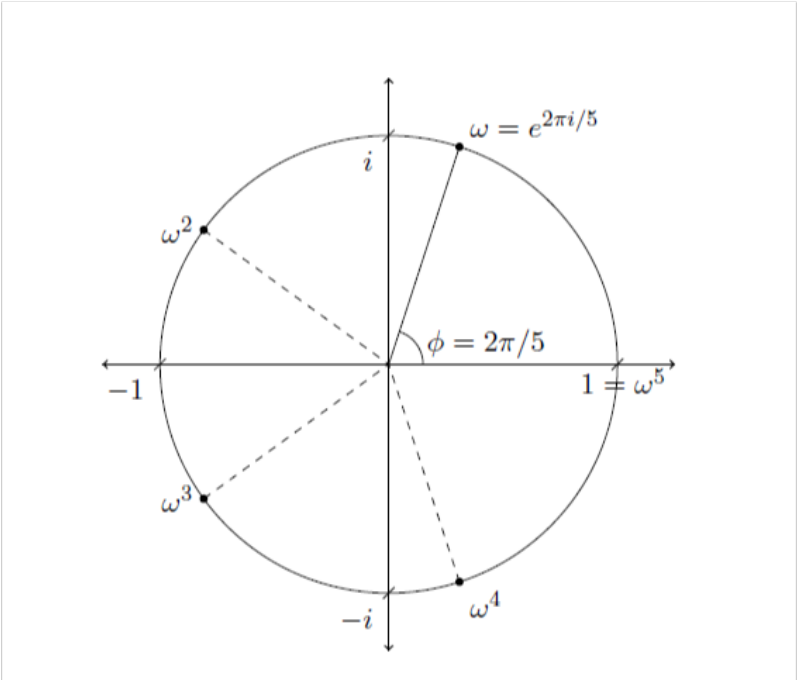
Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:

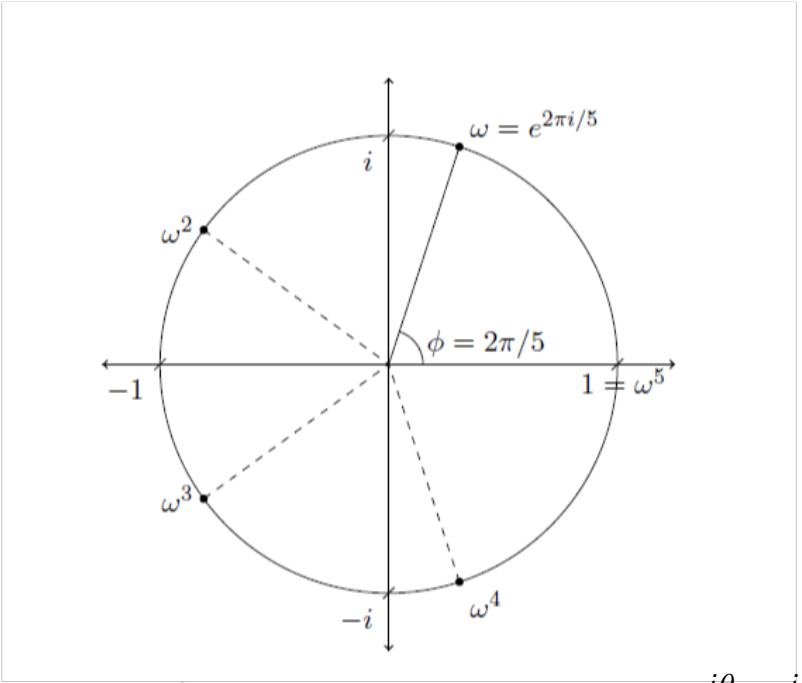


Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:



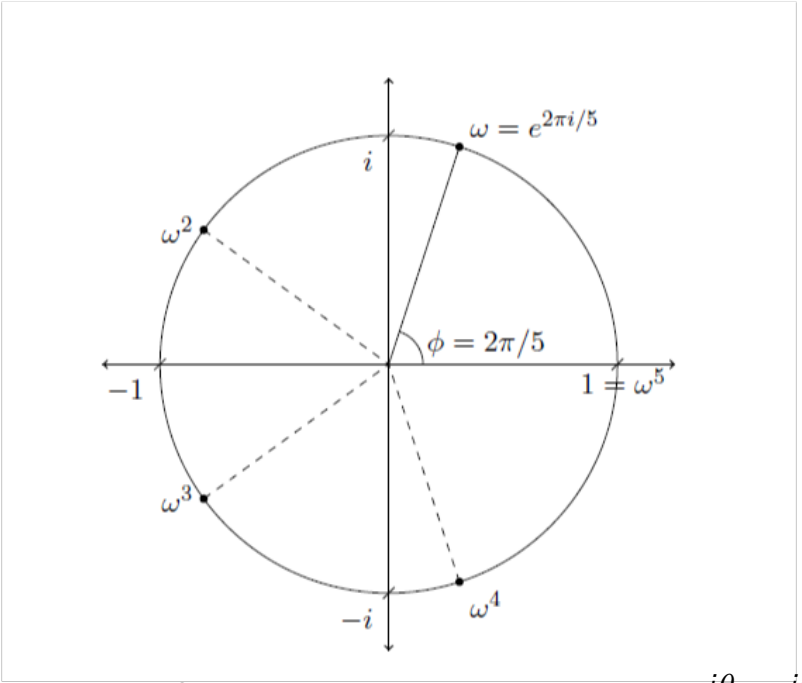
Lembre como multiplicação funciona com números complexos: $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:



Lembre como multiplicação funciona com números complexos: $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$

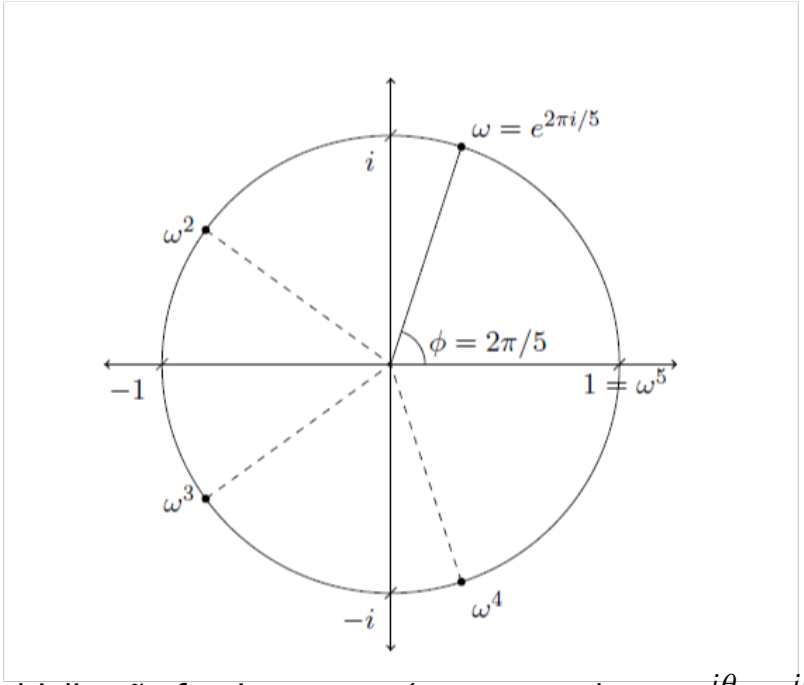
Seja $\omega = e^{2\pi i/5}$.

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:



Lembre como multiplicação funciona com números complexos: $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$

Seja $\omega = e^{2\pi i/5}$.

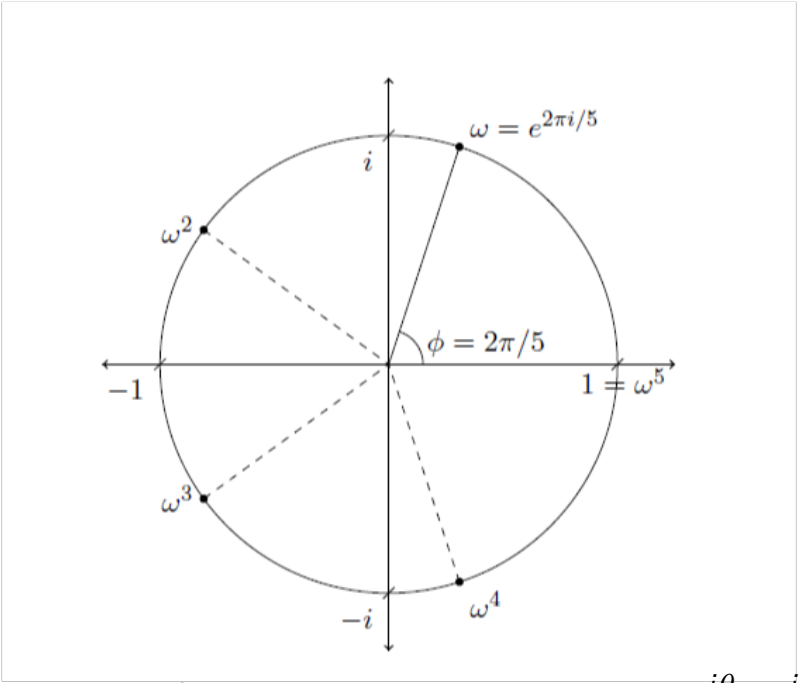
- Note que ao multiplicarmos ω consigo mesmo 5 vezes vamos somando o ângulo $2\pi/5$ até que o ângulo chegue a 2π, ou seja, o vetor chegue até 1.

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:



Lembre como multiplicação funciona com números complexos: $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$

Seja $\omega = e^{2\pi i/5}$.

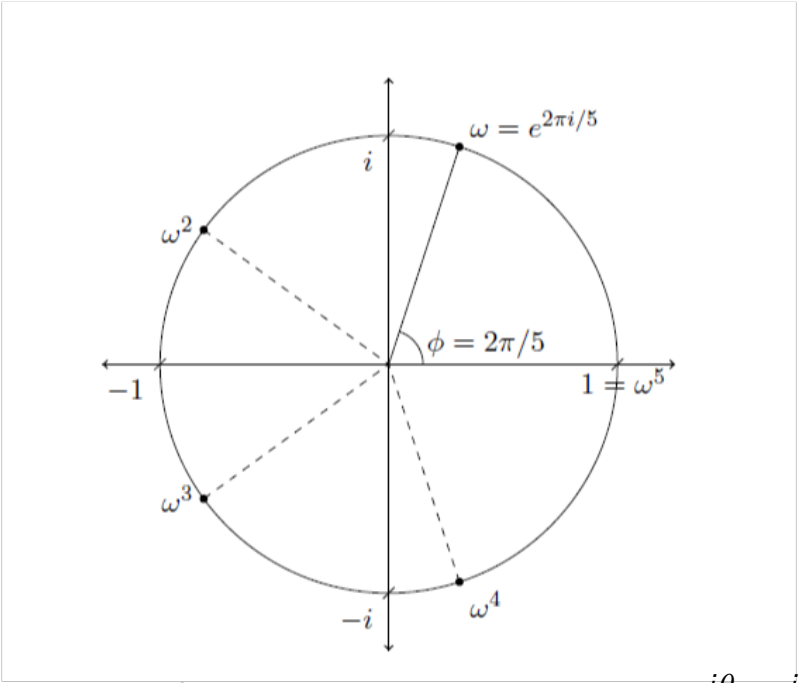
- Note que ao multiplicarmos ω consigo mesmo 5 vezes vamos somando o ângulo $2\pi/5$ até que o ângulo chegue a 2π, ou seja, o vetor chegue até 1.
- Note ao elevarmos ω^2 a quinta potência o vetor (depois de "duas voltas no círculo") também chega a 1.

Preliminares: A n-ésima raiz da unidade

Exemplo: Para $n = 5$, quais as raízes de $x^5 = 1$?

- Uma raíz é $x = 1$, pois $(1)^5 = 1$
- Outra raíz é $x = e^{2\pi i/5}$, pois $(e^{2\pi i/5})^5 = (e^{\pi i})^2 = (-1)^2 = 1$

Antes de procurar outras raízes vamos entender por que $e^{2\pi i/5}$ é uma raíz:



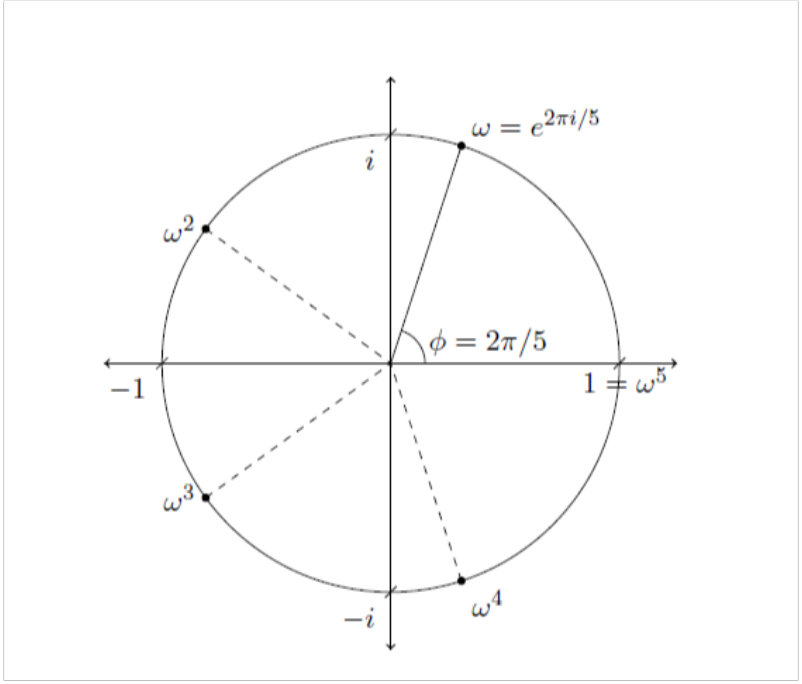
Lembre como multiplicação funciona com números complexos: $e^{i\theta} \cdot e^{i\theta'} = e^{i(\theta+\theta')}$

Seja $\omega = e^{2\pi i/5}$.

- Note que ao multiplicarmos ω consigo mesmo 5 vezes vamos somando o ângulo $2\pi/5$ até que o ângulo chegue a 2π, ou seja, o vetor chegue até 1.
- Note ao elevarmos ω^2 a quinta potência o vetor (depois de "duas voltas no círculo") também chega a 1.
- Pense no que acontece com ω^3 e ω^4 e conclua que as 5 raízes são $1, \omega, \omega^2, \omega^3$ e ω^4.

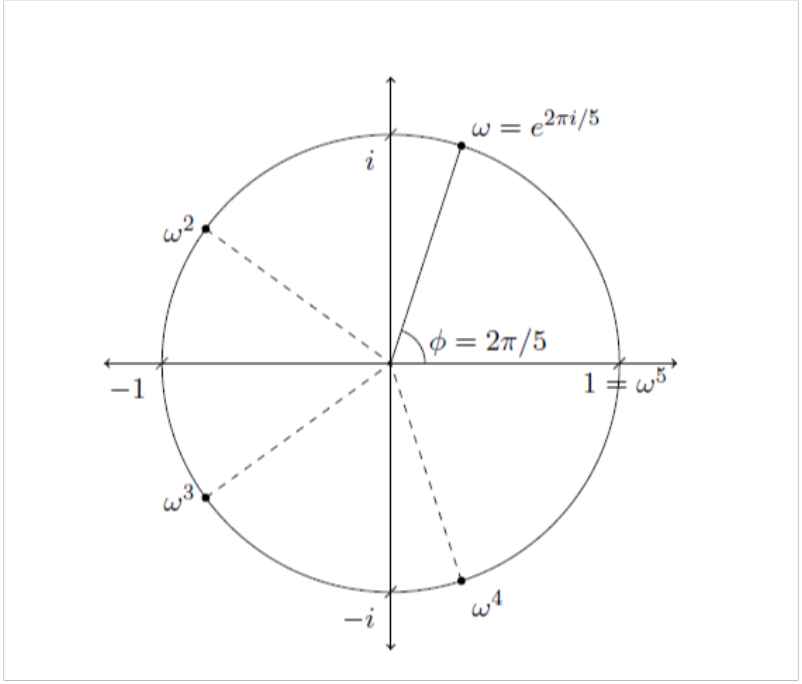
Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:



Preliminares: A n-ésima raiz da unidade

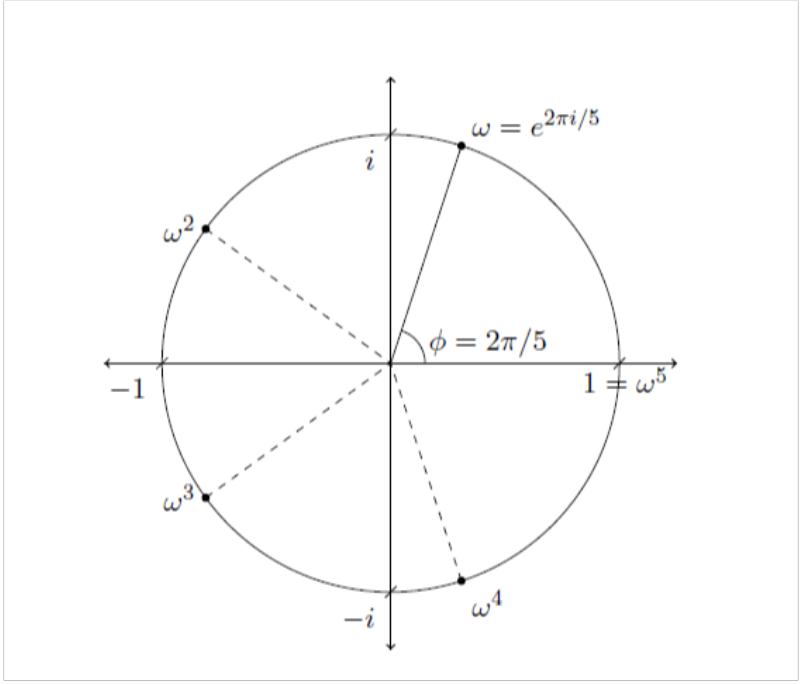
Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:



Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$?

Preliminares: A n-ésima raiz da unidade

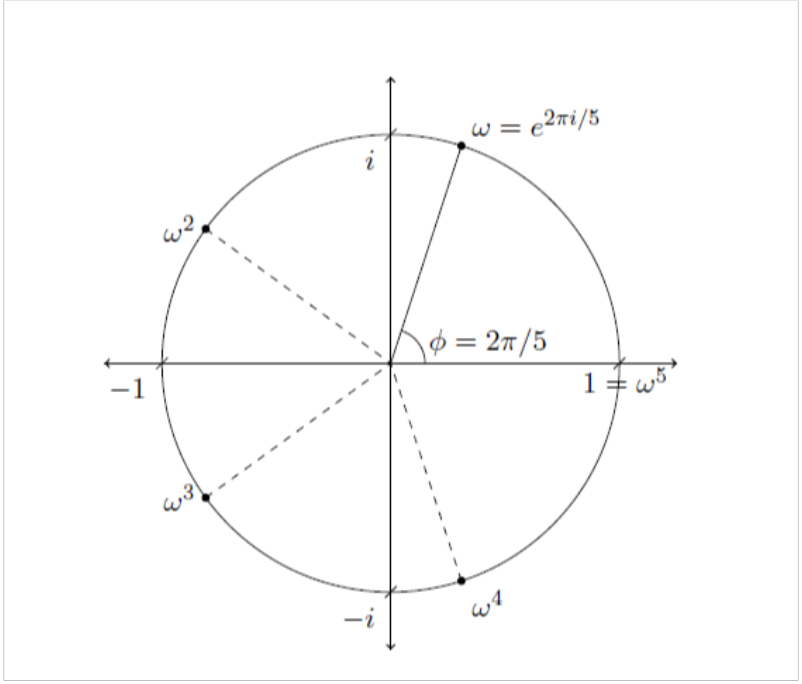
Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:



Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

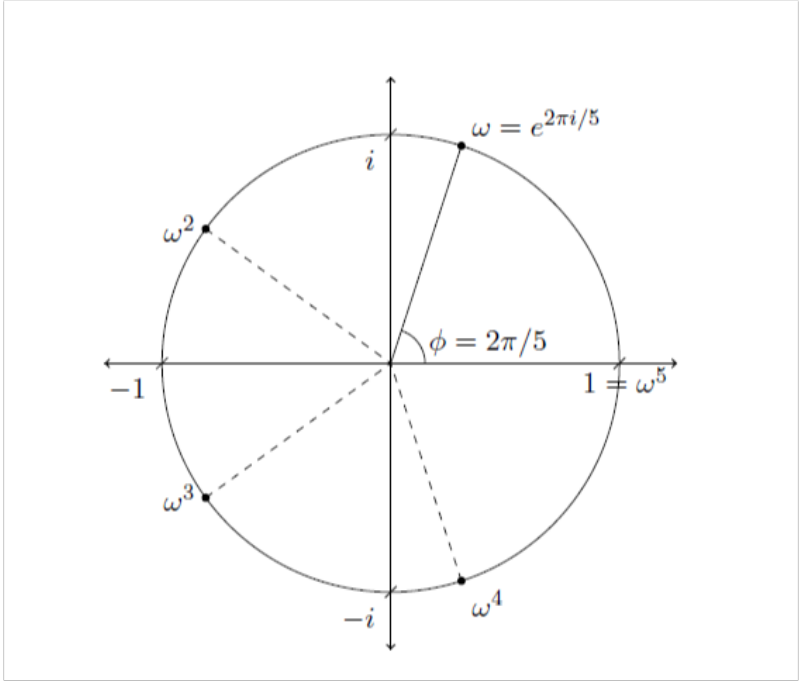


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n?

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

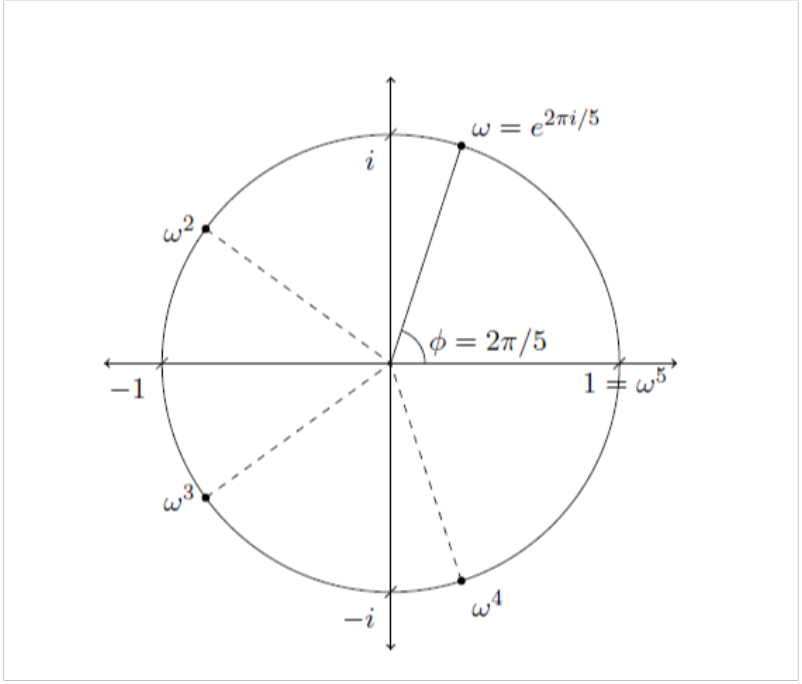


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

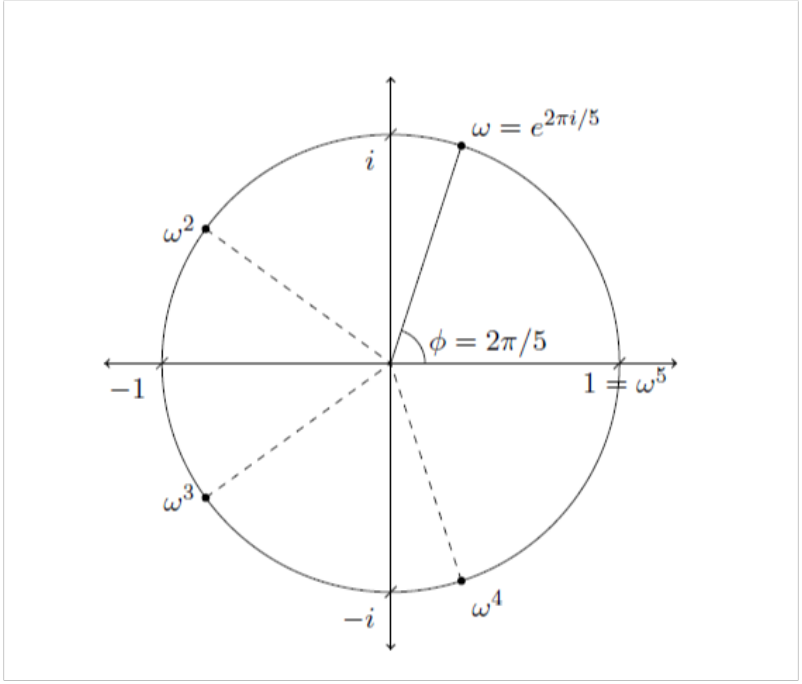


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$?

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

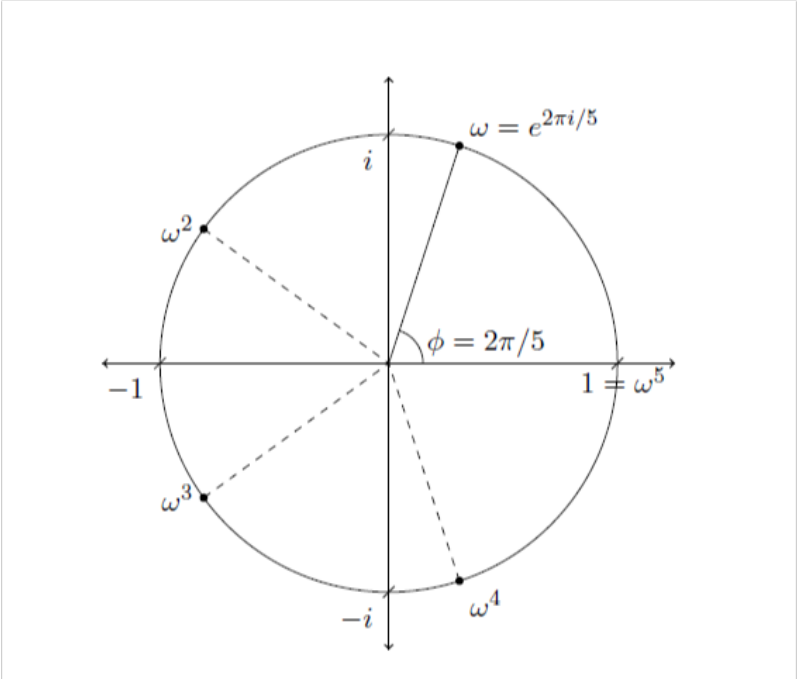


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

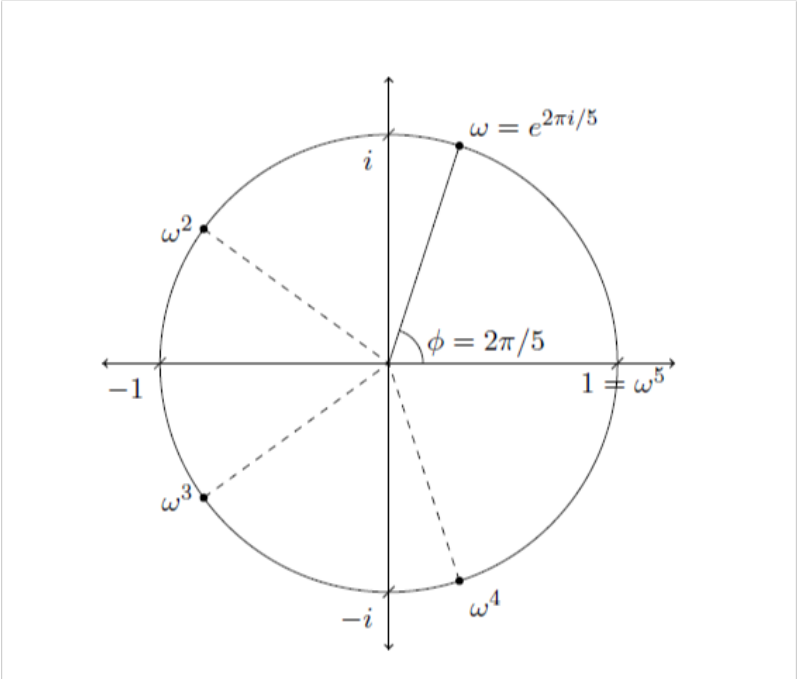


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1
- Pergunta: Para $m > n$, qual o valor de ω^m?

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

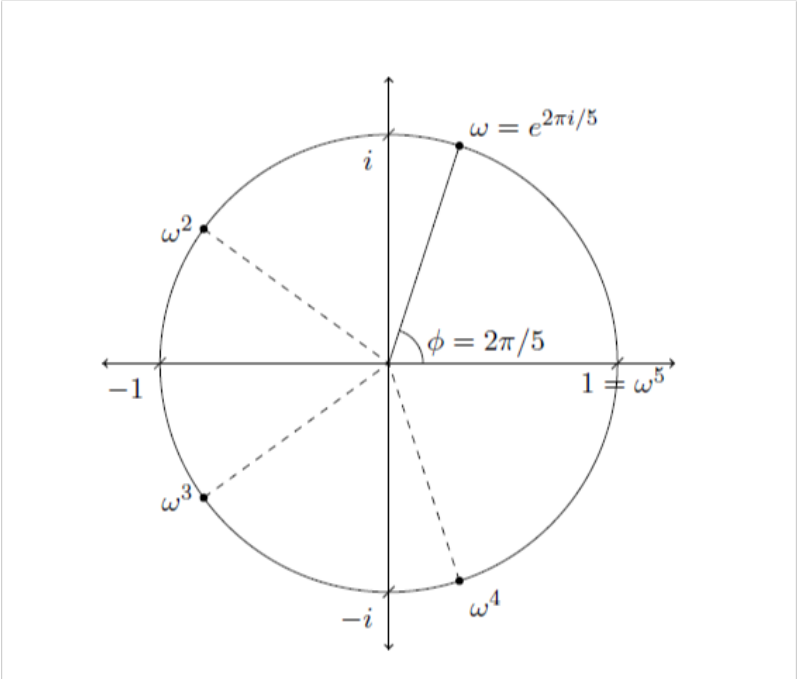


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1
- Pergunta: Para $m > n$, qual o valor de ω^m? Resposta ω^r, tal que $r = m$ (mod n)

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

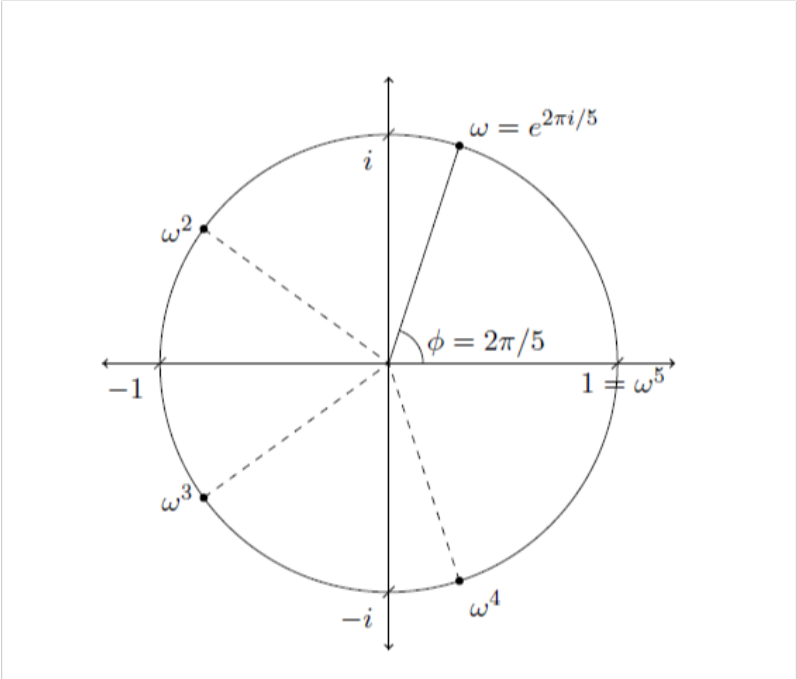


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1
- Pergunta: Para $m > n$, qual o valor de ω^m? Resposta ω^r, tal que $r = m$ (mod n)
- Exercício 1: Calcule $1 + \omega + \omega^2 + \ldots + \omega^{n-1}$

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:

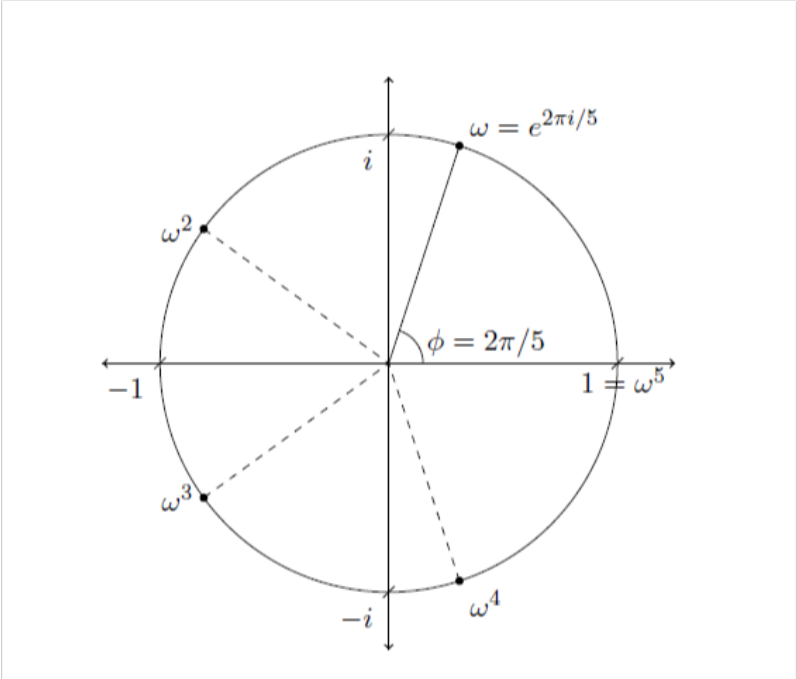


Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1
- Pergunta: Para $m > n$, qual o valor de ω^m? Resposta ω^r, tal que $r = m$ (mod n)
- Exercício 1: Calcule $1 + \omega + \omega^2 + \ldots + \omega^{n-1}$
- Exercício 2: Calcule $1 + \omega^j + \omega^2 j + \ldots + \omega^{n-1} j$

Preliminares: A n-ésima raiz da unidade

Então para $n = 5$, as raízes de $x^5 = 1$ são 1, ω^2, ω^3 e ω^4:



Para n em geral, sendo $\omega = e^{2\pi i/n}$, quais são as raízes de $x^n = 1$? ω^i, $i = 0, \ldots, n-1$

- Pergunta: qual o valor de ω^n? Resposta: 1
- Pergunta: Qual o valor de $(\omega^2)^n$? Resposta: 1
- Pergunta: Para $m > n$, qual o valor de ω^m? Resposta ω^r, tal que $r = m$ (mod n)
- Exercício 1: Calcule $1 + \omega + \omega^2 + \ldots + \omega^{n-1}$
- Exercício 2: Calcule $1 + \omega^j + \omega^2 j + \ldots + \omega^{n-1} j$
- Exercício 3: Calcule $|1|^2 + |\omega^j|^2 + |\omega^{2j}|^2 + \ldots + |\omega^{(n-1)j}|^2$

A transformada discreta de Fourier

Considere a seguinte matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

sendo que $\omega = e^{2\pi i/M}$

A transformada discreta de Fourier

Considere a seguinte matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

sendo que $\omega = e^{2\pi i/M}$

- **Note: posição (j,k) tem o valor ω^{jk}**

A transformada discreta de Fourier

Considere a seguinte matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

sendo que $\omega = e^{2\pi i/M}$

- **Note: posição (j,k) tem o valor ω^{jk}**
- Para $M = 2$, qual a matriz correspondente?

A transformada discreta de Fourier

Considere a seguinte matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

sendo que $\omega = e^{2\pi i/M}$

- **Note: posição (j,k) tem o valor ω^{jk}**
- Para $M = 2$, qual a matriz correspondente? Você conhece essa matriz?

A transformada discreta de Fourier

Considere a seguinte matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

sendo que $\omega = e^{2\pi i/M}$

- **Note: posição (j,k) tem o valor ω^{jk}**
- Para $M = 2$, qual a matriz correspondente? Você conhece essa matriz?
- Calcule agora a matriz para $M = 4$.

A transformada discreta de Fourier

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

A transformada discreta de Fourier

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

- Exercício 4: Calcule a QFT para $M = 8$.

A transformada discreta de Fourier

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

- Exercício 4: Calcule a QFT para $M = 8$.
- Exercício 5: Prove que matriz, para qualquer M, é unitária

A transformada discreta de Fourier

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

- Exercício 4: Calcule a QFT para $M = 8$.
- Exercício 5: Prove que matriz, para qualquer M, é unitária (Dica: Exercícios 1, 2, 3)

A transformada discreta de Fourier

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

- Exercício 4: Calcule a QFT para $M = 8$.
- Exercício 5: Prove que matriz, para qualquer M, é unitária (Dica: Exercícios 1, 2, 3)
- Afirmação: É possível implementar com um número polinomial de portas (provaremos mais adiante isso)

A transformada discreta de Fourier

Voltando a matriz $M \times M$

$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2M-2} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3M-3} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2M-2} & \omega^{3M-3} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Lembrando que $\omega = e^{2\pi i/M}$

- Exercício 4: Calcule a QFT para $M = 8$.
- Exercício 5: Prove que matriz, para qualquer M, é unitária (Dica: Exercícios 1, 2, 3)
- Afirmação: É possível implementar com um número polinomial de portas (provaremos mais adiante isso)

Qual a vantagem e a desvantagem da versão quântica da DFT?