



Nadai



Carlos



## Sesión 3: Las matemáticas detrás de las STARKs

● 4 de Mayo del 2023

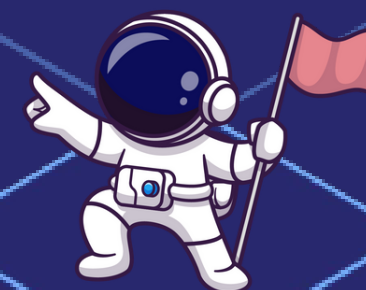
### Stark 101: Parte 4

 @Nadai02010

 <https://github.com/Nadai2010>

 @0xhasher\_

 <https://github.com/cliraa>



# Recapitulemos

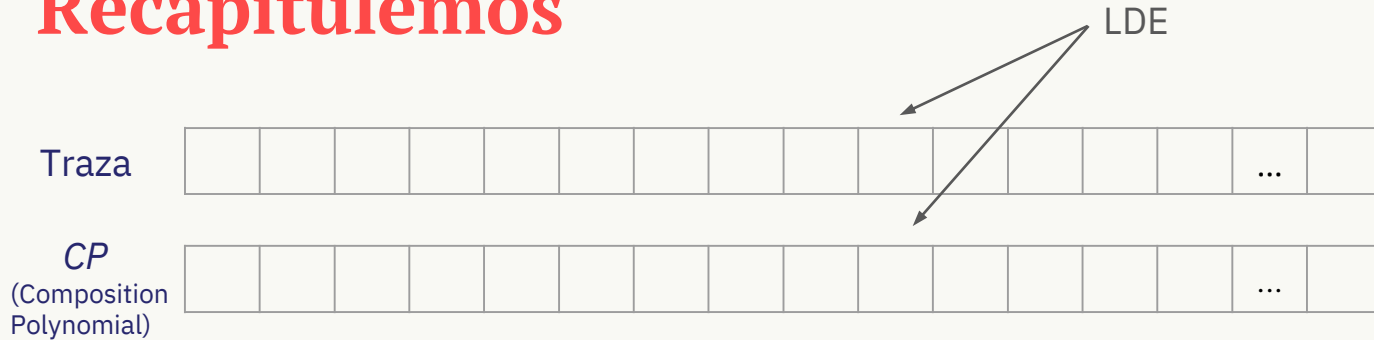
**Compromiso**

Traza



Raíz de la traza

# Recapitulemos



## Compromiso

Raíz de la traza

Raíz  $CP$

# Recapitulemos

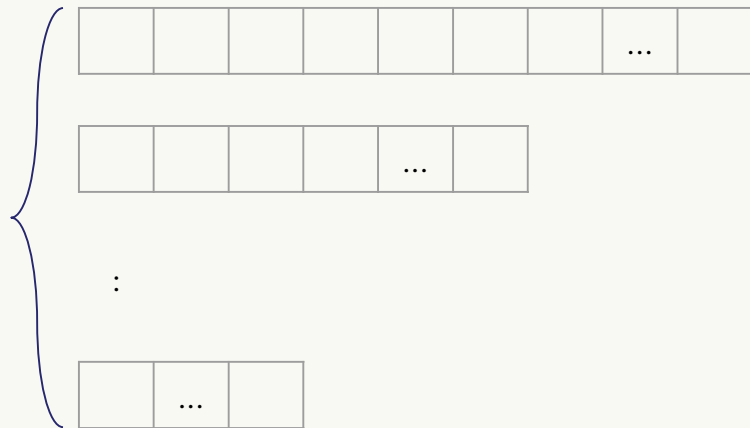
Traza



$CP$   
(Composition  
Polynomial)



FRI



## Compromiso

Raíz de la traza

Raíz  $CP$

Raíz  $CP_1$

Raíz  $CP_2$

:

Raíz  $CP_{10}$

# La Prueba Completa



Compromiso

- Descompromiso (Convenciendo)

# ¿Cómo puede el Probador convencer al Verificador?

Verificador: Envía elementos  $q$  random

Probador: Proporciona un dato de validación para cada uno

## ¿Qué son los datos de validación?

# Traza $\rightarrow$ CP

Traza



CP  
(Composition  
Polynomial)



FRI



## Compromiso

Raíz de la traza

Raíz CP

Raíz  $CP_1$

Raíz  $CP_2$

:

Raíz  $CP_{10}$

# Traza $\rightarrow CP$

## Compromiso

## Traza

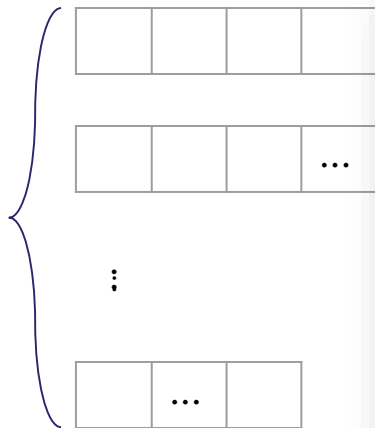


## Raíz de la traza

$CP$   
(Composition  
Polynomial)

Raíz  $CP$ 

FRI



### 3 Funciones Racionales

$$p_0(x) = \frac{f(x) - 1}{x - g^0}$$

$$p_1(x) = \frac{f(x) - 2338775057}{x - q^{1022}}$$

$$p_2(x) = \frac{f(g^2x) - f(gx)^2 - f(x)^2}{(x^{1024} - 1) / [(x - g^{1021})(x - g^{1022})(x - g^{1023})]}$$

## Combinando los $p_i(x)$ 's

Combinación lineal aleatoria:

$$CP = \alpha_0 \cdot p_0(x) + \alpha_1 \cdot p_1(x) + \alpha_2 \cdot p_2(x)$$

Raíz  $CP_1$ Raíz  $CP_2$ 

:

Raíz  $CP_{10}$



# FRI - Pasos

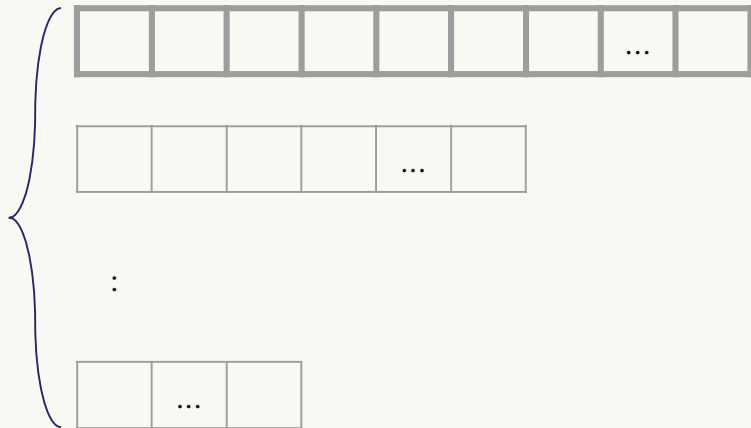
Traza



$CP$   
(Composition  
Polynomial)



FRI



## Compromiso

Raíz de la traza

Raíz  $CP$

Raíz  $CP_1$

Raíz  $CP_2$

:

Raíz  $CP_{10}$

## FRI - Pasos

$$\begin{cases} CP_i(x) = g(x^2) + xh(x^2) \\ CP_i(-x) = g(x^2) - xh(x^2) \end{cases} \longrightarrow \begin{cases} g(x^2) = \frac{CP_i(x) - CP_i(-x)}{2} \\ h(x^2) = \frac{CP_i(x) - CP_i(-x)}{2x} \end{cases}$$

Recuerde:

$$CP_{i+1}(x^2) = g(x^2) + \beta h(x^2)$$

En resumen:

*Para calcular  $CP_{i+1}(x^2)$  sólo necesitamos  $CP_i(x)$  y  $CP_i(-x)$*

# FRI - Pasos

Traza



$CP$   
(Composition  
Polynomial)



FRI



:



## Compromiso

Raíz de la traza

Raíz  $CP$

Raíz  $CP_1$

Raíz  $CP_2$

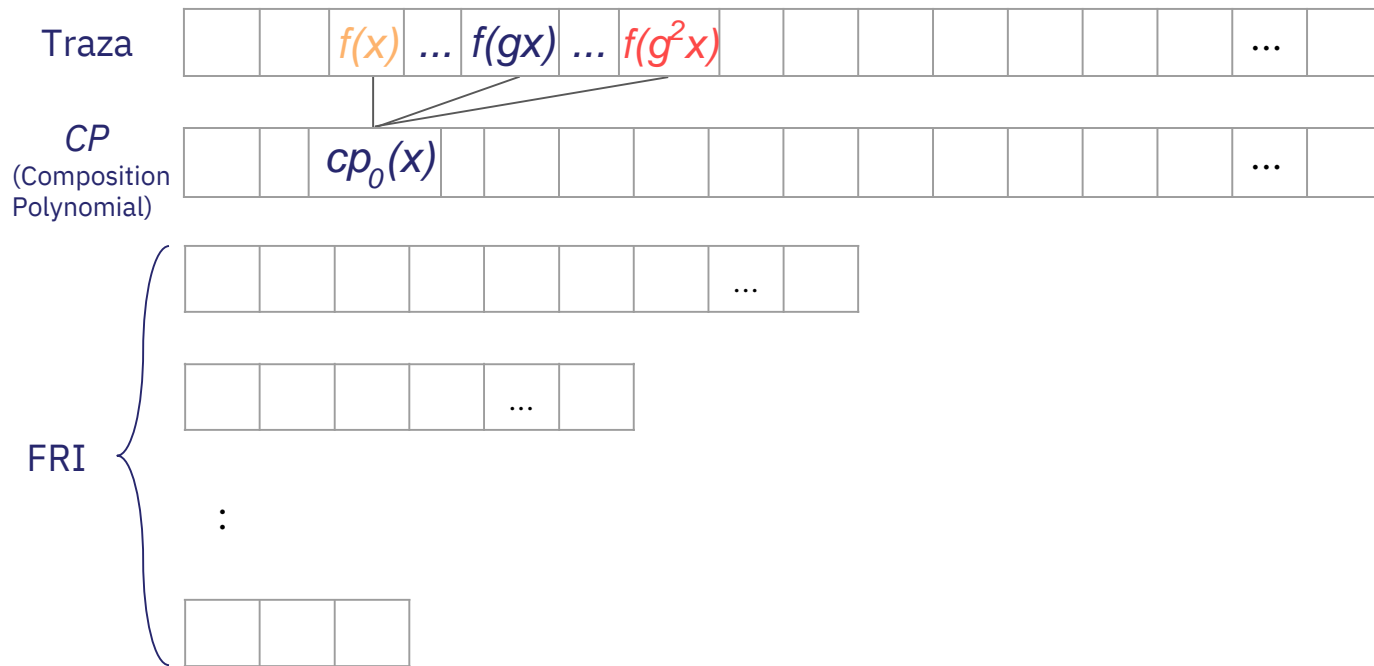
:

Raíz  $CP_{10}$

# Fase de Descompromiso (para la consulta x)

# Fase de Descompromiso (para la consulta x)

## Descompromiso



$f(x)$  + ruta  
 $f(gx)$  + ruta  
 $f(g^2x)$  + ruta  
 $cp_0(x)$  + ruta

# Fase de Descompromiso (para la consulta x)

## Descompromiso

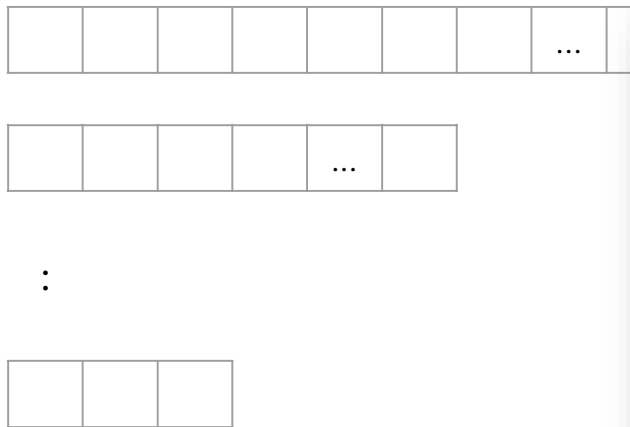
Traza



CP  
(Composition  
Polynomial)

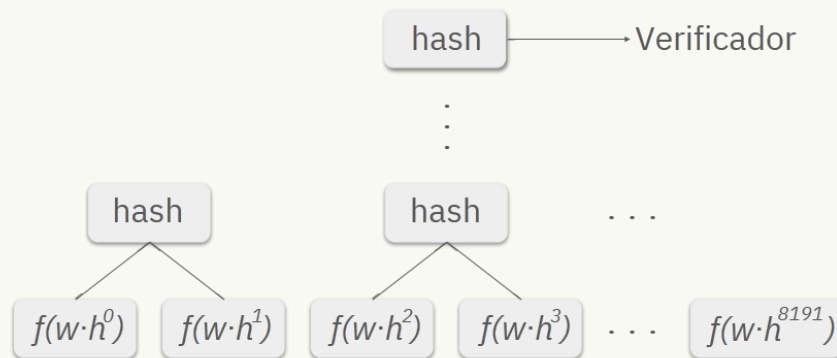


FRI

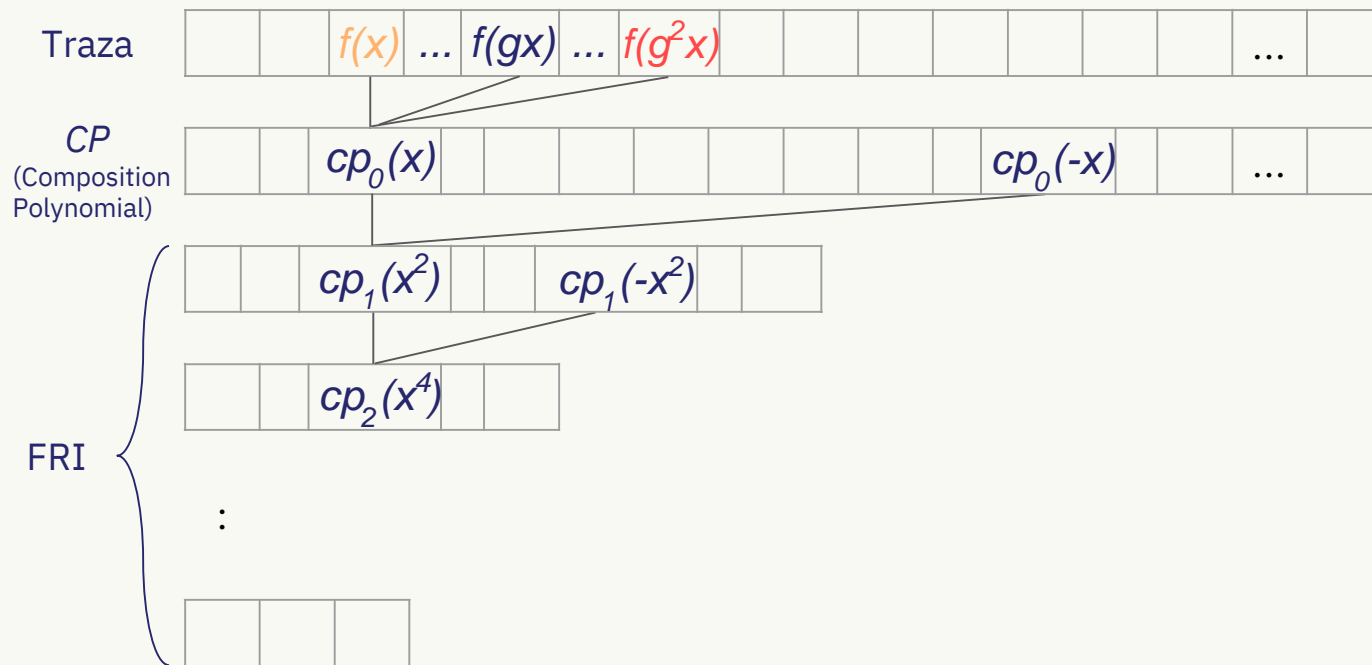


$f(x)$  + ruta  
 $f(gx)$  + ruta  
 $f(g^2x)$  + ruta  
 $cp_0(x)$  + ruta

## Compromiso sobre LDE



# Fase de Descompromiso (para la consulta x)



## Descompromiso

$f(x)$  + ruta  
 $f(gx)$  + ruta  
 $f(g^2x)$  + ruta  
 $cp_0(x)$  + ruta  
 $cp_0(-x)$  + ruta  
 $cp_1(x^2)$  + ruta  
 $cp_1(-x^2)$  + ruta  
 $cp_2(x^4)$  + ruta  
 $cp_2(-x^4)$  + ruta

:

$cp_{10}(x^{1024})$  + ruta

# La Prueba Completa



Compromiso



Descompromiso

- Obtener elementos  $q$  random
- Proporcionar un dato de validación para cada uno



# Longitud de la prueba

## Compromiso

## Descompromiso (para una consulta)

$O(\log(n))$ $n = \text{longitud de traza}$ $(1023)$	Raíz de Traza	$f(x)$	+ ruta
		$f(gx)$	+ ruta
		$f(g^2x)$	+ ruta
	Raíz CP	$cp_0(x)$	+ ruta
		$cp_0(-x)$	+ ruta
	Raíz CP <sub>1</sub>	$cp_1(x^2)$	+ ruta
		$cp_1(-x^2)$	+ ruta
	Raíz CP <sub>2</sub>	$cp_2(x^4)$	+ ruta
		$cp_2(-x^4)$	+ ruta
	:	:	
	Raíz CP <sub>10</sub>	$cp_{10}(x^{1024})$	+ ruta

# Longitud de la prueba

Compromiso		Descompromiso (para una consulta)	
$O(\log(n))$	Raíz de Traza	$f(x)$	+ ruta
		$f(gx)$	+ ruta
		$f(g^2x)$	+ ruta
	Raíz CP	$cp_0(x)$	+ ruta
		$cp_0(-x)$	+ ruta
	Raíz CP <sub>1</sub>	$cp_1(x^2)$	+ ruta
		$cp_1(-x^2)$	+ ruta
	Raíz CP <sub>2</sub>	$cp_2(x^4)$	+ ruta
		$cp_2(-x^4)$	+ ruta
	:	:	
	Raíz CP <sub>10</sub>	$cp_{10}(x^{1024})$	+ ruta

*En Total:*  
 $O(\log^2(n))$

$O(\log(n))$

# Longitud de Prueba

Compromiso		Descompromiso (para $q$ consultas)		
Raíz de Traza	$f(x)$	+ ruta	$f(x)$	+ ruta
	$f(gx)$	+ ruta	$f(gx)$	+ ruta
	$f(g^2x)$	+ ruta	$f(g^2x)$	+ ruta
Raíz $CP$	$cp_0(x)$	+ ruta	$cp_0(x)$	+ ruta
	$cp_0(-x)$	+ ruta	$cp_0(-x)$	+ ruta
Raíz $CP_1$	$cp_1(x^2)$	+ ruta	$cp_1(x^2)$	+ ruta
	$cp_1(-x^2)$	+ ruta	...	$cp_1(-x^2)$ + ruta
Raíz $CP_2$	$cp_2(x^4)$	+ ruta	$cp_2(x^4)$	+ ruta
	$cp_2(-x^4)$	+ ruta	$cp_2(-x^4)$	+ ruta
:	:	:	:	
Raíz $CP_{10}$	$cp_{10}(x^{1024})$	+ ruta	$cp_{10}(x^{1024})$	+ ruta

$O(\log^2(n))$

**Y ahora - Última parte del código.**

**Después de eso...**  
**Se convertirá en un experto en STARK**



**Gracias!**