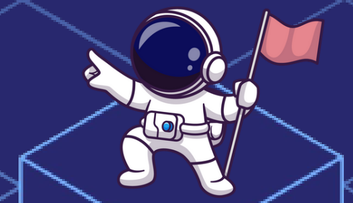
STARKWARE

Nadai Carlos

Sesión 3: Las matemáticas detrás de las STARKs

- 4 de Mayo del 2023

Stark 101: Parte 2



@Nadai02010

https://github.com/Nadai2010

@0xhasher_

https://github.com/cliraa

¿Qué queremos probar?

Hay un número x tal que:

$a_0 = 1$

$a_1 = x$

$a_{1022} = 2338775057$

Utilizaremos la parte I:

Traza - a

Generador de G - g

Polinomio de Traza - $f(x)$

Para $\{a_n\}$ CuadFibonacci: $a_{n+2} = a_{n+1}^2 + a_n^2$ mod primo, para cualquier n

Restricciones sobre $\{a_n\}$

Necesitamos:

$a_0 = 1$

$a_{1022} = 2338775057$

$a_{n+2} = a_{n+1}^2 + a_n^2$

Si $\{a_n\}$ satisface las restricciones ⟶ La declaración original es cierta

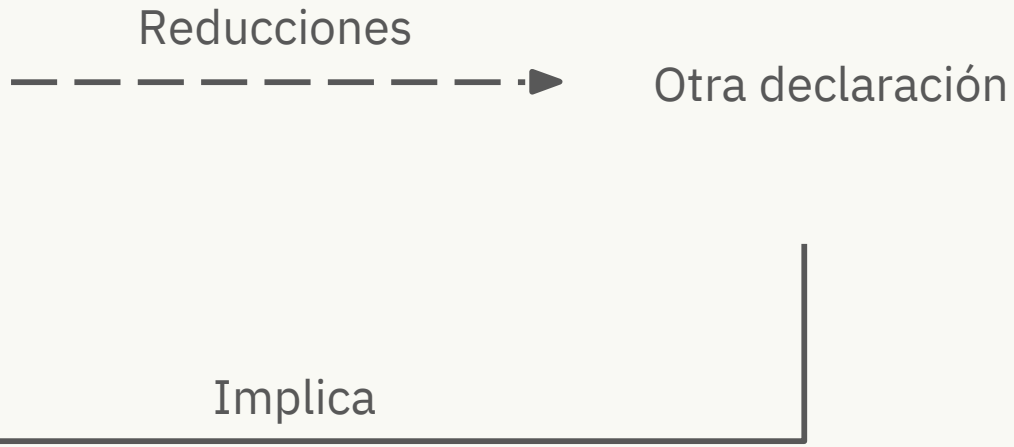
¿Hacia dónde vamos?

Restricciones sobre $\{a_n\}$:

$a_0 = 1$

$a_{1022} = 2338775057$

$a_{n+2} = a_{n+1}^2 + a_n^2$



¿Hacia dónde vamos?

Restricciones sobre $\{a_n\}$:

$a_0 = 1$

$a_{1022} = 2338775057$

$a_{n+2} = a_{n+1}^2 + a_n^2$

Reducciones

Existe un polinomio $f(x)$ tal que:

Polinomio de traza

3 funciones racionales

$p_0(x)$, $p_1(x)$, $p_2(x)$ son **polinomios**

$$\frac{a(x)}{b(x)}$$

Paso I - Desde $\{a_n\}$ hacia $f(x)$

Polinomio de traza

3 restricciones sobre $\{a_n\}$ ⟶ 3 restricciones sobre $f(x)$

$a_0 = 1$ ⟶ $f(x) = 1$, para $x = g^0$

$a_{1022} = 2338775057$ ⟶ $f(x) = 2338775057$, para $x = g^{1022}$

$a_{n+2} = a_{n+1}^2 + a_n^2$

x	$f(x)$
g^0	a_0
g^1	a_1
g^2	a_2
...	...
g^{1022}	a_{1022}

Paso I - Desde $\{a_n\}$ hacia $f(x)$

$$a_{n+2} = a_{n+1}^2 + a_n^2 \quad \longrightarrow \quad f(g^2x) = f(gx)^2 + f(x)^2,$$

para $x = g^i$, $0 \le i \le 1020$

Por ejemplo: para $x = g^5$:

$$f(\underbrace{g^2 \cdot g^5}_{g^7}) = f(\underbrace{g \cdot g^5}_{g^6})^2 + f(\underbrace{g^5}_{g^5})^2$$

x	$f(x)$
g^0	a_0
g^1	a_1
g^2	a_2
...	...
g^5	a_5
g^6	a_6
g^7	a_7
...	...
g^{1022}	a_{1022}

Paso I - Desde $\{a_n\}$ hacia $f(x)$

3 restricciones sobre $\{a_n\}$ ⟶ **3 restricciones sobre $f(x)$**

$a_0 = 1$ ⟶ $f(x) = 1$, para $x = g^0$

$a_{1022} = 2338775057$ ⟶ $f(x) = 2338775057$, para $x = g^{1022}$

$a_{n+2} = a_{n+1}^2 + a_n^2$ ⟶ $f(g^2x) = f(gx)^2 + f(x)^2$,

para $x = g^i$, $0 \leq i \leq 1020$

Paso I - Desde $\{a_n\}$ hacia $f(x)$

3 restricciones sobre $\{a_n\}$	⟶	3 restricciones sobre $f(x)$
$a_0 = 1$	⟶	$f(x) = 1$, para $x = g^0$
$a_{1022} = 2338775057$	⟶	$f(x) = 2338775057$, para $x = g^{1022}$
$a_{n+2} = a_{n+1}^2 + a_n^2$	⟶	$f(g^2x) = f(gx)^2 + f(x)^2$, para $x = g^i$, $0 \le i \le 1020$

Si $f(x)$ satisface las restricciones ⟶ La declaración original es cierta

Paso II - De las Restricciones a las Raíces

z es una raíz de *p(x)* si *p(z)=0*

***f(x) - 1** = 0*, para $x = g^0$ ⟶ raíz: g^0

($f(x) = 1$, para $x = g^0$)

Paso II - De las Restricciones a las Raíces

$f(x) - 1 = 0$, para $x = g^0$ ⟶ raíz: g^0

$f(x) - 2338775057 = 0$, para $x = g^{1022}$ ⟶ raíz: g^{1022}

Paso II - De las Restricciones a las Raíces

$f(x) - 1 = 0$, para $x = g^0$ ⟶ raíz: g^0

$f(x) - 2338775057 = 0$, para $x = g^{1022}$ ⟶ raíz: g^{1022}

$f(g^2x) - f(gx)^2 - f(x)^2 = 0$, para $x = g^i$, $0 \le i \le 1020$ ⟶ raíces: $\{g^i \mid 0 \le i \le 1020\}$

Paso II - De las Restricciones a las Raíces

$f(x) - 1 = 0$, para $x = g^0$ ⟶ raíz: g^0

$f(x) - 2338775057 = 0$, para $x = g^{1022}$ ⟶ raíz: g^{1022}

$f(g^2x) - f(gx)^2 - f(x)^2 = 0$, para $x = g^i$, $0 \le i \le 1020$ ⟶ raíces: $\{g^i \mid 0 \le i \le 1020\}$

g^0 es una raíz de $f(x) - 1$

g^{1022} es una raíz de $f(x) - 2338775057$ ⟶ La declaración original es cierta

$\{g^i \mid 0 \le i \le 1020\}$ son raíces de $f(g^2x) - f(gx)^2 - f(x)^2$

Paso III - De las Raíces a Funciones Racionales

Trm: *z* es una raíz de *p(x)* ⇔ *(x - z)* divide a *p(x)*

Def: *(x - z)* divide a *p(x)* si *p(x)* / *(x - z)* es un polinomio

Polinomio

$$\frac{x^2 - 3x + 2}{x - 2} = \frac{(x - 2)(x - 1)}{x - 2} = x - 1$$

2 es una raíz

No es un Polinomio

$$\frac{x^2 - 7x + 6}{x - 2} = \frac{(x - 1)(x - 6)}{x - 2}$$

2 NO es una raíz

Paso III - De las Raíces a Funciones Racionales

Trm: *z* es una raíz de *p(x)* ⇔ *(x - z)* divide a *p(x)*

Def: *(x - z)* divide a *p(x)* si *p(x)* / *(x - z)* es un polinomio

g^0 es una raíz de *f(x) - 1* ⟶ $\frac{f(x)-1}{x-g^0}$ es un polinomio

g^{1022} es una raíz de *f(x) - 2338775057* ⟶ $\frac{f(x)-2338775057}{x-g^{1022}}$ es un polinomio

Paso III - De las Raíces a Funciones Racionales

$\{g^i \mid 0 \le i \le 1020\}$ son raíces de $f(g^2x) - f(gx)^2 - f(x)^2$ ⟶

$$\frac{f(g^2x) - f(gx)^2 - f(x)^2}{\prod_{i=0}^{1020}(x - g^i)}$$

es un polinomio

$$\prod_{i=0}^{1023}(x - g^i) = x^{1024} - 1$$

Cambiar:

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

3 Funciones Racionales

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

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

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

Si $p_0(x)$, $p_1(x)$, $p_2(x)$ son polinomios ⟶ La declaración original es cierta

¿Hacia dónde vamos?

Restricciones sobre $\{a_n\}$:

$a_0 = 1$

$a_{1022} = 2338775057$

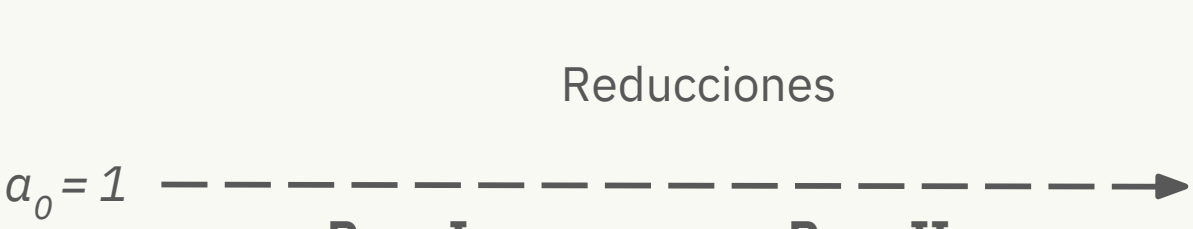
$a_{n+2} = a_{n+1}^2 + a_n^2$

Reducciones

Existe un polinomio $f(x)$ tal que:

3 funciones racionales $p_0(x)$, $p_1(x)$, $p_2(x)$ son **polinomios**

Resumen de Reducción - Primera Restricción



Paso III

Existe un polinomio $f(x)$ tal que:

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

es un **polinomio**

3 Funciones Racionales

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

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

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

Si $p_0(x)$, $p_1(x)$, $p_2(x)$ son polinomios ⟶ La declaración original es cierta

Combinando los $p_i(x)$'s

Combinación lineal aleatoria:

Composition Polynomial

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

Con alta probabilidad:

CP es un polinomio $\Leftrightarrow$ todos los p_i's son polinomios

Compromiso en *CP* con Merkle Tree

¿Y ahora qué?

Parte 3 - ¿cómo probar que *CP* es un polinomio?

Pero primero - el código.....

1) $p_0(x), p_1(x), p_2(x)$
2) $CP = \alpha_0 \cdot p_0(x) + \alpha_1 \cdot p_1(x) + \alpha_2 \cdot p_2(x)$
3) Comprometerse en CP

Gracias