ALGORITMO DE SHOR – Formalidades

Aula passada:

- Redução da fatoração à descoberta de período de $a^x \bmod N$ — $f_{a,N}(x)$
- Definição da QFT e uso na descoberta de período (DFT
- Intuição do Algoritmo de Shor, Desmistificar

Hoje:

- construção eficiente da QFT

Período (ordem) r

r par

$a^{r/2} \neq -1 \bmod N$

Análise Probabilística

$\bmod N$ 10 vezes

$(x^2)^2 \bmod N = x^8$

DFT|x⟩

|x⟩ $H^{\otimes n}$ U_f QFT^{-1} π

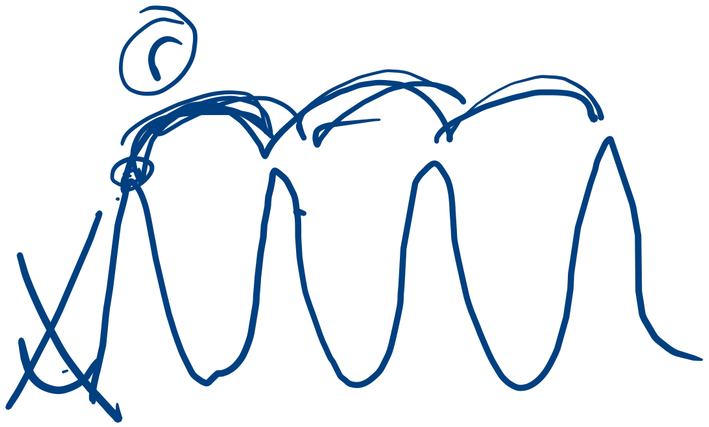
|y⟩ U_f

Aux

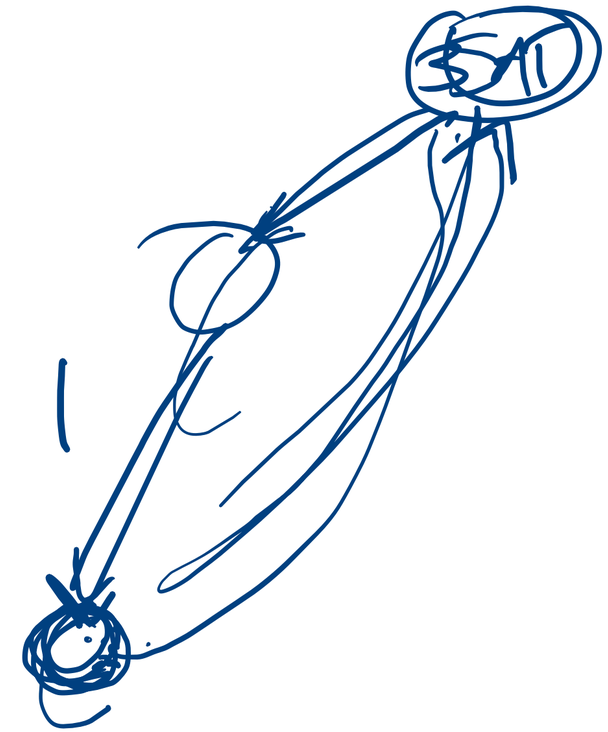
poly(n)

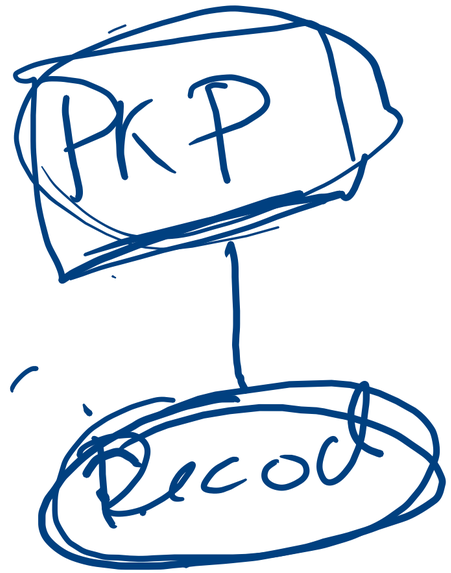
Algo Grover

$2^{100} \rightarrow 2^{50}$



'Luca Trevisan



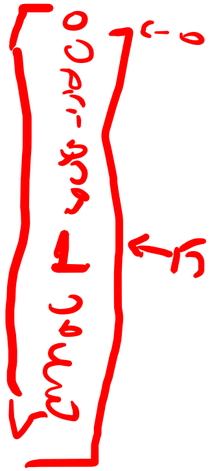


Sabemos que a QFT é definida como

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

para $|j\rangle$ estado básico de $n = \lceil \log N \rceil$ bits.

$$|j\rangle = |1010010\rangle = |15\rangle$$



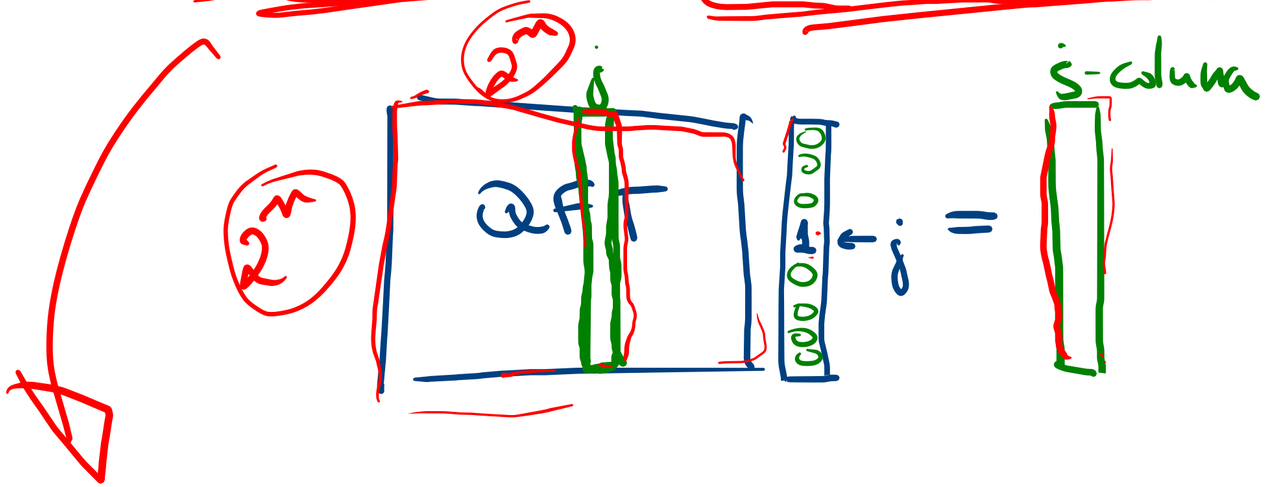
Para uma superposição $|\varphi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$, a acção da QFT é igual à DFT do vector $|\varphi\rangle$, isto é

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} = |\varphi\rangle \xrightarrow{QFT} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix} = \sum_{k=0}^{N-1} y_k |k\rangle \quad , \text{ onde}$$

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$$

A QFT é uma transformação unitária. Veja como a nossa definição explicita a j-ésima coluna da matriz QFT

$$QFT|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$



EXERCÍCIO: Provar que QFT é unitária.

Dica: Ver que $\langle QFT_i^\dagger, QFT_j \rangle = \begin{cases} 1 & \text{sse } (i=j) \\ 0 & \text{caso contrário} \end{cases}$

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

linha i — coluna j

Prop. Seja $|j\rangle$ um estado básico de registrador de n bits, cuja representação em binário é $|j\rangle = |j_1 j_2 \cdots j_n\rangle$. $\Leftrightarrow j = \sum_{i=1}^{n} j_i 2^{n-i}$

Denote por $0.j_l j_{l+1} \cdots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2^{m-l+1}}$

Então:

$$QFT|j\rangle = \bigotimes_{l=0}^{n-1} \frac{\left(|0\rangle + e^{2\pi i\, 0.j_{n-l}\cdots j_n}|1\rangle\right)}{\sqrt{2}}$$

(frac. bin.)

$|00\rangle = |0\rangle \otimes |0\rangle = |0\rangle|0\rangle$

0.234

$2.10^{-1} + 3.10^{-2} + 4.10^{-3}$

0.1011

$= 1.2^{-1} + 0.2^{-2} + 1.2^{-3} + 1.2^{-4}$

$e^{2\pi i\, 0.j_{n-l}\cdots j_n}$

$l=0 \rightarrow e^{2\pi i\, 0.j_n}$

$l=1 \rightarrow e^{2\pi i\, 0.j_{n-1} j_n}$

$l \ldots$

Esta representação permite a construção eficiente da QFT.

Considere a porta $|0\rangle$

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

$|0\rangle \longmapsto |0\rangle$

$|1\rangle \longmapsto e^{2\pi i/2^k}|1\rangle$

$R_k|1\rangle = e^{\frac{2\pi i}{2^k}}$

$R_k|0\rangle = |0\rangle$

Lembre que para toda porta que atua num qubit, temos a versão controlada

$$|x\rangle|y\rangle \longmapsto \begin{cases} |x\rangle|y\rangle & \text{se } x=0 \\ |x\rangle R_k|y\rangle & \text{se } x=1 \end{cases}$$

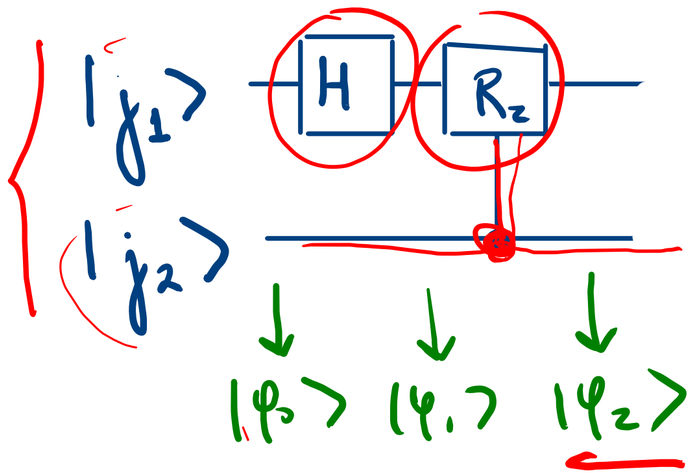
CR_k

$$CR_k = \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{matrix} xy & & & \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \end{array}$$

$|10\rangle \longmapsto |1\rangle R_k|1\rangle$

$$U_C \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cup & \\ 0 & 0 & & \end{bmatrix}$$

Considere o circuito abaixo



$$|\varphi_0\rangle = |j_1 j_2\rangle$$

$$|\varphi_1\rangle = H|j_1\rangle|j_2\rangle = \frac{(|0\rangle + e^{\pi i j_1}|1\rangle)}{\sqrt{2}}|j_2\rangle$$

$$|\varphi_2\rangle = R_2^{j_2}\frac{(|0\rangle + e^{2\pi i j_1}|1\rangle)}{\sqrt{2}}|j_2\rangle$$

$$R_z = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^z} \end{bmatrix}$$

$$= \begin{cases} -1 & \text{se } j_1 = 1 \\ +1 & \text{se } j_1 = 0 \end{cases}$$

$|0\rangle$
$|1\rangle$

$H|j_1\rangle$

$|0\rangle + (-1)^{j_1}|1\rangle$

$|0\rangle + e^{\pi i j_1}|1\rangle$

$R_2^0 = I$

$R_2^1 = R_2$

$$|\varphi_2\rangle = R_2^{j_2}\left(\frac{|0\rangle + e^{\pi i j_1}|1\rangle}{\sqrt{2}}\right)|j_2\rangle$$

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{2}}\left(R_2^{j_2}|0\rangle + R_2^{j_2} e^{\pi i j_1}|1\rangle\right)|j_2\rangle$$

$$R_2^{j_2}\cdot|1\rangle$$

$$R_2^{j_2} = \begin{bmatrix} 1 & \\ & e^{\frac{2\pi i j_2}{2^2}} \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i j_1}{2}} \cdot e^{2\pi i j_2/2^2}|1\rangle\right)|j_2\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2} + \frac{j_2}{2^2}\right)}|1\rangle\right)|j_2\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle\right)|j_2\rangle$$

H

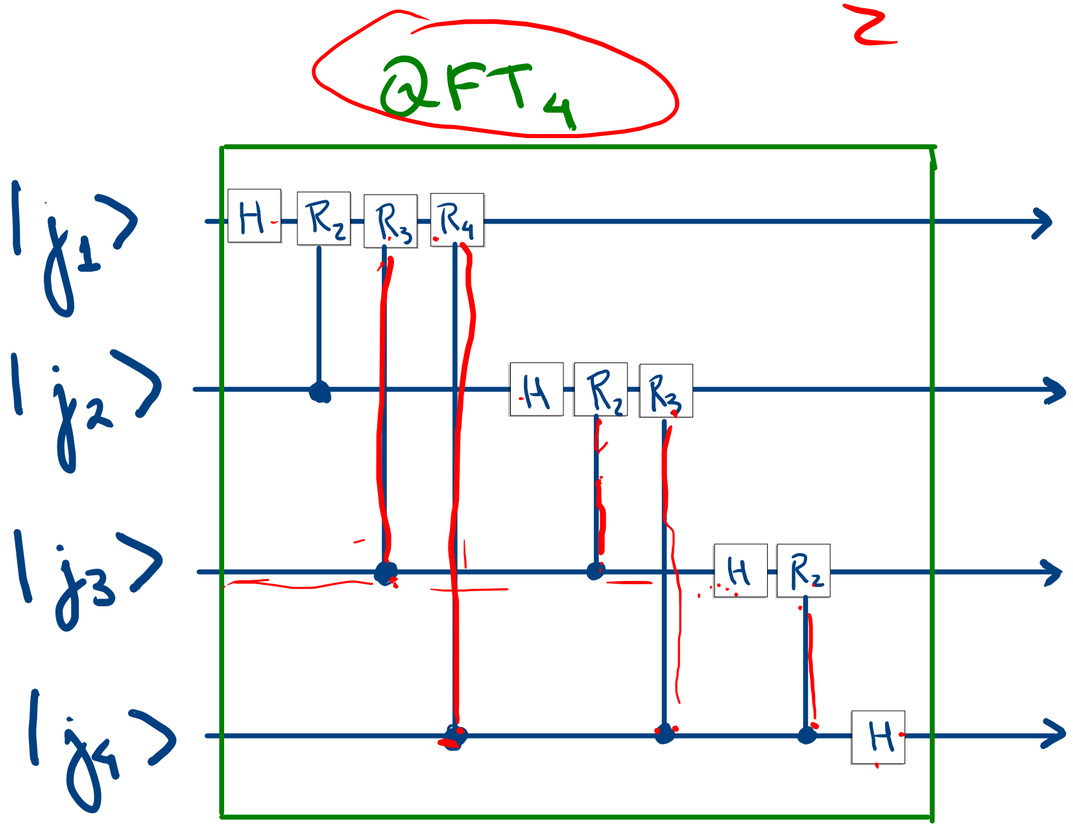
Podemos então implementar a QFT eficientemente usando um número quadrático de portas $\left(\frac{n(n+1)}{2}\right)$

$$\sum 4+3+2+1 = \frac{n(n+1)}{2} = O(n^2)$$

FFT $N = N \log N$

$2^n n$

$R_3 \to \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^3}} \end{bmatrix}$



$|0\rangle + e^{2\pi i\, 0.\, j_1 j_2 j_3 j_4} |1\rangle$

$|0\rangle + e^{2\pi i\, 0.\, j_2 j_3 j_4} |1\rangle$

$|0\rangle + e^{2\pi i\, 0.\, j_3 j_4} |1\rangle$

$|0\rangle + e^{2\pi i\, 0.\, j_4} |1\rangle$

$|0\rangle + e^{2\pi i \left(\frac{j_4}{2}\right)} |1\rangle$

$|0\rangle + e^{2\pi i\, 0.\, j_4} |1\rangle$

DEM Da proposição. $2^n = N$

$$|j\rangle \xrightarrow[\text{DEF}]{\text{QFT}} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} e^{2\pi i k j / N} |k\rangle$$

$$|k\rangle = |k_1 k_2 \dots k_n\rangle \qquad k_i \in \{0,1\}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left(\frac{2\pi i j}{2^n} \sum_{l=1}^{n} k_l 2^{n-l} \right) |k_1 k_2 \dots k_n\rangle$$

$$\frac{j}{2^n} \sum_{l=1}^{n} k_l 2^{n-l} \cdot 2^{-n} = \sum_{l=1}^{n} k_l 2^{-l}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left(2\pi i j \sum_{l=1}^{n} k_l 2^{-l} \right) |k_1 k_2 \dots k_n\rangle$$

$e^{2\pi i j k_1 2^{-1}} \quad e^{2\pi i j k_2 2^{-2}}$

$|k_1\rangle \otimes |k_2\rangle \otimes \dots \otimes |k_n\rangle$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left(2\pi i j \sum_{l=1}^{n} k_l 2^{-l}\right) |k_1 k_2 \dots k_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1,\dots,k_n \in \{0,1\}} \left(\prod_{l=1}^{n} \exp(2\pi i j k_l 2^{-l}) |k_l\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \left(\sum_{k_1 \in \{0,1\}} \exp(2\pi i j k_1 2^{-1}) |k_1\rangle \right) \sum_{k_2,\dots,k_n \in \{0,1\}} \left(\prod_{l=2}^{n} \exp(2\pi i j k_l 2^{-l}) |k_l\rangle \right)$$

k_1

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(\sum_{k_l \in \{0,1\}} \exp(2\pi i j k_l 2^{-l}) |k_l\rangle \right)$$

$$\left(|0\rangle + e^{2\pi i j 1 2^{-l}} |1\rangle \right)$$

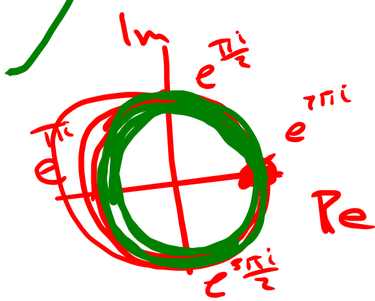
$$\frac{1}{\sqrt{2^n}} \sum_{k_1,\dots,k_n \in \{0,1\}} \left(\prod_{l=1}^{n} \exp(2\pi i j k_l 2^{-l}) |k_l\rangle \right)$$

$$\sum_{k_1} \exp(2\pi i j k_1 2^{-1}) |k_1\rangle \sum_{k_2 \dots k_n} \prod_{l=2}^{n} \exp(2\pi i j k_l 2^{-l}) |k_l\rangle$$

$$\left(|0\rangle + e^{2\pi i j 2^{-1}} |1\rangle \right) \quad k_2 \dots k_n$$

$$QFT|j\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(\sum_{k=0}^{1} \exp(2\pi i j k 2^{-l}) |k\rangle \right)$$

$e^{2\pi i j 2^{-l}}$



$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right)$$

$(0+\circlearrowright)(0+0)$

$= 00 + 00 + 00 + 00$

Importante: Sabemos que $e^{2\pi i k} = 1 \quad \forall k \in \mathbb{Z}$, então somente a parte fracionária de $j2^{-l}$ importa

$$j2^{-l} = 2^{-l} \sum_{k=1}^{n} j_k 2^{n-k} = \sum_{k=1}^{n} j_k \cdot 2^{n-k-l}$$

$j2^{-l}$ = δ

$$= j_1 \ldots \underbrace{j_{n-l}}_{n-l} \cdot j_{n-l+1} \ldots j_n$$

$$= 0.\, j_{n-l+1} \ldots j_n$$

$k = n - l$

$j_{n-l} \cdot 2^0 + \quad \cdot 2^{-1}$

$$QFT|j\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right)$$

$$= \bigotimes_{l=0}^{n-1} \frac{\left(|0\rangle + e^{2\pi i \, 0.j_{n-l} \cdots j_n} |1\rangle \right)}{\sqrt{2}}$$

= resto da div por 1 de $\frac{j 2^{-l}}{1}$

UFA

Recapitulando

O que sabemos?

- Achar período de $a^x \bmod N \Rightarrow$ fatorar N
- DFT ajuda a achar período quando damos sorte
  - r par (E) $a^{r/2} \neq -1 \bmod N$
  - Se possível extrair λ, r da fração $\lambda \frac{2^m}{r} = y \Rightarrow \frac{y}{2^m} = \frac{\lambda}{r}$
- Algoritmo de Shor usa QFT
- QFT tem implementação eficiente ($n(n+1)/2 = O(n^2)$ portas)

O que falta?

- Qual a prob de darmos sorte?

Quantum computation and Qu. Information

Michael Nielsen Isaac. Chuang

Teo. Seja $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ um inteiro ímpar.

Seja $x \xleftarrow{\$} \mathbb{Z}_N^*$ de ordem $r \bmod N$.

Então

$$\mathbb{P}(r \text{ par e } x^{r/2} \not\equiv -1 \bmod N) \geq \underbrace{1 - \frac{1}{2^m}}_{} \geq 3/4$$

Teo Simplificado. Seja $N = p_1 p_2$ inteiro ímpar. $x \xleftarrow{\$} \mathbb{Z}_N^*$ de ordem r. Então

$$\mathbb{P}(r \text{ par e } x^{r/2} \not\equiv -1 \bmod N) \geq 1 - \frac{1}{4} = 3/4.$$

DEM
Teo Simp

Se $N = p_1 p_2$, o teorema chinês do resto nos garante que

$$x \bmod N \iff \begin{cases} x \equiv x_1 \bmod p_1 \\ x \equiv x_2 \bmod p_2 \end{cases}$$

Então sortear $x \xleftarrow{\$} \mathbb{Z}_N^*$ é exatamente igual a sortear $x_1 \bmod p_1$ e $x_2 \bmod p_2$, que determinam x unicamente, pelo TCR.

Lembrando, pelo TCR

$$x = x_1 \cdot p_2 (p_2^{-1} \bmod p_1) + x_2 p_1 (p_1^{-1} \bmod p_2) \bmod N$$

Sejam $\begin{cases} r_1 = \text{período de } x_1 \bmod p_1 \\ r_2 = \text{período de } x_2 \bmod p_2 \end{cases}$

Note que $r_1 | r$ e $r_2 | r$ pois

$$x^r \equiv 1 \bmod N \Rightarrow x^r = kN + 1 \Rightarrow x^r \equiv 1 \bmod p_1$$

Como $r_1 \leq r$ e $x^{r_1} \equiv 1 \bmod p_1$, então

$r = u r_1$ para algum $u \in \mathbb{Z}^+$.

Então: Sejam d_1, d_2 os maiores inteiros tais que

$$2^{d_1} \mid r_1 \quad \text{e} \quad 2^{d_2} \mid r_2$$

Vamos mostrar que se t é impar ou se $x^{r/2} \equiv -1$, então $d_1 = d_2$.

Caso r impar $\Rightarrow$ r_1 e r_2 são impares

$$\Rightarrow d_1 = d_2 = 0$$

Caso r par e $x^{r/2} \equiv -1 \bmod N$

$$\Rightarrow \quad x^{r/2} \equiv -1 + K p_1 p_2$$

$$\Rightarrow \quad x^{r/2} \equiv -1 \bmod p_i \quad \forall i \in \{1,2\}$$

$$\Rightarrow \begin{cases} r_i \nmid \left(\frac{r}{2}\right) \\ r_i \mid r \end{cases} \Rightarrow \begin{cases} 2^{d_i} \nmid (r/2) \\ 2^{d_i} \mid r \end{cases}$$

$\Rightarrow d_1 = d_2 = d$, onde d é $\max d$ tq $2^d \mid N$

Então sabemos que

$$\text{AZAR} \Rightarrow \begin{cases} d_1 = d \\ d_2 = d \end{cases} \Rightarrow \mathbb{P}(\text{Azar}) \leq \mathbb{P}\begin{pmatrix} d_1 = d \\ d_2 = d \end{pmatrix}$$

r ímpar ou $a^{r/2} \equiv -1$

Qual é então a prob de $\begin{cases} d_1 = d \\ d_2 = d \end{cases}$?

Só falta mostrar que $\mathbb{P}(d_1 = d \text{ e } d_2 = d) \leq \frac{1}{4}$,

então $\mathbb{P}(\text{sorte}) = 1 - \mathbb{P}(\text{Azar}) \geq 3/4$.

Lema Se p é primo ímpar e $2^{\bar{d}}$ é maior potência de 2 que divide $\varphi(p_1)$, então

$$\mathbb{P}(2^{\bar{d}} \mid r) = 1/2$$

DEM Sabemos que $\varphi(p) = |\mathbb{Z}_p^*| = p - 1$ que é par.

Seja g um gerador de $\mathbb{Z}_p^*$, isto é $\mathbb{Z}_p^* = \{g^k : k = 1, \dots, \varphi(p)\}$

Seja r a ordem de $x_1 = g^k$.

Então temos 2 casos para $x \equiv g^k \bmod p$.

Caso k ímpar:

Pela def $x^r = g^{kr} \equiv 1$. Mas sabemos por Teo Euler que

$\varphi(p)$ é ordem de g com $g^{\varphi(p)} \equiv 1$, portanto $\varphi(p) \mid kr$.

Então $2^a \mid \varphi(p) \Rightarrow 2^a \mid kr$

$\Rightarrow 2^a \mid r$, pois k é ímpar

□

Queremos mostrar que

$$\mathbb{P}(d_1 = d \text{ e } d_2 = d) = \mathbb{P}(d_1 = d)\,\mathbb{P}(d_2 = d) \leq \frac{1}{4}$$

onde

$$2^{d_1} \mid r_1 \,, \quad 2^{d_2} \mid r_2 \text{ e } 2^{d} \mid r \,.$$

d é sempre $\geq d_1, d_2$. Então

$$\mathbb{P}(d_1 = d) \leq \mathbb{P}(d_1 = \bar{d}_1) \,, \text{ onde } \bar{d}_1 = \max_{2^i \mid \varphi(p_1)} i$$

$$\mathbb{P}(d_1 = d) \leq \underbrace{\mathbb{P}(d_1 = \bar{d}_1)}_{\leq \frac{1}{2} \text{ (Lemma)}}, \text{ onde } \bar{d}_1 = \max_{2^i \mid \varphi(p_1)} i$$

$$\mathbb{P}(d_2 = d) \leq \underbrace{\mathbb{P}(d_2 = \bar{d}_2)}_{\leq \frac{1}{2} \text{ (Lema)}}, \text{ onde } \bar{d}_2 = \max_{2^i \mid \varphi(p_2)} i$$

CASO K par Neste caso, temos que

$$g^{K\varphi(p_1)/2} = \left(g^{\varphi(p_1)}\right)^{K/2} = 1 \bmod p_1$$

$$\Rightarrow \left(g^{K}\right)^{\varphi(p_1)/2} = 1 \bmod p$$

$$\Rightarrow r_1 \mid \frac{\varphi(p_1)}{2} \Rightarrow 2^{d_1} \nmid r_1 \text{ pois } \boxed{2^{d_1} \mid \varphi(p_1)}$$