Computação Quântica
Aula 15

Murilo V. G. da Silva

DINF/UFPR

Algoritmo de Shor

Assunto da aula de hoje:

Algoritmo de Shor

Assunto da aula de hoje:

- Reduzindo o problema de fatoração para o seguinte problema:
  - encontrar raíz não trivial de 1 módulo n
- Reduzir o da raíz não trivial para o seguinte problema:
  - detectar o período da função $f(x) = b^x \pmod{n}$, para um b apropriado

    (obs: não é direto ver, mas essa função é periódica)

Fatoração

Problema: fatorar N em primos $p_1, p_2, ..., p_k$ tal que $p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k} = N$

Fatoração

Problema: fatorar N em primos $p_1, p_2, ..., p_k$ tal que $p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k} = N$

- Caso mais difícil N tem apenas dois fatores de tamanho semelhante

Fatoração

Problema: fatorar N em primos $p_1, p_2, ..., p_k$ tal que $p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k} = N$

- Caso mais difícil N tem apenas dois fatores de tamanho semelhante
- Este é o caso usado no sistema RSA

Fatoração

Problema: fatorar N em primos $p_1, p_2, ..., p_k$ tal que $p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k} = N$

- Caso mais difícil N tem apenas dois fatores de tamanho semelhante
- Este é o caso usado no sistema RSA
- Algoritmo clássico para isso:
  - $\mathcal{O}(2^{\sqrt[3]{n}})$

Fatoração

Problema: fatorar N em primos $p_1, p_2, ..., p_k$ tal que $p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k} = N$

- Caso mais difícil N tem apenas dois fatores de tamanho semelhante
- Este é o caso usado no sistema RSA
- Algoritmo clássico para isso:
  - $\mathcal{O}(2^{\sqrt[3]{n}})$ (aleatorizado)

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais:

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$
- Mais algum outro valor?

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$
- Mais algum outro valor? $x = -8$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$
- Mais algum outro valor? $x = -8$
  - $-8 \equiv ? \pmod{21}$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$
- Mais algum outro valor? $x = -8$
  - $-8 \equiv ? \pmod{21}$
  - $-8 \equiv 13 \pmod{21}$

Raízes de 1 módulo N

Vamos ver como encontrar os fatores de $N = 21$

- Ideia: encontre x tal que $x^2 \equiv 1 \pmod{21}$
- Raízes triviais: 1 e -1
  - $1^2 \equiv 1 \pmod{21}$ OK
  - Por quê -1 também é raiz?
  - $-1 \equiv 20 \pmod{21}$
  - $20^2 \equiv 1 \pmod{21}$ OK
- Existe algum outro valor x tal que $x^2 \equiv 1 \pmod{21}$?
- Faça o teste para $x = 8$
  - $8^2 = 64 \equiv 1 \pmod{21}$
- Mais algum outro valor? $x = -8$
  - $-8 \equiv ? \pmod{21}$
  - $-8 \equiv 13 \pmod{21}$
  - $13^2 = 169 \equiv 1 \pmod{21}$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

  Como encontrar estes fatores?

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

  Como encontrar estes fatores?
  - mdc(21, $8+1$)

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

  Como encontrar estes fatores?
  - $\text{mdc}(21, 8+1) = 3$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

  Como encontrar estes fatores?
  - $\text{mdc}(21, 8+1) = 3$
  - $\text{mdc}(21, 8-1) = 7$

Raízes de 1 módulo N

Por que estamos interessados em raízes não triviais de 1 mod 21?

- Afinal, como 8 e -8 podem ser úteis para nosso objetivo que é fatorar 21?

Observe o seguinte:

- $8^2 \equiv 1 \pmod{21}$
- $8^2 - 1^2 \equiv 1 - 1^2 \pmod{21}$
- $8^2 - 1^2 \equiv 0 \pmod{21}$ O que isso significa?
- 21 divide $8^2 - 1^2$
- Escrevendo $8^2 - 1^2$ como produto notável, temos
- 21 divide $(8+1)(8-1)$ Mas observe que:
  - 21 não divide $(8+1)$
  - 21 não divide $(8-1)$
- O que isso significa?
  - algum fator de 21 divide $(8+1)$
  - algum fator de 21 divide $(8-1)$

  Como encontrar estes fatores?
  - $\text{mdc}(21, 8+1) = 3$
  - $\text{mdc}(21, 8-1) = 7$

Com isso $21 = 3 \cdot 7$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21?

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando!

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \bmod (21)$
- $x = 1 \quad 2^1 \equiv 2 \bmod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, ...$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, ...$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$
- $x = 5 \quad 2^5 \equiv$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$
- $x = 5 \quad 2^5 \equiv 11 \mod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$
- $x = 5 \quad 2^5 \equiv 11 \mod (21)$
- $x = 6 \quad 2^6 \equiv$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, ...$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$
- $x = 5 \quad 2^5 \equiv 11 \mod (21)$
- $x = 6 \quad 2^6 \equiv 1 \mod (21)$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, ...$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$
- $x = 5 \quad 2^5 \equiv 11 \mod (21)$
- $x = 6 \quad 2^6 \equiv 1 \mod (21)$

Note que $2^6 = (2^3)^2 = 8^2$

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \mod 21$ para $x = 0, 1, 2, 3, ...$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \mod (21)$
- $x = 1 \quad 2^1 \equiv 2 \mod (21)$
- $x = 2 \quad 2^2 \equiv 4 \mod (21)$
- $x = 3 \quad 2^3 \equiv 8 \mod (21)$
- $x = 4 \quad 2^4 \equiv 16 \mod (21)$
- $x = 5 \quad 2^5 \equiv 11 \mod (21)$
- $x = 6 \quad 2^6 \equiv 1 \mod (21)$

Note que $2^6 = (2^3)^2 = 8^2$

Por que o valor $x = 6$ deu certo?

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \bmod (21)$
- $x = 1 \quad 2^1 \equiv 2 \bmod (21)$
- $x = 2 \quad 2^2 \equiv 4 \bmod (21)$
- $x = 3 \quad 2^3 \equiv 8 \bmod (21)$
- $x = 4 \quad 2^4 \equiv 16 \bmod (21)$
- $x = 5 \quad 2^5 \equiv 11 \bmod (21)$
- $x = 6 \quad 2^6 \equiv 1 \bmod (21)$

Note que $2^6 = (2^3)^2 = 8^2$

Por que o valor $x = 6$ deu certo? (obs: x é chamado de ordem do subgrupo de $(\mathbb{Z}_{21}, \times)$ gerado por 2)

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \bmod (21)$
- $x = 1 \quad 2^1 \equiv 2 \bmod (21)$
- $x = 2 \quad 2^2 \equiv 4 \bmod (21)$
- $x = 3 \quad 2^3 \equiv 8 \bmod (21)$
- $x = 4 \quad 2^4 \equiv 16 \bmod (21)$
- $x = 5 \quad 2^5 \equiv 11 \bmod (21)$
- $x = 6 \quad 2^6 \equiv 1 \bmod (21)$

Note que $2^6 = (2^3)^2 = 8^2$

Por que o valor $x = 6$ deu certo? (obs: x é chamado de ordem do subgrupo de $(\mathbb{Z}_{21}, \times)$ gerado por 2)

(1) Por que o valor x é par (tornou possível fazer o truque de dividir por 2)

(2) Por que $\frac{x}{2}$ não é raiz trivial como 1 ou 20

Raízes de 1 módulo N

Mas como descobrir que 8 é uma raiz de 1 mod 21? Chutando! Ou quase...

Ideia:

- Pegue uma base b aleatoriamente
- Calcule valores da função $f(x) = b^x \bmod 21$ para $x = 0, 1, 2, 3, \ldots$

Exemplo:

- Suponha que o valor aleatório é $b = 2$
- $x = 0 \quad 2^0 \equiv 1 \bmod (21)$
- $x = 1 \quad 2^1 \equiv 2 \bmod (21)$
- $x = 2 \quad 2^2 \equiv 4 \bmod (21)$
- $x = 3 \quad 2^3 \equiv 8 \bmod (21)$
- $x = 4 \quad 2^4 \equiv 16 \bmod (21)$
- $x = 5 \quad 2^5 \equiv 11 \bmod (21)$
- $x = 6 \quad 2^6 \equiv 1 \bmod (21)$

Note que $2^6 = (2^3)^2 = 8^2$

Por que o valor $x = 6$ deu certo? (obs: x é chamado de ordem do subgrupo de $(\mathbb{Z}_{21}, \times)$ gerado por 2)

(1) Por que o valor x é par (tornou possível fazer o truque de dividir por 2)

(2) Por que $\frac{x}{2}$ não é raiz trivial como 1 ou 20 (lembrando que $-1 \equiv 20 \pmod{21}$)

Quão sortudos nós fomos?

Raízes de 1 módulo N

Lembrando...

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

O teorema abaixo mostra, mesmo "chutando", temos boa probabilidade de encontrar b com as propriedades que queremos:

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

O teorema abaixo mostra, mesmo "chutando", temos boa probabilidade de encontrar b com as propriedades que queremos:

Teorema

Seja N ímpar, $N = PQ$, para P, Q primos distintos e seja b aleatório em $\{0, ..., N-1\}$ Se $\text{mdc}(b, N) = 1$, então a probabilidade da ordem a de $f(x) = b^x \pmod N$ é par e que $a/2$ seja uma raíz não trivial de 1 (mod N) é $\geq 1/2$

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

O teorema abaixo mostra, mesmo "chutando", temos boa probabilidade de encontrar b com as propriedades que queremos:

Teorema

Seja N ímpar, $N = PQ$, para P, Q primos distintos e seja b aleatório em $\{0, ..., N-1\}$ Se $\text{mdc}(b, N) = 1$, então a probabilidade da ordem a de $f(x) = b^x \pmod N$ é par e que $a/2$ seja uma raíz não trivial de 1 (mod N) é $\geq 1/2$

A probabilidade é boa, mas veja que temos uma condição a mais neste teorema: o teorema só funciona quando o valor b que chutamos tem a propriedade $\text{mdc}(b, N) = 1$.

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

O teorema abaixo mostra, mesmo "chutando", temos boa probabilidade de encontrar b com as propriedades que queremos:

Teorema

Seja N ímpar, $N = PQ$, para P, Q primos distintos e seja b aleatório em $\{0, ..., N-1\}$ Se $\text{mdc}(b, N) = 1$, então a probabilidade da ordem a de $f(x) = b^x \pmod N$ é par e que $a/2$ seja uma raíz não trivial de 1 (mod N) é $\geq 1/2$

A probabilidade é boa, mas veja que temos uma condição a mais neste teorema: o teorema só funciona quando o valor b que chutamos tem a propriedade $\text{mdc}(b, N) = 1$.

Isso é um problema?

Raízes de 1 módulo N

Lembrando...

- Amostramos $b \in \{0, ..., N-1\}$ aleatoriamente (no exemplo anterior, $b = 2$)
- Precisamos encontrar um inteiro a par tal que $f(a) = b^{a/2} \bmod 21$ era uma raíz não trivial de 1 (mod 21)

O teorema abaixo mostra, mesmo "chutando", temos boa probabilidade de encontrar b com as propriedades que queremos:

Teorema

Seja N ímpar, $N = PQ$, para P, Q primos distintos e seja b aleatório em $\{0, ..., N-1\}$ Se $\text{mdc}(b, N) = 1$, então a probabilidade da ordem a de $f(x) = b^x \pmod N$ é par e que $a/2$ seja uma raíz não trivial de 1 (mod N) é $\geq 1/2$

A probabilidade é boa, mas veja que temos uma condição a mais neste teorema: o teorema só funciona quando o valor b que chutamos tem a propriedade $\text{mdc}(b, N) = 1$.

Isso é um problema?

- Não! Caso chutemos b tal que Se $\text{mdc}(b, N) \neq 1$ já encontramos um fator de N

Raízes de 1 módulo N

Moral da história:
Chutamos um b e descobrimos a ordem do subgrupo de $(\mathbb{Z}_N, \times)$ gerado por b.

Raízes de 1 módulo N

Moral da história:
Chutamos um b e descobrimos a ordem do subgrupo de $(\mathbb{Z}_N, \times)$ gerado por b.

- Em outras palavras, queremos o período da função periódica $f(x) = b^x \pmod{N}$

Raízes de 1 módulo N

Moral da história:
Chutamos um b e descobrimos a ordem do subgrupo de $(\mathbb{Z}_N, \times)$ gerado por b.

- Em outras palavras, queremos o período da função periódica $f(x) = b^x \pmod N$
- O período pode ser exponencialmente grande, portanto o número de queries que precisaríamos fazer em f para encontrar uma colisão (observe que encontrada uma colisão temos informação para encontrar o período de f).

Raízes de 1 módulo N

Moral da história:
Chutamos um b e descobrimos a ordem do subgrupo de $(\mathbb{Z}_N, \times)$ gerado por b.

- Em outras palavras, queremos o período da função periódica $f(x) = b^x \pmod N$
- O período pode ser exponencialmente grande, portanto o número de queries que precisaríamos fazer em f para encontrar uma colisão (observe que encontrada uma colisão temos informação para encontrar o período de f).
- Entretanto, de maneira quântica, vamos usar a propriedade que QFT tem ao termos como entrada uma superposição descrita por uma função periódica, mesmo que este seja exponencialmente grande para encontrar este período!