INTRODUÇÃO

n → PRIMO

$n \geq 2$ → COMPOSTO: $n = ab$, $1 < a, b < n$ → $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$ →

→ $a > \sqrt{n}$ e $b > \sqrt{n}$

$n = ab > \sqrt{n}\sqrt{n} = n$ X

~~→ Se $d \nmid n$ $\forall d \in [2, \sqrt{n}]$, então n é PRIMO. Senão é COMPOSTO~~

~~→ Se $d \nmid n$ para todo d entre 2 e $\sqrt{n}$, então n é PRIMO. Senão é COMPOSTO~~

→ Se d não divide n $\forall d$ entre 2 e $\sqrt{n}$, então n é PRIMO. Senão é COMPOSTO

$n \sim 10^{150}$ $\sqrt{n} \sim 10^{75}$

divisões $\sim 10^{75}$

10^{10} divisões por segundo

menos 10^{10} segundos para uma

mais de 10^{55} anos

(idade do universo $1{,}5 \times 10^{10}$ anos)

TEMPO EXPONENCIAL

divisões $\sim \sqrt{n}$

TAMANHO DA ENTRADA

$\lfloor \log_2 n \rfloor + 1 \sim \log_2 n$

$\sqrt{n} = 2^{\frac{1}{2}\log_2 n}$

ALGORITMO DE RABIN

operações $< 200 \log_2 n$

$n \sim 10^{150}$

operações $< 10^5$

ERRO $< \frac{1}{10^{30}}$

(1) MEGASENA

(2) PRÁTICA NÃO IMPORTA

(3) MAIS FÁCIL DE COMP. COMPUTADORES

PEQUENO TEOREMA DE FERMAT

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

PROPRIEDADES USUAIS
$a+b := \text{res}(a+b, n)$
$ab := \text{res}(ab, n)$

EXEMPLOS ($n=12$)

$7+9 = 4$
$3 \cdot 5 = 3$

~~$5+7=0$~~
$3 \cdot 4 = 0$
$7 \cdot 7 = 1$

SEÇÃO 3.1

$a \in \mathbb{Z}_n$, $a \neq 0$

- $\text{MDC}(a,n) \neq 1$ (a é DIVISOR DE ZERO) (3)
  $\frac{a}{d} = a' \quad \frac{n}{d} = n' \quad ; \quad an' = a'dn' = 0$
- $\text{MDC}(a,n) = 1$ (a é INVERSÍVEL)
  $\alpha a + \beta n = 1 \quad ; \quad \overline{\alpha} \cdot a = 1$

SEÇÃO 3.2

$\mathbb{Z}_n^* = \{a \in \mathbb{Z} : \text{MDC}(a,n) = 1\}$

↑ $\varphi(n)$ elementos.

TEOREMA (EULER)

Se $a \in \mathbb{Z}_n^*$, então $a^{\varphi(n)} = 1$

Demo: $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ (injetiva & sobrejetiva)
$x \mapsto ax$

$$\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} f(x) = \prod_{x \in \mathbb{Z}_n^*} ax = a^{\varphi(n)} \prod_{x \in \mathbb{Z}_n^*} x$$

Quando n É PRIMO

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \neq 0\}$

$\varphi(n) = n-1$

TEOREMA (FERMAT) Sejam n primo. Se $a \in \mathbb{Z}_n$, $a \neq 0$, então $a^{n-1} = 1$

SEÇÃO 3.4

PSEUDOPRIMOS

n ímpar

$n-1 = 2^t m$, $t>0$ e m ímpar

$a \in \mathbb{Z}_n$, $a \neq 0$

$a^m, a^{2m}, a^{2^2 m}, a^{2^3 m}, \ldots, a^{2^t m}$

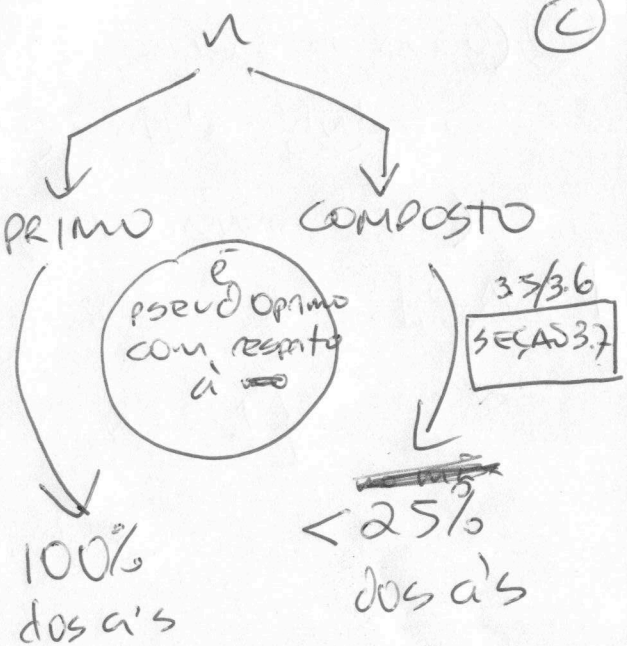
(cada seta: quadrado) — t multiplicações em $\mathbb{Z}_n$

Quando n é primo:

(i) $a^m = 1$

(ii) $a^{2^i m} = -1$ para algum $i < t$

n é pseudoprimo com respeito a a quando (i) ou (ii) ocorre.



Para i variando de 1 a 50 faça:

- escolha a aleatoriamente em $\mathbb{Z}_n$, $a \neq 0$
- se n não é pseudoprimo com respeito a a, então retorne COMPOSTO

Senão retorne (PRIMO).

$$\text{ERRO} < \underbrace{\frac{1}{4}\cdot\frac{1}{4}\cdots\frac{1}{4}}_{50 \text{ vezes}} = \left(\frac{1}{4}\right)^{50} = \frac{1}{2^{100}} = \frac{1}{(2^{10})^{10}} = \frac{1}{1024^{10}} < \frac{1}{(10^3)^{10}} \in \frac{1}{10^{30}}$$