Primalidade e algoritmos aleatorizados

Exercício 1 *Mostre que os algoritmos de primalidade baseados nas seguintes ideias são exponenciais (em termos de $|n| \approx \log n$)*

a) Testar se cada um dos inteiros 2, 3, ..., $\lfloor n/2 \rfloor$ é divisor de n.

a) Testar se cada um dos inteiros 2, 3, ..., $\lfloor \sqrt{n} \rfloor$ é divisor de n.
Nota. *Mesmo se nos limitarmos a testar como possíveis divisores os primos não superiores a $\lfloor \sqrt{n} \rfloor$, o algoritmo continua a não ser polinomial.*

```
Algoritmo aleatorizado para o problema da primalidade
Dado: n
Resultado:
   se n é primo: resposta SIM
   se n é composto: a resposta pode ser NÃO (correcta)
                    mas também pode ser SIM (errada)

(*) m = inteiro aleatório uniforme em {2,3,...,n-1}
   se m divide n:
      return NÃO
   senão:
      return SIM
```

```
Forma do algoritmo aleatorizado que se pretende
Dado: n
Resultado:
   se n é primo: resposta SIM
   se n é composto: resposta incorrecta com probabilidade <= 1/2

(*) m = inteiro aleatório uniforme (possível testemunha) ...
   se m é testemunha:
      return NÃO
   senão:
      return SIM
```

Pequeno teorema de Fermat / Demostração / frequência das testemunhas

```
Algoritmo aleatorizado para o problema da primalidade
Dado: n
Resultado:
   se n é primo: resposta SIM
   se n é composto: resposta incorrecta com probabilidade ???
                    (a determinar)

(*)  m = inteiro aleatório uniforme em {2,3,...,n-1}
(+)  x = m^(n-1)  (mod n)

   se x=1:
      return PRIMO
   senão:
      return COMPOSTO
```

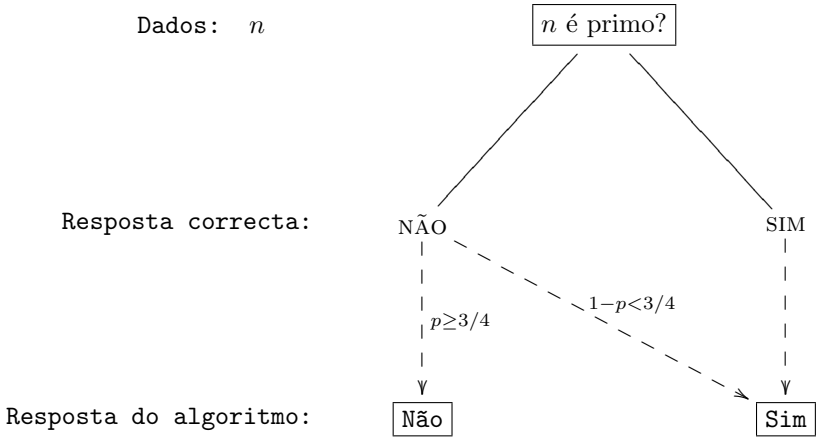
Potência modular eficiente

Inteiro	Frequência
561	0.428
1105	0.304
1729	0.250
2465	0.273
2821	0.234
6601	0, 200

Teorema 1 *Seja n um inteiro ímpar. Podemos escrever $n-1 = 2^s d$ com d ímpar*
Se n é composto, pelo menos metade dos inteiros $a \in \{2, 3, \ldots, n-1\}$ satisfazem

$$[a^d \neq 1 \,(\mathrm{mod}\, n)] \wedge [\forall i, 0 \leq i \leq s-1 : \; a^{2^i d} \neq -1 \,(\mathrm{mod}\, n)]$$

Se n é primo, nenhum inteiro $a \in \{2, 3, \ldots, n-1\}$ satisfaz a condição.
Nesse caso diz-se que a é uma testemunha de n ser composto.
Para n ímpar e para um inteiro $a \in_u \{2, 3, \ldots, n-1\}$ (escolha aleatória uniforme), a probabilidade de a ser uma testemunha da não-primalidade de n é pelo menos $3/4$.



Exercício 2 *Mostre que o teste mencionado no Teorema 1 pode ser efectuado eficientemente.*

Voltando às ordens de grandeza...

Exercício 3 *Determine funções $f(n)$, $g(n)$ de $\mathbb{R}$ em $\mathbb{R}$, estritamente crescentes tais que $f(n) \notin O(g(n))$ e $g(n) \notin O(f(n))$, ou, em alternativa, mostre que tais funções não existem.*