Sorteia n ? n primo

$a \in Z_n^*$: $a^{n-1} = 1 \equiv n$ primo $\mod n$

Teorema de Fermat

testemunho de primalidade (algo Euclides mdc)
{mentiroso}

Números de Carmichael

↓ $n = 561 = 3 \times 11 \times 17$

$\forall a \in Z_n^*$: $a^{n-1} = 1 \mod n$

↑ apesar de n ser composto TODOS mentem

p primo $\Rightarrow \sqrt{1} \mod p \begin{cases} +1 \\ -1 \end{cases}$

$n - 1 = 2^t \cdot c \rightarrow$ ímpar (c)

Escolhe a (testemunha)

$d \leftarrow a^c \mod n$

$(d)^{2^t} = a^{n-1} \mod n$

$x_1 = d^2$

$x_2 = (d^2)^2$

$x_t = d^{2^t}$

Se $r_j \neq 1$, então n não é primo

$\left(\frac{1}{4}\right)^{10} = 9,5367 \cdot 10^{-7}$

Tese: ao final de cada iteração, é verdade que $temp = m^{b_t 2^{t-j} + b_{t-1} 2^{t-j-1} + \ldots b_j}$ mod m

Vamos p/ indução:

Base indutiva $t = 0$: $e = b_0$.
$j = 0$: $temp \leftarrow temp^2$;
$b_0 = 0 \rightarrow temp$ vale $1 = m^0$ ok
$b_1 = 1 \rightarrow temp \leftarrow temp * m = m = m^1$ ok

Passo indutivo:
Supõe-se tese verdadeira p/ $j = t, t-1, \ldots, t-1$
Agora quero tese p/ $j = 0$:
$temp = (m)^{[b_t 2^{t-j} + b_{t-1} 2^{t-2} + \ldots b_1]}$
$j = 0$: $temp = (temp)^2 = \{(m)[b_t 2^t + b_t \ldots$

acabou a aula, ficaram na frente da lousa por tempo infinito