LISTA 9 - GABRIEL ALMEIDA MENDES - DRE: 117049459

(1) USE O PEQUENO TEOREMA DE FERMAT

a) O RESTO DE $10^{10^{100}}$ DIVIDIDO POR 7

RESPOSTA: TEMOS QUE 7 É PRIMO ENTÃO PODEMOS USAR A SEGUNDA VERSÃO DO TEOREMA DE FERMAT; ∴

$a^k \equiv a^{(p-1)q+r}$, A QUM $k = 10^{100}$ E $p-1 = 7-1 = 6 \pmod p$

USANDO A IDÉIA ACIMA BASTA CALCULAR A RESTO DA DIVISÃO DE 10^{100} POR 6. OBTEMOS $q = 166\ldots$ E $r = 4$, FICANDO:

$10^{10^{100}} \equiv (10^6)^q \cdot 10^4 \pmod 7$

PELO TEOREMA DE FERMAT $a^{p-1} \equiv 1 \pmod p$.

$10^{10^{100}} \equiv (1)^q \cdot 10^4 \pmod 7$

$\equiv 1 \cdot 10000 \pmod 7$

$\equiv 10000 \pmod 7$

(5) USE O TESTE DE FERMAT PARA VERIFICAR SE OS NÚMEROS n SÃO COMPOSTOS.

a) $M = 1687$, $b = 4$

4^{1687} → FATORANDO EXPOENTE $1687 = 7 \cdot 241$

$4^{1686} = (4^6)^{281} = (1)^{281} = 1 \pmod 7$

$4^{1686} = (4^{240})^7 \cdot 4^6 = (1)^7 \cdot 4^6 = 4^6 = 4096 = -1 \pmod{241}$

PORTANTO, $4^{1686} - 1$ É DIVISIVEL POR 7 MAS NAO POR 241

APESAR DE SEREM PRIMOS DISTINTOS, ESTE NÃO SÃO COPRIMOS.

ENTÃO 1687 SÃO NÚMEROS COMPOSTOS.

b) $m = 2107,\ b = 7$

$7^{2106} = (7^6)^{351} = 1^{351} \equiv 1 \bmod 7$

$7^{2106} = (7^{42})^{50} \cdot 7^6 = (1)^{50} \cdot 7^6 = 1 \cdot 7^3 \cdot 7^3 = 343 \cdot 343$

$\equiv -1 \cdot -1 \bmod 43$

$\equiv 1 \bmod 43$

VEMOS QUE $7^{2106} - 1$ É DIVISÍVEL POR 7 E 43.
COMO ESTES SÃO PRIMOS DISTINTOS, SEGUE QUE SÃO COPRIMOS.
LOGO, $7^{2106} - 1$ É DIVISÍVEL PELO PRODUTO $7 \cdot 7 \cdot 43 = 2107$,
OU SEJA: $7^{2106} \equiv 1 \pmod{2107}$ ENTÃO 2107 NÃO É COMPOSTO.

b) SENDO p PRIMO E $a \in \mathbb{Z}$ NÃO DIVISÍVEL POR p.
MOSTRE QUE O INVERSO DE $\bar{a}$ EM $\mathbb{Z}_p$ É $\bar{a}^{p-2}$.

RESPOSTA: PARA $\bar{a}$ POSSUA INVERSO EM $\mathbb{Z}_p$ É NECESSÁRIO QUE,
$\text{MDC}(a, p) = 1$.

$ax + py = 1 \rightarrow ax - 1 = -py \rightarrow ax \equiv 1 \bmod p$

APLICANDO FERMAT

$a^{p-1+1} \equiv 1 \bmod p$

$a^{p-2} \equiv 1 \bmod p$

O INVERSO É $\bar{a}^{p-2}$