

Teoria de Números Computacional

_____ prova complementar _____

23 julho '09 _____

Justifique todas as suas respostas convenientemente.

É permitida a utilização de máquinas de calcular, `pari/gp`, e outros elementos de consulta.

1. Seja $n = 2^6 \cdot 123 + 1$. Verifique se passa o teste de Miller de base 2. Construa a sequência-B. O que pode dizer sobre a primalidade de n ?
2. Considere o número primo $p = 67$.
 - (a) Mostre que 3 não é raiz primitiva módulo p .
 - (b) Numa certa comunicação é usado o esquema Elgamal com a chave pública $(67, 2, 9)$ para a transmissão de uma certa mensagem. Encontre a mensagem cifrada correspondente à mensagem original $X = 23$.
3. Dê um exemplo de uma construção de chave pública RSA, revelando a chave privada. Nesse exemplo, cifre a mensagem $x = 3$.
4. Calcule o símbolo de Jacobi $\left(\frac{21}{235}\right)$.

Para representar $7 \bmod 5$: `Mod(7,5)`

Para atribuir $x \equiv 7 \bmod 5$: `x=Mod(7,5)`

Para calcular $6^{10} \bmod 11$: `Mod(6,11)^10`

Cálculo de inverso modular $5^{-1} \bmod 11$: `Mod(1/5,11)`

Teste de primalidade: `isprime(1001)`

Factorização: `factor(1024)`