Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

exame de época especial — 18 de julho de 2022

A duração da prova é de 180 minutos. Justifique todas as suas respostas convenientemente.

1. Mostre que 7 é o último dígito (na expansão decimal) de F_n, para $n \geq 2$. 2 valores

2. Para $n > 1$, mostre que $n \mid \varphi(2^n - 1)$.
   [Sugestão: Mostre, em primeiro lugar, que $\mathrm{ord}_{2^n-1} 2 = n$.] 2 valores

Das seguintes questões, resolva apenas ***três***

3. Verifique se $n = 2^5 \cdot 21 + 1$ passa o teste de Miller-Rabin de base 2. Construa a sequência-B. O que pode dizer sobre a primalidade de n? 2 valores

4. Considere o primo $p = 12347$. Mostre, usando o `sagemath` para determinar a ordem, que $r = 2$ é uma raiz primitiva de p. Crie uma chave ElGamal usando os parâmetros p e r. Use a chave pública e cifre a mensagem `mens=1234`. 2 valores

5. Calcule o símbolo de Jacobi $\left(\dfrac{a}{n}\right)$ onde $a = 2^4 \cdot 5 \cdot 17$ e $n = 7^3 \cdot 13 \cdot 19^2$. 2 valores

6. Verifique se existe um natural n para o qual $823127 \mid (n^2 - 75214)$, sabendo que 823127 é primo. 2 valores

Das seguintes questões, resolva apenas ***duas***

7. Use o método $(p-1)$–Pollard para encontrar um divisor não trivial de 14647. 2 valores

8. Encontre um factor não trivial de 200819 usando a factorização de Fermat. 2 valores

9. Use o método ρ–Pollard para encontrar um divisor não trivial de 1458943, usando a sequência pseudo-aleatória dada por $x_0 = 2$ e gerada da forma usual por $f(x) = x^2 + 1$. 2 valores

Resolva as questões seguintes apenas se não pretender manter a classificação obtida nos trabalhos e mini-testes.

1. Encontre o menor pseudoprimo forte de bases 2, 3 e 5, simultaneamente. Construa as respectivas sequências–B.

2. Foi usada a chave pública RSA

$$(115792089237316195457599221700781754228191164230176216121081051032181659403923, 5)$$

no envio de uma mensagem cifrada, interceptada como

$$c = 100300601001201201000600300 1.$$

Sabe-se que a chave pública foi criada a partir de dois primos "próximos". Use a factorização de Fermat para descobrir a mensagem original.