Universidade do Minho
Departamento de Matemática e Aplicações — lcc+lmat – 3° ano

Teoria de Números Computacional

exame – época especial — 22 de julho de 2016

A duração da prova é de 180 minutos.
Justifique todas as suas respostas convenientemente.
É permitida a utilização de máquinas de calcular.

Parte I

Das questões desta parte, resolva *apenas* 4 delas caso pretenda manter a sua classificação do trabalho/testePL, e 6 caso contrário.

1. Use o Algoritmo de factorização ρ-Pollard para encontrar um factor não trivial de 9797, usando a sucessão pseudo-aleatória dada por $x_0 = 2$ e $f(x) = x^2 + 1$.
   [Sugestão: $(26 - 5, 9797) = (7668 - 26, 9797) = 1, (5236 - 677, 9797) = 97$]

2. Use o algoritmo $(p-1)$–Pollard para encontrar um divisor não trivial de 799.
   [Sugestão: $(63, 799) = 1$ e $(612, 799) = 17$].

3. Verifique se 137 passa o teste de Miller-Rabin de base 2. O que pode concluir sobre a primalidade de 137? Construa a sequência-B gerada pelo algoritmo de Miller.

4. Use a factorização de Fermat para encontrar um divisor não trivial de $n = 6161$ (sabe-se que $\sqrt{n} \approx 78.4920378127616$).

5. Use o Teste de Lucas-Lehmer para números de Mersenne para verificar se $M_7 = 2^7 - 1$ é um primo de Mersenne.

6. Considere o primo $p = 61$. Sabendo que $r = 2$ é uma raiz primitiva módulo p, crie uma chave ElGamal usando os parâmetros p e r. Use a chave pública para cifrar a mensagem $m = 5$.

7. Foi interceptada a mensagem cifrada $c = 40$ numa comunicação que usava uma chave-pública RSA $(119, 5)$. Use o algoritmo da divisão trivial para calcular $\phi(119)$ e decifre a mensagem c.

8. Verifique se $n = 511$ passa o teste de primalidade de Solovay-Strassen de base 2.

Parte II

9. Mostre que $\phi(n)$ é par, para todo o natural $n > 2$.

10. Mostre que se n é um pseudo-primo fraco na base 2, então $N = 2^n - 1$ é um pseudo-primo forte na base 2.

11. Indique se existe solução para $x^2 \equiv 7411 \mod 9283$, sabendo que 9283 é primo.

12. Suponha que n é tal que $\mathbb{Z}_n^*$ é cíclico, e sejam r uma raiz primitiva módulo n e a e b tais que $(a, n) = (b, n) = 1$. Mostre que $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \mod \phi(n)$.

Cotação:
cada questão: 2 valores