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

Teoria de Números Computacional

teste — 6 de junho de 2016

A duração da prova é de 2 (duas) horas. Justifique todas as suas respostas convenientemente.
É permitida a utilização de máquinas de calcular.

Parte I

Das questões seguintes, resolva apenas 6.

1. Use o Algoritmo de factorização ρ-Pollard para encontrar um factor não trivial de 6887, usando a sucessão pseudo-aleatória dada por $x_0 = 2$ e $f(x) = x^2 + 1$.
[Sugestão: $(26 - 5, 6887) = (3788 - 26, 6887) = 1, (2229 - 677, 6887) = 97$].
2. Use o algoritmo $(p - 1)$–Pollard para encontrar um divisor não trivial de 391.
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 $n = 2911$ (sabe-se que $\sqrt{n} \approx 53.9536838408648$).
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 $p = 67$. 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 $c = 98$ numa comunicação que usava uma chave-pública RSA $(187, 3)$. Use o algoritmo da divisão trivial para calcular $\phi(187)$ e decifre a mensagem c.
8. Indique se existe solução para $x^2 \equiv 404 \mod 1031$, sabendo que 1031 é primo.

Parte II

9. Seja p um primo ímpar. Mostre que $\left(\frac{3}{p}\right) = 1$ se e só se p é da forma $12k + 1$ ou da forma $12k + 11$. Obtenha uma caracterização análoga para p por forma a que $\left(\frac{-3}{p}\right) = 1$.
10. Seja p um primo.
    (a) Dado um polinómio $f(x) \in \mathbb{Z}_p[x]$ com grau n, mostre que $f(x)$ tem no máximo n raizes incongruentes módulo p.
    [Sugestão: Mostre que $x^k - r^k = (x - r)(x^{k-1} + x^{k-2}r + \cdots + xr^{k-2} + r^{k-1})$. Agora repare que se x_0 for uma raiz de $f(x)$ então $f(x) \equiv f(x) - f(x_0) \mod p$. Deduza que existe $g(x)$ tal que $f(x) \equiv (x - x_0)g(x) \mod p$.]
    (b) Mostre que $x^n \equiv 1 \mod p$ tem no máximo $\phi(n)$ soluções que não são solução de $x^m \equiv 1 \mod p$, onde $m < n$.
    [Sugestão: Use a alínea anterior.]

Cotação:
cada questão: 2 valores