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

Teoria de Números Computacional

teste prático — 15 de junho de 2016

A duração da prova é de 90 minutos. Justifique todas as suas respostas convenientemente.

1. Encontre o menor pseudoprimo de Euler de bases 2, 3 e 5, simultaneamente. Verifique se passa o Teste de Miller de base 2. Construa a respectiva sequência–B

2. Foi usada a chave pública RSA

   $$(1157920892373161954575992217007817542281911642301762161210810510321816594039 23, 5)$$

   no envio de uma mensagem cifrada, interceptada como

   $$c = 100300601001201201000600 3001.$$

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

3. Suponha que tem à sua disposição uma máquina que permite efectuar operações aritméticas que não excedam 2^{35}. Calcule

   $$1237940039285 + 24758800785707605.$$