Folha **H** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Março de 2017

1. Quais são os números naturais menores do que 20 que são soma de dois quadrados inteiros? E de três quadrados? E de quatro quadrados?

2. Através do método de fatorização de Fermat, fatorize (a) 8633, (b) 809009, (c) 92296873 e (d) 4601.

3. Tente o teste de Miller-Rabin para 172947529 com as testemunhas 17, 3 e 23 (muitas contas... use o SAGE).

4. (a) Dado $a \in \mathbb{Z}$, mostre que $a^2 \not\equiv 3 \pmod 4$.
   (b) Mostre que nenhum natural na sequência (a notação é a decimal)

   $$11, 111, 1111, 11111, 111111, \ldots$$

   é um quadrado. (Calcule o resíduo módulo 4 de cada elemento desta sequência.)

5. Heloísa publica a sua chave pública RSA: (2038667,103), onde $n = 2038667$ é produto de dois primos distintos e $e = 103$ é o expoente encriptador. [Para fazer este exercício e o próximo utilize um computador.]

   (a) Abelardo quer enviar a mensagem $M = 892383$ à Heloísa. Que cifra é que ele envia?
   (b) Heloísa sabe que 1301 divide 2038667. Encontre o expoente decifrador d da Heloísa.
   (c) Faça os cálculos que permitem à Heloísa obter M a partir da cifra enviada por Abelardo.
   (d) Heloísa também recebe a cifra 317730 de Abelardo. Decifre esta mensagem.

6. Neste exercício, n é o produto de dois primos distintos. Calcule estes primos (usando um método descrito na aula) sabendo que

   (a) $n = 352717$ e $\varphi(n) = 351520$.
   (b) $n = 172205490419$ e $\varphi(n) = 172204660344$.