Folha **L** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Abril de 2017

1. (a) Seja K um corpo, $b \in K$ e $n \in \mathbb{N}$ ímpar. Mostre que
$$b^n + 1 = (b+1)(b^{n-1} - b^{n-2} + \dots b^2 - b + 1).$$
   (b) Um *primo de Fermat* é um primo da forma $2^n + 1$, com $n \in \mathbb{N}$. Mostre que se $2^n + 1$ é um primo de Fermat então n é uma potência de 2.
   (c) Seja $F_n = 2^{2^n} + 1$. Fermat conjeturou que todos os números desta forma são primos. De facto, F_0, F_1, F_2, F_3 e F_4 são primos (calcule-os!). Mas F_5 não é primo (vá à Wikipédia para ver a fatorização de F_5 obtida por Euler). Não se sabe se há mais primos de Fermat.

2. Seja p um primo de Fermat.
   (a) Mostre que cada não resíduo quadrático módulo p é um gerador de $(\mathbb{Z}/p\mathbb{Z})^*$.
   (b) Mostre que 5 é gerador de $(\mathbb{Z}/p\mathbb{Z})^*$, exceto quando $p = 5$.

3. Seja a um inteiro positivo e p e q primos ímpares com $p \perp a$ e $q \perp a$ tais que $p + q \equiv 0 \pmod{4a}$.
   (a) Mostre primeiro que se a é ímpar, então $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
   (b) Mostre que $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

4. (a) Dado um número natural k, então $\left(\frac{-3}{6k-1}\right) = -1$.
   (b) Seja n um número inteiro. Dado um número natural k, mostre que $6k-1$ não divide $n^2 + n + 1$. (Note que $4n^2 + 4n + 4 = (2n+1)^2 + 3$.)

5. Neste exercício use um computador (por exemplo, o programa SAGE).
   (a) Aplique o teste de Solovay-Strassen ao número 56052361 para várias bases. Que conclusão é que pode tirar?
   (b) Aplique o teste de Solovay-Strassen ao número 2301745249 para várias bases. Que conclusão é que pode tirar?
   (c) Aplique o teste de Solovay-Strassen ao número 7427466391 para várias bases. Que conclusão é que pode tirar?