Folha **F** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Março de 2017

1. Seja $n \in \mathbb{N}$. Mostre que se n e n^2+2 são primos então $n=3$. (Veja o problema 2.18 do livro e a sua solução.)
2. Dado $n \in \mathbb{N}$, mostre que a fração $\frac{12n+1}{30n+2}$ está em forma reduzida. (Veja exercício 2.24 do livro e a sua solução.)
3. Para que valores de n é que $\varphi(n)$ é ímpar?
4. Mostre que se $n > 4$ é um número composto então $(n-1)! \equiv 0 \pmod{n}$.
5. Tente o teste de Miller-Rabin para 561 com as bases 4, 5 e 7.
6. Tente o teste de Miller-Rabin para 1105 com as bases 2, 3 e 4.
7. Seja G um grupo comutativo e a e b elementos de G com ordens n e m respetivamente. Suponha que $n \perp m$. Mostre que a ordem de ab é nm. (Veja no livro, p. 42, ou consulte os seus apontamentos de Álgebra.)
8. Seja p primo ímpar tal que $(p-1)/2$ também é primo. Mostre que os elementos de $\mathbb{Z}_p^*$ têm ordens 1, 2, $(p-1)/2$ ou $p-1$.
9. Quantos geradores tem o grupo $\mathbb{Z}_{23}^*$? E $\mathbb{Z}_{27}^*$? E $\mathbb{Z}_{50}^*$? E $\mathbb{Z}_{21}^*$?
10. Seja G um grupo cíclico finito de cardinalidade n. Mostre que G tem $\varphi(n)$ geradores. (Mostre que se a gera G, então a^k gera G se, e somente se, $k \perp n$. Use a relação de Bézout.)
11. Por que razão os quadrados perfeitos são exceção na conjetura de Artin?
12. Seja $n \in \mathbb{N}$ com $n \neq 1$.
    (a) Dados $a, b \in \mathbb{N}$ e r o resto da divisão de a por b. Mostre que $n^r - 1$ é o resto da divisão de $n^a - 1$ por $n^b - 1$. (Use judiciosamente o facto de que $(c-1) \mid (c^k - 1)$, para $c, k \in \mathbb{N}$ e $c > 1$.)
    (b) Mostre que $\mathrm{mdc}(n^a - 1, n^b - 1) = n^{\mathrm{mdc}(a,b)} - 1$. (Pense no algoritmo de Euclides para calcular o máximo divisor comum.)