Folha **J** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Abril de 2017

1. Usando o critério de Euler, calcule $4^{48} \pmod{97}$. Note que 97 é primo.
2. Mostre que a equação $x^2 \equiv 5 \pmod{2^{13}-1}$ tem duas soluções nos naturais x com $x < 2^{13}$. (Note que $2^{13}-1$ é um número primo.)
3. Seja p um número primo ímpar. Use o facto do grupo $(\mathbb{Z}/p\mathbb{Z})^*$ ser cíclico para mostrar diretamente que $\left(\frac{-3}{p}\right) = 1$ quando $p \equiv 1 \pmod 3$. (Sugestão: há um elemento $c \in (\mathbb{Z}/p\mathbb{Z})^*$ de ordem 3 (justifique); mostre que $(2c+1)^2 = -3$.)
4. Seja p primo ímpar tal que $p \equiv 1 \pmod 5$. Mostre diretamente que $\left(\frac{5}{p}\right) = 1$ pelo método do exercício anterior. (Sugestão: tome-se $c \in (\mathbb{Z}/p\mathbb{Z})^*$ de ordem 5 e mostre que $(c+c^4)^2 + (c+c^4) - 1 = 0$, etc.)
5. Um primo de Mersenne é um primo da forma 2^n-1, com n número natural.
   (a) Mostre que se $2^n - 1$ é primo então n é primo.
   (b) Seja p um primo ímpar tal que $p \equiv 3 \pmod 4$. Suponha também que $2p+1$ primo. Mostre que $2^p \equiv 1 \pmod{2p+1}$. (Sugestão: calcule $\left(\frac{2}{2p+1}\right)$ de duas formas distintas.)
   (c) Mostre que $2^{251} - 1$ não é primo de Mersenne.
6. Mostre que 3 é um não resíduo quadrático módulo os primos de Mersenne maiores do que 3.
7. Seja p um primo ímpar. Mostre que o produto P de todos os resíduos quadráticos $\pmod p$ satisfaz $P \equiv (-1)^{(p+1)/2} \pmod p$. [Sugestão: se g é raíz primitiva módulo p, então g^2, g^4, g^6, ..., g^{p-1} são os resíduos quadráticos módulo p.]
8. Sejam $p_1, p_2, \ldots, p_r$ primos ímpares distintos e considere-se $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$.
   (a) Seja $F \subseteq \{1, 2, \ldots, r\}$. Mostre que existe $x_F \in \mathbb{Z}$ tal que $x_F \equiv 1 \pmod{p_i}$, for $i \in F$, and $x_F \equiv -1 \pmod{p_j}$, for $j \notin F$ $(1 \leq j \leq r)$.
   (b) Mostre que a equação $x^2 \equiv 1 \pmod n$ tem exatamente 2^r soluções.
   (c) Encontre as oito soluções de $x^2 \equiv 1 \pmod{105}$.