Folha **O** de exercícios

Fernando Ferreira

Introdução à Teoria dos Números
Maio de 2017

1. Mostre que toda a fração continuada (simples) infinita periódica representa um número irracional quadrático. [Sugestão: veja a página 112 do livro.]

2. Seja E a seguinte curva sobre elíptica sobre os racionais: $y^2 = x^3 + 17$. Considere os pontos $P = (-1, 4)$ e $Q = (2, 5)$.

   (a) Verifique que estes pontos estão na curva

   (b) Calcule $P + Q$ e $P - Q$.

   (c) Calcule $2Q$.

3. Uma solução racional da equação $y^2 = x^3 - 2$ é $(3, 5)$. Encontre uma solução racional com $x \neq 3$ considerendo a linha tangente a este ponto e computando o segundo ponto de interseção.

4. Seja E a seguinte curva elíptica sobre o corpo $\mathbb{Z}_{13}$: $y^2 = x^3 + 3x + 8$.

   (a) Verifique que os pontos $(1, 5)$, $(1, 8)$ e $(9, 7)$ estão na curva.

   (b) Liste os nove elementos de $E(\mathbb{Z}_{13})$. [Sugestão: para facilitar as contas (1) ache os quadrados de $\mathbb{Z}_{13}$; (2) percorra x com os valores de $\mathbb{Z}_{13}$ e veja quando os valores $x^3 + 3x + 8$ são quadrados; (3) não se esqueça do $\mathcal{O}$.]

   (c) Calcule $(1, 8) + (9, 7)$ e $(1, 5) + (1, 8)$.

5. Seja E a seguinte curva elíptica sobre os racionais: $y^2 = x^3 - 2x + 4$. Considere os pontos $P = (0, 2)$ e $Q = (1/4, 15/8)$.

   (a) Verifique que estes pontos estão na curva.

   (b) Calcule $P + Q$. Interprete o resultado geometricamente.

6. Seja E a curva elíptica sobre o corpo finito $K = \mathbb{Z}/5\mathbb{Z}$ definida pela equação $y^2 = x^3 + x + 1$.

   (a) Liste os nove elementos de $E(K)$.

   (b) Qual a estrutura de $E(K)$ como produto de grupos cíclicos?