Introdução à Teoria dos Números
Exame de 17 de junho de 2016. **9h - 11h30m**
Professor Fernando Ferreira

1. Seja n um número natural e suponha que 3 não divide n. Mostre que 3 divide $n^2 + 2$.
2. Calcule $6^{73} \pmod{100}$. Apresente os cálculos.
3. Encontre as quatro soluções (módulo 91) da equação $x^2 + x + 1 \equiv 0 \pmod{91}$. [Sugestão: trabalhe módulo 7 e 13 e use o teorema chinês dos restos (várias vezes).]
4. (a) Mostre que $\varphi(1000) = 400$.
   (b) Seja $a \in \mathbb{N}$ com $a \perp 10$. Mostre que a e de a^{2001} têm os mesmos três últimos dígitos em notação decimal. [Sugestão: calcule $a^{2001} \pmod{1000}$.]
5. Descreva o protocolo de envio de mensagem secreta El Gamal sobre o corpo $\mathbb{Z}_p$, onde p é primo. Em que é que se baseia a (presumível) segurança deste protocolo?
6. Calcule o símbolo de Legendre $\left(\frac{1001}{9907}\right)$ das seguintes duas maneiras:
   (a) Através da fatorização de 1001 (note que $1001 = 7 \times 11 \times 13$).
   (b) Usando o símbolo de Jacobi e, com isso, evitando fatorizar 1001.
   (c) O teste probabilístico de primalidade de Solovay-Strassen baseia-se no facto de que se p é um número primo e a é um natural co-primo com p, então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Explique por que razão esta igualdade (módulo p) pode ser verificada eficientemente. Com o que foi dito, é capaz de explicar como é que o teste funciona?
7. Seja α um número racional. Mostre que existe apenas um número finito de números racionais $\frac{a}{b}$ ($a \in \mathbb{Z}$, $b \in \mathbb{N}$) tais que
$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$$
8. Calcule o irracional quadrático dado pela fração continuada periódica $[6, \overline{2, 12}]$. Simplifique a resposta.
9. Considere a seguinte curva elíptica sobre $\mathbb{R}$: $y^2 = x^3 + \frac{1}{4}x$.
   (a) Esboce o gráfico desta curva.
   (b) Mostre que o ponto $(\frac{1}{2}, \frac{1}{2})$ tem ordem quatro.