Introdução à Teoria dos Números
Exame de 4 de julho de 2018. **9h - 11h30m**
Professor Fernando Ferreira

1. Diz-se que uma fração positiva $\frac{r}{s}$ está em forma reduzida se $r, s \in \mathbb{N}$ e $r \perp s$. Mostre que se $\frac{a}{b}$ e $\frac{c}{d}$ estão em forma reduzida e $\frac{a}{b} = \frac{c}{d}$, então $a = c$ e $b = d$.

2. (a) Calcule $3^{37} \pmod{53}$ usando o método da repetição do quadrado.
   (b) Calcule $3^{90} \pmod{53}$. (Sugestão: use o pequeno teorema de Fermat para reduzir à alínea anterior.)

3. Descreva o teste probabilílistico de primalidade Miller-Rabin. Nesta descrição aborde as seguintes questões: Se o número for primo, o teste garante que o é? Se o número não for primo, o teste garante que não o é? Se o número não for primo, o teste dá um factor?

4. Enuncie e demonstre o teorema de Wilson.

5. (a) Utilizando as leis da reciprocidade quadrática, calcule os símbolos de Legendre $\left(\frac{3}{13}\right)$ e $\left(\frac{8}{17}\right)$. Apresente os cálculos.
   (b) Deve ter obtido o valor 1 em ambos os símbolos de Legendre acima. Encontre, por tentativa e erro, os resíduos quadráticos de 3 módulo 13 e de 8 módulo 17.
   (c) A equação $x^2 \equiv 42 \pmod{221}$ tem solução. Justifique. (Note que $221 = 13 \times 17$.)
   (d) Encontre uma solução desta equação. Apresente os cálculos.

6. Calcule o símbolo de Jacobi $\left(\frac{6823}{26575}\right)$ (apresente os cálculos). Pode concluir que 6823 não é um quadrado módulo 26575? Justifique cuidadosamente a sua resposta.

7. Seja dado um número primo ímpar p. Mostrou-se que $p \equiv 1 \pmod{4}$ é condição necessária e suficiente para p ser soma de dois quadrados inteiros.
   (a) Mostre a necessidade da condição.
   (b) Suponha que n é um número natural tal que $n = x^2 + y^2$, com $x, y \in \mathbb{N}$ e $x \perp y$. Mostre que se p é um número primo tal que $p \equiv 3 \pmod{4}$, então $p \nmid n$. (Sugestão: raciocine por absurdo e trabalhe mod p.)

8. Seja θ o número irracional dado pela seguinte fração continuada simples infinite: $[1, 2, 1, 3, 1, 4, 1, 5, \ldots]$.
   (a) Calcule os convergentes c_3 e c_4 de θ. Apresente os cálculos.
   (b) Como se posiciona θ em relação aos dois números que encontrou na alínea anterior?

9. Considere a curva elíptica E sobre $\mathbb{Z}/3\mathbb{Z}$: $y^2 = x^3 + 2x + 1$.
   (a) O grupo $E(\mathbb{Z}/3\mathbb{Z})$ tem sete elementos. Liste-os.
   (b) Tome P um qualquer elemento do grupo $E(\mathbb{Z}/3\mathbb{Z})$ diferente do elemento neutro. Calcule $2P$ e $3P$. Apresente os cálculos.
   (c) Diga a que é igual $4P$. (Não necessita de efetuar cálculos para responder a esta questão.)