Introdução à Teoria dos Números
Exame de 3 de julho de 2017. **9h - 11h30m**
Professor Fernando Ferreira

1. Seja n um número inteiro ímpar que não seja múltiplo de 5. Mostre que $10|(n^2-1)$ ou $10|(n^2+1)$. [Note que apenas se tem que preocupar com a divisibilidade por 5.]

2. (a) Encontre um inteiro x tal que $x \equiv 1 \pmod{21}$ e $x \equiv 10 \pmod{33}$. [Sugestão: às tantas, divida por 3.]
   (b) Mostre que a condição $\text{mdc}(n,m)|(b-a)$ é suficiente para que o sistema de equações $x \equiv a \pmod{n}$ e $x \equiv b \pmod{m}$ tenha solução nos inteiros.

3. Diga, para cada uma das duas seguintes asserções, se ela é verdadeira ou falsa. Caso seja verdadeira, apresente uma demonstração. Caso seja falsa, apresente um contraexemplo.
   (a) Dados $a, b \in \mathbb{N}$, se $a^2|b^2$ então $a|b$.
   (b) Dados a, n números naturais com $n \neq 1$, tem-se $a^{\varphi(n)+1} \equiv a \pmod{n}$.

4. Descreva o teste de fatorização de Fermat e diga (e explique) para que números (compostos) é que ele pode ser útil.

5. Calcule o símbolo de Legendre $\left(\frac{26}{61}\right)$ de duas maneiras diferentes:
   (a) Usando as leis de reciprocidade quadrática.
   (b) Usando o critério de Euler e o método da repetição do quadrado para calcular a exponenciação modular.

6. Mostre que 166273 não é um quadrado módulo 26575. Justifique. [Pode assumir que $166273 \perp 26575$.]

7. (a) Mostre que $\left(\frac{1}{5}\right) + 2\left(\frac{2}{5}\right) + 3\left(\frac{3}{5}\right) + 4\left(\frac{4}{5}\right) = 0$.
   (b) Seja $p = 4k+1$ um número primo (onde k é um número natural).
      (b1) Mostre que, para $1 \leq a \leq p-1$, se tem $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$.
      (b2) Mostre que $\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = 0$.

8. Encontre a fração continuada simples de $\sqrt{15}$.

9. Considere a seguinte curva elíptica E sobre $\mathbb{Z}/5\mathbb{Z}$: $y^2 = x^3 + 1$.
   (a) O grupo $E(\mathbb{Z}/5\mathbb{Z})$ tem seis elementos. Liste-os.
   (b) O ponto $P = (2,2)$ deve aparecer na sua lista. Calcule $3P$ e note que não é o elemento zero de $E(\mathbb{Z}/5\mathbb{Z})$. Qual é a ordem de P no grupo $E(\mathbb{Z}/5\mathbb{Z})$?
   (c) Apresente a tabela de adição do grupo $E(\mathbb{Z}/5\mathbb{Z})$. [É uma tabela com trinta e seis entradas, mas nota que não tem que fazer mais contas...]