Introdução à Teoria dos Números
Exame de 4 de julho de 2016. **9h - 11h30m**
Professor Fernando Ferreira

1. Mostre que se p é um número primo congruente com 3 módulo 4, então p não é soma de dois quadrados.

2. Calcule $5^{25} \pmod{1019}$ pelo método da repetição do quadrado. Apresente os cálculos.

3. Encontre as soluções simultâneas das congruências: $x \equiv 13 \pmod{71}$ e $x \equiv 40 \pmod{97}$.

4. (a) Calcule $\varphi(25)$, $\varphi(41)$ e $\varphi(73)$.
   (b) Seja $n = 25 \times 41 \times 73 = 74825$ e considere a um número inteiro tal que $a \perp n$. Mostre que $a^{362} \equiv a^2 \pmod{74825}$. [Sugestão: note que 360 é múltiplo dos valores encontrados na alínea anterior.]

5. Seja n um número natural ímpar diferente de 1 e escreva-se $n-1 = 2^k q$, onde k é um número natural e q é ímpar. Tome-se a um número natural tal que $1 < a < n$. Seja $b = a^q \pmod{n}$. Considere a seguinte sequência de números módulo n:

$$b,\ b^2,\ b^4,\ \ldots,\ b^{2^{k-1}}$$

   (a) Mostre que se n é um número primo então ou esta sequência só tem 1's, ou então existe um -1 nesta sequência.
   (b) Descreva o teste probabilístico de primalidade de Miller-Rabin.

6. (a) Diga se 350 é um resíduo quadrático módulo 13? Justifique.
   (b) Diga se 12088 é um resíduo quadrático módulo 3825? Justifique.
   (c) Diga se 17638 é um resíduo quadrático módulo 15485863? Justifique.

7. Seja $\alpha = [a_0, a_1, a_2, \ldots]$ uma fração continuada infinita simples. Na aula teórica definimos os números inteiros p_n e q_n associados a esta fração continuada e mostrámos as seguintes duas igualdades: $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$ e $p_n q_{n-2} - q_n p_{n-2} = (-1)^n a_n$. Seja $c_n = \frac{p_n}{q_n}$.

   (a) Mostre que $c_0 < c_2 < c_4 < \ldots$ e que $\ldots < c_5 < c_3 < c_1$.
   (b) Mostre que, para todo o número natural n, $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$. [Pode assumir que os convergentes pares são sempre menores do que os convergentes ímpares.]

8. Encontre a fração continuada simples de $\sqrt{30}$.

9. Considere a seguinte curva elíptica sobre $\mathbb{Z}_{11}$: $y^2 = x^3 + 2x + 7$.

   (a) Enumere os elementos desta curva (são sete).
   (b) Dentro dos elementos acima, escolha um não nulo. Chame-o de P. Compute $2P$.
   (c) Dentro dos elementos acima, escolha agora um também não nulo e que nem seja P, nem $-P$, nem $2P$, nem $-2P$. Chame-o de Q. Compute $P + Q$.
   (d) A que é igual $3P$? (Não necessita de fazer contas.)