Introdução à Teoria dos Números
Exame de 16 de junho de 2018. **9h - 11h30m**
Professor Fernando Ferreira

1. Sejam $m, n, q \in \mathbb{N}$ números naturais tais que $m = q^2 n$. Seja p um número primo. Mostre que se p aparece exatamente um número ímpar de vezes na fatorização de m como produto de primos, então $p \mid n$.

2. (a) Resolva a equação $91x \equiv 84 \pmod{147}$. Apresente os cálculos. (Sugestão: divida por 7.)
   (b) Mostre que a equação $91x \equiv 84 \pmod{143}$ não tem soluções. (Note que $143 = 11 \times 13$.)

3. (a) Usando o teorema φ de Euler, mostre que $7^{445} \equiv 7^{45} \pmod{1000}$.
   (b) Calcule $7^{45} \pmod{1000}$ pelo método da repetição do quadrado.

4. Descreva o protocolo de troca de mensagens RSA. Por que razão este protocolo seria inseguro caso fosse fácil fatorizar números?

5. Enuncie e demonstre o critério de Euler para o símbolo de Legendre.

6. O número 206989 é produto de dois primos próximos.
   (a) Verifique que o valor do símbolo de Jacobi $\left(\frac{300}{206989}\right)$ é 1. Apresente os cálculos.
   (b) Fatorize 206989 pelo método de fatorização de Fermat. Apresente os cálculos. (Note que $\sqrt{206989} = 454,96\ldots$)
   (c) É 300 resíduo quadrático módulo 206989? Justifique.

7. Escreva de duas maneiras distintas o número racional $\frac{61}{27}$ como fração continuada simples finita. Apresente os cálculos.

8. Encontre a fração continuada simples de $1 + \frac{\sqrt{15}}{3}$. Apresente os cálculos.

9. Considere a curva elíptica $y^2 = x^3 - 2$ (uma curva de Bachet). Bachet encontrou uma fórmula que, dado um ponto de coordenadas racionais na curva, permite obter outro ponto de coordenadas racionais na curva. A fórmula obtém-se consideranto a tangente à curva no ponto dado. Neste exercício não se pede para encontrar a fórmula de Bachet. Pede-se o seguinte: sabendo que o ponto $(3, 5)$ está na curva, encontre outro ponto de coordenadas racionais, diferente de $(3, -5)$, que também esteja na curva.