Introdução à Teoria dos Números
Exame de 19 de junho de 2017. **9h - 11h30m**
Professor Fernando Ferreira

1. Enuncie e demonstre a fórmula do produto de Euler.

2. (a) Verifique que $1^5 + 2^5 + 3^5 + 4^5 \equiv 0 \pmod 5$.
   (b) Mostre que, para todo o número ímpar m diferente de 1, se tem
   $$1^m + 2^m + \cdots + (m-1)^m \equiv 0 \pmod m$$

3. Encontre um inteiro x tal que $2x \equiv 1 \pmod 3$, $3x \equiv 1 \pmod 5$ e $x \equiv 3 \pmod{43}$.

4. (a) Usando o teorema de Euler, mostre que $17^{185} \equiv 17^{57} \pmod{256}$.
   (b) Calcule $17^{57} \pmod{256}$ pelo método da repetição do quadrado.

5. Descreva o protocolo de troca de chaves Diffie-Hellman no grupo $(\mathbb{Z}/p\mathbb{Z})^*$ e, também, numa curva elíptica E sobre o corpo $\mathbb{Z}/p\mathbb{Z}$ (p é primo). Em que é que se baseia a (presumível) segurança deste(s) protocolo(s)?

6. (a) Mostre que $\left(\frac{27}{1763}\right) = 1$.
   (b) Mostre que o discriminante da equação quadrática $x^2 + 5x + 881 \equiv 0 \pmod{1763}$ é 27. Esta equação <u>não</u> tem, porém, solução. Explique como é que isto é possível.
   (c) Agora mostre mesmo que a equação da alínea anterior não tem soluções. (Note que $\sqrt{1763} = 41,9880....$ Para bom entendedor meia palavra basta.)

7. Seja p um primo da forma $p = 4m + 1$ ($m \in \mathbb{N}$).
   (a) Seja q um primo ímpar tal que $q|m$. Mostre que $\left(\frac{q}{p}\right) = 1$. (Use a lei da reciprocidade quadrática.)
   (b) Seja $d \in \mathbb{Z}$ tal que $d|m$. Mostre que $\left(\frac{d}{p}\right) = 1$.

8. Calcule o irracional quadrático dado pela fração continuada simples infinita $[2, \overline{12, 3}]$.

9. Considere a seguinte curva elíptica sobre $\mathbb{Z}/13\mathbb{Z}$: $y^2 = x^3 + 2x + 1$.
   (a) Esta curva elíptica tem 8 elementos. Enumere-os.
   (b) Os pontos $(8, 3)$ e $(1, 11)$ devem aparecer na sua lista. Calcule $(8, 3) + (1, 11)$. Apresente os cálculos.
   (c) Que pontos de E têm ordem 2? Justifique.