Departamento de Matemática da Universidade de Coimbra
Exame de Teoria dos Números
Licenciatura em Matemática

31 de Janeiro de 2011 Duração 2h30

Observação: Não é permitido o uso de calculadoras. Justifique resumidamente as afirmações que efectuar.

1. (a) Defina número primo.
   (b) Prove que todo o primo $p \neq 2$ é da forma $4n+1$ ou $4n+3$ para algum inteiro n.
   (c) Prove que se um número primo dividir um produto de números inteiros, tem que dividir pelo menos um dos factores.

2. (a) Enuncie e demonstre o teorema de Euler.
   (b) Tendo em conta a alínea (a), mostre que se p é um primo então $a^p \equiv a \pmod{p}$, para todo o inteiro a.
   (c) Mostre que se $(a, 10) = 1$ então os três últimos dígitos de a^{2001} são os mesmos de a.

3. (a) Sejam m um número natural e a, b, c inteiros. Prove que

$$ab \equiv ac \pmod{m} \Leftrightarrow b \equiv c \left(\operatorname{mod} \frac{m}{(a,m)}\right).$$

   (b) Resolva o sistema de congruências

$$3x \equiv 6 \pmod{12},\ 3x \equiv 1 \pmod{5}.$$

4. Mostre que se p é um número primo tal que $p \equiv 1 \pmod{4}$, então

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}.$$

5. Determine todas as soluções inteiras da equação linear diofantina $71x + 8448y = 1$.

6. Considere o sistema criptográfico de chave pública, e suponha que a chave pública é o par $n = 8633 = 89 \times 97$, $e = 71$. Qual é a transformação decifradora?