Universidade do Minho
Departamento de Matemática L.C.C. – 3° ano

# Teoria de Números Computacional

folha 0 — 2° semestre, 2008/2009

1. Seja $n = 10^{15} + 3$.

   (a) Execute `factor(n,200000)` e `factor` no Pari/GP. Comente os resultados.

   (b) Recorde o Pequeno Teorema de Fermat: $n$ primo implica $a^{n-1} \equiv 1 \mod n$, se $(a, n) = 1$. Considere $a = 2$. Verifique se a tese é satisfeita (ou seja, se $2^{n-1} \equiv 1 \mod n$.

   (c) Tome `a=Mod(2,n)`. Calcule `a^(n-1)`. O que pode dizer da primalidade de $n$?

   (d) Insira as instruções

   ```
   for (i = 2, ceil(sqrt(n)), if (n%i==0, print(i); break))
   ```

   Comente o resultado. Faça `##` para saber o tempo de execução.

   (e) Insira a instrução

   ```
   factor(n)
   ```

   Faça `##`. Comente o resultado.

2. Investigue os comandos

   ```
   forprime, fordiv, forstep, nextprime, precprime, gcd, lcm, bezout, chinese
   ```

3. Sejam $a = 2354, n = 3269$.

   (a) Verifique que $(a, n) = 1$.

   (b) Determine $a^{-1}$.