Universidade do Minho
Departamento de Matemática

L.E.M., L.M.C.C. – 4° ano
Mat. (Esp. Ensino), L.C.C. – 3° ano

Teoria de Números Computacional

exercícios de revisão — 2° semestre, 2006/2007

Parte I

1. Mostre que toda a função aritmética multiplicativa não identicamente nula fixa o 1.

2. Enuncie e demonstre o Critério de Euler.

3. Sabendo que

   - $\frac{7410}{2}$ e $\frac{9282}{2}$ são ímpares, mas que $\frac{116}{2}$ é par;
   - $9283 \equiv 1872 \mod 7411$;
   - $1872 = 2^4 \cdot 117$;
   - $7411 \equiv 40 \mod 117$;
   - a congruência $x^2 \equiv 2 \mod 117$ não tem soluções;
   - $117 \equiv 2 \mod 5$;

   calcule o símbolo de Legendre $\left(\frac{7411}{9283}\right)$

4. (a) Demonstre a validade do teste de primalidade de Lucas-Lehmer: se $n \in \mathbb{N}$ e existir $x \in \mathbb{N}$ para o qual $x^{n-1} \equiv 1 \mod n$ e $x^{\frac{n-1}{q}} \not\equiv 1 \mod n$ para todo o factor primo q de $n-1$, então n é primo. A x chamamos "testemunha" (testemunha a primalidade de n).

   (b) Use o teste de Lucas-Lehmer para mostrar que 449 é primo. Para tal, use 3 como "testemunha" e a factorização $449 - 1 = 2^6 \cdot 7$.

5. Considere $p = 37, r = 2, a = 5$.

   (a) Mostre que r é raíz primitiva de p.

   (b) Usando o parâmetro aleatório $k = 4$, calcule a mensagem cifrada correspondente a $P = 12$ usando o ElGamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.

Parte II

6. De alguma forma foi possível saber que $\phi(n) = 1512$, onde $n = 1591$ é o produto de dois primos distintos numa chave pública do RSA. Fazendo uso da Factorização de Fermat, encontre a factorização em primos de n.

7. Use o algoritmo ρ–Pollard, com a sequência pseudo-aleatória dada por $f(x) = x^2 + 1$ e $x_0 = 2$, para encontrar um factor não trivial de 8051.

8. Mostre que 2047 passa o teste de Miller de base 2.