Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

folha 6

1. Verifique se $x^2 \equiv a \mod p$ tem solução, com

   (a) $p = 431$, $a = 5$
   (b) $p = 419$, $a = 74$
   (c) $p = 337$, $a = 153$
   (d) $p = 373$, $a = 177$
   (e) $p = 463$, $a = 15$
   (f) $p = 317$, $a = 147$
   (g) $p = 379$, $a = 195$
   (h) $p = 397$, $a = 230$
   (i) $p = 461$, $a = 397$
   (j) $p = 331$, $a = 184$
   (k) $p = 467$, $a = 66$
   (l) $p = 307$, $a = 218$
   (m) $p = 409$, $a = 203$
   (n) $p = 449$, $a = 147$

2. Use o Lema de Gauss para calcular o símbolo de Legendre $\left(\frac{a}{p}\right)$, com

   (a) $a = 2, n = 11$
   (b) $a = 4, n = 11$
   (c) $a = 6, n = 43$
   (d) $a = 8, n = 23$
   (e) $a = 2, n = 17$
   (f) $a = 6, n = 13$
   (g) $a = 5, n = 41$
   (h) $a = 4, n = 23$
   (i) $a = 10, n = 13$
   (j) $a = 8, n = 23$
   (k) $a = 7, n = 11$
   (l) $a = 3, n = 37$

(m) $a = 10, n = 11$

(n) $a = 10, n = 23$

(o) $a = 8, n = 29$

(p) $a = 10, n = 37$

(q) $a = 5, n = 29$

(r) $a = 4, n = 41$

(s) $a = 4, n = 31$

3. Calcule o símbolo de Jacobi $\left(\frac{a}{n}\right)$, com

(a) $a = 275, n = 591$

(b) $a = 295, n = 591$

(c) $a = 200, n = 513$

(d) $a = 214, n = 447$

(e) $a = 2, n = 295$

(f) $a = 30, n = 343$

(g) $a = 124, n = 363$

(h) $a = 7, n = 589$

(i) $a = 172, n = 507$

(j) $a = 129, n = 269$

(k) $a = 69, n = 281$

(l) $a = 32, n = 259$

(m) $a = 92, n = 505$

(n) $a = 138, n = 331$

(o) $a = 10, n = 91$

(p) $a = 178, n = 449$

(q) $a = 92, n = 205$

(r) $a = 15, n = 121$

(s) $a = 203, n = 495$

(t) $a = 199, n = 423$

(u) $a = 222, n = 545$

(v) $a = 23, n = 601$

(w) $a = 107, n = 397$

(x) $a = 284, n = 587$

(y) $a = 5, n = 167$

(z) $a = 269, n = 571$

4. Verifique se n passa o teste de Solovay-Strassen na base a, com

   (a) $n = 679$, $a = 623$

   (b) $n = 253$, $a = 115$

   (c) $n = 801$, $a = 639$

   (d) $n = 867$, $a = 183$

   (e) $n = 539$, $a = 413$

   (f) $n = 925$, $a = 735$

   (g) $n = 747$, $a = 339$

   (h) $n = 201$, $a = 111$

   (i) $n = 533$, $a = 377$

5. Resolva as seguintes congruências:

   (a) $3x^{11} \equiv 6 \mod 29$, sabendo que 2 é raiz primitiva de 29.

   (b) $5x^{8} \equiv 10 \mod 31$, sabendo que 3 é raiz primitiva de 31, $\text{ind}_3 5 = 20, \text{ind}_3 2 = 24$.

   (c) $10^{x} \equiv 8 \mod 17$, sabendo que 3 é raiz primitiva de 17, $\text{ind}_3 2 = 14$.

   (d) $13^{x} \equiv 15 \mod 19$, sabendo que 2 é raiz primitiva de 19, $\text{ind}_2 3 = 13, \text{ind}_2 5 = 16$.