Universidade do Minho
Departamento de Matemática e Aplicações

lcc+lmat – 3° ano

Teoria de Números Computacional

folha 5

1. Determine
   (a) $\text{ord}_5 2$ (b) $\text{ord}_{13} 10$ (c) $\text{ord}_{10} 3$ (d) $\text{ord}_{10} 7$

2. Calcule
   (a) $\text{ord}_{11} 3$ (b) $\text{ord}_{17} 2$ (c) $\text{ord}_{21} 10$ (d) $\text{ord}_{25} 9$

3. Sejam $F_n = 2^{2^n} + 1$ o n-ésimo número de Fermat e p um factor primo de F_n.
   (a) Mostre que $\text{ord}_{F_n} 2 \mid 2^{n+1}$.
   (b) Mostre que $\text{ord}_p 2 = 2^{n+1}$.
   (c) Mostre que p é necessariamente da forma $2^{n+1}k + 1$.

4. Mostre que
   (a) 5 é uma raiz primitiva de 6;
   (b) 2 é uma raiz primitiva de 11.

5. Encontre uma raiz primitiva módulo cada um dos seguintes naturais:
   (a) 4 (b) 5 (c) 10 (d) 13 (e) 14 (f) 18

6. Mostre que 12 não tem raízes primitivas.

7. Mostre que 20 não tem raízes primitivas.

8. Mostre que se $(a, n) = 1$ então $\text{ord}_n a^{-1} = \text{ord}_n a$.

9. Mostre que se a, b são raízes primitivas módulo $p \neq 2$ primo então ab não é raiz primitiva módulo p.

10. Calcule, módulo 7,
    (a) $\text{ind}_5 2$
    (b) $\text{ind}_5 3$
    (c) $\text{ind}_5 6$
    (d) $\text{ind}_5 3^4$

11. Resolva a congruência quadrática $6x^{12} \equiv 11 \mod 17$. Para tal, resolva cada uma das alíneas seguintes:
    (a) Sabendo que $3^8 \equiv -1 \mod 17$, mostre que 3 é raiz primitiva módulo 17.
    (b) Mostre que $\text{ind}_3 11 = 7$ e que $\text{ind}_3 6 = 15$

(c) Construa a tabela dos índices de 3 módulo 17.

(d) Mostre que $6x^{12} \equiv 11 \mod 17$ se e só se $15 + 12\text{ind}_3 x \equiv 7 \mod 16$

(e) Resolva a congruência $15 + 12y \equiv 7 \mod 16$

(f) Deduza que $\text{ind}_3 x \equiv 2, 6, 10, 14 \mod 16$

12. Resolva a congruência $7^x \equiv 6 \mod 17$, sabendo que $\text{ind}_3 7 = 11$ e que $\text{ind}_3 6 = 15$.

13. Recorde o teste de primalidade de Lucas. Use-o para mostrar que 2003 é primo, com $x = 5$.

14. Usando a chave pública $(p, r, b) = (2551, 6, 33)$ de um sistema de chave pública Elgamal, cifre a mensagem 133. Sabendo que $a = 13$ é a chave privada, decifre $(421, 95)$.

15. Usando a chave pública $(p, r, b) = (370113067, 3, 161485623)$ de um sistema de chave pública Elgamal, cifre a mensagem 138616298. Decifre $(267037772, 234691095)$, sabendo que a chave privada é 164943214.

16. Calcule

    (a) $\left(\dfrac{3}{11}\right)$

    (b) $\left(\dfrac{8}{11}\right)$

    (c) $\left(\dfrac{24}{11}\right)$

    (d) $\left(\dfrac{9}{11}\right)$

    (e) $\left(\dfrac{72}{11}\right)$

    (f) $\left(\dfrac{21}{235}\right)$

    (g) Sabendo que $\left(\dfrac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, calcule $\left(\dfrac{101}{159}\right)$.

17. Mostre se existem soluções para as congruências

    (a) $x^2 \equiv 90 \mod 101$

    (b) $x^2 \equiv 123 \mod 401$

    (c) $x^2 \equiv 43 \mod 179$

    (d) $x^2 \equiv 1093 \mod 65537$