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

Teoria de Números Computacional

folha vii — 2° semestre, 2008/2009

1. A chave pública RSA de um certo sistema é $(n, e) = (2876155033, 2239091181)$.
   (a) Cifre
      i. 1234
      ii. 4321
      iii. 78632
      iv. 7123
   (b) Sabendo que 5639 é factor de n,
      i. encontre o expoente de decifração;
      ii. decifre
         A. 78623
         B. 276555
         C. 198722121

2. Foi usada uma chave pública RSA (n, e) e interceptada a mensagem cifrada y. Tente encontrar a mensagem original, onde
   (a) $(n, e) = (9342391600471856881, 516835009790341993)$, $y = 1487195269633179588$
   (b)
   $$(n, e) = (676336727842175563533660962584217646963245490776660319681548758400382932228 41, 2261982797471456753)$$
   e $y = 1487195269633179588$
   (c)
   $$(n, e) = (908894735529905782803257640498301136666389001809893257027882216321099397598 1, 2261982797471456753)$$
   e $y = 1487195269633179588$, sabendo que
   $$\phi(n) = 908894735529905782803257640498301136632604483130204606610449654556977486326 4$$

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

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

5. 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 $2^{n+1}k+1$.

6. Existe um método iterativo de ataque ao RSA denominado "cycling attack". Suponha que se conhece a chave pública (e,n) de uma cifra RSA e que se interceptou a mensagem cifrada C. Pretende-se obter a mensagem original P. Considere a sucessão $\{C_j\}$, com $1 \leq C_j < n$ definida por

$$C_1 \equiv C^e \mod n,\ C_{j+1} \equiv C_j^e \mod n.$$

   (a) Mostre que $C_j \equiv C^{e^j} \mod n$.

   (b) Mostre que existe j tal que $C_j = C$ e $C_{j-1} = P$.

   (c) Para $n = 47 \cdot 59$ e $e = 17$, encontre a mensagem cifrada em 1504.

7. Mostre que

   (a) 5 é uma raiz primitiva de 6;

   (b) 2 é uma raiz primitiva de 11.

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

9. Mostre que 12 não tem raízes primitivas.

10. Mostre que 20 não tem raízes primitivas.

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

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

13. Calcule, módulo 7,

   (a) $\text{ind}_5 2$

   (b) $\text{ind}_5 3$

   (c) $\text{ind}_5 6$

   (d) $\text{ind}_5 3^4$

14. 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 $\text{ind}_3 x \equiv 2, 6, 10, 14 \mod 16$

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

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

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

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

19. Calcule

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

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

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

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

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

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

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

20. 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) $x^2 \equiv 1093 \mod 65537$