Universidade do Minho

Departamento de Matemática | lcc+lmat – 3° ano

Teoria de Números Computacional

folha 4

1. Encontre um sistema reduzido de resíduos dos inteiros
   (a) 6 (b) 9 (c) 10 (d) 14 (e) 16 (f)17

2. Use o Teorema de Euler para encontrar o resto da divisão de 3^{100000} por 35.

3. Use o Teorema de Euler para encontrar o último algarismo de 7^{1000} na representação na base decimal.

4. Use o Teorema de Euler para encontrar o último símbolo na expansão hexadecimal de $5^{1000000}$.

5. Fazendo uso do Teorema de Euler, resolva as congruências lineares
   (a) $5x \equiv 3 \mod 14$ (b) $4x \equiv 7 \mod 15$ (c) $3x \equiv 5 \mod 16$

6. Calcule $\phi(n)$ para $13 \leq n \leq 20$.

7. Calcule $\phi(n)$ com $n =$
   (a) 100 (b) 256 (c) 1001 (d) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ (e) 10! (f) 20!

8. Mostre que existe uma infinidade de primos, usando a função ϕ de Euler.
   [Sugestão: suponha que o conjunto $\mathbb{P}$ dos números primos é finito, e considere $N = \prod_{p_i \in \mathbb{P}} p_i$. Conclua que $\phi(N) = 1$.]

9. Lehmer conjecturou que n é primo se $\phi(n)$ divide $n - 1$. Teste a conjectura.

10. Encontre um factor não trivial de
    (a) $2^{15} - 1$
    (b) $2^{91} - 1$
    (c) $2^{1001} - 1$

11. Use o algoritmo de Lucas-Lehmer para verificar se os números de Mersenne seguintes são primos:
    (a) M_7
    (b) M_{11}
    (c) M_{17}
    (d) M_{29}

12. Implemente o algoritmo de Lucas-Lehmer para primos de Mersenne.

13. Encontre os primos p e q, sabendo que $n = pq = 14647$ e $\phi(n) = 14400$.

14. Encontre os primos p e q, sabendo que $n = pq = 4386607$ e $\phi(n) = 4382136$.

15. Suponha que um criptanalista encontra um certo $k < n$ que não é primo relativo com $n = pq$ usado no RSA. Mostre que o criptanalista pode quebrar a cifra. Calcule a probabilidade de tal acontecer.

16. 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

17. Foi usada uma chave pública RSA (n, e) e interceptada a mensagem cifrada y. Tente encontrar a mensagem original, onde

    (a) $(n, e) = (9342391600471856881, 5168350097903419993)$, $y = 1487195269633179588$

    (b)

    $$(n, e) =$$
    $$(676336727842175563533660962584217646963245490776660319681548758400382932222841,$$
    $$2261982797471456753)$$

    e $y = 1487195269633179588$

    (c)

    $$(n, e) =$$
    $$(9088947355299057828032576404983011366663890018098932570278822163210993975981,$$
    $$2261982797471456753)$$

    e $y = 1487195269633179588$, sabendo que

    $$\phi(n) = 90889473552990578280325764049830113663260448313020460661044965455697748632 64$$

18. Existe um método iterativo de ataque ao RSA denominado “cycle 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.