Universidade do Minho
Departamento de Matemática e Aplicações Mestrado em Matemática e Computação

Temas de Álgebra - Algoritmos em Teoria de Números

exercícios — 1° semestre

1. Considere $p = 19, r = 2, a = 5$.
   (a) Mostre que r é raiz primitiva de p.
   (b) Usando o parâmetro aleatório $k = 4$, calcule a mensagem cifrada correspondente a $P = 6$ usando o sistema de chave pública Elgamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.
2. Considere $p = 31, r = 3, a = 5$.
   (a) Mostre que r é raiz primitiva de p.
   (b) Usando o parâmetro aleatório $k = 4$, calcule a mensagem cifrada correspondente a $P = 6$ usando o sistema de chave pública Elgamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.
3. Numa comunicação foi usado o esquema Elgamal com a chave pública $(37, 2, 22)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(2, 29)$. Sabendo que $\mathrm{ind}_2 22 = 31$ módulo 37, encontre a mensagem original.
4. Sabendo que $(e, n) = (411, 667)$ é uma chave pública RSA, use a factorização de Fermat para decifrar a mensagem interceptada $y = 375$.
5. Sabendo que $(e, n) = (5, 21971)$ é uma chave pública RSA, cifre a mensagem $P = 7$.
6. Calcule o símbolo de Jacobi $\left(\dfrac{7}{3^2 \cdot 13}\right)$.
7. Calcule o símbolo de Jacobi $\left(\dfrac{83}{235}\right)$.
8. Verifique se $n = 701$ passa o teste de primalidade de Solovay-Strassen de base 3. O que pode dizer sobre a primalidade de n?
9. Mostre que 25 é um pseudo-primo de Euler de base 7.
10. Verifique se existe solução para a congruência $x^2 \equiv 2^2 \cdot 3 \cdot 11 \mod 223$, sabendo que 223 é primo.
11. Uma certa chave pública RSA é $(n, e) = (1520273, 575843)$, onde n é o produto de dois primos distintos e e é o expoente de cifração. Usando a factorização de Fermat, calcule $\phi(n)$. Se a mensagem 1218147 for interceptada por uma terceira pessoa, indique a forma como esta poderá obter a mensagem original.
12. Use a factorização de Fermat para encontrar um divisor não trivial de $n = 1643$.
13. Encontre um factor não trivial de 200819 usando a factorização de Fermat.
14. Verifique se $n = 727$ passa o teste de primalidade de Solovay-Strassen de base 3. O que pode dizer sobre a primalidade de n?
15. Calcule uma raiz primitiva de $\mathbb{Z}_p^*$, com $p = 21401101277$.
16. Mostre que $\left(\frac{761067}{1000033}\right) = 1$. Calcule uma raiz quadrada de 761067 módulo 1000033.
17. Mostre que $\mathbb{Z}_{13}^*$ é grupo multiplicativo cíclico. Calcule o número de raizes primitivas de $\mathbb{Z}_{13}^*$.
18. Calcule

(a) a raiz quadrada de 3 módulo 181;

(b) a raiz quadrada de 3 módulo 107.

19. Dado o primo $p = 76022987$, construa uma curva elíptica E sobre $\mathbb{Z}_p$ e implemente o protocolo de troca de chaves Diffie-Hellman em E.

20. Dado o primo $p = 60068563$, considere a curva elíptica $E : y^2 = x^3 + 56249671822x + 80819652625$ sobre $\mathbb{Z}_p$.

    (a) Calcule a ordem do grupo aditivo E. Verifique o teorema de Hasse.

    (b) Da forma usual, conversa `mens=2011` num ponto em E.

    (c) Construa uma chave pública Elgamal em E e cifre `mens`.

    (d) Verifique que a decifração do ponto que encontrou na alínea anterior corresponde a `mens`.

21. Considere a curva elíptica $E : y^2 = x^3 + 1164x + 4366$ sobre $\mathbb{Z}_{6151}$. Para $P = (497 : 4447 : 1) \in E$,

    (a) mostre que $E = \langle P \rangle$;

    (b) para $(k, a) = (4917, 1933)$, use o sistema Menezes-Vanstone para cifrar `mens=(213, 981)`;

    (c) conhecendo a chave privada, decifre o que obteve na alínea anterior.

22. Factorize, usando o método de Lenstra, o número $n = 63109$, usando a curva elíptica $E : y^2 = x^3 + 618x + 19471$ sobre $\mathbb{Z}_n$, e $P = [60863 : 27581 : 1] \in E$.

23. Factorize, usando o método de Lenstra, o número $n = 60291151$, usando a curva elíptica $E : y^2 = x^3 + 50920988x + 36385079$ sobre $\mathbb{Z}_n$, e $P = [14060140 : 18308124 : 1] \in E$.

24. Factorize, usando o método de Lenstra, o número $n = 3551$.

25. Mostre que de facto 37 passa o teste de Goldwasser-Kilian, tomando a curva elíptica $E : y^2 = x^3 + 31x$ sobre $\mathbb{Z}_{37}$, e $P = [20 : 31 : 1] \in E$.

26. Use o teste de Goldwasser-Kilian para aferir da primalidade de $n = 29$, usando a curva elíptica E dada por $y^2 = x^3 + 3x$ sobre $\mathbb{Z}_{29}$ e $(3, 23) \in E$.

27. Alice e Bob pretendem trocar chaves, usando o protocolo de troca de chave de Diffie-Helmann em curvas elípticas. Para tal, acordaram o uso da curva elíptica E definida por $y^2 = x^3 + 8880x + 4439$ sobre $\mathbb{Z}_{10007}$ e em $P = (4944 : 7683 : 1) \in E$. Calcule uma possível chave.

28. Considere a curva elíptica $E : y^2 = x^3 + 56249671822x + 80819652625$ sobre os inteiros módulo 100212232259.

    (a) Verifique que o teorema de Hasse é satisfeito.

    (b) Da forma usual, converta `mens=1000` num ponto em E.

    (c) Construa uma chave pública Elgamal em E e cifre `mens`.

    (d) Verifique que a decifração do ponto que encontrou na alínea anterior corresponde a `mens`.

29. Considere a curva elíptica $E : y^2 = x^3 + 1214x + 912$ sobre os inteiros módulo 10007. Para $P = (6771, 8564)$,

    (a) mostre que $P \in E$;

    (b) mostre que $E = \langle P \rangle$;

    (c) usando parâmetros à sua escolha, use o sistema Menezes-Vanstone para cifrar `mens=(5131, 9)`;

    (d) conhecendo a chave privada, decifre o que obteve na alínea anterior.

30. Considere os primos $p = 2243, q = 3779$, $n = pq$, $b = 1638$. Considere o sistema de chave pública KMOV-I com chave pública (n, e), com $e = 381001$.

    (a) Cifre a mensagem $M = (3706172, 7850557)$.

    (b) Decifre a mensagem recebida $C = (3444572, 279177)$.

31. Dispondo do sistema de assinatura digital KMOV de tipo 0 de chave pública $(n, e) = (86747, 1237)$ que Alice criou, usando a curva elítpica definida por $y^2 = x^3 + 36225x + 60571$ sobre os inteiros módulo $n = 223 * 389$,

    (a) assine a mensagem $(49623, 13201)$,

    (b) averigue a autenticidade da mensagem que Alice enviou Bob: $(49623, 13201)$ com assinatura $(84679, 40971)$.

32. Use o teste de Goldwasser-Kilian para aferir da primalidade de $n = 97$, usado a curva elíptica E dada por $y^2 = x^3 + 75x + 38$ e $P = (39 : 69 : 1) \in E$.

33. Alice e Bob pretendem trocar chaves, usando o protocolo de troca de chave de Diffie-Helmann em curvas elípticas. Para tal, acordaram o uso da curva elíptica E definida por $y^2 = x^3 + 11550x + 2848$ sobre $\mathbb{Z}_{12143}$ e em $P = (9375 : 10958 : 1) \in E$. Calcule uma possível chave.

34. Considere a curva elíptica definida por $y^2 = x^3 + 34873x + 55097$ sobre os inteiros módulo 61129 e $P = (60016 : 51678 : 1) \in E$. Considere a chave pública Elgamal (E, P, Q) com $Q = rP = (49480 : 14059 : 1)$, para algum r.

    (a) Cifre a mensagem mens= 1012 (não se esqueça que em primeiro lugar tem que converter mens num ponto da curva elíptica P em E).

    (b) Sabendo que $r = 24469$ é a chave privada, verifique a validade da assinatura digital, para este sistema, da mensagem $M = (55356 : 58151 : 1)$ e assinatura $[(31786 : 38557 : 1), (26123 : 23944 : 1)]$.

35. Considere o primo $p = 897223$. Defina uma curva elíptica E sobre os inteiros módulo p. Usando parâmetros à sua escolha, use o sistema Menezes-Vanstone para cifrar mens=$(501, 1112)$ na curva elíptica E. Conhecendo a chave privada, decifre o que cifrou.

36. Considere os primos $p = 8363$, $q = 1013$, e $n = pq$, $b = 59$. Considere o sistema de chave pública KMOV-I com chave pública (n, e), com $e = 934475$. Cifre a mensagem $M = (3341377, 6580911)$. Decifre a mensagem recebida $C = (2568949, 958190)$.

37. Dispondo do sistema de assinatura digital KMOV de tipo 0 de chave pública $(n, e) = (103973, 3137)$ que Alice criou, usando a curva elítpica definida por $y^2 = x^3 + 78134x + 30243$ sobre $\mathbb{Z}_n$, averigue a autenticidade da mensagem que Alice enviou Bob: $(9867, 56262)$ com assinatura $(16689, 60734)$.

38. Alice e Bob acordaram na curva elíptica E definida por $y^2 = x^3 + 1234x + 123452470$ sobre $\mathbb{Z}_{123456791}$ e em $P = (3322393 : 96597749 : 1) \in E$. Irão usar o protocolo de Massey-Omura. Explique como pode Alice enviar a mensagem `mens=1002` a Bob. Determine o texto cifrado e descreva todos os passos que seguiu, supondo que a forma de transformar a mensagem no ponto da curva elíptica é a proposta por Koblitz.