Instituto Superior Técnico - TagusPark
Matemática Discreta 2020/2021
Exercícios para as aulas de problemas e teorico-práticas

Lista 8

Após a aula teorico-prática e a de problemas da semana em que a lista foi publicada, os alunos deverão tentar resolver todos os exercícios que não foram resolvidos nas aulas. Se tiverem dificuldades ou dúvidas deverão contactar os docentes da disciplina. Vários dos exercícios (ou muito semelhantes) são apresentados como exemplos ou exercícios resolvidos nos Capítulo 2 e 3 do livro.

1 Calendário perpétuo

1. Determine o dia da semana correspondente à data[1]:
   (a) 14 de Agosto de 1385 (batalha de Aljubarrota)
   (b) 8 de Julho de 1497 (partida de Vasco da Gama para a Índia)
   (c) 22 de Abril de 1500 (chegada de Pedro Álvares Cabral ao atual Brasil)
   (d) 1 de novembro de 1755 (grande terramoto de Lisboa)
   (e) 6 de junho de 1944 (invasão da Normandia durante a II Guerra Mundial)
   (f) 25 de abril de 1974
   (g) dia de Natal em 2030
   (h) a data do seu aniversário em 2050

   Pode confirmar respostas em `http://www.onlineunitconversion.com/julian_date.html` e `https://www.fourmilab.ch/documents/calendar` por exemplo.
2. Quais são os meses de 2022 em que o dia 13 calha num domingo?
3. Quantas sextas-feiras 13 existem em 2022?

2 Sistema criptográfico RSA

1. Considere o sistema criptográfico de chave pública RSA. Determine um par de chaves (chave pública e chave privada) supondo que se consideram os primos
   (a) $p = 23$ e $q = 61$; (b) $p = 41$ e $q = 53$; (c) $p = 47$ e $q = 89$.
2. Considere o sistema criptográfico de chave pública RSA com primos $p = 23$ e $q = 29$.
   (a) Mostre que $(667, 15)$ e $(667, 575)$ podem constituir um par de chave pública e chave privada, respetivamente, neste sistema.

[1] Várias alíneas deste exercício resolvidas na aula teorico-prática 7 (19 de Abril).

(b) Vai enviar-se uma encriptação do número de cartão de crédito temporário 9882505757262927 para uma entidade que disponibilizou a chave pública indicada em (a). O número deve ser separado em blocos de 2 dígitos e a encriptação de cada bloco efetuada separadamente. Calcule a encriptação de cada um dos blocos de forma eficiente[2].

3. Repita o exercício 2 com $p=59$, $q=83$, e chaves pública e privada $(4897, 21)$ e $(4897, 453)$, respetivamente.

4. Considere o sistema criptográfico de chave pública RSA com primos $p = 13$ e $q = 11$.

   (a) Explique porque $(143, 103)$ é uma chave pública possível neste sistema. Qual é a chave privada correspondente?

   (b) Vai enviar-se uma encriptação do número de cartão de crédito temporário 5482440387222034 para uma entidade que disponibilizou a chave pública indicada em (a). O número deve ser separado em blocos de 2 dígitos e a encriptação de cada bloco efetuada separadamente. Calcule a encriptação de cada um dos blocos de forma eficiente[2].

5. Uma *password* vai ser enviada eletronicamente recorrendo ao sistema criptográfico RSA. Para esse efeito, após serem escolhidos os primos $p = 19$ e $q = 67$ é gerada a chave pública $(1273, 25)$, que é divulgada, e a chave privada correspondente, que é mantida em sigilo.

   (a) Apresente a chave privada correspondente à chave pública referida.

   (b) Supondo que a *password* é 984563 e que se deve encriptar em blocos de 2 dígitos, calcule a encriptação de cada um dos blocos de forma eficiente[2].

6. Considere o sistema criptográfico de chave pública RSA com primos $p = 23$ e $q = 41$.

   (a) Explique porque $(943, 21)$ é uma chave pública possível neste sistema. Qual é a chave privada correspondente?

   (b) Vai enviar-se uma encriptação do número de cartão de crédito temporário 548506012807651 para uma entidade que disponibilizou a chave pública indicada em (a). O número deve ser separado em blocos de 3 dígitos e a encriptação de cada bloco efetuada separadamente. Calcule a encriptação de cada um dos blocos de forma eficiente[2].

7. Repita o exercício 6 com $p = 47$ e $q = 61$, chave pública $(2867, 17)$ e número de cartão de crédito 4532440306227148.

8. Considere o sistema criptográfico de chave pública RSA com $p = 17$, $q = 37$ e chave pública $(629, 395)$, e assuma que se usa a encriptação de números de cartão de crédito descrita no exercício 6. Suponha que a entidade que disponibilizou esta chave pública recebeu a seguinte encriptação (com esta chave) de um número de cartão de crédito temporário: 359 552 12 538 156 533.

   (a) Que chave privada correspondente à chave pública $(629, 395)$ gerou a entidade em causa?

   (b) Desencripte, de forma eficiente, os valores indicados para obter o número do cartão de crédito.

9. Repita o exercício 8 com $p=19$, $q=47$, chave pública $(893, 265)$ e 75 461 748 766 614.

10. Considere o sistema criptográfico de chave pública RSA com $p = 83$, $q = 109$, e chave pública $(9047, 23)$.

    (a) Qual a chave privada correspondente à chave pública $(9047, 23)$?

    (b) De forma eficiente, encripte a mensagem MEET ME AT IST TOMORROW, dividindo-a previamente em blocos de duas letras (ignore os espaços em branco e duplique a última letra) e usando a codificação das letras do alfabeto abaixo indicada. Cada bloco é encriptado separadamente.

[2]Ou seja, recorrendo às propriedades das congruências e calculando apenas quadrados de base inferior a $p \times q$ e produtos com fatores inferiores a $p \times q$.

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	***branco***			
80	81	82	83	84	85	86	87	88	89	90	32			

Código ASCII do alfabeto latino

11. Considere os números primos do exercício 10, mas agora com chave pública $(9047, 2725)$. Suponha que 9011135463504600 corresponde à encriptação com esta chave de uma mensagem (em língua inglesa) em blocos de 2 letras e ignorando espaços, previamente traduzida para valores numéricos de acordo com a tabela acima. Qual é a chave privada correspondente à chave pública $(9047, 2725)$? De forma eficiente, desencripte a mensagem encriptada para obter a mensagem original.

3 Transformada de Fourier Discreta e FFT

1. Usando o algoritmo FFT calcule a transformada de Fourier discreta dos vetores seguintes e indique o significado dos valores obtidos[3]:

   (a) $(1, 1, 2, 0)$ (b) $(-2, 5, 0, 1)$ (c) $(3, 0, 1, 4)$ (d) $(1, 4, 0, 2)$ (e) $(2, 3, 0, 0)$
   (f) $(1, 0, 4, 0)$ (g) $(-6, 0, 3, 0)$ (h) $(8, -5, 0, 0)$ (i) $(1, -2, 1, 5, 2, 0, 0, 1)$

2. Usando o algoritmo FFT calcule a transformada de Fourier discreta inversa dos vetores seguintes e indique o significado dos valores obtidos[4]:

   (a) $(1, 0, 1, 1)$
   (b) $(0, i, 1, 1)$
   (c) $(0, 4i, -4, -4i)$
   (d) $(4, -1 + i, 2, -1 - i)$
   (e) $(4, -2 + 4i, -8, -2 - 4i)$
   (f) $(-2, -3 - 3i, 0, -3 + 3i)$
   (g) $(25, -6 - 9i, -5, -6 + 9i)$

3. Usando o algoritmo FFT calcule[4]

   (a) $(n + 1)(n + 2)$
   (b) $(3n^2 - 6)(-5n + 8)$
   (c) $(3n + 2)(4n^2 + 1)$
   (d) $(n^2 + 2n - 1)(-n + 1)$
   (e) $(n^2 - 2)(n + 1)$
   (f) $(2n^2 + n + 1)(-5n - 2)$
   (g) $(n^3 + n + 1)(n^4 + n^2 + 1)$
   (h) $(n^2 + n + 1)(4n^3 + 5n - 2)$

4. Mostre que o número t_r de operações aritméticas executado pelo algoritmo FFT para calcular a transformada de Fourier discreta de um vector X de dimensão r é $O(r \log_2 r)$.

   Sugestão: Recorde que r é uma potência de 2, e faça um raciocínio semelhante ao apresentado no exercício 1.5 da lista de exercícios 5. Nomeadamente, comece por concluir que, denotando por t_r o número de operações aritméticas necessárias para calcular recursivamente $\mathcal{F}_k X$ $(r = 2^k)$, então $t_1 = 0$ e $t_r = 2t_{r/2} + \frac{3}{2}r$ para $r > 1$; proceda depois como no exercício referido para concluir que $t_r = \frac{3}{2} r \log_2 r$.

[3] Várias alíneas deste exercício resolvidas na aula teorico-prática 8 e início da aula teórica 15 (26 de Abril).
[4] Várias alíneas deste exercício resolvidas na aula teórica 16.