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

Lista 7

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 no Capítulo 2 do livro (alguns de entre eles estão explicitamente indicados abaixo).

1 Resolução de congruências

1. Para cada uma das congruências seguintes: (i) determine se tem ou não solução; (ii) em caso afirmativo, indique *uma* solução e, depois, o conjunto de *todas* as soluções

   (a) $5x \equiv_7 3$ (c) $7x \equiv_9 1$ (e) $34x \equiv_{16} 8$ (g) $21x \equiv_{38} 4$ (i) $131x \equiv_{77} 21$ (k) $-12x \equiv_{23} 4$

   (b) $8x \equiv_{12} 2$ (d) $12x \equiv_9 6$ (f) $14x \equiv_{18} 4$ (h) $39x \equiv_{65} 26$ (j) $249x \equiv_{18} 84$ (l) $13x \equiv_{15} -20$

   Use o *WolframAlpha* para confirmar os resultados, com `(αx mod n)=β`. Se avaliar `(5x mod 7)=3` obtém a resposta à alínea (a). Notar que β tem de ser um natural menor que `n` e `n` um natural positivo. Como existem várias formas equivalentes de apresentar a resposta, a expressão obtida pode não ser exatamente igual à que calculou.

2. Calcule, se existir, *um* inverso de a módulo n quando

   (a) $a = 6$ e $n = 8$ (c) $a = 7$ e $n = 9$ (e) $a = -4$ e $n = 7$ (g) $a = -126$ e $n = 245$

   (b) $a = 5$ e $n = 7$ (d) $a = 54$ e $n = 7$ (f) $a = 21$ e $n = 102$ (h) $a = 240$ e $n = 321$

3. Para cada uma das alíneas do exercício 2 indique, quando existirem, *todos* os inversos de a módulo n.

2 Resolução de sistemas de congruências

1. Calcule todas as soluções dos sistemas de congruências seguintes, se existirem:

(a) $\begin{cases} x \equiv_8 3 \\ x \equiv_9 4 \end{cases}$ (b) $\begin{cases} 4x \equiv_7 3 \\ x \equiv_6 9 \end{cases}$ (c) $\begin{cases} 5x \equiv_{10} 7 \\ 12x \equiv_9 3 \end{cases}$

(d) $\begin{cases} x \equiv_3 2 \\ x \equiv_4 3 \\ x \equiv_5 4 \end{cases}$ (e) $\begin{cases} x \equiv_5 3 \\ x \equiv_7 2 \\ x \equiv_8 5 \end{cases}$ (f) $\begin{cases} x \equiv_4 3 \\ x \equiv_7 6 \\ x \equiv_{11} 2 \end{cases}$

(g) $\begin{cases} x \equiv_7 2 \\ x \equiv_9 5 \\ x \equiv_{10} 6 \end{cases}$ (h) $\begin{cases} x \equiv_5 -2 \\ x \equiv_{14} 2 \\ x \equiv_{27} 3 \end{cases}$ (i) $\begin{cases} x - 1 \equiv_3 1 \\ x \equiv_5 9 \\ 2x \equiv_8 6 \end{cases}$

(j) $\begin{cases} 2x & \equiv_8 & 6 \\ 6x & \equiv_{11} & 1 \\ 24x & \equiv_{28} & 16 \end{cases}$ (k) $\begin{cases} 8x & \equiv_{11} & 5 \\ 10x & \equiv_{14} & 4 \\ 5x & \equiv_{20} & 15 \end{cases}$ (l) $\begin{cases} 3x & \equiv_8 & 7 \\ 2x & \equiv_{14} & 4 \\ 6x & \equiv_{15} & 18 \end{cases}$

(m) $\begin{cases} x & \equiv_5 & 2 \\ x & \equiv_7 & 5 \\ x & \equiv_8 & 3 \\ x & \equiv_9 & 1 \end{cases}$ (n) $\begin{cases} x & \equiv_3 & 1 \\ 2x & \equiv_7 & 3 \\ x & \equiv_{10} & 1 \\ x & \equiv_{11} & 2 \end{cases}$ (o) $\begin{cases} x & \equiv_7 & 2 \\ 5x & \equiv_{17} & 2 \\ 2x & \equiv_{20} & 6 \\ x & \equiv_{27} & 1 \end{cases}$

Use o *WolframAlpha* para confirmar os resultados. Para representar $\alpha x+\gamma \equiv_n \beta$, escreva `(`$\alpha$`x+`$\gamma$`)mod n=`$\beta$ onde β tem de ser um natural menor que `n` e `n` um natural positivo. Se avaliar `x mod 3=2, x mod 4=3, x mod 5=4` obtém uma resposta à alínea (d). Note que existem várias formas equivalentes de apresentar a resposta.

2. Use a generalização do teorema chinês dos restos estudada para resolver os sistemas, se existir solução

(a) $\begin{cases} x & \equiv_5 & 2 \\ x & \equiv_8 & 2 \\ x & \equiv_{12} & 10 \end{cases}$ (b) $\begin{cases} x & \equiv_3 & 2 \\ x & \equiv_4 & 3 \\ x & \equiv_{15} & 14 \end{cases}$ (c) $\begin{cases} x & \equiv_4 & 2 \\ x & \equiv_6 & 4 \\ x & \equiv_{18} & 10 \end{cases}$ (d) $\begin{cases} x & \equiv_{10} & 2 \\ x & \equiv_{18} & 4 \\ x & \equiv_{20} & 12 \end{cases}$

(e) $\begin{cases} 4x & \equiv_9 & 2 \\ x+2 & \equiv_{10} & 8 \\ x & \equiv_{21} & 2 \end{cases}$ (f) $\begin{cases} 16x & \equiv_6 & 14 \\ 3x & \equiv_{12} & 21 \\ 12x & \equiv_{15} & 7 \end{cases}$ (g) $\begin{cases} 4x & \equiv_{12} & 8 \\ 5x & \equiv_{18} & 7 \\ 7x & \equiv_{36} & -1 \end{cases}$ (h) $\begin{cases} 30x & \equiv_{32} & 12 \\ 20x & \equiv_{25} & 10 \\ x & \equiv_6 & 4 \end{cases}$

3. Recorrendo ao teorema chinês dos restos encontre o mais pequeno inteiro positivo que

   (a) dá restos 3, 3 e 2 quando dividido por 4, 7 e 11, respetivamente.

   (b) dá resto 2 quando dividido por 7, resto 5 quando o seu triplo é dividido por 8 e resto 6 quando o seu dobro é dividido por 11.

   (c) dá restos 5, 4, 3 e 2 quando divididos por 6, 5, 4 e 3, respetivamente. (Livro: exercício página 127)

4. O teorema chinês dos restos tem aplicações em Astronomia, como por exemplo o cálculo das conjunções de planetas e Sol, das conjunções das luas e respetivos planetas e datas dos eclipses. Sabendo que os cometas 2P/Encke, 4P/Faye e 8P/Tuttle têm períodos orbitais de 2 anos, 7 anos e 11 anos, respetivamente, e que as últimas passagens destes cometas pelo seu periélio (ponto da órbita mais próximo do Sol) foram em 2017, 2014, e 2008, respectivamente, calcule quando atingem os três cometas os seus periélios no mesmo ano. Assuma que os períodos orbitais são constantes. Qual o ano futuro mais próximo?

5. Uma tripulação de 17 piratas dividiu equitativamente entre si o seu tesouro em moedas de ouro tendo sobrado 3 moedas. Depois, num confronto com um galeão espanhol, morreu um pirata. A sua parte, conjuntamente com estas 3 moedas, foi dividida irmãmente, tendo sobejado 10 moedas. Na disputa destas moedas, mais um dos piratas morreu, tendo o seu dinheiro, conjuntamente com as 10 moedas, sido distribuído equitativamente e não tendo sobrado nenhuma. Qual é, em moedas ouro, a mais pequena fortuna dos piratas? (Livro: página 109)

6. O oráculo dos ossos da dinastia chinesa Shang, no século 15a.C., contava os dias de 3 maneiras diferentes: em ciclos de 7 dias, digamos, para simplificar, de domingo (0) a sábado (6), e, ver abaixo, em ciclos de 10 troncos celestiais e em ciclos de 12 ramos terrestres. Supondo que certo dia de certo mês de certo ano é domingo do tronco de jia do ramo do rato, pretende-se saber quantos dias depois é terça-feira do tronco de bing do ramo do cavalo.

   (a) Modele este problema através de um sistema de congruências apropriado, resolva-o usando a técnica estudada, e indique o número de dias pedido.

   (b) De quantos em quantos dias é domingo do tronco de jia do ramo do rato?

TRONCOS CELESTIAIS		RAMOS TERRESTRES	
0	Jia	0	Rato
1	Yi	1	Boi
2	Bing	2	Tigre
3	Ding	3	Coelho
4	Wu	4	Dragão
5	Ji	5	Serpente
6	Geng	6	Cavalo
7	Xin	7	Cabra
8	Ren	8	Macaco
9	Gui	9	Galo
		10	Cão
		11	Porco

7. Num passado distante, num país longínquo, um exército ganhou uma batalha contra invasores estrangeiros. Às 5 horas (da manhã) enviaram três mensageiros à capital do país onde chegaram em dias e horas diferentes, levando as boas notícias. Os mensageiros viajaram, em cada dia, entre as 5 e as 17 horas e descansaram no resto do dia. Um dia de viagem é, assim, de 12 horas. O correio A chegou num certo dia às 17 horas, o correio B chegou alguns dias depois às 14 horas e o correio C chegou mais dias depois às 9 horas. De acordo com os suas declarações A cobre uma distância média de 30 km por dia de viagem, B uma distância média de 24 km por dia de viagem e C uma distância média de 18 km por dia de viagem. Determine a menor distância a que o lugar da batalha se encontra da capital. Assuma que as distâncias percorridas são proporcionais aos tempos gastos em as percorrer, i.e., se um mensageiro percorre uma certa distância em 12 horas, então percorre 1/12 dessa distância por hora.

3 Miscelânea

1. Sejam $a, b \in \mathbb{N}$. Mostre que se $a^2 - b^2$ é um número primo então a e b são inteiros consecutivos.

2. Mostre que se p é primo (a) se $p > 2$ então $p \equiv_4 1$ ou $p \equiv_4 -1$ (b) se $p > 3$ então $p \equiv_6 1$ ou $p \equiv_6 -1$

3. Seja $p, a, b, n \in \mathbb{N}$ e p primo. Mostre que se p é divisor de $a \times b$ então p é divisor de a ou p é divisor de b.

4. Mostre que $n \in \mathbb{N}$ é primo então as soluções de $x^2 - 1 \equiv_n 0$ são os inteiros tais que $x \equiv_n 1$ ou $x \equiv_n -1$.
Sugestão: recorra ao exercício anterior.

5. Mostre que existe um número infinito de números primos, isto é, mostre que não existe nenhum número primo maior que todos os outros. Sugestão: suponha que existia um primo p maior que todos os outros, e chegue a uma contradição a partir $q = q' + 1$, onde $q' = 2 \times 3 \ldots \times p$ (produto de todos os primos).

6. Seja $n \in \mathbb{N}_3$. Mostre que se n não é primo então tem um divisor primo menor ou igual a $\sqrt{n}$.
Sugestão: observe que, se não é primo, n pode escrever-se como $n = p \times q$ $(p, q \in \mathbb{N})$ onde p é o menor divisor primo de n; conclua que necessariamente se tem $p \leq \sqrt{n}$ pois, em caso contrário, se chega a uma contradição.