MAT0120 - Álgebra I para Licenciatura

Lista 4

Professor: Kostiantyn Iusenko
Monitor: Douglas de Araujo Smigly

1º Semestre de 2021

1 Sistemas de Congruências Lineares

(1) Resolva os seguintes sistemas de congruências lineares:

$$(a)\ \begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}, \qquad (b)\ \begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod 7 \end{cases}, \qquad (c)\ \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}.$$

(2) Resolva os seguintes sistemas de congruências lineares:

$$(a)\ \begin{cases} 4x \equiv 3 \pmod 7 \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases}, \qquad (b)\ \begin{cases} 3x \equiv 5 \pmod 2 \\ x \equiv -3 \pmod 5 \\ 4x \equiv 7 \pmod 9 \end{cases}.$$

(3) Determine o menor inteiro a, maior que 100, tal que:

$$2 \mid a;\ 3 \mid (a+1);\ 4 \mid (a+2);\ 5 \mid (a+3);\ 6 \mid (a+4).$$

(4) Se de uma cesta com ovos retiramos duas unidades por vez, sobra 1 ovo. O mesmo acontece se os ovos são retirados de 3 em 3, de 4 em 4, de 5 em 5, de 6 em 6. Mas não resta nenhum resto se retiramos 7 unidades cada vez. Qual é menor numero possível de ovos na cesta?

(5) William resolveu fazer uma tabela, onde cada elemento corresponde exatamente ao menor número natural que deixa o resto equivalente na coluna na divisão por 7 e o resto equivalente à linha na divisão por 3. Por exemplo, 19 pertence à linha assinalada com 1 e à coluna assinalada com 5, pois deixa restos 1 e 5 na divisão por 3 e 7, respectivamente.

	0	**1**	**2**	**3**	**4**	**5**	**6**
0							
1						19	
2							

(a) Ajude William, completando a tabela.

(b) Observe que todos os números de 0 a 20 apareceram na tabela uma única vez. Porquê isso ocorreu? O mesmo acontece se fizermos uma tabela semelhante para os restos por 4 e 6?

(6) Resolva a equação $x^2 \equiv 11 \pmod{35}$.

(7) * Sabemos que quando um sistema de congruências satisfaz as condições do Teorema Chinês dos Restos, então ele de fato possui uma única solução para certo módulo. Nesta questão, veremos um critério para determinar se um sistema arbitrário de congruências possui solução.

(a) Mostre que o sistema de congruências

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \end{cases}$$

possui solução apenas se $c_1 \equiv c_2 \pmod{\text{mdc}(n_1, n_2)}$. Mostre também que a solução é única $\pmod{\text{mmc}(n_1, n_2)}$.

(b) Utilizando o item anterior, pode-se provar por indução que o sistema de congruências

$$\begin{cases} x \equiv c_1 \pmod{n_1} \\ x \equiv c_2 \pmod{n_2} \\ \vdots \\ x \equiv c_k \pmod{n_k} \end{cases}$$

possui solução apenas se $c_i \equiv c_j \pmod{\text{mdc}(n_i, n_j)}$ para todos i, j, com $i \neq j$, sendo que, caso exista, a solução é única $\pmod{\text{mmc}(n_1, n_2, \ldots, n_k)}$. Verifique se o sistema de congruências

$$\begin{cases} x \equiv 15 \pmod{26} \\ x \equiv 25 \pmod{37} \\ x \equiv 48 \pmod{59} \\ x \equiv 57 \pmod{77} \\ x \equiv 78 \pmod{87} \\ x \equiv 15 \pmod{111} \\ x \equiv 49 \pmod{127} \end{cases}$$

possui solução.

(8) Seja $N = 1234567\ldots20202021$ o número obtido escrevendo os inteiros de 1 até 2021 concatenados. Qual é o resto que N deixa quando dividido por 40?
[Dica:] Note que $N \equiv 1 \pmod{5}$ e $N \equiv 5 \pmod{8}$ para, então, usar o Teorema Chinês dos Restos.

(9) * Gabriel, ao resolver o sistema com $n > 1$ congruências

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ \vdots \\ x \equiv 3n - 2 \pmod{F_{n+3}} \end{cases},$$

onde F_n denota o n-ésimo número de Fibonacci, percebeu que a menor solução inteira positiva era exatamente a soma dos produtos de cada resto por seu respectivo módulo. Qual foi o sistema de congruências que Gabriel resolveu?

(10) * Encontre uma lista de 17 inteiros positivos consecutivos tais que cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 13$.
[Dica:] Enumere as possibilidades de divisores para cada elemento da lista para avaliar uma possível composição, montando um sistema de congruências e usando o Teorema Chinês dos Restos para resolvê-lo e descobrir os elementos da lista.

2 Teoremas de Euler, Fermat e Wilson

(1) Seja a um inteiro. Demonstre as afirmações abaixo.

(a) $a^{21} \equiv a \pmod{15}$;

(b) Se $\text{mdc}(a, 35) = 1$ então $a^{12} = 1 \pmod{35}$;

(c) Se $\text{mdc}(a, 42) = 1$ então $168 \mid a^6 - 1$;

(d) $a^{25} \equiv a \pmod{26}$.

(2)

(a) Sejam a, b inteiros e seja p um primo positivo tal que $\text{mdc}(a, p) = 1$. Mostre que $x = a^{p-2}b$ é solução da congruência $ax \equiv b \pmod{p}$.

(b) Resolva as congruências $6x \equiv 5 \pmod{11}$ e $3x \equiv 17 \pmod{29}$.

(3) Encontre o resto da divisão de

(a) 5^{14} por 7.

(b) 5^{100} por 11.

(c) 15^{175} por 11.

(d) 31^{200} por 28.

(e) $2^{7^{2002}}$ por 352.

(4) Encontre os dois últimos dígitos de

(a) 2^{999};

(b) 3^{999};

(c) 5^{2020};

(d) 7^{2019};

(e) 123^{2010};

(f) 557^{2012}.

(5)

(a) Seja p um inteiro primo e sejam a, b inteiros arbitrários. Mostre que se $a^p \equiv b^p \pmod{p}$ então $a \equiv b \pmod{p}$.

(b) Seja $p > 2$ um primo. Mostre que

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

(6) Mostre que $2^8 \equiv 1 \pmod{17}$ e que $2^{16} \equiv 1 \pmod{17}$.

(7) Sejam p um primo e a um inteiro tal que $p \nmid a$. Prove que

(a) se $p > 2, a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;

(b) o menor inteiro positivo e tal que $a^e \equiv 1 \pmod{p}$ é divisor de $p-1$;

(c) se e é o inteiro acima de x é um inteiro tal que $a^x \equiv 1 \pmod{p}$ então $e \mid x$.

(8)

(a) Sejam p, q primos distintos e impares tais que $(p-1) \mid (q-1)$. Mostre que se $\text{mdc}(a, pq) = 1$ então $a^{q-1} \equiv 1 \pmod{pq}$.

(b) Seja a um inteiro. Prove que $a^{37} \equiv a \pmod{1729}$; $a^{79} \equiv a \pmod{158}$.

(9) Sejam a um inteiro e n um inteiro positivo tais que $\text{mdc}(a, n) = \text{mdc}(a-1, n) = 1$. Prove que

$$1 + a + \cdots + a^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

(10) Sejam m, n inteiros positivos relativamente primos. Prove que

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

(11) Determine o resto da divisão de a por b nos casos

(a) $a = 15!$ e $b = 17$.

(b) $a = 2 \cdot (26)!$ e $b = 29$.

(12) Reúna os inteiros $2, 3, \ldots, 21$ em pares (a, b) tais que $ab \equiv 1 \pmod{23}$.

(13) Mostre que $18! \equiv -1 \pmod{437}$.

(14) Encontre o resto da divisão de

(a) $5! \cdot 25!$ por 31;
(b) 97! por 101;
(c) 65! por 71;
(d) 53! por 61;
(e) 149! por 139;
(f) 97! por 103.

(15) Resolva cada uma das equações abaixo:

(a) $\varphi(n) = \frac{n}{3}$.
(b) $\varphi(2n) = \varphi(3n)$.
(c) $\varphi(n) = 2$.
(d) $\varphi(n) = \frac{2n}{3}$.
(e) $\varphi(n) = 6$.
(f) $\varphi(n) = 26$.

(16) Mostre que para todo n temos

(a) $\varphi(4n) = 2\varphi(2n)$;

(b) $\varphi(4n+2) = \varphi(2n+1)$;

(17) Observe que

$$\begin{aligned} 6! &\equiv -1 \pmod 7 \\ 5!1! &\equiv 1 \pmod 7 \\ 4!2! &\equiv -1 \pmod 7 \\ 3!3! &\equiv 1 \pmod 7 \end{aligned}$$

(a) Faça o mesmo cálculo para o módulo 11, ou seja, calcule $10! \pmod{11}, 9!1! \pmod{11}, \ldots, 5!5! \pmod{11}$.

(b) Com base no enunciado e nos resultados do item (a), conjecture uma fórmula para realizar esses cálculos e demonstre-a.

(c) Qual é o resto da divisão de $15! \cdot 31!$ por 2021?

(18) Existem exatamente 5 pares de números primos de 2 algarismos (p,q), $p < q$, tais que $p!$ deixa resto p na divisão por q, e 15 pares de números primos de 3 algarismos satisfazendo essa condição.

(a) Mostre que $(11,29), (19,59), (43,61), (47,83)$ e $(53,61)$ são todos os pares de primos de 2 algarismos satisfazendo essa condição.

(b) Mostre que $(653,661)$ é um par de números primos de 3 algarismos satisfazendo a condição do enunciado.
[Dica:] Use que $8! + 1 \equiv 0 \pmod{661}$ e $8 \cdot 248 \equiv 1 \pmod{661}$.

(19) Verifique se cada afirmação abaixo é verdadeira ou falsa:

(a) Se $\text{mdc}(m,n) = 1$ então $\text{mdc}(\varphi(n), \varphi(m)) = 1$.

(b) Se n não é primo, então $\text{mdc}(n, \varphi(n)) > 1$.

(c) Se m e n satisfazem $n\varphi(m) = m\varphi(n)$, então $m = n$.

(20) * Sejam $D(n) = \{d_1, \ldots, d_k\}$ os divisores positivos de n. Assim, $d_1 = 1$, e $d_k = n$.

(a) Se $n = 12$, calcule $\varphi(d_1) + \ldots + \varphi(d_k)$.

(b) Encontre o valor de

$$\varphi(1) + \varphi(2) + \ldots + \varphi(2^\ell),$$

onde $\ell \in \mathbb{N}$.

(c) Sendo p um número primo, encontre o valor de

$$\varphi(1) + \varphi(p) + \ldots + \varphi(p^\ell),$$

onde $\ell \in \mathbb{N}$.

(d) Prove que, para todo $n \in \mathbb{N}^*$,

$$\sum_{d \in D(n)} \varphi(d) = n$$

[Dica:] Utilize o Teorema Fundamental da Aritmética e o item anterior.

(21)

(a) Prove que, para n número natural e $a \in \mathbb{Z}$, com $\text{mdc}(a,n) = 1$ se m, k são naturais positivos tais que $m \equiv k \pmod{\varphi(n)}$, então $a^m \equiv a^k \pmod{n}$.

(b) Seja $a \in \mathbb{Z}$ tal que $\text{mdc}(a, 561) = 1$. Prove que $a^{560} \equiv 1 \pmod{561}$. Isto é um contraexemplo ao Pequeno Teorema de Fermat?

(22) * Mostre que

$$\frac{\sqrt{n}}{2} \leq \varphi(n) < n,$$

para todo n inteiro positivo.

(23) * Nessa questão, vamos analisar um algoritmo para determinar o menor n tal que $\varphi(n) = m$. Seja $D(m) = \{d_1, \ldots, d_k\}$ o conjunto dos divisores positivos de m, e seja $S(m)$ o conjunto dos números primos tais que seu antecessor é divisor de m. Para cada $p \in S(m)$, vamos criar o conjunto

$$L_p = \{(1,1)\} \cup \{(p^e, (p-1)p^{e-1}) | 1 \leq e \leq t+1\},$$

onde t é tal que $p^t \mid m$, mas $p^{t+1} \nmid m$. Note que cada L_p pode ser escrito na forma

$$L_p = \{(a_{d_1}, d_1), (a_{d_2}, d_2), \ldots, (a_{d_k}, d_k)\}.$$

Agora, definimos os conjuntos P_i, para $i \in \mathbb{N}^*$ recursivamente da seguinte maneira:

$$P_1 = L_{p_1}, P_\ell = \left\{ \left(\sum_{t|d} a_t b_{\frac{d}{t}}, d \right), (a_d, d) \in P_{\ell-1}, (b_d, d) \in L_{p_\ell} \right\}, \ell \geq 2.$$

Então, a soma de todos os n tais que $\varphi(n) = m$ é dada pelo termo de P_ℓ correspondente ao par (a_m, m). Vejamos um exemplo para entender este processo: Se $m = 6$, então $D(6) = \{1,2,3,6\}$, e $S(6) = \{2,3,7\}$. Temos então

$$L_2 = \{(1,1),(2,1),(4,2)\}, \quad L_3 = \{(1,1),(3,2),(9,6)\} \quad \text{e} \quad L_7 = \{(1,1),(7,6)\}.$$

Os conjuntos P_i respectivos serão

$$P_1 = L_2, \quad P_2 = \{(3,1),(13,2),(27,6)\} \quad \text{e} \quad P_3 = \{(3,1),(13,2),(48,6)\}.$$

Assim, a soma de todos os n tais que $\varphi(n) = 6$ é 48. De fato, $7 + 9 + 14 + 18 = 48$.
Utilize esse método para encontrar a soma de todos os valores de n que satisfazem

(a) $\varphi(n) = 12$ **(b)** $\varphi(n) = 28$

(24) * O sistema de criptografia RSA é um dos mais utilizados do mundo para criptografar mensagens. Nesse método, há uma chave pública e uma chave privada. A chave pública pode ser distribuída livremente, enquanto a chave privada é a única que permite decriptografar a mensagem. Para gerar essas chaves, seguem-se os seguintes passos:

- Escolha de forma aleatória dois números primos p e q;
- Calcule $n = pq$;

- Calcule $\varphi(n) = (p-1)(q-1)$;
- Escolha um inteiro e tal que $1 < e < \varphi(n)$, de forma que $\text{mdc}(e, \varphi(n)) = 1$;
- - Calcule d de forma que $de \equiv 1 \pmod{\varphi(n)}$, ou seja, d seja o inverso multiplicativo de e em $\pmod{\varphi(n)}$.

Portanto, a chave pública será o par (n, e), e a chave privada será a tripla (p, q, d).
Assim, se associarmos a cada letra do alfabeto o número que representa sua posição, ou seja, A valer 1, B valer 2, C valer 3, e assim por diante, podemos criptografar e decriptografar mensagens.

(a) Vamos criptografar a palavra IME. Podemos descrevê-la como 9-13-5. Utilizando $p = 3$ e $q = 11$:

- ♣ Encontre n e $\varphi(n)$.
- ♥ Verifique que $e = 7$ é um possível valor para compor a chave pública;
- ♠ Encontre o valor de d tal que (p, q, d) seja uma chave privada.
- ♦ Criptografe a palavra IME, calculando $m^e \pmod{n}$ para cada número m correspondente à respectiva letra.

(b) Utilizando a chave privada do item anterior, decriptografe a mensagem abaixo:

Z U L Z X C A E I