XIX Semana Olímpica de Matemática

Nível 2

Equações Diofantinas Lineares e o Teorema Chinês dos Restos

Samuel Feitosa

O projeto da XIX Semana Olímpica de Matemática foi patrocinado por:

impa
instituto nacional de matemática pura e aplicada

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico

fundação lemann

Semana Olímpica 2016
Equações Diofantinas Lineares e o Teorema Chinês dos Restos
Nível 2

Samuel Feitosa

1 Equações Diofantinas Lineares

Exercício 1. Em Gugulândia, o jogo de basquete é jogado com regras diferentes. Existem apenas dois tipo de pontuações para as cestas: 5 e 11 pontos. É possível um time fazer 39 pontos em uma partida?

Exercício 2. Qual o menor inteiro positivo m para o qual todo número maior que m pode ser obtido como pontuação no jogo de basquete mencionado anteriormente?

Exercício 3. Quais e quantos são os inteiros positivos n que não podem ser obtidos como pontuação nesse jogo de basquete?

Para responder o exercício anterior, precisamos relembrar o

Teorema 1 (Bachet-Bèzout) Se $d = mdc(a,b)$, então existem inteiros x e y tais que

$$ax + by = d.$$

A primeira observação que fazemos é que uma vez encontrados inteiros x e y, qualquer múltiplo de d pode ser representado como uma combinação linear de a e b, pois

$$a(kx) + b(ky) = kd.$$

Isso é particularmente interessante quando $mdc(a,b) = 1$, onde obtemos que qualquer inteiro é uma combinação linear de a e b. Veja que isso não entra em conflito com os exemplos anteriores pois os inteiros x e y mencionados no teorema podem ser negativos.

Exercício 4. Mostre que todo inteiro positivo k pode ser escrito (de modo único) de uma e, somente uma, das seguintes formas:

$$11y - 5x \text{ ou } 11y + 5x, \text{ com } 0 \leq y < 5 \text{ e } x \leq 0$$

Exercício 5. Dados os inteiros positivos a e b, com $mdc(a,b) = 1$, existem exatamente

$$\frac{(a-1)}{2} \cdot \frac{(b-1)}{2}$$

números inteiros não negativos que não são da forma $ax + by$ com $x, y \geq 0$.

Exercício 6. Suponha agora que as pontuações das cestas do basquete de Gugulândia tenham mudado para a e b pontos com $0 < a < b$. Sabendo que existem exatamente 35 valores impossíveis de pontuações e que um desses valores é 58, encontre a e b.

Exercício 7. Determine todas as soluções inteiras da equação $2x + 3y = 5$.

Exercício 8. Determine todas as soluções inteiras da equação $5x + 3y = 7$.

Teorema 2 A equação $ax + by = c$, onde a, b, c são inteiros, tem uma solução em inteiros (x, y) se, e somente se, $d = \text{mdc}(a,b)$ divide c. Neste caso, se (x_0, y_0) é uma solução, então os pares

$$(x_k, y_k) = \left(x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d}\right), \quad k \in \mathbb{Z}$$

são todas as soluções inteiras da equação.

Demonstração. Dada a discussão anterior, resta apenas encontrarmos a forma das soluções. Se (x, y) é outra solução, podemos escrever:

$$\begin{aligned} ax + by &= ax_0 + by_0 \\ a(x - x_0) &= b(y_0 - y) \\ \frac{a}{d}(x - x_0) &= \frac{b}{d}(y_0 - y) \end{aligned}$$

Como $mdc(a/d, b/d) = 1$, temos $b/d \mid x - x_0$ e assim podemos escrever $x = x_0 + bk/d$. Substituindo na equação original obtemos $y = y_0 - ak/d$.

Exercício 9. Encontre todas as soluções inteiras da equação $21x + 48y = 6$

Exercício 10. Resolva nos inteiros a equação $2x + 3y + 5z = 11$

Vamos estudar agora alguns outros exemplos de equações diofantinas não lineares:

Exercício 11. Encontre todas as soluções de $999x - 49y = 5000$.

Exercício 12. Encontre todos os inteiros x e y tais que $147x + 258y = 369$.

Exercício 13. Encontre todas as soluções inteiras de $2x + 3y + 4z = 5$.

Exercício 14. Encontre todas as soluções inteiras do sistema de equações:

$$\begin{aligned} 20x + 44y + 50z &= 10 \\ 17x + 13y + 11z &= 19. \end{aligned}$$

Exercício 15. (Torneio das Cidades 1997) Sejam a e b inteiros positivos tais que $a^2 + b^2$ é divisível por ab. Mostre que $a = b$.

Exercício 16. Encontre uma condição necessária e suficiente para que

$$x + b_1y + c_1z = d_1 \quad \text{e} \quad x + b_2y + c_2z = d_2$$

tenham pelo menos uma solução simultanea em inteiros x, y, z, assumindo que os coeficientes são inteiros com $b_1 \neq b_2$.

Exercício 17. (AMC 1989) Seja n um inteiro positivo. Se a equação $2x + 2y + n = 28$ tem 28 soluções em inteiros positivos x, y e z, determine os possíveis valores de n.

Exercício 18. (IMC 2010) Sejam a e b dois inteiros e suponha que n é um inteiro positivo para o qual

$$\mathbb{Z} \backslash \{ax^n + by^n | x, y \in \mathbb{Z}\}$$

é finito. Prove que $n = 1$

Exercício 19. (Jornal Kvant) Dois jogadores disputam um jogo em um quadro negro. Eles escrevem alternadamente inteiros maiores que 1, um por vez, de modo que nenhum deles seja uma combinação linear com coeficientes não negativos dos inteiros já escritos no quadro. O jogador que não puder jogar, perde. Qual jogador possui a estratégia vencedora?

Exercício 20. (Banco OBMEP 2015) Considere dois tambores de capacidade suficientemente grande, um deles vazio e o outro cheio de líquido.

a) Determine se é possível colocar exatamente um litro do líquido do tambor cheio, no vazio, usando dois baldes, um com capacidade de 5 litros e o outro com capacidade de 7 litros.

b) Determine se é possível colocar exatamente um litro do líquido de um dos tambores no outro usando dois baldes, um com capacidade de $2 - \sqrt{2}$ litros e o outro com capacidade de $\sqrt{2}$ litros.

Exercício 21. Sejam a e b inteiros positivos com $mdc(a, b) = 1$. Mostre que para todo $c \in \mathbb{Z}$ com $c > ab - a - b$, a equação $ax + by = c$ admite soluções inteiras com $x, y \geq 0$.

Exercício 22. (IMO 1984) Dados os inteiros positivos a, b e c, dois a dois, primos entre si, demonstrar que $2abc - ab - bc - ca$ é o maior número inteiro que não pode expressar-se na forma $xbc + yca + zab$ com x, y e z inteiros não negativos.

Exercício 23. (Vietnã 2000) Sejam a,b e c inteiros positivos primos entre si, dois a dois. Um inteiro $n \geq 1$ é chamado de teimoso se não pode ser escrito na forma

$$n = bcx + cay + abz$$

para quaisquer inteiros positivos x,y e z. Determine, em função de a,b e c, o número de inteiros teimosos.

Exercício 24. (Irlanda 1997) Ache todos os pares de inteiros (x, y) tais que

$$1 + 1996x + 1998y = xy.$$

2 O Teorema Chinês dos Restos

Teorema 3 Se $mdc(a, m) = 1$, então existe um inteiro x tal que:

$$ax \equiv 1 \pmod{m}.$$

Tal inteiro é único módulo m. Se $mdc(a, m) > 1$, não existe x satisfazendo tal equação.

Demonstração. Pelo teorema de Bachet-Bézout, existem inteiros x e y tais que $ax + my = 1$. Analisando essa congruência módulo m, obtemos $ax \equiv 1 \pmod{m}$. Se y é outro inteiro que satisfaz a mesma congruência, temos $ax \equiv ay \pmod{m}$. Pelo primeiro lema, $x \equiv y \pmod{m}$. Se $d = mdc(a, m) > 1$, não podemos ter $d \mid m$ e $m \mid ax - 1$ pois $d \nmid ax - 1$.

Exercício 25. Encontre x inteiro tal que:

$$\begin{aligned} x &\equiv 1 \pmod{11}; \\ x &\equiv 2 \pmod{7}. \end{aligned}$$

Exercício 26. Encontre x inteiro tal que:

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

Teorema 4 (**Teorema Chinês dos Restos**) Sejam $m_1, m_2, \ldots, m_r$, inteiros positivos primos entre si, dois a dois, e sejam $a_1, a_2, \ldots, a_r$; r inteiros quaisquer. Então, o sistema de conguências:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

admite uma solução x. Além disso, as soluções são únicas módulo $m = m_1 m_2 \ldots m_r$.

Demonstração. Escrevendo $m = m_1 m_2 \ldots m_r$, vemos que $\dfrac{m}{m_j}$ é um inteiro e $mdc\left(\dfrac{m}{m_j}, m_j\right) = 1$. Então, pelo lema inicial, para cada j, existe um inteiro b_j tal que $\left(\dfrac{m}{m_j}\right) b_j \equiv 1 \pmod{m_j}$. Claramente $\left(\dfrac{m}{m_j}\right) b_j \equiv 0 \pmod{m_i}$ para $i \neq j$. Definamos

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \ldots + \frac{m}{m_r} b_r a_r$$

Consideremos x_0 módulo m_i: $x_0 \equiv \dfrac{m}{m_i} b_j a_j \equiv a_i \pmod{m_i}$. Logo, x_0 é uma solução do nosso sistema. Se x_0 e x_1 também o são, podemos escrever $x_0 \equiv x_1 \pmod{m_i}$ para cada i. Como $mdc(m_i, m_j) = 1$, para $i \neq j$, pbtemos $x_0 \equiv x_1 \pmod{m}$.

Se cada uma das equações do sistema anterior fosse do tipo $b_i x \equiv a_i \pmod{m)_i}$, com $mdc(b_i, m) = 1$, ainda poderíamos usá-lo. Bastaria reescrever $b_i x \equiv a_i \pmod{m)_i}$ como $x \equiv \overline{b_i} a_i \pmod{m)_i}$, onde $\overline{b_i}$ é o inverso de $b_i \pmod{m)_i}$.

Exercício 27. Encontre o menor inteiro positivo x tal que $x \equiv 5 \pmod{7}$, $x \equiv 7 \pmod{11}$ e $x \equiv 3 \pmod{13}$.

Exercício 28. (OBM 2009) Sejam m e n dois inteiros positivos primos entre si. O Teorema Chinês dos Restos afirma que, dados inteiros i e j com $0 \leq i < m$ e $o \leq j < n$, existe exatamente um inteiro a, com $0 \leq a < mn$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j. Por exemplo, para $m = 3$ e $n = 7$, temos que 19 é o único número que deixa restos 1 e 5 quando dividido por 3 e 7, respectivamente. Assim, na tabela a seguir, cada número de 0 a 20 aparecerá exatamente uma vez.

	0	1	2	3	4	5	6
0		A				B	
1				C			D
2		E			F		

Qual a soma dos números das casas com as letras A, B, C, D, E e F?

Exercício 29. (Estônia 2000) Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.

Exercício 30. Para cada número natural n, existe uma sequência arbitrariamente longa de números natu rais consecutivos, cada um deles sendo divisível por uma s-ésima potência de um número natural maior que 1.

Exercício 31. (USAMO 1986)

(a) Existem 14 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 11$?

(b) Existem 21 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 13$?

Exercício 32. Sejam a e b inteiros positivos tais que, para qualquer n natural, $a^n + n \mid b^n + n$. Prove que $a = b$.

Exercício 33. (Olimpíada Nórdica 1998)

(a) Para quais inteiros positivos n existe um sequência $x_1, x_2, \ldots, x_n$ contendo cada um dos inteiros $1, 2, \ldots, n$ exatamente uma vez, e tal que k divide $x_1 + x_2 + \cdots + x_k$ para $k = 1, 2, \cdots, n$?

(b) Existe uma sequência infinita $x_1, x_2, \ldots$ contendo todo inteiro positivo exatamente uma vez, e tal que para cada inteiro positivo k, k divide $x_1 + x_2 + \cdots + x_k$?

Exercício 34. (Olimpíada de São Petesburgo 1990) Dado um polinômio $F(x)$ com coeficientes inteiros, tal que, para cada inteiro n, o valor de $F(n)$ é divisível por pelo menos um dos inteiros $a_1, a_2, \cdots, a_m$. Prove que podemos encontrar um índice k tal que $F(n)$ é divisível por a_k para cada inteiro positivo n.

Exercício 35. Encontre o menor inteiro positivo (com a exceção de $x = 1$) que satisfaça o seguinte sistema de congruências:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

Exercício 36. Encontre todas as soluções do sistema:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 2 \end{aligned}$$

Exercício 37. Encontre todos os inteiros que deixam restos $1, 2$ e 3 quando divididos por $3, 4$ e 5, respectivamente.

Exercício 38. Encontre todas as soluções do sistema:

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

Exercício 39. Encontre todas as soluções das congruências:

a) $20x \equiv 4 \pmod{30}$.

b) $20x \equiv 30 \pmod 4$.

c) $353x \equiv 254 \pmod{400}$.

Exercício 40. Se a é escolhido ao acaso no conjunto $\{1, 2, 3, \ldots, 14\}$ e b é escolhido ao acaso no conjunto $\{1, 2, \ldots, 15\}$, qual a probabilidade de que a equação $ax \equiv b \pmod{15}$ possua pelo menos uma solução?

Exercício 41. Sejam a e b inteiros tais que $mdc(a, b) = 1$ e $c > 0$. Prove que existe um inteiro x tal que $mdc(a + bx, c) = 1$.

Exercício 42. Existem n inteiros consecutivos tal que cada um contém um fator primo repetido k vezes?

Exercício 43. Seja n um número natural arbitrário. Prove que existe um par de naturais (a, b) tais que $mdc(a+r, b+s) > 1$ $\forall\ r, s = 1, 2, \ldots, n$.

Exercício 44. Um ponto $(x, y) \in Z^2$ é legal se $mdc(x, y) = 1$. Prove ou disprove: Dado um inteiro positivo n, existe um ponto $(a, b) \in Z^2$ cuja distância a todo ponto legal e pelo menos n?

Exercício 45. Sejam $m_o, m_1, ..., m_r$ inteiros positivos que são primos entre si, dois a dois. Mostre que existem $r + 1$ inteiros consecutivos $s, s + 1, ..., s + r$ tal que m_i divide $s + i$ *para* $i = 0, 1, ..., r$.

Exercício 46. (Romênia 1995) Seja $f : \mathbb{N} - \{0, 1\} \to \mathbb{N}$ definida por $f(n) = mmc[1, 2, ..., n]$. Prove que para todo $n \geq 2$, existem n números consecutivos para os quais f é constante.

Exercício 47. (OBM 2005) Dados os inteiros positivos a, c e o inteiro b, prove que existe um inteiro positivo x tal que $a^x + x \equiv b \pmod{c}$.

Exercício 48. (Cone Sul 2003) Demonstrar que existe uma sequência de inteiros positivos $x_1, x_2, \ldots$ que satisfaz as duas condições seguintes:

(a) contém exatamente uma vez cada um dos inteiros positivos,

(b) a soma parcial $x_1 + x_2 + \ldots x_n$ é divisível por n^n.

Exercício 49. (República Tcheca e Eslovaca 1997) Mostre que existe uma sequência crescente $\{a_n\}_{n=1}^{\infty}$ de números naturais tais que para $k \geq 0$, a sequência $\{a_n + k\}$ contém um número finito de primos.

Exercício 50. Considere o inteiro $c \geq 1$ e a sequência definida por $a_1 = c$ e $a_{i+1} = c^{a_i}$. Mostre que esta sequência se torna eventualmente constante quando a reduzimos módulo n para algum inteiro positivo n (isto significa que $a_m \equiv a_j \pmod{n}$ *se* $m \geq j$).

Exercício 51. (Coréia 1999) Encontre todos os inteiros n tais que $2^n - 1$ é um múltiplo de 3 e $\dfrac{2^n - 1}{3}$ é um divisor de $4m^2 + 1$ para algum inteiro m.

Exercício 52. (OBM 2006) Prove que, para todo inteiro $n \leq 2$, o número de matrizes quadradas 2×2 com entradas inteiras e pertencentes ao conjunto $\{0, 1, 2, \ldots, n - 1\}$ que têm determinante da forma $kn + 1$ para algum k inteiro é dado por

$$\prod_{\substack{p \text{ primo} \\ p \mid n}} \left(1 - \frac{1}{p^2}\right).$$

Exercício 53. Encontre todos os subconjuntos $S \subset \mathbb{Z}_+$ tais que todas as somas de uma quantidade finita de elementos de S(com possíveis repetições de elementos) são números compostos.

Exercício 54. Existe algum natural n para o qual existem $n - 1$ progressões aritméticas com razões $2, 3, \ldots, n$ tais que qualquer natural está em pelo menos uma das progressões?

Exercício 55. Seja $P(X)$ um polinômio com coeficientes inteiros e k é um inteior qualquer. Prove que existe um inteiro m tal que $P(m)$ tem pelo menos k fatores primos distintos.

Respostas e Soluções.

1. Sejam x e y os números de cestas de 5 e 11 pontos, respectivamente. O problema se resume em descobrirmos se existem inteiros não negativos x e y tais que $5x + 11y = 39$. Ao invés de testarmos os valores de x e y, somemos $11 + 5$ em ambos os lados da equação:

$$5(x+1) + 11(y+1) = 55.$$

Como $5 \mid 55$ e $5 \mid 5(x+1)$, segue que $5 \mid 11(y+1)$ e, com mais razão, $5 \mid y+1$ pois $mdc(5,11) = 1$. Do mesmo modo, $11 \mid x+1$. Assim,

$$55 = 5(x+1) + 11(y+1) \geq 5 \cdot 11 + 11 \cdot 5 = 110,$$

pois $x+1, y+1 \geq 1$. Obtemos uma contradição.

2. Como já sabemos que 39 não é possível, é natural começarmos procurando os números maiores que 39 que não podem ser pontuações. Veja que:

$$\begin{aligned} 40 &= 5 \cdot 8 + 11 \cdot 0 \\ 41 &= 5 \cdot 6 + 11 \cdot 1 \\ 42 &= 5 \cdot 4 + 11 \cdot 2 \\ 43 &= 5 \cdot 2 + 11 \cdot 3 \\ 44 &= 5 \cdot 0 + 11 \cdot 4 \end{aligned}$$

Ao somarmos 5 a cada uma dessas representações, obteremos representações para os próximos 5 números. Repetindo esse argumento, poderemos escrever qualquer número maior que 39 na forma $5x + 11y$ com x e y inteiros não negativos. Concluímos assim que $m = 39$. Poderíamos mostrar que todo número maior que 44 é da forma $5x + 11y$ com x e y inteiros não negativos de outro modo. Se $n > 44$, considere o conjunto:

$$n - 11 \cdot 0, n - 11 \cdot 1, n - 11 \cdot 2, n - 11 \cdot 3, n - 11 \cdot 4.$$

Como $mdc(11,5) = 1$, o conjunto anterior é um sistema completo de restos módulo 5 e consequentemente existe $y \in \{0,1,2,3,4\}$ tal que

$$n - 11 \cdot y = 5x$$

Como $n > 44$, segue que $x > 0$.

4. Pelo teorema de Bachet-Bèzout, existem m e n tais que $5m + 11n = 1$. Sejam q e r o quociente e resto da divisão de kn por 5, i.e., $kn = 5q + r,\ 0 \leq r < 5$. Assim,

$$\begin{aligned} k &= 5(km) + 11(kn) \\ &= 5(km) + 11(5q + r) \\ &= 5(km + 11q) + 11r. \end{aligned}$$

Basta fazer $x = km + 11q$ e $r = y$.

Para ver a unicidade, suponha que $11m \pm 5n = 11a \pm 5b$ com $0 \leq m, a < 5$. Então $11(m-a) = 5(\pm b \pm n)$. Usando que $mdc(11,5) = 1$, segue que $5 \mid m - a$. A única opção é termos $m = a$ pois o conjunto $\{0,1,2,3,4\}$ é um **scr**. Consequentemente $\pm 5n = \pm 5b$ e $n = b$.

Sendo assim, os elementos do conjunto

$$B(5,11) = \{11y - 5x \in \mathbb{Z}_+^*; 0 \leq y < 5 \text{ e } x > 0\}$$

constituem o conjunto das pontuações que não podem ser obtidas. Seus elementos são:

$$\begin{aligned} y = 1 &\Rightarrow 11y - 5x = 1, 6 \\ y = 2 &\Rightarrow 11y - 5x = 2, 7, 12, 17 \\ y = 3 &\Rightarrow 11y - 5x = 3, 8, 13, 18, 23, 28 \\ y = 4 &\Rightarrow 11y - 5x = 4, 9, 14, 19, 24, 29, 34, 39 \end{aligned}$$

A quantidade de tais inteiros é

$$20 = \frac{(5-1)}{2} \cdot \frac{(11-1)}{2}.$$

Vale o resultado geral:

6. Perceba que devemos ter $mdc(a,b) = 1$ pois caso contrário qualquer valor que não fosse múltiplo de $mdc(a,b)$ não seria uma pontuação possível e sabemos que existe apenas um número finito de tais valores. Em virtude da proposição anterior, $(a-1)(b-1) = 2 \cdot 35 = 70$. Analisemos os possíveis pares de divisores de 70 tendo em mente que $a < b$:

$$\begin{aligned}(a-1)(b-1) &= 1 \cdot 70 \Rightarrow (a,b) = (2,71)\\ (a-1)(b-1) &= 2 \cdot 35 \Rightarrow (a,b) = (3,36)\\ (a-1)(b-1) &= 5 \cdot 14 \Rightarrow (a,b) = (6,15)\\ (a-1)(b-1) &= 7 \cdot 10 \Rightarrow (a,b) = (8,11)\end{aligned}$$

Não podemos ter $(a,b) = (2,71)$ pois $58 = 2 \cdot 29$. Excluindo os outros dois casos em que $mdc(a,b) \neq 1$, temos $a = 8$ e $b = 11$.

7. Por paridade, $3y$ é ímpar, donde $y = 2k+1$ para algum inteiro k. Daí,

$$x = \frac{5 - 3(2k+1)}{2} = 1 - 3k,$$

e consequentemente todas as soluções da equação são da forma $(x,y) = (1-3k, 2k+1)$.

8. Analisando agora módulo 3, $5x \equiv 7 \equiv 1 \pmod 3$. Essa condição impõe restrições sobre o resto de x na divisão por 3. Dentre os possíveis restos na divisão por 3, a saber $\{0,1,2\}$, o único que satisfaz tal congruência é o resto 2. Sendo assim, x é da forma $3k+2$ e

$$y = \frac{7 - 5(3k+2)}{3} = -1 - 5k,$$

consequentemente, todas as soluções da equação são da forma $(x,y) = (3k+2, -1-5k)$.

Notemos que para a solução da congruência $x = 2$, obtemos a solução $(x,y) = (2,1)$ da equação. Baseado nesses exemplos, é natural imaginarmos que conhecendo uma solução da congruência consigamos descrever todas as outras.

9. O sitema é equivalente à $7x + 16y = 2$. Uma solução é $(x,y) = (-2,1)$. Pelo teorema anterior, todas as soluções são da forma:

$$(x_k, y_k) = (-2 + 16k, 1 - 7k).$$

10. Podemos transformar esse problema isolando qualquer uma das variáveis no problema que já sabemos resolver. Por exemplo, podemos resolver $2x + 3y = 11 - 5z$. Supondo z fixo, podemos encontrar a solução particular $(x,y) = (4-z, 1-z)$. Assim, todas as soluções são da forma:

$$(x,y) = (4 - z + 3k, 1 - z - 2k),$$

ou seja, as soluções da equação original são da forma $(x,y,z) = (4-z+3k, 1-z-2k, z)$ com k e z inteiros.

20.

a) Basta encher o tambor vazio com 15 litros (3×5 litros) usando três vezes o balde de 5 litros e, em seguida, retirar 14 litros (2×7 litros) usando o balde de 7 litros duas vezes. Dessa forma, transportamos $3 \times 5 - 2 \times 7 = 1$ litro.

b) A quantidade a que podemos transportar do tambor cheio para o vazio é da forma $k(2-\sqrt{2}) + l(\sqrt{2})$ litros, onde k e l são inteiros que indicam quantas vezes tiramos ou colocamos líquidos usando cada um dos baldes. Se $l - k \neq 0$, podemos escrever:

$$\begin{aligned}a &= k(2-\sqrt{2}) + l\sqrt{2}\\ a - 2k &= \sqrt{2}(l-k)\\ \frac{a-2k}{l-k} &= \sqrt{2}.\end{aligned}$$

Assim, o número $\sqrt{2}$ seria o quociente de dois inteiros o que resultaria em um número racional. Sabemos que isso não pode acontecer porque $\sqrt{2}$ é irracional. Falta analisarmos o que acontece quando $l = k$. A equação se transforma em:

$$\begin{aligned}a &= k(2-\sqrt{2}) + l\sqrt{2}\\ &= k(2-\sqrt{2}) + k\sqrt{2}\\ &= 2k.\end{aligned}$$

Veja que $2k$ é par e assim não podemos levar um valor ímpar como $a = 1$. Em qualquer caso, não é possível colocar exatamente 1 litro usando os baldes com as capacidades dadas neste item.

25. A primeira congruência nos diz que $x = 11k + 1$ para algum $k \in \mathbb{Z}$. Sejam q e r o quociente e o resto da divisão de k por 7, respectivamente. Assim, $k = 7q + r$ e $x = 77q + 11r + 1$. Para x satisfazer a segunda congruência, devemos encontrar $r \in \{0, 1, 2, 3, 4, 5, 6\}$ tal que $11r + 1 \equiv 2 \pmod 7$, ou seja, $4r \equiv 1 \pmod 7$. Como o inverso de 4 $\pmod 7$ é 2, obtemos $r = 2$ e $x = 77q + 23$. Veja que para qualquer q inteiro, tal x é solução do sistema de congruências.

26. Pelo exemplo anterior, para x satisfazer as duas primeiras equações, devemos ter $x = 77q + 23$. Dividindo q por 5, obtemos $q = 5l + s$ com $0 \leq s < 5$. Daí, $x = 385l + 77s + 23$. Para satisfazer a última congruência, devemos ter $77s + 23 \equiv 4 \pmod 5$, ou seja, $2s \equiv 1 \pmod 5$. Como 3 é o inverso de 2 $\pmod 5$, $s = 3$ e consequentemente $x = 385l + 254$.

Perceba que nos dois exemplos anteriores, o problema foi reduzido à encontrarmos o inverso de um inteiro. No último exemplo, a solução geral possui a forma: $x = 11 \cdot 7 \cdot 5l + 231 + 22 + 1$. Essencialmente, o trabalho de encontrar esses inversos foi possível pois os inteiros 5, 7 e 11 são primos entre si dois a dois.

27. Usando o teorema anterior com $m_1 = 5, m_2 = 7, m_3 = 11, a_1 = 5, a_2 = 7$ *e* $a_3 = 3$ podemos achar $x \equiv 887 \pmod{1001} = 7.11.13$. Como a solução é única módulo m, isso significa que, dentre os números $1, 2, \cdots, 1001$ a menor solução positiva é 887.

28. Usando o teorema chinês dos restos, podemos encontrar $A = 15, B = 12, C = 10, D = 13, E = 8$ e $F = 11$. Assim, $A + B + C + D + E + F = 69$.

29. Seja n tal que $mdc(n, 120) = 1$. Como $120 = 3 \cdot 5 \cdot 8$, temos que $n \not\equiv 0 \pmod 3$, $\pmod 5$ $\pmod 2$. Daí, $n^2 \equiv 1 \pmod 3$, $n^2 \equiv 1 \pmod 8$ e $n^2 \equiv 1$ ou $4 \pmod 5$. Sendo assim, n^2 satisfaz o sistema:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 8 \\ x &\equiv \pm 1 \pmod 5 \end{aligned}$$

cujas soluções são $x \equiv 1 \pmod{120}$ e $x \equiv 49 \pmod{120}$.

30. Dado $m \in \mathbb{N}$, considere o conjunto $\{p_1, p_2, \ldots, p_m\}$ de primos distintos. Como $mdc(p_i^s, p_j^s) = 1$, então pelo teorema 3, existe x tal que $x \equiv -i \pmod{p_i^s}$ para $i = 1, 2, \ldots m$. Cada um dos números do conjunto $\{x + 1, x + 2, \ldots, x + m\}$ é divisível por um número da forma p_i^s.

31. (a) Não. Suponha que existam tais inteiros. Da nossa lista de 14 inteiros consecutivos, 7 são números pares. Vamos observar os ímpares: $a, a + 2, a + 4, a + 6, a + 8, a + 10$ *e* $a + 12$. Podemos ter no máximo três deles divisíveis por 3, dois por 5, um por 7 e um por 11. Veja que 3 + 2 + 1 + 1 = 7. Pelo Princípio da Casa dos Pombos, cada um desses ímpares é divisível por exatamente um primo do conjunto $\{3, 5, 7, 11\}$. Além disso, note que os múltiplos de 3 só podem ser $\{a, a + 6, a + 12\}$. Dois dos números restantes em $(a + 2, a + 4, a + 8,$ *e* $a + 10)$ são divisíveis por 5. Mas isso é impossível. (b) Sim. Como os números $\{210, 11, 13\}$ são primos entre si, dois a dois, pelo teorema 3 existe um inteiro positivo $n > 10$ tal que:

$$n \equiv 0(\bmod 210 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot)$$

$$n \equiv 1(\bmod 11)$$

$$n \equiv -1(\bmod 13)$$

Veja que o conjunto $\{n - 10, n - 9, \ldots, n + 9, n + 10\}$ satisfaz as condições do item (b).

32. Seja p um primo maior que a e b. Então $mdc(p, a) = mdc(p, b) = 1$. Como $mdc(p, p - 1) = 1$, existe um inteiro positivo n tal que $n \equiv 1 \pmod{p - 1}$ e $n \equiv -a \pmod p$. Pelo teorema de Fermat, $a^n + n \equiv 0 \pmod{\ }$ e $b^n + n \equiv b - a \pmod p$. Assim, $p \mid |b - a|$. Como $|b - a| < p$, segue que $|b - a| = 0$ e $a = b$.

33. a) Suponha que n é um inteiro que satisfaz o enunciado. Naturalmente n divide a soma:

$$x_1 + x_2 + \ldots x_n = \frac{n(n+1)}{2}.$$

Daí, $\frac{n+1}{2}$ é um inteiro e n deve ser ímpar. Seja $m = \frac{n+1}{2}$. Usando que

$$(n-1) \mid x_1 + x_2 + \ldots x_{n-1} = mn - x_n,$$

temos $x_n \equiv m \pmod{n-1}$ se $n \geq 3$ e, consequentemente, $x_n = m$. Repetindo a mesma análise para $n-2$ no lugar de $n-1$, obtemos $x_{n-1} = m$ para $n \geq 5$. Como não podem existir dois termos iguais, temos um absurdo. Analisando os casos quando $n \leq 4$, encontramos $n = 1$ e $n = 3$ como únicas soluções.

b) Iremos construir a sequência indutivamente. Suponha que já tenhamos definido os termos $x_1, x_2, \ldots, x_n$ satisfazendo a condição $k \mid x_1 + x_2 \ldots x_k$ para todo $k \leq n$. Seja m o menor inteiro positivo que ainda não apareceu na sequência. Pelo Teorema Chinês dos Restos, existe x tal que $x \equiv -(x_1 + x_2 + \ldots + x_n) \pmod{n+1}$ e $x \equiv -(x_1 + x_2 + \ldots + x_n) - m \pmod{n+2}$. Escolha l, inteiro positivo, tal que $l > x_1, x_2, \ldots, x_n, m$ e $l \equiv x \pmod{(n+1)(n+2)}$. Defina $x_{n+1} = l$ e $x_{n+2} = m$. Veja que a condição $k \mid x_1 + x_2 \ldots x_k$ agora é verdadeira para todo $k \leq n+2$. Para o início, basta definir $x_1 = 1$.

34. Suponha que não exista tal índice. Para cada índice k ($k = 1, 2, \ldots, m$), existe um inteiro x_k tal que $F(x_k)$ não é divisível por a_k. Assim, existem números $d_k = p_k^{\alpha_k}$(onde p_k são números primos), tais que d_k divide a_k mas não divide $F(x_k)$. Se existem potências do mesmo primo entre esses números, podemos apagar aquelas repetidas deixando apenas uma que tem expoente mínimo. Caso $F(x)$ não seja divisível por uma potência apagada, não será pela potência que tem expoente mínimo. Essas deleções garatem que nossa nova coleção $d_1, d_2, \ldots, d_j$ de potências de primos contenham apenas inteiros primos entre si, dois a dois. Pelo teorema chinês dos restos, exite um inteiro N tal que $N \equiv x_k \pmod{d}_k$, para $k \in \{1, 2, \ldots, j\}$. Suponhamos que $d_k \mid F(N)$. Sabemos que $x - y \mid F(x) - F(y)$ e consequentemente $N - x_k \mid F(N) - F(x_k)$. Como $d_k \mid N - x_k$, devemos ter $d_k \mid F(x_k)$. Uma contradição! Logo, $F(N)$ não é divisível por nenhum d_k e isso contradiz a hipótese sobre os a_i.