É usual designarem-se equações diofantinas a equações com uma ou mais incógnitas que assumem valores no conjunto dos números inteiros (ou naturais). Existem numerosas aplicações deste tipo de equações, mas não existem processos gerais de resolução de tal tipo de problemas.

Neste curso abordaremos apenas os casos mais simples de equações diofantinas:

- equações diofantinas polinomiais com uma incógnita,
- equações diofantinas lineares com duas incógnitas.

Proposição

Sejam $n \in \mathbb{N}$, $b, c \in \mathbb{Z}$ tais que $c \neq 0$ e $\text{m.d.c.}(b, c) = 1$. Sejam $a_n, \ldots, a_1, a_0 \in \mathbb{Z}$ e $a_n \neq 0$. Se o número racional $\frac{b}{c}$ é raiz do polinómio

$$a_n x^n + \cdots + a_1 x + a_0,$$

então $b \mid a_0$ e $c \mid a_n$.

PROVA

Se $\frac{b}{c}$ é raiz do polinómio $a_n x^n + \cdots + a_1 x + a_0$, então

$$a_n \left(\frac{b}{c}\right)^n + a_{n-1} \left(\frac{b}{c}\right)^{n-1} + \cdots + a_1 \left(\frac{b}{c}\right) + a_0 = 0,$$

que é equivalente a $a_n b^n + a_{n-1} b^{n-1} c \cdots + a_1 b c^{n-1} + a_0 c^n = 0$.

Como $b|0$, $b|(a_n b^n + a_{n-1} b^{n-1} c \cdots + a_1 b c^{n-1})$ e $\text{m.d.c.}(b, c) = 1$, então $b|a_0$.
Como $c|0$, $c|(a_{n-1} b^{n-1} c \cdots + a_1 b c^{n-1} + a_0 c^n)$ e $\text{m.d.c.}(b, c) = 1$, então $c|a_n$.

Corolário

Se $b \in \mathbb{Z}$ é solução da equação polinomial de coeficientes inteiros

$$a_n x^n + \cdots + a_1 x + a_0 = 0,$$

então $b \mid a_0$.

Nota

O corolário anterior dá apenas uma condição necessária, mas permite listar os elementos de um conjunto finito que contém as possíveis soluções inteiras para a equação.

EXEMPLO 1

Considere-se o polinómio

$$2x^4 + 11x^3 - 23x + 10.$$

As raízes racionais, caso existam, são elementos do conjunto

$$\left\{ \frac{b}{c} : \ b|10 \wedge c|2 \right\} = \left\{ -10, -5, -\frac{5}{2}, -2, -1, -\frac{1}{2}, \frac{1}{2}, 1, 2, \frac{5}{2}, 5, 10 \right\}.$$

As raízes inteiras, caso existam, são elementos do conjunto

$$\{-10, -5, -2, -1, 1, 2, 5, 10\}.$$

De facto, $2x^4 + 11x^3 - 23x + 10 = 2(x-1)(x+2)(x+5)(x-1/2)$.

Definição

Uma equação difantina linear em duas incógnitas x e y é uma equação do tipo

$$ax + by = c$$

com $a, b, c \in \mathbb{Z}$.

Uma solução desta equação é um par de números inteiros (x', y') que verifica $ax' + by' = c$.

Nota

Se $a = 0$ ou $b = 0$, então a resolução da equação diofantina $ax + by = c$ é um exercício elementar. Iremos estar interessados no caso em que $a \neq 0$ e $b \neq 0$.

Teorema

Sejam $a, b, c \in \mathbb{Z}$ e a e b não nulos. Seja $d = \text{m.d.c.}(a, b)$. A equação diofantina linear, em duas incógnitas x e y, $ax + by = c$ tem solução sse $d \mid c$.

Verifica-se ainda que, se (x', y') é uma solução da equação, então os pares da forma

$$(x' + \frac{b}{d}k,\ y' - \frac{a}{d}k),$$

com $k \in \mathbb{Z}$, também são soluções da equação.

Nota

Se a equação diofantina $ax + by = c$ tem soluções, então tem uma infinidade de soluções.

PROVA

Se $d \mid a$ e $d \mid b$, então $d \mid (ax' + by')$, ou seja, $d \mid c$.

Reciprocamente, pelo algoritmo de Euclides estendido para o cálculo do $\mathrm{m.d.c.}$, existem x_0 e y_0 inteiros tais que $d = ax_0 + by_0$. Se $d \mid c$, então existe um inteiro k tal que $c = dk$. Logo,

$$c = dk = (ax_0 + by_0)k = a\,x_0k + b\,y_0k,$$

pelo que a equação diofantina $ax + by = c$ tem solução $(x_0k,\ y_0k)$.

Verifica-se ainda que, se (x', y') é uma solução da equação, então

$$a(x' + \frac{b}{d}k) + b(y' - \frac{a}{d}k) = ax' + \frac{ab}{d}k + by' - \frac{ba}{d}k = ax' + by' = c.$$

EXEMPLO 2

Considere-se a equação diofantina $\quad 486x + 218y = 2.$

$(48, -107)$ é uma solução da equação, que foi obtida por aplicação do algoritmo de Euclides estendido. Como $\mathrm{m.d.c}(486, 218) = 2$, são soluções da equação os pares

$$\left(48 + k\frac{218}{2},\ -107 - k\frac{486}{2}\right) \quad \text{em que} \quad k \in \mathbb{Z}.$$

Proposição

Sejam $a, b, c \in \mathbb{Z}$ e a e b não nulos. Seja $d = \text{m.d.c.}(a, b)$. Se (x', y') é uma solução da equação diofantina $ax + by = c$, então todas as soluções são da forma

$$\left(x' + \frac{b}{d}k,\ y' - \frac{a}{d}k\right) \qquad \text{com } k \in \mathbb{Z}.$$

PROVA

Seja (x_0, y_0) uma outra solução de $ax + by = c$. Então,

$$\left.\begin{array}{l} ax' + by' = c \\ ax_0 + by_0 = c \end{array}\right\} \Rightarrow (ax' + by') - (ax_0 + by_0) = 0 \quad \Leftrightarrow a(x' - x_0) = -b(y' - y_0)$$
$$\Leftrightarrow \tfrac{a}{d}(x' - x_0) = -\tfrac{b}{d}(y' - y_0).$$

Como $\text{m.d.c.}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{d}{d} = 1$, então $\frac{a}{d} \mid (y' - y_0)$, ou seja, $\exists_{k \in \mathbb{Z}}$ tal que $\frac{a}{d}k = (y' - y_0)$.
Logo, $y_0 = y' - \frac{a}{d}k$. Mais,

$$ax_0 = ax' + b(y' - y_0) = ax' + b\left(y' - \left(y' - \frac{a}{d}k\right)\right)$$

pelo que $x_0 = x' + \frac{b}{d}k$.

Definição

Chama-se congruência linear de incógnita x a uma expressão do tipo

$$ax \equiv b \pmod{m}$$

com $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$.

$x' \in \mathbb{Z}$ diz-se solução de $ax \equiv b \pmod{m}$ se $ax' \equiv b \pmod{m}$.

Notas

- Se x' é solução de $ax \equiv b \pmod{m}$, então $x' + mk$ também é solução para qualquer $k \in \mathbb{Z}$.
- $$ax \equiv b \pmod{m} \Leftrightarrow [a]_m[x]_m = [b]_m$$

  Assim, uma congruência linear é uma equação linear em $\mathbb{Z}_m$.
- $$ax \equiv b \pmod{m} \Leftrightarrow m \mid (ax - b) \Leftrightarrow \exists_{y \in \mathbb{Z}}\, ax + my = b$$

  Logo, as soluções de uma congruência linear podem ser obtidas a partir das soluções de uma equação diofantina.

Teorema

Sejam $a, b \in \mathbb{Z}$ tal que $a \neq 0$ e $m \in \mathbb{N}$. Seja $d = \text{m.d.c.}(a, m)$. A congruência linear $ax \equiv b \pmod{m}$ tem solução sse $d \mid b$.

PROVA

$$\exists_{x \in \mathbb{Z}}\ ax \equiv b \pmod{m} \Leftrightarrow \exists_{x \in \mathbb{Z}} \exists_{y \in \mathbb{Z}}\ ax + my = b \Leftrightarrow d \mid b$$

EXEMPLO 3

Considere-se a congruência $486x \equiv 2 \pmod{218}$.

Como $\text{m.d.c}(486, 218) = 2$, e $2 \mid 2$, então a congruência tem soluções.

NOTA

Uma congruência linear do tipo $ax \equiv b \pmod{m}$,

- ou não tem soluções, caso em que $d \nmid b$,
- ou é equivalente a uma congruência do tipo $x \equiv c \pmod{n}$ com $n = \frac{m}{d}$ e $c = a' \frac{b}{d}$ onde a' é o inverso de $\frac{a}{d}$ módulo n, caso contrário.

Resolver a congruência linear $ax \equiv b \pmod{m}$ significa calcular o conjunto das soluções módulo m, isto é, determinar as soluções no conjunto $\{0, 1, \ldots, m-1\}$.

Por abuso de linguagem diz-se que a equação tem k soluções se tem k soluções no conjunto $\{0, 1, \ldots, m-1\}$ (*i.e.*, k soluções incongruentes módulo m duas a duas).

EXEMPLO 3 - continuação

A congruência linear $486x \equiv 2 \pmod{218}$ tem duas soluções incongruentes módulo 218, a saber $x = 48$ e $x = 157$.

$$\begin{aligned} 486x \equiv 2 \pmod{218} &\Leftrightarrow 243x \equiv 1 \pmod{109} \\ &\Leftrightarrow x \equiv 48 \pmod{109} \end{aligned}$$

Recordar que as soluções da equação diofantina $486x + 218y = 2$ eram da forma $\left(48 + k\frac{218}{2},\ -107 - k\frac{486}{2}\right)$ em que $k \in \mathbb{Z}$.

Teorema

Sejam $a, b \in \mathbb{Z}$ tal que $a \neq 0$ e $m \in \mathbb{N}$. Seja $d = \text{m.d.c.}(a, m)$. Se x' é solução da congruência linear $ax \equiv b \pmod{m}$, então

$$\left\{x',\ x' + \frac{m}{d},\ x' + \frac{2m}{d},\ \ldots,\ x' + \frac{(d-1)m}{d}\right\}$$

é o conjunto das soluções incongruentes módulo m duas a duas.

PROVA

$$\exists_{x\in\mathbb{Z}}\ ax \equiv b \pmod{m} \Leftrightarrow \exists_{x\in\mathbb{Z}}\exists_{y\in\mathbb{Z}}\ ax + my = b.$$

As soluções da equação diofantina $ax + my = b$ são os pares de inteiros da forma

$$\left(x' + \frac{m}{d}k,\ y' - \frac{a}{d}k\right) \qquad \text{com } k \in \mathbb{Z}.$$

Logo o conjunto das soluções da congruência é $\left\{x' + \frac{mk}{d}\ :\ k \in \mathbb{Z}\right\}$.

Como

$$x' + \frac{mk}{d} \equiv x' + \frac{m(k+d)}{d} \pmod{m},$$

então basta considerar $k \in \{0, \ldots, d-1\}$ para obter um conjunto de soluções incongruentes módulo m duas a duas.

EXEMPLO 3 - continuação

$x = 48$ é uma solução da congruência linear $\quad 486x \equiv 2 \pmod{218}$.

Como $\mathrm{m.d.c}(486, 218) = 2$, um conjunto completo de soluções incongruentes módulo 218 é

$$\left\{ 48 + k\frac{218}{2} \ : \ k \in \{0, 1\} \right\}.$$

No entanto, o conjunto de todas as soluções inteiras é $\left\{ 48 + k\frac{218}{2} \ \mid \ k \in \{0, 1\} \right\}$.

Faz-se notar que, para qualquer $k \in \mathbb{Z}$,

$$48 + \frac{218}{2} \equiv 48 + (2k + 1)\frac{218}{2} \pmod{218}$$

e

$$48 \equiv 48 + 2k\frac{218}{2} \pmod{218}.$$

Teorema

Sejam $a, b, s \in \mathbb{Z}$ tal que $a \neq 0$ e $m \in \mathbb{N}$. Se a fatorização de m em primos é $m = p_1^{e_1} \cdots p_r^{e_r}$, então s é solução de $ax \equiv b \pmod{m}$ sse s é solução de todas as seguintes congruências lineares:

$$\begin{cases} ax \equiv b \pmod{p_1^{e_1}} \\ \quad \vdots \\ ax \equiv b \pmod{p_r^{e_r}} \end{cases}$$

Resolver a congruência $ax \equiv b \pmod{m}$ é equivalente a resolver um sistema de congruências módulo potências de primos.

Proposição

Sejam $a, b, s \in \mathbb{Z}$ tal que $a \neq 0$ e $p \in \mathbb{P}$. Seja $k \in \mathbb{N}$ s é solução de $ax \equiv b \pmod{p^k}$ então s é solução das congruências lineares da forma

$$ax \equiv b \pmod{p^{k'}} \quad \text{com } k' \leq k.$$

EXEMPLO 4

Resolver a congruência $453x \equiv 30 \pmod{4200}$.

Como $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$, $453 = 3 \cdot 151$ e $30 = 3 \cdot 10$, então

$$453x \equiv 30 \pmod{4200} \Leftrightarrow 151x \equiv 10 \pmod{2^3 \cdot 5^2 \cdot 7}$$

$$\Leftrightarrow \begin{cases} 151x \equiv 10 \pmod{2^3} \\ 151x \equiv 10 \pmod{5^2} \\ 151x \equiv 10 \pmod{7} \end{cases}$$

$$\Leftrightarrow \begin{cases} 7x \equiv 2 \pmod{2^3} \\ x \equiv 10 \pmod{5^2} \\ 4x \equiv 3 \pmod{7} \end{cases}$$

- $7x \equiv 2 \pmod{2} \Leftrightarrow x \equiv 0 \pmod{2} \Rightarrow$ são pares as soluções de $7x \equiv 2 \pmod{2^3}$
- $x \equiv 10 \pmod{5} \Leftrightarrow x \equiv 0 \pmod{5} \Rightarrow$ são múltiplos de 5 as soluções de $x \equiv 10 \pmod{5^2}$
- $4x \equiv 3 \pmod{7} \Leftrightarrow -3x \equiv 3 \pmod{7} \Leftrightarrow x \equiv -1 \pmod{7} \Leftrightarrow x \equiv 6 \pmod{7}$

$$453x \equiv 30 \pmod{4200} \Leftrightarrow \begin{cases} x \equiv 6 \pmod{2^3} \\ x \equiv 10 \pmod{5^2} \\ x \equiv 6 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} x = 6 + 2^3 k_1 \\ x = 10 + 5^2 K_2 \\ x = 6 + 7k_3 \end{cases} \qquad (k_1, k_2, k_3 \in \mathbb{Z})$$

EXEMPLO 5

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$n \bmod 2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
$n \bmod 3$	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
$n \bmod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Considere o par $(n \bmod 2, n \bmod 3) = (0, 1)$. Tal par identifica algum número n menor do que 6? E que números identifica menores do que 12?

Considere agora o par $(n \bmod 2, n \bmod 5) = (0, 1)$. Tal par identifica algum número n menor do que 10? Quando se voltaria a repetir tal par?

- Analise os pares de restos $(n \bmod 2,\ n \bmod 3)$ para $0 \leq n \leq 5$.
- Analise os pares de restos $(n \bmod 3,\ n \bmod 5)$ para $0 \leq n \leq 14$.
- Analise os pares de restos $(n \bmod 2,\ n \bmod 5)$ para $0 \leq n \leq 9$.

Primeiro enunciado do Teorema Chinês dos Restos

Se $\text{m.d.c.}(a, b) = 1$ então os pares de restos do tipo

$$(n \bmod a,\ n \bmod b),$$

para $n \in \{0, \ldots, ab - 1\}$, são todos distintos.

EXEMPLO 6

$$\begin{cases} x \equiv 6 \pmod{3^2} \\ x \equiv 3 \pmod{2^3} \end{cases}$$

Pelo Teorema Chinês dos Restos, há uma única solução comum às duas equações módulo $2^3 \times 3^2$:

$$\left.\begin{array}{ll} x \equiv 6 \pmod{3^2} & \Leftrightarrow x = 6 + 9k\ (k \in \mathbb{Z}) \\ x \equiv 3 \pmod{2^3} & \Leftrightarrow x = 3 + 8t\ (t \in \mathbb{Z}) \end{array}\right\} \Rightarrow x \equiv 51 \pmod{72}$$

EXEMPLO 7

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
$n \bmod 2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	...
$n \bmod 3$	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	...
$n \bmod 5$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	...

Considere o terno $(n \bmod 2, n \bmod 3, n \bmod 5) = (1, 0, 4)$. Tal triplo está associado a algum número n menor do que 29?

Será tal número único?

Qual é o próximo inteiro que está associado ao mesmo terno?

- Complete a tabela para valores de n até 29 e analise os ternos de restos $(n \bmod 2,\ n \bmod 3,\ n \bmod 5)$.

Teorema Chinês dos Restos

Sejam $m_1, m_2, \ldots, m_n$ números primos entre si dois a dois. Então o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

tem uma única solução módulo $M = m_1 m_2 \cdots m_n$.

A única solução é dada por:

$$x_0 \equiv a_1 M_1 x_1 + \cdots + a_n M_n x_n \pmod{M}$$

onde $M_i = \frac{M}{m_i}$ e x_i é o inverso de M_i módulo m_i para $1 \leq i \leq n$.

EXEMPLO 8

A única solução do sistema de congruências lineares

$$\begin{cases} x \equiv 7 \pmod{2^3} \\ x \equiv 16 \pmod{5} \\ x \equiv 32 \pmod{7^2} \end{cases}$$

módulo $M = 2^3 \cdot 5 \cdot 7^2 = 1960$ é

$$x_0 \equiv 7 \cdot (5 \cdot 7^2) \cdot 5 + 1 \cdot (2^3 \cdot 7^2) \cdot 3 + 32 \cdot (2^3 \cdot 5) \cdot 38 \pmod{1960}, \qquad \text{isto é,}$$

$$x_0 \equiv 1551 \pmod{1960}$$

pois:

$$m_1 = 2^3 \qquad M_1 = \frac{2^3 \cdot 5 \cdot 7^2}{2^3} = 5 \times 7^2 \qquad 5 \times 7^2 x_1 \equiv 1 \pmod{2^3} \Leftrightarrow x_1 \equiv 5 \pmod{2^3}$$

$$m_2 = 5 \qquad M_2 = \frac{2^3 \cdot 5 \cdot 7^2}{5} = 2^3 \times 7^2 \qquad 2^3 \times 7^2 x_2 \equiv 1 \pmod{5} \Leftrightarrow x_2 \equiv 3 \pmod{5}$$

$$m_3 = 7^2 \qquad M_3 = \frac{2^3 \cdot 5 \cdot 7^2}{7^2} = 2^3 \times 5 \qquad 2^3 \times 5\, x_3 \equiv 1 \pmod{7^2} \Leftrightarrow x_3 \equiv 38 \pmod{7^2}$$

Extensão do Teorema Chinês dos Restos

Sejam $m_1, m_2, \ldots, m_n$ inteiros tais que $\text{m.d.c.}(m_i, m_j) \mid a_i - a_j$ para quaisquer $i \neq j$. Então o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

tem uma única solução módulo $M = \text{m.m.c.}(m_1, m_2, \ldots, m_n)$.

EXEMPLO 9

O sistema de congruências lineares

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod{54} \\ x \equiv 8 \pmod{15} \end{cases}$$

tem uma única solução módulo $M = \text{m.m.c.}(4, 54, 15) = 2^2 \times 3^3 \times 5$, pois

$$\begin{array}{lll} \text{m.d.c.}(4, 54) = 2 & \text{e} & 2 \mid (5-3) \\ \text{m.d.c.}(4, 15) = 1 & \text{e} & 1 \mid (8-3) \\ \text{m.d.c.}(54, 15) = 3 & \text{e} & 3 \mid (8-5), \end{array}$$

Como $4 = 2^2$, $54 = 2 \times 3^3$ e $15 = 3 \times 5$, o sistema acima é equivalente ao seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 3 \pmod{2^2} \\ x \equiv 5 \pmod 2 \\ x \equiv 5 \pmod{3^3} \\ x \equiv 8 \pmod 3 \\ x \equiv 8 \pmod 5 \end{cases}.$$

EXEMPLO 9 - continuação

Este último sistema é por sua vez equivalente ao sistema:

$$\begin{cases} x \equiv 3 \pmod{2^2} \\ x \equiv 1 \pmod{2} \\ x \equiv 5 \pmod{3^3} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}.$$

Qualquer solução de $x \equiv 3 \pmod{2^2}$ é solução de $x \equiv 1 \pmod{2}$, porque

$$\left.\begin{array}{lll} \text{m.d.c.}(2^2, 2) = 2 & \wedge & 2 \mid (3-1) \\ x \equiv 3 \pmod{2^2} & \Rightarrow & 2 \mid (x-3) \end{array}\right\} \text{Então, } 2 \mid (x-1).$$

Qualquer solução de $x \equiv 5 \pmod{3^3}$ é solução de $x \equiv 2 \pmod{3}$, porque

$$\left.\begin{array}{lll} \text{m.d.c.}(3^3, 3) = 3 & \wedge & 3 \mid (5-2) \\ x \equiv 5 \pmod{3^3} & \Rightarrow & 3 \mid (x-5) \end{array}\right\} \text{Então, } 3 \mid (x-2).$$

Consequentemente, o sistema acima é equivalente ao sistema:

$$\begin{cases} x \equiv 3 \pmod{2^2} \\ x \equiv 5 \pmod{3^3} \\ x \equiv 3 \pmod{5} \end{cases}.$$

EXEMPLO 9 - continuação

$$\begin{cases} x \equiv 3 \pmod{2^2} \\ x \equiv 5 \pmod{3^3} \\ x \equiv 3 \pmod{5} \end{cases}$$

tem uma única solução módulo $M = 2^2 \times 3^3 \times 5$ que é dada pelo Teorema Chinês dos Restos:

$$x_0 \equiv 3 \cdot (3^3 \cdot 5) \cdot 3 + 5 \cdot (2^2 \cdot 5) \cdot 20 + 3 \cdot (2^2 \cdot 3^3) \cdot 2 \pmod{540}, \qquad \text{isto é,}$$

$$\equiv 383 \pmod{540}$$

pois:

$$m_1 = 2^2 \qquad M_1 = \frac{M}{2^2} = 3^3 \cdot 5 \qquad 3^3 \cdot 5\, x_1 \equiv 1 \pmod{2^2} \Leftrightarrow x_1 \equiv 3 \pmod{2^2}$$

$$m_2 = 5 \qquad M_2 = \frac{M}{3^3} = 2^2 \cdot 5 \qquad 2^2 \cdot 5\, x_2 \equiv 1 \pmod{3^3} \Leftrightarrow x_2 \equiv 23 \pmod{3^3} \quad .$$

$$m_3 = 7^2 \qquad M_3 = \frac{M}{5} = 2^2 \cdot 3^3 \qquad 2^2 \cdot 3^3 x_3 \equiv 1 \pmod{5} \Leftrightarrow x_3 \equiv 2 \pmod{5}$$

O conjunto das soluções inteiras é $\left\{383 + 540k : k \in \mathbb{Z}\right\}$.