Equações diofantinas

Definição: Uma equação diofantina é uma equação do tipo

$$a_1 x_1^{n_1} + a_2 x_2^{n_2} + \dots + a_k x_k^{n_k} = c$$

onde, para cada $i \in \{1, \dots, k\}$, $n_i \in \mathbb{N}$, $a_i \in \mathbb{Z}$ e $c \in \mathbb{Z}$.

Os x_i são as incógnitas e as soluções da equação supõem-se números inteiros.

Nesta UC vamos estudar apenas equações do tipo

$$ax + by = c$$

com $a, b, c \in \mathbb{Z}$, $a, b \neq 0$.

Chama-se solução da equação $ax + by = c$ a um par $(x_0, y_0) \in \mathbb{Z}^2$ tal que $ax_0 + by_0 = c$.

Exemplo: A equação $2x+10y=17$ não tem solução pois $2x+10y$ é um número par, quaisquer que sejam $x, y \in \mathbb{Z}$ e 17 é um número ímpar.

Exemplo A equação $3x+6y=18$ tem várias soluções. Por exemplo: $(x_0, y_0) = (4, 1)$ e $(x_1, y_1) = (-6, 6)$ são duas soluções.

Questão: Dada a equação diofantina $ax+by=c$

1) Quando é que tem solução?

2) Se tem solução a solução é única? Uma infinidade?

Proposição: Seja $ax+by=c$ uma eq. diofantina. Existe solução sse $m.d.c(a,b) \mid c$.

Demonst: Sejam $d = m.d.c(a,c)$. Sabemos que existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + by_0 = d$.

Suponhamos que $d | c$ então $c = kd$ logo $c = a(kx_0) + b(ky_0)$ e (kx_0, ky_0) é solução da equação.

Supondo que a equação tem solução com $d|a$ e $d|b$ então $d | ax+by$, quaisquer que sejam $x, y \in \mathbb{Z}$, logo $d|c$. $\square$

Proposição: Se $ax+by=c$ admite solução, então admite uma infinidade de soluções.

Demonst: Seja (x_0, y_0) uma solução particular de $ax+by=c$.

Se (x', y') é outra solução de $ax+by=c$. Então

$$ax_0 + by_0 = ax' + by' \iff a(x'-x_0) = b(y_0 - y') \quad (*)$$

Seja $d = m.d.c\,(a,b)$. Então

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$$

Como $m.d.c\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ então resulta que de $\frac{a}{d} \mid \frac{b}{d}(y_0 - y')$ se tem que $\frac{a}{d} \mid (y_0 - y')$, ou seja, existe $t \in \mathbb{Z}$ tal que

$$y_0 - y' = \frac{a}{d}t \iff y' = y_0 - \frac{a}{d}t$$

Substituindo em $(*)$ vem que

$$a(x' - x_0) = b\,\frac{a}{d}t \iff x' - x_0 = \frac{b}{d}t$$

$$\iff x' = x_0 + \frac{b}{d}t$$

Logo $\begin{cases} x' = x_0 + \frac{b}{d}t \\ y' = y_0 - \frac{a}{d}t \end{cases}$ $t \in \mathbb{Z}$ é uma infinidade de soluções de $ax+by=c$

De facto $a\left(x_0+\frac{b}{d}t\right)+b\left(y_0-\frac{a}{d}t\right) = ax_0+by_0 = c$ $\square$

Definição Chama-se solução geral da equação $ax+by=c$ ao par (x', y') em que

$$\begin{cases} x' = x_0 + \frac{b}{d}t, & t \in \mathbb{Z} \\ y' = y_0 - \frac{a}{d}t \end{cases}$$

sendo (x_0, y_0) uma solução particular de $ax+by=c$ e $d = m.d.c(a,b)$

Exemplo: $172x + 20y = 1000$

$172 = 8 \times 20 + 12$

$20 = 12 + 8$

$12 = 8 + 4$

$8 = 2 \times 4 + 0$

$m.d.c(172, 20) = 4$ logo como $4 \mid 1000$ a equação tem solução

$$172x + 20y = 1000 \iff 43x + 5y = 250$$

$$\text{m.d.c}(43,5) = 1 \implies \exists\, x_0, y_0 \in \mathbb{Z} \quad 43x_0 + 5y_0 = 1$$

$$\implies 43(250x_0) + 5(250y_0) = 1$$

$$\begin{aligned} 43 &= 8 \times 5 + \underline{3} \\ 5 &= 1 \times \underline{3} + \underline{2} \\ 3 &= 1 \times \underline{2} + \underline{1} \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5-3) = \\ &= -5 + 2\times 3 \\ &= -5 + 2\times(43 - 8\times 5) \\ &= 2\times 43 - 17\times 5 \end{aligned}$$

$$1 = 2\times 43 - 17\times 5 \implies 250 = 43\times(500) - 5\times(4250)$$

Logo $(x_0, y_0) = (500, -4250)$ é uma solução particular da equação $43x + 5y = 250$

Pela proposição anterior $\begin{cases} x' = 500 + 5t \\ y' = -4250 - 43t \end{cases} \quad t \in \mathbb{Z}$

é a solução geral pretendida.

Congruências módulo n

Definição: Seja $n \in \mathbb{N}$. Diz-se que um inteiro a é congruente módulo n com um inteiro b e escreve-se $a \equiv b \pmod{n}$ se n é um divisor de $a-b$. Se a não é congruente com b módulo n então escrevemos $a \not\equiv b \pmod{n}$.

Teorema Para quaisquer dois inteiros a, b, temos que $a \equiv b \pmod{n}$ sse o resto da divisão de a por n e o resto da divisão de b por n forem iguais.

Demonst: Do Teorema do Algoritmo da Divisão, existem q, q' e r e r' tais que

$$a = nq + r \qquad q, q' \in \mathbb{Z}$$
$$b = nq' + r \qquad 0 \leq r, r' < n$$

Se $r = r'$ então $a - b = n(q - q')$ logo $n \mid a-b$

ou seja, $a \equiv b \pmod{n}$

Reciprocamente, se $a \equiv b \pmod{n}$. Então $n \mid a-b$

ou seja $a - b = nk$, $k \in \mathbb{Z}$, logo $a = b + nk$.

Pelo teorema do algoritmo da divisão $b = np + r$, $0 \leq r < n$

logo $a = b + nk = np + r + nk = n(p+k) + r$, $0 \leq r < n$

Pela unicidade do resto, então a e b têm ambos resto r na divisão por n.

$\square$

<u>Observação</u> Cada inteiro a é congruente módulo n com o seu resto na divisão por n. Assim cada inteiro é congruente com um e um só dos inteiros $0, 1, 2, \ldots, n-1$.

Teorema: Sejam $a, b, c \in \mathbb{Z}$. Então:

(i) $a \equiv a \pmod{n}$

(ii) $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$

(iii) $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

(iv) $\left.\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a + c \equiv b + d \pmod{n} \\ ac \equiv bd \pmod{n} \end{array}\right.$

(v) $a \equiv b \pmod{n} \Rightarrow \left\{\begin{array}{l} ac \equiv bc \pmod{n} \\ a + c \equiv b + c \pmod{} \end{array}\right.$

(vi) $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}, \ \forall k \in \mathbb{N}$

Demonst: (i) e (ii) são imediatas

(iii) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ então $n \mid a-b$ e $n \mid b-c$ logo $n \mid (a-b)+(b-c)$, ou seja, $n \mid a-c$.

Assim $a \equiv c \pmod{n}$

(iv) Suponhamos que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Então $n \mid a-b$ e $n \mid c-d$. Logo $n \mid (a-b)x + (c-d)y$, $x, y \in \mathbb{Z}$

Considerando $x = 1$ e $y = 1$ vem $n \mid (a-b) + (c-d)$

$\Leftrightarrow n \mid (a+c) - (b+d)$ logo $a+c \equiv b+d \pmod{n}$.

Considerando $x = c$ e $y = b$ temos $n \mid (a-b)c + (c-d)b$

logo $n \mid ac - bd$, ou seja $ac \equiv bd \pmod{n}$.

(v) Resulta de (iv) e (i)

(vi) resulta de (iv) aplicando indução.

$\square$

<u>Observação:</u> As propriedade (i) + (ii) + (iii) significam que a relação de congruência módulo n, que denotamos

$\equiv \pmod{n}$ é uma relação de equivalência em $\mathbb{Z}$.

O conjunto das classes de equivalência é dado por

$$\{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

Além disso as propriedades (iv) e (v) significam que $\equiv \pmod{n}$ é compatível com a adição e a multiplicação em $\mathbb{Z}$.

<u>Exemplo</u> Mostrar que $41 \mid 2^{20} - 1$

Queremos mostrar que $2^{20} \equiv 1 \pmod{41}$

Temos $2^5 \equiv -9 \pmod{41}$

Temos também $(-9)^2 \equiv -1 \pmod{41}$

Logo $(-9)^4 \equiv (-1)^2 \pmod{41}$

Então $(2^5)^4 \equiv (-9)^4 \pmod{41}$

$(-9)^4 \equiv 1 \pmod{41}$

Logo, por transitividade, $2^{20} \equiv 1 \pmod{41}$

Exemplo Determinar o resto da divisão de $\sum_{n=1}^{100} n!$ por 12

Temos $\sum_{n=1}^{100} n! = 1! + 2! + 3! + 4! + 5! + 6! + \cdots$

$4! = 24$, $5! = 5 \times 4!$, $6! = 6 \times 5 \times 4!$

Portanto temos $\sum_{n=1}^{100} n! = \sum_{n=1}^{3} n! + \sum_{n=4}^{100} n!$

$\sum_{n=1}^{3} n! \equiv 9 \pmod{12}$ $\qquad 1! + 2! + 3! = 9$

$\sum_{n=1}^{100} n! \equiv 0 \pmod{12}$ $\qquad 12 \mid 4! \Rightarrow 12 \mid n!, \ n \geq 4$

Logo $\displaystyle\sum_{n=1}^{100} n! \equiv 9 \pmod{12}$

Lei do corte

$ab \equiv ac \pmod{n} \overset{?}{\Longrightarrow} b \equiv c \pmod{n}$

Temos $6 \equiv 2 \pmod{4}$ mas $3 \not\equiv 1 \pmod{4}$

Não é válida a lei do corte. (Mas $3 \equiv 1 \pmod{2}$)

Teorema Sejam $n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$. Se $ca \equiv cb \pmod{n}$ então $a \equiv b \left(\bmod \frac{n}{d}\right)$ onde $d = m.d.c(c, n)$

Demonst: Ver sebenta.

Corolário: Se $ca \equiv cb \pmod{n}$ e $m.d.c(c,n) = 1$ então $a \equiv b \pmod{n}$

Lei do anulamento do produto

$$ab \equiv 0 \pmod n \overset{?}{\Longrightarrow} a \equiv 0 \pmod n \ \vee\ b \equiv 0 \pmod n$$

$4 \equiv 0 \pmod 4$ mas $2 \not\equiv 0 \pmod 4$

$6 \equiv 0 \pmod 6$ mas $2 \not\equiv 0 \pmod 6$ e $3 \not\equiv 0 \pmod 6$

Não é válida a lei do anulamento do produto.

Teorema Sejam $a, b \in \mathbb{Z}$. Se $ab \equiv 0 \pmod n$ e $m.d.c(a,n) = 1$

então $b \equiv 0 \pmod n$

Demonst: Imediata do teorema anterior.