Teoria Elementar de Números

2021/2022

Unidade curricular do 1º ano do Mestrado em Ensino do 1.º Ciclo do Ensino Básico e de Matemática e Ciências Naturais no 2.º Ciclo do Ensino Básico, da Universidade do Minho

António Veloso da Costa

Teoria Elementar de Números

1. Divisibilidade de números inteiros
2. Equações Diofantinas
3. Números primos
4. Congruências módulo um inteiro n

1 - Divisibilidade de números inteiros

Exemplo

Se dividirmos 171 objectos por caixas com capacidade para 14 objectos, quantas caixas conseguimos completar e quantos objectos sobram?

Queremos determinar o quociente e o resto da divisão de 171 por 14 :

$$\begin{array}{r|l} 171 & 14 \\ \cline{2-2} 31 & 12 \\ 3 & \end{array} \qquad \text{e portanto} \qquad 171 = 12 \times 14 + 3$$

pelo que o quociente da divisão é 12 e o resto é igual a 3.

Exemplo

Também podemos resolver este problema usando a recta real.

A partir da origem vamos avançando 14 unidades obtendo os inteiros $14, 28, 42, \cdots$ até obtermos o inteiro mais próximo de 171 que não excede 171, neste caso o inteiro 168.

O número de vezes que avançamos 14 unidades indica-nos o valor do quociente e o número de unidades necessárias para atingir o inteiro 171, a partir do inteiro 168, indica-nos o valor do resto.

$$0 \underset{14}{\longrightarrow} 14 \underset{14}{\longrightarrow} 28 \underset{14}{\longrightarrow} 42 \underset{14}{\longrightarrow} \cdots \underset{14}{\longrightarrow} 168 \underset{3}{\longrightarrow} 171$$

Exemplo

Vejamos uma forma mais interessante de ver o problema na recta real:

A partir do inteiro 171 vamos avançando 14 unidades na direção da origem da recta real, até atingirmos um inteiro positivo inferior a 14.

Esse inteiro será o valor do resto e o número de vezes que nos deslocamos 14 unidades indica-nos o valor do quociente .

Neste exemplo, a partir do inteiro 171 vamos obtendo os inteiros: $157, 143, 129, 115, \cdots$ que têm a particularidade de todos eles darem resto 3, quando divididos por 14.

$$\begin{array}{ccccccccccccc} 0 & \xleftarrow{3} & 3 & \xleftarrow{14} & 17 & \xleftarrow{14} & \cdots & \xleftarrow{14} & 143 & \xleftarrow{14} & 157 & \xleftarrow{14} & 171 \end{array}$$

Exemplo

Assim, para calcular o resto da divisão de 171 por 14, em vez de efectuarmos a divisão, podemos subtrair a 171 múltiplos de 14 até obter um inteiro entre 0 e 13.

$$171 - 140 = 31 \qquad 31 - 28 = 3$$

Da primeira vez subtraímos, 10×14 e da segunda vez, 2×14. No total, subtraímos 12 vezes 14.

Logo o quociente da divisão de 171 por 14, é 12 e o resto é 3.

Algoritmo da divisão (para inteiros positivos)

Dados $a, b \in \mathbb{N}$ existem inteiros únicos, $q, r \in \mathbb{N}_0$, tais que:

$$a = q \times b + r \quad \text{com} \quad 0 \leq r < b$$

Este resultado pode ser generalizado para inteiros (positivos ou negativos):

Algoritmo da divisão (para inteiros)

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, existem inteiros únicos, $q, r \in \mathbb{Z}$, tais que:

$$a = q \times b + r \quad \text{com} \quad 0 \leq r < |b|$$

Exemplos (inteiros negativos)

1. Vamos calcular o quociente e o resto da divisão de 171 por -14:

Sabemos que: $171 = 12 \times 14 + 3$
pelo que, $171 = (-12) \times (-14) + 3$
Logo

$$q = -12 \quad \text{e} \quad r = 3$$

2. Vamos calcular o quociente e o resto da divisão de -171 por 14:

Sabemos que: $171 = 12 \times 14 + 3$
pelo que, $-171 = -12 \times 14 - 3 = -12 \times 14 - 14 + 14 - 3 =$
$= -13 \times 14 + 11$
Logo

$$q = -13 \quad \text{e} \quad r = 11$$

Exemplos (inteiros negativos)

3. Vamos calcular o quociente e o resto da divisão de -171 por -14:

Sabemos que: $171 = 12 \times 14 + 3$

pelo que, $-171 = 12 \times (-14) - 3 = 12 \times (-14) - 14 + 14 - 3 =$
$= 13 \times (-14) + 11$

Logo

$$q = 13 \quad \text{e} \quad r = 11$$

4. Vamos calcular o resto da divisão de 1351 por -14:

Basta subtrair múltiplos de 14 a 1351 até obter um inteiro entre 0 e 13

$$1351 - 1400 = -49 \qquad -49 + 56 = 7$$

Logo o resto da divisão de 1351 por -14 é igual a 7.

Nota: $q = -100 + 4 = -96$.

A relação de divisibilidade

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, quando o resto da divisão de a por b é zero, temos que $a = q \times b$ e nesse caso escrevemos $b|a$, isto é

$$b|a \quad \Longleftrightarrow \quad \exists\, q \in \mathbb{Z} \ : \ \ a = q \times b$$

Dizemos então que:

- b divide a
- b é um divisor de a
- a é divisível por b
- a é um múltiplo de b

Exemplo : $3|18$ uma vez que $18 = 6 \times 3$

Logo 3 é um divisor de 18, ou seja, 18 é um múltiplo de 3.

Propriedades da relação de divisibilidade

Sejam $a, b, c, d \in \mathbb{Z}\backslash\{0\}$. Então:

1. $a|a$
2. $a|b \ \wedge \ b|a \ \Rightarrow \ a = \pm b$
3. $a|b \ \wedge \ b|c \ \Rightarrow \ a|c$

4. $a|b \ \Rightarrow \ a|-b \ \wedge \ -a|b \ \wedge \ -a|-b$
5. $a|b \ \wedge \ c|d \ \Rightarrow \ ac|bd$

6. $a|b \ \wedge \ a|c \ \Rightarrow \ a|b+c$
7. $a|b \ \wedge \ a|c \ \Rightarrow \ a|b-c$
8. $a|b+c \ \wedge \ a|b \ \Rightarrow \ a|c$
9. $a|b \ \wedge \ a|c \ \Rightarrow \ a|bx+cy \quad \forall x, y \in \mathbb{Z}$

Propriedades da relação de divisibilidade

Demonstração 9.

Como $a|b$ temos que $b = q_1\, a$ com $q_1 \in \mathbb{Z}$
Como $a|c$ temos que $c = q_2\, a$ com $q_2 \in \mathbb{Z}$

Logo, quaisquer que sejam $x, y \in \mathbb{Z}$

$$bx + cy = (aq_1)x + (aq_2)y = a(q_1x + q_2y)$$

e como $q_1x + q_2y \in \mathbb{Z}$ temos que $a|bx + cy$

Exemplo

Como $7|28$ e $7|56$ então $7|28 + 56$

Dado $b \in \mathbb{Z}$, se $7|28 + b$ como $7|28$ então $7|b$

Máximo divisor comum

Definição

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, chama-se máximo divisor comum entre a e b, e representa-se por m.d.c.(a, b), ao maior inteiro positivo que é simultaneamente divisor de a e divisor de b.

Exemplo Vamos calcular m.d.c.$(36, 45)$:

divisores positivos de 36 : $1, 2, 3, 4, 6, 9, 12, 18, 36$

divisores positivos de 45 : $1, 3, 5, 9, 15, 45$

Logo, m.d.c.$(36, 45) = 9$.

Nota : m.d.c.$(-36, 45) =$ m.d.c.$(-36, -45) =$ m.d.c.$(36, 45) = 9$

Máximo divisor comum

Vamos agora calcular m.d.c.$(36, 45)$, por outro processo:

$36 = 2 \times 2 \times 3 \times 3 \qquad 45 = 3 \times 3 \times 5$

Logo, m.d.c.$(36, 45) = 3 \times 3 = 9$.

Definição

Dados $a, b \in \mathbb{Z}\backslash\{0\}$*, se* m.d.c.$(a, b) = 1$ *, dizemos que os inteiros* a *e* b *são primos entre si .*

Nota : Se m.d.c.$(a, b) = c > 1$ então $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros e são primos entre si.

Máximo divisor comum (propriedades)

Teorema

Dados $a, b \in \mathbb{Z}\backslash\{0\}$ *existem inteiros* $x, y \in \mathbb{Z}$ *tais que:*

$$m.d.c.(a, b) = ax + by$$

Proposição

Dados $a, b, c \in \mathbb{Z}\backslash\{0\}$

$$a|c \quad \wedge \quad b|c \quad \wedge \quad m.d.c.(a, b) = 1 \quad \Longrightarrow \quad ab|c$$

Proposição

(Lema de Euclides): Dados $a, b, c \in \mathbb{Z}\backslash\{0\}$

$$a|bc \quad \wedge \quad m.d.c.(a, b) = 1 \quad \Longrightarrow \quad a|c$$

Nota : $4|12$ e $6|12$ mas no entanto $4 \times 6 \nmid 12$

Nota : $6|4 \times 9$ mas no entanto $6 \nmid 4$ e $6 \nmid 9$

Mínimo múltiplo comum

Definição

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, *chama-se mínimo múltiplo comum entre* a *e* b , *e representa-se por* $m.m.c.(a, b)$, *ao menor inteiro positivo que é simultaneamente múltiplo de* a *e múltiplo de* b .

Teorema

Dados $a, b \in \mathbb{Z}\backslash\{0\}$, $\quad m.m.c.(a, b) = \dfrac{|\, a\ b\,|}{m.d.c.(a, b)}$

Exemplo

$$m.m.c.(36, 45) = \frac{|\, 36 \times 45\,|}{m.d.c.(36, 45)} = \frac{36 \times 45}{9} = 4 \times 45 = 180$$

Algoritmo de Euclides (250 a.c.)

Dados $a, b \in \mathbb{N}$ queremos calcular m.d.c.(a, b).
Supondo que $a > b$, pelo algoritmo da divisão existem $q, r \in \mathbb{N}_0$, únicos, tais que

$$a = qb + r \quad \text{com} \quad 0 \leq r < b$$

vamos mostrar que;

$$\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r)$$

Seja $d \in \mathbb{N}$ tal que $d|a$ e $d|b$ então $d|a - qb = r$. Logo $d|b$ e $d|r$
Reciprocamente, se $d|b$ e $d|r$ então $d|qb + r = a$. Logo $d|a$ e $d|b$.

Algoritmo de Euclides

Assim, em vez de calcularmos m.d.c.(a, b) podemos calcular m.d.c.(b, r).

Como $b > r$, pelo algoritmo da divisão existem $q_1, r_1 \in \mathbb{N}_0$, tais que

$$b = q_1 r + r_1 \quad \text{com} \quad 0 \leq r_1 < r$$

Pelo que teremos

$$\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r) = \text{m.d.c.}(r, r_1)$$

Dividindo agora r por r_1 e repetindo sucessivamente este processo, como os restos obtidos são cada vez menores, a certa altura teremos que obter resto zero na divisão.
Nessa divisão de resto zero, o menor dos inteiros será o m.d.c. , ou seja, o m.d.c. será o último resto não nulo que obtivermos.

Algoritmo de Euclides - Exemplo

Vamos usar o algoritmo de Euclides para calcular m.d.c.$(340, 812)$

$812 = 2 \times 340 + 132$

$340 = 2 \times 132 + 76$

$132 = 1 \times 76 + 56$

$76 = 1 \times 56 + 20$

$56 = 2 \times 20 + 16$

$20 = 1 \times 16 + 4$

$16 = 4 \times 4 + 0$

Logo m.d.c.$(340, 812) = 4$

Algoritmo de Euclides - Exemplo

Vamos agora usar o algoritmo de Euclides para escrever o m.d.c.$(340, 812)$ como combinação linear de 340 e 812

$$4 = 20 - 1 \times 16 =$$

$$= 20 - 1 \times (56 - 2 \times 20) = -56 + 3 \times 20 =$$

$$= -56 + 3 \times (76 - 56) = 3 \times 76 - 4 \times 56 =$$

$$= 3 \times 76 - 4 \times (132 - 76) = -4 \times 132 + 7 \times 76 =$$

$$= -4 \times 132 + 7 \times (340 - 2 \times 132) = 7 \times 340 - 18 \times 132 =$$

$$= 7 \times 340 - 18 \times (812 - 2 \times 340) = -18 \times 812 + 43 \times 340$$

$$\text{m.d.c.}(340, 812) = 4 = 43 \times 340 - 18 \times 812$$

2 - Equações Diofantinas

Equações diofantinas

Dados $a, b, c \in \mathbb{Z}$, com $a, b \neq 0$, queremos encontrar $x, y \in \mathbb{Z}$, tais que:

$$a\,x + b\,y = c$$

Uma equação deste tipo diz-se uma equação diofantina .

Equações diofantinas - existência de solução

Seja d=m.d.c.(a,b) .

Se a equação tiver solução, como $d|a$ e $d|b$ então

$$d|a\,x + b\,y = c$$

Por outro lado, se $d|c$, então existe $q \in \mathbb{Z}$ tal que $c = q\,d$.

Sabemos, pelo Algoritmos de Euclides, que existem $x_1, y_1 \in \mathbb{Z}$ tais que

$$d = a\,x_1 + b\,y_1$$

e multiplicando ambos os membros por q,

$$c = q\,d = a\,q\,x_1 + b\,q\;\; y_1 = a\,(q\,x_1) + b\,(q\,y_1)$$

e portanto a equação diofantina tem solução, $x = q\,x_1$ e $y = q\,y_1$.

Equações diofantinas - solução geral

Teorema

Dados $a, b, c \in \mathbb{Z}$, com $a, b \neq 0$, seja d=m.d.c.(a, b) e considere-se a equação diofantina

$$a\,x + b\,y = c$$

1. *A equação $a\,x + b\,y = c$ tem solução $\Leftrightarrow$ $d \mid c$*

2. *Se a equação tem uma solução $x = x_0$ e $y = y_0$, então a equação tem uma infinidade de soluções, dadas por:*

$$x = x_0 + \frac{b}{d}\,k$$

$$y = y_0 - \frac{a}{d}\,k \qquad k \in \mathbb{Z}$$

Equações diofantinas - Exemplo 1

Vamos encontrar todas as soluções da equação diofantina

$$812\,x + 340\,y = 12$$

Já vimos que m.d.c.$(812, 340) = 4$ e como $4|12$ a equação tem solução.

Vimos também, usando o algoritmo de Euclides, que

$$4 = 812 \times (-18) + 340 \times 43$$

Multplicando ambos os membros por 3, obtemos:

$$12 = 812 \times (-18 \times 3) + 340 \times (43 \times 3)$$

pelo que $x_0 = -54$ e $y_0 = 129$ é uma solução da equação.

Equações diofantinas - Exemplo 1

Então a solução geral da equação será:

$$x = -54 + \frac{340}{4}\, k = -54 + 85\, k$$

$$y = 129 - \frac{812}{4}\, k = 129 - 203\, k$$

com $k \in \mathbb{Z}$.

Abaixo temos uma tabela com algumas das soluções

k	$\cdots\cdots$	-2	-1	0	1	2	3	$\cdots\cdots$
x	$\cdots\cdots$	-224	-139	-54	31	116	201	$\cdots\cdots$
y	$\cdots\cdots$	535	332	129	-74	-277	-480	$\cdots\cdots$

Também podíamos ter começado por simplificar a equação dividindo ambos os membros pelo m.d.c.$(812, 340) = 4$

$$812\, x + 340\, y = 12 \iff 203\, x + 85\, y = 3$$

Equações diofantinas - Exemplo 2

Vamos agora resolver a equação diofantina

$$13\,x - 17\,y = 42$$

Como 13 e 17 são primos então m.d.c.$(13, 17) = 1$.

Vamos usar o Algoritmo de Euclides para escrever 1 como combinação linear de 13 e -17 .

$$\begin{aligned} 17 &= 1 \times 13 + 4 \\ 13 &= 3 \times 4 + 1 \\ 4 &= 4 \times 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 13 - 3 \times 4 = \\ &= 13 - 3\,(17 - 13) = \\ &= 13 \times 4 - 17 \times 3 \quad (*) \end{aligned}$$

Logo m.d.c.$(13, 17) = 1$ e multiplicando $(*)$ por 42 , obtemos

$$42 = 13(4 \times 42) - 17(3 \times 42)$$

pelo que $x_0 = 168$ e $y_0 = 126$ é uma solução da equação.

Equações diofantinas - Exemplo 2

Então a solução geral da equação será:

$$x = 168 + \frac{-17}{1}\, k = 168 - 17\, k$$

$$y = 126 - \frac{13}{1}\, k = 126 - 13\, k$$

com $k \in \mathbb{Z}$.

Abaixo temos uma tabela com algumas das soluções

k	$\cdots\cdots$	-2	-1	0	1	2	3	$\cdots\cdots$
x	$\cdots\cdots$	202	185	168	151	134	117	$\cdots\cdots$
y	$\cdots\cdots$	152	139	126	113	100	87	$\cdots\cdots$

Equações diofantinas - Exemplo 3

Vamos agora resolver a equação diofantina

$$-36\,x - 21\,y = 39$$

Dividindo ambos os membros por -3 obtemos a seguinte equação :

$$12\,x + 7\,y = -13$$

Vamos usar o Algoritmo de Euclides para escrever m.d.c.$(12, 7)$ como combinação linear de 12 e 7 .

$$\begin{aligned} 12 &= 1 \times 7 + 5 \\ 7 &= 1 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 5 - 2 \times 2 = \\ &= 5 - 2\,(7 - 5) = -2 \times 7 + 3 \times 5 = \\ &= -2 \times 7 + 3(12 - 7) \\ &= 12 \times 3 + 7 \times (-5) \quad (*) \end{aligned}$$

Logo m.d.c.$(12, 7) = 1$ e multiplicando $(*)$ por -13 , obtemos

$$-13 = 12(3 \times (-13)) + 7(-5 \times (-13))$$

pelo que $x_0 = -39$ e $y_0 = 65$ é uma solução da equação.

Equações diofantinas - Exemplo 3

Então a solução geral da equação será:

$$x = -39 + \frac{7}{1}\, k = -39 + 7\, k$$

$$y = 65 - \frac{12}{1}\, k = 65 - 12\, k$$

com $k \in \mathbb{Z}$.

Abaixo temos uma tabela com algumas das soluções

k	$\cdots\cdots$	-2	-1	0	1	2	3	$\cdots\cdots$
x	$\cdots\cdots$	-53	-46	-39	-32	-25	-18	$\cdots\cdots$
y	$\cdots\cdots$	89	77	65	53	41	29	$\cdots\cdots$

3 - Números Primos

Números primos - definição

Definição

Um inteiro $p > 1$ diz-se um número primo se 1 e p são os seus únicos divisores positivos.

Exemplo:

7 é um número primo porque os seus divisores positivos são 1 e 7.

12 não é um número primo uma vez que os seus divisores positivos são: $1, 2, 3, 4, 6, 12$.

Note-se que como 12 não é primo, podemos escrevê-lo como o produto de dois factores inteiros maiores do que 1:

$$12 = 3 \times 4 \qquad \text{ou} \qquad 12 = 2 \times 6$$

razão pela qual dizemos que 12 é um número composto.

Números primos - propriedades

Teorema

Sejam $a, b \in \mathbb{N}$ *e* p *um número primo. Então:*

$$p|ab \quad \Longrightarrow \quad p|a \quad \vee \quad p|b$$

Exemplo : $3|4 \times 9$ e como 3 é primo, temos que ter $3|4$ (falso) ou $3|9$ (verdadeiro).

Exemplo : $6|4 \times 9$ mas no entanto $6 \nmid 4$ e $6 \nmid 9$. Isto acontece porque 6 não é primo.

Corolário

Sejam $a_1, a_2, \cdots, a_n \in \mathbb{N}$ *e* p *um número primo. Então:*

$$p|a_1\, a_2\, \cdots\, a_n \quad \Longrightarrow \quad p|a_i \quad \text{para algum } i$$

Decomposição em números primos

Se um número inteiro n não for primo, ou seja, se for composto, então ele pode escrever-se como o produto de dois factores inteiros: $a > 1$ e $b > 1$, isto é:

$$n = a\, b$$

Se a e/ou b não forem primos, então eles próprios podem ser decompostos como o produto de dois factores inteiros > 1.

Repetindo este processo para todos os factores que não são primos, a certa altura iremos obter n como um produto de um número finito de factores primos.

Ordenando os factores primos por ordem crescente e agrupando os primos repetidos numa única potência, obtemos uma decomposição única para n como um produto de factores primos.

Decomposição em números primos - exemplo

O número 792 é composto, uma vez que é divisível por 2.

Vamos decompor 792 num produto de factores primos:

792	2	$792 = 2 \times 396$
396	2	$396 = 2 \times 198$
198	2	$198 = 2 \times 99$
99	3	$99 = 3 \times 33$
33	3	$33 = 3 \times 11$
11	11	
1		

Logo, $792 = 2 \times 2 \times 2 \times 3 \times 3 \times 11 = 2^3 \times 3^2 \times 11$

Esta decomposição de 792 em factores primos é única .

Teorema fundamental da Aritmética

Teorema

Todo o inteiro $n > 1$ *pode ser decomposto como um produto de números primos, de forma <u>única</u>:*

$$n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \cdots\ p_k^{\alpha_k}$$

onde,

$p_1 < p_2 < \cdots < p_k$ *são números primos e* $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_k \in \mathbb{N}$.

Divisores positivos

Proposição

Se um inteiro $n > 1$ *tem decomposição em primos:*

$$n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \cdots\ p_k^{\alpha_k}$$

então os divisores positivos de n *são da forma:*

$$p_1^{\beta_1}\ p_2^{\beta_2}\ \cdots\ p_k^{\beta_k} \qquad \text{com} \qquad 0 \leq \beta_i \leq \alpha_i$$

e o número de divisores positivos de n *é dado por:*

$$(\alpha_1 + 1)\ (\alpha_2 + 1)\ \cdots (\alpha_k + 1)$$

Divisores positivos - exemplo

Já vimos que

$$792 = 2^3 \times 3^2 \times 11$$

Logo o número de divisores positivos de 792 é dado por:

$$(3+1) \times (2+1) \times (1+1) = 4 \times 3 \times 2 = 24$$

Para determinarmos todos os divisores positivos de 792, temos que considerar todas as combinações possíveis para os expoentes dos primos $2, 3$ e 11 .

Para o expoente do primo 2 temos as possibilidades: $0, 1, 2, 3$

Para o expoente do primo 3 temos as possibilidades: $0, 1, 2$

Para o expoente do primo 11 temos as possibilidades: $0, 1$

Divisores positivos - exemplo

Abaixo temos a lista de todos os divisores positivos do inteiro:

$$792 = 2^3 \times 3^2 \times 11$$

1	2	2^2	2^3
3	2×3	$2^2 \times 3$	$2^3 \times 3$
3^2	2×3^2	$2^2 \times 3^2$	$2^3 \times 3^2$
11	2×11	$2^2 \times 11$	$2^3 \times 11$
3×11	$2 \times 3 \times 11$	$2^2 \times 3 \times 11$	$2^3 \times 3 \times 11$
$3^2 \times 11$	$2 \times 3^2 \times 11$	$2^2 \times 3^2 \times 11$	$2^3 \times 3^2 \times 11$

Teorema

Sejam n *e* m *inteiros maiores do que* 1*, com a seguinte decomposição em primos:*

$$n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \cdots\ p_k^{\alpha_k} \qquad\qquad m = q_1^{\beta_1}\ q_2^{\beta_2}\ \cdots\ q_r^{\beta_r}$$

Então

1. *O m.d.c.*(n, m) *é o produto dos primos comuns às duas decomposições, elevados ao menor dos expoentes.*

2. *O m.m.c.*(n, m) *é o produto dos primos comuns e não comuns às duas decomposições, elevados ao maior dos expoentes.*

M.D.C. e M.M.C. - exemplo

Vamos usar a decomposição em primos para calcular m.d.c. e o m.m.c. entre os inteiros 792 e 738.

738	2
369	3
123	3
41	41
1	

Temos então que:

$$792 = 2^3 \times 3^2 \times 11 \qquad 738 = 2 \times 3^2 \times 41$$

e portanto

$$\text{m.d.c.}(792, 738) = 2 \times 3^2 \qquad \text{m.m.c.}(792, 738) = 2^3 \times 3^2 \times 11 \times 41$$

Decomposição em números primos - exemplo

Para decompor um inteiro $n > 1$ em factores primos, ou para testar se esse inteiro é primo, basta procurar divisores de n que sejam primos , até ao valor $\sqrt{n}$, uma vez que

$$n = \sqrt{n} \times \sqrt{n}$$

Exemplo: Queremos decompor 1379 em factores primos.

Como $40 \times 40 = 1600$ temos que $\sqrt{1379} < 40$ e portanto basta testar como divisores os primos até 40.

Por exemplo, 41 é primo, mas se 1379 fosse divisível por 41 teríamos

$$1379 = 41 \times a$$

e portanto a seria um divisor inteiro de 1379 menor do que 40.

Decomposição em números primos - exemplo

O inteiro 1379 não é divisível pelos primos $2, 3, 5$ mas é divisível por 7 . De facto

$$1379 = 7 \times 197$$

Basta-nos agora decompor 197 e para isso basta-nos procurar divisores primos até $\sqrt{197} < 15$.

Como já testamos os primos $2, 3, 5$ basta então testar como divisores os primos $7, 11, 13$.

Como 197 não é divisível pelos primos $7, 11, 13$ então 197 é um número primo. Logo a decomposição de 1379 em factores primos é:

$$1379 = 7 \times 197$$

Existência de uma infinidade de primos

Teorema

Existe uma infinidade de números primos.

Demonstração - Vamos supor que existe um número finito de números primos

$$p_1 < p_2 < \cdots < p_k$$

e seja

$$n = (p_1\ p_2\ \cdots\ p_k) + 1$$

Como $n > p_k$ então n não é primo e portanto existe um primo p_i tal que $p_i | n$. Então,

$$p_i | n = (p_1\ p_2\ \cdots\ p_k) + 1 \quad \wedge \quad p_i | p_1\ p_2\ \cdots\ p_k \quad \Longrightarrow \quad p_i | 1$$

o que é uma contradição pois como p_i é primo, temos que $p_i > 1$.

O Crivo de Eratóstenes

O O Crivo de Eratóstenes é um processo para encontrar todos os inteiros primos até um valor previamente fixado.

Vamos usar esse processo para encontrar todos os primos até 100:

- Começamos por listar todos os inteiros até 100 e riscamos o número 1
- O número seguinte da lista é o 2 (que é *primo*) e riscamos da lista todos os múltiplos de 2
- O número seguinte da lista é o 3 (que é *primo*) e riscamos da lista todos os múltiplos de 3
- O número seguinte da lista é o 5 (que é *primo*) e riscamos da lista todos os múltiplos de 5
- O número seguinte da lista é o 7 (que é *primo*) e riscamos da lista todos os múltiplos de 7

A lista dos números não riscados é a lista de todos os *primos* até 100.

O Crivo de Eratóstenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

O Crivo de Eratóstenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Os números a vermelho constituem a lista dos primos até 100.

4 - Congruências módulo um inteiro n

Congruências - definição

Definição

Sejam $n \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$. *Diz-se que* a *e* b *são congruentes módulo* n *se* a *e* b *têm o mesmo resto quando divididos por* n, *e escreve-se:*

$$a \equiv_n b \qquad (ou \quad a \equiv b \ (mod\, n))$$

Nota importante :

$$a \equiv_n b \iff n \mid a - b$$

Proposição

A relação $\equiv_n$ *é uma relação de equivalência em* $\mathbb{Z}$, *isto é, dados* $a, b, c \in \mathbb{Z}$:

1. $a \equiv_n a$
2. $a \equiv_n b \Rightarrow b \equiv_n a$
3. $a \equiv_n b \ \wedge \ b \equiv_n c \Rightarrow a \equiv_n c$

Classes de congruência

Para calcularmos o resto da divisão de 171 por 14 podemos deslocar-nos na recta real em direcção à origem, 14 unidades de cada vez, até atingirmos um inteiro positivo inferior a 14.

Todos os valores intermédios obtidos têm o mesmo resto que 171 quando divididos por 14 e portanto são todos congruentes módulo 14.

$$\underset{}{0} \overset{}{\longleftarrow} \underset{3}{3} \overset{14}{\longleftarrow} \underset{}{17} \overset{14}{\longleftarrow} \cdots \overset{14}{\longleftarrow} \underset{}{143} \overset{14}{\longleftarrow} \underset{}{157} \overset{14}{\longleftarrow} \underset{}{171}$$

$$171 \equiv_{14} 157 \equiv_{14} 143 \equiv_{14} \cdots \equiv_{14} 17 \equiv_{14} 3$$

Classes de congruência

Definição

Dados $n \in \mathbb{N}$ e $a \in \mathbb{Z}$, chama-se classe de congruência de a módulo n ao conjunto de todos os inteiros que têm o mesmo resto que a quando divididos por n, e representa-se por: $[a]_n$.

Nota : Existem n restos possíveis na divisão por n: $0, 1, 2, 3, \cdots, n-1$ e portanto existem n classes de congruência módulo n.

A classe de congruência de 3 módulo 14 é constituida por todos os inteiros que divididos por 14 dão resto 3.

$$[3]_{14} = \{ \cdots, -25, -11, 3, 17, 31, \cdots \}$$

$$[3]_{14} = [-25]_{14} = [-11]_{14} = [17]_{14} = [31]_{14}$$

O conjunto $\mathbb{Z}_n$

Definição

Dado $n \in \mathbb{N}$ o conjunto de todas as classes de congruência módulo n representa-se por $\mathbb{Z}_n$ e diz-se o conjunto quociente de $\mathbb{Z}$ pela relação $\equiv_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$$

Neste conjunto definem-se as operações $+$ e $\times$ da seguinte forma:

$$[a]_n + [b]_n = [a+b]_n \qquad [a]_n \times [b]_n = [a \times b]_n$$

Exemplo :

$$[4]_7 + [5]_7 = [9]_7 = [2]_7$$

$$[4]_7 \times [5]_7 = [20]_7 = [6]_7$$

Sistema completo de resíduos módulo n

Definição

Dado $n \in \mathbb{N}$ chama-se sistema completo de resíduos (ou restos) módulo n a qualquer conjunto de n inteiros que tenha exactamente um representante de cada classe de congruência módulo n .

Exemplo :

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$$

é um sistema completo de resíduos módulo 14

$$\{14, 29, -12, 17, 32, 5, -8, -7, 22, 37, -4, -3, -2, -1\}$$

também é um sistema completo de resíduos módulo 14

Proposição

Dados $n \in \mathbb{N}$ *e* $a, b, c, d \in \mathbb{Z}$*:*

1. $a \equiv_n b \quad \wedge \quad c \equiv_n d \quad \Rightarrow \quad a + c \equiv_n b + d$
2. $a \equiv_n b \quad \wedge \quad c \equiv_n d \quad \Rightarrow \quad ac \equiv_n bd$
3. $a \equiv_n b \quad \Rightarrow \quad a + c \equiv_n b + c$
4. $a \equiv_n b \quad \Rightarrow \quad ac \equiv_n bc$
5. $a \equiv_n b \quad \Rightarrow \quad a^k \equiv_n b^k \qquad \forall\, k \in \mathbb{N}$

Congruências - Exemplo 1

Queremos calcular o resto da divisão de $a \times b$ por 17, onde:

$$a = 132467 \times 17 + 11 \qquad b = 455344 \times 17 + 6$$

Como $a \equiv_{17} 11$ e $b \equiv_{17} 6$

pela propriedade 2

$$a \times b \equiv_{17} 11 \times 6$$

Logo

$$a \times b \equiv_{17} 66 \equiv_{17} 15$$

E portanto o resto da divisão de $a \times b$ por 17 é 15

Congruências - Exemplo 2

Queremos calcular o resto da divisão por 18 de:

$$131 \times 15 + 29 \times 142$$

$131 \equiv_{18} 5 \qquad (131 - 180 = -49 \quad \text{e} \quad -49 + 36 = -13 \equiv_{18} 5)$

$15 \equiv_{18} -3$

$29 \equiv_{18} 11 \equiv_{18} -7$

$142 \equiv_{18} -2 \qquad (142 - 180 = -38 \equiv_{18} -2)$

Logo, pelas propriedades das congruências:

$$131 \times 15 + 29 \times 142 \equiv_{18} 5 \times (-3) + (-7) \times (-2) = -15 + 14 = -1 \equiv_{18} 17$$

E portanto o resto da divisão é 17

Congruências - Exemplo 3

Queremos calcular o resto da divisão de 19^{279} por 17:

$$\text{Como} \quad 19 \equiv_{17} 2 \qquad \text{então} \qquad 19^{279} \equiv_{17} 2^{279}$$

Vamos agora procurar uma potência de base 2 que seja congruente módulo 17, com 1 ou -1.

$$2^4 = 16 \equiv_{17} -1$$

Dividindo o expoente 279 por 4, obtemos:

$$279 = 69 \times 4 + 3$$

e portanto

$$2^{279} = 2^{69\times 4+3} = 2^{69\times 4} \times 2^3 = (2^4)^{69} \times 2^3 \equiv_{17} (-1)^{69} \times 2^3 = -8 \equiv_{17} 9$$

E portanto o resto da divisão é 9

Congruências - Exemplo 4

Queremos calcular o resto da divisão de $135^{43} + 42^{131}$ por 13:

Como $135 \equiv_{13} 5$ e $42 \equiv_{13} 3$ então $135^{43} + 42^{131} \equiv_{13} 5^{43} + 3^{131}$

$$5^2 = 25 \equiv_{13} -1 \quad \text{e} \quad 43 = 21 \times 2 + 1$$

$$3^3 = 27 \equiv_{13} 1 \quad \text{e} \quad 131 = 43 \times 3 + 2$$

$$5^{43} = 5^{21\times 2+1} = (5^2)^{21} \times 5 \equiv_{13} (-1)^{21} \times 5 = -5 \equiv_{13} 8$$

$$3^{131} = 3^{43\times 3+2} = (3^3)^{43} \times 3^2 \equiv_{13} (1)^{43} \times 9 = 9$$

$$135^{43} + 42^{131} \equiv_{13} 5^{43} + 3^{131} \equiv_{13} 8 + 9 = 17 \equiv_{13} 4$$

E portanto o resto da divisão é 4

Critérios de divisibilidade

Dado um inteiro $a = \overline{a_k\, a_{k-1} \cdots a_3\, a_2\, a_1\, a_0}$ com $k+1$ algarismos, isto é:

$$a = a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_3 \times 10^3 + a_2 \times 10^2 + a_1 \times 10 + a_0$$

queremos calcular o resto da divisão de a por um inteiro positivo n.

Se $n = 3$ (ou $n = 9$) como $10 \equiv_3 1$, teremos

$$a \equiv_3 a_k \times 1^k + a_{k-1} \times 1^{k-1} + \cdots + a_3 \times 1^3 + a_2 \times 1^2 + a_1 \times 1 + a_0$$

e portanto

$$a \equiv_3 a_k + a_{k-1} + \cdots + a_3 + a_2 + a_1 + a_0$$

Critérios de divisibilidade

Se $n = 4$ como $10^2 \equiv_4 0$, teremos

$$a \equiv_4 a_1 \times 10 + a_0 = \overline{a_1\, a_0}$$

Se $n = 8$ como $10^3 \equiv_8 0$, teremos

$$a \equiv_8 a_2 \times 10^2 + a_1 \times 10 + a_0 = \overline{a_2\, a_1\, a_0}$$

Exemplo : $67389645127 \equiv_8 127 \equiv_8 7$

$$67389645127 \equiv_3 6+7+3+8+9+6+4+5+1+2+7 = 58 \equiv_3 -2 \equiv_3 1$$

Critérios de divisibilidade

Se $n = 11$ como $10 \equiv_{11} -1$, teremos

$$a \equiv_{11} a_k \times (-1)^k + a_{k-1} \times (-1)^{k-1} + \cdots + a_3 \times (-1)^3 + a_2 \times 1^2 + a_1 \times (-1) + a_0$$

e portanto

$$a \equiv_{11} a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$$

Exemplo : $645127 \equiv_{11} 7 - 2 + 1 - 5 + 4 - 6 = -1 \equiv_{11} 10$

Critérios de divisibilidade

Proposição

Seja $a = \overline{a_k\, a_{k-1} \cdots a_3\, a_2\, a_1\, a_0}$ *um inteiro com* $k+1$ *algarismos. Então*

- $a \equiv_2 a_0$
- $a \equiv_4 \overline{a_1\, a_0}$
- $a \equiv_8 \overline{a_2\, a_1\, a_0}$
- $a \equiv_5 a_0$
- $a \equiv_3 a_k + a_{k-1} + \cdots + a_3 + a_2 + a_1 + a_0$
- $a \equiv_9 a_k + a_{k-1} + \cdots + a_3 + a_2 + a_1 + a_0$
- $a \equiv_{11} a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$

Congruências lineares

Dados $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$ com $a \neq 0$, queremos encontrar todos os inteiros $x \in \mathbb{Z}$ tais que:

$$a\, x \equiv_n b$$

Esta expressão diz-se uma congruência linear (ou do 1º grau) na incógnita x.

Exemplo : A congruência linear

$$3\, x \equiv_7 5$$

tem solução, por exemplo: $x = 4$

Note-se que todos os elementos de $[4]_7 = \{\cdots, -10, -3, 4, 11, 18, \cdots\}$ são também solução. Basta-nos portanto procurar as soluções num sistema completo de resíduos módulo 7, por exemplo: $\{0, 1, 2, 3, 4, 5, 6\}$.

Congruências lineares - existência de solução

Sabemos que

$$a\,x \equiv_n b \iff n \mid a\,x - b$$

ou seja existe $y \in \mathbb{Z}$ tal que

$$a\,x - b = n\,y \iff a\,x - n\,y = b$$

Logo

$$a\,x \equiv_n b \text{ tem solução} \iff a\,x - n\,y = b \text{ tem solução}$$

Teorema

Dados $n \in \mathbb{N}$ *e* $a, b \in \mathbb{Z}$ *com* $a \neq 0$,

$$a\,x \equiv_n b \text{ tem solução} \iff \text{m.d.c.}(a, n) \mid b$$

Congruências lineares - unicidade da solução

Se a congruência linear

$$a\,x \equiv_n b$$

tem solução então $\text{m.d.c.}(a,n)|b$ e portanto

$$\text{m.d.c.}(a,n)|b \quad \wedge \quad \text{m.d.c.}(a,n)|a \quad \wedge \quad \text{m.d.c.}(a,n)|n$$

Logo podemos (e devemos!) dividir a, b, n por $\text{m.d.c.}(a,n)$ de forma a obter uma congruência linear equivalente, onde o módulo e o coeficiente da incógnita são primos entre si.

Exemplo : A congruência

$$33\,x \equiv_{45} 18$$

tem solução pois $\text{m.d.c.}(33,45) = 3|18$. Logo, dividindo por 3, temos:

$$33\,x \equiv_{45} 18 \quad \Leftrightarrow \quad 11\,x \equiv_{15} 6$$

Congruências lineares - unicidade da solução

Se $\text{m.d.c.}(a, n) = 1$ a congruência linear

$$a\ x \equiv_n b$$

tem solução e pela equação diofantina

$$a\ x - n\ y = b$$

sabemos que, dada uma solução x_0, a solução geral para a incógnita x, é dada por:

$$x = x_0 + n\ k \quad \text{com} \quad k \in \mathbb{Z} \qquad \text{ou seja} \qquad x = [x_0]_n$$

Teorema

Seja $a\ x \equiv_n b$ uma congruência linear. Se $\text{m.d.c.}(a, n) = 1$ então a congruência linear tem exactamente uma classe de congrência módulo n como solução.

Congruências lineares - Exemplo

$$33\,x \equiv_{45} 18 \quad \Leftrightarrow \quad 11\,x \equiv_{15} 6$$

Como $\text{m.d.c.}(11, 15) = 1$ a congruência tem exactamente uma solução módulo 15 e portanto basta procurar a única solução num sistema completo de resíduos módulo 15, por exemplo:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$

Como $x_0 = 6$ é solução da congruência, a solução geral é dada por:

$$x = [6]_{15} = 6 + 15\,k \quad \text{com} \quad k \in \mathbb{Z}$$

Note-se que a congruência linear tem 3 soluções módulo 45:

$$x = [6]_{45} \quad \vee \quad x = [21]_{45} \quad \vee \quad x = [36]_{45}$$

Resolução de Congruências Lineares

Sabemos que se $a\ x \equiv_n b$ é uma congruência linear e m.d.c.$(a, n) = 1$ então a congruência linear tem exactamente uma classe de congrência módulo n como solução.

Para encontrarmos essa solução temos os seguintes métodos:

1º Método Por tentativas - procurando a solução num sistema completo de resíduos módulo n .

2º Método Equação diofantina - usando o algoritmo de Euclides para encontrar as soluções da equação diofantina:

$$a\ x - n\ y = b$$

Resolução de Congruências Lineares

3º Método Redução do coeficiente - tentando reduzir o coeficiente a da incónita x, a 1 (ou -1), à semelhança do que fazemos na resolução de equações. Para este método vamos usar o seguinte resultado:

Proposição

Seja $a\ x \equiv_n b$ *uma congruência linear e* $k \in \mathbb{Z}$ *tal que:*

$$m.d.c.(n,k) = 1$$

Então:

$$\textit{(Regra 1)} \qquad a\ x \equiv_n b \iff k\ a\ x \equiv_n k\ b$$

e se $k|a$ *e* $k|b$

$$\textit{(Regra 2)} \qquad a\ x \equiv_n b \iff \frac{a}{k}\ x \equiv_n \frac{b}{k}$$

Resolução de Congruências Lineares - Exemplo 1

$$33\,x \equiv_{45} 18 \quad \overset{/3}{\Leftrightarrow} \quad 11\,x \equiv_{15} 6 \quad \Leftrightarrow \quad -4\,x \equiv_{15} 6 \quad \overset{/(-2)}{\Leftrightarrow}$$

$$2\,x \equiv_{15} -3 \quad \overset{\times 8}{\Leftrightarrow} \quad 16\,x \equiv_{15} -24 \quad \Leftrightarrow \quad x \equiv_{15} 6$$

Logo a solução da congruência é dada por

$$x = [6]_{15} = 6 + 15\,k \quad k \in \mathbb{Z}$$

Em alternativa também podíamos ter feito o seguinte:

$$2\,x \equiv_{15} -3 \quad \Leftrightarrow \quad 2\,x \equiv_{15} 12 \quad \overset{/2}{\Leftrightarrow} \quad x \equiv_{15} 6$$

Resolução de Congruências Lineares - Exemplo 2

$$4\,x \equiv_{17} 15 \quad \Leftrightarrow \quad 4\,x \equiv_{17} -2 \quad \underset{\times 4}{\Leftrightarrow} \quad 16\,x \equiv_{17} -8 \quad \Leftrightarrow$$

$$-x \equiv_{17} -8 \quad \underset{\times(-1)}{\Leftrightarrow} \quad x \equiv_{17} 8$$

Logo a solução da congruência é dada por

$$x = [8]_{17} = 8 + 17\,k \quad k \in \mathbb{Z}$$

Em alternativa também podíamos ter feito o seguinte:

$$4\,x \equiv_{17} 15 \quad \Leftrightarrow \quad 4\,x \equiv_{17} 32 \quad \underset{/4}{\Leftrightarrow} \quad x \equiv_{17} 8$$

Resolução de Congruências Lineares - Exemplo 3

$$32\,x \equiv_{23} 21 \quad \Leftrightarrow \quad 9\,x \equiv_{23} 21 \quad \Leftrightarrow \quad 3\,x \equiv_{23} 7 \quad \Leftrightarrow$$
$$/3 \qquad\qquad \times 8$$

$$24\,x \equiv_{23} 56 \quad \Leftrightarrow \quad x \equiv_{23} 10$$

Logo a solução da congruência é dada por

$$x = [10]_{23} = 10 + 23\,k \quad k \in \mathbb{Z}$$

Em alternativa também podíamos ter feito o seguinte:

$$3\,x \equiv_{23} 7 \quad \Leftrightarrow \quad 3\,x \equiv_{23} 30 \quad \Leftrightarrow \quad x \equiv_{23} 10$$
$$/3$$

Resolução de Congruências Lineares - Exemplo 4

Vamos agora usar este método para resolver uma equação diofantina:

$$18\,x + 5\,y = 48 \quad \Rightarrow \quad 18\,x \equiv_5 48 \quad \Leftrightarrow \quad 3\,x \equiv_5 3 \quad \underset{/3}{\Leftrightarrow} \quad x \equiv_5 1$$

Logo a solução da congruência é dada por

$$x = [1]_5 = 1 + 5\,k \quad k \in \mathbb{Z}$$

Substituindo na equação diofantina a solução $x_0 = 1$ obtemos para y o valor $y_0 = 6$. Logo a solução geral da equação diofantina é dada por:

$$\begin{cases} x = 1 + 5\,k \\ \\ y = 6 - 18\,k \qquad k \in \mathbb{Z} \end{cases}$$

Sistemas de congruências lineares

- Um sistema de congruências lineares terá solução se existir um valor $x \in \mathbb{Z}$ que satisfaça todas as congruências lineares do sistema.
- Obviamente, se uma das congruências lineares do sistema não tiver solução o sistema também não tem solução.
- No entanto é possível que todas as congruências lineares do sistema tenham solução mas o sistema seja impossível.

Sistemas de congruências lineares - Exemplo 1

Vejamos como podemos resolver um sistema de equações lineares usando o método de substituição :

$$\left\{\begin{array}{ll} 7\,x \equiv_{11} 1 & \times 3 \\ 5\,x \equiv_{8} 3 & \\ 8\,x \equiv_{14} 6 & /2 \end{array}\right. \iff \left\{\begin{array}{ll} 21\,x \equiv_{11} 3 & \\ 5\,x \equiv_{8} 3 & \\ 4\,x \equiv_{7} 3 & \end{array}\right. \iff \left\{\begin{array}{ll} -x \equiv_{11} 3 & \times(-1) \\ -3\,x \equiv_{8} 3 & /(-3) \\ -3\,x \equiv_{7} 3 & /(-3) \end{array}\right.$$

$$\left\{\begin{array}{l} x \equiv_{11} -3 \\ x \equiv_{8} -1 \\ x \equiv_{7} -1 \end{array}\right. \iff \left\{\begin{array}{l} \boxed{x = -3 + 11\,k} \\ -3 + 11\,k \equiv_{8} -1 \\ -3 + 11\,k \equiv_{7} -1 \end{array}\right. \iff (*) \left\{\begin{array}{ll} \cdots & \\ 3\,k \equiv_{8} 2 & \times(3) \\ 4\,k \equiv_{7} 2 & \times(2) \end{array}\right.$$

$$\left\{\begin{array}{l} \cdots \\ 9\,k \equiv_{8} 6 \\ 8\,k \equiv_{7} 4 \end{array}\right. \iff \left\{\begin{array}{l} \cdots \\ k \equiv_{8} -2 \\ k \equiv_{7} 4 \end{array}\right. \iff \left\{\begin{array}{l} \cdots \\ \boxed{k = -2 + 8\,u} \\ -2 + 8\,u \equiv_{7} 4 \end{array}\right.$$

$(*)$ Na resolução de uma congruência linear podemos passar qualquer termo de um membro para o outro, trocando-lhe o sinal (Propriedade 3).

Sistemas de congruências lineares -Exemplo 1

$$\begin{cases} \boxed{x = -3 + 11\,k} \\ \boxed{k = -2 + 8\,u} \\ u \equiv_7 6 \end{cases} \iff \begin{cases} \cdots \\ \cdots \\ u \equiv_7 -1 \end{cases} \iff \begin{cases} \boxed{x = -3 + 11\,k} \\ \boxed{k = -2 + 8\,u} \\ \boxed{u = -1 + 7\,t} \end{cases}$$

$$x = -3 + 11\,k = -3 + 11(-2 + 8\,u) = -3 - 22 + 88\,u = -25 + 88(-1 + 7\,t) = -25 - 88 + 616\,t = -113 + 616\,t$$

A solução geral do sistema é então:

$$x = [-113]_{616} = -113 + 616\,t \quad t \in \mathbb{Z}$$

- Note-se que existe uma única solução módulo $616 = 11 \times 8 \times 7$.
- Se na resolução do sistema pelo método de substituição obtivermos uma congruência linear impossível, isso significa que o sistema não tem solução.

Sistemas de congruências lineares

Teorema

Seja $a\ x \equiv_n b$ *uma congruência linear e sejam* $r, s \in \mathbb{Z}$ *tais que* $n = r \times s$ *e* $m.d.c.(r.s) = 1$ *. Então:*

$$a\ x \equiv_n b \quad \Longleftrightarrow \quad \begin{cases} a\ x \equiv_r b \\ a\ x \equiv_s b \end{cases}$$

Corolário

Se $n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \cdots\ p_k^{\alpha_k}$ *é a decomposição de* n *em números primos:*

$$a\ x \equiv_n b \quad \Longleftrightarrow \quad \begin{cases} a\ x \equiv_{p_1^{\alpha_1}} b \\ a\ x \equiv_{p_2^{\alpha_2}} b \\ \cdots \\ a\ x \equiv_{p_k^{\alpha_k}} b \end{cases}$$

Sistemas de congruências lineares - Exemplo 2

Vamos usar o Teorema para resolver a seguinte congruência linear:

$$17\,x \equiv_{276} 9$$

Como

$$276 = 280 - 4 = 4(70 - 1) = 4 \times 69 = 2^2 \times 3 \times 23$$

temos que:

$$17\,x \equiv_{276} 9 \quad \Longleftrightarrow \quad \begin{cases} 17\,x \equiv_4 9 \\ 17\,x \equiv_3 9 \\ 17\,x \equiv_{23} 9 \end{cases}$$

Sistemas de congruências lineares - Exemplo 2

$$\left\{\begin{array}{l} 17\,x \equiv_4 9 \\ 17\,x \equiv_3 9 \\ 17\,x \equiv_{23} 9 \end{array}\right. \iff \left\{\begin{array}{ll} x \equiv_4 1 & \\ -x \equiv_3 0 & \times(-1) \\ -6\,x \equiv_{23} 9 & /(-3) \end{array}\right. \iff \left\{\begin{array}{ll} x \equiv_4 1 & \\ x \equiv_3 0 & \\ 2\,x \equiv_{23} -3 & \times 12 \end{array}\right.$$

$$\left\{\begin{array}{l} x \equiv_4 1 \\ x \equiv_3 0 \\ 24\,x \equiv_{23} -36 \end{array}\right. \iff \left\{\begin{array}{l} x \equiv_4 1 \\ x \equiv_3 0 \\ x \equiv_{23} 10 \end{array}\right. \iff \left\{\begin{array}{l} 10 + 23\,k \equiv_4 1 \\ 10 + 23\,k \equiv_3 0 \\ \boxed{x = 10 + 23\,k} \end{array}\right.$$

$$\left\{\begin{array}{ll} -k \equiv_4 -9 & \times(-1) \\ -k \equiv_3 -10 & \times(-1) \\ \cdots & \end{array}\right. \iff \left\{\begin{array}{l} k \equiv_4 9 \\ k \equiv_3 10 \\ \cdots \end{array}\right. \iff \left\{\begin{array}{l} k \equiv_4 1 \\ k \equiv_3 1 \\ \cdots \end{array}\right.$$

Sistemas de congruências lineares - Exemplo 2

$$\begin{cases} k \equiv_{12} 1 \\ \boxed{x = 10 + 23\ k} \end{cases} \iff \begin{cases} \boxed{k = 1 + 12\ t} \\ \boxed{x = 10 + 23\ k} \end{cases}$$

Logo

$$x = 10 + 23\ k = 10 + 23(1 + 12\ t) = 33 + 276\ t \qquad t \in \mathbb{Z}$$