# IA012 - Tarefa 5

Rodrigo Seiji Piubeli Hirao (186837)

16 de dezembro de 2021

**01)** gcd(a, b) = gcd(b, a mod b)

**gcd(973, 301) = 7**

| Dividendo | Divisor | Resto |
|---|---|---|
| 973 | 301 | 70 |
| 301 | 70 | 21 |
| 70 | 21 | 7 |
| 21 | **7** | 0 |

**gcd(787, 301) = 1 (coprimos)**

| Dividendo | Divisor | Resto |
|---|---|---|
| 787 | 301 | 185 |
| 301 | 185 | 116 |
| 185 | 116 | 69 |
| 116 | 69 | 47 |
| 69 | 47 | 22 |
| 47 | 22 | 3 |
| 22 | 3 | 1 |
| 3 | **1** | 0 |

**gcd(973, 301) = 1 (coprimos)**

| Dividendo | Divisor | Resto |
|---|---|---|
| 973 | 787 | 186 |
| 787 | 186 | 43 |
| 186 | 43 | 14 |
| 43 | 14 | 1 |
| 14 | **1** | 0 |

**02)** Temos a seguinte tabela

| Dividendo | Divisor | Quociente | Resto |
|---|---|---|---|
| $a_4$ | $a_3$ | 2 | $a_2$ |
| $a_3$ | $a_2$ | 1 | $a_1$ |
| $a_2$ | $a_1$ | 3 | 20 |
| $a_1$ | **20** | 2 | 0 |

Que pode ser resolvida a seguir

$$\begin{cases} a_1 = 20 \times 2 + 0 = 40 \\ a_2 = a_1 \times 3 + 20 = 140 \\ a_3 = a_2 \times 1 + a_1 = 180 \\ a_3 = a_2 \times 1 + a_1 = 180 = y \\ a_4 = a_3 \times 2 + a_2 = 500 = x \end{cases} \tag{1}$$

| Dividendo | Divisor | Quociente | Resto |
|---|---|---|---|
| $x = 500$ | $y = 180$ | 2 | 140 |
| 180 | 140 | 1 | 40 |
| 140 | 40 | 3 | 20 |
| 40 | **20** | 2 | 0 |

**03)** $5000 mod 7 = 6$, logo $segunda - feira + 6 = domingo$

**04)** Prove que $(2^{20} - 1) mod 41 = 0$

$$(2^{20} - 1) mod 41 = r, 0 \leq r < 41$$

$$2^{20} - 1 \equiv r(mod 41) \rightarrow 41|(2^{20} - 1 - r)$$

$$2^{20} \equiv r + 1(mod 41)$$

$$2^{10} mod 41 \times 2^{10} mod 41 \equiv r + 1(mod 41)$$

$$(2^4 mod 41 \times 2^6 mod 41) mod 41 \times (2^4 mod 41 \times 2^6 mod 41) mod 41 \equiv r + 1(mod 41)$$

$$(16 \times 23) mod 41 \times (16 \times 23) mod 41 \equiv r + 1(mod 41)$$

$$368 mod 41 \times 368 mod 41 \equiv r + 1(mod 41)$$

$$40 \times 40 \equiv r + 1(mod 41)$$

$$1600 \equiv r + 1(mod 41)$$

$$410 + 410 + 410 + 370 \equiv r + 1(mod 41)$$

$$370 \equiv r + 1(mod 41)$$

$$370 \equiv r + 1(mod 41)$$

$$1 \equiv r + 1(mod 41)$$

$$r = 0$$

**05)** Podemos considerar que $gcd(a, b) = xa + yb$, logo que o máximo divisor comum entre a e b é uma combinação linear de a e b, e os coeficientes da combinação linear pode ser calculado usando o AEE. Sendo o AEE uma extensão do algoritmo de Euclides com o cálculo iterativo de $x_n$ e $y_n$ da forma do sistema 02, onde $k_n$ é o quoeficiente da divisão, de forma que $gcd(a, b) = x_{n-1}a + y_{n-1}b$

$$\begin{cases} x_{-2} = 1 \\ x_{-1} = 0 \\ y_{-2} = 0 \\ y_{-1} = 1 \\ x_n = x_{n-2} - k_n x_{n-1} \\ y_n = y_{n-2} - k_n y_{n-1} \end{cases} \tag{2}$$

| a | b | $k_1$ | $r_i$ | $x_i$ | $y_i$ | Bezóut |
|---|---|---|---|---|---|---|
| | | | | 1 | 0 | |
| | | | | 0 | 1 | |
| $a_1$ | $a_2$ | $k_1$ | $r_1$ | $1 - k_1 \times 0$ | $0 - k_1 \times 1$ | $r_i$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $a_{n-1}$ | $b_{n-1}$ | $k_{n-1}$ | $gcd(a,b)$ | $\mathbf{x}_{n-1}$ | $\mathbf{y}_{n-1}$ | $gcd(a,b)$ |
| $a_n$ | $b_n$ | $k_n$ | 0 | $x_n$ | $y_n$ | 0 |

**06)** Se $gcd(a,b) = 1$ então temos que os coeficientes também são inversos multiplicativos ($bb^{-1} \equiv 1(moda)$), que pode ser provado da forma a seguir

$$xa + yb = 1 \rightarrow yb = 1 - xa$$

$$yb \equiv 1moda \rightarrow b^{-1} = y$$

Por conseguência $a^{-1} = x$

**07)** Todo elemento $w$ do corpo $Z_p$, exceto 0, possui um inverso multiplicativo $w^{-1}$, tal que $ww^{-1} \equiv 1modp$

**08)** A partir do AEE temos que o inverso multiplicativo de 6762 é 1582 no corpo $Z_{10007}$

| a | b | $k_1$ | $r_i$ | $x_i$ | $y_i$ | Bezóut |
|---|---|---|---|---|---|---|
| | | | | 1 | 0 | |
| | | | | 0 | 1 | |
| 10007 | 6762 | 1 | 3245 | 1 | -1 | 3245 |
| 6762 | 3245 | 2 | 272 | -2 | 3 | 272 |
| 3245 | 272 | 11 | 253 | 23 | -34 | 253 |
| 272 | 253 | 1 | 19 | -25 | 37 | 19 |
| 253 | 19 | 13 | 6 | 338 | -515 | 6 |
| 19 | 6 | 3 | 1 | -413 | **1582** | 1 |

**09)** Devemos provar que $a \cdot b = b \cdot a$, ou, no caso, $a - b + 3 = b - a + 3$, mas temos que essa identidade é verdadeira apenas quando $a = b$, ou seja, G não é um grupo abeliano.

**10)** Todos os conjuntos respeitam as regras A1 à A3 e A5, sendo 0 o elemento identidade aditivo.

A partir do conjunto dos inteiros A4 é satisfeito com números negativos, que também respeitam as regras M1 à M6, tendo 1 como o elemento de identidade multiplicativa.

A partir dos conjuntos racionais M7 também é satisfeita, com $a^{-1} = \frac{1}{a}$, $a \neq 0$

Então temos que nos escalares:

- Naturais - (nada)
- Inteiros - Anel de Integridade
- Racionais - Corpo

Enquanto nas matrizes quadradas temos que $A \times B \neq B \times A$, logo não satisfas M4, assim sendo grupos

- Matriz quadrada com números inteiros - Grupo
- Matriz quadrada com números reais - Grupo