

OBTENIR UN INVERSE PAR L'ALGORITHME D'EUCLIDE

CLASSE INVERSE  
ALGORITHME  
D'EUCLIDE  
PGCD

ADC  
C7

$$[511]_{1000}^{-1} \implies 511x = 1000y + 1$$

TARICANT

$$y = \begin{matrix} 1 \\ -1 \\ 2 \\ -2 \end{matrix} \left| \begin{array}{l} 511x = 1001? \\ 511x = -999 \\ 511x = 2001 \\ 511x = -1999 \end{array} \right.$$

IMPOSSIBLE.

① CALCUL DU PGCD (1000, 511)

$$1000 = 1 \cdot 511 + 489$$

$$511 = 1 \cdot 489 + 22$$

$$489 = 22 \cdot 22 + 5$$

$$22 = 4 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + \boxed{1} \leftarrow \text{DRNN} \quad \text{donc } [511]_{1000}^{-1} \text{ existe! (1)}$$

② RENOUVE DE L'ALGORITHME D'EUCLIDE.

VOIR FOCUS ADC 07 B

LA RENOUVEE DONNE  $209_M - 409a = 1$

$$[511]_{1000}^{-1} = [a]_M^{-1} = [-409]_{1000} = [591]_{1000}$$

LE PASSAGE S'EFFECTUE COMME CECI:

$$409 \oplus 591 = 1000$$

ça s'annule!

③ REECRIRE

L'inverse de  $[511]_{1000}^{-1}$  est  $[591]_{1000}$



~~a = 0~~ 1. REECRIRE EN PACAT les équations.

RECHERCHE  
ALGORITHME  
D'EUCLIDE

ADC  
C7  
B

$$a = \boxed{1}b + r_1$$

$$b = \boxed{1}r_1 + r_2$$

$$r_1 = \boxed{22}r_2 + r_3$$

$$r_2 = \boxed{4}r_3 + r_4$$

$$r_3 = \boxed{2}r_4 + r_5 \leftarrow \text{DRNN}$$

$$n = \boxed{\phantom{00}}a + r_1$$

⚠ en cours de route a devient n  
b devient a

2. Ecrire la ligne où reste DRNN = 1  
RACER les r correspondants  
seuls les fleches.

$$\begin{array}{ccccc} 5 & = & 2 & \times & 2 & + & 1 \\ \uparrow & & \uparrow & & \uparrow & & \\ r_3 & & r_4 & & r_5 & & \end{array}$$

REECRIRE LA LIGNE DE LA RAO PAS EN RETENANT  
LE DRNN à 1, ou RS.

$$\boxed{r_3 = 2r_4 + r_5}$$

$$r_3 = 2r_4 + 1$$

$$r_5 = 1$$

$$1 = r_3 - 2r_4 \leftarrow \text{ISOLER LE 1}$$

3. SE DERBARASSER des R de du + grand au + petit.

3.1 REVENIR A GRILLE. EN REPACAT les équations du plus grand R au plus petit R.

$$\begin{array}{rcl} r_5 & = & r_3 - \boxed{2}r_4 \\ r_4 & = & r_2 - \boxed{4}r_3 \\ \hline r_3 & = & r_1 - \boxed{22}r_2 \\ r_2 & = & b - \boxed{1}r_1 \\ r_1 & = & a - \boxed{1}b \end{array}$$

$$\left. \begin{array}{l} 1 = r_3 - 2r_4 \\ 1 = r_3 - 2(r_2 - 4r_3) \\ 1 = r_3 - 2r_2 + 8r_3 \\ 1 = -2r_2 + 9r_3 \end{array} \right\} r_4 \text{ éliminé}$$

$$\left. \begin{array}{l} 1 = -2r_2 + 9(r_1 - 22r_2) \\ 1 = -2r_2 + 9r_1 - 198r_2 \\ 1 = 9r_1 - 200r_2 \end{array} \right\} r_3$$

$$\left. \begin{array}{l} 1 = 9r_1 - 200(b - 1r_1) \\ 1 = 9r_1 - 200b + 200r_1 \\ 1 = -200b + 209r_1 \\ 1 = -200b + 209(a - 1b) \\ 1 = -200b + 209a - 209b \end{array} \right\} r_2$$

$$1 = -409b + 209a$$

$$\left. \begin{array}{l} 1 = -200b + 209a - 209b \\ 1 = -409b + 209a \end{array} \right\} r_1$$