

CLASSE INVERSE par CORRECTION de TIR:

CLASSE INVERSE
CORRECTION DE
TIR

ADC
C8

$[19]_{31}^{-1} \Rightarrow$ j'approche 31 par un multiple simple de 19

$19 \cdot 2 = 38$ c'est 2 qui ne permet d'aller le
meins loin de 31 avec 19,
j'obtiens 38

1^{er} TIR = 2.

$38 - 31$ je fais resultat - 31 j'obtiens 7

\Downarrow je réécrit

7 mod 31

$35 - 31$

2^{ème} TIR = 5

$$7 \cdot 5 = 35 \equiv 4 \pmod{31}$$

$32 - 31$

3^{ème} TIR = 8

$$4 \cdot 8 = 32 \equiv 1 \pmod{31}$$

\Downarrow

Réécrire la conclusion.

$$19 \cdot (2 \cdot 5 \cdot 8) \equiv 1 \pmod{31}$$

$$\text{d'où } [19]_{31}^{-1} = [2]_{31} \cdot [40]_{31} = [2]_{31} \cdot [9]_{31} = [18]_{31}$$

$r = 40 - 31$

1^{ère} FACIL.
EN GROUPANT
5 et 8

$$19 \cdot (2 \cdot 5 \cdot 8) \equiv 1 \pmod{31}$$

$$\text{d'où } [19]_{31}^{-1} = [10]_{31} \cdot [8]_{31} = [80]_{31} = [18]_{31}$$

$r = 80 - 31 \times 2$

2^{ème} FACIL.
EN GROUPANT
2 et 5

TROP PETITS
PAR FAIRE DES
GROUPES

j'aurais pu grouper
2.5.8 e même
tape et taper
sur $[80]_{31}$

LA CLASSE INVERSE de $[19]_{31}^{-1}$ est $[18]_{31}$