

Feuille 1 : Arithmétique dans \mathbb{Z}

Exercice 1.

1. Donner la liste des entiers positifs qui divisent 100.
2. Combien le nombre 600000 a-t-il de diviseurs positifs ?
3. Combien $13!$ admet-il de diviseurs ?

Exercice 2. Combien d'entiers strictement compris entre 101 et 1001 sont divisibles par 7 ?

Exercice 3. La différence de deux nombres entiers est 538. Si l'on divise l'un par l'autre, le quotient est 13 et le reste 22. Quels sont ces nombres ?

Exercice 4. Quels sont les restes possibles de la division euclidienne d'un entier impair par 4 ? En déduire que le reste du carré d'un entier impair dans la division euclidienne par 8 est 1.

Exercice 5. Les nombres a, b, c, d étant des éléments non nuls de \mathbb{Z} , dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si a divise b et b divise c , alors a divise c .
2. Si a divise b et c , alors a divise $2b + 3c$.
3. Si a divise b et c , alors $c^2 - 2b$ est multiple de a .
4. S'il existe u et v entiers tels que $au + bv = 4$ alors $\text{pgcd}(a, b) = 4$.
5. Si a est premier avec b , alors a est premier avec b^3 .
6. Si a divise $b + c$ et $b - c$, alors a divise b et a divise c .
7. Si $7a - 9b = 1$ alors a et b sont premiers entre eux.
8. Si a divise b et b divise c et c divise a , alors $|a| = |b|$.
9. Si 19 divise ab , alors 19 divise a ou 19 divise b .
10. Si a est multiple de b et si c est multiple de d , alors $a + c$ est multiple de $b + d$.
11. « a et b premiers entre eux » équivaut à « $\text{ppcm}(a, b) = |ab|$ ».
12. Si a divise c et b divise d , alors ab divise cd .
13. Si 9 divise ab et si 9 ne divise pas a , alors 9 divise b .
14. Si a divise b ou a divise c , alors a divise bc .
15. « a divise b » équivaut à « $\text{ppcm}(a, b) = |b|$ ».
16. Si a divise b , alors a n'est pas premier avec b .
17. Si a n'est pas premier avec b , alors a divise b ou b divise a .
18. Si 4 ne divise pas bc , alors b ou c est impair.
19. Si a divise b et b ne divise pas c , alors a ne divise pas c .
20. Si 5 divise b^2 , alors 25 divise b^2 .
21. Si 12 divise b^2 , alors 4 divise b .
22. Si 12 divise b^2 , alors 36 divise b^2 .
23. Si 91 divise ab , alors 91 divise a ou 91 divise b .

Exercice 6.

1. Montrer que le produit de trois nombres consécutifs est divisible par 6.
2. Montrer que le produit de quatre nombres consécutifs est divisible par 24.

Exercice 7. Pour chaque entier $n \in \{8, 16, 6, 12, 30, 90, 98, 72, 8100, 900\}$ trouver le plus petit entier positif m tel que n divise m^2 .

Exercice 8. Ecrire le nombre 2017 en base 7.

Exercice 9. Soit n l'entier naturel dont l'écriture en base 9 est 512121. Ecrire n en base 10.

Exercice 10. Ecrire en base 7 le nombre qui s'écrit 713 en base 8.

Exercice 11.

1. Décomposer $10!$ en produit de facteurs premiers.
2. Trouver la plus grande puissance de 2 qui divise $100!$.
3. Trouver le nombre de zéros qui figurent à la fin de l'écriture décimale de $100!$.

Exercice 12. Soit $n \in \mathbb{N}^*$. On considère M_n l'entier dont l'écriture en base 2 est composée de n un. Par exemple, $M_3 = 111$. Donner l'écriture en base deux de M_n^2 .

Exercice 13. Trouver le pgcd et le ppcm de $a = 2^3 \times 3^5 \times 7^2$ et $b = 2 \times 5^2 \times 7^3$.

Exercice 14. Soit n un entier tel que $10 \leq n \leq 100$. Montrer que n est un nombre premier si et seulement si $\text{pgcd}(n, 210) = 1$.

Exercice 15. Soit a, b, c des entiers non nuls.

1. Montrer que $\text{pgcd}(ca, cb) = |c| \text{pgcd}(a, b)$.
2. Montrer que $\text{pgcd}(a^2, b^2) = (\text{pgcd}(a, b))^2$.
3. Montrer que si $\text{pgcd}(a, b) = 1$ et si c divise a , alors $\text{pgcd}(c, b) = 1$.
4. Montrer que $\text{pgcd}(a, bc) = 1$ si et seulement si $\text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$.
5. Montrer que si $\text{pgcd}(a, b) = 1$ alors $\text{pgcd}(a+b, a-b) = 1$ ou 2 et $\text{pgcd}(a+b, ab) = 1$.

Exercice 16. Soit n un entier positif. Que vaut $\text{pgcd}(n, n+1)$ et $\text{ppcm}(n, n+1)$?

Exercice 17.

1. Calculer le pgcd de 637 et 595.
2. Trouver les entiers x et y tels que $637x + 595y = 91$.
3. Trouver les entiers x et y tels que $637x + 595y = 143$.

doutau@idif.fr

Cours

a divise b
 $\Leftrightarrow \exists k \in \mathbb{N}$ tel que $b = ak$

p : premier

\Leftrightarrow Si $a \in \mathbb{N}$ divise p alors

$a = 1$ ou $a = p$ & $p \neq 1$

Soit $a \in \mathbb{N} \setminus \{0\}$

On peut décomposer a

Soit la forme $a = p^\alpha q^\beta \dots$

p, q des nombres premiers

Ex 1, 2, 3, 4, 6, 7

$$100 \begin{array}{c} | \\ \text{f} \\ \hline b \end{array}$$

$$b \begin{array}{c} | \\ \text{f} \\ \hline a \end{array}$$

1y

$$\begin{array}{r|l} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

$$1, 2, 4, 5, 10, 20, 25 \\ 50, 100$$

$$100 = 10 \times 10$$

Si a divise 100
 $a = 2^\alpha 5^\beta$

avec $0 \leq \alpha \leq 2$

$0 \leq \beta \leq 2$ 3 choix

$\alpha = 0, \beta = 0 \quad a = 2^0 \times 5^0 \cdot 1$ décomposition en

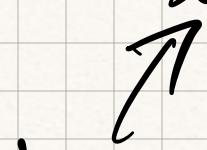
$\alpha = 0, \beta = 1 \quad a = 5$

$\alpha = 0, \beta = 2 \quad a = 25$

$\alpha = 1, \beta = 0 \quad a = 2$

$$= 2 \times 5 \times 2 \times 5$$

$$= 2^2 \times 5^2$$



facteur premier de 100

$$a = 10$$

∴

$$\text{d}y \quad 6000000 = 6 \times 1000000$$

$$= 2 \times 3 \times (10)^6$$

$$= 2 \times 3 \times (2 \times 5)^6$$

$$= 2^7 \times 3 \times 5^6$$

$$6000000 = 2 \times 3000000$$

$$= 2 \times 2 \times 1500000$$

$$= 2 \times 2 \times 2 \times 1500000$$

$$= 2^4 \times 375000$$

$$= 2^5 \times 187500$$

$$= 2^6 \times 93750$$

$$= 2^7 \times 46875$$

$$= 2^7 \times 5 \times 9375$$

$$\begin{aligned}
 &= 2^7 \times 5^2 \times 1875 \\
 &= 2^7 \times 5^3 \times 375 \\
 &= 2^7 \times 5^4 \times 75 \\
 &= 2^7 \times 5^5 \times 15 \\
 &= 2^4 \times 5^6 \times 3 \\
 &= 2^4 \times 3 \times 5^6
 \end{aligned}$$

Si a divise 6 000 000

$$a = 2^\alpha 3^\beta 5^\gamma$$

avec $0 \leq \alpha \leq 7$ 8 choix

$0 \leq \beta \leq 1$ 2 choix

$0 \leq \gamma \leq 6$ 7 choix

$\Rightarrow 8 \times 2 \times 7$ diviseurs

$\Rightarrow 112$ diviseurs

3x Cambien 13! admet-il de diviseurs?

$$\begin{aligned}13^! &= 13 \times 12 \times 11 \times 10 \times \\&\quad 9 \times 8 \times 7 \times 6 \times 5 \times 4 \\&\quad \times 3 \times 2 \times 1 \\&= 13 \times 2^2 \times 3 \times 11 \times 2 \times 5 \\&\quad \times 3 \times 3 \times 2 \times 2 \times 7 \times 2 \times 3 \\&\quad \times 5 \times 2 \times 2 \times 3 \times 2 \times 1 \\&= 13 \times 11 \times 7 \times 5^2 \\&\quad \times 3^5 \times 2^{10} \times 1\end{aligned}$$

$$\begin{aligned}&= 2^{10} \times 3^5 \times 5^2 \times 7 \times 11 \times 13 \\&= 2^A 3^B 5^C 7^D 11^E 13^F\end{aligned}$$

$$0 \leq A \leq 10 \quad 11$$

$$0 \leq B \leq 5 \quad 6$$

$$\begin{array}{ccccc}0 & 1 & 2 & 3 & 4 \\0 & 1 & 2 & 1 & 2 \\0 & 1 & 1 & 2 & 2\end{array}$$

$$14 \times 6 = 3 \times 2 \times 2 \times 2$$

$$= 1584 \text{ diviseurs positifs}$$

3168 diviseurs de 13!

Ex 2

Multiples de 7 strictement compris entre 101 et 1000

Si $a \in_{101} 102, \dots, 1000$ et a divise 7 alors $a = k7$

avec $102 \leq k7 \leq 1000$

$$\Rightarrow 102 : 7 \leq k \leq 1000 : 7 \Leftrightarrow 15 \leq k \leq 143$$

$$\Rightarrow 15 \leq k \leq 143$$

$$\text{abanc} \quad 143 - 15 \quad \text{possibilités}$$

$$= 128$$

$$k \in \{15, \dots, 143\}$$

Ex 3

$$\begin{aligned} * a - b &= 538 \\ a &= 13b + 22 \end{aligned}$$

ou

$$b = 13a + 22$$

$$\left\{ \begin{array}{l} a = 538 + b \\ a = 13b + 22 \end{array} \right. \quad \text{ou} \quad \left\{ \begin{array}{l} b = a - 538 \\ b = 13a + 22 \end{array} \right.$$

$$\Leftrightarrow \left\{ \begin{array}{l} 13b + 22 = 538 + b \\ a = 538 + b \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} 13a + 22 = 538 \\ b = 13a + 22 \end{array} \right.$$

$$\Leftrightarrow \left\{ \begin{array}{l} 12b = 516 \\ a = 538 + b \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} 12a = 560 \\ b = 13a + 22 \end{array} \right.$$

$$\left\{ \begin{array}{l} b = 516/12 = 43 \Leftrightarrow \\ a = 538 + 43 = 581 \end{array} \right. \quad \left\{ \begin{array}{l} a = -560/12 \\ \text{pas de solution} \end{array} \right.$$

$\Rightarrow A$

Soit n impair

$$\exists k \in \mathbb{N} \text{ tel que } n = 2k + 1$$

- Si k est pair, $k = 2l$ pour $l \in \mathbb{N}$
 alors $n = 2(2l) + 1$
 $= 4l + 1$

$$\text{donc } n \equiv 1 \pmod{4}$$

- Si k est impair, il existe $l \in \mathbb{N}$,
 $k = (2l + 1)$

$$\text{alors } n = 2(2l + 1) + 1$$

$$\text{donc } n = 4l + 3 \pmod{4}$$

Donc si n est impair

$$\rightarrow n \equiv 1 \pmod{4}$$

$$\text{ou } n \equiv 3 \pmod{4}$$

Sait n impair

- Si $n = 4k+1$, alors

$$\begin{aligned} n^2 &= (4k+1)^2 \\ &= 16k^2 + 8k + 1 \\ &= 8(2k^2 + k) + 1 \\ &\in \mathbb{N} \end{aligned}$$

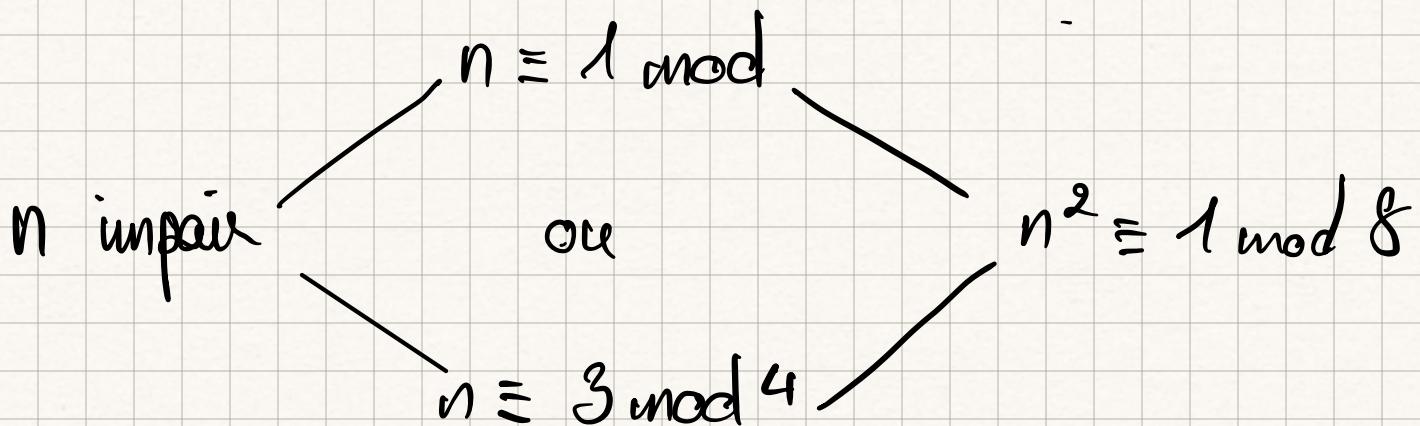
$$= (8k+1)$$

donc $n^2 \equiv 1 \pmod{8}$

- Si $n = 4k+3$

$$\begin{aligned} n^2 &= (4k+3)^2 \\ &= 16k^2 + 24k + 9 \\ &= 8(2k^2 + 3k + 1) + 1 \end{aligned}$$

donc $n^2 \equiv 1 \pmod{8}$



Ex6 :

Soit $n \in \mathbb{N}$

$$n(n+1)(n+2) \equiv 0 \pmod{6}$$

Il suffit de montrer que

ay $\frac{2}{n(n+1)(n+2)}$

by $\frac{3}{n(n+1)(n+2)}$

ay Si n pair $\frac{2}{n}$ donc

(Si $\frac{a}{b}$ alors $\frac{a}{bk} \Rightarrow bk = (lk)_a \Leftrightarrow \exists l \in \mathbb{N} \text{ tq } b=la$)

$$\frac{2}{n(n+1)(n+2)}$$

Si n impair, $n+1$ est paire et $\frac{2}{n+1}$ donc

$$\frac{2}{n(n+1)n+2} \text{ dans tout les cas } \frac{2}{n(n+1)(n+2)}$$

$$\text{By } n = 3q + r \quad r \in \mathbb{N}$$

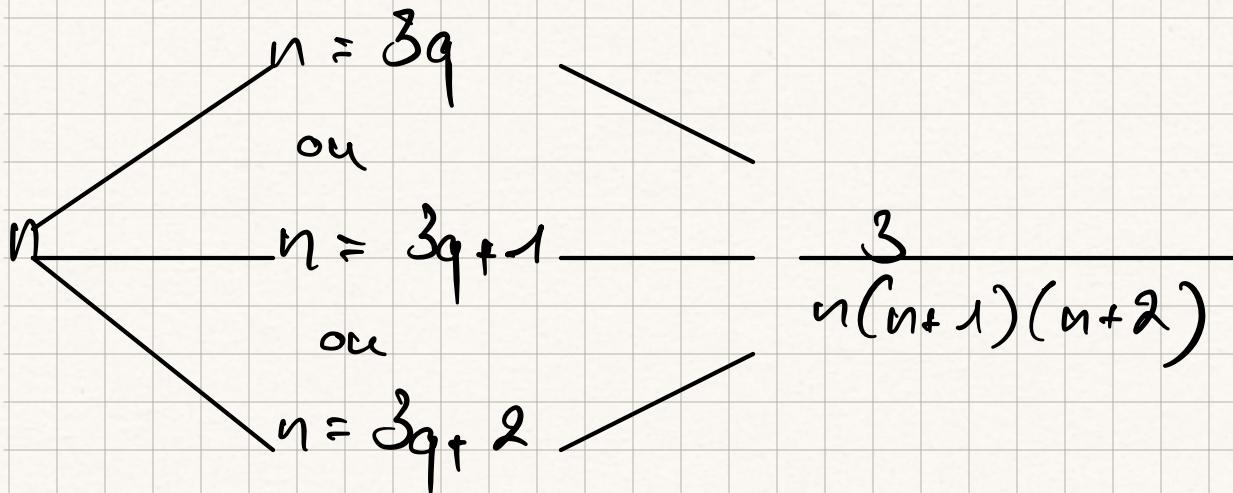
$$0 \leq r \leq 2$$

$$\therefore r = 0, \quad n = 3q \quad \text{dans } \frac{3}{n} \quad \text{dans } \frac{3}{n(n+1)(n+2)}$$

$$\circ r = 1 \quad n = 3q+1 \quad \text{dans} \quad n+2 = 3q+3 \\ = 3(q+1)$$

$$\circ r = 2 \quad n = 3q+2 \quad \text{dans} \quad n+1 = 3q+3 \\ \text{dans} \quad \frac{3}{n+1} \quad \text{dans} \quad \frac{3}{n(n+1)(n+2)}$$

dans tous les cas $\frac{3}{n(n+1)(n+2)}$



On a 2 et 3 diviser $n(n+1)(n+2)$
 2 et 3 sont premières entre eux donc on
 en déduit $b = 2 \times \frac{3}{n(n+1)(n+2)}$

2) Soit $n \in \mathbb{N}$

$$\frac{24}{n(n+1)(n+2)(n+3)}$$

ap $\frac{3}{n(n+1)(n+2)(n+3)}$

On sait que

$$\frac{3}{n(n+1)(n+2)}$$

donc $\frac{3}{n(n+1)(n+2)(n+3)}$

b) $\frac{8}{n(n+1)(n+2)(n+3)}$

On a :

$$n = 4q + 1 \text{ avec}$$

$$q \in \mathbb{N}$$

$$0 < n \leq 3$$

$$\text{si } n=0 \quad n=4q$$

$$n+2=4q+2$$

$$\begin{aligned} \text{donc } n(n+2) &= 4q(4q+2) \\ &= 8q(2q+1) \end{aligned}$$

donc $\frac{8}{n(n+2)}$

alors $\frac{8}{n(n+1)(n+2)(n+3)}$

- Si $n=1$ $n+1=4q+2$ $n+3=4q+4$
 $= 4(q+1)$

$$(n+1)(n+3)=8(q+1)(2q+1)$$

done 8

$$\frac{8}{n(n+1)(n+2)(n+3)}$$

- si $n=2$ $n+2 = 4q+4 = 4(q+1)$

$$n = 4q + 2 = 2(2q + 1)$$

done $\frac{8}{n(n+2)}$

done $\frac{8}{n(n+1)(n+2)(n+3)}$

- si $n=3$

$$n+1 = 4q+4 = 4(q+1)$$

$$n+3 = 4q+6 = 2(q+3)$$

done $\frac{8}{(n+1)(n+3)}$

done $\frac{8}{n(n+1)(n+2)(n+3)}$

dans tous les cas $\frac{8}{n(n+1)(n+2)(n+3)}$

done, comme 3 et 8 sont premier entre eux

$$3 \times 8 = \frac{24}{n(n+1)(n+2)(n+3)}$$

23/01

- ✗ Division Euclidienne
- ✗ Décomposition en facteurs premiers
- ✗ ppcm / pgcd
- ✗ changement de base
- ✗ $\sum_{a,b \in \mathbb{Z}}$
 $\exists x, y \in \mathbb{Z},$
 $ax + by = \text{pgcd}(a, b)$

$$n = qk + r$$

↑ ↙
quotient reste

$\in \mathbb{Z}$

$$0 \leq r < k$$

$\text{pgcd}(a, b) = \text{"le plus grand div commun"}$

$\max \{ c \mid \begin{array}{l} c \text{ divise } a \text{ et } c \\ \text{divise } b \end{array} \}$

$$\frac{a}{\text{pgcd}(a, b)}$$

↑ ↗
entiers premiers entre eux

$$\frac{c}{\text{pgcd}(a, b)}$$

$\text{ppcm}(a, b) = \text{"le plus petit multiple commun"}$

$= \min \{ c \mid \begin{array}{l} c \text{ multiple de } a, c \\ \text{multiple de } b \end{array} \}$

$$= \min(\{k|a|(k \in \mathbb{N}), \{l|b|(l \in \mathbb{N})\})$$

Fx 5

1_x Vrai

2_y Faux

3_y Vrai

4_x Faux \rightarrow si $a_0 + b_0 = 4$

alors $\text{pgcd}(a, b) = 4$

par exemple :

$$a = 3, \quad b = 2$$

$$\text{pgcd}(a, b) = 1$$

$$3 \times 1 + 2 \times 2 = 4$$

$$\exists x, y \in \mathbb{Z} \quad \text{tq} \quad 3x + 2y = 1$$

$$\text{avec } x = 1 \quad \text{et} \quad y = -1$$

$$\text{On a bien } 3 \times 1 + 2(-1) = 1$$

5_x Vrai. Si $\text{pgcd}(a, b) = 1$

produit $\Leftrightarrow a$ et b premiers entre eux

$$a = \prod_{i \in I} p_i^{a_i}$$

où p_i premier $\forall i$

$$b = \prod_{j \in J} q_j^{\beta_j} \quad q_j \text{ premier}, \beta_j \in \mathbb{N}_0$$

$$\operatorname{pgcd}(0, b) = 1$$

$$\Rightarrow \forall i, \nexists p_i \neq q_j$$

$\Leftrightarrow a$ et b n'ont pas de facteurs premiers communs

$$b^3 = \prod_{j \in J} q_j^{3\beta_j} \quad \text{dans } b^3 \text{ et } a \text{ n'ont pas de facteurs premiers communs}$$

$$\text{Ex} \quad a \mid b+c \quad \text{et} \quad a \mid b-c$$

$$a \mid (b+c) + (b-c) = 2b$$

dans $a \mid 2b \Rightarrow a \mid 2$ ou $a \mid b$

On cherche a, b et c

tg $a/b+c$ $a/b-c$ et $a+b$

On prend $a=2$

On prend b impair et c impair
 $b=3$ $c=5$

alors $a \mid b+c$ donc $2|8$

$a \mid b-c$ donc $2|1-2$

$a \nmid b$ car $2 \nmid 3$

$$f_x: fa - fb = ① \leftarrow$$

multiple de $\text{pgcd}(a,b)$

On déduit que $\text{pgcd}(a,b)=1$

Donc a et b premiers entre eux

$$\delta_y(a \leq b \leq c \leq a)$$

Remarque $a \mid b \Rightarrow a \leq b$ quand $a, b > 0$)

On suppose que !

$$\begin{aligned}
 a &= m \times c = m \times l \times b \\
 &= \underbrace{m \times l \times k}_{=1} \times a \\
 &\quad (\text{cau } a \neq 0) \\
 &\quad (\text{cau } a \neq b)
 \end{aligned}$$

$$\text{dann } |m| = |l| = |k| = 1$$

$$\Rightarrow |b| = |k| \times |a| = |a|$$

$a \mid b$ et $b \mid a$ alors $|a| = |b|$

Si $p \mid ab$ avec p premier alors $p \mid a$
ou $p \mid b$

10) a multiple de b

c multiple de d

" $a+c$ multiple de $b+d$ "

$$a = 4, \quad c = 9 \\ b = 2, \quad d = 3$$

$$a+c = 13 \text{ pas multiple} \\ \text{de } 5 = 2+3$$

11) a et b premiers entre eux

$$\Rightarrow \text{ppcm}(a, b) = |ab|$$

$$\text{ppcm}(a, b) = \frac{|ab|}{\text{pgcd}(a, b)}$$

$$a \times \frac{b}{\text{pgcd}(a, b)} = \frac{a}{\text{pgcd}(a, b)} \times b$$

a et b premiers entre eux
 $\Rightarrow \text{pgcd}(a, b) = 1$

$\Rightarrow \text{ppcm}(a, b) = ab$

13) $a \mid bd$ avec $a \mid b$ et $c \mid d$

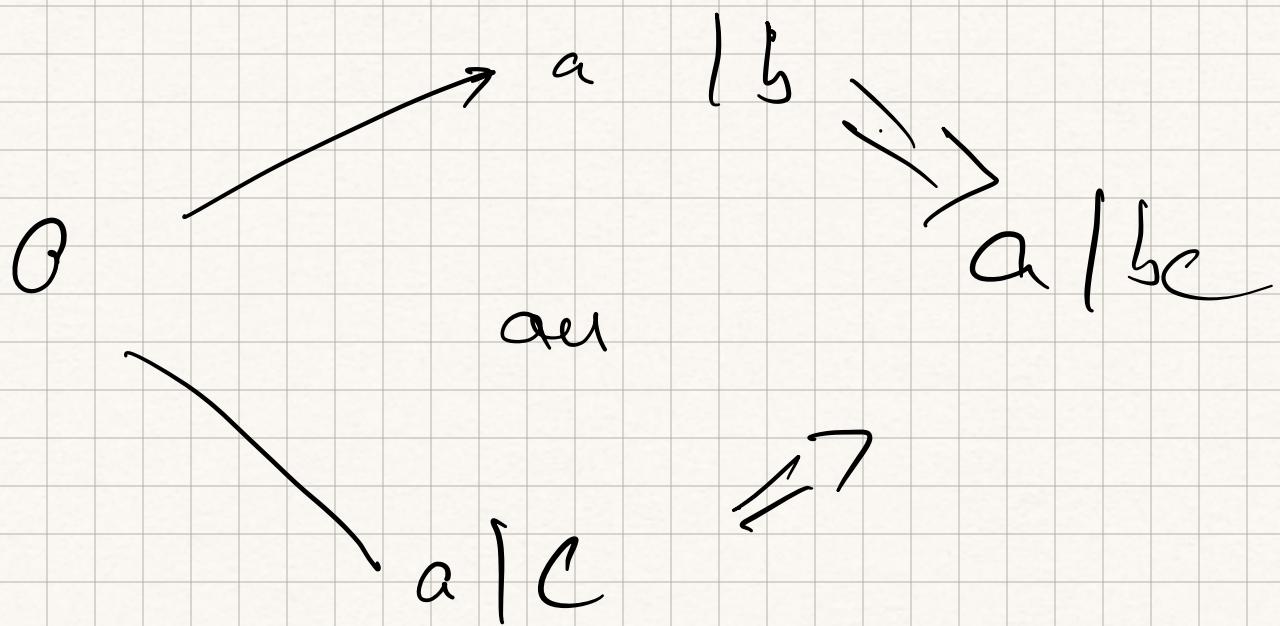
($A \Rightarrow (B \text{ ou } C)$)

($\in A$ et $\nexists B \Rightarrow C$)

12) faux car $9 \mid 3 + 3$

et $9 \nmid 3$ et $9 \nmid 3$

14



$$15 \times \text{ppcm}(a, b) = \frac{|ab|}{\text{pgcd}(a, b)}$$

$$\Leftrightarrow \text{ppcm}(a, b) = \frac{|ab|}{|a|} = |b|$$

$$\text{pgcd}(a, b) = |a| \Leftrightarrow a \mid b$$

(*) Si $\text{pgcd}(a, b) = |a|$
alors $|a| \mid b$ donc $a \mid b$

Si $a \mid b$ alors $a \mid a$, et b
donc $a \mid \text{pgcd}(a, b)$

On $\text{pgcd}(a, b)$ la donc $\text{pgcd}(a, b) \mid a$

16x Vrai à condition que $a \neq 1$

17x Faux, 6 n'est pas premier de
 $\text{pgcd}(6, 0)$

et $6 \nmid 10$, et $10 \nmid 6$

18) Vrai, b, c pair $\Rightarrow 4 \mid bc$
Contre-aposée : $4 \nmid bc \Rightarrow$ " b et c pairs"

$\Leftrightarrow b$ impair ou c impair

Ex 15

1) Montrer que $(ca, cb) = c \operatorname{pgcd}(a, b)$

$$3 \times \left\{ \begin{array}{l} \text{pgcd}(a, b) = 1 \quad \text{clique} \\ \text{pgcd}(c, d) = 1 \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \text{hypothèse} \\ \text{conclusion} \end{array} \right\}$$

Cela démontre que $\text{pgcd}(a, b) = 1$.

01/02

$$\text{1p Mg pgcd}(ca, cb) = c \text{ pgcd}(a, b)$$

$a, b, c > 0$

$$\text{pgcd}(a, b) \mid a$$

\uparrow

def du pgcd

dans $\text{cogcd}(a, b) \mid a$

$$\text{done } \text{cpgcd}(a,b) \mid cb$$

$\exists k \in \mathbb{N}^*$

$$\text{tq } \text{pgcd}(ca, cb) = k \ L \text{ pgcd}(a, b)$$

de plus $\exists l \in \mathbb{N}^* \text{ tq } ca = l \times \text{pgcd}(ca, cb)$

$$\exists m \in \mathbb{N}^* \text{ tq } cb = m \times \text{pgcd}(ca, cb)$$

on a :

$$ca = l \times k \times c \times \text{pgcd}(a, b)$$

dans

$$a = l \times k \times \text{pgcd}(a, b)$$

de même

$$b = m \times k \times \text{pgcd}(a, b)$$

dans $k \times \text{pgcd}(a, b)$ divise a et b

dans $k \times \text{pgcd}(a, b) \mid \text{pgcd}(a, b)$

dans $k = l$

dans $\text{pgcd}(ca, cb) = c \text{pgcd}(a, b)$

$$2 \times (\text{pgcd}(a, b))^2 = \text{pgcd}(a^2, b^2)$$

* On note que a et b premiers entre eux

$\Leftrightarrow a^2, b^2$ premiers entre eux

\Leftarrow On suppose a^2 et b^2 premier entre eux

Berout : $\exists u, v \in \mathbb{Z}$ tq $a^2u + b^2v = 1$

$$\Leftrightarrow a(au) + b(bv) = 1$$

$$\Leftrightarrow au' + bv' = 1$$

avec $u' = au, v' = bv$

dans a et b sont premiers entre eux

\Rightarrow par contreposée

Si $\text{pgcd}(a^2, b^2) \neq 1$

dans $\exists p$ premier pl $\text{pgcd}(a^2, b^2)$

$p \mid a^2$ dans $p \mid a$

$p \mid b^2$ dans $p \mid b$

dans $p \mid \text{pgcd}(a, b) \neq 1$

* En général

$$d = \text{pgcd}(a, b)$$

$$a = a' d \quad \text{avec } a' \in \mathbb{Z}$$

$$b = b' d \quad \text{avec } b' \in \mathbb{Z}$$

avec a', b' premiers entre eux

$$\operatorname{pgcd}(a^2, b^2) = \operatorname{pgcd}((ad)^2, (bd)^2)$$

$$= \operatorname{pgcd}(a^2 d^2, b^2 d^2)$$

$$\text{Or} = d^2 \operatorname{pgcd}(a'^2, b'^2)$$

$$= d^2 = (\operatorname{pgcd}(a, b))^2$$

Question 1 : Propre

$$1x \quad a, b, c$$

p_1, \dots, p_n : les nombres premiers apparaissent dans la décomposition de a ou b ou c

Théorème de décomposition :

$$a = \prod_i p_i^{\alpha_i} \quad 0 \leq \alpha_i$$

$$b = \prod_i p_i^{\beta_i}$$

$$c = \prod_i p_i^{\gamma_i}$$

$$c \operatorname{pgcd}(a, b) = c \prod_i p_i^{\min(\alpha_i, \beta_i)} \leftarrow \text{minimum entre les } \alpha_i$$

$$= \prod_i p_i^{\alpha_i} \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

$$= \prod_i p_i (\alpha_i + \min(\alpha_i, \beta_i))$$

$$ca = \prod_i p_i^{\alpha_i + \gamma_i}$$

$$cb = \prod_i p_i^{\beta_i + \gamma_i}$$

$$\operatorname{pgcd}(ca, cb) = \prod_i p_i^{\min(\alpha_i + \gamma_i, \beta_i + \gamma_i)}$$

$$= \prod_i p_i^{\gamma_i + \min(\alpha_i, \beta_i)}$$

$$(\min(\alpha_i + \gamma_i, \beta_i + \gamma_i)) = \min(\alpha_i, \beta_i) + \gamma_i$$

Question 2 :

$$a^2 = \left(\prod_i p_i^{\alpha_i} \right)^2$$

$$= \prod_i (p_i^{\alpha_i})^2$$

$$= \prod_i p_i^{2\alpha_i}$$

$$b^2 = \prod_i p_i^{2\beta_i}$$

$$\operatorname{pgcd}(a^2, b^2) = \prod_i p_i^{\min(2\alpha_i, 2\beta_i)}$$

$$\operatorname{pgcd}(a, b) = \prod_i p_i^{\min(\alpha_i, \beta_i)}$$

$$(\operatorname{pgcd}(a, b))^2 = \left(\prod_i p_i^{\min(\alpha_i, \beta_i)} \right)^2$$

$$= \prod_i^{\infty} p_i^{2\min(\alpha_i, \beta_i)}$$

$$\min(2\alpha_i, 2\beta_i) = 2 \cdot \min(\alpha_i, \beta_i)$$

Question 4

$$\text{pgcd}(a, bc) = 1 \Leftrightarrow \text{pgcd}(a, b) = \text{pgcd}(a, c) = 1$$

\Rightarrow Soit p premier tq $p \mid a$ alors $p \nmid b$ et $p \nmid c$
dans $p \nmid b$ et $p \nmid c$

$$\text{dans } \text{pgcd}(a, b) = 1, \text{ pgcd}(a, c) = 1$$

\Leftarrow Par contreposée :

$$\text{Si } p \mid \text{pgcd}(a, bc)$$

$\underbrace{\qquad}_{\text{premier}}$

alors $p \mid a$ et $p \nmid bc$

dans $p \mid b$ ou $p \mid c$

(car p est premier)

dans $p \mid \text{pgcd}(a, b)$ ou $p \mid \text{pgcd}(a, c)$

dans un des deux est $\neq 1$

$$5 \times \text{pgcd}(a, b) = 1$$

$$\text{Mq } \text{pgcd}(a+b, a-b) = 1 \text{ ou } 2$$

Si $p \mid a+b$ et $p \mid a-b$
T^e premier

$$\text{Alors } p \mid a+b + (a-b) = 2a$$

$$\text{et } p \mid a+b - (a-b) = 2b$$

$$\begin{array}{ccc} p \mid 2 & \text{ou} & p \mid b \\ p \mid 2 & \checkmark & \checkmark \end{array}$$

ou

$$\begin{array}{ccc} p \mid a & \checkmark & \times \end{array}$$

Donc, dans tous les cas possibles, $p \mid 2$

$$\text{donc } \text{pgcd}(a+b, a-b) \mid 2$$

$$\text{donc } \underline{\text{pgcd}(a+b, a-b) = 1 \text{ ou } 2}$$

$$\text{pgcd}(a+b, ab)$$

$$\text{Si } p \text{ premier } p \mid \text{pgcd}(a+b, ab)$$

alors $p \mid ab$

$$\text{donc } \underline{p \mid a} \text{ ou } p \mid b$$

Si $p \mid a$ et $p \mid a+b$ alors
 $p \mid b$ impossible

Donc si $p \mid b$ alors $p \nmid a$, impossible
donc il n'y a pas de nombre premier
 $\underbrace{p \mid \text{pgcd}(ab, a+b)}$
 $= 1$

Ex 16

Sait $n \in \mathbb{N}$

$$\text{Mq } \text{pgcd}(a, n+1) = 1$$

Si $k \mid n$ et $k \mid n+1$

$$\text{alors } k \mid (n+1) - n = 1$$

$$\text{dans } (k) = 1 \text{ d'où } \text{pgcd}(n, n+1) = 1$$

$$\text{ppcm}(n, n+1) = \frac{n(n+1)}{\text{pgcd}(n, n+1)} = n(n+1)$$

Ex 1f

$$\begin{aligned}1) \quad 637 &= 1 \times 595 + 42 \\595 &= 14 \times 42 + 7 \\42 &= 6 \times 7 + 0\end{aligned}$$

$$\text{PGCD}(637, 595) = 7$$

2)

$$\begin{aligned}637x + 595y &= 91 \\&= 7 \times 13\end{aligned}$$

On remonte l'algo Euclide pour trouver une solution de

$$637x + 595y = 7$$

$$7 = 595 - 42 \times 14$$

$$7 = 595 - (637 - 595) \times 14$$

$$7 = 15 \times 595 - 14 \times 637$$

$$13 \times 7 = (13 \times 15) \times 595 - (13 \times 14) \times 637$$

$$\Leftrightarrow 637 \times (-182) + 595 \times 195 = 91$$

On sait trouver 1 solution à :

$$(E) \quad ax + by = \text{pgcd}(a, b)$$

pour résoudre $\xrightarrow{13}$

$$(E') \quad ax + by = c \text{pgcd}(a, b)$$

on prend une solution de (E) (x_E, y_E)

On a (cx_E, cy_E) est une solution de (E')

$$\begin{aligned} a(cx_E) + b(cy_E) &= c(ax + by) \\ &= c \text{pgcd}(a, b) \end{aligned}$$

On calcule $63f : f = 91$

$$595 : f = 85$$

les solutions générales de (E_2) sont

$$\{(-182 + k85, 195 - k91) \mid k \in \mathbb{Z}\}$$

$$3, \quad 63f_x + 595_y = 143$$

$= 13 \times 11$ pas un multiple de f

D'où pas de solution

6/02

Ex 18 (8, 9, 10) (26)

$$a \equiv b \pmod{n}$$

$$\Leftrightarrow b \equiv a \pmod{n}$$

$$\begin{aligned} a &\equiv b \pmod{a} \Rightarrow ka \equiv kb \pmod{n} \\ a &\equiv b \pmod{a} \end{aligned}$$

$$\text{division de } a \text{ par } n : a = q_a n + r_a$$

$$\begin{aligned} \text{division de } b \text{ par } n : b = q_b n + r_b \\ (\text{Normalement si } a \equiv b \pmod{a}) \end{aligned}$$

$$r_a = r_b$$

$$\text{Ex } 5 \equiv 3 \pmod{2}$$

$$5 = 2 \times 2 + 1$$

$$3 = 1 \times 2 + 1$$

$$a \equiv b \pmod{a}$$

$$\text{"}\exists a' \text{ tq } a a^{-1} \equiv 1 \pmod{n}\text{"}$$

$$n = 4, a = 2$$

$$0 \times 2 \equiv 0 \pmod{4}$$

$$1 \times 2 \equiv 2 \pmod{4}$$

$$2 \times 2 \equiv 0 \pmod{4}$$

$$3 \times 2 \equiv 2 \pmod{4}$$

Si a, n premiers entre eux

$\exists x, y \in \mathbb{Z}$ tq

$$\boxed{ax + ny = 1}$$

autrement dit $ax = ny + 1$

autrement dit $ax \equiv 1 \pmod{n}$

Rappel : Vérifier si n est premier

Si n n'est pas premier, $\exists p$ premier qui divise n . Il suffit de vérifier si $p \mid n$ pour p premier et $p \leq n$

observation

Si $n = k \times l$

alors $k \leq \sqrt{n}$

ou $l \leq \sqrt{n}$

car si $k > \sqrt{n}$

et $l > \sqrt{n}$

alors $k \times l > \sqrt{n} \times \sqrt{n} = n$

dans Si $\exists p$ premier qui divise n

alors $\exists p$ premier $\leq \sqrt{n}$ qui divise n

L'équation $ax + by = c$

où a, b , c les inconnues a, b, c constantes admet des solutions si $(a, b) \mid c$

Ex 18

$$1) \quad 283x + 1422y = 31$$

pgcd : 1

$$\begin{aligned} 1422 &- 6 \times 283 + 24 \\ 283 &= 11 \times 24 + 19 \\ 24 &= 1 \times 19 + 5 \\ 19 &= 3 \times 5 + 4 \\ 5 &= 1 \times 4 + 1 \\ 4 &= 4 \times 1 + 0 \end{aligned}$$

Algo d'Euclide :

$$(E_1') \quad 283x + 1422y = 1$$

$$1 = 5 - 4$$

$$= 5 - (19 - 5 \times 3)$$

$$= 5 - 19 + 5 \times 3$$

$$= 5 \times 4 - 19$$

$$= 4 \times (24 - 19) - 19$$

$$= 4 \times 24 - 4 \cdot 19 - 19$$

$$= 4 \times 24 - 5 \times 19$$

$$= 4 \times 24 - 5 \times (283 - 11 \times 24) = 59 \times 24 - 5 \times 283$$

$$= 59 \times (1422 - 6 \times 283) - 5 \times 283$$

$$= 59 \times 1422 - 359 \times 283$$

Final (-359, 59) est solution de (E_1')

$(-359 \uparrow, 59, 1422k, 1829 - 283k)$ est solution de (E_1)
solution particulière

l'ensemble de solutions de (E)

$$(-359 + 1422k, 59 + 283k, 1829 - 283k) \mid k \in \mathbb{Z}$$

$$\left\{ \left(x_p + \frac{b}{\text{pgcd}(a,b)}k, y_p - \frac{a}{\text{pgcd}(a,b)}k \right) \mid k \in \mathbb{Z} \right\}$$

$$2y \cdot 365x + 72y = 18$$

pgcd : 1

$$365 = 5 * 72 + 5$$

$$72 = 14 * 5 + 2$$

$$5 = 2 * 2 + 1$$

On résout $365x + 72y = 1$

$$1 = 5 - 2 * 2$$

$$1 = 5 - 2(72 - 14 * 5)$$

$$1 = 5 - 2 * 72 + 28 * 5 = 2 * 72 + 29 * 5$$

$$\begin{aligned}1 &= 29 * (365 - 5 * 72) - 2 * 72 \\&= 29 * 365 - 14 * 72\end{aligned}$$

On a : $(29, -147)$ solution de (E'_x)

donc $(29 * 18, -147 * 18)$ solution de (E'_z)

Ensemble de solutions E_2

$$\{(29 * 18 + 72k, -147 * 18 - 365k) \mid k \in \mathbb{Z}\}$$

$$3x \cdot 101 \text{ g} + 150 \text{ g} = 15$$

pgcd : 1

$$150 = 1 \times 101 + 49$$

$$101 = 2 \times 49 + 3$$

$$49 = 16 \times 3 + 1$$

On résout (E'_3)

$$1 = 49 - 3 \times 16$$

$$1 = 49 - (101 - 2 \times 49) \times 16 = 33 \times 49 - 16 \times 101$$

$$= 33 \times (150 - 101) - 16 \times 101$$

$$= 33 \times 150 - 49 \times 101$$

solution de (E'_3) : $(-49, 33)$

solution particulière de (E_3) $(-49 \times 5, 33 \times 15)$

Ensemble de solution de E_3

$$\{(-49 \times 15k + 150k, 33 \times 15 - 101k) \mid k \in \mathbb{Z}\}$$

$$4. \quad 282x + 678y = 66$$

$$\text{pgcd}(282, 678) = 6$$

$$678 = 2 \times 282 + 114$$

$$282 = 2 \times 114 + 54$$

$$114 = 2 \times 54 + 6$$

$$54 = 6 \times 9 + 0 \leftarrow \text{stop}$$

$\text{pgcd}(678, 282)$

On résout (E'_4)

$$282x + 678y = \text{pgcd}(282, 678)$$

$$= 6$$

$$6 = 114 - 2 \times 54$$

$$6 = 114 - 2 \times (282 - 2 \times 54)$$

$$= 5 \times 114 - 2 \times 282$$

$$= 5 \times (678 - 2 \times 282) - 2 \times 282$$

$$6 = 5 \times 678 - 12 \times 282$$

donc $(-12, 5)$ solution de (E'_4)

$$\text{et } 66 = 6 \times 11$$

$\text{pgcd}(678, 282)$

donc $(-12 \times 11, 5 \times 11)$ solution particulière de (E_4)

formuler générale pour les solution

$$\left(x_p + \frac{b}{\text{pgcd}(a,b)} k, y_p - \frac{a}{\text{pgcd}(a,b)} k \right) | k \in \mathbb{Z}$$

Ici : $282/6 = 47$

$$678/6 = 113$$

l'ensemble des solutions de (E_x)
et $\{(-132 + 113k, 55 - 47k) | k \in \mathbb{Z}\}$

Changement de base - Écriture en base N

Ex 9 : $(512121)_g$. Écrire en base 10

$$\begin{aligned}
 (512121)_g &= 5 \times g^5 + 1 \times g^4 + 2 \times g^3 + 1 \times g^2 + 2 \times g^1 + 1 \times g^0 \\
 &= 5 \times 59049 + 1 \times 6561 + 2 \times 129 \\
 &\quad + 1 \times 81 + 1 \times 1 \\
 &= 303364
 \end{aligned}$$

Ex 8 2014 en base 7

$$\begin{array}{c}
 2014 \Big| \begin{array}{r} 7 \\ 288 \end{array} \Big| \begin{array}{r} 7 \\ 41 \end{array} \Big| \begin{array}{r} 7 \\ 5 \end{array} \Big| \begin{array}{r} 0 \end{array} \\
 \begin{array}{r} 14 \\ 61 \\ 57 \end{array} \Big| \begin{array}{r} 8 \\ 1 \end{array} \Big| \begin{array}{r} 6 \\ 5 \end{array} \Big| \begin{array}{r} 7 \\ 0 \end{array} \\
 \hline
 \begin{array}{r} 1 \\ 1 \\ 5 \end{array}
 \end{array}$$

$$\begin{aligned}
 2014 &= (5611)_7 \\
 &= 7 \times 288 + 1 \\
 &= 7 \times (41 \times 7 + 1) + 1 \\
 &= 7 \times [(5 \times 7 + 6)7 + 1] + 1 \\
 &= 7^3 \times 5 + 7^2 \times 6 + 7 \times 1 + 1
 \end{aligned}$$

Ex 10

$$\begin{aligned}
 (713)_8 &= 7 \times 8^2 + 1 \times 8^1 + 3 \times 8^0 \text{ en base } 7 \\
 &= 448 + 8 + 3 \\
 &= (459)_{10}
 \end{aligned}$$

$$\begin{array}{c}
 459 \Big| \begin{array}{r} 7 \\ 65 \end{array} \Big| \begin{array}{r} 7 \\ 9 \end{array} \Big| \begin{array}{r} 7 \\ 2 \\ 1 \end{array} \\
 \begin{array}{r} 39 \\ 4 \end{array} \Big| \begin{array}{r} 2 \\ 1 \end{array} \\
 \hline
 \end{array}$$

$$\begin{aligned}
 459 &= 7 \times 65 + 4 \\
 &= 7^2 \times (9 \times 7 + 2) + 4 \\
 &= 7^2 \times 9 + 7 \times 2 + 4
 \end{aligned}$$

$$459 = 343 + 126$$

$$= 343 + 2 \times 49 + 28$$

$$= 1x^3 + 2x^2 + 4x + 0$$

$$(13)_8 \rightarrow (1240)_7$$

Ex 8

Méthode 2

1	x	x^2	x^3	x^4
		49	343	2401

202	1	1	5	5
$\overline{-}$		$\overline{302}$		

$$202 = 5 \times 4^3 + 302$$

$$= 5 \times x^3 + 6 \times x^2 + 8$$

$$= 5x^3 + 6x^2 + 1x + 1$$

Ex26

Si $n \in \mathbb{N}$ est tq $\exists m \in \mathbb{N}, l \in \mathbb{N}$ tq

$$n = m^2 = l^3$$

alors $n \equiv 0$ ou $1 \pmod{2}$

o mq $\exists k' \in \mathbb{N}$ tq $n = (k')^6$

Décomposition au facteur 1^{er}

$$n = \prod_i p_i^{\alpha_i} \quad p_i \text{ premier } \alpha_i \geq 0$$

$$m = \prod_i q_i^{\beta_i} \quad l = \prod_i v_i^{\gamma_i}$$

$$n = m^2 \Rightarrow \prod_i p_i^{\alpha_i} = \prod_i q_i^{2\beta_i}$$

$$\Rightarrow p_i = q_i \text{ et } 2\beta_i = \alpha_i \text{ donc } 2|\alpha_i \text{ si }$$

$$n = l^3 \Rightarrow \prod_i p_i^{\alpha_i} = \prod_i v_i^{\beta_i}$$

On a $p_i = v_i$ et donc $3\beta_i = \alpha_i$ donc $3|\alpha_i$ si
donc $\forall i \ 2 \nmid 3\beta_i$ et $\text{pgcd}(2, 3) = 1$ donc $6|\alpha_i$
donc $\forall i, \exists \sigma_i \in \mathbb{N} \ \text{uq } \alpha_i = 6\sigma_i$

On pose $k' = \prod_i p_i^{\alpha_i}$ et on a $n = (k')^6$

o si $k' \equiv 0 \pmod{7}$

$$\text{alors } n = (k')^6 \equiv 0^6 \pmod{7}$$

- si $k' \equiv 1 \pmod{f}$
alors $n = (k')^6 \equiv 1^6 = 1 \pmod{f}$
- si $k \equiv 2 \pmod{f}$
alors ...

$$2^6 = 64$$

2^n	2	4	8	2^4	2^5	2^6
$2^n \pmod{f}$	2	4	1	2	4	1

dans $n = (k')^6 = 2^6 \equiv 1 \pmod{f}$

- si $k' \equiv 3 \pmod{f}$

n	1	2	3	4	5	6
3^n	3	9	27	81	3^5	3^6
\pmod{f}	3	2	6	4	5	1

dans $3^6 \equiv 1 \pmod{f}$

dans $n = (k')^6 \equiv 1 \pmod{f}$

- si $k' \equiv 4 \pmod{f}$

n	1	2	3	4	5	6
4^n	4	16	64			
\pmod{f}	4	2	1	4	2	1

dans $4^6 \equiv 1 \pmod{f}$

dans $n = (k')^6 \equiv 4^6 \equiv 1 \pmod{f}$

- si $k' \equiv 5 \pmod{f}$

n	1	2	3	4	5	6
\pmod{f}	5	4	5	4	3	1

dans $n = (k')^6 \equiv 5^6 \equiv 1 \pmod{f}$

Si $k' \equiv b \pmod{f}$

n	1	2	3	4	5	6
mod f	-1	1	-1	1	-1	1

$$\text{dans } n = (k')^6 \equiv 6^6 \equiv 1 \pmod{4}$$

Théorème : Si p premier si $a \in \mathbb{Z}$

$$a^p \equiv a \pmod{p}$$

Dém : Si $a \not\equiv 0 \pmod{p}$ alors $\exists a' \in \mathbb{Z} \text{ tq}$
 $aa' \equiv 1 \pmod{p}$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \text{ si } a \not\equiv 0 \pmod{p}$$
$$a^{p-1} \equiv 0 \pmod{p}$$

Théorème : Soient n, m ≥ 2

$$\text{pgcd}(n, m) = 1$$

Soient $a, b \in \mathbb{Z} \quad \exists k \in \mathbb{Z} \text{ tq } \begin{cases} k \equiv a \pmod{n} \\ k \equiv b \pmod{m} \end{cases}$

k est unique modulo $(n \times m)$

et Soient $x, y \in \mathbb{Z} \text{ tq } nx + my = 1$

alors $k = bnx + amy$ vérifie (E)