ch(15) : Arithmétique des entiers relatifs

I. Divisibilité dans $\mathbb{Z}$:

Déf :
Soient $a, b \in \mathbb{Z}$
on dit que a divise b (ou b est un multiple de a)
ssi $\exists k \in \mathbb{Z} : b = ka$
et on note : $a|b$ ou $a \setminus b$
l'ensemble des multiples de a est noté : $a\mathbb{Z}$
l'ensemble des diviseurs de a est noté $Div(a)$

Exemple :
$Div(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$

Rque :
1/ $\forall a \in \mathbb{Z} : a|0$
2/ $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^* : a|b \Rightarrow |a| \leq |b|$
$\forall a \in \mathbb{Z}, \forall b \in \mathbb{N}^* : a|b \Rightarrow a \leq b$

Propriétés (de la division) :
1/ La relation de "division" est une relation d'ordre sur $\mathbb{N}$
mais elle n'est pas antisymétrique sur $\mathbb{Z}$
$(\forall a \in \mathbb{Z}. a|a, \forall a,b,c \in \mathbb{Z} : (a|b \text{ et } b|c) \Rightarrow a|c,$
$\forall a,b \in \mathbb{Z} : (a|b \text{ et } b|a \Rightarrow |a| = |b|))$

2/ si $d|a$ et $d|b$, alors $d|au+bv$ où $a,b,d,u,v \in \mathbb{Z}$

3/ si $a|b$ et $c|d \Rightarrow ac|bd$
si $a|b$ alors $\forall k \in \mathbb{N} : a^k | b^k$

Dém: (Exercice)

3/ supp que $a|b$ et $c|d$.

Donc: $\exists k_1, k_2 \in \mathbb{Z}$ tq: $b = k_1 a$ et $d = k_2 c$

d'où $bd = (k_1 k_2)\, ac$ et $k_1 k_2 \in \mathbb{Z}$

Donc: $ac \mid bd$.

Exercice:

Résoudre dans $\mathbb{Z}$ (resp $\mathbb{Z}^2$) les equations suivantes:

1/ $x-1 \mid x-3$

2/ $xy = 2x + 3y$

Solut:

1/(*) $x-1 \mid x-3 \Rightarrow x-1 \mid x-3$ et $x-1 \mid x-1$

$\Rightarrow x-1 \mid x-3-x+1$

$\Rightarrow x-1 \mid -2$

$\Rightarrow x-1 \mid 2$

$\Rightarrow x-1 = \pm 1$ ou $x-1 = \pm 2$

$\Rightarrow x = 3$ ou $x = -1$ ou $x = 0$ ou $x = 2$

réciproquement ces valeurs vérifient (*)

donc $S = \{-1, 0, 2, 3\}$

2/ on a: $xy = 2x + 3y \Leftrightarrow y(x-3) = 2x - 6 + 6$

$\Leftrightarrow (x-3)(y-2) = 6$

$\Leftrightarrow (x-3, y-2) \in \{(6,1), (1,6), (2,3), (3,2), (-6,-1)$

$(-1,-6), (-2,-3), (-3,-2)\}$

$\Leftrightarrow (x,y) \in \{(9,3), (4,2), (5,5), (6,4), (-3,1), (2,-4)$

$(1,-1), (0,0)\}$

1.2. Congruence modulo n:

Déf:

Soit $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$

On dit que a congru à b modulo n

ssi $n \mid a-b$ et on note: $a \equiv b \ [n]$

Remarque:

1/ Pour $n=0$, la congruence modulo "0" n'est autre que l'égalité

$(a \equiv b \ [0] \Leftrightarrow a = b)$

2/ La congruence généralise la division

$\forall n \in \mathbb{N}, \forall a \in \mathbb{Z} : \quad n \mid a \Leftrightarrow a \equiv 0 \ [n]$

Propriétés: (de la congruence)

Soit $n \in \mathbb{N}$

1/ La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

$(\forall a \in \mathbb{Z} : a \equiv a \ [n]$; $a \equiv b \ [n] \Rightarrow b \equiv a \ [n]$

$(a \equiv b \ [n]$ et $b \equiv c \ [n] \Rightarrow a \equiv c \ [n]$

2/ (Somme):

Si $a \equiv b \ [n]$ et $c \equiv d \ [n]$ alors $a+c \equiv b+d \ [n]$

3/ (Produit):

Si $a \equiv b \ [n]$ et $c \equiv d \ [n]$ alors $ac \equiv bd \ [n]$

En particulier:

Si $a \equiv b \ [n]$, alors $\forall k \in \mathbb{N}, \ a^k \equiv b^k \ [n]$

4/ Soit $m \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$:

$a \equiv b \ [n] \Leftrightarrow ma \equiv mb \ [nm]$

Dém:

3/ Supp que $a \equiv b\ [n]$ et $c \equiv d\ [n]$
alors $n \mid a-b$ et $n \mid c-d$
d'où : $n \mid c(a-b) + b(c-d)$

Donc : $n \mid ac - bd$.

4/ $\Rightarrow$ 1/ $a \equiv b\ [n] \Leftrightarrow n \mid a-b$
$\Rightarrow mn \mid m(a-b)$
$\Rightarrow ma \equiv mb\ [mn]$

Rappel : $a \mid b \Leftrightarrow ma \mid mb \quad (m \neq 0)$

Rque :
1/ $a \equiv b\ [n] \Rightarrow ma \equiv mb\ [n]$
2/ **Attention :** $ma \equiv mb\ [n] \not\Rightarrow a \equiv b\ [n]$
$3 \times 3 \equiv 3\ [6]$ et $3 \not\equiv 1\ [6]$

Exemple : ①
Mq : $2^{345} + 5^{432}$ est divisible par 3
on a : $2 \equiv -1\ [3]$
$\Rightarrow 2^{345} \equiv (-1)^{345}\ [3]$
$\Rightarrow 2^{345} \equiv -1\ [3]$
$5 \equiv -1\ [3]$
d'où $5^{432} \equiv (-1)^{432}\ [3]$
$\Rightarrow 5^{432} \equiv 1\ [3]$
d'où : $2^{345} + 5^{432} \equiv 0\ [3]$

Exercice :
1/a/ Mq : $\forall n \in \mathbb{Z}$ impair $n^2 \equiv 1\ [8]$
b) que peut on dire si n est pair
2/ Déterminer le reste de la division euclidienne de 2^n par 3

3/ Mq : $\forall n \in \mathbb{N}$: $6 \mid 5n^3 + n$

Rappel :

$\forall n \in \mathbb{Z}$: $n(n+1) \in 2\mathbb{Z}$

Solut :

$n \equiv [8]$	0	1	2	3	4	5	6	7
$n^2 \equiv [8]$	0	1	4	1	0	1	4	1

si n est impair, alors $n \equiv r\ [8]$ avec $r \in \{1, 3, 5, 7\}$

alors $n^2 \equiv 1\ [8]$

si n est pair, alors $n \equiv r'\ [8]$ où $r' \in \{0, 2, 4, 6\}$

alors $n^2 \equiv 0\ [8]$ ou $n^2 \equiv 4\ [8]$

2/ $2 \equiv -1\ [3]$

$2^n \equiv (-1)^n\ [3]$

si n est pair $2^n \equiv 1\ [3]$

si n est impair $2^n \equiv 2\ [3]$

3/ $5 \equiv -1\ [6]$

donc : $5n^3 + n \equiv -n^3 + n\ [6]$

donc on Mq : $6 \mid -n^3 + n$

$-n^3 + n = -n(n^2 - 1)$

$n \equiv [6]$	0	1	2	3	4	5
$n^2 - 1$	-1	0	3	2	3	0
$-n(n^2-1)$	0	0	0	0	0	0

donc : $\forall n \in \mathbb{N}$: $6 \mid 5n^3 + n$

5

Rque : on peut faire un raisonnement par récurrence.

$5(n+1)^3 + (n+1) = 5(n^3+3n^2+3n+1) + n+1$

$= \underbrace{5n^3+n}_{\in 6\mathbb{N}} + \underbrace{15n(n+1)}_{\in 2\mathbb{N}} + 6$

1.3- Division euclidienne :

Théorème et Déf :

Soit, $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, alors :

$\exists ! (q,r) \in \mathbb{Z} \times \mathbb{N}$ tq :

$a = bq + r$ et $0 \leq r < b$

on dit qu'on a effectué la division euclidienne de a par b.

Dém :

- Par l'existence, par analyse synthèse, on a :

$q = E(\frac{a}{b})$ et $r = a - bq$

$(a/b = q + r/b \Rightarrow E(\frac{a}{b}) = q + E(\frac{r}{b}) = q)$

- Unicité :

supp qu'$\exists (q_1, r_1), (q_2, r_2) \in \mathbb{Z} \times \mathbb{N}$ tq :

$a = bq_1 + r_1$ et $0 \leq r_1 < b$

$a = bq_2 + r_2$ $0 \leq r_2 < b$

Donc : $\underbrace{b(q_1 - q_2)}_{\in b\mathbb{Z}} = r_2 - r_1$ et $-b < r_2 - r_1 < b$

Donc : $r_2 - r_1 = 0$ et $q_1 = q_2$

Exemple :

$2017 = (201 \times 10) + 7$ (division sur 10)

$2017 = (-202 \times 10) + 3$

$2013 = (201 \times 10) + 9$

$2013 = (-202 \times 10) + 1$

1.4 Nombres premiers :

Déf :

Soit $p \in \mathbb{N}^*$, on dit que p est premier ssi $p \neq 1$ et les seuls diviseurs de p dans $\mathbb{N}$ sont 1 et p.

si p n'est pas premier, on dit que p est composé.

on note $\mathbb{P}$ l'ensemble de nombres entiers naturels premiers

$\{2, 3, 5, 7, 11, 13, 17, 19\} \subset \mathbb{P}$

Prop :

Tout entier naturel non nul est le produit de puissances de nombres premiers.

Rque :

1 est le produit de 0 nombres premiers (convention)

Dém : (récurrence forte)

pour $n=1$ (convention)

$n=2 \quad 2=2$

Soit $n \in \mathbb{N}^*$, supp que la propriété est vraie jusqu'à l'ordre n.

- si $n+1$ est premier, c'est fini $n+1 = (n+1)$
- si $(n+1)$ n'est pas premier :

$\exists a, b \in \mathbb{N}^* : \quad n+1 = a \times b$

$b, a \in [\![2, n]\!]$

D'après H.R, a (resp b) sont produits de nbres premiers donc $(n+1)$ est produit de nbres premiers

Exemple :

2016 | 2
1008 | 2
504 | 2
252 | 2
126 | 2
63 | 3

$2016 = 2^5 \times 3^2 \times 7$

$2018 = 2 \times 1009$ premier

$2020 = 2^2 \times 5 \times 101$

Prop:

L'ensemble des entiers naturels non nuls premiers est infini.

Dém:

Supp que $\mathbb{P}$ est fini

$\mathbb{P} = \{ p_1, p_2, \dots, p_r \}$ avec $p_1 < p_2 < \dots < p_r$

On pose $N = (p_1 p_2 \dots p_r) + 1$

$= \left(\prod_{k=1}^{r} p_k \right) + 1$

N est premier car sinon

N est divisible par un nombre premier p_{i_0}.

$p_{i_0} \mid N$ et $p_{i_0} \mid \prod_{k=1}^{r} p_k$

$\Rightarrow p_{i_0} \mid \left(N - \prod_{k=1}^{r} p_k \right) = 1$

$\Rightarrow p_{i_0} \mid 1$ (Absurde)

Donc N est premier et $N > p_r$ Absurde

Donc $\mathbb{P}$ est infini.

Crible d'Eratosthène:

Le Crible d'Eratosthène permet une détermination simple de tous les nombres premiers inférieurs à un entier donné.

Soit $n \in \mathbb{N}^*$:

Si n est composé (n n'est pas premier), soit p le plus petit nombre premier divisant n $n = pK$ ($K \in \mathbb{N}^*$)

comme tout diviseur premier de K est $\geq$ à p alo

alors $n = pK \geq p^2$ (c.à.d: $p \leq \sqrt{n}$)

Résumé :

Tout nombre composé admet un diviseur premier p tq : $p \leq \sqrt{n}$

Exemple :

- Cherchons les nombres premiers $\leq$ à 80

~~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~~

$E = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79\}$

- Vérifions que 2017 est premier

les nombres premiers $\leq \sqrt{2017}$ et < 44 — $= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$

8.17

$2017 \equiv$	$[p]$		16	19
1	2		10	23
1	3		10	29
1	5		27	31
2	7		13	37
9	11		2	41
9	13		33	43
5	17			

Donc 2017 est premier

9

I PGCD ; PPCM : (plus grand commun diviseur, plus petit multiple (commun))

Déf : (Diviseur commun, multiple commun)

Soient $a_n, a_2 \dots, a_1 \in \mathbb{Z}$

i/ On appelle diviseur commun à $a_1, a_2 \dots$ et a_n tout entier relatif qui divise à la fois $a_1, a_2 \dots$ et a_n

ii/ On appelle multiple commun à $a_1, a_2, \dots a_n$ tout entier relatif à la fois multiple de $a_1, a_2, \dots$ et a_n

Exemple :

- $Div(12) \cap Div(18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$
- $Div(12) \cap Div(18) \cap Div(32) = \{\pm 1, \pm 2\}$
- $12\mathbb{Z} \cap 18\mathbb{Z} = 36\mathbb{Z}$ $\quad |ab| = (a \wedge b) \times (a \vee b)$
  $= \{0, \pm 36, \pm 72, \dots\}$

Déf : PGDC de deux entiers relatifs : soit $a, b \in \mathbb{Z}$, le maximum de $(Div(a) \cap Div(b))$ s'appelle le pgcd de a et b que l'on note $a \wedge b$ ou $\Delta(a, b)$

Rques :

1/ $\forall a, b \in \mathbb{Z}$: $\quad a \wedge b = |a| \wedge |b|$

$a \wedge b \in \mathbb{N}^*$

2/ $\forall a \in \mathbb{Z}^*$: $\quad a \wedge 0 = |a|$

$a \wedge a = |a|$

3/ si p premier : $\quad a \wedge p = \begin{cases} p & \text{si } p \mid a \\ 1 & \text{si } p \nmid a \end{cases}$

(10)

Prop :

Soient $a, b \in \mathbb{Z}$, alors : $\quad a \wedge b = (a + kb) \wedge b$, $\forall k \in \mathbb{Z}$

Dém:

M.q: $Div(a) \cap Div(b) = Div(a+kb) \cap Div(b)$.

$c|a$ et $c|b \Rightarrow c|b$ et $c|a+kb$

$\Rightarrow c \in Div(a+kb) \cap Div(b)$

De même si $c|b$ et $c|a+kb \Rightarrow c|b$ et $c|(a+kb)-kb$

$\Rightarrow c|b$ et $c|a$

Exemple:

Déterminer $(3n+1) \wedge (2n+5)$ pour tout $n \in \mathbb{N}$.

Solut:

$$(3n+1) \wedge (2n+5) = \big((3n+1)-(2n+5)\big) \wedge (2n+5)$$
$$= (n-4) \wedge (2n+5)$$
$$= (n-4) \wedge (2n+5-2(n-4))$$
$$= (n-4) \wedge 13$$

$d_n \in \{1, 13\}$; $d_n = 13 \Leftrightarrow 13 | n-4$

$\Leftrightarrow n = 4 \ [13]$

$d_n = 1 \Leftrightarrow n \neq 4 \ [13]$

Rque:

Si $a = bq+r$, alors $a \wedge b = b \wedge r$

Algorithme d'Euclide:

Soit $a, b \in \mathbb{N}$ tq: $0 \leq b \leq a$

En effectuant la division euclidienne de a par b

on a: $\exists (q_1, r_1) \in \mathbb{N}$ tq: $a = bq_1 + r_1 \quad (0 \leq r_1 < b)$

si $r_1 = 0$, alors $b|a$ Donc $a \wedge b = b$

si $0 < r_1 < b$, alors $a \wedge b = b \wedge r_1$

En utilisant la division euclidienne de b par r_1

$\exists (q_1, r_1) \in \mathbb{N}$: $b = q_1 r_1 + r_2$ $(0 < r_2 < r_1)$

si $r_2 = 0$, donc $r_1 | b$

Donc $a \wedge b = b \wedge r_1 = r_1$

si $r_2 \neq 0$ $(0 < r_2 < r_1)$

alors $a \wedge b = b \wedge r_1 = r_1 \wedge r_2$

$\exists (q_3, r_3) \in \mathbb{N}$ tq : $r_1 = q_3 r_2 + r_3$ $(0 < r_3 < r_2 < r_1$

si $r_3 = 0$, alors : $a \wedge b = r_1 \wedge r_2 = r_2$

et ainsi de suite, on constate une suite (r_n) strict décroissante d'entiers naturels

Donc : $\exists k \in \mathbb{N}^*$: $r_k = 0$ et $a \wedge b = r_{k-1}$

Ce procédé s'appelle l'algorithme d'Euclide pour la recherche du pgcd

Exemple :

$d = 2016 \wedge 40$

$2016 = (40 \times 50) + 16$

$d = 40 \wedge 16$

$40 = (2 \times 16) + 8$

$d = 16 \wedge 8$

$16 = (2 \times 8) + 0$

Donc : $d = 8$

Prop : (Théorème de Bezout)

On pose $d = a \wedge b$ alors

$\exists (u, v) \in \mathbb{Z}^2$: $d = au + bv$

Dém : (Exemple) $8 = 2016 \wedge 40$.

On a : $40 = (2 \times 16) + 8$

Donc : $8 = 40 - (2 \times 16)$

$= 40 - 2(2016 - 40 \times 50) = \underbrace{(2017)}_{u} \times 40 - \underbrace{2}_{v} \times (2016)$

Rque :

1/ Le couple (u,v) s'appelle les coefficients de Bezout

2/ Le couple (u,v) n'est pas unique.

$6 \wedge 4 = 2$

$2 = 6 - 4$

$= (-3 \times 6) - (5 \times 4)$

$= (5 \times 6) - (7 \times 4)$

3/ On n'a pas l'équivalence

$2 = 6 - 4$

$2 \times 6 - 2 \times 4 = 4$

Propriétés :

$\forall a,b,c,d \in \mathbb{Z}$

1/ $d|a$ et $d|b \Rightarrow d|a \wedge b$

2/ $(a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b \wedge c$

3/ $(ka) \wedge (kb) = |k| \times (a \wedge b)$

Dem :

1/ on pose $S = a \wedge b$

d'après Bezout, il existe $(u,v) \in \mathbb{Z}^2$: $S = au + bv$

$d|a$ et $d|b \Rightarrow d|au+bv$

$\Rightarrow d|S$

2/ $d_1 = (k \wedge b) \wedge c$, $d_2 = a \wedge (b \wedge c)$, $d_1|d_2$ et $d_2|d_1$

3/ On pose : $d_1 = (ka) \wedge (kb)$ et $S = a \wedge b$

$d_1|ka$ et $d_1|kb$

$\exists (u,v) \in \mathbb{Z}^2 : S = au + bv$

$S|k| = a|k|u + b|k|v$

donc $d_1 | S|k|$

$\exists (u',v') \in \mathbb{Z}^2 : d_1 = kau' + kbv'$

1.3

$\delta | a$ et $\delta | b$

$\delta | |k| | ka$ et $\delta | |k| | kb$. $\Rightarrow \delta | |k| | d$ ①.

Donc $\delta | |k| | ka' u' + kbv'$ d'où $\delta | |k| | d_1$

Donc : $(ka) \wedge (kb) = |k| (a \wedge b)$.

2.2 PGCD d'une famille finie d'entiers :

Déf :

Soient $a_1, a_2, \dots, a_n \in \mathbb{Z}$.

On définit $a_1 \wedge a_2 \wedge \dots \wedge a_n = \text{Max}(\text{Div}(a_1) \cap \text{Div}(a_2) \dots \cap \text{Div}(a_n))$

Exemple :

$28 \wedge 42 \wedge 98 = (28 \wedge 42) \wedge 98$

$= 14 \wedge (98) = 14$

Prop :

1/ $\text{Div}(a_1) \cap \text{Div}(a_2) \dots \cap \text{Div}(a_n) = \text{Div}(a_1 \wedge a_2 \wedge \dots \wedge a_n)$.

2/ $(ka_1) \wedge (ka_2) \wedge \dots \wedge (ka_n) = |k| (a_1 \wedge a_2 \wedge \dots \wedge a_n)$.

3/ si $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$

alors : $\exists u_1, u_2 \dots u_n \in \mathbb{Z}$ tq : $d = \sum_{i=1}^{i=n} a_i u_i$ } Généralisation à n

2.3 Nombres premiers entre eux :

Déf :

Soit $a, b \in \mathbb{Z}$, On dit que a et b sont premiers entre eux si $a \wedge b = 1$

Exemple :

$14 \wedge 45 = 1$

Prop :

Soit $a, b \in \mathbb{Z}$, $d \in \mathbb{N}^*$

$d = a \wedge b \iff \exists a', b' \in \mathbb{Z} \; ; \; a = da', \; b = db' \text{ et } a' \wedge b' = 1$

Théorème de Bezout : ⚠

Soit $a, b \in \mathbb{Z}$

$a \wedge b = 1$ ssi $\exists u, v \in \mathbb{Z} \quad au + bv = 1$

Dém :

$\Rightarrow$ / C'est déjà fait ds le cas général

$\Leftarrow$ / on pose $d = a \wedge b$

On a : $d \mid a$ et $d \mid b$

donc $d \mid au + bv = 1$ donc $d = 1$

Rque :

Attention, la réciproque n'est pas vraie dans le cas où $d \neq 1$

$\exists (u,v) \in \mathbb{Z}^2 : au + bv = d$ et $d \neq 1 \not\Rightarrow d = a \wedge b$

C. exemple :

$2 \times 6 - (2 \times 4) = 4 \not\Rightarrow 4 = 6 \wedge 4$

Théorème de Gauss :

$\forall a, b, c \in \mathbb{Z}$

$(a \mid bc \text{ et } a \wedge b = 1) \Rightarrow a \mid c$

Dém :

$a \wedge b = 1 \Rightarrow \exists (u,v) \in \mathbb{Z}^2 : au + bv = 1$

$\Rightarrow$ " " : $acu + bcv = c$

$a \mid bc$ et $a \mid ac \Rightarrow a \mid bcv + acu$.

$\Rightarrow a \mid c$

15

Rque :

Attention : $a|bc \not\Rightarrow a|c$ ou $a|b$

C. exemple : $12|8\times 3$ et $12 \nmid 8$ et $12|3$

① Défs :

Soient $a_1, a_2, \dots, a_n \in \mathbb{Z}$

On dit $a_1, a_2 \dots, a_n$ sont premiers entre eux dans leur ensemble ssi $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$

On dit que $a_1, a_2 \dots, a_n$ sont premiers entre 2 à 2 ssi $\forall i,j \in [\![1,n]\!]$:

$i \neq j \Rightarrow a_i \wedge a_j = 1$

Rque :

1/ si $a_1, a_2 \dots, a_n$ sont premiers entre eux 2 à 2, alors ils sont premiers entre eux dans leur ensemble

2/ La réciproque est fausse

C. exemple :

$14 \wedge 21 \wedge 11 = 1$

et pourtant $14 \wedge 21 = 7$

2.4 P.P.C.M de deux relatifs :

① Déf :

Soit $a, b \in \mathbb{Z}$, le plus petit entier naturel non nul de $a\mathbb{Z} \cap b\mathbb{Z}$ s'appelle le p.p.c.m de a et b qu'on note : $a \vee b$

Prop :

Si $a|m$ et $b|m$ alors : $a \vee b \,|\, m$. $\forall a, b, m \in \mathbb{N}$

16

① Dém :

Supp que $a|m$ et $b|m$

alors : $a \vee b \leq m$

En effectuant la division euclidienne de m par $a \vee b$:

$m = qM + r \quad 0 \leq r < M$

si $r \neq 0$

$a|m$ et $a|M \Rightarrow a|m - qM \Rightarrow a|r$

$b|m$ et $b|M \Rightarrow b|m - qM \Rightarrow b|r$

Donc r est un multiple commun non nul de a et b tq $r < M$

(Absurde)

Donc $r = 0$

$\mathcal{C}$: $a \vee b | m$

Prop : (lien avec pgcd)

1) $\forall a, b \in \mathbb{Z}$: $(a \wedge b) \times (a \vee b) = |ab|$

2) $\forall k \in \mathbb{Z}^*$: $(ka) \vee (kb) = |k|(a \vee b)$

Dem : Soit $a, b \in \mathbb{N}$

1) On pose : $\delta = a \wedge b$ et $m = a \vee b$

$\exists a', b' \in \mathbb{N}$: $a = \delta a'$ et $b = \delta b'$ et $a' \wedge b' = 1$

$ab = \delta^2 a'b' \overset{?}{=} \delta(a \vee b)$

$= \delta(\delta a'b')$

$a | \underbrace{\delta a'b'}_{a}$ et $b | \underbrace{\delta b'a'}_{b}$

$\Rightarrow a \vee b | \delta a'b'$

$\Rightarrow \exists k \in \mathbb{N}$: $\delta a'b' = k(a \vee b)$

$a|m$ et $b|m$

$m = \alpha a = \beta b \quad \alpha, \beta \in \mathbb{N}$

Donc : $\delta a'b' = k a \alpha = k \delta a' \alpha$

$\Rightarrow b' = k\alpha \Rightarrow k | b'$ (1)

D'autre part :

$\delta a'b' = k\alpha\beta = k\,\delta b'\beta$

$\Rightarrow a' = k\beta$

$\Rightarrow k \mid a'$ ②

de ① et ②

donc : $k \mid a' \wedge b' = 1$.

d'où : $k = 1$

Ac : $\delta a'b' = m$.

2/ Soit $a, b, k \in \mathbb{N}^*$

$$(ka) \vee (kb) = \frac{k^2 ab}{(ka) \wedge (kb)}$$

$$= \frac{kab}{(a \wedge b)}$$

D'autre part :

$$k(a \vee b) = k\left(\frac{ab}{a \wedge b}\right) = (ka) \vee (kb)$$

Exemple :

Résoudre dans $(\mathbb{N}^*)^2$, le système :

$$\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases}$$

Solut :

$$\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases} \Leftrightarrow \exists a, b \in \mathbb{N}^* : \begin{cases} x = 5a \\ y = 5b \\ xy = 300 \end{cases} \text{ et } a \wedge b = 1$$

$$\Leftrightarrow \exists a, b \in \mathbb{N}^* : \begin{cases} x = 5a \\ y = 5b \\ a \wedge b = 1 \\ ab = 12 \end{cases}$$

$\Leftrightarrow : \exists a,b \in \mathbb{N}^* : \begin{cases} x = 5a \\ y = 5b \\ a \wedge b = 1 \end{cases}$

$et (a,b) \in \{(1,12),(3,4),(4,3),(12,1)\}$

$\Leftrightarrow (x,y) \in \{(5,60),(15,20),(20,15),(60,5)\}$

2.5. Valuations p-adiques d'un entier :

Déf : (Valuations p-adique)

Soit $n \in \mathbb{N}^*$ et $p \in \mathbb{P}$.

le plus grand élt de $\{k \in \mathbb{N} / p^k / n\}$ s'appelle la valuation p adique de n notée : $v_p(n)$.

Exemple :

$60 = 2^2 \times 3 \times 5$

$v_2(60) = 2$, $v_3(60) = 1$, $v_5(60) = 1$, $v_7(60) = 0$

$\forall p \in \mathbb{P} - \{2,3,5\} : v_p(60) = 0$

Prop :

$\forall a,b \in \mathbb{N}^*$, $\forall p \in \mathbb{P}$

$v_p(ab) = v_p(a) + v_p(b)$

Dém :

$a = p^{v_p(a)} \times a'$ tq $p \nmid a'$

$b = p^{v_p(b)} \times b'$ tq $p \nmid b'$

Donc $ab = p^{v_p(a)+v_p(b)} \times (a'b')$

Rque :

si $p \in \mathbb{P}$ alors : $p \mid ab \Leftrightarrow p \mid a$ ou $p \mid b$

$\Rightarrow$ / si $p \mid ab$ et $p \nmid a$

$$p \wedge a = \begin{cases} 1 & \text{si } p \nmid a \\ p & \text{si } p \mid a \end{cases}$$

Donc : $p \wedge a = 1$, d'après Gauss $p \mid b$.

Attention : l'implication est fausse si $p \notin \mathbb{P}$

$6 \mid 4 \times 3$ et $6 \nmid 4$ et $6 \nmid 3$

puisque $p \mid a$ et $p \mid b$ et p premier, alors $p \mid a \wedge b$

d'où : $v_p(ab) = v_p(a) + v_p(b)$

Prop : (Décomposition en nombres premiers)

$\forall a \in \mathbb{Z}^*$, $\exists p_1, p_2, \dots, p_m \in \mathbb{P}$ et $\varepsilon \in \{-1, 1\}$ tq :

$$a = \varepsilon \prod_{i=1}^{i=m} p_i^{v_{p_i}(a)}, \quad \varepsilon \in \{-1, 1\}$$

si $a \in \mathbb{N}^*$, $\varepsilon = 1$; si $a \in \mathbb{Z}^-$: $\varepsilon = -1$

Déc (Existence : récurrence forte sur $n \in \mathbb{N}$, $n \geq 2$

→ $n+1$ est premier, fini, $n+1 = a \times b$

$2 \leq a \leq n$

$2 \leq b \leq n$.

H_n $2 \leq k \leq n$ et $2 \leq b \leq n$.

Prop :

Soit $a, b \in \mathbb{N}^*$ tq :

$$a = \prod_{i=1}^{i=m} p_i^{v_{p_i}(a)} \quad \text{et} \quad b = \prod_{i=1}^{i=m} p_i^{v_{p_i}(b)}$$

$(v_{p_i}(a) \in \mathbb{N})$

alors : $a \wedge b = \prod_{i=1}^{m} p_i^{\text{Min}(v_{p_i}(a), v_{p_i}(b))} = A$

$$a \vee b = \prod_{i=1}^{m} p_i^{\text{Max}(v_{p_i}(a), v_{p_i}(b))}$$

$A \mid a$, $A \mid b$ $\Rightarrow A \mid a \wedge b$ $\Rightarrow a \wedge b \geq A$ $\forall k \neq 1$

tout p un div. premier de k

$p \mid a \wedge b$

$\Rightarrow p \mid a$ et $p \mid b$.

$\exists j$: $p = p_j$

p_j Min( ) $\neq 0$ $\mid a$

$\Rightarrow$

Absurde

$v_{p_i} \in$ Max

Exemple :

$60 \wedge 882 = (2^2 \times 3 \times 5) \wedge (2 \times 3^2 \times 7^2)$

$= 2^1 \times 3^1$

$= 6$.

$60 \vee 882 = (2^2 \times 3 \times 5) \vee (2 \times 3^2 \times 7^2)$

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

$= 8820$

2.6 Théorèmes de Fermat :

Théorème :

Soit $p \in \mathbb{P}$, alors :

1/ $\forall n \in \mathbb{Z} : n^p \equiv n \ [p]$

2/ si $p \nmid n$, alors : $n^{p-1} \equiv 1 \ [p]$

Dém : (Trois étapes)

1/ $\forall k \in [\![1, p-1]\!] : p \mid C_p^k$.

2/ Par récurrence sur n, on montre que

$\forall n \in \mathbb{N} : n^p \equiv n \ [p]$

3/ $\forall n \in \mathbb{Z} : n^p \equiv n \ [p]$

1/ $\forall k \in [\![1, p-1]\!]$

$$C_p^k = \frac{p!}{k!(p-k)!}$$

$$= \frac{p\,(p-1)!}{k(k-1)!\,((p-1)-(k-1))!}$$

$$= \frac{p}{k} C_{p-1}^{k-1}$$

$$k C_p^k = p C_{p-1}^{k-1}$$

Donc : $p \mid k C_p^k$

or : $p \wedge k = 1$ car : $p \nmid k \quad k \in [\![1, p-1]\!]$

D'après Gauss on a : $p \mid C_p^k \quad \forall k \in [\![1, p-1]\!]$

2/ Pour $n = 0$, relation vérifiée.

Soit $n \in \mathbb{N}$, supp que : $n^p \equiv n \ [p]$

$(n+1)^p \overset{F.B.N}{=} \sum_{k=0}^{p} C_p^k n^k$

$= 1 + n^p + \sum_{k=1}^{p-1} C_p^k n^k$

D'après H.R : $(1+n)^p \equiv 1+n^p \ [p]$

$\sum_{k=1}^{p-1} C_p^k n^k \equiv 0 \ [p]$

Donc : $(n+1)^p \equiv 1+n^p \ [p]$

c/c : $\forall n \in \mathbb{N}$: $n^p \equiv n \ [p]$

- si $p \geq 3$

$\forall n \in \mathbb{Z}^{*-}$ $(n = -m \ / \ m \in \mathbb{N}^*)$

$n^p = (-m)^p = (-1)^p m^p = -m^p$

or : $m^p \equiv m \ [p]$ donc $n^p \equiv n \ [p]$

pour $p = 2$

- $\forall n \in \mathbb{Z}$: $n^2 \equiv n \ [2]$

$\forall n \in \mathbb{Z}$: $2 \mid n(n-1)$ (discuter selon la parité de n)

c/c :

$\forall n \in \mathbb{Z}$: $n^p \equiv n \ [p]$

si $p \nmid n$, alors : $n \wedge p = 1$

D'après Gauss : $p \mid n(n^{p-1}-1) \Rightarrow p \mid n^{p-1}-1$

c.à.d : si $p \nmid n$ alors : $n^{p-1} \equiv 1 \ [p]$

Exemple :

2017 est premier

$\forall n \in \mathbb{Z}$: $n^{2017} \equiv n \ [2017]$

- si $2017 \nmid n$ alors : $n^{2016} \equiv 1 \ [2017]$

22