N désigne L'ensemble des entiers naturels : $N = \{0,1,2,...,n.....\}$

L'arithmétique *est l'étude des nombres entiers et des opérations sur ces nombres*

Raisonnement par récurrence

Soit à démontrer : pour tout entier naturel $n \geq n_0$ $\wp(n)$ où $\wp$ est une propriété dépendant de l'entier naturel n.

La démonstration par récurrence consiste à :
1°)Vérifier que la propriété est vraie pour la valeur n_0 : c'est l'initialisation de la récurrence et
2°)puis vérifier que si La propriété est vraie pour un certain n (fixé quelconque), alors la propriété est vraie au rang (n+1) (la propriété est dite héréditaire)
Alors , on peut conclure que pour tout $n \geq n_0$, la propriété $\wp(n)$ est vraie.

Proposition : *Pour tout $a \in N$ et $b \in N$*

$(a+b=0) \Rightarrow (a=b=0)$	$(ab=0) \Rightarrow (a=0 \quad ou \quad b=0)$	$(ab=1) \Rightarrow (a=b=1)$

La divisibilité dans N :

Soient a et d deux entiers naturels , tels que $d \neq 0$
On dit que d divise a , s'il existe $k \in N$ tel que a = kd. L'entier k est appelé le quotient de a par d.
d est appelé un diviseur de a et a est dit un multiple de d.
Notation : d \| a . $(d|a \Leftrightarrow \exists k \in N / a = kd)$

Propositions :*Pour tout $a \in N^*$, $b \in N^*$ et $c \in N^*$*

Si $(a\|b \quad et \quad b\|a)$ alors $(a=b)$	*$1\|a \qquad a\|a$*	*Si $(a\|b \quad et \quad b\|c)$ alors $(a\|c)$*
Si $(c\|a \quad et \quad c\|b)$alors $(c\|(a-b))$	*Si $(a\|b)$alors $(1 \leq a \leq b)$*	*Si c|a et c ne divise pas b alors c ne divise pas a + b.*
Si $(c\|a \quad et \quad c\|b)$ alors $(c\|(xa+yb))$ pour tout x et y de N .		

Division euclidienne dans N

Soient a et b deux entiers naturels où b > 0.

Il existe un couple unique d'entiers naturels (q,r) tels que : $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$, q est appelé le quotient , r le reste, a le dividende et b le diviseur de la division euclidienne de a par b .

Remarque important : $q = E\left(\frac{a}{b}\right) et \quad r = a - bE\left(\frac{a}{b}\right)$ *; Justifier ?*

Le PGCD de deux entiers naturels

Soient a et b deux entiers naturels non nuls.
Le PGCD de a et b est le plus grand élément de l'ensemble des diviseurs communs aux deux entiers a et b . On note par PGCD(a , b) ou $a \wedge b$. Autrement dit : $d = a \wedge b \Leftrightarrow \begin{cases} d \in D_a \cap D_b \\ \forall k \in D_a \cap D_b, \quad k|d \end{cases}$

Exemple : *Calculer $a \wedge b$ avec a = 36 et b = 24*

$a = 2^2 \times 3^2$ *et* $b = 3 \times 2^3$

On a

×	1	2	4
1	1	2	4
3	3	6	12
9	9	18	36

Alors $D_{36} = \{1,2,3,4,6,9,12,18,36\}$ *et on a*

×	1	2	4	8
1	1	2	4	8
3	3	6	12	24

Alors

$D_{24} = \{1,2,3,4,6,8,12,24\}$
Alors $D_{24} \cap D_{36} = \{1,2,3,4,6,12\}$ *alors* $24 \wedge 36 = 12$

Détermination du PGCD(a,b) en utilisant l'algorithme d'Euclide :

- *Soit r le reste de la division euclidienne de a par b alors : $a \wedge b = b \wedge r$*
- *Le $PGCD(a,b)$ est le dernier reste non nul de la suite des divisions euclidiennes dans*

L'algorithme d'Euclide:Recherche de PGCD(a,b).

On pose $a = bq_1 + r_1$, $0 \le r_1 < b$ *alors* $a \wedge b = b \wedge r_1$ *si* $r_1 \neq 0$
si $r_1 = 0$ *alors* $a \wedge b = b$.

$b = r_1q_2 + r_2$, $0 \le r_2 < r_1$ *alors* $b \wedge r_1 = r_1 \wedge r_2$ *si* $r_2 \neq 0$
si $r_2 = 0$ *alors* $b \wedge r_1 = r_1$.

$r_1 = r_2q_3 + r_3$, $0 \le r_3 < r_2$ *alors* $r_1 \wedge r_2 = r_2 \wedge r_3$ *si* $r_3 \neq 0$
si $r_3 = 0$ *alors* $r_1 \wedge r_2 = r_2$.

puisque la suite des nombres entiers positifs (r_n) *est strictement décroissante et minorée par 0, le nombre d'étapes est majoré par b et* $a \wedge b$ *est le dernier reste* r_n *non nul.*

Exemple : *Calculer* $385 \wedge 140$

a	b	r_1	r_2	r_3
385	140	105	35	0
quotient →	2	1	3	

alors $385 \wedge 140 = 35$

Entiers premiers entre eux

On dit que les deux entiers a et b sont étrangers ou premiers entre eux , si $a \wedge b = 1$

Exemple : *Montrer que 144 et 385 sont premiers entre eux .*

a	b	r_1	r_2	r_3	r_4	r_5	r_6
385	144	97	47	3	2	1	0
quotient →	2	1	2	15	1	2	

alors $144 \wedge 385 = 1$

•***Remarque :*** *On dit que* $\frac{a}{b}$ *est une fraction irréductible si et seulement si* $a \wedge b = 1$

Le PPCM de deux entiers naturels

Soient a et b deux entiers naturels non nuls. Le PPCM de a et b est le plus petit commun multiple de a et b . On note par : PPCM(a , b) ou $a \vee b$.

Autrement dit : $m = a \vee b \Leftrightarrow \begin{cases} m \in M_a \cap M_b \\ \forall k \in M_a \cap M_b, \quad m \mid k \end{cases}$

Propriétés :

Soit $a \in N^*$, $b \in N^*$ *et* $k \in N^*$

$a \mid b \rightarrow a \wedge b = a$	$ka \wedge kb = k(a \wedge b)$	$ab = (a \wedge b)(a \vee b)$
$a \mid b \rightarrow a \vee b = b$	$ka \vee kb = k(a \vee b)$	$d = a \wedge b \Rightarrow \begin{cases} a' \wedge b' = 1 \quad avec : \begin{matrix} a = da' \\ b = db' \end{matrix} \end{cases}$

Lemme de Gauss :

Soit $a \in N^*$, $b \in N^*$ *et* $c \in N^*$ *: Si :* $\begin{cases} a \wedge b = 1 \\ a \mid bc \end{cases}$ *Alors* $a \mid c$

Critères de divisibilité (rappel 2ème année)

Convention d'écriture

Pour ne pas confondre un nombre avec son écriture dans sa décomposition en base 10, on notera $\overline{a_n a_{n-1} \ldots a_1 a_0}$ *le nombre pour lequel* a_0 *est le chiffre des unités,* a_1 *celui des dizaines, etc.*

On a ainsi $x = \overline{a_n a_{n-1} \ldots a_1 a_0} = a_0.1 + a_1.10 + \ldots + a_n.10^n$

(Exemple : $x = 10296 = 6 + 9 \times 10 + 2 \times 10^2 + 0 \times 10^{13} + 1 \times 10^4$ *)*

$2 \mid x \Leftrightarrow 2 \mid a_0$
$3 \mid x \Leftrightarrow 3 \mid (a_0 + a_1 + ... + a_n)$
$4 \mid x \Leftrightarrow 4 \mid \overline{a_1 a_0}$
$5 \mid x \Leftrightarrow 5 \mid a_0$
$8 \mid x \Leftrightarrow 8 \mid \overline{a_2 a_1 a_0}$
$9 \mid x \Leftrightarrow 9 \mid (a_0 + a_1 + ... + a_n)$
$11 \mid x \Leftrightarrow 11 \mid \left(\mid a_0 - a_1 + a_2 - ... + (-1)^n a_n \mid \right)$
$25 \mid x \Leftrightarrow 25 \mid \overline{a_1 a_0}$

autres critères
$7 \mid x \Leftrightarrow 7 \mid \left(\overline{a_n a_{n-1} ... a_1} - 2a_0 \right)$
$13 \mid x \Leftrightarrow 13 \mid \left(\overline{a_n a_{n-1} ... a_1} + 4a_0 \right)$
$17 \mid x \Leftrightarrow 17 \mid \left(\overline{a_n a_{n-1} ... a_1} - 5a_0 \right)$
$19 \mid x \Leftrightarrow 19 \mid \left(\overline{a_n a_{n-1} ... a_1} + 2a_0 \right)$
$21 \mid x \Leftrightarrow 21 \mid \left(\overline{a_n a_{n-1} ... a_1} - 2a_0 \right)$
$23 \mid x \Leftrightarrow 23 \mid \left(\overline{a_n a_{n-1} ... a_1} + 7a_0 \right)$
$29 \mid x \Leftrightarrow 29 \mid \left(\overline{a_n a_{n-1} ... a_1} + 3a_0 \right)$
$31 \mid x \Leftrightarrow 31 \mid \left(\overline{a_n a_{n-1} ... a_1} - 3a_0 \right)$
$41 \mid x \Leftrightarrow 41 \mid \left(\overline{a_n a_{n-1} ... a_1} - 4a_0 \right)$

Exemple :
10296 est-il divisible par 2 ? par 3? par 4 ? par 5 ?
par 8 ? par 9 ? par 11 ? par 25 ?

On a :
[1] *Divisibilité par 2 : On a* $2 \mid 6$ *alors* $2 \mid 10296$
[2] *Divisibilité par 3 : On a :* $1+0+2+9+6=18$
alors $3 \mid (1+0+2+9+6)$ *alors* $3 \mid 10296$
[3] *Divisibilité par 4 :On a* $4 \mid 96$ *alors* $4 \mid 10296$
[4] *Divisibilité par 5 : On a 5 ne divise pas 6 alors 10296 non divisible par 5.*
[5] *Divisibilité par 8 : On a* $296 = 8 \times 37$ *alors* $8 \mid 296$ *alors* $8 \mid 10296$
[6] *Divisibilité par 9 : On a :* $1+0+2+9+6=18$ *alors* $9 \mid (1+0+2+9+6)$ *alors* $9 \mid 10296$
[7] *Divisibilité par 11 : On a :* $1-0+2-9+6=0$ *alors* $11 \mid \left(\mid 1-0+2-9+6 \mid \right)$ *alors* $11 \mid 10296$
[8] *Divisibilité par 25 : On a 25 ne divise pas 96 alors 10296 non divisible par 25.*

Nombres premiers :

Définitions :
- *Un entier naturel* $p \geq 2$ *est dit premier, si ses seuls diviseurs sont 1 et lui-meme.*
- *Un entier naturel, distinct de 1, non premier est appelé entier composé.*
- *Un entier naturel est un carré parfait lorsque sa racine carrée est un entier naturel.*

Théorèmes
- *Tout entier naturel n admet au moins un diviseur premier.*
- *Si n est un entier naturel distinct de 1, alors le plus petit diviseur de n distinct de 1 est premier.*
- *Un entier naturel n >1 est composé, si et seulement si, il admet un diviseur premier p tel que* $p \leq \sqrt{n}$

Comment reconnaître qu'un nombre est premier ?
Pour reconnaître si un nombre entier naturel n est premier, on effectue les divisions Euclidiennes successives par les nombres premiers inférieurs à $\sqrt{n}$ *pris dans l'ordre croissant.*
- *si l'une de ces divisions donne pour reste 0, alors ce nombre n'est pas premier ;*
- *si aucune division ne donne pour reste 0, on peut alors conclure que ce nombre est premier.*

Exemple : *217 est –il un nombre premier ?*
On a : $\sqrt{217} = 14.7309...$ *alors* $14^2 < 217 < 15^2$ *alors les nombres premiers* ≤ 14 *sont 2,3,5,7,11,13. Si l'un des ces nombres divise 217 alors est un nombre composé , si non , 217 est un nombre premier.*
On a : 2, 3 , 5 ne divise pas 217 mais 7 divise 217 alors 217 est un nombre composé .

Crible d'Erathostène :

C'est un tableau permettant de déterminer les nombres premiers inférieurs à 100.

Les nombres dans les cases grisées sont des nombres premiers.

Pour remplir ce tableau, on procède par élimination:

- *On élimine le 1;*
- *On garde 2 et on élimine tous les multiples de 2;*
- *On garde 3 et on élimine tous les multiples de 3;*
- *…etc*

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
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Propriétés

•Il existe une infinité de nombres premiers.

•Tout entier naturel $n \geq 2$ *, se décompose en un produit fini de nombres premiers.*

• Pour tout entier naturel $n \geq 2$ *,il existe des nombres premiers distincts deux à deux* $p_1,...,p_k$ *et des entiers naturels non nuls* $a_1,...,a_k$ *tels que* $p_1 < p_2 < .... < p_k$ *et n se décompose de façon unique sous la forme* $n = p_1^{a_1} \times p_2^{a_2} \times ... \times p_k^{a_k}$

Exemple : $n = 216$:

$$\begin{array}{r|l} 216 & 2 \\ 108 & 2 \\ 54 & 2 \\ 27 & 3 \\ 9 & 3 \\ 3 & 3 \end{array}$$

alors $216 = 2^3 \times 3^3$

•Soit a et b deux entiers naturels et p un nombre premier : Si $p|ab$ *et p ne divise pas a alors* $p|b$

Autrement :soit p un nombre premier : Si $p|ab$ *alors* $p|b$ *ou* $p|a$

•Petit théorème de Fermat

Soit p un nombre premier et a un entier naturel alors : $p|a^p - a$

Exemple : *Montrer que, si* $13|n^{13}$ *alors* $13|n$ *.*

On a : 13 est un nombre premier alors $13|n^{13} - n$ *et d'autre part on a :* $13|n^{13}$ *alors* $13|\left(n^{13} - (n^{13} - n)\right.$

alors $13|n$

Quelques repères historiques.

A. ***Pierre de Fermat (****1 601-1665) a affirmé que les nombres qui s'écrivent « $u_n = 2^{2^n} + 1$ » sont tous premiers. Vérifier ce résultat pour u_0, u_1, u_2, u_3 (Euler a prouvé que pour n=5, le nombre 4 294 967 297 est divisible par 641).*

B. ***Léonard Euler*** *(1707-1783) a trouvé que les nombres qui s'écrivent sous la forme $f(n) = n^2 + n + 41$ avec n entier naturel quelconque compris entre 0 et 39 sont premiers. Vérifier ce résultat pour $f(0), f(1), f(3)$.*

C. ***Christian Goldbach*** *(1690-1764) a conjecturé que : « tout nombre entier pair supérieur à 2 s'écrit comme somme de 2 nombres premiers ». La conjecture de Goldbach n'est toujours pas prouvée. Vérifier chacun ce résultat sur un exemple de votre choix. Vous prendrez chacun des exemples différents.*

D. ***Martin Mersenne*** *(1588-1648) a introduit les nombres qui portent son nom à l'occasion de ses recherches sur les nombres parfaits. Ce sont les nombres qui s'écrivent sous la forme $M_p = 2^p - 1$ avec p entier naturel. Mersenne savait que : « si M_p est premier alors p est premier ». Montrer que la réciproque de cette proposition est fausse.*

La recherche des nombres de Mersenne qui sont premiers continue encore aujourd'hui, on en trouve chaque année de nouveaux.

Même des non mathématiciens se sont intéressés aux nombres premiers : Marcel Pagnol a fait la proposition suivante (qui est fausse !) : « si n et n+2 sont deux nombres impairs alors $n + (n+2) + n(n+2)$ est un nombre premier ».