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* $r = a - bE\left(\frac{a}{b}\right)$*. 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 $a = bq_1 + r_1$, $0 \leq r_1 < b$ *alors* $a \wedge b = b \wedge r_1$ *si* $r_1 \neq 0$
si $r_1 = 0$ *alors* $a \wedge b = b$.

$b = r_1 q_2 + r_2,\quad 0 \le r_2 < r_1$ alors $b \wedge r_1 = r_1 \wedge r_2$ si $r_2 \neq 0$

si $r_2 = 0$ alors $b \wedge r_1 = r_1$.

$r_1 = r_2 q_3 + r_3,\quad 0 \le r_3 < r_2$ 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	$\underline{35}$	0
quotient $\to$	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	$\underline{1}$	0
quotient $\to$	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* $k \in N^*$

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

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* $a \mid c$

Nombres premiers :

Définitions :

•*Un entier naturel* $p \ge 2$ *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* $p \le \sqrt{n}$

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 $p_1,\dots,p_k$ et des entiers naturels non nuls $a_1,\dots,a_k$ tels que $p_1 < p_2 < \dots < p_k$ et n se décompose de façon unique sous la forme

$$n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}$$

Exemple : *$n = 216$:*

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

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

Théorème

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 $p|a$