Cours de mathématiques M.P.S.I.

D'après les cours de M. De Granrut

Henriet Quentin
Ausseil Lucas
Perard Arsène
Philipp Maxime

Arithmétique dans $\mathbb{Z}$

1. Multiples et diviseurs

Définition :

Soient $a, b \in \mathbb{Z}$. On dit que a divise b ou que b est un multiple de a si $\exists k \in \mathbb{Z}$ tel que $a \times k = b$.
On écrit $a|b$. On note $\mathscr{D}(a)$ l'ensemble des diviseurs de a et $a\mathbb{Z}$ l'ensemble des multiples de a.

Propriétés :

La somme de deux multiples de b est un multiple de b.
L'opposé d'un multiple de b est un multiple de b.
Tout multiple d'un multiple de b est un multiple de b.
Si b divise deux entiers, il divise leur somme.
Restreintes à $\mathbb{N}$, les relations 'multiplie' et 'divise' sont des relations d'ordre partiel.

Tout diviseur d'un diviseur de a est un diviseur de a.
0 est un multiple de tout entier. Tout entier divise 0.
Si a divise b et b divise a, alors $a = \pm b$.

Proposition :

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

1. Si $d|a$ et $d|b$ alors $\forall u, v \in \mathbb{Z},\ d|au+bv$
2. Si $x \neq 0,\ a|b \Leftrightarrow ax|bx$
3. $a|b \Leftrightarrow \mathscr{D}(a) \subset \mathscr{D}(b) \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$

Preuve :

1. $\exists k \in \mathbb{Z}$ tel que $d \times k = a$ et $\exists k' \in \mathbb{Z}$ tel que $d \times k' = b$.
   $\forall u, v \in \mathbb{Z},\ au+bv = udk+vdk' = d(uk+vk')$ Donc $d|au+bv$.
2. $\exists k \in \mathbb{Z}$ tel que $a \times k = b \Leftrightarrow axk = bx$ et $x \neq 0$ donc $ax|bx$.
3. 1. $\Rightarrow$ 2. : $\exists k \in \mathbb{Z}$ tel que $ak = b$ Soit $d \in \mathscr{D}(a)$: $\exists k' \in \mathbb{Z}$ tel que $a = dk'$
      Donc $d(kk') = b$ donc $d \in \mathscr{D}(b)$ donc $\mathscr{D}(a) \subset \mathscr{D}(b)$.
   2. $\Rightarrow$ 3. : $a \in \mathscr{D}(b)$ donc $a|b$ donc $\exists k' \in \mathbb{Z}$ tel que $ak' = b$
      $\forall m \in b\mathbb{Z},\ \exists k \in \mathbb{Z}$ tel que $m = bk = a(kk')$ donc $m \in a\mathbb{Z}$ donc $b\mathbb{Z} \subset a\mathbb{Z}$
   3. $\Rightarrow$ 1. : $b \in a\mathbb{Z}$ donc $\exists k \in \mathbb{Z}$ tel que $b = ak$ donc $a|b$.

Proposition : Division euclidienne :

Soient $a, b \in \mathbb{Z},\ b \neq 0$ alors :
Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :
$$\begin{cases} a = bq+r \\ 0 \leqslant r < |b| \end{cases}$$

Preuve :

– Unicité : Si (q', r') est un autre couple qui convient : $\begin{cases} a = bq+r \\ a = bq'+r' \end{cases}$ et $\begin{cases} 0 \leqslant r < |b| \\ 0 \leqslant r' < |b| \end{cases}$

$0 = b(q-q')+(r-r')$ et $-|b| < r-r' < |b|$
$r-r'$ est un multiple de b et $|r-r'| < |b|$ donc $r-r' = 0$ donc $b(q-q') = 0$ Or $b \neq 0$ donc $q-q' = 0$

– Existence : $a \in \mathbb{N},\ b \in \mathbb{N}^*$, Récurrence sur n : H_n : $\forall a < n,\ a \in \mathbb{N},\ \exists (q, r) \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq+r \\ 0 \leqslant r < |b| \end{cases}$

· H_b est vraie : en effet $\forall a < b$ $\begin{cases} a = b \times 0 + a \\ 0 \leqslant a < b \end{cases}$

· Supposons $n \in \mathbb{N},\ n \geqslant b$ et H_n vraie.
$\forall a < n+1$: Si $a < n$ H_n vraie $\Rightarrow$ existence de (q, r)

Sinon $a = n \geqslant b \Rightarrow 0 \leqslant a-b < n \Rightarrow \exists (q, r) \in \mathbb{N}^2$ tel que $\begin{cases} a-b = bq+r \\ 0 \leqslant r < b \end{cases} \Rightarrow \begin{cases} a = b(q+1)+r \\ 0 \leqslant r < b \end{cases}$

Donc H_{n+1} est vraie.

Par récurrence, l'existence est prouvée.

2. Diviseurs communs et PGCD

2.1. Définition

Définition :

Soient $a, b \in \mathbb{Z}$.

- $\mathscr{D}(a) \cap \mathscr{D}(b)$ est une partie non vide de $\mathbb{Z}$, majorée par $|a|$ ou $|b|$, elle possède donc un plus grand élément appelé pgcd de a et de b noté $a \wedge b$.
- $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}$ est une partie non vide de $\mathbb{N}$.
  Si $a=0$ ou $b=0$: $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N} = \{0\}$
  Sinon cette partie possède un plus petit élément strictement positif appelé ppcm de a et de b noté $a \vee b$.

On convient que : $0 \vee n = 0 \quad 0 \wedge 0 = 0 \quad \forall a \in \mathbb{N},\ a \wedge 0 = a$

2.2. Algorithme d'Euclide

Proposition :

$\forall a, b \in \mathbb{Z},\ b \neq 0$
Si $a = bq + r$, alors $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$.

Preuve :

$\subset$: $\forall d \in \mathscr{D}(a) \cap \mathscr{D}(b)$
$\begin{cases} d|a \\ d|b \end{cases} \Rightarrow d|a - bq = r$ Donc $d \in \mathscr{D}(r)$

$\supset$: $\forall d \in \mathscr{D}(b) \cap \mathscr{D}(r)$
$\begin{cases} d|b \\ d|r \end{cases} \Rightarrow d|bq + r = a$ Donc $d \in \mathscr{D}(a)$

Algorithme :

On construit une suite de d'entiers naturels ainsi :

- $r_0 = a \quad r_1 = b$
- Si $r_{n+1} \neq 0$, r_{n+2} = reste de la division euclidienne de r_n par r_{n+1}
- Sinon, on s'arrête.

D'après la proposition, $\mathscr{D}(r_n, r_{n+1}) = \mathscr{D}(r_{n+1}, r_{n+2})$ donc $r_n \wedge r_{n+1} = r_{n+1} \wedge r_{n+2}$
Or, $0 \leqslant r_{n+2} < r_{n+1}$ $(r_n)_{n \geqslant 1}$ est une suite d'entiers naturels strictement décroissante.
Donc il existe un rang N tel que $r_{N+1} = 0$ et $\forall n < N+1,\ r_n \neq 0$
$a \wedge b = r_n \wedge r_{n+1} = r_N \wedge 0 = r_N$: Dernier reste non nul.

2.3. Couple de Bézout

Proposition :

$\forall a, b \in \mathbb{Z} \quad \exists (u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$
Ce couple (u, v) s'appelle couple de Bézout.

Preuve :

Prenons $b \in \mathbb{N}$. Récurrence sur b : H_b : $\forall a \in \mathbb{Z},\ \exists (u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$

- Pour $b=0$: $a \wedge 0 = a = a \times 1 + b \times 0$ $(1, 0)$ convient.
- Supposons $b \in \mathbb{N}$ et $H_b, H_{b-1}, \ldots, H_0$ vraies.

  $\forall a \in \mathbb{Z},\ a \wedge (b+1) = (b+1) \wedge r$ où r = reste de $\dfrac{a}{b-1}$

  $H_r \Rightarrow \exists (u, v) \in \mathbb{Z}^2$ tel que $(b+1)u + rv = (b+1) \wedge r \Leftrightarrow (b+1)u + (a - (b+1)q)v = a \wedge (b+1)$
  $\Leftrightarrow av + (b+1)(u - qv) = a \wedge (b+1)$

  Donc H_{b+1} est vraie.

Par récurrence, la propriété est vraie $\forall b \in \mathbb{N}$.

Remarques :

– Un tel couple n'est pas unique.

– S'il existe $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=d$ alors $a\wedge b|d$.

2.4. Nombres premiers entre eux

Définition :

On dit que deux entiers a et b sont premiers entre eux si $a\wedge b=1$.

Théorème de Bézout :

$$a\wedge b=1 \Leftrightarrow \exists(u,v)\in\mathbb{Z}^2 \text{ tel que } au+bv=1$$

Preuve :

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

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

Donc $a\wedge b=1$ ou $a\wedge b=-1$ Or, $a\wedge b\leqslant 0$ Donc $a\wedge b=1$.

Théorème de Gauss :

$$\forall a,b,c\in\mathbb{Z},\quad \begin{cases} a|bc \\ a\wedge b=1 \end{cases} \Rightarrow a|c$$

Preuve :

$\exists k\in\mathbb{Z}$ tel que $ak=bc$, $\exists(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

$au+bv=1 \Leftrightarrow auc+bvc=c \Leftrightarrow a(uc+vk)=c \Leftrightarrow a|c$.

Corollaire 1 :

$$\begin{cases} a|c \\ b|c \\ a\wedge b=1 \end{cases} \Rightarrow ab|c$$

Preuve :

$\exists k,k'\in\mathbb{Z}$ tels que $c=ak=bk'$

$\exists(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1 \Rightarrow acu+bcv=c$

$\Rightarrow abk'u+bakv=c \Rightarrow ab(k'u+kv)=c \Rightarrow ab|c$.

Corollaire 2 :

$$\begin{cases} a\wedge c=1 \\ b\wedge c=1 \end{cases} \Rightarrow ab\wedge c=1$$

Preuve :

$\exists(u,v)\in\mathbb{Z}^2$ tel que $au+cv=1$, $\exists(u',v')\in\mathbb{Z}^2$ tel que $bu'+cv'=1$

$(ab)(uu')+c(auv'+bu'v+cvv')=1$

Donc ab et c sont premiers entre eux.

Proposition : Caractérisation du PGCD :

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

$$d=a\wedge b \Leftrightarrow \exists a',b'\in\mathbb{Z} \text{ tels que } \begin{cases} a=da' \\ b=db' \\ a'\wedge b'=1 \end{cases}$$

Preuve :

$\Rightarrow$: $d|a$: $\exists a'\in\mathbb{Z}$ tel que $a=da'$ $d|b$: $\exists b'\in\mathbb{Z}$ tel que $b=db'$

$\exists(u,v)\in\mathbb{Z}^2$ tel que $au+bv=d \Leftrightarrow da'u+db'v=d \Leftrightarrow a'u+b'v=1 \Leftrightarrow a'\wedge b'=1$

$\Leftarrow$: $d|a$ et $d|b \Rightarrow d|a\wedge b$

$\exists(u,v)\in\mathbb{Z}^2$ tel que $a'u+b'v=1 \Leftrightarrow a'du+b'dv=d \Leftrightarrow au+bv=d$ Donc $a\wedge b|d$

Donc $d=\pm a\wedge b$ Or, $d\in\mathbb{N}$ donc $d=a\wedge b$.

Proposition : Calcul du PPCM :

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

Preuve :

– Si $a=0$ ou $b=0$: alors $a\vee b=0$, $|ab|=0$ La formule est vérifiée.

– Si $a,b\in\mathbb{Z}^*$, $d=a\wedge b$, $\exists a',b'\in\mathbb{Z}$ tels que $\begin{cases} a=da' \\ b=db' \\ a'\wedge b'=1 \end{cases}$ Il faut montrer que $a\vee b=d|a'b'|$

· $da'b'=ab'=a'b$ donc $da'b'$ est un multiple commun de a et de b.

· Si m est un multiple de a et de b : $\exists k,q\in\mathbb{Z}$ tels que $m=ak=bq=da'k=db'q \Rightarrow a'|q$

Donc $\exists q'\in\mathbb{Z}$ tel que $q=a'q'$ Donc $m=db'a'q'$ est un multiple de $db'a'$ Donc $|db'a'|$ est le ppcm.

3. Nombres premiers

Définition :

Un nombre premier est un entier supérieur ou égal à 2 divisible uniquement par 1 et par lui-même.

Crible d'Ératosthène :

	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	

Proposition :

Soit $p>1$. Les assertions suivantes sont équivalentes :

1. p est premier
2. p est premier avec tout nombre entier qu'il ne divise pas : $p\nmid n \Rightarrow p\wedge n=1$
3. $\forall k\in[\![1,p-1]\!],\ p\wedge k=1$.

Preuve :

1. $\Rightarrow$ 2. : Par l'absurde, si $p\wedge k=d,\ d\neq 1$

$$\begin{cases} d\mid p \\ d\neq 1 \\ p \text{ premier} \end{cases} \Rightarrow d=p \Rightarrow p\mid k$$ Impossible.

2. $\Rightarrow$ 3. : $1\leqslant k\leqslant p-1 \Rightarrow p\nmid k \Rightarrow p\wedge k=1$

3. $\Rightarrow$ 1. : p n'a pas de diviseur inférieur à p autre que 1 : p est premier.

Corollaire :

Si p est premier : $p\mid ab \Rightarrow p\mid a$ ou $p\mid b$.

Preuve :

Par contraposition, $p\nmid a$ et $p\nmid b \Rightarrow \begin{cases} p\wedge a=1 \\ p\wedge b=1 \end{cases} \Rightarrow p\wedge(ab)=1 \Rightarrow p\nmid ab$

Remarque :

p non premier $\Leftrightarrow \exists a,b\in\mathbb{N}^*\setminus\{1\}$ tels que $q=ab$.

Théorème fondamental de l'arithmétique :

Tout entier supérieur ou égal à 2 se décompose en produit de nombres premiers. Cette décomposition est unique à l'ordre des facteurs près.

Théorème :

Il y a une infinité de nombres premiers.

Preuve :

1ère méthode : On suppose qu'il n'existe que N nombres premiers $p_1, p_2, \ldots, p_n$

Soit $q=p_1p_2\ldots p_n+1 \quad \forall k\in[\![1,N]\!],\ q>p_k$, donc q n'est pas premier.

Donc $\exists k\in[\![1,N]\!]$ tel que $p_k\mid q$ Par différence, $p_k\mid 1$ Impossible.

2ème méthode : $n\neq m \Rightarrow F_n\wedge F_m=1$ Il existe deux nombres premiers différents, p_n et p_m tels que $p_n\mid F_n$ et $p_m\mid F_m \Rightarrow$ Infinité de nombres premiers.

Preuve du théorème fondamental :

Existence de la décomposition : Par récurrence sur n : H_n : n se décompose en produit de nombres premiers.

- Pour $n=2$: $2=2$ premier Vrai.
- Supposons $n\geqslant 2$ et $H_n, H_{n-1}, \ldots, H_2$ vraies.

  Si $n+1$ est premier : $n+1=n+1$ premier Donc H_{n+1} vraie.

  Sinon, $\exists a, b\in\mathbb{N}\setminus\{0,1\}$ tels que $n+1=ab$

  $a\geqslant 2 \Rightarrow b\leqslant\dfrac{n+1}{2}\leqslant 2$ et $b\geqslant 2 \Rightarrow a\leqslant\dfrac{n+1}{2}\leqslant n$

  H_a vraie $\Rightarrow \exists p_1,\ldots,p_\alpha$ des nombres premiers tels que $a=p_1\ldots p_\alpha$

  H_b vraie $\Rightarrow \exists q_1,\ldots,q_\beta$ des nombres premiers tels que $b=q_1\ldots q_\beta$

  $n+1=ab=p_1\ldots p_\alpha q_1\ldots q_\beta$ Donc H_{n+1} est vraie.

Par récurrence, H_n est vraie $\forall n\geqslant 2$.

Unicité : Par récurrence sur n : H_n : La décomposition de n est unique à l'ordre des facteurs près.

- Pour $n=2$: $2=2$ Vrai
- Supposons $n\geqslant 2$ et $H_n, H_{n-1}, \ldots H_2$ vraies.

  Si $n+1$ est premier, $n+1=n+1$ premier Donc H_{n+1} est vraie.

  Sinon, si $n+1=p_1\ldots p_\alpha=q_1\ldots q_\beta$

  $\begin{cases} p_1 \text{ premier} \\ p_1 | q_1\ldots q_\beta \end{cases} \Rightarrow \exists k\in[\![1,\beta]\!] \text{ tel que } p_1|p_k \Rightarrow p_1=q_k$

  Alors $p_2\ldots p_\alpha=q_1\ldots q_{k-1}q_{p+1}\ldots q_\beta=\dfrac{n+1}{p_1}\leqslant n$ $\left(\dfrac{n+1}{p_1}\in\mathbb{N}\right)$

  Or, $H_{\frac{n+1}{p_1}}$ est vraie, donc H_{n+1} est vraie.

Par récurrence, la propriété est vraie $\forall n\geqslant 2$.

Définition :

Soit $n=2^{v_2}\cdot 3^{v_3}\cdot\ldots\cdot p^{v_p}$

v_k est appelé valuation de k dans $\mathbb{N}$.

Proposition (admise) :

Soient $n=2^{v_2}\cdot 3^{v_3}\cdot\ldots\cdot p^{v_p}$ et $m=2^{w_2}\cdot 3^{w_3}\cdot\ldots\cdot p^{w_p}$

Alors : $n\wedge m=2^{\min(v_2,w_2)}\cdot 3^{\min(v_3,w_3)}\cdot\ldots\cdot p^{\min(v_p,w_p)}$ et $n\vee m=2^{\max(v_2,w_2)}\cdot 3^{\max(v_3,w_3)}\cdot\ldots\cdot p^{\max(v_p,w_p)}$

* * * * *