1. Cours 1: Arithmétique dans Z

1.1. Divisibilité:

Soient a , b deux entiers ($a, b \in Z$)
On dit que b divise a , s'il exite $q \in Z$ tel que $a = qb$

Exemple 1: 1 divise tout entier a En effet: $a = a.1$
Exemple 2: Tout entier b divise 0 En effet: $0 = 0.b$
Exemple 3: $n+1$ divise n^2+n En effet: $n^2+n = n(n+1)$

1.1.1 Remarques:

R1) 0 ne divise que 0
R2) Les seuls diviseurs de 1 sont 1 et -1.
R3) Si b divise a , on dit aussi que a est un multiple de b

1.1.2 Proposition: *Soient a* et b deux entiers
i) a divise b , si et seulement, si $bZ \subset aZ$
ii) $a = \pm\, b$, si et seulement, si $bZ = aZ$

Preuve: Evidente

1.2. Division euclidienne dans Z :

Soient a , b deux entiers ($a, b \in Z$)
Si $b \neq 0$, alors il existe un couple $(q, r) \in Z^2$ tels que
$a = qb + r$ *et* $0 \leq r < |b|$

Preuve:a) Pour montrer l'existence, on a deux cas.

a.1) Si $b > 0$, soit r le plus petit élément positif ou nul de $a - bZ = \{..., a+2b, a+b, a, a-b, a-2b, ...\}$. On a $r = a - bq$ pour un certain $q \in Z$ et $r \geq 0$. Pour montrer que $r < |b| = b$, on suppose que $b \leq r$, alors on aura $0 \leq r - b = a - (q+1)\, b \in a - bZ$, donc $r \leq r - b$ (car r est le plus petit) ,ce qui est imppossible car $b > 0$.

a.2) Si $b < 0$, alors $-b > 0$ et d'après le cas **a.1)**, il existe (q, r) tel que $a = q(-b) + r$ avec $0 \leq r < -b$, ce qui revient à dire que $a = (-q)\, b + r$ avec $0 \leq r < |b| = -b$

Dans les deux cas : $\exists\, (q, r) \in Z^2$ tel que $a = qb + r$ et $0 \leq r < |b|$

1.3. Sous groupes de $(Z,+)$

Un sous groupe de $(Z,+)$ est un sous ensemble non vide de Z stable par sommation et par passage au symétrique. C.à.d .Un sous ensemble H de Z est un sous groupe[1] de $(Z,+)$, si, et seulement si $H \neq \emptyset$ et $\forall x, y \in H : (x+y \in H$ et $-x \in H)$
Exemple 1: On peut facilement vérifier que les ensembles aZ sont des sous groupes de $(Z,+)$. Le théorème suivant montre que tous les sous groupes de $(Z,+)$ sont de la forme aZ.

1.3.1.Théorème: *Soit H un sous groupe de $(Z,+)$.*
Il existe un unique entier naturel a , tel que $H = aZ$
Preuve:

1^{er} cas: Si $H = \{0\}$, alors $H = 0Z$ et 0 est l'unique entier a vérifiant $aZ = \{0\}$.

$2^{ème}$ cas: Si $H \neq \{0\}$, Soit a le plus petit élément strictement positif de H. Comme H est un sous groupe de $(Z,+)$, alors $as = \underbrace{a+a+...+a}_{s \text{ termes}} \in H$ d'où $aZ \subset H$.

Inversement; pour tout $x \in H$, il existe $(q,r) \in Z^2$ tel que $r = x - qa$, avec $0 \leq r < a$ (**Voir 1.2**). Comme H est un sous groupe et $x \in H$, $qa \in H$, alors $x - qa \in H$ et le fait que $0 \leq r < a$, implique $r = 0$ (car a est le plus petit entier naturel appartenant à H). Par conséquent $x = aq$ et $H \subset aZ$

Les deux inclusions obtenues donnent l'égalité $H = aZ$.

Si $aZ = a'Z$, alors $a = a't$ et $a' = at'$ donc a divise a' et a' divise a , d'où l'égalité $a = a'$ et l'unicité de a.

1.4. Notion de pgcd et de ppcm.

Soient $a_1, a_2, ..., a_p$ des entiers. On rappelle que

$\bigcap_{i=1}^{p} a_i Z = a_1 Z \cap a_2 Z \cap ... \cap a_p Z$ et $\sum_{i=1}^{p} a_i Z = a_1 Z + a_2 Z + ... + a_p Z$

1.4.1.Théorème et définition: *Soient $a_1, a_2, ..., a_p$ des entiers.*

1) Il existe un entier naturel unique d vérifiant $\sum_{i=1}^{p} a_i Z = dZ$.

2) Il existe un entier naturel unique m vérifiant $\bigcap_{i=1}^{p} a_i Z = mZ$.

d s'appelle le plus grand commun diviseur de la fammille $a_1, a_2, ..., a_p$ et il est noté $pgcd\,(a_1, a_2, ..., a_p)$

[1] Les notions de groupes et de sous groupes vont être étudiées en détail dans le **cours 4.**

m s'appelle le plus petit commun multiple de la fammille $a_1, a_2, ..., a_p$ et il est noté $ppcm\,(a_1, a_2, ..., a_p)$

Preuve:

1) Montrons que $\sum_{i=1}^{p} a_i Z$ est un sous groupe de $(Z, +)$. En effet: Si $x,\ y \in \sum_{i=1}^{p} a_i Z$, alors $x = a_1x_1 + a_2x_2 + ... + a_px_p$ et $y = a_1y_1 + a_2y_2 + ... + a_py_p$ d'où $x + y = a_1(x_1 + y_1) + a_2(x_2 + y_2) + ... + a_p(x_p + y_p) \in \sum_{i=1}^{p} a_i Z$ et $-y = a_1(-y_1) + a_2(-y_2) + ... + a_p(-y_p) \in \sum_{i=1}^{p} a_i Z$. Donc $\sum_{i=1}^{p} a_i Z$ est un sous groupe de $(Z, +)$ et par application du **th 1.3.1** on conclut l'existence et l'unicité de l'entier naturel d vérifiant $\sum_{i=1}^{p} a_i Z = dZ$.

2) Montrons que $\bigcap_{i=1}^{p} a_i Z$ est un sous groupe de $(Z, +)$. En effet: Si $x, y \in \bigcap_{i=1}^{p} a_i Z$, alors $\forall i \in \{1, 2, ..., p\}$ on a $x \in a_i Z$ et $y \in a_i Z$ d'où $x + y \in a_i Z$ et $-y \in a_i Z$. Donc $\bigcap_{i=1}^{p} a_i Z$ est un sous groupe de $(Z, +)$ et par application du **th 1.3.1** on conclut l'existence et l'unicité de l'entier naturel m vérifiant $\bigcap_{i=1}^{p} a_i Z = mZ$. ■

Exemple: $4Z = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}$ et $6Z = \{..., -12, -6, 0, 6, 12, ...\}$ alors $4Z \cap 6Z = 12Z$ donc $ppcm(4, 6) = 12$

1.4.2 Remarque: Le $pgcd\,(a_1, a_2, ..., a_p)$ et le $ppcm\,(a_1, a_2, ..., a_p)$ son parfois notés respectivement $a_1 \wedge a_2 \wedge ... \wedge a_p$ et $a_1 \vee a_2 \vee ... \vee a_p$

1.4.3 Théorème (Caractérisation du *pgcd* et du *ppcm*): *Soient $a_1, a_2, ..., a_p$ des entiers.*

1) L'entier naturel d est le $pgcd\,(a_1, a_2, ..., a_p)$, si et seulement, si

$$\begin{cases} \text{i) } \forall i \in \{1, 2, ..., p\} \text{ : } d \text{ divise } a_i \\ \text{ii) } (\forall i \in \{1, 2, ..., p\} \text{ : } d' \text{ divise } a_i) \Longrightarrow d' \text{ divise } d \end{cases}$$

2) L'entier naturel m est le $ppcm\,(a_1, a_2, ..., a_p)$, si et seulement, si

$$\begin{cases} \text{i) } \forall i \in \{1, 2, ..., p\} \text{ : } a_i \text{ divise } m \\ \text{ii) } (\forall i \in \{1, 2, ..., p\} \text{ : } a_i \text{ divise } m) \Longrightarrow m \text{ divise } m' \end{cases}$$

Preuve:1) i) Si $d = pgcd\,(a_1, a_2, ..., a_p)$, pour tout i on a $a_i Z \subset \sum_{i=1}^{p} a_i Z = dZ$ donc d'après la **prop1.1.1** d divise a_i, pour tout i.

ii) Si d' divise tous les a_i, alors d'après la **prop 1.1.1** $a_iZ \subset d'Z$ pour tout i , d'où $d'Z \supset \sum_{i=1}^{p} a_iZ = dZ$ et toujours d'après la **prop 1.1.1** d' divise d.

Inversement, soit d un entier naturel vérifiant i) et ii). D'après i), d divise tous les a_i donc $a_iZ \subset dZ$ et $\sum_{i=1}^{p} a_iZ \subset dZ$, d'où d divise $pgcd\,(a_1, a_2, ..., a_p)$. En utilisant ii) et le fait que, $\forall i \in \{1, 2, ..., p\}$: $pgcd\,(a_1, a_2, ..., a_p)$ divise a_i, on conclut qe $pgcd\,(a_1, a_2, ..., a_p)$ divise d , d'où l'égalité $pgcd\,(a_1, a_2, ..., a_p) = d$.

L'assertion 2) se démotre de la même façon que 1)

.

1.4.4 Propriétés du *pgcd* **et du** *ppcm***:** *Soient $a_1, a_2, ..., a_p$ des entiers.*

1) Le pgcd et le ppcm ne changent pas en permuttant les a_i

2) $pgcd\,(\pm a_1, \pm a_2, ..., \pm a_p) = pgcd\,(a_1, a_2, ..., a_p)$
et $ppcm\,(\pm a_1, \pm a_2, ..., \pm a_p) = ppcm\,(a_1, a_2, ..., a_p)$

3) Pour tout $c \in Z$ *on a* $pgcd\,(ca_1, ca_2, ..., ca_p) = |c|\,pgcd\,(a_1, a_2, ..., a_p)$ *et* $ppcm\,(ca_1, ca_2, ..., ca_p) = |c|\,ppcm\,(a_1, a_2, ..., a_p)$

4) Pour tout $q \in \{1, 2, ..., p-1\}$ *, on a:*
$pgcd\,(a_1, a_2, ..., a_p) = pgcd\,(pgcd\,(a_1, a_2, ..., a_q)\,, pgcd\,(a_{q+1}, a_{q+2}, ..., a_p))$
et $ppcm\,(a_1, a_2, ..., a_p) = ppcm\,(ppcm\,(a_1, a_2, ..., a_q)\,, ppcm\,(a_{q+1}, a_{q+2}, ..., a_p))$

(C.à. d pgcd et ppcm sont associatifs)

Preuve: La est donnée seulement pour le *pgcd* car elle est analogue pour le *ppcm*.

1) $\sum_{i=1}^{p} a_iZ$ ne change pas en permuttant les a_i d'où le résultat.

2) Pour tout i , ona $\pm a_iZ = a_iZ$, donc $\sum_{i=1}^{p} a_iZ$ ne change pas en remplaçant les a_i par $\pm a_i$, d'où le résultat.

3) Pour tout i , ona $ca_iZ = \pm ca_iZ = |c|\,a_iZ$, donc $\sum_{i=1}^{p} ca_iZ = |c| \sum_{i=1}^{p} a_iZ$,d'où le résultat, par appliction de la **prop 1.1.1**.

4) $\sum_{i=1}^{p} a_iZ = \sum_{i=1}^{q} a_iZ + \sum_{i=q+1}^{p} a_iZ$, donc le *pgcd* est associatif. ■

Exemple: $pgcd\,(-2, 4, -7) = pgcd\,(2, 4, 7) = pgcd\,(pgcd\,(2, 4)\,, pgcd\,(7))$
$= pgcd\,(2pgcd\,(1, 2)\,, 7) = pgcd\,(2, 7) = 1$

1.5. Nombres premiers entre eux

1.5.1 Définition: *Soit* $(a_1, a_2, ..., a_q) \in Z^p$
1) On dit que $a_1, a_2, ..., a_q$ *sont premiers entre eux si* $a_1 \wedge a_2 \wedge ... \wedge a_q = 1$.
2) On dit que $a_1, a_2, ..., a_q$ *sont deux à deux premiers entre eux si* $a_i \wedge a_j = 1$. *pour* $i \neq j$ *(* $i, j \in \{1, 2, ..., p\}$*)*

1.5.1.1 Remarque: 2) $\Longrightarrow$ 1) . En effet 2) $\Longrightarrow a_1 \wedge a_2 = 1$ d'où $a_1 \wedge a_2 \wedge ... \wedge a_q = 1 \wedge a_3 \wedge ... \wedge a_q = 1$ par appllication de la **propriété 1.4.4, 4)**

La réciproque est trivialement fausse.

1.5.2 Théorème de Bezout: *Les entiers* $a_1, a_2, ..., a_q$ *sont premiers entre eux si, et seulement, s'il existe* $(u_1, u_2, ..., u_q) \in Z^p$ *tel que* $\sum_{i=1}^{p} a_i u_i = 1$

Preuve: On a $a_1 \wedge a_2 \wedge ... \wedge a_q = 1$ donc $\sum_{i=1}^{p} a_i Z = 1.Z$, alors il existe $(u_1, u_2, ..., u_q) \in Z^p$ tel que $\sum_{i=1}^{p} a_i u_i = 1$.

Inversement, si $\sum_{i=1}^{p} a_i u_i = 1$, alors tout diviseur commun des a_i divise 1, donc $a_1 \wedge a_2 \wedge ... \wedge a_q$ divise 1, alors il est égal à 1 ■

1.5.3 Théorème de Gauss: Soient a, b, c d*es entiers*

Si a divise bc et , alors *sont premiers entre eux si, et seulement, s'il existe* $(u_1, u_2, ..., u_q) \in Z^p$ *tel que* $\sum_{i=1}^{p} a_i u_i = 1$

Preuve: IL existe u et v tels que $au + bv = 1$ en multipliant par $c = auc + bvc$ donc a divise c car a divise $auc + bvc$ ■

1.5.4 Propriétés des nombres premiers entre eux: *Soient* $a_1, a_2, ..., a_q, a, b, c$ *des entiers et* m, n *des entiers naturels*

1)Si $\forall i \in \{1, 2, ..., p\} : a_i \wedge c = 1$, *alors* $\left(\prod_{i=1}^{p} a_i\right) \wedge c = 1$

2) Si $a \wedge b = 1$ *Alors* $a^n \wedge b^m = 1$

3) Si $a_1, a_2, ..., a_q$ *sont premiers entre eux, alors* $a_1 \vee a_2 \vee ... \vee a_q = \left|\prod_{i=1}^{p} a_i\right|$

4) $(a \wedge b)(a \vee b) = |ab|$ *(cette propriété n'est toujours vraie que pour deux*

entiers)

5) Si $a_1, a_2, ..., a_q$ sont premiers entre eux et chaque a_i divise b , alors $\prod_{i=1}^{p} a_i$ divise b

Preuve:

1) $a_i \wedge c = 1$, alors il existe des entires u_i et v_i tels que $a_i u_i + c v_i = 1$. En multipliant ces égalités, on obtient $1 = \prod_{i=1}^{p} (a_i u_i + c v_i) = \left(\prod_{i=1}^{p} a_i u_i \right) + R$ où R est la somme des termes qui restent , qui contiennent tous c comme facteur.

Alors $1 = \left(\prod_{i=1}^{p} a_i \right) .u + cv$; où $u = \prod_{i=1}^{p} u_i$ et $v = \frac{R}{c} \in Z$. donc $\left(\prod_{i=1}^{p} a_i \right) \wedge c = 1$ (d'après le théorème de Bezout: Th 1.5.2)

2) Si $n = 0$ où $m = 0$, il est clair que $a^n \wedge b^m = 1$.

Et si $n \neq 0$ et $m \neq 0$, alors d'après 1), on a $a^n \wedge b = 1$ en choisissant $a_1 = a_2 = ... = a_p = a$ et $c = b$, en suite $a^n \wedge b^m = 1$ toujours d'après 1), en choisissant $a_1 = a_2 = ... = a_p = b$ et $c = a^n$.

3) Commençons par le cas $p = 2$, et soit $m = a_1 \vee a_2$. On $a_1 \wedge a_2 = 1$, alors il existe u_1, $u_2 \in Z$ tels que $a_1 u_1 + a_2 u_2 = 1$, donc $m = a_1 u_1 m + a_2 u_2 m$, or $m = a_1 m_1$ et $m = a_2 m_2$ d'où $m = a_1 a_2 (u_1 m_1 + u_2 m_2)$, et $a_1 a_2$ divise m, mais m divise $a_1 a_2$ (car $a_1 a_2$ est un multiple commun de a_1 et a_2), alors on a l'égalité $a_1 a_2 = m = a_1 \vee a_2$.

Pour le cas p quelconque , on procède par récurence en supposant la propriété vraie à l'ordre q et montons la à l'ordre $q = q + 1$.

On a d'après 1) $\left(\prod_{i=1}^{q} a_i \right) \wedge a_{q+1} = 1$ et d'après le cas $p = 2$, ona $\left(\prod_{i=1}^{q} a_i \right) \vee a_{q+1} = \left| \prod_{i=1}^{q+1} a_i \right|$. En utilisant l'hypothèse de réccurence et l'associativité du *ppcm* (**Pté 1.4.1**), on conclut que: $\left| \prod_{i=1}^{q+1} a_i \right| = (a_1 \vee a_2 \vee ... \vee a_q) \vee a_{q+1} = a_1 \vee a_2 \vee ... \vee a_q \vee a_{q+1}$

4) Si $a = 0$ ou $b = 0$ l'égalité est triviale.

Et si $a \neq 0$ et $b \neq 0$, les entiers $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premier entre eux, alors d'après 3) $\frac{a}{a \wedge b} \vee \frac{b}{a \wedge b} = \frac{a}{a \wedge b} \times \frac{b}{a \wedge b}$ et en utilisant **Pté 1.4.1,** on conclut que $ab = (a \wedge b)^2 \frac{a \vee b}{a \wedge b} = (a \wedge b)(a \vee b)$.

5) b est un multiple commun des a_i, donc c'est un multiple de leur *ppcm* qui est égal, d'après 3), à $\left| \prod_{i=1}^{p} a_i \right|$, donc $\prod_{i=1}^{p} a_i$ divise b. ■

1.5.5 Application à la résolution d'équations linéaires dans Z:

Soient a, b des entiers non nuls et c un entier quelconque et soit l'équation

$$ax + by = c \tag{1.1}$$

d'inconnues x et y.

Soit $d = pgcd\,(a, b)$;

1) Si d ne divise pas c, alors l'équation (1) n'a pas de solution.

2) Si d divise c l'équation (1) est èquivalente à l'équation $a'x + b'y = c'$ (1'), où $a' = \frac{a}{d}$, $b' = \frac{b'}{d}$ et $c' = \frac{c}{d}$.

On a $a' \wedge b' = 1$, alors il existe u' et v' dans Z tels que $a'u' + b'v' = 1$, donc $a'u'c' + b'v'c' = c'$ et le couple $(x_0, y_0) = (u'c', v'c')$ est une solution particulière de l'équation (1).

Pour trouver toutes les solutions de (1), il suffit de remarquer que $a'x + b'y = c' = a'x_0 + b'y_0$, d'où $a'\,(x - x_0) = -b'\,(y - y_0)$ et par application du théorème de Gauss **(Th 1.5.3)** , on conlut du fait que $a' \wedge b' = 1$, que $x - x_0 = b'q$, $q \in Z$, ce qui entraîne $y - y_0 = -a'q$.

Inversement, il est clair que les couples trouvés $(x, y) = (b'q + x_0, -a'q + y_0)$, $q \in Z$, vérifient l'équation (1).

Exemple 1: L'équation $4x + 6y = 7$ n'admet pas de solutions, car $pgcd\,(4, 6)$ ne divise pas 7.

Exemple 2: Soit l'équation $4x + 6y = 8$.

$pgcd\,(4, 6) = 2$ et l'équation donnée et équivalante à $2x + 3y = 4$ qui admet $(x_0, y_0) = (-1, 2)$ comme solution particulière, ansi $2x + 3y = 2\,(-1) + 3\,(2)$, alors $2\,(x + 1) = -3\,(y - 2)$, donc $\begin{cases} x + 1 = 3q \\ y - 2 = -2q \end{cases}$ $q \in Z$ et les couples $(x, y) = (3q - 1, -2q + 2)$, $q \in Z$ sont toutes les solutions de l'équation donnée.

1.6. Congruences

1.6.1 Théorème et définition: *Pour chaque $n \in N$, soit la relation $\mathcal{R}_n$ définit sur Z par:*

$$x\mathcal{R}_n y \text{ si, et seulement, si } n \text{ divise } y - x \tag{1.2}$$

1) La relation $\mathcal{R}_n$ est une relation d'équivalence[2]*, appellée relation de congruence modulo n.*
$x\mathcal{R}_n y$ est noté $x \equiv y\,[n]$ et se lit :" x est congru y modulo n".
2) L'ensemble des classes d'équivalence $\overline{x}$ de cette relation est noté Z/nZ

$$\overline{x} = \{x + nq : q \in Z\}$$

Preuve: Il est facile de monter que $\mathcal{R}_n$ est une relation d'équivalence.

1.6.2 Théorème: *La relation de congruence modulo n est compatible avec les lois $+$ et $\times$.*

C.à.d: $\begin{cases} x \equiv y\,[n] \\ x' \equiv y'\,[n] \end{cases} \Longrightarrow \begin{cases} x + x' \equiv (y + y')\,[n] \\ xx' \equiv yy'\,[n] \end{cases}$

Preuve:

1) On a $\begin{cases} x \equiv y\,[n] \\ x' \equiv y'\,[n] \end{cases}$, alors n divise $(y - x)$ et $(y' - x')$

et comme $\begin{cases} (y + y') - (x + x') = (y - x) + (y' - x') \\ yy' - xx' = y\,(y' - x') + x'\,(y - x) \end{cases}$, alors

n divise $(y + y') - (x + x')$ et $yy' - xx'$, et par conséquent $\begin{cases} x + x' \equiv (y + y')\,[n] \\ xx' \equiv yy'\,[n] \end{cases}$

Exemple: Déterminons les entiers naturels n tels que 7 divise $2^n - 1$.

Ce qui revient à trouver n tel que $2^n \equiv 1\,[7]$. On a $2^0 \equiv 1\,[7]$
$2^1 \equiv 2\,[7]$
$2^2 \equiv 4\,[7]$
$2^3 \equiv 1\,[7]$

En utilisant la compatibilité de la congruence et sa transitivité, on peut montrer que la suite des restes de la division de 2^n par 7 est périodique, de période égale à 3, donc $2^n \equiv 1\,[7]$,ssi, $n = 3p$, $p \in N$

1.7. Nombres premiers

1.7.1 Théorème: *On appelle nombre premier tout entier $p > 1$ dont les seuls diviseurs positifs sont 1 et p.*

Exemple 1: 2 est un nombre premier (et c'est le seul nombre premier pair)

[2] La notion de relation d'équivalence sera étudiée en détail dans le **cours 3**

Exemple 2: 1 n'est pas un nombre premier.
Exemple 3: -3 n'est pas un nombre premier.

1.7.2 Proposition: *Soient p un nombre premier et $a, a_1, a_2, ..., a_P$ des entiers, alors:*
1) Ou bien p est premier avec a ou bien p divise a.
2) Si p divise $\prod_{i=1}^{p} a_i$, alors p divise au moins l'un des a_i.
Preuve:

1) Les seule diviseurs positifs de p sont 1 et p, alors ou bien $pgcd\,(a,p) = 1$, donc p et premier avec a, ou bien $pgcd\,(a,p) = p$ et p divise a.

2) Supposons que p ne divise aucun a_i , alors d'après 1) , il est premier avec tous les a_i, et d'après **Pté 1.5.4** , p est premier avec $\prod_{i=1}^{p} a_i$, ce qui est absurde. ■

1.7.3 Théorème: *Tout entier $n > 1$ possède au moins un diviseur premier*

Preuve: **L'**Enseble $\mathcal{D}_n$ des diviseurs de n, qui son plus grands que 1 n'est pas vide (car $n \in \mathcal{D}_n$), alors il possède un plus petit élément p. Cet élément p est premier. En effet: Soit d un diviseur de p tel que $d > 1$, alors $d \in \mathcal{D}_n$, donc $d \geq p$ (car $p = \min \mathcal{D}_n$), d'où l'égalité $d = p$, alors p est premier. ■

1.7.4 Théorème: (Décomposition en facteurs premiers)

Pour tout entier $n > 1$, il existe, de façon unique, des nombres premiers $p_1 < p_2 < ... < p_r$ et des nombres entiers naturels $\alpha_1, \alpha_2, ..., \alpha_r$ tels que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.

Preuve: Supposons qu'il y a des entiers $n > 1$ qui ne s'écrivent pas sous forme de produit de facteurs premiers et soit n_0 le plus petit de ces entiers. n_0 n'est pas premier (Sinon il s'écrira comme produit d'un seul facteur) , alors $n_0 = n_1 n_2$ tels que $n_1 > 1, n_2 > 1$ et $n_1 < n_0$, $n_2 < n_0$, donc n_1 et n_2 s'écrivent comme produit de facteurs premiers, et par suite leur produit n_0 s'écrit comme produit de facteurs premiers, ce qui est absurde. D'où l'existence de la décomposition.

Pour l'unicité, supposons $n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{j=1}^{s} q_j^{\beta_j}$. On a chaque p_i divise $\prod_{j=1}^{s} q_j^{\beta_j}$, alors d'après **Prop 1.7.2** p_i divise au moins l'un des q_j , alors $p_i = q_j$. Par cconséquent $\{p_1, p_2, ..., p_r\} \subset \{q_1, q_2, ..., q_s\}$. De la même façon, on montre l'autre inclusion, d'où l'égalité $\{p_1, p_2, ..., p_r\} = \{q_1, q_2, ..., q_s\}$.

Alors $r = s$ et $p_i = q_i$, car $(p_i)_i$ et $(q_j)_j$ sont strictement ordonés.

Pour montrer que $\alpha_i = \beta_i$, supposons $\alpha_i < \beta_i$ et éliminons p_i du premier membre de l'égalité $\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r} q_i^{\beta_i}$, alors $\prod_{\substack{k=1 \\ k\neq i}}^{r} p_k^{\alpha_k} = q_i^{\beta_i - \alpha_i} \prod_{\substack{k=1 \\ k\neq i}}^{r} q_k^{\beta_k}$ et p_i divise le deuxième membre sans diviser le premier, ce qui est impossible. De la même façon, on montre qu'il est impossible d'avoir $\alpha_i > \beta_i$, d'où l'égalité $\alpha_i = \beta_i$ ■

1.7.5 Calcul du *pgcd* et du *ppcm* à l'aide de la décomposition en facteurs premiers:

Soit $n \in N^*$, Pour tout nombre premier p , on note par $v_p(n)$, l'exposant de p dans la décomposition en facteurs premiers de n. Alors:

$v_p(n) = 0$, si p ne divise pas n

$v_p(n) \neq 0$, si p divise n

Donc la décomposition donnée par le théorème **Th 1.7.4** , peut être écrite $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$, où $\mathcal{P}$ est l'ensemble de tous les nombres premiers.

Exemple 1: $v_2(20) = 2$, $v_3(20) = 0$
$v_5(20) = 1$, $v_p(20) = 0$ pour tout nombre premier $p \geq 7$

Exemple 1: Pour tout nombre premier p, ona: $v_p(p) = 1$ et $v_p(p^m) = m$.

1.7.5.1 Remarque: Pour tout entier n , les $v_p(n)$ sont nuls à partir d'un certain rang p.

1.7.6 Théorème: *Soient $a_1, a_2, ...a_s$ des entiers naturels non nuls.*

On a, alors
$$\begin{cases} pgcd(a_1, a_2, ...a_s) = \prod_{p\in\mathcal{P}} p^{\min(v_p(a_1), v_p(a_2), ..., v_p(a_s))} \\ ppcm(a_1, a_2, ...a_s) = \prod_{p\in\mathcal{P}} p^{\max(v_p(a_1), v_p(a_2), ..., v_p(a_s))} \end{cases}$$

Preuve: 1) Soit $d = pgcd(a_1, a_2, ...a_s)$ et $\delta = \prod_{p\in\mathcal{P}} p^{\min(v_p(a_1), v_p(a_2), ..., v_p(a_s))}$.

Pour tout i ; $p^{\min(v_p(a_1), v_p(a_2), ..., v_p(a_s))}$ divise les $p^{v_p(a_i)}$, d'où
$\prod_{p\in\mathcal{P}} p^{\min(v_p(a_1), v_p(a_2), ..., v_p(a_s))}$ divise les $\prod_{p\in\mathcal{P}} p^{v_p(a_i)} = a_i$ et d'après le **Th 1.4.3** on conclut que δ divise d.

Inversement, $d = \prod_{p\in\mathcal{P}} p^{\min(v_p(a_1), v_p(a_2), ..., v_p(a_s))}$ et comme d divise les a_i, alors $v_p(d) \leq v_p(a_i)$, pour tout $i \in \{1, 2, ..., s\}$, donc
$v_p(d) \leq \min(v_p(a_1), v_p(a_2), ..., v_p(a_s))$ et $p^{v_p(d)}$ divise $p^{\min(v_p(a_1), v_p(a_2), ..., v_p(a_s))}$, et par passage au produit, on aura d divise δ , d'où l'égalité $d = \delta$. ■

Université Ibn Khaldoun de Tiaret.
Département d'Informatique.
Module:Algèbre 1 ($1^{ère}$ Année LMD)

Fiche de T.D N^0 1

Exercice 1: Détérminer les couples $(a,b) \in N^2$ vérifiant:
$2m + 7d = 111$ où $d = pgcd\,(a,b)$ et $m = ppcm\,(a,b)$

Exercice 2: Résoudre dans N^2 le système $\begin{cases} x^2 - y^2 = 5440 \\ x \wedge y = 8 \end{cases}$

Exercice 3: Pour tout $n \in N$, on pose $u_n = 2^n + 3^n$
1) Montrer que u_n et u_{n+1} sont premiers entre eux.
2) Calculer $u_{n+1} \wedge u_{n+2}$

Exercice 4: Soient $(a,b) \in Z^{*2}$, et $d = a \wedge b$
Calculer $pgcd\,(a^2, ab, b^2)$ et $pgcd\,(a^3, a^2b, ab^2, b^3)$

Exercice 5: Soient a et b des entiers, tels que $a > b > 0$.
Montrer que $\frac{a^2+b^2}{a^2-b^2}$ n'est pas un entier.

Exercice 6: Pour quel entier n a t-on :
$3.5^{2n+1} + 2^{3n+1} \equiv 0\,[7]$
$2^{2n} + 2^n + 1 \equiv 0\,[21]$

Exercice 7: Démontrer les affirmation suivantes:
1) Pour que $2^n - 1$ soit premier il faut que n soit premier.
2) Pour que $2^n + 1$ soit premier il faut que n soit une puissance de 2.

Exercice 8: En travaillant sur la décomposition en facteurs premiers, montrer que: $pgcd\,(ab, bc, ca)\,.ppcm\,(a,b,c) = abc$

Exercice 9: Résoudre les équations suivantes:
1) $5x + 7y = 11$, $(x,y) \in Z^2$
2) $5x + 7y + 11z = 11$, $(x,y,Z) \in Z^3$