157	Arithmétique dans $\mathbb{Z}$.	Th. fondamental de l'arithmétique (Monier p.119)	Monier alg.MPSI Damphousse Terracher T.S.

I. Divisibilité.

Def.1 : Soit (a,b)∈$\mathbb{Z}^2$. On dit que **a divise b** dans $\mathbb{Z}$, et on note a|a ssi ∃c∈$\mathbb{Z}$ tel que b=ac.

On dit aussi a est un diviseur de b, ou b est un multiple de a.
On notera **Div(a)** l'ensemble des diviseurs de a.
On notera $a\mathbb{Z}=\{b\in\mathbb{Z}/\exists c\in\mathbb{Z}:b=ac\}$; alors ∀a,b∈$\mathbb{Z}$, $a\mid b\Leftrightarrow a\mathbb{Z}\supset b\mathbb{Z}$.(1)

Th.1 et Def.2 (TER) : (2)
Soit $(a,b)\in\mathbb{Z}\times\mathbb{N}^*$. $\exists!(q,r)\in\mathbb{Z}^2$ t.q.
$$\begin{cases}a=bq+r\\0\le r<b\end{cases}$$
On dit que q est le quotient et r le reste de la **division Euclidienne** de a par b.

Remarque: ∀a∈$\mathbb{N}^*$, ∀b∈$\mathbb{Z}$, a|b ssi le reste de la division Euclidienne de b par a est nul.

Application(DAM): Expression d'un nombre dans une base.

II. PGCD, PPCM.

Prop.1 et Def.3: Soient $n\in\mathbb{N}^*,(x_1,\dots,x_n)\in(\mathbb{Z}^*)^n$. (3)

1) L'ensemble des diviseurs communs à $x_1,\dots,x_n$ est fini et admet un plus grand élément appelé **plus grand commun diviseur** de $x_1,\dots,x_n$ et noté $\text{pgcd}(x_1,\dots,x_n)$.
2) L'ensemble des éléments de $\mathbb{N}^*$ multiples communs à $x_1,\dots,x_n$ admet un plus petit élément appelé **plus petit commun multiple** de $x_1,\dots,x_n$ et noté $\text{ppcm}(x_1,\dots,x_n)$

Pour a,b∈$\mathbb{Z}^*$,on notera:
pgcd(a,b)=$a\wedge b$; ppcm(a,b)=$a\vee b$

Prop.2: Soient $n\in\mathbb{N}^*,(x_1,\dots,x_n)\in(\mathbb{Z}^*)^n$,
$\delta=\text{pgcd}(x_1,\dots,x_n)$, $\mu=\text{ppcm}(x_1,\dots,x_n)$. On a:
$$\delta\mathbb{Z}=\sum_{i=1}^{n}x_i\mathbb{Z}\quad\text{et}\quad\mu\mathbb{Z}=\bigcap_{i=1}^{n}x_i\mathbb{Z}.$$

Prop.3: Avec les notations précédentes,
a divise tous les x_i ssi a divise δ;
tous les x_i divisent b ssi μ divise b. (4)

Une première méthode de calcul de pgcd(a,b): l'Algorithme d'Euclide.

III. Nombres premiers entre eux.

Def.4: Soient $n\in\mathbb{N}^*,(x_1,\dots,x_n)\in(\mathbb{Z}^*)^n$.
1) On dit que $x_1,\dots,x_n$ sont **premiers entre eux dans leur ensemble** ssi $\text{pgcd}(x_1,\dots,x_n)=1$.
2) On dit que $x_1,\dots,x_n$ sont **premiers entre eux deux à deux** ssi :
$$\forall(i,j)\in\{1,\dots,n\}^2,(i\neq j\Rightarrow x_i\wedge x_j=1)$$

Remarque: "premiers entre eux deux à deux "⟹ "premiers entre eux dans leur ensemble", mais la réciproque est fausse.

Prop.4: $\forall(a,b,c)\in(\mathbb{Z}^*)^3,\left(\begin{cases}a\wedge b=1\\c\mid b\end{cases}\Rightarrow a\wedge c=1\right)$

Th.2: **Théorème de Bézout** (5)
Soient $n\in\mathbb{N}^*,(x_1,\dots,x_n)\in(\mathbb{Z}^*)^n$.

Pour que $x_1,\dots,x_n$ soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existe $(u_1,\dots,u_n)\in\mathbb{Z}^n$ t.q.:
$$\sum_{i=1}^{n}x_iu_i=1.$$

Remarque: La Pté.2 et le th. de Bézout font un lien entre une pté arithmétique et une écriture algébrique.

Méthode: Les coefficients de Bézout peuvent se calculer en utilisant "**l'algorithme d'Euclide étendu**".

Exercice: Calculer des coefficients de Bézout pour a=693 et b=680.(6)

Application (DAM): **Construction de polygones réguliers**.
Si m et n sont premiers entre eux, et que les polygones réguliers à m et n côtés sont constructibles à la règle et au compas, alors le polygone à mn côtés l'est aussi.(7)

Th.3: **Théorème de Gauss** (8)
$$\forall(a,b,c)\in(\mathbb{Z}^*)^3,\left(\begin{cases}a\mid bc\\a\wedge b=1\end{cases}\Rightarrow a\mid c\right).$$

Application (DAM): **Problème de visibilité**.
Dans un verger, le puits est en (0,0) et les arbres occupent exactement les autres points de coordonnées entières. Quels sont les arbres visibles depuis le puits?(9)

Prop.5: Soient n∈$\mathbb{N}^*$, a, $x_1,\dots x_n$∈$\mathbb{Z}^*$. On a:
$$\left(\forall i\in[\![1;n]\!],a\wedge x_i=1\right)\Leftrightarrow a\wedge\left(\prod_{i=1}^{n}x_i\right)=1.$$

IV. Utilisation des nombres premiers.

Def.5: $p\in\mathbb{N}$ est dit **premier** ssi $p\geq 2$ et: $\forall a\in\mathbb{N}^*, \left(a \mid p \Rightarrow \left(a=1 \text{ ou } a=p\right)\right)$.

Un entier non premier est dit composé. On dira que $n\in\mathbb{Z}$ est premier ssi $|n|$ est premier.

Th.4: **Décomposition en facteurs premiers**.
Tout élément de $\mathbb{N}-\{0;1\}$ admet une décomposition en facteurs premiers, unique à l'ordre des facteurs près.

Exemples: $9100=2^2.5^2.7.13$, et $1848=2^3.3.7.11$.

Remarque 1: cette décomposition s'appelle aussi "décomposition primaire".

Remarque 2(DAM): L'unicité de cette décomposition ne va pas de soi; dans l'ens. des entiers pairs, 60=6x10=2x30.

Prop.6: Soit $(a,b)\in\left(\mathbb{N}-\{0;1\}\right)^2$,

$a=\prod_{i=1}^{N} p_i^{r_i}, b=\prod_{i=1}^{N} p_i^{s_i}$, où $N\in\mathbb{N}^*$,

$p_1,\ldots,p_N$ sont premiers et deux à deux distincts,

$r_1,\ldots,r_N,s_1,\ldots,s_N\in\mathbb{N}$ éventuellement nuls.

On a: $a\wedge b=\prod_{i=1}^{N} p_i^{Min(r_i,s_i)}$ et $a\vee b=\prod_{i=1}^{N} p_i^{Max(r_i,s_i)}$.

Exemples:

$9100\wedge 1848=2^2.7^1=28$

$9100\vee 1848=2^3.3^1.5^2.7^1.11^1.13^1=600\ 600$

Application: Les lois $\wedge$ et $\vee$ sont distributives l'une sur l'autre dans $\mathbb{Z}^*$.

°Prop.7:
Soient $a,b\in\mathbb{Z}^*$. On a: $\text{pgcd}(a,b)\times\text{ppcm}(a,b)=|ab|$

V. Notes.

Utilise:"Découvrir l'arithmétique" de Pierre Damphousse, Ellipses (B.U. Ref:511DAM).
°Modifications apportées par rapport au cours de Monier.

(1): La relation | (divise) est réflexive et transitive, mais pas antisymétrique: ce n'est pas une relation d'ordre. Contre-ex: -2 et 2. En revanche, c'est une relation d'ordre (non total) dans $\mathbb{N}$.

(2): Démo dans le Terracher T.S.

(3): Toute partie **finie** non vide de $\mathbb{Z}$ admet un plus grand élément. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément ("on dit que $\mathbb{N}$ est bien ordonné").

(4): Ainsi les mots "grand" et "petit" dans pgcd et ppcm le sont au sens de la divisibilité.

(5): Bézout: Ce serait en fait le théorème de Bachet dans les entiers, étendu par Bézout aux polynômes.
Attention, il n'y a PAS unicité des coefficients.
Démo de Bézout:
$\Rightarrow$ Supp. les x_i premiers entre eux ds leur ensemble.
D'après la Pté2, $\sum_{i=1}^{n} x_i\mathbb{Z}=\delta\mathbb{Z}=\mathbb{Z}$
Comme $1\in\mathbb{Z}$, $\exists(u_i)\in\mathbb{Z}^n$ convenable.
$\Leftarrow$ Supp $\exists(u_i)\in\mathbb{Z}^n$ convenable, i.e. $\sum_{i=1}^{n} x_iu_i=1$
Alors $1\in\sum_{i=1}^{n} x_i\mathbb{Z}=\delta\mathbb{Z}$, donc $\delta=1$.

(6): Pour a=693 et b=680.
693=680x1+13 (3)
680=13x52+4 (2)
13=4x3+1 (1)
(4=1x4+0)
(1) → 1=13-**4**x3
On remplace 4 par sa valeur issue de (2): 4=680-13x52
Il vient: 1=**13**-[680-**13**x52]x3.
On remplace 13 par sa valeur issue de (3): 13=693-680x1
Il vient: 1=(693-680x1)-[680-(693-680x1)x52]x3.
Finalement: 1=693-680-680.3+693.52.3-680.52.3
i.e. 1=693(1+52.3)-680(1+3+52.3)
i.e. 1=157.693+ (-160).680

(7): M.q. l'on peut construire un angle de $\frac{2\pi}{mn}$, sachant que l'on peut construire ceux de $\frac{2\pi}{m}$ et $\frac{2\pi}{n}$.

$\lambda m+\mu n=1$, donc $\lambda\frac{2\pi}{n}+\mu\frac{2\pi}{m}=\frac{2\pi}{mn}$.

Pour construire l'angle $\frac{2\pi}{mn}$, on reporte λ fois l'angle $\frac{2\pi}{n}$, et μ fois l'angle $\frac{2\pi}{m}$.

(8): Gauss: D'après Bézout, a|bc et a∧b=1 ⟹ ∃u,v t.q. au+bv=1. Alors c = c.1 = cau + cbv = a(cu) + (bc)v. Or a|bc, donc a|(bc)v. Comma a|a(cu), finalement a|c.

(9): Si on note δ=pgcd(a,b), alors l'arbre (a,b) est caché derrière l'arbre $\left(\frac{a}{\delta};\frac{b}{\delta}\right)$. Donc les arbres visibles satisfont pgcd(a,b)=1.
Réciproquement, si pgcd(a,b)=1, et (a,b) est caché par (u,v), on a $\frac{b}{a}=\frac{v}{u}$,
donc $bu=av$, i.e. $a\mid bu$ et $u<a$. Or a et b premiers entre eux, donc a|u, ce qui contredit u<a.