Arithmétique dans Z

I. Divisibilité

1°) Divisibilité dans Z

Déf : Soit $a,b\in\mathbb{Z}$. On dit que a divise b ssi $\exists k\in\mathbb{Z}$ tel que $b=ak$.
On note alors $a\mid b$ et on dit que a est un diviseur de b et que b est un multiple de a.

Prop : $\forall a,b\in\mathbb{Z}, a\mid b\Rightarrow(-a)\mid b, a\mid(-b)$ et $(-a)\mid(-b)$.

Prop : $\forall a,b\in\mathbb{Z}$ avec $b\neq 0$. $a\mid b\Rightarrow|a|\leq|b|$.

Déf : Pour $a\in\mathbb{Z}$ on note Div(a) l'ensemble des diviseurs de a et Mul(a) l'ensemble des multiples de a.
Ainsi : Div(a) $=\{k\in\mathbb{Z}/k\mid a\}$ et Mul(a) $=\{ak/k\in\mathbb{Z}\}$ (aussi noté $a\mathbb{Z}$).

Prop : $a\mid b$ et $b\mid c\Rightarrow a\mid c$, $a\mid b$ et $b\mid a\Rightarrow|a|=|b|$,
$a\mid b$ et $a\mid c\Rightarrow a\mid(b+c)$, $a\mid b$ et $c\mid d\Rightarrow ac\mid bd$,
$a\mid b\Rightarrow\forall p\in\mathbb{N}, a^p\mid b^p$.

2°) Division euclidienne

Théorème :

$\forall a\in\mathbb{Z},\forall b\in\mathbb{N}^*,\exists!(q,r)\in\mathbb{Z}^2$ tel que $\begin{cases}a=bq+r\\0\leq r<b\end{cases}$.

q et r sont respectivement appelés quotient et reste de la division euclidienne de a par b. (visualisation dans la barre de division).

Prop : $\forall a\in\mathbb{Z}$ et $\forall b\in\mathbb{N}^*$, on a équivalence entre :
(i) $b\mid a$,
(ii) le reste de la division euclidienne de a par b est nul.

3°) Calculs en congruence

Déf : Soit $a,b\in\mathbb{Z}$. On dit que a est congru à b modulo n ssi $n\mid(a-b)$. On note alors $a=b\ [n]$. Ainsi $a=b\ [n]\Leftrightarrow\exists k\in\mathbb{Z}, a=b+k.n$.

Prop : $\forall a\in\mathbb{Z},\exists!r\in\{0,1,\ldots,n-1\}$ tel que $a=r\ [n]$.
De plus r correspond au reste de la division euclidienne de a par n.

Prop : $a=b\ [n]\Leftrightarrow b=a\ [n]$
$a=b\ [n]$ et $b=c\ [n]\Rightarrow a=c\ [n]$.

Prop : Soit $a,a',b,b'\in\mathbb{Z}$ vérifiant $a=a'\ [n]$ et $b=b'\ [n]$. On a
$a+b=a'+b'\ [n]$, $ab=a'b'\ [n]$, $-a=-a'\ [n]$ et $\forall p\in\mathbb{N}, a^p=a'^p\ [n]$.

II. PGCD et PPCM

1°) PGCD de deux entiers

Déf : Soit $a,b\in\mathbb{Z}$. Tout $d\in\mathbb{Z}$ tel que $d\mid a$ et $d\mid b$ est appelé diviseur commun à a et b.
On note Div(a,b) l'ensemble des diviseurs communs à a et b. Ainsi Div(a,b) = Div(a) $\cap$ Div(b).

Prop : $\forall a,b\in\mathbb{Z}$ tels que $(a,b)\neq(0,0)$ l'ensemble Div(a,b) possède un plus grand élément.

Déf : Soit $a,b\in\mathbb{Z}$ tels que $(a,b)\neq(0,0)$. Le plus grand élément de Div(a,b) est appelé pgcd de a et b. On le note pgcd(a,b) ou encore $a\wedge b$.

Convention : On pose pgcd(0,0) = 0.

Prop : $\forall a,b\in\mathbb{Z}$, pgcd(a,b) $\in\mathbb{N}$, pgcd(a,b) = pgcd(b,a) et pgcd(a,b) = pgcd($|a|,|b|$).

Prop : $\forall a,b \in \mathbb{Z}, a \mid b \Rightarrow \text{pgcd}(a,b) = |a|$.

Prop : Soit $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et r le reste de la division euclidienne de a par b.
On a $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

On peut calculer le pgcd de deux entiers par une succession de division euclidienne diviseur par reste : c'est l'algorithme d'Euclide.

2°) Egalité de Bézout

Théorème :
$\forall a,b \in \mathbb{Z}, \exists u,v \in \mathbb{Z}$, $\text{pgcd}(a,b) = au + bv$. Une telle relation est appelée égalité de Bézout.

3°) Propriété arithmétique du pgcd

Théorème :
$\forall a,b \in \mathbb{Z}, \forall d \in \mathbb{Z}$, $d \mid a$ et $d \mid b \Leftrightarrow d \mid \text{pgcd}(a,b)$.

Cor : $\text{Div}(a,b) = \text{Div}(\text{pgcd}(a,b))$.

Prop : $\forall a,b \in \mathbb{Z}, \forall \lambda \in \mathbb{N}, \text{pgcd}(\lambda a, \lambda b) = \lambda \,\text{pgcd}(a,b)$.

4°) PPCM de deux entiers

Déf : Soit $a,b \in \mathbb{Z}$. Tout $m \in \mathbb{Z}$ tel que $a \mid m$ et $b \mid m$ est appelé multiple commun à a et b. L'ensemble des multiples communs à a et b est noté $\text{Mul}(a,b)$. Ainsi $\text{Mul}(a,b) = \text{Mul}(a) \cap \text{Mul}(b)$.

Prop : $\forall a,b \in \mathbb{Z}^*$, l'ensemble $\text{Mul}(a,b) \cap \mathbb{N}^*$ possède un plus petit élément.

Déf : Soit $a,b \in \mathbb{Z}$ tels que $a \neq 0$ et $b \neq 0$, le plus petit élément de $\text{Mul}(a,b) \cap \mathbb{N}^*$ est appelé ppcm de a et b.
On le note $\text{ppcm}(a,b)$ ou $a \vee b$.

Convention : Si $a = 0$ ou $b = 0$, on pose $\text{ppcm}(a,b) = 0$.

Prop : $\forall a,b \in \mathbb{Z}$, $\text{ppcm}(a,b) \in \mathbb{N}$, $\text{ppcm}(a,b) = \text{ppcm}(b,a)$ et $\text{ppcm}(a,b) = \text{ppcm}(|a|,|b|)$.

Prop : $\forall a,b \in \mathbb{Z}$, $a \mid b \Rightarrow \text{ppcm}(a,b) = |b|$.

5°) Propriété arithmétique du ppcm

Théorème :
$\forall a,b \in \mathbb{Z}, \forall m \in \mathbb{Z}, a \mid m$ et $b \mid m \Leftrightarrow \text{ppcm}(a,b) \mid m$.

Cor : Par suite : $\text{Mul}(a,b) = \text{Mul}(\text{ppcm}(a,b))$.

Prop : $\forall a,b \in \mathbb{Z}, \forall \lambda \in \mathbb{N}, \text{ppcm}(\lambda a, \lambda b) = \lambda \,\text{ppcm}(a,b)$.

III. Nombres premiers entre eux

1°) Définition

Déf : Soit $a,b \in \mathbb{Z}$. On dit que a et b sont premiers entre eux ssi ils n'ont pas d'autres diviseurs communs que 1 et -1.

Prop : Soit $a,b \in \mathbb{Z}$. On a équivalence entre :
(i) a et b sont premiers entre eux,
(ii) $\text{pgcd}(a,b) = 1$.

Prop : $\forall a,b,a',b' \in \mathbb{Z}$, $(a' \mid a, b' \mid b$ et $a \wedge b = 1) \Rightarrow a' \wedge b' = 1$.

2°) Théorème de Bézout

Théorème :
Soit $a,b \in \mathbb{Z}$. On a équivalence entre :
(i) a et b sont premiers entre eux,
(ii) $\exists u,v \in \mathbb{Z}, au + bv = 1$.

Prop : $\forall a,b,c \in \mathbb{Z}$, $(a \wedge b = 1$ et $a \wedge c = 1) \Rightarrow a \wedge bc = 1$.

Prop : $a \wedge b_1 = \ldots = a \wedge b_n = 1 \Rightarrow a \wedge (b_1 \ldots b_n) = 1$

$a \wedge b = 1 \Rightarrow \forall n, m \in \mathbb{N}, a^n \wedge b^m = 1.$

3°) Théorème de Gauss

Théorème :

$\forall a, b, c \in \mathbb{Z}$, $(a \mid bc$ et $a \wedge b = 1) \Rightarrow a \mid c$.

Théorème :

$\forall a, b, c \in \mathbb{Z}$, $(a \mid c, b \mid c$ et $a \wedge b = 1) \Rightarrow ab \mid c$.

Prop : Si $a_1 \mid b, \ldots, a_n \mid b$ et $a_1, \ldots, a_n$ deux à deux premiers entre eux alors $a_1 \ldots a_n \mid b$.

4°) Applications

a) factorisation du pgcd

Théorème :

$\forall a, b \in \mathbb{Z}$, en notant $\delta = \text{pgcd}(a, b)$ on peut écrire :

$a = \delta a'$ et $b = \delta b'$ avec $a', b' \in \mathbb{Z}$ tels que $\text{pgcd}(a', b') = 1$.

b) produit du pgcd et du ppcm de deux entiers

Théorème :

$\forall a, b \in \mathbb{Z}$, $\text{pgcd}(a, b)\,\text{ppcm}(a, b) = |ab|$.

c) représentant irréductible d'un nombre rationnel

Théorème :

$$\forall r \in \mathbb{Q}, \exists!(p, q) \in \mathbb{Z} \times \mathbb{N}^*,\ r = \frac{p}{q} \text{ et } p \wedge q = 1.$$

Le rapport $\frac{p}{q}$ est appelé représentant irréductible du nombre rationnel r.

IV. Décomposition primaire d'un entier

1°) Nombres premiers

Déf : Soit $p \in \mathbb{N}$ tel que $p \geq 2$. On dit que p est premier ssi ses seuls diviseurs positifs sont 1 et p.
Sinon, l'entier p est dit composé.
On note $\mathcal{P}$ l'ensemble des nombres premiers.

Prop : Soit $n \geq 2$, si n est composé alors n possède un diviseur d avec $2 < d \leq \sqrt{n}$.

Déf : On appelle facteur premier d'un entier n tout $p \in \mathcal{P}$ tel que $p \mid n$.

Prop : Tout $n \geq 2$ possède au moins un facteur premier.

Prop : $\mathcal{P}$ est infini.

2°) Propriétés arithmétiques des nombres premiers

Prop : $\forall a \in \mathbb{Z}$, $\forall p \in \mathcal{P}$, $p \nmid a \Rightarrow p \wedge a = 1$

Théorème : (lemme d'Euclide)

$\forall a, b \in \mathbb{Z}$, $\forall p \in \mathcal{P}$, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

Cor : $\forall a_1, \ldots, a_n \in \mathbb{Z}, \forall p \in \mathcal{P}$, $p \mid a_1 \ldots a_n \Rightarrow \exists 1 \leq i \leq n, p \mid a_i$.

3°) Décomposition primaire

Théorème :

$\forall n \in \mathbb{N} \setminus \{0,1\}$, $\exists N \in \mathbb{N}^*, \exists p_1, \ldots, p_N \in \mathcal{P}$ distincts, $\exists \alpha_1, \ldots, \alpha_n \in \mathbb{N}^*$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_N^{\alpha_N}$.

De plus cette décomposition est unique à l'ordre près des facteurs.

Déf : Cette écriture est appelée décomposition primaire de l'entier $n \geq 2$.
Les $p_1, \ldots, p_N$ correspondent alors aux facteurs premiers de n.

4°) Diviseurs d'un entier

Théorème :

Soit $n \in \mathbb{N}^*$ s'écrivant $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ avec $p_1, \dots, p_N$ nombres premiers deux à deux distincts et $\alpha_1, \alpha_2, \dots, \alpha_N \in \mathbb{N}$. Les diviseurs positifs de n sont les entiers d pouvant s'écrire $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_N^{\beta_N}$ avec $\forall 1 \leq i \leq N, 0 \leq \beta_i \leq \alpha_i$.

5°) Pgcd, ppcm et décomposition primaire

Soit $a, b \in \mathbb{N}$ tels que $a, b \geq 2$.

A partir des décompositions primaires de a et b on peut écrire simultanément :

$a = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ et $b = p_1^{\beta_1} \dots p_N^{\beta_N}$ avec $p_1, \dots, p_N$ nombre premiers deux à deux distincts et $\alpha_1, \dots, \alpha_N, \beta_1, \dots, \beta_N \in \mathbb{N}$.

Théorème :

Avec les écriture ci-dessus : $\text{pgcd}(a,b) = \prod_{i=1}^{N} p_i^{\min(\alpha_i, \beta_i)}$ et $\text{ppcm}(a,b) = \prod_{i=1}^{N} p_i^{\max(\alpha_i, \beta_i)}$.