Arithmétique dans $\mathbb{Z}$

I. Division euclidienne dans $\mathbb{Z}$

Définition. *Soit $(n,p) \in \mathbb{Z}^2$ on dit que p divise n ou que p est un diviseur de n ou que n est un multiple de p et l'on note p/n s'il existe un entier relatif q tel que $n = pq$.*
L'ensemble des multiples de p est noté $p\mathbb{Z} = \{pq,\ q \in \mathbb{Z}\}$

Remarque : Ainsi, 0 est un multiple de tous les entiers et tous les entiers divise 0.
Par contre, n'a qu'un seul multiple : lui-même.
Remarque : Si p divise n et si n est non nul, alors $|p| \leq |n|$.

Définition. *Deux entiers relatifs n et p sont dits associés lorsque n/p et p/n.*

Proposition. *Deux entiers relatifs n et p sont associés si et seulement si $n = \pm p$.*

Proposition. *Soit $(n,p) \in \mathbb{Z}^2$ alors p divise n si et seulement si $n\mathbb{Z} \subset p\mathbb{Z}$.*

Théorème. *(*) Soient $(m,n) \in \mathbb{Z} \times \mathbb{N}^*$.*
Il existe un unique couple d'entiers $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tels que $0 \leq r < m$ et $m = nq + r$.
On dit que r est le reste de la division Euclidienne de m par n et que q en est le quotient.

Théorème. *(*) Tout sous-groupe de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{N}$ unique.*

II. PGCD et PPCM

1. PGCD

Définition. *Soient a et b deux entiers naturels non nuls. On appelle Plus Grand Diviseur Commun de a et b et l'on note $pgcd(a,b)$ ou $a \wedge b$, le plus grand des diviseurs communs à a et b.*

Remarque : Cette définition a un sens car l'ensemble des diviseurs communs à a et b est une partie de $\mathbb{Z}$ non vide (elle contient 1) et majorée par a (car $a \neq 0$). Elle possède donc un plus grand élément.

En pratique pour obtenir le PGCD de deux entiers naturels a et b non nuls tels que $a < b$, on utilise l'algorithme d'Euclide.
On pose $r_0 = b$, $r_1 = a$, $r_2 = r_0 \% r_1$ et tant que r_k est non nul, $r_{k+1} = r_{k-1} \% r_k$.

Proposition. *(*) L'algorithme d'Euclide se termine et le dernier reste non nul est égal à $a \wedge b$.*

Proposition. *(*) Soient a et b deux entiers naturels non nuls.*
L'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ (u,v) \in \mathbb{Z}^2\}$ est un groupe égal à $(a \wedge b)\mathbb{Z}$.

Théorème. ***(*) avec l'algorithme d'Euclide et avec les groupes***
Soient a et b deux entiers naturels non nuls. Leur PGCD vérifie les propriétés suivantes :
- *$pgcd(a,b)$ est un diviseur commun à a et b*
- *tout diviseur commun à a et b divise $pgcd(a,b)$*

De plus il existe des entiers relatifs u et v tels que $a \wedge b = au + bv$
Cette relation est appelée relation de Bézout.

Définition. *Si a et b sont deux entiers relatifs non nuls, alors on appelle PGCD de a et b celui de $|a|$ et $|b|$*
Si $a \in \mathbb{Z}^*$ alors $a \wedge 0 = a$.

Remarque : Il n'y a pas de plus grand diviseur de zéro donc on ne peut pas parler du PGCD de 0 et 0.
Remarque : Soient $(a, b) \in \mathbb{Z}^2$ et $c \in \mathbb{N}$ alors $c = a \wedge b$ si et seulement si

$$c/a, \quad c/b \quad \text{et} \quad \forall d \in \mathbb{Z},\ (d/a \text{ et } d/b) \Rightarrow d/c$$

On dit que le PGCD de a et b est le plus grand diviseur positif de a et b au sens de la divisibilité.
Remarque : Soient $(a, b) \in \mathbb{Z}^2$ et $c \in \mathbb{N}$ alors $c = a \wedge b$ si et seulement si

$$\forall d \in \mathbb{Z}, \quad (d/a \text{ et } d/b) \Leftrightarrow d/c$$

Définition. *Deux entiers relatifs a et b sont dits premiers entre eux si $a \wedge b = 1$*

Proposition. *(*) Soient $(a, b, c) \in \mathbb{Z}^3$ alors $(ac) \wedge (bc) = |c|(a \wedge b)$*

Proposition. *(*) Soient $(a, b) \in \mathbb{Z}^2$ et d un diviseur commun à a et b alors $\frac{a}{d} \wedge \frac{b}{d} = \frac{a \wedge b}{d}$*
En particulier $\frac{a}{a \wedge b}$ et $\frac{b}{a \wedge b}$ sont premiers entre eux.

2. PPCM

Définition. *Soient a et b deux entiers naturels non nuls. On appelle Plus Petit Multiple Commun de a et de b et noté $ppcm(a, b)$ ou $a \vee b$, le plus petit des multiples strictement positifs communs à a et b.*

Remarque : Cette définition a un sens car l'ensemble des multiples strictement positifs communs à a et b est une partie de $\mathbb{N}$ non vide (elle contient ab car $a \neq 0$ et $b \neq 0$). Elle possède donc un plus petit élément.

Définition. *Si a et b sont deux entiers relatifs non nuls, alors on appelle PPCM de a et b celui de $|a|$ et $|b|$*

Théorème. *(*) Soient $(a, b) \in (\mathbb{Z}^*)^2$. Leur PPCM vérifie les propriétés suivantes :*
- *$ppcm(a, b)$ est un multiple commun à a et b*
- *tout multiple commun à a et b est un multiple de $ppcm(a, b)$*

Remarque : Soient $(a, b) \in (\mathbb{Z}^*)^2$ et $c \in \mathbb{N}$ alors $c = a \vee b$ si et seulement si

$$a/c, \quad b/c \quad \text{et} \quad \forall m \in \mathbb{Z},\ (a/m \text{ et } b/m) \Rightarrow c/m$$

On dit que le PPCM de a et b est le plus petit multiple strictement positif commun de a et b au sens de la divisibilité.

Proposition. *Soient $(a, b) \in \mathbb{Z}^2$ et $c \in \mathbb{N}$ alors $c = a \vee b$ si et seulement si*
- *c est un multiple commun à a et b*
- *tout multiple commun à a et b est un multiple c*

Proposition. *(*) Soient $(a, b, c) \in \mathbb{Z}^3$ alors $(ac) \vee (bc) = |c|(a \vee b)$*

Proposition. *(*) Soient $(a, b) \in \mathbb{Z}^2$ et d un diviseur commun à a et b alors $\frac{a}{d} \vee \frac{b}{d} = \frac{a \vee b}{d}$*

Proposition. *(*) Soient $(a, b) \in \mathbb{Z}^2$ alors $(a \wedge b)(a \vee b) = |ab|$*

III. Entiers premiers entre eux

Proposition. *(Théorème de Bezout) (*)*
Soit $(a,b) \in \mathbb{Z}^2$ alors a et b sont premiers entre eux si et seulement si $\exists (u,v) \in \mathbb{Z}^2$: $au+bv=1$.

Corollaire. *(*) Soit $(a_1,...,a_r,b) \in \mathbb{Z}^{r+1}$ tel que $\forall k \in [\![1,r]\!]$, $a_k \wedge b = 1$. Alors $\left(\prod_{k=1}^{r} a_i\right) \wedge b = 1$.*

Remarque : La réciproque est évidemment vraie.

Proposition. *(Lemme de Gauss) (*) Soit $(a,b,c) \in \mathbb{Z}^3$ alors $(a/bc$ et $a \wedge b = 1) \Rightarrow a/c$*

Proposition. *(Forme irréductible d'un rationnel) Soit $r \in \mathbb{Q}$ alors*

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

On dit alors que p/q est la forme irréductible de r.

Corollaire. *(*) Soit $(a_1,...,a_r,b) \in \mathbb{Z}^{r+1}$ tel que*

$$\forall k \in [\![1,r]\!], \ a_k/b \ \ et \ \ \forall (k,k') \in [\![1,r]\!]^2, \ k \neq k' \Rightarrow a_k \wedge a_{k'} = 1$$

alors $\prod_{k=1}^{r} a_k/b$.

Corollaire. *Si $n_1 \wedge n_2 = 1$, alors $\forall (\alpha_1, \alpha_2) \in \mathbb{N}^2$, $n_1^{\alpha_1} \wedge n_2^{\alpha_2} = 1$.*

IV. Nombres premiers

Définition. *Un entier naturel p est dit premier s'il a exactement deux diviseurs dans $\mathbb{N}$, 1 et lui-même.*

Remarque : 1 n'est pas premier.

Proposition. *Soit $(n,p) \in \mathbb{N}^2$ tel que p soit premier alors soit p/n soit $p \wedge n = 1$.*

Proposition. *(*) Tout entier $n \geq 2$ possède un diviseur premier.*

Théorème. *(*) Il existe une infinité de nombres premiers.*

Théorème. *(*) Tout entier naturel non nul se décompose de façon unique, à l'ordre près, en produit de nombres premiers.*

Remarque : Par convention 1 est le produit de zéro nombre premier
Remarque : Par convention, un nombre premier est le produit d'un nombre premier.
Remarque : Le théorème se traduit ainsi : pour tout entier naturel $n > 1$, il existe des nombres premiers $p_1 < ... < p_r$ et des entiers naturels non nuls α_1,..., α_r tels que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et s'il existe des nombres premiers $q_1 < ... < q_s$ et des entiers naturels non nuls β_1,..., β_s tels que $n = \prod_{i=1}^{s} q_i^{\beta_i}$ alors $r = s$ et pour tout $i \in [\![1,r]\!]$, $q_i = p_i$ et $\alpha_i = \beta_i$.

Définition. *Soit $n \in \mathbb{N}^*$ et p un nombre premier. On appelle valuation p-adique de n, l'entier*

$$v_p(n) = \max\{k \in \mathbb{N}, \ p^k/n\}$$

Proposition. *Pour tout $n \in \mathbb{N}^*$, on a $n = \prod_{p \ premier} p^{v_p(n)}$.*

Proposition. *(*) Soit $(a,b) \in \mathbb{N}^2$ alors*

$$v_p(ab) = v_p(a) + v_p(b) \quad et \quad v_p(a+b) \geq \min(v_p(a), v_p(b))$$

Si $v_p(a) \neq v_p(b)$ alors l'inégalité est une égalité.

Proposition. *Soit $(a,b) \in \mathbb{N}^2$ alors a/b ssi, pour tout nombre premier p, on a $v_p(a) \leq v_p(b)$.*

Proposition. *Soit $(a,b) \in \mathbb{N}^2$ tels qu'il existe des nombres premiers $p_1 < ... < p_r$ et des entiers naturels α_1,..., α_r et β_1,..., β_s tels que $a = \prod_{i=1}^{r} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{r} p_i^{\beta_i}$ alors :*

$$a \wedge b = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)} \quad et \quad a \vee b = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$$

V. Congruences

Définition. *Soit $n \in \mathbb{N}$. On définit sur $\mathbb{Z}$ la relation de congruence modulo n par*

$$\forall (a,b) \in \mathbb{Z}^2, \quad a \equiv b[n] \Leftrightarrow b - a \in n\mathbb{Z}$$

Proposition. *Soit $n \in \mathbb{N}$ alors la relation de congruence modulo n est une relation d'équivalence possédant n classes d'équivalence.*

Proposition. *Soit $n \in \mathbb{N}$ et $(a,a',b,b') \in \mathbb{Z}^4$ alors*

$$\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \Rightarrow \begin{cases} a+b \equiv a'+b'[n] \\ ab \equiv a'b'[n] \end{cases}$$

Théorème. *(*) Théorème chinois : Soit $(m,n) \in (\mathbb{N}^*)^2$ premiers entre eux.*
Pour tout $(a,b) \in \mathbb{Z}^2$, il existe $c \in \mathbb{Z}$ tel que $c \equiv a[n]$ et $c \equiv b[m]$.
Cet entier c n'est pas unique. Plus précisément, $\{k \in \mathbb{Z} : k \equiv a[n] \text{ et } k \equiv b[m]\} = c + nm\mathbb{Z}$

Proposition. *(*) Soit $n \in \mathbb{N}$ tel que $n > 2$ alors*

$$n \text{ est premier} \Leftrightarrow \forall k \in [\![1, n-1]\!], \binom{n}{k} \equiv 0[n]$$

Théorème. *(*) (Petit théorème de Fermat) Soit p un nombre premier alors*

$$\forall n \in \mathbb{N}, \quad n^p \equiv n[p]$$

ce qui est équivalent à

$$\forall n \in \mathbb{N}, \quad n \wedge p = 1 \Rightarrow n^{p-1} \equiv 1[p]$$