Chapitre 14

Arithmétique dans $\mathbb{Z}$

Dans tout ce chapitre, les lettres minuscules désignent des entiers relatifs.

1 Divisibilité dans $\mathbb{Z}$

1.1 Divisibilité

Définition 1.1 (Divisibilité)

Soient $a, b \in \mathbb{Z}$. L'entier a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. On note alors $a|b$, et a est alors un diviseur de b et b un multiple de a.

Définition 1.2

Soit $a \in \mathbb{Z}$. On note $\mathcal{D}(a)$ l'ensemble des diviseurs dans $\mathbb{N}$ de a et $a\mathbb{Z} = \{na,\ n \in \mathbb{Z}\}$ l'ensemble de ses multiples.

Proposition 1.3

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

$$a|b \iff -a|b \iff a|-b \iff -a|-b.$$

Remarque.

On peut donc se contenter d'étudier la divisibilité dans $\mathbb{N}$ plutôt que dans $\mathbb{Z}$.

Proposition 1.4

Soient $a, b \in \mathbb{Z}$. Alors $\big(a|b \text{ et } b|a\big) \iff |a| = |b|$.

Proposition 1.5

La relation "divise" est une relation d'ordre partiel sur $\mathbb{N}$, *i.e.* si $a, b, c \in \mathbb{N}$, on a :

1. $a|a$.
2. $a|b$ et $b|a \implies a = b$.

3. $a|b$ et $b|c \Longrightarrow a|c$.

Remarques.

1. La divisibilité dans $\mathbb{Z}$ n'est pas une relation d'ordre, puisque $x|y$ et $y|x$ n'implique pas $x = y$, mais seulement $|x| = |y|$.
2. Soient $a, b \in \mathbb{N}$. Alors a est plus petit que b pour la relation "divise" si $a|b$. On peut remarquer que 0 est alors le plus grand élément de $\mathbb{N}$ (tout entier divise 0), et 1 le plus petit (1 divise tous les entiers).

Proposition 1.6

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

1. $c|a$ et $c|b \Longrightarrow \forall\ u, v \in \mathbb{Z},\ c|au + bv$.
2. Si $c \neq 0$, alors $ac|bc \iff a|b$.

Remarque.

Comparez aussi avec le paragraphe sur les congruences ci-dessous.

1.2 Congruences dans $\mathbb{Z}$

Définition 1.7 (Congruences)

Soient $a, b, \alpha \in \mathbb{Z}$. Les entiers a et b sont congrus modulo α s'il existe $k \in \mathbb{Z}$ tel que $a - b = k\alpha$. On note alors $a \equiv b \mod \alpha$.

Proposition 1.8

Soient $a, b, d \in \mathbb{Z}$. Alors d divise $a - b$ si et seulement si $a \equiv b \mod d$.

Proposition 1.9

Soient $a, b, a', b', n, \alpha \in \mathbb{Z}$ tels que $a \equiv b \mod \alpha$ et $a' \equiv b' \mod \alpha$. Alors

1. $a + a' \equiv b + b' \mod \alpha$.
2. $na \equiv nb \mod \alpha$.
3. $aa' \equiv bb' \mod \alpha$.

Remarques.

1. On remarque que cette proposition est une réécriture avec des congruences de la proposition 1.6.
2. On notera que le point 3 de cette proposition n'est pas vraie pour les congruences avec les réels. Mais en général, les congruences entre réels et entre entiers ne sont pas utilisés de la même façon.
3. On ne peut pas diviser les congruences par un entier ! Par exemple, $6 \equiv 0 \mod 6$, mais $3 \not\equiv 0 \mod 6$.

1.3 Division euclidienne

Théorème 1.10 (Division euclidienne)

Soient $a, b \in \mathbb{Z} \times \mathbb{N}^*$. il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

L'entier q est le quotient et r est le reste de la division euclidienne de a par b.

Proposition 1.11

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul.

2 PGCD

2.1 Définition et caractérisation

Définition 2.1 (PGCD)

Soient $a, b \in \mathbb{N}$ tels que $a \neq 0$ ou $b \neq 0$. Le pgcd de a et b, noté $a \wedge b$, est le plus grand diviseur commun dans $\mathbb{N}$ à a et b.

Remarques.

1. Par définition, un pgcd est toujours strictement positif.
2. Par définition, le pgcd de a et b divise a et b.
3. On a $a \wedge 0 = a$.

Proposition 2.2

Soient $a, b \in \mathbb{N}$ avec $a \neq 0$. Alors $a|b \iff a \wedge b = a$.

Proposition 2.3

Soient $a, b, q, r \in \mathbb{N}$ tels que $a = bq + r$. Alors

1. Les diviseurs communs à a et b sont les diviseurs communs à b et r, *i.e.* $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(r) \cap \mathcal{D}(b)$.
2. Si $a \neq 0$ ou $b \neq 0$, on a $a \wedge b = r \wedge b$.

Cas particulier important : q est le quotient et r le reste de la division de a par $b \neq 0$.

Remarque.

On retiendra que "le pgcd ne change pas lorsqu'on retranche à un des entiers un multiple de l'autre".

Théorème 2.4 (Caractérisation du PGCD)

Soient $a, b, d \in \mathbb{N}$ avec $a \neq 0$ ou $b \neq 0$, et $d \neq 0$. Les affirmations suivantes sont équivalentes :

1. $d = a \wedge b$.

2. $\mathcal{D}(d) = \mathcal{D}(a) \cap \mathcal{D}(b)$, *i.e.* les diviseurs communs dans $\mathbb{N}$ à a et b sont les diviseurs de d, ou encore : $\forall\, n \in \mathbb{N},\ \big(n|a \text{ et } n|b\big) \iff n|d$.

3. $d|a$, $d|b$ et : $\forall\, n \in \mathbb{N}$ tel que $n|a$ et $n|b$, on a $n|d$, *i.e.* d est le plus grand diviseur commun dans $\mathbb{N}$ à a et b pour la relation d'ordre "divise".

Remarques.

1. Il faut savoir reconnaître les situations !
2. Cette caractérisation permet de définir $0 \wedge 0$: on a $\mathcal{D}(0) = \mathcal{D}(0) \cap \mathcal{D}(0)$ donc $0 \wedge 0 = 0$. Cela permet d'éviter de toujours devoir supposer qu'un des entiers est non nul.

Méthode 2.5

Pour déterminer le pgcd de deux entiers a et b, il suffit de déterminer un entier positif d qui divise a et b et tel que, si $n|a$ et $n|b$, alors $n|d$.

2.2 Algorithme d'Euclide

Théorème 2.6 (Algorithme d'Euclide)

Soient $a, b \in \mathbb{N}^*$. On construit par récurrence (tant que c'est possible) une suite d'entiers naturels par :

1. $r_{-1} = a$ et $r_0 = b$.
2. Pour $n \geqslant 0$, si $r_n \neq 0$, on définit r_{n+1} comme le reste de la division euclidienne de r_{n-1} par r_n, sinon r_{n+1} n'est pas défini.

Alors :

1. Il existe un entier $p \geqslant 0$ tel que pour tout $n \leqslant p$, r_n est bien défini et non nul, et $r_{p+1} = 0$ (*i.e.* r_p divise r_{p-1}).
2. r_p est le pgcd de a et b, *i.e.* le dernier reste non nul est le pgcd de a et de b.

2.3 Extension aux entiers relatifs et relation de Bézout

Définition 2.7

Soient $a, b \in \mathbb{Z}$. On définit leur pgcd par $a \wedge b = |a| \wedge |b|$.

Proposition 2.8

Soient $a, b, p \in \mathbb{Z}$. Alors $(pa) \wedge (pb) = |p|\,(a \wedge b)$.

Proposition 2.9 (Relation de Bézout)

Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que $a \wedge b = au + bv$.

Méthode 2.10

Voici deux façons de déterminer des coefficients de Bézout. Avec les notations de la proposition 2.6, on note q_n le quotient de la division euclidienne de r_{n-2} par r_{n-1} ($1 \leqslant n \leqslant p$), et on a

$$r_{n-2} = q_n r_{n-1} + r_n.$$

1. On utilise l'algorithme donné dans la démonstration. On part de la relation $a \wedge b = r_p = r_{p-2} - q_p r_{p-1}$. On remplace alors r_{p-1} par $r_{p-1} = r_{p-3} - q_{p-1} r_{p-2}$, donc

$$a \wedge b = r_{p-2} - q_p(r_{p-3} - q_{p-1} r_{p-2}) = (1 + q_p q_{p-1}) r_{p-2} - q_p r_{p-3}.$$

Puis on remplace r_{p-2} par $r_{p-2} = r_{p-4} - q_{p-2} r_{p-3}$, et ainsi de suite. Notez qu'on ne remplace qu'un reste à la fois. Lorsqu'il ne reste que r_{-1} et r_0, on a une relation de Bézout.

2. Voici un algorithme plus efficace pour une programmation. On détermine par récurrence des entiers $u_n, v_n \in \mathbb{Z}$ pour $-1 \leqslant n \leqslant p$ tels que

$$u_n a + v_n b = r_n.$$

Pour $n = p$, on a $r_p = a \wedge b$, ce qui donne des coefficients de Bézout.

On pose $u_{-1} = 1$ et $v_{-1} = 0$ (car $r_{-1} = a$) et $u_0 = 0$, $v_0 = 1$ (car $r_0 = b$). Si pour $0 \leqslant n < p$ $u_{n-1}, v_{n-1}, u_n, v_n$ sont construits, on a

$$r_{n+1} = r_{n-1} - q_{n+1} r_n = (u_{n-1} - q_{n+1} u_n) a + (v_{n-1} - q_{n+1} u_n) b,$$

et on pose

$$u_{n+1} = u_{n-1} - q_{n+1} u_n \quad \text{et} \quad v_{n+1} = v_{n-1} - q_{n+1} u_n.$$

Cet algorithme a l'avantage de prendre moins de place mémoire.

Pour les deux algorithmes, il est intéressant d'obtenir les coefficients de Bézout formellement en fonction des différents q_n, r_n (ou u_n et v_n le cas échéant), et de faire les calculs explicites une fois pour toute à la fin. En effet, les coefficients sont, en fonction de q_n, r_n, (ou u_n et v_n), toujours les mêmes, donc on "s'habitue" au calcul. De plus, certains produits se répètent, ce que l'on ne remarque pas en effectuant les calculs au fur et à mesure. Enfin, quand on remplace au fur et à mesure, on ne reconnaît plus les r_n à remplacer, et on est vite perdu !

3 Entiers premiers entre eux et théorème de Bézout

3.1 Entiers premiers entre eux

Définition 3.1

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

Proposition 3.2

Soient $a, b \in \mathbb{Z}$. Il existe $a_1, b_1 \in \mathbb{Z}$ premiers entre eux tels que

$$a = (a \wedge b) a_1, \qquad b = (a \wedge b) b_1.$$

3.2 Théorème de Bézout

Théorème 3.3 (Théorème de Bézout)

Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que

$$au + bv = 1.$$

Remarque.

Attention, s'il existe u et v tel que

$$au + bv = d,$$

on n'a pas nécessairement $d = \pm a \wedge b$, puisque par exemple si

$$au' + bv' = a \wedge b \quad \text{alors} \quad a(cu') + b(cv') = c(a \wedge b)$$

pour tout entier c. Par exemple, $4 \times 3 + (-2) \times 5 = 2$, mais 2 n'est pas le pgcd de 3 et 3.

4 PPCM

Définition 4.1 (PPCM)

Soient $a, b \in \mathbb{N}^*$. Le ppcm de a et b, noté $a \vee b$, est le plus petit multiple stictement positif commun à a et b.

Remarques.

1. Si $a = 0$ ou $b = 0$, il n'y a pas de plus petit multiple > 0, puisque le seul multiple commun est 0. On peut le définir comme ppcm.
2. Si $a < 0$ ou $b < 0$, on définit $a \vee b = |a| \vee |b|$.

Théorème 4.2 (Caractérisation du ppcm)

Soient $a, b, m \in \mathbb{N}^*$. Les affirmations suivantes sont équivalentes.

1. $m = a \vee b$.
2. $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, *ie* l'ensemble des multiples communs à a et b est l'ensemble des multiples de m, ou encore : $\forall\, n \in \mathbb{N},\ m \mid n \iff a \mid n$ et $b \mid n$
3. m est le plus petit multiple strictement positif commun à a et b pour la relation "divise", ou encore : $a|m$, $b|m$, et $\forall\, n \in \mathbb{N},\ a \mid n$ et $b \mid n \Longrightarrow m \mid n$.

Remarque.

Le thorème reste vrai même si $a = 0$ ou $b = 0$.

Méthode 4.3

Pour déterminer le ppcm de a et b, on exhibe un multiple m commun à a et b tel que, pour tout $n \in \mathbb{N}$, $\big(a|n \text{ et } b|n\big) \Longrightarrow m|n$.

Proposition 4.4

Soient $a, b, p \in \mathbb{N}$. Alors $(pa) \vee (pb) = p\,(a \vee b)$.

5 Lemme de Gauss

5.1 Lemme de Gauss

Théorème 5.1 (Lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}$. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Corollaire 5.2

Soient a et b deux entiers premiers entre eux. Alors

$$a \vee b = |ab|.$$

Proposition 5.3

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

Théorème 5.4 (Forme irréductible d'un rationnel)

Tout nombre rationnel non nul s'écrit de manière unique

$$\frac{p}{q},$$

avec $p, q \in \mathbb{Z}$, $q > 0$ et $p \wedge q = 1$.

5.2 Entiers premiers avec un produit

Proposition 5.5

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

1. a est premier avec bc si et seulement si a est premier avec b et c.
2. Si a et b divisent c et si a et b sont premiers entre eux, alors ab divise c.

Proposition 5.6

1. Un entier est premier avec un produit si et seulement s'il est premier avec chacun de ses facteurs.
2. Si des entiers deux à deux premiers entre eux divisent un entier p, alors leur produit divise p.

6 PGCD d'un nombre fini d'entiers

Les démonstrations de ce paragraphe ne sont pas exigibles. Je ne les mets pas. Il s'agit en fait simplement de se poser la question "à quelle condition divise-t-on plusieurs entiers ?".

6.1 Cas de trois entiers

Proposition 6.1

Soient $a, b, c \in \mathbb{N}^*$. Alors

$$\mathcal{D}(a) \cap \mathcal{D}(b) \cap \mathcal{D}(c) = \mathcal{D}(a \wedge b) \cap \mathcal{D}(c) = \mathcal{D}(a) \cap \mathcal{D}(b \wedge c) = \mathcal{D}(a \wedge c) \cap \mathcal{D}(b).$$

Définition 6.2 (PGCD de trois entiers)

Soient $a, b, c \in \mathbb{N}^*$. Le pgcd de a, b et c est le plus grand diviseur commun à a, b et c. On le note $a \wedge b \wedge c$.

Proposition 6.3

Soient $a, b, c \in \mathbb{N}^*$. Alors

$$a \wedge b \wedge c = a \wedge (b \wedge c) = (a \wedge b) \wedge c.$$

Proposition 6.4

Soient $a, b, c \in \mathbb{N}^*$. Un entier $n \in \mathbb{N}$ divise a, b et c si et seulement s'il divise $a \wedge b \wedge c$.

6.2 Généralisation

Voici les résultats pour un nombre quelconque d'entiers.

Définition 6.5 (PGCD de n entiers)

Soient $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in (\mathbb{N}^*)^n$. Le pgcd des a_k est le plus grand diviseur commun aux a_k. On le note $a_1 \wedge \cdots \wedge a_n$.

Proposition 6.6

Soient $n \in \mathbb{N}$, $n \geqslant 2$, et $(a_1, \dots, a_n) \in (\mathbb{N}^*)^n$. Alors

$$a_1 \wedge \cdots \wedge a_n = (a_1 \wedge \cdots \wedge a_{n-1}) \wedge a_n = a_1 \wedge (a_2 \wedge \cdots \wedge a_n).$$

Remarques.

1. Comme pour deux entiers, on peut généraliser aux entiers relatifs.
2. De même, le pgcd de n entier est caractérisé comme étant le seul entier dont l'ensemble des diviseurs est l'ensemble des diviseurs communs aux n entiers.

Proposition 6.7 (Relation de Bézout)

Soient $n \in \mathbb{N}$, $n \geqslant 2$, et $(a_1, \dots, a_n) \in \mathbb{Z}^n$. Il existe $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que

$$u_1 a_1 + \cdots + u_n a_n = a_1 \wedge \cdots \wedge a_n.$$

Définition 6.8 (Entiers premiers entre eux dans leur ensemble)

Soient $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in (\mathbb{N}^*)^n$. Les entiers a_k sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_n = 1$.

Définition 6.9 (Entiers premiers entre eux deux à deux)

Soient $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in (\mathbb{N}^*)^n$. Les entiers a_k sont premiers entre eux deux à deux si

$$\forall\, (i,j) \in [\![1,n]\!],\ i \neq j \Longrightarrow a_i \wedge a_j = 1.$$

Remarque.

Attention à ne pas confondre ces deux notions. Par exemple, 6,10 et 15 sont premiers entre eux dans leur ensemble, mais pas deux à deux (et pris deux à deux, ils ne sont pas premiers entre eux !).

Proposition 6.10

Soient $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in (\mathbb{N}^*)^n$ premiers entre eux deux à deux. Alors ils sont premiers entre eux dans leur ensemble.

7 Nombres premiers

Dans ce paragraphe, tous les entiers sont des entiers naturels sauf mention explicite du contraire.

7.1 Définition

Définition 7.1 (Nombres premiers)

Un entier naturel p est *premier* s'il admet exactement deux diviseurs, 1 et lui-même. Autrement dit, pour $p > 1$, si $p = ab$, alors $a = 1$ ou $b = 1$.

Remarque.

1 n'est pas un nombre premier.

Proposition 7.2

Un nombre premier est premier avec tout entier qu'il ne divise pas.

Corollaire 7.3

Un nombre premier divise un produit si et seulement s'il divise un des facteurs.

7.2 Décomposition en produit de nombres premiers

Théorème 7.4 (Existence d'un diviseur premier)

Tout entier plus grand que 2 admet un diviseur premier.

Proposition 7.5

L'ensemble des nombres premiers est infini.

Théorème 7.6

Tout entier naturel > 1 se décompose de manière unique en produit de nombres premiers, *i.e.* pour tout $a > 1$, il existe $n \in \mathbb{N}^*$, des nombres premiers $p_1, \dots, p_n$ distincts deux à deux, et des entiers > 0 $r_1, \dots, r_n$ tels que

$$a = \prod_{k=1}^{n} p_k^{r_k},$$

et si

$$a = \prod_{k=1}^{m} q_k^{s_k},$$

avec $q_1, \dots, q_m$ des nombres premiers deux à deux distincts, alors $n = m$ et quitte à réordonner on a

$$p_k = q_k,\ r_k = s_k \quad \text{pour tous} \quad k = 1, \dots, n.$$

On dit qu'il y a unicité de l'écriture à l'ordre des facteurs près.

Remarque.

Il est parfois nécessaire de considérer des puissances nulles, *i.e.* des $r_k = 0$, *cf.* plus bas les valuations p-adiques. Lorsque $a = \prod_{k=1}^{n} p_k^{r_k}$ est la décomposition en facteurs premiers (donc les $r_k > 0$), on peut aussi dire que $a = \prod_{k=1}^{m} p_k^{r_k}$ avec un $m > n$, et $r_k = 0$ si $k > n$. Par exemple, on a $980 = 2^2 \times 5 \times 7^2 = 2^2 \times 3^0 \times 5 \times 7^2 \times 11^0$.

7.3 Valuation p-adique

Dans ce paragraphe, on note $\mathcal{P}$ l'ensemble des nombres premiers.

Définition 7.7

Soit $n \in \mathbb{N}^*$ et $p \in \mathcal{P}$. La valuation p-adique de n est le plus grand entier k tel que p^k divise n. On la note $v_p(n)$.

Proposition 7.8

Soient $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$. Alors

$$v_p(n) = k \iff \exists\, q \in \mathbb{N}^*,\ p \wedge q = 1 \text{ et } n = p^k q.$$

Proposition 7.9

Soient $n, s \in \mathbb{N}^*$ tel que $a = \prod_{k=1}^{s} p_k^{r_k}$, où les p_k sont des nombres premiers deux à deux distincts, et $r_k \in \mathbb{N}^*$. Alors

1. $\forall\, k \in [\![1, s]\!],\ v_{p_k}(n) = r_k$.
2. $\forall\, p \in \mathcal{P} \setminus \{p_1, \ldots, p_s\},\ v_p(n) = 0$.

Corollaire 7.10 (Décomposition en facteurs premiers)

Soit $a \in \mathbb{N}$. Alors $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$.

Proposition 7.11 (Valuation p-adique d'un produit)

Soient $p \in \mathcal{P}$, et $a, b \in \mathbb{N}^*$. Alors $v_p(ab) = v_p(a) + v_p(b)$.

Proposition 7.12

Soient $a, b \in \mathbb{N}^*$. Alors

1. $a|b \iff \forall\, p \in \mathcal{P},\ v_p(a) \leqslant v_p(b)$.
2. Pour tout $p \in \mathcal{P}$, on a $v_p(a \wedge b) = \min(v_p(a), v_p(b))$, $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Corollaire 7.13

Soient a et b deux entiers > 1 tels que $a = \prod_{k=1}^{n} p_k^{r_k}$ et $b = \prod_{k=1}^{n} p_k^{s_k}$, où les p_k sont des nombres premiers distincts deux à deux et $r_k, s_k \in \mathbb{N}$. Alors

$$a \wedge b = \prod_{k=1}^{n} p_k^{\min(r_k, s_k)} \quad \text{et} \quad a \vee b = \prod_{k=1}^{n} p_k^{\max(r_k, s_k)}.$$