

Chapitre 9

ARITHMÉTIQUE ÉLÉMENTAIRE

Mohamed TARQI

Table des matières

1	Divisibilité dans l'anneau $\mathbb{Z}$	1
1.1	Division euclidienne dans $\mathbb{Z}$	1
1.2	Congruence modulo n	3
2	PGCD, PPCM	4
2.1	Plus grand commun diviseur d'éléments de $\mathbb{Z}$	4
2.1.1	Algorithme d'Euclide pour la recherche du $a \wedge b$	6
2.1.2	Plus grand commun diviseur d'une famille finie d'éléments de $\mathbb{Z}$	7
2.2	Plus petit commun multiple de deux ou plusieurs éléments de $\mathbb{Z}$	7
3	Décomposition d'un entier relatif en facteurs premiers	8
4	Numération	9
4.1	Bases de numération dans $\mathbb{N}$	9
4.2	Comparaison de deux nombres écrits en base a	10
4.3	Somme et produit de deux nombres écrits en base a	10
4.3.1	Somme de deux nombres écrits en base a	10
4.3.2	Produit de deux nombres écrits en base a	10
4.4	Application : Algorithme d'exponentiation rapide	11

•••••

1 Divisibilité dans l'anneau $\mathbb{Z}$

1.1 Division euclidienne dans $\mathbb{Z}$

Théorème et définition 1.1 Étant donné un couple d'entiers relatifs a et b ($b > 0$), il existe un couple unique q et r tels que :

$$a = bq + r \text{ et } 0 \leq r < b$$

Cette application de $\mathbb{Z} \times \mathbb{N}^*$ dans $\mathbb{Z} \times \mathbb{N}$ est appelée la division euclidienne¹, q est le quotient et r le reste dans cette division euclidienne.

Démonstration : • Soient a et b des entiers relatifs ($b > 0$), si $a \geq 0$, il existe q unique tel que :

$$qb \leq a < (q+1)b$$

C'est le plus grand élément de la partie de $\mathbb{N}$ décrite par l'entier naturel m tel que $mb \leq a$.

• Si $a < 0$, $-a > 0$, il existe donc q' positif tel que :

$$q'b \leq -a < (q'+1)b$$

1. Euclide (3^{ème} siècle avant J.-C.) est un mathématicien grec, auteur du plus célèbre ouvrage de l'histoire des mathématiques, les Éléments, qui reste longtemps un modèle de raisonnement mathématique.

si $q'b = -a$ posons $q = -q'$ on a $qb = a$

si $qb' < a$ posons $q = -(q' + 1)$ on a dans ce cas $-(q + 1)b < -a < -qb$ ou encore $qb < a < (q + 1)b$

d'où, dans tous les cas :

$$qb \leq a < (q + 1)b$$

Il en résulte que, si on pose $r = a - bq$, $0 \leq r < b$ et r est évidemment unique. $\square$

Définition 1.1 Soient a et b deux éléments de $\mathbb{Z}$. On dit que b divise a ou a est un multiple de b , et on note $b|a$, si, et seulement si, il existe un entier relatif q tel que $a = bq$. On note, pour tout entier relatif n , $\mathcal{D}(n)$ l'ensemble des diviseurs de n .

Remarques :

1. Dire que b divise a ($b > 0$) c'est-à-dire le reste de la division euclidienne de a par b est 0.
2. 0 est un multiple de tout entier b (car $0 = 0b$), mais ne divise que lui même ($a = 0q \implies a = 0$).
3. Pour tout entier relatif n , $\mathcal{D}(n) = \mathcal{D}(-n)$.
4. Pour tous a, b dans $\mathbb{Z}$, on a :

$$a|b \iff b \in a\mathbb{Z} \iff a \in \mathcal{D}(b)$$

5. La relation $a|b$ est une relation binaire sur $\mathbb{Z}$, qui est reflexive et transitive, contrairement à sa restriction à $\mathbb{N}$, elle n'est pas antisymétrique. En effet si $a|b$ et $b|a$ alors il existe c et c' de $\mathbb{Z}$ tels que $a = bc$ et $b = ac'$, donc $a = acc'$ ou encore $a(cc' - 1) = 0$, d'où :

$$\begin{cases} a|b \\ b|a \end{cases} \iff |a| = |b|$$

6. Pour tous entiers a, b , on a : $a\mathbb{Z} \subset b\mathbb{Z} \iff b|a \iff \mathcal{D}(b) \subset \mathcal{D}(a)$. On en déduit $a\mathbb{Z} = b\mathbb{Z} \iff |b| = |a| \iff \mathcal{D}(b) = \mathcal{D}(a)$.

Proposition 1.1 Dans la division euclidienne de a par b , a, b et r ont les mêmes diviseurs communs.

Démonstration : Soit d un diviseur commun strictement positif de a et b ($b > 0$) et r le reste de la division de a par b . Il existe donc a' et b' des entiers rationnels les que $a = a'd$ et $b = b'd$.

De la division euclidienne de a par b et de a' par b' ($b' > 0$) on déduit :

$$a' = b'q' + r' \quad \text{et} \quad 0 \leq r' < b'$$

donc

$$a'd = b'dq' + r'd \quad \text{et} \quad 0 \leq r'd < b'd = b$$

d'où $r = a'd - b'q'd = (a' - b'q')d = rd$, donc d divise aussi r . $\square$

Définition 1.2 Deux éléments a et b sont premiers entre eux s'ils n'ont pour diviseurs communs que 1 et -1 .

Remarquons que tout élément divise 0 ($0a = 0$), donc deux éléments sont premiers sont non nuls.

Définition 1.3 Les éléments $a_1, a_2, \dots, a_n$ sont premiers entre eux dans leur ensemble s'ils n'ont pour diviseurs communs que 1 et -1 .

Remarque : Ne pas confondre une famille finie d'éléments premiers entre eux dans leur ensemble et une famille d'éléments premiers deux deux : cette deuxième famille est un cas particulier de la première. Par exemple 6, 10, 15 sont premiers entre eux dans leur ensemble mais 2 divise 6 et 10, 3 divise 6 et 15, et 5 divise 10 et 15.

Définition 1.4 Un entiers relatif p est dit premier si $\mathcal{D}(p) = \{-1, 1, p, -p\}$.

1.2 Congruence modulo n

Définition 1.5 Soient a et b deux entiers relatifs. On dit que a est congrue à b modulo n et on écrit $a \equiv b[n]$ si, et seulement si, n divise $a - b$.

Autrement dit :

$$a \equiv b[n] \iff n|(a - b) \iff \exists k \in \mathbb{Z} : a - b = kn$$

Proposition 1.2 La relation " $\equiv$ ", congruence modulo n , est une relation d'équivalence dans $\mathbb{Z}$. On note $\bar{x}$ la classe de x pour cette relation.

Démonstration :

1. Pour tout a de $\mathbb{Z}$, on a : $a - a = 0.n$, donc $a \equiv a[n]$.
2. Si $a \equiv b[n]$, alors il existe $k \in \mathbb{Z}$ tel que $a - b = kn$, donc $b - a = (-k)n$, c'est-à-dire $b \equiv a[n]$.
3. Soient a, b et c dans $\mathbb{Z}$ tel que $a \equiv b[n]$ et $b \equiv c[n]$, alors il existe deux entiers relatifs k et k' tels que $a - b = kn$ et $b - c = k'n$, en suite

$$a - c = (a - b) + (b - c) = (k + k')n$$

c'est-à-dire $a \equiv c[n]$.

□

Proposition 1.3 Si $a \equiv b[n]$, alors a et b ont le même reste dans la division euclidienne par n .

Démonstration : Soient a et b deux entiers relatifs tels que :

$$a = nq_1 + r_1 \text{ et } b = nq_2 + r_2$$

avec

$$0 \leq r_1 < n \text{ et } 0 \leq r_2 < n$$

Si a et b ont le même reste dans la division euclidienne par n , c'est-à-dire $r_1 = r_2$ alors $a - b = (q_1 - q_2)n$, donc $a \equiv b[n]$.

Réciproquement, si $a \equiv b[n]$, alors il existe $k \in \mathbb{Z}$ tel que $a - b = kn$, donc $r_1 - r_2 = (k - q_1 - q_2)n$, c'est-à-dire n divise $r_1 - r_2$, mais $0 \leq r_1 < n$ et $0 \leq r_2 < n$ impliquent $|r_1 - r_2| < n$, d'où $r_1 - r_2 = 0$. □

L'ensemble $\mathbb{Z}/n\mathbb{Z}$: Pour tout $x \in \mathbb{Z}$, il existe q et r uniques tels que $x = nq + r$ et $0 \leq r < n$. On a donc $\bar{x} = \bar{r}$ et par conséquent

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{x \in \mathbb{Z}} \{\bar{x}\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

Proposition 1.4 Soient x, y, z et t des entiers relatifs. Si $x \equiv y[n]$ et $z \equiv t[n]$ alors $x + y \equiv z + t[n]$ et $xz \equiv yt[n]$. On dit que la congruence modulo n est compatible avec l'addition et la multiplication.

Démonstration : Soient x, y, z et t des entiers relatifs tels que $x \equiv y[n]$ et $z \equiv t[n]$ alors il existe k et k' des entiers relatifs tels que

$$x - y = kn \text{ et } z - t = k'n$$

d'où $(x + z) - (y + t) = (k + k')n$, c'est-à-dire $x + y \equiv z + t[n]$.

D'autre part :

$$xz - yt = xz - yz + yz - yt = z(x - y) + y(z - t) = (zk' + yk')n$$

donc $xz \equiv yt[n]$.

□

Corollaire 1.1 Pour tous a et b de $\mathbb{Z}$ et $n \in \mathbb{N}^*$, si $a \equiv b[n]$ alors $\forall m \in \mathbb{N}^*$, $a^m \equiv b^m[n]$.

Exemple : $(2222)^{3333} + (3333)^{2222} \equiv 1[5]$, en effet :

On a $2222 = 2[5]$ et $3333 = 3[5]$, donc

$$(2222)^{3333} + (3333)^{2222} \equiv 2^{3333} + 3^{2222} [5]$$

D'autre part

$$2^{3333} = (2^3)^{1111} \equiv (-2)^{1111} \equiv -(2^2)^{555} 2 \equiv -(-1)^{555} 2 \equiv 2[5]$$

et

$$3^{2222} = (3^2)^{1111} \equiv (-1)^{1111} \equiv -1[5]$$

d'où

$$(2222)^{3333} + (3333)^{2222} \equiv 2 + (-1)[5] \equiv 1[5].$$

2 PGCD, PPCM

2.1 Plus grand commun diviseur d'éléments de $\mathbb{Z}$

Proposition 2.1 Soit $(G, +)$ un groupe commutatif. Soient H et K deux sous-groupes de G . Alors $H + K = \{h + k / h \in H, k \in K\}$ est un sous-groupe de G , c'est le sous-groupe engendré par la partie $H \cup K$.

Démonstration : $H + K$ est une partie non vide ($0 \in K + K$). Soient $x = h + k$ et $y = h' + k'$ deux éléments de $H + K$, alors $x - y = (h - h') + (k - k') \in K + K$. $\square$

Généralisation : Ce résultat peut être généralisé à une famille finie $H_1, H_2, \dots, H_n$ de sous-groupes de $(G, +)$: $H_1 + H_2 + \dots + H_n = \{h_1 + h_2 + \dots + h_n / h_i \in H_i\}$ est le sous-groupe engendré par $\bigcup_{i=1}^n H_i$.

Définition 2.1 Soient a et b deux entiers relatifs. Alors il existe un unique entier d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. On dit que d est le pgcd de a et de b . On le note $d = \text{pgcd}(a, b)$ ou $d = a \wedge b$.

Remarques :

1. D'après la définition il existe des entiers relatifs u et v tels que $a \wedge b = ua + vb$ et tout élément de la forme $xa + yb$ ($x, y \in \mathbb{Z}$) est un multiple de $a \wedge b$.
2. Les entiers relatifs a et b sont premiers entre eux si, et seulement si, $a \wedge b = 1$.
3. $a \wedge b = |a|$ si, et seulement si, a divise b .

D'après la définition et les propriétés précédentes on déduit facilement le théorème suivant :

Théorème 2.1 Étant donné deux entiers relatifs a et b , les propriétés suivantes sont équivalentes :

1. a et b sont premiers entre eux.
2. il existe des entiers relatifs u et v tels que

$$au + bv = 1 \quad (\text{égalité de BEZOUT})$$

3. pour tout entier relatif z , il existe des entiers relatifs x et y tels que $ax + by = z$.

Remarque : Les couples (u, v) et (x, y) ne sont pas uniques (cf. TD).

Proposition 2.2 Soient a et $b \geq 2$ deux entiers naturels non nuls premiers entre eux. Alors

$$\exists!(u_0, v_0) \in \mathbb{N}^2 \text{ tel que } au_0 - bv_0 = 1,$$

avec $0 \leq u_0 < b$ et $0 \leq v_0 < a$.

Démonstration : • **L'existence :** D'après l'égalité de BEZOUT il existe deux entiers α et β tels que $1 = \alpha a - \beta b$. Effectuons la division euclidienne de α par b : $\alpha = bq + u_0$, avec $0 \leq u_0 < b$.

On obtient

$$\begin{aligned} 1 &= (bq + u_0)a - \beta b \\ &= u_0a - (\beta - qa)b \\ &= u_0a - v_0b \end{aligned}$$

avec $v_0 = \beta - qa$ donc $-1 \leq v_0b = u_0a - 1 < u_0a < ba$ et par simplification $0 \leq v_0 < a$.

• **L'unicité :** Soit $(u, v) \in \mathbb{N}^2$ tel que $au - bv = 1$ et par soustraction on a :

$$(*) \quad (u - u_0)a - (v - v_0)b = 0$$

donc a divise $(v - v_0)b$ et comme $a \wedge b = 1$ alors a divise $v - v_0$, c'est-à-dire $\exists k \in \mathbb{Z} : v = v_0 + ka$. En remplaçant dans $(*)$ on obtient $u = u_0 + kb$.

Réciproquement, tout couple $(u_0 + kb, v_0 + ka)$, $k \in \mathbb{Z}$ est solution. $\square$

Exemple : Déterminer deux entiers u et v tels que : $1 = 8u - 93v$. Les entiers 93 et 8 sont premiers entre eux, donc ils existent u et v tels que $1 = 8u - 93v$.

On a

$$\begin{aligned} 93 &= 8 \times 11 + 5 \\ 8 &= 5 \times 1 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \end{aligned}$$

donc en commençant par la dernière égalité, on obtient :

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (5 - 3 \times 1) \times 1 \\ &= 3 \times 2 - 5 \times 1 \\ &= (8 - 5 \times 1) \times 2 - 5 \times 1 \\ &= 8 \times 2 - 5 \times 3 \\ &= 8 \times 2 - (93 - 11 \times 8) \times 3 \\ &= 8 \times 35 - 93 \times 3 \end{aligned}$$

d'où $(u, v) = (35, 3)$.

Théorème 2.2 Soient a et b des entiers relatifs non nuls :

1. Pour tout c non nul : $\text{pgcd}(ac, bc) = |c| \text{pgcd}(a, b)$.
2. Pour tout diviseur commun d de a et de b : $\text{pgcd}(ad^{-1}, bd^{-1}) = |d^{-1}| \text{pgcd}(a, b)$.

Démonstration : 1. Soient a, b et c des entiers relatifs non nuls, on a :

$$ac\mathbb{Z} + bc\mathbb{Z} = \{c(a + b)k/k \in \mathbb{Z}\} = |c|(a\mathbb{Z} + b\mathbb{Z})$$

d'où

$$(ac) \wedge (bc) = |c|(a \wedge b)$$

2. D'après 1. $|d|[(ad^{-1}) \wedge (bd^{-1})] = (add^{-1}) \wedge (bdd^{-1}) = a \wedge b$. $\square$

Théorème 2.3 Les trois propriétés suivantes sont équivalentes :

1. a et b sont premiers entre eux.
2. Pour tout x , a divise bx entraîne a divise x . (théorème de GAUSS²)
3. Pour tout y , b divise ay entraîne b divise y .

2. Gauss, Carl Friedrich Gauss, Carl Friedrich (1777-1855), mathématicien, physicien et astronome allemand, dit le prince des mathématiciens, qui apporta des contributions essentielles à la plupart des branches des sciences exactes et appliquées.

Démonstration : (1) est symétrique, il suffit donc de montrer que $(1) \iff (2)$. En effet $a \wedge b = 1$ entraîne $(ax) \wedge (bx) = |x|$, a divise ax et bx , donc divise $|x| = (ax) \wedge (bx)$.

Montrons $(2) \implies (3)$: supposons b divise ay , donc il existe $q \in \mathbb{Z}$ tel que $ay = bq$, donc a divise q , donc $q = aq'$ ($q' \in \mathbb{Z}$), $ay = baq'$, d'où $y = bq'$. De même $(3) \implies (2)$.

Montrons enfin que $(2) \implies (1)$; soit d un diviseur commun de a et b :

$$(a = a'd \text{ et } b = b'd \implies ab' = ba')$$

donc a divisant ba' divise a' , or a' divisant a , donc $a' = \mp a$ et $d = \mp 1$. Donc a et b sont premiers entre eux. $\square$

Corollaire 2.1 (Variante du théorème de Gauss)

Soient a, b, c des entiers relatifs. Si a divise c , b divise c et $a \wedge b = 1$, alors ab divise c .

Démonstration : Si a divise c , donc il existe $k \in \mathbb{Z}$ tel que $c = ka$. On a aussi b divise c , donc b divise ka et comme $a \wedge b = 1$, il vient du théorème de Gauss que b divise k et par conséquent ab divise c . $\square$

Application : résolution de l'équation (E) $ax + by = c$ dans $\mathbb{Z}^2$ ($a, b \neq (0, 0)$).

On a $\forall x, y \in \mathbb{Z}, ax + by \in (a \wedge b)\mathbb{Z}$, d'où la discussion suivante :

1. Si c n'est pas un multiple de $a \wedge b$, alors l'équation (E) n'a pas de solutions de $\mathbb{Z}^2$.
2. Supposons $c = a(a \wedge b)$ avec $a \in \mathbb{Z}$. D'après le théorème de Bezout, il existe un couple (x_0, y_0) tel que $ax_0 + by_0 = a \wedge b$, donc $aa x_0 + ab y_0 = a(a \wedge b) = c$. Ainsi le couple (ax_0, ay_0) est solution particulière de (E).

Cherchons la solution générale de (E), l'équation (E) s'écrit

$$ax + by = aax_0 + aby_0$$

c'est-à-dire $a(x - ax_0) = b(ay_0 - y)$. Soient a' et b' les deux entiers relatifs premiers tels que :

$$a = a'(a \wedge b) \text{ et } b = b'(a \wedge b)$$

la dernière équation s'écrit alors :

$$a'(x - ax_0) = b'(ay_0 - y)$$

par le théorème de Gauss b' divise $x - ax_0$, soit $x = ax_0 + kb'$, avec $k \in \mathbb{Z}$, en remplaçant dans la dernière équation on obtient $y = ay_0 - ka'$.

Les solutions de sont donc les couples $(ax_0 + kb', ay_0 - ka')$ avec $k \in \mathbb{Z}$.

2.1.1 Algorithme d'Euclide pour la recherche du $a \wedge b$

Proposition 2.3 Soit r le reste de la division euclidienne de a par b avec $b > 0$. Alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$

Démonstration : En effet soit d un diviseur commun de a et b , alors d divise aussi r , de même si d divise r et b il divise a , donc $a \wedge b = b \wedge r$. $\square$

Soient a et b des entiers relatifs. Effectuons les divisions euclidiennes (Algorithme³ d'Euclide⁴ (on supposera $b > 0$)

$$a = bq_0 + r_0 \quad \text{et} \quad 0 \leq r_0 < b$$

$$b = r_0q_1 + r_1 \quad \text{et} \quad 0 \leq r_1 < r_0$$

$$r_0 = r_1q_2 + r_2 \quad \text{et} \quad 0 \leq r_2 < r_1$$

.

.

$$r_{n-1} = r_nq_{n+1} + r_{n+1} \quad \text{et} \quad 0 \leq r_{n+1} < r_n$$

On forme ainsi une suite $b > r_1 > r_2 > r_3 > \dots > r_{n-1} > r_n > \dots \geq 0$ strictement décroissante d'entiers, on arrive forcément à un premier reste $r_{n+1} = 0$. D'après le théorème

$$\text{pgcd}(a, b) = \text{pgcd}(b, r_1) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$$

Ainsi $a \wedge b$ est le dernier reste non nul dans cette succession de divisions.

3. Le mot algorithme est une déformation du nom du mathématicien arabe ALKWARIZMI (IX^e siècle) origine de *Kkwarizm*, ville nommée aujourd'hui *Khiva* et située en Ouzbékistan. Le nom du mathématicien a été déformé en *algorithmus*, puis *algorisme*, pour donner enfin algorithme.

4. Khuwarizmi, al- Khuwarizmi, al- (v. 780-v. 850), mathématicien arabe, dont les travaux sur l'algèbre, l'arithmétique et les tables d'astronomie ont considérablement fait progresser la pensée mathématique.

Khuwarizmi fut bibliothécaire à la cour du Calife Ald Allah al-Ma'mun et astronome à l'observatoire de Bagdad. Il fut le premier à utiliser à des fins mathématiques l'expression al jabr, dont est dérivé le mot français algèbre. La version latine (par le traducteur italien Gérard de Crémone) du traité d'algèbre d'al-Khuwarizmi fut à l'origine de la connaissance mathématique en Europe médiévale. Ses travaux sur les algorithmes, terme dérivé de son nom, permirent d'introduire la méthode de calcul utilisant les chiffres arabes et la notation décimale. Microsoft 6 Encarta 6 2006.

Exemple : Calculons $\text{pgcd}(3928, 382)$

$$\begin{aligned} 3928 &= 382 \times 10 + 10 \\ 382 &= 108 \times 3 + 5 \\ 108 &= 58 \times 1 + 8 \\ 58 &= 50 \times 1 + 8 \\ 50 &= 8 \times 6 + 2 \\ 8 &= 4 \times 2 \end{aligned}$$

d'où $\text{pgcd}(3928, 382) = 2$.

Travaux pratiques : Utilisation de Maple La procédure suivante prend comme arguments a et b et renvoie le pgcd de a et b .

```
> pgcd : = proc(a,b)
    local x,y,r;
    x:=a;y:=b;
    while y>0 do
        r:=irem(x,y);x:=y;y:=r;
    od;
    x;
end;
```

2.1.2 Plus grand commun diviseur d'une famille finie d'éléments de $\mathbb{Z}$

Théorème et définition 2.1 Étant donné une famille finie d'entiers relatifs $a_1, a_2, \dots, a_n$. Alors il existe un unique entier d tel que $a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$.

On dit que d est le pgcd de $a_1, a_2, \dots, a_n$. On le note $d = \text{pgcd}(a_1, a_2, \dots, a_n)$ ou $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$.

Démonstration : En effet, $H = a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$, donc il existe un unique entier naturel tel que $H = d\mathbb{Z}$. $\square$

D'après la définition ci-dessus et la définition 2.3, on déduit le théorème suivant :

Théorème 2.4 Étant donné des entiers relatifs $a_1, a_2, \dots, a_n$, les propriétés suivantes sont équivalentes :

1. $a_1, a_2, \dots, a_n$ sont premiers entre eux dans leur ensemble.

2. il existe des entiers relatifs $u_1, u_2, \dots, u_n$ tels que

$$a_1u_1 + a_2u_2 + \dots + a_nu_n = 1 \quad (\text{égalité de BEZOUT})$$

3. pour tout entier relatif z , il existe des entiers relatifs $x_1, x_2, \dots, x_n$ tels que $a_1x_1 + a_2x_2 + \dots + a_nx_n = z$.

Théorème 2.5 Soient $a_i, i = 1, 2, \dots, n$ des entiers relatifs non nuls :

1. Pour tout b non nul : $\text{pgcd}(a_1b, a_2b, \dots, a_nb) = |b|\text{pgcd}(a_1, a_2, \dots, a_n)$.

2. Pour tout diviseur commun d de $a_1, a_2, \dots, a_n$:

$$\text{pgcd}(a_1d^{-1}, a_2d^{-1}, \dots, a_nd^{-1}) = |d^{-1}|\text{pgcd}(a_1, a_2, \dots, a_n)$$

Démonstration : La démonstration est analogue à celle du théorème 2.2.

2.2 Plus petit commun multiple de deux ou plusieurs éléments de $\mathbb{Z}$

Théorème et définition 2.2 Soient a, b dans $\mathbb{Z}$. Il existe un unique entier m dans $\mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. L'entier m s'appelle le plus petit commun multiple de a et de b . On le note $m = \text{ppcm}(a, b)$, ou $m = a \vee b$.

Démonstration : En effet, $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$. $\square$

Remarque : Soient a et b deux entiers relatifs et $m = a \vee b$. D'une part m est un multiple de a et de b . D'autre part tout multiple de a et de b est un multiple de m . Donc m est le plus petit multiple commun strictement positif de a et de b , ces propriétés caractérisent entièrement l'entier $m = a \vee b$.

De même on peut généraliser la notion de *ppcm* à une famille finie d'entiers relatifs : on a le résultat suivant :

Théorème et définition 2.3 *Étant donné des entiers relatifs $a_1, a_2, \dots, a_n$ non nuls, il existe un unique entier m dans $\mathbb{N}$ tel que $a_1\mathbb{Z} \cap a_2\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = m\mathbb{Z}$. L'entier m s'appelle le plus petit commun multiple de $a_1, a_2, \dots, a_n$. On le note $m = \text{ppcm}(a_1, a_2, \dots, a_n)$, ou $m = a_1 \vee a_2 \vee \dots \vee a_n$.*

Proposition 2.4 **Pour tous entiers relatifs a et b , on l'égalité suivante :**

$$|ab| = (a \wedge b)(a \vee b)$$

Démonstration : Soient a et b des entiers relatifs, il existe des entiers relatifs a', b', a'' et b'' tels que :

$$a = da', b = db', m = aa'' = bb'', \text{ avec } d = a \wedge b \text{ et } m = a \vee b \text{ et } a' \wedge b' = 1$$

on a $a'b'd = ab' = a'b$, donc $a'b'd \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ et par suite $(a'b'd)\mathbb{Z} \subset m\mathbb{Z}$.

Inversement $aa'' = bb''$ ou $da'a'' = db'b''$ donc $a'a'' = b'b''$ et comme $a' \wedge b' = 1$, on peut écrire d'après le théorème de Gauss $b'' = ka' (k \in \mathbb{Z})$; d'où $m = ka'b$ ou $m = ka'b'd$, on a donc $m \in (a'b'd)\mathbb{Z}$ et en suite $m\mathbb{Z} \subset (a'b'd)\mathbb{Z}$.

Finalement $m\mathbb{Z} = (a'b'd)\mathbb{Z}$. D'où $(md)\mathbb{Z} = (a'b'd^2)\mathbb{Z} = (ab)\mathbb{Z}$ et par conséquent $md = |md| = |ab|$. $\square$

Remarque : Si a et b sont premiers entre eux, alors $a \vee b = |ab|$ et la réciproque est vraie d'après la dernière proposition.

3 Décomposition d'un entier relatif en facteurs premiers

1. Si a est premier il admet au moins un diviseur premier : lui-même ; supposons a non premier, il admet donc au moins un diviseur b distinct de ∓ 1 et $\mp a$.

Si b divise a , $\mp b$ divise $\mp a$, on peut donc supposer a et b positifs, nous avons donc :

$$a = bq \quad \text{et} \quad 1 < b < a.$$

Ces diviseurs $b > 1$ sont en nombres finis, le plus petit d'entre eux est certainement premier, d'où :

Proposition 3.1 **Tout entier relatif distinct de 1 et -1 admet un diviseur premier.**

2. Soit a un entier rationnel non nul, il admet un diviseur premier $p_1 : a = p_1 a_1$, si a_1 n'est pas premier il admet un diviseur premier $p_2 > 0$, donc $a_1 = p_2 a_2$, $a = p_1 p_2 a_2$. Nous pouvons recommencer cette opération ; nous aurons :

$$a = p_1 p_2 \dots p_n a_n$$

avec $|a| > |a_1| > \dots > |a_{n-1}| > |a_n|$. Si nous n'arrivons pas à a_i premier, nous arriverons à $a_j = \mp 1$, donc :

$$a = u p_1 p_2 \dots p_n$$

où $u = \mp 1$ et $p_1, p_2, \dots, p_n$ sont des entiers premiers strictement positifs. Montrons qu'une telle décomposition est unique, soit

$$u p_1 p_2 \dots p_n a = v q_1 q_2 \dots q_n$$

avec les p_i et les q_i des entiers premiers strictement positifs et $u = \mp 1, v = \mp 1$. On a $u = v$, p_1 divise l'un des facteurs de $q_1 q_2 \dots q_n$, soit q_1 , mais q_1 est premier donc $p_1 = q_1$, on simplifie donc par p_1 ; en répétant ce raisonnement un nombre fini de fois on arrive à épuiser tous les facteurs de l'un des membres, d'où : $r_1, r_2, \dots, r_l$ étant les facteurs premiers restants :

$$r_1, r_2, \dots, r_l = 1$$

ceci est impossible car les r_i sont supérieurs ou égaux à 2, donc on épuise en même temps les facteurs de deux membres. En regroupant les facteurs égaux dans la décomposition précédente on obtient le théorème suivant :

Théorème 3.1 **Tout entiers relatifs non nul et distinct de ∓ 1 peut s'écrire d'une manière unique sous la forme :**

$$a = u p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

où $u = \mp 1$ et $p_1, p_2, \dots, p_m$ sont des entiers premiers strictement positifs tous distincts et $k_1, k_2, \dots, k_m$ des entiers strictement positifs.

Application 1. Les diviseurs d'un entier a ayant la décomposition $a = up_1^{k_1}p_2^{k_2}\dots p_n^{k_n}$ sont tous de la forme :

$$d = up_1^{h_1}p_2^{h_2}\dots p_n^{h_n} \quad u = \mp 1 \quad 0 \leq h_i \leq k_i$$

Application 2. Désignons par $p_1, p_2, \dots, p_n$ l'ensemble des facteurs premiers strictement positifs de a et de b , on peut écrire :

$$a = up_1^{k_1}p_2^{k_2}\dots p_n^{k_n}, k_i \geq 0$$

$$b = vp_1^{l_1}p_2^{l_2}\dots p_n^{l_n}, l_i \geq 0$$

On obtient :

$$a \wedge b = \prod_{i=1}^{i=n} p_i^{\inf(k_i, l_i)}$$

et

$$a \vee b = \prod_{i=1}^{i=n} p_i^{\sup(k_i, l_i)}$$

4 Numération

4.1 Bases de numération dans $\mathbb{N}$

Lemme 4.1 Soit $a \in \mathbb{N}^* \setminus \{1\}$ et x entier naturel non nul, alors il existe un entier naturel unique n tel que $a^n \leq x < a^{n+1}$.

Démonstration : Soit $E = \{i \in \mathbb{N} / a^i \leq x\}$, E est une partie non vide ($0 \in E$) et bornée ($\forall i \in E, i \leq \frac{\ln(x)}{\ln(a)}$), soit $n = \max E$, alors $a^n \leq x < a^{n+1}$. $\square$

Théorème et définition 4.1 Soit $a \in \mathbb{N}^* \setminus \{1\}$. Tout entier naturel x non nul s'écrit d'une manière unique sous la forme

$$x = x_n a^n + x_{n-1} a^{n-1} + \dots + x_1 a + x_0$$

avec $0 < x_n < a$ et $\forall i \in \{0, 1, \dots, n-1\}, 0 \leq x_i < a$.

On pose $x = \overline{x_n x_{n-1} \dots x_1 x_0}_a$ ou tout simplement $x = \overline{x_n x_{n-1} \dots x_1 x_0}$, cette écriture est appelée écriture de x dans la base a , $x_n, x_{n-1}, \dots, x_1, x_0$ sont les chiffres de la représentation de x en base a .

Démonstration : • Soit x_n la partie entière de $\frac{x}{a^n}$ (n étant définie par le lemme), alors $x_n \leq \frac{x}{a^n} < x_n + 1$ ou encore $x_n a^n \leq x < (x_n + 1)a^n$.

• $x_n \neq 0$, car sinon on aura $0 \leq x_n < a^n$ ce qui est absurde.

• On a $0 \leq x - x_n a^n < a^n$, effectuons la division euclidienne de $r_n = x - x_n a^n$ par a^{n-1} , donc il existe un unique couple (x_{n-1}, r_{n-1}) tel que :

$$x - x_n a^n = x_{n-1} a^{n-1} + r_{n-1} \text{ et } 0 \leq r_{n-1} < a^{n-1}$$

de plus $x_{n-1} a^{n-1} \leq x_{n-1} a^{n-1} + r_{n-1} = x - x_n a^n < a^n$, ce qui entraîne $0 \leq x_{n-1} < a$. En réitérant ce raisonnement un nombre fini de fois on arrivera à construire deux suites finies $x_{n-1}, \dots, x_1, x_0$ et $r_{n-1}, \dots, r_1, r_0$ avec x_i le quotient de la division euclidienne de $r_{i+1} = x - x_n a^n - x_{n-1} a^{n-1} - \dots - x_{i+1} a^{i+1}$ par a^i et r_i le reste.

D'autre part :

$$0 \leq x_i a^i \leq x_i a^i + r_i = r_{i+1} < a^{i+1}$$

ce qui entraîne $0 \leq x_i < a$. $\square$

Exemples :

- On utilise le plus souvent les bases $x = 2$ (numération binaire, les chiffres sont 0 et 1), $x = 8$ (numération octale, les chiffres sont 0,1,2,...,7), $x = 10$ (numération décimale, les chiffres sont 0,1,2,...,9).
- L'entier $n = 2005$ (en numération décimale) s'écrit $n = \overline{11111010101}_2$ en numération binaire et $n = \overline{3725}_8$ en numération octale.

4.2 Comparaison de deux nombres écrits en base a

Soient x et y deux entiers naturels et $x = \overline{x_n x_{n-1} \dots x_1 x_0}^a$ $y = \overline{y_m y_{m-1} \dots y_1 y_0}^a$ leurs représentations dans la base a ($a > 1$).
Si $m > n$, alors $m \geq n + 1$, d'où $a^m \geq a^{n+1}$ et on sait, d'après le lemme, que $x < a^{n+1}$ et $a^m \leq y$; alors

$$x < a^{n+1} \leq a^m \leq y$$

donc $x < y$.

Proposition 4.1 $x = \overline{x_n x_{n-1} \dots x_1 x_0}^a$ et $y = \overline{y_m y_{m-1} \dots y_1 y_0}^a$ étant deux entiers écrits dans la base a ($a > 1$). Si $m > n$ alors $x < y$.

Remarque : Si $m = n$, alors x et y sont dans le même ordre que les $(n + 1)$ -uplets $(x_n, x_{n-1}, \dots, x_1, x_0)$ et $(y_n, y_{n-1}, \dots, y_1, y_0)$ classés suivant l'ordre lexicographique. En effet supposons

$$x_n = y_n, x_{n-1} = y_{n-1}, \dots, x_i = y_i \text{ et } x_i \neq y_i$$

Supposons par exemple $y_i > x_i$, considérons $z = x_{i-1}a^{i-1} + \dots + x_1a + x_0$. On a $z < a^i$, d'où $x = x_n a^n + \dots + x_i a^i + z < x_n a^n + \dots + x_i a^i + a^i$, d'autre part on a : $y \geq y_n a^n + \dots + y_i a^i \geq x_n a^n + \dots + (x_i + 1)a^i$, car $y_i > x_i$, donc

$$y \geq x_n a^n + \dots + x_i a^i + a^i > x$$

d'où $y > x$.

Exemple : Dans la base 5, on a : $1233 > 333$ et $32142 > 32242$.

4.3 Somme et produit de deux nombres écrits en base a

4.3.1 Somme de deux nombres écrits en base a

Soient x et y deux entiers naturels et $x = \overline{x_n x_{n-1} \dots x_1 x_0}^a$ et $y = \overline{y_m y_{m-1} \dots y_1 y_0}^a$ leurs représentations dans la base a ($a > 1$).
Supposons $m \neq n$, par exemple $m < n$, on peut écrire y sous la forme $y = \overline{y_n y_{n-1} \dots y_{m+1} y_m y_{m-1} \dots y_1 y_0}^a$ avec

$$y_n = y_{n-1} = \dots = y_{m+1} = 0$$

Donc

$$(1) \quad x + y = (x_n + y_n)a^n + \dots + (x_i + y_i)a^i + \dots + (x_1 + y_1)a + (x_0 + y_0)$$

- Si pour tout i , $x_i + y_i < a$ alors l'écriture (1) est la représentation de $x + y$ dans la base a .
- S'il existe i tel que $x_i + y_i \geq a$, alors, puisque $b_i + y_i < 2a$, il existe $d_i < a$ tel que $x_i + y_i = 1a + d_i$, donc $x_i + y_i = \overline{1d_i}^a$.
Donc $(x_i + y_i)a^i = a^{i+1} + d_i a^i$ et $x_{i+1} + y_{i+1}$ doit être remplacé par $x_{i+1} + y_{i+1} + 1$.

Conclusion : Pour obtenir la représentation de $x + y$ dans la base a , il faut utiliser et reporter une retenue de 1 à chaque fois que la somme intermédiaire obtenue est supérieure ou égale à a .

Exemple :

$$\begin{aligned} x + y &= \overline{4241}^6 + \overline{14532}^6 \\ &= 1.6^4 + 8.6^3 + 7.6^2 + 7.6 + 3 \\ &= 1.6^4 + (6+2)6^3 + (6+1)6^2 + (6+1)6 + 3 \\ &= 2.6^4 + 3.6^3 + 2.6^2 + 1.6 + 3 \\ &= \overline{23213}^6 \end{aligned}$$

4.3.2 Produit de deux nombres écrits en base a

Soit x un entier naturel et $x = \overline{x_n x_{n-1} \dots x_1 x_0}^a$ sa représentation dans la base a ($a > 1$).
Pour tout entier k , on a :

$$a^k x = x_n a^{n+k} + \dots + x_1 a^{k+1} + x_0 a^k + 0a^{k-1} + \dots + 0a + 0$$

c'est-à-dire $a^k x = \overline{x_n x_{n-1} \dots x_1 x_0 0 \dots 0}^a$ et on aussi pour tout entier α .

$$(1) \quad \alpha x = (\alpha x_n)a^n + \dots + (\alpha x_1)a + (\alpha x_0)$$

- Si pour tout i , $\alpha x_i < a$, alors (1) est la représentation de αx dans la base a .
- S'il existe un entier i tel que $\alpha x_i \geq a$ on refait la même chose comme dans le cas d'addition.
- Si maintenant $y = \overline{y_m y_{m-1} \dots y_1 y_0}^a$, alors

$$xy = x_n(a^n y) + x_{n-1}(a^{n-1} y) + \dots + x_1(a y) + x_0 y$$

et d'après ce qui précède on peut calculer le produit xy .

Exercice : Existe-t-il un entier naturel a tel que $\overline{xxx^a yyy^a} = \overline{yyyyyy^a}$ (1) ?
Supposons qu'il existe un tel a tel que l'égalité (1) soit vérifiée. Alors

$$(1) \iff x^2(a^2 + a + 1)^2 = y(b^5 + a^4 + a^3 + a^2 + a + 1) = y(a^2 + a + 1)(a^3 + 1)$$

ou encore

$$\begin{aligned} x^2(a^2 + a + 1) &= y(a^3 + 1) \\ &= y(a^3 - 1) - 2y \\ &= y(a^2 + a + 1)(a - 1) - 2y \end{aligned}$$

donc $2y$ divise $a^2 + a + 1$ et puisque $0 < y < a$, alors $0 < 2y < 2a$, et on a $2a < a^2 + 1 < a^2 + a + 1$, donc $2y < a^2 + a + 1$ ce qui est absurde puisque $2y$ divise $a^2 + a + 1$. Donc notre hypothèse est fausse.

4.4 Application : Algorithme d'exponentiation rapide

Soit a un réel et n entier naturel non nul. Calculons a^n , directement il est inefficace d'effectuer le produit de n exemplaires de a , on peut obtenir le même résultat avec moins d'opérations en utilisant la représentation binaire de n .

Posons $n = \overline{b_k b_{k-1} \dots b_1 b_0} = \sum_{i=0}^k b_i 2^i$ (pour tout i , $b_i = 0$ ou $b_i = 1$).

Notons S l'ensemble des $i \in \{0, 1, 2, \dots, k\}$ tels que $b_i = 1$. Alors $n = \sum_{i \in S} b_i 2^i = \sum_{i \in S} 2^i$ puis $a^n = a^{\sum_{i \in S} 2^i} = \prod_{i \in S} a^{2^i}$. Il suffit donc de calculer les $u_i = a^{2^i}$. Or $u_0 = a$ et pour tout i on a $u_{i+1} = u_i^2$. On calcule les u_i (pour $i \in S$) par des élévations au carré successives, et on les multiplie.

Exemple : On a : $2005 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^2 + 2^0 = \overline{11111010101}^2$. Pour calculer a^{2005} , il suffit donc de calculer

- $u_2 = a^{2^2} = a^4$ (3 produits)
- $u_4 = a^{2^4} = (u_2^2)^2$ (2 élévations au carré)
- $u_6 = a^{2^6} = (u_4^2)^2$ (2 élévations au carré)
- $u_7 = a^{2^7} = u_6^2$ (1 élévation au carré)
- $u_8 = a^{2^8} = u_7^2$ (1 élévation au carré)
- $u_9 = a^{2^9} = u_8^2$ (1 élévation au carré)
- $u_{10} = a^{2^{10}} = u_9^2$ (1 élévation au carré)

D'où $a^{2005} = u_0 u_2 u_4 u_6 u_7 u_8 u_9 u_{10}$ (7 produits), ainsi 18 produits suffisent à calculer a^{2005} .

.....