Université Paris 13, Institut Galilée
Département de Mathématiques
Licence 2ème année Informatique
2013-2014

Cours de Mathématiques pour l'Informatique
Des nombres aux structures
Sylviane R. Schwer

Leçon du 4 février 2014 l'ensemble des entiers relatifs $\mathbb{Z}$

1 Ensemble des entiers relatifs $\mathbb{Z}$

Il s'agit de construire un ensemble dont une partie – nommée $\mathbb{Z}_+$ se comporte exactement comme $\mathbb{N}$, c'est-à-dire que

- les opérations et relations vues dans $\mathbb{N}$ ont exactement le même comportement dans $\mathbb{Z}_+$
- l'opération de soustraction est partout définie dans $\mathbb{Z}$
- tout élément de $\mathbb{Z}$ possède un élément symétrique pour l'addition

En confondant $\mathbb{Z}_+$ et $\mathbb{N}$, on dit que $\mathbb{Z}$ est une extension de $\mathbb{N}$.

Nous proposerons une construction plus standard de $\mathbb{Z}$ dans la seconde partie du cours fondée sur la notion de relation d'équivalence sur des couples d'entiers naturels. Ici, nous nous inspirons de ce qu'écrit Cauchy en 1821 dans son cours d'analyse de l'Ecole Royale: "Nous prendrons toujours la dénomination de *nombres* dans le sens où on l'emploie en Arithmétique, en faisant naître les nombres de la mesure absolue des grandeurs, et nous appliquerons uniquement la dénomination de *quantités* aux quantités positives ou négatives, c'est-à-dire aux nombres précédés des signes + ou −."

Définition 1.1 $\mathbb{Z} = \{(\delta, n), n \in \mathbb{N}_*, \delta = +ou-\} \cup \{0\}$.
δ est le signe de u
n est la valeur absolue *de $u = (\pm, n)$, que l'on note $|u|$.*

Par convention, on notera $0 = (+, 0) = (-, 0)$. Il faudrait vérifier à chaque fois que l'on obtient bien le même résultat en prenant l'une ou l'autre des notations. Nous laissons cela au lecteur.
Remarque : $(+, n) = (-, n) \Longleftrightarrow n = 0$.

1.1 addition sur Z

L'addition dans $\mathbb{Z}$ est définie par cas à partir de l'addition dans $\mathbb{N}$ en posant

Définition 1.2 $\forall(\delta_1, n_1), (\delta_2, n_2) \in \mathbb{Z}$

- *si* $\delta_1 = \delta_2 = \delta$, *alors* $(\delta, n_1) + (\delta, n_2) = (\delta, n_1 + n_2)$
- *si* $\delta_1 \neq \delta_2$ *et* $n_1 \geq n_2$ *alors* $(\delta_1, n_1) + (\delta_2, n_2) = (\delta_1, n_1 - n_2)$
- *si* $\delta_1 \neq \delta_2$ *et* $n_1 < n_2$ *alors* $(\delta_1, n_1) + (\delta_2, n_2) = (\delta_2, n_2 - n_1)$

Exemples (+,3)+(+,20)=(+,23) ; (-,3)+(-,20)=(-,23) ; (+,3)+(-,20)=(-,17) ; (-,3)+(+,20)=(+,17)

L'addition sur $\mathbb{Z}$ est une opération interne partout définie, associative, commutative, d'élément neutre 0, et tout élément (δ, n) est régulier et possède un unique inverse $(-\delta, n)$, appelé son opposé. On note

$$(-\delta, n) = -(\delta, n).$$

$< \mathbb{Z}, + >$ est un groupe additif commutatif.

Dans $\mathbb{Z}$, non seulement 0 peut être ajouté ou enlevé sans modifier une addition, mais il peut être remplacé par $(\delta, n) + (-\delta, n)$, quelque soit n, sans modifier une addition.

$$(\delta, x) = (\delta, x) + (+, 0) = (\delta, x) + (-, 0) = (\delta, x) + (\delta, n) + (-\delta, n)$$

1.2 soustraction sur Z

Soustraire un entier, c'est ajouter son opposé

$$(\delta_1, n_1) - (\delta_2, n_2) = (\delta_1, n_1) + (-\delta_2, n_2)$$

La soustraction est une opération interne partout définie, non associative, non commutative, d'élément neutre 0 à droite mais pas à gauche [car $a - u = u \Longleftrightarrow a = 2u$.].

Tout élément $u = (\delta, n)$ est régulier à droite et à gauche.

1.3 multiplication sur Z

1.3.1 multiplication des signes

Table 1: règle des signes pour la multiplication

×	+	-
+	+	-
-	-	+

1.3.2 produit de deux entiers relatifs

$$(\delta_1, n_1) \times (\delta_2, n_2) = (\delta_1 \times \delta_2, n_1 \times n_2)$$

La multiplication sur $\mathbb{Z}$ est une opération interne partout définie, associative, commutative, d'élément neutre 1, d'élément absorbant 0, dont les seuls éléments inversibles sont $(-, 1)$ et $(+, 1)$ et tout élément non nul est régulier. La multiplication est distributive par rapport à l'addition.

On dit que $< \mathbb{Z}, +, . >$ possède une structure d'anneau commutatif unitaire.

1.4 Relation d'ordre naturel sur $\mathbb{Z}$: $\leq$

Définition 1.3 $(\delta_1, n_1) < (\delta_2, n_2)$ *si*
soit $[(\delta_1 = -$ *et* $\delta_2 = +)$ *soit* $(\delta_1 = \delta_2 = +$ *et* $n_1 < n_2)$ *soit* $(\delta_1 = \delta_2 = -$ *et* $n_1 > n_2)]$
$(\delta_1, n_1) \leq (\delta_2, n_2)$*si* $(\delta_1, n_1) < (\delta_2, n_2)$ *ou* $(\delta_1, n_1) = (\delta_2, n_2)$

La relation $\leq$ confère à $\mathbb{Z}$ une structure d'ordre linéaire discrète sans plus grand ni plus petit élément. Il n'est donc pas possible de faire un raisonnement par récurrence sur tout $\mathbb{Z}$. Mais, tout ensemble borné possède un plus petit et un plus grand élément.

1.5 $\mathbb{N}$ comme sous-ensemble de $\mathbb{Z}$

$\{(+, n), n \in \mathbb{N}\}$ se comporte vis-à-vis des opérations arithmétiques et de la relation $\leq$ comme $\mathbb{N}$. On assimile donc ce sous ensemble de $\mathbb{Z}$ à $\mathbb{N}$ et l'on pose $(+, n) = n$ et $(-, n) = -(+, n) = -n$. On a donc

$$Z = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

$$z \in \mathbb{Z}, \quad \text{soit} \quad z = 0 \quad \text{soit} \quad z \in \mathbb{N}_* \quad \text{soit} \quad -z \in \mathbb{N}_*$$

Soit $z \in \mathbb{Z}$, sa valeur absolue est $|z| = z$ si $z \in \mathbb{N}$ et $|z| = -z$ si $z \notin \mathbb{N}$
On note aussi

$$\mathbb{Z}_* = \mathbb{Z} - \{0\} \quad ; \quad \mathbb{Z}_+ = N \quad ; \quad \mathbb{Z}_- = \mathbb{Z} - \mathbb{N}_* \quad ; \quad \mathbb{Z}_{+,*} = \mathbb{N}_* \quad ; \quad \mathbb{Z}_{-,*} = \mathbb{Z} - \mathbb{N}$$

Lemme 1.1
(1) Il n'existe pas de suite strictement décroissante sur $\mathbb{Z}_+$
(2) Il n'existe pas de suite strictement croissante sur $\mathbb{Z}_-$

Preuve. (1) découle des propriétés de $\mathbb{N}$.
(2) Si (v_n) était une suite strictement croissante de $\mathbb{Z}_-$, alors $(-v_n)$ serait une suite strictement décroissante de $\mathbb{Z}_+ = \mathbb{N}$ $\square$.

2 Relation de divisibilité dans $\mathbb{Z}$

2.1 Définition et premières propriétés

Définition 2.1 *Etant donné deux entiers relatifs a et b, on dit que a divise b ou que b est un multiple de a - noté $a|b$ - si il existe un entier relatif c tel que $b = ac$.*
On note $a\mathbb{Z}$ l'ensemble des multiples de a dans $\mathbb{Z}$ et $D_{\mathbb{Z}}(a)$ l'ensemble des diviseurs de a dans $\mathbb{Z}$.

Nous avons noté deux entiers relatifs particuliers pour le produit :
L'élément neutre 1 est un diviseur de tout élément de $\mathbb{Z}$, y compris de lui-même, mais ce n'est plus le seul, -1 est aussi un diviseur de tout élément de $\mathbb{Z}$, y compris de lui-même et de 1.
L'élément absorbant 0 est un multiple de tout élément de $\mathbb{N}$, y compris de lui-même. C'est pourquoi la division de 0 par 0 est *indéterminée*.

En revanche, si $a \neq 0$, alors si $a|b$, il existe un unique $c \in \mathbb{Z}$ tel que $b = ca$.

Preuve : Supposons que $\exists c_1 \in \mathbb{Z}$ et $c_2 \in \mathbb{Z}$ tel que $b = ac_1 = ac_2$. Comme $a \neq 0$, il est régulier pour le produit, donc $c_1 = c_2$. □

Proposition 2.1
• *Un produit d'entiers relatifs est nul si et seulement si l'un de ses termes est nul.*
• *Un produit d'entiers relatifs est égal à 1 si et seulement si*
– *(i) tous ses termes valent 1 ou -1*
– *(ii) il y a un nombre pair de termes valant -1.*

$0\mathbb{Z} = 0$; $1\mathbb{Z} = -1\mathbb{Z} = \mathbb{Z}$; $z\mathbb{Z} = (-z)\mathbb{Z} = |z|\mathbb{Z}$
$D_{\mathbb{Z}}(0) = \mathbb{Z}$; $D_{\mathbb{Z}}(1) = D_{\mathbb{Z}}(-1) = \{-1, 1\}$;
$\forall z \in \mathbb{Z}, D_{\mathbb{Z}}(z) = D_{\mathbb{Z}}(-z) = D_{\mathbb{N}}(|z|) \cup -1D_{\mathbb{N}}(|z|)$
On en déduit que $a\mathbb{Z}$ et $D_{\mathbb{Z}}(a)$ sont des parties non vides de $\mathbb{Z}$.
$\forall z \in \mathbb{Z}$, $z, -z, 0 \in |z|\mathbb{Z}$ et $z, -z, 1, -1 \in D_{\mathbb{N}}(|z|)$
$D_{\mathbb{Z}}(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$; $12\mathbb{Z} = \{0, \pm 12, \pm 24, \pm 36, \cdots\}$

Exemples $D_{\mathbb{Z}}(7) = \{\pm 1, \pm 7\}$; $7\mathbb{Z} = \{0, \pm 7, \pm 14, \pm 21, \cdots\}$

Si $k \in D_{\mathbb{Z}}(z)$ alors $-|z| \leq k \leq +|z|$. $D_{\mathbb{Z}}(n)$ est donc une partie bornée de $\mathbb{Z}$ pour la relation $\leq$ qui n'est pas un $\leq$-intervalle.

2.2 Etude de la relation |

$\forall n, m, p \in \mathbb{Z}$, la relation | :
– est *réflexive* : $n|n$, car $n = 1.n$
– n'est pas *antisymétrique* : car $m|n$ et $n|m \Rightarrow n = \pm m$
– *transitivité* : $m|n$ et $n|p \Rightarrow m|p$
• elle est *partielle* : $\exists n, m \in \mathbb{N}$, tel que ni $n|m$ ni $m|n$, par exemple, 2 et 5 ne sont pas comparables pour la divisiblité dans $\mathbb{N}$.
• elle ne possède pas d'éléments minimum car les deux candidats potentiels seraient 1 et

-1mais $1|-1$ et $-1|1$
• elle possède un plus grand élément : 0
• Attention : 0 n'ayant pas de plus proche voisin, puisque $\forall a \in \mathbb{Z}_*, a|2a|0$, l'ordre $|$ n'est pas discret sur $\mathbb{Z}$. En revanche, il est discret sur $\mathbb{Z}_*$

Diagramme de Hasse On ne représente que $< D_{\mathbb{N}}(|n|), | >$, pour $n \in \mathbb{Z}_*$.

Lemme 2.1 *pour la relation de divisibilité* $\forall n \in \mathbb{Z}$,

1. $|n|$ *est le plus petit élément strictement positif de* $n\mathbb{Z}$
2. 0 *est le plus grand élément de* $n\mathbb{Z}$
3. 1 *est le plus petit élément de* $D_{\mathbb{N}}(|n|)$
4. $|n|$ *est le plus grand élément de* $D_{\mathbb{N}}(|n|)$
5. *Si* $|n| \geq 2$, $D_{\mathbb{Z}}(n)$ *possède au moins quatre éléments :* $1, -1, n, -n$
6. *Si* $|n| \geq 1$, $n\mathbb{Z}$ *possède une infinité d'éléments*

2.3 Etude de $|$ vis à vis des opérations de $\mathbb{Z}$

Stabilité de la division par linéarité : Soit a, b, c trois entiers relatifs,

$$(a|b \quad \text{et} \quad a|c) \Rightarrow (\forall \lambda, \mu \in \mathbb{Z}, \quad a|\lambda.b \pm \mu.c)$$

Attention, si $a|c$ et $b|c$, alors il est faut d'affirmer que $\lambda.a + \mu.b|c$ comme on pourra s'en convaincre avec $2|6$ et $3|6$ mais $2 + 3$ ne divise pas 6 !

Stabilité de la division par produit : Soit a, b, c, d quatre entiers relatifs,

$$(a|b \quad \text{et} \quad c|d) \Rightarrow (a.c|b.d)$$

Régularité de tout entier relatif non nul pour la division : Soit a, b, u trois entiers relatifs,

$$(au|bu) \Leftrightarrow (u = 0) \quad \text{ou} \quad (a|b)$$

3 Division entière dans $\mathbb{Z}$

Théorème 3.1 (division euclidienne) *Soit* $a \in \mathbb{Z}$ *et* $b \in Z_*$, *il existe un couple unique* $(q_{a,b}, r_{a,b}) \in \mathbb{Z}^2$ *qui satisfont*

$$a = b.q_{a,b} + r_{a,b} \quad \textbf{\textit{et}} \quad 0 \leq r_{a,b} < |b|$$

Attention : dans $\mathbb{N}$, nous avions vu qu'il pouvait exister plusieurs écritures de a sous la forme $bq+r$ si l'on supprime la contrainte $0 \leq r_{a,b} < b$. Dans $\mathbb{Z}$, il peut exister une infinité d'écritures de a sous la forme $bq + r$ si l'on supprime la contrainte $0 \leq r_{a,b} < |b|$. Par exemple $20 = 3.6 + 2 = 3.5 + 5 = 3.4 + 8 = 3.3 + 11 = 3.2 + 14 = 3.1 + 17 = 3.0 + 20 = 3.(-1) + 23 = \cdots$.
Preuve : La suite $(a + |b|k)_{k\in\mathbb{N}}$ est strictement croissante, donc elle ne peut (lemme 1.1) être incluse dans $\mathbb{Z}_-$. Il existe donc un entier naturel k pour lequel $a + |b|k \in \mathbb{N}$. La division euclidienne sur $\mathbb{N}$ de $a + |b|k$ par $|b|$ produit un couple unique (q_k, r_k) tel que $0 \leq r_k < |b|$ et $a + |b|k = q_k|b| + r_k$. On en déduit que $a = |b|[q_k - k] + r_k$. Or $b \neq 0$, donc $a = b\dfrac{|b|}{b}[q_k - k] + r_k$. Posons $q = \dfrac{|b|}{b}[q_k - k]$ et $r = r_k$, alors $a = bq + r$ avec $0 \leq r_{a,b} < |b|$.
Montrons maintenant l'unicité du couple. Supposons qu'il existe (q, r) et (q', r') deux candidats possibles avec $r' \geq r$.
$(*) a = bq+r = bq'+r'$ avec $(**) 0 \leq r < |b|$ et $0 \leq r' < |b|$. De $(*)$ on déduit $b(q-q') = r'-r$ c'est-à-dire que $|r' - r| \in |b|\mathbb{N}$ et de $(**)$ on déduit que $0 < |r' - r| < |b| - r \geq |b|$. Or le seul multiple de $|b|$ strictement inférieur à $|b|$ est 0, donc $r = r'$ et $q = q' \square$

Remarque 1 : a est multiple de b ou b divise a si et seulement si $r_{a,b} = 0$

Remarque 2 : On peut toujours se ramener à $b > 0$. En effet, supposons que $b < 0$ et $a = |b|q + r$ avec $0 \leq r < |b|$, alors $a = -bq + r = b(-q) + r$.

Exemple 1 : division entière de 120 par -7 : $120 = 7.17 + 1$, donc $120 = (-7)(-17) + 1$

Exemple 2 : $-120 = 7(-17) - 1 = 7(-18) + 6$, donc $-120 = (-7)(18) + 6$.

Définition 3.1 *Pour tout $a \in \mathbb{Z}$ et $b \in Z_*$, soit le couple unique $q_{a,b} \in \mathbb{Z}$ et $r_{a,b} \in \mathbb{N}$ qui satisfait*

$$a = b.q_{a,b} + r_{a,b} \quad \textbf{\textit{et}} \quad 0 \leq r_{a,b} < |b|$$

$q_{a,b}$ est appelé division entière de a par b et est noté $DIV(a, b)$. C'est une opération de $\mathbb{Z} \times \mathbb{Z}_* \to \mathbb{Z}$.
$r_{a,b}$ est appelé le reste de a par b ou résidu de a modulo b.

Remarque : si $a = b\,c+r$ avec $0 \leq r < inf(b, c)$, il peut y a une ambiguïté sur le diviseur de la division euclidienne puisque la multiplication est commutative. Par exemple pour $62 = 7\times8+6$ mais pas pour $63 = 3\times20+3$ n'est pas ambiguë pour la division euclidienne. C'est la division euclidienne de 63 par 20 et non de 63 par 3.

Exemple de division euclidienne : Calculons le quotient et le reste de la division euclidienne de 35421 par 31 en explicitant la potence classique
$35421 = \underline{35} \times 1000 + 421 = (31 + 4)1000 + 421 = 31 \times 1000 + 4421$
$= 31 \times 1000 + 4421 = 31 \times 1000 + \underline{44} \times 100 + 21 = 31 \times 1000 + (31 + 13) \times 100 + 21$
$= 31 \times 1000 + 31 \times 100 + 1321 = 31 \times 1000 + 31 \times 100 + \underline{132} \times 10 + 1$
$= 31 \times 1000 + 31 \times 100 + (31 \times 4 + 8) \times 10 + 1 = 31 \times 1000 + 31 \times 100 + 31 \times 4 \times 10 + \underline{81}$

Table 2: division euclidienne de 35421 par 31

35421	31
4421	1142
1321	
81	
19	

$= 31 \times 1000 + 31 \times 100 + 31 \times 4 \times 10 + (31 \times 2 + 19)$
$= 31 \times 1000 + 31 \times 100 + 31 \times 4 \times 10 + 31 \times 2 + 19 = 31 \times 1142 + 19.$

3.1 sous-ensembles linéairement stables de $\mathbb{Z}$

Définition 3.2 *Un ensemble E est dit* stable *pour un opérateur f de E si $f(E) = \{f(x), x \in E\} \subseteq E$.*

Théorème 3.2 *Les seuls ensembles de $\mathbb{Z}$ stables par combinaison linéaire sont les $a\mathbb{Z} = \{at, t \in \mathbb{Z}\}$, $a \in \mathbb{N}$.*

Preuve
• $a\mathbb{Z} = (-a)\mathbb{Z}$
• $a\mathbb{Z}$ est stable par combinaison linéaire, en particulier $0 \in a\mathbb{Z}$, et si $k \in a\mathbb{Z}$, alors $-k \in a\mathbb{Z}$
• Montrons que si H est un sous-ensemble non vide de $\mathbb{Z}$ stable par combinaison linéaire, alors il existe $a \in \mathbb{N}$ tel que $H = a\mathbb{Z}$.
– si $H = \{0\}$, alors $H = 0\mathbb{Z}$
– sinon, $\forall x \in H$ comme H est stable par combinaison linéaire, x et -x sont dans H. Il existe donc un plus petit $a \in \mathbb{N}_*$ tel que $a \in H$. $\forall x \in H, \exists (q, r) \in \mathbb{Z}^2$ tel que $x = a.q + r$ et $0 \leq r < a$. La stabilité par combinaison linéaire de H fait que $a\mathbb{Z}$ est inclus dans H et $r = x - aq \in H$. la minimalité de a fait que $r = 0$, c'est-à-dire que x est un multiple de a. □

4 Plus Grand Commun Diviseur

Théorème 4.1 (PGCD) *Soient a et b deux entiers relatifs dont l'un au moins est non nul. L'ensemble des diviseurs communs à a et b, qui est $D_{\mathbb{Z}}(a, b) = D_{\mathbb{Z}}(a) \cap D_{\mathbb{Z}}(b)$, possède un $\leq$ plus grand élément positif, appelé le Plus Grand Commun Diviseur de a et b. On le note $PGCD(a, b)$ ou $a \wedge b$. Donc $a \wedge b = |a| \wedge |b|$.*

Preuve : L'intersection des ensembles de diviseurs n'est pas vide car elle contient 0. Puisque l'un des entiers est non nul, son ensemble de diviseurs est fini, donc l'intersection des ensembles de diviseurs est une partie non vide et finie de $< \mathbb{Z}, \leq >$, elle admet donc un plus grand élément positif. □

$b|a \Leftrightarrow b \wedge a = |b|$.

4.1 Détermination de $a \wedge b$

Théorème 4.2 (Egalité de Bachet-Bezout) *Soit a et b deux entiers relatifs non tous les deux nuls. $a \wedge b$ peut s'exprimer comme une combinaison linéaire de a et b, c'est-à-dire qu'il existe deux entiers u et v satisfaisant*

$$d = au + bv$$

Autrement dit :

$$(a \wedge b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$

Preuve non constructible :
• Soit $H = a\mathbb{Z} + b\mathbb{Z}$, H est une partie de $\mathbb{Z}$ stable par combinaison linéaire, donc $\exists d \in \mathbb{N}_*$ tel que $H = d\mathbb{Z}$ puisque au moins a ou b est non nul. $d \in H$, donc $\exists u, v \in \mathbb{Z}$ tels que $d = au + bv$ par définition de H.
• d est un diviseur commun à a et b car $a, b \in H$ donc $\exists \alpha, \beta \in \mathbb{Z}$ tels que $a = \alpha d$ et $b = \beta d$.
• Montrons que d est le plus grand diviseur commun. Soit $c \in \mathbb{Z}$, un diviseur commun quelconque à a et b. Montrons que c'est un diviseur de d. $\exists a', b' \in \mathbb{Z}$ tels que $a = ca'$ et $b = cb'$. Donc $d = au + bv = ca'u + cb'v = c(a'u + b'v)$, c'est-à-dire $c|d$. Donc $d = a \wedge b$ □

La résolution effective repose sur l'algorithme[1] d'Euclide, qui permet de trouver et le $PGCD(a, b)$ et puis par substitution en remontant les calculs l'expression de ce PGCD comme combinaison linéaire de a et b.

```
données : a et b deux entiers non nuls
résultat : PGCD(a, b)
variable A, B, Q, R
traitement
A:= sup(a,b)
B:=inf(a,b)
Q:= DIV(a,b)
R:=A-BQ
TANT QUE R strictement supérieur à 0 FAIRE
A:=B (remplacer le contenu de A par le contenu de B)
B:=R (remplacer le contenu de B par le contenu de R)
Q:=DIV(A,B)
R:= A-QB
FIN TANT QUE
AFFICHER B
```

[1]Nous donnons des représentations des algorithmes le plus proche des méthodes manuelles, sans aucune considération de performance.

Table 3: déroulement du calcul de $1492 \wedge 1066$ par la méthode d'Euclide

	a	q	b	r
i=0	1492	1	1066	426
i=1	1066	2	426	214
i=2	426	1	214	212
i=3	214	1	212	2
i=4	212	106	2	0

Remarquons[2] que $r_i = a_i - b_i q_i$ soit

$$r_i = r_{i-2} - q_i r_{i-1} \quad \text{en notant} \quad r_{-1} = b \quad \text{et} \quad r_{-2} = a.$$

La lecture de la Table 3 nous permet d'écrire :
(a) $2[= r_3] = 214[= r_1] - 1[= q_3].212[= r_2]$
(b) $212[= r_2] = 426[= r_0] - 1[= q_2].214[= r_1]$
(c) $214[= r_1] = 1066[= r_{-1}] - 2[= q_1].426[= r_0]$
(d) $426[= r_0] = 1492[= r_{-2}] - 1[= q_0].1066[= r_{-1}]$

En reprenant les égalités du bas vers le haut et en faisant les substitutions, on trouve successivement :
(d) $426 = 1492 - 1066$
(c) avec (d) $214 = 1066 - 2(1492 - 1066) = 3.1066 - 2.1492$
(b) avec (c) et (d) $212 = 426 - 214 = -4.1066 + 3.1492$
(a) avec (b) et (c) $2 = 214 - 212 = 7.1066 - 5.1492$.

Les coefficients u et v peuvent aussi être calculer en remarquant que : $r_1 = a - bq_1 \in a\mathbb{Z}+b\mathbb{Z}$, $r_2 = b - r_1 q_2 \in a\mathbb{Z}+b\mathbb{Z}$, donc par récurrence, on montre que si $r_{k+1} = r_{k-1} - q_{k+1} r_k$, alors on peut écrire $r_k = au_k + bv_k$.
En substituant, on obtient

$$r_{k+1} = r_{k-1} - q_{k+1} r_k = (au_{k-1} + bv_{k-1}) - q_{k+1}(au_k + bv_k) = a(u_{k-1} - q_{k+1}u_k) + b(v_{k-1} - q_{k+1}v_k)$$

Par identification, on déduit que les suites (u_k) et (v_k) satisfont la même relation de récurrence que (r_k) : $u_{k+1} = u_{k-1} - q_{k+1}u_k$ et $v_{k+1} = v_{k-1} - q_{k+1}v_k$. Les coefficients cherchés sont u_{n-1} et v_{n-1}.

En posant :
$r_{-1} = a$, $u_{-1} = 1$ et $v_{-1} = 0$, on obtient $a = b.0 + a$,
$r_0 = b$, $u_0 = 0$ et $v_0 = 1$, on obtient $b = a.0 + b$
soit l'initialisation des suites. En translatant les indices, on obtient l'algorithme de Bezout

```
données : a et b deux entiers non nuls
résultat : u, v tels que au+bv=PGCD(a,b)
variables : R1:=a ; U1:=1 ; V1:=0 ; R2:=b ; U2:=0 ; V2:=1 ; Q ;
traitement
```

[2]On peut toujours commencer une récurrence sur un nombre négatif.

```
 FAIRE
------ les calculs
Q:=DIV(R1,R2)
R:= R1-Q.R2
U:= U1-Q.U2
V:=V1-Q.V2
----- les incrémentations
R1:= R2 ; R2:= R
U1:= U2 ; U2:= U
V1:= V2 ; V2:= V
JUSQU'A R=0
AFFICHER R1= a U1 +b V1
```

Table 4: Déroulement du calcul des coefficients de$1492 \wedge 1066$ par la méthode de Bezout

	Q	R	U	V	R1	R2	U1	U2	V1	V2
i=0	-	-	-	-	1492	1066	1	0	0	1
i=1	1	426	1	-1	1066	426	0	1	1	-1
i=2	2	214	-2	3	426	214	1	-2	-1	3
i=3	1	212	3	-4	214	212	-2	3	3	-4
i=4	1	2	-5	7	212	2	3	-5	-4	7
i=5	106	0	inutile	inutile	2	inutile	-5	inutile	7	inutile

C'est-à-dire $2 = 1492.(-5) + 1066(7)$.

Corollaire 4.3 (Théorème de Bezout) *Deux entiers a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que $au + bv = 1$. Autrement dit si et seulement si tout entier peut s'exprimer comme combinaison linéaire entière de a et b.*

$$a \wedge b = 1 \Longleftrightarrow a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$$

Théorème 4.4 (de Gauss) *Soit $a, b, c \in \mathbb{N}_*$,*

$$[(a \mid bc) \quad et \quad (a \wedge b = 1)] \Rightarrow (a \mid c)$$

Nouvelle preuve. Si $a \wedge b = 1$ alors, d'après le théorème de Bezout, $\exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$, donc $c = auc + bvc$. Or $a|bc \quad$ et $\quad a|a$ donc par combinaison linéaire $a|c$. □