Arithmétique des entiers relatifs

Lycée Berthollet, MPSI1 2023-24

!!! RÉSUMÉ DE COURS EN TRAVAUX !!!

I Divisibilité

1 Relation de divisibilité

Définition : pour $a, b \in \mathbb{Z}$, $a|b$ ss'il existe $k \in \mathbb{Z}$ tel que $ak = b$.

On remarque en particulier que tout entier divise 0 et que -1 et 1 divisent tout entier.

Propriétés de cette relation binaire : réflexivité et transitivité sur $\mathbb{Z}$, pas d'antisymétrie, mais presque : deux entiers sont *associés* (*i.e.* codivisibles) ss'il sont égaux au signe près.

Conséquence : la divisibilité sur $\mathbb{N}$ est une relation d'ordre non total, admettant un plus petit élément (1) et un plus grand élément (0).

Lien avec les lois de $\mathbb{Z}$:

— si $d|a$ et $d|b$, alors d divise toute combinaison linéaire entière de a et b ;

— si $a|b$ et $c|d$, alors $ac|bd$.

2 Division euclidienne

Théorème 1 $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^\star, \exists\,!(q,r) \in \mathbb{Z} \times [\![0, |b|-1]\!],\ a = bq + r.$

Définition 2 Avec les notations du théorème, l'écriture $a = bq + r$ s'appelle la *division euclidienne* de a par b, l'entier relatif q s'appelle le *quotient* de cette division euclidienne et l'entier naturel r s'appelle le *reste* de cette division euclidienne.

Démonstration: Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$. On montre d'abord l'existence du couple (q,r) convenant, puis son unicité.

Soit $A = (a - b\mathbb{Z}) \cap \mathbb{N}$. Montrons que $A \neq \emptyset$. Soit $x = a + |ab|$. Tout d'abord, $\pm|a| \in \mathbb{Z}$, donc $x \in a - b\mathbb{Z}$. De plus, x est clairement entier. Enfin, en multipliant par $|a| \geq 0$ l'inégalité $|b| \geq 1$, $|ab| \geq |a|$, donc $x \geq a + |a| \geq 0$, donc $x \in \mathbb{N}$. Ainsi $x \in A$.

Comme A est une partie non vide de $\mathbb{N}$, elle admet un plus petit élément qu'on note r. Par définition de A, il existe alors $q \in \mathbb{Z}$ tel que $r = a - bq$. On a donc trouvé $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$. Montrons alors par l'absurde que $r \leq |b| - 1$. Si tel n'etait pas le cas, on aurait $r \geq |b|$ et en posant $r' = r - |b| = a - b(q \pm 1)$, on obtiendrait un élément de A strictement plus petit que r, ce qui contredit le fait que $r = \min A$. Le couple (q,r) convient donc.

Supposons maintenant qu'on ait un autre couple (q',r') convenant. Alors $bq'+r' = a = bq+r$, donc $b(q'-q) = r-r'$. Ainsi $b|r-r'$. Cependant, comme $r,r' \in [\![0,|b|-1]\!]$, $|r-r'| \leq |b|-1$, donc $r-r' = 0$, *i.e.* $r = r'$. Puis, $b(q'-q) = 0$ et comme $b \neq 0$, $q = q'$. □

Cette démonstration n'utilise que les entiers. Si on utilisait $\mathbb{R}$ et les conséquences de la propriété de la borne supérieure, on aurait accès aux fonctions parties entières, qui permettraient une démonstration plus directe. En tout état de cause, il est utile de connaître le résultat suivant.

Proposition 3 *Avec les notations précédentes, on a,* ***dans le cas où*** $b > 0$*,*

$$q = \left\lfloor \frac{a}{b} \right\rfloor \quad \text{et} \quad r = a - b\left\lfloor \frac{a}{b} \right\rfloor.$$

Démonstration: On note $q' = \left\lfloor \frac{a}{b} \right\rfloor$ et $r' = a - b\left\lfloor \frac{a}{b} \right\rfloor$. On a bien $q' \in \mathbb{Z}$. D'après la définition de la partie entière inférieure, $q' \leq \frac{a}{b} < q'+1$, donc $0 \leq \frac{a}{b} - q' < 1$ et, en multipliant par $b > 0$, $0 \leq r' < b$. Comme r' est clairement entier, $r' \in [\![0, b-1]\!]$. Par l'unicité prouvée dans le théorème, $(q',r') = (q,r)$. □

II Diviseurs et multiples communs

1 Cas des entiers naturels

On ne considère ici que des entiers naturels et on rappelle que la divisibilité est une relation d'ordre sur $\mathbb{N}$.

On commence par introduire une notation **non universelle**, mais pratique :

Définition 4 Pour $a,b \in \mathbb{N}$, on note $\mathrm{CD}(a,b)$ l'ensemble de leurs *diviseurs communs*, c'est à dire l'ensemble des entiers naturels qui divisent à la fois a et b.

Remarquons que $\mathrm{CD}(b,a) = \mathrm{CD}(a,b)$.

On a alors le résultat fondateur de l'algorithme d'Euclide à venir :

Lemme 5 *(Lemme clé de l'algorithme d'Euclide.)*
Soient $(a,b) \in \mathbb{N} \times \mathbb{N}^\star$ et r le reste de la division euclidienne de a par b. Alors,

$$\mathrm{CD}(a,b) = \mathrm{CD}(b,r).$$

Démonstration: Soit $d \in \mathrm{CD}(a,b)$. Il divise toute combinaison linéaire entière de a et b et en particulier $a - bq = r$, où q désigne le quotient de la division euclidienne de a par b. Comme $d|b$ par hypothèse, alors $d \in \mathrm{CD}(b,r)$.

Réciproquement, si $d \in \mathrm{CD}(b,r)$ il divise b et $bq+r = a$, donc $d \in \mathrm{CD}(a,b)$. □

On décrit maintenant l'algorithme d'Euclide. Il prend en entrée $a,b \in \mathbb{N}$ et coniste en la construction d'une suite finie r_{-1}, r_0,..., r_N, r_{N+1} d'entiers naturels définie par récurrence de la manière suivante :

— Initialisation : on pose $r_{-1} = a$ et $r_0 = b$.
— Hérédité : supposant avoir construit jusqu'au terme r_k, pour un certain $k \in \mathbb{N}$:
  — si $r_k = 0$, on s'arrête et on pose $N = k-1$;

— sinon, on note r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k.

La terminaison de cet algorithme est assurée car la suite $(r_k)_{k\geq 0}$ est une suite d'entiers naturels strictement décroissante (par définition de la division euclidienne) et ne peut donc pas être infinie. On a alors $r_{N+1} = 0$.

En utilisant le lemme clé précédent et une récurrence immédiate, on a alors

$$\mathrm{CD}(a,b) = \mathrm{CD}(r_{-1},r_0) = \mathrm{CD}(r_0,r_1) = \ldots = \mathrm{CD}(r_N,r_{N+1}) = \mathrm{CD}(r_N,0).$$

Or $\mathrm{CD}(r_N,0)$ est l'ensemble des diviseurs de r_N, puisque tout entier naturel divise 0, donc cet ensemble admet r_N comme plus grand élément pour l'ordre de la divisibilité.

On a donc prouvé le

Théorème 6 *(Existence du PGCD et son calcul par l'algorithme d'Euclide)*

Pour tous $a,b \in \mathbb{N}$, l'ensemble $\mathrm{CD}(a,b)$ de leurs diviseurs (positifs) communs possède un plus grand élément au sens de la divisibilité, qu'on note $a \wedge b$ et qu'on appelle le PGCD (plus grand commun diviseur) de a et b.

De plus, $a \wedge b$ est l'avant-dernier reste obtenu dans l'algorithme d'Euclide. Dans le cas où $(a,b) \neq (0,0)$, il est non nul et c'est donc le "dernier reste non nul" de l'algorithme.

Remarque 7 Comme $\mathrm{CD}(b,a) = \mathrm{CD}(a,b)$, il s'ensuit que $b \wedge a = a \wedge b$.

Exemple 8 Pour $a = 468$ et $b = 3939$, l'algorithme d'Euclide donne

$$\begin{aligned} 468 &= 3939 \times 0 + 468, \\ 3939 &= 468 \times 8 + 195, \\ 468 &= 195 \times 2 + 78, \\ 195 &= 78 \times 2 + 39, \\ 78 &= 39 \times 2 + 0. \end{aligned}$$

La suite $(r_k)_{k=-1}^{N+1}$ est ici : $(468, 3939, 468, 195, 78, 39, 0)$. On en déduit que $468 \wedge 3939 = 39$.

Remarquez qu'il n'est pas nécéssaire de commencer l'algorithme d'Euclide avec $a \geq b$ (cela a son intérêt pour une implémetation courte en Python par exemple). Cependant, lorsqu'on exécute cet algorithme à la main, la première ligne de l'algorithme ci-dessus est inutile.

Remarquons aussi le

Lemme 9 *(Lien entre divisibilité et ordre usuel)*

Si $n \in \mathbb{N}^\star$, tout diviseur de n est inférieur ou égal à n au sens de l'ordre usuel.

Démonstration: Soit $n \in \mathbb{N}^\star$, et $d \in \mathbb{Z}$ un de ses diviseurs. Il existe $k \in \mathbb{Z}$ tel que $dk = n$ et $k \neq 0$ car $n \neq 0$. Comme $1/k \leq 1$ (soit car $k \geq 1$, soit car $k < 0$), en multipliant par $n > 0$, $d = n/k \leq n$. □

qui permet une interprétation (restreinte) du PGCD en terme de l'ordre usuel :

Proposition 10 *(PGCD et ordre usuel)*

Pour $(a,b) \in \mathbb{N}^2 \setminus \{(0,0)\}$, $a \wedge b$ est aussi le plus grand des diviseurs communs de a et b au sens de l'ordre usuel.

Remarque 11 Cela n'est pas le cas pour $a = b = 0$, puisque 0 n'est pas le plus grand élément de $\mathbb{N}$ pour l'ordre usuel.

Par ailleurs, lors de l'algorithme d'Euclide effectué sur a et b , on voit facilement que tous les r_k s'écrivent comme combinaisons linéaires entières (*i.e.* à coefficients entiers **relatifs**) de a et b, par récurrence double finie rapide : c'est trivialement le cas pour a et b eux mêmes et si c'est le cas pour r_{k-2} et r_{k-1}, comme r_k s'écrit comme combinaison linéaire entière de r_{k-2} et r_{k-1} par la division euclidienne de reste r_k, alors il s'écrit aussi comme combinaison linéaire entière de a et b. En particulier, c'est le cas de $r_N = a \wedge b$ et on a la

Proposition 12 *(Relation de Bézout dans $\mathbb{N}$)*

$$\forall a, b \in \mathbb{N}, \exists u, v \in \mathbb{Z}, \quad a \wedge b = au + bv.$$

Remarque 13 Les coefficients u et v ne sont pas uniques. On peut voir facilement qu'il existe en fait une infinité de relations de Bézout possibles.

La méthode précédente à partir de l'algorithme d'Euclide nous en fournit une.

L'obtention de cette relation de Bézout en même temps que le calcul du PGCD est appelé *algorithme d'Euclide étendu*. On le décrit un peu plus précisément.

Pour cela on introduit des notations ;

— on note q_k ($1 \leq k \leq N+1$) le quotient de la division euclidienne de r_{k-2} par r_{k-1} qui s'écrit alors

$$r_{k-2} = r_{k-1} q_k + r_k ;$$

— on note, à chaque étape, u_k et v_k les coefficients de la combinaison linéaire entière de a et b obtenue qui vaut r_k.

L'algorithme d'Euclide étendu est alors celui-ci :

1. Initialisation : $r_{-1} = a,\ u_{-1} = 1,\ v_{-1} = 0$ et $r_0 = b,\ u_0 = 0,\ v_0 = 1$ et $k = 0$
2. Boucle : tant que $r_k \neq 0$,
   — $k \leftarrow k+1$
   — Calculer q_k et r_k en faisant la division euclidienne de r_{k-2} par r_{k-1}
   — Calculer $u_k = u_{k-2} - q_k u_{k-1}$ et $v_k = v_{k-2} - q_k v_{k-1}$
3. Résultat (k vaut alors $N+1$) : renvoyer $r_{k-1} = a \wedge b$ et $u_{k-1} = u,\ v_{k-1} = v$ qui vérifient $au + bv = a \wedge b$.

Lors de l'exécution, on voit que pour calculer les données du rang k, on n'a plus besoin de celles des rangs inférieurs à $k-2$, donc il est totalement inutile de stocker toutes les données, contrairement à la méthode usuelle de "remontée" de l'algorithme d'Euclide pour trouver une relation de Bézout. Voici une implémentation en Python de cet algorithme :

```
def EuclideEtendu(a,b):
    up,vp,u,v = 1,0,0,1
    while b!=0:
        q = a//b
        a,b = b,a%b
        up,u = u,up-q*u
        vp,v = v,vp-q*v
    return a,up,vp
```

Pour le calcul à la main, il est recommandé de présenter les résultats dans un tableau :

EXEMPLE A FAIRE !!!!!!!!!!!!!

On peut aussi, surtout dans les petits cas, effectuer une "remontée" de l'agorithme d'Euclide classique, ce qui donne, pour les mêmes nombres :

EXEMPLE A FAIRE !!!!!!!!!!!!!

2 Cas des entiers relatifs

Définition 14 Pour $a, b \in \mathbb{Z}$, on appelle PGCD de a et b le nombre

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

Proposition 15 *(Caractérisation)*

Pour tous $a, b \in \mathbb{Z}$ et $d \in \mathbb{N}$, $d = a \wedge b$ si, et seulement si, les deux conditions suivantes sont réalisées :

1. *d divise a et b ;*
2. *tout diviseur commun de a et b divise d.*

Démonstration: Adaptation facile du cas des entiers naturels. □

Remarque 16 Lorsque $(a,b) \neq (0,0)$, $a \wedge b$ est encore le plus grand des diviseurs (relatifs) communs de a et b au sens de l'ordre usuel.

La proposition suivante se déduit immédiatement du cas des entiers naturels :

Proposition 17 *(Relation de Bézout dans $\mathbb{Z}$)*

$$\forall a, b \in \mathbb{Z}, \exists u, v \in \mathbb{Z}, \quad a \wedge b = au + bv.$$

On par ailleurs la proposition utile :

Proposition 18

$$\forall a, b \in \mathbb{Z},\ \forall k \in \mathbb{Z}^\star, \quad (ka) \wedge (kb) = |k|\,(a \wedge b).$$

Démonstration: A FAIRE ! □

3 Nombres premiers entre eux

Définition, théorème de Bézout, théorème de Gauss, théorème de divisibilité par un produit lorsque deux facteurs divisent un même nombre et sont premiers entre eux, le produit de deux nombres premiers avec un entier donné est encore premier avec cet entier, forme irréductible des nombres rationnels : existence et unicité.

4 PGCD de plus de deux entiers

Cas de trois entiers naturels

On remarque que les diviseurs naturels communs de $a, b, c \in \mathbb{N}$ sont les diviseurs de $(a \wedge b) \wedge c$, donc ce dernier est le plus grand des diviseurs communs de a, b, c au sens de la divisibilité. On l'appelle le PGCD de a, b et c. On voit par un raisonnement analogue que ce plus grand diviseur commun est aussi $a \wedge (b \wedge c)$.

Cela prouve que l'opération $\wedge$ est associative sur $\mathbb{N}$ et justifie la notation $a \wedge b \wedge c$.

Remarque : cette loi est aussi commutative et admet pour élément neutre 0. On dit que $(\mathbb{N}, \wedge)$ est un monoïde commutatif unitaire.

Cas de n entiers naturels

Par récurrence immédiate, l'ensemble des diviseurs communs de $a_1, ..., a_n$ possède un plus grand élément pour la divisibilité qui est

$$\bigwedge_{i=1}^{n} a_i = a_1 \wedge a_2 \cdots \wedge a_n,$$

nombre bien défini par associativité de $\wedge$ qu'on appelle le PGCD de a_1,...,a_n.

Cas de n entiers relatifs

Le PGCD de a_1,...,a_n est

$$\bigwedge_{i=1}^{n} a_i = \bigwedge_{i=1}^{n} |a_i| .$$

Proposition 19 *(Caractérisation)*
Pour tous $a_1, ..., a_n \in \mathbb{Z}$ et $d \in \mathbb{N}$, $d = \bigwedge a_i$ si, et seulement si, les deux conditions suivantes sont réalisées :

1. *d divise tous les a_i ;*
2. *tout diviseur commun des a_i divise d.*

Démonstration: Adaptation facile du cas de deux entiers relatifs. □

Remarque 20 Lorsque $(a_1, ..., a_n) \neq (0, ..., 0)$, $\bigwedge a_i$ est le plus grand des diviseurs (relatifs) communs des a_i au sens de l'ordre usuel.

La proposition suivante se déduit par une simple récurrence :

Proposition 21 *(Relation de Bézout pour n entiers)*

$$\forall a_1, ..., a_n \in \mathbb{Z}, \exists u_1, ..., u_n \in \mathbb{Z}, \quad \bigwedge_{i=1}^{n} a_i = \sum_{i=1}^{n} a_i u_i.$$

Définition des nombres premiers entre eux deux à deux et des nombres premiers entre eux dans leur ensemble ($\bigwedge a_i = 1$)
La première est (beaucoup) plus forte que la seconde : il suffit d'avoir deux des a_i premiers entre eux pour que les a_i soient premiers entre eux dans leur ensemble.

Proposition 22 *(Théorème de Bézout pour n entiers)*

$$\forall a_1, ..., a_n \in \mathbb{Z}, \left(\bigwedge_{i=1}^{n} a_i = 1 \iff \left(\exists u_1, ..., u_n \in \mathbb{Z}, \sum_{i=1}^{n} a_i u_i = 1 \right) \right).$$

5 PPCM

Définition dans $\mathbb{N}$ comme le plus petit des multiples commun au sens de la divisibilité, notation $a \vee b$.

Définition dans $\mathbb{Z}$ comme le PPCM des valeurs absolues.

Remarque que c'est aussi, pour $a \neq 0$ et $b \neq 0$, le plus petit multiple commun strictement positif au sens de l'ordre usuel.

Caractérisation du PPCM comme étant entier naturel, multiple commun et divisant tout multiple commun.

Relation

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

Formule du PPCM des produits de a et b par un même nombre.

III Nombres premiers

1 Définition et premières propriétés

Définition.

Exemple d'application du crible d'Ératosthène.

Les entiers relatifs premiers à un p premier donné sont ceux non divisibles par p. Pour les autres, leur PGCD avec p est p. Lemme d'Euclide : si un premier p divise un produit, il divise l'un des deux facteurs.

Rappel des deux résultats vus en début d'année :

— existence de la décomposition d'un naturel non nul en produit de nombres premiers ;

— infinitude de l'ensemble $\mathcal{P}$ des nombres premiers.

2 Décomposition en facteurs premiers

Unicité de cette décomposition à l'ordre près. Formalisation de la décomposition à l'aide d'un produit infini et des valuations p-adiques, appelée factorisation première. Théorème sur les propriétés des valuations p-adiques : valuation p-adique d'un produit, traduction de la divisibilité en termes de valuations, expression du PGCD et du PPCM à l'aide des valuations.

IV Congruences

Définition, propriétés : relation d'équivalence, compatibilité avec la somme et le produit, si $m \in \mathbb{N}^\star$, alors $a \equiv a'[n] \iff am \equiv a'm[nm]$. Toutes ces propriétés sont à (re)démontrer en exercice sauf la compatibilité avec le produit qu'on démontre :

Démonstration: Soient $n \in \mathbb{N}^\star$ et $a, a', b, b' \in \mathbb{Z}$ tels que $a \equiv a'[n]$ et $b \equiv b'[n]$.

Alors $a'b' - ab = a'(b' - b) + (a' - a)b$ est une combinaison linéaire à coefficuents entiers de $b' - b$ et $a' - a$, tous deux divisibles par n, donc elle est elle-même divisible par n, *i.e.* $a'b' \equiv ab\ [n]$. □

En exercice : pour a entier, l'existence de $b \in \mathbb{Z}$ tel que $ab \equiv 1\ [n]$ équivaut à ce que $a \wedge n = 1$.

Petit théorème de Fermat (on prouve par récurrence sur a que $a^p \equiv a[p]$ puis on utilise Bézout pour simplifier par a lorsque $p \not| a$.)

On utilise au passage le lemme : pour p premier et $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.