Arithmétique dans Z

Dans ce chapitre, « entier » signifie « élément de Z », et « entier naturel » ou « entier positif » « élément de N ».

Rappel : la relation de divisibilité est une relation d’ordre sur N (mais pas sur Z).

* 1. Diviseurs communs à deux entiers

Pour tous entiers *a* et *b*, notons  l’ensemble des diviseurs communs de *a* et *b* dans Z. On remarque tout de suite que , et en dehors de ce cas, c'est-à-dire lorsque , l’ensemble  ne contient pas 0, est symétrique par rapport à 0, est fini et est aussi égal à . C’est la raison pour laquelle, en pratique, on ne recherche que les diviseurs communs positifs de deux entiers positifs non tous deux nuls. Mais, afin de conserver la généralité des énoncés, nous n’allons pas, pour le cours, nous limiter aux entiers positifs.

* + 1. PGCD et algorithme d’Euclide

Etant donnés deux entiers *a* et *b*, avec , on cherche à déterminer l’ensemble  des diviseurs communs de *a* et *b*.

Remarque essentielle :

Pour tout entier *q*, on a l’égalité : .

En particulier, si on suppose , la division euclidienne de *a* par *b* donne :  avec , et on a alors 

D’où l’algorithme suivant :

On note .

Si , la division euclidienne de  par  donne  avec 

Si , la division euclidienne de  par  donne  avec 

Si , la division euclidienne de  par  donne  avec 

…Si , la division euclidienne de  par  donne  avec 

On s’arrête quand on obtient un reste nul, ce qui se produit nécessairement, sinon la suite  formerait une suite strictement décroissante d’entiers naturels, ce qu’on sait impossible.

Il existe donc  tel que  est défini est non nul, mais le reste suivant, c'est-à-dire  est nul. Alors, compte tenu de la remarque précédente :



Or,  est évidemment l’ensemble des diviseurs de .

Ainsi, l’ensemble des diviseurs communs à *a* et *b* est égal à l’ensemble des diviseurs de . Donc  est un diviseur commun positif à *a* et *b*, et tout diviseur commun à *a* et *b* divise . Donc  est le plus grand, au sens de la relation de divisibilité, des diviseurs communs positifs de *a* et *b*.

Théorème, définition :

Soient *a*, *b* deux entiers non tous deux nuls.

1. L’ensemble des diviseurs communs positifs de *a* et *b* admet un plus grand élément, au sens de la divisibilité (et aussi au sens de ). On l’appelle le plus grand diviseur commun (PGCD) de *a* et *b*, noté  ou .
2. Le PGCD de *a* et *b* est par conséquent l’unique entier  tel que :

 est un diviseur commun positif à *a* et *b*, et tout diviseur commun à *a* et *b* divise .

1. Avec l’algorithme d’Euclide, le PGCD de *a* et *b* est le dernier reste non nul.

Exemple :

L’algorithme d’Euclide appliqué à  et  donne :

 donc .

Définition :

Soient *a*, *b* deux entiers.

On dit que *a* et *b* sont premiers entre eux lorsque les seuls diviseurs communs de *a* et *b* sont -1 et 1. Autrement dit, lorsque  et .

Proposition :

Soient *a* et *b* deux entiers non nuls, et soit .

Si on pose  et , alors  et  sont premiers entre eux.

En effet, si  et  avaient un diviseur commun , alors  serait un diviseur commun à *a* et *b* strictement supérieur à .

* + 1. Egalité de Bézout

Théorème :

Soient *a* et *b* deux entiers non tous deux nuls. On a alors l’équivalence :



Démonstration :

Le sens  est immédiat, puisque si *d* divise *a* et *b*, il divise  pour tous  de Z, et donc divise 1.

Pour l’autre implication, on reprend ici les notations de l’algorithme d’Euclide : en particulier, *n* est l’élément de N tel que .

Montrons par récurrence (sur *k*) que pour tout *k* entre 0 et , il existe  et  dans Z tels que 

* Déjà, le résultat est vrai pour  et  :

 et  (selon les signes)

* Soit , supposons que le résultat est vrai pour  et *k*.

On a :  et . Si on retranche  fois la deuxième égalité de la première, on obtient :

, c'est-à-dire :

 avec :  et .

Ce qui achève la récurrence.

Ainsi, avec , on a  et  dans Z tels que .

Si , on a donc bien l’existence de *u* et *v* comme voulus, puisque .

Exemple :

Avec  et  :



. Or, , donc  donne :

. Or, , donc  donne :

. Or, , donc  donne :

.

Remarque :

La récurrence précédente est valable quelle que soit la valeur de , et cela montre que si , alors il existe *u*, *v* dans Z tels que . (La réciproque est fausse). Mais ce dernier résultat est aussi clair en multipliant par  les deux membres de l’égalité de Bézout appliquée aux entiers  et  tels que  et , puisque ceux-ci sont premiers entre eux.

* + 1. Le théorème de Gauss et autres propriétés

Proposition :

Pour tous entiers *a*, *b* non tous deux nuls, .

(Evident, puisque l’ensemble des diviseurs communs à *a* et *b* est évidemment celui des diviseurs communs à *b* et *a*!)

Proposition :

Pour tous entiers *a*, *b* non tous deux nuls, et tout entier *c* non nul :



Démonstration :

Notons . On a vu qu’il existe  tels que . Donc , et donc tout diviseur commun à  et  divise . De plus,  est évidemment un diviseur commun à  et , donc  est bien le PGCD de  et .

Corollaire :

Soient *a* et *b* deux entiers non tous deux nuls, et soit *d* un diviseur commun à *a* et *b*

Si on pose  et , alors  est le PGCD de *a* et *b* si et seulement si .

En effet :

On a  d’où on tire immédiatement l’équivalence.

Théorème (Gauss) :

Soient trois entiers *a*, *b*, *c*.

Si *c* divise le produit , et si *c* est premier avec *b*, alors *c* divise *a*.

Démonstration :

Si , le résultat est évident, sinon on peut écrire . Mais comme *c* divise  et , il divise leur PGCD, c'est-à-dire *a*.

Théorème :

Soient trois entiers *a*, *b* et *c*. Si *a* est premier avec *b* et avec *c*, alors *a* est premier avec .

Démonstration :

Selon l’une des implications du théorème de Bézout, il existe des entiers relatifs  tels que  et . En multipliant, on a alors :

, d’où le résultat par l’autre implication du théorème de Bézout.

On en déduit alors la proposition suivante par récurrence :

Proposition :

Si *a* est premier avec *n* nombres () , alors *a* est premier avec leur produit.

En effet, pour , c’est le résultat précédent, et si c’est vrai pour , alors *a* est premier avec le produit  et avec , donc est premier avec  selon le résultat précédent.

Il en résulte :

Proposition :

Si *a* et *b* sont premiers entre eux, alors, pour tous entiers naturels *m* et *p*,  et  sont premiers entre eux.

En effet, en supposant *m* et *p* non nuls (sinon c’est évident), et en appliquant le résultat précédent avec *a* et , on obtient , puis en appliquant encore ce résultat avec  et , on obtient .

Théorème :

Soient trois entiers *a*, *b*, *c*.

Si *b* et *c* sont premiers entre eux et divisent *a*, alors  divise *a*.

Démonstration :

*a* s’écrit , *c* divise  et est premier avec *b* donc, selon le théorème de Gauss, *c* divise , et finalement  divise *a*.

On en déduit par récurrence :

Proposition :

Si *a* est divisible par , et si les  sont premiers entre eux deux à deux, alors *a* est divisible par le produit des .

En effet, pour , c’est le résultat précédent, et si c’est vrai pour , alors *a* est divisible par  et par , mais comme  est premier avec chaque  pour , il est premier avec leur produit, donc *a* est divisible par  selon le résultat précédent.

Par exemple :

Si 20 et 9 divisent *a*, alors 180 divise *a*, mais si 10 et 18 divisent *a*, cela ne prouve pas que 180 divise *a* (*a* pourrait être 90).

Donnons pour finir la résolution classique de l’équation .

*a*, *b* et *c* sont trois entiers (*a* et *b* sont supposés non nuls), et on cherche les solutions  dans . Notons  le PGCD de *a* et *b*.

Si *c* n’est pas un multiple de , il n’y a pas de solutions (car  divise  pour tous *x*, *y* de Z).

Supposons maintenant que  avec .

Notre équation équivaut donc à l’équation , où  et  sont les nombres premiers entre eux tels que  et . Selon le théorème de Bézout, on peut trouver (et on connaît une méthode pour le faire) *u* et *v* dans Z tels que . On a donc une solution  à notre équation. On doit maintenant trouver les autres.

Soit  une autre solution. On a : 

Donc . Or,  est premier avec . Donc selon le théorème de Gauss, il divise . Il existe donc  tel que , et par remplacement on obtient .

Réciproquement, on remarque aisément que les couples  avec  sont bien solutions. Ils constituent donc l’ensemble des solutions.

* 1. PPCM

Proposition, définition :

Soient *a*, *b* deux entiers non nuls. L’ensemble des multiples communs strictement positifs de *a* et *b* admet un plus petit élément au sens de la divisibilité (donc aussi au sens de ). On l’appelle le plus petit multiple commun (PPCM) de *a* et *b*.

Démonstration :

L’ensemble des multiples communs à *a* et *b* (dans Z) est  qui est un sous-groupe de , donc du type , avec .  n’est pas nul car , qui est non nul, appartient à ce sous-groupe. Le générateur positif  est donc bien le plus petit multiple commun strictement positif, le sens « plus petit » étant pris pour la relation de divisibilité.

Proposition :

Soient *a* et *b* deux entiers positif non nuls. Alors , où  est la PGCD de *a* et *b* et  le PPCM.

Démonstration :

Posons , et  avec .

Alors  est un multiple commun à *a* et à *b*.

Soit maintenant *m* un multiple commun de *a* et *b*.

Alors , donc . Donc . Ainsi,  divise . Or,  est premier avec , donc  divise *x*. Ainsi, , donc , donc . Donc tout multiple de *a* et *b* est multiple de . Donc le plus petit multiple commun à *a* et *b* est , d’où l’égalité 

On notera que si *a* et *b* sont premiers entre eux, alors le PGCD vaut 1 et le PPCM vaut .

* 1. Les nombres premiers

On appelle nombre premier tout entier naturel, strictement supérieur à 1, dont les seuls diviseurs positifs sont 1 et lui-même.

Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41…

Le crible d’Eratosthène permet de prolonger cette liste.

Les résultats suivant s’obtiennent aisément :

1. Si *p* est premier, alors *p* est premier avec tout nombre qu’il ne divise pas.

En effet, pour tout entier *a*, le PGCD de *a* et *p* est un diviseur positif de *p*, donc vaut 1 ou *p*. Si ce n’est pas *p*, c’est 1.

Il en résulte que deux nombres premiers distincts sont toujours premiers entre eux.

1. Si  sont des nombres premiers distincts, et si pour tout *i*,  divise *a*, alors *a* est divisible par les produit des .

C’est en effet une application directe d’un résultat déjà vu, en remarquant que les  sont premiers entre eux deux à deux.

1. Si *p* est premier et divise un produit de facteurs, alors *p* divise l’un des facteurs.

En effet, sinon *p* serait premier avec chacun des facteurs, donc avec le produit.

(Le résultat est faux si *p* n’est pas premier, par exemple 4 divise  mais 4 ne divise ni 2 ni 6)

Théorème :

Tout entier naturel strictement plus grand que 1 se décompose de manière unique (à commutativité près) en produit (éventuellement réduit à un seul terme) de nombres premiers.

Démonstration :

Existence :

Supposons que l’ensemble *A* des entiers strictement supérieurs à 1 n’admettant pas de décomposition en facteurs premiers soit non vide : il admet donc un plus petit élément *a*. Cet élément *a* n’est pas premier car sinon  est une décomposition de *a* en facteurs premiers. Donc *a* s’écrit , avec  et . Mais comme *a* est le minimum de *A*, *b* et *c* ne sont pas éléments de *A*, et se décomposent donc en produit de facteurs premiers. Il en est donc de même pour *a*, ce qui mène donc à une contradiction.

Unicité :

Soit un entier naturel strictement plus grand que 1.

Supposons qu’on ait deux décompositions. Après avoir éventuellement complété avec des , on obtient , où les  et les  sont des entiers naturels (dont certains sont éventuellement nuls).

Ainsi, d’après le théorème de Gauss,  divise le membre de droite, mais est premier avec , donc divise , donc . De façon symétrique, . Donc , et on fait de même avec les autres puissances.

Théorème :

L’ensemble des nombres premiers est infini (démonstration connue depuis Euclide)

Démonstration :

En effet, soient  *n* nombres premiers.

Montrons qu’il en existe nécessairement un autre.

Soit *q* un diviseur premier du nombre  (il en existe un car ce nombre se décompose en facteurs premiers). Alors *q* est nécessairement différent de chaque , car , qui divise , ne peut évidemment pas diviser  (car sinon il diviserait 1). Ainsi, *q* est un nombre premier différent de chaque , d’où le résultat.

(Remarque : il se peut que )

Proposition :

Si  et , où les  sont des nombres premiers distincts (et les  sont éventuellement nuls), alors le PGCD de *a* et *b* est égal à  où  et le PPCM de *a* et *b* est égal à , où .

Par exemple :

 et .

Donc le PGCD vaut  et le PPCM vaut 

Cependant, rechercher le PGCD ou le PPCM en passant par la décomposition en facteurs premiers est inefficace pour des grands nombres, qu’on ne peut pas factoriser en temps raisonnable. Il est nettement préférable de déterminer le PGCD par l’algorithme d’Euclide.

Quelques repères historiques :

Euclide : 3ème siècle avant JC.

Eratosthène : 3ème siècle avant JC.

Bézout : 18ème siècle.

Gauss : début du 19ème siècle.