Chapitre 14 : ARITHMÉTIQUE DANS $\mathbb{Z}$

I Division euclidienne et divisibilité

I.1 Relation de divisibilité

Définition

Soit a et b dans $\mathbb{Z}$. S'il existe c dans $\mathbb{Z}$ tel que $b = ac$, on écrit $a|b$ et on dit que :

$*$ b est multiple de a $*$ a est un diviseur de b $*$ a divise b $*$ b est divisible par a

L'ensemble des multiples de a est : $a\mathbb{Z} = \{ac\}_{c\in\mathbb{Z}}$

L'ensemble des diviseurs de a est noté : div(a) = div$(|a|)$. Il contient toujours 1.

Pratique 1 :

1. A-t-on $2|6$ ou $6|2$? A-t-on $3|8$ ou $8|3$? Quels nombres divisent tous les autres ?

2. Donner div(0) et div(6).

Propriétés

1) La relation $|$ est une relation d'ordre sur $\mathbb{N}$; sur $\mathbb{Z}$ elle est réflexive et transitive mais n'est pas antisymétrique ($a|b$ et $b|a$ implique $a = \pm b$)

2) 0 est divisible par tout entier relatif mais ne divise que 0

3) Si $a \neq 0$, alors div$(a) \subset [\![-|a|, |a|]\!]$

4) Si $a|b$ et $a|c$ alors $a|(ub + vc)$ pour tous u et v dans $\mathbb{Z}$

5) Si $a|c$ et $b|d$ alors $ab|cd$. En particulier, si $a|b$ alors $a^k|b^k$ pour tout $k \in \mathbb{N}$.

1►

I.2 Division euclidienne

Théorème de la division euclidienne :

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que : $\boxed{a = bq + r \quad \text{et} \quad 0 \leqslant r < b}$

Dans cette division, a est le dividende, b le diviseur, q le quotient ($q = \lfloor \frac{a}{b} \rfloor$), et r le reste.

2►

$|$ b divise a si, et seulement si, le reste de la division de a par b est 0.

I.3 Une généralisation : l'écriture en base b

b désigne ici un naturel supérieur ou égal à 2.

THÉORÈME

Soit a un entier naturel non nul.

Il existe un unique entier naturel n et une unique famille $(a_k)_{k\in[\![0,n]\!]}$ tels que

$$a = \sum_{k=0}^{n} a_k b^k \quad \textit{et} \quad \forall k \in [\![0,n]\!],\ 0 \leqslant a_k \leqslant b-1 \quad \textit{et enfin} \quad a_n \neq 0$$

Cela constitue l'écriture de a en base b. On note aussi : $a = \overline{a_n a_{n-1} \dots a_1 a_0}^{\,b}$

3▶

Pratique 2 :

1. Écrire 19 en base 3. **2.** Quel entier s'écrit $\overline{141}^5$? **3.** Écrire 390 en base 16.

Application au calcul des puissances : **l'exponentiation rapide**

On calcule a^p en utilisant l'écriture de p en base 2 : $p = \sum_{i=0}^{n} p_i 2^i$

Alors : $a^p = \prod_{i=0}^{n} a^{p_i 2^i} = \prod_{\{i|p_i\neq 0\}} a^{2^i}$

Comme $a^{2^i} a^{2^i} = a^{2^{i+1}}$, il y a n multiplications pour disposer des a^{2^i} utiles, puis au plus n multiplications pour multiplier les puissances utiles et obtenir a^p.

En résumé, $2n$ multiplications au plus ($p-1$ dans le cas d'une multiplication naïve).

4▶

I.4 Congruences modulo un naturel

DÉFINITION

Soit $n \in \mathbb{N}$ et deux entiers relatifs a et b.

On dit que a est congru à b modulo n s'il existe un entier relatif k tel que : $a = b + kn$
ou encore si n divise $b - a$.

On écrit alors : $a \equiv b\ [n]$

PROPRIÉTÉS

n est un naturel, a, b, c, d sont des entiers relatifs.

1) Lien entre congruence modulo n et divisibilité par n : $n|a \iff a \equiv 0\ [n]$

2) La relation de congruence modulo n est une relation d'équivalence.

La classe d'équivalence de a est : $\{a + kn, k \in \mathbb{Z}\} = a + n\mathbb{Z}$

En particulier, $a \equiv b\ [n]$ signifie que a et b ont même reste dans la division euclidienne par n.

3) Compatibilité avec la somme : si $a \equiv c\ [n]$ et $b \equiv d\ [n]$ alors $a + b \equiv c + d\ [n]$

4) Compatibilité avec le produit : si $a \equiv c\ [n]$ et $b \equiv d\ [n]$ alors $ab \equiv cd\ [n]$.

En particulier, pour tout naturel k : si $a \equiv b\ [n]$ alors $a^k \equiv b^k\ [n]$

5) Multiplication et division par un entier naturel non nul m :

$$a \equiv b\ [n] \text{ si, et seulement si, } \ ma \equiv mb\ [mn]$$

5►

Pratique 3 :

1. Montrer que le reste de la division euclidienne de 2^{355} par 3 est 2.

2. Montrer que pour tout entier relatif impair n, on a $n^2 \equiv 1\ [8]$.

II PGCD de deux entiers relatifs

II.1 Définition du pgcd

DÉFINITION

Soit a et b deux entiers relatifs, l'un au moins étant non nul.

Le Plus Grand Commun Diviseur de a et b, noté $pgcd(a, b)$ ou $a \wedge b$ est le plus grand élément au sens de $\leqslant$ de l'ensemble $div(a) \cap div(b)$ des diviseurs communs à a et à b.

On pose aussi : $pgcd(0, 0) = 0$.

6►

Pratique 4 :

1. Donner $pgcd(2, 8)$, $pgcd(12, -18)$, $pgcd(14, 22)$.

2. Vérifier que $a \wedge b = b \wedge a = |a| \wedge |b|$, que $a \wedge 1 = 1$ et $a \wedge 0 = |a|$.

II.2 Recherche d'un pgcd : l'algorithme d'Euclide

Idée fondamentale : $a \wedge b = (a - bq) \wedge b$, où a, b et q sont des entiers relatifs. En particulier :

si r est le reste de la division euclidienne de a par b : $a = bq + r$ donc : $\boxed{a \wedge b = b \wedge r}$

7►

Comme $a \wedge b = b \wedge a = |a| \wedge |b|$ et $0 \wedge 0 = 0$, on peut se ramener à la recherche de $a \wedge b$ dans le cas $0 \leqslant a \leqslant b$, b non nul.

En utilisant l'idée fondamentale, on obtient l'**algorithme d'Euclide** :

1) On pose : $r_0 = a$ et $r_1 = b$

2) Pour $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, r_{k+2} est le reste de la division euclidienne de r_k par r_{k+1}.
On change k en $k+1$.

La suite des restes $(r_k)_{k\geqslant 1}$ est nulle à partir d'un certain rang $n+1$, sinon elle décroît strictement et prend des valeurs naturelles. On quitte donc l'étape 2) en un temps fini.

3) $a \wedge b = r_n \wedge r_{n+1} = r_n$ est donc le dernier reste non nul r_n de la suite.

8►

II.3 L'identité de Bezout

Théorème de l'identité de Bezout :

> *Soit a et b deux entiers relatifs. Alors il existe $(u, v) \in \mathbb{Z}^2$ tel que : $a \wedge b = au + bv$*
>
> *Un tel couple (u, v) est* **un couple de Bezout** *associé à a et b.*

9►

Algorithme d'Euclide étendu :

1) On pose : $r_0 = a$ et $r_1 = b$
et on pose : $(u_0, u_1) = (1, 0)$ et $(v_0, v_1) = (0, 1)$

2) Pour $k \in \mathbb{N}$, tant que $r_{k+1} \neq 0$, soit $r_k = q_{k+1}r_{k+1} + r_{k+2}$ la div. euclidienne de r_k par r_{k+1}
on pose : $u_k = q_{k+1}u_{k+1} + u_{k+2}$ et $v_k = q_{k+1}v_{k+1} + v_{k+2}$ (qui définissent u_{k+2} et v_{k+2}).
On change k en $k+1$.

3) $a \wedge b = r_n \wedge r_{n+1} = r_n$ est donc le dernier reste non nul r_n de la suite des restes
et on a : $au_n + bv_n = a \wedge b$.

Pratique 5 :

Trouver $28 \wedge 50$ ainsi qu'un couple de Bezout associé à 28 et 50.

II.4 Propriétés du pgcd

a, b et c sont des entiers relatifs.

Propriétés

1) $a \wedge b = b \wedge a = |a| \wedge |b|$

2) $a \wedge 1 = 1$ et $a \wedge 0 = |a|$

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

4) $\mathrm{div}(a) \cap \mathrm{div}(b) = \mathrm{div}(a \wedge b)$,
autrement dit c divise a et b si, et seulement si, c divise $a \wedge b$

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

10►

II.5 Nombres relatifs premiers entre eux

Définition

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

Théorème

| *Soit $(a, b) \in \mathbb{Z}^2$. Alors il existe a' et b' premiers entre eux tels que : $a = (a \wedge b)\, a'$ et $b = (a \wedge b)\, b'$*

11▶

Définition

| *Soit r un rationnel.*
| *Alors il existe p et q premiers entre eux tels que $r = \frac{p}{q}$, c'est une forme irréductible de r.*

Théorème de Bezout :

| *Soit $(a, b) \in \mathbb{Z}^2$.*
| *a et b sont premiers entre eux* **si, et seulement si,** *il existe $(u, v) \in \mathbb{Z}^2$ tels que : $au + bv = 1$*

12▶

Théorème de Gauss :

| *Soit $(a, b, c) \in \mathbb{Z}^3$.*
| *Si a divise bc et si a est premier avec b, alors a divise c.*

13▶

Proposition

| *Soit $(a, b, c) \in \mathbb{Z}^3$. Si a et b divisent c et si $a \wedge b = 1$, alors ab divise c.*

14▶

Proposition

| *Soit $(a, b, c) \in \mathbb{Z}^3$. Si a est premier avec b et avec c, alors a est premier avec bc.*

15▶

II.6 Exemples d'applications

• **Équations diophantiennes** :

Soit $(a, b, c) \in \mathbb{Z}^3$: on cherche les couples $(x, y) \in \mathbb{Z}^2$ tels que $ax + by = c$

| Idée : se ramener à une relation de Bezout !

a) si $a \wedge b$ ne divise pas c, l'équation n'a pas de solution

b) sinon, $c = (a \wedge b)c'$, $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$, l'algorithme d'Euclide étendu associé à a' et b' donne une solution (x_0, y_0) après multiplication par c'.

c) Par soustraction de $ax_0 + by_0 = c$ et $ax + by = c$, en utilisant $a' \wedge b' = 1$ et le théorème de Gauss, on obtient toutes les solutions $(x_0 + kb', y_0 - ka')$ pour $k \in \mathbb{Z}$.

Pratique 6 :

Résoudre l'équation : $4x - 10y = 4$ d'inconnues $(x, y) \in \mathbb{Z}^2$.

• **Systèmes de congruences** :

Soit $(a, b) \in \mathbb{Z}^2$ et p et q deux naturels premiers entre eux et supérieurs à 2.

On cherche les entiers relatifs x tels que : $\begin{cases} x \equiv a \ [p] \\ x \equiv b \ [q] \end{cases}$

Si $pu + qv = 1$, on voit que $x_0 = pub + qva$ est une solution (l'inverse de p modulo q est u, celui de q modulo p est v), et on vérifie que les autres solutions sont les $x_0 + pq\mathbb{Z}$. (**Lemme chinois**)

Pratique 7 :

16 brigands décident de partager un butin de pièces en parts égales et de laisser le reste, soit 3 pièces, au cuisinier chinois. Mais ils se querellent, et 9 pirates sont tués ; il revient alors 4 pièces au cuisinier. Quel gain minimum celui-ci peut-il espérer s'il trucide les pirates restants ?

III PPCM de deux entiers relatifs

Définition

> *Le Plus Petit Commun Multiple de deux entiers relatifs a et b non nuls, noté $ppcm(a, b)$ ou $a \vee b$, est le plus petit élément au sens de $\leqslant$ de l'ensemble des multiples strictement positifs communs à a et b.*
>
> *On pose aussi :* $a \vee 0 = 0 \vee a = 0$

16►

Pratique 8 :

Donner $12 \vee 3$, $(-10) \vee 15$ et $6 \vee (-5)$.

Propriétés

Soit a, b et c dans $\mathbb{Z}$.

1) $a \vee a = |a|$, $a \vee b = b \vee a$, $1 \vee a = |a|$ et $0 \vee a = 0$

2) $(a \wedge b)(a \vee b) = |ab|$; en particulier, si a et b sont premiers entre eux, $a \vee b = |ab|$

3) $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$, autrement dit les multiples communs à a et b sont les multiples de $a \vee b$

4) $(ac) \vee (bc) = |c|(a \vee b)$

17►

IV PGCD et PPCM d'une famille finie d'entiers

On généralise ce qui précède, mais attention aux propriétés qui disparaissent ! !

Soit $n \geqslant 3$ et des entiers relatifs a_1, a_2, ..., a_n, l'un au moins étant non nul.

• $a_1 \wedge a_2 \wedge \ldots \wedge a_n = pgcd(a_1, \ldots, a_n)$ désigne le plus grand élément (au sens de $\leqslant$) de l'ensemble des diviseurs communs aux a_i.
On pose aussi $0 \wedge 0 \wedge \ldots \wedge 0 = 0$.

L'associativité du pgcd ramène de proche en proche au calcul d'un pgcd de deux entiers.
On retrouve donc les propriétés :

a) les diviseurs communs aux a_i sont exactement ceux de $pgcd(a_1, \ldots, a_n)$

b) pour tout b dans $\mathbb{Z}$: $pgcd(a_1 b, \ldots, a_n b) = |b| pgcd(a_1, \ldots, a_n)$

c) relation de Bezout :

il existe des entiers relatifs u_1, u_2, ..., u_n tels que $\sum_{i=1}^{n} a_i u_i = pgcd(a_1, \ldots, a_n)$

18►

• Les a_i sont **premiers entre eux dans leur ensemble** si $pgcd(a_1, \ldots, a_n) = 1$.

Les a_i sont **premiers entre eux deux à deux** si

$$\text{pour tout } (i,j) \in [\![1,n]\!],\ i \neq j \Longrightarrow pgcd(a_i, a_j) = 1.$$

Si les a_i sont premiers entre eux deux à deux, alors ils le sont dans leur ensemble.
La réciproque est fausse.

Pratique 9 :

Que dire de 4, 9 et 10 ?

On généralise les résultats précédents :

- il existe des a'_i premiers entre eux dans leur ensemble tels que $a_i = pgcd(a_1, \ldots, a_n) a'_i$

- théorème de Bezout : les a_i sont premiers entre eux dans leur ensemble si, et seulement si, il existe $(u_1, \ldots, u_n) \in \mathbb{Z}^n$ tels que $\sum_{i=1}^{n} a_i u_i = 1$

- si les a_i divisent b et sont premiers entre eux deux à deux, alors $\prod_{i=1}^{n} a_i$ divise b

- si b est premier avec chaque a_i, alors b est premier avec $\prod_{i=1}^{n} a_i$.

• $a_1 \vee a_2 \vee \ldots \vee a_n = ppcm(a_1, \ldots, a_n)$ désigne le plus petit élément (au sens de $\leqslant$) de l'ensemble des multiples communs aux a_i, supposés ici non nuls.

Comme $(a_1\mathbb{Z} \cap a_2\mathbb{Z}) \cap \ldots \cap a_n\mathbb{Z} = ((a_1 \vee a_2)\mathbb{Z}) \cap \ldots \cap a_n\mathbb{Z}$, on généralise les résultats :

a) les multiples communs aux a_i sont exactement ceux de $ppcm(a_1, \ldots, a_n)$

b) pour tout b dans $\mathbb{Z}$: $ppcm(a_1 b, \ldots, a_n b) = |b| ppcm(a_1, \ldots, a_n)$

La relation $|ab| = (a \wedge b)(a \vee b)$ ne se généralise pas ! !

Pratique 10 :

Le vérifier avec 4, 9 et 10

V Nombres premiers

V.1 Première approche

Définition

Un naturel est un nombre premier s'il admet exactement deux diviseurs naturels : 1 *et lui-même.*

On note $\mathbb{P}$ *l'ensemble des nombres premiers.*

1 n'est pas un nombre premier, 2 est le plus petit élément de $\mathbb{P}$!

Pratique 11 :

Donner la liste des nombres premiers inférieurs à 40.

Théorème

1) Tout entier naturel supérieur ou égal à 2 *s'écrit comme produit de nombres premiers.*

2) $\mathbb{P}$ *est infini.*

19►

Une méthode pour décrire $\mathbb{P}$: le **crible d'Ératosthène**

20►

Propriétés

1) Si $a \in \mathbb{N}$ et p premier, alors $a \wedge p = p$ si p divise a, $a \wedge p = 1$ sinon.
Autrement dit, a est inversible modulo p si, et seulement si, $a \not\equiv 0\,[p]$.

2) Soit $(a, b) \in \mathbb{Z}^2$ et p un nombre premier. Alors $ab \equiv 0\ [p] \iff (a \equiv 0\ [p]$ ou $b \equiv 0\ [p])$.
Autrement dit, si p premier divise un produit, alors il divise l'un des facteurs.

3) Si p et q sont deux nombres premiers distincts, alors $p \wedge q = 1$.

21►

Théorème de Fermat (petit) :

Soit p *un nombre premier et* a *un entier relatif. Alors :* $a^p \equiv a\ [p]$

En particulier, si a *n'est pas multiple de* p *(ou* a *inversible modulo* p*) :* $a^{p-1} \equiv 1\ [p]$

22►

V.2 Théorème de factorisation première

Théorème

Soit n *un naturel supérieur ou égal à* 2.

Il existe une et une seule famille $(\nu_p(n))_{p\in\mathbb{P}}$ *d'entiers naturels nuls sauf pour un nombre fini, telle que :* $n = \prod_{p\in\mathbb{P}} p^{\nu_p(n)}$

C'est la factorisation première de n.

$\nu_p(n)$ *est la valuation* p*-adique de* n*, la plus grande puissance* q *de* p *telle que* p^q *divise* n.

23►

Pratique 12 :

Donner les factorisations premières de 16, 18, 38 ainsi que leurs valuations p-adiques.

PROPOSITION

Pour tout $p \in \mathbb{P}$ et tout a et b entiers relatifs non nuls : $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
En particulier, pour tout $k \in \mathbb{N}$: $\nu_p(a^k) = k\nu_p(a)$

24►

THÉORÈME

Soit a et b deux entiers relatifs non nuls.

1) a divise b si, et seulement si, pour tout nombre premier p on a $\nu_p(a) \leqslant \nu_p(b)$

2) $a \wedge b = \prod_{p \in \mathbb{P}} p^{\mathrm{Min}(\nu_p(a), \nu_p(b))}$ *et* $a \vee b = \prod_{p \in \mathbb{P}} p^{\mathrm{Max}(\nu_p(a), \nu_p(b))}$

25►

Pratique 13 :

Calculer ainsi le pgcd et le ppcm de 432 et 328

Pensez à utiliser mentalement la factorisation première pour retrouver les propriétés du pgcd ou du ppcm !

26►

SAVOIR...

(1) *... appliquer l'algorithme d'Euclide et le « remonter » pour obtenir pgcd et couple de Bezout*

2) *... traduire en terme de congruences les propriétés de divisibilité et de pgcd*

3) *... que les principaux outils sont les théorèmes de Bezout, Gauss, et factorisation première*

4) *... résoudre facilement les équations diophantiennes linéaires et les systèmes de congruences*

THÉORÈMES et PROPOSITIONS...	**... OUTILS pour...**
Théorème de la division euclidienne	*La base de l'arithmétique*
Théorème de l'écriture en base b	*Écritures en b, exponentiation rapide*
Algorithme d'Euclide (étendu)	*Obtention pgcd, relations de Bezout*
Théorème de l'identité de Bezout, théorème de Bezout	*Relation de Bezout, cas réciproque*
Théorème d'écriture de a et b avec $a \wedge b$	*Se ramener à des entiers premiers entre eux*
Théorème de Gauss	*Un diviseur d'un produit divise un des facteurs ?*
Proposition sur produit de diviseurs	*Un produit de diviseurs reste un diviseur ?*
Proposition sur premier avec un produit	*Primalité avec produit et avec ses facteurs*
Théorème de l'infinitude de $\mathbb{P}$	*Propriétés des naturels premiers*
Petit Théorème de Fermat	*Calculs de congruences avec nombres premiers*
Théorème de la factorisation première	*résolution de problèmes arithmétiques multiples par changement d'écriture des naturels*
Théorème de calcul de pgcd et ppcm par factorisation première	*Calculs pratiques de pgcd, ppcm*