Arithmétique dans $\mathbb{Z}$

I Divisibilité

1) Divisibilité

Soient $a, b \in \mathbb{Z}$, on dit que a <u>divise</u> b si il existe $k \in \mathbb{Z}$ tel que $b = ka$. On note alors $a \mid b$, on dit que a est un <u>diviseur</u> de b et que b est un <u>multiple</u> de a.

Notez que $-1, 1, a$ et $-a$ divisent a.

Notez que $a \mid 0$.

<u>Proposition</u>

$\forall a, b \in \mathbb{Z}$, on a
$a \mid b \Rightarrow (-a) \mid b,\ a \mid (-b),\ (-a) \mid (-b)$.

(Exercice).

On note <u>Div(a)</u> l'ens. des diviseurs de a :

$$\mathrm{Div}(a) = \{k \in \mathbb{Z},\ k \mid a\}$$

On note <u>Mult(a)</u> l'ens. des multiples de a :

$$\mathrm{Mult}(a) = \{ka, k \in \mathbb{Z}\}.$$

Notez que $\mathrm{Div}(a) \subset [\![-a, a]\!]$, donc c'est un ens. fini.

Par contre $\mathrm{Mult}(a)$ est infini, sauf pour $a=0$.

Proposition

$\forall a,b,c,d \in \mathbb{Z}$,

i) $a|b$ et $b|c \Rightarrow a|c$

ii) $a|b$ et $b|a \Rightarrow |a|=|b|$.

iii) $a|b$ et $a|c \Rightarrow a|(b+c)$

iv) $a|b$ et $c|d \Rightarrow ac|bd$

v) $a|b \Rightarrow \forall p \in \mathbb{N}\ a^p|b^p$.

Dem

i) $b=ak$, $c=bk' \Rightarrow c=akk'$ ✓

ii) $b=ak$ et $a=k'b \Rightarrow b=kk'b \Rightarrow kk'=1$ (si $b\neq 0$). Mais comme $k,k' \in \mathbb{Z}$ ça laisse peu de choix : $k'=k=\pm 1$ et donc $|b|=|a|$.
↪ si $b=0$, le fait que $0|a \Rightarrow a=0$. et donc $|a|=|b|$ aussi.

iii) $b=ak$, $c=ak' \Rightarrow b+c=a(k+k')$ ✓

iv) $b=ak$, $d=ck' \Rightarrow bd=ac(kk')$ ✓

v) $b=ak \Rightarrow b^p=a^p k^p$ ✓ ∎

2) Division euclidienne

Thm

Pour tout $a \in \mathbb{Z}$, tout $b \in \mathbb{N}^*$, il existe un unique couple (q,r) tel que $q \in \mathbb{Z}$, $b \in [\![0, b-1]\!]$ tel que $a=bq+r$

Dem

Existence : on prend $q = \left[\frac{a}{b}\right]$ et $r = a - bq$ et ça marche.

Unicité : si $a = bq + r = bq' + r'$, avec $r, r' \in [\![0, n-1]\!]$, alors

$b(q-q') = r' - r$. En particulier $-b < r - r' < b$ et donc $-b < b(q-q') < b$.

Donc, comme $b \neq 0$ et $b > 0$, on a $-1 < q - q' < 1$. Mais comme $q - q' \in \mathbb{Z} \Rightarrow q = q'$.

Par suite $r = r'$.

∎

q et r sont appelés quotient et reste de la division euclidienne de a par b.

3) Congruences

Soit $n \in \mathbb{N}^*$. Soient $a, b \in \mathbb{Z}$, on dit que a est congru à b modulo n, si $n \mid b - a$.

Autrement dit, si $\exists k \in \mathbb{Z}$ tq $\boxed{a = b + kn}$

On note ça $a \equiv b\ [n]$.

Par exemple : $13 \equiv 3\ [5]$, $13 \equiv 8\ [5]$, $13 \equiv (-2)\ [5]$.

Remarque

$n \mid a \iff a \equiv 0\ [n]$.

Proposition

Pour tout $n \in \mathbb{N}^*$, tout $a \in \mathbb{Z}$, il existe un unique $r \in [\![0, n-1]\!]$ tq $a \equiv r\ [n]$. Ce r est le reste de la div. euclidienne de a par n.

Dem

Si r est le reste de la div. eucl. de a par n, on a $a = nq + r$

et $r \in [\![0, n-1]\!]$. Donc $a \equiv r\ [n]$ et $r \in [\![0, n-1]\!]$.
L'unicité, si $a \equiv r'\ [n]$ avec $r' \in [\![0, n-1]\!]$, alors $a = nq + r = nq' + r'$.
On conclut facilement par l'unicité de la div. eucl. ∎

Proposition

$\forall a, b, c \in \mathbb{Z}$:

- $a \equiv b\ [n] \iff b \equiv a\ [n]$
- $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$.

Dem

- $a = b + nk \Rightarrow b = a - nk$. ✓
- $a = b + nk$ et $b = c + nk' \Rightarrow a = c + nk' + nk = c + n(k + k')$ ✓ ∎

Proposition

Soient $a, a', b, b' \in \mathbb{Z}$ tq $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$. Alors on a :

i) $a + b \equiv a' + b'\ [n]$
ii) $ab \equiv a'b'\ [n]$.
iii) $-a \equiv -a'\ [n]$
iv) $a^p \equiv a'^p\ [n]$.

Dem

$a = a' + kn$, $b = b' + k'n$

i) $\Rightarrow a + b = a' + b' + (k + k')n$. ✓

ii) $ab = a'b' + b'kn + ak'n + kk'n^2 = a'b' + Kn$. ✓

iii) $-a = -a' - kn$ ✓

iv) Soit on récrit $aa \equiv a'a'\ [n]$ etc. par récurrence, soit on écrit

$$a^p = (a' + kn)^p = a'^p + \sum_{i=0}^{p-1} \binom{p}{i} a'^i (kn)^{n-i}$$

$$= a'^p + Kn. \quad \blacksquare$$

II PGCD et PPCM

1) PGCD

Soient $a, b \in \mathbb{Z}$. Pour tout $d \in \mathbb{Z}$ tel que $d \mid a$ et $d \mid b$ on dit que d est un <u>diviseur commun</u> de a et de b. On note $Div(a,b)$ l'ens. des diviseurs communs de a et b. On a donc

$$Div(a,b) = Div(a) \cap Div(b).$$

Par exemple $Div(24,18) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$

<u>Proposition</u>

$\forall a, b \in \mathbb{Z}$ avec $(a,b) \neq (0,0)$, l'ensemble $Div(a,b)$ admet un plus grand élément.

<u>Dem</u>

$Div(a,b) \subset \mathbb{Z}$ par définition, il est non vide car il contient 1. Enfin $Div(a,b) \subset Div(a)$ donc $Div(a,b)$ est fini. Il admet donc un plus grand élément. $\blacksquare$

Le plus grand élément de $Div(a,b)$ est appelé <u>PGCD de a et b</u>. On le note <u>$pgcd(a,b)$</u> ou encore <u>$a \wedge b$</u>.

Dans l'exemple on voit que $pgcd(24,18) = 6$.

Par convention on pose $pgcd(0,0) = 0$.

Proposition

$\forall a,b \in \mathbb{Z}$, on a :

- $pgcd(a,b) \in \mathbb{N}$
- $pgcd(a,b) = pgcd(b,a)$
- $pgcd(a,b) = pgcd(|a|,|b|)$.
- si $a|b$ alors $pgcd(a,b) = |a|$.

Dem laissée en exercice.

2) Algorithme d'Euclide

Proposition

Si $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, si r est le reste de la div. eucl. de a par b, alors $pgcd(a,b) = pgcd(b,r)$.

Dem

$a = bq + r$, donc si $d|a$ et $d|b \Rightarrow d | r = a - bq$.

Réciproquement si $d|r$ et $d|b$, alors $d| a = bq + r$.

Donc $Div(a,b) = Div(b,r)$. D'où $pgcd(a,b) = pgcd(b,r)$. ∎

Notons que $pgcd(a,0) = |a|$ et $pgcd(1,a) = 1$.

On en déduit l'algorithme d'Euclide

Soient $a,b \in \mathbb{Z}$, on veut calculer $\delta = pgcd(a,b)$. Déjà on peut remplacer a,b par $|a|,|b|$; donc on peut supposer, sans perte de généralité, que $a,b \in \mathbb{N}$. On peut aussi supposer que $a \geq b$, sinon on inverse les rôles.

(et si $a=b$, $pgcd(a,b) = a$). On écarte le cas $b=0$ aussi car $pgcd(a,0) = a$

On note $a_0 = a$, $a_1 = b$, puis a_2 le reste de a_0/a_1.

On a donc $\delta = pgcd(a_1, a_2)$ avec $a_2 < a_1$.

→ si $a_2 = 0$ alors c'est fini, $\delta = a_1$

→ si $a_2 \neq 0$ alors on recommence : soit a_3 le reste de a_1/a_2.

On a $\delta = pgcd(a_2, a_3)$ et $a_3 < a_2$.

Et ainsi de suite, l'algorithme s'arrête forcement à un $a_m = 0$ car $a_1 > a_2 > a_3 > \cdots \geq 0$.

On trouve donc un $a_m = 0$ et donc $\delta = pgcd(a_{m-1}, a_m) = a_{m-1}$.

(Le pgcd est le dernier reste non nul).

Exemples :

$24 = 1 \times 18 + 6$, $18 = 3 \times 6 + 0 \Rightarrow pgcd(24, 18) = 6$.

$24 = 2 \times 9 + 6$, $9 = 1 \times 6 + 3$, $6 = 2 \times 3 + 0 \Rightarrow pgcd(24, 9) = 3$.

3) Théorème de Bezout

Théorème (Egalité de Bezout)

> Soient $a, b \in \mathbb{Z}$, alors il existe $u, v \in \mathbb{Z}$ tels que
> $au + bv = pgcd(a, b)$.

Dem

On reprend l'algorithme d'Euclide :

$a_0 = q_1 a_1 + a_2$, $a_1 = q_2 a_2 + a_3$, $\cdots$, $a_{m-2} = q_{m-1} a_{m-1} + 0$.

On a clairement $a_0 = au_0 + bv_0$ avec $u_0, v_0 \in \mathbb{Z}$, et $a_1 = au_1 + bv_1$, avec $u_1, v_1 \in \mathbb{Z}$. Ensuite

$a_2 = a_0 - a_1 q_1$ donc $a_2 = au_2 + bv_2$, $u_2, v_2 \in \mathbb{Z}$.

et ainsi de suite jusqu'à $pgcd(a,b) = a_{m-1} = au+bv$, avec $u, v \in \mathbb{Z}$. ∎

On a même l'algo. pour trouver u, v :

* $24 = 1\times 18 + 6$, $6 = 2\times 3 + 0 \Rightarrow 6 = 24 - 18$ ✓

* $24 = 2\times 9 + 6$, $9 = 1\times 6 + 3$, $6 = 2\times 3 + 6$

$\Rightarrow 6 = 24 - 2\times 9 \Rightarrow 3 = 9 - 6 = 9 - (24 - 2\times 9) = -24 + 3\times 9$

* $150 = 2\times 54 + 42$, $54 = 1\times 42 + 12$, $42 = 3\times 12 + 6$, $12 = 2\times 6 + 0$

$\Rightarrow pgcd(150, 54) = 6$ et

$42 = 150 - 2\times 54$, $12 = 54 - 42 = -150 + 3\times 54$, $6 = 42 - 3\times 12 =$

$= 150 - 2\times 54 - 3(-150 + 3\times 54) = 4\times 150 - 11\times 54$.

Autre façon :

$6 = 42 - 3\times 12 = 42 - 3(54 - 42) = 4\times 42 - 3\times 54 = 4\times(150 - 2\times 54) - 3\times 54$

$= 4\times 150 - 11\times 54$.

4) Propriétés du pgcd.

Théorème

> $\forall a, b \in \mathbb{Z}$, $\forall d \in \mathbb{Z}$, on a
>
> $d \mid a$ et $d \mid b \iff d \mid a \wedge b$.

Dem

Si $d \mid a \wedge b$ alors, comme $a \wedge b \mid a \Rightarrow d \mid a$; et comme $a \wedge b \mid b \Rightarrow d \mid b$.

Inversement, par Bezout $a \wedge b = au + bv$, donc si $d \mid a$ et $d \mid b \Rightarrow d \mid au + bv$ et $d \mid a \wedge b$. ∎

Corollaire

$\mathrm{Div}(a,b) = \mathrm{Div}(a \wedge b)$.

Proposition

$\forall a,b \in \mathbb{Z}$, $\forall \lambda \in \mathbb{N}$, on a $\mathrm{pgcd}(\lambda a, \lambda b) = \lambda \, \mathrm{pgcd}(a,b)$.

Dem

$\mathrm{pgcd}(a,b) \mid a \Rightarrow \lambda \, \mathrm{pgcd}(a,b) \mid \lambda a$; de même $\lambda \, \mathrm{pgcd}(a,b) \mid \lambda b$. Donc $\lambda \, \mathrm{pgcd}(a,b) \mid \mathrm{pgcd}(\lambda a, \lambda b)$.

De plus $\mathrm{pgcd}(a,b) = au + bv \Rightarrow \lambda \, \mathrm{pgcd}(a,b) = \lambda a u + \lambda b v \Rightarrow \mathrm{pgcd}(\lambda a, \lambda b)$ divise $\lambda \, \mathrm{pgcd}(a,b)$.

On sait $\alpha \mid \beta$ et $\beta \mid \alpha \Rightarrow |\alpha| = |\beta|$ (exercice). ☒

5) PPCM

Soient $a,b \in \mathbb{Z}$. Tout entier $m \in \mathbb{Z}$ tel que $a \mid m$ et $b \mid m$ est appelé multiple commun de a,b. L'ens. des multiples communs de a,b est noté $\mathrm{Mul}(a,b)$. On a donc

$$\mathrm{Mul}(a,b) = \mathrm{Mul}(a) \cap \mathrm{Mul}(b).$$

L'ens. $\mathrm{Mul}(a,b) \cap \mathbb{N}^*$ possède un plus petit élément. (exercice)

On le note ppcm(a,b) ou encore $a \vee b$.

Si a ou $b = 0$, alors ppcm$(a,b) = 0$.

Proposition

Si $a, b \in \mathbb{Z}$, alors

- $\operatorname{ppcm}(a,b) \in \mathbb{N}$
- $\operatorname{ppcm}(a,b) = \operatorname{ppcm}(b,a)$
- $\operatorname{ppcm}(a,b) = \operatorname{ppcm}(|a|,|b|)$.
- si $a \mid b$ alors $\operatorname{ppcm}(a,b) = |b|$.

(exercice).