UNIVERSITÉ DE TOURS– L2– ARITHMÉTIQUE 2021-2022

Leçon 1 : Divisibilité, factorisation et algorithme d'Euclide sur $\mathbb{N}$ et $\mathbb{Z}$

Conventions

• Les nombres suivants $a, b, c, d, m, n, p, q, \alpha, \beta, \lambda$ seront tous supposés être des entiers de $\mathbb{N}$ dans la section 1 et des entiers rationnels -i.e. $\mathbb{Z}$ - dans les sections suivantes (sauf mention du contraire).

---

1 Divisibilité

Définition 1.1. *le nombre d divise n- noté $d|n$- ssi $\exists c : n = dc$.*

Théorème 0.
La relation "divise" vérifie les propriétés suivantes :

1. *$|$ est une relation d'ordre partiel sur $\mathbb{N}$; plus généralement - sur $\mathbb{Z}$-*
   - $n|n$
   - $m|n$ *et* $n|m \implies m = \pm n$
   - $m|n$ *et* $n|p \implies m|p$
2. *linéarité :*
   - $d|m$ *et* $d|n \implies d|am + bn$
3. *multiplicativité:*
   - $d|n \implies d|an$
4. *diviseur conjugué:*
   - $d|n \implies \frac{n}{d}| \ n$
5.
   - $1|n$ *et* $n|\ 0$
     (1 (resp. 0) est le plus petit élément (resp. plus grand élément) pour la relation d'ordre $|$) .

Définition 1.2. *d est diviseur commun de a et b si $d|a$ et $d|b$*

Théorème 1. *Pour tout a, b il existe un diviseur commun d de la forme $d = \alpha a + \beta b$ et tel que tout autre diviseur commun de a et b divise d*

Théorème 2. *(pgcd)*
Pour tout a, b il existe un seul d tel que

- $d \geq 0$

- $d|a$ *et* $d|\ b$
- $q|a$ *et* $q|\ b \implies q|d$

d - noté (a, b) *ou* $pgcd(a, b)$ *est le plus grand commun diviseur de* a *et* b. (a, b) *est le plus grand des minorants pour la relation d'ordre* $|$.

Remarque 1.1. *Nous verrons au chapitre suivant un algorithme qui permet de calculer le pgcd de 2 nombres. Cet algorithme fournit une autre démonstration du théorème précédent et se traduit par la fonction récursive suivante en* `Python` *:*

```
def reste(a,b):
        if a < b:
            (a,b) = (b,a)
        a -=b
        return a

 def pgcd(a,b):
       while b>0 :
        (a,b) = (b, reste(a,b))
    return a
```

Remarque 1.2. *La plus petite valeur positive de* $xa + yb$ *où* $x, y \in \mathbb{Z}$ *est égale à* (a, b)

Définition 1.3. *Si* $(a, b) = 1$ *a et b sont dits premiers entre eux.*

Proposition 1.1. *1. (a,b) = (b,a)*

2. *(a,(b,c)) = ((a,b),c)*
3. *(1,a) = (a,1) = 1*
4. *(0,a) = (a, 0) = a*
5. *(ab,ac) = |a| (b,c)*

Théorème 3 (Euclide-Gauss)**.** $a|bc$ *et* $(a, b) = 1 \implies a|c$

Remarque 1.3. ** Les notions précédentes : définition de la relation* $|$*, nombre premier,... ont un sens dans tout anneau. Il est utile de connaitre quelques anneaux de nombre plus exotiques par exemple l'anneau des entiers de Gauss* $\mathbb{Z}[i] := \{m + in : m; n \in \mathbb{Z}\}. \subset \mathbb{C}$ *ou quadratiques* $\mathbb{Z}[\sqrt{d}] := \{m + \sqrt{d}n : m; n \in \mathbb{Z}\}. \subset \mathbb{R}$ *où d n'est pas un carré, ou encore des anneaux de polynomes* $\mathbb{Q}[X]$ *ou* $\mathbb{R}[X]$.

2 Nombres premiers

Définition 2.1. *n est premier si*

- $n > 1$

- *les seuls diviseurs de n sont ± 1 et $\pm n$ (n et les éléments inversibles).*

Théorème 4. *Tout nombre positif est soit 1, soit premier, soit produit de nombres premiers*

Théorème 5 (Euclide)**.** *Il y a une infinité de nombres premiers*

Théorème 6. *Si p est premier et $p \not| a$ alors $(p, a) = 1$*

Théorème 7. *Si p premier est tel que $p|a_1 \cdot a_2 \cdots a_n$ alors $p|a_i$ pour au moins un $i \in \{1, \cdots n\}$*

3 Théorème fondamental de l'arithmétique

Théorème 8. *Tout entier > 1 se décompose de façon unique en produit de nombres premiers à l'ordre des facteurs près.*

Corollaire 3.1. *Tout entier*

$$n = \pm \prod_1^\infty p_k^{\alpha_k}$$

où p_k est le k-ième nombre premier, et où $\alpha_k = 0$ sauf pour un nombre fini de k où $\alpha_k \geq 1$

Corollaire 3.2. *Si*

$$a = \pm \prod_1^\infty p_k^{\alpha_k}, b = \pm \prod_1^\infty p_k^{\beta_k}$$

alors

$$(a, b) = \prod_1^\infty p_k^{min(\alpha_k, \beta_k)}, ppcm(a, b) = \prod_1^\infty p_k^{max(\alpha_k, \beta_k)}$$

Exercice 3.1. *Calculer*

$$(a, b) \cdot ppcm(a, b)$$

4 Nombres Pythagoriciens (*voir note 1*)

Définition 4.1. *un nombre est pythagoricien si son carré est la somme de deux autres carrés positifs. Un triplet pythagoricien est un triplet (a,b,c) terl que $a^2 + b^2 = c^2$. On dira qu'un triplet est primitif s'ils n'ont pas de diviseur commun.*

Example 4.1. *(3,4,5); (5,12,13) ; (11,60,61) ; (15,8,17) ; (16,63,65)....*

Théorème 9. *Toute solution entière de*

$$x^2 + y^2 = z^2$$

est (en permutant éventuellement x et y) de la forme

$$x = \lambda ab, y = \lambda(a^2 - b^2), z = \lambda(a^2 + b^2)$$

où $a > b \geq 1$ sont impairs et premiers entre eux.

Réciproquement, pour tout a, b, λ, et en permutant éventuellement x et y, le triplet

$$(x, y, z) := \big(\lambda 2ab, \lambda(a^2 - b^2), \lambda(a^2 + b^2)\big)$$

est solution de $x^2 + y^2 = z^2$.

Example 4.2. *2019 est un nombre Pythagoricien (on mettra à profit un petit programme* Python*) !*

Remarque 4.1. *Tout entier plus grand que* 1 *est somme de deux carrés si et seulement si chacun de ses facteurs premiers de la forme 4k + 3 intervient à une puissance paire (Théorème des 2 carrés de Fermat). Mais tout entier plus grand que* 1 *est somme de quatre carrés (théorème des 4 carrés, Lagrange).*