I. Arithmétique

On rappelle que l'on note $\mathbb{Z}$ l'ensemble des entiers relatifs (ou entiers), $\mathbb{N}$ l'ensemble des entiers naturels et qu'un entier naturel différent de 0 s'appelle un entier positif.

1 Divisibilité

Définition 1.1. Soient a et b des entiers. On dit que a divise b, ou que a est un diviseur de b, ou encore que b est un multiple de a s'il existe un entier q tel que $b = aq$.

Exemple.
– Tout entier divise 0. Le seul multiple de 0 est 0.
– Tout entier est multiple de 1et de -1.
– Si n est un entier non nul, alors n et $-n$ sont des multiples et des diviseurs de n.
– L'entier 908070605040302010 est multiple de 9.

Lemme 1.2. *Soit b un entier non nul. Si a est un diviseur de b, alors il existe un unique q tel que $b = aq$.*

Démonstration. L'existence de $q \in \mathbb{Z}$ tel que $b = aq$ est la définition même de divisibilité. Montrons que q est unique. Supposons qu'il existe q_1 et q_2 tels que $b = aq_1$ et $b = aq_2$. On a alors $0 = b - b - aq_1 - aq_2$ et donc $a(q_1 - q_2) = 0$. Puisque b est non nul, a est non nul. Un produit d'entier non nuls étant non nul, $q_1 - q_2$ ne peut pas être non nul. On a donc $q_1 - q_2 = 0$ et donc $q_1 = q_2$. □

Lemme 1.3. *Soit n un entier positif. Si d est un diviseur de n, alors on a $-n \leqslant d \leqslant n$.*

Démonstration. Soit d un diviseur de n. Il existe donc un entier q tel que $dq = n$. Si d est positif alors q aussi. Il s'ensuit $q- \geqslant 0$ et donc que $n - d = d(q - 1)$ est positif ou nul, ce qui implique $0 \leqslant d \leqslant n$. Si d est négatif, alors -d- est un diviseur positif de n, donc on a $0 \leqslant -d \leqslant n$, ou encore $-n \leqslant d \leqslant 0$. □

On en déduit qu'un entier non nul n'a qu'un nombre fini de diviseurs. en particulier, les seuls diviseurs de 1 sont 1 et -1.

Lemme 1.4. *Soient a, b, c des entiers*
– $i)$ Si a divise b et si b divise c, alors a divise c.
– $ii)$ Si a divise b et si b divise a, alors $b = \pm a$.
– $iii)$ Si a divise b et c, alors a divise $b + c$.

Démonstration. Montrons $i)$. Par hypothèse, il existe des entiers q_1 et q_2 tels que $b = aq_1$ et $c = bq_2$. En remplaçant b par aq_1 dans l'expression de c, on obtient $c = aq_1q_2$ et donc $c = aq$ avec $q = q_1q_2$. L'entier a est donc un diviseur de c.

Montrons $ii)$. Par hypothèse, il existe des entiers q_1 et q_2 tels que $a = bq_1$ et $b = aq_2$. En remplaçant b par son expression dans celle de a on obtient $a = aq_1q_2$. Si a est nul alors b l'est

aussi et on a bien $b = \pm a$. Si a est non nul alors la relation $a = aq_1q_2$ devient $1 = q_1q_2$. Dans ce cas q_1 et q_2 sont des diviseurs de 1. Comme seuls -1 et 1 divisent 1 , on a $q_1 = 1$ ou $q_1 = -1$ et donc $b = \pm a$.

Montrons $iii)$. Par hypothèse, il existe des entiers q_1 et q_2 tels que $b = aq_1$ et $c = aq_2$ On a alors $b + c = aq_1 + aq_2 = a(q_1 - q_2)$. L'entier $b + c$ est onc un multiple de a. □

Proposition 1.5. *Soit b un entier relatif. Si a est un entier, alors in existe des entiers q et r uniques tels que $a = bq + r$ et $0 \leqslant r < b$.*

Démonstration. Commençons par l'existence des entiers q et r. Si $a = 0$, il suffit de prendre $q = r = 0$.

Supposons $a > 0$. Alors il existe $n \in \mathbb{N}$ tel que $nb \leqslant a$, par exemple $n = 0$. D'autre part, si $n \in \mathbb{N}$, on a $n \leqslant bn$, puisque $b \geqslant 1$. Il s'ensuit que tout entier naturel n tel que $bn \leqslant a$ est plus petit ou égal à a. Il n'y a qu'un nombre fini de $n \in \mathbb{N}$ tels que $bn \leqslant a$. Notons q le plus grand d'entre eux. On a alors $bq \leqslant a < b(q+1)$, c'est-à-dire, $bq \leqslant a < bq+b$ et donc $0 \leqslant a-bq < q$. On pose $r = a - bq$. On alors $a = bq + r$ et $0 \leqslant r < q$.

Supposons $a < 0$. D'après ce qu'il précède il existe des entiers q' et r' tels que $-a = bq' + r'$ avec $0 \leqslant r' < b$. Si $r' = 0$, les entiers $q = -q'$ et $r = 0$ conviennent. Si $r \neq 0$, il suffit de prendre $q = -(q' + 1)$ et $r = b - r'$.

Démontrons l'unicité de ces entiers. Soient q_1 et r_1 des entiers vérifiant les conditions de la proposition ainsi que q_2 et r_2. On a $a = bq_1 + r_1$ et $a = bq_2 + r_2$, d'où $bq_1 + r_1 = bq_2 + r_2$ et donc $b(q_1 - q_2) = r_2 - r_1$. D'autre part, on a $0 \leqslant r_1 < b$, donc $-b < -r_1 \leqslant 0$. Mais on a aussi $0 \leqslant r_2 < b$. En ajoutant ces inégalités, on obtient $-b < r_2 - r_1 < b$, c'est à dire $-b < b(q_1 - q_2) < b$. Comme b est positif, on a $-1 < q1 - q2 < 1$. Il s'ensuit $q_1 - q_2 = 0$ et donc $q_1 = q_2$. Puisque $r_2 - r_1 = b(q_1 - q_2)$, on en déduit $r_1 = r_2$. □

Définition 1.6. Dans la proposition précédente, l'entier q s'appelle le quotient et l'entier r le reste de la division euclidienne de a par b.

Soient a un entier et b un entier positif. D'après l'unicité énoncée dans la proposition di9-dessus, b divise a si et seulement si le reste de la division euclidienne de a par b est nul. Dans ce cas, le quotient de la division euclidienne de a par b s'appelle plus simplement le quotient de $a$par b que l'on note $\frac{a}{b}$.

Exemple.
– On a $45 = 19 \times 2 + 7$ donc 2 est le quotient et 7 est le reste de la division euclidienne de 45 par 19.
– On a $-45 = -19 \times 3 + 12$ donc -3 est le quotient et 12 le reste de la division euclidienne de -45 par 19.

2 Nombres premiers

Définition 1.7. Un *nombre premier* est un entier p supérieur ou égale à2 dont les seuls diviseurs positifs sont 1 et p

Exemple.
– Les cins premiers nombres premiers sont $2, 3, 5, 7$ et 11.
– L'entier 9123 n'est pas premier : il est divisible par 3.
– L'entier $2^{13} - 1$ est premier.

Définition 1.8. Soit n un entier supérieur ou égale à 2. Un nombre premier qui divise n s'appelle un facteur premier de n.

Lemme 1.9. *Tout facteur entier supérieur ou égal à 2 a au moins un facteur premier.*

Démonstration. Soit n un entier supérieur ou égale à 2. Il existe un diviseur k de n tel que $k \geqslant 2$, par exemple $k = n$. Soit p le plus petit diviseur de n tel que $p \geqslant 2$. Si ℓ est un diviseur de p et si $\ell \geqslant 2$, alors ℓ divise n. Ce qui par définition de p donne $p \leqslant \ell$. Tout diviseur de p supérieur ou égale à 2 est donc donc égale à p. Il s'ensuit que p est un nombre premier. Or p divise n, par suite p est un facteur premier de n. □

Proposition 1.10. *Il existe une infinité de nombres premiers.*

Démonstration. Il existe au moins deux nombres premiers, par exemple 2 et 3. Raisonnons par l'absurde et supposons qu'il n'y a qu'un nombre fini de nombres premiers, notés $p_1, p_2, ..., p_n$. Considérons l'entier $N = 1 + p_1p_2...p_n$. Puisque $N \geqslant 2$, il existe un facteur premier p de N. Comme p est premier c'est l'un des p_i, par suite p divise $p_1p_2....p_n$, donc p divise $1 = N - p_1p_2...p_n$. Mais ceci est impossible, puisque les seuls diviseurs de 1 sont 1 et -1 et que l'on a $p \geqslant 2$. □

Proposition 1.11. *Soit n un entier supérieur ou égame à 2. Si n n'est pas premoer alors il existe un facteur premier p de n tel que $p \leqslant \sqrt{n}$.*

Démonstration. Soient k un diviseur de n tel que $1 < k < n$ et q le soutient de n par k. Puisque $n = kq$, l'un des deux entiers k ou q est plus petit ou égale à $\sqrt{n}$. Il suffit alors de prendre pour p un facteur premier de celui des eniters k ou q qui est plus petit ou égale à $\sqrt{n}$. □

Théorème 1.12. *Soit n un entier supérieur ou égale à 2. Alors il existe un unique entier positif r et des nombres premiers $p_1, ..., p_r$ uniques tels que $p_1 \leqslant ... \leqslant p_r$ et $n = p_1...p_r$*

Démonstration. Admise □

3 Plus grand commun diviseur

Si a et b sont des entiers, 1 est diviseur de a et b. D'autre part, un entier non nul n'a qu'un nombre fini de diviseurs. Ces deux propriétés permettent d'introduire la définition suivante.

Définition 1.13. Soient a et b des entiers non tous deux nuls. Le plus grand entier qui divise a et b s'appelle le plus grand commun diviseur d ea et de b et se note $\mathrm{pgcd}(a, b)$.

Exemple.
- Si a est un entier positif, on a $\mathrm{pgcd}(a, 0) = a$.
- Pour tout $a \in \mathbb{N}$, on a $\mathrm{pgcd}(a, 1) = 1$.
- Si a est un entier et si b est un diviseur positif de a alors $\mathrm{pgcd}(a, b) = b$.
- On a $\mathrm{pgcd}(8, 12) = 4$, $\mathrm{pgcd}(12, 15) = 3$, $\mathrm{pgcd}(25, 9) = 1$, $\mathrm{pgcd}(16, 6) = 2$.

Proposition 1.14. *Soient a et b des entiers positifs. Si r est le reste de la division euclidienne de a par b, alors* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.

Proposition 1.15. *Notons q le quotient de la division euclidienne de a par b. Il vient $a = bq + r$. Si d est un diviseur de a et b, alors d divise a et bq, donc $a - bq$, c'est-à-dire d divise r. Réciproquement, si δ est un diviseur de b et r, alors δ divise r et bq donc $bq + r$, c'est-à-dire δ divise a. On a ainsi démontré que les diviseurs de a et b sons exactement les diviseurs de b et r. En particulier, on a* $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r)$.

La proposition ci-dessus permet de présenter un algorithme de calcul du plus grand commun diviseur.

L'algorithme d'Euclide

Soient a et b des entiers positifs tels que $a \geqslant b$. Notons r_1 le reste de la division euclidienne de a par b. La proposition précédente implique que l'on a $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, r_1)$.

Si r_1 est nul, alors $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(b, 0) = b$.

Si r_1 n'es pas nul, posons $r_0 = b$ et notons r_2 le reste de la division euclidienne de r_0 par r_1. D'après la proposition précédente, on a $\mathrm{pgcd}(r_0, r_1) = \mathrm{pgcd}(r_1, r_2)$.

Si r_2 est nul, alors on a $\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_0, r_1) = \mathrm{pgcd}(r_1, 0) = r_1$.

Si r_2 n'est pas nul, définissons de proche ne proche les entiers r_n de la manière suivante : si $n \geqslant 3$ et si $r_{n-1} > 0$, alors r_n est le reste de la division euclidienne de r_{n-2} par r_{n-1}. Puisqu'on a

$$0 \leqslant r_n < r_{n-1} < ... < r_2 < r_1 < r_0,$$

il existe un entier $N \geqslant 2$ tel que $r_N > 0$ et que le reste de la division euclidienne de r_{N-1} par r_N est nul. D'après la proposition précédente, on a alors

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(r_0, r_1) = \mathrm{pgcd}(r_1, r_2) = ... = \mathrm{pgcd}(r_{N-1}, r_N) = \mathrm{pgcd}(r_N, 0) = R_N.$$

Exemple. Calculons le plus grand commun diviseur de 585 et 247. Il vient successivement

$$\begin{aligned} 585 &= 247 \times 2 + 91 \\ 247 &= 91 \times 2 + 65 \\ 91 &= 65 \times 1 + 26 \\ 65 &= 26 \times 2 + 13 \\ 26 &= 12 \times 2 + 0 \end{aligned}$$

et le plus grand commun diviseur de 585 et 247 est ainsi égal à 13.

Définition 1.16. Soient a et b des entiers non tous deux nuls. On dit que a et b sont *premiers entre eux* si $\mathrm{pgcd}(a, b) = 1$.

Lemme 1.17. *Si a et b sont des entiers non nuls, alors le quotient de a et b par* $\mathrm{pgcd}(a, b)$ *sont des entiers premiers entre eux.*

Démonstration. Posons $d = \mathrm{pgcd}(a, b)$, $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ et $d' = \mathrm{pgcd}(a', b')$. On a $a = da'$ et d' divise a' d'où dd' divise a. De même, on a $b = db'$ et d' divise b' d'où dd' divise b L'entier dd' est donc un diviseur commun de a et b. Comme d est le plus grand commun diviseur de a et b, on a $dd' \leqslant d$. Comme $d > 0$, on $0 < d' \leqslant 1$ et donc $d' = 1$. □

Lemme 1.18. *Soient n un entier positif et p un nombre premier. Alors ou bien p divise n ou bien n et p sont premiers entre eux.*

Démonstration. Notons d le plus grand commun diviseur de p et n. En particulier d est un diviseur positif de p, par suite $d = 1$ ou $d = p$. Si $d = 1$, les entiers p et n sont premiers entre eux. Si $d = p$ alors p divise n. □

Proposition 1.19. *Soient a et b des entiers positifs.*
– Tout diviseur de a et b est un diviseur de $\text{pgcd}(a, b)$.
– Pour tout entier positif n, on $\text{pgcd}(na, nb) = \text{pgcd}(a, b)$.

Exercice 1.20. Démontrer cette proposition.

4 Théorème de Bézout

Si a et b sont des entiers positifs, alors pour tous entiers x et y, $\text{pgcd}(a, b)$ divise $ax + by$. Il s'ensuit que si l'équation $ax+by = c$ a des solutions entières, alors c est multiple de $\text{pgcd}(a, b)$. Nous a allons démontrer que réciproquement, si c est multiple de $\text{pgcd}(a, b)$, alors il existe $x, y \in \mathbb{Z}$ tels que $c = ax + by$.

Théorème 1.21. *Si a et b sont des entiers positifs, alors il existe des entiers u et v tels que* $\text{pgcd}(a, b) = au + bv$.

Démonstration. Admise. □

En s'inspirant de l'algorithme d'Euclide, on peut à partir de deux entiers a et b trouver $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$. Notons $r_{-1} = a$ et $r_0 = b$. En notant q_1 et r_1 le quotient et le reste de la division euclidienne de r_0 par r_{-1}, on obtient $r_0 = q_1 r_{-1} + r_1$. On note alors q_2 et r_2 le quotient et le reste de la division euclidienne de r_1 par r_0 pour obtenir $r_1 = q_2 r_0 + r_2$. En continuant ainsi, à l'étape i on a $r_{i-1} = q_i r_{i-2} + r_i$. Notons N l'entier tel que $r_N = 0$. Un tel N existe d'après l'algorithme d'Euclide. L'idée est maintenant de cpnctruire deux suites u_i et v_i pour $i = -1, 0, ..., N$ tels que $au_i + bv_i = r_i$. Comme $a = r_{-1}$ et $b = r_0$, on a $u_{-1} = 1$, $v_{-1} = 0$, $u_0 = 0$ et $v_0 = 1$. Supposons qu'on ait construit u_{i-2}, v_{i-2}, u_i et v_i pouur $i \in \{1, ..., N\}$. On recherche alors u_i et v_i tels que $au_i + bv_i = r_i$. Par construction de r_i, on a $r_{i-1} = q_i r_{i-2} + r_i$ et donc $r_i = r_{i-1} - q_i r_{i-2}$. D'où

$$\begin{aligned} au_i + bv_i &= r_{i-1} - q_i r_{i-2} \\ &= (au_{i-1} + bv_{i-1}) - q_i(au_{i-2} + bv_{i-2}) \\ &= a(u_{i-1} - q_i u_{i-2}) + b(v_{i-1} - q_i + v_{i-2}) \end{aligned}$$

On pose alors $u_i = u_{i-1} - q_i u_{i-2}$ et $v_i = v_{i-1} - q_i + v_{i-2}$. Comme $r_N = 0$, on a $\text{pgcd}(a, b) = r_{N-1}$ et donc $au_{N-1} + bv_{n-1} = r_{n-1} = \text{pgcd}(a, b)$. Il suffit alors de prendre $u = u_{n-1}$ et $v = v_{n-1}$.

Exercice 1.22. Déterminer des entiers u et v tels que $585u + 247v = \text{pgcd}(585, 247)$.

Théorème 1.23. *Si a et b sont des entiers positifs, alors a et b sont premiers entre eux si et seulement s'il existe u et v tels que $au + bv = 1$.*

Exercice 1.24. Démontre ce théorème.

Théorème 1.25 (de Gauss)**.** *Soient a, b et c des entiers positifs. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.*

Démonstration. D'après la proposition précédente, on a $\mathrm{pgcd}(ac, bc) = c\,\mathrm{pgcd}(a, b)$. Or a et b sont premiers entre eux, d'où $\mathrm{pgcd}(a, b) = 1$ et conc $\mathrm{pgcd}(ac, bc) = c$. Puisque a divise ac et a divise bc par hypothèse, a divise le pgcd de ac et bc qui est c. □

Exercice 1.26.

1. Existe-t-il des entiers $x$et y tels que $161x + 368y = 15$? Si oui, les trouver tous.

2. Existe-t-il des entiers $x$et y tels que $161x + 368y = 115$? Si oui, les trouver tous.

Lemme 1.27 (d'Eculide)**.** *Soient a et b des entiers positifs et p un nombre premier. Si p divise ab, alors p divise a ou p divise b.*

Démonstration. Supposons que p ne divise pas a. D'après le lemme 1.18, p et a sont premiers entre eux. D'où, par le théorème de Gauss, p divise b.

□