Lyce Saint-Henri IV-Le Grand

arithmtique

cours avec exercices


EVCLIDI MEGAREN

1 Divisibilit dans $\mathbb{N}$

1 1 Diviseurs

Définition 1

Soient d et n des entiers naturels. On dit que d divise (*ou* « est un diviseur de » *ou* « est divisible par ») n s'il existe $q \in \mathbb{N}$ tel que $n = dq$.

Exemple. Le nombre 385 est divisible par 5 car $385 = 5 \times 77$.

Remarques.

a. Le nombre 1 divise tous les nombres. C'est le seul avoir cette proprit.

b. Un nombre n est toujours divisible par n.

c. Le seul nombre divisible par 0 est 0 lui-mme.

d. Le nombre 0 est divisible par tous les nombres. C'est le seul avoir cette proprit.

Définition 2

Soit n un entier naturel. L'ensemble des diviseurs de n, not $\mathscr{D}(()n)$, est l'ensemble des $d \in \mathbb{N}$ qui divisent n.

Exemple. On a $\mathscr{D}(385) = \{1, 5, 7, 11, 35, 55, 77, 385\}$. On verra plus tard une mthode simple pour justifier rigoureusement cela.

Propriétés 1

a. Si dd' divise n, alors d divise n et d' divise n.

b. Si $n \neq 0$ et si d divise n, alors $1 \leq d \leq n$.

c. Si d divise b et si c divise d, alors c divise n.

d. Si d divise n et m, alors d divise $un + vm$ pour tous les entiers u et v.

1 2 Multiples

Définition 3

Soient n et m deux entiers naturels. On dit que m est un multiple de n s'il existe $k \in \mathbb{N}$ tel que $m = kn$.

Exemple. Le nombre 42 est un multiple de 6 car $42 = 6 \times 7$.

Propriété 2

m est un multiple de n si et seulement si n divise m.

2 Division euclidienne dans $\mathbb{N}$

Théorème 1

Soient a et b deux entiers naturels. Si $b \neq 0$, alors il existe un unique couple (q, r) tel que

$$a = bq + r \quad \text{avec } 0 \leq r < b.$$

Démonstration. Puisque b est non nul, il existe q tel que $bq \leq a < b(q+1)$. On pose $r = a - bq$ et on a le rsultat voulu. □

Exemple. Trouvons la division euclidienne de 314 par 78. On a $2\times 78 = 156$, $3\times 78 = 234$, $4 \times 78 = 312$ et $5 \times 78 = 390$ et donc $312 \leq 314 < 390$, d'o $q = 4$ et $r = 314 - 312 = 2$. La division euclidienne est donc $314 = 78 \times 4 + 2$.

Définition 4

L'entier q est appel le *quotient* de la division euclidienne et l'entier r est le *reste* de la division euclidienne.

Propriétés 3

a. Le nombre b divise a si et seulement si $r = 0$.
b. Si $b < a$, alors $q = 0$ et $r = b$.
c. Tout entier n positif s'crit sous la forme $bq+r$ avec $r = 0$, $r = 1, \dots$ ou $r = n-1$.

3 Diviseurs communs deux entiers

3 1 Dfinition

Définition 5

Si a et b sont deux entiers naturels, on note $\mathscr{D}(a, b)$ l'ensemble des diviseurs communs a et b.

Exemple. On a $\mathscr{D}(12, 8) = \{1, 2, 4\}$.

Propriétés 4

a. Si a et b sont deux entiers naturels, $\mathscr{D}(a, b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.
b. On a toujours $1 \in \mathscr{D}(a, b)$.
c. Si $d \in \mathscr{D}(a, b)$ avec $a \neq 0$ et $b \neq 0$, alors $d \leq \max(a, b)$.
d. $\mathscr{D}(a, 0) = \mathscr{D}(a)$.

Théorème 2

Si a et b ne sont pas tous nuls, l'ensemble $\mathscr{D}(a, b)$ a un plus grand lment d que l'on appelle le *pgcd* (plus grand diviseur commun) de a et b.

Démonstration. Si $a = 0$ et $b \neq 0$, on a $\mathscr{D}(a, b) = \mathscr{D}(a, 0) = \mathscr{D}(a)$ et donc $d = a$ convient ; si $b = 0$ et $a \neq 0$, de mme $d = b$ convient. Si $a \neq 0$ et $b \neq 0$, alors, d'aprs la proprit **??**, l'ensemble $\mathscr{D}(a, b)$ est non vide et est major ; il possde donc un plus grand lment d. □

Remarque. Le pgcd de 0 et 0 n'est pas dfini car $\mathscr{D}(0, 0) = \mathscr{D}(0) = \mathbb{N}$ n'a pas de plus grand lment.

3 2 Algorithme d'Euclide

L'algorithme d'Euclide permet de trouver le pgcd de deux nombres. L'ide est de construire une suite d'entiers r_i tels que

$$\mathscr{D}(a, b) = \mathscr{D}(b, r_1) = \mathscr{D}(r_1, r_2) = \dots \mathscr{D}(r_n, 0) = \mathscr{D}(r_n)$$

auquel cas r_n sera le plus grand diviseur commun a et b.

1. Ensemble des diviseurs et division euclidiennes

Lemme 1

Soient a et b deux entiers naturels non nuls. Si on peut crire $a = bq + r$ avec $q, r \in \mathbb{N}$ (on ne suppose pas *a priori* que $0 \leq r < b$), alors $\mathscr{D}(a,b) = \mathscr{D}(b,r)$.

Démonstration. Si $d \in \mathscr{D}(a,b)$, alors d divise a et b donc divise $a - bq = r$ et donc $d \in \mathscr{D}(b,r)$. Rciproquement, si $d \in \mathscr{D}(b,r)$, alors d divise $bq + r = a$ et donc $d \in \mathscr{D}(a,b)$. □

2. Divisions euclidiennes successives

Théorème 3

Algorithme d'Euclide

Soient a et b deux entiers naturels non nuls. On crit les divisions euclidiennes successives

$$\begin{array}{lll} a = bq_1 + r_1 & \text{avec } 0 \leq r_1 < b & \\ b = r_1 q_2 + r_2 & \text{avec } 0 \leq r_2 < r_1 & (\text{possible si } r_1 \neq 0) \\ r_1 = r_2 q_3 + r_3 & \text{avec } 0 \leq r_3 < r_2 & (\text{possible si } r_2 \neq 0) \\ \ldots & & \end{array}$$

Il existe un rang $n \in \mathbb{N}^*$ tel que $r_n = 0$.

Démonstration. Il suffit de remarquer que s'il n'existait pas de rang n tel que $r_n = 0$, alors la suite (r_i) serait une suite strictement dcroissante d'entiers naturels, ce qui est absurde. □

3. Consquence pour le pgcd

Corollaire 1

Soient a et b deux entiers naturels non tous nuls. Le pgcd de a et b est l'unique entier d tel que $\mathscr{D}(a,b) = \mathscr{D}(d)$.

Démonstration. C'est juste une reformulation de l'algorithme d'Euclide : $\mathscr{D}(a,b) = \mathscr{D}(b,r_1) = \cdots = \mathscr{D}(r_n, 0) = \mathscr{D}(r_n)$ et donc le plus grand lment de $\mathscr{D}(a,b)$ est $d = r_n$. □

3 3 Relation de Bzout

Théorème 4

Soient a et b deux entiers naturels non tous nuls. Un entier d est le pgcd de a et b si et seulement si d divise a et b et s'il existe u et v tels que

$$au + bv = d$$

Démonstration. $\Longleftarrow$: Supposons que d divise a et b et qu'on puisse crire $d = au + bv$. Si c est un diviseur commun a et b, alors c divise $au + bv = d$; autrement dit, tout lment de $\mathscr{D}(a,b)$ divise d ; on en dduit que le pgcd de a et b est $\leq d$. Puisqu'il est aussi $\geq d$ car $d \in \mathscr{D}(a,b)$, on conclut que d est le pgcd de a et b ;

$\Longrightarrow$: Soit d le pgcd de a et b ; il est vident que d divise a et b ; montrons l'existence de u et v. On utilise l'algorithme d'Euclide :

$$\begin{array}{l} a = bq_1 + r_1 \quad \text{avec } 0 \leq r_1 < b \\ b = r_1 q_2 + r_2 \quad \text{avec } 0 \leq r_2 < r_1 \ (\text{possible si } r_1 \neq 0) \\ r_1 = r_2 q_3 + r_3 \quad \text{avec } 0 \leq r_3 < r_2 \ (\text{possible si } r_2 \neq 0) \\ \ldots \\ r_{n-1} = r_n q_{n+1} + 0 \end{array}$$

On a $d = r_n$. Montrons par rcurrence sur $i \leq n$ que l'on peut crire $r_i = au_i + bv_i$. On a

$$r_1 = a - bq_1 \quad et donc u_1 = 1 \quad \text{et} \quad v_1 = -q_1.$$

Supposons que $r_i = au_i + bv_i$ avec $i < n$ et montrons que $r_{i+1} = au_{i+1} + bv_{i+1}$. On a

$$r_{i+1} = r_{i-1} - q_{i+1}r_i = au_{i-1} + bv_{i-1} - q_{i+1}(au_i + bv_i) = a(u_{i-1} - q_{i+1}u_i) + b(v_{i-1} - q_{i+1}v_i),$$

et donc le choix $u_{i+1} = u_{i-1} - q_{i+1}u_i$ et $v_{i+1} = v_{i-1} - q_{i+1}v_i$ convient. En particulier, pour $i = n$, on obtient, en posant $u_n = u$ et $v_n = v$,

$$d = r_n = au_n + bv_n = au + bv.$$

La dmonstration est termine. □

4 Proprits du pgcd

4 1 Entiers premiers entre eux

Définition 6

Deux entiers naturels non nuls a et b sont dit premiers entre eux si et seulement si leur pgcd vaut 1.

Lemme 2

lemme de Gauss

Soient a, b et c des entiers naturels non nuls. Si a divise bc avec a et b premiers entre eux, alors a divise b ou a divise c.

Démonstration. Puisque a et b sont premiers entre eux, il existe u et v tels que $au + bv = 1$; en multipliant par c, on obtient $acu + bcu = c$. Puisque a divise bc, on en dduit que a divise c. □

Corollaire 2

Soient a et b deux entiers naturels premiers entre eux. Si a et b divisent n, alors ab divise n.

Démonstration. Puisque a divise n, on peut crire $n = aq$; puisque b divise n, il divise aq et puisque a et b sont premiers entre eux, b divise q et donc on peut crire $q = bk$ et donc $n = abk$, ce qui montre que ab divise n. □

4 2 Mutliplicativit

Propriété 5

Soient a, b et c trois entiers naturels non nuls et d le pgcd de a et b. Le pgcd de ac et bc est dc.

Démonstration. Il est vident que dc est un diviseur commun ac et bc. C'est le pgcd car on peut crire $au + bv = d$ et donc $(ac)u + (bc)v = dc$. □

5 Notion de ppcm

5 1 Dfinition

L'ensemble des multiples communs a et b est non vide (il contient ab) et minor par $\min(a, b)$; il possde donc un plus petit lment, not m et appel le *ppcm* (plus petit commun multiple) de a et b.

5 2 Lien avec le pgcd

Propriété 6

Soient a et b deux entiers naturels non nuls, d leur pgcd et m leur ppcm.

a. $md = ab$.

b. Tout multiple commun a et b est multiple de m.

Démonstration.

a. Notons tout d'abord que $m' = \frac{ab}{d}$ est un multiple commun a et b ; en effet, si on pose $a = da'$ et $b = db'$, on a $m' = a'b$ donc m' est un multiple de b et $m' = ab'$ donc m' est un multiple de a.

Reste montrer que $m' = m$. Soit μ un multiple quelconque de a et b ; puisque μ est un multiple commun a et b donc on peut crire $\mu = ak$ et $\mu = bk'$. On a donc $a'dk = b'dk'$ d'o $a'k = b'k'$; puisque a' et b' sont premiers entre eux (consquence de la relation de Bzout), on en dduit que a' divise k' et donc $k' = a'k''$; ainsi, $m = a'b'dk'' = m'k''$ et donc $m' \leq \mu$, ce qui montre que μ est multiple de m' ; le multiple μ tant arbitraire, on en dduit que m' est le ppcm de a et b.

b. Comme on vient de le voir, tout multiple de a et b est multiple de $m' = m$, d'o le rsultat.

$\square$

Exercices et problmes

Diviseurs et multiples

1 crire la liste des diviseurs des nombres suivants.

13, 56, 198, 6754, 12553.

2 crire la liste des multiples ≤ 200 des nombres suivants.

7, 36, 27, 89, 101, 59, 13.

3 Si $a \in \mathbb{N}$, montrer que $a(a-1)$ est pair et que $a(a^2-1)$ est divisible par 3.

4 ★ Dterminer les entiers n tels que $u_n = n^2 - 3n + 6$ soit un multiple de n.

Division euclidienne

5 Effectuer les divisions euclidiennes de a par b dans les cas suivants.

a. $a = 87$ et $b = 5$.
b. $a = 454$ et $b = 33$.
c. $a = 765$ et $b = 890$.
d. $a = 8997$ et $b = 654$.

6 On effectue la division euclidienne de $a = 124$ par un entier b et on trouve un quotient q un reste gal $r = 9$. Quelles sont les valeurs possibles de b et q ?

7 On crit $a = bq + r$ la division euclidienne de a par b. Quelle est la division euclidienne de $a + 1$ par b ? de $a + kb$ par b ?

Algorithme d'Euclide, pgcd

8 En utilisant l'algorithme d'Euclide, calculer le pgcd des nombres a et b suivants.

a. $a = 87$ et $b = 5$.
b. $a = 454$ et $b = 33$.
c. $a = 765$ et $b = 890$.
d. $a = 8997$ et $b = 654$.

9 On effectue l'algorithme d'Euclide pour des nombres a et b et on trouve pour pgcd $r_4 = 39$ et comme suite de quotients successifs $q_1 = 1$, $q_2 = 5$, $q_3 = 1$, $q_4 = 6$ et $q_5 = 2$. Quelle est la valeur de a et b ?

10 ★ Trouver des entiers naturels tels que $a + b = 72$ et $\operatorname{pgcd}(a, b) = 8$.

11 Reprendre les entiers de l'exercice **??** et crire une relation de la forme $au + bv = d$ o $d = \operatorname{pgcd}(a, b)$.

ppcm

12 Reprendre les entiers de l'exercice **??** et trouver leur ppcm.

13 Trouver deux entiers naturels a et b tels que $\operatorname{pgcd}(a, b) = 24$ et $\operatorname{ppcm}(a, b) = 2160$.

14 Vrifier que

$$\begin{aligned}\operatorname{ppcm}(1,2,3,4) = 2\sin\tfrac{\pi}{2} \times 2\sin\tfrac{\pi}{3} \times 2\sin\tfrac{2\pi}{3} \\ \times 2\sin\tfrac{\pi}{4} \times 2\sin\tfrac{3\pi}{4}\end{aligned}$$

(On fait le produit sur les $2\sin\frac{k\pi}{n}$ avec k et n premiers entre eux pour $n = 2$, 3 ou 4.)

1 Dfinitions

Définition 1 Un nombre entier $p \geq 2$ est *premier* s'il divisible uniquement par 1 et par lui-mme.

Remarque. Noter que 1 n'est pas un nombre premier. La raison est que c'est le seul nombre qui divise tous les autres. Les nombres premiers ont une proprit moins forte : tout nombre ≥ 2 est divisible par un nombre premier.

Exemples.

a. Les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, etc. Il y a une infinit de nombre premiers, comme on le verra dans le corollaire **??**.

b. L'un des nombres premiers les plus grands est $2^{43112609} - 1$ (c'est un nombre premier de Mersenne, c'est–dire un nombre premier de la forme $2^k - 1$).

2 Proprits de divisibilit des nombres premiers

Lemme 1 **Lemme de Gauss**

Un nombre $p \geq 2$ est premier si et seulement si $p \mid ab \implies p \mid a$ ou $p \mid b$.

Démonstration. Soit $p \geq 2$ vrifiant $p \mid ab \implies p \mid a$ ou $p \mid b$. Si d divise p, alors on peut crire $p = dq$ et donc $p \mid d$ ou $p \mid q$. Dans le premier cas, $d = p$, et dans le second, $d = 1$, ce qui montre que les seuls diviseurs de p sont 1 et p.

Rciproquement, considrons un nombre premier p et supposons que $p \mid ab$. Le pgcd de p et a est soit 1 soit p ; si ce n'est pas p, alors on peut crire $pu + av = 1$ et donc $pub + abv = b$ c'est–dire que p divise b vu que $p \mid ab$. □

3 Dcomposition en facteurs premiers

3 1 Thorme fondamental

Théorème 1 **Thorme fondamental de l'arithmtique**

Tout nombre premier $n \geq 2$ s'crit comme produit de nombres premiers.

Démonstration. Pour l'existence, on procde par rcurrence. Si $n = 2$, c'est vident car n est premier. Si $n \geq 3$ n'est pas premier, alors on peut l'crire sous la forme $n = dq$ avec $1 < d < n$ et $1 < q < n$. Par hypothse de rcurrence, d et q sont des produits de nombres premiers et donc il en est de mme de n.

Montrons l'unicit en utilisant le lemme de Gauss (lemme **??**). Si $n = p_1 \dots p_r = q_1 \dots q_s$ avec les p_i et les q_j premiers, alors, puisque $p_1 \mid q_1 \dots q_s$, p_1 divise un des q_j, disons q_1 (quitte r-indexer les q_j si ncessaire) ; ces deux nombres tant premiers, on en dduit que $p_1 = q_1$ et donc on obtient $p_2 \dots p_r = q_2 \dots q_s$. Le mme raisonnement fournit $p_2 = q_2$ (quitte rindexer les q_j au besoin), etc. Finalement, $r = s$ et $p_i = q_i$ pour tout i. □

Tout entier $n \geq 2$ s'crit donc de manire unique sous la forme $n = p^{\alpha_1} \ldots p_r^{\alpha_r}$ avec les p_i des nombres premiers distincts et les α_i des entiers ≥ 1.

Exemples.

a. $24 = 2^3 \times 3$

b. $255 = 3 \times 5 \times 17$

c. $663 = 7 \times 13 \times 17$

3 2 Consequences

Soit $n \geq 2$ qu'on crit sous la forme $n = p^{\alpha_1} \ldots p_r^{\alpha_r}$ avec les p_i des nombres premiers deux deux distincts. On pose $v_{p_i}(n) = \alpha_i$ et $v_p(n) = 0$ si p n'est pas l'un des p_i. Ceci permet d'crire

$$n = \prod_{p \text{ premier}} p^{v_p(n)}.$$

Corollaire 1

Calcul du pgcd

$$\operatorname{pgcd}(m, n) = \prod_{p \text{ premier}} p^{\min(v_p(n), v_p(m))}$$

Exemple. Le pgcd de $24 = 2^3 \times 3$ et $306 = 2 \times 3^2 \times 17$ est $2^1 \times 3^1 \times 17^0 = 6$.

Corollaire 2

Calcul du ppcm

$$\operatorname{ppcm}(m, n) = \prod_{p \text{ premier}} p^{\max(v_p(n), v_p(m))}$$

Exemple. Le ppcm de $24 = 2^3 \times 3$ et $306 = 2 \times 3^2 \times 17$ est $2^3 \times 3^2 \times 17^1 = 1224$.

4 Quelques proprits de l'ensemble des nombres premiers

Théorème 2

Thorme d'Euclide

Il existe une infinit de nombre premiers.

Démonstration. Considrons un ensemble fini $\{p_1, \ldots, p_r\}$ de nombre premiers et posons $N = p_1 \ldots p_r + 1$. Le nombre N est ≥ 2 donc est divisible au moins par un nombre premier q, mais ce nombre premier ne peut tre l'un des p_i car aucun des p_i ne divise N (dans le cas contraire, ce p_i diviserait 1). Ceci montre qu' chaque fois qu'on a un nombre fini de nombres premiers, on peut en construire un autre ; c'est le rsultat voulu. □

Exercices et problmes

Nombres premiers

Pour les deux exercices suivants, dire si les nombres donns sont premiers.

1 353 ; 457 ; 101 ; 89 ; 113.

2 1453 ; 1267 ; 7651 ; 1789.

3 Les nombres 1, 11, 111, 1111, 11111, 111111 sont-ils premiers ?

4 crire la liste des nombres premiers compris entre 100 et 200.

Dcompositions en facteurs premiers

Pour les deux exercices suivants, trouver la dcomposition en facteurs premiers des nombres donns. En dduire l'ensemble des diviseurs de chacun des nombres

5 567 ; 546 ; 897 ; 564 ; 890.

6 4637 ; 3560 ; 9884 ; 2010.

7 ★ On pose $n = 900\ldots0$. Combien faut-il de zros pour que b admette 108 diviseurs (positifs) ?

8 Comment reconnat-on sur la dcomposition en facteurs premiers de n que n est un carr ?

9 On pose $u_0 = 2$ et $u_{n+1} = 1 + \prod_{p \text{ premier}} p^{v_p(u_n)}$.

a. O a-t-on dj rencontr cette suite ?

b. Calculer u_1, u_2, u_3, u_4, u_5.

10 **a.** Montrer que si n et m sont deux nombres premiers entre eux tels que nm est un carr, alors n et m sont des carrs ?

b. Le rsultat prcdent reste-t-il valable pour des puissances k-imes avec $k \geq 2$?

Pgcd et ppcm

11 Pour chacun des couples suivants, trouver leur pgcd et leur ppcm en utilisant la dcomposition en facteurs premiers.

$$(1236, 764)\ ; \quad (784, 8760)\ ; \quad (765, 875).$$

Ensemble des nombres premiers

12 Dmontrer que la suite $((n+2)! + k)_{2 \leq k \leq n+1}$ est une suite de n nombres tous non premiers.

13 ★ Montrer qu'il existe une infinit de nombre premiers de la forme $4k - 1$.

14 ★★ Montrer qu'il existe une infinit de nombre premiers de la forme $4k + 1$.

Exercices de recherche

15 ★★★ Montrer que si p est premier et si a est premier p, alors $a^{p-1} - 1$ est divisible par p.

16 ★★ Soit n un nombre tel que, pour tout a premier p, le nombre $a^{p-1} - 1$ est divisible par n. Est-ce que n est premier ?

17 ★★★ Montrer que p est premier si et seulement si $(p-1)! + 1$ est divisible par p.