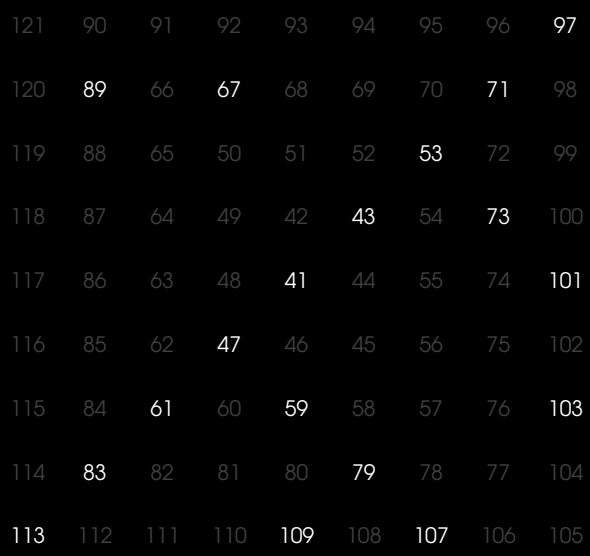
2009-2010

Terminale S

Arithmétique



Lycée Saint-Henri IV-Le Grand

arithmétique

cours avec exercices

SOMMAIRE

CHAPITRE 1

Divisibilité, PGCD, PPCM

Euclide, en grec ancien *Eukleidês* (né vers –325, mort vers –265 à Alexandrie) est un mathématicien de la Grèce antique ayant probablement vécu en Afrique, auteur des Éléments, qui sont considérés comme l'un des textes fondateurs des mathématiques modernes.

Peu d'informations sont connues à propos de la vie d'Euclide. Contemporain d'Archimède (né en –287 et mort en –212), il naît vers –325 et meurt vers –265, mais, selon le mathématicien Christian Velpryses, ses dates de naissance et de mort sont inconnues.

Il part en Égypte pour y enseigner les mathématiques sous le règne de Ptolémée Ier. Il travaille au musée d'Alexandrie et à l'école de mathématiques. Entouré de ses disciples, il mène de nombreux travaux de recherche.

(*Source :* Wikipédia)

1 Divisibilité 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 à avoir cette propriété.

b. Un nombre n est toujours divisible par n.

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

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

Définition 2

Soit n un entier naturel. L'ensemble des diviseurs de n, noté $\mathscr{D}(()n)$, 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 méthode 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 résultat 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'où $q = 4$ et $r = 314 - 312 = 2$. La division euclidienne est donc $314 = 78 \times 4 + 2$.

Définition 4

L'entier q est appelé 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'écrit sous la forme $bq + r$ avec $r = 0$, $r = 1$, ... ou $r = n - 1$.

3 Diviseurs communs à deux entiers

3 1 Définition

Définition 5

Si a et b sont deux entiers naturels, on note $\mathscr{D}(a,b)$ l'ensemble des diviseurs communs à 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 élément 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 même $d = b$ convient. Si $a \neq 0$ et $b \neq 0$, alors, d'après la propriété 4, l'ensemble $\mathscr{D}(a,b)$ est non vide et est majoré ; il possède donc un plus grand élément d. □

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

3 2 Algorithme d'Euclide

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

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

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

1. Ensemble des diviseurs et division euclidiennes

Lemme 1

Soient a et b deux entiers naturels non nuls. Si on peut écrire $a = bq + r$ 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 $d \in \mathscr{D}(b,r)$. Réciproquement, 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 écrit les divisions euclidiennes successives

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

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 décroissante d'entiers naturels, ce qui est absurde. □

3. Conséquence 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 : $\mathscr{D}(a,b) = \mathscr{D}(b,r_1) = \dots = \mathscr{D}(r_n,0) = \mathscr{D}(r_n)$ et donc le plus grand élément de $\mathscr{D}(a,b)$ est $d = r_n$. □

3 3 Relation de Bézout

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 écrire $d = au + bv$. Si c est un diviseur commun à a et b, alors c divise $au + bv = d$; autrement dit, tout élément de $\mathscr{D}(a,b)$ divise d ; on en déduit 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 évident que d divise a et b ; montrons l'existence de u et v. On utilise l'algorithme d'Euclide :

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

On a $d = r_n$. Montrons par récurrence sur $i \leq n$ que l'on peut écrire $r_i = au_i + bv_i$. 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 démonstration est terminée. □

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

4 2 Mutliplicativité

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

5 Notion de ppcm

5 1 Définition

L'ensemble des multiples communs à a et b est non vide (il contient ab) et minoré par $\min(a, b)$; il possède donc un plus petit élément, noté m et appelé 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 à a et b est multiple de m.

Démonstration.

a. Notons tout d'abord que $m' = \frac{ab}{d}$ est un multiple commun à 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 à montrer que $m' = m$. Soit μ un multiple quelconque de a et b ; puisque μ est un multiple commun à a et b donc on peut écrire $\mu = ak$ et $\mu = bk'$. On a donc $a'dk = b'dk'$ d'où $a'k = b'k'$; puisque a' et b' sont premiers entre eux (conséquence de la relation de Bézout), on en déduit 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 étant arbitraire, on en déduit 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'où le résultat.

□

Exercices et problèmes

Diviseurs et multiples

1 Écrire la liste des diviseurs des nombres suivants.

13, 56, 198, 6754, 12553.

2 Écrire 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 ★ Déterminer 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 égal à $r = 9$. Quelles sont les valeurs possibles de b et q ?

7 On écrit $a = bq + r$ 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 $\text{pgcd}(a, b) = 8$.

11 Reprendre les entiers de l'exercice 8 et écrire une relation de la forme $au + bv = d$ où $d = \text{pgcd}(a, b)$.

ppcm

12 Reprendre les entiers de l'exercice 8 et trouver leur ppcm.

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

14 Vérifier que

$$\text{ppcm}(1,2,3,4) = 2\sin\tfrac{\pi}{2} \times 2\sin\tfrac{\pi}{3} \times 2\sin\tfrac{2\pi}{3} \times 2\sin\tfrac{\pi}{4} \times 2\sin\tfrac{3\pi}{4}$$

(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.)

CHAPITRE 2

Nombres premiers

Johann Carl Friedrich Gauss (30 avril 1777 – 23 février 1855) est un mathématicien, astronome et physicien allemand. Doté d'un grand génie, il a apporté de très importantes contributions à ces trois sciences. Surnommé « le prince des mathématiciens », il est considéré comme l'un des plus grands mathématiciens de tous les temps.

La qualité extraordinaire de ses travaux scientifiques était déjà reconnue par ses contemporains. Dès 1856, le roi de Hanovre fit graver des pièces commémoratives avec l'image de Gauss et l'inscription Mathematicorum Principi (« prince des mathématiciens » en latin). Gauss n'ayant publié qu'une partie infime de ses découvertes, la postérité découvrit la profondeur et l'étendue de son œuvre uniquement lorsque son journal intime, publié en 1898, fut découvert et exploité.

Considéré par beaucoup comme distant et austère, Gauss ne travailla jamais comme professeur de mathématiques, détestait enseigner et collabora rarement avec d'autres mathématiciens. Malgré cela, plusieurs de ses étudiants devinrent de grands mathématiciens, notamment Richard Dedekind et Bernhard Riemann.

Gauss était profondément pieux et conservateur. Il soutint la monarchie et s'opposa à Napoléon qu'il vit comme un semeur de révolution.

(*Source :* Wikipédia)

1 Définitions

Définition 1

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

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 propriété 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 infinité de nombre premiers, comme on le verra dans le corollaire 2.

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

2 Propriétés de divisibilité 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 $p \geq 2$ vérifiant $p \mid ab \implies p \mid a$ ou $p \mid b$. Si d divise p, alors on peut écrire $p = dq$ 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.
Réciproquement, considérons 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 écrire $pu + av = 1$ et donc $pub + abv = b$ c'est-à-dire que p divise b vu que $p \mid ab$. □

3 Décomposition en facteurs premiers

3 1 Théorème fondamental

Théorème 1

Théorème fondamental de l'arithmétique
Tout nombre premier $n \geq 2$ s'écrit comme produit de nombres premiers.

Démonstration. Pour l'existence, on procède par récurrence. Si $n = 2$, c'est évident car n est premier. Si $n \geq 3$ n'est pas premier, alors on peut l'écrire sous la forme $n = dq$ avec $1 < d < n$ et $1 < q < n$. Par hypothèse de récurrence, d et q sont des produits de nombres premiers et donc il en est de même de n.
Montrons l'unicité en utilisant le lemme de Gauss (lemme 1). 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 à ré-indexer les q_j si nécessaire) ; ces deux nombres étant premiers, on en déduit que $p_1 = q_1$ et donc on obtient $p_2 \dots p_r = q_2 \dots q_s$. Le même raisonnement fournit $p_2 = q_2$ (quitte à réindexer les q_j au besoin), etc. Finalement, $r = s$ et $p_i = q_i$ pour tout i. □

Tout entier $n \geq 2$ s'écrit donc de manière unique sous la forme $n = p^{\alpha_1} \dots p_r^{\alpha_r}$ 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 Conséquences

Soit $n \geq 2$ qu'on écrit sous la forme $n = p^{\alpha_1} \dots p_r^{\alpha_r}$ avec les p_i des nombres premiers deux à 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'écrire

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

Corollaire 1

Calcul du pgcd

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

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

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

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 propriétés de l'ensemble des nombres premiers

Théorème 2

Théorème d'Euclide
Il existe une infinité de nombre premiers.

Démonstration. Considérons un ensemble fini $\{p_1, \dots, p_r\}$ de nombre premiers et posons $N = p_1 \dots p_r + 1$. Le nombre N est ≥ 2 donc est divisible au moins par un nombre premier q, mais ce nombre premier ne peut être 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'à chaque fois qu'on a un nombre fini de nombres premiers, on peut en construire un autre ; c'est le résultat voulu. □

Exercices et problèmes

Nombres premiers

Pour les deux exercices suivants, dire si les nombres donnés 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 Écrire la liste des nombres premiers compris entre 100 et 200.

Décompositions en facteurs premiers

Pour les deux exercices suivants, trouver la décomposition en facteurs premiers des nombres donnés. En déduire 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 zéros pour que b admette 108 diviseurs (positifs) ?

8 Comment reconnaît-on sur la décomposition en facteurs premiers de n que n est un carré ?

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

a. Où a-t-on déjà rencontré 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 carré, alors n et m sont des carrés ?

b. Le résultat précédent reste-t-il valable pour des puissances k-ièmes avec $k \geq 2$?

Pgcd et ppcm

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

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

Ensemble des nombres premiers

12 Démontrer 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 infinité de nombre premiers de la forme $4k - 1$.

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

Exercices de recherche

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

16 ★★ Soit n un nombre tel que, pour tout a premier à 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.