Chapitre 5

Nombres premiers

I Exercices

5.1 Les nombres premiers

5.1.a Vérifier si un nombre est premier

Exercice 5.1

Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui même.

1. zéro est-il premier ? Justifier.
2. 1 est-il premier ? Justifier.
3. Indiquer sans justifier les nombres premiers entre 2 et 20.

Exercice 5.2 (Crible d'Ératosthène)

Le crible d'Eratosthène consiste à déterminer tous les nombres premiers inférieurs ou égaux à un nombre donné. Déterminons par exemple tous les nombres premiers inférieurs ou égaux à 100 de la manière suivante, en utilisant le tableau ci-dessous.

1. Barrer 1 qui n'est pas premier.
2. Entourer 2 qui est premier.
3. Les autres multiples de 2 à partir de 4 ne sont pas premiers donc les barrer tous jusqu'à 100.
4. Entourer 3 qui est premier, puis barrer tous ses autres multiples à partir de 9.
5. Continuer ainsi jusqu'à obtenir tous les nombres premiers inférieurs ou égaux à 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Exercice 5.3

Pour chacun des nombres suivants, vérifier s'il est premier et s'il ne l'est pas indiquer son plus petit diviseur : 196, 219, 223, 259.

Exercice 5.4

Même consigne que pour l'exercice 5.3 pour les nombres suivants : 391, 409, 12 319.

Exercice 5.5

Voici un algorithme et le programme correspondant à la calculatrice.

1. Exécuter cet algorithme en complétant le tableau ci-dessous pour $n = 35$.

k											
r											

2. Que fait cet algorithme ?
3. Les nombres 223 et 259 ont été utilisés dans l'exercice 5.3. Combien y aura-t-il de passages dans la boucle Tant que

   a) pour $n = 223$ **b)** pour $n = 259$

4. Modifier cet algorithme et ce programme pour diminuer le nombre de passages dans la boucle.

Entrée(s) : un nombre entier $n \geqslant 2$
Sortie(s) : affichage « Premier » ou sinon affichage « Non premier » et plus petit diviseur.
Variables : des entiers n, k, r

Algorithme	**Programme sur la calculatrice**
Lire n	`Prompt N`
$k \leftarrow 1$	`1→K`
$r \leftarrow 1$	`1→R`
Tant que $r \neq 0$	`While R≠0`
$k \leftarrow k + 1$	`K+1→K`
$r \leftarrow n - k \times \text{Ent}(n/k)$	`N-K*ent(N/K)→R`
Fin du Tant que	`End`
Si $k = n$	`If K=N`
alors	`Then`
afficher « Premier »	`Disp "PREMIER"`
Sinon	`Else`
afficher « Non premier, plus petit diviseur», k	`Disp "NON PREM PLUS P DIV",K`
Fin du Si	`End`

5.1.b Infinitude et répartition des nombres premiers

Exercice 5.6 (Infinitude)

Nous allons démontrer que l'ensemble des nombres premiers est infini. Pour cela, nous allons supposer que l'ensemble des nombres premiers est fini, et nous allons prouver qu'il y alors une impossibilité.

On appelle cette façon de faire une *démonstration par l'absurde*.

Si l'ensemble des nombres premiers est fini alors cet ensemble s'écrit sous la forme : $E = \{p_1, p_2, \cdots, p_n\}$

Soit alors le nombre : $a = p_1 \times p_2 \times \cdots \times p_n + 1$.

Le nombre a admet un diviseur premier. Expliquer où est le problème.

Exercice 5.7 (Répartition)

Pour un entier naturel n, on appelle $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.

1. À l'aide du crible d'Ératosthène de l'exercice 5.2, déterminer $\pi(100)$.
2. Compléter le tableau ci-dessous.
3. D'après ce tableau, comment semble évoluer la fréquence de nombres premiers inférieurs ou égaux à x lorsque x tend vers $+\infty$?
4. Gauss en 1792 et Legendre en 1808 conjecturent que $\pi(x) \approx \dfrac{x}{\ln x}$.
   On appelle cette propriété le *théorème des nombres premiers*. Il a finalement été démontré par Hadamard et De La Vallée Poussin en 1896.

x	100	1 000	10 000	100 000	1 000 000
$\pi(x)$		168	1 229	9 592	78 498
$\frac{\pi(x)}{x}$					
$\frac{x}{\ln x}$					

Exercice 5.8 (Des trous aussi grands que l'on veut)

Dans cet exercice, nous allons montrer qu'on peut obtenir des suites d'entiers naturels successifs sans nombres premiers aussi longues que l'on veut.

Pour cela, nous allons utiliser la factorielle d'un nombre : la factorielle d'un entier naturel n non nul est le produit $n! = 1 \times 2 \times 3 \times \cdots \times n$, par exemple $5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$.

Factorielle sur la calculatrice TI 82 : math PRB 4:

1. Justifier que : $4! + 2$ est multiple de 2, $4! + 3$ est multiple de 3, $4! + 4$ est multiple de 4.
   Il n'est pas utile de calculer 4! pour répondre.
2. Donner sans calcul une suite de 10 nombres consécutifs non premiers.
3. Pour un nombre entier naturel n non nul, indiquer comment obtenir une suite de n nombres consécutifs non premiers.

5.1.c Les nombres de Mersenne et de Fermat

Exercice 5.9 (Nombres de Mersenne)

Marin Mersenne (1588-1648), est un moine français, mathématicien et philosophe qui s'est intéressé aux nombres premiers de la forme $2^n - 1$. On appelle ces nombres les *nombres de Mersenne*. Le plus grand nombre premier connu en 2016 est $2^{274\,207\,281} - 1$, il s'écrit avec plus de 22 millions de chiffres.

1. Compléter le tableau ci-dessous sans détailler ni justifier. Dans la 3e ligne, compléter par *Vrai* ou *Faux*.
2. Le but des questions suivantes est de démontrer la propriété :
   Si n n'est pas premier, alors $2^n - 1$ n'est pas premier.
   a) Vérifier cette propriété dans le tableau.
   b) Si n n'est pas premier, alors il existe des entiers naturels supérieurs ou égaux à 2 tels que $n = rs$. Justifier que $2^n - 1$ est divisible par $2^r - 1$, puis conclure.
   On pourra utiliser l'égalité $a^k - 1 = (a-1)(1 + a + a^2 + \cdots + a^{k-1})$.
3. Écrire la contraposée[1] de la propriété précédente.

1. La contraposée de *Si A alors B* est *Si non B alors non A* et elle est équivalente à *Si A alors B*.

4. Peut-on dire que *si n est premier, alors $2^n - 1$ est premier* ? Justifier.

n	2	3	4	5	6	7	8	9	10	11
$M_n = 2^n - 1$										
Premier ?										

Exercice 5.10 (Nombres de Fermat)

On appelle *nombre de Fermat* un nombre défini par $F_n = 2^{2^n} + 1$ où n est un entier naturel. Pierre de Fermat (1600-1665), magistrat, et mathématicien français conjectura que tous ces nombres sont premiers. Vérifier cette conjecture pour les 6 premiers nombres de Fermat en complétant le tableau ci-dessous.

n	0	1	2	3	4	5
$F_n = 2^{2^n} + 1$						
Premier ?						

5.1.d Système RSA

Le système RSA a été mis au point en secret par les mathématiciens britanniques James Ellis et Clifford Cocks en 1973, puis retrouvée et publiée en 1977 par les américains Ronald Rivest, Adi Shamir (deux informaticiens), et Leonard Adleman (un mathématicien).

Aujourd'hui ce système reste très utilisé pour la sécurité des cartes bancaires et pour la confidentialité des échanges sur Internet.

Propriété mathématique

Si p et q sont des nombres premiers distincts et si e est un entier premier avec $(p-1)(q-1)$, alors,

- il existe un entier d vérifiant $ed \equiv 1\ [(p-1)(q-1)]$,
- et pour tout entier naturel t on a : $(t^e)^d \equiv t\ [pq]$.

Exercice 5.11 (Exemple)

On choisit $p = 3$ et $q = 11$ et on calcule $(p-1)(q-1) = 2 \times 10 = 20$.

Comme nombre e premier avec 20 on choisit $e = 7$, et comme entier d vérifiant $ed \equiv 1\ [20]$ on choisit $d = 3$.

Le nombre t est le nombre associé au texte, par exemple $t = 8$ associé à la lettre H.

1. Codage : la lettre codée est la congruence de $t^e \equiv c\ [pq]$. Calculer le nombre c et laisser le résultat sous forme de nombre.

2. Décodage : le récepteur reçoit ce nombre c et le décode en calculant modulo pq le nombre c^d, c'est à dire $(t^e)^d$, or la propriété ci-dessus indique que $(t^e)^d \equiv t\ [pq]$ ce qui donne la lettre de départ. Vérifier qu'on a bien $c^d \equiv t\ [pq]$.

3. Reprendre le processus précédent (codage puis décodage) avec la lettre S.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Remarque

L'exemple ci-dessus fait intervenir de petits nombres premiers p et q. Dans la réalité ce sont de très grands nombres premiers qui sont utilisés.

Le nombre $n = pq$ et le nombre e sont rendus publics, on dit que le couple $(n\,;\,e)$ est la **clé publique**.

Les nombres p et q sont gardés secrets, or, pour des grands nombres, il est difficile en ayant le nombre n de le décomposer en produit de nombres premiers. On ne peut alors pas calculer le nombre $(p-1)(q-1)$ et on ne peut pas obtenir le nombre d qui permet le décodage.

Le nombre d n'est connu que du récepteur, on l'appelle la **clé privée**.

Enfin, il faut préciser aussi qu'un message n'est en réalité pas codé lettre par lettre mais par blocs de lettres, par exemple le mot MATHÉMATIQUE correspondrait à $t = 1301200805130120091721 05$.

5.2 Décomposition en facteurs premiers

Exercice 5.12 (Exemples)

Tout entier naturel supérieur ou égal à deux admet une unique décomposition sous forme de produit de puissances de nombres premiers, par exemple, $12 = 2^2 \times 3$ et $360 = 2^3 \times 5 \times 3^2$.

Décomposer de cette façon les nombres suivants : 42 ; 72 ; 150 ; 2 904 ; 34 425.

Exercice 5.13 (Diviseurs d'un entier naturel)

1. Écrire les décompositions en facteurs premiers de 252 ; 14 ; 18 ; 33 ; 60.
2. Indiquer parmi 14 ; 18 ; 33 ; 60 lesquels sont des diviseurs de 252.
3. Comment s'écrivent les décompositions en facteurs premiers des diviseurs de 252 ?
4. Déterminer alors tous les diviseurs de 252. On pourra s'aider d'un arbre.
5. 252 a 18 diviseurs : comment aurait-on pu calculer le nombre 18 à l'aide de la décomposition en facteurs premiers de 252 ?

Exercice 5.14

On donne les nombres suivants qu'on ne demande pas de calculer.

$a = 3^4 \times 7^2 \times 19^3$ $b = 3^2 \times 7 \times 19^2$ $c = 3^5 \times 7 \times 19$ $d = 3^2 \times 7^2 \times 11$ $e = 3^3 \times 19^3$

1. Parmi les nombres b, c, d, e, lesquels sont des diviseurs de a ?
2. Calculer le nombre de diviseurs de a.

Exercice 5.15

On donne les nombres suivants qu'on ne demande pas de calculer.

$a = 3^4 \times 5^3 \times 7^3$ $b = 2^5 \times 5^2 \times 7^6$

1. Déterminer d le PGCD de a et b.
2. Écrire les décompositions en facteurs premiers de a, b, d avec les nombres premiers 2 ; 3 ; 5 ; 7 quitte à mettre certains exposants égaux à zéro, puis comparer les trois expressions et leurs exposants.

Exercice 5.16

Déterminer le PGCD de a et b dans les cas suivants.

1. $a = 2^4 \times 5^3 \times 7^3$ $b = 2^5 \times 5 \times 11$
2. $a = 3^2 \times 5^4 \times 7^5$ $b = 3^5 \times 5^2 \times 7^3$
3. $a = 3^4 \times 7^3 \times 13$ $b = 2^5 \times 5^2 \times 11$

5.3 Pour réviser

Chapitre du livre n° 3 – Nombres premiers

Les exercices résolus

- ex 1 p 73 : reconnaître un nombre premier
- ex 2 p 73 : déterminer si un nombre est premier
- ex 10 p 81 : décomposition en facteurs premiers
- ex 11 p 81 : déterminer tous les diviseurs d'un entier naturel

Rubrique *Pour s'exercer*, corrigés page 157

- ex 3 p 73 : vérifier si des nombres sont premiers
- ex 6 p 73 : $n^2 + 2n + 1$ peut-il être premier ?
- ex 12 p 81 : décomposition en facteurs premiers, divisibilité
- ex 14 p 81 : décomposition en facteurs premiers, liste des diviseurs

Rubrique *Objectif bac*, corrigés page 158

- ex 68, 69 p 86 (QCM) : décomposition en facteurs premiers, nombre de Mersenne, division euclidienne, congruence, PGCD
- ex 70, 71 p 86 (Vrai-Faux)
- ex 72 p 87 : exercice de type bac

II Cours

5.1 Définition et propriétés

Définition 5.1

Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui même.

Exemples

Étudions les entiers de 0 à 20.

0 n'est pas premier, il a une infinité de diviseurs.

1 n'est pas premier parce qu'il a un seul diviseur : 1.

Les nombres 2, 3, 5, 7, 11, 13, 17, 19 sont premiers.

Le nombre 4 n'est pas premier puisque 4 a 3 diviseurs : 1, 2, 4.

De même les nombres 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 ne sont pas premiers.

Remarque : d'après ce qui précède un nombre premier est supérieur ou égal à 2.

Propriété 5.1

Deux nombres premiers distincts sont premiers entre eux.

Démonstration

Pour deux nombres premiers distincts p et q, les diviseurs de p sont 1 et p et les diviseurs de q sont 1 et q, donc le seul diviseur commun à p et q est 1, de sorte que p et q sont bien premiers entre eux.

Propriété 5.2

Pour un nombre entier naturel n et un nombre premier p,
p et n sont premiers entre eux si et seulement si p ne divise pas n.

Démonstration

Pour un nombre entier naturel n et un nombre premier p, si p et n sont premiers entre eux, alors il est évident que p ne divise pas n puisque p serait alors un diviseur commun supérieur ou égal à 2.

Réciproquement, si p ne divise pas n, soit d un diviseur commun à p et n.

Ce nombre d divise alors p qui est premier, par conséquent d est égal à 1 ou p. Or d ne peut être égal à p puisque d divise n et p ne divise pas n, donc $d = 1$.

On a prouvé qu'un diviseur commun à p et à n ne peut être qu'égal à 1, donc p et n sont premiers entre eux.

Remarque

La propriété 5.2 n'est plus vraie si p n'est pas premier.

Par exemple si $p = 6$ (non premier) et $n = 15$, alors 6 ne divise pas 15 et pourtant 6 et 15 ne sont pas premiers entre eux puisque leur PGCD est 3.

Propriété 5.3

Pour un nombre entier naturel $n \geqslant 2$,
- si n n'est pas premier, alors il admet un diviseur premier p tel que $p \leqslant \sqrt{n}$;
- si n n'a aucun diviseur premier p tel que $p \leqslant \sqrt{n}$, alors n est premier.

Exemple

Vérifions si 97 est premier. $\sqrt{97} \approx 9,8$

Les nombres premiers inférieurs ou égaux à 9,8 sont : 2, 3, 5, 7.

97 n'est ni multiple de 2 ni de 5.

$9 + 7 = 16$ et 16 n'est pas multiple de 3, donc 97 n'est pas multiple de 3.

$97 = 7 \times 13 + 6$, donc 97 n'est pas multiple de 7.

Donc 97 n'a pas de diviseur premier inférieur ou égal à $\sqrt{97}$, par conséquent 97 est premier.

Démonstration de la première partie de la propriété.

Soit n un entier naturel supérieur ou égal à 2 et non premier. Cela signifie que n admet au moins un diviseur autre que 1 ou lui même.

Soit p le plus petit des diviseurs de n différents de 1.

➡ Démontrons que p est premier.

Soit d un diviseur de p. On peut avoir $d = 1$ ou $d \neq 1$.

Si $d \neq 1$, comme p divise n, le nombre d divise aussi n, or p est le plus petit des diviseurs de n différents de 1, donc $p \leqslant d$, mais comme d divise p, on a aussi $d \leqslant p$, donc finalement, $d = p$.

On a prouvé qu'un diviseur de p ne peut être qu'égal à 1 ou à p, donc p est premier.

➡ Démontrons maintenant que $p \leqslant \sqrt{n}$.

Puisque p est un diviseur de n, il existe un nombre entier naturel k tel que $pk = n$. Le nombre k est différent de 1 puisque sinon $p = n$ ce qui n'est pas le cas. Or p est le plus petit des diviseurs de n différents de 1, donc $p \leqslant k$, donc $p^2 \leqslant pk$, c'est à dire $p^2 \leqslant n$, soit $p \leqslant \sqrt{n}$.

Démonstration de la deuxième partie de la propriété.

La deuxième partie est la contraposée de la première partie. Justifions le.

Pour un nombre entier naturel $n \geqslant 2$, appelons A l'affirmation « n n'est pas premier » et B l'affirmation « n admet un diviseur premier p tel que $p \leqslant \sqrt{n}$ ».

Ainsi l'affirmation « n est premier » est l'affirmation contraire de A, qu'on appelle l'affirmation *non A*. De même l'affirmation « n n'a aucun diviseur premier p tel que $p \leqslant \sqrt{n}$ » est l'affirmation *non B*.

La première partie de la propriété s'écrit alors : *si A alors B*, et la deuxième partie de la propriété s'écrit : *si non B alors non A* et c'est la contraposée de *si A alors B*.

Or, la contraposée d'une propriété est équivalente à cette propriété.

Ainsi les deux parties de cette propriété sont équivalentes, donc la deuxième partie est vraie parce que la première partie est vraie.

Propriété 5.4

Tout nombre entier admet un diviseur premier.

Démonstration

Si un nombre entier naturel est premier, la propriété est vraie parce que ce nombre est divisible par lui même.

Si un nombre entier naturel n'est pas premier, on sait qu'il admet un diviseur premier d'après la propriété 5.3.

Si un nombre entier n est négatif, alors $-n$ est positif et admet un diviseur premier qui divise aussi n.

Propriété 5.5

L'ensemble des nombres premiers est infini.

Démonstration

Nous allons démontrer cette propriété par l'absurde, c'est à dire que nous allons supposer que l'ensemble des nombres premiers est fini et prouver qu'il y alors une impossibilité.

Si l'ensemble des nombres premiers est fini alors cet ensemble s'écrit sous la forme : $E = \{p_1, p_2, \cdots, p_n\}$

Soit alors le nombre : $a = p_1 \times p_2 \times \cdots \times p_n + 1$.

Comme tout nombre entier, le nombre a admet un diviseur premier donc l'un des nombres p_1, ou p_2, ou $\cdots$, ou p_n est un diviseur de a et donc aussi un diviseur de $a - p_1 \times p_2 \times \cdots \times p_n$ qui est égal à 1.

On aurait donc un nombre premier diviseur de 1 ce qui est impossible.

Donc a admet un diviseur premier qui ne fait pas partie de l'ensemble E, par conséquent, cet ensemble ne peut pas être un ensemble fini.

5.2 Décomposition en facteurs premiers

Propriété 5.6 (Décomposition en facteurs premiers)

Tout entier naturel supérieur ou égal à deux admet une unique décomposition sous forme de produit de puissances de nombres premiers.

Exemples

$12 = 2^2 \times 3$ $\qquad$ $360 = 2^3 \times 5 \times 3^2$

Propriété 5.7 (Diviseur d'un entier naturel)

Si la décomposition en facteurs premiers d'un entier naturel n est $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$,
alors la décomposition en facteurs premiers de tout diviseur de n s'écrit :
$p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r}$ avec $\beta_1 \leqslant \alpha_1$, $\beta_2 \leqslant \alpha_2$, $\ldots$, $\beta_r \leqslant \alpha_r$.

Ensemble des diviseurs d'un entier naturel

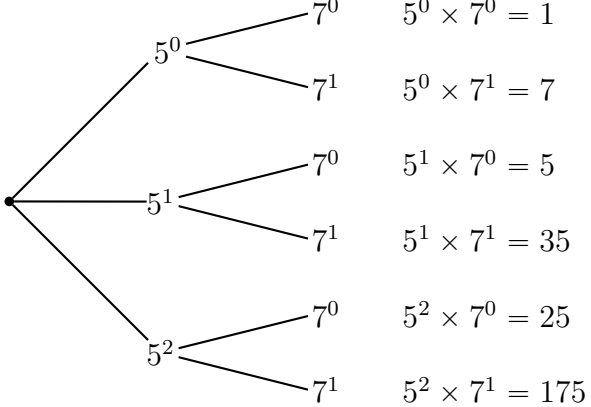
On peut utiliser la décomposition en facteurs premiers d'un entier naturel pour déterminer l'ensemble de ses diviseurs.

Déterminons par exemple l'ensemble des diviseurs de 175.

La décomposition en facteurs premiers de 175 est $175 = 5^2 \times 7$, donc d'après la propriété précédente, tout diviseur de 175 s'écrit : $5^{\beta_1} \times 7^{\beta_2}$ avec $\beta_1 \leqslant 2$, $\beta_2 \leqslant 1$.

Autrement dit β_1 peut être égal à 0, 1 ou 2 et β_2 peut être égal à 0 ou 1.

L'arbre ci-dessous permet de déterminer toutes les combinaisons possibles et donc tous les diviseurs de 175.



L'ensemble des diviseurs de 175 est donc $\boxed{1\,;\,5\,;\,7\,;\,25\,;\,35\,;\,175}$.

Nombre de diviseurs d'un entier naturel

Si la décomposition en facteurs premiers d'un entier naturel est $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, alors le nombre de diviseurs de cet entier naturel est égal à $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \cdots \times (\alpha_r + 1)$.

Par exemple la décomposition en facteurs premiers de 175 est $175 = 5^2 \times 7^1$ et le nombre de ses diviseurs, c'est à dire le nombre de chemins dans l'arbre tracé plus haut est égal à :
$(2 + 1) \times (1 + 1) = 3 \times 2 = \boxed{6}$.

Un autre exemple concernant l'ensemble des diviseurs d'un entier naturel et le nombre de ses diviseurs est détaillé dans l'exercice résolu n° 11 p 81.

Propriété 5.8 (PGCD de deux entiers naturels)

Si les décompositions en facteurs premiers de deux entiers naturels a et b sont :
$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$, et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_r^{\beta_r}$,
alors la décomposition en facteurs premiers du PGCD de a et b est :
$p_1^{\gamma_1} \times p_2^{\gamma_2} \times \cdots \times p_r^{\gamma_r}$ où γ_1 est le plus petit des deux exposants α_1 et β_1, γ_2 est le plus petit des deux exposants α_2 et β_2, etc.

Exemple

Déterminons le PGCD de 1 440 et 324.

$1\,440 = 2^5 \times 3^2 \times 5 = 2^5 \times 3^2 \times 5^1$ et $324 = 2^2 \times 3^4 = 2^2 \times 3^4 \times 5^0$

$\text{PGCD}(1\,440; 324) = 2^{\gamma_1} \times 3^{\gamma_2} \times 5^{\gamma_3}$

γ_1 est le plus petit des deux exposants 5 et 2, γ_2 est le plus petit des deux exposants 2 et 4, γ_3 est le plus petit des deux exposants 1 et 0.

$\text{PGCD}(1\,440; 324) = 2^2 \times 3^2 \times 5^0 = \boxed{36}$

Propriété 5.9 (Nombres premiers entre eux)

Deux entiers naturels sont premiers entre eux si et seulement si ils n'ont aucun diviseur premier en commun.

Exemples

$2 \times 7 = 14$ et $3 \times 11 = 33$ 14 et 33 sont premiers entre eux.

$2^3 \times 7 = 56$ et $3^4 \times 5^2 = 2\,025$ 56 et 2 025 sont premiers entre eux.