4 Nombres premiers

On dit qu'un entier naturel p est **premier** s'il possède *exactement* deux diviseurs positifs : 1 et lui-même.

Un entier naturel ayant plus de deux diviseurs est dit **composé**.

Remarque : par convention, 1 n'est ni premier ni composé.

Théorème des diviseurs premiers

Soit n un entier naturel avec $n \geqslant 2$. Alors :

1) n admet au moins un diviseur premier.

2) Si n n'est pas premier, il admet au moins un diviseur premier p tel que $p \leqslant \sqrt{n}$.

4.1 Le but de cet exercice est de prouver le théorème des diviseurs premiers.

1) Supposons n premier. Quel diviseur premier n admet-il ?
2) Supposons n non premier. Il admet donc au moins un diviseur positif propre. Soit p le plus petit diviseur positif propre de n.
   (a) Montrer par l'absurde que p est premier.
   (b) Il existe $q \in \mathbb{N}$ tel $p\,q = n$. Justifier que $p \leqslant q$.
   (c) En déduire que $p^2 \leqslant n$, puis que $p \leqslant \sqrt{n}$.

Corollaire : test de primalité

Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à sa racine carrée, on peut affirmer qu'il est premier.

4.2 Montrer que 397 est un nombre premier.

Quel est le nombre minimal de diviseurs à tester pour établir ce résultat ?

4.3 Le crible d'Ératosthène[1]

On écrit tous les entiers (de 1 à 100 par exemple) et on va éliminer (en les barrant) successivement tous ceux qui ne sont pas premiers.

On élimine 1 en le barrant : il n'est pas premier.

1. Ératosthène (276-194 avant J.-C.), mathématicien grec de l'école d'Alexandrie (contemporain d'Archimède), est connu pour son crible, mais il était aussi poète, historien, géographe, astronome : il fut le premier à avoir mis en évidence la rotondité de la Terre.

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

1) Le plus petit nombre non barré est 2. On le garde : il est premier. Éliminer tous les autres multiples de 2 (en les barrant), car, par définition, ils ne sont pas premiers.
2) Le plus petit nombre non barré est 3. Puisqu'il est premier, on le garde. Éliminer tous les autres multiples de 3 qui ne sont pas encore barrés.
3) Procéder de même avec 5 et 7.
4) Expliquer alors pourquoi tous les nombres non encore barrés du tableau sont premiers.
5) Si l'on veut dresser la liste des nombres premiers inférieurs ou égaux à 1000, jusqu'à quel nombre premier p faut-il barrer les multiples ?

4.4 Énumérer les cinq nombres consécutifs composés les plus petits.

4.5 Les entiers suivants sont-ils premiers ?

1) 61 2) 661 3) 6661 4) 66 661

4.6 Montrer que tout nombre premier différent de 2 et de 3 est de la forme $6\,q \pm 1$, avec q entier.

Indication : montrer qu'un entier n n'est pas premier si $n \equiv 0 \mod 6$, $n \equiv \pm 2 \mod 6$ ou $n \equiv 3 \mod 6$.

Théorème d'Euclide

Il existe une infinité de nombre premiers.

4.7 Le but de cet exercice est de prouver le théorème d'Euclide par l'absurde. Supposons qu'il existe un nombre fini de nombres premiers : $p_1, p_2, \ldots, p_n$. Posons $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

1) Calculer $q \mod p_i$ pour tout $1 \leqslant i \leqslant n$.
2) Expliquer pourquoi le résultat précédent contredit le théorème des diviseurs premiers et achève ainsi la démonstration.

Décomposition en produit de facteurs premiers

Tout nombre entier $n \geqslant 2$ est un produit de nombres premiers.

Preuve Soit $n \geqslant 2$.

Vu le théorème des diviseurs premiers, il existe un nombre premier p_1 tel que $n = p_1 \cdot q_1$.

Si $q_1 = 1$, on a obtenu le résultat souhaité : $n = p_1$.

Si $q_1 \neq 1$, alors $q_1 \geqslant 2$ et le théorème des diviseurs premiers assure l'existence d'un nombre premier p_2 tel que $q_1 = p_2 \cdot q_2$, d'où suit $n = p_1 \cdot p_2 \cdot q_2$.

Si $q_2 = 1$, le résultat souhaité est atteint : $n = p_1 \cdot p_2$.

Si $q_2 \neq 1$, on recourt à nouveau au théorème des diviseurs premiers pour trouver un nombre premier p_3 tel que $q_2 = p_3 \cdot q_3$, si bien que $n = p_1 \cdot p_2 \cdot p_3 \cdot q_3$.

Si $q_3 = 1$, la démonstration est terminée.

Sinon, on itère ce raisonnement jusqu'à l'obtiention d'un $q_k = 1$. Étant donné que la suite des quotients $q_1, q_2, \ldots, q_k$ est strictement décroissante et à valeurs dans $\mathbb{N}$, on a l'assurance qu'elle est finie. Finalement $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.

Théorème fondamental de l'arithmétique

La décomposition d'un entier $n \geqslant 2$ en facteurs premiers est unique, à l'ordre des facteurs près.

4.8 Cet exercice a pour but de prouver le théorème fondamental de l'arithmétique.

Soit n un entier avec $n \geqslant 2$. Supposons qu'il existe deux décompositions en facteurs premiers : $n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$.

Procédons par récurrence sur r.

Initialisation : supposons $r = 1$.

Montrer que $n = p_1 = q_1 \cdot \ldots \cdot q_s$ entraîne $s = 1$ et $q_1 = p_1$.

Hérédité : supposons $r \geqslant 2$ et le résultat vrai pour $r - 1$.

Grâce au lemme de Gauss, montrer que $n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ implique que p_r divise l'un des facteurs premiers q_i $(1 \leqslant i \leqslant s)$.

Quitte à changer l'ordre des facteurs, on peut supposer que p_r divise q_s. Montrer que $p_r = q_s$, puis que $p_1 \cdot \ldots \cdot p_{r-1} = q_1 \cdot \ldots \cdot q_{s-1}$ et conclure.

4.9 Écrire la décomposition de 2000^{2000} en facteurs premiers.

4.10 Quel est le plus petit entier qui, multiplié par 1998, donne un carré parfait ?

Diviseurs d'un entier

Soit $n \geqslant 2$ un entier se décomposant en produit de facteurs premiers sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Alors les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant k$.

4.11 Le but de cet exercice est de démontrer la précédente affirmation.

1) Soit $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant k$. Prouver que d divise n.
2) Soit d un diviseur positif de n. Il existe donc $q \in \mathbb{N}$ tel que $n = d\,q$.
   (a) Si l'on décompose tour à tour d et q en facteurs premiers, que peut-on dire du produit de leur décomposition ?
   (b) En conclure que $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $1 \leqslant i \leqslant k$.

4.12

1) Décomposer 1500 en produits de facteurs premiers.
2) En déduire tous les diviseurs positifs de 1500.

4.13 Si l'entier $n \geqslant 2$ admet $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ comme décomposition en produit de facteurs premiers, combien possède-t-il de diviseurs positifs ?

4.14 Un entier naturel n a cinq diviseurs positifs. À quoi n peut-il être égal ?

4.15 Quel est le plus petit entier naturel admettant douze diviseurs positifs ?

4.16 Un entier naturel n a exactement 36 diviseurs positifs. Quel est ce nombre, sachant que sa décomposition en facteurs premiers comporte 2, élevé à la puissance 3, ainsi que 5 et 7, élevés à une même puissance ?

4.17 On considère l'équation (E) : $n^2 - \mathrm{S}\,n + 11\,994 = 0$ d'inconnue $n \in \mathbb{N}$. On s'intéresse aux valeurs de S telles que (E) admette deux solutions dans $\mathbb{N}$.

1) Peut-on déterminer un entier S tel que 3 soit solution de (E) ? Si oui, préciser la seconde solution.
2) Peut-on déterminer un entier S tel que 5 soit solution de (E) ?
3) Montrer que tout entier n solution de (E) est un diviseur de 11 994.
4) En déduire toutes les valeurs possibles de S telles que (E) admette deux solutions entières.

PGCD, PPCM et décomposition en facteurs premiers

4.18 Soient a et b des entiers supérieurs ou égaux à 2. Quitte à admettre des exposants nuls, nous pouvons considérer que leurs facteurs premiers sont les mêmes. Écrivons donc $a = p_1^{\alpha_1}\, p_2^{\alpha_2}\, \dots\, p_k^{\alpha_k}$ et $b = p_1^{\beta_1}\, p_2^{\beta_2}\, \dots\, p_k^{\beta_k}$.
Il s'agit de prouver que $\operatorname{pgcd}(a,b) = p_1^{\min(\alpha_1,\beta_1)}\, p_2^{\min(\alpha_2,\beta_2)}\, \dots\, p_k^{\min(\alpha_k,\beta_k)}$.

1) Vérifier que $p_1^{\min(\alpha_1,\beta_1)}\, p_2^{\min(\alpha_2,\beta_2)}\, \dots\, p_k^{\min(\alpha_k,\beta_k)}$ divise a et b.
2) (a) Soit d un diviseur de a et de b. Montrer, grâce à l'exercice 4.11, que $d = p_1^{\delta_1}\, p_2^{\delta_2}\, \dots\, p_k^{\delta_k}$ avec $0 \leqslant \delta_i \leqslant \min(\alpha_i, \beta_i)$ pour tout $1 \leqslant i \leqslant k$.
   (b) En déduire que d divise $p_1^{\min(\alpha_1,\beta_1)}\, p_2^{\min(\alpha_2,\beta_2)}\, \dots\, p_k^{\min(\alpha_k,\beta_k)}$.

Soient a et b deux entiers relatifs non nuls. L'ensemble des multiples communs strictement positifs de a et de b est une partie de $\mathbb{N}$ non vide contenant $|a\,b|$. Il admet donc un plus petit élément que l'on appelle **plus petit commun multiple** de a et de b et que l'on note $\operatorname{ppcm}(a,b)$.

4.19 **Relation PGCD - PPCM**
Il s'agit de prouver que $\operatorname{pgcd}(a,b) \cdot \operatorname{ppcm}(a,b) = a\,b$ pour tous $a, b \in \mathbb{N}$.
Posons $d = \operatorname{pgcd}(a,b)$. Il existe des entiers a' et b' tels que $a = d\,a'$ et $b = d\,b'$.

1) Vérifier que $d\,a'\,b'$ est un multiple commun à a et à b.
2) Soit m un multiple commun à a et à b. On peut écrire $m = \alpha\,a = \beta\,b$ avec $\alpha, \beta \in \mathbb{Z}$. On a donc $m = \alpha\,d\,a' = \beta\,d\,b'$.
   (a) Montrer, grâce à l'exercice 3.12 et au lemme de Gauss, que $a' \mid \beta$.
   (b) En déduire l'existence d'un entier k tel que $m = k\,(d\,a'\,b')$.
3) Que vaut par conséquent $\operatorname{ppcm}(a,b)$?
4) Conclure que $\operatorname{pgcd}(a,b) \cdot \operatorname{ppcm}(a,b) = a\,b$.

4.20 1) Soient α et β deux nombres réels. En examinant successivement les cas
   (a) $\alpha < \beta$ (b) $\alpha = \beta$ (c) $\alpha > \beta$
   montrer que $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$.
2) Soient a et b des entiers supérieurs ou égaux à 2. Quitte à admettre des exposants nuls, nous pouvons considérer que leurs facteurs premiers sont les mêmes, de sorte que nous pouvons écrire $a = p_1^{\alpha_1}\, p_2^{\alpha_2}\, \dots\, p_k^{\alpha_k}$ et $b = p_1^{\beta_1}\, p_2^{\beta_2}\, \dots\, p_k^{\beta_k}$.
   Montrer que $\operatorname{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)}\, p_2^{\max(\alpha_2,\beta_2)}\, \dots\, p_k^{\max(\alpha_k,\beta_k)}$.

4.21 Calculer $\operatorname{ppcm}(1008, 540)$ de deux façons différentes.

4.22 Déterminer les entiers naturels a et b sachant que
1) $a\,b = 1350$ et $\operatorname{ppcm}(a,b) = 90$ 2) $a\,b = 2352$ et $\operatorname{ppcm}(a,b) = 168$

Réponses

4.2 8

4.3 5) 31

4.4 $24\,;25\,;26\,;27\,;28$

4.5 1) oui 2) oui 3) oui 4) non

4.7 1) $q \equiv 1 \mod p_i$ pour tout $1 \leqslant i \leqslant n$

4.9 $2000^{2000} = 2^{8000} \cdot 5^{6000}$

4.10 222

4.12 1) $1500 = 2^2 \cdot 3 \cdot 5^3$

2) 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 10 ; 12 ; 15 ; 20 ; 25 ; 30 ; 50 ; 60 ; 75 ; 100 ; 125 ; 150 ; 250 ; 300 ; 375 ; 500 ; 750 ; 1500

4.13 $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1)$

4.14 $n = p^4$ où p est un nombre premier

4.15 60

4.16 9800

4.17 1) $n^2 - 4001\,n + 11\,994 = 0$ admet pour solutions $n = 3$ et $n = 3998$.

2) non

4) $\mathrm{S} \in \{2005\,;4001\,;5999\,;11\,995\}$

4.19 3) $\mathrm{ppcm}(a, b) = d\,a'\,b'$

4.21 15 120

4.22 1) 15 et 90 ou bien 30 et 45 2) 14 et 168 ou bien 42 et 56