CHAPITRE 3

Les nombres premiers

SÉQUENCE 1 Les nombres premiers (page 76)

RÉSOLUTION DE PROBLÈMES

Problème 1

A **1.** *Conjecture possible* : le produit des nombres associés aux extrémités est égal à l'ordonnée du point de l'axe $(O ; \vec{j})$.

2. Les segments [2 ; 6], [3 ; 4] et leurs symétriques coupent l'axe $(O ; \vec{j})$ au point d'ordonnée 12.
Les nombres associés aux extrémités de ces segments sont des diviseurs de 12.

3. a) Ce sont les nombres pairs (sauf 0).

b) Ce sont les multiples de 3 (sauf 0).

B On a $y = \dfrac{n^2 - m^2}{n^2 + m^2} x + b = (n - m)x + b$;
d'où $n^2 = (n - m)n + b$ soit $b = mn$.
Le produit des nombres associés aux extrémités est bien l'ordonnée du point d'intersection de segment et de l'axe $(O ; \vec{j})$.

C **1.** Dire que le point P de coordonnées $(0 ; p)$ n'est atteint par aucun des segments équivaut à dire que p n'est divisible par aucun des nombres entiers n tels que $1 < n < p$.

2. les douze premiers de ces nombres premiers sont :
2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37.

Problème 2

A **1.** Un seul nombre pair est premier : le nombre 2.

B **1. a)** Il a, au minimum, 3 diviseurs.
6 n'est pas premier et ses diviseurs sont au nombre de 4 : {1 ; 2 ; 3 ; 6}.
b) Oui, au moins par celui qui a guidé son élimination du tableau.

2. a) Non. Voir la raison ci-dessus.
b) Oui, car tout nombre entier naturel supérieur à 1 admet un diviseur premier.

Problème 3

A **1. a)** On effectue la division euclidienne de 41 par tous les nombres premiers inférieurs à 41.
Aucune de ces divisions ne donne un quotient entier (c'est-à-dire un reste nul). Le nombre 41 est donc premier.
b) Il n'y a que douze nombres premiers inférieurs à 41 (*cf.* Problème **1. C. 2.)**.
c) La liste (2 ; 3 ; 5) suffit car si aucun de ces trois nombres premiers ne divise 41, un diviseur premier p est au moins égal à 7 et $41 = p \times q$ avec $q < 6$.
q n'étant pas premier (les premiers inférieurs à 6 étant 2, 3 et 5), il est divisible par un premier (parmi 2, 3 et 5). Ce qui est impossible.

2. $\sqrt{491} \approx 22{,}1$; donc le plus grand premier à utiliser est 19.
Le nombre 491 est premier.

B **1.** Le calcul peut être arrêté lorsqu'on a atteint le plus grand nombre premier inférieur à la racine carrée du nombre.

2. a) Le seul nombre pair premier est 2 et la reconnaissance de la parité est particulièrement simple.

b) On obtient son premier diviseur premier.
c) Les nombres premiers de la liste sont : 577 ; 1 237 et 37 589.

Problème 4

A **1. a)** $u_1 = 3$, $u_2 = 7$, $u_3 = 31$, $u_4 = 211$ et $u_5 = 2311$. Tous sont premiers.
b) $u_6 = 30\,031 = 59 \times 509$;
$u_7 = 510\,511 = 19 \times 26\,869$;
$u_8 = 11\,741\,731 = 3\,209 \times 3\,659$.
2.

u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8
3	7	31	211	2311	59	19	3 209

Le plus petit diviseur premier de chacun des nombres n'est pas utilisé pour la construction du nombre.

B **1. a)** pour p non nul, $2p > p$ donc $u_N > p$.
u_N n'est pas premier car il est strictement supérieur à p qui est supposé le plus grand des premiers.
b) Soit d un diviseur premier de u_N.
$d \in \{2 ; 3 ; 5 ; \ldots ; p\}$, donc d divise à la fois :
$2 \times 3 \times 5 \times \ldots \times p$ et $2 \times 3 \times 5 \ldots \times p + 1$.
p divise donc leur différence 1, ce qui est impossible.
On arrive donc à une contradiction : il n'existe pas de plus grand nombre premier.
c) L'ensemble des nombres premiers est infini.

Problème 5

A **1.** Notons x le côté du grand carré compté en rosiers et y celui d'un petit carré.
2. $(x - 1)(x + 1) = 5y^2$.
5 est un nombre premier ; il divise un des deux facteurs $(x - 1)$ ou $(x + 1)$.

3. a) Dans $\mathbb{N}$:
$0 < x^2 < 1\,000 \Leftrightarrow 0 < x < 32$
$\Leftrightarrow 0 < 5k + 1 < 32$
$\Leftrightarrow -1 < 5k < 31$,
d'où $0 \leqslant k \leqslant 6$.
Si $x - 1 = 5k$, alors $x^2 - 1 = 5k(5k + 2) = 5y^2$; donc :
$k(5k + 2) = y^2$.
b)

k	0	1	2	3	4	5	6
$5k + 2$	2	7	12	17	22	27	32
$k(5k + 2)$	0	7	24	51	88	135	192

Pour $0 \leqslant k \leqslant 6$, le nombre $k(5k + 2)$ n'est pas un carré ; donc, l'hypothèse « $(x - 1)$ est un multiple de 5 » ne convient pas.

4. a) Dans $\mathbb{N}$:
$0 < x < 32 \Leftrightarrow 0 < 5k - 1 < 32 \Leftrightarrow 1 < 5k < 33$,
d'où $1 \leqslant k \leqslant 6$.
Si $x + 1 = 5k$, alors $x^2 - 1 = 5k(5k - 2) = 5y^2$;
donc $k(5k - 2) = y^2$.
b)

k	1	2	3	4	5	6
$5k - 2$	3	8	13	18	23	28
$k(5k + 2)$	3	**16**	39	72	115	168

Il y a un seul carré dans la dernière ligne du tableau ; donc une seule solution est possible : $k = 2$, soit $x = 9$.
La Reine de Cœur possède donc 81 rosiers.

B **1.** y pair $\Leftrightarrow 5y^2$ pair $\Leftrightarrow x^2$ impair $\Leftrightarrow x$ impair.
$x(x) + (-5y)y = 1$: théorème de Bézout ; donc x et y sont premiers entre eux.
2. a) $(9a + 20b)^2 - 5(4a + 9b)^2 = a^2 - 5b^2$.
b) (9 ; 4) ; (161 ; 72) ; (2 889 ; 1 292).
3. Il n'y a que deux solutions : (9 ; 4) et (161 ; 72) ; soit 81 rosiers ou 25 921 rosiers.

EXERCICES — Application (page 84)

1 $A = a^2 + 2a - 3 = (a - 1)(a + 3)$.
A est premier, donc A n'admet que deux diviseurs : 1 et lui-même.
Soit $a - 1 = 1$ et $a = 2$,
soit $a + 3 = 2$ et $a = -1$ (impossible).
Donc $a = 2$.

2 $A = (a + 1)(a - 1)(a^2 + 1)$.
Si $a = 2$, $A = 3 \times 5$, donc A n'est pas un nombre premier.
Si $a > 2$, alors $1 < a - 1 < a + 1 < a^2 + 1$.
A admet trois diviseurs stricts ; donc A n'est pas un nombre premier.

3 p divise n^2 et p premier (Théorème 5) entraîne p divise n.
Donc $n = kp$, soit $n^2 = k^2p^2$ et p^2 divise n^2.

4 $a^2 - b^2 = (a + b)(a - b)$, avec $0 < a - b < a + b$.
$a^2 - b^2$ premier $\Leftrightarrow a - b = 1$ et $a + b = A$.

SÉQUENCE 2

Décomposition en produit de facteurs premiers (page 85)

RÉSOLUTION DE PROBLÈME

Problème 6

1. a) $441 = 21^2$.
b) 441 est divisible par 3 (et pas par 2) ; donc 3 est son plus petit diviseur premier. $441 = 3 \times 147$.
c) $147 = 3 \times 49$.
d) $441 = 3 \times 3 \times 49$.
e) $441 = 3 \times 3 \times 7 \times 7$. Tous les facteurs sont premiers.
Tout nombre entier naturel non premier se décompose en produit de facteurs premiers.
f) Non, il y a unicité de la décomposition.

2. $248 = 2^3 \times 31$; $325 = 5^2 \times 13$; $595 = 5 \times 7 \times 17$; $633 = 3 \times 211$; $676 = 2^2 \times 13^2$; $1\,225 = 5^2 \times 7^2$.

3. $676 = (2 \times 13)^2$ et $1\,225 = (5 \times 7)^2$.
Dans la décomposition d'un carré en produit de facteurs premiers, toutes les puissances sont paires.

4. a) $D_{325} = \{1, 5, 13, 25, 65, 325\}$, soit 6 diviseurs.
b) $D_{248} = \{1, 2, 4, 8, 31, 62, 124, 248\}$, soit 8 diviseurs.
$D_{595} = \{1, 5, 7, 17, 35, 85, 119, 595\}$, soit 8 diviseurs.
$D_{676} = \{1, 2, 4, 13, 26, 52, 169, 338, 676\}$, soit 9 diviseurs.
c) Le nombre de diviseurs est le produit :
$$(\alpha + 1)(\beta + 1) \ldots (\gamma + 1)$$
où α, β, …, γ sont les puissances des facteurs premiers de la décomposition.

EXERCICES

Application (page 87)

6 **a)** $600 = 2^3 \times 3 \times 5^2$. **b)** $4\,998 = 2 \times 3 \times 7^2 \times 17$.
c) $41\,724 = 2^2 \times 3^2 \times 19 \times 61$. **d)** $57\,132 = 2^2 \times 3^3 \times 23^2$.

7 **a)** $400 = 2^4 \times 5^2$. **b)** $1\,050 = 2 \times 3 \times 5^2 \times 7$.
c) $13\,552 = 2^4 \times 7 \times 11^2$. **d)** $11\,737 = 11^2 \times 97$.

8 **a)** $45^2 - 4 = (45 - 2)(45 + 2) = 43 \times 47$.
b) $55^2 - 16 = (55 - 4)(55 + 4) = 51 \times 59 = 3 \times 17 \times 59$.

9 **a)** $150 = 2 \times 3 \times 5^2$.
$D_{150} = \{1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150\}$
b) $4\,012 = 2^2 \times 17 \times 59$.
$D_{4\,012} = \{1, 2, 4, 17, 34, 59, 68, 118, 236, 1\,003, 2\,006, 4\,012\}$.
c) $11\,339 = 17 \times 23 \times 29$.
$D_{11\,339} = \{1, 17, 23, 29, 391, 493, 667, 11\,339\}$.

10 **a)** $7\,429 = 17 \times 19 \times 23$.
$D_{7\,429} = \{1, 17, 19, 23, 323, 391, 437, 7\,429\}$.
b) $87\,616 = 2^6 \times 37^2$.
$D_{87\,616} = \{1, 2, 4, 8, 16, 32, 37, 64, 74, 148, 296, 592, 1\,184, 1\,369, 2\,368, 2\,738, 5\,476, 10\,952, 21\,904, 43\,808, 87\,616\}$.
c) 2 357 est premier.

11 **1.** PGCD $(a, b) = 2^2 \times 5^2 = 100$.
2. PGCD $(a, b) = 3 \times 5 = 15$.

12 **1.** $a = 2^3 \times 3 \times 5^2$ et $b = 2^2 \times 3 \times 5 \times 7$;
donc PGCD $(a, b) = 2^2 \times 3 \times 5 = 60$.
2. $a = 2 \times 3^3 \times 5$ et $b = 2^2 \times 3 \times 7$;
donc PGCD $(a, b) = 2 \times 3 = 6$.

13 **1.** $a = 2 \times 3^4 \times 5$ et $b = 2^2 \times 3^2 \times 7^2$;
donc PGCD $(a, b) = 2 \times 3^2 = 18$.
2. $a = 3^2 \times 5^3 \times 11$ et $b = 2 \times 3^3 \times 5 \times 11$;
donc PGCD $(a, b) = 3^2 \times 5 \times 11 = 495$.

14 **a)** $\dfrac{412}{236} = \dfrac{2^2 \times 103}{2^2 \times 59} = \dfrac{103}{59}$.
b) $\dfrac{1\,024}{96} = \dfrac{2^{10}}{2^5 \times 3} = \dfrac{2^5}{3} = \dfrac{32}{3}$.
c) $\dfrac{395}{123} = \dfrac{5 \times 79}{3 \times 41}$: la fraction irréductible.

15 $a = 2^6 \times 3^4 \times 5^2 = (2^3 \times 3^2 \times 5)^2 = 360^2$.
$b = 2^3 \times 3^2 \times 7^3 \times 19$: b n'est pas un carré.
$B = 2^4 \times 3^2 \times 7^4 \times 19^2 = 11\,172^2$.
$B = 2 \times 7 \times 19 \times b$.
$c = 2 \times 3^2 \times 5^2 \times 7 \times 11 \times 37$: c n'est pas un carré.
$C = 2 \times 7 \times 11 \times 37 \times c = 85\,470^2$.

16 $a = 19 \times 23$ et $A = a^2 = 190\,969$.
$b = 5 \times 53 \times 59$ et $B = b^2 = 244\,453\,225$.
$c = 2^2 \times 503$ et $C = 503 \times c = 1\,006^2 = 1\,012\,036$.

17 **1.** $a = 2^4 \times 3^3 \times 5^2$: a n'est pas un cube.
2. $A = 2^2 \times 5 \times a = (2^2 \times 3 \times 5)^3 = 60^3 = 216\,000$.

18 à **21** *Corrigés sur le site élève.*

EXERCICES sur l'ensemble des séquences

EXERCICES Activités de recherche (page 90)

22 Utiliser l'ensemble des diviseurs d'un entier

• ***Les outils***

– Résolution d'un système de deux équations du 1er degré à deux inconnues.

– Décomposition en produit de facteurs premiers d'un entier naturel.

• ***Les objectifs***

– Savoir résoudre des équations dans $\mathbb{N}$.

1. (E) $(x-y)(x+y)=197$.

2. a) $D_{197}=\{1\,;\,197\}$.

b) On obtient deux décompositions : 197×1 et 1×197.

3. a) En remarquant que $x-y\leqslant x+y$, on a :

$$\begin{cases} x-y=1 \\ x+y=197 \end{cases} \Leftrightarrow \begin{cases} x=99 \\ y=98. \end{cases}$$

b) $x^2-y^2=99^2-98^2=197$.

Conclusion : il existe un seul couple solution $(99\,;\,98)$.

4. a) (E') $(x-y)(x+y)=196=2^2\times 7^2$;

donc, il y a 9 diviseurs :

$$D_{196}=\{1, 2, 4, 7, 14, 28, 49, 98, 196\}.$$

b) $196=1\times 196=196\times 1$
$=2\times 98=98\times 2$
$=4\times 49=49\times 4$
$=7\times 28=28\times 7$
$=14\times 14$.

5. a) En remarquant que les deux facteurs doivent être de la même parité, on a :

$$S_1\begin{cases} x+y=98 \\ x-y=2 \end{cases} \Leftrightarrow \begin{cases} x=50 \\ y=48 \end{cases}$$

$$S_2\begin{cases} x+y=14 \\ x-y=14 \end{cases} \Leftrightarrow \begin{cases} x=14 \\ y=0. \end{cases}$$

b) $50^2-48^2=196$ et $14^2-0^2=196$.

L'équation (E') admet deux couples solution : $(50\,;\,48)$ et $(14\,;\,0)$.

23 Divisibilité et nombres premiers

• ***Les outils***

– Propriétés de la division euclidienne.

– Raisonnement par disjonction des cas.

• ***Les objectifs***

– Caractériser les nombres premiers strictement supérieurs à 5.

– Savoir démontrer une propriété caractéristique des nombres premiers strictement supérieurs à 5.

1. a) les restes dans la division euclidienne par 6 sont : 0, 1, 2, 3, 4 et 5. Tout entier est de la forme $6n+k$ avec $k\in\{0\,;\,1\,;\,2\,;\,3\,;\,4\,;\,5\}$.

b) $6n+0$, $6n+2$, $6n+3$ et $6n+4$ ne sont pas premiers.

2. a) $p=6n+1$, donc :

$$p^2-1=6n(6n+2)=12n(3n+1).$$

b) Si n est pair, $12n$ est divisible par 24.

Si n est impair, $3n+1$ est pair et $12(3n+1)$ est divisible par 24.

3. $p^2-1=(6n+6)(6n+4)=12(n+1)(3n+2)$.

Si n est pair, $3n+2$ est pair $12(3n+2)$ est divisible par 24.

Si n est impair, $n+1$ est pair et $12(n+1)$ est divisible par 24.

24 Narration de recherche

1. $3=2^2-1^2$; $5=3^2-2^2$; $7=4^2-3^2$;
$11=6^2-5^2$; $13=7^2-6^2$; $17=9^2-8^2$
$19=10^2-9^2$; $23=12^2-11^2$.

2. Soit p premier impair.

le système $\begin{cases} x+y=p \\ x-y=1 \end{cases}$ admet un couple solution de nombres entiers naturels :

$$x=\frac{p+1}{2} \text{ et } y=\frac{p-1}{2}.$$

Vérification : pour p impair et $p\geqslant 3$ donc $p+1$ et $p-1$ sont des entiers naturels pairs. Ainsi x et y sont des entiers naturels.

Enfin, $x^2-y^2=\frac{1}{4}[(p+1)^2-(p-1)^2]=p$.

3. Non. Si on supprime cette hypothèse, il faut préciser : $p\geqslant 3$.

25 Narration de recherche

Posons $a=2^p+p^2$.

• Si $p=2$, alors $a=8$, a est non premier.

• Si $p=3$, alors $a=2^3+3^2=17$, a est premier.

◦ Si $p\equiv 0 \pmod 3$, seul 3 est premier.

◦ Si $p\equiv 1 \pmod 3$, $p=3k+1$ (avec k pair) car p est impair.

Donc $p=6m+1$.

$2^{6m+1}=4^{3m}\times 2\equiv 2 \pmod 3$ car 4 est congru à 1 (mod 3) et $(6m+1)^2\equiv 1 \pmod 3$,

d'où $a\equiv 0 \pmod 3$ et a n'est pas premier.

◦ Si $p\equiv 2 \pmod 3$, $p=3k+2$ (avec k impair).

Donc $p=6m+5$.

$2^{6m+5}=4^{3m}\times 2^5\equiv 2 \pmod 3$ et $(6m+5)^2\equiv 1 \pmod 3$,

d'où $a\equiv 0 \pmod 3$ et a n'est pas premier.

Conclusion : il y a une seule solution, $p=3$.

26 TD – Densité des nombres premiers

1. La densité des nombres premiers :
– inférieurs à 10^{14} est $\approx 0{,}003\,2$;
– inférieurs à 10^{18} est $\approx 0{,}002\,2$.
On peut conjecturer que la densité diminue lorsque l'exposant n (de 10^n) augmente.

2. $\dfrac{223 \cdot 10^6}{222 \cdot 10^6} \approx 10^{-10}$, soit 0,000 000 01 %.
On peut parler de grande précision…

3. a) $\forall\, m \in \mathbb{N}$, tel que $2 \leqslant m \leqslant k$, u_m est divisible par m.
b) $\forall\, n > 10^5$, les nombres $u_1, u_2, \ldots, u_{105}$ constituent une suite de 10^5 nombres entiers naturels consécutifs non premiers.

27 TD – À la recherche du plus grand

A. 1.

n	1	2	3	4	5	6	7	8	9	10
$2^n - 1$	1	3	7	15	31	63	127	255	511	1023

2. $2^n - 1$ est premier pour n = 2, 3, 5 et 7, c'est-à-dire pour n premier.
Conjecture : « $2^n - 1$ est premier » $\Leftrightarrow$ « n premier ».

B. 1. a) $1 + 2^p + (2^p)^2 + \ldots + (2^p)^{q-1} = \dfrac{1 - 2^{pq}}{1 - 2^p}$

b) $2^n - 1 = (2^p - 1)\,[1 + 2^p + (2^p)^2 + \ldots + (2^p)^{q-1}]$, avec $(2^p - 1) > 1$.
$2^n - 1$ n'est donc pas premier, et la condition est nécessaire.
c) $2^{33} - 1$ est divisible par $2^3 - 1$ (comme par $2^{11} - 1$).
$2^{33} - 1$ est donc divisible par 7.

2. a) $2^{11} - 1 = 2\,047 = 23 \times 89$.
b) $2^{23} - 1 = 47 \times 178\,481$ et $2^{29} - 1 = 233 \times 2\,304\,167$.

3. Il est nécessaire (mais pas suffisant) que n soit premier pour que le nombre de Mersenne $2^n - 1$ soit premier.
Ou, « $2^n - 1$ est premier » $\Rightarrow$ « n est premier » et la réciproque est fausse.

C. 1. $F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$.

2. $F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$.

28 TD – Cryptographie : le système RSA

1. $23 \times 7 - 40 \times 4 = 1$ donc $d = 23$ convient.
Pour l'unicité, supposons qu'il existe d' tel que $7d' \equiv 1 \pmod{40}$ avec $2 \leqslant d' \leqslant 39$.
Il en résulte $7(d - d') \equiv 0 \pmod{40}$.
Étant premier avec 7, 40 divise $d - d'$.
Comme $-37 \leqslant d - d' \leqslant 37$, $d - d' = 0$ (seul multiple de 40 compris entre –37 et 37), et $d = d'$.

2. a) Voir tableau ci-contre.

b)

	J	O	I	E
nombre	10	15	9	5
code	10	5	4	25

c)

nombre	17	4	17	25
code	18	9	18	5
	R	I	R	E

	A	B	C	D
	nombres secrets connus d'Alice		clé publique	
	p	q	n	e
	5	11	55	7
			codage	
1		1	1	
2		128	18	
3		2187	42	
4		16384	49	
5		78125	25	
6		279936	41	
7		823543	28	
8		2097152	2	
9		4782969	4	
10		10000000	10	
11		19487171	11	
12		35831808	23	
13		62748517	7	
14		105413504	9	
15		170859375	5	
16		268435456	36	
17		410338673	8	
18		612220032	17	
19		893871739	24	
20		1280000000	15	
21		1801088541	21	
22		2494357888	33	
23		3404825447	12	
24		4586471424	29	
25		6103515625	20	
26		8031810176	16	

29 TD – Test probabiliste de primalité

A. 1.

mod 3	reste	
a	1	2
a^2	1	1

mod 5	reste			
a	1	2	3	4
a^2	1	4	4	1
a^4	1	1	1	1

mod 7	reste					
a	1	2	3	4	5	6
a^3	1	1	6	1	6	6
a^6	1	1	1	1	1	1

2. a) a est non divisible par p.
« p premier » $\Rightarrow$ « $a^{p-1} \equiv 1 \pmod{p}$ ».
Par contraposition :
« a^{p-1} non congru à $1 \pmod{p}$ » $\Rightarrow$ « p non premier ».
b) La réciproque du théorème est fausse.

3. a) $341 = 11 \times 31$ et $2^{340} \equiv 1 \pmod{341}$.

b) $p = \dfrac{245}{10^6} = 0{,}000\,245$.

B. 1. $p = \dfrac{8\,220\,777}{10^{20}} \approx 8{,}22 \times 10^{-14}$.

2. $561 = 3 \times 11 \times 17$;
$1\,105 = 5 \times 13 \times 17$;
$1\,729 = 7 \times 13 \times 19$;
$2\,465 = 5 \times 17 \times 29$.
$7^8 \equiv 16 \pmod{1\,105}$ et $16^6 \equiv 1 \pmod{1\,105}$, donc :
$7^{48} \equiv 1 \pmod{1\,105}$ soit $(7^{48})^{23} \equiv 1 \pmod{1\,105}$.

EXERCICES Entraînement (page 96)

DE TÊTE

30 Sont premiers : 37, 41, 43, 47, 71 et 91.

31 $50 = 2 \times 5^2$; $64 = 2^6$; $70 = 2 \times 5 \times 7$
$120 = 2^3 \times 3 \times 5$; $800 = 2^5 \times 5^2$
$1\,000 = 2^3 \times 5^3$; $600\,000 = 2^6 \times 3 \times 5^5$.

32 $2\,012 = 2^2 \times 503$ donc $2\,012 \times 503 = 1\,006^2$.

33 $48 = 2^4 \times 3$ donc $(4 + 1) \times (1 + 1) = 10$ diviseurs.
$60 = 2^2 \times 3 \times 5$ donc $(2 + 1) \times (1 + 1) \times (1 + 1) = 12$ diviseurs.

34 $7\,! = 2 \times 3 \times 2^2 \times 5 \times 2 \times 3 \times 7 = 2^4 \times 3^2 \times 5 \times 7$.

NOMBRES PREMIERS

35 *Corrigés sur le site élève.*

36 *Faux* : 103, 113, 163, 173, 193 se terminent par 3 et 107, 127, 137, 157, 167 et 197 par 7.

37 n est premier car non divisible par tous les nombres premiers inférieurs à $\sqrt{n} \leqslant \sqrt{130}$.

38 Pour 2012 : 2012 est encadré par les nombres premiers 2011 et 2017. Donc, l'année la plus proche est 2011.

39 *Vrai* : Les restes possibles dans la division par 6 sont 0, 1, 2, 3, 4 et 5.
Les nombres $6n$, $6n + 2$, $6n + 3$, $6n + 4$ sont divisibles respectivement par 6, 2, 3 et 2.
Donc, les nombres premiers strictement supérieurs à 5 sont de la forme $6n + 1$ ou $6n + 5$.

40 **1.** ~~1~~, 3, 5, 7, ~~9~~, 11, 13, ~~15~~, 17, 19, ~~21~~, 23, ~~25~~, ~~27~~, 29, 31, ~~33~~, ~~35~~, 37, ~~39~~.

2. La plus longue série est 3, 5, 7.

3. Notons (u_n) la suite des nombres impairs ($\forall\, n \in \mathbb{N}$, $u_n = 2n + 1$).
$\forall\, k \in \mathbb{N}$, $u_{3k+1} = 6k + 3$. C'est un multiple de 3 et dans cinq termes consécutifs de la suite, on trouve (au moins) un tel terme.

41 Soient trois entiers naturels impairs consécutifs :
n, $n + 2$ et $n + 4$.
Les restes dans la division par 3 sont :

n	0	1	2
$n + 2$	2	0	1
$n + 4$	1	2	0

Un des trois nombres (et un seul) est multiple de 3.
Une telle suite contient donc le seul nombre premier multiple de 3 : le nombre 3.
3, 5 et 7 est donc la seule suite possible.

42 **1.** La table donne les nombres premiers et des nombres (non premiers) accompagnés de leur plus petit diviseur propre. On fait abstraction des cas où le plus petit diviseur premier est accessible avec les critères de divisibilité classiques (par 2 , 3 , 5 , 9 et 11).

2. 2 429 (7)
2 437
2 441
2 443 (7).

DÉCOMPOSITION EN PRODUIT DE NOMBRES PREMIERS

43 • $1\,400 = 2^3 \times 5^2 \times 7$; • $1\,287 = 3^2 \times 11 \times 13$;
• $2\,275 = 5^2 \times 7 \times 13$; • $6\,435 = 3^2 \times 5 \times 11 \times 13$.

44 • $398 = 2 \times 199$; • $1\,357 = 23 \times 59$;
• $2\,658 = 2 \times 3 \times 443$; • $2\,958 = 2 \times 3 \times 17 \times 29$.

45 • $39^2 - 4 = 37 \times 41$; • $75^2 - 16 = 71 \times 79$.

46 L'objectif est d'afficher la décomposition en produit de facteurs premiers.
On obtient : 15 = 3*5*, 72 = 2*2*2*3*3* et 23 = 23*.

47 *Corrigés sur le site élève.*

48 • $42 = 2 \times 3 \times 7$
$D_{42} = \{1, 2, 3, 6, 7, 14, 21, 42\}$.
• $220 = 2^2 \times 5 \times 11$
$D_{220} = \{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, 220\}$.
• $450 = 2 \times 3^2 \times 5^2$
$D_{450} = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 25, 30, 45, 50, 75, 90, 150, 225, 450\}$.
• $1\,352 = 2^3 \times 13^2$
$D_{1\,352} = \{1, 2, 4, 8, 13, 26, 52, 104, 169, 338, 676, 1\,352\}$.

49 • $108 = 2^2 \times 3^3$
$D_{108} = \{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$.
• $490 = 2 \times 5 \times 7^2$
$D_{490} = \{1, 2, 5, 7, 10, 12, 35, 49, 70, 98, 245, 490\}$.
• $726 = 2 \times 3 \times 11^2$
$D_{726} = \{1, 2, 3, 6, 11, 22, 33, 66, 121, 242, 363, 726\}$.
• $210 = 2 \times 3 \times 5 \times 7$
$D_{210} = \{1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210\}$.

50 **1.** $a = 2^3 \times 3^2 \times 5 \times 7 \times 11$ et $b = 2 \times 5 \times 7 \times 11$.
2. $a = b \times 2^2 \times 3^2$ et $\dfrac{a}{b} = 36$.

51 **a)** $A = 2^6 \times 7^2 \times 13^2 = (2^3 \times 7 \times 13)^2$,
d'où $A = 728^2$.
b) $B = 2^{14} \times 167^2 = (2^7 \times 167)^2$,
d'où $B = 21\,376^2$.
c) $C = 2^2 \times 3^4 \times 5^2 \times 7^2 \times 17^4 = (2 \times 3^2 \times 5 \times 7 \times 17^2)^2$,
d'où $C = 182\,070^2$.

52 **1.** $n = 1\,350 = 2 \times 3^3 \times 5^2$.
2. $m = 2^2 \times 3^4 \times 5^2 = 6n = 90^2$.

53 *Corrigés sur le site élève.*

54 $2\,013 = 3 \times 11 \times 61$; et le plus petit entier naturel qui multiplié par 2 013 donne un carré parfait est 2 013 lui-même.

55 $(x + y)(x - y) = 28$ et $D_{28} = \{1, 2, 4, 7, 14, 28\}$.
En remarquant que les deux facteurs doivent être de la même parité, et que $x - y \leqslant x + y$, on a :

$$\begin{cases} x + y = 14 \\ x - y = 2 \end{cases} \Leftrightarrow \begin{cases} x = 8 \\ y = 6. \end{cases}$$

56 $(E) \Leftrightarrow (x + 2)^2 = y^2 + 31 \Leftrightarrow (x + 2)^2 - y^2 = 31$
$\Leftrightarrow (x + y + 2)(x - y + 2) = 31$
$D_{31} = \{1, 31\}$ et $x + y + 2 \geqslant x - y + 2$.

Donc : $S\begin{cases}x+y+2=31\\x-y+2=1\end{cases}\Leftrightarrow\begin{cases}x=14\\y=15.\end{cases}$

57 (E) $\Leftrightarrow (x^2-6x+9)+45=y^2$
$\Leftrightarrow (y+x-3)(y-x+3)=45.$
$D_{45}=\{1, 3, 5, 9, 15, 45\}$.

• **Si $x>3$**, $y+x-3>y-x+3$.

$S_1\begin{cases}y+x-3=45\\y-x+3=1\end{cases}\Leftrightarrow\begin{cases}x=25\\y=23\end{cases}$

$S_2\begin{cases}y+x-3=15\\y-x+3=3\end{cases}\Leftrightarrow\begin{cases}x=9\\y=9\end{cases}$

$S_3\begin{cases}y+x-3=9\\y-x+3=5\end{cases}\Leftrightarrow\begin{cases}x=5\\y=7\end{cases}$

• **Si $x<3$**, $y+x-3<y-x+3$.

$S_4\begin{cases}y+x-3=1\\y-x+3=45\end{cases}\Leftrightarrow\begin{cases}x=-19\\y=23\end{cases}$, impossible.

$S_5\begin{cases}y+x-3=3\\y-x+3=15\end{cases}\Leftrightarrow\begin{cases}x=-5\\y=9\end{cases}$, impossible.

$S_6\begin{cases}y+x-3=5\\y-x+3=9\end{cases}\Leftrightarrow\begin{cases}x=-3\\y=7\end{cases}$, impossible.

L'équation (E) admet trois couples $(x\,;\,y)$ solution :
$(5\,;\,7)$, $(9\,;\,9)$ et $(25\,;\,23)$.

58 *Corrigés sur le site élève.*

59 $n+(n+1)+(n+2)+\ldots+(n+p)=286$ (E).
$\Leftrightarrow n(p+1)+\dfrac{p(p+1)}{2}=286$
$\Leftrightarrow (p+1)(2n+p)=572.$
$572=2^2\times 11\times 13$
et $D_{572}=\{1, 2, 4, 11, 13, 22, 26, 44, 52, 143, 286, 572\}$.
n est non nul donc $2n+p>p+1\geqslant 2$.

(E) $\Leftrightarrow$ $S_1\begin{cases}p+1=1\\2n+p=572\end{cases}\Leftrightarrow\begin{cases}p=0\\n=286\end{cases}$, impossible.

$S_2\begin{cases}p+1=2\\2n+p=286\end{cases}\Leftrightarrow\begin{cases}p=1\\n=142{,}5\end{cases}$, impossible.

$S_3\begin{cases}p+1=4\\2n+p=143\end{cases}\Leftrightarrow\begin{cases}p=3\\n=70\end{cases}$

$S_4\begin{cases}p+1=11\\2n+p=52\end{cases}\Leftrightarrow\begin{cases}p=10\\n=21\end{cases}$

$S_5\begin{cases}p+1=13\\2n+p=44\end{cases}\Leftrightarrow\begin{cases}p=12\\n=16\end{cases}$

$S_6\begin{cases}p+1=22\\2n+p=26\end{cases}\Leftrightarrow\begin{cases}p=21\\n=2{,}5\end{cases}$, impossible.

L'équation admet trois couples $(n\,;\,p)$ solution :
$(70\,;\,3)$ $70+71+72+73=286$;
$(21\,;\,10)$ $21+22+\ldots+31=286$;
$(16\,;\,12)$ $16+17+\ldots+28=286$.

60 $384=2^7\times 3$;
donc 384 admet $(7+1)(1+1)=16$ diviseurs.
Considérons un entier naturel N ayant exactement 16 diviseurs et dont la décomposition en produit de facteurs premiers est $a^\alpha\times b^\beta$.
$(\alpha+1)(\beta+1)=16$.

$\begin{cases}\alpha+1=1\\\beta+1=16\end{cases}\Leftrightarrow\begin{cases}\alpha=0\\\beta=15\end{cases}$

$2^{15}=32\,768$.

$\begin{cases}\alpha+1=2\\\beta+1=8\end{cases}\Leftrightarrow\begin{cases}\alpha=1\\\beta=7\end{cases}$

$2^7\,3=384$.

$\begin{cases}\alpha+1=4\\\beta+1=4\end{cases}\Leftrightarrow\begin{cases}\alpha=3\\\beta=3\end{cases}$

$2^3\,3^3=216$.
Ce contre-exemple suffit : la proposition est fausse.

61 $8\,!=2^7\times 3^2\times 5\times 7$, donc $8\times 3\times 2\times 2=96$ diviseurs.

62 $5(n+1)^2\leqslant 60\Leftrightarrow (n+1)^2\leqslant 12$
n étant strictement positif, le carré $(n+1)^2$ est égal à 4 ou à 9 : $n=2$ ou $n=3$.
$A=2^4\times 5\times 7=560$ ou $A=2^4\times 5^2\times 7^2=19\,600$.

63 $n=p^\alpha\times q^\beta$ et $n^2=p^{2\alpha}\times q^{2\beta}$
$(2\alpha+1)(2\beta+1)=2(\alpha+1)(\beta+1)\Leftrightarrow 2\alpha\beta=1$ ce qui est impossible (dans $\mathbb{N}$).

64 *Corrigés sur le site élève.*

DIVISIBILITÉ ET NOMBRES PREMIERS

65 n étant premier, s'il divise le produit de $(n-1)$ facteurs $1\times 2\times 3\ \ldots\times(n-1)$, il divise un des facteurs d'après le théorème 5.
Ce qui est impossible car tous ces facteurs sont strictement inférieurs à n.

66 **1.** Posons $A=n^2+4n+3$.

n	1	2	3	4	5	6	7	8
A	8	15	24	35	48	63	80	99

Aucun des nombres A n'est premier.

2. Le trinôme A se factorise ($\Delta=2^2$).
$A=(n+1)(n+3)$; donc, pour tout n non nul, A est le produit de deux entiers naturels strictement supérieurs à 1 : A est composé.

67 **1.** Posons $A=2n^2+9n-5$.

n	1	2	3	4	5	6	7	8
A	6	21	40	63	90	121	156	195

Aucun des nombres A n'est premier.

2. Le trinôme A se factorise ($\Delta=11^2$).
$A=(2n-1)(n+5)$; donc, pour tout n non nul, A est le produit de deux entiers naturels strictement supérieurs à 1 : A est composé.

68 $2^4+2^2+1=21$, non premier ;
$3^4+3^2+1=91=7\times 13$, non premier ;
$4^4+4^2+1=273=3\times 7\times 13$, non premier.
Conjecture : pour $n\geqslant 2$, n^4+n^2+1 n'est pas premier.

Démonstration :

$n^4 + n^2 + 1 = (n^2 + 1)^2 - n^2 = (n^2 + n + 1)(n^2 - n + 1)$.

Pour tout $n \geqslant 2$, les nombres $n^2 + n + 1$ et $n^2 - n + 1$ sont strictement supérieurs à 1 ; donc $n^4 + n^2 + 1$ n'est pas premier.

69 **1. a)** Les nombres surlignés en jaune sont premiers.

b) On passe du $n^{\text{ième}}$ nombre au suivant en parcourant deux côtés du carré de côté n.

Soit, pour tout n non nul, $u_{n+1} = u_n + 2n$.

c) $(P_n) : u_n = n^2 - n + 17$

$u_1 = 1^2 - 1 + 17 = 17$: (P_1) est vraie.

Supposons (P_n) vraie pour un entier n non nul.

$u_{n+1} = u_n + 2n = n^2 - n + 17 + 2n$

$= (n^2 + 2n + 1) - (n + 1) + 17$

$= (n + 1)^2 - (n + 1) + 17$: (P_{n+1}) est vraie.

(P_1) vraie et (P_n) vraie $\Rightarrow (P_{n+1})$ vraie.

Conclusion : $\forall\, n \in \mathbb{N}^*$, $u_n = n^2 - n + 17$.

2. $v_n = u_n + 24$

41, 43, 47, 53, 61, 71, 83, …sont premiers.

77	76	75	74	73	72	71
78	57	56	55	54	53	70
79	58	45	44	43	52	69
80	59	46	41	42	51	68
81	60	47	48	49	50	67
82	61	62	63	64	65	66
83	64	85	86	87	88	89

3. a)

	A	B	C
1	*n*	*Un*	*Vn*
2	0	17	41
3	1	19	43
4	2	23	47
5	3	29	53
6	4	37	61
7	5	47	71
8	6	59	83
9	7	73	97
10	8	89	113
11	9	107	131
12	10	127	151
13	11	149	173
14	12	173	197
15	13	199	223
16	14	227	251
17	15	257	281
18	16	289	313
19	17	323	347
20	18	359	383
21	19	397	421
22	20	437	461

b) Remarque. Les termes ne sont pas tous premiers :

$u_{17} = 17^2$ et $v_{41} = 41^2$.

70 • « Si n divise a^2, alors n divise a. »

a) La proposition est **fausse** : 8 divise 16, mais 8 ne divise pas 4.

Remarque. Pour qu'elle soit vraie, il faut supposer de plus que n est premier.

b) Proposition réciproque : « Si n divise a, alors n divise a^2 ».

c) Cette réciproque est **vraie**.

• « Si n est premier, alors n est impair. »

a) La proposition est **fausse** car 2 est un nombre premier.

b) Proposition réciproque : « Si n est impair, alors n est premier ».

c) Cette réciproque est **fausse** : 9 n'est pas premier.

• « Si p et q sont deux nombres premiers distincts, alors p et q sont premiers entre eux. »

a) La proposition est **vraie** : ils n'ont chacun que deux diviseurs {1, p} et {1, q} et leur PGCD est égal à 1.

b) Proposition réciproque : « Si p et q sont premiers entre eux, alors p et q sont deux nombres premiers distincts ».

c) Cette réciproque est **fausse** : 5 et 9 sont premiers entre eux.

• « Si p est un nombre premier, alors p admet exactement deux diviseurs. »

a) La proposition est **vraie** (par définition).

b) Proposition réciproque : « Si p admet exactement deux diviseurs, alors p est un nombre premier ».

c) Cette réciproque est **vraie** (par définition).

• « Si p premier divise le produit ab, alors p divise a ou p divise b. »

a) La proposition est **vraie** (théorème 5).

b) Proposition réciproque : « Si p premier divise a ou divise b, alors p divise le produit ab ».

c) Cette réciproque est **vraie** (même si p n'est pas premier).

• « p est un nombre premier. Si $a \equiv p \pmod p$, alors a est premier. »

a) La proposition est **fausse** : $4 \equiv 2 \pmod 2$.

b) Proposition réciproque : « p est un nombre premier. Si a est premier, alors $a \equiv p \pmod p$ ».

c) Cette réciproque est **fausse** : 3 et 2 n'ont pas le même reste dans la division euclidienne par 2.

NOMBRES PREMIERS ET PGCD

71 **1.**

n	5	7	11	13	17	19	23
$n^2 + 11$	36	60	132	180	300	372	540

2. a) PGCD (36 ; 60) = 12.

b) $132 = 12 \times 11$, $180 = 12 \times 15$, $200 = 12 \times 25$;

$372 = 12 \times 31$, $540 = 12 \times 45$.

3. *Conjecture* : pour tout nombre premier $n \geqslant 5$, $n^2 + 11$ est divisible par 12.

Démonstration : un nombre premier $n \geqslant 5$ est de la forme $(6k + 1)$ ou $(6k + 5)$ avec k naturel non nul (*cf.* Ex. 23 p. 90).

• Si $n = 6k + 1$, $n^2 + 11 = 36\,k^2 + 12\,k + 12$ divisible par 12.

• Si $n = 6k + 5$, $n^2 + 11 = 36\,k^2 + 60\,k + 12$ divisible par 12.

Conclusion : pour tout nombre premier $n \geqslant 5$, $n^2 + 11$ est divisible par 12.

72 **1. a)** Dans $\mathbb{Z}$, si p divise x et y, alors p divise $mx + ny$ (m et n entiers relatifs).

p divise $(a + b)$ et ab donc la combinaison linéaire $a \times (a + b) - ab = a^2$.

b) Théorème 5 : si p premier divise ab, alors p divise a ou p divise b. p divisant a^2 , p divise a.

c) $b^2 = b(a + b) - ab$; donc, de même, p divise b^2 et b.

d) Notons d le PGCD $(a ; b)$.

d divisant a et b, divise $(a + b)$ et ab ainsi que leur PGCD ; donc d divise p.

p divisant a et b divise leur PGCD ; donc p divise d.

Finalement, $p = d$.

2. Le système est équivalent à : $\begin{cases}\text{PGCD}(a ; b) = 5 \\ ab = 850\end{cases}$

soit encore à :

$$\begin{cases}a = 5k \\ b = 5k' \\ kk' = 34\end{cases}, k \text{ et } k' \text{ étant premiers entre eux.}$$

$D_{34} = \{1, 2, 17, 34\}$. Comme $a \leqslant b$, on a :

$$\begin{cases}a = 5 \\ b = 5 \times 34\end{cases} \text{ ou } \begin{cases}a = 5 \times 2 \\ b = 5 \times 17\end{cases}.$$

Le système admet deux couples solution :

$(5 ; 170)$ et $(10 ; 85)$.

AVEC LES TICE

73 **1. a)**

A	B	C	D	E
p	$p+2$	$p+6$	$p+8$	$p+14$
2	4	8	10	16
3	5	9	11	17
4	6	10	12	18
5	7	11	13	19
6	8	12	14	20
7	9	13	15	21
8	10	14	16	22
9	11	15	17	23
10	12	16	18	24
11	13	17	19	25
12	14	18	20	26
13	15	19	21	27
14	16	20	22	28
15	17	21	23	29
16	18	22	24	30
17	19	23	25	31
18	20	24	26	32
19	21	25	27	33
20	22	26	28	34

b) $2 \notin \mathscr{C}$, $3 \notin \mathscr{C}$ et $5 \in \mathscr{C}$.

c) et **d)** Non : il semble qu'un des nombres de chaque ligne est un multiple de 5.

2. a) p est premier, $p \geqslant 6$.

Modulo 5 :

p	1	2	3	4
$p+2$	3	4	0	1
$p+6$	2	3	4	0
$p+8$	4	0	1	2
$p+14$	0	1	2	3

Pour p premier supérieur ou égal à 6, un des nombres est multiple de 5. *Conclusion* : $\mathscr{C} = \{5\}$.

74 **1. a)**

	A	B	C
1	1	1	
2	2	2	
3	3	6	5
4	4	24	19
5	5	120	101
6	6	720	619
7	7	5040	4421
8	8	40320	35899
9	9	362880	326981
10	10	3628800	3301819
11	11	39916800	36614981
12	12	479001600	442386619

b) La case Bn contient n!.

2. a) $3 ! - 2 ! + 1 ! = 6 - 2 + 1 = 5$.

$4 ! - 3 ! + 2 ! - 1 ! = 24 - 6 + 2 - 1 = 19$.

b) *Conjecture* : pour n entier naturel, $n \geqslant 3$:

$c_n = n ! - (n - 1) ! + (n - 2) ! + \ldots + (-1)^{n+1} 1 !$

$c_3 = 3 ! - 2 ! + 1 ! = 5$: (P_3) est vraie.

Supposons (P_n) vraie.

$c_{n+1} = (n + 1) ! - c_n$

$= (n + 1) ! - n ! + (n - 1) ! - \ldots + (-1)^n 1 !$

donc (P_{n+1}) est vraie.

Conclusion : (P_n) est vraie pour tout naturel $n \geqslant 3$.

3. a) $C_3 = 5$, $C_4 = 19$, $C_5 = 101$, $C_6 = 619$, tous premiers.

b) Non : $C_9 = 326\,981 = 79 \times 4\,139$.

Prendre toutes les initiatives

75 • n admet 3 diviseurs : $D_n = \{1, p, n\}$, $n = p^\alpha$ avec $\alpha + 1 = 3$; donc $\alpha = 2$ et n est un carré.

• n admet 5 diviseurs : 5 étant premier, $\alpha + 1 = 5$; donc $\alpha = 4$ et n est un carré.

• n admet k diviseurs, avec k impair.

Or $k = (\alpha + 1)(\beta + 1) \ldots (\gamma + 1)$.

Tous les facteurs $(\alpha + 1)$, $(\beta + 1)$, … et $(\gamma + 1)$ sont impairs, donc tous les exposants α, β, …, γ sont pairs et n est un carré.

76 Tout nombre premier n, strictement supérieur à 3, est congru à 1 ou 2 modulo 3 ; donc $n^2 \equiv 1 \pmod 3$. Ainsi, $p^2 + q^2 + r^2 \equiv 0 \pmod 3$; soit :

$p^2 + q^2 + r^2$ est un multiple de 3.

77 Remarquons que $a = b = 243$ fournit un couple solution ($243 = 3^5$ donc 6 diviseurs).

On suppose dans la suite que $a < b$.

Notons $d = \text{PGCD}(a ; b)$. d a 6 diviseurs.

$486 = 2 \times 35$ et d divise a et b donc leur somme 486.

Il en résulte :

$d = 2^\alpha \times 3^\beta$, avec $0 \leqslant \alpha \leqslant 1$ et $0 \leqslant \beta$.

Comme $(\alpha + 1)(\beta + 1) = 6$ et $(\alpha + 1) < (\beta + 1)$, on a :

$$\begin{cases}\alpha + 1 = 1 \\ \beta + 1 = 6\end{cases} \Leftrightarrow \begin{cases}\alpha = 0 \\ \beta = 5\end{cases} \text{ et } d = 243 = a = b ;$$

$$\begin{cases}\alpha + 1 = 2 \\ \beta + 1 = 3\end{cases} \Leftrightarrow \begin{cases}\alpha = 1 \\ \beta = 2\end{cases} \text{ et } d = 18.$$

Si $d = 18$, $a = 18\,k$ et $b = 18\,k'$, avec k et k' premiers entre eux et $k + k' = 27$.
Les couples $(k\,;\,k')$, avec $k < k'$ qui conviennent, sont : (1 ; 26), (2 ; 25), (4 ; 23), (5 ; 22), (7 ; 20), (8 ; 19), (10 ; 17), (11 ; 16) et (13 ; 14).
Les couples solution $(a\,;\,b)$ associés sont : (18 ; 468), (36 ; 450), (72 ; 414), (90 ; 396), (126 ; 360), (144 ; 342), (180 ; 306), (198 ; 288), (234 ; 252) auxquels on ajoute (243 ; 243).

78 Comme p est premier, il est donc premier avec tous les nombres qui ne sont pas multiples de p. Donc, il existe $np - n = n\,(p - 1)$ nombres premiers avec p inférieurs à np.

79 Notons n la mesure de l'arête du cube (en cm).
$n^3 + 1 \leqslant 1\,000 \Rightarrow n \leqslant 9$.

n	1	2	3	4	5	6	7	8	9
$n^3 + 1$	2	9	28	65	126	217	344	513	730

Il reste à trouver, parmi ces nombres $(n^3 + 1)$, ceux dont la décomposition en produit de trois entiers distincts et strictement supérieurs à 1 est possible.
$9 = 3^2$; $28 = 2^2 \times 7$; $65 = 5 \times 13$; $126 = 2 \times 7 \times 9$; $217 = 7 \times 31$; $344 = 2^3 \times 43$; $513 = 3^3 \times 19$ et $730 = 2 \times 5 \times 73$.
Ceux qui conviennent sont :
$126 = 2 \times 7 \times 9$; $344 = 2 \times 4 \times 43$; $513 = 3 \times 9 \times 19$ et $730 = 2 \times 5 \times 73$.
En résumé :

Le cube	5	7	8	9
Le pavé	2 ; 7 ; 9	2 ; 4 ; 43	3 ; 9 ; 19	2 ; 5 ; 73

80 $a = 4 \times 10^{\alpha} = 2^{\alpha+2} \times 5^{\alpha}$
donc $(\alpha + 3)(\alpha + 1) = 143 = 13 \times 11$
soit $\alpha = 10$ et $a = 4 \times 10^{10}$.

EXERCICES Le jour du BAC (page 100)

81 *Corrigé sur le site élève.*

82 **1.** $2^{11} - 1 = 23 \times 89$.
2. a) $2^p = (2^p - 1) + 1$ soit $2^p \equiv 1 \pmod{(2^p - 1)}$.
$2^{pq} = (2^p)^q$, donc $2^{pq} \equiv 1^q \pmod{(2^p - 1)}$.
b) De même $2^{pq} \equiv 1 \pmod{(2^q - 1)}$.
$2^{pq} - 1 \equiv 0 \pmod{(2^p - 1)}$ et $2^{pq} - 1 \equiv 0 \pmod{(2^q - 1)}$.
$2^{pq} - 1$ est divisible par $(2^p - 1)$ et par $(2^q - 1)$.
3. Par contraposition :
Si n n'est pas premier, $n = p \times q$ avec p et q entiers naturels strictement supérieurs à 1.
Alors, d'après ce qui précède, $2^n - 1$ est divisible par $2^p - 1$ (diviseur strict) donc $2^n - 1$ n'est pas premier.
La réciproque est fausse : *cf.* **1.**

83 **1.** p premier supérieur ou égal à 7 est congru à 1 ou 2 modulo 3, donc p^4 est congru à 1 modulo 3, soit :
$$p^4 - 1 \equiv 0 \pmod 3.$$
2. $p = 2k + 1$ avec $k \geqslant 3$.
$p^2 - 1 = (p - 1)(p + 1) = 4k\,(k + 1)$
$p^2 + 1 = 4k^2 + 4k + 2 = 2\,(2k^2 + 2k + 1)$
$p^4 - 1 = 8k\,(k+1)\,(2k^2 + 2k + 1)$.
k et $k + 1$ sont deux entiers consécutifs : leur produit est pair ainsi $p^4 - 1$ est divisible par 16.
3. p premier supérieur ou égal à 7 donc modulo 5 :

p	1	2	3	4
$p^2 + 1$	2	0	0	2
$p^2 - 1$	0	3	3	0
$p^4 - 1$	0	0	0	0

Dans tous les cas, 5 divise n.

4. a) $c = ak = bk'$ avec k et k' premiers entre eux.
a divise bk' et est premier avec b, donc (théorème de Gauss) a divise k', soit $k' = ak''$ et $c = abk''$.
Conclusion : ab divise c.
b) n est multiple de 3 et de 16 donc de 48.
n est multiple de 48 et de 5 donc de 240.
5. $A = (p_1^4 - 1) + (p_2^4 - 1) + \ldots + (p_{15}^4 - 1) + 15$.
Pour tout entier k compris entre 1 et 15, $p_k^4 - 1$ est divisible par 15. Il est en de même de A qui n'est donc pas premier.
Il n'existe pas 15 nombres premiers supérieurs ou égaux à 7 tel que A soit premier.

84 **1. a)** $a_1 = 39$, $b_1 = 19$, $c_1 = 21$,
$a_2 = 399$, $b_2 = 199$, $c_2 = 201$,
$a_3 = 3\,999$, $b_3 = 1\,999$, $c_3 = 2\,001$.
b) a_n, b_n et c_n s'écrivent (comme 10^n) avec $n + 1$ chiffres.
a_n ne s'écrit qu'avec des 9 et un 3, et la somme des chiffres apparaissant dans c_n est 3 : ils sont divisibles par 3 (critère de divisibilité par 3).
c) $\sqrt{b_3} \leqslant 45$ et b_3 n'est divisible par aucun des premiers inférieurs ou égaux à 43 donc b_3 est un nombre premier.
d) $\forall\, n \in \mathbb{N}^*$, $b_n \times c_n = 4 \times 10^{2n} - 1 = a_n$.
$a_6 = b_3 \times c_3 = 1\,999 \times 3 \times 23 \times 29 = 3 \times 23 \times 29 \times 1\,999$.
e) $\text{PGCD}(b_n\,;\,c_n) = \text{PGCD}(c_n\,;\,c_n - b_n) = \text{PGCD}(c_n\,;\,2)$.
Or, c_n étant impair, $\text{PGCD}(c_n\,;\,2) = 1$; donc $\text{PGCD}(b_n\,;\,c_n) = 1$: b_n et c_n sont premiers entre eux.
2. a) Théorème de Bézout appliqué à b_3 et c_3.
b) $2\,001 = 1\,999 \times 1 + 2$
$1\,999 = (2\,001 - 1\,999)\,999 + 1$
donc $1\,000 \times 1\,999 - 2\,001 \times 999 = 1$.
Une solution particulière de [1] est $(1\,000\,;\,-999)$.
c) Soit $(x\,;\,y)$ un couple solution de [1] :
$$1\,999\,x + 2\,001\,y = 1.$$

Or, $1\,999 \times 1000 - 2\,001 \times 999 = 1$, donc :

$$1\,999(x - 1\,000) + 2\,001(y + 999) = 0,$$

soit $1\,999(1\,000 - x) = 2\,001(y + 999)$.

2 001 et 1 999 étant premiers entre eux, le théorème de Gauss permet de conclure :

$$\begin{cases} 1\,000 - x = 2\,001k \\ y + 999 = 1\,999k \end{cases} \text{ (avec } k \in \mathbb{Z}) ;$$

d'où l'ensemble-solution de [1] :

$$\{(1\,000 - 2\,001\,k ; -999 + 1\,999\,k, k \in \mathbb{Z}\}.$$

85 **A. 1.** $4 \equiv 1 \pmod 3$ donc $4^n \equiv 1^n \pmod 3$.

2. 29 est premier, 4 est premier avec 29, donc (Théorème de Fermat) $4^{28} \equiv 1 \pmod{29}$ soit $4^{28} - 1 \equiv 0 \pmod{29}$.

3. $1 \leqslant n \leqslant 4$.

$4 \equiv 4 \pmod{17}$, $4^2 \equiv 16 \pmod{17}$ et $4^4 \equiv 1 \pmod{17}$.

Pour tout entier k naturel non nul, $(4^4)^k \equiv 1^k \pmod{17}$, donc $4^{4k} \equiv 1 \pmod{17}$, soit $4^{4k} - 1 \equiv 0 \pmod{17}$: $4^{4k} - 1$ est divisible par 17.

4. Modulo 5 :

n	1	2	3	4
$4^n - 1$	3	0	3	0

$4^2 \equiv 1 \pmod 5$, donc $4^{2k} \equiv 1 \pmod 5$ et $4^{2k+1} \equiv 4 \pmod 5$; soit $4^{2k} - 1 \equiv 0 \pmod 5$ et $4^{2k+1} - 1 \equiv 3 \pmod 5$.

Conclusion : $4^n - 1$ est divisible par 5 si, et seulement si, n est pair (non nul).

5. $4^{28} - 1$ est divisible par 3 (*cf.* **1.**) ;
$4^{28} - 1$ est divisible par 29 (*cf.* **2.**) ;
$4^{28} - 1$ est divisible par 17 (*cf.* **3.**) ;
$4^{28} - 1$ est divisible par 5 (*cf.* **4.**).

B. p premier > 2 donc p premier impair.

1. 2 étant premier avec p premier, $2^{p-1} \equiv 1 \pmod p$ (Petit théorème de Fermat).

p étant impair, $p - 1 = 2n$, avec n entier naturel non nul. Ainsi, $2^{2n} \equiv 1 \pmod p$ soit $4^n \equiv 1 \pmod p$.

2. a) $n = bq + r$ avec $r < b$.

$4^{bq+r} \equiv 1 \pmod p$, et $4^{bq+r} = (4^b)^q \times 4^r$ donc $4^r \equiv 1 \pmod p$.

Or $r < b$ et b est le plus petit entier strictement positif tel que $4^b \equiv 1 \pmod p$, donc $r = 0$.

b) Il résulte du **a)** que si $4^n \equiv 1 \pmod p$, alors n est multiple de b.

Réciproquement, si $n = bq$, $(4^b)^q \equiv 1 \pmod p$ donc $4^n \equiv 1 \pmod p$.

c) 4 est premier avec p (premier impair) donc :

$$4^{p-1} \equiv 1 \pmod p \text{ (Petit théorème de Fermat).}$$

D'après **b)** $p - 1$ est un multiple de b.

EXERCICES Pour aller plus loin (page 102)

86 **1. a)** $D_a = \{1, 2, 4, 8, 16, p, 2p, 4p, 8p, 16p\}$.

b) a parfait

$$\Leftrightarrow 1 + 2 + 4 + 8 + 16 + p + 2p + 4p + 8p + 16p = 32p$$
$$\Leftrightarrow 31 + 31p = 32\,p \Leftrightarrow p = 31.$$

2. a) $D_\alpha = \{1, 2, \ldots, 2^n, p, 2p, \ldots, 2^n p\}$.

$S = (1 + p)(1 + 2 + \ldots + 2^n) = (1 + p)(2^{n+1} - 1)$.

b) α parfait $\Leftrightarrow (1 + p)(2^{n+1} - 1) = 2^{n+1}\,p$

$$\Leftrightarrow p = 2^{n+1} - 1.$$

3. $S = \dfrac{1}{1} + \dfrac{1}{2} + \ldots + \dfrac{1}{2^n} + \dfrac{1}{p} + \dfrac{1}{2p} + \ldots + \dfrac{1}{2^n p}$

$$S = \left(1 + \frac{1}{p}\right) \times \frac{1 - \dfrac{1}{2^{n+1}}}{1 - \dfrac{1}{2}}$$

$$S = 2\left(1 + \frac{1}{2^{n+1} - 1}\right)\left(1 - \frac{1}{2^{n+1}}\right)$$

$$S = 2 \times \frac{2^{n+1}}{2^{n+1} - 1} \times \frac{2^{n+1} - 1}{2^{n+1}} = 2$$

4. Les 4 premiers nombres premiers de la forme $2^{n+1} - 1$ sont 3, 7, 31 et 127. Les nombres parfaits associés sont respectivement 6, 28, 496 et 8 128.

87 **1.** $p = 2$. (E) : $x^2 + y^2 = 4 \Leftrightarrow y^2 = 4 - x^2$

$$\begin{cases} x^2 \geqslant 1 \\ y^2 = 4 - x^2 \end{cases} \Leftrightarrow \begin{cases} 1 \leqslant y^2 \leqslant 3 \\ y^2 = 4 - x^2 \end{cases} \Rightarrow \begin{cases} y = 1 \\ x^2 = 3 \end{cases} \text{ impossible.}$$

2. $p \neq 2$.

a) Pour tout entier naturel n, n et n^2 sont de même parité.

p premier différent de 2 est impair.

p^2 est donc impair d'où x^2 et y^2 sont de parités différentes. Il en est de même de x et y.

b) *Par l'absurde*.

Si p divise x et y, alors p^2 divise x^2 et y^2.

Il existe deux entiers naturels non nuls k et k' tels que $x^2 = kp^2$ et $y^2 = k'p^2$.

Il en résulte $x^2 + y^2 = (k + k')\,p^2$, et donc $k + k' = 1$; ce qui est impossible.

c) Un diviseur commun de x et y est un diviseur de p^2, c'est-à-dire 1, p ou p^2. D'après ce qui précède, x et y ne sont pas divisibles par p. Ils ne sont donc pas divisibles par p^2 : leur PGCD est 1.

3. a) $|u^2 - v^2|^2 + 4u^2v^2 = u^4 + 2u^2v^2 + v^4$

$$= (u^2 + v^2)^2 = p^2.$$

b) • $5 = 2^2 + 1^2$ donc $(|2^2 - 1^2| ; 2 \times 1 \times 2)$, c'est-à-dire $(3 ; 4)$ est solution.

Vérification : $3^2 + 4^2 = 5^2$.

• $13 = 3^2 + 2^2$ donc $(|3^2 - 2^2| ; 2 \times 2 \times 3)$, c'est-à-dire $(5 ; 12)$ est solution.

Vérification : $5^2 + 12^2 = 13^2$.

4. a) $3 = 1 + 2$. 3 n'est pas somme de deux carrés.

$7 = 1 + 6 = 2 + 5 = 3 + 4$. 7 n'est pas somme de deux carrés.

b) • $y^2 = 9 - x^2 < 9$ donc $1 \leqslant y < 3$.

Si $y = 1$, alors $x^2 = 8$: ce qui est impossible ;

si $y = 2$, alors $x^2 = 5$: ce qui est impossible.

• $y^2 = 49 - x^2 < 49$ donc $1 \leqslant y < 7$.

y	1	2	3	4	5	6
x^2	48	45	40	33	24	13

Ce qui est impossible.

88 **1. a)** $D_a = \{1, a, a^2, \ldots, a^n\}$

b) $S(a^n) = \dfrac{1-a^{n+1}}{1-a}$ (a premier donc $a \neq 1$).

2. a)

$\otimes$	5^0	5^1	5^2	5^3	5^4
3^0	3^05^0	3^05^1	3^05^2	3^05^3	3^05^4
3^1	3^15^0	3^15^1	3^15^2	3^15^3	3^15^4
3^2	3^25^0	3^25^1	3^25^2	3^25^3	3^25^4
3^3	3^35^0	3^35^1	3^35^2	3^35^3	3^35^4
somme	$S(3^3)$	$5S(3^3)$	$5^2S(3^3)$	$5^3S(3^3)$	$5^4S(3^3)$

b) $S(16\,875) = S(3^3) \times (1 + 5^2 + 5^3 + 5^4)$
$= S(3^3) \times S(5^4)$.

c) $S(16\,875) = 40 \times 781 = 31\,240$.

3. a) Généralisation : en utilisant un tableau $n \times m$, on a :
$$S(N) = S(a^n) \times S(b^m) = \frac{1-a^{n+1}}{1-a} \times \frac{1-b^{m+1}}{1-b}.$$

b) $S(M) = \prod_{i=1}^{k} S(p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{1-p_i^{\alpha_i+1}}{1-p_i}$.

4. $472 = 2^3 \times 59$; $S(472) = \dfrac{1-2^4}{1-2} \times 60 = 900$.

$2\,310 = 2 \times 3 \times 5 \times 7 \times 11$; donc :
$$S(2\,310) = 3 \times 4 \times 6 \times 8 \times 12 = 6\,912.$$

89 **1.** Tout nombre p premier différent de 2 est impair donc congru à 1 ou 3 modulo 4, c'est-à-dire de la forme : $p = 4n + 1$ ou $p = 4n + 3$.

2. 3, 7, 11, 19 sont premiers de la forme $4n + 3$.

3. a) N est de la forme $4n - 1$ donc impair.
$$1 = 4 \times p_1 \times p_2 \times \ldots \times p_k - N.$$
Théorème de Bézout : N est premier avec tous les p_i.
N est donc divisible ni par 2, ni par aucun des éléments de $\mathscr{E}$.

b) Compte tenu du résultat précédent, les diviseurs premiers de N sont tous de la forme $4n + 1$.

c) Ainsi, $N = q_1 \times q_2 \times \ldots \times q_k$ avec $\forall\, i \in \mathbb{N}$, $1 \leqslant i \leqslant k$, $q_i \equiv 1 \pmod 4$ donc $N \equiv 1 \pmod 4$, soit N est de la forme $4n + 1$.
Ainsi, sous l'hypothèse « il existe un nombre fini de nombres premiers de la forme $4n + 3$ où n est un entier naturel », $N \equiv 1 \pmod 4$.
Or, par définition, $N \equiv -1 \pmod 4$.
L'hypothèse est donc fausse.
Conclusion : il existe une infinité de nombres premiers de la forme $4n + 3$ où n est un entier naturel.

90 **1. a)** $r_k = 0 \Leftrightarrow p$ divise ka. Or p ne divise pas k (car $0 < k < p$), donc (Théorème de Gauss) p divise a ; ce qui est contraire à l'hypothèse : a est un entier naturel non divisible par p.
Conclusion : $\forall\, k \in \mathbb{N}$, $r_k \neq 0$.

b) Remarque. Il est équivalent de démontrer :
$k = k' \Leftrightarrow r_k = r_{k'}$ (par contraposition).
L'implication $k = k' \Rightarrow r_k = r_{k'}$ est évidente.
Si $r_k = r_{k'}$, alors $ka \equiv k'a \pmod p$ soit $a(k - k') \equiv 0 \pmod p$.
a étant premier avec p, p divise $(k - k')$.
Or $0 \leqslant |k - k'| < p$ donc $k - k' = 0$, soit $k = k'$.

2. $a \times 2a \times \ldots \times (p-1)a \equiv r_1 r_2 \ldots r_{p-1} \pmod p$
$\Leftrightarrow a^{p-1}(p-1)! \equiv (p-1)! \pmod p$
$\Leftrightarrow (p-1)!\,(a^{p-1} - 1) \equiv 0 \pmod p$.
p premier ne divise aucun des facteurs de $(p - 1)!$ donc ne divise pas $(p - 1)!$.
Il divise donc $(a^{p-1} - 1)$ et $a^{p-1} - 1 \equiv 0 \pmod p$, soit $a^{p-1} \equiv 1 \pmod p$.

3. Si a est divisible par p :
$a \equiv 0 \pmod p$ et $a^p \equiv 0 \pmod p$ donc $a^p \equiv a \pmod p$.
Si a n'est pas divisible par p :
$a^{p-1} \equiv 1 \pmod p$ d'où $a^p \equiv a \pmod p$.

91 **1. a)** si $x = 1$: égalité $0 = 0$.
si $x \neq 1$: $1 + x + x^2 + \ldots + x^{k-1} = \dfrac{1-x^k}{1-x}$.

b) $(x^a - 1) = (x^b)^c - 1 = (x^b - 1)(1 + x^b + x^{2b} + \ldots + x^{b(c-1)})$ donc $(x^b - 1)$ divise $(x^a - 1)$.

2. a) $330 = 2 \times 3 \times 5 \times 11$. Tous les facteurs sont premiers (donc premiers entre eux) et corollaire du Théorème de Gauss (p. 56).

b) $n^{21} - n = n(n^{20} - 1)$. D'après **1.**, $n^{20} - 1$ est divisible par $n^{10} - 1$, par $n^4 - 1$ et par $n^2 - 1$.

c) Comme $A = n(n^{20} - 1)$, si n est un multiple de 3, 5 ou 11, A est divisible respectivement par 3, 5 ou 11.
Si n n'est pas un multiple de 3, 5 ou 11, n est premier avec 3, 5 et 11.
Petit théorème de Fermat : $n^{10} - 1 \equiv 0 \pmod{11}$,
$n^4 - 1 \equiv 0 \pmod 5$ et $n^2 - 1 \equiv 0 \pmod 3$.
Ainsi, A est divisible par 3, 5 et 11.

3. A est divisible par $n^2 - 1$ donc par $n + 1$.
Divisible par deux entiers consécutifs n et $n + 1$, A est pair.
Divisible par les nombres premiers 2, 3, 5 et 11, il est divisible par leur produit 330.

92 **1. a)** 109 est premier et $226 = 2 \times 113$:
PGCD (109 ; 226) = 1.
L'équation (E) admet bien des solutions (Théorème de Bézout).

b) L'algorithme d'Euclide donne une solution particulière $(-85 ; 41)$. Soit $(x ; y)$ un couple solution :
$$\begin{cases} -85 \times 109 + 41 \times 226 = 1 \\ x \times 109 - y \times 226 = 1 \end{cases}$$
d'où, $109(x + 85) = 226(y + 41)$.
109 étant premier avec 226, 109 divise $(y + 41)$, soit :
$y = -41 + 109k'$ (avec $k' \in \mathbb{Z}$).
Il en découle $x = -85 + 226\,k'$.
Ce qui peut se traduire (en posant $k = k' - 1$) par :
$$\begin{cases} x = 141 + 226k \\ y = 68 + 109k \end{cases} \text{(avec } k \in \mathbb{Z}\text{)}.$$

c) Pour avoir $0 \leqslant 141 + 226\,k \leqslant 226$, il faut prendre $k = 0$; d'où l'unique couple solution (141 ; 68).

2. Les nombres premiers inférieurs à $\sqrt{227}$ sont :

2 , 3, 5, 7, 11 et 13.

Ils ne divisent pas 227 qui est donc premier.

3. a) $f(0)$ est le reste de la division euclidienne de 0 par 227 donc $f(0) = 0$.

De même, $g(0)$ est le reste de la division euclidienne de 0 par 227 donc $g(0) = 0$,

soit $g[f(0)] = 0$.

b) 227 est premier avec tous les éléments (différents de 0 et 1) de A.

Petit théorème de Fermat : $a^{226} \equiv 1 \pmod{227}$, ce qui reste vrai pour $a = 1$.

c) $\forall\ a \in A^*$, $g[f(a)] \equiv [f(a)]^{141} \equiv (a^{109})^{141} \pmod{227}$

D'après **1. b)**, $109 \times 141 = 1 + 226 \times 68$; donc :

$$g[f(a)] \equiv a \times (a^{226})^{68} \pmod{227}.$$

Comme $a^{226} \equiv 1 \pmod{227}$, $g[f(a)] \equiv a \pmod{227}$.

$g[f(a)]$ et a appartient à A^* donc sont égaux.

$f[g(a)] = [g(a)]^{109} \equiv a^{141 \times 109} \pmod{227}$.

De même, on trouve $f[g(a)] = a$.