Arithmétique partie III Nombres premiers, Fermat

$\boxed{D}$ Un **nombre premier** est un entier naturel qui admet **exactement deux** diviseurs positifs, ce sont alors : 1 et lui-même.

$\boxed{i}$ Liste des 25 nombres premiers inférieurs à 100 :

2, 3, 5, 7,11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.

$\boxed{i}$ Au lieu de dire « un diviseur qui est un nombre premier » on dit plus simplement un **diviseur premier**.

$\boxed{P}$ ▶Tout entier supérieur ou égal à 2 admet un diviseur premier.

A01 Pour chacun des entiers $n \geqslant 2$ suivants donner un diviseur premier (au choix) :

$n = 2, n = 3, n = 4, n = 5, n = 6$ et $n = 237\,411$.

A02 (voir PDF) On souhaite démontrer la propriété précédente.
Pour tout $n \in \mathbb{N}$ on considère la proposition P_n : « tout entier naturel compris au sens large entre 2 et n admet un diviseur premier ».
Démontrer par récurrence que, pour tout entier $n \geqslant 2$, P_n est vraie.
Faire le lien avec la propriété du cours.

$\boxed{P}$ Si un entier est supérieur à 2 et n'est pas premier, alors il admet un diviseur premier compris au sens large entre 2 et $\sqrt{n}$.

A03 Le nombre $n = 5$ est supérieur ou égal à 2 et est premier.
Admet-il un diviseur premier compris au sens large entre 2 et $\sqrt{n}$?
Dans la propriété précédente la condition « n n'est pas premier » est essentielle.

A04 (voir PDF) On souhaite démontrer la propriété précédente.
Soit n un entier supérieur ou égal à 2 et qui n'est pas premier.
Il existe a et b entiers supérieurs ou égaux à 2 tels que $n = ab$.

1. On suppose $a > \sqrt{n}$ et $b > \sqrt{n}$, montrer que $ab > n$ puis aboutir à une contradiction. Conséquence : $2 \leqslant a \leqslant \sqrt{n}$ ou $2 \leqslant b \leqslant \sqrt{n}$.
2. On suppose $2 \leqslant a \leqslant \sqrt{n}$.
   a. Si a est premier, conclure.
   b. Si a n'est pas premier justifier l'existence d'un diviseur premier p de a puis que $2 \leqslant p \leqslant \sqrt{n}$, conclure.
   c. Traiter à l'oral le cas $2 \leqslant b \leqslant \sqrt{n}$.

$\boxed{M}$ Pour démontrer qu'un entier n est premier :

• **calculs à la main**

on écrit la liste de tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$ puis on vérifie qu'aucun de ces nombres ne divise n

• **utilisation d'un programme Python**

on teste tous les entiers compris entre 2 et $\sqrt{n}$:

```
from math import *
n=int(input("n="))
flag=1
k=2
while (flag!=0 and k<=sqrt(n)):
    if n%k==0:
        flag=0
    k=k+1
if flag==1 and n>=2:
    print(n,"est premier")
else:
    print(n,"n'est pas premier")
```

A05 Déterminer si 139 est ou non premier.

P ▶Il existe une infinité de nombres premiers.

A06 On veut démontrer qu'il y a une infinité de nombres premiers.
Supposons qu'il existe un nombre fini de nombres premiers notés $p_1, p_2, \dots, p_N$ et posons $A = p_1 \times p_2 \times \dots + p_N + 1$.

1. Justifier que : $A \geqslant 3$.
2. En déduire que A admet un diviseur premier que l'on notera p_α.
3. Justifier que $p_\alpha | A - p_1 \times \dots \times p_N$ puis montrer que cette assertion est nécessairement fausse.

Conclure.

Affiche la liste des nombres premiers inférieur ou égaux à n :

```
def EstPremier(n:int):
    nombredediviseurs=0
    for k in range(1,n+1):
        if n%k==0:
            nombredediviseurs=nombredediviseurs+1
        k=k+1
    if nombredediviseurs==2:
        return "oui"
    else:
        return "non"
n=int(input("n="))
L=[]
for k in range(1,n+1):
    if EstPremier(k)=="oui":
        L.append(k)
print(L)
```

P ▶Soit p un nombre **premier** alors tout entier strictement compris entre 0 et p est **premier avec p**.

exemple 7 est premier donc pour tout entier a tel que $0 < a < 7$ les nombres n et 7 sont premiers entre eux.

A07 Démontrer la propriété précédente.

P ▶**Lemme d'Euclide**
Soit p un nombre **premier**, a et b deux entiers relatifs, alors on a l'implication : $p|ab \Rightarrow p|a$ ou $p|b$.

(si un nombre **premier** divise un produit, alors il divise au moins l'un des facteurs de ce produit)

A08 On souhaite démontrer le Lemme d'Euclide.
Soit p **premier** tel que : $p|ab$, montrons que : $p|a$ ou $p|b$.
Procédons par disjonction de cas suivant que p divise ou non a.

1. On suppose $p|a$: conclure.
2. On suppose que p ne divise pas a :
   • montrer que $\text{PGCD}(a,p) \neq p$, en déduire que a et p sont premiers entre eux
   • on a : $p|ab$ avec p et a premiers entre eux, que peut-on en déduire ?

Conclure.

Rappels
Pour tout $n \in \mathbb{N}$ et tous réels a et b, formule du binôme de Newton :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$
$$= \binom{n}{0} a^0 b^n + \binom{n}{1} a^1 b^{n-1} + \dots + \binom{n}{k} a^k b^{n-k} + \dots + \binom{n}{n} a^n b^0$$

[P] Petit théorème de Fermat version a^p

▶ Soit p un nombre premier, alors pour tout $a \in \mathbb{Z}$, on a :

$$\boldsymbol{a^p \equiv a\ [p]} \quad (a \in \mathbb{Z})$$

A09 On souhaite démontrer le théorème de Fermat version a^p.
Soit p un nombre premier.

1. Vérifier que, pour k entier naturel tel que $1 \leqslant k \leqslant p$ on a :

$$p\binom{p-1}{k-1} = k\binom{p}{k}$$

En déduire que, pour tout $k \in \mathbb{N}$ tel que $1 \leqslant k < p$, on a : $p|\binom{p}{k}$.

2. Démontrer que, pour tout $a \in \mathbb{Z}$:

$$(a+1)^p = 1 + a^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k$$

3. Pour tout $a \in \mathbb{N}$, on note P_a la proposition : $a^p \equiv a\ [p]$.
Démontrer par récurrence sur a que : $\forall a \in \mathbb{N}$, P_a est vraie.

4. Démontrer que pour tout entier a strictement négatif on a :
$a^p \equiv a\ [p]$, puis conclure.

A10 A-t-on : $7|15^7 - 15$, $7|21^7 - 21$, $7|3^7 - 3$?

A11 Démontrer que, pour tout entier relatif a : $34|a^{17} - a$.

A12 Démontrer que, pour tout entier relatif a : $78|a^{13} - a$.

[P] ▶Petit théorème de Fermat version a^{p-1}

Soit p un nombre premier, alors pour tout $a \in \mathbb{Z}$ non multiple de p on a :

$$\boldsymbol{a^{p-1} \equiv 1\ [p]}\ (a \in \mathbb{Z}\ \textbf{non multiple de}\ p)$$

A13 Démontrer le petit théorème de Fermat version a^{p-1}.

A14 Démontrer que : $23^{18} \equiv 1\ [19]$.

A15 Démontrer que : $12^{16} \equiv 1\ [17]$.

A16 A-t-on : « $44^{10} \equiv 1\ [11]$ » ?

A17 Montrer que : $7|8^{72} - 1$ et $13|8^{72} - 1$, en déduire : $91|8^{72} - 1$.

A18 Démontrer que : $190|17^{180} - 1$.

A19 Un élève affirme « si p est un nombre premier, alors pour tout entier naturel n on a : $p|3^{n+p} - 3^{n+1}$ » : si cette est affirmation est fausse en donner un contre-exemple, sinon la démontrer.

A20 [d'après une question bac S]

1. Montrer que : $29|4^{28} - 1$.

2. Soit $n \in \mathbb{N}$, montrer que : $3|4^n - 1$.

3. Soit $k \in \mathbb{N}$, montrer que : $5|4^{4k} - 1$ et $17|4^{4k} - 1$.

4. Déduire de **1.**, **2.**, **3.** quatre diviseurs premiers de $4^{28} - 1$.

A21 [d'après Bac S Amériques du Nord, Juin 2009

On pose : $A = \{1; 2; 3; \ldots; 45; 46\} = [\![1\,;46]\!]$.

1. On considère l'équation $(E) : 23x + 47y = 1$ où $(x, y) \in \mathbb{Z}^2$.

a. Résoudre (E).

b. En déduire qu'il existe un unique entier x appartenant à A tel que : $23x \equiv 1\ [47]$ et préciser cet entier.

2. Soient a et b deux entiers relatifs.

a. Montrer que : si $ab \equiv 0\,[47]$ alors $a \equiv 0\,[47]$ ou $b \equiv 0\,[47]$

b. En déduire que :
si $a^2 \equiv 1\ [47]$, alors : $a \equiv 1\,[47]$ ou $a \equiv -1\ [47]$.

3. a. Montrer que pour tout entier p de A, il existe un entier relatif q tel que $p \times q \equiv 1\ [47]$.

Pour la suite, on admet que, pour tout entier p appartenant à A, il existe un unique entier appartenant à A noté $inv(p)$ tel que : $p \times inv(p) \equiv 1$ [47].

b. Quels sont les entiers p de A qui vérifient : $p = inv(p)$?

c. Démontrer que : $46\,! \equiv -1\ [47]$.

A22 Déterminer le reste modulo 37 de 56^{4000}.

A23 [d'après bac S Amérique du Nord – Mai 2011]

On considère la suite (u_n) définie pour tout entier naturel n par :

$$u_n = 2^n + 3^n + 6^n - 1$$

1. Calculer u_0, u_1 et u_2.
   On admettra que : $u_3 = 250$, $u_4 = 1\,392$ et $u_5 = 8\,050$.
2. Justifier que $7|u_5$.
3. Montrer que, pour tout entier naturel n, u_n est pair.
4. Montrer que, pour tout entier naturel n non nul et pair, u_n est divisible par 4.

Dans toute la suite, on note (E) l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n).

5. Justifier que : 2, 3, 5 et 7 appartiennent à (E).
6. Soit p un nombre premier strictement plus grand que 3.
   a. Montrer que : $6 \times 2^{p-2} \equiv 3\ [p]$ et $6 \times 3^{p-2} \equiv 2\ [p]$.
   b. En déduire que : $6 \times u_{p-2} \equiv 0\ [p]$.
   Est-il exact d'affirmer que « tout nombre premier divise au moins l'un des termes de la suite (u_n) » ?

A24 [d'après bac S CE – Juin 2006]

Soit p un nombre premier différent de 2.

1. Démontrer qu'il existe un entier $n \geqslant 1$ tel que $4^n \equiv 1\ [p]$.
2. Soit $n \geqslant 1$ un entier tel que $4^n \equiv 1\ [p]$, on note b le plus petit entier strictement positif tel que $4^b \equiv 1\ [p]$ et r le reste de la division euclidienne de n par b.
   a. Démontrer que $4^r \equiv 1\ [p]$, en déduire que $r = 0$.
   b. Prouver l'équivalence : $4^n - 1$ est divisible par p si et seulement si n est un multiple de b.
   c. En déduire que b divise $p - 1$.

[P] & [D] Décomposition en produit de facteurs premiers (DPFP)

Soit n un entier naturel, $n \geqslant 2$:

• il existe k nombres premiers distincts $p_1, \dots, p_k$ et k entiers naturels non nuls $\alpha_1, \dots, \alpha_k$ tels que : $n = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$, cette écriture unique à l'ordre des facteurs près, c'est la **décomposition en produit de facteurs premiers**, parfois notée DPFP

• les facteurs premiers sont $\underbrace{p_1, \dots, p_1}_{\alpha_1 \text{ nombres}}, \dots, \underbrace{p_k, \dots, p_k}_{\alpha_k \text{ nombres}}$ et non les nombres $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$ (si $\alpha_i > 1$, alors $p_i^{\alpha_i}$ n'est pas premier)

• n admet $(\alpha_1 + 1) \times (\alpha_2 + 2) \times \dots \times (\alpha_k + 1)$ diviseurs positifs distincts, chacun étant de la forme : $p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$ avec, pour tout i entier tel que $1 \leqslant i \leqslant k$, $0 \leqslant \beta_i \leqslant \alpha_i$
(on utilise un arbre de choix pour obtenir les diviseurs positifs de n)

A25 Donner la DPFP de $n = 200$, en déduire le nombre de diviseurs positifs de n puis les écrire tous dans l'ordre croissant.

[D] $a \neq 0$ et $b \neq 0$ entiers relatifs, le **plus petit commun multiple** de a et b, noté $\text{PPCM}(a, b)$, est le plus petit des entiers **strictement positifs** multiple de a et multiple de b.

Notation : le $\text{PPCM}(a, b)$ est parfois noté $a \vee b$.

exemple
$a = 3, b = -4$
multiples strict. positifs de a : 3, 6, 9, 12, 15, 18, 21, 24, 27 etc.
multiples strict. positifs de b : 4, 8, 12, 16, 20, 24, 28, etc.
multiples strict. positifs communs : 12, 24 etc.
On a donc : $\text{PPCM}(a, b) = 12$, ce qui se note aussi : $a \vee b = 12$.

$\boxed{P}$ m et n sont deux entiers naturels supérieurs ou égaux à 2, on peut déduire de leurs DPFP respectives les écritures :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k} \text{ et } m = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_k^{\beta_k}$$

$p_1, p_2, \ldots, p_n$ sont des nombres premiers, $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k$ sont tous positions ou nuls, alors on a :

$$\text{PGCD}(m,n) = \prod_{i=1}^{k} p_i^{min(\alpha_i;\, \beta_i)}$$
$$= p_1^{min(\alpha_1\,;\, \beta_1)} \times p_2^{min(\alpha_2\,;\, \beta_2)} \times \ldots \times p_k^{min(\alpha_k\,;\, \beta_k)}$$

$$\text{PPCM}(m,n) = \prod_{i=1}^{k} p_i^{max(\alpha_i;\, \beta_i)}$$
$$= p_1^{max(\alpha_1\,;\, \beta_1)} \times p_2^{max(\alpha_2\,;\, \beta_2)} \times \ldots \times p_k^{max(\alpha_k\,;\, \beta_k)}$$

exemple

On a les DPFP : $440 = 2^3 \times 5 \times 11$ et $350 = 2 \times 5^2 \times 7^1$.

On en déduit :

$440 = 2^3 \times 5^1 \times 7^0 \times 11^1$ et $350 = 2^1 \times 5^2 \times 7^1 \times 11^0$.

$$\text{PGCD}(440,350) = 2^{\min(3;1)} \times 5^{\min(1;2)} \times 7^{\min(0;1)} \times 11^{\min(1;0)}$$
$$= 2^1 \times 5^1 \times 7^0 \times 11^0 = 2 \times 5 \times 1 \times 1 = 10$$

$$\text{PPCM}(440,350) = 2^{\max(3;1)} \times 5^{\max(1;2)} \times 7^{\max(0;1)} \times 11^{\max(1;0)}$$
$$= 2^3 \times 5^2 \times 7^1 \times 11^1 = 8 \times 25 \times 7 \times 11 = 15\,400$$

$\boxed{P}$ Pour a et b entiers relatifs non nuls :

▶ $\text{PGCD}(a,b) \times \text{PPCM}(a,b) = |a| \times |b|$

A26 $a = 112$ et $b = 40$, on va déterminer $\text{PPCM}(a,b)$ par deux méthodes différentes :

1. Déterminer $\text{PGCD}(a,b)$, en déduire $\text{PPCM}(a,b)$.
2. Déterminer les DPFP de 112 et 40, en déduire $\text{PPCM}(a,b)$

A27 Reprendre le même exercice avec $a = 315$ et $b = 44\,550$.