ARITHMÉTIQUE

✠ ***Exercice 1.*** [○]
Démontrer que $\dfrac{\ln 2}{\ln 5}$ n'est pas un nombre rationnel.

Par l'absurde : supposons que $\ln 2/\ln 5$ est un nombre rationnel. Il existe alors $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$ tel que $\ln 2/\ln 5 = a/b$, c'est-à-dire $2^b = 5^a$. L'unicité de la décomposition en nombres premiers nous dit alors que $a = b = 0$. C'est absurde ! Donc

$$\boxed{\frac{\ln 2}{\ln 5} \text{ est irrationnel.}}$$

✠ ***Exercice 2.*** [★]
Soit $n \in \mathbb{N}^*$. Pour tout $k \in \mathbb{N}^*$, on note $\tau(k)$ le nombre de diviseurs positifs de k. On pose

$$\overline{\tau}(n) = \frac{1}{n}\sum_{k=1}^{n} \tau(k).$$

1. Démontrer que
$$\Big(\sum_{d=1}^{n} \frac{1}{d}\Big) - 1 < \overline{\tau}(n) \leqslant \sum_{d=1}^{n} \frac{1}{d}.$$
2. En utilisant l'encadrement $\ln(n) \leqslant \sum\limits_{d=1}^{n} \dfrac{1}{d} \leqslant \ln(n) + 1$, donner un encadrement de $\overline{\tau}(n)$.

1. On a
$$\overline{\tau}(n) = \frac{1}{n}\sum_{k=1}^{n} \tau(k) = \frac{1}{n}\sum_{k=1}^{n}\sum_{d|k} 1 = \frac{1}{n}\sum_{d=1}^{n}\sum_{\substack{1\leqslant k\leqslant n\\ d|k}} 1 = \frac{1}{n}\sum_{d=1}^{n} \Big\lfloor \frac{n}{d} \Big\rfloor$$
donc, compte tenu de l'encadrement $x - 1 < \lfloor x \rfloor \leqslant x$ valable pour tout $x \in \mathbb{R}$, on a
$$\frac{1}{n}\sum_{d=1}^{n} \Big(\frac{n}{d} - 1\Big) < \overline{\tau}(n) \leqslant \frac{1}{n}\sum_{d=1}^{n} \frac{n}{d},$$
c'est-à-dire
$$\boxed{\Big(\sum_{d=1}^{n} \frac{1}{d}\Big) - 1 < \overline{\tau}(n) \leqslant \sum_{d=1}^{n} \frac{1}{d}.}$$
2. L'encadrement indiqué s'obtient avec des intégrales. Il implique que
$$\boxed{\ln(n) - 1 < \overline{\tau}(n) \leqslant \ln(n) + 1}$$

✠ ***Exercice 3.*** [○]
Résoudre l'équation $42x \equiv 85\ [121]$ d'inconnue $x \in \mathbb{Z}$.

L'algorithme d'Euclide donne

q_i	r_i	u_i	v_i
	121	1	0
2	42	0	1
1	37	1	-2
7	5	-1	3
2	2	8	-23
2	1	-17	49
	0		

donc, d'une part, $121 \wedge 42 = 1$, ce qui démontre que 42 est inversible dans $\mathbb{Z}/121\mathbb{Z}$ et, d'autre part, on a $-17 \times 121 + 49 \times 42 = 1$, ce qui donne $49 \times 42 \equiv 1\ [121]$ et prouve ainsi que 49 est l'inverse de 42 dans $\mathbb{Z}/121\mathbb{Z}$. Dès lors, on a

$$42x \equiv 85\ [121] \quad \Longleftrightarrow \quad x \equiv 85 \times 49\ [121] \quad \Longleftrightarrow \quad x \equiv 51\ [121].$$

Donc

$$\boxed{\text{les solutions de } 42x \equiv 85\ [121] \text{ sont les } x \in \mathbb{Z} \text{ tels que } x \equiv 51\ [121]}$$

✠ ***Exercice 4.*** [○]
Soient $a, b \in \mathbb{Z}$.

1. Démontrer que $(3a + 7b) \wedge (2a + 5b) = a \wedge b$.
2. Démontrer que $(a^2 + b^2) \wedge (ab) = (a \wedge b)^2$.

1. On pose $\delta = a \wedge b$, $A = 3a + 7b$, $B = 2a + 5b$ et $\Delta = A \wedge B$.
   Il est clair que δ divise A et B et donc que $\delta \mid \Delta$.
   De plus, on vérifie que $a = 5A - 7B$ et $b = -2A + 3B$, ce qui permet d'affirmer que Δ divise a et b, d'où $\Delta \mid \delta$.
   Finalement, $\delta = \Delta$ puisque δ et Δ sont tous les deux positifs. Donc
   $$\boxed{(3a + 7b) \wedge (2a + 5b) = a \wedge b.}$$
2. Posons $d = a \wedge b$. Il existe $A, B \in \mathbb{Z}^*$ tels que $a = dA$ et $b = dB$, avec A et B premiers entre eux. Soit p un facteur premier commun à AB et à $A^2 + B^2$. Alors p divise A ou B, disons par exemple A. Dans ce cas, il divise A^2 et donc $B^2 = B^2 + A^2 - A^2$, donc il divise B. Donc $p = 1$. Donc $A^2 + B^2 \wedge AB = 1$ donc
   $$\boxed{a^2 + b^2 \wedge ab = d^2.}$$

✠ ***Exercice 5.*** [⋆]
Pour tout $n \in \mathbb{N}$, on définit les entiers a_n et b_n par

$$(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}.$$

1. Justifier l'existence de a_n et b_n pour tout $n \in \mathbb{N}$.
2. Démontrer que $a_n \wedge b_n = 1$ pour tout $n \in \mathbb{N}$. *Indication : Utiliser* $(1 - \sqrt{2})^n$.

On pourrait traiter les deux questions de cet exercice par récurrence… mais ce ne serait vraiment pas fun !

1. Pour tout $n \in \mathbb{N}$, on a
$$\begin{aligned}
(1 + \sqrt{2})^n &= \sum_{k=0}^{n} \binom{n}{k} \sqrt{2}^k \\
&= \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} \sqrt{2}^k + \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} \sqrt{2}^k \\
&= \underbrace{\sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} 2^{k/2}}_{=a_n} + \sqrt{2} \underbrace{\sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} 2^{(k-1)/2}}_{=b_n}
\end{aligned}$$

avec $a_n, b_n \in \mathbb{N}$. Donc

$$\boxed{\text{pour tout } n \in \mathbb{N}, \text{ il existe } a_n, b_n \in \mathbb{N} \text{ tels que } (1+\sqrt{2})^n = a_n + b_n\sqrt{2}.}$$

2. En reprenant *mutatis mutandis* les calculs de la question précédente, on voit que, pour tout $n \in \mathbb{N}$,

$$(1-\sqrt{2})^n = a_n - b_n\sqrt{2}.$$

En multipliant entre elles les deux égalités $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$ et $(1-\sqrt{2})^n = a_n - b_n\sqrt{2}$, on obtient, pour tout $n \in \mathbb{N}$,

$$(-1)^n = {a_n}^2 - 2{b_n}^2.$$

Avec le théorème de Bézout, on en déduit que

$$\boxed{\text{pour tout } n \in \mathbb{N}^*, \ a_n \text{ et } b_n \text{ sont premiers entre eux.}}$$

✠ ***Exercice 6.*** [○]
Soit $n \in \mathbb{N}$.

1. Soit $p \in \mathbb{P}$. Démontrer la *formule de Legendre*

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor,$$

en expliquant pourquoi cette formule a bien un sens.

2. Soient $k_1, k_2, \ldots, k_p \in \mathbb{N}$ tel que $k_1 + k_2 + \cdots + k_p = n$. Démontrer que le coefficient multinomial

$$\frac{n!}{k_1!\, k_2!\, \ldots\, k_p!} \in \mathbb{N}.$$

1. Entre 1 et n, il y a $\lfloor n/p \rfloor$ multiples de p ; $\lfloor n/p^2 \rfloor$ multiples de p^2 ; etc ; $\lfloor n/p^k \rfloor$ multiples de p^k tant que $p^k \leqslant n$, c'est-à-dire $k \leqslant \lfloor \ln(n)/\ln(p) \rfloor$. D'où

$$v_p(n!) = \sum_{k=1}^{\lfloor \ln(n)/\ln(p) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Notons que l'on peut étendre la somme jusqu'à $+\infty$ puisque les termes au delà du rang $\lfloor \ln(n)/\ln(p) \rfloor$ sont nuls. Donc

$$\boxed{v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.}$$

2. A faire.

✠ ***Exercice 7.*** [★] (Nombres parfaits pairs)

1. Soit $M_p = 2^p - 1$ un nombre de Mersenne premier. On rappelle que cela implique que p est premier. Démontrer que $n = 2^{p-1}M_p$ est un nombre parfait, c'est-à-dire que la somme de ses diviseurs stricts (i.e. sauf lui-même) est égale à lui-même.
2. Démontrer que tout nombre parfait pair est du type précédent.

On conjecture qu'il n'existe pas de nombres parfaits impairs.

On note $\sigma(k)$ la somme des diviseurs de l'entier k et on rappelle que σ est une fonction multiplicative, c'est-à-dire $(k \wedge \ell = 1) \Longrightarrow \big(\sigma(k\ell) = \sigma(k)\sigma(\ell)\big)$.

1. On a

$$\sigma(n) = \sigma(2^{p-1}M_p) = \sum_{k=0}^{p-1} 2^k + \sum_{k=0}^{p-1} 2^k M_p = (1+M_p)\sum_{k=0}^{p-1} 2^k = 2^p(2^p-1) = 2^p M_p = 2n,$$

donc

$$\sigma(n) - n = n,$$

ce qui démontre que

$$\boxed{n = 2^{p-1}M_p \text{ est un nombre parfait.}}$$

2. Soit n un nombre parfait pair. On sait donc que $\sigma(n) = 2n$ et qu'il existe $\alpha, a \in \mathbb{N}^*$ tels que $n = 2^\alpha a$ avec a impair. On a donc
$$\sigma(2^\alpha a) = 2^{\alpha+1}a,$$
ce qui donne, compte tenu de la multiplicativité de σ et du fait que $2^\alpha \wedge a = 1$,
$$\begin{aligned} & \sigma(2^\alpha) \times \sigma(a) = 2^{\alpha+1}a \\ \iff \quad & \sum_{k=0}^{\alpha} 2^k \times \sigma(a) = 2^{\alpha+1}a \\ \iff \quad & (2^{\alpha+1}-1)\sigma(a) = 2^{\alpha+1}a. \end{aligned}$$
Comme $2^{\alpha+1}-1$ et a sont impairs, on en déduit qu'il existe $b \in \mathbb{N}^*$ impair tel que $\sigma(a) = 2^{\alpha+1}b$, ce qui donne
$$(2^{\alpha+1}-1)b = a.$$
Raisonnons par l'absurde en supposant que $b \neq 1$. Distinguons deux cas :

▷ Premier cas : $b \neq 2^{\alpha+1}-1$
On constate alors que 1, b, $2^{\alpha+1}-1$ et $(2^{\alpha+1}-1)b$ sont des diviseurs distincts de a, ce qui implique que
$$\sigma(a) \geqslant 1 + b + (2^{\alpha+1}-1) + (2^{\alpha+1}-1)b = 2^{\alpha+1}(1+b),$$
c'est-à-dire
$$2^{a+1}b \geqslant 2^{\alpha+1}(1+b) \quad \iff \quad b \geqslant 1+b \quad \iff \quad 0 \geqslant 1,$$
ce qui est absurde !

▷ Second cas : $b = 2^{\alpha+1}-1$
On constate alors que 1, $2^{\alpha+1}-1$ et $(2^{\alpha+1}-1)^2$ sont des diviseurs distincts de a, ce qui implique que
$$\sigma(a) \geqslant 1 + (2^{\alpha+1}-1) + (2^{\alpha+1}-1)^2 = 2^{a+1}(2^{\alpha+1}-1) + 1,$$
c'est-à-dire
$$2^{a+1}(2^{\alpha+1}-1) \geqslant 2^{a+1}(2^{\alpha+1}-1) + 1 \quad \iff \quad 0 \geqslant 1,$$
ce qui est absurde !

Donc $b = 1$, ce qui donne
$$\sigma(a) = 2^{\alpha+1} \qquad \text{et} \qquad a = 2^{\alpha+1}-1.$$
En particulier, on a
$$\sigma(a) = a + 1,$$
ce qui signifie que a est premier (ses seuls diviseurs sont 1 et a). Comme $a = 2^{\alpha+1}-1$, on voit donc bien que a est un nombre de Mersenne premier.
En conclusion,

tout nombre parfait pair est de la forme $2^{p-1}M_p$ où M_p est un nombre de Mersenne premier.

✠ ***Exercice 8.*** [⋆]
Dans cet exercice, la lettre p désigne un nombre premier.

1. Soit $k \geqslant 1$. Démontrer que si p est un nombre premier tel que $k+2 \leqslant p \leqslant 2k+1$ alors p divise le coefficient binomial $\binom{2k+1}{k}$. En déduire que
$$\prod_{k+2 \leqslant p \leqslant 2k+1} p \leqslant 4^k.$$
2. Démontrer que
$$\forall n \geqslant 0, \qquad \prod_{p \leqslant n} p \leqslant 4^n.$$

Une étude plus fine montre que $\prod_{p \leqslant n} p \leqslant c^n$ *pour tout* $n \geqslant 1$ *avec* $c = 2,82590\ldots$ *C'est le meilleur coefficient possible : il y a égalité pour* $n = 113$ *et seulement dans ce cas (théorème prouvé par Rosser et Schœnfeld en 1962).*

1. On a
$$k!(k+1)!\binom{2k+1}{k} = (2k+1)!$$
donc
$$p \mid k!(k+1)!\binom{2k+1}{k}.$$
Comme $p \in [\![k+2; 2k+1]\!]$, on sait que p ne divise pas $k!(k+1)!$ et par conséquent que p divise $\binom{2k+1}{k}$. On en déduit que
$$\prod_{k+2\leqslant p\leqslant 2k+1} p \mid \binom{2k+1}{k}.$$
Or
$$(1+1)^{2k+1} = \binom{2k+1}{0} + \cdots + \binom{2k+1}{k} + \binom{2k+1}{k+1} + \cdots + \binom{2k+1}{2k+1} \geqslant 2 \times \binom{2k+1}{k},$$
donc
$$\binom{2k+1}{k} \leqslant 4^k.$$
En conclusion,
$$\boxed{\prod_{k+2\leqslant p\leqslant 2k+1} p \leqslant 4^k.}$$

2. Pour tout $n \in \mathbb{N}$, on pose
$$\mathscr{P}(n) : \quad \prod_{p\leqslant n} p \leqslant 4^n$$
- Initialisation : L'inégalité $\prod_{p\leqslant n} p \leqslant 4^n$ est clairement vérifiée pour $n = 0, 1, 2$.
Hérédité : Fixons $n \geqslant 2$ tel que $\mathscr{P}(0)$, $\mathscr{P}(1)$, …, $\mathscr{P}(n)$ sont vraies et démontrons $\mathscr{P}(n+1)$.
Si $n+1$ est pair, alors
$$\prod_{p\leqslant n+1} p = \prod_{p\leqslant n} p \leqslant 4^n \leqslant 4^{n+1}.$$
Si $n+1$ est impair, on l'écrit $n+1 = 2k+1$, d'où
$$\prod_{p\leqslant n+1} p = \prod_{p\leqslant 2k+1} p = \prod_{p\leqslant k+1} p \times \prod_{k+1<p\leqslant 2k+1} p \leqslant 4^{k+1} \times 4^k = 4^{n+1}$$
d'après l'hypothèse d erécurrrence et la question précédente.
Donc $\mathscr{P}(n+1)$ est vraie.
Conclusion : D'après le principe de récurrence, $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$, c'est-à-dire
$$\boxed{\forall n \geqslant 0, \qquad \prod_{p\leqslant n} p \leqslant 4^n.}$$

✠ ***Exercice 9.*** [○]
Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b\ [n]$. Démontrer que $a^n \equiv b^n\ [n^2]$.

On a
$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k.$$
D'une part, on a
$$n \mid a - b$$
D'autre part, on a
$$\sum_{k=0}^{n-1} a^{n-1-k}b^k \equiv \sum_{k=0}^{n-1} a^{n-1-k}a^k \equiv na^{n-1} \equiv 0 \quad [n],$$
donc
$$n \mid \sum_{k=0}^{n-1} a^{n-1-k}b^k.$$
Ainsi,
$$n^2 \mid a^n - b^n,$$
c'est-à-dire
$$\boxed{a^n \equiv b^n\ [n^2].}$$

✠ ***Exercice 10.*** [○]
Démontrer qu'un entier n congru à 3 modulo 4 ne peut être la somme de deux carrés.

Modulo 4, les seuls carrés sont 0 et 1. Il est donc impossible d'obtenir 3 en ajoutant deux carrés. Par conséquent,

un entier n congru à 3 modulo 4 ne peut être la somme de deux carrés.

✠ ***Exercice 11.*** [⋆]
Résoudre l'équation $15x^2 - 7y^2 = 9$ d'inconnues $x, y \in \mathbb{Z}$. *Indication :* $\mathbb{F}_3$.

Dans $\mathbb{F}_3$, l'équation devient $2y^2 = 0$, c'est-à-dire $y^2 = 0$ puisque 2 est inversible ($\mathbb{F}_3$ est un corps), d'où $y = 0$ (par intégrité). Ainsi, y est divisible par 3, c'est-à-dire $y = 3b$ où $b \in \mathbb{Z}$.

En reportant l'information $y = 3b$ dans l'équation $15x^2 - 7y^2 = 9$, on obtient $5x^2 - 21b^2 = 3$, ce qui donne $2x^2 = 0$ dans $\mathbb{F}_3$. Comme ci-dessus, on en déduit que x est divisible par 3, c'est-à-dire $x = 3a$ où $a \in \mathbb{Z}$.

En reportant l'information $y = 3b$ dans l'équation $5x^2 - 21b^2 = 3$, on obtient $15a^2 - 7b^2 = 1$, ce qui donne $2b^2 = 1$ dans $\mathbb{F}_3$ ou encore $b^2 = 2$ puisque 2 est l'inverse de 2 dans $\mathbb{F}_3$. Or 2 n'est pas un carré dans $\mathbb{F}_3$, donc

$15x^2 - 7y^2 = 9$ n'a pas de solutions dans $\mathbb{Z}$.

✠ ***Exercice 12.*** [★]

1. On appelle *triangle pythagorique* un triplet $(x, y, z) \in (\mathbb{N}^*)^3$ tel que $x^2 + y^2 = z^2$ où x, y et z sont premiers entre eux deux à deux.
   a) Démontrer que x et y ne sont pas de même parité.
   Quitte à échanger x et y, on suppose par la suite que x est impair et y est pair.
   b) Démontrer qu'il existe $t \in \mathbb{Q}$ tel que
   $$\frac{x}{z} = \frac{1-t^2}{1+t^2} \qquad \text{et} \qquad \frac{y}{z} = \frac{2t}{1+t^2}.$$
   c) En déduire qu'il existe $a, b \in \mathbb{N}^*$ premiers entre eux et de parités différentes tels que
   $$x = b^2 - a^2, \qquad y = 2ab \qquad \text{et} \qquad z = a^2 + b^2.$$
2. Démontrer que l'aire $\mathscr{A} = xy/2$ d'un triangle pythagorique (x, y, z) n'est jamais un carré parfait (Lemme de Fermat).
3. Démontrer le grand théorème de Fermat dans le cas $n = 4$: l'équation $x^4 + y^4 = z^4$ n'admet pas de solutions entières non triviales (c'est-à-dire telles que $xy \neq 0$).

1. a) Si x et y sont de même parité, ils ne peuvent être qu'impairs sinon ils ne seraient pas premiers entre eux. On peut donc écrire x et y sous la forme $x = 2k + 1$ et $y = 2\ell + 1$, ce qui donne $z^2 = x^2 + y^2 = 4(k^2 + k + \ell^2 + \ell) + 2$. Or un carré ne peut pas être de la forme $4m + 2$. En effet, si tel était le cas, il serait pair mais donc aussi multiple de 4 (puisque c'est un carré) et serait donc de la forme $4m$. On aboutit donc à une contradiction. On en déduit que

   x et y ne sont pas de même parité.

   b) Comme $z \neq 0$, l'équation $x^2 + y^2 = z^2$ est équivalente à $(x/z)^2 + (y/z)^2 = 1$. Le point $(x/z, y/z)$ appartient donc au cercle $\mathscr{C} : X^2 + Y^2 = 1$ privé du point $(-1; 0)$. Or ce cercle épointé admet la représentation paramétrique
   $$\begin{cases} X = \dfrac{1-t^2}{1+t^2} \\ Y = \dfrac{2t}{1+t^2} \end{cases} \qquad (t \in \mathbb{R}).$$
   On en déduit l'existence de $t \in \mathbb{R}$ tel que
   $$\frac{x}{z} = \frac{1-t^2}{1+t^2} \qquad \text{et} \qquad \frac{y}{z} = \frac{2t}{1+t^2}.$$

Or

$$\frac{x}{z}+t\frac{y}{z}=\frac{1-t^2}{1+t^2}+\frac{2t^2}{1+t^2}=1,$$

donc

$$t=\frac{z}{y}\Big(1-\frac{x}{z}\Big)\in\mathbb{Q}.$$

On a bien démontré que

$$\boxed{\exists t\in\mathbb{Q},\qquad \frac{x}{z}=\frac{1-t^2}{1+t^2}\qquad\text{et}\qquad \frac{y}{z}=\frac{2t}{1+t^2}.}$$

Remarque : la relation $t=(z/y)(1-x/y)$ semble tenir de la pure astuce. En fait, le paramétrage du cercle correspond aux relations $x/z=\cos\theta$, $y/z=\sin\theta$ et $t=\tan(\theta/2)$. Dès lors, on a

$$t=\tan(\theta/2)=\frac{\sin(\theta/2)}{\cos(\theta/2)}=\frac{2\sin^2(\theta/2)}{2\sin(\theta/2)\cos(\theta/2)}=\frac{1-\cos\theta}{\sin\theta}=\frac{z}{y}\Big(1-\frac{x}{z}\Big).$$

c) Écrivons t sous la forme $t=a/b$ où $\operatorname{pgcd}(a,b)=1$ de sorte que

$$\frac{x}{z}=\frac{a^2-b^2}{a^2+b^2}\qquad\text{et}\qquad \frac{y}{z}=\frac{2ab}{a^2+b^2}.$$

Démontrons que b^2-a^2 et b^2+a^2 sont premiers entre eux. Soit δ un diviseur de b^2-a^2 et b^2+a^2. Alors δ divise $2b^2$ et $2a^2$ et comme $\operatorname{pgcd}(a,b)=1$, on a nécessairement $\delta=1$ ou $\delta=2$. Si $\delta=2$, alors $(a^2-b^2)/2$ et $(a^2+b^2)/2$ sont premiers entre eux et comme

$$\frac{x}{z}=\frac{(a^2-b^2)/2}{(a^2+b^2)/2},$$

l'unicité de l'écriture irréductible d'une fraction irréductible (d'entiers positifs) nous dit que

$$x=\frac{a^2-b^2}{2}\qquad\text{et}\qquad z=\frac{a^2+b^2}{2}.$$

Mézalors, l'égalité

$$\frac{y}{z}=\frac{ab}{(a^2+b^2)/2},$$

nous dit que $y=ab$. Comme $\delta=2$, a et b sont tous les deuxs impairs, donc y est impair. Absurde ! Donc $\delta=1$, ce qui signifie bien que b^2-a^2 et b^2+a^2 sont premiers entre eux.
Dès lors, en utilisant de nouveau l'unicité de l'écriture irréductible d'une fraction irréductible (d'entiers positifs) avec l'égalité

$$\frac{x}{z}=\frac{a^2-b^2}{a^2+b^2},$$

on en déduit que

$$\boxed{x=a^2-b^2\qquad\text{et}\qquad z=a^2+b^2.}$$

Il s'ensuit immédiatement que

$$\boxed{y=2ab.}$$

Comme x est impair, a^2-b^2 est impair donc

$$\boxed{a\text{ et }b\text{ sont de parités différentes.}}$$

2. Raisonnons par l'absurde en supposant l'existence d'un triangle pythagorique (x,y,z) dont l'aire $\mathscr{A}=xy/2$ est un carré parfait.
Pour aboutir à une absurdité, nous allons construire un autre triangle pythagorique dont l'aire $\mathscr{A}'$ est un carré parfait strictement plus petit que $\mathscr{A}$. Le processus pouvant alors être répété indéfiniment, on obtiendrait ainsi une suite strictement décroissante d'entiers naturels ce qui n'est bien sûr pas possible (c'est le fameux procédé de *descente infinie* de Fermat).
D'après la question précédente, on sait qu'il existe $a,b\in\mathbb{N}^2$ premiers entre eux et de parités différentes tels que

$$x=b^2-a^2,\qquad y=2ab\qquad\text{et}\qquad z=a^2+b^2.$$

Dès lors, on a $\mathscr{A}=xy/2=ab(a^2-b^2)$, ce qui prouve que $ab(a^2-b^2)$ est un carré parfait. On constate que a, b et a^2-b^2 sont premiers entre eux deux à deux : on le sait déjà pour a et b ; par ailleurs, si un nombre premier p divise a et a^2-b^2, alors il divise $a^2-(a^2-b^2)=b^2$ et donc aussi b

(car p est premier), ce qui n'est pas possible ; on fait de même pour b et a^2-b^2. Comme un produit de nombres premiers deux à deux ne peut être un carré parfait que si chacun de ces nombres est aussi un carré parfait (c'est évident si l'on se penche sur la décomposition en facteurs premiers), on peut donc affirmer qu'il existe trois entiers α, β, γ tels que

$$a=\alpha^2, \qquad b=\beta^2 \qquad \text{et} \qquad a^2-b^2=\gamma^2.$$

En particulier, on a $\gamma^2+b^2=a^2$ avec a, b et γ premiers entre eux deux à deux (car la relation qui les lie dit qu'un éventuel diviseur premier commun à deux de ces trois nombres serait un diviseur premier commun de a et b, qui sont premiers entre eux). Autrement dit, le triplet (γ, b, a) est un triangle pythagorique. On va bien sûr lui appliquer le résultat de la question 1. Mais, avant cela, remarquons que γ est nécessairement impair puisque $\gamma^2=a^2-b^2$ avec a et b de parité différentes. Cela justifie l'existence d'entiers naturels non nuls A et B, premiers entre eux et de parités différentes, tels que

$$\gamma=A^2-B^2, \qquad b=2AB \qquad \text{et} \qquad a=A^2+B^2.$$

Dès lors, en combinant les relations $a=\alpha^2$ et $a=A^2+B^2$, on voit que $A^2+B^2=\alpha^2$. Comme A et B sont premiers entre eux, le même raisonnement que pour le triplet (γ, b, a) nous dit que A, B et α sont premiers entre eux deux à deux. Ainsi, (A, B, γ) est un triangle pythagorique. Si l'on note $\mathscr{A}'$ son aire, on a alors

$$\mathscr{A}'=\frac{AB}{2}=b=\beta^2,$$

ce qui signifie que $\mathscr{A}'$ est un carré parfait. Enfin, on constate que

$$\mathscr{A}'=b\leqslant ab=\frac{y}{2}<\frac{xy}{2}=\mathscr{A},$$

car $x>1$ sinon $z^2=y^2+1$ alors que deux carrés (non nuls) ne sont jamais consécutifs.
Partant d'un triangle pythagorique dont l'aire est un carré parfait, on a donc pu fabriquer un second triangle pythagorique dont l'aire est un carré parfait strictement plus petit. Le procédé de descente infinie nous dit que c'est absurde, donc

l'aire $\mathscr{A}=xy/2$ d'un triangle pythagorique (x,y,z) n'est jamais un carré parfait.

3. Supposons l'existence de trois entiers x, y et z tels que $x^4+y^4=z^4$ avec $xy\neq 0$. Quitte à diviser chacun de ces nombres par le pgcd des trois, on obtient un triplet d'entiers premiers dans leur ensemble. La relation qui les lie nous dit alors qu'ils sont premiers entre eux deux à deux. Dans ces conditions, le triplet (x^2, y^2, z^2) est un triangle pythagorique. Le résultat de la question 1 nous dit alors qu'il existe $a, b\in\mathbb{N}^2$ premiers entre eux et de parités différentes tels que

$$x^2=b^2-a^2, \qquad y^2=2ab \qquad \text{et} \qquad z^2=a^2+b^2.$$

Mézalors la relation $a^2+b^2=z^2$ couplée au fait que a , b et z sont premiers entre eux deux à deux (encore le même raisonnement) nous dit que (a, b, z) est un triangle pythagorique dont l'aire $\mathscr{A}=ab/2=y^2$ est un carré parfait. C'est absurde d'après le lemme de Fermat ! Donc

l'équation $x^4+y^4=z^4$ n'admet pas de solutions entières non triviales

Note historique (trouvée sur le net) :

Au XVIIè siècle, alors que les mathématiques ont un regain d'intérêt en Europe, le juge toulousain Pierre de Fermat consacre son temps libre à étudier l'Arithmetica de Diophante. Dans un passage consacré au théorème de Pythagore, Fermat note, dans la marge de son exemplaire de l'Arithmetica, l'observation suivante :

Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere.

Il est impossible pour un cube d'être écrit comme la somme de deux cubes ou pour une quatrième puissance d'être écrite comme la somme de deux quatrièmes puissances ou, en général, pour n'importe quel nombre égal à une puissance supérieure à deux d'être écrit comme la somme de deux puissances semblables.

Quelques lignes plus bas, il inscrit :

Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet

J'ai une démonstration véritablement merveilleuse de cette proposition, que cette marge est trop étroite pour contenir.

On ne retrouva jamais la « preuve » de Fermat (tout indique qu'il n'en avait d'ailleurs pas) et ce problème (l'inexistence de solutions entières non triviales pour l'équation $x^n+y^n=z^n$) fut la plus grande énigme, dans le monde des mathématiciens, pendant 4 siècles.

Le cas n=4 fut rapidement résolu (par Fermat lui-même, en utilisant la méthode de descente infinie). Le premier progrès important fut ensuite réalisé par Euler, près d'un siècle plus tard, qui vint à bout du cas n=3 en utilisant les nombres complexes. Il fallut ensuite attendre encore 75 ans pour que Sophie Germain, Dirichlet et Legendre prouvent le cas n=5. Quatorze ans plus tard, Lamé enrichit encore la méthode pour traiter le cas n=7. De nombreux travaux continuèrent sur ce problème, permettant des avancées considérables en mathématiques. Mais il fallut attendre 1996, et le mathématicien anglais Andrew Wiles, pour trouver une réponse définitive à cette énigme. Au fait, Fermat avait raison ! Il n'y pas de solutions à cette fameuse équation. Ce qui fut longtemps la conjecture de Fermat s'appelle désormais le théorème de Fermat–Wiles.

Pour en savoir plus sur l'aventure de ce théorème, on recommande la lecture de Le dernier théorème de Fermat, de Simon Singh, publié chez Lattès et chez Hachette Littératures. À un niveau très supérieur, celui qui s'intéresse au type de mathématiques nécessaires pour la démonstration, pourra lire Invitation aux mathématiques de Fermat–Wiles d'Yves Hellegouarch.