✍ *La première question repose sur la* ***décomposition d'un entier en produit de facteurs premiers****. Il est important de bien comprendre en quels sens cette décomposition est unique. (Veuillez noter le pluriel.)*

❧ *Cette décomposition est naturellement unique quand on l'écrit sous la forme d'un produit infini où apparaissent* <u>*tous*</u> *les nombres premiers : pour tout entier naturel $n \in \mathbb{N}^*$, il existe une, et une seule, famille $(\nu_p)_{p\in\mathscr{P}}$ d'entiers naturels presque tous nuls tels que*

$$n = \prod_{p\in\mathscr{P}} p^{\nu_p}.$$

La condition "presque tous nuls" signifie qu'il n'existe qu'un nombre fini de nombres premiers p de valuation non nulle ($\nu_p \geqslant 1$) et, puisqu'il n'y a donc qu'un nombre fini de facteurs p^{ν_p} différents de 1, cette condition assure l'existence du produit.

❧ *Une autre écriture est possible et consiste à ne faire apparaître que les facteurs premiers nécessaires à la décomposition de n, c'est-à-dire ceux dont la valuation est supérieure à 1. Dans ce cas, on écrit*

$$n = \prod_{k=1}^{d} p_k^{\alpha_k}$$

où les α_k sont des entiers au moins égaux à 1 (les valuations), les p_k sont des nombres premiers ($p_k \in \mathscr{P}$) deux à deux distincts et d, un entier naturel qui donne le nombre de facteurs premiers de n (qui dépend donc de n et est par exemple nul pour $n = 1$).

Cette expression est alors unique à l'ordre près :

$$\forall\, \sigma \in \mathfrak{S}_d, \quad \prod_{k=1}^{d} p_k^{\alpha_k} = \prod_{k=1}^{d} p_{\sigma(k)}^{\alpha_{\sigma(k)}}$$

mais je n'imagine pas qu'on puisse être assez agité du bonnet pour s'aventurer à de telles permutations.

❧ *Si on ne se limite pas aux seuls facteurs premiers nécessaires, la décomposition de n n'est plus unique :*

$$n = \prod_{k=1}^{d} p_k^{\alpha_k} = \prod_{k=1}^{d} p_k^{\alpha_k} \times \prod_{k=d+1}^{d+q} p_k^{0}.$$

Mais là encore, je ne vois pas pour quelle raison on s'amuserait à faire apparaître des facteurs fantômes.

❧ *En revanche, on peut décider arbitrairement de choisir une famille finie de nombres premiers deux à deux distincts $(p_k)_{1\leqslant k\leqslant d}$ et de considérer tous les entiers naturels non nuls n qu'on peut décomposer à l'aide de ces seuls nombres premiers (et seulement ces entiers n).*

On s'intéresse alors à un ensemble $E \subset \mathbb{N}^*$ tel que

$$\forall\, n \in E,\ \exists\,!\,(\alpha_k)_{1\leqslant k\leqslant d} \in \mathbb{N}^d, \quad n = \prod_{k=1}^{d} p_k^{\alpha_k}.$$

Cette factorisation est alors unique car les facteurs premiers qui interviennent ont été fixés une fois pour toutes.

❧ *En résumé, la décomposition d'un entier en produit de facteur premier est unique dès lors qu'on impose une* <u>*contrainte*</u> *sur les nombres premiers qui apparaissent :*

- *ils doivent* <u>*tous*</u> *apparaître lorsque le produit est indexé par $\mathscr{P}$ (et ils apparaissent alors presque tous avec une valuation nulle) ;*
- *on se restreint aux seuls facteurs nécessaires à la décomposition de n (ils apparaissent alors tous avec une valuation non nulle) ;*
- *on choisit une famille finie $(p_k)_{1\leqslant k\leqslant d}$ de nombres premiers deux à deux distincts et on se limite aux entiers qu'on peut factoriser à l'aide des nombres qu'on a choisis.*

1❧ On considère un entier naturel non nul n et on le décompose en produit de facteurs premiers :

$$n = \prod_{k=1}^{d} p_k^{\alpha_k}.$$

On sait alors qu'un entier m est un diviseur de n si, et seulement si, il existe une famille d'entiers $(\beta_k)_{1\leqslant k\leqslant d}$ tels que

$$m = \prod_{k=1}^{d} p_k^{\beta_k} \quad \text{et} \quad \forall\, 1 \leqslant k \leqslant d, \quad 0 \leqslant \beta_k \leqslant \alpha_k.$$

❧ L'unicité de la décomposition de m en produit de facteurs premiers assure qu'il y a autant de diviseurs de n que de familles $(\beta_k)_{1\leqslant k\leqslant d}$.

✍ *Ici, on a imposé une contrainte sur la décomposition de m : utiliser tous les facteurs qui ont servi à décomposer n et seulement ces facteurs. Il y a donc bien unicité de la décomposition de m.*

Pour chaque indice k, il y a donc $(\alpha_k + 1)$ choix possibles pour β_k, il y a donc

$$N = \prod_{k=1}^{d} (\alpha_k + 1)$$

diviseurs de n.

✍ *Si un galopin s'amusait à introduire des facteurs fantômes dans la décomposition de n (c'est-à-dire des facteurs $p_k^{\alpha_k}$ avec $\alpha_k = 0$), cela ne changerait rien à la valeur de N : si $\alpha_k = 0$, alors $(\alpha_k + 1) = 1$...*

❧ Si l'entier N est impair, alors chacun des facteurs dans cette décomposition est impair, donc chacune des valuations α_k est paire :

$$\forall\, 1 \leqslant k \leqslant d,\ \exists\, a_k \in \mathbb{N}, \quad \alpha_k = 2a_k.$$

L'entier n peut alors se décomposer sous la forme

$$n = \prod_{k=1}^{d} p_k^{2a_k} = \left(\prod_{k=1}^{d} p_k^{a_k}\right)^2,$$

c'est donc un carré parfait.

Réciproquement, si n est un carré parfait, alors il existe un entier m tel que $n = m^2$. De la décomposition du facteur m :

$$m = \prod_{k=1}^{d} p_k^{a_k},$$

on peut déduire que

$$n = m^2 = \prod_{k=1}^{d} p_k^{2a_k}$$

et donc que le nombre N de diviseurs de n est impair :

$$N = \prod_{k=1}^{d} (2a_k + 1).$$

2❧ On considère la famille $\mathscr{D} = (d_k)_{1\leqslant k\leqslant N}$ des diviseurs de N, rangés par ordre croissant :

$$1 = d_1 < d_2 < \cdots < d_{N-1} < d_N = n.$$

On peut démontrer (voir plus loin) que

$$\forall\, 1 \leqslant k \leqslant N, \quad d_k d_{N+1-k} = n.$$

✍ *Cette propriété permet de retrouver le résultat précédent.*

❧ *Si l'entier N est pair : $N = 2q$, alors la somme des deux indices est impaire*

$$k + (N + 1 - k) = 2q + 1$$

ce qui prouve que les deux indices k et $(N+1-k)$ sont distincts ! Les deux facteurs d_k et d_{N+1-k} sont alors distincts et cela prouve que n n'est pas un carré parfait.

❧ *Si l'entier N est impair : $N = 2q+1$, alors on peut choisir $k = (q+1)$ et dans ce cas, $N+1-k = (2q+1)+1-(q+1) = q+1$. On a alors $n = d_k d_{N+1-k} = d_{q+1}^2$ et n est un carré parfait.*

En posant

$$P = \prod_{k=1}^{N} d_k,$$

on obtient

$$P^2 = \left(\prod_{k=1}^{N} d_k\right)^2 = \prod_{k=1}^{N} d_k \times \prod_{\ell=1}^{N} d_\ell.$$

Avec le changement d'indice $\ell = N+1-k$,

$$P^2 = \prod_{k=1}^{N} d_k \times d_{N+1-k} = \prod_{k=1}^{N} d_k d_{N+1-k} = n^N.$$

✍ *La relation $d_k d_{N+1-k} = n$ est plus simple à deviner (sur une figure) qu'à démontrer !*

Elle est évidente pour $k=1$: le plus petit diviseur d_1 de n est égal à 1 et le plus grand diviseur d_N de n est égal à n.

Supposons qu'il existe un entier $1 \leqslant k < N$ tel que

$$d_k d_{N+1-k} = n.$$

Comme d_{k+1} est un diviseur de n, il existe un entier q tel que $d_{k+1} q = n$. Ce quotient q est aussi un diviseur de n, donc il existe un indice $1 \leqslant j \leqslant N$ tel que $q = d_j$ et on a

$$n = d_{k+1} d_j.$$

Si $j \geqslant N+1-k$, alors $d_j \geqslant d_{N+1-k}$ et donc

$$n = d_{k+1} d_j > d_k d_j \geqslant d_k d_{N+1-k} \overset{\text{HR}}{=} n.$$

C'est impossible ! Donc $j \leqslant N+1-k$.

Si $j < N-k$, alors $d_j < d_{N-k} = d_{(N+1)-(k+1)}$. Comme d_{N-k} est un diviseur de n, il existe un quotient $q' = d_\ell$ tel que $n = d_\ell d_{N-k}$. Si $\ell < k$, alors $d_\ell < d_k$ et

$$n = d_\ell d_{N-k} < d_k d_{N-k} < d_k d_{N+1-k} \overset{\text{HR}}{=} n.$$

C'est impossible ! Donc $j \geqslant N-k$ et finalement $j = N-k$.