# Questions & réponses

## Réponses

**R779. Posé dans RMS 123-2.**
**Étudier la limite de $(p_n)$ où $p_n$ est le plus grand diviseur premier de $2^n - 1$.**
**(Omar Sonebi)**

### *Réponse de Vincent Devinck*

Les entiers de la forme $2^n - 1$ sont appelés les nombres de Mersenne. Pour qu'un tel nombre soit premier, il faut que $n$ le soit aussi et la réciproque est fausse. En 1886, Bang (voir [1]) a démontré que pour tout entier $n \geqslant 2$, on a la minoration $p_n \geqslant n+1$, ce qui répond directement à la question. Nous montrerons ici ce résultat par une méthode élémentaire accessible avec un niveau prépa deuxième année , inspirée de celle de Zsigmondy, ce dernier ayant prouvé en 1892 (voir [7]), plus généralement, que si $a$ et $b$ sont des entiers naturels tels que $a > b > 0$, alors le plus grand facteur premier de $a^n - b^n$, noté $P(a^n - b^n)$ est au moins égal à $n + 1$.
À propos de $p_n$, Erdös a conjecturé en 1965 que $\lim\limits_{n\to+\infty} \dfrac{p_n}{n} = +\infty$ ; très récemment, Stewart a démontré cette conjecture (voir [6]). Mentionnons de plus le résultat suivant de Ford, Luca et Shparlinski (voir [3], 2009) : pour tout $\alpha < 1/2$, on a $\displaystyle\sum_{n\geqslant 1} \frac{(\ln n)^\alpha}{p_n} < +\infty$. La liste est loin d'être exhaustive et la recherche de minoration de $P(a^n - b^n)$ fait actuellement l'objet de nombreux travaux très profonds (certains résultats reposant notamment sur l'hypothèse de Riemann généralisée, voir par exemple [4]).
La preuve élémentaire annoncée repose sur l'étude des polynômes cyclotomiques. Nous allons donc montrer que $p_n \geqslant n + 1$ pour tout $n \geqslant 7$, ce qui répond à la question posée.
Notons, pour tout nombre premier $p$, $O_p(2)$ l'ordre de $2 \bmod p$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.
Bien que ce ne soit pas nécessaire, montrons simplement d'abord que si $q$ est premier, $q \geqslant 3$, alors $p_q \geqslant 2q + 1$. Le lemme ci-dessous fournit une description assez précise des facteurs premiers potentiels de $2^q - 1$ lorsque $q$ est un nombre premier impair.

**Lemme 1.** *Soit $q$ un nombre premier impair. Pour tout nombre premier $p$ divisant $2^q - 1$, il existe un entier naturel $k$ non nul tel que $p = 2kq + 1$.*

*Démonstration.* Comme $p$ divise $2^q - 1$, on a $2^q \equiv 1 \bmod p$. Donc $O_p(2)$ divise $q$. Or $q$ est un nombre premier et $O_p(2) > 1$ donc $O_p(2) = q$. Par ailleurs, on sait d'après le petit théorème de Fermat que $2^{p-1} \equiv 1 \bmod p$, donc $q = O_p(2)$ divise $p - 1$. De plus, $p$ est impair donc $2q$ divise $p - 1$. Il existe donc bien un entier naturel $k$ non nul tel que $p = 2kq + 1$. □

Puisque $p_q = 2kq + 1$ pour un certain $k \geqslant 1$, on a bien le résultat annoncé. Remarquons de plus que comme $p_2 = 3$, $p_4 = 5$ et $p_6 = 7$, on a $p_n \geqslant n + 1$ pour $2 \leqslant n \leqslant 6$ ; il suffit donc de prouver que $p_n \geqslant n + 1$ pour $n \geqslant 7$ pour établir que le résultat prouvé par Bang.
La démonstration du lemme 1 ne vaut pas pour un entier naturel $n$ quelconque (au lieu de $q$ premier) puisqu'on ne peut plus invoquer le fait que $O_p(2)$, où $p$ est un diviseur premier de $2^n - 1$, vaut exactement $n$. Toutefois, la preuve du lemme 1 contient l'idée essentielle de ce qui suit : nous allons montrer que si $n$ est un entier naturel assez grand fixé, alors on peut trouver un nombre premier $p$ tel que $O_p(2) = n$ (théorème 1), ce qui nous permettra de répondre à la question (corollaire 1). La preuve de l'existence d'un tel facteur premier $p$ repose essentiellement sur l'étude des polynômes cyclotomiques, qui fournissent une factorisation naturelle de $X^n - 1$ (voir 1. de la proposition 1).
Dans la suite, on note $\varphi$ la fonction indicatrice d'Euler définie par

$$\forall n \in \mathbb{N}^*, \quad \varphi(n) = \text{Card}\big(\big\{k \in [\![1, n]\!]\,;\, n \wedge k = 1\big\}\big)$$

On note $\mu$ la fonction de Möbius définie sur $\mathbb{N}^*$ par $\mu(1) = 1$, $\mu(n) = 0$ si $n$ a un facteur carré et $\mu(n) = (-1)^k$ si $n$ est le produit de $k$ nombres premiers distincts. Ces deux fonctions sont multiplicatives, c'est-à-dire que si $m$ et $n$ sont deux entiers naturels non nuls premier entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$ et $\mu(mn) = \mu(m)\mu(n)$. Le pgcd de deux entiers $m$ et $n$ sera noté $m \wedge n$. Si $d$ divise $n$, on note $d|n$ et, au besoin, $d \nmid n$ signifiera que $d$ ne divise pas $n$.
Pour tout $n \in \mathbb{N}^*$, on appelle $n^e$ polynôme cyclotomique le polynôme $\Phi_n$ défini par

$$\Phi_n(X) = \prod_{\substack{1 \leqslant k \leqslant n \\ n \wedge k = 1}} \big(X - \zeta_n^k\big)$$

où $\zeta_n = \mathrm{e}^{\frac{2i\pi}{n}}$. En particulier, si $p$ est un nombre premier, alors

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}$$

Parmi les nombreuses propriétés vérifiées par ces polynômes, nous aurons besoin des suivantes.

**Proposition 1.** *Soit $n \in \mathbb{N}^*$.*

1. *On a la factorisation $X^n - 1 = \prod_{d|n} \Phi_d(X)$.*
2. *Le polynôme $\Phi_n$ est à coefficients entiers.*
3. *Pour tout $n \geqslant 3$ et tout $x \in \mathbb{R}$, on a $\Phi_n(x) > 0$. De plus, $\Phi_n(2)$ est un entier impair au moins égal à 3.*
4. *Pour tout $x > 1$,*
$$\Phi_n(x) = \prod_{d|n} \big(x^d - 1\big)^{\mu(n/d)}$$

5. *Si $n = q^j m$ où $q$ est un nombre premier ne divisant pas $m$ et $j \in \mathbb{N}^*$ alors pour tout $x > 1$,*

$$\Phi_n(x) = \Phi_{q^{j-1}m}\big(x^q\big) = \cdots = \Phi_{qm}\big(x^{q^{j-1}}\big) = \frac{\Phi_m\big(x^{q^j}\big)}{\Phi_m\big(x^{q^{j-1}}\big)}$$

*Démonstration.* 1. Les racines dans $\mathbb{C}$ du polynôme $X^n-1$ étant les racines $n^e$ de l'unité, on a la factorisation $X^n - 1 = \prod_{k=1}^{n} \big(X - \zeta_n^k\big)$. En utilisant la partition

$$[\![1, n]\!] = \bigsqcup_{\delta|n} \big\{k \in [\![1, n]\!] \,;\, n \wedge k = \delta\big\}$$

(le symbole $\bigsqcup$ signifiant que la réunion est disjointe), on a

$$X^n - 1 = \prod_{\delta|n} \prod_{\substack{1\leqslant k\leqslant n\\ n\wedge k=\delta}} \big(X - \zeta_n^k\big)$$

Or, pour tout diviseur $\delta$ de $n$ et pour tout $k \in [\![1, n]\!]$, on a $n \wedge k = \delta$ si et seulement si $(n/\delta) \wedge k = 1$. En faisant le changement d'indice $j = k/\delta$ dans le produit intérieur, on obtient

$$X^n - 1 = \prod_{\delta|n} \prod_{\substack{1\leqslant j\leqslant n/\delta\\ (n/\delta)\wedge j=1}} \big(X - \zeta_n^{\delta j}\big)$$

Pour tout $\delta \in \mathbb{N}^*$, $\delta$ est un diviseur de $n$ si et seulement si $n/\delta$ est un diviseur de $n$ donc, en faisant le changement d'indice $n/\delta = d$, il vient

$$X^n - 1 = \prod_{d|n} \prod_{\substack{1\leqslant j\leqslant d\\ d\wedge j=1}} \big(X - \zeta_n^{nj/d}\big) = \prod_{d|n} \Phi_d(X)$$

puisque $\zeta_n^{n/d} = \mathrm{e}^{\frac{2\mathrm{i}\pi}{d}} = \zeta_d$.

2. On utilise une récurrence forte. Tout d'abord, $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Soit $n \in \mathbb{N}^*$ tel que pour tout $d < n$, on ait $\Phi_d \in \mathbb{Z}[X]$. En utilisant 1., il vient

$$X^n - 1 = \Phi_n(X)P(X) \qquad \text{où} \qquad P(X) = \prod_{\substack{d|n\\ d\neq n}} \Phi_d(X) \in \mathbb{Z}[X]$$

par hypothèse de récurrence. Raisonnons par l'absurde : supposons que $\Phi_n \notin \mathbb{Z}[X]$. Notons $\Phi_n(X) = \sum_{0\leqslant k\leqslant \varphi(n)} a_k X^k$ et $P(X) = \sum_{0\leqslant k\leqslant n-\varphi(n)} b_k X^k$. Posons

$$k_0 = \min\big\{k \in [\![0, n]\!] \,;\, a_k \notin \mathbb{Z}\big\}$$

où les coefficients $a_k$ sont a priori des nombres complexes et où les $b_k$ sont des entiers. Le coefficient de $X^{k_0}$ du polynôme $X^n - 1 = \Phi_n(X)P(X)$ est

$$a_0 b_{k_0} + a_1 b_{k_0-1} + \cdots + a_{k_0-1} b_1 + a_{k_0} b_0$$

qui est un entier (puisque $X^n - 1 \in \mathbb{Z}[X]$). Or $b_0 = P(0) = \pm 1$. Ceci entraîne que $a_{k_0}$ est un entier, contredisant la définition de $k_0$. Finalement, $\Phi_n \in \mathbb{Z}[X]$.

3. D'après 2., le polynôme $\Phi_n$ (vu comme fonction définie sur $\mathbb{R}$) prend des valeurs réelles et ne change pas de (car toutes ses racines sont complexes non réelles). Comme $\lim\limits_{x\to+\infty} \Phi_n(x) = +\infty$, on en déduit le résultat.

   Montrons maintenant que $\Phi_n(2) \geqslant 3$ si $n \geqslant 2$. Comme $\Phi_n(2)$ est un entier qui divise $2^n - 1$, c'est un entier impair et il suffit de montrer que $\Phi_n(2) > 1$. On a

$$\Phi_n(2) = |\Phi_n(2)| = \prod_{\substack{1\leqslant k\leqslant n \\ n\wedge k=1}} \left|2 - \zeta_n^k\right| > 1$$

   car pour tout $k \in [\![1, n]\!]$ tel que $n \wedge k = 1$, on a $\zeta_n^k \neq 1$.

4. Soit $x > 1$. Alors, d'après 1. et 3.,

$$\ln(x^n - 1) = \sum_{d|n} \ln(\Phi_n(x))$$

   et donc, d'après la formule d'inversion de Möbius,

$$\ln(\Phi_n(x)) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \ln(x^d - 1) = \ln\left(\prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}\right)$$

   d'où l'égalité annoncée en composant par la fonction exponentielle.

5. On démontre ces égalités en utilisant la propriété 4. Par exemple, pour la première, on remarque que les diviseurs $d$ de $n = q^j m$ pour lesquels $\mu(n/d) \neq 0$ sont nécessairement de la forme $q\delta$ où $\delta | q^{j-1} m$. On a donc

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{\delta | q^{j-1}m} \left(x^{q\delta} - 1\right)^{\mu(q^{j-1}m/\delta)} = \Phi_{q^{j-1}m}\left(x^q\right)$$

   On procède de la même manière pour établir les autres égalités.

□

D'aprés 1. de la proposition 1, si un nombre premier $q$ est tel que $O_q(2) = n$, alors $q$ divise $\Phi_n(2)$ mais ne divise aucun des $\Phi_d(2)$ où $d \neq n$ est un diviseur de $n$. D'où l'idée de chercher un tel facteur premier de $2^n - 1$ parmi les facteurs premiers de $\Phi_n(2)$. Son existence fait l'objet du résultat suivant.

**Théorème 1.** *Soit $n$ un entier naturel supérieur ou égal à 7. Il existe un nombre premier $q$ tel que $\mathrm{O}_q(2) = n$.*

*Démonstration.* On raisonne par l'absurde : supposons qu'un tel nombre premier n'existe pas. Soit $q$ un facteur premier de $\Phi_n(2)$ ; $q$ existe et est impair puisque $\Phi_n(2) \geqslant 3$. De plus, d'après l'hypothèse, $O_q(2) < n$.

- **Première étape :** *où l'on montre que $q$ divise $n$*
  Comme $O_q(2) < n$ (et $O_q(2)$ divise $n$), il existe un facteur premier $p$ de $n$ tel que $2^{n/p} \equiv 1 \bmod q$. En utilisant l'égalité 1. de la proposition 1, on voit que

$$2^n - 1 = \left(\prod_{d\mid \frac{n}{p}} \Phi_d(2)\right)\left(\prod_{\substack{d\mid n\\ d\nmid \frac{n}{p}\\ d\neq n}} \Phi_d(2)\right)\Phi_n(2) = \left(2^{n/p}-1\right)\left(\prod_{\substack{d\mid n\\ d\nmid \frac{n}{p}\\ d\neq n}} \Phi_d(2)\right)\Phi_n(2)$$

  ce qui montre que $\Phi_n(2)$ divise $\dfrac{2^n-1}{2^{n/p}-1}$ et donc, par transitivité, $q$ divise $\dfrac{2^n-1}{2^{n/p}-1}$. Or

$$\frac{2^n-1}{2^{n/p}-1} = \sum_{i=0}^{p-1} \left(2^{n/p}\right)^i \equiv \sum_{i=0}^{p-1} 1 \equiv p \bmod q$$

  Il s'ensuit donc que $q$ divise $p$ et comme tous deux sont des nombres premiers, $q = p$. Ainsi, $q$ divise $n$.

- **Deuxième étape :** *où l'on montre que $q$ est le plus grand facteur premier de $n$*
  D'après la première étape, pour tout facteur premier $p$ de $n$ différent de $q$, on a $2^{n/p} \not\equiv 1 \bmod q$. Donc il existe $j \in \mathbb{N}^*$ tel que $O_q(2) = \dfrac{n}{q^j}$. De plus, cet ordre est nécessairement un diviseur de $q-1$ d'après le petit théoréme de Fermat. Ainsi, l'entier $n$ s'écrit $n = q^j m$ où $m < q$. Par conséquent, $q$ est le plus grand facteur premier de $n$.

- **Troisième étape :** *où l'on montre que $\Phi_n(2) = q$*
  D'après les deux premières étapes, $q$ est le seul facteur premier de $\Phi_n(2)$ (*un* facteur premier de $\Phi_n(2)$ étant *le* plus grand facteur premier de $n$). Il s'agit donc de montrer que $q$ divise *exactement* $\Phi_n(2)$ (c'est-à-dire que $q^2 \nmid \Phi_n(2)$). On précise les calculs de la première étape. Posons $a = 2^{n/q} - 1$. Comme $q \geqslant 3$, on a

$$\frac{2^n-1}{2^{n/q}-1} = \frac{(a+1)^q - 1}{a} = q + \sum_{i=2}^{q-1} \binom{q}{i} a^{i-1} + a^{q-1}$$

  Si $i \in [\![2, q-1]\!]$, alors $q$ divise $\binom{q}{i}$ et $a^{i-1}$ et puisque $q-1 \geqslant 2$, $q^2$ divise $a^{q-1}$. Donc $\dfrac{2^n-1}{2^{n/q}-1} \equiv q \bmod q^2$, d'où $q^2 \nmid \Phi_n(2)$. Finalement, $\Phi_n(2) = q$.

- **Quatrième étape :** *où l'on aboutit à une absurdité*
  Rappelons que $n = q^j m$ où $q \geqslant 3$, $j \geqslant 1$ et $1 \leqslant m < q$. On aura besoin des estimations suivantes.

**Lemme 2.** *Soit $\alpha \geqslant 2$. Pour tout $d \geqslant 3$, on a*

$$(\alpha-1)^{\varphi(n)} < \Phi_d(\alpha) < (\alpha+1)^{\varphi(n)}$$

*Démonstration.* En effet, d'après 3. de la proposition 1, on a

$$\Phi_d(\alpha) = |\Phi_d(\alpha)| = \prod_{\substack{1\leqslant k\leqslant d\\(d\wedge k)=1}} \left|\alpha-\zeta_d^k\right|$$

et pour tout $k \in [\![1,d]\!]$ tel que $d \wedge k = 1$, on a (d'après l'inégalité triangulaire)

$$\alpha - 1 < \left|\alpha-\zeta_d^k\right| < \alpha+1$$

Les inégalités sont strictes car $\zeta_d^k \neq \pm 1$. Le nombre d'entiers $k \in [\![1,d]\!]$ premiers avec $d$ est égal à $\varphi(d)$, d'où le résultat. □

Si $j \geqslant 2$, alors $\Phi_n(2) = \Phi_{qm}\left(2^{q^{j-1}}\right)$ (d'après 5. de la proposition 1) et en appliquant le lemme 2 à $\alpha = 2^{q^{j-1}} \geqslant 8$ et à $d = qm \geqslant 3$, on obtient $q = \Phi_n(2) > 7^{\varphi(n)}$. Comme $\varphi$ est une fonction multiplicative, on a $\varphi(n) = \varphi(q^j)\varphi(m) \geqslant q-1$. Donc $q > 7^{q-1}$ ce qui est impossible si $q \geqslant 3$. Supposons maintenant que $j = 1$. En utilisant encore le lemme 2, il vient

$$q = \Phi_{qm}(2) = \frac{\Phi_m(2^q)}{\Phi_m(2)} > \left(\frac{2^q-1}{3}\right)^{\varphi(m)} \geqslant \frac{2^q-1}{3}$$

puisque $\varphi(m) \geqslant 1$. On obtient donc l'inégalité $2^q < 3q+1$. Ceci entraîne que $q = 3$ et comme $1 \leqslant m < 3$, il vient $n \leqslant 6$, ce qui est exclu par hypothèse. Finalement, le théorème est démontré.

□

Ceci permet de répondre à la question.

**Corollaire 1.** *On a* $\lim\limits_{n\to+\infty} p_n = +\infty$.

*Démonstration.* Soit $n \geqslant 7$. D'après le théorème 1, il existe un nombre premier $q$ tel que $O_q(2) = n$. En particulier, $q$ divise $2^n - 1$ et comme d'après le petit théorème de Fermat $2^{q-1} \equiv 1 \bmod q$, on a $n|q-1$. Donc $p_n \geqslant q \geqslant n+1$, d'où le résultat. □

***Bibliographie***

[1] A.S. Bang, *Taltheoretiske undersøgelser,* Tidsskrift for Mat., 1886.

[2] W. Feit, *On large Zsigmondy primes,* Proceedings of the American Mathematical Society, Volume 102, 1988.

[3] K. Ford, F. Luca and I.E. Shparlinski, *On the largest prime factor of the Mersenne numbers,* Bulletin of the Australian Mathematical Society, Volume 79, 2009.

[4] L. Murata and C. Pomerance, *The largest prime factor of a Mersenne number,* Number Theory, CNTA Proceedings, Lecture Notes Montreal, 2002.

[5] M. Roitman, *On Zsigmondy primes,* Proceedings of the American Mathematical Society, Volume 125, 1997.

[6] C.L. Stewart, *On divisors of Lucas and Lehmer numbers,* submitted to Acta Mathematica.

[7] K. Zsigmondy, *Zur Theorie der Potenzreste,* Monatshefte für Math. u. Phys..