

BROUILLON - N DIVISE $2^N + 1$

CHRISTOPHE BAL

*Document, avec son source L^AT_EX, disponible sur la page
<https://github.com/bc-writing/drafts>.*

Mentions « légales »

Ce document est mis à disposition selon les termes de la licence Creative Commons “Attribution – Pas d’utilisation commerciale – Partage dans les mêmes conditions 4.0 International”.



TABLE DES MATIÈRES

1.	Ce qui nous intéresse	2
2.	Des résultats basiques	2
3.	Un peu de codage pour y voir plus clair	3
4.	Structure de l’ensemble des solutions	3
5.	AFFAIRE À SUIVRE...	4

1. CE QUI NOUS INTÉRESSE

Nous allons étudier succinctement $\mathcal{S} = \{n \in \mathbb{N}^* \text{ tel que } n \mid 2^n + 1\}$ où $n \mid 2^n + 1$ signifie que n divise $2^n + 1$.

Dans la suite, nous utiliserons les notations suivantes.

- \mathbb{P} désigne l'ensemble des nombres premiers.
- $2\mathbb{N}$ désigne l'ensemble des nombres naturels pairs.
- $2\mathbb{N} + 1$ désigne l'ensemble des nombres naturels impairs.
- $\forall (n, m) \in \mathbb{N}^2$, $n \vee m$ désigne le PPCM de n et m .
- $\forall (n, m) \in \mathbb{N}^2$, $n \wedge m$ désigne le PGCD de n et m .

2. DES RÉSULTATS BASIQUES

Fait 2.1. $1 \in \mathcal{S}$.

Démonstration. C'est clair. □

Fait 2.2. $\forall k \in \mathbb{N}^*, 2^k \notin \mathcal{S}$.

Démonstration. C'est clair car $2^k \mid 2^{(2^k)}$. □

Fait 2.3. $\mathcal{S} \cap 2\mathbb{N} = \emptyset$.

Démonstration. TODO □

Fait 2.4. $\mathcal{S} \cap \mathbb{P} = \{3\}$.

Démonstration. $2^p \equiv -1 \pmod{p}$ implique $2^{2p} \equiv 1 \pmod{p}$ donc l'ordre σ de 2 divise à la fois $2p$ et $p-1$, ce qui n'est possible que si $\sigma = 2$, puis $\mathcal{S} \cap \mathbb{P} \subseteq \{3\}$.

Clairement, $3 \mid (2^3 + 1)$ donc $3 \in \mathcal{S}$, d'où finalement $\mathcal{S} \cap \mathbb{P} = \{3\}$. □

Fait 2.5. $\forall k \in \mathbb{N}^*, 3^k \in \mathcal{S}$.

Démonstration. Nous allons raisonner par récurrence. Cette démonstration montre que le fait 2.5 est immédiat à deviner.

Initialisation pour $k = 1$. Vu avant.

Étape de récurrence. On a les implications logiques suivantes.

$$\begin{aligned}
 & (3^k) \mid (2^{(3^k)} + 1) \\
 \implies & \exists m \in \mathbb{Z}. \left[2^{(3^k)} + 1 = m \cdot 3^k \right] \\
 \implies & \exists m \in \mathbb{Z}. \left[2^{(3^k)} = -1 + m \cdot 3^k \right] \\
 \implies & \exists m \in \mathbb{Z}. \left[(2^{(3^k)})^3 = (-1 + m \cdot 3^k)^3 \right] \\
 \implies & \exists m \in \mathbb{Z}. \left[2^{(3^{k+1})} = -1 + 3 \cdot m \cdot 3^k - 3 \cdot (m \cdot 3^k)^2 + (m \cdot 3^k)^3 \right] \\
 \implies & 2^{(3^{k+1})} \equiv -1 \pmod{3^{k+1}}
 \end{aligned}$$

) *Besoin de $k \neq 0$ ici.*

En résumé, $3^k \mid 2^{(3^k)} + 1$ implique $3^{k+1} \mid 2^{(3^{k+1})} + 1$.

Conclusion : par récurrence sur $k \in \mathbb{N}^*$, nous savons que $3^k \in \mathcal{S}$. □

3. UN PEU DE CODAGE POUR Y VOIR PLUS CLAIR

Il est assez aisé de faire des codes informatiques brutaux pour obtenir d'autres solutions que les puissances de 3. On obtient par exemple les naturels suivants.

$$\begin{array}{lllll}
 \bullet 3^2 \cdot 19 & \bullet 3^3 \cdot 19 & \bullet 3^4 \cdot 19 & \bullet 3^5 \cdot 19 & \bullet 3^6 \cdot 19 \\
 & \bullet 3^3 \cdot 87\,211 & \bullet 3^4 \cdot 163 & \bullet 3^5 \cdot 163 & \bullet 3^6 \cdot 163 \\
 & & \bullet 3^4 \cdot 87\,211 & \bullet 3^5 \cdot 1459 & \bullet 3^6 \cdot 1459 \\
 & & & \bullet 3^5 \cdot 87\,211 & \bullet 3^6 \cdot 87\,211
 \end{array}$$

On peut aussi chercher d'autres formes de naturels comme les suivantes.

$$\begin{array}{lll}
 \bullet 3^2 \cdot 19^2 & \bullet 3^3 \cdot 19^2 & \bullet 3^2 \cdot 19 \cdot 571 \cdot 9137 \\
 \bullet 3^2 \cdot 19 \cdot 571 & \bullet 3^3 \cdot 19 \cdot 571 &
 \end{array}$$

Voici ce que nous apprennent ces résultats.

- (1) XXX
- (2) XXX

4. STRUCTURE DE L'ENSEMBLE DES SOLUTIONS

Fait 4.1. $\forall n \in \mathcal{S}, \forall p \in \mathbb{P}, \text{ si } p \mid n \text{ alors } pn \in \mathcal{S}.$

Démonstration. Nous savons que $p > 2$. Ensuite, comme $2^n = -1 + kn$ où $k \in \mathbb{Z}$, nous avons :

$$\begin{aligned}
 2^{pn} &= (2^n)^p \\
 &= (-1 + kn)^p \\
 &= \sum_{i=0}^p \binom{p}{i} (-1)^{p-i} \cdot (kn)^i \\
 &= -1 + \sum_{i=1}^{p-1} p c_i \cdot (-1)^{p-i} \cdot (kn)^i + k^p \cdot n^p \\
 &= -1 + pn \sum_{i=1}^{p-1} c_i \cdot (-1)^{p-i} \cdot k^i n^{i-1} + pq \cdot n \cdot k^p \cdot n^{p-2}
 \end{aligned}$$

$\left. \begin{array}{l} p \mid \binom{p}{i} \text{ si } 0 < i < p \\ n = pq \end{array} \right\}$

On obtient finalement $2^{pn} = -1 + pn \cdot r$ avec $r \in \mathbb{Z}$ comme souhaité. □

Notons au passage que le fait 2.4 et le fait précédent donnent un exemple de preuve par récurrence où l'initialisation est essentielle car nous avons : $\forall p \in \mathbb{P}, p^k \mid 2^{(p^k)} + 1$ implique $p^{k+1} \mid 2^{(p^{k+1})} + 1$.

Fait 4.2. $\forall (n, m) \in \mathcal{S}^2, n \vee m \in \mathcal{S}.$

Démonstration. TODO □

Fait 4.3. $\forall (n, m) \in \mathcal{S}^2, n \wedge m \in \mathcal{S}.$

Démonstration. TODO □

Fait 4.4. Ordonné via la relation de divisibilité, l'ensemble \mathcal{S} est un treillis.

Démonstration. TODO □

Fait 4.5. $\forall (n, m) \in \mathcal{S}^2, nm \in \mathcal{S}.$

Démonstration. TODO

□

Fait 4.6. $\forall n \in \mathcal{S}, 2^n + 1 \in \mathcal{S}.$

Démonstration. TODO

□

5. AFFAIRE À SUIVRE...
