

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.	Notations utilisées	2
3.	Des résultats basiques	2
4.	Comportement des solutions	3
5.	Structure de l’ensemble des solutions	4
6.	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 $2^n + 1$.

2. NOTATIONS UTILISÉES

Dans la suite, nous utiliserons les notations suivantes.

- \mathbb{P} désigne l'ensemble des nombres premiers.
- $\forall (p; n) \in \mathbb{P} \times \mathbb{N}^*$, $v_p(n)$ est la valuation p -adique de n .
- $2\mathbb{N}$ 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 .

3. DES RÉSULTATS BASIQUES

Fait 3.1. $1 \in \mathcal{S}$.

Démonstration. C'est clair. □

Fait 3.2. $\mathcal{S} \cap 2\mathbb{N} = \emptyset$.

Démonstration. Notant $n = 2k$, nous avons $n \in \mathcal{S}$ si, et seulement si, $2^{2k} = 1 + 2kr$ où $r \in \mathbb{N}$; ceci permet de conclure. □

Fait 3.3. $\mathcal{S} \cap \mathbb{P} = \{3\}$.

Démonstration. Travaillons modulo p . Comme $2^p \equiv -1$ implique $2^{2p} \equiv 1$, l'ordre σ de 2 divise à la fois $2p$ et $p - 1$, et vérifie forcément $\sigma \neq 1$. Ceci n'est possible que si $\sigma = 2$, d'où $\mathcal{S} \cap \mathbb{P} \subseteq \{3\}$.

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

Fait 3.4. $\forall k \in \mathbb{N}^*$, $3^k \in \mathcal{S}$.

Démonstration. Nous allons raisonner par récurrence. Cette démonstration montre que le fait 3.4 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 $3^k \in \mathcal{S}$. □

4. COMPORTEMENT DES SOLUTIONS

La preuve du fait 3.4 amène naturellement au fait suivant.

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. $2^n = -1 + kn$, où $k \in \mathbb{Z}$, donne :

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

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

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

Notons au passage que ce qui précède et le fait 3.3 donnent un exemple non trivial pour insister sur la nécessité de l'initialisation dans une preuve par récurrence 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. Soit $r \in \mathbb{N}$ tel que $n \vee m = nr$. Rappelons que d'après le fait 3.2, aucun des entiers considérés ne peut être pair.

Posons $d = 2^n$. Comme $r \in 2\mathbb{N} + 1$, nous avons :

$$\begin{aligned}
 &2^{nr} + 1 \\
 &= 1 - (-d)^r \quad \left. \begin{array}{l} r \in 2\mathbb{N} + 1 \end{array} \right\} \\
 &= (1 + d) (1 + (-d) + \cdots + (-d)^{r-1})
 \end{aligned}$$

Comme $n \mid 2^n + 1$, c'est-à-dire $n \mid d + 1$, nous obtenons que $n \mid 2^{nr} + 1$, i.e. $n \mid 2^{n \vee m} + 1$. Par symétrie des rôles, nous avons aussi $m \mid 2^{n \vee m} + 1$. Finalement, $n \vee m \in \mathcal{S}$. \square

Notons que la preuve précédente donne une démonstration alternative du fait 4.1 mais pour tout diviseur p non trivial, premier ou non, de $n \in \mathcal{S}$. En effet, posons $d = 2^n$ et partons de nouveau de $2^{np} + 1 = (1 + d) (1 + (-d) + \cdots + (-d)^{p-1})$. Comme $p \mid n \mid 2^n + 1$, nous avons modulo p :

$$\begin{aligned}
 &1 + (-d) + \cdots + (-d)^{p-1} \\
 &\equiv 1 + 1 + \cdots + 1^{p-1} \quad \left. \begin{array}{l} d \equiv 2^n \equiv -1 \pmod{p} \end{array} \right\} \\
 &\equiv p \\
 &\equiv 0
 \end{aligned}$$

Finalement, $n \mid d + 1$ et $p \mid (1 + (-d) + \cdots + (-d)^{p-1})$ de sorte que $np \mid 2^{np} + 1$.

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

Démonstration. Nous avons $n = \prod_{p \mid n} p^{v_p(n)}$ et $m = \prod_{p \mid m} p^{v_p(m)}$ où les produits sont finis. Les faits suivants permettent de conclure.

- $n \vee m = \prod_{p|m} p^{\max(v_p(n); v_p(m))}$
- Si $\max(v_p(n); v_p(m)) < v_p(n) + v_p(m)$, alors le fait 4.1 donne que $p^\delta \cdot (n \vee m) \in \mathcal{S}$ où $\delta = v_p(n) + v_p(m) - \max(v_p(n); v_p(m))$.
- En répétant l'opération précédente autant de fois que nécessaire, on arrive à obtenir que $nm \in \mathcal{S}$.

□

Fait 4.4. $\forall (n, m) \in \mathcal{S}^2, n \wedge m \in \mathcal{S}$.

Démonstration. Cela découle directement des faits 4.2 et 4.3.

□

Fait 4.5. $\forall n \in \mathcal{S}, 2^n + 1 \in \mathcal{S}$.

Démonstration. Le principe est similaire à la preuve du fait 4.2. Notant $M = 2^n + 1 = nk$ et $d = 2^n$, nous avons :

$$2^M + 1 = 2^{nk} + 1$$

□

$$= (1 + d) (1 + (-d) + \dots + (-d)^{k-1})$$

$$= M (1 + (-d) + \dots + (-d)^{k-1})$$

5. STRUCTURE DE L'ENSEMBLE DES SOLUTIONS

Un ensemble \mathcal{T} est appelé treillis s'il vérifie les conditions suivantes.

- $(\mathcal{T}; \leq)$ est un ensemble ordonné.
- $\forall (a; b) \in \mathcal{T}^2$, l'ensemble $\{a; b\}$ possède une borne inférieure et une borne supérieure¹.

Fait 5.1. La relation de divisibilité ordonne l'ensemble \mathcal{S} via $n \leq m$ si, et seulement si, $n \mid m$. Muni de cet ordre, \mathcal{S} est un treillis.

Démonstration. Voir les faits 4.2 et 4.4.

□

Fait 5.2. $\forall n \in \mathcal{S}_{>1}, 3 \mid n$, autrement dit 3 est le minimum de $\mathcal{S}_{>1}$ dans le treillis $(\mathcal{S}; \mid)$.

Démonstration. Soit $p \in \mathbb{P}$ tel que $p \mid n$. Modulo p , nous avons $2^{2n} \equiv (-1)^2 \equiv 1$ et $2^{p-1} \equiv 1$ d'où $2^{(2n) \wedge (p-1)} \equiv 1$. Or, on sait que 2 est impair, donc $(2n) \wedge (p-1) = 2 \cdot (n \wedge \frac{p-1}{2})$. Dès lors, l'ordre σ de 2 divise $2 \cdot (n \wedge \frac{p-1}{2})$.

Considérons maintenant p minimal, pour l'ordre usuel, parmi les diviseurs premiers de n . Clairement, $n \wedge \frac{p-1}{2} = 1$ ², d'où $\sigma = 2$ puisque forcément $\sigma \neq 1$. Finalement, $p = 3$. □

6. AFFAIRE À SUIVRE...

1. Rappelons que ces bornes ne sont pas forcément dans $\{a; b\}$.
 2. Tout diviseur premier q de $n \wedge \frac{p-1}{2}$ vérifierait $q \leq \frac{p-1}{2} < p$.