BROUILLON - N DIVISE 2^N + 1

CHRISTOPHE BAL

Document, avec son source LATEX, disponible sur la page
https://github.com/bc-writing/drafts.

Table des matières

Date: 16 Jan. 2024 – 20 Jan. 2024.

1. Ce qui nous intéresse

Nous allons étudier succinctement $\mathcal{S} = \left\{n \in \mathbb{N}^* \text{ tel que } n \mid 2^n + 1\right\}$ 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.
- $a \mid\mid b$ signifie que $a \mid b$ et $a \neq b$ (division stricte).

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, $3 \mid \left(2^3 + 1\right)$ 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.

$$
\begin{aligned}
& (3^k) \mid 2^{(3^k)} + 1 \\
\Longrightarrow\ & \exists m \in \mathbb{Z} \,.\left[2^{(3^k)} + 1 = m \cdot 3^k\right] \\
\Longrightarrow\ & \exists m \in \mathbb{Z} \,.\left[2^{(3^k)} = -1 + m \cdot 3^k\right] \\
\Longrightarrow\ & \exists m \in \mathbb{Z} \,.\left[\left(2^{(3^k)}\right)^3 = \left(-1 + m \cdot 3^k\right)^3\right] \\
\Longrightarrow\ & \exists m \in \mathbb{Z} \,.\left[2^{(3^{k+1})} = -1 + 3 \cdot m \cdot 3^k - 3 \cdot \left(m \cdot 3^k\right)^2 + \left(m \cdot 3^k\right)^3\right] \quad \textit{Besoin de } k \neq 0 \textit{ ici.} \\
\Longrightarrow\ & 2^{(3^{k+1})} \equiv -1 \mod (3^{k+1})
\end{aligned}
$$

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

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

$$\begin{aligned}
2^{pn} &= \big(2^n\big)^p \\
&= \big(-1 + kn\big)^p \\
&= \sum_{i=0}^{p} \tbinom{p}{i} (-1)^{p-i} \cdot (kn)^i && p \mid \tbinom{p}{i} \ \textit{si } 0 < i < p \\
&= -1 + \sum_{i=1}^{p-1} pc_i \cdot (-1)^{p-i} \cdot (kn)^i + k^p \cdot n^p && n = pq \\
&= -1 + pn \sum_{i=1}^{p-1} c_i \cdot (-1)^{p-i} \cdot k^i n^{i-1} + pq \cdot n \cdot k^p \cdot n^{p-2}
\end{aligned}$$

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

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 :

$$\begin{aligned}
&2^{nr} + 1 && r \in 2\mathbb{N} + 1 \\
=\ &1 - (-d)^r \\
=\ &\big(1 + d\big) \big(1 + (-d) + \cdots + (-d)^{r-1}\big)
\end{aligned}$$

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, $n \vee m \in \mathcal{S}$. □

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 $2^{np} + 1 = \big(1 + d\big) \big(1 + (-d) + \cdots + (-d)^{p-1}\big)$. Comme $p \mid n \mid 2^n + 1$, nous avons modulo p :

$$\begin{aligned}
&1 + (-d) + \cdots + (-d)^{p-1} && d \equiv 2^n \equiv -1 \mod p \\
\equiv\ &1 + 1 + \cdots + 1^{p-1} \\
\equiv\ &p \\
\equiv\ &0
\end{aligned}$$

Finalement, $n \mid d + 1$ et $p \mid \big(1 + (-d) + \cdots + (-d)^{p-1}\big)$ 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 $n = \prod\limits_{p \mid n} p^{v_p(n)}$ et $m = \prod\limits_{p \mid m} p^{v_p(m)}$ où les produits sont finis. Les faits suivants permettent de conclure.

- $n \vee m = \prod\limits_{p|m} p^{\max(v_p(n);v_p(m))}$
- 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. TODO □

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 :

$$\begin{aligned} 2^M + 1 &= 2^{nk} + 1 \\ &= \big(1 + d\big)\left(1 + (-d) + \cdots + (-d)^{k-1}\right) \\ &= M\left(1 + (-d) + \cdots + (-d)^{k-1}\right) \end{aligned}$$

□

5. Structure de l'ensemble des solutions

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

- $\big(\mathcal{T}\,;\leq\big)$ est un ensemble ordonné.
- $\forall (a\,;b) \in \mathcal{T}^2$, l'ensemble $\{a\,;b\}$ possède une borne inférieure et une borne supérieure [1] .

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. □

Dans la suite, $\inf_d$ et $\sup_d$ désigneront des bornes inférieures et supérieures dans le treillis $\big(\mathcal{S}\,;|\,\big)$ où « d » est pour « division » .

Fait 5.2. $\forall n \in \mathcal{S}_{>1}$, $3 \mid n$, *autrement dit* $3 = \inf_d\big(\mathcal{S}_{>1}\big)$.

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 p est impair, donc $(2n) \wedge (p-1) = 2 \cdot \left(n \wedge \frac{p-1}{2}\right)$. Dès lors, l'ordre σ de 2 divise $2 \cdot \left(n \wedge \frac{p-1}{2}\right)$.

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, $p = 3$. □

Fait 5.3. $\forall n \in \mathcal{S}_{>3}$, $9 \mid n$, *autrement dit* $9 = \inf_d\big(\mathcal{S}_{>3}\big)$.

Démonstration. Si $n = 3^k$, il n'y a rien à faire. Supposons donc que $3^k \mid\mid n$. D'après le fait précédent, nous savons que $k \geq 1$. Notons $n = 3^k m$ où $m \wedge 3 = 1$, et considérons $p \in \mathbb{P}$ minimal, pour l'ordre usuel, parmi les diviseurs premiers de m .

Modulo $3^k p$, nous avons $2^{2n} \equiv 1$ et $2^{2\cdot 3^{k-1}\cdot(p-1)} \equiv 1$ via l'indicatrice d'Euler. Dès lors, comme $n = 3^k m$, l'ordre σ de 2 , avec forcément $\sigma \neq 1$, divise $(2\cdot 3^k m) \wedge (2 \cdot 3^{k-1} \cdot (p-1))$, c'est-à-dire $2 \cdot 3^{k-1} \cdot \big((3m) \wedge (p-1)\big)$. Comme dans la démonstration précédente, le caractère minimal de p implique que $m \wedge (p-1) = 1$ d'où $(3m) \wedge (p-1) = 3 \wedge (p-1) \in \{1\,;3\}$.

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 $q \leq \frac{p-1}{2} < p$.

- Si $3 \wedge (p-1) = 1$ alors, modulo p, nous avons $2^{2 \cdot 3^{k-1}} \equiv 1$. Ceci implique que $k > 1$ car $p \neq 3$. Notons au passage que $2^{(3^{k-1})} \equiv \pm 1$ et $3 \wedge (p-1) = 1$, et donc $3^{k-1} \nmid p-1$, impliquent que $2^{(3^{k-1})} \equiv -1$ modulo p.
- KO ou OK ?

  Si $3 \wedge (p-1) = 3$ alors $2^{2 \cdot 3^k} \equiv 1$ modulo $3^k p$ rend impossible d'avoir $k = 1$. En effet, dans le cas contraire, on a $63 \equiv 0$ modulo $3p$ avec $p \in \mathbb{P}_{>3}$, d'où forcément $p = 7$. XXXX Notons au passage que XXXX

$\square$

La preuve précédente nous donne le fait intéressant suivant.

Fait 5.4. $\forall n \in \mathcal{S}_{>3}$ *tel que* $3^k \mid\mid n$, *si* $p \in \mathbb{P}_{>3}$ *est un diviseur minimal, pour l'ordre usuel, de* n *parmi les diviseurs dans* $\mathbb{P}_{>3}$, *alors* $k > 1$ *et deux alternatives sont possibles.*

(1) Soit $3 \wedge (p-1) = 1$, *et dans ce cas* $p \mid 2^{(3^{k-1})} + 1$.

(2) Soit $3 \wedge (p-1) = 3$, *et dans ce cas* $p \mid 2^{(3^k)} + 1$. *KO ou OK ?*

---

6. AFFAIRE À SUIVRE...
