Sur les entiers n qui divisent $2^n + 1$

M.Gouy G.Huvent A. Ladureau

10 juin 2002

Dans le célébre livre de SIERPINSKI, "250 problèmes de théorie élémentaire des nombres", on trouve deux exercices portant sur les entiers n qui divisent $2^n + 1$ (exercices 1/21 et 4/88). Dans les Olympiades Internationales de Mathématiques de 1990 et 2000, on retrouve ces entiers dans les énoncés de deux sujets.
Quels sont donc ces entiers, pourquoi y porter autant d'intérêt ? La première difficulté que l'on rencontre dans leur étude est de trouver quelques solutions non triviales. Passée cette étape, l'analyse des solutions découvertes laisse perplexe. Quelles propriétés ont-ils donc ? Comment construire d'autres solutions ?
On se propose de donner quelques réponses à ces questions. Pour cela on utilisera l'arithmétique modulo n. On rappelle que $a = b\ (n)$ signifie que n divise $a - b$.

Partie I

Détermination des entiers inférieurs à 100 et solutions du problème . Premières conjectures

1 Avec une calculatrice ou avec Maple, l'approche naïve

Une rapide mais instructive étude du problème permet de dire que les solutions sont nécessairement des nombres impairs.

Comme il est hors de question de faire les calculs à la main, faisons-les faire par notre calculatrice favorite (ou notre ordinateur préféré).

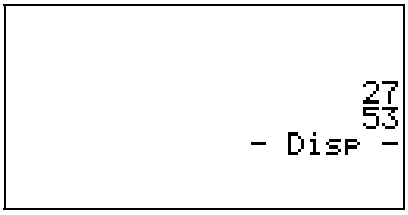
Algorithme
Effacement de l'écran
Pour N allant de 1 à 100 (avec un pas de 2)
Si N divise 2^N+1
Alors
Afficher N
Pause
Fin du Si
Fin du Pour

Programme sur TI-83	Programe sur Casio Graph 100
ClrHome	ClrText
For(N, 1, 100, 2)	For 1 → I to N Step 1
If Fpart((2^N+1)/N)= 0	If Frac((2^N+1)/N) = 0
Then	Then N ▲
Disp N	
Pause	
End	IfEnd
End	Next

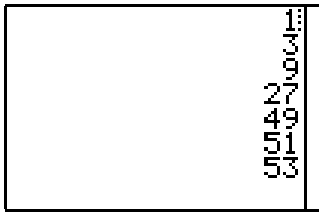
Programme (1) sur TI-92	Programme (2) sur TI-92
puissan2()	puissa21()
Prgm	Prgm
ClrIO	ClrIO
setMode(''Exact/Approx'',''APPROXIMATE'')	setMode(''Exact/Approx'',''EXACT'')
For i, 1, 100, 1	For i, 1, 100, 1
If mod(2^i+1, i) = 0 Then	If mod(2^i+1, i) = 0 Then
Disp i :Pause	Disp i :Pause
EndIf	EndIf
EndFor	EndFor
setMode(''Exact/Approx'',''AUTO'')	setMode(''Exact/Approx'',''AUTO'')
EndPrgm	EndPrgm

Qu'obtient-on ?

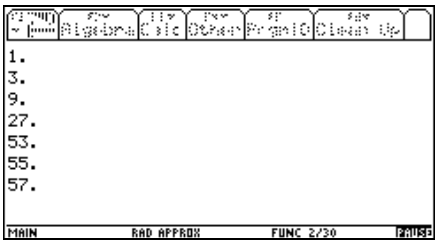
Sur CASIO



Sur TI-83



Sur TI-92 (programme 1)



Sur TI-92(programme 2)

Le moins que l'on puisse dire c'est que les réponses diffèrent suivant les machines et les programmes utilisés (voir TI-92).

1.1 L'exemple de 53, est-ce une solution ?

Vérifions si 53 est bien solution de notre problème : 53 étant un nombre premier, on a (d'après le théorème de FERMAT) :

$$\begin{aligned} & 2^{52} \equiv 1 \ (53) \\ \Longrightarrow \quad & 2^{53} \equiv 2 \ (53) \\ \Longrightarrow \quad & 2^{53}+1 \equiv 3 \ (53) \end{aligned}$$

d'où

53 n'est pas solution du problème posé.

2 Quelles conclusions peut-on déduire des résultats expérimentaux.

Affirmation 1 *Les premières solutions sont de la forme* 3^k *(*k *entier naturel)*

Affirmation 2 *Les calculatrices semblent, pour les trois premiers programmes, s'égarer à partir d'environ* $N = 50$.

2.1 Un premier résultat : 3^k est solution.

Etudions les entiers N de la forme $N = 3^k$. Montrons par récurrence que la propriété $\mathcal{P}(k) =$ "3^k divise $2^{3^k}+1$" est vraie.

- $\mathcal{P}(0)$ est vraie car $1 = 3^0$ divise $2^1 + 1 = 3$
- Soit k un entier naturel, supposons que $\mathcal{P}(k)$ est vraie, montrons alors que $\mathcal{P}(k+1)$ l'est également.
  On a

$$\begin{aligned} 2^{3^{k+1}}+1 &= \left(2^{3^k}\right)^3+1 \\ &= \left(2^{3^k}+1\right) \times \left(\left(2^{3^k}\right)^2 - 2^{3^k}+1\right) \end{aligned}$$

et d'autre part

$$2 \equiv -1 \ (3)$$

donc

$$\begin{aligned} 2^{3^k} \quad &\equiv \quad -1 \ (3) \Longrightarrow \left(2^{3^k}\right)^2 \equiv 1 \ (3) \\ &\Longrightarrow \quad \left(2^{3^k}\right)^2 - 2^{3^k}+1 \equiv 0 \ (3) \end{aligned}$$

D'où 3 divise $\left(2^{3^k}\right)^2 - 2^{3^k}+1$. Mais $\mathcal{P}(k)$ étant vraie, 3^k divise $2^{3^k}+1$. On en déduit que $2^{3^{k+1}}+1$ est divisible par 3^{k+1}d'où $\mathcal{P}(k+1)$ est vraie.

Proposition 3 *Les entiers de la forme* 3^k *pour* $k \in \mathbb{N}$ *sont solutions du problème posé.*

2.2 Quelle explication donner aux résultats aberrants donnés par la calculatrice ?

Prenons l'exemple de la TI 83. Le programme tel qu'il a été conçu teste le quotient de $2^N + 1$ par N. Examinons en détail le cas de $N = 49$.

Pour la TI-83, $\frac{(2^{49}+1)}{49} = 1.148877456 \times 10^{13}$ à l'affichage. En fait la machine affiche 10 chiffres mais travaille avec quatorze chiffres. Pour ce dernier calcul, elle a en mémoire $1.1488774559619 \times 10^{13}$. Ce dernier nombre est entier donc la machine considère que 49 est solution.

Exercice 4 *Testez le cas* $N = 47$ *sur la TI-83.*

Exercice 5 *Pourquoi la Casio 100 ne considère pas* 49 *comme solution.*

Exercice 6 *Comment expliquer que le second programme sur la TI-92 ne sorte pas les solutions parasites apparues avec les autres programmes.*

Partie II

Détermination des entiers supérieurs à 100 et solutions du problème. L'exponentiation rapide

Les programmes précédents sauf le dernier ayant montré leurs limites, il nous faut trouver une autre solution. La première solution consistait à naïvement faire la division de 2^N+1 par N. On s'est vite aperçu des problèmes posés. En fait, on a besoin uniquement de connaître le reste de cette division. Celui-ci ne dépassant pas N, on devrait bien avoir un moyen de le calculer sans dépasser les capacités de la machine. Testons une méthode sur un exemple.

1 Le calcul intelligent de 2^{13} modulo N

Imaginons que l'on veuille trouver le reste r de 2^{13} modulo N.
On écrit que

$$\begin{aligned}
2^{13} &= 2\times 2^{12} = 2\times\left(2^2\right)^6 \\
&= a_1\times(a_2)^6 \qquad \text{où } a_1=2,\ a_2=(a_1)^2=2^2 \\
(a_2)^6 &= \left((a_2)^2\right)^3 \\
&= (a_3)^3 \qquad \text{où } a_3=(a_2)^2=\left(2^2\right)^2 \\
(a_3)^3 &= a_3\times(a_3)^2 = a_3\times a_4
\end{aligned}$$

Ainsi

$$2^{13}=a_1\times a_3\times a_4$$

ce qui traduit l'égalité

$$2^{13}=2\times\left(2^2\right)^2\times\left(\left(2^2\right)^2\right)^2$$

Si l'on travaille modulo N, ceci montre qu'il suffit de calculer $\alpha_1=2$ modulo N, $\alpha_2=\alpha_1^2$ modulo N, $\alpha_3=\alpha_2^2$ modulo N et enfin $\alpha_4=\alpha_3^2$ modulo N. On a alors

$$\begin{aligned}
\alpha_1 &\equiv 2\ (N)\\
\alpha_2 &\equiv 2^2\ (N)\\
\alpha_3 &\equiv \left(2^2\right)^2\ (N)\\
\alpha_4 &\equiv \left(\left(2^2\right)^2\right)^2\ (N)
\end{aligned}$$

ce qui donne immédiatement

$$2^{13}\equiv\alpha_1\times\alpha_3\times\alpha_4\ (N)$$

En pratique, on calcule α_2,α_3 puis

$$\beta_1=\alpha_1\times\alpha_3 \text{ modulo } N$$

et enfin α_4 et

$$\beta_2=\beta_1\times\alpha_4 \text{ modulo } N$$

Ainsi modulo 13 par exemple, $\alpha_1=2$, $\alpha_2=4$, $\alpha_3=3$ car $16\equiv 3\ (13)$, $\beta_1=6$ et enfin $\alpha_4=9$ qui donne $2^{13}=54=2\ (13)$ car $6\times 9=54=2+4\times 13$ (résultat évident avec le petit théorème de Fermat)
Pour comprendre le mécanisme, il est intéressant de remarquer que

$$13=8+4+1=2^3+2^2+1$$

donc s'écrit en base deux

$$13=\overline{\mathbf{1101}}$$

Ainsi

$$\begin{aligned}\alpha^{13} &= \left(\alpha^{2^3}\right)^{\mathbf{1}} \times \left(\alpha^{2^2}\right)^{\mathbf{1}} \times \left(\alpha^2\right)^{\mathbf{0}} \times (\alpha)^{\mathbf{1}} \\ &= (\alpha_4)^{\mathbf{1}} \times (\alpha_3)^{\mathbf{1}} \times (\alpha_2)^{\mathbf{0}} \times (\alpha_1)^{\mathbf{1}} \\ &\quad \text{où} \\ \alpha_1 &= \alpha,\ \alpha_2 = (\alpha_1)^2,\ \alpha_3 = (\alpha_2)^2 \ldots\end{aligned}$$

Cette méthode porte le nom d'exponentiation rapide. On constate qu'en pratique il semble nécessaire de déterminer le développement en base 2 de la puissance à laquelle on élève α. Numériquement, il suffit de calculer les chiffres binaires un par un.

2 Calcul pratique des chiffres binaires d'un entier

Rappelons que si n est un entier, $\overline{b_k b_{k-1} \cdots b_2 b_1 b_0}$ est son développement en base deux si et seulement si

$$\begin{aligned}n &= b_0 + 2b_1 + 2^2 b_2 + \ldots + 2^k b_k \text{ et } b_k \neq 0 \\ \forall i,\ b_i &\in \{0,1\}\end{aligned}$$

Il est donc très simple d'obtenir b_0. Si n est pair, alors $b_0 = 0$, sinon $b_0 = 1$.

$$b_0 \text{ est le reste de la division euclidienne de } n \text{ par } 2$$

Comment obtenir alors b_1

$$\frac{n - b_0}{2} = b_1 + 2b_2 + \ldots + 2^{k-1} b_k = \overline{b_k b_{k-1} \cdots b_2 b_1}$$

Ainsi

$$b_1 \text{ est le reste de la division euclidienne de } n_1 = \frac{n - b_0}{2} \text{ par } 2$$

Avant de réitérer le processus, on remarque que

$$n_1 = \frac{n - b_0}{2} \text{ est le quotient de la division euclidienne de } n \text{ par } 2$$

puis

$$b_2 \text{ est le reste de la division euclidienne de } n_2 = \frac{n_1 - b_1}{2} \text{ par } 2$$

Le processus s'arrête lorsque le dernier quotient est nul (ce qui se produit car la suite n_k est strictement décroissante). Par exemple pour 13, on a

$$\begin{aligned}13 &= 2 \times 6 + \mathbf{1} \\ 6 &= 2 \times 3 + \mathbf{0} \\ 3 &= 2 \times 1 + \mathbf{1} \\ 1 &= 2 \times 0 + \mathbf{1}\end{aligned}$$

d'où

$$13 = \overline{\mathbf{1101}}$$

On récupère alors les chiffres dans l'ordre inverse. Ce qui donne l'algorithme suivant qui calcule un par un les chiffres du développement en base 2

Entrer l'entier N
    Tant que $N \neq 0$ faire
    Afficher le reste de la division de N par 2
    N est remplacé par le quotient de la division de N par 2
Fin du Tant que

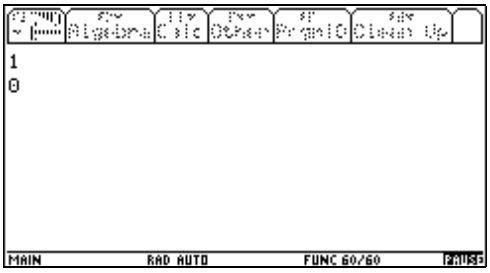
Ce qui donne les programmes suivants

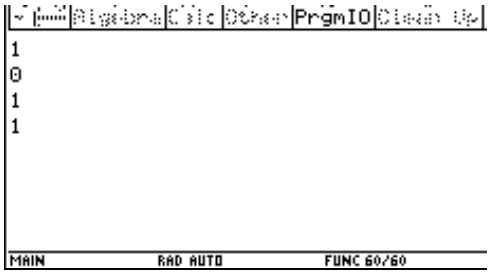
TI-83
ClrHome Prompt N While N≠0 Disp N-2*Int(N/2) Pause Int(N/2)→N End

Casio
ClrText ''N='' ?→N While N≠0 N-2*Int(N/2) ▲ Int(N/2)→N WhileEnd

TI-92
base2(n) prgm ClrIo While n≠0 Disp mod(n,2) :Pause int(n/2)→n EndWhile EndPrgm

Par exemple avec une TI 92, on obtient pour $n = 13$





Remarque 7 *On peut bien sûr faire la même chose dans une base quelconque.*

3 Programmation de l'exponentiation rapide

On va de manière plus générale calculer le reste de X^E modulo N, on notera Y ce reste. On peut maintenant donner deux algorithmes de calcul de l'exponentiation rapide. Le premier est récursif, le second exploite le développement en base 2 dont on calcule les chiffres un par un.

3.1 Algorithme récursif

Il est basé sur le fait que pour calculer $Y = X^E \ (N)$,

si $E = 1$, c'est évident.

si E est pair, on calcule $Z = X^{\left(\frac{E}{2}\right)}$ modulo N puis $Y = Z^2$ modulo n

si E est impair, on calcule $Z = X^{\left(\frac{E}{2}\right)}$ modulo N et alors $Y = X \times Z^2$ modulo N

On obtient alors l'algorithme suivant :

Si $E = 1$ alors
    Y est le reste de la division de X par N
Sinon
    Si E est pair alors
        Mettre $\frac{E}{2}$ dans E
        Calculer le reste Y de X^E par N
        Mettre le reste de Y^2 par N dans Y
    Sinon
        Mettre $\frac{E-1}{2}$ dans E
        Calculer le reste Y de X^E par N
        Mettre $X \times Y^2$ dans Y
        Mettre le reste de Y par N dans Y
    Fin du Si
Fin du Si

Programme EXPDR

Programmation sur Casio 100
If E=1 Then X-N*Int(X/N)→Y Else If Frac(E/2)=0 Then E/2→E Prog ''EXPDR'' Y^2-N*Int(Y^2/N)→Y Else (E-1)/2→E Prog ''EXPDR'' X*Y^2 → Y Y-N*Int(Y/N)→Y IfEnd

Sur TI-83
If E=1 Then X-N*Int(X/N)→Y Else If Fpart(E/2)=0 Then E/2→E PrgmEXPDR Y^2-N*Int(Y^2/N)→Y Else (E-1)/2→E PrgmEXPDR X*Y^2 → Y Y-N*Int(Y/N)→Y End

Ecriture de la fonction expdr sur TI-92

expdr(x,n,e)
Func
If e=1 then
mod(x,n)
Else
Ifmod(e,2)=0 Then
mod((expdr(x,n,e/2))^2,n)
Else
mod(x*(expdr(x,n,(e-1)/2))^2,n)
EndIf
EndIf
EndFunc

Ecriture du programme cherchant les solutions inférieures ou égales à un entier F donné (L'algorithme ne différant pas du précédent, on écrit directement les programmes)

Sur Casio Graph 100
ClrText ''F=''?→F For 1→N To F Step 2 2→X :N→E Prog ''EXPDR'' If Y+1=N Then N IfEnd Next

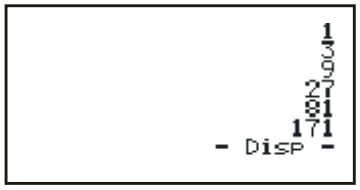
Sur TI-83
ClrHome Prompt F for(N,1,F,2) 2→X :N→E PrgmEXPDR If Y+1=N Then Disp N Pause End End

sur TI-92

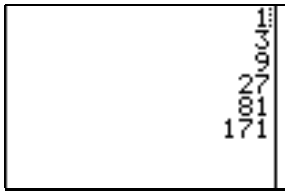
puissa22(f)
Prgm
ClrIO
setMode(''Exact/Approx'',''EXACT'')
For i,1,f,1
If expdr(2,i,i)+1=N Then
Disp i
EndIf
EndFor
EndPrgm

Ce qui donne par exemple pour $F = 200$, les écrans :

Sur Casio 100



Sur TI-83



Etant donné le nombre important de solutions et pour les étudier après, il peut être utile de les stocker dans une liste. Cela donne les versions suivantes :

Sur Casio Graph 100

```
ClrText
"F=" ?→F
{1}→List 1
For 3→N To F Step 2
2→X :N→E
Prog "EXPDR"
If Y+1=N
Then
Augment({N},List 1)→List 1
IfEnd
Next
List 1
```

Sur TI-83

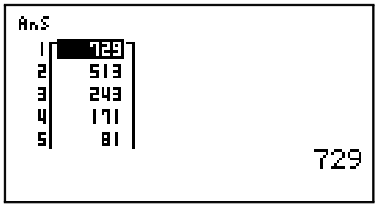
```
ClrHome
Prompt F
{1}→L1
For( N,1,F,2)
2→X :N→E
PrgmEXPDR
If Y+1=N
Then
Disp N :augment(L1,{N})→L1
End
End
Pause L1
```

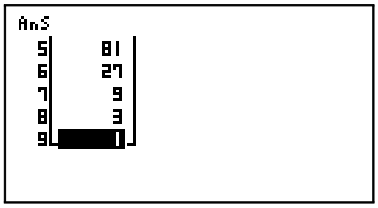
Sur TI-92

```
puissa23(f)
Prgm
{1}→l1
ClrIO
setMode("Exact/Approx","EXACT")
For i,1,f,1
If expdr(2,i,i)+1=N Then
Disp i
augment(l1,{N})→l1
EndIf
EndFor
Pause l1
setMode("Exact/Approx","AUTO")
EndPrgm
```

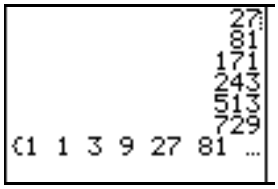
Ce qui donne par exemple pour écran :

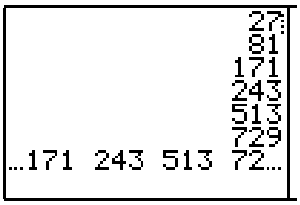
Sur Casio 100

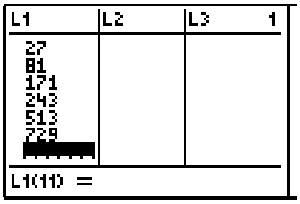




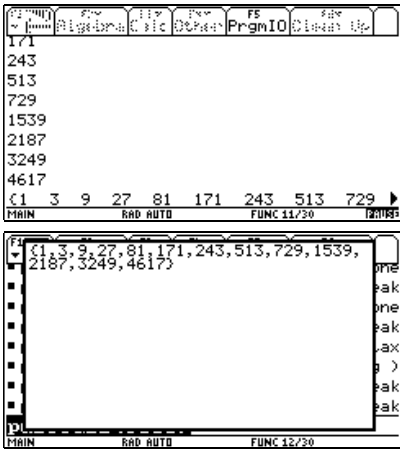
Sur TI-83







Sur TI-92



3.2 Algorithme non récursif

On peut utiliser le développement en base 2 de E dont on calcule les chiffres un par un. Cela donne l'algorithme suivant

Mettre 1 dans Y
Tant que $E \neq 0$ faire
    Si E est impair alors
        Mettre dans Y le reste de $Y \times X$ par N
    Fin du Si
    Mettre le reste de X^2 dans X
    Mettre le quotient de la division de E par 2 dans E
Fin du Tant que

On obtient alors les programmes suivants

TI-83

`1→Y`
`While E≠0`
`If Fpart(E/2)≠0`
`Then`
`Y*X-N*int(Y*X/N)→Y`
`End`
`X²-N*Int(X²/N)→X`
`Int(E/2)→E`
`End`

Casio

`1→Y`
`While E≠0`
`If Frac(E/2)≠0`
`Then Y*X-N*int(Y*X/N)→Y`
`IfEnd`
`X²-N*Int(X²/N)→X`
`Int(E/2)→E`
`WhileEnd`

TI-92

`expdr1(x,n,e)`
`func`
`while e≠0`
`If mod(e,2)≠0 Then`
`y*x-n*int(y*x/n)→y`
`EndIf`
`X²-n*Int(X²/n)→x`
`Int(e/2)→e`
`EndWhile`
`y`
`Endfunc`

Remarque 8 *En Maple, l'exponentiation rapide est donnée par la commande $X\&\hat{}E \bmod N$*

4 Résultats

On obtient les premières solutions au problème qui sont[1]

$$1, 3, 9, 27, 81, 171, 243, 513, 729, 1539, 2187, 3249, 4617, 6561, 9747, 13203, 13851, 19683,$$
$$29241, 39609, 41553, 59049, 61731, 87723, 97641, 118827, 124659, 177147, 185193,$$
$$250857, 263169, 292923, 354537, 356481, 373977, 531441, 555579, 752571$$

Lorsque l'on factorise ces solutions, on trouve

$$3, 3^2, 3^3, 3^4, ...$$
$$3^2 \times 19, 3^3 \times 19, 3^4 \times 19...$$
$$3^2 \times 19^2, 3^3 \times 19^2, ...$$
$$3^2 \times 19^3, ...$$
$$...$$
$$3^4 \times 163, 3^5 \times 163,$$
$$3^4 \times 19 \times 163, ...$$

On récupère donc les puissances de 3 et d'autres solutions. On remarque que toutes les solutions (sauf une) sont multiples de 3, et même (sauf deux) multiples de 9.

[1] Cette suite porte le numéro *A006521* dans l'encyclopédie des suites entières (http ://www.research.att.com/~njas/sequences/indexfr.html#L)

Partie III
Propriétés des solutions Généralisations

1 Premières propriétés de ces entiers

On rappelle l'identité fondamentale suivante,

$$a^n-(-1)^n=(a+1)\times\left(a^{n-1}-a^{n-2}+a^{n-3}-\cdots\right)$$

Cette identité permet alors d'établir que si a et b sont des entiers impairs, alors

$$\begin{aligned}2^{ab}+1 &= \left((2^a)^b-(-1)^b\right)\\ &= (2^a+1)\left((2^a)^{b-1}+\ldots+(-1)^{b-1}\right)\end{aligned}$$

En particulier

$$2^a+1=0\ (a)\Longrightarrow 2^{ab}+1=0\ (a)$$

1.1 Comment obtenir de nouvelles solutions

La première remarque, bien qu'évidente réside dans la proposition suivante.

Proposition 9 *Les solutions sont des nombres impairs*
Preuve. *Deux secondes de réflexion suffisent pour s'en convaincre.* ■

Ensuite, ayant une solution n (et on en dispose), les facteurs de 2^n+1 permettent d'en obtenir beaucoup d'autres.

Proposition 10 *Si n est solution et si m divise 2^n+1 alors mn est solution*
Preuve. *Puisque m et n sont solutions, on écrit que*

$$2^{mn}+1=(2^n+1)\left((2^n)^{m-1}-(2^n)^{m-2}+\cdots+1\right)$$

On sait que n divise 2^n+1, il suffit de prouver que m divise le facteur

$$\left((2^n)^{m-1}-(2^n)^{m-2}+\cdots+1\right)=\sum_{k=0}^{m-1}(-1)^k\,(2^n)^k$$

Mais par hypothèse m divise 2^n+1 donc $2^n=-1\ (m)$ et

$$\left((2^n)^{m-1}-(2^n)^{m-2}+\cdots+1\right)=\sum_{k=0}^{m-1}1=m=0\ (m)$$

ce qui termine la preuve. ■

Remarque 11 *On peut établir un résultat un peu plus fort. Sous les hypothèses de la proposition précédente, on note d le pgcd de m et n, alors $n=dn'$ et $m=dm'$. Il est clair que d,m',n' sont impairs. On factorise $2^{mn}+1$.*

$$\begin{aligned}2^{mn}+1 &= 2^{(nm')\times d}+1\\ &\quad \left(2^{nm'}+1\right)\left(\left(2^{nm'}\right)^{d-1}-\cdots+1\right)\\ &= (2^n+1)\left((2)^{m'-1}-\cdots+1\right)\left(\left(2^{nm'}\right)^{d-1}-\cdots+1\right)\end{aligned}$$

On pose alors

$$\begin{aligned}\alpha &= (2^n+1)\\ \beta &= \left((2)^{m'-1}-\cdots+1\right)\\ \gamma &= \left(\left(2^{nm'}\right)^{d-1}-\cdots+1\right)\end{aligned}$$

On sait que n *divise* 2^n+1 *ainsi*

$$\begin{aligned}2^n=-1\ (n) &\Longrightarrow 2^{nm'}=-1\ (n)\\ &\Longrightarrow 2^{nm'}=-1\ (d)\ \textit{car } d \textit{ divise } n\\ &\Longrightarrow \gamma=d\ (d)\\ &\Longrightarrow d \textit{ divise } \gamma\end{aligned}$$

De même m *divise* 2^n+1*, d'où*

$$\begin{aligned}2^n=-1\ (m) &\Longrightarrow \beta=m'\ (m)\\ &\Longrightarrow m \textit{ divise } \beta\end{aligned}$$

enfin on se souvient que n *divise* α*. En conclusion* $n\times m\times d$ *divise* $\alpha\times\beta\times\gamma$*, ce qui se traduit par*

$$2^{mn}+1 \textit{ est divisible par } \frac{n^2m^2}{\operatorname{pgcd}(m,n)}=m\times n\times\operatorname{pgcd}(m,n)$$

Corollaire 12 *Si* n *est solution alors*

$$\begin{aligned}\forall\alpha \in \mathbb{N},\ n^\alpha &\textit{ est solution}\\ 2^n+1 &\textit{ est solution}\end{aligned}$$

Preuve. *Pour* $\alpha=0$*,* $n^\alpha=1$ *est solution sinon on applique la proposition précédente.*
Pour la seconde affirmation, on peut aussi écrire que $2^n+1=n\times q$ *avec* q *impair alors* $2^{2^n+1}+1=((2^n)^q-(-1)^q)$ *est divisible par* 2^n+1*.* ■

Proposition 13 *Si* n *et* m *sont solutions du problème alors* $ppcm(n,m)$ *aussi.*

Preuve. *On utilise la remarque donnée dans le préliminaire. Puisque* $2^n+1=0\ (n)$*, avec* $a=n$*,* $b=\frac{ppcm(n,m)}{n}$*,on en déduit que*

$$2^{ppcm(n,m)}+1=0\ (n)$$

Puisque $2^m+1=0\ (m)$*, avec* $a=\frac{ppcm(n,m)}{m}$*,* $b=m$*,on en déduit que*

$$2^{ppcm(n,m)}+1=0\ (m)$$

En combinant les deux

$$2^{ppcm(n,m)}+1=0\ (ppcm(n,m))$$

■

Corollaire 14 *Si* m *et* n *sont solutions, alors* mn *aussi*

Preuve. *En effet* $mn=ppcm(m,n)\times pgcd(m,n)$*. Or* $pgcd(m,n)$ *divise* $ppcm(m,n)$ *donc aussi* $2^{ppcm(n,m)}+1$*.*
■

Exemple 15 *On sait que* 3 *est solution donc* $2^3+1=9$ *est solution. Mais* $2^9+1=513=9\times57=3^3\times19$*. Ainsi* 513 *est solution, mais aussi* $9\times19=171$*.*

1.2 De nouvelles solutions obtenues par division

Il semble que toutes les solutions soient divisibles par 3 et même par 9 (si l'on exclut 3). On va prouver ce résultat. Pour cela on aura besoin de la notion d'ordre d'un élément modulo n.

Rappel 16 *Soit $n \in \mathbb{N}$, $n \geq 2$ et a premier avec n, i.e. $pgcd(a,n) = 1$. L'ordre de a modulo n est le plus petit entier naturel non nul k tel que $a^k = 1\ (n)$.*
L'ordre est toujours inférieur ou égal à $n-1$ et si k' est tel que $a^{k'} = 1\ (n)$ alors k divise k'.
Pour plus d'informations, on pourra lire l'article "l'ordre dans le désordre" ([Gouy, Huvent, Ladureau])

Revenons à notre problème, si n divise $2^n + 1$, on a vu que nécessairement n est impair. Ainsi 2 est premier avec n et on peut définir l'ordre de 2 modulo n que l'on notera δ.
Puisque $2^n = -1\ (n)$, on a $2^{2n} = 1\ (n)$ et δ divise $2n$. Effectuons alors la division euclidienne de n par δ.

$$n = \delta q + r,\ 0 \leq r < \delta$$

alors

$$2^n = \left(2^\delta\right)^q \times 2^r = 2^r\ (n)$$

d'où

$$\begin{array}{rcl} 2^r & = & -1\ (n) \Longrightarrow 2^{2r} = 1\ (n) \\ & \Longrightarrow & \delta \text{ divise } 2r \end{array}$$

Mais on sait que $0 \leq 2r < 2\delta$ donc $2r = 0$ (impossible car sinon $r = 0$ et $2^r = 1$) ou

$$\delta = 2r \tag{1}$$

Et ainsi

$$n = r \times (2q+1) \tag{2}$$

On a donc prouvé que r divise n et que $2^r = -1\ (n)$, ce qui permet d'affirmer que

$$r \text{ divise } 2^r + 1,\ r \text{ est solution du problème}$$

On n'oubliera pas que

$$r \text{ est égal à la moitié de l'ordre de 2 modulo } n$$

On peut ainsi construire une suite strictement décroissante d'entiers naturels solutions (car $r < \frac{n}{2}$). Cette suite ne peut être infinie, on obtient alors nécessairement la valeur $r = 1$. Mais alors $\delta = 2$ et $2^2 = 4 = 1\ (n)$ qui n'est possible que si $n = 3$.
L'avant dernier reste est égal à 3.

$$\text{Toutes les solutions sont divisibles par 3}$$

De plus si $r = 3, \delta = 6,\ 2^6 = 64 = 1\ (n) \Longrightarrow 63 = 9 \times 7 = 0\ (n)$. Donc n divise 63. Mais n est un multiple de r est $n > 3$. La seule solution est $n = 9$.

$$\text{Toutes les solutions, sauf 1 et 3, sont divisibles par 9} \tag{3}$$

2 Une famille de solutions plus étranges

2.1 Le calcul de $2^{\frac{p-1}{2}}$ modulo p

Théorème 17 *Si p est un nombre premier impair alors*

$$2^{\frac{p-1}{2}} = (-1)^{\frac{p^2-8}{2}}$$

En d'autres termes

$$2^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } p = 1 \text{ ou } 7 \text{ modulo } 8 \\ -1 \text{ si } p = 3 \text{ ou } 5 \text{ modulo } 8 \end{cases}$$

Preuve. *Si $p=1$ ou 5 modulo 8, alors $p-1$ est divisible par 4 et $\frac{p-1}{2}$ est un multiple de 2*

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2\times 4\times 6\times\cdots\times(p-1)\\ &= 2\times 4\times 6\times\cdots\times\frac{p-1}{2}\times\left(-\frac{p-3}{2}\right)\times\cdots\times(-5)\times(-3)\times(-1)\ (p)\end{aligned}$$

car

$$\begin{aligned}\frac{p-1}{2}+2 &= \frac{p+3}{2}=p-\frac{p-3}{2}=-\frac{p-3}{2}\ (p)\\ \frac{p-1}{2}+4 &= \frac{p+5}{2}=p-\frac{p-5}{2}=-\frac{p-5}{2}\ (p)\\ &\vdots\\ p-1 &= -1\ (p)\end{aligned}$$

d'où

$$\begin{aligned}2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= (-1)^{\frac{p-1}{4}}\left(\frac{p-1}{2}\right)!\ (p)\\ 2^{\frac{p-1}{2}} &= (-1)^{\frac{p-1}{4}}\ (p)\end{aligned}$$

De la même façon, si $p=3$ ou 7 modulo 8

$$\begin{aligned}2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2\times 4\times 6\times\cdots\times\frac{p-3}{2}\times\left(-\frac{p-1}{2}\right)\times\cdots\times(-5)\times(-3)\times(-1)\ (p)\\ &= (-1)^{\frac{p+1}{4}}\left(\frac{p-1}{2}\right)!\ (p)\end{aligned}$$

d'où

$$2^{\frac{p-1}{2}}=(-1)^{\frac{p+1}{4}}\ (p)$$

Il reste à vérifier que dans tous les cas cela revient bien à

$$2^{\frac{p-1}{2}}=(-1)^{\frac{p^2-8}{2}}$$

■

On obtient alors le résultat suivant

Lemme 18 *Si p est un nombre premier impair qui vérifie $p=\pm 3\ (8)$ alors, si $p=2n+1$*

$$2^{\frac{p-1}{2}}=-1\ (p)$$

Preuve. *Car $p=\pm 3\ (8)$ si et seulement si $p=3$ ou 5 modulo 8.* ■

2.2 Les solutions annoncées

Théorème 19 *Si n est solution du problème et si $\alpha\in\mathbb{N}^*$ est tel que*

$$p=2n^\alpha+1 \text{ est premier et congru à } \pm 3 \text{ modulo } 8$$

alors

$$m=p\times n^\alpha \text{ est solution du problème}$$

Preuve. *En effet n^α et $p=2n^\alpha+1$ sont premiers entre eux. Il suffit donc de vérifier que*

$$\begin{aligned}2^m &= -1\ (n^\alpha)\\ 2^m &= -1\ (p)\end{aligned}$$

Pour la première congruence, on a

$$2^m = \left(2^{n^\alpha}\right)^p$$

et on sait que n^α *est encore solution du problème donc*

$$2^{n^\alpha} = -1 \ (n^\alpha)$$

puisque p *est impair*

$$\left(2^{n^\alpha}\right)^p = 2^m = -1 \ (n^\alpha)$$

Pour la seconde congruence, il suffit d'appliquer le lemme 18 pour obtenir

$$2^{\frac{p-1}{2}} = -1 \ (p)$$

puis, p *étant impair*

$$2^{\frac{p(p-1)}{2}} = 2^m = -1 \ (p)$$

■

Proposition 20 *Considérons la suite (infinie ?) des entiers premiers* p_i *de la forme* $2 \times 9^{\alpha_i} + 1$. *Les premiers termes sont*

$$\begin{aligned}
p_0 &= 3 = 2 \times 9^0 + 1, \ \alpha_0 = 0 \\
p_1 &= 19 = 2 \times 9 + 1, \ \alpha_1 = 1 \\
p_2 &= 163 = 2 \times 9^2 + 1, \ \alpha_2 = 2 \\
p_3 &= 1459 = 2 \times 9^3 + 1, \ \alpha_3 = 3 \\
p_4 &= 86093443 = 2 \times 9^8 + 1, \ \alpha_4 = 8 \\
p_5 &= 411782264189299 = 2 \times 9^{15} + 1, \ \alpha_5 = 15 \\
p_6 &= 1162994740060801193807803 39 = 2 \times 9^{27} + 1 \\
p_7 &= 847823165504324070285888664 03 = 2 \times 9^{30} + 1 \\
p_8 &= 2 \times 9^{66} + 1 \\
&\vdots
\end{aligned}$$

Alors

$$n_i = 9^{\alpha_i} \times p_i \text{ est solution}$$

Preuve. 3 *est solution, on applique le résultat précédent en remarquant que pour* $j \geq 1$

$$\begin{aligned}
2 \times 3^{2j} + 1 &= 3 \ (8) \\
2 \times 3^{2j+1} + 1 &= 7 \ (8)
\end{aligned}$$

ce qui impose de ne retenir que les indices pairs. ■

3 Sujets connexes[2]

On peut se poser plusieurs questions relatives à ce problème. Dans cette partie, on propose quelques compléments et généralisations.

[2] Par arcs, il existe donc un chemin qui vous y menera.

3.1 Compléments sur l'équation diophantienne $(2^n+1)=nq$

3.1.1 L'ordre de 2 modulo 3^k

Le premier résultat simple est que cet ordre est de la forme 2×3^i où $i\leq k$ (cf (1) et (2)). On se propose de déterminer exactement cet ordre.

Proposition 21 *L'ordre de 2 modulo 3^k est exactement $2\times 3^{k-1}$, ceci pour $k\in\mathbb{N}^*$*

Preuve. *La preuve se fait par récurrence sur k. C'est clair si $k=1$. Supposons que $2^{2\times 3^{k-1}}=1\ \left(3^k\right)$. Notons δ l'ordre de 2 modulo 3^{k+1}, puisque $2^\delta=1\ \left(3^{k+1}\right)$, on a $2^\delta=1\ \left(3^k\right)$ et ainsi $2\times 3^{k-1}$ divise δ. On sait déjà que δ est de la forme 2×3^i.*
En conclusion, $\delta=2\times 3^{k-1}$ ou $\delta=2\times 3^k$. On utilise alors le lemme suivant :

Lemme 22 $\forall n\in\mathbb{N}^*$

$$2^{2\times 3^{n-1}}=1+3^n\ \left(3^{n+1}\right)$$

Preuve du lemme. *Par récurrence sur n, c'est clair pour $n=1$. Puis il existe $m\in\mathbb{N}$ tel que*

$$\begin{aligned}2^{2\times 3^n} &= \left(2^{2\times 3^{n-1}}\right)^3=\left(1+3^n+m3^{n+1}\right)^3\\ &= 1+3^{n+1}+3^{n+2}M\end{aligned}$$

ce qui prouve le résultat ■

En définitive, $2^{2\times 3^{k-1}}=1+3^k\neq 1\ \left(3^{n+1}\right)$, il ne reste qu'une solution $\delta=2\times 3^k$. ■

On peut déduire de ce résultat le corollaire suivant

Corollaire 23 *Si $2^n+1=0\ \left(3^k\right)$ alors 3^{k-1} divise n.*
Preuve. $2^n+1=0\ \left(3^k\right)\Longrightarrow 2^{2n}=1\ \left(3^k\right)\Longrightarrow 2\times 3^{k-1}$ *divise* $2n\Longrightarrow 3^{k-1}$ *divise* n. ■

3.2 Le troisième problème des Olympiades de Mathématiques de 1990

Problème 1 *Trouver tous les entiers naturels $n>1$ tels que*

$$\frac{2^n+1}{n^2}\in\mathbb{N}$$

On trouvera dans [OIM] une solution à ce problème. On se propose d'en donner une autre.

Soit n une solution, n divise 2^n+1 donc n est divisible par 3. Soit k l'exposant de 3 dans la décomposition en facteurs premiers de n. Alors 3^k divise n mais pas 3^{k+1}. Puisque 3^{2k} divise n^2 et que n^2 divise 2^n+1, on en déduit que $2^n+1=0\ \left(3^{2k}\right)$. D"après la proposition 21, l'ordre de 2 modulo 3^{2k} divise n,d'où $2\times 3^{2k-1}$ divise n. Nécessairement $2k-1\leq k$ et donc $k=1$.

L'exposant de 3 dans n est égal à 1

Mais si n^2 divise 2^n+1, alors n divise 2^n+1 et d'après (3) toutes les solutions, exceptées 1 et 3 sont divisibles par 9.

Proposition 24 *Le seul entier $n>1$ tel que $\dfrac{2^n+1}{n^2}\in\mathbb{N}$ est $n=3$.*

3.3 Le cinquième problème des olympiades de 2000

Problème 2 *Existe-t-il un entier strictement positif n tel que :*

1. *n soit divisible par exactement 2000 nombres premiers distincts*
2. *n divise 2^n+1*

Pour résoudre ce problème, il suffit de construire une suite $(n_k)_{k\in\mathbb{N}}$ de solutions telle que $n_{k+1}=p_k\times n_k$ où p_k est un facteur premier de $2^{n_k}+1$ sans en être un de n_k (ainsi n_{k+1}divise bien $2^{n_{k+1}}+1$). L'entier n_{1999} est alors solution du problème des Olympiades.
Compte tenu du fait que $2^9+1=513=19\times 27$, on va poser $n_0=9,\ n_1=19\times 9$. Il s'agit ensuite de prouver que

Proposition 25 *Si p premier (impair) divise 2^n+1 et ne divise pas n, alors il existe un facteur premier p' de $2^{np}+1$ différent de p.*

Preuve. *On part de l'égalité*

$$2^{np}+1=(2^n+1)\underbrace{\left((2^n)^{p-1}-(2^n)^{p-2}+(2^n)^{p-3}+\cdots+1\right)}_{A}$$

Soit α l'exposant de p dans la décomposition en facteurs premiers de 2^n+1 alors $2^n=-1+p^\alpha q$. On en déduit que

$$A=(-1+p^\alpha q)^{p-1}-(-1+p^\alpha q)^{p-2}+\cdots+1$$

ce qui donne, en développant par le binôme

$$\begin{array}{rccccccc}
A= & + & (-1)^{p-1} & + & C^1_{p-1}(-1)^{p-2}p^\alpha q & + & C^2_{p-1}(-1)^{p-3}p^{2\alpha}q^2 & + \cdots \\
 & - & (-1)^{p-2} & - & C^1_{p-2}(-1)^{p-3}p^\alpha q & + & \cdots & + \cdots \\
 & + & (-1)^{p-2} & + & C^1_{p-3}(-1)^{p-4}p^\alpha q & + & \cdots & + \cdots \\
 & \vdots & & \vdots & & \vdots & & \\
 & + & 1 & - & C^1_2 p^\alpha q & + & C^2_2 p^{2\alpha}q^2 & \\
 & - & 1 & + & C^1_1 p^\alpha q. & & & \\
 & + & 1 & & & & &
\end{array}$$

Si l'on se souvient que p est impair, on a en sommant par colonnes

$$\begin{aligned}
A &= \underbrace{p}_{\text{colonne 1}} \underbrace{-\left((p-1)+(p-2)+(p-3)+\cdots+1\right)p^\alpha q}_{\text{colonne 2}} + \underbrace{p^{2\alpha}(\cdots)}_{\text{autres colonnes}} \\
&= p-\frac{p-1}{2}p^{\alpha+1}q+p^{2\alpha}(\cdots) \\
&= p+p^2(\cdots)
\end{aligned}$$

On constate donc que A est divisible par p mais pas par p^2. Puisque $A>p$, A contient un autre facteur premier p'. ■

3.4 Remplaçons 2 par un autre entier

On peut généraliser le problème posé.

Problème 3 *Soit $a\in\mathbb{N}$, $a\geq 2$, que dire des entiers n tels que*

$$\frac{a^n+1}{n}\in\mathbb{N}$$

A priori certaines des méthodes employées ici doivent se généraliser sans peine.

Remarque 26 *Rem pour des informations sur les équations $2^n-c=0$ (n) voir aussi http ://www.spacefire.com/numbertheory/2nmodn.htm*

Références

[OIM] *Olympiades Internationales de Mathématiques*, J.P. Boudine, F. Lo Jacomo, R. Cuculiere. Editions du Choix.

[Sierpinski] *250 problèmes de théorie élémentaire des nombres*, W.Sierpinski, Editions Jacques Gabay.

[Gouy, Huvent, Ladureau] *De l'ordre dans le désordre,* M.Gouy, G.Huvent, A.Ladureau, Document Irem, `http://perso.wanadoo.fr/gery.huvent`