Par Babacar Gueye.....Bargny le 30/07/2021

PREUVE DE LA CONJECTURE D'ERDOS SUR LE PROBLEME DE BROCARD

I) INTRODUCTION

Le problème de Brocard est un problème en mathématiques qui demande de trouver des valeurs entières de n et m de l'équation diophantienne
$n! + 1 = m^2$,
où $n!$ est la fonction factorielle.
Celui-ci a été posé par Henri Brocard dans deux articles en 1876 et 1885 et indépendamment en 1913 par Srinivasa Ramanujan.
NOMBRES DE BROWN :
Les couples d'entiers (n, m) étant solution du problème de Brocard sont dits nombres de Brown. Il n'y a que trois couples connus de nombres de Brown : $(4, 5)$, $(5, 11)$ et $(7, 71)$.
Paul Erdos a conjecturé que ceux-là, sont les seules solutions.
Berndt et Galway en 2000, ont effectué des calculs pour n inférieur à 10^9 et n'ont trouvé aucune solution supplémentaire.

En faisant une étude sur des valeurs de n assez grands, on va montrer ici qu'il n'existe pas d'autre solution à cette équation diophantienne.

II) PREUVE

Lemme 1 :
Pour $n \geq 2$, $n! + 1 = m^2 \iff \exists\, M$entier pair$/\dfrac{n!}{4} = (M \pm 1)M$.

Preuve :
Si n et m sont deux entiers naturels tels que $n! + 1 = m^2 \quad (1)$,
alors $n! = m^2 - 1 = (m-1)(m+1)$.
Pour $n \geq 2$ on a $n!+1$ impair et donc m impair. Alors $m-1$ et $m+1$ sont deux nombres pairs consécutifs, et donc $v_2(m-1) = 1$ et $v_2(m+1) = v_2(n!) - 1$,
ou $v_2(m+1) = 1$ et $v_2(m-1) = v_2(n!) - 1$
où $v_2(x)$ est la valuation 2-adique de x.
Alors on a (1) si et seulement si $n! = 2^{v_2(n!)-1}s\big(2^{v_2(n!)-1}s \pm 2\big) = 4\big(2^{v_2(n!)-2}s\big(2^{v_2(n!)-2}s \pm 1\big)\big)$
où s est un entier naturel impair.
C'est dire que (1) si et seulement si $\dfrac{n!}{4} = (M \pm 1)M \quad (2)$
où on a posé $M = 2^{v_2(n!)-2}s$. D'où le lemme.

Remarque 1 :
Rappelons le principe suivant : si deux nombres entiers A et B sont tels que

$Au - vB = 1, u, v \in \mathbb{N}^*$, toutes les solutions U et V de l'équation diophantienne $AU - VB = 1$ sont de la forme $U = u + Bb$ et $V = v + Ab$, avec b entier.

Résoudre l'équation diophantienne (1) pour n assez grand, revient à résoudre l'équation diophantienne : $\dfrac{n!}{4} = (M \pm 1)M$.
On va ci-dessous montrer que $\dfrac{n!}{4}$ ne peut pas s'écrire sous cette forme avec M nombre entier, pour n assez grand.
Notons que M et $M \pm 1$ sont deux nombres premiers entre eux.

Lemme 2 :
L'équation diophantienne $\dfrac{n!}{4} = (M \pm 1)M$ n'a pas de solution pour $n \geq 10$.

Preuve :
On va considérer n assez grand (par exemple ≥ 10) de telle sorte que $M \pm 1$ a au moins deux facteurs premiers.
Il s'agit donc de montrer que $\dfrac{n!}{4}$ ne peut s'écrire, ni sous la forme $(M+1)M$, ni sous la forme $(M-1)M$, avec M nombre entier, pour n assez grand.

•) Montrons par l'absurde qu'on ne peut avoir $\dfrac{n!}{4} = (M+1)M$, pour $n \geq 10$.
Nous savons que 2 est un facteur de M et il est aisé de voir que pour $n \geq 10$, $M+1$ doit avoir au moins deux facteurs premiers. Soit $p = 2a+1$ un nombre premier facteur de $M+1$.
Si M existe on a alors :
$(M+1)M = Pp \times 2Q = P(2a+1) \times 2Q = \dfrac{n!}{4}, P, Q \in \mathbb{N}^*$ (3)
(Q est pair pour n assez grand).
On a $P = 2q+1$ (q nombre entier) est un facteur de $M+1$ (et 2 est un facteur de M).
Soit $P - 2q = 1$, et alors d'après le principe rappelé à la remarque 1 ; il existerait un nombre entier d tel que :
$(M+1)M = P(1+2d) \times 2(q+Pd) = \dfrac{n!}{4}$. Et d'après (3), $d = a$ ($Q = q+Pd$).
On aurait alors $(M+1)M = P(1+2a) \times 2(q+Pa) = \dfrac{n!}{4}$ (3′).
On a alors :
$P(1+2a) \times 2(q+Pa) = \dfrac{n!}{4}$
$\iff P(1+2a)2q + P(1+2a)2Pa = \dfrac{n!}{4}$
$\iff P(1+2a)2q = \dfrac{n!}{4} - 2P^2(1+2a)a$
$\iff P(1+2a)2q = 2P(1+2a)a\big(2^{v_2(n!)-v_2(a)-3}r - P\big)$
$\iff q = a\big(2^{v_2(n!)-v_2(a)-3}r - P\big)$

où r est un nombre entier (pair pour n assez grand).
Alors a divise q et d'après $(3')$, a est un facteur de M.
Par ailleurs si $p^2 = 4a^2+4a+1 = 2(2a(a+1))+1$ est une facteur de $M+1$, alors il existerait $P' = 2q'+1$, (P' et q' des nombres entiers) facteur de $M+1$, tel que : $P'p^2 \times 2Q' = \dfrac{n!}{4}, Q' \in \mathbb{N}^*$ (en fait alors $P' = \dfrac{P}{p}$ et $Q' = Q$).
Le mème raisonnement que ci-dessus implique alors que $2a(a+1)$ est un facteur de M.
Ce qui entraine que $a+1$ est un facteur de M.
$2a+1$ est un facteur de $M+1$ et $2(a+1)-(2a+1) = 1$, donc d'après le mème principe, il existerait un entier c tel que :
$\big(2+(2a+1)c\big)(a+1) \times (2a+1)\big(1+(a+1)c\big) = \dfrac{n!}{4}$.
Pour n assez grand (tel que $v_2\big(\dfrac{n!}{4}\big) > v_2(a+1)$; ce qui est vérifié pour $n \geq 10$), alors c est pair, c'est-a-dire que $c = 2c'$, c' nombre entier. C'est dire qu'on a :
$\big(2+(2a+1)2c'\big)(a+1) \times (2a+1)\big(1+(a+1)2c'\big) = \dfrac{n!}{4}$.
C'est-à-dire que : $(2a+1)\big(1+2(a+1)c'\big) \times 2\big(1+(2a+1)c'\big)(a+1) = \dfrac{n!}{4}$ (4).
(4) et $(3')$ impliquent :
$\begin{cases} 1+2(a+1)c' = P \\ \big(1+(2a+1)c'\big)(a+1) = q+Pa \end{cases}$
La première égalité donne $c' = \dfrac{P-1}{2(a+1)} = \dfrac{q}{a+1}$, et cette valeur de c' dans la deuxième égalité implique :
$a+1+(2a+1)q = q+Pa = q+(2q+1)a \iff a+1+2aq+q = q+2aq+a \iff 1 = 0$, ce qui est absurde.
C'est dire que $M+1$ ne peut pas avoir un carré comme facteur.
Mais donc pour n assez grand (≥ 10), $M+1$ ne peut avoir comme facteurs que des nombres premiers strictement supérieurs à $\dfrac{n}{2}$.
Montrons enfin qu'avec cette contrainte sur $M+1$, pour n assez grand (≥ 10), il n'existe alors pas de valeur de M telle que $\dfrac{n!}{4} = (M+1)M$.
On sait qu'il y a plus de nombres premiers (au pire autant) sur l'intervalle $\big[2, \frac{n}{2}\big]$ que sur l'intervalle $\big]\frac{n}{2}, n\big]$.
On va montrer que pour chaque nombre premier x du premier intervalle (donc facteur de M), $x^{v_x\left(\frac{n!}{4}\right)} > n$ (donc supérieur strictement à tout éventuel facteur de $M+1$).
- Pour $x = 2$, il suffira que $n \geq 8$ pour que $v_2\big(\dfrac{n!}{4}\big) > \dfrac{n}{2}$, et on a bien $2^{\frac{n}{2}} > n$ dans ce domaine.
- Pour x dans l'intervalle $\big]\dfrac{n}{3}, \frac{n}{2}\big]$ on a $v_x\big(\dfrac{n!}{4}\big) = 2$, et là, on a bien $x^2 > n$.

- Enfin sur l'intervalle $\left]2, \frac{n}{3}\right]$, on a $v_x\left(\frac{n!}{4}\right) > \frac{n}{x} - 1$.
On veut montrer que $x^{\frac{n-x}{x}} - n > 0$ sur cet intervalle.
Pour cela, pour n donné, soit la fonction $f(x) = x^{\frac{n-x}{x}} - n$. Il faut alors montrer qu'elle est positive sur $\left]2, \frac{n}{3}\right]$.
Pour cela, on peut montrer que la fonction $g(x) = \frac{n-x}{x} ln(x) - ln(n)$ est positive sur $\left]2, \frac{n}{3}\right]$
(où ln est la fonction logarithme népérien).
On a $g'(x) = \left(\frac{n-x}{x}\right)' ln(x) + \frac{1}{x}\left(\frac{n-x}{x}\right) = \frac{n - nln(x) - x}{x^2} < 0$ sur $\left]2, +\infty\right[$.
Donc la fonction g est décroissante sur ce dernier intervalle, donc décroissante sur $\left]2, \frac{n}{3}\right]$.
On a $g\left(\frac{n}{3}\right) = \frac{n - \frac{n}{3}}{\frac{n}{3}} ln\left(\frac{n}{3}\right) - ln(n) = 2ln\left(\frac{n}{3}\right) - ln(n) = ln(n) - 2ln(3)$.
Mais alors $g\left(\frac{n}{3}\right) > 0 \iff n > 3^2 = 9$. D'où le résultat voulu pour $n > 9$.
On a donc montré que pour n assez grand (≥ 10), on aurait, $M = \prod_{i=1}^{t} a_i$, et $M + 1 = \prod_{i=1}^{t'} a'_i$, avec $t \geq t'$ et $a_i > a'_i, \forall i \in [\![1, t']\!]$. Mais alors on aurait $M > M + 1$. Ce qui est évidemment absurde.
C'est dire que l'équation $\frac{n!}{4} = (M+1)M$, n'a pas de solution pour $n \geq 10$.

•) Montrons par l'absurde qu'on ne peut avoir $\frac{n!}{4} = (M-1)M$, pour $n \geq 10$.
Nous savons que 2 est un facteur de M et on sait que pour $n \geq 10$, $M - 1$ doit avoir au moins deux facteurs premiers.
Soit $p = 2a - 1$ un nombre premier facteur de $M - 1$.
Si M existe on a alors :
$(M-1)M = Pp \times 2Q = P(2a-1) \times 2Q = \frac{n!}{4}, P, Q \in \mathbb{N}^*$ (5)
(Q est pair pour n assez grand).
On a $P = 2q - 1$ (q nombre entier supérieur à 1) est un facteur de $M - 1$ (et 2 est un facteur de M).
Soit $2q - P = 1$, et alors d'après le principe rappelé à la remarque 1 ; il existerait un nombre entier d tel que :
$(M-1)M = P(1+2d) \times 2(q+Pd) = \frac{n!}{4}$. Et d'après (5), $d = a - 1$ ($Q = q + Pd$).
On aurait alors $(M-1)M = P\big(1 + 2(a-1)\big) \times 2\big(q + P(a-1)\big) = \frac{n!}{4}$ (5').
On a alors :
$P\big(1 + 2(a-1)\big) \times 2\big(q + P(a-1)\big) = \frac{n!}{4}$
$\iff P\big(1 + 2(a-1)\big)2q + P\big(1 + 2(a-1)\big)2P(a-1) = \frac{n!}{4}$

$\iff P\big(1+2(a-1)\big)2q = \dfrac{n!}{4} - 2P^2\big(1+2(a-1)\big)(a-1)$
$\iff P\big(1+2(a-1)\big)2q = 2P\big(1+2(a-1)\big)(a-1)\big(2^{v_2(n!)-v_2(a-1)-3}r - P\big)$
$\iff q = (a-1)\big(2^{v_2(n!)-v_2(a-1)-3}r - P\big)$
où r est un nombre entier (pair pour n assez grand).
Alors $a-1$ divise q et d'après $(5')$, $a-1$ est un facteur de M.
$2a-1$ est un facteur de $M-1$ et $(2a-1)-2(a-1)=1$, donc d'après le mème principe de la remarque 1, il existerait un entier c tel que : $(M-1)M = (2a-1)\big(1+(a-1)c\big) \times \big(2+(2a-1)c\big)(a-1) = \dfrac{n!}{4}$.
Pour n assez grand (tel que $v_2\big(\dfrac{n!}{4}\big) > v_2(a-1)$; ce qui est vérifié pour $n \geq 10$), alors c est pair, c'est-a-dire que $c = 2c'$, c' nombre entier. C'est dire qu'on a :
$(M-1)M = (2a-1)\big(1+(a-1)2c'\big) \times \big(2+(2a-1)2c'\big)(a-1) = \dfrac{n!}{4}$.
C'est-à-dire que :
$(M-1)M = \big(1+2(a-1)c'\big)(2a-1) \times 2\big(1+(2a-1)c'\big)(a-1) = \dfrac{n!}{4}$ (6).
(6) et $(5')$ impliquent :
$\begin{cases} 1+2(a-1)c' = P \\ \big(1+(2a-1)c'\big)(a-1) = q + P(a-1) \end{cases}$
La première égalité donne $c' = \dfrac{P-1}{2(a-1)} = \dfrac{q-1}{a-1}$, et cette valeur de c' dans la deuxième égalité implique :
$a-1+(2a-1)(q-1) = q + P(a-1) = q + (2q-1)(a-1) \iff a-1+2aq-2a-q+1 = q+2aq-2q-a+1 \iff 0=1$, ce qui est absurde.
C'est dire que l'équation $\dfrac{n!}{4} = (M-1)M$, n'a pas de solution pour $n \geq 10$.
D'où le lemme 2.

Et donc pour $n \geq 10$, il n'y a pas de solution de l'équation (2), et par suite pas de solution de l'équation (1).
On vérifie aisément (on le sait d'ailleurs) que pour $n < 10$, les seules solutions de l'équation (1), sont celles correspondant aux valeurs 4, 5 et 7 de n.
On peut donc énoncer le théorème suivant.

Théorème :
Les seules solutions (n, m) de l'équation diophantienne $n!+1 = m^2$, sont les couples de nombres de Brown $(4, 5)$, $(5, 11)$ et $(7, 71)$.

Auteur : Babacar Gueye
Professeur contractuel de mathématiques au lycée de Sébikhotane
e-mail :gbabacar155@yahoo.fr

Tel :221 77 651 49 09

.....

Références :

- Les notes ont été partiellement prises dans WIKIPEDIA.
- Pour de plus amples informations sur le problème de Brocard, on peut consulter la page WIKIPEDIA qu'on retrouve en tapant dans google "le problème de Brocard".