On the Agoh-Giuga conjecture
Sur la conjecture d'Agoh-Giuga

Méhdi Pascal

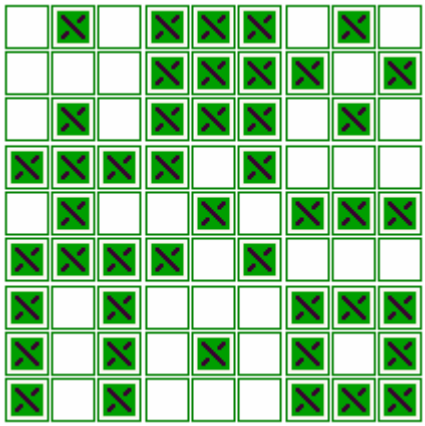
Février 2021

Abstract

This paper contains everything you need to know about the Agoh-Giuga conjecture, all the theorems related to this problem are given with the demonstrations well detailed so that they are easily readable to students, including the equivalence between the Agoh conjecture and Giuga conjecture, Theorem (36) is a new characterizes Carmichael numbers, it allows a combinatorial aspect of these numbers, at the end of this paper I give my remarks which show that it is possible to prove this conjecture if we focus on Carmichael's numbers, and not on Giuga's numbers.

Résumé

Ce papier contient tous ce qu'il faut savoir sur la conjecture d'Agoh-Giuga, tous les théorèmes liés à ce problème sont donnés avec les démonstrations bien détailler pour qu'ils soient bien lisibles aux étudiants, y compris l'équivalence entre la conjecture d'Agoh et la conjecture de Giuga, le théorème (36) est un nouveau caractérise les nombres de Carmichael, il permet un aspect combinatoire de ces nombres, à la fin de ce papier je donne mes remarques qui montrent qu'il est possible de prouver cette conjecture si on se concentre sur les nombres de Carmichael, et non sur les nombres de Giuga.



Un grand merci à viXra

Sur la conjecture d'Agoh-Giuga

Méhdi Pascal

Février 2021

En 1950 Giuseppe Giuga a conjecturer que,

(1) :
$$\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \; Modulo(n) \Leftrightarrow n \; est \; premier$$

Et en 1995 Takashi Agoh a conjecturer que,

(2) :
$$nb_{n-1} \equiv -1 \; Modulo(n) \Leftrightarrow n \; est \; premier$$

Où b_n est le nième nombre de Bernoulli.

La conjecture d'Agoh se justifie par l'équivalence suivant :

(3) :
$$\sum_{j=1}^{n-1} j^{n-1} \equiv nb_{n-1} \; Modulo(n)$$

Preuve :

Notons par $B_n(x)$ le nième polynôme de Bernoulli, et par $b_n=B_n(0)$ le nième nombre de Bernoulli, on a ,

$$S_k(n) = \sum_{j=0}^{n-1} j^k = \frac{B_{k+1}(n) - B_{k+1}(0)}{k+1} = \frac{B_{k+1}(n) - b_{k+1}}{k+1}$$

Comme les polynômes de Bernoulli sont des polynômes d'Appell, alors on a,

$$B_{k+1}(n) = \sum_{t=0}^{k+1} \binom{k+1}{t} b_{k+1-t} n^t$$

Donc,

$$\frac{S_k(n)}{n} = \frac{B_{k+1}(n) - b_{k+1}}{n(k+1)} = \frac{1}{n(k+1)} \left(\left(\sum_{t=0}^{k+1} \binom{k+1}{t} b_{k+1-t} n^t \right) - b_{k+1} \right)$$

$$\frac{S_k(n)}{n} = \frac{1}{(k+1)} \sum_{t=1}^{k+1} \binom{k+1}{t} b_{k+1-t} n^{t-1}$$

$S_k(n)/n$ est un polynôme de degré égale à k, et dont le terme constant vaut à b_k, tel que,

$$\left. \frac{S_k(n)}{n} \right|_{n=0} = b_k$$

Il en résulte,

(4) :
$$\frac{S_k(n)}{n} \equiv b_k \; Modulo(n)$$

Ou bien,

(5) :
$$S_k(n) \equiv nb_k \ Modulo(n^2)$$

Et bien sûr si une telle différence est multiple de n^2, alors elle est multiple de n, donc on peut écrire,

(6) :
$$S_k(n) \equiv nb_k \ Modulo(n)$$

Il suffit de remplacer k par n-1 pour achever la démonstration.
C.Q.F.D

Dans la suite de ce papier, on notera par $G(n) := \sum_{j=1}^{j=n-1} j^{n-1}$ « dite la somme de Giuga ».

(7) Lemme :

Soit p un nombre premier, pour tout entier n>0 on a,
$$\sum_{j=1}^{p-1} j^{n-1} \equiv \begin{cases} -1 \ Modulo(p) \ si \ \ (p-1)\,|\,(n-1) \\ 0 \ \ Modulo(p) \ si \ \ (p-1)\nmid (n-1) \end{cases}$$

Preuve :

Si p-1 divise n :

On applique le petit théorème de Fermat, tel que pour $0 \le j \le p-1$, on a, $j^n \equiv 1 \ \ Modulo(p)$ donc $\sum_{j=1}^{p-1} j^n \equiv \sum_{j=1}^{p-1} 1 \equiv p-1 \equiv -1 \ \ Modolo(p)$.

Si p-1 ne divise pas n :

Soit g une racine primitive $Modulo(p)$, i.e. g est un générateur de $\mathbb{F}_p^*$, on sait que $g^k \equiv 1 \, Modulo(p)$ si et seulement si $p-1\,|\,k$, comme g est un générateur de $\mathbb{F}_p^*$ alors l'ensemble $\{g, 2g, ..[]..\, , (p-1)g\}$ Modulo(p) est équivalente à $\{1, 2, ..[]..\, , p-1\}$.

On a,
$$(g^n-1)\sum_{j=0}^{p-1} j^n = \sum_{j=0}^{p-1} (jg)^n - \sum_{j=0}^{p-1} j^n \equiv \sum_{j=0}^{p-1} j^n - \sum_{j=0}^{p-1} j^n \equiv 0 \ Modulo(p)$$

Comme $(g^n-1) \neq 0 Modulo(p)$, donc $\sum_{j=0}^{p-1} j^n \equiv 0 \ Modulo(p)$.

C.Q.F.D

(8) Premier théorème de Giuga :

Soit n un entier composé, $G(n) \equiv -1 \ Modulo(n)$ si et seulement si, pour tout facteur premier p de n, on a, $p-1 \left| \left(\frac{n}{p} - 1 \right) \right.$ et $p \left| \left(\frac{n}{p} - 1 \right) \right.$.

Preuve :

En reprend le lemme (7), à savoir,
$$\sum_{j=1}^{p-1} j^{n-1} \equiv \begin{cases} -1 \ Modulo(p) \ si \ \ (p-1)\,|\,(n-1) \\ 0 \ \ Modulo(p) \ si \ \ (p-1)\nmid (n-1) \end{cases}$$

Valable pour tout nombre premier p.

Soit p un facteur premier de n, tel que $n = pq$, on a :

(1.[]) :
$$\sum_{j=1}^{n-1} j^{n-1} \equiv q\sum_{j=1}^{p-1} j^{n-1} \equiv \begin{cases} -q \ Modulo(p) \ si \ \ (p-1)\,|\,(n-1) \\ 0 \ \ Modulo(p) \ si \ \ (p-1)\nmid (n-1) \end{cases}$$

Premier sens

On suppose que $G(n) \equiv -1 \ Modulo(n)$ soit p un facteur premier de n, où $n = pq$ alors on a,

(2.[]) :
$$-1 \equiv \begin{cases} -q \ Modulo(p) \ si \ \ (p-1)\,|\,(n-1) \\ 0 \ \ Modulo(p) \ si \ \ (p-1)\nmid (n-1) \end{cases}$$

Ceci n'est possible que ci (p-1)|(n-1)=q(p-1)+q-1, donc (p-1)|(q-1)=(n/p-1)
Et comme -1≡-q Modulo(p), alors p|(q-1)=(n/p-1).

Second sens

On suppose que $(p-1)|(q-1)$ et $p|(q-1)$, pour tout facteur premier p de $n = pq$.
Il suit de (1.[]) que $G(n) \equiv -q \ Modulo(p)$, et puisque $p|q-1$, donc $q = 1 \ Modulo(p)$, d'où $G(n) \equiv -1 \ Modulo(p)$ pour tout facteur premier p de n.
n est un entier sans facteur carré, car sinon, il existe un facteur premier p tel que p^2 divise $n = pq$, donc p divise q, ce qu'est absurde, car p divise $(q\text{-}1)$.
Le fait que chaque facteur premier p de n divise $G(n)+1$, et que n est un entier sans facteur carré, montre que n=$PPCM$(des p) divise $G(n)+1$, donc, $G(n) \equiv -1 \ Modulo(n)$.
C.Q.F.D

Donc il s'agit de trouver des solutions du système suivant :

(9) : pour tout facteur premier p de n, $\begin{cases} p\,|\,(\frac{n}{p}-1) \\ (p-1)\,|\,(\frac{n}{p}-1) \end{cases}$

A savoir que ce système admet des solutions, dites les solutions triviales, qui sont tout simplement les nombres premiers.
Ce système nous permet de définir deux classes des nombres, qui sont les nombres de Giuga et les nombres de Carmichael, tels que,

(10) : Un entier n composé, tel que pour tout facteur premier p de n, on a $p|(n/p\text{-}1)$ est dite un nombre de Giuga.

(11) : Un entier composé n, tel que pour tout facteur premier p de n, on a $(p-1)$ divise $(n/p-1)$ est dite un nombre de Carmichael.

La définition (11) est équivalente à (12), telle que,

(12) : Un entier composé n, tel que pour tout facteur premier p de n, on a $(p-1)$ divise $(n\text{-}1)$ est dite un nombre de Carmichael.

En effet, pour le premier sens on a,
$$p-1\,|\left(\frac{n}{p}-1\right) \Rightarrow \frac{n}{p} \equiv 1 \ Modulo(p-1)$$

Comme $(p,p-1)=1$ alors $n \equiv p \ Modulo(p-1)$

Comme $p \equiv 1 \ Modulo(p-1)$ alors $n \equiv 1 \ Modulo(p-1)$

D'où, $p-1 \mid n-1$.

Pour le sens inverse on a,

$$p-1 \mid n-1 \Rightarrow n \equiv 1 \ Modulo(p-1)$$

Comme $p \equiv 1 \ Modulo(p-1)$

$$n \equiv p \ Modulo(p-1)$$

Et comme $(p,p-1)=1$ alors on peut diviser par p tel que,

$$\frac{n}{p} \equiv \frac{p}{p} \equiv 1 \ Modulo(p-1)$$

D'où, $p-1 \mid \left(\frac{n}{p}-1\right)$.

C.Q.F.D

Le théorème (8) veut dire qu'un entier n tel que, $G(n) \equiv -1 \ Modulo(n)$ doit être à la fois un nombre de Giuga et un nombre de Carmichael.
Giuga a conjecturé qu'un tel entier non trivial n'existe pas, et depuis, ça reste une question ouverte.

Donc pour comprendre ce problème, il faut savoir qu'est ce que un nombre de Giuga ? Et qu'est ce que un nombre de Carmichael ?

On commence par les nombres de Giuga, avec le théorème suivant,

(13) Second théorème de Giuga :

Soit n un entier positive sans facteur carrée, et p un nombre premier,

n est un nombre de Giuga si et seulement si, $\sum_{p \mid n} \frac{1}{p} - \prod_{p \mid n} \frac{1}{p} \in \mathbb{N}$

Remarquons que si n est un entier sans facteur carré alors, $\prod_{\substack{p,\ premier \\ p \mid n}} \frac{1}{p} = \frac{1}{n}$

(14) Lemme :
Soient n un entier sans facteur carré, et,

$$a := \sum_{p \mid n} \frac{1}{p} - \prod_{p \mid n} \frac{1}{p} \in \mathbb{N}$$

$$b := \sum_{p \mid n} \frac{n}{p} \equiv 1 \ Modulo(n)$$

Alors on a, $a \Leftrightarrow b$.
Preuve :

On a, $a=\sum_{p|n}\frac{1}{p}-\prod_{p|n}\frac{1}{p}=\frac{\sum_{p|n}\frac{n}{p}}{n}-\frac{1}{n}$, donc $na=\sum_{p|n}\frac{n}{p}-1$, d'où $\sum_{p|n}\frac{n}{p}\equiv 1 Modulo(n)$.

Inversement, $\sum_{p|n}\frac{n}{p}\equiv 1 Modulo(n)$ implique $\exists a\in\mathbb{Z}$ tel que $na=\sum_{p|n}\frac{n}{p}-1$, donc

$a=\frac{\sum_{p|n}\frac{n}{p}}{n}-\frac{1}{n}=\sum_{p|n}\frac{1}{p}-\prod_{p|n}\frac{1}{p}$, comme $\left(\sum_{p|n}\frac{n}{p}\right)-1>0$ alors $a\in\mathbb{N}$.

C.Q.F.D

Preuve de (13) :

Premier sens :

Soit n un nombre de Giuga, donc n est un entier sans facteur premier, et on a, $\sum_{p|n}\frac{1}{p}-\prod_{p|n}\frac{1}{p}=\sum_{p|n}\frac{1}{p}-\frac{1}{n}>0$ car $p<n$ et donc $\frac{1}{p}>\frac{1}{n}$.

Supposons que n est composé de k nombres premiers, donc $n=\prod_{j=1}^{k}p_j$, et on a, n est un nombre de Giuga alors :

1. pour tout $1\le j\le k$, $p_j\left|\left(\frac{n}{p_j}-1\right)\right.\Leftrightarrow\frac{n}{p_j}\equiv 1\ Modulo(p_j)$.
2. n est un entier sans facteur carré, donc si $i\neq j$ alors $p_i\neq p_j$, et dans on a $\frac{n}{p_i}\equiv 0 Modulo(p_j)$.

Ainsi $\frac{n}{p_j}\equiv\begin{cases}1\ Modulo(p_i) & si\ i=j\\ 0\ Modulo(p_i) & si\ i\neq j\end{cases}$, ce qui entraîne que $\sum_{j=1}^{k}\frac{n}{p_j}\equiv 1\ Modulo(p_i)$, pour tout $i\in\{1,2,\ ..[]..\ ,k\}$.

Et par le théorème des restes chinois on a bien $\sum_{j=1}^{k}\frac{n}{p_j}=\sum_{p,\ premier\ p|n}\frac{n}{p}\equiv 1\ Modulo(n)$.

Le sens inverse :

On a,

$$\sum_{p|n}\frac{n}{p}\equiv 1 Modulo(n)\Rightarrow\sum_{p|n}\frac{n}{p}-1=kn$$

Soit q l'un des facteurs premiers de n, on a :

$$\frac{n}{q}-1=kn-\sum_{p,premier\ et\ p|n\ \atop p\neq q}\frac{n}{p}$$

q divise kn et q divise aussi n/p, donc q divise $\frac{n}{q}-1$ donc n est un nombre de Giuga.

C.Q.F.D

(15) Lemme:

Pour tout entier $n>0$ on a, $\sum_{k=1}^{n-1} k^{\varphi(n)} \equiv nb_{\varphi(n)}\ Modulo(n)$ où $\varphi(n)$ est l'indicatrice d'Euler, et b_n est le nième nombre de Bernoulli.

Preuve :

Il suffit de remplacer k par $\varphi(n)$ dans (6).
C.Q.F.D

(16) Théorème :

Soit n un entier sans facteur carré,

n est un nombre de Giuga si et seulement si, $\sum_{k=1}^{n-1} k^{\varphi(n)} \equiv -1\ Modulo(n)$.

Où $\varphi(n)$ est la fonction indicatrice d'Euler.

Le lemme (15) montre l'équivalence entre (16) et (17), tel que,

(17) Théorème :

Soit n un entier sans facteur carré,

n est un nombre de Giuga si et seulement si, $nb_{\varphi(n)} \equiv -1\ Modulo(n)$.

Preuve :

Premier sens :

n est un nombre de Giuga, donc n est sans facteur carré, tel que pour tout facteur premier p de n, on a $p\,|\,(\frac{n}{p}-1)$, soit $n=\prod_{j=1}^{k} p_j$, donc $\varphi(n)=\prod_{j=1}^{k}\left(p_j-1\right)$.

Soit $D_{\varphi(n)}=\prod_{\substack{p,\,premier\\ p-1|\varphi(n)}} p$ le dénominateur de $b_{\varphi(n)}$, il est claire que n divise $D_{\varphi(n)}$.

Le théorème de Von Staudt-Clausen à savoir :

$$\left(b_n+\sum_{\substack{p,\,premier\\ p-1|n}}\frac{1}{p}\right)\in\mathbb{Z}$$

Soit q un nombre premier, et $\mathbb{Z}q$ l'anneau des q-entier, i.e. un rationnel a/b est un q-entier si et seulement si $(b,q)=1$.

On sait que $\mathbb{Z}\subset\mathbb{Z}q$ pour tout premier q, ce qui nous permet d'écrire,

$$\left(b_n+\sum_{\substack{p,\,premier\\ p-1|n}}\frac{1}{p}\right)\equiv 0\ Modulo\ (\mathbb{Z}q)$$

On multiple par n, et on a,

$$\left(nb_{\varphi(n)}+\sum_{\substack{p,\,premier\\ p-1|\varphi(n)}}\frac{n}{p}\right)=\left(nb_{\varphi(n)}+\sum_{\substack{p,\,premier\\ p|n}}\frac{n}{p}+\sum_{\substack{p,\,premier\\ p-1|\varphi(n)\ \&\ p\nmid n}}\frac{n}{p}\right)\equiv 0\ Modulo\ (n\mathbb{Z}q)$$

Et on a $\sum_{p|n}\frac{n}{p}\equiv 1\ Modulo\ (n\mathbb{Z}q)$, « déjà vu dans la preuve de (13) » et $\sum_{\substack{p,\,premier\\ p-1|\varphi(n)\ \&\ p\nmid n}}\frac{n}{p}\equiv 0\ Modulo\ (n\mathbb{Z}q)$ d'où $\left(nb_{\varphi(n)}+1\right)\equiv 0\ Modulo\ (n\mathbb{Z}q)$.

Le sens inverse :

Dans ce sens en part de $nb_{\phi(n)}\equiv -1 Modulo(n\mathbb{Z}_n)$, et par le théorème de V.S.C on a,

$$\left(b_{\phi(n)}+\sum_{\substack{p,\,premier\\ p-1|\phi(n)}}\frac{1}{p}\right)\in\mathbb{Z}$$

Donc,

$$\left(nb_{\phi(n)}+\sum_{\substack{p,\,premier\\ p-1|\phi(n)}}\frac{n}{p}\right)\in n\mathbb{Z}q\ ,\ \forall q\in\mathbb{P}$$

On remplace $nb_{\phi(n)}$ par -1, et on a,

$$\sum_{\substack{p,\,premier\\ p-1|\phi(n)}}\frac{n}{p}-1\in n\mathbb{Z}q \quad \text{ou bien,} \quad \sum_{\substack{p,\,premier\\ p-1|\phi(n)}}\frac{n}{p}\equiv -1\ Modulo(n\mathbb{Z}q)\ .$$

Dire que p est premier tel que $p-1|\phi(n)$ est équivalant à dire que p est premier tel que $p|n$, puisque n est sans facteur carré, donc :

$$\sum_{\substack{p,\,premier\\ p|n}}\frac{n}{p}\equiv -1\ Modulo(n\mathbb{Z}q)$$

C.Q.F.D
[]

Les nombres de Giuga sont très rares, voici les 12 premières valeurs connues :

- **3 facteurs :**

30=2.3.5

- **4 facteurs :**

858=2.3.11.13
1722=2.3.7.41

- **5 facteurs :**

66198=2.3.11.17.59

- **6 facteurs :**

2214408306=2.3.11.23.31.47057
24423128562=2.3.7.43.3041.4447

- **7 facteurs :**

432749205173838=2.3.7.59.163.1381.775807
14737133470010574=2.3.7.71.103.67213.713863
550843391309130318=2.3.7.71.103.61559.29133437

- **8 facteurs :**

244197000982499715087866346=2.3.11.23.31.47137.28282147.3892535183
554079914617070801288578559178=2.3.11.23.31.47059.225969649.110725121051
191066718142050798455575991633850 6=2.3.7.43.1831.138683.2861051.
1456230512169437

Dans cette liste on remarque que ces nombres sont pairs, et pour plus de précision ils admettent 6 comme le plus grand diviseur commun, mais rien ne preuve que ça est vrai pour tout nombre de Giuga.

Cette liste vérifie aussi que l'on a, $\sum_{p|n}\frac{1}{p}-\prod_{p|n}\frac{1}{p}=1$.

On ne sait plus s'il existe une infinité de ces nombres, certainement ils sont très rares, mais le plus proche à l'esprit, c'est qu'elle existe une infinité.

Pour les nombres de Carmichael, leur histoire a commencer avec le petit théorème de Fermat, tel que pour tout premier p et pour tout entier a tel que $(a,p)=1$, on a, $a^{p-1}\equiv 1\ Modulo(p)$, et on se demande si cette propriété est vraie seulement pour les nombres premiers, pour ça, soit $n=\prod_{1\le j\le k} p_j$, où les p_j sont les facteurs premiers de n, on suppose que n est sans facteur carré, si $p_j-1\,|\,n-1$, alors le petit théorème de Fermat nous conduit au système suivant,

$$\begin{cases} a^{p_1-1}\equiv a^{n-1}\equiv 1\ Modulo(p_1) & \forall (a,p_1)=1 \\ a^{p_2-1}\equiv a^{n-1}\equiv 1\ Modulo(p_2) & \forall (a,p_2)=1 \\ \quad ..[].. & \\ a^{p_k-1}\equiv a^{n-1}\equiv 1\ Modulo(p_k) & \forall (a,p_k)=1 \end{cases}$$

Et le théorème chinois permet d'écrire,

$$a^{n-1}\equiv 1\ Modulo(n)$$

Un tel nombre est dit nombre de Carmichael, et c'est la raison pour la quelle on appels ces nombres les monteurs de Fermat, comme si Fermat mont.

Un nombre de Carmichael n est entier composé impair, car si n est pair alors $n-1$ est impair, et donc pour un facteur premier $p\neq 2$ de n, on a $p-1$ est pair, donc $(p-1)\nmid(n-1)$.

Un nombre de Carmichael n est entier composé sans facteur carré, car pour tout entier a, on a $a^n-a\equiv 0\ Modulo(n)$, posons $a=p$, si $p^2|n$ alors p^2 divise $(p^n-p)=p(p^{n-1}-1)$, donc p^2 divise p ce qu'est impossible.

Un nombre de Carmichael n est entier composé au moins de trois facteurs premiers, car sinon $n=pq$ où p et q sont des nombres premiers, et on a, $p-1\,|\,n-1$ & $q-1\,|\,n-1$, or $n-1=pq-1=(p-1)q+q-1$, puisque $p-1\,|\,n-1$ donc $p-1$ divise aussi $q-1$, de même raisonnement on trouve $q-1\,|\,p-1$, donc $p=q$, ce qu'est impossible puisque n est sans facteur carré.

Tous ça se résume en un seul critère dite critère de Korselt, tel que,

(18) Théorème « Korselt » :

Un nombre de Carmichael n est entier impair composé au moins de trois facteurs premiers, et sans facteur carré, tel que pour chaque facteur premier p de n, $p-1 \mid n-1$.

Mais il existe un autre critère, due cette fois à R. Carmichael, c'est un critère basé sur une grande intuition, que même D. Lehmer n'a pas pue la démontrer.

Soit G un groupe multiplicative finie de cardinal égale à $n \in \mathbb{N}^*$, dans ce qui suit on note par :

- $Card(G) = |G|$ le cardinal de G, dite aussi l'ordre de G, est le nombre des éléments de G.
- Soit g un élément de G, on appels ordre de g, noté par $Ord(g)$ le plus petit entier l tel que $g^l = 1$, où 1 est l'élément neutre de G.
- On note par $\langle g \rangle$ avec $g \in G$, le sous groupe de G engendré par g, i.e. $\langle g \rangle = \{g, g^2, ..[]..., g^{Ord(g)} = 1\}$.

Les deux théorèmes suivant sont très fondamentaux dans la théorie des groupes, ils sont dus à Lagrange.

(19) Théorème :

$$\forall g \in G, \quad g^{|G|} = 1.$$

(20) Théorème :

$$\forall g \in G, \quad Ord(g) \text{ divise } |G|.$$

Ce dernier théorème veut dire que si H est un sous groupe de G, alors $|H|$ divise $|G|$.

(21) L'ordre de Carmichael, « Définition »:

L'ordre de Carmichael d'un groupe G, est le plus petit entier $\lambda = \lambda(G)$, tel que $\forall g \in G, \quad g^{\lambda} = 1$.

A partir de cette définition en déduis immédiatement que l'ordre de Carmichael d'un groupe G, vaut au plus petit multiple commun des ordres de tous les sous groupe cyclique du groupe G. en particulier si le groupe G est cyclique, alors $\lambda(G) = |G|$.

Et par le théorème (20) en déduis que $\lambda(G)$ divise $|G|$.

NOTE : *Un groupe cyclique est un groupe fini engendrer par un de ses éléments, i.e. il existe $x \in G$ tel que $G = \langle x \rangle$.*

Exemple :

Pour $|G| = 4$, $G = \{1, a, b, c\}$ il existe deux groupes possibles, le premier est un groupe cyclique C_4, l'autre est le groupe de Klein noté par K, tel que :

C4	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

K	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Et on a, $\lambda(C_4)=|C_4|=4$ alors que $\lambda(K)=|K|/2=2$, car tout sous groupes de Klein distinct de K, est d'ordre 2, sauf le trivial $\{1\}$.

Voilà ça c'est en générale, mais dans le cadre de la théorie des nombres en prend seulement les groupes $G_n=(\mathbb{Z}/n\mathbb{Z})^*$ le groupe des classes inversibles modulo (n).

Comme on sait bien qu'une classe a admet un inverse modulo(n) si et seulement si $(a,n)=1$, donc $|G_n|=\varphi(n)$, où $\varphi(n)$ est la fonction indicatrice d'Euler, donc le théorème (19) se traduit au théorème d'Euler, tel que,

(22) Théorème d'Euler :

Pour tout entier a, tel que$(a,n)=1$, on a, $a^{\varphi(n)}\equiv 1\ Modulo(n)$.

Supposons que $\varphi(n)$ divise $n-1$, alors certainement on peut dire que pour tout entier a, tel que$(a,n)=1$, que l'on a, $a^{n-1}\equiv 1\ Modulo(n)$, ou tout simplement que n est un nombre de Carmichael !!!
Sauf que ça est très loin d'être vais, comme il indique la conjecture de Lehmer, telle que,

(23) Conjecture de Lehmer :

n est premier, si et seulement si, $n\equiv 1\ Modulo\left(\varphi(n)\right)$.

Le premier sens est évident, pour le second cela veut dire qu'il existe un entier positif k tel que $n-1=k\varphi(n)$, or le théorème d'Euler nous dit que pour tout entier a premier avec n, que l'on a,

$$a^{\varphi(n)}\equiv 1\ Modulo(n)$$

Donc,

$$a^{k\varphi(n)}\equiv 1^k\ Modulo(n)$$

$$a^{n-1}\equiv 1\ Modulo(n)$$

Cela veut dire que n ne peut être qu'un nombre premier, ou un nombre de Carmichael.

Note :

La conjecture de Lehmer peut être énoncer d'une manière plus simple telle que :

n est premier si et seulement si $\varphi(n)\,|\,n-1$.

(24) Proposition :

Soit n un entier sans facteur carré, si $\varphi(n)\,|\,n-1$ alors $nb_{\varphi(n)}\equiv nb_{n-1}Modulo(n)$

Preuve :
Par le théorème de Von Staudt-Clausen on a,

$$nb_{\varphi(n)} + \sum_{\substack{p,\,premier \\ p-1|\varphi(n)}} \frac{n}{p} \in n\mathbb{Z}$$

&

$$nb_{n-1} + \sum_{\substack{p,\,premier \\ p-1|n-1}} \frac{n}{p} \in n\mathbb{Z}$$

Donc,

$$nb_{n-1} + \sum_{\substack{p,\,premier \\ p-1|n-1}} \frac{n}{p} \equiv nb_{\varphi(n)} + \sum_{\substack{p,\,premier \\ p-1|\varphi(n)}} \frac{n}{p} \quad Modulo(n)$$

$$nb_{n-1} + \sum_{\substack{p,\,premier \\ p-1|n-1 \\ p-1\nmid\varphi(n)}} \frac{n}{p} \equiv nb_{\varphi(n)} \quad Modulo(n)$$

Comme $\sum_{\substack{p,\,premier \\ p-1|n-1 \\ p-1\nmid\varphi(n)}} \frac{n}{p} \equiv 0 \quad Modulo(n)$, alors $nb_{\varphi(n)} \equiv nb_{n-1} Modulo(n)$.

C.Q.F.D
[]

La définition (21) conduit à la fonction indicatrice de Carmichael, telle que,

(25) Définition :

La fonction indicatrice de Carmichael $\lambda(n)$ est le plus petit entier, tel que pour tout entier a premier avec n on a, $a^{\lambda(n)} \equiv 1\, Modulo(n)$.

Car $\lambda(n) = \lambda(G_n)$ où $G_n = (\mathbb{Z}/n\mathbb{Z})^*$.

Par exemple pour n=15 on a $G_{15} = \{1,2,4,7,8,11,13,14\}$, faisons une table des puissances, telle que,

				λ				φ
^	^1	^2	^3	^4	^5	^6	^7	^8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

Donc les sous groupes de G_{15} sont le sous groupe trivial <1> d'ordre 1, trois sous groupe d'ordre 2 qui sont <4>, <11> et <14>, et deux sous groupes d'ordre 4 qui sont <2> et <7>.

Donc $\lambda(15)=\lambda\left(G_{15}\right)=ppcm(1,2,4)=4$.

On a $\lambda\left(G_n\right)=\left|G_n\right|$ si et seulement si G_n est cyclique, ce qui entraîne le théorème suivant,

(26) Théorème :

$\lambda(n)=\varphi(n)$ si et seulement si,

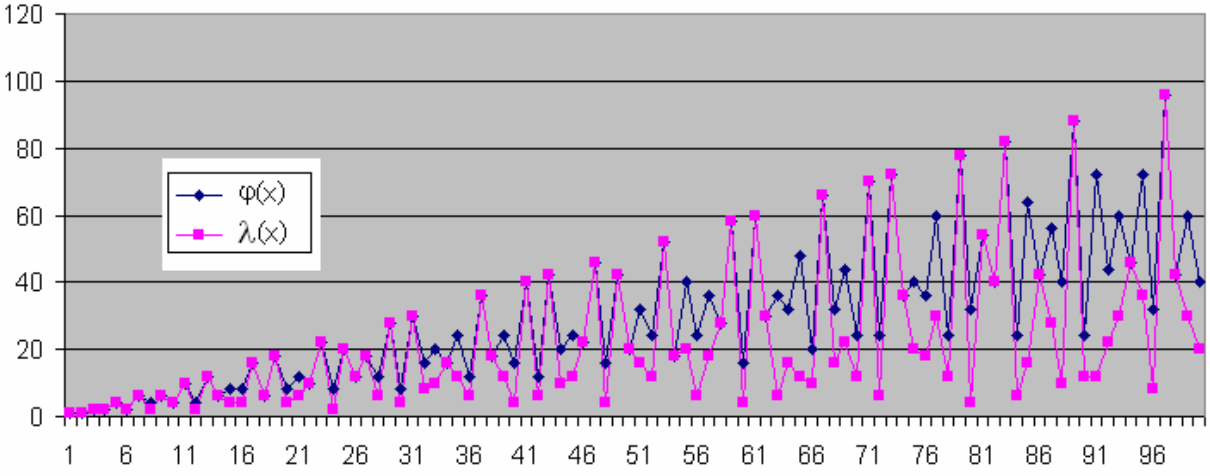
- $n=1$.
- $n=2$ ou $n=4$.
- $n=p^r$ ou $n=2p^r$, où p est un nombre premier impair et r est un entier positive.

En déduis donc le critère qui nous permet de calculer les valeurs de cette fonction.

(27) Définition & Critère :

L'indicatrice de Carmichael est une fonction définie pour tout entier n strictement positive telle que :

- $\lambda(1)=1$.
- Si n est premier alors $\lambda(n)=n-1=\varphi(n)$.
- Si $n=p^r$, p est premier $\neq 2$ alors $\lambda(n)=\lambda(p^r)=p^{r-1}(p-1)=\varphi(p^r)$.
- Si $n=2^r$, alors $\lambda(2)=1$, $\lambda(4)=\lambda(8)=2$, et pour $r\geq 4$, $\lambda(2^r)=2^{r-2}$.
- Donc pour $n=p_1^{\alpha 1}.p_2^{\alpha 2}$ ..[].. $p_j^{\alpha j}$, $\lambda(n)=ppcm\left(\lambda(p_1^{\alpha 1}),\lambda(p_2^{\alpha 2}),\ ..[]..\ ,\lambda(p_j^{\alpha j})\right)$



On a les propriétés suivantes,

(28) : Pour tout n≥2 $\lambda(n)$ est paire, conséquence immédiate de (27).

(29) : $\lambda(n)\,|\,\varphi(n)$ car $\lambda\left(G_n\right)\,|\,\left|G_n\right|$.

Contrairement à l'indicatrice d'Euler, l'indicatrice de Carmichael n'est pas une fonction multiplicative, par exemple $\lambda(15)=4\neq\lambda(3)\lambda(5)$.

(30) Théorème de Carmichael :

Un entier composé n est un nombre de Carmichael si et seulement si,

$$\lambda(n)\,|\,(n-1)\ .$$

Preuve :

Premier sens :

n est un nombre de Carmichael, donc n est un entier composé impair et sans facteur carré, tel que pour chacun de ses facteurs premiers p on a $p\text{-}1|n.$

Posons $n=p_1.p_2..[]..p_k$ on a,

$$\begin{cases} p_1-1\,|\,n-1 \\ p_2-1\,|\,n-1 \\ \quad ..[].. \\ p_k-1\,|\,n-1 \end{cases} \text{ implique que, } \quad ppcm\left(p_1-1,p_2-1,..[]..,p_k-1\right)|\,n-1$$

$$\text{Donc, } \quad \lambda(n)\,|\,n-1\ .$$

Second sens :

$\lambda(n)\,|\,(n-1)$, donc il existe un entier k tel que $k\lambda(n)=(n-1)$, et on a pour tout entier a premier avec n,

$$a^{\lambda(n)}\equiv 1\ Modulo(n)$$

$$\left(a^{\lambda(n)}\right)^k\equiv 1^k\ Modulo(n)$$

$$a^{n-1}\equiv 1\ Modulo(n)\ .$$

C.Q.F.D

Voilà ce sont les deux critères permettant de définir et de trouver ces nombres de Carmichael, mais ils existent des formules qui permettent de les trouver, par exemple la célèbre formule de J.Chernick à savoir :

(31) : Soit, $n(x)=(6x+1)(12x+1)(18x+1)$

$$n(x)=1296x^3+396x^2+36x+1$$

Si les trois facteurs de $n(x)$ sont des nombres premiers pour une valeur de x, alors $n(x)$ est un nombre de Carmichael.

Pour la preuve il suffit de vérifier que $6x$, $12x$ et $18x$ divisent $n(x)-1$.

Certainement ils existent plusieurs formules de ce genre, mais lorsque je reprends ces trois entiers 6, 12 et 18 qu'on a dans la formule de J.Chernick, je me trouve devant une petite curiosité, car on a 6 est un diviseur commun de $6x$, $12x$ et $18x$, et 6 est un nombre parfait, et aussi la présences des diviseurs propres de 6 qui sont 1, 2 & 3, « 6=1+2+3 ».

Donc, si je prends un autre nombre parfait, tel que par exemple 28=1+2+4+7+14, on aura par analogie à la formule de J.Chernick, la suivante :

(32) : $n(x)=(28x+1)(28*2x+1)(28*4x+1)(28*7x+1)(28*14x+1)$

$$n(x)=(28x+1)(56x+1)(112x+1)(196x+1)(392x+1)\ .$$

Qui donne des nombres de Carmichael à cinq facteurs premiers, exemples n(2136), n(2211), n(4071), n(5106), n(5430)..[]..

On démontre aisément que cette analogie est vraie pour tout nombre parfait.

Les nombres parfaits pairs sont liés aux nombres de Mersenne $M_p = 2^p - 1$, tel que si M_p est premier alors $2^{p-1} M_p$ est un nombre parfait, et pour que M_p soit premier il faut mais il ne suffit pas que p soit aussi premier.
Soit $N_p = 2^{p-1} M_p$, et trichons un peu, par exemple faisons comme si 4 est un nombre premier, pire encore comme si M_4=15 est aussi premier, alors dans ce cas on a N_4 = 120 est bien un nombre parfait, puisqu'il vaut à la somme de ces diviseurs propres, tel que, 120 = 1+2+4+8+15+30+60, ainsi le polynôme suivant :

(33) : $n(x)=(120x+1)(120*2x+1)(120*4x+1)(120*8x+1)(120*15x+1)(120*30x+1)(120*60x+1)$
$=(120x+1)(240x+1)(480x+1)(960x+1)(1800x+1)(3600x+1)(7200x+1)$

est un nombre de Carmichael si ses facteurs sont tous premiers.

Bien que 120 n'est pas un nombre parfait, mais au moins les deux nombres suivant sont des nombres de Carmichael :

18476201214199947713772800482642383458415739200 1
31313711489256386181781268983633053474051333888 01

Respectivement pour x = 6055 & x = 9072.
De cette méthode on peut donner une infinité de ces polynômes qui seront analogue au polynôme de Chernick, et les nombres de Carmichael qu'on tire de ces polynômes ont une importance majeure, car ils ne peuvent pas êtres des contres exemples à la conjecture d'Agoh-Giuga.
[]

(34) Proposition :

Soit n un nombre de Carmichael, et p et q deux quelconques facteurs premiers de n, alors $p \neq 1 \; Modulo(q)$.

Exemple 561=3*11*17, aucun de ces facteurs premiers n'est congrus à 1 modulo l'autre.

Preuve :

Supposons que $q=kp+1$ donc $q-1=kp|(n-1)$ donc $p|(n-1)$ et $p|n$, ce qu'est absurde.

(35) Proposition :

Soient n un entier sans facteur carré, et $\Omega(n)$ le nombres de ses facteurs premiers, le nombre des diviseur de n vaut à $2^{\Omega(n)}$.

Preuve :
Posons $n = p_1 p_2 .. [] .. p_k$, comme n est sans facteur carré alors les p_1, p_2 .. [] .. p_k sont tous différents, posons $A = (1+p_1)(1+p_2)..[]..(1+p_k)$ après le développement de A on aura :

$$A = 1 + \underbrace{(p_1 + p_2 + .. [] .. + p_k)}_{\binom{k}{1} termes} + \underbrace{(p_1 p_2 + p_1 p_3 + .. [] .. + p_{k-1} p_k)}_{\binom{k}{2} termes} + .. [] .. + \underbrace{p_1 p_2 .. [] .. p_k}_{\binom{k}{k} termes}$$

Ce développement donne tous les diviseurs de n, dont le nombre vaut à 2^k.

C.Q.F.D

(36) Théorème « *Aspect combinatoire des nombres de Carmichael* » :

Soit n un nombre de Carmichael, $\Omega(n)$ le nombre de facteurs premiers de n, alors on a :

$$\sum_{d|n} d^{n-1} \equiv 2^{\Omega(n)-1} \; Modulo(n) \; .$$

Preuve :

Soient n un nombre de Carmichael, et d l'un de ces diviseurs, notons par q le complément de d « i.e. $n=dq$ », donc le nombre de couple (d,q) « (diviseur, compliment) » vaut à la moitié de tous les diviseurs, qui par (35) vaut à $2^{\Omega(n)-1}$, et on a,

$$d^{n-1} + q^{n-1} \equiv 1 \; Modulo(n)$$

En effet,

$$(d+q)^{n-1} = \left(d^{n-1} + q^{n-1}\right) + \sum_{j=1}^{n-2} \binom{n-1}{j} d^{n-j-1} q^{j} = \left(d^{n-1} + q^{n-1}\right) + \underbrace{\sum_{j=1}^{n-2} \binom{n-1}{j} n d^{n-j-2} q^{j-1}}_{\equiv 0 \; Modulo(n)}$$

Donc,

$$(d+q)^{n-1} \equiv \left(d^{n-1} + q^{n-1}\right) \; Modulo(n)$$

Et comme n est sans facteur carré, alors $(d+q,n)=1$, d'où,

$$\left(d^{n-1} + q^{n-1}\right) \equiv (d+q)^{n-1} \equiv 1 \; Modulo(n)$$

Et comme le nombre de couple (d,q) vaut à $2^{\Omega(n)-1}$, alors,

$$\sum_{d|n} d^{n-1} \equiv 2^{\Omega(n)-1} \; Modulo(n)$$

C.Q.F.D

NOTE :

Une formule analogue vraie pour les nombres de Giuga est :

$$\sum_{d|n} d^{\varphi(n)} \equiv 2^{\Omega(n)-1} \; Modulo(n)$$

Mais ça reste sans aucune importance, puisque ce n'est pas une propriété des nombres de Giuga, car c'est une propriété de tout entier n sans facteur carré, cela veut dire qu'elle est vraie pour les nombres de Giuga, elle est vraie pour les nombres de Carmichael, et même vraie pour une infinité des nombres qui ne sont ni de Giuga ni de Carmichael.

(37) Théorème :

Pour tout nombre de Carmichael n on a,

$$G(n) \equiv n\left(1 - \sum_{\substack{p,\, premier \\ p|n}} \frac{1}{p}\right) Modulo(n)$$

Exemples :

$$G(561) = 561\left(1 - \left(\frac{1}{3} + \frac{1}{11} + \frac{1}{17}\right)\right) = 290$$

$$G(41041)=41041\left(1-\left(\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{41}\right)\right)=27289$$

Preuve :

La formule (6) nous permet d'écrire,

$$G(n):=\sum_{j=1}^{j=n-1} j^{n-1}\equiv nb_{n-1}\ Modulo(n)$$

Le théorème de Von Staudt-Clausen à savoir $\left(b_n+\sum_{\substack{p,premier\\ p-1|n}}\frac{1}{p}\right)\in\mathbb{Z}$ nous permet d'écrire,

$$nb_{n-1}\equiv -n\sum_{\substack{p,premier\\ p-1|n-1}}\frac{1}{p}\ Modulo(n)$$

$$nb_{n-1}\equiv -\left(\sum_{\substack{p|n\\ p-1|n-1}}\frac{n}{p}+\sum_{\substack{p\nmid n\\ p-1|n-1}}\frac{n}{p}\right)Modulo(n)$$

Or,

$$\sum_{\substack{p\nmid n\\ p-1|n-1}}\frac{n}{p}\equiv 0\ Modulo(n)$$

Donc,

$$nb_{n-1}\equiv -n\sum_{\substack{p|n\\ p-1|n-1}}\frac{1}{p}\equiv n\left(1-\sum_{\substack{p|n\\ p-1|n-1}}\frac{1}{p}\right)Modulo(n)$$

C.Q.F.D

Notation :

Soit le polynôme suivant :

$$P(x)=\prod_{j=1}^{j=n}(x+s_j)$$

Apres le développement on obtient,

$$P(x)=\sigma_0x^n+\sigma_1x^{n-1}+\sigma_2x^{n-2}+..[]..+\sigma_{n-1}x+\sigma_n$$

Avec,

$$\sigma_1=s_1+s_2+..[]..+s_n$$

$$\sigma_2=s_1s_2+s_1s_3+..[]..+s_{n-1}s_n$$

$$..[]..$$

$$\sigma_j=\sum_{1\le i_1<i_2..[]..<i_j\le n}s_{i_1}s_{i_2}..[]..s_{i_j}$$

$$..[]..$$

$$\sigma_n=s_1s_2..[]..s_n$$

σ_j est la notation usuelle qu'on donne à une fonction symétrique élémentaire, et pour les besoin de fiabilité je propose la notation suivante :

(38) :
$$M_n^j(s)=\sigma_j\,,\quad M_n^0(s)=1$$
$$M_n^j(s)=0\,,\ \text{si } j<0 \text{ ou } j>n.$$

Et donc le polynôme $P(x)=\prod_{j=1}^{j=n}(x+s_j)$ peut s'exprimer en terme des fonctions symétriques élémentaire comme suivant $P(x)=\sum_{j\in\mathbb{Z}} M_n^j(s)x^j$.

Et on a la formule de récurrence suivante :

(39) :
$$M_n^j(s)=M_{n-1}^j(s)+s_nM_{n-1}^{j-1}(s)$$

Facile à démontrer, par exemple on a,
$$M_3^1(s)=\underbrace{(s_1+s_2)}_{M_2^1(s)}+\underbrace{s_3.1}_{s_3M_2^0(s)}$$
$$M_3^2(s)=\underbrace{s_1s_2}_{M_2^2(s)}+\underbrace{s_3(s_1+s_2)}_{s_3M_2^1(s)}$$
$$M_3^3(s)=\underbrace{0}_{M_2^3(s)}+\underbrace{s_3(s_1s_2)}_{s_3M_2^2(s)}$$

On a aussi,

(40) :
$$M_n^j\left(\frac{1}{s}\right)=\frac{M_n^{n-j}(s)}{M_n^n(s)}$$

Exemple :
$$\frac{1}{s_1}+\frac{1}{s_2}+\frac{1}{s_3}=\frac{s_2s_3+s_1s_3+s_1s_2}{s_1s_2s_3}$$

Fin notation.

Soit n un nombre de Carmichael tel que, $n=p_1p_2..[]..p_k$ on a,
$$\varphi(n)=(p_1-1)(p_2-1)..[]..(p_k-1)$$
$$\varphi(n)=n-M_k^{k-1}(p)+M_k^{k-2}(p)+..[]..+(-1)^kM_k^0(p)$$

On a, $G(n)=n\left(1-\sum_{\substack{p,\text{premier}\\ p|n}}\frac{1}{p}\right)=n-M_k^{k-1}(p)$

On remarque que,

(41) :
$$\varphi(n)=\underbrace{n-M_k^{k-1}(p)}_{G(n)}+\underbrace{M_k^{k-2}(p)-..[]..+(-1)^kM_k^0(p)}_{r(n)}$$

Cette formule explique vraiment ce que se passe dans la somme de Giuga, en examinant un grand nombre des nombres de Carmichael, on remarque que $G(n)\approx\varphi(n)$, voir les tables dans les pages suivantes, mais les démonstrations ne seront jamais aisées.
Donc pour démontrer cette conjecture il faut surmonter les trois points suivants :

Le premier point il faut démontrer que $G(n)$ est un entier strictement positif, car si $G(n)$ est négative, alors en terme modulo (n) elle peut dépasser $\varphi(n)$, c'est le point le plus compliqué.

Le second point il faut démontrer que $r(n)$ est aussi un entier positif, ce qui n'est pas vraiment facile à cause de l'alternance des signes, mais il apparaît que ce point est vrais pour tout entier sans facteur carré, et non seulement pour les nombres de Carmichael, donc je peux imaginer une démonstration par récurrence à l'aide de la formule (39).

Le troisième point c'est tout ce que j'ai pu démontrer correctement, et on a,

(42) Théorème :

La fonction $\frac{G(n)}{\varphi(n)}$ croît en fonction de la croissance des facteurs premiers de n.

Preuve :

Posons $n = p_1 p_2 ..[]..p_k$, $n_0 = p_1 p_2 ..[]..p_{k-1} = n / p_k$ et $n' = n_0(p_k + N)$, avec N est un entier positive tel que $(p_k + N)$ est premier, on a,

$$G(n') = G(n) + NG(n_0)$$

&

$$\varphi(n') = \varphi(n) + N\varphi(n_0)$$

En effet,

$$\varphi(n') = \varphi(n_0)(p_k + N - 1) = \varphi(n_0)(p_k - 1) + N\varphi(n_0) = \varphi(n) + N\varphi(n_0)$$

De même,

$$G(n') = n_0(p_k + N)\left(1 - \frac{1}{p_k + N} - \sum_{j=1}^{k-1}\frac{1}{p_j}\right) = n_0(p_k + N)\left(1 - \sum_{j=1}^{k-1}\frac{1}{p_j}\right) - n_0$$

$$= n_0 p_k\left(1 - \sum_{j=1}^{k-1}\frac{1}{p_j}\right) - n_0 + Nn_0\left(1 - \sum_{j=1}^{k-1}\frac{1}{p_j}\right)$$

$$= n\left(1 - \sum_{j=1}^{k-1}\frac{1}{p_j}\right) - \frac{n}{p_k} + Nn_0\left(1 - \sum_{j=1}^{k-1}\frac{1}{p_j}\right)$$

$$= n\left(1 - \sum_{j=1}^{k}\frac{1}{p_j}\right) + Nn_0\left(1 - \sum_{j=1}^{k-1}\frac{1}{p_j}\right)$$

$$= G(n) + NG(n_0)$$

Dans un autre raisonnement il suffit de prouver que,

$$M_k^j\left(p, p_k \to p_k + N\right) = M_k^j(p) + NM_{k-1}^{j-1}(p)$$

Par exemple, $p_1p_2 + p_1(p_3 + N) + p_2(p_3 + N) = p_1p_2 + p_1p_3 + p_2p_3 + N(p_1 + p_2)$

Et le reste découle des formules précédentes.

Soit, $\Delta = \frac{G(n')}{\varphi(n')} - \frac{G(n)}{\varphi(n)}$ il suffit de prouver que $\Delta > 0$.

En effet,

$$\Delta = \frac{G(n) + NG(n_0)}{\varphi(n) + N\varphi(n_0)} - \frac{G(n)}{\varphi(n)}$$

$$= \frac{N\left(G(n_0)\varphi(n) - G(n)\varphi(n_0)\right)}{\varphi(n)\left(\varphi(n) + N\varphi(n_0)\right)}$$

$$= \frac{N\delta}{\varphi(n)\left(\varphi(n) + N\varphi(n_0)\right)}$$

Or,

$$G(n_0)\varphi(n) = G(n_0)\varphi(n_0)(p_k - 1) = p_k G(n_0)\varphi(n_0) - G(n_0)\varphi(n_0)$$

$$G(n)\varphi(n_0) = \left(p_k G(n_0) - n_0\right)\varphi(n_0) = p_k G(n_0)\varphi(n_0) - n_0\varphi(n_0)$$

Donc,

$$\delta = \varphi(n_0)\left(n_0 - G(n_0)\right) = \varphi(n_0)\left(\sum_{j=1}^{k-1}\frac{1}{p_j}\right) > 0\ .$$

C.Q.F.D

Bien sur que la démonstration de ces trois points, prouve que pour des grands nombres de Carmichael que l'on a $\frac{G(n)}{\varphi(n)} \approx 1$, ce qui prouvera la conjecture d'Agoh-Giuga.

n	$\varphi(n)$	G(n)	G(n)/φ(n)	$\varphi(n)$-G(n)
561	320	290	0,90625	30
1105	768	734	0,95572917	34
1729	1296	1258	0,97067901	38
2465	1792	1742	0,97209821	50
2821	2160	2110	0,97685185	50
6601	5280	5210	0,98674242	70
8911	7128	7036	0,98709315	92
10585	8064	7958	0,98685516	106
15841	12960	12850	0,99151235	110
29341	25920	25810	0,99575617	110
46657	41472	41326	0,99647955	146
52633	44064	43882	0,99586964	182
115921	103680	103390	0,99720293	290
1193221	1134000	1133278	0,99936332	722
1461241	1399680	1399030	0,99953561	650
4335241	4218240	4217510	0,99982694	730
5968873	5778864	5777602	0,99978162	1262
14913991	14447160	14444260	0,99979927	2900
15247621	14904000	14902378	0,99989117	1622
17098369	16859136	16858238	0,99994674	898
17316001	16872960	16870670	0,99986428	2290
60957361	59616000	59610238	0,99990335	5762
362569201	358256640	358246670	0,99997217	9970

Nombres de Carmichael à 5 facteurs

n	φ(n)	G(n)	G(n)/φ(n)	φ(n)-G(n)
41041	28800	27289	0,94753472	1511
62745	32384	27241	0,84118701	5143
63973	46656	44817	0,96058385	1839
75361	57600	55849	0,96960069	1751
101101	72000	68689	0,95401389	3311
126217	93312	90105	0,96563143	3207
172081	129600	125889	0,97136574	3711
188461	139968	135393	0,96731396	4575
278545	200704	194381	0,96849589	6323
340561	278784	274441	0,98442163	4343
449065	326592	317377	0,97178437	9215
552721	460800	455149	0,98773655	5651
656601	392000	368209	0,93930867	23791
658801	518400	507049	0,97810378	11351
670033	513216	501297	0,97677586	11919
748657	559872	542985	0,96983775	16887
838201	648000	634689	0,97945833	13311
852841	720000	713017	0,99030139	6983
1033669	793152	775185	0,97734734	17967
1082809	839808	823353	0,98040624	16455
2100901	1800000	1786897	0,99272056	13103
4909177	3825792	3756345	0,98184768	69447

Nombres de Carmichael à 4 facteurs

n	φ (n)	G(n)	G(n)/φ(n)	φ (n)-G(n)
825265	497664	439032	0,88218557	58632
101957401	75582720	73059152	0,96661184	2523568
1150270849	859963392	833932328	0,96973003	26031064
7103660473	5275673856	5103179888	0,9673039	172493968

Nombres de Carmichael à 5 facteurs

n	φ (n)	G(n)	G(n)/φ(n)	φ (n)-G(n)
321197185	217147392	203986263	0,9393908	13161129
1039531253629140.	770621761612800.	744892089514231.	0.9666118	

Nombres de Carmichael à 6 facteurs

x	n(x)	G(n)/φ(n)
2136	599966117492747584686619009.	0.999999999647689
4071	150875671216807248448957308 49.	0.9999999999030105
9000	796750146168243628351543056001.	0.9999999999801554
17655	231444334701866331423837090139 21.	0.9999999999948431
18315	278062547897895063235650956145 61.	0.999999999995208
21381	602903370730071866771301416954 89.	0.9999999999964838
29616	307425052006295621588527279504129.	0.9999999999981674
49920	418292148787139675392401820858 3681.	0.999999999999355
62205	125670453205130411676001867054 29121.	0.9999999999995846
95910	109502993576342388768285915706763041.	0.9999999999998253
111885	236573351628229522348274676488749441.	0.9999999999998715

Nombres de Carmichael sous forme de,
n(x)=(28x+1)(56x+1)(112x+1)(196x+1)(392x+1).

Note :

Les valeurs de $G(n)$ pour les deux premières tables sont calculer on sommant par Maxima de la manière suivante :

```
(%i7)  n:561$
       mod(sum(i^(n-1),i,1,n-1),n);
(%o7)  290
```

Et aussi par la formule (37).

Une dernière curiosité

Il s'agit de prouver que pour tout entier n strictement positive, et pour tout entier a que l'on a,

$$a^{\lambda(n)} \equiv a^{\phi(n)} Modulo(n)$$

Où $\lambda(n)$ et $\varphi(n)$ représentent respectivement l'indicatrice de Carmichael, et l'indicatrice d'Euler.

Si $(a,n)=1$ alors $a^{\lambda(n)} \equiv a^{\phi(n)} \equiv 1\, Modulo(n)$, seule le cas où $(a,n)\neq 1$ qui pose le problème, alors je me demande si quelqu'un peut démontrer cette proposition.

Biographie

- Giuga's conjecture on primality, D. Borwein, J. M. Borwein, P. B. Borwein, R. Girgensohn.
- The Equivalence of Giuga's and Agoh's Conjectures, Bernd C. Kellner 2003.
- ON FERMAT'S SIMPLE THEOREM, Jack CHERNICK.
- Autour des nombres et des polynômes de Bernoulli, Gaëtan Bisson.
- https://fr.m.wikipedia.org/wiki/Indicatrice_de_Carmichael.
- https://fr.m.wikipedia.org/wiki/Nombre_de_Carmichael.