COLLOQUIUM MATHEMATICUM
VOL. LXV 1993 FASC. 2

PROPRIÉTÉS ARITHMÉTIQUES DE CERTAINS NOMBRES EULÉRIENS

PAR

JEAN-LOUIS NICOLAS (LYON)

1. Introduction. Le nombre Eulérien $A(n,k)$ dépend de deux paramètres entiers $n \geq 1$ et k, $1 \leq k \leq n$. On peut le définir à l'aide de la relation de récurrence triangulaire

$$A(n,k) = kA(n-1,k) + (n-k+1)A(n-1,k-1) \tag{1}$$

valable pour $n \geq 2$, et des conditions initiales

$$A(n,1) = A(n,n) = 1, \qquad n \geq 1\,.$$

Il est commode de poser, comme pour les coefficients du binôme, pour $n \geq 1$, $A(n,k) = 0$ pour $k \in \mathbb{Z}$, $k \leq 0$ ou $k \geq n+1$ et alors la relation (1) est valable pour tout $k \in \mathbb{Z}$. Les nombres Eulériens vérifient la relation de symétrie

$$A(n,k) = A(n,n-k+1) \tag{2}$$

et pour n fixé, la suite $A(n,k)$ est croissante en k, pour $k \leq \lfloor (n+1)/2 \rfloor$, puis décroissante en k, pour $k \geq \lfloor (n+1)/2 \rfloor$, où $\lfloor x \rfloor$ désigne la partie entière de x. Nous poserons

$$M_n = \max_k A(n,k)\,.$$

Lorsque $n = 2m$, ce maximum est atteint deux fois :

$$M_{2m} = A(2m,m) = A(2m,m+1)\,.$$

Lorsque n est impair, il n'est atteint qu'une seule fois :

$$M_{2m+1} = A(2m+1,m+1)\,,$$

et la relation (1) donne

$$M_{2m+1} = (2m+2)M_{2m}, \qquad m \geq 1\,. \tag{3}$$

On pourra trouver les définitions et propriétés ci-dessus dans les œuvres d'Euler ([Eul], p. 373) ou dans [Com] ou [Knu]. Dans les articles [Nic] et [L-N2], des représentations intégrales de $A(n,k)$ permettent d'étendre la définition de $A(n,k)$ lorsque n et k sont réels.

Dans [L-N1], le maximum M_n a été étudié; un développement asymptotique et différentes inégalités ont été présentées. De plus, une table de M_n pour $n \le 50$ est donnée. La lecture de cette table montre que M_n se termine fréquemment par 0, et laisse conjecturer que les valeurs de M_n ne sont pas équiréparties modulo 10.

Compte tenu de (3), il suffit d'étudier les congruences vérifiées par M_n lorsque n est pair. Nous démontrerons les théorèmes suivants.

THÉORÈME 1.1. *Soit p un nombre premier, et $\alpha \ge 1$ un nombre entier. Il existe des nombres entiers a_r dépendant de m, p, et α tels que l'on ait*

$$M_{2m} \equiv \sum_{r=0}^{(\alpha p^\alpha - 1)/2} a_r \cdot \frac{1}{2}\binom{2m-2r}{m-r} \bmod p^\alpha$$

pour m vérifiant $2m \ge \alpha p^\alpha - 1$.

THÉORÈME 1.2. 1. *M_n est pair pour tout $n \ge 1$, sauf lorsque $n = 2^k$, $k = 0, 1, 2, \ldots$*

2. *Soit p un nombre premier impair et $m \ge 1$. Soit*

$$m = \sum_{i=0}^{I} m_i p^i$$

son écriture en base p. S'il existe un chiffre m_i, $1 \le i \le I$, vérifiant $m_i \ge (p+1)/2$, alors $M_{2m} \equiv 0 \bmod p$.

3. *Si tous les chiffres m_i, $1 \le i \le I$, vérifient $m_i \le (p-1)/2$, et $m_0 = 0$, alors $M_{2m} \not\equiv 0 \bmod p$.*

4. *Soit p un nombre premier ≥ 2, et $\alpha \ge 1$. Soit β tel que $\alpha \le p^\beta$. Si $m_{\alpha+\beta} \ge 1$, et si parmi les chiffres m_i avec $i \ge \alpha + \beta + 1$, il y en a au moins α tels que $m_i \ge (p+1)/2$, alors $M_{2m} \equiv 0 \bmod p^\alpha$.*

La démonstration du théorème 1.2 repose sur celle du théorème 1.1, et sur les propriétés de congruences des coefficients binômiaux $\binom{2m-2r}{m-r}$ (cf., ci-dessous, lemme 2.2).

La démonstration du théorème 1.1 est basée sur la formule suivante, due à Worpitzky (cf. [Wor]) :

$$A(n,k) = \sum_{0 \le j \le k} (-1)^j \binom{n+1}{j} (k-j)^n \,,$$

qui donne

$$M_{2m} = A(2m, m) = \sum_{0 \le j \le m} (-1)^j \binom{2m+1}{j} (m-j)^{2m} \,, \tag{4}$$

et sur les propriétés arithmétiques des sommes

$$S(n,k,l) = \sum_{\substack{0\le j\le n\\ j\equiv l \bmod k}} (-1)^j \binom{n}{j} \tag{5}$$

et

$$\sigma(n,k,l) = \sum_{\substack{0\le j\le n/2\\ j\equiv l \bmod k}} (-1)^j \binom{n}{j}. \tag{6}$$

Dans le §2, nous donnons la preuve de certains lemmes généraux, dans le §3, nous démontrons les théorèmes 1.1 et 1.2, et les §4 et §5 étudient plus précisément le cas des congruences mod 8 et mod 3 vérifiées par M_n. Ces propriétés ont été vérifiées par ordinateur pour $n \le 200$.

Dans [C-R], Carlitz et Riordan ont démontré que, pour p premier et k fixé, $p^{i-1} < k \le p^i$, les nombres $A(n,k)$ vérifiaient, pour $n \ge e$,

$$A(n + p^{i+e-1}(p-1), k) \equiv A(n,k) \bmod p^e .$$

Mais, à part ce résultat, nous ne connaissons pas d'autres congruences vérifiées par les nombres Eulériens.

J'ai plaisir à remercier P. Erdős et A. Schinzel pour les discussions que nous avons eues sur ce sujet, L. Lesieur qui a attiré mon attention sur les nombres Eulériens, et plus spécialement sur les nombres M_n, et les collègues de l'Université Nicolas Copernic de Toruń, Pologne, qui m'ont accueilli en octobre 1992 : c'est pendant ce séjour que la plus grande partie de ce travail a été effectuée.

2. Quelques lemmes

LEMME 2.1 (Théorème de Lucas). *Soit p un nombre premier, et deux nombres entiers n et k qui s'écrivent en base p :*

$$n = \sum_{i=0}^{I} n_i p^i, \quad 0 \le n_i < p, \qquad k = \sum_{i=0}^{I} k_i p^i, \quad 0 \le k_i < p .$$

Alors on a la congruence pour le coefficient du binôme :

$$\binom{n}{k} \equiv \prod_{i=0}^{I} \binom{n_i}{k_i} \bmod p$$

avec les conventions habituelles $\binom{n_i}{k_i} = 0$ si $k_i > n_i$ et $\binom{0}{0} = 1$.

Démonstration : cf. [Luc], p. 417, ou [Ber], p. 113.

LEMME 2.2. *Soit p un nombre premier. On désigne par $v_p(n)$ la valuation p-adique de l'entier n, c'est-à-dire le plus grand exposant α tel que p^α*

divise n. Soit $m \in \mathbb{N}$, et son écriture en base p :

$$m = \sum_{i=0}^{I} m_i p^i, \qquad 0 \le m_i < p\,.$$

Alors on a :

1. $v_p\big(\binom{2m}{m}\big) = 0$ *si et seulement si* $m_i \le (p-1)/2$, $0 \le i \le I$.

2. $v_p\big(\binom{2m}{m}\big) \ge \sum_{i=0}^{I} \lfloor 2m_i/(p+1) \rfloor$ (*cette somme compte le nombre de chiffres m_i qui sont $\ge (p+1)/2$*).

3. *Lorsque $p = 2$, l'inégalité ci-dessus est une égalité : c'est-à-dire, $v_p\big(\binom{2m}{m}\big)$ est exactement égal au nombre de chiffres* 1 *dans le développement binaire de m.*

4. *Lorsque $p \ge 3$, on pose*

   (a) $\omega_i = 0$ *si* $m_i \le (p-1)/2$,

   (b) $\omega_i = 1$ *si* $m_i \ge (p+1)/2$ *et* $m_{i-1} < (p-1)/2$,

   (c) $\omega_i = t \ge 2$ *si* $m_i \ge (p+1)/2$, *et si* $m_{i+1} = m_{i+2} = \ldots = m_{i+t-1} = (p-1)/2$.

Alors,

$$v_p\left(\binom{2m}{m}\right) = \sum_{i=0}^{I} \omega_i\,.$$

D é m o n s t r a t i o n. Comme $\binom{2m}{m} = 2m!/m!^2$, on a

$$\alpha = v_p\left(\binom{2m}{m}\right) = \sum_{j=1}^{\infty} (\lfloor 2mp^{-j} \rfloor - 2\lfloor mp^{-j} \rfloor)\,.$$

Or la fonction $x \mapsto \lfloor 2x \rfloor - 2\lfloor x \rfloor$ vaut 0 ou 1 suivant que $\{x\}$, la partie fractionnaire de x, est $< 1/2$ ou $\ge 1/2$. Ici,

$$\{mp^{-j}\} = m_{j-1}p^{-1} + m_{j-2}p^{-2} + \ldots + m_0 p^{-j}\,. \tag{7}$$

Si tous les chiffres m_i sont $\le (p-1)/2$, on a

$$\{mp^{-j}\} < \frac{p-1}{2}\frac{1}{p-1} = 1/2\,,$$

et cela démontre le point 1.

Si $m_{j-1} \ge (p+1)/2$, alors $mp^{-j} \ge (p+1)/2p > 1/2$, et cela démontre le point 2.

Lorsque $p = 2$, la condition nécessaire et suffisante pour que le membre de droite de (7) soit $\ge 1/2$ est $m_{j-1} = 1$, et cela démontre le point 3.

Lorsque $p > 2$, le membre de droite de (7) peut être $\ge 1/2$ lorsque $m_{j-1} < (p+1)/2$, mais seulement dans le cas suivant : il existe $k \ge 1$ avec

$$m_{j-1} = m_{j-2} = \ldots = m_{j-k} = (p-1)/2$$

et $m_{j-k-1} \ge (p+1)/2$, et cela achève la démonstration du lemme.

Tout entier n peut s'écrire $n = 2^s t$, avec t impair. On définit la partie impair de n :

$$\mathrm{imp}(n) = t\,.$$

LEMME 2.3. *Soit $n \in \mathbb{N}$, et son écriture en base 2 :*

$$n = \sum_{i=0}^{\infty} n_i 2^i\,;$$

alors

$$\mathrm{imp}(n!) \equiv (-1)^{\Sigma_{i=0}^{\infty} \lfloor (n_i + 2n_{i+1} + 4n_{i+2} + 3)/4 \rfloor \bmod 4} \tag{8}$$

et

$$\mathrm{imp}(2^k!) \equiv 3 \bmod 8 \qquad \textit{pour tout } k \geq 2\,. \tag{9}$$

Démonstration. Définissons d'abord

$$f_\alpha(n) = \prod_{\substack{k \leq n \\ k \equiv 2^\alpha \bmod 2^{\alpha+1}}} k\,.$$

Pour $\alpha = 0$, $f_0(n)$ est le produit des nombres impairs $\leq n$, et $f_0(n) \bmod 4$ est une fonction périodique de n, de période 8. Il est facile de voir que

$$\begin{aligned} f_0(n) &\equiv (-1)^{\lfloor (n+3)/4 \rfloor \bmod 4} \\ &\equiv (-1)^{\lfloor (n_0 + 2n_1 + 4n_2 + 3)/4 \rfloor \bmod 4}\,. \end{aligned}$$

Ensuite $\mathrm{imp}(f_1(n)) = f_0(\lfloor n/2 \rfloor)$ et donc

$$\mathrm{imp}(f_1(n)) \equiv (-1)^{\lfloor (n_1 + 2n_2 + 4n_3 + 3)/4 \rfloor \bmod 4}\,.$$

De façon similaire, on a

$$\mathrm{imp}(f_\alpha(n)) \equiv (-1)^{\lfloor (n_\alpha + 2n_{\alpha+1} + 4n_{\alpha+2} + 3)/4 \rfloor \bmod 4}$$

et (8) résulte alors des formules

$$n! = f_0(n) f_1(n) \dots f_\alpha(n) \dots \tag{10}$$

et

$$\mathrm{imp}(n!) = \mathrm{imp}(f_0(n))\,\mathrm{imp}(f_1(n)) \dots \mathrm{imp}(f_\alpha(n)) \dots$$

Pour démontrer (9), nous observons d'abord que

$$\mathrm{imp}(2^k!) = f_0(2^k) f_0(2^{k-1}) f_0(2^{k-2}) \dots f_0(8) f_0(4) f_0(2)\,.$$

Mais, pour tout a entier,

$$(8a+1)(8a+3)(8a+5)(8a+7) \equiv 1 \cdot 3 \cdot 5 \cdot 7 \equiv 1 \bmod 8$$

et donc, pour $k \geq 2$,

$$\mathrm{imp}(2^k!) \equiv f_0(4) f_0(2) \equiv 3 \bmod 8\,.$$

LEMME 2.4. *Soit*

$$S(n,k,l) = \sum_{j \equiv l \bmod k} (-1)^j \binom{n}{j},$$

p un nombre premier, et $\alpha \geq 1$ un nombre entier. Alors

$$S(n,p^\alpha,l) \equiv 0 \bmod p^r \tag{11}$$

pour tout $l \in \mathbb{Z}$ et $n \geq rp^\alpha$.

Démonstration. En utilisant la relation $\binom{n}{j} = \binom{n-1}{j} + \binom{n-1}{j-1}$ on observe d'abord que, pour $n \geq 1$,

$$S(n,k,l) = S(n-1,k,l) - S(n-1,k,l-1)\,. \tag{12}$$

En itérant la relation (12) on obtient

$$S(n,p^\alpha,l) = \sum_{j=0}^{p^\alpha} (-1)^j S(n-p^\alpha, p^\alpha, l-j) \binom{p^\alpha}{j}. \tag{13}$$

Mais dans la somme ci-dessus le terme en $j=0$ et celui en $j=p^\alpha$ s'annulent, car $S(n,k,l) = S(n,k,l-k)$. Par ailleurs, par le lemme 2.1, $\binom{p^\alpha}{j}$ est multiple de p, pour $1 \leq j \leq p^\alpha - 1$. On voit donc que pour $n \geq p^\alpha$, $S(n,p^\alpha,l)$ est multiple de p, et par récurrence, la formule (13) démontre (11).

Remarque. A. Schinzel a observé qu'en calculant la somme $S(n,k,l)$ à partir des racines k-ièmes de l'unité, on peut démontrer que

$$v_p(S(n,k,l)) \geq \lceil n/\varphi(p^\alpha) \rceil - \alpha$$

où φ désigne la fonction d'Euler, et $\lceil x \rceil = \min_{n \geq x} n$ désigne le plafond de x. Ce résultat améliore le lemme 2.4 pour $n > \alpha p^\alpha (p-1)$.

LEMME 2.5. *On définit*

$$\sigma(n,k,l) = \sum_{\substack{0 \leq j \leq n/2 \\ j \equiv l \bmod k}} (-1)^j \binom{n}{j}$$

et

$$\chi(n,k,l) = \begin{cases} 1 & \text{si } n \equiv l \bmod k, \\ 0 & \text{si } n \not\equiv l \bmod k. \end{cases}$$

Alors on a, pour $n \geq 1$,

$$\sigma(n,k,l) = \sigma(n-1,k,l) - \sigma(n-1,k,l-1) + a(n,k,l)$$

avec

$$a(n,k,l) = (-1)^{n/2} \cdot \frac{1}{2} \binom{n}{n/2} \chi(n/2,k,l)$$

si n est pair et

$$a(n,k,l) = (-1)^{(n-1)/2}\binom{n-1}{(n-1)/2}\chi((n-1)/2,k,l-1)$$

si n est impair.

D é m o n s t r a t i o n. On écrit $\sigma(n,k,l) = S_1 + S_2$ avec

$$S_1 = \sum_{\substack{0\le j\le n/2\\ j\equiv l \bmod k}} (-1)^j\binom{n-1}{j} \quad\text{et}\quad S_2 = \sum_{\substack{0\le j\le n/2\\ j\equiv l \bmod k}} (-1)^j\binom{n-1}{j-1}.$$

Or S_1 est très voisin de $\sigma(n-1,k,l)$. En fait, si n est pair,

$$S_1 = \sigma(n-1,k,l) + (-1)^{n/2}\binom{n-1}{n/2}\chi(n/2,k,l)\,,$$

et si n est impair, $S_1 = \sigma(n-1,k,l)$. Quant à S_2, on a

$$S_2 = \sum_{\substack{-1\le i\le n/2-1\\ i\equiv l-1 \bmod k}} -(-1)^i\binom{n-1}{i}$$

et l'on a $S_2 = -\sigma(n-1,k,l-1)$ si n est pair, et

$$\begin{aligned} S_2 = {} & -\sigma(n-1,k,l-1)\\ & + (-1)^{(n-1)/2}\binom{n-1}{(n-1)/2}\chi\left(\frac{n-1}{2},k,l-1\right)\end{aligned}$$

si n est impair, ce qui achève la preuve du lemme 2.5.

3. Démonstration des théorèmes 1.1 et 1.2. En itérant αp^α fois la formule du lemme 2.5, avec $k = p^\alpha$, on obtient

$$\begin{aligned}\sigma(n,p^\alpha,l) = {} & \sum_{t=0}^{\alpha p^\alpha}\sigma(n-\alpha p^\alpha,p^\alpha,l-t)(-1)^t\binom{\alpha p^\alpha}{t}\\ & + \sum_{i=0}^{\alpha p^\alpha-1}\sum_{t=0}^{i}(-1)^t\binom{i}{t}a(n-i,p^\alpha,l-t)\,.\end{aligned}$$

Or, dans la première somme, on peut regrouper les termes suivant la valeur de $l-t \bmod p^\alpha$: On obtient

$$\sum_{s=0}^{p^\alpha-1}\sigma(n-\alpha p^\alpha,p^\alpha,l-s)S(\alpha p^\alpha,p^\alpha,s)$$

où $S(n,k,l)$ a été défini dans le lemme 2.4. Par application de ce même

lemme, la somme ci-dessus est nulle modp^α, et l'on a

$$\sigma(n,p^\alpha,l) \equiv \sum_{i=0}^{\alpha p^\alpha-1}\sum_{t=0}^{i}(-1)^t\binom{i}{t}a(n-i,p^\alpha,l-t) \bmod p^\alpha\,. \tag{14}$$

Il vient ensuite, par (4),

$$\begin{aligned} M_{2m} &= \sum_{0\le j\le m}(-1)^j\binom{2m+1}{j}(m-j)^{2m}\\ &\equiv \sum_{s \bmod p^\alpha} s^{2m}\sigma(2m+1,p^\alpha,m-s) \bmod p^\alpha \end{aligned}$$

où la somme ci-dessus porte sur une famille de résidus s modulo p^α. Par application de (14), on a

$$M_{2m} \equiv \sum_{s \bmod p^\alpha} s^{2m}\sum_{i=0}^{\alpha p^{\alpha-1}}\sum_{t=0}^{i}(-1)^t\binom{i}{t}a(2m+1-i,p^\alpha,m-s-t)\,.$$

On permute les sommations, et on distingue dans la somme en i les termes pairs ($i=2r$) et les termes impairs ($i=2r+1$) :

$$\begin{aligned} M_{2m} \equiv{}& \sum_{r=0}^{(\alpha p^\alpha-1)/2}\sum_{t=0}^{2r}(-1)^t\binom{2r}{t}\sum_{s \bmod p^\alpha} s^{2m}(-1)^{m-r}\\ &\times\binom{2m-2r}{m-r}\chi(m-r,p^\alpha,m-s-t-1)\\ &+\sum_{r=0}^{(\alpha p^\alpha-2)/2}\sum_{t=0}^{2r+1}(-1)^t\binom{2r+1}{t}\sum_{s \bmod p^\alpha} s^{2m}(-1)^{m-r}\\ &\times\frac12\binom{2m-2r}{m-r}\chi(m-r,p^\alpha,m-s-t)\,. \end{aligned}$$

Mais dans les sommes en s mod p^α, la fonction χ est presque toujours nulle. Elle vaut 1 si et seulement si, lorsque i est pair,

$$m-r \equiv m-s-t-1 \bmod p^\alpha$$

soit $s \equiv r-t-1 \bmod p^\alpha$, et similairement $s \equiv r-t \bmod p^\alpha$ lorsque i est impair. On obtient alors

$$\begin{aligned} (-1)^m M_{2m} \equiv{}& \sum_{r=0}^{(\alpha p^\alpha-1)/2}(-1)^r\binom{2m-2r}{m-r}A_r\\ &+\sum_{r=0}^{(\alpha p^\alpha-2)/2}(-1)^r\cdot\frac12\binom{2m-2r}{m-r}B_r \end{aligned} \tag{15}$$

avec

$$A_r = \sum_{t=0}^{2r} (-1)^t \binom{2r}{t} (t-r+1)^{2m} \tag{16}$$

et

$$B_r = \sum_{t=0}^{2r+1} (-1)^t \binom{2r+1}{t} (t-r)^{2m}\,, \tag{17}$$

et (15)–(17) prouvent le théorème 1.1.

Pour les premières valeurs de r, les formules (16) et (17) donnent

$A_0{=}1$, $B_0{=}-1$,
$A_1{=}-2+2^{2m}$, $B_1{=}4-2^{2m}$,
$A_2{=}7-4\cdot 2^{2m}+3\cdot 2^{2m}$, $B_2{=}-15+6\cdot 2^{2m}-3^{2m}$,
$A_3{=}-26+16\cdot 2^{2m}-6\cdot 3^{2m}+4\cdot 2^{2m}$, $B_3{=}56-28\cdot 2^{2m}+8\cdot 3^{2m}-4^{2m}$.

Lorsque $p=2$, la formule (15) donne

$$M_{2m} \equiv \left(A_0 + \frac{1}{2}B_0\right)\binom{2m}{m} \bmod 2\,,$$

soit

$$M_{2m} \equiv \frac{1}{2}\binom{2m}{m} \bmod 2\,.$$

En vertu du lemme 2.2, M_{2m} est pair, sauf pour les m qui s'écrivent en base 2 avec un seul chiffre 1, soit $m=2^k$, $k\geq 1$. Par (3), M_{2m+1} est toujours pair, sauf $M_1=1$, et cela prouve le point 1 du théorème 1.2.

Si p est impair, et s'il existe m_i avec $i\geq 1$ et $m_i \geq (p+1)/2$, les nombres $m-1, m-2, \ldots, m-(p-1)/2$ s'écrivent tous avec au moins un chiffre $\geq (p+1)/2$. Alors on a bien $M_{2m}\equiv 0 \bmod p$, par le théorème 1.1 et le lemme 2.2, et cela prouve le point 2.

Avec les hypothèses du point 3, on note que $m-1, m-2, \ldots, m-(p-1)/2$ vont avoir leur dernier chiffre en base p qui est $\geq (p+1)/2$. Par le théorème 1.1 et le lemme 2.5, on a donc, pour un tel m,

$$(-1)^m M_{2m} \equiv \left(A_0 + \frac{1}{2}B_0\right)\binom{2m}{m} \equiv \frac{1}{2}\binom{2m}{m} \bmod p\,,$$

et par le lemme 2.5, ceci est $\not\equiv 0 \bmod p$.

Si, avec les mêmes hypothèses sur les chiffres m_i pour $i\geq 1$, on regarde ce qui se passe pour $m_0=1$, lorsque $p\geq 5$, on a

$$(-1)^m M_{2m} \equiv \frac{1}{2}\binom{2m}{m} - \frac{1}{2}\binom{2m-2}{m-1}2^{2m} \bmod p\,.$$

Posons

$$\mu = \prod_{i=1}^{I} \binom{2m_i}{m_i} \not\equiv 0 \bmod p\,.$$

On a, par le lemme 2.1,

$$\binom{2m}{m} \equiv \mu\binom{2}{1} = 2\mu, \qquad \binom{2m-2}{m-1} \equiv \mu\binom{0}{0} = \mu$$

et

$$(-1)^m M_{2m} \equiv \mu(1 - 2^{2m-1}) \bmod p\,.$$

Si l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$ est impair, alors pour certaines valeurs de m, $M_{2m} \equiv 0 \bmod p$.

La démonstration du point 4 est semblable à celle du point 3 : elle utilise le théorème 1.1 et le lemme 2.2. Notons qu'il est possible de construire une infinité de m tel que M_{2m} soit divisible par p^α et pas par $p^{\alpha+1}$: choisir par exemple $m_{\alpha+\beta+1} = 1$, $m_i = 0$ pour $0 \le i \le \alpha+\beta$ et tous les chiffres m_i, $i \ge \alpha+\beta+2$, inférieurs à $(p-3)/2$ sauf exactement α parmi eux qui sont tous $\ge (p+1)/2$.

Soit $N_p(x)$ le nombre de $n \le x$ tels que $M_n \not\equiv 0 \bmod p$ lorsque p est impair. On déduit du théorème 1.2 que

$$\left(\frac{p+1}{2}\right)^{k-1} p - 1$$

nombres m, $1 \le m < p^k$, s'écrivent avec $m_i \le (p-1)/2$ pour $i \ge 1$ et m_0 quelconque. On a donc

$$\mathrm{Card}\{n : n \text{ pair}, n < 2p^k, M_n \equiv 0 \bmod p\} \le \left(\frac{p+1}{2}\right)^{k-1} p - 1\,.$$

Les mêmes nombres, mais avec $m_0 \ne p-1$, et incluant $m = 0$, vont donner

$$\mathrm{Card}\{n : n \text{ impair}, n < 2p^k, M_n \not\equiv 0 \bmod p\} \le \left(\frac{p+1}{2}\right)^{k-1} (p-1)\,,$$

d'où l'on déduit

$$N_p(2p^k) \le \left(\frac{p+1}{2}\right)^{k-1} (2p-1)\,.$$

En choisissant dans les deux cas $m_0 = 0$, on a la minoration

$$N_p(2p^k) \ge 2\left(\frac{p+1}{2}\right)^{k-1} - 1\,.$$

4. Les congruences mod 8**.** Dans ce cas, la relation (15) se réduit à

$$M_{2m} \equiv \frac{(-1)^m}{2}\binom{2m}{m} \bmod 8\,. \tag{18}$$

En effet, les carrés modulo 8 sont 0 et 1. On peut alors soit refaire le calcul du §3, soit déduire (18) de (15)–(17). Avec la notation (5), on a, pour $r \geq 1$,

$$A_r \equiv \sum_{\substack{t=0 \\ t\equiv r \bmod 2}}^{2r} (-1)^t \binom{2r}{t} \equiv S(2r,2,r) \bmod 8\,,$$

et il est facile de voir que

$$S(2r,2,r) = (-1)^r 2^{2r-1}\,.$$

De même

$$B_r \equiv (-1)^{r+1} 2^{2r} \bmod 8\,.$$

On a donc $A_r + \frac{1}{2}B_r \equiv 0 \bmod 8$, pour $r \geq 1$, et (15) devient (18).

PROPOSITION 4.1. *Soit $n \geq 8$ et $s(n)$ la somme des chiffres de n en base* 2*. Alors* :

1. *Si* $s(n) \geq 4$, $M_n \equiv 0 \bmod 8$.
2. *Si* $s(n) = 1$, $M_n \equiv 3 \bmod 8$.
3. *Si* $s(n) = 2$,
   (a) *si* $n = 3 \cdot 2^k$, *ou si* $n = 2^k + 1$, *alors* $M_n \equiv 6 \bmod 8$,
   (b) *dans les autres cas*, $M_n \equiv 2 \bmod 8$.
4. *Si* $s(n) = 3$,
   (a) *si* $n \not\equiv 3 \bmod 4$, $M_n \equiv 4 \bmod 8$,
   (b) *si* $n \equiv 3 \bmod 4$, $M_n \equiv 0 \bmod 8$.

Démonstration. Lorsque $s(n) = 4$, le résultat provient de (18) et du lemme 2.2 lorsque n est pair, de (18), du lemme 2.2, et de (3) lorsque n est impair.

Lorsque $s(n) = 1$, et $n \geq 8$, n est pair, et $m = n/2$ aussi. Le résultat provient de (18), du lemme 2.2, et de (9). On a en effet

$$\mathrm{imp}((m!)^2) \equiv 1 \bmod 8$$

et donc

$$\mathrm{imp}\binom{2m}{m} \equiv \mathrm{imp}((2m)!) \bmod 8\,.$$

Lorsque $s(n) = 3$, et que n est pair, (18) et le lemme 2.2 montrent que $M_n \equiv 4 \bmod 8$.

Lorsque $s(n) = 3$, et que $n = 2m+1$, avec $s(m) = 2$, le lemme 2.2 et (18) donnent alors $M_{2m} \equiv 2 \bmod 4$. La relation (3) donne alors le résultat.

Lorsque $s(n) = 2$ et n impair, $n = 2m+1$, $s(m) = 1$ et donc $m = 2^k$, soit $M_{2m} \equiv 3 \bmod 8$. Par (3), il vient :

$$M_n = (2^{k+1}+2)M_{2m} \equiv 6 \bmod 8\,.$$

Lorsque $s(n) = 2$, et que n est pair, il résulte de (18) et du lemme 2.2 que

$$M_n = M_{2m} \equiv 2\left(\operatorname{imp}\left(\binom{2m}{m}\right) \bmod 4\right) \bmod 8\,.$$

Or

$$\operatorname{imp}\left(\binom{2m}{m}\right) \equiv \operatorname{imp}((2m)!) \bmod 4\,.$$

On applique alors le lemme 2.3, (8), et en considérant les places possibles du deuxième chiffre 1 de n, on achève la preuve de la proposition 4.1.

5. Les congruences mod 3**.** La formule (15) donne, avec $p = 3$ et $\alpha = 1$,

$$(-1)^m M_{2m} \equiv \left(A_0 + \frac{1}{2}B_0\right)\binom{2m}{m} - A_1\binom{2m-2}{m-1} \bmod 3\,,$$

soit

$$M_{2m} \equiv (-1)^{m+1}\binom{2m}{m} + (-1)^m\binom{2m-2}{m-1} \bmod 3\,. \tag{19}$$

Proposition 5.1. *Soit $m \geq 1$, et son écriture en base 3 :*

$$m = \sum_{i=0}^{I} m_i 3^i, \qquad 0 \leq m_i \leq 2\,.$$

1. *Pour que $M_{2m} \not\equiv 0 \bmod 3$, il faut et il suffit que tous les chiffres m_i pour $i \geq 1$ soient égaux à 0 ou 1.*
2. *Si $M_{2m} \not\equiv 0 \bmod 3$, alors*
   (a) *si $m \equiv 1 \bmod 3$, $M_{2m} \equiv 1 \bmod 3$,*
   (b) *si $m \equiv 0$ ou $2 \bmod 3$, $M_{2m} \equiv 2 \bmod 3$.*
3. *Si n est impair, $n = 2m+1$, pour que $M_n \not\equiv 0 \bmod 3$, il faut et il suffit que m s'écrive en base 3 sans utiliser le chiffre 2. Si $M_n \not\equiv 0 \bmod 3$, alors $M_n \equiv 1 \bmod 3$.*
4. *Les nombres n vérifiant $1 \leq n \leq 2\cdot 3^k - 1$ et $M_n \not\equiv 0 \bmod 3$ sont en nombre $5\cdot 2^{k-1} - 1$. Parmi eux $3\cdot 2^{k-1}$ vérifient $M_n \equiv 1 \bmod 3$ et $2^k - 1$ vérifient $M_n \equiv 2 \bmod 3$.*

Démonstration. Compte tenu du théorème 1.2, il suffit de montrer que si $m_i \leq 1$ pour $i \geq 1$ alors $M_{2m} \not\equiv 0 \bmod 3$. Si $m_0 = 2$, alors d'après le

lemme 2.1, $\binom{2m}{m} \equiv 0 \bmod 3$, mais m_1 s'écrit sans 2 en base 3, et par (19) et le lemme 2.1,

$$M_{2m} \equiv (-1)^{m+1}\binom{2m-2}{m-1} \not\equiv 0 \bmod 3\,.$$

Si $m_0 = 0$, de façon similaire, nous avons

$$M_{2m} \equiv (-1)^{m+1}\binom{2m}{m} \not\equiv 0 \bmod 3\,.$$

Si $m_0 = 1$, on pose

$$\mu = \prod_{i=1}^{I}\binom{2m_i}{m_i} \not\equiv 0 \bmod 3\,.$$

Par le lemme 2.1, on a

$$\binom{2m}{m} \equiv \mu\binom{2}{1} \equiv 2\mu \bmod 3\,,$$

$$\binom{2m-2}{m-1} \equiv \mu\binom{0}{0} \equiv \mu \bmod 3$$

et (19) donne alors

$$M_{2m} \equiv (-1)^{m+1}(2\mu - \mu) \not\equiv 0 \bmod 3\,,$$

et cela prouve le point 1.

Pour le point 2, supposons $m \equiv 1 \bmod 3$. Soit s le nombre de chiffres 1 dans l'écriture de m en base 3. On a

$$\binom{2m}{m} \equiv \prod_{i=0}^{I}\binom{2m_i}{m_i} \equiv (-1)^s \equiv (-1)^m \bmod 3$$

et

$$\binom{2m-2}{m-1} \equiv \prod_{i=1}^{I}\binom{2m_i}{m_i} \equiv (-1)^{m-1} \bmod 3\,,$$

d'où, par (19), $M_{2m} \equiv 1 \bmod 3$. Les cas $m \equiv 0$ ou $2 \bmod 3$ sont semblables.

Par (3), on a $M_{2m+1} \equiv 0 \bmod 3$ si $m \equiv 2 \bmod 3$ ou si $M_{2m} \equiv 0 \bmod 3$. Autrement dit, pour que $M_{2m+1} \not\equiv 0 \bmod 3$, on doit avoir $m_0 \le 1$, et $m_i \le 1$ pour $i \ge 1$, en utilisant le point 1. La dernière assertion du point 3 résulte du point 2 et de (3).

Enfin le point 4 résulte des points 2 et 3 : les 2^k nombres m qui s'écrivent avec k chiffres 0 ou 1 vont engendrer 2^k nombres impairs $n = m+1 \le 2\cdot 3^k - 1$, et vérifiant $M_n \equiv 1 \bmod 3$.

Les $3 \cdot 2^{k-1}$ nombres m vérifiant $m_i \le 1$ pour $i \ge 1$ vont engendrer les nombres $n = 2m$ tels que $M_n \not\equiv 0 \bmod 3$. D'après le point 2 ils se partagent

en 2 classes : 2^{k-1} nombres m vérifient $m \equiv 1 \bmod 3$, et les autres vérifient $m \equiv 0$ ou $2 \bmod 3$. Enfin il faut enlever dans cette dernière classe $m = 0$.

REFERENCES

[Ber] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, 1968.

[C-R] L. Carlitz and J. Riordan, *Congruences for Eulerian numbers*, Duke Math. J. 20 (1953), 339–343.

[Com] L. Comtet, *Analyse combinatoire*, tomes 1 et 2, Presses universitaires de France, Paris 1970.

[Eul] L. E. Euler, *Opera Omnia*, Series prima, *Institutiones calculi differentialis*, X, 1755, p. 373.

[Knu] D. E. Knuth, *The Art of Computer Programming*, Vol. 3, *Sorting and Searching*, Addison-Wesley, 1973, 34–47.

[L-N1] L. Lesieur et J.-L. Nicolas, *On the Eulerian numbers* $M_n = \max_{1 \le k \le n} A(n,k)$, European J. Combin. 13 (1992), 379–399.

[L-N2] —, —, *Double interpolation des nombres Eulériens*, à paraître.

[Luc] E. Lucas, *Théorie des nombres*, tome 1, Gauthier-Villars, Paris 1891, et A. Blanchard, Paris 1961.

[Nic] J.-L. Nicolas, *An integral representation for Eulerian numbers*, in: Sets, Graphs and Numbers, Budapest 1991, Colloq. Math. Soc. János Bolyai 60, 513–527.

[Wor] J. Worpitzky, *Studien über die Bernoullischen und Eulerschen Zahlen*, Crelle J. 94 (1883), 203–232.

DÉPARTEMENT DE MATHÉMATIQUES, BÂT. 101
UNIVERSITÉ CLAUDE BERNARD (LYON 1)
69622 VILLEURBANNE CEDEX, FRANCE
E-mail: jlnicola@frcpn11.bitnet

Reçu par la Rédaction le 17.2.1993