JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

F.-W. BURSTALL

Congruence se rapportant aux nombres de Bernoulli et d'Euler au module p^{i+1}

Journal de mathématiques pures et appliquées 7^e série, tome 3 (1917), p. 247-261.
<http://www.numdam.org/item?id=JMPA_1917_7_3__247_0>

Congruence se rapportant aux nombres de Bernoulli et d'Euler au module p^{i+1};

PAR F.-W. BURSTALL.

Au Volume 41 du *Journal de Crelle*, dans un article intitulé *Ueber eine allgemeine Eigenschaft der rationalen Entwickelungscoëfficienten einer bestimmten Gattung analytischen Functionen*, Kummer nous donne une congruence générale se rapportant aux nombres de Bernoulli et d'Euler, ces derniers étant appelés *coefficients sécants* et désignés par le symbole c_n.

Nous nous proposons, dans le présent article, de développer ces congruences et de leur donner des formes plus générales, à l'aide d'une nouvelle congruence qui traite des différences de zéro, attendu que ces différences se prêtent facilement à l'étude des fonctions périodiques dans la théorie des nombres.

Propriétés congruentes de $\Delta^r o^n$.

Le symbole $\Delta u_x = u_{x+1} - u_x$ a des propriétés bien connues lorsque u_x est une fonction entière rationnelle de x qui est de degré n. L'expression $\Delta^r o^n$ veut dire qu'on fait r fois l'opération Δ sur x^n, et qu'alors on fait x égal à zéro.

On a immédiatement d'après la définition

$$\Delta^r o^n = r\,\Delta^{r-1} o^{n-1} + r\,\Delta^r o^{n-1},$$

d'où il est facile de déduire que $\Delta^r o^n$ est divisible par $\lfloor r$ (1), pour r

(1) JEFFREY, *Quart. Journal*, vol. VII, p. 75.

plus grand que n,

$$\Delta^r 0^n = 0.$$

D'après sa définition, le symbole Δ obéit évidemment aux lois ordinaires de l'Algèbre, et pourvu qu'on l'emploie à opérer sur une fonction entière rationnelle de x, les résultats seront aussi strictement exacts que si l'on usait de toute autre méthode. Pour un traitement complet des méthodes symboliques, et pour la légitimité de leur emploi, nous pouvons nous en référer à Cesàro (¹).

Si comme de coutume nous écrivons

$$(1+x)^r = 1 + (r)_1 x + (r)_2 x^2 + \ldots + (r)_s x^s + \ldots$$

il s'ensuit que

$$\Delta^r 0^n = r^n - (r)_1 (r-1)^n + (r)_2 (r-2^n)^n + \ldots + (-1)^s (r-s)(r)_s + \ldots + (-1)^r (r)_{r-1} 1^n.$$

Le théorème de Fermat énonce que

$$r^{p-1} - 1 \equiv 0 \pmod{p},$$

tant que r et p sont premiers entre eux.

D'où, si i est un nombre entier,

$$r^{p^i(p-1)} - 1 \equiv 0 \pmod{p^{i+1}}.$$

Comme dans ce Mémoire on aura fréquemment l'occasion d'employer l'expression $p^i(p-1)$, nous la désignerons par un symbole unique

$$\nu = p^i(p-1).$$

Si maintenant nous écrivons $n = k\nu + l$, où l est plus petit que ν pour p plus grand que r puisque

$$\Delta^r 0^n \equiv r^l - (r)_1 (r-1)^l + \ldots + (-1)^{r-1} (r)_{r-1} 1^l \pmod{p^{i+1}},$$

il s'ensuit que

$$\Delta^r 0^n \equiv \Delta^r 0^l \pmod{p^{i+1}}.$$

Lorsque l est égal à zéro,

$$\Delta^r 0^n \equiv 1 - (r)_1 + (r)_2 + \ldots + (-1)^{r-1} (r)_{r-1},$$
$$\equiv (-1)^{r+1} \pmod{p^{i+1}}.$$

(¹) *Principes du calcul symbolique* (*Mathesis*, 1883, p. 10).

Si $i = 0$, comme $\Delta^r 0^n$ contient $\lfloor r$ en facteur

$$\Delta^r 0^n \equiv 0 \pmod{p}, \qquad r \geq p;$$
$$\Delta^r 0^n \equiv (-1)^{r+1} \pmod{p}, \qquad r < p.$$

Quand p est plus petit que r, les résidus prennent la forme de séries, et toutes les fois que r excède un multiple de p, une nouvelle série commence, si bien que le résultat devient compliqué.

Il est possible d'obtenir des résultats utiles par des méthodes plus simples.

Considérons la fonction

$$\Phi^r (ax+b)^m [(ax+b)^v - 1]^n,$$

dans laquelle Φ est un facteur de la forme

$$\Phi = \alpha_1 \Delta + \alpha_2 \Delta^2 + \ldots + \alpha_s \Delta^s,$$

les α_s étant des entiers; $v = p^r(p-1)$ dans cette expression, p est un nombre premier, a et b sont des nombres entiers, et en même temps a, b, p sont premiers entre eux, m et n sont des entiers positifs, x est une variable qui peut prendre n'importe quelle valeur entière, y compris zéro, après qu'on a fait l'opération Φ^r.

Φ^r se composera de termes de la forme $A_t \Delta^t$ et

$$\Delta^t (ax+b)^m [(ax+b)^v - 1]^m = (-1)^t \sum_{q=1}^{q=t} (t)_q \left[a\overline{x+q} + b\right]^m \left[(a\overline{x+q}+b)^v - 1\right]$$

tant que $a(x+q)+b$ et p sont premiers entre eux

$$(a\overline{x+q} - b)^v - 1 \equiv 0 \pmod{p^{i+1}}.$$

Lorsque $a\overline{x+q}$ et p cessent d'être premiers entre eux

$$(a\overline{x+q}+b)^m \equiv 0 \pmod{p^m},$$

c'est-à-dire

$$\Delta^t (ax+b)^m [(ax+b)^v - 1]^n \equiv 0 \pmod{p^{\overline{i+1}n}}.$$

Lorsque $m \geq \overline{i+1}n$, si $m = n$,

$$\Delta^t (ax+b)^m [(ax+b)^v - 1] \equiv 0 \pmod{p^{in}},$$

c'est-à-dire

$$\Phi^r (ax+b)^m [(ax+b)^v - 1]^n \equiv 0 \pmod{p^{i+1}}.$$

On remarque qu'on n'impose aucune restriction pour r et pour x, si bien que le théorème a un caractère très général. Il est même facile de le généraliser encore davantage. En effet, considérons une série dont les termes sont des puissances de Φ; la somme de ces séries aura la même propriété que chacun de ses termes, et il devient ainsi possible de supprimer la restriction qui veut que les α soient des entiers; ceci conduit aux fonctions de Bernoulli et d'Euler, mais il nous faut pour l'instant laisser de côté un examen détaillé de ces fonctions importantes.

Pour ce qui regarde le calcul des différences, ce théorème est, je crois, nouveau; on trouve cependant une formule semblable dans un Mémoire de Stern (1), mais il ne traite que d'un cas spécial. La notation non symbolique l'empêche, dans une large mesure, d'obtenir l'entière généralisation des résultats.

J'appellerai *complétement périodique* toute fonction de la forme

$$\Phi^r(ax+b)^m[(ax+b)^r-1]^n$$

avec une restriction pour m et n, mais sans restriction pour r. S'il y a une restriction pour r, j'appellerai la fonction *partiellement périodique*.

Les nombres de Bernoulli.

Par égard pour la symétrie, qui a une grande importance dans tout calcul symbolique, nous adopterons pour les nombres de Bernoulli la notation de Glaisher (2), à savoir

$$\frac{x}{e^x-1}=1+V_1\frac{x}{\lfloor 1}+V_2\frac{x^2}{\lfloor 2}+\ldots+V_n\frac{x^n}{\lfloor n}+\ldots,$$

où

$$V_{2n+1}=0, \qquad n>0, \qquad x<2\pi.$$

Cette notation a été employée pour la première fois par Blissard.

A l'aide de cette notation nous pouvons facilement déduire deux

---

(1) *Theorie der Eulerschen zahlen* (*Journ. de Crelle*, vol. 79, p. 67).

(2) *Quart. Journal*, vol. XXXI, p. 193.

formules pour les nombres de Bernoulli,

$$(2^{2n}-1)\frac{V_{2n}}{2n}=+\left[-\frac{\Delta}{2}+\frac{\Delta^2}{2^2}-\frac{\Delta^3}{2^3}-\ldots-\frac{\Delta^{2n-1}}{2^{2n}}\right]0^{2n-1},$$

$$V_{2n}=\left(-\frac{\Delta}{2}+\frac{\Delta^2}{3}-\frac{\Delta^3}{4}+\ldots+\frac{\Delta^{2n}}{2n+1}\right)0^{2n}.$$

La première de ces formules se prête aisément à déterminer les propriétés congruentes des nombres de Bernoulli, et il est assez curieux de voir que c'est la formule obtenue par Brinkley qui, le premier, fit usage de la notation de $\Delta^n 0^m$ (¹).

Nous pouvons maintenant appliquer le théorème directement à la première formule en écrivant les nombres de Bernoulli de la façon suivante :

$$2^r\left(-\frac{\Delta}{2}+\frac{\Delta^2}{2^2}+\ldots+(-1)^r\frac{\Delta^r}{2^r}\right)0^m(0^\nu-1)^n\equiv 0 \qquad (\bmod \overline{p^{i+1}n}),$$

$$m\geq n(i+1),$$

c'est-à-dire, si $r=m+n\nu$,

$$(2^{r+1}-1)\frac{V_{r+1}}{r+1}-(2^{r+1-\nu}-1)(n)_1\frac{V_{r+1-\nu}}{r+1-\nu}+\ldots+(-1)^n(2^{m+1}-1)\frac{V_{m+1}}{m+1}\equiv 0$$

$$(\bmod p^{i(n+1)}), \qquad m\geq(i+1)n.$$

Faisons $n=1$:

$$(2^{m+1+\nu}-1)\frac{V_{m+1+\nu}}{m+1+\nu}-(2^{m+1}-1)\frac{V_{m+1}}{m+1}\equiv 0 \qquad (\bmod p^{i+1}), \qquad m\geq i+1.$$

Tant que $m+1$ ne contient pas $p-1$ en facteur,

$$2^{m+1+\nu}-1\equiv 2^{m+1}-1 \qquad (\bmod p^{i+1});$$

d'où

$$\frac{V_{m+1+\nu}}{m+1+\nu}\equiv\frac{V_{m+1}}{m+1} \qquad (\bmod p^{i+1}), \qquad m\geq i+1, \qquad \nu=p^i(p-1),$$

$m+1$ n'étant pas un multiple de $p-1$ (²).

En donnant successivement à n les valeurs 2, 3, ..., n, il est facile

---

(¹) *Phil. Trans.*, 1807, p. 131.

(²) SYLVESTER et SERRET, *Comptes rendus Acad. Sc.*, t. 52, p. 307.

de voir que

$$\frac{V_{n\nu+m+1}}{n\nu+m+1}-(n)_1\frac{V_{\overline{n-1}\nu+m+1}}{\overline{n-1}\nu+m+1}+(n)_2\frac{V_{\overline{n-1}\nu+m+1}}{\overline{n+2}\nu+m+1}+\ldots+(-1)^n\frac{V_{m+1}}{m+1}\equiv 0 \pmod{\overline{p^{i+1}}n},\qquad m\geq n(i+1).$$

Lorsque $i=0$, nous obtenons la congruence de Kummer (1). Glaisher donne ce théorème pour $n=1$, $i=0$ dans plusieurs articles (2); il est certain qu'il ignorait les résultats auxquels était arrivé Kummer.

En donnant à $m+1$ des valeurs diverses, on obtient quelques résultats intéressants.

Soit $m+1=p^i+p^a$ (a étant un nombre entier), $n=1$; $m+1$ ne contient pas $p-1$ en facteur et est pair.

$$\frac{V_{p^{i+1}+p^a}}{p^{i+1}+p^a}\equiv\frac{V_{p^i+p^a}}{p^i+p^a}\pmod{p^{i+1}},\qquad a=i;$$

$$\frac{V_{p^i(p+1)}}{p^i(p+1)}\equiv\frac{V_{2p^i}}{2p^i}\pmod{p^{i+1}},\qquad a=i+1;$$

$$\frac{V_{2p^{i+1}}}{2p^{i+1}}\equiv\frac{V_{p^i(p+1)}}{p^i(p+1)}\pmod{p^{i+1}};$$

mais

$$V_{2p}\equiv 0\pmod{p}.$$

En donnant successivement à i les valeurs 1, 2, 3, ..., n, nous obtenons

$$V_{2p^n}\equiv 0\pmod{p^n}.$$

Soit $m+1=p^i(\lambda\overline{p-1}+2\mu)$, où μ n'est pas égal à zéro et $2\mu<p-1$,

$$\frac{V_{p^i(\lambda\overline{p-1}+2\mu)}}{p^i(\lambda\overline{p-1}+2\mu)}\equiv\frac{V_{2\mu}}{2\mu}\pmod{p^{i+1}};$$

si $\lambda=2\mu$,

$$\frac{V_{2\mu p^{i+1}}}{2\mu p^{i+1}}\equiv\frac{V_{2\mu}}{2\mu}\pmod{p^{i+1}};$$

si $\mu=1$,

$$\frac{V_{2p^{i+1}}}{2p^{i+1}}\equiv\frac{V_2}{2}\equiv\frac{1}{12}\pmod{p^{i+1}}.$$

---

(1) *Journal de Crelle*, vol. 41, p. 371.
(2) *Quart. Journal*, vol. XXXI, p. 253

Généralement, comme 2μ est au plus égal à $p-2$ et comme, d'après le théorème de Staudt,

$$V_{2\mu} = \text{entier} - \frac{1}{2} - \frac{1}{3} - \ldots - \frac{1}{2\mu+1},$$

si 2μ est un nombre premier $\frac{V_{2\mu}}{2\mu}$ ne contiendra pas p au dénominateur; d'où

$$V_{2\mu p^{i+1}} \equiv 0 \qquad (\mathrm{mod}\, p^{i+1})$$

tant que $2\mu < p-1$.

Adams (1), dans l'Introduction de sa Table agrandie des nombres de Bernoulli, fait allusion au théorème que, lorsque V_{2n} contient p et non $p-1$, il est divisible par p, et il suppose que le résultat compris dans les limites de ses Tables est vrai, en général, ces dernières allant jusqu'à V_{124}.

Dans tous les résultats ci-dessus p doit être un nombre premier plus grand que 3.

J'ai obtenu le résidu de V_{2n} au module p^{i+1} quand

$$2n = \nu - p^i(p-1),$$

ce qui complète le traitement général des nombres de Bernoulli; le résultat, qui fait pendant au théorème de Sylvester sur les résidus des nombres eulériens, est susceptible d'un certain nombre de déductions qui seraient trop longues pour le présent Mémoire.

Les nombres d'Euler sont particulièrement intéressants du fait qu'ils sont entiers, et que, contrairement aux nombres de Bernoulli, ils sont complètement périodiques; il vaut la peine de signaler que les nombres d'Euler et de Bernoulli sont des cas spéciaux de nombres que Cesàro (2) appelle « les nombres ultra-Bernoulliens et ultra-Eulériens » et dont les propriétés ont un rapport marqué avec les nombres plus familiers de Bernoulli.

Je compte donner plus tard certains résultats généraux sur la division de nombres dans lesquels ces nombres jouent un rôle important.

Je définirai les nombres d'Euler comme suit :

$$\frac{2}{e^x + e^{-x}} = 1 + E_2 \frac{x^2}{\lfloor 2} + E_4 \frac{x^4}{\lfloor 4} + \ldots + E_{2n} \frac{x^{2n}}{\lfloor 2n} + \ldots;$$

(1) *Journal de Crelle*, vol. 85, p. 269.

(2) *Nouvelles Annales*, t. V, p. 312-317.

$x < \frac{\pi}{2}$ donne une série convergente. Lorsqu'on l'exprime en termes des différences des zéros,

$$E_{2n} = \sum_{s=1}^{s=2n} (-1)^s \frac{\Delta^s 0^{2n}}{2^{s+1}} \cos \overline{p+1} \frac{\pi}{4}$$

ou, ce qui est la même chose,

$$E_{2n} = \sum_{s=1}^{s=2n} (-1)^s \frac{\Delta^s 0^{2n}}{2^{s+1}} \left[(1+\sqrt{-1})^{s+1} + (1-\sqrt{-1})^{s+1} \right],$$

on peut avec avantage écrire cette série comme suit :

$$E_{2n} = \sum_{1}^{2n} (-1)^s \Delta^s 0^{2n} (\alpha^{s+1} + \beta^{s+1}).$$

Le théorème général de congruence s'applique maintenant; après avoir multiplié par une puissance de 2, on obtient

$$E_{2n+n\nu} - (n)_1 E_{2m+\overline{n-1}\nu} + (n)_2 E_{2m+\overline{n-2}\nu} + \ldots + (-1)^n E_{2m} \equiv 0 \pmod{p^{(i+1)n}},$$
$$2m \geq n(i+1), \qquad \nu = p^i(p-1);$$

si $n = 1$,

$$E_{2m+\nu} \equiv E_{2m} \pmod{p^{i+1}}, \qquad 2m \geq i+1;$$

si $2m = i$,

$$E_{i+\nu} \equiv E_i \pmod{p^i}.$$

$2m$ n'est pas soumis à la restriction qu'il doit être un multiple de $p-1$ comme c'était le cas avec les nombres Bernoulliens.

Ce théorème fut donné, sans démonstration, par Sylvester (1) et fut démontré par Stern (2). En mettant pour $2m$ diverses valeurs ces congruences intéressantes deviennent manifestes; si $2m = p^i + p^\alpha$, alors

$$E_{p^i+1+p^\alpha} \equiv E_{p^i+p^\alpha} \pmod{p^{i+1}};$$

si $\alpha = i$,

$$E_{p^{i+1}+p^i} \equiv E_{2p^i} \pmod{p^{i+1}};$$

si $\alpha = i+1$,

$$E_{2p^i+1} \equiv E_{p^{i+1}+p^i} - E_{2p^i} \pmod{p^{i+1}};$$

---

(1) *Comptes rendus Acad. Sc.*, t. 52, p. 213.

(2) *Journal de Crelle*, t. 79, p. 89.

d'où

$$E_{2p} \equiv E_2 \pmod{p},$$
$$E_{2p^2} \equiv E_{2p} \pmod{p^2},$$
$$E_{2p^n} \equiv E_{2p^{n-1}} \pmod{p^n};$$

si $2m = (\lambda - 1)[p^i(p-1) + 2t]$,

$$E_{\lambda p^i(p-1)+2t} \equiv E_{\overline{\lambda-1}p^i(p-1)+2t} \equiv \ldots \equiv E_{p^i(p-1)+2t} \pmod{p^{i+1}},$$

où $2t$ peut avoir n'importe quelle valeur, y compris zéro, et

$$E_{p^i(p-1)+2t} \equiv E_{2t} \pmod{p^{i+1}}, \qquad 2t \geqq i+1;$$

si $2t = p-1$,

$$E_{(p^i+1)(p-1)} \equiv E_{p-1} \pmod{p^{i+1}}.$$

Un résultat qui est vrai pour toute fonction périodique et aussi pour les nombres Eulériens est la relation entre les résidus de $E_{p^i(p-1)}$ et de E_{p-1}, le module étant p^{i+1},

$$E_{p-1} \equiv E_{(p^i+1)p-1} \equiv E_{(p^i+2)\overline{p-1}} \equiv E_{(p^i+r)\overline{p-1}} \pmod{p^{i+1}},$$

où i est n'importe quel nombre entier, soit $r = p^i$, d'où

$$E_{2p^i(p-1)} \equiv E_{p-1} \pmod{p^{i+1}},$$

mais

$$E_{rp^i(p-1)} \equiv E_{\overline{r-1}p^i(p-1)} + \ldots \equiv E_{2p^i\overline{p-1}} \equiv E_{p^i\overline{p-1}} \pmod{p^{i+1}},$$

c'est-à-dire

$$E_{rp^i(p-1)} \equiv E_{p-1} \pmod{p^{i+1}}, \qquad p-1 \geqq i+1.$$

Je vais démontrer maintenant le très élégant théorème donné par Sylvester dans la Note citée plus haut.

Stern trouve les résultats suivants :

$$E_{2n} \equiv 0 \pmod{p},$$

lorsque $\frac{p-1}{2}$ est pair;

$$E_{2n} \equiv 2 \pmod{p},$$

lorsque $\frac{p-1}{2}$ est impair, $p-1$ étant un facteur de $2n$.

Le théorème général de Sylvester est

$$E_{2n} \equiv 0 \pmod{p^{i+1}}, \qquad \frac{p-1}{2} \text{ pair};$$

$$E_{2n} \equiv 2 \pmod{p^{i+1}}, \qquad \frac{p-1}{2} \text{ impair},$$

$p^i(p-1)$ étant un facteur de $2n$.

Après avoir donné sa démonstration, le module étant (p), Stern renvoie au théorème général dans les termes suivants :

« J'ai déjà parlé plus haut de cette généralisation et de son rapport avec la formule simple. »

La généralisation à laquelle il fait allusion est l'extension du théorème de congruence du module p au module p^{i+1} ; il ne donne aucune preuve que le reste sera le même dans le cas du module plus général et il me semble qu'une démonstration complète devrait traiter du module général, vu qu'il y entre des termes qui n'apparaissent pas dans le cas simple.

L'expression $\Delta^n(a\,0+1)^m$ est employée pour exprimer le résultat $\Delta^n(ax+1)^m$ où, après avoir fait n fois l'opération Δ sur $(ax+1)^m$, la variable x devient égale à zéro.

Il est facile de démontrer que les nombres Eulériens peuvent être écrits comme suit :

$$E_{2n}=\left(1-\frac{\Delta}{2}+\frac{\Delta^2}{2^2}-\frac{\Delta^3}{2^3}+\ldots+\frac{\Delta^{2n}}{2^{2n}}\right)(2\,0+1)^{2n}.$$

Les propriétés congruentes peuvent se déduire de la formule

$$\Delta^r(2\,0+1)^{1n}=(-1)^r[1^{2n}-(r)_1\,3^{2n}+(r)_2\,5^{2n}+\ldots+(-1)^s(r)_s(2\,s+1)^{2n}+\ldots];$$

si $2n=kp^i(p-1)$, alors le théorème de Fermat prouve que

$$(2\,s+1)^{2n}\equiv 1 \pmod{p^{i+1}}$$

excepté lorsque

$$2\,s+1\equiv 0 \pmod{p}.$$

Soit q la plus petite racine de la congruence

$$2x+1\equiv 0 \pmod{p},$$

or

$$q=\frac{p-1}{2};$$

les autres racines seront

$$q+p,\qquad q+2p,\qquad \ldots,\qquad q+\lambda p_1,\qquad \ldots,$$

où λ est exprimé par

$$\lambda p+t=r-q,$$

t étant moindre que p, c'est-à-dire

$$\Delta^r(2\,0+1)^{1n}\equiv(-1)^{q+1+r}[(r)_q-(r)_{q+p}+\ldots+(-1)^{\lambda}(r)_{q+\lambda p}] \pmod{p^{i+1}},$$

comme

$$1-(r)_1+(r)_2+\ldots+(-1)^r(r)_r=(1-1)^r=0,$$

d'où pour des valeurs de r jusqu'à $r=q$,

$$\Delta^r(20+1)^{2n}\equiv 0 \pmod{p^{i+1}}.$$

Comme $\Delta^r(20+1)^{2n}$ est multiple de $\lfloor r$ pour des valeurs de r égales ou supérieures à $p(i+1)$, les termes $\Delta^r(20+1)^{2n}$ se divisent par p^{i+1}, mais nous garderons certains de ces termes dans le reste.

En introduisant les valeurs de $\Delta^r(20+1)^{2n}$ et en arrêtant la série quand $r=p^{i+1}-1$

$$2^{2n}E_{2n}\equiv -\sum_{r=q}^{r=p^{i+1}-1}(-1)^q[(r)_q-(r)_{q+p}+\ldots+(-1)^\lambda(r)_{q+\lambda p}]2^{2n-r} \pmod{p^{i+1}}.$$

Pour illustrer les différentes méthodes de preuves pour le cas général et le cas particulier de $i=0$, considérons d'abord le dernier.

Comme $(r)_{q+p}$ et les plus grandes valeurs n'apparaissent pas,

$$2^{p-1}E_{p-1}\equiv 1+(-1)^{q+1}2^{p-1-q}\times\left[1+\frac{q+1}{\lfloor 1}\frac{1}{2}+\frac{\overline{q+2}\,q+1}{\lfloor 2}\frac{1}{2^2}+\ldots+\frac{\overline{q+1}\ldots p-1}{\lfloor p-q}\frac{1}{2^{p-q}}\right].$$

Dienger (1) donne la série suivante :

$$1+\frac{m}{\lfloor 1}x+\frac{m(m+1)}{\lfloor 2}x^2+\ldots+\frac{m(m+1)\ldots(m+n-1)}{\lfloor n}x^n$$
$$=-\frac{1}{(1-x)^m}\left[x^{m+n}-1+\frac{m+n}{\lfloor 1}(1-x)x^{m+n-1}+\ldots+\frac{(m+n)\ldots\overline{n+2}}{\lfloor m-1}\overline{1-x^{m-1}}x^{n+1}\right],$$

ce qui est vrai lorsque m et n sont des nombres entiers positifs et que x a n'importe quelle valeur, l'unité exceptée.

Si $m+n=p$, tous les termes après les deux premiers contiennent p

(1) *Journal de Crelle*, vol. 41, p. 48.

en facteur, soit $x = \frac{1}{2}$, $m = q + 1$,

$$\begin{aligned} E_{p-1} &\equiv 1 + (-1)^q \frac{2^{q+1}}{2^q}(2^p - 1)x\,2^{p-1} \qquad (\mathrm{mod}\,p) \\ &\equiv 1 + (-1)^q(1 - 2^p) \qquad (\mathrm{mod}\,p) \\ &\equiv 1 + (-1)^{q+1}; \end{aligned}$$

d'où pour q pair

$$E_{p-1} \equiv 0 \qquad (\mathrm{mod}\,p),$$

pour q impair

$$E_{p-1} \equiv 2 \qquad (\mathrm{mod}\,p).$$

Cette méthode ne peut pas être appliquée au cas général parce qu'alors tous les termes de la série de Dienger ne se divisent pas par p^{i+1}; il faut en conséquence rechercher une preuve tout à fait différente; l'emploi des racines de l'unité en rapport avec les propriétés congruentes des nombres Bernoulliens fut porté à ma connaissance par une étude d'Hermite (1). Soit

$$x^p - 1 = (x-1)(x-\omega_1)(x-\omega_2)\ldots(x-\omega_{p-1})$$

et soit

$$S[f(\omega)] = f(\omega_1) + f(\omega_2) + \ldots + f(\omega_{p-1}),$$

alors il est bien connu que

$$S(\omega^r) = 0 \qquad (\text{excepté pour } r = \mu p),$$
$$S(\omega^{\mu p}) = p - 1;$$

d'où

$$S(1-\omega)^r \omega^{p-q} = \Sigma (-1)^q [(r)_q - (r)_{q+p} + \ldots + (-1)^\lambda (r)_{q+\lambda p}](p-1),$$

où λ a la même valeur qu'auparavant, c'est-à-dire

$$E_{2n} = 1 - \sum_{r=1}^{r=p^{i+1}-1} \frac{S(1-\omega)^r \omega^{p-q}}{2^r(p-1)} \qquad (\mathrm{mod}\,p^{i+1}),$$

$$1 + \frac{1-\omega}{2} + \frac{(1-\omega)^2}{2^2} + \ldots + \frac{(1-\omega)^{p^{i+1}-1}}{2^{p^{i+1}}-1} = \frac{1 - \frac{(1-\omega)^{p^{i+1}}}{2^{p^{i+1}}}}{1 - \frac{1-\omega}{2}}$$

$$= \frac{2}{1+\omega} - \frac{2(1-\omega)^{p^{i+1}}}{2^{p^{i+1}}(1+\omega)};$$

(1) *Journat de Crelle*, vol. 81, p. 94.

$S\left(\frac{\omega^t}{1+\omega}\right)$ prend une forme remarquablement simple que je n'ai pas encore vue, mais qui est probablement connue.

Comme $\omega_t\omega_{p-1-t}=1$,

$$S\left(\frac{\omega}{1+\omega}\right)=S\left(\frac{1}{1+\omega}\right)=S\left(\frac{\omega+1-1}{\omega+1}\right),$$

c'est-à-dire

$$S\left(\frac{\omega}{1+\omega}\right)=\frac{p-1}{2};$$

si t est pair, écrivons

$$\begin{aligned}S\left(\frac{\omega^t}{1+\omega}\right)&=S\left(\frac{\omega^t-1}{\omega+1}\right)+S\left(\frac{1}{1+\omega}\right)\\&=S\left[\frac{(\omega^{\frac{t}{2}}+1)(\omega^{\frac{t}{2}}-1)}{\omega+1}\right]+\frac{p-1}{2};\\&=S\left[\left(\omega^{\frac{t}{2}}+1\right)\left(\omega^{\frac{t}{2}-1}-\omega^{\frac{t}{2}-2}-\ldots-1\right)\right]+\frac{p-1}{2};\end{aligned}$$

si $t<p$, $S(\omega^t)=0$,

$$S\left(\frac{\omega^t}{1+\omega}\right)=-(p-1)+\frac{p-1}{2}=-\frac{(p-1)}{2};$$

pour t impair, la même méthode donne

$$S\left(\frac{\omega^t}{1+\omega}\right)=\frac{p-1}{2};$$

pour $t>p$, soit $t=\mu p+\tau$ $(\tau<p)$,

$$S\left(\frac{\omega^t}{1+\omega}\right)=S\frac{\omega^\tau}{1+\omega}=(-1)^{\tau+1}\frac{p-1}{2}.$$

Nous pouvons passer ensuite à l'évaluation de E_{2n}, où

$$2n=kp^i(p-1)>p^{i+1}:$$

$$E_{2n}\equiv 1-\frac{2}{p-1}S\left[\frac{\omega^{p-q}}{(1+\omega)}\right]+\frac{2}{2p^{i+1}p-1}S\omega^{p-q}\frac{(1-\omega)^{p^{i+1}}}{(1+\omega)}\qquad(\mathrm{mod}\,p^{i+1});$$

comme $q=\frac{p-1}{2}$, $p-q=\frac{p+1}{2}$.

Considérons l'expression

$$\frac{2}{p-1}\,S\frac{\omega^{p-q}}{2^{p^{i+1}}}(1+\omega)^{p^{i+1}}$$

$$=\frac{2}{(p-1)2^{p^{i+1}}}\,S\left[\omega^{p-q}-(p^{i+1})_1\omega^{p-q+1}+\ldots+(-1)^t(p^{i+1})_t\omega^{p-q+t}+\ldots\right],$$

en notant que p^{i+1} est impair, et de là qu'il y a un nombre pair de termes dans la série; le terme entre crochets est égal à

$$\pm\frac{1}{2^{p^{i+1}}}\left[1+(p^{i+1})_1+(p^{i+1})_2+\ldots+(p^{i+1})_q\right.$$
$$-(p^{i+1})_{q+1}-(p^{i+1})_{q+2}-\ldots-(p^{i+1})_{q+p}$$
$$+(p^{i+1})_{q+p+1}+\ldots+(p^{i+1})_{q+2p}$$
$$+\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\left.+(p^{i+1})_{p^{i+1}-q-1}+\ldots+(p^{i+1})_{p^{i+1}}\right],$$

c'est-à-dire que la série est formée de p termes positifs suivis de termes négatifs; ceux-ci peuvent être nommés les « vagues de Sylvester » (1).

Comme les coefficients binomiaux sont égaux de chaque côté et qu'il y a un nombre égal de vagues positives et négatives, la série est égale à zéro et

$$E_{2n}\equiv 1-\frac{2}{p-1}\,S\left(\frac{\omega^{p-1}}{1+\omega}\right)\qquad(\mathrm{mod}\,p^{i+1}).$$

Si $\frac{p+1}{2}$ est impair,

$$S\left(\frac{\omega^{p-q}}{1+\omega}\right)=\frac{p-1}{2},$$
$$E_{2n}\equiv 0\qquad(\mathrm{mod}\,p^{i+1});$$

si $\frac{p+1}{2}$ est pair,

$$S\left(\frac{\omega^{p-q}}{1+\omega}\right)=-\frac{p-1}{2},$$
$$E_{2n}\equiv 2\qquad(\mathrm{mod}\,p^{i+1}).$$

Il est à remarquer que la preuve est tout à fait générale par rapport à la valeur de q, c'est-à-dire que le théorème est applicable à des

(1) *Quart. Journal*, vol. I, p. 142.

expressions telles que $\frac{e^x}{e^{ax}+2}$, où a est un nombre premier, puisque dans ce cas q sera la plus petite racine de

$$ax + 1 \equiv 0 \pmod{p}.$$

Le cas plus général $\frac{e^x}{e^{ax}+t}$ donne un reste de même forme, mais les vagues ne s'anuulent pas l'une l'autre.