OVERSIGT OVER DET KGL. DANSKE VIDENSKABERNES SELSKABS
FORHANDLINGER. 1915. N° 3–4.

NOTE SUR LA CONGRUENCE DE KUMMER RELATIVE AUX NOMBRES DE BERNOULLI.

PAR

KAJ LØCHTE JENSEN.

I. Introduction et formules auxiliaires.

Désignons par $p = 2\mu + 1$ un nombre premier impair, tel que $p - 1$ ne divise pas le positif entier pair $2n$, KUMMER[1] a indiqué la congruence suivante relative aux nombres de BERNOULLI:

$$\sum_{s=0}^{s=r} (-1)^{s+s\mu} \binom{r}{s} \frac{B_{n+s\mu}}{n+s\mu} \equiv 0 \qquad (\mathrm{mod}\; p^{\lambda}),$$

où il faut supposer à la fois

$$\lambda \leqq 2n - 1, \quad \lambda \leqq r.$$

La démonstration de KUMMER est transcendente, parce que l'éminent géomètre allemand applique des propriétés de la fonction exponentielle.

Or, il est très intéressant, ce me semble, que l'on puisse déduire la congruence susdite comme une conséquence de la formule classique de JAQUES BERNOULLI relative aux sommes de puissances

$$S_n(r-1) = 1^n + 2^n + 3^n \ldots + (r-1)^n,$$

savoir

$$(1) \quad S_n(r-1) = \frac{r^{n+1}}{n+1} - \frac{r^n}{2} + \sum_{s=1}^{\leqq \frac{n}{2}} \frac{(-1)^{s-1}}{n-2s+1} \binom{n}{2s} B_s r^{n-2s+1},$$

où il faut supposer $r \geqq 2$.

[1] Journal de Crelle, t. 41, p. 368; 1851.

De plus, le même procédé nous permet de traiter le cas, excepté par KUMMER, où $2n$ est supposé divisible par $p-1$, et d'étudier la congruence analogue pour le nombre premier 2.

A cet effet, nous avons tout d'abord à étudier l'identité

$$\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{ax^s-1}=\frac{\psi(x)}{(a-1)(ax-1)\ldots(ax^r-1)},$$

où a désigne un entier plus grand que l'unité.

Nous aurons immédiatement

$$\psi(1)=0;$$

posons ensuite pour abréger

$$D_x^q\left(\frac{1}{ax^s-1}\right)=\frac{f_q(x,a,s)}{(ax^s-1)^{q+1}},$$

puis différentions encore une fois par rapport à x, nous aurons l'équation fonctionelle

$$f_{q+1}(x,a,s)=(ax^s-1)D_xf_q(x,a,s)-(q+1)sax^{s-1}f_q(x,a,s)$$

ce qui montrera que $f_q(1,a,s)$ est un polynome entier de s, précisément du degré q; c'est-à-dire que nous aurons

$$\psi^{(q)}(1)=0,\qquad 0\leqq q\leqq r-1.$$

Cela posé, nous aurons finalement

$$\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{ax^s-1}=\frac{(x-1)^r\varphi(x)}{(a-1)(ax-1)\ldots(ax^r-1)},\tag{2}$$

où $\varphi(x)$ désigne un polynome entier de x, dont tous les coefficients sont des nombres entiers.

Revenons maintenant à la formule (1); posons $2n$ à la place de n et p^r à la place de r, nous aurons

$$\frac{S_{2n}(p^r-1)}{n}=\frac{p^{(2n+1)r}}{(2n+1)n}-\frac{p^{2nr}}{2n}+$$

$$+\sum_{s=1}^{s=n-1}\frac{(-1)^{s-1}2B_s}{(2n-2s)(2n-2s+1)}\binom{2n-1}{2s}p^{(2n-2s+1)r}+\frac{(-1)^{n-1}B_np^r}{n}.$$

Soit ensuite p un nombre premier impair, le théorème de v. STAUDT et de TH. CLAUSEN montrera que les dénominateurs des fractions irréductibles

$$pB_s, \quad 1 \leqq s \leqq n-1$$

sont premiers à p, ce qui donnera sans peine la congruence suivante[1]

$$\frac{(-1)^{n-1}B_n}{n} \equiv \frac{S_{2n}(p^r-1)}{n \cdot p^r} \pmod{p^r}, \tag{3}$$

où il faut supposer $r > 1$ pour $p = 3$.

Quant au nombre premier 2, nous aurons de même

$$\frac{(-1)^{n-1}B_n}{n} \equiv \frac{S_{2n}(2^r-1)}{n \cdot 2^r} \pmod{2^{r+1}}, \tag{4}$$

où il faut supposer à la fois $r > 1$ et $n > 1$.

Telles sont les réflexions qui nous conduiront à notre démonstration élémentaire de la congruence de Kummer et des extensions susdites[2].

II. La congruence de Kummer.

Désignons par r et μ des positifs entiers, la formule (3) donnera

$$(5)\left\{\begin{aligned} &\sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}\frac{B_{n+s\mu}}{n+s\mu} \equiv \\ &\equiv (-1)^{n-1}\sum_{s=0}^{s=r}(-1)^{s}\binom{r}{s}\frac{1}{p^r}\sum_{a=1}^{a=p^r-1}\frac{a^{2n+2s\mu}}{n+s\mu} \pmod{p^r}, \end{aligned}\right.$$

où $p > 2$, et où il faut supposer $r > 1$ pour $p = 3$.

[1] Soient a et b des nombres rationnels, n un entier, nous écrivons $a \equiv b \pmod{n}$, pourvu que la différence $a - b$ soit égale à une fraction irréductible, dont le numérateur est divisible par n.

[2] Après avoir présenté cette Note à l'Académie Royale j'ai vu que M. Frobenius (Berliner Sitzungsberichte, 1910, p. 809) a donné une autre démonstration élémentaire de la congruence de Kummer.

De plus M. Nielsen vient de publier un Mémoire, (Mémoires de l'Académie Royale des Sciences et des Lettres de Danemark, 7me série, Section des Sciences, t. XII, p. 55—101; 1915) où l'on trouve une autre démonstration élémentaire d'une congruence plus générale qui donne comme des cas particuliers la congruence de Kummer et les congruences analogues pour les nombres d'Euler et les coefficients des tangentes.

J'espère de donner, dans une autre occasion, une quatrième dé-

Supposons maintenant que a ne soit pas divisible par p, puis désignons par g une racine primitive qui correspond au module p^r, nous aurons

$$a = g^v + p^r t_v\,,$$

où t_v est un nombre entier, ce qui donnera

$$(6)\quad \left\{\begin{aligned} &\frac{a^{2n+2s\mu}}{(n+s\mu)p^r} = \frac{g^{v(2n+2s\mu)}}{(n+s\mu)p^r} + 2t_v g^{v(2n+2s\mu-1)} + \\ &+\sum_{q=2}^{q=2n+2s\mu} \frac{g^{v(2n+2s\mu-q)}}{(n+s\mu)p^r}\cdot\frac{2n+2s\mu}{q}\binom{2n+2s\mu-1}{q-1} t_v^q p^{rq}\,, \end{aligned}\right.$$

où la somme qui figure an second membre est toujours divisible par p^r.

Supossons

$$2\mu \equiv 0 \qquad (\operatorname{mod}\ p-1)$$

nous aurons de même

$$\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}2t_v g^{v(2n+2s\mu-1)} = (-1)^r 2t_v g^{v(2n-1)}(g^{2\mu v}-1)^r \equiv 0$$
$$(\operatorname{mod}\ p^r)\,,$$

d'où, en vertu de (6)

$$(7)\quad \left\{\begin{aligned} &\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{p^r}\sum\frac{a^{2n+2s\mu}}{n+s\mu} \equiv \\ &\sum_{s=0}^{s=r}\frac{(-1)^s\binom{r}{s}}{(n+s\mu)p^r}\cdot\frac{g^{(2n+2s\mu)(p^r-p^{r-1})}-1}{g^{2n+2s\mu}-1} \qquad (\operatorname{mod}\ p^r)\,, \end{aligned}\right.$$

où la seconde sommation qui figure au premier membre doit être étendue à tous les a plus petits que p^r et premiers à p.

Soit maintenant

$$g^{p^r-p^{r-1}} = 1 + tp^r\,,$$

où t est un nombre entier, nous aurons de même

monstration élémentaire et très simples de la congruence susdite. Or, cette méthode ne conduira ni à l'extension au cas où $2n$ est divisible par $p-1$ ni à la congruence correspondante pour $p = 2$.

$$(8)\left\{\begin{aligned}\frac{g^{(2n+2s\mu)(p^r-p^{r-1})}-1}{(n+s\mu)p^r} = 2t+\sum_{q=2}^{q=2n+2s\mu}\frac{2t^q p^{r(q-1)}}{q}\binom{2n+2s\mu-1}{q-1} \equiv 2t \\ \pmod{p^r}.\end{aligned}\right.$$

Supposons ensuite que $2n$ ne soit pas divisible par $p-1$, puis posons dans (2)

$$a = g^{2n},\ x = g^{2\mu},$$

nous aurons, en vertu de (7) et (8),

$$(9)\qquad \sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{p^r}\sum\frac{a^{2n+2s\mu}}{n+s\mu} \equiv 0 \pmod{p^r}.$$

De plus, la formule (6) donnera

$$\frac{a^{2n+2s\mu}}{n+s\mu} \equiv \frac{g^{v(2n+2s\mu)}}{n+s\mu} \pmod{p^r},$$

d'où, en vertu de (8),

$$(10)\sum\frac{a^{2n+2s\mu}}{n+s\mu} \equiv \frac{g^{(2n+2s\mu)(p^r-p^{r-1})}-1}{(n+s\mu)(g^{2n+2s\mu}-1)} \equiv 0 \pmod{p^r},$$

où la sommation qui figure au premier membre est à étendre à tous les a plus petits que p^r et premiers à p.

Étudions maintenant, dans la formule (5), la somme des nombres a qui sont divisibles précisément par la puissance p^α, savoir

$$M_\alpha = \sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{p^{(2n+2s\mu)\alpha}}{p^r}\sum\frac{a^{2n+2s\mu}}{n+s\mu},$$

où la derniere somme doit être étendue à tous les a plus petits que $p^{r-\alpha}$ et premiers à p, ce qui donnera, en vertu de (10),

$$(11)\qquad M_\alpha \equiv 0 \pmod{p^{(2n-1)\alpha}}.$$

Cela posé, nous aurons finalement la congruence cherchée

$$(12)\qquad \sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}\frac{B_{n+s\mu}}{n+s\mu} \equiv 0 \pmod{p^\lambda},$$

où 2μ est divisible par $p-1$, tandis que $2n$ ne doit posséder cette propriété, et où il faut supposer à la fois

$$\lambda \leqq r,\ \lambda \leqq 2n-1.$$

III. Extension de la formule de Kummer.

Étudions maintenant le cas, excepté par KUMMER, où

$$2n \equiv 2\mu \equiv 0 \pmod{p-1}, \quad p > 2;$$

nous aurons

$$g^{2n+2s\mu} = 1 + a_s p,$$

où a_s désigne un nombre entier, ce qui donnera conformément à la formule (7)

$$(13) \begin{cases} \dfrac{1}{p^r(n+s\mu)} \cdot \dfrac{g^{(2n+2s\mu)(p^r-p^{r-1})}-1}{g^{2n+2s\mu}-1} = \dfrac{1}{n+s\mu} \cdot \dfrac{p-1}{p} + \\ \quad + \displaystyle\sum_{q=1}^{q=p^r-p^{r-1}-1} \frac{a_s^q}{n+s\mu} \cdot \frac{p^q}{p^r} \cdot \frac{p^r-p^{r-1}}{q+1} \binom{p^r-p^{r-1}-1}{q}. \end{cases}$$

Posons maintenant

$$2n = (p-1)n', \quad 2\mu = (p-1)\mu',$$

nous avons à étudier l'expression

$$\sum_{s=0}^{s=r} (-1)^s \binom{r}{s} \frac{a_s^q}{n'+s\mu'}, \quad q \geqq 1.$$

A cet effet, posons

$$g^{p-1} = 1 + tp,$$

nous aurons

$$\frac{a_s}{n'+s\mu'} = \frac{(1+tp)^{n'+s\mu'}-1}{p(n'+s\mu')},$$

d'où, en appliquant la formule binomiale,

$$(14) \begin{cases} \dfrac{a^s}{n'+s\mu'} = t + \displaystyle\sum_{q=2}^{q=r} \frac{(n'+s\mu'-1)(n'+s\mu'-2)\ldots(n'+s\mu'-q+1)}{q!} t^q p^{q-1} + \\ \quad + \displaystyle\sum_{q=1}^{q=n'+s\mu'-r} \binom{n'+s\mu'-1}{r+q-1} \frac{p^{r+q-1}}{r+q} \cdot t^{r+q}, \end{cases}$$

où il faut supprimer la dernière somme qui figure au second membre dans le cas, où $n'+s\mu' < r+1$.

Soit maintenant ρ le positif entier le plus grand qui satisfait à la condition $p^\rho \leqq r+1$, nous aurons pour $q \geqq 1$

$$\frac{p^{r+q-1}}{r+q} \equiv 0 \pmod{p^{r-\rho}},$$

ce qui montrera que la dernière somme qui figure au second membre de (14) est toujours divisible par la puissance $p^{r-\rho}$.

Remarquons ensuite que la première somme qui figure au second membre de (14) est un polynome entier du degré $r-1$ par rapport à s, nous aurons finalement

$$\sum_{s=0}^{s=r} (-1)^s \binom{r}{s} \frac{a_s}{n'+s\mu'} \equiv 0 \pmod{p^{r-s}}.$$

Étudions ensuite

$$\frac{a_s^q}{n'+s\mu'},$$

le même procédé que nous avons appliqué dans la démonstration de la formule (14) nous conduira ici à une somme des termes de la forme

$$(15)\quad A = c\cdot\frac{p^{k_1-1}}{k_1}\binom{n'+s\mu'-1}{k_1-1}p^{k_2-1}\binom{n'+s\mu'}{k_2}\dots p^{k_q-1}\binom{n'+s\mu'}{k_q},$$

où c est un nombre entier qui ne dépend pas de s.

Il saute aux yeux que le terme A est, considéré comme fonction de s, un polynome entier du degré

$$\varkappa = k_1-1+k_2+k_3+\dots+k_q,$$

ce qui donnera $\varkappa > r-1$, pourvu que

$$(k_1-1)+(k_2-1)+\dots+(k_q-1) > r-q.$$

Supposons maintenant $k_1 > r$, nous aurons

$$A \equiv 0 \pmod{p^{r-\rho}};$$

soit, au contraire, $k_1 \leqq r$, le nombre k_1 est divisible par p^ρ au plus, ce qui donnera

$$A \equiv 0 \pmod{p^{r-q-\rho+1}},$$

de sorte que nous aurons finalement

$$(16)\quad \sum_{s=0}^{s=r} (-1)^s \binom{r}{s} \frac{a_s^q}{n'+s\mu'} \equiv 0 \pmod{p^{r-q-\rho+1}},$$

où $q \geqq 1$.

Posons ensuite

$$(17)\quad \frac{a_s^q}{n'+s\mu'} = \frac{c}{d},\quad q \geqq 1,$$

où la fraction qui figure au second membre est supposée irréductible, nos réflexions sur le terme (15) montreront que d n'est pas divisible par p.

Soit k un entier non négatif, nous aurons évidemment

$$\frac{p^{2r+k-1}}{2r+k-1} \equiv 0 \pmod{p^r}, \ k \geqq 0, \ p > 3;$$

tandis que l'hypothèse $p = 3$ exige $r > 1$.

Cela posé, revenons à la somme qui figure au second membre de la formule (13), nous verrons, en vertu de (17), que les termes qui correspondent à $q \geqq 2r$ sont tous divisibles par p^r.

Quant aux autres termes de la somme susdite, il est évident que le nombre $q+1$ ne peut jamais être divisible par une puissance plus élévée que $p^{\rho+1}$, ou ρ désigne le positif entier le plus grand qui satisfait à la condition $r+1 \geqq p^\rho$. Soit ρ' le positif entier le plus petit qui satisfait à la condition $2r \leqq p^{\rho'+1}-1$, nous pouvons dire aussi que $q+1$ ne peut jamais être divisible par une puissance plus élévée que $p^{\rho'}$; nous aurons de plus $\rho \leqq \rho'$.

Désignons maintenant par σ le plus petit des deux nombres $2\rho+1$ et $2\rho'$, nous aurons, en vertu de (7) et (13)

$$(18)\left\{\begin{aligned}\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{p^r}\sum{}' \frac{a^{2n+2s\mu}}{n+s\mu} &\equiv \frac{p-1}{p}\cdot\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{n+s\mu}\\ &\pmod{p^{r-\sigma}},\end{aligned}\right.$$

où la dernière sommation qui figure au premier membre doit être étendue à tous les a plus petits que p^r et premiers à p.

Appliquons ensuite le même procédé qui nous avait conduit de (6) à (10), nous aurons ici le résultat analogue

$$\sum{}' \frac{a^{2n+2s\mu}}{n+s\mu} \equiv \frac{g^{(2n+2s\mu)(p^r-p^{r-1})}-1}{(n+s\mu)(g^{2n+2s\mu}-1)} \pmod{p^r},$$

de sorte que les formules (13) et (17) donneront

$$(19)\qquad \sum{}' \frac{a^{2n+2s\mu}}{n+s\mu} \equiv \frac{p^r(p-1)}{p}\cdot\frac{1}{n+s\mu} \pmod{p^r}.$$

Quant aux nombres a qui figurent dans la formule (5) et qui sont divisibles par p, nous aurons, en vertu de (19),

$$\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{1}{p^r}\sum_{\alpha=1}^{\alpha=r-1}p^{(2n+2s\mu-1)\alpha}\sum_{a=1}^{a=p^{r-\alpha}-1}\frac{a^{2n+2s\mu}}{n+s\mu}\equiv$$

$$\equiv\frac{p-1}{p}\cdot\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\sum_{\alpha=1}^{\alpha=r-1}\frac{p^{(2n+2s\mu-1)\alpha}}{n+s\mu}\qquad(\mathrm{mod}\ p^{2n-1}).$$

Soit ν le positif entier le plus petit qui satisfait à la condition

$$n\leqq p^{\nu+1}-1\,,$$

nous verrons que la somme étendue aux résidus divisibles par p, qui figurent dans la formule (5), est divisible par $p^{2n-\nu-2}$, ce qui donnera, en vertu de (18), la congruence suivante

$$(20)\left\{\sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}\frac{B_{n+s\mu}}{n+s\mu}\equiv\frac{p-1}{p}\cdot\sum_{s=0}^{s=r}(-1)^{s+n-1}\binom{r}{s}\frac{1}{n+s\mu}\right.$$
$$(\mathrm{mod}\ p^{\lambda})\,,$$

où il faut supposer à la fois

$$\lambda\leqq r-\sigma\,,\ \lambda\leqq 2n-\nu-2\,.$$

Dans cette congruence p désigne un nombre premier impair; soit particulièrement $p=3$, il faut supposer de plus $r>1$.

Il est évident que la congruence (20) se presénte dans ces deux autres formes aussi

$$(21)\left\{\sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}\frac{B_{n+s\mu}}{n+s\mu}\equiv\frac{(-1)^{n-1}r\,!\,\mu^r}{n(n+\mu)\ldots(n+r\mu)}\cdot\frac{p-1}{p}\right.$$
$$(\mathrm{mod}\ p^{\lambda})$$

$$(22)\quad\sum_{s=0}^{s=r}(-1)^s\binom{r}{s}\frac{(-1)^{n+s\mu}B_{n+s\mu}+\frac{p-1}{p}}{n+s\mu}\equiv 0\quad(\mathrm{mod}\ p^{\lambda})\,.$$

Soit particulièrement

$$r\leqq\frac{p-1}{2}\,,\ n\geqq\frac{r+2}{2}\,,\ p>3\,,$$

nous pouvons admettre $\lambda=r$.

Quant à la détermination de l'exposant λ, remarquons en passant qu'il soit possible de donner des conditions plus compliquées qui sont, dans certains cas, plus générales que les précédentes. Cependant de telles généralisations ne sont que d'un intérêt médiocre.

M. NIELSEN[1] a démontré les deux congruences, valables pour $r \geqq 2$,

$$\sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}B_{n+s\mu} \equiv 0 \pmod{p}$$

$$1-\frac{1}{p} \equiv \sum_{s=1}^{s=r}(-1)^{s+s\mu}\binom{r}{s}B_{s\mu} \pmod{p},$$

congruences qui jouent un rôle dans la théorie des résidus quadratiques.

Quant au nombré premier $p=2$, nous posons pour a impair

$$a = \pm 5^v + 2^r t_v, \quad 5^{2n+s\mu} = 1+8a_s.$$

Appliquons ensuite la formule (4), un procédé analogue à celui qui nous a conduit à la congruence (20) donnera ici généralement

$$(23)\left\{\sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}\frac{B_{n+s\mu}}{n+s\mu} \equiv \frac{1}{2}\cdot\sum_{s=0}^{s=r}(-1)^{s+n-1}\binom{r}{s}\frac{1}{n+s\mu} \pmod{2^\lambda},\right.$$

où λ doit satisfaire aux deux conditions suivantes

$$\lambda \leqq r+1, \quad \lambda \leqq 2n-\nu'-2,$$

où ν' est le positif entier le plus petit pour lequel $n \leqq 2^{\nu'+1}-1$, tandis que le cas $r=1$ est une conséquence de la congruence obtenue de (4) en y posant $r=2$.

Quant à la congruence (23) analogue à (20), nous aurons les formules qui correspondent à (21) et (22)

$$(24)\quad \sum_{s=0}^{s=r}(-1)^{s+s\mu}\binom{r}{s}\frac{B_{n+s\mu}}{n+s\mu} \equiv \frac{1}{2}\cdot\frac{(-1)^{n-1}r!\,\mu^r}{n(n+\mu)\ldots(n+r\mu)} \pmod{2^\lambda}$$

$$(25)\quad \sum_{s=0}^{s=r}(-1)^{s}\binom{r}{s}\frac{(-1)^{n+s\mu}B_{n+s\mu}+\frac{1}{2}}{n+s\mu} \equiv 0 \pmod{2^\lambda}.$$

[1] Annales de l'École Normale, (3) t. 31, p. 168; 1914.

Quant aux trois congruences (12), (22) et (25), écrivons dans (12)

$$\frac{B_{n+s\mu}}{n+s\mu} = \frac{a}{b},$$

où la fraction qui figure au second membre est supposée irréductible, nous savons en vertu d'un théorème de v. STAUDT que b ne peut jamais être divisible par p.

Or, il est très intéressant, ce me semble, que les termes correspondants

$$\frac{(-1)^{n+s\mu} B_{n+s\mu} + \frac{p-1}{p}}{n+s\mu}$$

des congruences (22) et (25) possèdent la même propriété.

Je me réserve de revenir à cette question dans une autre occasion.