OVERSIGT OVER DET KGL. DANSKE VIDENSKABERNES SELSKABS FORHANDLINGER. 1915. N° 2.

NOTE SUR LES POLYNOMES RÉGULIERS ET SUR LEUR APPLICATION DANS LA THÉORIE DES NOMBRES.

PRÉSENTÉ DANS LA SÉANCE DU 26 FÉVRIER 1915

PAR

NIELS NIELSEN.

M. GLAISHER, dans deux Mémoires[1] assez étendus, a indiqué, parmi beaucoup d'autres formules, des congruences intéressantes relatives aux coefficients de factorielle C_p^r, dont le rang p est un nombre premier.

Dans une Note[2] récente j'ai déduit des résultats susdits comme des conséquences immédiates du célèbre théorème de v. STAUDT et de TH. CLAUSEN relatif aux nombres de BERNOULLI.

Or, il est très intéressant, ce me semble, que les congruences remarquables en question se présentent aussi comme des cas très particuliers des propriétés générales des polynomes réguliers qui jouent un rôle fondamental dans la théorie élémentaire des nombres de BERNOULLI.

De plus, une telle démonstration nous conduira immédiatement à des généralisations simples et très remarquables des congruences de M. GLAISHER.

En effet, désignons par

$$a_1\ a_2\ a_3 \ldots a_n \tag{1}$$

des nombres complexes assujettis à satisfaire aux conditions

$$a_s + a_{n-s+1} = m\,, \quad 1 \leqq s \leqq n\,, \tag{2}$$

[1] Quarterly Journal of Mathematics, t. 31, p. 1—35; 1899; p. 321—353; 1900.

[2] Annali di matematica (3) t. 22, p. 249—261; 1914.

mais étant du reste aussi arbitraires que ces conditions le permettent. Dans (2) m désigne un nombre complexe différent de zéro, mais quelconque du reste.

Cela posé, les identités

$$(3) \qquad -x-1+\frac{a_s}{m} = -\left(x+\frac{a_{n-s+1}}{m}\right),$$

tirées directement de (2), montrent clairement que le polynome entier

$$(4) \qquad f(x) = \left(x+\frac{a_1}{m}\right)\left(x+\frac{a_2}{m}\right)\ldots\left(x+\frac{a_n}{m}\right),$$

du degré n par rapport à x, satisfait à la condition

$$(5) \qquad (-1)^n f(-x-1) = f(x),$$

ce qui est précisément l'équation fonctionnelle des polynomes réguliers.

Posons maintenant

$$(6) \quad (x+a_1)(x+a_2)\ldots(x+a_n) = x^n + a_1 x^{n-1} + \ldots + a_n,$$

nous aurons

$$(7) \qquad f(x) = \sum_{s=0}^{s=n} \frac{a_s}{m^s} x^{n-s}, \qquad a_0 = 1,$$

Ordonnons ensuite selons des puissances descendantes de x le premier membre de (5), puis cherchons le coefficient de la puissance x^{n-p}, nous aurons la relation suivante entre les a_s

$$(8) \qquad \left(1-(-1)^p\right) a_p = \sum_{s=0}^{s=p-1} (-)^s \binom{n-s}{p-s} m^{p-s} a_s,$$

où il faut supposer $p \geq 1$.

Étudions ensuite le polynome entier

$$(9) \quad F(x) = \left(x+\frac{a_1}{m}\right)^r + \left(x+\frac{a_2}{m}\right)^r + \ldots + \left(x+\frac{a_n}{m}\right)^r,$$

du degré r par rapport à x, l'identité (3) donnera

$$(10) \qquad (-1)^r F(-x-1) = F(x);$$

c'est-à-dire que $F(x)$ est un polynome régulier aussi.

Posons pour abréger

$$(11) \qquad s_q = a_1^q + a_2^q + \ldots + a_n^q, \qquad s_0 = n,$$

nous aurons en vertu de (9),

$$F(x) = \sum_{q=0}^{q=r} \binom{r}{q} \frac{s_q}{m^q} x^{r-q}, \tag{12}$$

de sorte que la formule (8) deviendra ici

$$\left(1-(-1)^p\right) s_p = \sum_{q=0}^{q=p-1} (-1)^q \binom{p}{q} m^{p-q} s_q. \tag{13}$$

Remarquons encore que la formule de NEWTON donnera ici

$$s_p - a_1 s_{p-1} + a_2 s_{p-2} - \ldots + (-1)^{p-1} a_{p-1} s_1 + (-1)^p p a_p = 0, \tag{14}$$

où il faut supposer $1 \leq p \leq n$.

Supposons maintenant remplies les conditions suivantes:

1° Le nombre m est un positif entier impair.

2° Tous les coefficients a_s sont des nombres rationnels, dont les dénominateurs sont tous premiers à m.

Cela posé, nous aurons immédiatement, en vertu de (8),

$$a_{2p+1} \equiv 0 \pmod{m}, \quad 0 \leq p \leq \frac{n-1}{2}. \tag{15}$$

De plus, la formule (14) montrera que les sommes de puissances s_p sont des nombres rationnels de la même nature que les coefficients a_p, ce qui donnera

$$s_{2p+1} \equiv 0 \pmod{m}, \quad 0 \leq p \leq \frac{n-1}{2}. \tag{16}$$

Désignons plus généralement par

$$\Phi(a_1, a_2, \ldots, a_n) \tag{17}$$

une fonction rationnelle et entière, homogène et symétrique des n nombres a_s, puis supposons que le degré de Φ soit un nombre impair, savoir $2N+1$, tandis que tous les coefficients de Φ soient des nombres rationnels dont les dénominateurs sont premiers à m, nous aurons de même

$$\Phi(a_1, a_2, \ldots, a_n) \equiv 0 \pmod{m}. \tag{18}$$

En effet, la fonction Φ en question se présente sous la forme

$$\Phi = \Sigma A_{\alpha, \beta, \ldots, \nu} a_1^{\alpha} a_2^{\beta} \ldots a_n^{\nu},$$

où les coefficients $A_{\alpha, \beta, \ldots, \nu}$ sont des nombres rationnels

de la même nature que les coefficients de Φ, et nous aurons de plus

$$\alpha + 2\beta + \ldots + n\nu = 2N + 1,$$

ce qui montrera que l'ensemble des exposants

$$\alpha\ \beta\ \ldots\ \nu$$

contient toujours un nombre impair au moins.

Supposons maintenant que les coefficients a_s satisfassent aux conditions ultérieures

$$a_{2p} \equiv 0 \pmod{m}, \quad 1 \leq p \leq \mu, \tag{19}$$

la formule (8) donnera immédiatement

$$a_{2p+1} \equiv 0 \pmod{m^2}, \quad 1 \leq p \leq \mu, \tag{20}$$

d'où plus généralement

$$\Phi(a_1, a_2, \ldots, a_n) \equiv 0 \pmod{m^2}, \quad 1 \leq N \leq \mu. \tag{21}$$

Remarquons ensuite que la formule (14) donnera, en vertu de (19),

$$s_{2p} \equiv 0 \pmod{m}, \quad 1 \leq p \leq \mu, \tag{22}$$

de sorte que nous aurons, en vertu de (13),

$$s_{2p+1} \equiv 0 \pmod{m^2}, \quad 1 \geq p \geq \mu. \tag{23}$$

Revenons maintenant aux formules (8) et (13), nous aurons encore ces deux autres congruences

$$\frac{a_{2p+1}}{m^2} \equiv \left(\frac{n}{2} - p\right)\frac{a_{2p}}{m} \pmod{m}, \tag{24}$$

$$\frac{s_{2p+1}}{m^2} \equiv \left(p + \frac{1}{2}\right)\frac{s_{2p}}{m} \pmod{m}, \tag{25}$$

où il faut supposer naturellement $1 \leq p \leq \mu$.

Posons ensuite, dans (14), $2p$ puis $2p+1$ à la place de p, nous aurons respectivement

$$\frac{s_{2p}}{m} \equiv -2p\frac{a_{2p}}{m} \pmod{m}, \tag{26}$$

$$\frac{s_{2p+1}}{m^2} - (2p+1)\frac{a_{2p+1}}{m^2} \equiv \frac{a_1 s_{2p} - a_{2p} s_1}{m^2} \pmod{m}, \tag{27}$$

où il faut supposer également $1 \leq p \leq \mu$.

Remarquons encore que nous aurons

$$a_1 = s_1,$$

la formule (27) se présente dans ces deux autres formes aussi

$$(28)\quad (2p+1)\frac{a_{2p+1}}{m^2} \equiv \frac{s_{2p+1}}{m^2} - \frac{2p+1}{2p}\cdot\frac{s_1 s_{2p}}{m^2} \pmod m,$$

$$(29)\quad \frac{s_{2p+1}}{m^2} \equiv \frac{(2p+1)(a_{2p+1} - a_1 a_{2p})}{m^2} \pmod m.$$

Telles sont les propriétés fondamentales des polynomes réguliers qui nous sont utiles dans nos recherches suivantes.

Soit maintenant m égal au nombre premier impair $p = 2n+1$, nous définissons les nombres a_s comme l'ensemble

$$1,\ 2,\ 3,\ \ldots,\ 2n,$$

de sorte que nous aurons pour les coefficients a_r

$$(30)\qquad a_r = C_p^r,$$

où les C_p^r sont précisément les coefficients de factorielle du rang p, tandis que nous trouvons

$$(31)\qquad s_r = s_r(p-1) = 1^r + 2^r + 3^r + \ldots + (p-1)^r.$$

Cela posé, nous avons à appliquer la formule de Jacques Bernoulli [1]

$$(32)\quad s_r(p-1) = \frac{p^{r+1}}{r+1} - \frac{p^r}{2} + \sum_{s=1}^{\leq \frac{r}{2}} \frac{(-1)^{s-1}}{r+1}\binom{r+1}{2s} B_s p^{r-2s+1},$$

où les B_s désignent les nombres de Bernoulli, et où il faut supposer naturellement $r \geq 2$.

Remarquons en passant que la formule (13) qui correspond aux sommes $s_r(p-1)$, savoir

$$(33)\quad \left(1-(-1)^r\right) s_r(p-1) = \sum_{q=0}^{q=r-1} (-1)^q \binom{r}{q} p^{r-q}\, s_q(p-1)$$

est due à Euler. [2]

Supposons maintenant

$$(34)\qquad 1 \leq r \leq \frac{p-3}{2},$$

[1] Ars conjectandi, p. 95—97; Bâle 1713.

[2] Institutiones calculi differentialis, p. 348—351; Saint-Pétersbourg 1755.

la formule (32) donnera immédiatement ces deux congruences

$$s_{2r}(p-1) \equiv 0 \pmod{p}, \tag{35}$$

$$s_{2r+1}(p-1) \equiv 0 \pmod{p^2}, \tag{36}$$

et nous aurons de plus

$$\frac{s_{2r}(p-1)}{p} \equiv (-1)^{r-1} B_r \pmod{p}, \tag{37}$$

$$\frac{s_{2r+1}(p-1)}{p^2} \equiv (-1)^{r-1}\left(r + \frac{1}{2}\right) B_r \pmod{p}, \tag{38}$$

se qui s'accorde bien avec la formule générale (25).

Appliquons ensuite la formule (14), nous aurons ces deux autres congruences

$$C_p^{2r} \equiv 0 \pmod{p}, \tag{39}$$

$$C_p^{2r+1} \equiv 0 \pmod{p^2}, \tag{40}$$

où il faut supposer remplies les conditions (34).

Il est bien connu que LAGRANGE[1] a trouvé la congruence (39) dans sa démonstration du théorème de WILSON ; néanmoins M. GLAISHER attribue à FERRERS cette même congruence. Il est très curieux, ce me semble, que le *Jahrbuch über die Fortschritte der Mathematik*[2]) indique sans réservation la remarque fausse de M. GLAISHER.

Quant à la formule (40), WOLSTENHOLME[3] a indiqué le cas particulier

$$C_p^{p-2} \equiv 0 \pmod{p^2}.$$

Dans une petite Note[4] j'ai démontré la formule générale (40) ; mais j'ignore si la priorité appartient à moi.

Remarquons en passant que nous aurons dans ce cas, avec la définition (17),

$$\Phi(1, 2, 3, \ldots, 2n) \equiv 0 \pmod{p^2}, \tag{41}$$

ce qui s'accorde bien avec une remarque de feu M. VALENTINER.[5] Dans (41) il faut supposer naturellement

[1] Nouveaux Mémoires de l'Académie de Berlin, t. 2 (1771), p. 125—137 ; 1773.

[2] Voir t. 30, pp. 180, 182; 1899.

[3] Quarterly Journal of Mathematics, t. 5, p. 35—39 ; 1862.

[4] Nyt Tidsskrift for Matematik, t. 4 B, p. 1—10 ; 1893.

[5] Ibid. t. 21 B, p. 36—37 ; 1910.

$$1 \leq N \leq \frac{p-3}{2},$$

où $2N+1$ désigne le degré de Φ par rapport aux quantités $a_1\ a_2\ \ldots\ a_{2n}$.

Appliquons maintenant les formules (24) et (26), nous aurons ces deux autres congruences

$$\frac{C_p^{2r}}{p} \equiv \frac{(-1)^r B_r}{2r} \pmod{p}, \tag{42}$$

$$\frac{C_p^{2r+1}}{p^2} \equiv \frac{(-1)^{r-1}(2r+1)B_r}{4r} \pmod{p}, \tag{43}$$

dont la dernière peut être déduite aussi à l'aide de la formule (28).

Dans les deux congruences (42) et (43) qui sont précisément celles de M. Glaisher il faut supposer remplies les conditions (34).

Revenons maintenant à la formule (32), nous aurons

$$s_{p-1}(p-1) \equiv (-1)^{n-1} B_n p \pmod{p^2},$$

ou, conformément au théorème de v. Staudt et de Th. Clausen

$$s_{p-1}(p-1) \equiv -1 + p\left((-1)^{n-1}B_n + \frac{1}{p}\right) \pmod{p^2}, \tag{44}$$

de sorte que la formule (14) donnera

$$-1 + p\left((-1)^{n-1}B_n + \frac{1}{p}\right) + (p-1)\cdot(p-1)! \equiv 0 \pmod{p^2}, \tag{45}$$

ce qui nous conduira au théorème de Wilson:

$$(p-1)! + 1 \equiv 0 \pmod{p}. \tag{46}$$

Posons ensuite

$$(p-1)! = -1 + pW_p, \tag{47}$$

le nombre W_p, que nous désignons pour abréger comme le quotient de Wilson et par conséquent un positif entier. De plus, la formule (45) donnera après un simple calcul

$$W_p \equiv (-1)^{n-1}B_n - \frac{p-1}{p} \pmod{p}; \tag{48}$$

cette dernière congruence est indiquée sans démonstration par M. Lerch.[1]

[1] Mathematische Annalen, t. 60, p. 477; 1905.

Il est évident du reste que la formule de M. LERCH représente un supplément à la formule (42) de M. GLAISHER, savoir pour $r = n = \frac{p-1}{2}$.

En second lieu, désignons par

$$m = p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r} \tag{49}$$

un nombre impair décomposé dans ses facteurs premiers, où nous supposons

$$p_1 < p_2 < p_3 < \dots < p_r ;$$

les

$$2\mu = \varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

positifs entiers, plus petits que m et premiers à m

$$a_1\, a_2\, a_3 \dots a_{2\mu} \tag{50}$$

satisfont aux conditions (2).

Posons ensuite

$$\varphi_b(m) = (p_1^b-1)\,(p_2^b-1)\dots(p_r^b-1)\,, \tag{51}$$

nous aurons pour la somme de puissances

$$s_n = a_1^n + a_2^n + \dots + a_{2\mu}^n$$

l'expression suivante

$$s_n = \frac{m^n\varphi(m)}{n+1} + \frac{(-1)^r}{n+1}\cdot\sum_{s=1}^{\leqq\frac{n}{2}}(-1)^{s-1}\binom{n+1}{2s}\varphi_{2s-1}(m)\,B_s\,m^{n-2s+1}, \tag{52}$$

où il faut supposer $n \geqq 2$, tandis que nous aurons particulièrement

$$s_0 = \varphi(m)\,, \quad s_1 = \frac{m}{2}\varphi(m). \tag{53}$$

THACKER[1] a indiqué, par des exemples, l'existence de la formule (52), tandis que J. BINET[2] a étudié en même temps, mais d'un autre point de vue, les sommes de puissances s_n en question.

[1] Journal de Crelle, t. 40, p. 89—92; 1850.
[2] Comptes rendus, t. 32, p. 918—921; 1851.

On voit du reste que la formule (52) est une généralisation directe de celle de JACQUES BERNOULLI, que l'on obtient, après un calcul simple, de (52).

Posons maintenant pour abréger

$$p_1 = 2q+1, \tag{54}$$

puis supposons

$$1 \leq n \leq q-1, \tag{55}$$

la formule (52) donnera immédiatement les deux congruences suivantes

$$s_{2n} \equiv 0 \pmod{m}, \tag{56}$$

$$s_{2n+1} \equiv 0 \pmod{m^2}. \tag{57}$$

De plus, nous trouvons

$$\frac{s_{2n}}{m} \equiv (-1)^{r+n-1} \varphi_{2n-1}(m) B_n \pmod{m}, \tag{58}$$

$$\frac{s_{2n+1}}{m^2} \equiv (-1)^{r+n-1}\left(n+\frac{1}{2}\right) \varphi_{2n-1}(m) B_n \pmod{m}. \tag{59}$$

Quant aux coefficients a_s formés des nombres (50), nous aurons, en vertu de (14),

$$a_{2n} \equiv 0 \pmod{m}, \tag{60}$$

$$a_{2n+1} \equiv 0 \pmod{m^2}, \tag{61}$$

où il faut supposer naturellement

$$1 \leq n \leq q-1.$$

Appliquons maintenant les formules (26) et (28), nous aurons de plus

$$\frac{a_{2n}}{m} \equiv \frac{(-1)^{r+n} \varphi_{2n-1}(m) B_n}{2n} \pmod{m}, \tag{62}$$

$$\frac{a_{2n+1}}{m^2} \equiv \frac{(-1)^{r+n-1}\left(2n-\varphi(m)\right)\varphi_{2n-1}(m) B_n}{4n} \pmod{m}. \tag{63}$$

Il saute aux yeux que nos quatre dernières formules représentent des généralisations, remarquables ce me semble, de celles étudiées par M. GLAISHER.

Posons maintenant dans (52)

$$n = 2q = p_1 - 1,$$

nous aurons

$$(64) \qquad s_{2q} \equiv (-1)^{r+q-1} \varphi_{2q-1}(m) B_q m \pmod{m^2},$$

ce qui donnera, en vertu du théorème de v. STAUDT et de TH. CLAUSEN,

$$(65) \qquad s_{2q} \equiv (-1)^{r+1} \varphi_{2q-1}(m) \frac{m}{p_1} \pmod{m}$$

Remarquons ensuite que la formule (14) donnera ici

$$(66) \qquad s_{2q} + 2q\, a_{2q} \equiv 0 \pmod{m^2},$$

nous aurons tout d'abord

$$(67) \qquad 2q + a_{2q} \equiv (-1)^r \varphi_{2q-1}(m) \frac{m}{p_1} \pmod{m},$$

ce qui nous conduira à poser

$$(68) \qquad 2q\, a_{2q} = (-1)^r \varphi_{2q-1}(m) \frac{m}{p_1} + m\, \Omega_{p_1},$$

où Ω_{p_1} désigne un nombre entier.

Cela posé, les formules (64) et (66) donnent immédiatement

$$(69) \qquad \Omega_{p_1} \equiv (-1)^{r+1} \varphi_{2q-1}(m) \left((-1)^{q-1} B_q + \frac{1}{p_1} \right).$$

On voit que les formules (67) et (69) représentent des généralisations remarquables respectivement du théorème de WILSON et de la congruence de M. LERCH.

On pourrait étendre beaucoup plus loin l'étude de la formule (52), cependant les résultats ainsi obtenus deviendront plus compliqués. C'est pourquoi nous nous bornerons aux applications précédentes.

L'application sur la fonction Φ définie dans la formule (17) est évidente.

En troisième lieu, désignons par m un nombre premier de la forme $4q+1$, l'ensemble des résidus quadratiques de m

$$(70) \qquad r_1\ r_2\ r_3\ \ldots\ r_{2q}$$

satisfont aux conditions (2), et c'est la même chose pour l'ensemble des non-résidus de m

$$(71) \qquad i_1\ i_2\ i_3\ \ldots\ i_{2q}.$$

Nous nous bornerons à ces indications parce que j'ai étudié plus amplement, dans mon Mémoire sur les résidus quadratiques, les deux ensembles (70) et (71).