OVERSIGT OVER DET KGL. DANSKE VIDENSKABERNES SELSKABS FORHANDLINGER. 1915. N° 6.

SUR LES NOMBRES DE BERNOULLI ET LEUR APPLICATION DANS LA THÉORIE DES NOMBRES.

PAR

NIELS NIELSEN.

(PRÉSENTÉ DANS LA SÉANCE DU 5 NOVEMBRE 1915.)

I. Remarques sur la formule de Bernoulli.

Posons pour abréger

(1) $$S_n(a) = 1^n + 2^n + 3^n + \dots + a^n,$$

où a et n désignent des positifs entiers; on sait que JACQUES BERNOULLI[1] a indiqué la formule suivante, valable pour $n \geqq 2$:

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

où les B_s sont les nombres de BERNOULLI.

Le grand géomètre suisse indique sa formule (2) sans démonstration; cependant il détermine successivement les nombres

$$B_1 B_2 B_3 \dots B_n \dots$$

en posant dans (2) $a = 1$, puis donnant n les valeurs successives

$$2, 3, 4, 5, \dots,$$

savoir à l'aide de la formule récursive générale

(3) $$\frac{n-1}{2} = \sum_{s=1}^{\leqq \frac{n}{2}} (-1)^{s-1} \binom{n+1}{2s} B_s;$$

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

c'est-à-dire que la formule (3) appartient à BERNOULLI; néanmoins on partage généralement la formule (3) en deux autres selon que n est supposé pair ou impair et on attribue à MOIVRE[1] la première de ces formules, à JACOBI[2] la seconde.

Dans ce qui suit nous aurons besoin d'une généralisation de la formule (2).

En effet, soit

(4) $$M = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_\nu^{r_\nu}$$

un nombre décomposé en facteurs premiers, et soient

$$a_1\, a_2\, a_3 \dots a_\mu, \qquad \mu = \varphi(M),$$

les positifs entiers plus petits que M et premiers à M, nous aurons à étudier la somme de puissances

(5) $$S'_n(M) = a_1^n + a_2^n + a_3^n + \dots a_\mu^n.$$

Dans le cas particulier, où M est égal à un nombre premier p, nous aurons par conséquent

(6) $$S'_n(p) = S_n(p-1).$$

Soit ensuite m un positif entier quelconque, et soient

$$b_1\, b_2\, b_3 \dots b_{m\mu}.$$

l'ensemble des $m\varphi(M)$ positifs entiers plus petits que mM et premiers à M, nous posons

(7) $$S_n(m, M) = b_1^n + b_2^n + b_3^n + \dots + b_{m\mu}^n,$$

ce qui donnera évidemment

(8) $$S_n(1, M) = S'_n(M).$$

Étudions tout d'abord le cas, où M est la puissance d'un nombre premier, savoir

$$M = p^r;$$

il est évident que

$$p,\ 2p,\ 3p, \dots,\ mp^r$$

sont tous les multiples de p qui ne depassent pas à mM; c'est-à-dire que nous aurons

$$S_n(m, p^r) = S_n(mp^r) - p^n S^n(mp^{r-1}),$$

ce qui donnera, en vertu de (2),

[1] Miscellanea analytica de seriebus et quadraturis; complementum p. 6; Londres 1730.

[2] Journal de Crelle, t. 12, p. 265; 1834.

$$(9)\quad \left\{\begin{aligned} S_n(m, p^r) &= \frac{m^{n+1}p^{nr}\varphi(p^r)}{n+1} - \\ &- \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s-1}}{n+1}\binom{n+1}{2s} B_s (mp^r)^{n-2s+1}(p^{2s-1}-1). \end{aligned}\right.$$

Soit ensuite

$$M_1 = p_2^{r_2} p_3^{r_3} \dots p_\nu^{r_\nu}$$

un nombre décomposé contenant $\nu - 1$ facteurs premiers; nous supposons vraie la formule

$$(10)\quad \left\{\begin{aligned} S_n(m_1, M_1) &= \frac{m_1^{n+1} M_1^n \varphi(M_1)}{n+1} + \\ &+ (-1)^{\nu-1} \cdot \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s-1}}{n+1}\binom{n+1}{2s} B_s (m_1 M_1)^{n-2s+1} \varphi_{2s-1}(M_1), \end{aligned}\right.$$

où nous avons posé pour abréger

$$(11)\qquad \varphi_k(M_1) = (p_2^k - 1)(p_3^k - 1)\dots(p_\nu^k - 1).$$

Cela posé, introduisons dans (10)

$$m_1 = m p_1^{r_1},$$

ce qui donnera, en vertu de la définition (4),

$$m_1 M_1 = mM;$$

nous aurons évidemment

$$S_n(m, M) = S_n(mp_1^{r_1}, M_1) - p_1^n S_n(mp_1^{r_1-1}, M_1),$$

d'où, en vertu de (10),

$$(12)\quad \left\{\begin{aligned} S_n(m, M) &= \frac{m^{n+1} M^n \varphi(M)}{n+1} + \\ &+ (-1)^{\nu} \cdot \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s-1}}{n+1}\binom{n+1}{2s} B_s (mM)^{n-2s+1} \varphi_{2s-1}(M), \end{aligned}\right.$$

formule que est précisément de la même forme que (10); c'est-à-dire que la formule (12) est valable pour un nombre décomposé quelconque M.

Posons dans (12)

$$m = 1,$$

nous aurons particulièrement, en vertu de (8),

$$(13)\quad \left\{\begin{aligned} S'_n(M) &= \frac{M^n \varphi(M)}{n+1} + \\ &+ (-1)^{\nu} \cdot \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s-1}}{n+1}\binom{n+1}{2s} B_s M^{n-2s+1} \varphi_{2s-1}(M), \end{aligned}\right.$$

ce qui est précisément la formule générale de laquelle THACKER[1] a indiqué des cas spéciaux, tandis que J. BINET[2] a étudié presque contemporainément, mais d'un autre point de vue, la somme $S_n'(M)$.

Il est évident que la formule (13) est une généralisation de la formule (2) de BERNOULLI.

En effet, soit dans (13) M égal à un nombre premier p; une application de la formule récursive (3) nous conduira immédiatement à la formule obtenue de (2) en y posant $a = p - 1$.

Soit particulièrement, dans (4),

$$r_1 = r_2 = r_3 = \ldots = r_\nu = 1,$$

savoir

$$M = p_1 p_2 p_3 \cdots p_\nu,$$

nous aurons évidemment

$$\varphi_1(M) = \varphi(M). \tag{14}$$

II. Sur la nature des nombres de Bernoulli.

Soit p un nombre premier impair quelconque, tandis que n est un positif entier tel que $2n$ est divisible par $p - 1$, nous disons pour abréger que le nombre premier p est du rang n; c'est-à-dire que le nombre premier 3 est d'un rang quelconque.

Soient ensuite

$$p_1 p_2 p_3 \cdots p_\nu$$

l'ensemble des nombres premiers du rang n, le célèbre théorème de VON STAUDT[3] et de TH. CLAUSEN[4] donnera pour le n-ième nombre de BERNOULLI une expression de la forme

$$(-1)^n B_n = A_n + \frac{1}{2} + \frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_\nu} \tag{1}$$

où A_n est un nombre entier.

[1] Journal de Crelle, t. 40, p. 89—92; 1850.
[2] Comptes rendus, t. 32, p. 918—921; 1851.
[3] Journal de Crelle, t. 21, p. 372—374; 1840.
[4] Astronomische Nachrichten, t. 17, col. 351—352; 1840.

Écrivons ensuite

$$B_n = \frac{a_n}{2\,b_n}, \tag{2}$$

où la fraction qui figure au second membre est supposée irréductible, nous aurons par conséquent

$$b_n = p_1\, p_2\, p_3 \ldots p_\nu; \tag{3}$$

c'est-à-dire que b_n est le produit de tous les nombres premiers du rang n.

Soit maintenant G_n le plus petit dénominateur commun, des n fractions

$$B_1\, B_2\, B_3 \ldots B_n,$$

nous verrons par conséquent que G_n est le produit de tous les nombres premiers impairs qui ne dépassent pas à $2\,n + 1$.

Dans ce qui suit, nous posons encore pour abréger

$$G_n = b_n\, g_n, \tag{4}$$

ce qui montrera que g_n est un nombre impair.

Quant au numérateur a_n du n-ième nombre de BERNOULLI, il est d'une nature beaucoup plus compliquée que b_n.

Posons

$$n = A \cdot B, \tag{5}$$

où B ne contient que des facteurs premiers qui sont du rang n, tandis que A n'est pas divisible par aucun de ces nombres premiers, VON STAUDT[1] a observé la congruence

$$a_n \equiv 0 \pmod{A}. \tag{6}$$

De plus l'éminent géomètre allemand a démontré les deux autres congruences[2]

$$\left\{\begin{aligned} a_{2m} + b_{2m} &\equiv 0 \pmod{8}, \\ a_{2m+1} + 3\,b_{2m+1} &\equiv 0 \pmod{8}, \end{aligned}\right. \tag{7}$$

où il faut supposer $m \geqq 1$.

Or, suivant une méthode que j'ai indiquée récemment[3]

[1] De numeris BERNOULLIANIS commentatio; Erlangue 1845.

[2] De numeris BERNOULLIANIS commentatio altera; Erlangue 1845.

[3] Nyt Tidsskrift for Matematik, t. 25 B; 1914.

pour démontrer les congruences (7), il est possible d'aller un peu plus loin.

A cet effet, prenons pour point de départ la formule de JACQUES BERNOULLI, savoir la formule (2) du paragraphe I, nous aurons

$$(8)\quad \begin{cases} (2n+1)\, S_{2n}(a-1) = \\ (-1)^{n-1}(2n+1)\, B_n a + (-1)^n \binom{2n+1}{3} B_{n-1} a^3 + a^4 K, \end{cases}$$

où K est un nombre rationnel, dont le dénominateur est premier à a.

Introduisons maintenant dans (8) $a = 4$, puis multiplions par

$$G_n = b_n g_n$$

les deux membres de la formule susdite, nous aurons

$$2\,(2n+1)\, a_n g_n - \binom{2n+1}{3} (G_n B_{n-1})\, 64 \equiv$$

$$\equiv (-1)^{n-1}(2n+1)\,(1^{2n} + 2^{2n} + 3^{2n})\, b_n g_n \pmod{128},$$

ce qui donnera

$$(9)\quad \begin{cases} (2n+1)\ a_n - 16\, n \cdot \dfrac{4n^2-1}{3} \equiv \\ (-1)^{n-1} \dfrac{2n+1}{2}\, (1^{2n} + 2^{2n} + 3^{2n})\ b_n \pmod{32}; \end{cases}$$

car

$$2\, G_n B_{n-1} = 2\, b_n g_n B_{n-1}$$

est un nombre entier impair.

Supposons ensuite $n \geqq 3$, nous aurons, en vertu de (9),

$$(10)\quad \begin{cases} (2n+1)\ a_n - 16\, n \cdot \dfrac{4n^2-1}{3} \equiv \\ \equiv (-1)^{n-1}(2n+1) \cdot \dfrac{1+3^{2n}}{2} \cdot b_n \pmod{32}; \end{cases}$$

soit maintenant n un nombre pair, savoir

$$n = 2m, \qquad m \geqq 2,$$

nous aurons par conséquent

$$(11)\qquad a_{2m} \equiv -\frac{1+3^{4m}}{2}\, b_{2m} \pmod{32}.$$

Or, la formule binomiale donnera

$$3^{4m} = (1 - 4)^{4m} \equiv 1 - 48\,m \pmod{64};$$

c'est-à-dire que nous aurons, en vertu de (11),

$$a_{2m} \equiv (24\,m - 1)\,b_{2m} \pmod{32}$$

ou, ce qui est la même chose

(12) $$a_{2m} + (8\,m + 1)\,b_{2m} \equiv 0 \pmod{32},$$

où il faut supposer par conséquent $m \geqq 2$.

Quant au cas exclu $m = 1$, nous aurons

$$B_2 = \frac{1}{30};\quad a_2 = 1,\quad b_2 = 15,$$

ce qui donnera

$$a_2 + 9\,b_2 = 136,$$

savoir

(13) $$a_2 + b_2 \equiv 0 \pmod{8}.$$

Étudions maintenant le cas général, où n est supposé impair, savoir

$$n = 2\,m + 1,\quad m \geqq 1,$$

nous aurons, en vertu de (9),

$$(4\,m + 3)\,a_{2m+1} - 16 \cdot \frac{(4\,m + 3)\,(4\,m + 1)}{3} \equiv$$

$$\equiv \frac{1 + 3^{4m+2}}{2} \cdot (4\,m + 3)\,b_{2m+1} \pmod{32},$$

ce qui donnera sans peine

(14) $$a_{2m+1} \equiv \left(16 + \frac{1 + 3^{4m+2}}{2}\right) \pmod{32}.$$

Dans ce cas la formule binomiale donnera

$$3^{4m+2} = (1 - 4)^{4m+2} \equiv 9 + 80\,m \pmod{64},$$

d'où, en vertu de (14),

$$a_{2m+1} \equiv (21 + 40\,m)\,b_{2m+1} \pmod{32},$$

ou, ce qui est la même chose

(15) $$a_{2m+1} - (8\,m - 11)\,b_{2m+1} \equiv 0 \pmod{32},$$

où il faut supposer $m \geqq 1$.

Quant au cas exclu $m = 0$, nous aurons

$$B_1 = \frac{1}{6};\quad a_1 = 1,\quad b_1 = 3,$$

ce qui donnera

$$a_1 + 11\,b_1 = 34,$$

savoir

$$(16)\qquad a_1 + 3\, b_1 \equiv 0 \pmod 2$$

Cela posé, nous avons démontré la proposition suivante:

Soit $m \geqq 1$, les deux nombres a_n et b_n satisfont toujours aux congruences

$$(17)\qquad \begin{cases} a_{2m+2} + (8\,m + 1)\, b_{2m+2} \equiv 0 \pmod{32} \\ a_{2m+1} - (8\,m - 11)\, b_{2m+1} \equiv 0 \pmod{32}. \end{cases}$$

On voit que le module 16 ne présente qu'un intérêt médiocre, tandis que le module 8 nous conduira immédiatement aux congruences de VON STAUDT.

Quant au numérateur a_n du n-ième nombre de BERNOULLI, nous avons à démontrer une autre congruence, nouvelle que je sache.

A cet effet, posons dans la formule générale (13) du paragraphe I

$$M = b_n = p_1\, p_2\, p_3 \cdots p_\nu$$

puis remplaçons n par $2\,n$, nous aurons

$$2\,n \equiv 0 \pmod{\varphi\,(b_n)},$$

ce qui donnera

$$S'_{2n}\,(b_n) \equiv \varphi\,(b_n) \pmod{b_n},$$

de sorte que nous aurons

$$\varphi\,(b_n) \equiv (-1)^{\nu+n-1} \varphi_{2n-1}\,(b_n) \cdot B_n\, b_n \pmod{b_n};$$

c'est-à-dire que nous aurons le théorème suivant:

Le numérateur a_n du n-ième nombre de BERNOULLI satisfait toujours à la congruence

$$(18)\qquad \frac{(-1)^{n+\nu-1}}{2} \cdot a_n \equiv \frac{(p_1^{2n-1} - 1)(p_2^{2n-1} - 1)\cdots(p_\nu^{2n-1} - 1)}{(p_1 - 1)\,(p_2 - 1)\cdots(p_\nu - 1)} \pmod{b_n}.$$

Il est très interéssant, ce me semble, que le second membre de (18) ne dépend que des nombres premiers du rang n.

M. KAJ LÖCHTE JENSEN que j'ai communiqué le résultat susdit a verifié la congruence (18) à l'aide du théorème de VON STAUDT et de TH. CLAUSEN, savoir la formule (1).

Revenons maintenant à ce théorème célèbre; supposons premier le nombre

$$p = 2n + 1,$$

p est toujours du rang n; c'est-à-dire que le dénominateur de B_n savoir b_n, est divisible par p, tandis que le dénominateur de la fraction

$$(-1)^{n-1} B_n + \frac{1}{p}$$

n'est pas divisible par p.

Cela posé, appliquons la formule obtenue de (3) du paragraphe I en y posant $p-1$, an lieu de n, savoir

$$\frac{p-2}{2} = \sum_{s=1}^{s=n} (-1)^{s-1} \binom{p}{2s} B_s,$$

puis appliquons la congruence évidente

$$\frac{1}{p}\binom{p}{2s} \equiv -\frac{1}{2s} \pmod{p},$$

nous aurons par conséquent

$$(19) \quad \sum_{s=1}^{s=n-1} \frac{(-1)^{s-1} B^s}{2s} \equiv -\frac{1}{2} + \frac{1}{p} + (-1)^{n-1} B_n \pmod{p}.$$

De plus, la formule (1) donnera

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

d'où, en vertu de la formule d'Euler[1]

$$(2n+1) B_n = \sum_{s=1}^{s=n-1} \binom{2n}{2s} B_s B_{n-s},$$

la congruence nouvelle

$$(20) \qquad \sum_{s=1}^{s=n-1} B_s B_{n-s} \equiv (-1)^n \pmod{p}.$$

III. Sur les quotients de Fermat et de Wilson.

Soit

$$p = 2n + 1$$

un nombre premier, tandis que a est un entier non divisible par p, le théorème de Fermat donnera

[1] Opuscula analytica, t. II, p. 266; Saint-Pétersbourg 1785.

$$(1) \qquad a^{2n} = 1 + p\,k_p(a),$$

où $k_p(a)$, le quotient de FERMAT, est un nombre entier.

Cette définition adoptée, nous aurons immédiatement

$$(2) \qquad p\,(k_p(1) + k_p(2) + \ldots + k_p(a)) = S_{2n}(a) - a,$$

de sorte que la somme qui figure au premier membre peut être determinée à l'aide de la formule de JACQUES BERNOULLI, savoir la formule (2) du paragraphe I.

Soit particulièrement

$$a = p - 1,$$

nous posons pour abréger

$$(3) \qquad K_p = k_p(1) + k_p(2) + \ldots + k_p(p-1),$$

et nous aurons par conséquent après une rèduction simple

$$(4) \quad \left\{ \begin{aligned} K_p &= (-1)^{n-1} B_n + \frac{1}{p} - 1 + \\ &+ \frac{p^{2n-1}}{2} + \sum_{s=1}^{s=n-1} \frac{(-1)^{s-1}}{2s} \binom{2n}{2s-1} B_s p^{2n-2s}, \end{aligned} \right.$$

ce qui donnera immédiatement

$$(5) \qquad K_p \equiv (-1)^{n-1} B_n + \frac{1}{p} - 1 \pmod{p^2},$$

résultat qui est bien intéressant, ce me semble.

Revenons maintenant à la formule de BERNOULLI

$$S_{2n}(a-1) =$$
$$= \frac{a^p}{p} - \frac{a^{p-1}}{2} + \sum_{s=1}^{s=n} \frac{(-1)^{s-1} B_s}{2s} \binom{2n}{2s-1} B_s a^{p-2s},$$

puis appliquons la définition (1) et la congruence évidente

$$\binom{2n}{2s-1} \equiv -1 \pmod{p},$$

nous aurons après une réduction simple

$$a - 1 \equiv$$
$$\frac{a}{p} + a\,k_p(a) - \frac{1}{2} + (-1)^{n-1} B_n a + \sum_{s=1}^{s=n-1} \frac{(-1)^s B_s}{2s} a^{p-2s}$$
$$\pmod{p},$$

ou, ce qui est la même chose

$$(6) \quad k_p(a) \equiv -\frac{1}{2a} - K_p + \sum_{s=1}^{s=n-1} \frac{(-1)^{s-1} B_s}{2s} a^{2n-2s} \pmod{p},$$

Posons ensuite dans (6) $a = 1$, nous aurons conformément à (5) et la congruence (19) du paragraphe II

$$K_p \equiv -\frac{1}{2} + \sum_{s=1}^{s=n-1} \frac{(-1)^{s-1} B_s}{2s} \pmod{p},$$

ce qui donnera finalement

$$(7)\quad k_p(a) \equiv \frac{a-1}{2a} + \sum_{s-1}^{s=n-1} \frac{(-1)^{s-1} B_s}{2s} (a^{2n-2s} - 1) \pmod{p};$$

cette congruence, nouvelle que je sache, est entièrement différente de celle indiquée ordinairement pour $k_p(a)$, savoir[1]

$$(8)\qquad a\, k_p(a) \equiv \sum_{r=1}^{r=p-1} \frac{(-1)^{r-1}}{r} S_{p-r}(a-1) \pmod{p}.$$

Soit particulièrement $a = 2$, la formule (8) donnera

$$(9)\qquad k_p(2) \equiv \frac{1}{2} \lambda'(p-1) \pmod{p},$$

où nous avons posé pour abréger

$$(10)\qquad \lambda'(a) = \frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \cdots + \frac{(-1)^{a-1}}{a}, \quad a \geqq 1;$$

on sait que la congruence (9) est due à Eisenstein.[2]

Quant à la formule (6), elle donnera dans ce cas

$$k_p(2) \equiv -\frac{1}{4} - K_p + \sum_{s=1}^{s=n-1} \frac{(-1)^{s-1} B_s}{s} \cdot 2^{2n-2s},$$

d'où, en vertu de (9),

$$(11)\quad \left\{ \begin{aligned} &\sum_{s=1}^{s=n-1} \frac{(-1)^{s-1} B_s}{2s} \cdot 2^{2n-2s} \equiv \\ &\equiv \frac{1}{2} \lambda'(p-1) + (-1)^{n-1} B_n + \frac{1}{p} - \frac{3}{4} \pmod{p}, \end{aligned} \right.$$

congruence que je n'ai pas réussi à démontrer directement.

Étudions maintenant d'un autre point de vue le problème qui nous occupe ici.

[1] Voir par exemple M. P. Bachmann : Niedere Zahlentheorie, t. I, p. 161; Leipsic 1902.

[2] Berliner Monatsberichte 1850, p. 41.

A cet effet, nous prenons pour point de départ la factorielle ordinaire

$$\omega_m(x) = x(x+1)\dots(x+m-1), \quad m \geqq 1,$$

et nous posons ensuite

$$\omega_m(x) = x^m + C_m^1 x^{m-1} + \dots + C_m^{m-1} x,$$

où les C_m^r soit les coefficients de factorielle du rang m, ce qui donnera immédiatement

$$(12) \begin{cases} \omega_{p-1}(x+1) - (x^{p-1} - 1) = \\ = C_p^1 x^{p-2} + C_p^2 x^{p-3} + \dots + C_p^{p-2} x + (1 + (p-1)!). \end{cases}$$

Remarquons maintenant que le premier membre de (12) est toujours divisible par p pour

$$(13) \qquad x = 1, 2, 3, \dots, p-1,$$

il est évident que la congruence

$$C_p^1 x^{p-2} + C_p^2 x^{p-3} + \dots + C_p^{p-2} x + (1 + (p-1)!) \equiv 0 \pmod{p},$$

du degré $p-2$ par rapport à x, aura précisément les $p-1$ racines incongruentes (13); c'est-à-dire que nous aurons à la fois le théorème de WILSON

$$(14) \qquad (p-1)! + 1 \equiv 0 \pmod{p}$$

et les congruences de LAGRANGE[1]

$$(15) \qquad C_p^r \equiv 0 \pmod{p}, \quad 1 \leqq r \leqq p-2,$$

appliquées précisément dans sa démonstration du théorème de WILSON.

Posons, conformément à (14),

$$(16) \qquad (p-1)! = -1 + p W_p,$$

le nombre W_p, le quotient de WILSON, est un entier.

Soit maintenant a un des nombres (13), nous aurons

$$\frac{1}{p} \omega_{p-1}(a+1) \equiv -\frac{1}{a} \pmod{p}$$

$$\frac{1}{p} C_p^1 a^{p-2} = \frac{p-1}{2a} a^{p-1} \equiv -\frac{1}{2a} \pmod{p};$$

posons ensuite dans (12) $x = a$, puis divisons par p les deux membres de la formule ainsi obtenue, nous aurons immédiatement

[1] Nouveaux Mémoires de l'Académie de Berlin (1771) p. 125; 1773.

$$k_p(a) \equiv -\frac{1}{2a} - W_p - \sum_{s=2}^{s=p-2} \frac{C_p^s}{p} \cdot a^{2n-s} \pmod{p},$$

ce qui donnera, en vertu de (6),

$$K_p + \sum_{s=1}^{s=n-1} \frac{(-1)^s B_s}{2s} \cdot a^{2n-2s} \equiv$$

$$\equiv W_p + \sum_{s=2}^{s=n-2} \frac{C_p^s}{p} \cdot a^{2n-s} \pmod{p},$$

congruence qui est du degré $p-3$ par rapport à a; néanmoins elle aura les $p-1$ racines incongruentes (13); c'est-à-dire que nous aurons

$$W_p \equiv K_p \pmod{p} \tag{17}$$

$$\frac{1}{p} C_p^{2r} \equiv \frac{(-1)^r B_r}{2r} \pmod{p}, \quad 1 \leq r \leq \frac{p-3}{2}, \tag{18}$$

$$C_p^{2r+1} \equiv 0 \pmod{p^2}, \quad 1 \leq r \leq \frac{p-3}{2}. \tag{19}$$

La congruence (18) est due à M. Glaisher[1], tandis que Wolstenholme[2] a indiqué déjà la formule

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

Quant à la congruence (17), elle donnera en vertu de (5)

$$W_p \equiv (-1)^{n-1} B_n + \frac{1}{p} - 1 \pmod{p}, \tag{20}$$

congruence qui est généralement attribuée à M. Lerch[3]; néanmoins M. Kaj Löchte Jensen a observé qu'elle appartient à M. Glaisher[4] aussi.

Revenons maintenant à la formule (12) que nous écrivons sous la forme

$$\omega_{p-1}(a+1) - p\,k_p(a) =$$
$$= C_p^1 a^{p-2} + C_p^2 a^{p-3} + \ldots + C_p^{p-2} a + p\,W_p,$$

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

[2] Ibid. t. 5, p. 35—39; 1862.

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

[4] Loc. cit. p. 327.

puis introduisons, au lieu de a, les $p-1$ valeurs (13), nous aurons en ajoutant toutes les équations ainsi obtenues

$$\frac{1}{p}(\omega_p(p)-p!)-pK_p=$$
$$=\sum_{r=1}^{r=p-2} C_p^r S_{p-r-1}(p-1)+p(p-1)W_p,$$

ou, ce qui est la même chose,

$$\sum_{r=0}^{r=p-2} C_p^r p^{2n-r}-pK_p=$$
$$=\sum_{r=1}^{r=p-2} C_p^r S_{2n-r}(p-1)+p(p-1)W_p.$$

Appliquons ensuite les congruences

$$\frac{1}{p}S_{2r}(p-1)\equiv(-1)^{r-1}B_r \pmod{p},\quad 1\leq r\leq n-1$$
$$S_{2r+1}(p-1)\equiv 0 \pmod{p^2},\quad 1\leq r\leq n-1$$

nous aurons, en vertu de (18) et (19),

$$\text{(21)}\quad \frac{1}{p}(W_p-K_p)\equiv(-1)^n\cdot\sum_{s=1}^{s=n-1}\frac{B_s B_{n-s}}{s} \pmod{p},$$

ce qui donnera finalement, en vertu de (5),

$$\text{(22)}\quad \left\{\begin{array}{l}\frac{1}{p}\left(W_p+(-1)^n B_n-\frac{1}{p}+1\right)\equiv(-1)^n\cdot\sum_{s=1}^{s=n-1}\frac{B_s B_{n-s}}{s}\\ \pmod{p}.\end{array}\right.$$

Revenons encore une fois à la congruence (7), nous aurons le théorème suivant rélatif à un problème très difficil proposé par ABEL[1]:

La condition suffisante et nécessaire pour l'existence de la congruence

$$\text{(23)}\qquad a^{p-1}-1\equiv 0 \pmod{p^2},$$

où p est un nombre premier qui ne divise pas a, est réprésentée par l'autre congruence

[1] Journal de Crelle, t. 3; 1828. Œuvres t. I, p. 619.

$$(24)\quad \frac{1-a}{2a} \equiv \sum_{s=1}^{s=n-1} \frac{(-1)^{s-1} B_s}{2s} (a^{2n-2s}-1) \quad (\text{mod } p).$$

Quant au théorème de WILSON, savoir

$$(p-1)!+1 = p W_p,$$

nous aurons

$$1!+1=2, \quad 2!+1=3, \quad 4!+1=5^2,$$

tandis que LIOUVILLE[1] a démontré l'impossibilité d'une équation de la forme

$$(p-1)!+1 = p^k,$$

où p est un nombre premier plus grand que 5.

On voit que la congruence (20) de M. GLAISHER donnera immédiatement cet autre théorème:

La condition suffisante et nécessaire pour l'existence de la congruence

$$(25)\qquad (p-1)!+1 \equiv 0 \quad (\text{mod } p^2),$$

où p est un nombre premier, est réprésentée par l'autre congruence

$$(26)\qquad (-1)^n B_n - \frac{1}{p} + 1 \equiv 0 \quad (\text{mod } p).$$

On voit que la congruence (25) est remplie pour le nombre premier $p = 5$. De plus, nous aurons

$$-B_6 + \frac{1}{13} - 1 = -\frac{691}{2730} + \frac{1}{13} - 1 = -\frac{247}{210} \equiv 0 \,(\text{mod } 13),$$

ce qui donnera

$$12!+1 \equiv 0 \quad (\text{mod } 13^2)$$

on trouvera en effet

$$12!+1 = 478001601 = 169.2834329.$$

Il saute aux yeux que les deux théorèmes que nous venons d'énoncer indiquent des applications remarquables et profondes des nombres de BERNOULLI dans des problèmes trés intéressants et trés difficils de la théorie de nombres.

Mentionnons encore une application plus élémentaire des nombres de BERNOULLI, dèduite de la formule

[1] Journal de Mathématiques (2) t. 1, p. 351; 1856.

$$\frac{1}{p^2} C_p^{2n-1} \equiv \frac{(-1)^n (2n-1) B_{n-1}}{4n-4} \equiv \frac{(-1)^n B_{n-1}}{3} \pmod{p};$$

l'identité évidente

$$C_p^{2n-1} = (p-1)! \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}\right) =$$

$$= p! \sum_{r=1}^{r=n} \frac{1}{r(p-r)}$$

donnera tout d'abord

$$\sum_{r=1}^{r=n} \frac{1}{r(p-r)} \equiv 0 \pmod{p}; \tag{27}$$

de plus nous aurons

$$\frac{1}{p} \cdot \sum_{r=1}^{r=n} \frac{1}{r(p-r)} \equiv \frac{(-1)^{n-1}}{3} \cdot B_{n-1} \pmod{p}. \tag{28}$$