

ANNALES SCIENTIFIQUES DE L'É.N.S.

NIELS NIELSEN

Recherches sur les résidus quadratiques et sur les quotients de Fermat

Annales scientifiques de l'É.N.S. 3^e série, tome 31 (1914), p. 161-204

http://www.numdam.org/item?id=ASENS_1914_3_31__161_0

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1914, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (<http://www.elsevier.com/locate/ansens>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

RECHERCHES

SUR LES RÉSIDUS QUADRATIQUES

ET

SUR LES QUOTIENTS DE FERMAT,

PAR M. NIELS NIELSEN,
à Copenhague.

PREMIÈRE PARTIE.

FORMULES AUXILIAIRES.

I. — Séries arithmétiques d'ordre supérieur.

Dans les recherches qui nous occupent ici des sommes de la forme

$$b^n + (b + a)^n + (b + 2a)^n + \dots + (b + qa)^n,$$

où a, b, q et n désignent des positifs entiers, jouent un rôle fondamental; c'est pourquoi nous avons à donner, avant tout, quelques propriétés des sommes susdites.

A cet effet, nous prenons pour point de départ les fonctions de Bernoulli, savoir :

$$(1) \quad \left\{ \begin{array}{l} B_0(x) = 1, \quad B_1(x) = x + \frac{1}{2}, \\ B_n(x) = \frac{x^n}{n!} + \frac{1}{2} \frac{x^{n-1}}{(n-1)!} + \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s-1} B_s x^{n-2s}}{(2s)!(n-2s)!}, \end{array} \right.$$

où les B_n sont les nombres de Bernoulli; ces fonctions sont parfaite-

ment définies à l'aide des deux équations fonctionnelles

$$(2) \quad B'_n(x) = B_{n-1}(x),$$

$$(3) \quad B_n(x) - B_n(x-1) = \frac{x^{n-1}}{(n-1)!},$$

où il faut supposer $n \geq 1$.

Désignons en premier lieu par q un positif entier, l'équation aux différences finies (3) donnera

$$(4) \quad B_{n+1}(x+q) = B_{n+1}(x-1) + \frac{1}{n!} \sum_{s=0}^{s=q} (x+s)^n.$$

Soit particulièrement $x=0$, nous aurons par conséquent pour la somme de puissances

$$(5) \quad S_n(a) = 1^n + 2^n + 3^n + \dots + a^n,$$

où a désigne un positif entier, l'expression suivante :

$$(6) \quad S_n(a) = n! [B_{n+1}(a) - B_{n+1}(0)] \quad (n \geq 1),$$

ce qui donnera, en vertu de (1), la formule classique

$$(7) \quad S_n(a) = \frac{a^{n+1}}{n+1} + \frac{a^n}{2} + \sum_{s=1}^{\leq \frac{n}{2}} \frac{(-1)^{s-1}}{n-2s+1} \binom{n}{2s} B_s a^{n-2s+1},$$

indiquée par Jacques Bernoulli (1).

Quant à l'équation fonctionnelle (2), nous aurons le développement de Taylor,

$$(8) \quad B_{n+1}(x) = \sum_{s=0}^{s=n+1} \frac{(x+\alpha)^{n-s+1}}{(n-s+1)!} B_s(-\alpha),$$

où x et α sont des nombres complexes quelconques.

Cela posé, introduisons dans (8)

$$x = a, \quad \alpha = \frac{r}{q},$$

puis posons

$$(9) \quad aq + r = p,$$

(1) *Ars conjectandi*, p. 95-97; Bâle, 1713.

nous aurons, en vertu de (6),

$$(10) \quad S_n(a) = -n! B_{n+1}(0) + \sum_{s=0}^{s=n+1} \frac{n! p^{n-s+1}}{(n-s+1)! q^{n-s+1}} B_s\left(-\frac{r}{q}\right).$$

Posons ensuite, dans (8), $x + q$ au lieu de x , introduisons

$$x = \frac{b}{a}, \quad \alpha = \frac{c}{a},$$

puis posons

$$(11) \quad aq + b + c = p,$$

nous aurons de même, en vertu de (4),

$$(12) \quad \frac{1}{n! a^n} \sum_{s=0}^{s=q} (b + sa)^n = -B_{n+1}\left(-\frac{a-b}{a}\right) + \sum_{s=0}^{s=n+1} \frac{p^{n-s+1}}{(n-s+1)! a^{n-s+1}} B_s\left(-\frac{c}{a}\right).$$

Quant aux deux formules (10) et (12) qui sont essentielles dans nos recherches suivantes, nous avons à appliquer le théorème de v. Staudt (1) et de Th. Clausen (2) relatif aux nombres de Bernoulli.

A cet effet, nous dirons pour abrégé que le nombre premier impair p est du rang n , pourvu que $2n$ soit divisible par $p - 1$. Désignons ensuite par

$$(13) \quad \lambda_1, \lambda_2, \lambda_3, \dots, \lambda_\nu$$

l'ensemble des nombres premiers du rang n , nous aurons pour le $n^{\text{ième}}$ nombre de Bernoulli l'expression suivante :

$$(14) \quad (-1)^n B_n = A_n + \frac{1}{2} + \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \dots + \frac{1}{\lambda_\nu},$$

où A_n est un nombre entier.

Soit maintenant dans (10) p un nombre premier impair, tandis que q et r désignent des entiers non négatifs, nous aurons la

(1) *Journal de Crelle*, t. 21, 1840, p. 372-374.

(2) *Astronomische Nachrichten*, t. XVII, 1840, col. 351-352.

congruence

$$(15) \quad S_n(a) \equiv n! \left[B_{n+1}\left(-\frac{r}{q}\right) - B_{n+1}(0) \right] \pmod{p},$$

où il faut supposer $1 \leq n \leq p - 3$.

Soit également dans (12) p un nombre premier impair, a un positif entier, tandis que b et c désignent des entiers non négatifs, nous aurons de même

$$(16) \quad \sum_{s=0}^{s=q} (b + sa)^n \equiv n! a^n \left[B_{n+1}\left(-\frac{c}{a}\right) - B_{n+1}\left(-\frac{a-b}{a}\right) \right] \pmod{p},$$

où il faut supposer, comme dans (15), $1 \leq n \leq p - 3$.

Quant à la formule classique (7), désignons par p un nombre premier plus grand que 3, par m un entier plus grand que 2, tandis que s est un positif entier quelconque, je dis que nous aurons toujours

$$(17) \quad \frac{B_s p^m}{m} \equiv 0 \pmod{p^2}.$$

Il est évident que le cas le plus désavantageux est celui où p est du rang s et où m est en même temps divisible par p . Soit p^α la puissance la plus élevée qui divise m , nous avons par conséquent à démontrer que

$$m - 3 \geq \alpha.$$

Or, nous aurons évidemment

$$m \geq p^\alpha = [1 + (p - 1)]^\alpha,$$

ce qui donnera

$$m \geq 1 + \alpha(p - 1), \quad m - 3 \geq 4\alpha - 2 \geq 2\alpha > \alpha.$$

Cela posé, la formule

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

tirée directement de (7), donnera, en vertu de (17), ces deux

congruences, où il faut supposer $n \geq 1$:

$$(18) \quad S_{2n}(p-1) \equiv (-1)^{n-1} B_n p \pmod{p^2},$$

$$(19) \quad S_{2n+1}(p-1) \equiv (-1)^{n-1} \left(n + \frac{1}{2} \right) B_n p^2 \pmod{p^2}.$$

Supposons maintenant que le nombre premier p ne soit pas du rang n , nous aurons par conséquent pour $n \geq 1$

$$(20) \quad S_{2n}(p-1) \equiv 0 \pmod{p},$$

$$(21) \quad S_{2n+1}(p-1) \equiv 0 \pmod{p^2},$$

soit, au contraire, p du rang n , nous aurons toujours

$$(22) \quad S_{2n}(p-1) \equiv -1 \pmod{p}$$

et pour $2n + 1 > p$

$$(23) \quad S_{2n+1}(p-1) \equiv 0 \pmod{p},$$

tandis que l'hypothèse $p = 2n + 1$ donnera, à cause du facteur $n + \frac{1}{2}$ qui figure au second membre de (19),

$$(24) \quad S_p(p-1) \equiv 0 \pmod{p^2}.$$

II. — Formules relatives aux nombres de Bernoulli.

Soit $p = 2m + 1$ un nombre premier qui n'est pas du rang n , Kummer (1) a démontré la congruence remarquable

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

où il faut supposer

$$(2) \quad n \geq \frac{1}{2}(r+1).$$

Désignons maintenant pour abrégé par α_r l'expression qui figure

(1) *Journal de Crelle*, t. 41, 1851, p. 368-372.

au premier membre de (1), l'identité évidente

$$\binom{r}{s} \frac{n+rm}{n+sm} - \binom{r-1}{s} \frac{mr}{n+sm} = \binom{r}{s}$$

donnera immédiatement

$$(n+rm)\alpha_r - mr\alpha_{r-1} = \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} B_{n+sm};$$

c'est-à-dire que nous aurons aussi

$$(3) \quad \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} B_{n+sm} \equiv 0 \pmod{p^{r-1}}.$$

Cette dernière congruence, nouvelle peut-être, est analogue aux deux autres connues pour les nombres d'Euler et pour les coefficients des tangentes, savoir :

$$(4) \quad \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} E_{n+sm} \equiv 0 \pmod{p^r}, \quad n \geq \frac{r}{2},$$

$$(5) \quad \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} T_{n+sm} \equiv 0 \pmod{p^r}, \quad n \geq \frac{r+1}{2},$$

où le nombre premier p peut être du rang n aussi.

La première de ces deux congruences est due à Kummer (1), la seconde à Stern (2).

Or, il est très facile de généraliser beaucoup les trois dernières congruences. En effet, posons pour abréger

$$A_{r,q} = \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} \binom{n+sm}{q} \alpha_{n+sm},$$

l'identité évidente

$$\frac{n+rm-q}{q+1} \binom{r}{s} \binom{n+sm}{q} - \frac{rm}{q+1} \binom{r-1}{s} \binom{n+sm}{q} = \binom{r}{s} \binom{n+sm}{q+1}$$

(1) *Loc. cit.*, p. 372.

(2) *Journal de Crelle*, t. 88, 1889, p. 91.

donnera immédiatement

$$\frac{n + rm - q}{q + 1} A_{r,q} - \frac{rm}{q + 1} A_{r-1,q} = A_{r,q+1}.$$

Cela posé, les trois formules (3), (4) et (5) donnent ces trois autres congruences, où il faut supposer $p > q$:

$$(6) \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} \binom{n+sm}{q} B_{n+sm} \equiv 0 \pmod{p^{r-q-1}}, \quad n = \frac{r+1}{2},$$

$$(7) \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} \binom{n+sm}{q} E_{n+sm} \equiv 0 \pmod{p^{r-q}}, \quad n = \frac{r}{2},$$

$$(8) \sum_{s=0}^{s=r} (-1)^{s+sm} \binom{r}{s} \binom{n+sm}{q} T_{n+sm} \equiv 0 \pmod{p^{r-q}}, \quad n \geq \frac{r+1}{2},$$

qui semblent être nouvelles.

Il est évident du reste que l'on puisse, dans les trois dernières congruences, remplacer les coefficients binomiaux

$$\binom{n+sm}{q}$$

par le polynome quelconque du degré q

$$a_0(n+sm)^q + a_1(n+sm)^{q-1} + \dots + a_{q-1}(n+sm) + a_q,$$

dont les coefficients

$$a_0, a_1, a_2, \dots, a_q$$

sont des nombres entiers, ou, plus généralement, des nombres rationnels, dont les dénominateurs ne sont pas divisibles par p .

Dans les congruences (1), (3) et (6), nous avons supposé que le nombre premier impair ne soit pas du rang n , condition qui ne semble pas être nécessaire. Nous nous bornerons à démontrer ici seulement des formules particulières qui sont indispensables dans nos recherches suivantes.

A cet effet, nous prenons pour point de départ les sommes de puissances $S_n(a)$ définies dans la formule (5) du paragraphe I.

Désignons par m et r des positifs entiers, par α un entier non négatif,

nous aurons

$$\sum_{q=0}^{q=r} (-1)^q \binom{r}{q} S_{2\alpha+2qm}(\alpha) = \sum_{q=2}^{q=\alpha} q^{2\alpha} (1 - q^{2m})^r;$$

soit maintenant $p = 2m + 1$ un nombre premier, et soit $\alpha \leq p - 1$, nous aurons, en vertu du théorème de Fermat,

$$(9) \quad \sum_{q=0}^{q=r} (-1)^q \binom{r}{q} S_{2\alpha+2qm}(\alpha) \equiv 0 \pmod{p^r}.$$

Soit particulièrement $\alpha = p - 1$, la formule (18) du paragraphe I donnera pour $\alpha \geq 1$ et $r \geq 2$

$$(10) \quad \sum_{q=0}^{q=r} (-1)^{q+qm} \binom{r}{q} B_{\alpha+qm} \equiv 0 \pmod{p},$$

même dans le cas où le nombre premier p est du rang α .

Supposons maintenant $\alpha = 0$, nous avons, dans (9), à poser

$$S_0(p-1) = p-1,$$

ce qui donnera

$$(11) \quad 1 - \frac{1}{p} \equiv \sum_{q=1}^{q=r} (-1)^{q+qm} \binom{r}{q} B_{qm} \pmod{p}.$$

Il est évident que les termes qui contiennent le diviseur p disparaîtront dans la formule (11), et c'est la même chose pour la formule (10) dans le cas où p est du rang α .

Dans les recherches qui nous occupent ici, nous avons à appliquer les cas particuliers de (10) et (11) qui correspondent à $r = 2$, savoir :

$$(12) \quad B_{\alpha+2m} \equiv (-1)^m 2 B_{\alpha+m} - B_{\alpha} \pmod{p},$$

$$(13) \quad B_{2m} \equiv (-1)^m 2 B_{m+1} - \frac{1}{p} \pmod{p},$$

et le cas particulier $r = 1$ de la congruence de Kummer, savoir :

$$(14) \quad (-1)^m B_{m+n} \equiv \frac{m+n}{n} B_n \equiv \frac{2n-1}{2n} B_n \pmod{p}.$$

Posons dans (14) $2m + 1$ au lieu de m , savoir $p = 4m + 3$, puis remplaçons n par $m + 1$, nous aurons

$$(15) \quad B_{3m+2} \equiv B_{m+1} \pmod{p}.$$

En me réservant de revenir, dans une autre occasion, aux congruences que nous venons d'étudier, je remarque expressément que les objections que l'on a faites contre la démonstration de Kummer pour sa congruence (1) ne sont pas correctes, parce que la fonction

$$(e^{\alpha x} - e^{\beta x})^n,$$

où n désigne un positif entier, a dans $x = 0$ un zéro du $n^{\text{ième}}$ ordre; c'est-à-dire que les séries qui figurent dans la démonstration de l'illustre géomètre allemand sont toutes finies.

III. — Table des formules auxiliaires.

Pour ne pas interrompre le développement suivant, il nous semble utile d'énumérer ici une suite de formules particulières qui sont indispensables pour nos recherches sur les résidus quadratiques.

Soit $n \geq 1$, nous aurons (1)

- (1) $B_{2n}(0) - B_{2n}\left(-\frac{1}{2}\right) = \frac{(-1)^{n-1}(2^{2n}-1)B_n}{(2n)! 2^{2n-1}},$
- (2) $B_{2n}(0) - B_{2n}\left(-\frac{1}{3}\right) = \frac{(-1)^{n-1}(3^{2n}-1)B_n}{(2n)! 2 \cdot 3^{2n-1}},$
- (3) $B_{2n}(0) - B_{2n}\left(-\frac{1}{4}\right) = \frac{(-1)^{n-1}(2^{2n}-1)(2^{2n-1}+1)B_n}{(2n)! 2 \cdot 4^{2n-1}},$
- (4) $B_{2n}(0) - B_{2n}\left(-\frac{1}{6}\right) = \frac{(-1)^{n-1}(6^{2n-1}+3^{2n-1}+2^{2n-1}-1)B_n}{(2n)! 2 \cdot 6^{2n-1}},$
- (5) $B_{2n}\left(-\frac{1}{2}\right) - B_{2n}\left(-\frac{1}{3}\right) = \frac{(-1)^n(6^{2n-1}-2 \cdot 3^{2n-1}+2^{2n-1})B_n}{(2n)! 2 \cdot 6^{2n-1}},$
- (6) $B_{2n}\left(-\frac{1}{2}\right) - B_{2n}\left(-\frac{1}{4}\right) = \frac{(-1)^n(2^{2n}-1)(2^{2n-1}-1)B_n}{(2n)! 2 \cdot 4^{2n-1}},$
- (7) $B_{2n}\left(-\frac{1}{2}\right) - B_{2n}\left(-\frac{1}{6}\right) = \frac{(-1)^n(2^{2n-1}-1)(3^{2n}-1)B_n}{(2n)! 2 \cdot 6^{2n-1}},$
- (8) $B_{2n}\left(-\frac{1}{3}\right) - B_{2n}\left(-\frac{1}{4}\right) = \frac{(-1)^n(12^{2n-1}-6^{2n-1}-4^{2n-1}+3^{2n-1})B_n}{(2n)! 2 \cdot 12^{2n-1}},$
- (9) $B_{2n}\left(-\frac{1}{3}\right) - B_{2n}\left(-\frac{1}{6}\right) = \frac{(-1)^n(3^{2n-1}-1)(2^{2n}-1)B_n}{(2n)! 2 \cdot 6^{2n-1}},$
- (10) $B_{2n}\left(-\frac{1}{4}\right) - B_{2n}\left(-\frac{1}{6}\right) = \frac{(-1)^n(2^{2n-1}-1)(6^{2n-1}+3^{2n-1}-2^{2n-1})B_n}{(2n)! 2 \cdot 12^{2n-1}}.$

(1) Quant aux démonstrations, voir par exemple mon Mémoire: *Recherches sur les Ann. Éc. Norm., (3), XXXI. — AVRIL 1914.*

Soit encore $n \geq 1$, nous aurons de même

$$(11) \quad B_{2n+1}\left(-\frac{1}{2}\right) = B_{2n+1}(0) = 0,$$

$$(12) \quad B_{2n+1}\left(-\frac{1}{4}\right) = -B_{2n+1}\left(-\frac{3}{4}\right) = \frac{(-1)^n E_n}{(2n)! 2^{4n+2}},$$

où E_n désigne le $n^{\text{ième}}$ nombre d'Euler.

Soit x un nombre complexe quelconque, nous aurons généralement

$$(13) \quad B_n(-x-1) = (-1)^n B_n(x).$$

Il n'est pas possible de déterminer sous forme simple les valeurs numériques

$$(14) \quad B_{2n+1}\left(-\frac{1}{3}\right), \quad B_{2n+1}\left(-\frac{1}{6}\right),$$

où n désigne un positif entier quelconque.

DEUXIÈME PARTIE.

LES QUOTIENTS DE FERMAT.

IV. — Les quotients de Fermat, d'Euler et de Sylvester.

Soit $p = 2m + 1$ un nombre premier impair quelconque, et soit a un positif entier non divisible par p , le théorème de Fermat s'écrira sous la forme suivante :

$$(1) \quad a^{p-1} = 1 + pq(a),$$

où $q(a)$, le quotient de Fermat, est pour $a > 1$ un positif entier,

nombre de Bernoulli (Mémoires de l'Académie royale de Danemark, 7^e série, t. X, 1913, p. 302).

tandis que nous aurons

$$(2) \quad q(1) = 0.$$

Il est bien connu que les quotients de Fermat possèdent des propriétés analogues à celles des indices ou même des logarithmes (¹).

En effet, remplaçons dans (1) a par le positif entier b non divisible par p , puis multiplions les deux équations ainsi obtenues, nous aurons immédiatement

$$(3) \quad q(ab) \equiv q(a) + q(b) \pmod{p}.$$

Soient ensuite dans la congruence

$$ax \equiv b \pmod{p},$$

a et b premiers à p ; nous écrivons aussi

$$x \equiv \frac{b}{a} \pmod{p},$$

ce qui donnera, en vertu de (3),

$$(4) \quad q\left(\frac{b}{a}\right) \equiv q(b) - q(a) \pmod{p}.$$

Disons pour abrégé que la fraction

$$\frac{a}{b}$$

est première à p , pourvu que ni a ni b ne soient divisibles par p ; nous aurons le théorème suivant :

I. Soient a_1, a_2, \dots, a_r des nombres rationnels premiers à p , tels que

$$(5) \quad a_1 a_2 a_3 \dots a_r \equiv \pm 1 \pmod{p},$$

puis posons

$$(6) \quad a_1 a_2 a_3 \dots a_r = \pm (1 - pA),$$

(¹) Voir par exemple le beau Livre de M. BACHMANN, *Niedere Zahlentheorie*, t. I, Leipzig, 1902, p. 160.

nous aurons toujours

$$(7) \quad A \equiv \sum_{s=1}^{s=r} q(a_s) \pmod{p}$$

En effet, la formule (6) donnera

$$(a_1 a_2 a_3 \dots a_r)^{p-1} = 1 - (p-1)pA + p^2 K,$$

ce qui nous conduira immédiatement à la congruence (7).

Choisissons par exemple de l'ensemble

$$1, 2, 3, \dots, p-1,$$

$2r$ nombres différents

$$(8) \quad \begin{cases} a_1 & a_2 & a_3 & \dots & a_r, \\ b_1 & b_2 & b_3 & \dots & b_r, \end{cases}$$

de sorte que nous aurons pour $1 \leq s \leq r$

$$(9) \quad a_s + b_s = p;$$

l'identité évidente

$$(10) \quad a_1 a_2 a_3 \dots a_r = (p - b_1)(p - b_2) \dots (p - b_r)$$

donnera

$$(11) \quad \frac{a_1 a_2 \dots a_r}{b_1 b_2 \dots b_r} \equiv (-1)^r \pmod{p}.$$

Posons ensuite

$$(12) \quad \frac{a_1 a_2 \dots a_r}{b_1 b_2 \dots b_r} = (-1)^r (1 - pA),$$

nous aurons en vertu de (10)

$$(13) \quad A \equiv \frac{1}{b_1} + \frac{1}{b_2} + \dots + \frac{1}{b_r} \pmod{p},$$

tandis que le théorème I donnera de même

$$(14) \quad A \equiv \sum_{s=1}^{s=r} q(a_s) - \sum_{s=1}^{s=r} q(b_s) \pmod{p}.$$

Ces remarques faites, nous avons à mentionner quelques relations

intéressantes entre les quotients de Fermat et d'autres nombres essentiels.

Soit en premier lieu, comme ordinairement,

$$\left(\frac{a}{p}\right) = \pm 1$$

le symbole de Legendre, nous aurons une égalité de la forme

$$(15) \quad a^m = \left(\frac{a}{p}\right) [1 + pq_1(a)], \quad p = 2m + 1,$$

où $q_1(a)$, le quotient d'Euler, est un nombre entier, ce qui donnera

$$a^{p-1} = 1 + 2pq_1(a) + p^2q_1^2(a),$$

de sorte que nous aurons, en vertu de (1), la congruence bien connue (1)

$$(16) \quad q(a) \equiv 2q_1(a) \pmod{p}.$$

Soit en second lieu a un positif entier quelconque, Sylvester (2) a démontré que le produit

$$(17) \quad \frac{a^{2m}(a^{2m}-1)B_m}{2m} = q_2(a)$$

est toujours un positif entier; nous désignons $q_2(a)$ comme le quotient de Sylvester. Il est bien connu que Lipschitz (3) a retrouvé le résultat susdit de Sylvester. J'ai démontré du reste que $q_2(a)$ est toujours divisible par a^{m-1} , c'est-à-dire que le produit

$$\frac{a^{m+1}(a^{2m}-1)B_m}{2m}$$

est un positif entier, pourvu que a le soit (4).

Désignons maintenant par

$$\lambda_1 \lambda_2 \lambda_3 \dots \lambda_v$$

(1) Voir le beau Mémoire de M. LERCH, *Mathematische Annalen*, t. LX, 1905, p. 479.

(2) *Philosophical Magazine*, février 1861.

(3) *Journal de Crelle*, t. 96, 1884, p. 3; *Bull. des Sc. math.*, 2^e série, t. X, 1886, p. 141.

(4) *Mémoires de l'Académie royale de Danemark*, 7^e série, t. X, 1913, p. 350.

l'ensemble des nombres premiers du rang m , l'expression

$$\frac{\alpha^{2m}(\alpha^{2m}-1)}{2\lambda_1\lambda_2\dots\lambda_\nu}$$

est en vertu du théorème de Fermat un nombre entier.

Soit ensuite $2m+1=p$ un nombre premier, tandis que a ne soit pas divisible par p ; nous aurons, en vertu du théorème de v. Staudt et de Th. Clausen, savoir la formule (14) du paragraphe I :

$$(-1)^m a^{2m}(\alpha^{2m}-1)B_m \equiv \frac{\alpha^{2m}(\alpha^{2m}-1)}{p} \pmod{p},$$

ce qui donnera immédiatement

$$(18) \quad q(a) \equiv (-1)^{m-1} q_2(a) \pmod{p},$$

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

II. *Désignons par $p=2m+1$ un nombre premier impair quelconque, par a un positif entier qui n'est pas divisible par p , les quotients de Fermat $q(a)$, d'Euler $q_1(a)$ et de Sylvester $q_2(a)$ sont liés par les congruences*

$$(19) \quad q(a) \equiv 2q_1(a) \equiv (-1)^{m-1} q_2(a) \pmod{p}.$$

Soit particulièrement $a=2$, nous aurons

$$q_2(2) = \frac{2^{2m}(2^{2m}-1)T_m}{2m} = T_m,$$

où T_m est le $m^{\text{ième}}$ coefficient des tangentes, ce qui donnera en vertu de (19)

$$(20) \quad q(2) \equiv 2q_1(2) \equiv (-1)^{m-1} T_m \pmod{p}.$$

Revenons maintenant à la formule (15), nous aurons la congruence

$$(21) \quad \left(\frac{a}{p}\right) \equiv a^m \pmod{p}$$

et l'identité ultérieure

$$\alpha^{2m} = \left(\frac{a}{p}\right) [1 + 3pq_1(a) + 3p^2q_1^2(a) + p^3q_1^3(a)],$$

ce qui donnera en vertu de (15)

$$(22) \quad 2 \left(\frac{\alpha}{p} \right) \equiv 3\alpha^m - \alpha^{3m} \pmod{p^2}.$$

Nous aurons de même

$$(23) \quad 8 \left(\frac{\alpha}{p} \right) \equiv 15\alpha^m - 10\alpha^{3m} + 3\alpha^{5m} \pmod{p^3},$$

et ainsi de suite.

V. — Expressions explicites diverses.

Soit p un entier plus grand que l'unité, et soit n un entier non négatif; nous posons pour abrégier

$$(1) \quad \mathfrak{A}_p^n = \sum_{s=0}^{s=p-2} (-1)^s \binom{p-1}{s} (p-s-1)^n,$$

$$(2) \quad A_p^n = \sum_{s=0}^{s=p-2} \binom{p-1}{s} (p-s-1)^n,$$

ce qui donnera immédiatement

$$(3) \quad \mathfrak{A}_p^0 = (-1)^p, \quad A_p^0 = 2^{p-1} - 1;$$

de plus, les principes du calcul aux différences finies donnent

$$(4) \quad \begin{cases} \mathfrak{A}_p^n = 0 & (1 \leq n \leq p-2), \\ \mathfrak{A}_p^{p-1} = (p-1)! \end{cases}$$

Soit maintenant p un nombre premier impair, tandis que le positif entier a n'est pas divisible par p ; nous aurons, en vertu de la formule (1) du paragraphe IV,

$$(5) \quad p a^n q(a) = a^{n+p-1} - a^n,$$

ce qui donnera, en vertu des définitions (1) et (2),

$$(6) \quad p \sum_{s=0}^{s=p-2} (-1)^s \binom{p-1}{s} (p-s-1)^n q(p-s-1) = \mathfrak{A}_p^{n+p-1} - \mathfrak{A}_p^n,$$

$$(7) \quad p \sum_{s=0}^{s=p-2} \binom{p-1}{s} (p-s-1)^n q(p-s-1) = A_p^{n+p-1} - A_p^n,$$

d'où, particulièrement pour $n = 0$,

$$(8) \quad p \sum_{s=0}^{s=p-2} (-1)^s \binom{p-1}{s} q(p-s-1) \equiv (p-1)! + 1,$$

$$(9) \quad p \sum_{s=0}^{s=p-2} \binom{p-1}{s} q(p-s-1) \equiv A_p^{p-1} - pq(2).$$

Cela posé, nous aurons les deux congruences

$$(10) \quad (p-1)! + 1 \equiv 0 \pmod{p}, \quad A_p^{p-1} \equiv 0 \pmod{p},$$

dont la première n'est autre chose que le théorème de Wilson.

Posons pour abrégé

$$(11) \quad (p-1)! + 1 = pW_p, \quad A_p^{p-1} = pW'_p,$$

les formules (8) et (9) donnent pour les deux quotients W_p et W'_p ainsi définis les expressions explicites suivantes :

$$(12) \quad W_p = \sum_{s=0}^{s=p-2} (-1)^s \binom{p-1}{s} q(p-s-1),$$

$$(13) \quad W'_p = q(2) + \sum_{s=0}^{s=p-2} \binom{p-1}{s} q(p-s-1).$$

Appliquons ensuite la congruence évidente

$$\binom{p-1}{s} \equiv (-1)^s \pmod{p},$$

nous aurons de plus

$$(14) \quad W_p \equiv \sum_{s=0}^{s=p-2} q(p-s-1) \pmod{p}.$$

$$(15) \quad W'_p \equiv q(2) + \sum_{s=0}^{s=p-2} (-1)^s q(p-s-1) \pmod{p};$$

la première de ces deux congruences est due à M. Lerch (1).

(1) *Mathematische Annalen*, t. LX, 1905, p. 472.

Supposons connu le théorème de Wilson, savoir la première des formules (11), la congruence de M. Lerch est une conséquence immédiate de notre théorème I du paragraphe IV, démonstration qui coïncide avec celle de M. Lerch.

Quant à la congruence (15), posons en vertu de la formule (12) du paragraphe IV

$$(16) \quad \frac{2.4.6 \dots (p-1)}{1.3.5 \dots (p-2)} = (-1)^m (1 - p\omega_p) \quad (p = 2m + 1),$$

nous aurons par conséquent les deux congruences

$$(17) \quad \omega_p \equiv \frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \pmod{p},$$

$$(18) \quad \omega_p \equiv \sum_{s=0}^{s=p-2} (-1)^s q(p-s-1) \pmod{p},$$

ce qui donnera, en vertu de (15),

$$(19) \quad W'_p \equiv \omega_p + q(2) \pmod{p}.$$

Pour trouver maintenant une expression explicite du quotient de Fermat $q(a)$, nous posons dans l'identité

$$(x+1)^p - x^p = \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \dots + \binom{p}{p-1} x + 1$$

successivement $x = 1, 2, 3, \dots, a-1$, puis nous ajoutons toutes les équations ainsi obtenues. De cette manière nous aurons la formule

$$(20) \quad a^p - a = \sum_{r=1}^{r=p-1} \binom{p}{r} S_{p+r}(a-1),$$

connue déjà par Euler (1).

Il est évident que la formule (20) donnera une nouvelle démonstration du théorème de Fermat; de plus, nous aurons, en divisant par p ,

$$(21) \quad a q(a) = \sum_{r=1}^{r=p-1} \frac{1}{r} \binom{p-1}{r-1} S_{p-r}(a-1),$$

(1) *Institutiones calculi differentialis*, Saint-Petersbourg, 1755, p. 406.

d'où, particulièrement pour $a = 2$,

$$(22) \quad {}_2q(2) = \sum_{r=1}^{r=p-1} \frac{1}{r} \binom{p-1}{r-1}.$$

Introduisons maintenant dans (12), au lieu des $q(p-s-1)$, les expressions correspondantes tirées de (21), nous aurons une expression explicite, mais très compliquée, pour le nombre W_p .

Remarquons que les formules (21) et (22) donnent les congruences suivantes :

$$(23) \quad a q(a) \equiv \sum_{r=1}^{r=p-1} \frac{(-1)^{r-1}}{r} S_{p-r}(a-1) \pmod{p},$$

$$(24) \quad {}_2q(2) \equiv \sum_{r=1}^{r=p-1} \frac{(-1)^{r-1}}{r} \pmod{p}.$$

Appliquons ensuite l'identité évidente

$$\frac{1}{a} + \frac{1}{p-a} = \frac{p}{a(p-a)},$$

nous aurons

$$(25) \quad \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p},$$

ce qui donnera, en vertu de (24),

$$(26) \quad q(2) \equiv \frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \pmod{p},$$

de sorte que nous aurons, en appliquant les congruences (15), (17) et (19), les résultats suivants :

$$(27) \quad \omega_p \equiv q(2) \pmod{p}, \quad W'_p \equiv {}_2q(2) \pmod{p},$$

$$(28) \quad \sum_{s=3}^{s=p-1} (-1)^s q(s) \equiv 0 \pmod{p}.$$

Posons ensuite $p = 2m + 1$, nous aurons de plus

$$(29) \quad W'_p \equiv (-1)^{m-1} {}_2T_m \pmod{p}.$$

Dans le paragraphe suivant, nous avons à étudier des généralisa-

tions très étendues des deux sommes qui figurent aux seconds membres des deux congruences (14) et (15).

VI. — Détermination des sommes diverses.

Posons dans la formule

$$(1) \quad a^n q(a) = \frac{a^{n+2m} - a^n}{p} \quad (p = 2m + 1),$$

où n désigne un entier non négatif, successivement

$$a = 1, 2, 3, \dots, p - 1,$$

puis ajoutons toutes les équations ainsi obtenues, nous aurons

$$(2) \quad \sum_{a=1}^{a=p-1} a^n q(a) = \frac{S_{n+2m}(p-1) - S_n(p-1)}{p}.$$

Soit tout d'abord $n = 0$, la formule (18) du paragraphe I donnera immédiatement

$$(3) \quad \sum_{a=1}^{a=p-1} q(a) \equiv (-1)^{m-1} B_m + \frac{1}{p} - 1 \pmod{p},$$

tandis que l'hypothèse $n = 1$ donnera de même

$$(4) \quad \sum_{a=1}^{a=p-1} a q(a) \equiv \frac{1}{2} \pmod{p},$$

congruences qui sont dues à M. Lerch (1). Combinons ensuite (3) et la formule (14) du paragraphe V, nous aurons par conséquent

$$(5) \quad W_p \equiv (-1)^{m-1} B_m + \frac{1}{p} - 1 \pmod{p},$$

formule qui est indiquée par M. Lerch (2). Dans le paragraphe X nous avons à donner une autre démonstration de la congruence (5).

(1) *Mathematische Annalen*, t. LX, 1905, p. 477.

(2) *Loc. cit.*, p. 488.

Soit maintenant dans (2) n un positif entier pair, nous remplaçons n par $2n$, ce qui donnera, en vertu de la formule (14) du paragraphe II,

$$(6) \quad \sum_{a=1}^{a=p-1} a^{2n} q(a) \equiv \frac{(-1)^n B_n}{2n} \pmod{p}, \quad n \geq 1.$$

Remplaçons ensuite dans (2) n par $2n + 1$, nous aurons

$$(7) \quad \sum_{a=1}^{a=p-1} a^{2n+1} q(a) \equiv 0 \pmod{p}, \quad n \geq 1;$$

appliquons ensuite la congruence (14) du paragraphe II, un simple calcul donnera

$$(8) \quad \frac{1}{p} \sum_{a=1}^{a=p-1} a^{2n+1} q(a) \equiv (-1)^n B_n \pmod{p}, \quad n \geq 1.$$

Il est digne de remarque, ce me semble, que les seconds membres des formules (6) et (8) sont indépendants du nombre premier p .

Posons pour abrégé

$$\sigma_n(a) = a^n - (a-1)^n + (a-2)^n + \dots + (-1)^{a-1} 1^n,$$

la formule (1) donnera de même

$$(9) \quad \sum_{a=1}^{a=p-1} (-1)^a a^n q(a) = \frac{\sigma_{n+2m}(p-1) - \sigma_n(p-1)}{p}.$$

Or, $\sigma_{2n+1}(p-1)$ n'étant pas généralement divisible par p , nous nous bornerons à l'étude du cas où n est un nombre pair, et nous remplaçons n par $2n$, de sorte que nous avons à appliquer la formule d'Euler (1)

$$(10) \quad \sigma_{2n}(p-1) = \frac{p^{2n}}{2} + \sum_{r=1}^{r=n} \frac{(-1)^r}{2^{2r}} \binom{2n}{2r-1} T_r p^{2n-2r+1}.$$

Soit tout d'abord $n = 0$, nous aurons

$$\sigma_0(p-1) = 0,$$

(1) *Institutiones calculi differentialis*, Saint-Petersbourg, 1755, p. 499.

ce qui donnera

$$(11) \quad \sum_{a=1}^{a=p-1} (-1)^a q(a) \equiv \frac{(-1)^m 2^m T_m}{2^{2m}} \pmod{p^2},$$

ou, ce qui est la même chose,

$$(12) \quad \sum_{a=1}^{a=p-1} (-1)^a q(a) \equiv q(2) \pmod{p},$$

de sorte que nous aurons une nouvelle démonstration de la formule (28) du paragraphe V, savoir

$$(13) \quad \sum_{a=3}^{a=p-1} (-1)^a q(a) \equiv 0 \pmod{p}.$$

Appliquons maintenant la congruence

$$\frac{2^m}{2^m} + 1 \equiv p q(2) \equiv (-1)^{m-1} p T_m \pmod{p},$$

nous aurons, en vertu de (11), la formule curieuse

$$(14) \quad \frac{1}{p} \sum_{a=3}^{a=p-1} (-1)^a q(a) \equiv -T_m^2 \pmod{p}.$$

Posons, dans la congruence (5) du paragraphe II, $r = 1$, nous aurons, en appliquant les formules (9) et (10), ce résultat plus général

$$(15) \quad \sum_{a=1}^{a=p-1} (-1)^a a^{2n} q(a) \equiv \frac{(-1)^{n-1} T_n}{2^{2n}} \pmod{p}, \quad n \geq 1;$$

remarquons en passant que le second membre de (15) est indépendant du nombre premier p .

La formule (1) donnera encore, en vertu de la congruence (21) du paragraphe IV,

$$(16) \quad \sum_{a=1}^{a=p-1} a^n \left(\frac{a}{p}\right) q(a) \equiv \frac{S_{n+3m}(p-1) - S_{n+m}(p-1)}{p} \pmod{p}.$$

Soit en premier lieu $n + m$ un nombre pair, savoir

$$(17) \quad n + m = 2r,$$

nous aurons, en vertu de la congruence (14) du paragraphe II,

$$(18) \quad \sum_{a=1}^{a=p-1} a^n \left(\frac{a}{p}\right) q(a) \equiv \frac{(-1)^r B_r}{2r} \pmod{p}.$$

Posons particulièrement $n = 0$, ce qui donnera $m = 2r$, $p = 4r + 1$, puis remplaçons r par m , nous aurons par conséquent

$$(19) \quad \sum_{a=1}^{a=p-1} \left(\frac{a}{p}\right) q(a) \equiv (-1)^{m-1} 2B_m \pmod{p}, \quad p = 4m + 1;$$

cette congruence particulière est due à M. Lerch ⁽¹⁾.

Soit en second lieu $n + m$ un nombre impair, savoir

$$(20) \quad n + m = 2r + 1;$$

la formule (16) donnera

$$(21) \quad \sum_{a=1}^{a=p-1} a^n \left(\frac{a}{p}\right) q(a) \equiv 0 \pmod{p}.$$

Appliquons maintenant la congruence (22) du paragraphe IV, nous aurons dans ce cas

$$\sum_{a=1}^{a=p-1} a^n \left(\frac{a}{p}\right) q(a) \equiv \frac{4S_{2r+2m+1}(p-1) - 3S_{2r+1}(p-1) - S_{2r+4m+1}(p-1)}{2p} \pmod{p^2},$$

ce qui donnera, en vertu des congruences (12) et (14) du paragraphe II,

$$(22) \quad \frac{1}{p} \sum_{a=1}^{a=p-1} a^n \left(\frac{a}{p}\right) q(a) \equiv \frac{(-1)^r (4r+1)}{4r} B_r \pmod{p}.$$

Posons $n = 0$, ce qui donnera $m = 2r + 1$, $p = 4r + 3$; nous aurons,

(1) *Mathematische Annalen*, t. LX, 1905, p. 480.

en remplaçant r par m ,

$$(23) \quad \frac{1}{p} \sum_{a=1}^{a=p-1} \left(\frac{a}{p}\right) q(a) \equiv (-1)^m \frac{2}{3} B_m \pmod{p}, \quad p = 4m + 3.$$

Nous aurons de même

$$\sum_{a=1}^{a=p-1} (-1)^a a^n \left(\frac{a}{p}\right) q(a) \equiv \frac{\sigma_{n+3m}(p-1) - \sigma_{n+m}(p-1)}{p} \pmod{p},$$

ce qui donnera, en vertu de la congruence (5) du paragraphe II, pourvu que $n + m = 2r$,

$$(24) \quad \sum_{a=1}^{a=p-1} (-1)^a a^n \left(\frac{a}{p}\right) q(a) \equiv \frac{(-1)^{r-1} T_r}{2^{2r}} \pmod{p}.$$

Soit particulièrement $n = 0$, ce qui donnera $m = 2r$, $p = 4r + 1$; nous aurons, en remplaçant r par m ,

$$(25) \quad \sum_{a=1}^{a=p-1} (-1)^a \left(\frac{a}{p}\right) q(a) \equiv -T_m \pmod{p}, \quad p = 4m + 1.$$

TROISIÈME PARTIE.

LES RÉSIDUS QUADRATIQUES.

VII. — Nombres des résidus dans un intervalle donné.

Soit $p = 2m + 1$ un nombre premier impair quelconque, et soit a un entier qui satisfait à la condition

$$1 \leq a \leq p - 1,$$

nous désignons par $R(a)$ le nombre des résidus quadratiques de p qui se trouvent parmi les nombres

$$(1) \quad 1, 2, 3, \dots, a,$$

tandis que $I(a)$ est le nombre des non-résidus trouvés parmi les nombres (1).

Cela posé, nous aurons évidemment

$$(2) \quad R(a) + I(a) = a;$$

soit ensuite a un résidu quadratique de p , nous aurons

$$\left(\frac{a}{p}\right) = 1,$$

tandis que nous trouvons

$$\left(\frac{a}{p}\right) = -1,$$

pourvu que a soit un non-résidu de p .

Appliquons ensuite la congruence (21) du paragraphe IV, nous aurons par conséquent

$$(3) \quad R(a) - I(a) \equiv S_m(a) \pmod{p},$$

ce qui donnera, en vertu de la congruence (15) du paragraphe I, le théorème suivant :

I. Soit $p = 2m + 1$ un nombre premier impair quelconque, puis posons

$$(4) \quad aq + r = p,$$

les définitions susdites de $R(a)$ et $I(a)$ donnent

$$(5) \quad R(a) - I(a) \equiv m! \left[B_{m+1}\left(-\frac{r}{q}\right) - B_{m+1}(0) \right] \pmod{p}.$$

Désignons ensuite par a_1 un autre entier tel que $a < a_1 \leq p - 1$, puis posons

$$(6) \quad a_1 q_1 + r_1 = p;$$

il est évident qu'on pourrait, en vertu du théorème susdit, déterminer les nombres des résidus ou des non-résidus parmi les nombres

$$a + 1, \quad a + 2, \quad \dots, \quad a_1;$$

c'est-à-dire que les fonctions de Bernoulli jouent un rôle fondamental dans la théorie des résidus quadratiques.

Dans ce qui suit nous ne donnons que les applications qui permettent de déterminer sous forme simple le second membre de (5).

Première application : $r = q = 1$, $a = p - 1$. — Nous aurons le résultat évident

$$(7) \quad R(p-1) = I(p-1) = m.$$

Deuxième application : $q = 2$, $r = 1$, $a = m$. — Les formules (1) et (11) du paragraphe III montrent qu'il sera nécessaire de considérer séparément les deux cas suivants :

1° m est un nombre pair, savoir $m = 2n$, $p = 4n + 1$; nous aurons le résultat évident

$$(8) \quad R(2n) = I(2n) = n;$$

2° Soit, au contraire, m un nombre impair, savoir $m = 2n + 1$, $p = 4n + 3$; nous aurons, en vertu de la formule (1) du paragraphe III,

$$(9) \quad R(2n+1) - I(2n+1) \equiv \frac{(-1)^{n+1}(2^{2n+2}-1)B_{n+1}}{(4n+4)2^{2n}} \pmod{p}$$

ou, ce qui est la même chose,

$$(10) \quad R(2+1) - I(2n+1) \equiv (-1)^{n+1} 2 T_{n+1} \pmod{p}.$$

Appliquons ensuite l'égalité

$$\left(\frac{2}{4n+3}\right) = (-1)^{n-1},$$

nous aurons pour n pair, savoir $p = 8m + 3$,

$$(11) \quad R(4m+1) - I(4m+1) \equiv -6B_{2m+1} \pmod{p},$$

tandis que l'hypothèse $p = 8m + 7$ donnera de même

$$(12) \quad R(4m+3) - I(4m+3) \equiv 2B_{2m+2} \pmod{p}.$$

Ces deux résultats sont dus à Cauchy (1).

Remarquons en passant que Lagrange (2), dans sa démonstration du théorème de Wilson, a indiqué la congruence

$$(2m+1)! \equiv (-1)^\delta \pmod{p}, \quad p = 4m+3,$$

et que Dirichlet (3) a indiqué l'égalité

$$\delta = \mathbf{I}(2m+1).$$

Troisième application : $q = 4$. — Nous avons à étudier séparément les deux cas suivants :

1° $p = 4m+1$, $a = m$, $r = 1$; ce qui donnera, en vertu de la formule (12) du paragraphe III,

$$(13) \quad \mathbf{R}(m) - \mathbf{I}(m) \equiv \frac{(-1)^m \mathbf{E}_m}{4} \pmod{p};$$

2° $p = 4m+3$, $a = m$, $r = 3$; la formule (3) du paragraphe III donnera

$$(14) \quad \mathbf{R}(m) - \mathbf{I}(m) \equiv (-1)^{m+1} (2^{2m+2} - 1) (2^{2m+1} + 1) \mathbf{B}_{m+1} \pmod{p}.$$

Soit ensuite

$$m = 2n, \quad p = 8n+3, \quad \left(\frac{2}{p}\right) = -1;$$

nous aurons

$$\mathbf{R}(2n) = \mathbf{I}(2n) = n,$$

tandis que l'hypothèse

$$m = 2n+1, \quad p = 8n+7, \quad \left(\frac{2}{p}\right) = 1$$

donnera de même

$$(15) \quad \mathbf{R}(2n+1) - \mathbf{I}(2n+1) \equiv 2 \mathbf{B}_{2n+2} \pmod{p}.$$

Quatrième application : $q = 3$. — Nous avons à étudier séparément les deux cas suivants :

(1) *Mémoires de l'Institut*, t. XVII, 1840 (1830), p. 265-266, 442-443.

(2) *Nouveaux Mémoires de l'Académie de Berlin*, t. II, 1773 (1771), p. 125-137.

(3) *Journal de Crelle*, t. 3, 1828, p. 407-408. (*Werke*, t. I, Berlin, 1889, p. 107-108.)

1° $p = 12m + 7$, $a = 4m + 2$, $r = 1$, $\left(\frac{3}{p}\right) = -1$; ce qui donnera, en vertu de la formule (2) du paragraphe III,

$$(16) \quad R(4m + 2) - I(4m + 2) \equiv (-1)^m 4B_{3m+2} \pmod{p};$$

2° $p = 12m + 11$, $a = 4m + 3$, $r = 2$, $\left(\frac{3}{p}\right) = 1$; nous aurons ici

$$(17) \quad R(4m + 3) - I(4m + 3) \equiv (-1)^m 2B_{3m+3} \pmod{p}.$$

Cinquième application : $q = 6$. — Nous avons à étudier les mêmes cas comme dans l'application précédente :

1° $p = 12m + 7$, $a = 2m + 1$, $r = 1$; ce qui donnera, en vertu de la formule (4) du paragraphe III,

$$(18) \quad R(2m + 1) - I(2m + 1) \equiv (-1)^m 2B_{3m+2} \pmod{p};$$

2° $p = 12m + 11$, $a = 2m + 1$, $r = 5$; nous aurons dans ce cas

$$(19) \quad R(2m + 1) - I(2m + 1) \equiv (-1)^m 2B_{3m+3} \pmod{p}.$$

VIII. — Nombre des résidus dans une série arithmétique.

Soit $p = 2m + 1$ un nombre premier impair, et soit a un positif entier plus petit que p ; nous avons à étudier les nombres $R_{a,b}$ et $I_{a,b}$ des résidus respectivement des non-résidus qui se trouvent parmi les termes de la série arithmétique

$$(1) \quad b, \quad b + a, \quad b + 2a, \quad \dots, \quad b + qa,$$

où il faut supposer

$$b + qa < p \quad (1 \leq b \leq a).$$

Ces définitions adoptées, nous aurons tout d'abord

$$(2) \quad R_{a,b} + I_{a,b} = q + 1;$$

posons ensuite

$$p = am + d \quad (1 \leq d \leq a - 1);$$

nous avons à déterminer le nombre entier c , tel que

$$(3) \quad b + c + aq = p \quad (0 \leq c \leq a - 1),$$

ce qui donnera

$$(4) \quad \begin{cases} b + c = d, & m = q & (b \leq d), \\ b + c = a + d, & m = q + 1 & (b > d). \end{cases}$$

Remarquons maintenant que la congruence (21) du paragraphe IV donnera cette autre

$$(5) \quad R_{a,b} - I_{a,b} \equiv \sum_{s=0}^{s=q} (b + as)^m \pmod{p};$$

nous aurons, en vertu de la formule (16) du paragraphe I, le théorème suivant :

I. Soient $R_{a,b}$ et $I_{a,b}$ les nombres des résidus respectivement des non-résidus parmi les termes de la série arithmétique (1), nous aurons avec la définition (3) du nombre c

$$(6) \quad R_{a,b} - I_{a,b} \equiv m! a^m \left[B_{m+1} \left(-\frac{c}{a} \right) - B_{m+1} \left(-\frac{a-b}{a} \right) \right] \pmod{p}.$$

L'étude des nombres $R_{a,b}$ et $I_{a,b}$ est par conséquent aussi réduite à l'étude des fonctions de Bernoulli des arguments rationnels.

Considérons tout d'abord l'équation (4), puis supposons donnés les nombres a et b , nous avons à choisir un autre positif entier b_1 , tel que

$$(7) \quad b + b_1 = d \quad \text{ou} \quad b + b_1 = a + d,$$

selon que $b < d$ ou $b \geq d$.

Cela posé, la formule (6) donnera, en vertu de l'équation fonctionnelle (13) du paragraphe III,

$$(8) \quad R_{a,b} - I_{a,b} = (-1)^m (R_{a,b_1} - I_{a,b_1}),$$

résultat qui est évident du reste.

Soit maintenant d un nombre pair, savoir $d = 2\delta$, ce qui exige a impair; soit ensuite $a + d = 2\delta$, ce qui exige aussi a impair; nous

aurons en posant, dans (7), $b = b_1 = \hat{c}$,

$$(9) \quad \begin{cases} R_{a,\delta} = I_{a,\delta}, & p = 4m + 3, \\ R_{a,\delta} - I_{a,\delta} \equiv (2m)! 2 a^{2m} B_{2m+1} \left(-\frac{\delta}{a}\right) \pmod{p}, & p = 4m + 1; \end{cases}$$

le premier de ces deux résultats est évident aussi.

Dans nos recherches suivantes, nous nous bornons à l'étude de tels cas particuliers, dont les résultats se présentent sous forme simple.

Première application : a = 2. — Nous avons à étudier séparément les deux cas suivants :

1° $p = 4m + 1$; nous aurons les résultats évidents

$$(10) \quad R_{2,1} = I_{2,1} = m + 1, \quad R_{2,2} = I_{2,2} = m - 1;$$

2° $p = 4m + 3$; dans ce cas, nous trouvons

$$R_{2,1} - I_{2,1} = I_{2,2} - R_{2,2},$$

tandis que la formule (1) du paragraphe III donnera

$$(11) \quad R_{2,1} - I_{2,1} \equiv \frac{(-1)^m (2^{2m+2} - 1) B_{m+1}}{2m + 2} \pmod{p},$$

ce qui donnera finalement

$$(12) \quad \begin{cases} R_{2,1} - I_{2,1} \equiv -6 B_{2m+1} \pmod{p}, & p = 8m + 3, \\ R_{2,1} - I_{2,1} \equiv -2 B_{2m+2} \pmod{p}, & p = 8m + 7. \end{cases}$$

Deuxième application : a = 4. — 1° Soit $p = 4m + 1$; nous aurons

$$R_{4,1} - I_{4,1} = R_{4,2} - I_{4,2}, \quad R_{4,3} - I_{4,3} = R_{4,4} - I_{4,4},$$

tandis que la formule (12) du paragraphe III donnera

$$(13) \quad R_{4,1} - I_{4,1} \equiv I_{4,3} - R_{4,3} \equiv \frac{1}{4} E_m \pmod{p};$$

2° Soit $p = 4m + 3$; nous aurons de même

$$R_{4,1} - I_{4,1} = I_{4,2} - R_{4,2}, \quad R_{4,3} - I_{4,3} = I_{4,4} - R_{4,4},$$

et les formules (3) et (6) du paragraphe III donneront respectivement

$$\begin{aligned} R_{k,3} - I_{k,3} &\equiv (-1)^m (2^{2m+2} - 1) (2^{2m+2} + 2) B_{m+1} \pmod{p}, \\ R_{k,1} - I_{k,3} &\equiv (-1)^m (2^{2m+2} - 1) (2^{2m+2} - 2) B_{m+1} \pmod{p}; \end{aligned}$$

ce qui donnera, pour $p = 8m + 3$,

$$(14) \quad \begin{cases} R_{k,3} = I_{k,3}, \\ R_{k,1} - I_{k,1} \equiv -12 B_{2m+1} \pmod{p}, \end{cases}$$

tandis que nous aurons, pour $p = 8m + 7$,

$$(15) \quad \begin{cases} R_{k,3} - I_{k,3} \equiv -4 B_{2m+2} \pmod{p}, \\ R_{k,1} = I_{k,1}. \end{cases}$$

Troisième application : $a = 3$. — L'hypothèse $p = 12m + 7$ donnera

$$\begin{aligned} R_{3,2} &= I_{3,2} = 2m + 1, \\ R_{3,1} - I_{3,1} &= I_{3,3} - R_{3,3}; \end{aligned}$$

nous aurons ensuite, en vertu de la formule (4) du paragraphe III,

$$(16) \quad R_{3,1} - I_{3,1} \equiv -4 B_{3m+2} \pmod{p};$$

2° Soit ensuite $p = 12m + 11$; nous aurons

$$\begin{aligned} R_{3,1} &= I_{3,1}, \\ R_{3,2} - I_{3,2} &= I_{3,3} - R_{3,3}, \end{aligned}$$

et la formule (4) du paragraphe III donnera ici

$$(17) \quad R_{3,2} - I_{3,2} \equiv (-1)^m 2 B_{3m+3} \pmod{p}.$$

Quatrième application : $a = 6$. — 1° $p = 2m + 2$; dans ce cas nous avons

$$R_{6,1} - I_{6,1} = I_{6,6} - R_{6,6}, \quad R_{6,2} - I_{6,2} = I_{6,5} - R_{6,5}, \quad R_{6,3} - I_{6,3} = I_{6,4} - R_{6,4};$$

de plus, nous trouvons

$$(18) \quad \begin{cases} R_{6,1} - I_{6,1} \equiv (-1)^m 2 B_{3m+2} \pmod{p}, \\ R_{6,2} - I_{6,2} \equiv (-1)^{m+1} 6 B_{3m+2} \pmod{p}, \\ R_{6,3} - I_{6,3} \equiv (-1)^{m+1} 4 B_{3m+2} \pmod{p}; \end{cases}$$

2° L'hypothèse $p = 12m + 11$ donnera

$$(19) \quad \begin{cases} R_{6,1} = I_{6,1}, & R_{6,4} = I_{6,4}, \\ R_{6,2} - I_{6,2} = I_{6,3} - R_{6,3} \equiv (-1)^m 4 B_{3m+3} \pmod{p}, \\ R_{6,5} - I_{6,5} = I_{6,6} - R_{6,6} \equiv (-1)^m 2 B_{3m+3} \pmod{p}. \end{cases}$$

Cinquième application : $a = 12$. — 1° Soit $p = 12m + 7$; nous trouvons

$$(20) \quad R_{12,3} - I_{12,3} = I_{12,4} - R_{12,4} \equiv (-1)^{m+1} 2 B_{3m+2} \pmod{p};$$

2° L'hypothèse $p = 12m + 11$ donnera

$$(21) \quad \begin{cases} R_{12,3} - I_{12,3} = I_{12,8} - R_{12,8} \equiv (-1)^{m+1} 4 B_{3m+3} \pmod{p}, \\ R_{12,2} - I_{12,2} = I_{12,9} - R_{12,9} \equiv (-1)^m 4 B_{3m+3} \pmod{p}. \end{cases}$$

IX. — Sommes de puissances.

Désignons par a un positif entier, tel que $1 \leq a \leq p - 1$, où $p = 2m + 1$ est un nombre premier impair, puis désignons par $R_n(a)$ et $I_n(a)$ les sommes des $n^{\text{ièmes}}$ puissances des résidus respectivement des non-résidus de p qui se trouvent parmi les nombres

$$(1) \quad 1, 2, 3, \dots, a;$$

nous aurons évidemment

$$(2) \quad R_n(a) + I_n(a) = S_n(a),$$

tandis que la congruence (21) du paragraphe IV donnera

$$R_n(a) - I_n(a) \equiv S_{n+m}(a) \pmod{p};$$

c'est-à-dire que nous aurons

$$(3) \quad \begin{cases} 2 R_n(a) \equiv S_n(a) + S_{n+m}(a) \pmod{p}, \\ 2 I_n(a) \equiv S_n(a) - S_{n+m}(a) \pmod{p}. \end{cases}$$

Étudions tout d'abord le cas $a = p - 1$; les formules (3) donnent, en vertu des congruences (20) et (21) du paragraphe I, le théorème suivant qui est très connu :

I. Soit p un nombre premier impair quelconque, nous aurons

$$(4) \quad R_n(p-1) \equiv I_n(p-1) \equiv 0 \pmod{p}, \quad 1 \leq n \leq \frac{p-3}{2}.$$

Appliquons maintenant la congruence (22) du paragraphe IV, nous aurons

$$2 R_n(a) - 2 I_n(a) \equiv 3 S_{n+m}(a) - S_{n+3m}(a) \pmod{p^2};$$

ce qui donnera, en vertu de (2),

$$(5) \quad \begin{cases} 4 R_n(a) \equiv 2 S_n(a) + 3 S_{n+m}(a) - S_{n+3m}(a) \pmod{p^2}, \\ 4 I_n(a) \equiv 2 S_n(a) - 3 S_{n+m}(a) + S_{n+3m}(a) \pmod{p^2}, \end{cases}$$

de sorte que nous aurons cet autre théorème :

II. Soit p un nombre premier de la forme $4m+1$, nous aurons

$$(6) \quad R_{2n+1}(p-1) \equiv I_{2n+1}(p-1) \equiv 0 \pmod{p^2}, \quad 1 \leq n \leq m-1.$$

Dans ce cas nous appliquons la formule (23) du paragraphe I et nous aurons

$$8 R_n(a) - 8 I_n(a) \equiv 15 S_{n+m}(a) - 10 S_{n-3m}(a) + 3 S_{n+5m}(a) \pmod{p^3};$$

ce qui donnera, en vertu de (2),

$$(7) \quad \begin{cases} 16 R_n(a) \equiv 8 S_n(a) + 15 S_{n+m}(a) - 10 S_{n+3m}(a) + 3 S_{n+5m}(a) \pmod{p^3}, \\ 16 I_n(a) \equiv 8 S_n(a) - 15 S_{n+m}(a) + 10 S_{n+3m}(a) - 3 S_{n+5m}(a) \pmod{p^3}. \end{cases}$$

Cela posé, il est évident qu'il faut étudier séparément le cas particulier $n=1$.

L'hypothèse $p=4m+1$ ne présente aucun intérêt, parce que nous aurons

$$(8) \quad R_1(p-1) = I_1(p-1) = \frac{p(p-1)}{4}.$$

Soit maintenant $p=4m+3$, les congruences (5) donneront

$$4 R_1(p-1) \equiv -p + (-1)^m (3 B_{m+1} + B_{3m+2}) p, \pmod{p^2},$$

de sorte que nous aurons finalement, en vertu de la congruence (15) du

paragraphe II,

$$(9) \quad \begin{cases} \frac{4 R_1(p-1)}{p} \equiv -1 + (-1)^m 4 B_{m+1} \pmod{p}, \\ \frac{4 I_1(p-1)}{p} \equiv -1 - (-1)^m 4 B_{m+1} \pmod{p}; \end{cases}$$

ces résultats sont dus à M. Voronoï (1).

Étudions maintenant le cas général. Supposons tout d'abord $p = 4m + 3$, nous aurons, en vertu de (5),

$$(10) \quad \frac{R_{2n}(p-1)}{p} \equiv \frac{I_{2n}(p-1)}{p} \equiv \frac{(-1)^{n-1} B_n}{2} \pmod{p};$$

il est très curieux, ce me semble, que les seconds membres de ces congruences ne dépendent pas du nombre premier p .

Appliquons ensuite la congruence (14) du paragraphe II, nous aurons de plus

$$(11) \quad \frac{R_{2n+1}(p-1)}{p} \equiv - \frac{I_{2n+1}(p-1)}{p} \equiv \frac{(-1)^{n+m}(8n+1)}{8n+2} B_{n+m} \pmod{p}.$$

Soit ensuite $p = 4m + 1$, le même procédé donnera

$$(12) \quad \begin{cases} \frac{R_{2n}(p-1)}{p} \equiv (-1)^{n-1} \left[\frac{B_n}{2} + \frac{(-1)^m 2n}{4n-1} B_{n+m} \right] \pmod{p}, \\ \frac{I_{2n}(p-1)}{p} \equiv (-1)^{n-1} \left[\frac{B_n}{2} - \frac{(-1)^m 2n}{4n-1} B_{n+m} \right] \pmod{p}. \end{cases}$$

Quant aux sommes $R_{2n+1}(p-1)$ et $I_{2n+1}(p-1)$, nous avons à appliquer les congruences (7); ce qui donnera, en vertu des congruences (12) et (14) du paragraphe II,

$$(13) \quad \begin{cases} \frac{R_{2n+1}(p-1)}{p^2} \equiv (-1)^{n-1} \left(n + \frac{1}{2} \right) \left[\frac{B_n}{2} + \frac{(-1)^m 2n}{4n-1} B_{n+m} \right] \pmod{p}, \\ \frac{I_{2n+1}(p-1)}{p^2} \equiv (-1)^{n-1} \left(n + \frac{1}{2} \right) \left[\frac{B_n}{2} - \frac{(-1)^m 2n}{4n-1} B_{n+m} \right] \pmod{p}, \end{cases}$$

(1) *Jahrbuch über die Fortschritte der Mathematik*, t. XXX, 1899, p. 184.

c'est-à-dire que nous aurons

$$(14) \quad \begin{cases} \frac{R_{2n+1}(p-1)}{p^2} \equiv \left(n + \frac{1}{2}\right) \frac{R_{2n}(p-1)}{p} \pmod{p}, \\ \frac{I_{2n+1}(p-1)}{p^2} \equiv \left(n + \frac{1}{2}\right) \frac{I_{2n}(p-1)}{p} \pmod{p}. \end{cases}$$

Appliquons les congruences (3), nous verrons que la formule (15) du paragraphe I admet des applications immédiates sur les sommes $R_n(a)$ et $I_n(a)$. Or, les résultats généraux étant assez compliqués, nous nous bornerons à indiquer les formules les plus simples, tirées directement des congruences (3).

Soit p de la forme $4m+3$, nous aurons

$$(15) \quad \begin{cases} R_{2n}(2m+1) \equiv -I_{2n}(2m+1) \equiv \frac{(-1)^{n+m+1} T_{n+m+1}}{2^{4n+3}} \pmod{p}, \\ R_{2n+1}(2m+1) \equiv I_{2n+1}(2m+1) \equiv \frac{(-1) T_{n+1}}{2^{4n+4}} \pmod{p}; \end{cases}$$

il est bien curieux, ce me semble, que le second membre de la dernière formule susdite est indépendant des membres premiers p .

Soit maintenant p de la forme $4m+1$, nous aurons au contraire

$$(16) \quad R_{2n}(2m) \equiv I_{2n}(2m) \equiv 0 \pmod{p};$$

l'étude ultérieure de ces congruences, établie à l'aide des congruences (5), donnera des résultats assez compliqués.

Dans le cas $p = 4m+1$, nous aurons ces deux autres congruences :

$$(17) \quad \begin{cases} R_{2n}(m) \equiv \frac{(-1)^n}{2^{4n+3}} [E_n + (-1)^m E_{n+m}] \pmod{p}, \\ I_{2n}(m) \equiv \frac{(-1)^n}{2^{4n+3}} [E_n - (-1)^m E_{n+m}] \pmod{p}. \end{cases}$$

Les formules que nous venons de développer montrent clairement qu'il existe une analogie très étendue entre les sommes de puissances $S_n(a)$ et les sommes $R_n(a)$ et $I_n(a)$.

Or, il est possible de pousser beaucoup plus loin l'analogie susdite.

QUATRIÈME PARTIE.

LES RÉSIDUS QUADRATIQUES ET LES NOMBRES NATURELS.

X. — Analogies des coefficients de factorielle.

Désignons par

$$(1) \quad x_1 x_2 x_3 \dots x_m$$

les racines de l'équation algébrique du degré m

$$(2) \quad x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m = 0;$$

puis posons

$$(3) \quad S_n = x_1^n + x_2^n + \dots + x_m^n,$$

nous aurons les formules de Newton

$$(4) \quad S_r + a_1 S_{r-1} + \dots + a_{r-1} S_1 + r a_r = 0 \quad (1 \leq r \leq m).$$

Soient particulièrement tous les coefficients a_p de l'équation (2) des nombres entiers, il est évident que les sommes de puissances des racines S_p ont la même propriété; ce qui donnera, en vertu de (4), le théorème suivant, essentiel dans les recherches qui nous occupent ici :

I. *Supposons que tous les coefficients a_n soient des nombres entiers, supposons ensuite qu'il existe un nombre premier p plus grand que m , tel que*

$$(5) \quad S_n \equiv 0 \pmod{p}, \quad 1 \leq n \leq q, \quad q \leq m,$$

nous aurons ces deux autres congruences

$$(6) \quad a_n \equiv 0 \pmod{p}, \quad 1 \leq n \leq q,$$

$$(7) \quad S_n + a_n a_n \equiv 0 \pmod{p^2}, \quad 1 \leq n \leq q.$$

Première application. — Soit $p = 2m + 1$ un nombre premier impair

et soient les racines (1) les nombres naturels

$$1, 2, 3, \dots, p-1,$$

nous aurons évidemment

$$a_r = (-1)^r C_p^r, \quad a_{p-1} = (p-1)! \\ S_r = S_r(p-1),$$

où les C_p^r désignent les coefficients de la factorielle du rang p ; ce qui donnera, en vertu de (4),

$$(8) \quad S_n(p-1) - C_p^1 S_{n-1}(p-1) + \dots \\ + (-1)^{n-1} C_p^{n-1} S_1(p-1) + (-1)^n n C_p^n = 0,$$

où il faut admettre $1 \leq n \leq p-1$.

Cela posé, nous aurons immédiatement les congruences de Lagrange (1)

$$(9) \quad C_p^n \equiv 0 \pmod{p}, \quad 1 \leq n \leq p-2;$$

de plus, la formule (8) donnera

$$(10) \quad C_p^{2n+1} \equiv 0 \pmod{p^2}, \quad 1 \leq n \leq \frac{p-3}{2},$$

de sorte qu'il faut supposer, dans (10), $p \geq 5$.

Appliquons ensuite la formule (7), nous aurons immédiatement

$$(11) \quad \frac{C_p^{2r}}{p} \equiv \frac{(-1)^r B_r}{2r} \pmod{p}, \quad 1 \leq r \leq \frac{p-3}{2},$$

tandis que les identités

$$S_1(p-1) = C_p^1 = \frac{p(p-1)}{2}$$

donnent, en vertu de (8),

$$S_{2r+1}(p-1) - \frac{p(p-1)}{2} [S_{2r}(p-1) - C_p^{2r}] \equiv (2r+1) C_p^{2r+1} \pmod{p^2};$$

c'est-à-dire que nous aurons

$$(12) \quad \frac{C_p^{2r+1}}{p^2} \equiv \frac{(-1)^{r-1} (2r+1)}{4r} B_r \pmod{p}, \quad 1 \leq r \leq \frac{p-3}{2}$$

(1) *Nouveaux Mémoires de l'Académie de Berlin*, t. II, 1773 (1771), p. 125-137.

ou, ce qui est la même chose,

$$(13) \quad \frac{C_p^{2r+1}}{p^2} \equiv - \left(r + \frac{1}{2} \right) \frac{C_p^{2r}}{p} \pmod{p}.$$

Les congruences (11) et (12) sont dues à M. Glaisher (1).

Soit maintenant $n = p - 1$, la formule (8) donnera

$$(14) \quad S_{p-1}(p-1) + (p-1)(p-1)! \equiv 0 \pmod{p^2};$$

d'où, en vertu de l'identité

$$S_{p-1}(p-1) = p-1 + p \sum_{s=1}^{s=p-1} q(s),$$

le théorème de Wilson et la congruence de M. Lerch, savoir la formule (14) du paragraphe V, tandis que le résultat

$$S_{p+1}(p-1) \equiv (-1)^{m-1} B_m p \pmod{p^2}$$

donnera la formule (5) du paragraphe VI, savoir la seconde congruence indiquée par M. Lerch pour le nombre W_p .

Deuxième application. — Soit $p = 2m + 1$ un nombre premier impair quelconque et soient les racines (1) l'ensemble des résidus quadratiques de p :

$$(15) \quad r_1 r_2 r_3 \dots r_m \pmod{p},$$

nous aurons

$$(16) \quad \begin{cases} a_m = (-1)^m r_1 r_2 \dots r_m, \\ S_n = R_n(p-1), \end{cases}$$

tandis que $(-1)^n a_n$ deviendra la somme de tous les produits possibles contenant n facteurs différents choisis parmi les nombres (15).

Cela posé, nous avons le résultat connu

$$(17) \quad a_n \equiv 0 \pmod{p}, \quad 1 \leq n \leq m-1.$$

(1) *Quarterly Journal of Mathematics*, t. XXXI, 1900, p. 321-353.

Soit maintenant p de la forme $4m + 3$, nous aurons, en vertu de (7),

$$(18) \quad \left\{ \begin{array}{l} \frac{a_{2n}}{p} \equiv \frac{(-1)^n B_n}{4n} \pmod{p}, \quad 1 \leq n \leq 2m, \\ \frac{a_{2n+1}}{p} \equiv \frac{(-1)^{n+m} (8n+1)}{(2n+1)(8n+2)} B_{n+m} \pmod{p}, \quad 0 \leq n \leq 2m. \end{array} \right.$$

Soit ensuite p de la forme $4m + 1$, nous aurons de même

$$(19) \quad \frac{a_{2n}}{p} \equiv (-1)^n \left[\frac{B_n}{4n} + \frac{(-1)^m B_{n+m}}{4n-1} \right] \pmod{p}, \quad 1 \leq n \leq 2m-1,$$

tandis que les a_{2n+1} satisfont à la condition

$$(20) \quad a_{2n+1} \equiv 0 \pmod{p^2}, \quad 1 \leq n \leq 2m-1;$$

nous aurons dans ce cas

$$(21) \quad \frac{a_{2n+1}}{p^2} \equiv (-1)^{n-1} \left(n + \frac{1}{4} \right) \left[\frac{B_n}{4n} + \frac{(-1)^m B_{n+m}}{4n-1} \right] \pmod{p}$$

ou, ce qui est la même chose,

$$(22) \quad \frac{a_{2n+1}}{p^2} \equiv - \left(n + \frac{1}{4} \right) \frac{a_{2n}}{p} \pmod{p}.$$

Quant au cas particulier $n = m$, nous aurons pour $p = 2m + 1$

$$(23) \quad R_m(p-1) + (-1)^m m r_1 r_2 \dots r_m \equiv 0 \pmod{p^2};$$

appliquons maintenant la formule

$$2 R_m(p-1) = p-1 + p \sum_{s=1}^{s=m} q(r_s),$$

nous aurons le résultat bien connu

$$(24) \quad r_1 r_2 \dots r_m \equiv (-1)^{m-1} \pmod{p}.$$

Posons ensuite

$$(25) \quad r_1 r_2 \dots r_m = (-1)^{m-1} (1 - p \Omega_p),$$

nous aurons pour le nombre entier Ω_p

$$(26) \quad \Omega_p \equiv \sum_{s=1}^{s=m} q(r_s) \pmod{p}.$$

Appliquons ensuite les congruences (5) du paragraphe IX, et (13) du paragraphe II, nous aurons de plus, en vertu de (23),

$$(27) \quad \Omega_p \equiv \frac{(-1)^{m-1}}{2} B_m + \frac{1}{2p} - \frac{1}{2} + \frac{S_m(p-1)}{p} \pmod{p}.$$

Soit p de la forme $4m + 1$, nous aurons par conséquent

$$(28) \quad \Omega_p \equiv -\frac{1}{2} B_{2m} + \frac{1}{2p} - \frac{1}{2} + (-1)^{m-1} B_m \pmod{p},$$

tandis que l'hypothèse $p = 4m + 3$ donnera

$$(29) \quad \Omega_p \equiv \frac{1}{2} B_{2m+1} + \frac{1}{2p} - \frac{1}{2} \pmod{p}.$$

Troisième application. — Soit $p = 2m + 1$ un nombre premier impair, et soient les nombres (1) l'ensemble des non-résidus de p

$$i_1 i_2 i_3 \dots i_m,$$

nous aurons

$$S_n = I_n(p-1),$$

et il est évident que nous trouvons des résultats parfaitement analogues aux précédents; c'est pourquoi nous nous bornerons à l'étude du cas particulier

$$(30) \quad I_m(p-1) + (-1)^m m i_1 i_2 \dots i_m \equiv 0 \pmod{p}.$$

Appliquons l'identité

$$2 I_m(p-1) = -p + 1 - p \sum_{s=1}^{s=m} q(i_s),$$

nous aurons le résultat bien connu

$$(31) \quad i_1 i_2 \dots i_m \equiv (-1)^m \pmod{p}.$$

Posons maintenant

$$(32) \quad i_1 i_2 \dots i_m = (-1)^m (1 - p \Omega'_p),$$

nous aurons par conséquent

$$(33) \quad \Omega'_p \equiv \sum_{s=1}^{s=m} q(i_s) \pmod{p}$$

et nous trouvons de même

$$(34) \quad \begin{cases} \Omega'_p \equiv -\frac{1}{2} B_{2m} + \frac{1}{2p} - \frac{1}{2} + (-1)^m B_m & (\text{mod } p), \\ \Omega'_p \equiv \frac{1}{2} B_{2m+1} + \frac{1}{2p} - \frac{1}{2} & (\text{mod } p), \end{cases}$$

selon que $p = 4m + 1$ ou $p = 4m + 3$.

L'analogie des deux congruences (24) et (31) et du théorème de Wilson est parfaite. On voit de plus que chacun des deux nombres entiers Ω_p et Ω'_p est très semblable au nombre W_p qui figure dans le théorème de Wilson.

Multiplions les deux formules (25) et (32), nous aurons évidemment

$$(35) \quad W_p \equiv \Omega_p + \Omega'_p \pmod{p},$$

ce qui nous conduira immédiatement aux congruences de M. Lerch, relatives au nombre W_p .

XI. — Applications des polynomes réguliers.

Pour mettre en pleine lumière l'analogie qui existe entre l'ensemble des positifs entiers plus petits que le nombre premier impair p et les ensembles des résidus ou des non-résidus de p , nous désignons par

$$(1) \quad \alpha_1 \alpha_2 \alpha_3 \dots \alpha_m$$

des nombres complexes quelconques qui satisfont aux conditions

$$(2) \quad \alpha_s + \alpha_{m-s+1} = p \quad (1 \leq s \leq m).$$

Cela posé, il est évident que le polynome entier du $m^{\text{ième}}$ degré

$$f(x) = \left(x + \frac{\alpha_1}{p}\right) \left(x + \frac{\alpha_2}{p}\right) \dots \left(x + \frac{\alpha_m}{p}\right)$$

satisfait à l'équation fonctionnelle

$$(-1)^m f(-x-1) = f(x);$$

c'est-à-dire que $f(x)$ est un polynome régulier du degré m .

Posons ensuite

$$(3) \quad (x + \alpha_1)(x + \alpha_2) \dots (x + \alpha_m) = \sum_{r=0}^{r=m} a_r x^{m-r},$$

où il faut supposer $\alpha_0 = 1$, nous aurons pour les coefficients a_r les quatre formules suivantes qui sont équivalentes (1) :

$$(4) \quad [1 - (-1)^k] a_k = \sum_{s=0}^{s=k-1} (-1)^s \binom{m-s}{k-s} p^{k-s} a_s,$$

$$(5) \quad \sum_{s=0}^{s=2k-1} (-1)^s \binom{m-s}{2k-s+1} 2^s p^{2k-s+1} a_s = 0,$$

$$(6) \quad (-1)^k \left[a_{2k+1} - \frac{(n-2k)p}{2} a_{2k} \right] \\ = \sum_{s=0}^{s=k-1} (-1)^s \binom{m-2s-1}{2k-2s} p^{2k-2s} a_{2s+1} B_{k-s},$$

$$(7) \quad (-1)^k a_{2k+1} = \sum_{s=0}^{s=k} (-1)^s \binom{m-2s}{2k-2s+1} \left(\frac{p}{2}\right)^{2k-2s+1} a_{2s} T_{k-s+1}.$$

Posons de même

$$(8) \quad S_k = \alpha_1^k + \alpha_2^k + \dots + \alpha_m^k \quad (S_0 = m),$$

nous aurons aussi (2)

$$(9) \quad [1 - (-1)^k] S_k = \sum_{r=0}^{r=k-1} (-1)^r \binom{k}{r} p^{k-r} S_r,$$

$$(10) \quad \sum_{r=0}^{r=2k-1} (-1)^r \binom{2k+1}{r} 2^r p^{2k-r+1} S_r = 0,$$

$$(11) \quad (-1)^k \left[S_{2k+1} - \left(k + \frac{1}{2}\right) p S_{2k} \right] = \sum_{r=0}^{r=k-1} (-1)^r \binom{2k+1}{2r+1} p^{2k-2r} S_{2r+1} B_{k-r},$$

$$(12) \quad (-1)^k S_{2k+1} = \sum_{r=0}^{r=k} (-1)^r \binom{2k+1}{2r} \left(\frac{p}{2}\right)^{2k-2r+1} S_{2r} T_{k-r+1}.$$

(1) Voir mon Mémoire, *Recherches sur les suites régulières et les nombres de Bernoulli et d'Euler* (*Annali di matematica*, 3^e série, t. XXII, 1913, p. 78-79).

(2) *Loc. cit.*, p. 86.

Supposons maintenant que tous les coefficients a_k soient des nombres entiers, les sommes de puissances S_k auront la même propriété; soit ensuite p un nombre impair quelconque, nous aurons, en vertu de (4) et (9),

$$(13) \quad a_{2k+1} \equiv S_{2k+1} \equiv 0 \pmod{p}.$$

Considérons en particulier le cas où p est un nombre premier, puis supposons remplies les deux congruences équivalentes

$$(14) \quad a_k \equiv S_k \equiv 0 \pmod{p},$$

nous aurons de même

$$(15) \quad a_{2k+1} \equiv S_{2k+1} \equiv 0 \pmod{p^2}, \quad k \geq 1;$$

la formule (9) donnera dans ce cas

$$(16) \quad \frac{S_{2k+1}}{p^2} \equiv \left(k + \frac{1}{2}\right) \frac{S_{2k}}{p} \pmod{p}, \quad k \geq 1,$$

tandis que nous aurons, en vertu de (4),

$$(17) \quad \frac{2a_{2k+1}}{p^2} \equiv \frac{(m-2k)a_{2k}}{p} \pmod{p}, \quad k \geq 1.$$

Soit ensuite, dans (17), $m = p - 1$, nous trouvons par conséquent

$$(18) \quad \frac{a_{2k+1}}{p^2} \equiv -\left(k + \frac{1}{2}\right) \frac{a_{2k}}{p} \pmod{p},$$

tandis que l'hypothèse $p = 2m + 1$ donnera de même

$$(19) \quad \frac{a_{2k+1}}{p^2} \equiv -\left(k + \frac{1}{4}\right) \frac{a_{2k}}{p} \pmod{p}.$$

Premier cas particulier. — $p = 2m + 1$ est un nombre premier, tandis que l'ensemble (1) est

$$1, 2, 3, \dots, p-1,$$

nous aurons

$$(20) \quad a_n = C_p^n, \quad S_n = S_n(p-1);$$

la formule correspondante (9) est due à Euler (1).

(1) *Institutiones calculi differentialis*, Saint-Petersbourg, 1755, p. 348-351.

Deuxième cas particulier. — p est un nombre premier de la forme $4m + 1$, et l'ensemble (1) contient tous les résidus quadratiques de p , savoir l'ensemble susdit est

$$r_1 r_2 r_3 \dots r_{2m};$$

dans ce cas nous aurons

$$(21) \quad S_n = R_n(p-1).$$

Troisième cas particulier. — $p = 4m + 1$ est un nombre premier et (1) est l'ensemble des non-résidus de p

$$i_1 i_2 i_3 \dots i_{2m};$$

nous aurons

$$(22) \quad S_n = I_n(p-1).$$

Supposons maintenant que le nombre entier m qui figure dans (1) soit pair, savoir $m = 2\mu$, il est possible d'ordonner les nombres (1), que nous supposons entiers, en deux groupes

$$(23) \quad \alpha'_1, \alpha'_2, \dots, \alpha'_\mu, \alpha''_1, \alpha''_2, \dots, \alpha''_\mu.$$

de sorte que nous aurons

$$(24) \quad \alpha'_s + \alpha''_s = p, \quad 1 \leq s \leq \mu,$$

et ce problème admet 2^μ solutions au plus.

Cela posé, choisissons un quelconque des groupes susdits, puis désignons par S_k la somme des $k^{\text{ièmes}}$ puissances de tous ses μ éléments, nous aurons (1)

$$(25) \quad \frac{p(p^{2n}-1)B_n}{2} + \sum_{r=1}^{r=n-1} (-1)^r \binom{2n}{2r} p^{2n-2r} S_{2r} B_{n-r} \\ = (-1)^n (S_{2n} - n p S_{2n-1}),$$

où il faut supposer $n \geq 2$, tandis que l'hypothèse $n = 1$ donnera

$$(26) \quad p S_1 - S_2 = \frac{p(p^2-1)}{12}.$$

Supposons maintenant que les sommes de puissances S_k soient des nombres entiers, tandis que p est un nombre premier, nous aurons,

(1) Voir mon Mémoire dans les *Annali di matematica*, 3^e série, t. XXII, 1913, p. 100.

par conséquent,

$$(27) \quad S_{2n} \equiv 0 \pmod{p}, \quad 1 \leq n \leq \frac{p-3}{2};$$

de plus, nous trouvons

$$(28) \quad \frac{S_{2n}}{p} - n S_{2n-1} \equiv \frac{(-1)^{n-1} B_n}{2} \pmod{p}.$$

Supposons ensuite que les sommes de puissances S_k satisfassent aux conditions

$$(29) \quad S_k \equiv 0 \pmod{p};$$

nous aurons, en vertu de (28),

$$(30) \quad \frac{S_{2n}}{p} \equiv \frac{(-1)^{n-1} B_n}{2} \pmod{p}, \quad 1 \leq n \leq \frac{p-3}{2}.$$

Soit, par exemple, p un nombre premier de la forme $4m+3$, nous pouvons admettre

$$(31) \quad S_n = R_n(p-1), \quad S_n = I_n(p-1),$$

ce qui nous conduira à des résultats trouvés dans le paragraphe IX, savoir les formules (10).

Les formules (26) et (8) du paragraphe IX, combinées avec l'égalité

$$R_n(p-1) + I_n(p-1) = S_n(p-1),$$

conduisent à poser pour $n \geq 1$

$$\begin{aligned} R_n(p-1) &= a_{n,0} p^{n+1} + a_{n,1} p^n + \dots + a_{n,n} p, \\ I_n(p-1) &= b_{n,0} p^{n+1} + b_{n,1} p^n + \dots + b_{n,n} p, \end{aligned}$$

ce qui donnera

$$\begin{aligned} a_{n,0} + b_{n,0} &= \frac{1}{n+1}, \\ a_{n,1} + b_{n,1} &= -\frac{1}{2}, \end{aligned}$$

et, pourvu que $n \geq 2$, $r \geq 1$,

$$\begin{aligned} a_{n,2r} + b_{n,2r} &= \frac{(-1)^{r-1}}{2^r} \binom{n}{2r-1} B_r, \\ a_{n,2r+1} + b_{n,2r+1} &= 0. \end{aligned}$$

Mais comment déterminer les coefficients $a_{n,r}$ et $b_{n,r}$?