OVERSIGT OVER DET KGL. DANSKE VIDENSKABERNES SELSKABS
FORHANDLINGER. 1916. N° 3.

NOTE SUR LES RÉSIDUS QUADRATIQUES.

PAR

NIELS NIELSEN.

(PRÉSENTÉ DANS LA SÉANCE DU 10 MARS 1916.)

I. Théorèmes sur les polynomes réguliers.

Dans ce qui suit nous désignons par

$$a_1,\ a_2,\ a_3 \ldots a_{2r} \tag{1}$$

des nombres rationnels, différents de zéro, et assujettis à satisfaire aux trois conditions suivantes, mais étant du reste aussi arbitraires que ces conditions le permettent:

1° Soit $1 \leqq q \leqq r$, nous aurons toujours

$$a_q + a_{2r-q+1} = p, \tag{2}$$

où p est un nombre entier.

2° Tous les dénominateurs des nombres (1) sont premiers à p.

3° Posons pour abréger

$$\begin{cases} (x+a_1)\,(x+a_2) \ldots (x+a_{2r}) = \\ = x^{2r} + A_1 x^{2r-1} + \ldots + A_{2r-1}\, x + A_{2r}, \end{cases} \tag{3}$$

nous supposons de plus

$$A_{2r} \equiv \pm 1 \pmod{p}, \tag{4}$$

ou, ce qui est la même chose

$$A_{2r} = (-1)^{\delta} + p\, Q_p,$$

où Q_p est un nombre rationnel dont le dénominateur est premier à p.

Considérons encore le polynome entier du degré r

$$(6)\quad \begin{cases} f(x) = (x-a_1)(x-a_2)\ldots(x-a_r) = \\ \qquad = x^r - a_1 x^{r-1} + \ldots + (-1)^{r-1} a_{r-1} x + (-1)^r a_r, \end{cases}$$

nous aurons, en vertu de (2),

$$A_{2r} = f(p)\, a_r,$$

de sorte que l'équation (5) se présente sous cette autre forme

$$f(p)\, a_r = (-1)^{\delta} + p\, Q_p,$$

d'où après une légère transformation

$$(7)\quad a_r^2 - a_r a_{r-1} p + K p^2 = (-1)^{r+\delta} + (-1)^r p\, Q_p,$$

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

Cela posé, nous aurons, en vertu de (7),

$$(8)\qquad a_r^2 \equiv (-1)^{r+\delta} \pmod{p};$$

posons

$$(9)\qquad a_r^2 = (-1)^{r+\delta} + p\, Q'_p,$$

la formule (7) donnera

$$(10)\qquad Q'_p \equiv a_r a_{r-1} + (-1)^r Q_p \pmod{p}.$$

Introduisons ensuite la somme des valeurs réciproques

$$(11)\qquad \lambda_r = \frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_r},$$

nous aurons évidemment

$$a_r a_{r-1} = a_r^2 \lambda_r,$$

ce qui donnera, en vertu de (8) et (10),

$$(12)\qquad Q'_p \equiv (-1)^{r+\delta} \lambda_r + (-1)^r Q_p \pmod{p}.$$

Soit maintenant, dans (8), $r+\delta$ un nombre pair, nous aurons de plus

$$a_r \equiv \pm 1 \pmod{p};$$

posons

$$a_r = (-1)^{\varepsilon} + p\,Q_p'', \tag{13}$$

il résulte, en vertu de (9),

$$2\,Q_p'' \equiv (-1)^{\varepsilon}\,Q_p' \pmod{p},$$

de sorte que nous aurons finalement

$$Q_p'' \equiv \frac{(-1)^{\varepsilon}}{2}\,\lambda_r + \frac{(-1)^{r+\varepsilon}}{2}\,Q_p \pmod{p}. \tag{14}$$

Il saute aux yeux que l'on puisse déduire de ces formules générales un grand nombre des résultats spéciaux, très intéressants du reste.

Dans ces applications nous aurons à étudier des sommes de puissances qui correspondent à

$$\begin{cases} s_n = a_1^n + a_2^n + \ldots + a_{2r}^n, & s_0 = 2r \\ s_n' = a_1^n + a_2^n + \ldots + a_r^n, & s_0' = r\,; \end{cases} \tag{15}$$

c'est pourquoi il nous semble utile de développer déjà ici des formules fondamentales relatives aux sommes s_n et s_n'.

A cet effet, nous prenons pour point de départ l'identité

$$s_n = s_n' + (p - a_1)^n + (p - a_2)^n + \ldots + (p - a_r)^n,$$

tirée directement de la formule (2), ce qui donnera immédiatement pour $n \geq 1$

$$s_n = \left(1 + (-1)^n\right) s_n' + \sum_{q=0}^{q=n-1}{}' (-1)^q \binom{n}{q} p^{n-q}\, s_q'; \tag{16}$$

c'est-à-dire que nous aurons toujours pour $n \geq 0$

$$\begin{cases} s_{2n+1} \equiv 0 \pmod{p} \\ s_{2n} \equiv 2 s_{2n}' \pmod{p} \end{cases} \tag{16}$$

et, pourvu que $n \geq 1$:

$$\frac{s_{2n} - 2 s_{2n}'}{p} \equiv -2n\, s_{2n-1}' \pmod{p}. \tag{18}$$

Remarquons encore que les formules de NEWTON donnent, en vertu de (3) et (6), ces deux relations

$$(19)\quad s_n - A_1 s_{n-1} + A_2 s_{n-2} - \ldots + (-1)^{n-1} A_{n-1} s_1 + (-1)^n n A_n = 0$$

$$(20)\quad s'_n - a_1 s'_{n-1} + a_2 s'_{n-2} - \ldots + (-1)^{n-1} a_{n-1} s'_1 + (-1)^n n\, a_n = 0,$$

où il faut supposer $1 \leq n \leq 2r$ respectivement $1 \leq n \leq r$.

II. Applications sur les nombres naturels.

Soit particulièrement $p = 2r + 1$ un nombre premier impair, il est évident que les nombres

$$(1)\qquad 1,\ 2,\ 3,\ \ldots,\ p-1$$

satisfont aux deux premières des trois conditions indiquées dans le paragraphe I.

Nous trouvons ici

$$(2)\qquad \begin{cases} A_q = C_p^q, \quad A_{2r} = (p-1)! \\ a_q = C_{r+1}^q, \quad a_r = r!, \end{cases}$$

où les C_m^q sont les coefficients de factorielle du rang m, tandis que les sommes de puissances s_n et s'_n deviennent

$$(3)\qquad \begin{cases} s_n = s_n(p-1) = 1^n + 2^n + \ldots + (p-1)^n \\ s'_n = s_n(r) = 1^n + 2^n + \ldots + r^n. \end{cases}$$

Quant aux deux sommes ainsi définies, nous prenons pour point de départ l'identité évidente

$$(x+1)^{n+1} - x^{n+1} = \binom{n+1}{1} x^n + \binom{n+1}{2} x^{n-1} + \ldots + \binom{n+1}{n} x + 1.$$

posons ensuite

$$x = 1,\ 2,\ 3,\ \ldots,\ p-1,$$

puis ajoutons toutes les équations ainsi obtenues, is résulte la formule récursive

$$p^{n+1} - p =$$

$$= \binom{n+1}{1} s_n(p-1) + \binom{n+1}{2} s_{n-1}(p-1) + \ldots + \binom{n+1}{n} s_1(p-1),$$

ce qui donnera immédiatement

$$s_n(p-1) \equiv 0 \pmod{p}, \quad 1 \leq n \leq p-2 \tag{4}$$

$$s_{p-1}(p-1) \equiv -1 \pmod{p}. \tag{5}$$

Appliquons ensuite la formule générale (16) du paragraphe I, nous aurons par conséquent

$$s_{2n+1}(p-1) \equiv 0 \pmod{p^2}, \quad 1 \leq n \leq \frac{p-3}{2} \tag{6}$$

$$s_{2n}\left(\frac{p-1}{2}\right) \equiv 0 \pmod{p}, \quad 1 \leq n \leq \frac{p-3}{2} \tag{7}$$

$$s_{p-1}\left(\frac{p-1}{2}\right) \equiv -\frac{1}{2} \pmod{p}, \tag{8}$$

ce qui donnera, en vertu des formules de NEWTON,

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

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

$$s_{p-1}(p-1) + (p-1)\,C_p^{p-1} \equiv 0 \pmod{p}. \tag{11}$$

Il est évident que la congruence (11) n'est autre chose que le théorème de WILSON, qui nous écrivons sous la forme

$$(p-1)! = -1 + p\,W_p, \tag{12}$$

où W_p est un nombre entier, souvent désigné comme le quotient de WILSON.

Cela posé, la formule générale (8) du paragraphe I donnera ici la congruence de LAGRANGE

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{r+1} \pmod{p}, \tag{12}$$

d'où, pour r impair, savoir $r = 2m+1$, ce qui donnera $p = 4m+3$,

$$\frac{p-1}{2}! \equiv (-1)^{\varepsilon} \pmod{p}; \tag{13}$$

posons

$$\frac{p-1}{2}! = (-1)^{\varepsilon} + p\,W'_p, \tag{14}$$

la formule générale (14) du paragraphe I donnera

$$W_p' \equiv \frac{(-1)^\varepsilon}{2} \lambda_{2m+1} - \frac{(-1)^\varepsilon}{2} W_p \pmod{p}, \tag{15}$$

où nous avons posé pour abréger

$$\lambda_q = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{q}. \tag{16}$$

Dans le paragraphe V nous avons à étudier d'un autre point de vue les congruences (13) et (15).

III. Sur les résidus quadratiques.

Soit $p = 2n+1$ un nombre premier impair, et soient

$$r_1 r_2 \ldots r_n;\ i_1 i_2 \ldots i_n \tag{1}$$

les ensembles des résidus quadratiques respectivement des non-résidus qui correspondent à p, puis posons

$$\begin{cases} s_q = r_1^q + r_2^q + \ldots + r_n^q,\ s_o = n \\ s_q' = i_1^q + i_2^q + \ldots + i_n^q,\ s_o' = n, \end{cases} \tag{2}$$

nous aurons par conséquent

$$s_q + s_q' = s_q(p-1).$$

De plus, nous trouvons

$$s_q \equiv s_{2q}\left(\frac{p-1}{2}\right) \pmod{p}, \tag{4}$$

ce qui donnera immédiatement

$$s_q \equiv s_q' \equiv 0 \pmod{p}, \quad 1 \leq q \leq n-1, \tag{5}$$

tandis que nous aurons, en vertu de la congruence (8) du paragraphe II

$$s_n \equiv -s_n' \equiv -\frac{1}{2} \pmod{p}. \tag{6}$$

Posons ensuite

$$\begin{cases} f(x) = (x-r_1)(x-r_2)\ldots(x-r_n) = \\ \quad = x^n - a_1 x^{n-1} + \ldots + (-1)^{n-1} a_{n-1} x + (-1)^n a_n \end{cases} \tag{7}$$

$$(8)\quad \begin{cases} \varphi(x) = (x-i_1)(x-i_2)\ldots(x-i_n) = \\ \qquad = x^n - \beta_1 x^{n-1} + \ldots + (-1)^{n-1}\beta_{n-1}x + (-1)^n\beta_n, \end{cases}$$

les formules de NEWTON deviennent ici

$$(9)\quad s_q - \alpha_1 s_{q-1} + \alpha_2 s_{q-2} - \ldots + (-1)^{q-1}\alpha_{q-1}s_1 + (-1)^q q\,\alpha_q = 0$$

$$(10)\quad s'_q - \beta_1 s'_{q-1} + \beta_2 s'_{q-2} - \ldots + (-1)^{q-1}\beta_{q-1}s'_1 + (-1)^q q\,\beta_q = 0,$$

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

Cela posé, nous aurons immédiatement

$$(11)\quad \alpha_q \equiv \beta_q \equiv 0 \pmod{p}, \quad 1 \leq q \leq n-1,$$

tandis que l'hypothèse $q = n$ donnera

$$(12)\quad \alpha_n \equiv (-1)^{n-1} \pmod{p}$$

$$(13)\quad \beta_n \equiv (-1)^n \pmod{p},$$

ce qui nous conduira à poser

$$(14)\quad \alpha_n = (-1)^{n-1}(1 - p\,\Omega_p)$$

$$(15)\quad \beta_n = (-1)^n(1 - p\,\Omega'_p),$$

où Ω_p et Ω'_p sont des nombres entiers.

Remarquons que les deux dernières formules donnent

$$(p-1)! \equiv -1 + p(\Omega_p + \Omega'_p) - p^2\,\Omega_p\,\Omega'_p,$$

nous aurons, en vertu du theorème de WILSON, savoir la formule (12) du paragraphe II,

$$(16)\quad \Omega_p + \Omega'_p \equiv W_p \pmod{p}.$$

Posons maintenant dans (9) et (10), $q = n$, puis ajoutons les deux équations ainsi obtenues, nous aurons, en vertu de (14) et (15),

$$s_n(p-1) \equiv np(\Omega_p - \Omega'_p) \pmod{p^2}.$$

Soit ensuite n un nombre impair, savoir $n = 2m+1$, ce qui donnera $p = 4m+3$, nous aurons par conséquent

$$(17)\quad \Omega_p \equiv \Omega'_p \equiv \frac{1}{2}W_p \pmod{p},$$

tandis que l'hypothèse $p = 4m+1$ donnera

$$(18)\quad \Omega_p - \Omega'_p \equiv -\frac{2}{p}s_{2m}(p-1) \pmod{p}.$$

Les deux dernières congruences que nous venons de démontrer directement, par une méthode parfaitement élémentaire, sont des conséquences immédiates des résultats généraux que j'ai développés autrefois[1] en appliquant les nombres de BERNOULLI.

IV. Le nombre premier est de la forme $4n+1$.

Soit maintenant $p = 4n+1$, l'ensemble des résidus

$$r_1 r_2 r_3 \dots r_{2n} \tag{1}$$

satisfait aux conditions indiquées dans le paragraphe I, et c'est la même chose pour l'ensemble des non-résidus

$$i_1 i_2 i_3 \dots i_{2n}. \tag{2}$$

Dans ce qui suit nous supposons ordonnés d'après leur grandeur et les r_s et les i_s; de plus nous appliquons les définitions des coefficients α_s et β_s indiquées dans les formules (7) et (8) du paragraphe III, ce qui donnera

$$\alpha_{2n} = -1 + p\,\Omega_p \tag{3}$$

$$\beta_{2n} = -1 + p\,\Omega'_p, \tag{4}$$

d'où, en vertu de la formule (8) du paragraphe I,

$$(r_1 r_2 r_3 \dots r_n)^2 \equiv (-1)^{n-1} \pmod p \tag{5}$$

$$(i_1 i_2 i_3 \dots i_n)^2 \equiv (-1)^n \pmod p. \tag{6}$$

Soit maintenant n un nombre impair, savoir $n = 2m+1$, ce qui donnera

$$p = 8m+5,$$

il résulte, en vertu de (5),

$$r_1 r_2 r_3 \dots r_{2m+1} \equiv \pm 1 \pmod p; \tag{7}$$

posons ensuite

$$r_1 r_2 r_3 \dots r_{2m+1} = (-1)^\delta + p\,\Omega''_p, \tag{8}$$

[1] Annales de l'École Normale (3) t. 31, p. 199—200; 1914.

nous aurons, en vertu de la formule (14) du paragraphe 1,

$$(9)\quad \Omega_p'' \equiv \frac{(-1)^\delta}{2}\left(\frac{1}{r_1}+\frac{1}{r_2}+\ldots+\frac{1}{r_{2m+1}}\right)-\frac{(-1)^\delta}{2}\Omega_p \pmod p.$$

Je n'ai pas réussi à déterminer la valeur de l'exposant δ qui figure au second membre de (8).

Soit, au contraire, n un nombre pair, savoir $n = 2m$, ce qui donnera

$$p = 8m+1,$$

nous aurons, en vertu de (6),

$$(10)\qquad i_1 i_2 i_3 \ldots i_{2m} \equiv \pm 1 \pmod p;$$

posons ensuite

$$(11)\qquad i_1 i_2 i_3 \ldots i_{2m} = (-1)^\varepsilon + p\,\Omega_p''',$$

nous aurons par conséquent

$$(12)\quad \Omega_p''' = \frac{(-1)^\varepsilon}{2}\left(\frac{1}{i_1}+\frac{1}{i_2}+\ldots+\frac{1}{i_{2m}}\right)+\frac{(-1)^\varepsilon}{2}\Omega_p'.$$

V. Le nombre premier est de la forme $4n+3$.

Soit ensuite p de la forme $4n+3$, les ensembles des résidus respectivement des non-résidus

$$(1)\qquad r_1 r_2 r_3 \ldots r_{2n+1}$$

$$(2)\qquad i_1 i_2 i_3 \ldots i_{2n+1},$$

supposés ordonnés d'après leur grandeur, satisfont aux conditions

$$(3)\qquad r_s + i_{2n-s+2} = p, \quad 1 \leq s \leq 2n+1;$$

dans ce cas nous aurons

$$(4)\qquad r_1 r_2 r_3 \ldots r_{2n+1} = 1 - p\,\Omega_p$$

$$(5)\qquad i_1 i_2 i_3 \ldots i_{2n+1} = 1 + p\,\Omega_p'.$$

Soient maintenant

$$(6)\qquad r_1 r_2 r_3 \ldots r_\mu$$

l'ensemble des résidus égaux à $2n+1$ au plus,

$$i_1\, i_2\, i_3 \ldots i_\nu \tag{7}$$

l'ensemble des non-résidus qui satisfont à la même condition, nous aurons par conséquent

$$\mu + \nu = 2n+1. \tag{8}$$

De plus, la formule (4) donnera, en vertu de (3),

$$r_1\, r_2 \ldots r_\mu\,(p-i_1)\,(p-i_2)\ldots(p-i_\nu) = 1-p\,\Omega_p,$$

ou, ce qui est la même chose,

$$(-1)^\nu \frac{p-1}{2}! - (-1)^\nu \frac{p-1}{2}!\, p\left(\frac{1}{i_1}+\frac{1}{i_2}+\ldots+\frac{1}{i_\nu}\right)+p^2K = 1-p\,\Omega_p, \tag{9}$$

où K est un nombre entier; c'est-a-dire que nous aurous la congruence de DIRICHLET

$$\frac{p-1}{2}! \equiv (-1)^\nu \pmod p. \tag{10}$$

Posons ensuite

$$\frac{p-1}{2}! = (-1)^\nu + p\,W_p', \tag{11}$$

où W_p' est un nombre entier, la formule (9) donnera

$$W_p' \equiv (-1)^\nu\left(\frac{1}{i_1}+\frac{1}{i_2}+\ldots+\frac{1}{i_\nu}\right)-(-1)^\nu\,\Omega_p. \tag{12}$$

Prenons ensuite pour point de départ la formule (5), nous aurons de même

$$i_1\, i_2 \ldots i_\nu\,(p-r_1)\,(p-r_2)\ldots(p-r_\mu) = -1+p\,\Omega_p',$$

ce qui donnera

$$(-1)^\mu \frac{p-1}{2}! - (-1)^\mu \frac{p-1}{2}!\, p\left(\frac{1}{r_1}+\frac{1}{r_2}+\ldots+\frac{1}{r_\mu}\right)+p^2K' = -1+p\,\Omega_p',$$

où K' est un nombre entier, de sorte que nous aurons ici

$$W_p' \equiv (-1)^\nu\left(\frac{1}{r_1}+\frac{1}{r_2}+\ldots+\frac{1}{r_\mu}\right)-(-1)^\nu\,\Omega_p'. \tag{13}$$

Appliquons ensuite la congruence (17) du paragraphe III, il résulte le théorème suivant, nouveau que je sache:

Soit $p = 4n + 3$ un nombre premier, et soient

$$r_1 r_2 r_3 \ldots r_\mu$$
$$i_1 i_2 i_3 \ldots i_\nu$$

les ensembles des résidus respectivement des non-résidus égaux à $2n+1$ au plus[1], nous aurons toujours

$$(14) \quad \frac{1}{r_1} + \frac{1}{r_2} + \ldots + \frac{1}{r_\mu} \equiv \frac{1}{i_1} + \frac{1}{i_2} + \ldots + \frac{1}{i_\nu} \pmod{p}.$$

Cela posé, nous aurons de même ces deux autres congruences

$$(15) \quad \frac{1}{r_1} + \frac{1}{r_2} + \ldots + \frac{1}{r_\mu} \equiv \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{2n+1}\right) \pmod{p}$$

$$(16) \quad \frac{1}{i_1} + \frac{1}{i_2} + \ldots + \frac{1}{i_\nu} = \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{2n+1}\right) \pmod{p}.$$

Soit par exemple $p = 7$, nous aurons

$$\frac{1}{1} + \frac{1}{2} \equiv \frac{1}{3} \pmod{7},$$

tandis que l'hypothèse $p = 11$ donnera

$$\frac{1}{1} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} \equiv \frac{1}{2} \pmod{11};$$

nous aurons de même pour $n = 19$

$$\frac{1}{1} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{9} \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{8} \pmod{19}.$$