JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

V.-A. LEBESGUE

Démonstration de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques

Journal de mathématiques pures et appliquées 1re série, tome 7 (1842), p. 137-159.
<http://www.numdam.org/item?id=JMPA_1842_1_7__137_0>

DÉMONSTRATION

DE QUELQUES THÉORÈMES

RELATIFS

AUX RÉSIDUS ET AUX NON-RÉSIDUS QUADRATIQUES;

Par V.-A. LEBESGUE,

Professeur à la Faculté des Sciences de Bordeaux.

Le nombre p étant premier, la suite $1, 2, 3, \ldots, p-1$ se partage en deux autres : 1° les résidus $a', a'', a''', \ldots, a^{\left(\frac{p-1}{2}\right)}$ et généralement a. Leur nombre est $\frac{1}{2}(p-1)$, leur somme sera représentée par Σa; 2° les non-résidus $b', b'', b''', \ldots, b^{\left(\frac{p-1}{2}\right)}$ et généralement b. Leur nombre est $\frac{1}{2}(p-1)$; leur somme sera représentée par Σb.

Si l'on partage la série des résidus en deux autres, 1° les résidus compris entre 0 et $\frac{p}{2}$; 2° les résidus compris entre $\frac{p}{2}$ et p, on pourra représenter les nombres de termes de chaque série par $R\frac{1}{2}$, $R\frac{2}{2}$, et les sommes des termes des mêmes séries par $\Sigma a\frac{1}{2}$, $\Sigma a\frac{2}{2}$.

La série des non-résidus étant partagée de même, $N\frac{1}{2}$, $N\frac{2}{2}$ exprimeront combien il y a de non-résidus compris entre 0 et $\frac{p}{2}$ et entre $\frac{p}{2}$ et p. Pareillement $\Sigma b\frac{1}{2}$, $\Sigma b\frac{2}{2}$ exprimeront les sommes de chaque série.

Si l'on divise la série des résidus et celle des non-résidus en quatre autres, la première contenant les nombres compris entre 0 et $\frac{p}{4}$, la seconde ceux entre $\frac{p}{4}$ et $\frac{p}{2}$, la troisième ceux entre $\frac{p}{2}$ et $\frac{3}{4}p$, la quatrième ceux entre $\frac{3}{4}p$ et p, les notations

$$R\tfrac{1}{4},\ R\tfrac{2}{4},\ R\tfrac{3}{4},\ R\tfrac{4}{4};\quad N\tfrac{1}{4},\ N\tfrac{2}{4},\ N\tfrac{3}{4},\ N\tfrac{4}{4}$$

indiqueront le nombre de termes de ces séries, et

$$\Sigma a\tfrac{1}{4},\ \Sigma a\tfrac{2}{4},\ \Sigma a\tfrac{3}{4},\ \Sigma a\tfrac{4}{4};\quad \Sigma b\tfrac{1}{4},\ \Sigma b\tfrac{2}{4},\ \Sigma b\tfrac{3}{4},\ \Sigma b\tfrac{4}{4}$$

représenteront les sommes de ces séries.

Par $\Sigma \sin a\,\omega$ nous désignerons la somme

$$\sin a'\omega + \sin a''\omega + \sin a'''\omega + \ldots + \sin a^{\left(\frac{p-1}{2}\right)}\omega,$$

et par $\Pi \sin a\omega$ nous désignerons le produit

$$\sin a'\omega \,.\, \sin a''\omega . \sin a'''\omega \ldots \sin a^{\left(\frac{p-1}{2}\right)}\omega.$$

Les expressions

$$\Sigma \cos a\omega,\ \Sigma \operatorname{tang} a\omega,\ \Sigma \cot a\omega,\ \Sigma \operatorname{séc} a\omega,\ \Sigma \operatorname{coséc} a\omega,$$

et

$$\Pi \cos a\omega,\ \Pi \operatorname{tang} a\omega,\ \Pi \cot a\omega,\ \Pi \operatorname{séc} a\omega,\ \Pi \operatorname{coséc} a\omega,$$

auront des significations analogues. Il en sera de même de

$$\Sigma \sin b\omega, \quad \text{et} \quad \Pi \sin b\omega, \text{ etc.}$$

Nous calculerons les sommes $\Sigma \sin a\omega$, etc., dans l'hypothèse de $\omega = \frac{2\pi}{p}$; pour le cas des tangentes et cotangentes, on en déduit le cas de $\omega = \frac{\pi}{p}$.

Nous calculerons les produits $\Pi \sin a\omega$, etc., dans les deux hypothèses de $\omega = \frac{\pi}{p}$ et $\omega = \frac{2\pi}{p}$.

Enfin nous donnerons différentes conséquences de ces formules.

« *Problème.* Soit $\omega = \frac{2\pi}{p}$, on demande les sommes

$$\begin{array}{llll} \Sigma \sin a\omega, & \Sigma \operatorname{tang} a\omega, & \Sigma \cot a\omega, & \Sigma \operatorname{cos\acute{e}c} a\omega, \\ \Sigma \cos a\omega, & \Sigma \operatorname{s\acute{e}c} a\omega; & \Sigma \sin b\omega, & \Sigma \operatorname{tang} b\omega, \\ \Sigma \cot b\omega, & \Sigma \operatorname{cos\acute{e}c} b\omega, & \Sigma \cos b\omega, & \Sigma \operatorname{s\acute{e}c} b\omega. \text{ »} \end{array}$$

Solution. On a, d'après M. Gauss :

Pour $p = 4q + 1$,

$$(1) \quad \left\{ \begin{array}{ll} \Sigma \sin a\omega = 0, & \Sigma \sin b\omega = 0, \\ \Sigma \cos a\omega = \frac{1}{2}\sqrt{p} - \frac{1}{2}, & \Sigma \cos b\omega = -\frac{1}{2}\sqrt{p} - \frac{1}{2}; \end{array} \right.$$

pour $p = 4q + 3$,

$$(2) \quad \left\{ \begin{array}{ll} \Sigma \cos a\omega = -\frac{1}{2}, & \Sigma \cos b\omega = -\frac{1}{2}, \\ \Sigma \sin b\omega = \frac{1}{2}\sqrt{p}, & \Sigma \sin b\omega = -\frac{1}{2}\sqrt{p}; \end{array} \right.$$

où l'on voit que le changement de a en b revient au changement de signe du radical.

De là toutes les autres sommes se déduisent sans difficulté au moyen des formules suivantes, démontrées dans l'article 362 des *Recherches arithmétiques* de M. Gauss :

$$(3) \quad \left\{ \begin{array}{l} \operatorname{tang} \omega = 2[\sin 2\omega - \sin 4\omega + \sin 6\omega + \ldots \mp \sin(p-1)\omega], \\ \cot \omega = -\frac{2}{p}[\sin \omega + 3 \sin \omega + 5 \sin 5\omega + \ldots + (p-2)\sin(p-2)\omega], \\ \operatorname{cos\acute{e}c} \omega = -\frac{2}{p}[2 \sin 2\omega + 4 \sin 4\omega + \ldots\ldots\ldots + (p-1)\sin(p-1)\omega], \\ \operatorname{s\acute{e}c} \omega = (-1)^{\frac{p-1}{2}}[1 - 2\cos 2\omega + 2\cos 4\omega + \ldots \pm 2\cos(p-1)\omega]. \end{array} \right.$$

Il est à remarquer que dans ces formules ω est égal à $\frac{2\pi}{p}$, multiplié par l'un quelconque des nombres $1, 2, 3, \ldots, p-1$.

La première et la dernière des équations (3) peuvent s'écrire ainsi :

$$(4)\quad\left\{\begin{aligned}\operatorname{tang}\omega &= 2[\sin 2\omega + \sin 4\omega + \ldots + \sin(p-1)\omega]\\ &\quad - 4[\sin 4\omega + \sin 8\omega + \ldots + \sin(p-1)\omega] \ldots p=4q+1,\\ \operatorname{tang}\omega &= 2[\sin 2\omega + \sin 4\omega + \ldots + \sin(p-1)\omega]\\ &\quad - 4[\cos 4\omega + \sin 8\omega + \ldots + \sin(p-3)\omega] \ldots p=4q+3;\end{aligned}\right.$$

$$(5)\quad\left\{\begin{aligned}\operatorname{séc}\omega &= 1-2[\cos 2\omega + \cos 4\omega + \ldots + \cos(p-1)\omega]\\ &\quad + 4[\cos 4\omega + \cos 8\omega + \ldots + \cos(p-1)\omega] \ldots p=4q+1,\\ \operatorname{séc}\omega &= -1+2[\cos 2\omega + \cos 4\omega + \ldots + \cos(p-1)\omega]\\ &\quad - 4[\cos 4\omega + \cos 8\omega + \ldots + \cos(p-3)\omega] \ldots p=4q+3.\end{aligned}\right.$$

La deuxième et la troisième équation (3) étant ajoutées, comme l'on a, pour toute valeur de α,

$$\cot\frac{\alpha}{2} = \cot\alpha + \operatorname{coséc}\alpha,$$

il en résultera

$$(6)\quad \cot\frac{\omega}{2} = -\frac{2}{p}[\sin\omega + 2\sin 2\omega + 3\sin 3\omega + \ldots + (p-1)\sin(p-1)\omega].$$

On a encore les formules suivantes, quel que soit α,

$$(7)\qquad \operatorname{coséc}\alpha = \cot\frac{\alpha}{2} - \cot\alpha,\qquad \operatorname{tang}\frac{\alpha}{2} = \cot\frac{\alpha}{2} - 2\cot\alpha.$$

Enfin l'on a :

Pour $p = 8k \pm 1$,

$$(8)\quad\left\{\begin{aligned}&\Sigma\operatorname{tang} a\omega = \Sigma\operatorname{tang} a\frac{\omega}{2},\qquad \Sigma\cot a\omega = \Sigma\cot a\frac{\omega}{2},\\ &\Sigma\operatorname{tang} b\omega = \Sigma\operatorname{tang} b\frac{\omega}{2},\qquad \Sigma\cot b\omega = \Sigma\cot b\frac{\omega}{2};\end{aligned}\right.$$

pour $p = 8q \pm 3$,

$$(9)\quad\left\{\begin{aligned}&\Sigma\operatorname{tang} a\omega = \Sigma\operatorname{tang} b\frac{\omega}{2},\qquad \Sigma\cot a\omega = \Sigma\cot b\frac{\omega}{2},\\ &\Sigma\operatorname{tang} b\omega = \Sigma\operatorname{tang} a\frac{\omega}{2},\qquad \Sigma\cot b\omega = \Sigma\cot a\frac{\omega}{2}.\end{aligned}\right.$$

Cela résulte de ce que k, $2k$ sont tous deux résidus ou tous deux non-résidus si $p = 8q \pm 1$, et l'un résidu et l'autre non résidu si $p = 8q \pm 3$. D'ailleurs quand $2a$ est $> p$, il est aussi plus petit que $2p$, de sorte que $2a = p + r$; par suite

$$a\omega = 2a\,\frac{\omega}{2} = 2a\,\frac{\pi}{p} = \pi + \frac{r\pi}{p};$$

donc

$$\operatorname{tang} a\omega = \operatorname{tang} r\,\frac{\omega}{2}, \qquad \cot a\omega = \cot r\,\frac{\omega}{2}.$$

de même

$$\operatorname{tang} b\omega = \operatorname{tang} r'\,\frac{\omega}{2}, \qquad \cot b\omega = \cot r'\,\frac{\omega}{2},$$

en supposant $2b = p + r'$. De là les formules (8) et (9).

Cas de $p = 4q + 1$.

Dans ce cas, parmi les nombres $1, 2, 3, \ldots, \frac{p-1}{2}$, il y a autant de résidus que de non-résidus. Cela résulte de ce que m et $p - m$ sont tous deux résidus ou tous deux non-résidus; ainsi les résidus et les non-résidus, qui sont en nombre $\frac{p-1}{2}$, se partageant également entre les séries $1, 2, 3, \ldots, \frac{p-1}{2}$ et $\frac{p+1}{2} \ldots p - 1$, il y aura dans chacune d'elles $\frac{p-1}{4}$ résidus et $\frac{p-1}{4}$ non-résidus.

D'après cela, si dans la première des équations (5) on remplace ω par $a'\omega$, $a''\omega$, $a'''\omega, \ldots, a^{\frac{(p-1)}{2}}\omega$, et qu'on somme, en réduisant par le moyen des équations (1), on trouvera

$$(10)\qquad \left\{ \begin{aligned} &\Sigma\, \text{séc.}\, a\omega = \frac{p-1}{2} + 2\sqrt{p}\,(\mathrm{R}\tfrac{1}{4} - \mathrm{N}\tfrac{1}{4}),\\ &\text{et de même}\\ &\Sigma\, \text{séc.}\, b\omega = \frac{p-1}{2} - 2\sqrt{p}\,(\mathrm{R}\tfrac{1}{4} - \mathrm{N}\tfrac{1}{4}). \end{aligned} \right.$$

Les autres sommes relatives aux tang, cot et coséc sont nulles; voici le tableau de ces sommes :

$$(11)\left\{\begin{array}{l}\Sigma \sin a\omega = 0,\ \ \Sigma \operatorname{tang} a\omega = 0,\ \ \Sigma \cot a\omega = 0,\ \ \Sigma \operatorname{cos\acute{e}c} a\omega = 0;\\ \Sigma \operatorname{tang} a\frac{\omega}{2} = 0,\ \ \Sigma \cot a\frac{\omega}{2} = 0,\ \ \Sigma \sin b\omega = 0,\ \ \Sigma \operatorname{tang} b\omega = 0,\\ \Sigma \cot b\omega = 0,\ \ \Sigma \operatorname{cos\acute{e}c} b\omega = 0,\ \ \Sigma \operatorname{tang} b\frac{\omega}{2} = 0,\ \ \Sigma \cot b\frac{\omega}{2} = 0,\\ \Sigma \cos a\omega = +\frac{1}{2} - \frac{1}{2}\sqrt{p},\ \ \Sigma \operatorname{s\acute{e}c} a\omega = \frac{p-1}{2} + 2(\mathrm{R}\tfrac{1}{4} - \mathrm{N}\tfrac{1}{4})\sqrt{p},\\ \Sigma \cos b\omega = -\frac{1}{2} - \frac{1}{2}\sqrt{p},\ \ \Sigma \operatorname{s\acute{e}c} b\omega = \frac{p-1}{2} - 2(\mathrm{R}\tfrac{1}{4} - \mathrm{N}\tfrac{1}{4})\sqrt{p}.\end{array}\right.$$

On a évidemment $\mathrm{R}\frac{1}{4} + \mathrm{N}\frac{1}{4} = \frac{p-1}{4}$; il suffira donc de connaître $\mathrm{R}\frac{1}{4}$ ou $\mathrm{N}\frac{1}{4}$ pour déterminer les sommes Σ séc $a\omega$, Σ séc $b\omega$. Quand p ne surpassera pas 1000, on trouvera très-facilement $\mathrm{R}\frac{1}{4}$ ou $\mathrm{N}\frac{1}{4}$ au moyen du *Canon arithmeticus* de M. Jacobi. Quand p surpassera 1000, si l'on représente par h le nombre de formes quadratiques différentes déterminant $-p$, comme on a, d'après M. Dirichlet (*Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres;* journal de M. Crelle, tome XXI),

$$h = 2(\mathrm{R}\tfrac{1}{4} - \mathrm{N}\tfrac{1}{4}),$$

il en résultera

$$\Sigma \operatorname{s\acute{e}c} a\omega = \frac{p-1}{2} + h\sqrt{p},\quad \Sigma \operatorname{s\acute{e}c} b\omega = \frac{p-1}{2} - h\sqrt{p}.$$

On calculera h par la formation directe des formes quadratiques, ce qui pour un grand nombre p est plus court que le calcul direct des résidus. Si cependant $\sqrt{\frac{p}{5}}$ était un grand nombre, le calcul des formes quadratiques différentes et par suite la détermination de h deviendrait impraticable, vu sa longueur.

Cas de $p = 4q + 3$.

Dans ce cas on parvient aux formules suivantes :

$$(12)\quad \Sigma \cos a\omega = -\frac{1}{2},\quad \Sigma \operatorname{s\acute{e}c} a\omega = -\frac{p+1}{2},\quad \Sigma \sin a\omega = \frac{1}{2}\sqrt{p},$$

$$
(13)\left\{
\begin{array}{ll}
p=8q+7. & p=8q+3. \\
\Sigma\ \cot a\omega = \dfrac{\Sigma b-\Sigma a}{p}\sqrt{p}, & \Sigma\cot a\omega = -\dfrac{\Sigma b-\Sigma a}{p}\sqrt{p}, \\
\Sigma\ \mathrm{tang}\ a\omega = -\dfrac{\Sigma b-\Sigma a}{p}\sqrt{p}, & \Sigma\ \mathrm{tang}\ a\omega = -3\dfrac{\Sigma b-\Sigma a}{p}\sqrt{p}, \\
\Sigma\ \mathrm{cos\acute{e}c}\ a\omega = 0, & \Sigma\ \mathrm{cos\acute{e}c}\ a\omega = 2\dfrac{\Sigma b-\Sigma a}{p}\sqrt{p}.
\end{array}
\right.
$$

Quand dans ces formules on changera a en b, il suffira, comme on l'a dit, de changer le signe du radical.

La valeur de $\Sigma\ \mathrm{s\acute{e}c}\, a\omega$ suit immédiatement de la quatrième équation (3). L'équation (6) donne les deux formules

$$
(14)\qquad \Sigma\cot a\frac{\omega}{2} = \frac{\Sigma b-\Sigma a}{p}\sqrt{p}, \qquad \Sigma\cot b\frac{\omega}{2} = -\frac{\Sigma b-\Sigma a}{p}\sqrt{p},
$$

d'où par les formules (9) on tire

$$
\Sigma\cot a\omega \qquad \text{et} \qquad \Sigma\cot b\omega.
$$

Les formules (7) donnent ensuite

$$
\Sigma\ \mathrm{tang} \qquad \text{et} \qquad \Sigma\ \mathrm{cos\acute{e}c}.
$$

Si l'on eût employé la deuxième des équations (3), on eût trouvé, en représentant par $\Sigma' a$ la somme des résidus impairs, et par $\Sigma' b$ la somme des non-résidus impairs,

$$
\Sigma\cot a\omega = \frac{\Sigma' b - \Sigma' a}{p}\sqrt{p};
$$

ainsi l'on aurait

$$
(15)\quad \left\{
\begin{array}{ll}
\text{pour}\quad p = 8q+7, & \Sigma b - \Sigma a = \Sigma' b - \Sigma' a; \\
\text{pour}\quad p = 8q+3, & \Sigma b - \Sigma a = \Sigma' a - \Sigma' b.
\end{array}
\right.
$$

Et les équations (13) deviendraient

$$
(13')\left\{
\begin{array}{ll}
p=8q+7. & p=8q+3. \\
\Sigma\ \cot a\omega = \dfrac{\Sigma' b-\Sigma' a}{p}\sqrt{p}, & \Sigma\ \cot a\omega = \dfrac{\Sigma' b-\Sigma' a}{p}\sqrt{p}, \\
\Sigma\ \mathrm{tang}\ a\omega = -\dfrac{\Sigma' b-\Sigma' a}{p}\sqrt{p}, & \Sigma\ \mathrm{tang}\ a\omega = 3\dfrac{\Sigma' b-\Sigma' a}{p}\sqrt{p}, \\
\Sigma\ \mathrm{cos\acute{e}c}\ a\omega = 0, & \Sigma\ \mathrm{cos\acute{e}c}\ a\omega = -2\dfrac{\Sigma' b-\Sigma' a}{p}\sqrt{p}.
\end{array}
\right.
$$

Par la troisième des équations (3) on eût trouvé

$$\text{pour}\quad p = 8q + 7,\quad \Sigma\,\text{coséc}\, a\omega = 2\left(\frac{\Sigma b_{\frac{1}{2}} - \Sigma a_{\frac{1}{2}}}{p}\right)\sqrt{p};$$

$$\text{pour}\quad p = 8q + 3,\quad \Sigma\,\text{coséc}\, a\omega = -2\left(\frac{\Sigma b_{\frac{1}{2}} - \Sigma a_{\frac{1}{2}}}{p}\right)\sqrt{p}.$$

La comparaison des deux valeurs donne

$$(16)\quad \left\{\begin{array}{l} \text{pour}\quad p = 8q + 7,\quad \Sigma a_{\frac{1}{2}} = \Sigma b_{\frac{1}{2}};\\ \text{pour}\quad p = 8q + 3,\quad \Sigma b - \Sigma a = \Sigma a_{\frac{1}{2}} - \Sigma b_{\frac{1}{2}},\\ \qquad\qquad\qquad\qquad \text{ou}\ \Sigma b_{\frac{2}{2}} - \Sigma a_{\frac{2}{2}} = 2(\Sigma a_{\frac{1}{2}} - \Sigma b_{\frac{1}{2}}). \end{array}\right.$$

Mais comme k et $p - k$ sont l'un résidu et l'autre non-résidu, on trouvera sans difficulté

$$\Sigma a = \Sigma a_{\frac{1}{2}} + p\mathrm{N}_{\frac{1}{2}} - \Sigma b_{\frac{1}{2}},\qquad \Sigma b = \Sigma b_{\frac{1}{2}} + p\mathrm{R}_{\frac{1}{2}} - \Sigma a_{\frac{1}{2}},$$

d'où

$$\Sigma b - \Sigma a = p(\mathrm{R}_{\frac{1}{2}} - \mathrm{N}_{\frac{1}{2}}) + 2(\Sigma b_{\frac{1}{2}} - \Sigma a_{\frac{1}{2}});$$

par conséquent on aura

$$(17)\quad \left\{\begin{array}{l} \text{pour}\quad p = 8q + 7,\quad \dfrac{\Sigma b - \Sigma a}{p} = \mathrm{R}_{\frac{1}{2}} - \mathrm{N}_{\frac{1}{2}};\\ \qquad\quad\ \ p = 8q + 3,\quad 3\,\dfrac{\Sigma b - \Sigma a}{p} = \mathrm{R}_{\frac{1}{2}} - \mathrm{N}_{\frac{1}{2}}. \end{array}\right.$$

Ces deux formules peuvent s'écrire ainsi en une seule

$$\left[2 - \left(\frac{2}{p}\right)\right]\frac{\Sigma b - \Sigma a}{p} = \mathrm{R}_{\frac{1}{2}} - \mathrm{N}_{\frac{1}{2}},$$

le symbole $\left(\frac{2}{p}\right)$ étant $+1$ pour 2 résidu quadratique, et -1 pour 2 non-résidu quadratique de p. Cette formule est de M. Dirichlet, elle représente le nombre de formes quadratiques différentes pour le déterminant premier $-p$, p étant de forme $4q + 3$. (Voyez *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*; journal de M. Crelle, tome XXI.)

Au moyen de ces diverses relations, on aura les formules

$$
(18)\quad\left\{\begin{array}{l}
\Sigma \operatorname{tang} a\omega = (N\tfrac{1}{2} - R\tfrac{1}{2})\sqrt{p},\quad \Sigma \operatorname{cos\acute{e}c} a\omega = \tfrac{2}{3}(R\tfrac{1}{2} - N\tfrac{1}{2})\sqrt{p}, \text{ pour } p = 8q+3;\\
\Sigma \cot a\omega = (R\tfrac{1}{2} - N\tfrac{1}{2})\sqrt{p},\quad \text{pour}\quad p = 8q+7;\\
\Sigma \cot a\omega = \tfrac{1}{3}(N\tfrac{1}{2} - R\tfrac{1}{2})\sqrt{p},\quad \text{pour}\quad p = 8q+3,
\end{array}\right.
$$

et si l'on représente par R' le nombre des résidus impairs, et par N' le nombre des non-résidus impairs, ces équations deviendront

$$
(19)\quad\left\{\begin{array}{llll}
\Sigma \operatorname{tang} a\omega & = (R' - N')\sqrt{p}, & \text{pour } p = 8q+7;\\
\Sigma \operatorname{tang} a\omega & = (N' - R')\sqrt{p}, & p = 8q+3;\\
\Sigma \cot a\omega & = (N' - R')\sqrt{p}, & p = 8q+7;\\
\Sigma \cot a\omega & = \tfrac{1}{3}(N' - R')\sqrt{p}, & p = 8q+3;\\
\Sigma \operatorname{cos\acute{e}c} a\omega & = \tfrac{2}{3}(R' - N')\sqrt{p}, & p = 8q+3;
\end{array}\right.
$$

comme on le verra plus bas. Comme l'on a

$$R\tfrac{1}{2} + N\tfrac{1}{2} = \frac{p-1}{2},\quad R' + N' = \frac{p-1}{2},$$

on pourra éliminer l'un des nombres

$$R\tfrac{1}{2},\ N\tfrac{1}{2}\qquad \text{ou}\qquad R' \text{ et } N'.$$

De la seconde des équations (4) on tire

$$\text{pour } p = 8q+7,\ \Sigma \operatorname{tang} a\omega = (R\tfrac{1}{2} - N\tfrac{1}{2})\sqrt{p} - 2(R\tfrac{1}{4} - N\tfrac{1}{4})\sqrt{p},$$
$$\text{pour } p = 8q+3,\ \Sigma \operatorname{tang} a\omega = -(R\tfrac{1}{2} - N\tfrac{1}{2})\sqrt{p} - 2(R\tfrac{1}{4} - N\tfrac{1}{4})\sqrt{p}.$$

La comparaison des deux valeurs de $\Sigma \operatorname{tang} a\omega$ donnera donc

$$\text{pour}\quad p = 8q+7,\quad R\tfrac{1}{2} - N\tfrac{1}{2} = R\tfrac{1}{4} - N\tfrac{1}{4};$$
$$\text{pour}\quad p = 8q+3,\quad R\tfrac{1}{4} - N\tfrac{1}{4} = 0.$$

Mais on a en général

$$R\tfrac{1}{2} = R\tfrac{1}{4} + R\tfrac{2}{4},\quad N\tfrac{1}{2} = N\tfrac{1}{4} + N\tfrac{2}{4},$$

et de plus $R\tfrac{1}{4} + N\tfrac{1}{4}$ est l'entier de $\frac{p}{4}$. De même $R\tfrac{2}{4} + N\tfrac{2}{4}$ est égal à l'entier de $\frac{p}{2}$ moins l'entier de $\frac{p}{4}$, on aura donc

pour $\quad p = 8q + 7, \quad R\frac{2}{4} = N\frac{2}{4} = \frac{p+1}{8};$

pour $\quad p = 8q + 3, \quad R\frac{1}{4} = N\frac{1}{4} = \frac{p-3}{8}.$

Comme des deux nombres k, $p - k$, l'un résidu et l'autre non-résidu, on aura

$$R\tfrac{1}{2} = N\tfrac{2}{2},\; N\tfrac{1}{2} = R\tfrac{2}{2};\; R\tfrac{1}{4} = N\tfrac{4}{4},\; N\tfrac{1}{4} = R\tfrac{4}{4},\; R\tfrac{2}{4} = N\tfrac{3}{4},\; N\tfrac{2}{4} = R\tfrac{3}{4},$$

d'où résultera

$$R\tfrac{1}{2} + N\tfrac{1}{2} = R\tfrac{2}{2} + N\tfrac{2}{2} = \frac{p-1}{2}, \quad R\tfrac{1}{4} + N\tfrac{1}{4} = R\tfrac{4}{4} + N\tfrac{4}{4} = \frac{p-3}{4},$$

$$R\tfrac{2}{4} + N\tfrac{2}{4} = R\tfrac{3}{4} + N\tfrac{3}{4} = \frac{p-1}{2} - \frac{p+3}{4} = \frac{p-1}{4},$$

on a aussi évidemment

$$\Sigma a + \Sigma b = p\frac{p-1}{2}, \quad \Sigma a\tfrac{1}{2} + \Sigma b\tfrac{1}{2} = \frac{p^2-1}{8}, \quad \Sigma a\tfrac{2}{2} + \Sigma b\tfrac{2}{2} = \frac{p.\overline{p-1}}{2} - \frac{p^2-1}{8}.$$

D'ailleurs, comme les nombres $a', a'', a''', \ldots, a^{\left(\frac{p-1}{2}\right)}$ sont les racines de la congruence $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$, et $b', b'', \ldots, b^{\left(\frac{p-1}{2}\right)}$ celles de la congruence $x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$, en exceptant le cas de $p = 3$, on aura

$$\Sigma a \equiv 0 \pmod{p}, \quad \Sigma b \equiv 0 \pmod{p},$$

c'est-à-dire que $\frac{\Sigma a}{p}$ et $\frac{\Sigma b}{p}$ seront entiers.

L'équation

$$\Sigma a + \Sigma b = \frac{p.\overline{p-1}}{2} = p\left(R\tfrac{1}{2} + N\tfrac{1}{2}\right)$$

devient donc

$$\frac{1}{p}\Sigma a + \frac{1}{p}\Sigma b = R\tfrac{1}{2} + N\tfrac{1}{2};$$

mais pour $p = 8q + 7$ on a aussi l'équation

$$\frac{1}{p}\Sigma b - \frac{1}{p}\Sigma a = \mathrm{R}\tfrac{1}{2} - \mathrm{N}\tfrac{1}{2}.$$

Il en résulte donc

$$\frac{1}{p}\Sigma a = \mathrm{N}\tfrac{1}{2}, \quad \frac{1}{p}\Sigma b = \mathrm{R}\tfrac{1}{2}.$$

Pour le cas de $p = 8q + 3$ on a l'équation

$$\frac{3}{p}\Sigma b - \frac{3}{p}\Sigma a = \mathrm{R}\tfrac{1}{2} - \mathrm{N}\tfrac{1}{2},$$

et par suite

$$\begin{aligned}\frac{3}{p}\Sigma b &= p - 1 - \mathrm{N}\tfrac{1}{2} = \frac{p-1}{2} + \mathrm{R}\tfrac{1}{2},\\ \frac{3}{p}\Sigma a &= p - 1 - \mathrm{R}\tfrac{1}{2} = \frac{p-1}{2} + \mathrm{N}\tfrac{1}{2}.\end{aligned}$$

Si l'on combine les équations précédentes avec celles-ci

$$\mathrm{R}\tfrac{2}{4} = \mathrm{N}\tfrac{2}{4}, \quad \mathrm{R}\tfrac{1}{4} = \mathrm{N}\tfrac{1}{4}, \quad \Sigma a\tfrac{1}{2} = \Sigma b\tfrac{1}{2}, \quad \Sigma b\tfrac{2}{2} - \Sigma a\tfrac{2}{2} = 2(\Sigma a\tfrac{1}{2} - \Sigma b\tfrac{1}{2}),$$

qui ont été trouvées plus haut et qui sont relatives les unes au cas de $p = 8q + 7$, les autres à celui de $p = 8q + 3$, on obtiendra les résultats suivants :

Pour $p = 8q + 7$,

$$(20)\quad \left\{\begin{aligned}
&\mathrm{R}\tfrac{2}{4} = \mathrm{N}\tfrac{2}{4} = \mathrm{R}\tfrac{3}{4} = \mathrm{N}\tfrac{3}{4} = \frac{p+1}{8},\\
&\mathrm{N}\tfrac{1}{4} = \mathrm{R}\tfrac{4}{4} = \frac{p-3}{8} - \mathrm{R}\tfrac{1}{4}, \quad \mathrm{N}\tfrac{4}{4} = \mathrm{R}\tfrac{1}{4},\\
&\Sigma a \;= p\left(\frac{p+1}{8} + \mathrm{N}\tfrac{1}{4}\right) = p\left(\frac{3p-5}{8} - \mathrm{R}\tfrac{1}{4}\right),\\
&\Sigma b \;= p\left(\frac{p+1}{8} + \mathrm{R}\tfrac{1}{4}\right),\\
&\Sigma a\tfrac{1}{2} = \Sigma b\tfrac{1}{2} = \tfrac{1}{16}(p^2 - 1),\\
&\Sigma a\tfrac{2}{2} = p\left(\frac{3p-5}{8} - \mathrm{R}\tfrac{1}{4}\right) - \tfrac{1}{16}(p^2 - 1),\\
&\Sigma b\tfrac{2}{2} = p\left(\frac{p+1}{8} + \mathrm{R}\tfrac{1}{4}\right) - \tfrac{1}{16}(p^2 - 1);
\end{aligned}\right.$$

et pour $p = 8q + 3$,

$$(21)\quad \left\{\begin{array}{l} \mathrm{R}\frac{1}{4} = \mathrm{N}\frac{1}{4} = \mathrm{R}\frac{4}{4} = \mathrm{N}\frac{4}{4} = \frac{p-3}{8}, \\ \mathrm{N}\frac{2}{4} = \mathrm{R}\frac{3}{4} = \frac{p+1}{8} - \mathrm{R}\frac{2}{4}, \quad \mathrm{N}\frac{3}{4} = \mathrm{R}\frac{2}{4}, \\ 3\Sigma a \ = p\left(\frac{7p-5}{8} - \mathrm{R}\frac{2}{4}\right), \quad 3\Sigma b = p\left(\frac{5p-7}{8} + \mathrm{R}\frac{2}{4}\right), \\ 3\Sigma a\frac{1}{2} = \frac{p+1}{4}.\frac{p-3}{4} + p.\mathrm{R}\frac{2}{4}, \quad 3\Sigma b\frac{1}{2} = \frac{p+1}{4}.\frac{5p-3}{8} - p\mathrm{R}\frac{2}{4}, \\ 3\Sigma a\frac{2}{2} = p\,\frac{7p-5}{8} - \frac{p+1}{4}.\frac{p-3}{4} - 2p\mathrm{R}\frac{2}{4}, \\ 3\Sigma b\frac{2}{2} = p\,\frac{5p-7}{8} - \frac{p+1}{4}.\frac{5p-3}{4} + 2p\mathrm{R}\frac{2}{4}. \end{array}\right.$$

Si l'on partage les résidus a, dont la somme est Σa, en deux séries, les impairs en nombre R', ayant pour somme $\Sigma' a$, et les pairs en nombre R'', ayant pour somme $\Sigma'' a$, on aura les équations

$$\Sigma' a + \Sigma'' a = \Sigma a, \qquad \mathrm{R}' + \mathrm{R}'' = \frac{p-1}{2}.$$

De même si les non-résidus b, dont la somme est Σb, sont distribués en deux séries, les impairs en nombre N', ayant pour somme $\Sigma' b$, et les pairs en nombre N'', ayant pour somme $\Sigma'' b$, on aura les équations

$$\Sigma' b + \Sigma'' b = \Sigma b, \qquad \mathrm{N}' + \mathrm{N}'' = \frac{p-1}{2}.$$

Et de plus il est facile de voir que l'on a

pour $p = 8q + 7$,

$$\Sigma'' a = 2\Sigma a\tfrac{1}{2}, \quad \Sigma'' b = 2\Sigma b\tfrac{1}{2}, \quad \mathrm{R}'' = \mathrm{R}\tfrac{1}{2}, \quad \mathrm{N}'' = \mathrm{N}\tfrac{1}{2};$$

d'où

$$\Sigma' a = \Sigma a\tfrac{2}{2} - \Sigma a\tfrac{1}{2}, \quad \Sigma' b = \Sigma b\tfrac{2}{2} - \Sigma b\tfrac{1}{2},$$

$$\mathrm{R}' = \frac{p-1}{2} - \mathrm{R}\tfrac{1}{2}, \qquad \mathrm{N}' = \frac{p-1}{2} - \mathrm{N}\tfrac{1}{2};$$

pour $p = 8q + 3$,

$$\Sigma'' a = 2\Sigma b\tfrac{1}{2}, \quad \Sigma'' b = 2\Sigma a\tfrac{1}{2}, \quad \mathrm{R}'' = \mathrm{N}\tfrac{1}{2}, \quad \mathrm{N}'' = \mathrm{R}\tfrac{1}{2};$$

d'où

$$\Sigma' a = \Sigma a - 2\Sigma b\tfrac{1}{2}, \qquad \Sigma' b = \Sigma b - 2\Sigma a\tfrac{1}{2},$$
$$R' = \frac{p-1}{2} - N\tfrac{1}{2}, \qquad N' = \frac{p-1}{2} - R\tfrac{1}{2},$$

au moyen desquelles on retrouvera les équations (19).

Problème. Trouver les produits

$$\Pi\, 2\sin k\,\frac{\pi}{p}, \qquad \Pi\, 2\cos k\,\frac{\pi}{p} \qquad \text{et} \qquad \Pi\, 2\sin k\,\frac{2\pi}{p}, \qquad \Pi\, 2\cos k\,\frac{2\pi}{p},$$

pris depuis $k = 1$ jusqu'à $k = p - 1$.

Solution. On a l'identité

$$(22)\qquad \left\{\begin{aligned} \frac{x^p - 1}{x-1} &= x^{p-1} + x^{p-2} + \ldots + x + 1 \\ &= \Pi\left(x - \cos k\,\frac{2\pi}{p} - \sin k\,\frac{2\pi}{p}\sqrt{-1}\right). \end{aligned}\right.$$

Si l'on y fait $x = 1$, comme il en résulte

$$\begin{aligned} 1 - \cos k\,\frac{2\pi}{p} - \sin k\,\frac{2\pi}{p}\sqrt{-1} &= 2\sin^2 k\,\frac{\pi}{p} - 2\sin k\,\frac{\pi}{p}\cos k\,\frac{\pi}{p}\sqrt{-1} \\ &= 2\sqrt{-1}\,\sin k\,\frac{\pi}{p}\left(\cos k\,\frac{\pi}{p} + \sin k\,\frac{\pi}{p}\sqrt{-1}\right), \end{aligned}$$

le second membre deviendra

$$(-1)^{\frac{p-1}{2}}\,\Pi\, 2\sin k\,\frac{\pi}{p}\left[\cos(1+2+3\ldots+p-1)\frac{\pi}{p} + \sin(1+2+3\ldots+p-1)\frac{\pi}{p}\sqrt{-1}\right];$$

or

$$(1 + 2 + 3 + \ldots p - 1)\frac{\pi}{p} = \frac{(p-1)}{2}\pi,$$

de sorte que le troisième facteur se réduit à $(-1)^{\frac{p-1}{2}}$, à cause de

$$\cos\frac{p-1}{2}\pi = (-1)^{\frac{p-1}{2}}, \quad \sin\frac{p-1}{2}\pi = 0.$$

L'équation (22) devient donc

$$(23)\qquad \Pi\, 2\sin k\,\frac{\pi}{p} = p.$$

La substitution de $x = -1$, pour laquelle

$$-1 - \cos k\frac{2\pi}{p} - \sin k\frac{2\pi}{p}\sqrt{-1} = -2\cos^2 k\frac{\pi}{p} - 2\sin k\frac{\pi}{p}\cos k\frac{\pi}{p}\sqrt{-1}$$
$$= -2\cos k\frac{\pi}{p}\left(\cos k\frac{\pi}{p} + \sin k\frac{\pi}{p}\sqrt{-1}\right),$$

donne pareillement

$$\Pi\, 2\cos k\frac{\pi}{p} = (-1)^{\frac{p-1}{2}}, \tag{24}$$

par suite

$$\Pi\, \mathrm{tang}\, k\frac{\pi}{p} = (-1)^{\frac{p-1}{2}} p. \tag{25}$$

Si l'on remplace k par $2k$, les sinus et cosinus qui répondent à $k > \frac{p}{2}$ ou $2k > p$, sont, au signe près, les sinus et cosinus du reste de $2k$ divisé par p; on aura, d'après cela,

$$\left\{\begin{array}{l} \Pi\, 2\sin k\frac{2\pi}{p} = (-1)^{\frac{p-1}{2}} p, \quad \Pi\, 2\cos k\frac{2\pi}{p} = 1, \\ \Pi\, \mathrm{tang}\, k\frac{2\pi}{p} = (-1)^{\frac{p-1}{2}} p. \end{array}\right. \tag{26}$$

Les formules précédentes reviennent à celles-ci

$$\left\{\begin{array}{l} \Pi\, 2\sin a\frac{\pi}{p}\, \Pi\, 2\sin b\frac{\pi}{p} = p, \\ \Pi\, 2\cos a\frac{\pi}{p}\, \Pi\, 2\cos b\frac{\pi}{p} = (-1)^{\frac{p-1}{2}}, \\ \Pi\, \mathrm{tang}\, a\frac{\pi}{p}\, \Pi\, \mathrm{tang}\, b\frac{\pi}{p} = (-1)^{\frac{p-1}{2}}; \end{array}\right. \tag{27}$$

$$\left\{\begin{array}{l} \Pi\, 2\sin a\frac{2\pi}{p}\, \Pi\, \sin b\frac{2\pi}{p} = (-1)^{\frac{p-1}{2}} p, \\ \Pi\, 2\cos a\frac{2\pi}{p}\, \Pi\, \cos b\frac{2\pi}{p} = 1, \\ \Pi\, \mathrm{tang}\, a\frac{2\pi}{p}\, \Pi\, \mathrm{tang}\, b\frac{2\pi}{p} = (-1)^{\frac{p-1}{2}} p. \end{array}\right. \tag{28}$$

On voit encore sans difficulté, que l'on a,

d'abord pour $p = 8q \pm 1$,

$$(29)\quad \left\{\begin{aligned}
&\Pi\, 2 \sin a \,\frac{2\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}}\, \Pi\, 2 \sin a \,\frac{\pi}{p},\\
&\Pi\, 2 \sin b \,\frac{2\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}}\, \Pi\, 2 \sin b \,\frac{\pi}{p},\\
&\Pi\, 2 \cos a \,\frac{2\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}}\, \Pi\, 2 \cos a \,\frac{\pi}{p},\\
&\Pi\, 2 \cos b \,\frac{2\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}}\, \Pi\, 2 \sin b \,\frac{\pi}{p},\\
&\Pi \tang a \,\frac{2\pi}{p} = \Pi \tang a \,\frac{\pi}{p},\\
&\Pi \tang b \,\frac{2\pi}{p} = \Pi \tang b \,\frac{\pi}{p};
\end{aligned}\right.$$

et puis pour $p = 8q \pm 3$,

$$(30)\quad \left\{\begin{aligned}
&\Pi\, 2 \sin a \,\frac{2\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}}\, \Pi\, 2 \sin b \,\frac{\pi}{p},\\
&\Pi\, 2 \sin b \,\frac{2\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}}\, \Pi\, 2 \sin a \,\frac{\pi}{p},\\
&\Pi\, 2 \cos a \,\frac{2\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}}\, \Pi\, 2 \cos b \,\frac{\pi}{p},\\
&\Pi\, 2 \cos b \,\frac{2\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}}\, \Pi\, 2 \cos a \,\frac{\pi}{p},\\
&\Pi \tang a \,\frac{2\pi}{p} = \Pi \tang b \,\frac{\pi}{p},\\
&\Pi \tang b \,\frac{2\pi}{p} = \Pi \tang a \,\frac{\pi}{p}.
\end{aligned}\right.$$

Problème. « Trouver les quatre produits

$$\Pi\, 2 \sin a \,\frac{\pi}{p},\qquad \Pi\, 2 \sin b \,\frac{\pi}{p},\qquad \Pi\, 2 \cos a \,\frac{\pi}{p},\qquad \Pi\, 2 \cos b \,\frac{\pi}{p}.\text{ »}$$

Solution. Nous représenterons leurs valeurs absolues par K, L, M, N, et il viendra, eu égard au nombre des facteurs négatifs,

$$\Pi\, 2 \sin a \,\frac{\pi}{p} = \mathrm{K},\qquad \Pi\, 2 \sin b \,\frac{\pi}{p} = \mathrm{L},$$

$$\Pi\, 2 \cos a \,\frac{\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}}\, \mathrm{M},\quad \Pi\, 2 \cos b \,\frac{\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}}\, \mathrm{N};$$

et l'on aura les relations

$$KL = p, \qquad MN = 1.$$

Cela posé, on sait que l'on a

$$Y^2 \mp pZ^2 = 4\left(\frac{x^p - 1}{x - 1}\right),$$

selon que l'on a $p = 4q + 1$ ou $p = 4q - 1$, et que

$$(31)\qquad \tfrac{1}{2}Y + \tfrac{1}{2}Z\sqrt{\pm p} = \Pi\left(x - \cos a\frac{2\pi}{p} - \sin a\frac{2\pi}{p}\sqrt{-1}\right),$$

le produit Π s'étendant aux $\frac{p-1}{2}$ valeurs de a, savoir $a', a'', \ldots, a^{\frac{p-1}{2}}$.

Dans l'équation (31), nous ferons successivement $x = 1$ et $x = -1$, et nous trouverons

$$(32)\quad \begin{cases} \Pi\left(1 - \cos a\frac{2\pi}{p} - \sin a\frac{2\pi}{p}\sqrt{-1}\right) \\ = (-1)^{\frac{p-1}{2}}\left(\sqrt{-1}\right)^{\frac{p-1}{2}}\Pi\, 2\sin a\frac{\pi}{p}\left(\cos\frac{\Sigma a}{p}\pi + \sin\frac{\Sigma a}{p}\pi\sqrt{-1}\right), \\ \Pi\left(-1 - \cos a\frac{2\pi}{p} - \sin a\frac{2\pi}{p}\sqrt{-1}\right) \\ = (-1)^{\frac{p-1}{2}}\Pi\, 2\cos a\frac{\pi}{p}\left(\cos\frac{\Sigma a}{p}\pi + \sin\frac{\Sigma a}{p}\pi\sqrt{-1}\right). \end{cases}$$

Nous supposerons que dans le premier cas Y et Z deviennent A et B, et dans le second cas A′ et B′. Le facteur $\cos\frac{\Sigma a}{p}\pi + \sin\frac{\Sigma a}{p}\pi\sqrt{-1} = (-1)^{\frac{\Sigma a}{p}}$ (le cas $p = 3$ est excepté), devient $(-1)^q$ pour $p = 4q + 1$, car on trouve sans difficulté $\frac{\Sigma a}{p} = q$; et pour $p = 4q + 3$, si $p = 8k + 7$, on aura

$$\frac{\Sigma a}{p} = N\tfrac{1}{2},$$

d'où

$$(-1)^{\frac{\Sigma a}{p}} = (-1)^{N\frac{1}{2}};$$

et si $p = 8q + 3$, on aura

$$\frac{\Sigma a}{p} = \tfrac{1}{3}(p - 1 - \mathrm{R}\tfrac{1}{2}) \equiv \mathrm{R}\tfrac{1}{2} \ (\mathrm{mod.}\ 2),$$

d'où

$$(-1)^{\frac{\Sigma a}{p}} = (-1)^{\mathrm{R}\frac{1}{2}}.$$

On aura donc, pour le cas de $p = 4q + 1$,

$$\mathrm{K} = \tfrac{1}{2}\left(\mathrm{A} + \mathrm{B}\sqrt{p}\right), \quad \text{d'où} \quad \mathrm{L} = \tfrac{1}{2}(\mathrm{A} - \mathrm{B}\sqrt{p}),$$

à cause de $\mathrm{A}^2 - p\mathrm{B}^2 = 4p$;

$$\mathrm{M} = \tfrac{1}{2}\left(\mathrm{A}' + \mathrm{B}'\sqrt{p}\right), \quad \text{d'où} \quad \mathrm{N} = \tfrac{1}{2}\left(\mathrm{A}' - \mathrm{B}'\sqrt{p}\right),$$

à cause de $\mathrm{A}'^2 - p\mathrm{B}'^2 = 4$,

et de $\mathrm{R}\frac{1}{2} = \mathrm{R}\frac{2}{2} = q = \frac{p-1}{4}, \quad \mathrm{N}\frac{1}{2} = \mathrm{N}\frac{2}{2} = q.$

N. B. Les équations $\mathrm{A}^2 - p\mathrm{B}^2 = 4p$, $\mathrm{A}'^2 - p\mathrm{B}'^2 = 4$, peuvent servir à trouver une solution de l'équation $y^2 - pz^2 = 1$, par les fonctions circulaires (cas de $p = 4q + 1$ premier). (*Voyez* une Note de M. Dirichlet, Journal de M. Crelle, tome XVII, page 286.)

On écrira

$$\left(\frac{\mathrm{A}'}{2}\right)^2 - p\left(\frac{\mathrm{B}'}{2}\right)^2 = 1;$$

et en formant le cube de $\frac{\mathrm{A}'}{2} + \frac{\mathrm{B}'}{2}\sqrt{p}$, on obtiendra

$$\left[\frac{\mathrm{A}'(p\mathrm{B}'^2 + 1)}{2}\right]^2 - p\left[\frac{\mathrm{B}'(p\mathrm{B}'^2 + 3)}{2}\right]^2 = 1.$$

On a donc une solution en entiers de $y^2 - pz^2 = 1$, les inconnues étant, comme A′ et B′, exprimées en fonctions circulaires.

L'équation

$$\mathrm{A}^2 - p\mathrm{B}^2 = 4p$$

donne

$$A = pA';$$

on a donc

$$B^2 - pA'^2 = 4,$$

ou

$$\left(\frac{B}{2}\right)^2 - p\left(\frac{A'}{2}\right)^2 = -1,$$

d'où, comme plus haut,

$$\left[\frac{B(pA'^2 - 1)}{2}\right]^2 - p\left[\frac{A'(pA'^2 - 3)}{2}\right]^2,$$

ou

$$a'^2 - pb'^2 = -1,$$

qui donne

$$(a'^2 + pb'^2)^2 - p(2a'b')^2 = 1;$$

l'équation $y^2 - pz^2 = 1$ est donc encore résolue en nombres entiers par le moyen de fonctions circulaires.

M. Dirichlet a montré que l'équation $y^2 - pz^2 = 1$ peut être traitée de même, quel que soit le nombre p, non carré.

Pour le cas de $p = 4q - 1$, les formules (32) donneront, en remarquant que l'équation $A^2 + pB^2 = 4p$ suppose $A = 0$, $B^2 = 4$, et que l'équation $A'^2 + pB'^2 = 4$, suppose $B' = 0$, $A'^2 = 4$, $(p > 3)$,

$$\tfrac{1}{2}B\sqrt{p} = (-1)^{q + N\frac{1}{3}}K, \quad \tfrac{1}{2}A' = M;$$

une conséquence de ces équations, c'est qu'on a

$$K = L = \sqrt{p} \quad \text{et} \quad M = N = 1;$$

de plus, le signe de B (ou de Z pour $x = 1$) fera connaître si $N\frac{1}{3}$, et par suite $R\frac{1}{7}$ est pair ou impair. Comme l'on n'a point l'expression générale de Z, cette solution est plus théorique que pratique.

On a donc les formules suivantes :

pour $p = 4q + 1$,

$$(31)\quad \left\{ \begin{array}{ll} \Pi 2 \sin a \frac{\pi}{p} = \frac{1}{2}\left(\mathrm{A}+\mathrm{B}\sqrt{p}\right), & \Pi 2 \cos a \frac{\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}} \frac{1}{2}\left(\mathrm{A}'+\mathrm{B}'\sqrt{p}\right), \\ \Pi 2 \sin b \frac{\pi}{p} = \frac{1}{2}\left(\mathrm{A}-\mathrm{B}\sqrt{p}\right), & \Pi 2 \cos b \frac{\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}} \frac{1}{2}\left(\mathrm{A}'-\mathrm{B}'\sqrt{p}\right); \end{array} \right.$$

pour $p = 4q - 1$,

$$(32)\quad \left\{ \begin{array}{ll} \Pi 2 \sin a \frac{\pi}{p} = \sqrt{p}, & \Pi 2 \cos a \frac{\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}}, \\ \Pi 2 \sin b \frac{\pi}{p} = \sqrt{p}, & \Pi 2 \cos b \frac{\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}}, \end{array} \right.$$

desquelles on tire, par la division,

$$(33)\quad \left\{ \begin{array}{ll} \text{pour} \quad p = 4q+1, & \Pi \operatorname{tang} a \frac{\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}} \frac{\mathrm{A}+\mathrm{B}\sqrt{p}}{\mathrm{A}'+\mathrm{B}'\sqrt{p}}; \\ \text{pour} \quad p = 4q-1, & \Pi \operatorname{tang} a \frac{\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}} . \sqrt{p}. \end{array} \right.$$

Au moyen des formules (29) et (30) on aura les formules analogues où π serait remplacé par 2π, entre autres ces deux-ci :

pour $p = 8k + 7$,

$$\Pi \operatorname{tang} a \frac{2\pi}{p} = (-1)^{\mathrm{R}\frac{2}{2}} \sqrt{p} = (-1)^{\mathrm{N}\frac{1}{2}} \sqrt{p};$$

pour $p = 8k + 3$,

$$\Pi \operatorname{tang} a \frac{2\pi}{p} = (-1)^{\mathrm{N}\frac{2}{2}} \sqrt{p} = (-1)^{\mathrm{R}\frac{1}{2}} \sqrt{p} = -(-1)^{\mathrm{N}\frac{1}{2}} \sqrt{p}.$$

Dans le tome XVIII du Journal de M. Crelle, p. 375, M. Stern a donné, sans démonstration, les valeurs de

$$\Sigma \cot a \frac{360}{p} \quad \text{et} \quad \Pi \cot a \frac{360}{p};$$

il y a faute d'impression.

Au lieu de $\Sigma \cot a \frac{360^\circ}{p} = \sqrt{p}$, il faut, comme nous l'avons vu plus haut, $\pm \left(\frac{\Sigma b - \Sigma a}{p}\right)\sqrt{p}$, le signe $+$ étant pour $p = 8k + 7$, et le signe $-$ pour $p = 8k + 3$.

Au lieu de $\Pi \cot a \frac{360^\circ}{p} = \frac{1}{\sqrt{p}}$, il faut $= (-1)^{N\frac{1}{2}} \frac{1}{\sqrt{p}}$ pour $p = 8k + 7$, et $(-1)^{1+N\frac{1}{2}} \frac{1}{\sqrt{p}}$ pour $p = 8k + 3$.

La règle que M. Stern a donnée dans le *Journal de Mathématiques*, tome V, page 216, pour fixer le signe de $\Pi \cot a \frac{2\pi}{p}$, revient à la précédente, car si l'on représente par N le nombre de diviseurs quadratiques différents de $y^2 + (4q - 1)z^2$, dans la classification de Legendre, les nombres N et $N\frac{1}{2}$ sont ensemble pairs ou impairs, ainsi que l'a montré M. Jacobi (Journal de M. Crelle, tome IX, page 189).

Problème. Le produit $1.2.3\ldots\frac{p-1}{2}$, où l'on suppose p premier de forme $4q - 1$, est-il résidu ou non-résidu quadratique de p?

Solution. Il résulte du théorème de Waring que l'on a

$$1.2.3\ldots\frac{p-1}{2} \equiv \pm 1 \ (\text{mod.}\ p) \quad \text{ou} \quad \equiv (-1)^{\mu} \ (\text{mod.}\ p).$$

La question est donc de savoir si les non-résidus compris entre o et $\frac{p}{2}$ sont en nombre pair ou impair, car $+1$ étant résidu et -1 non-résidu, le premier cas répondra à $N\frac{1}{2}$ pair et le second à $N\frac{1}{2}$ impair. Le problème précédent, proposé depuis longtemps par M. Dirichlet (Journal de M. Crelle, tome III, page 307), revient donc à demander une règle praticable pour savoir si $N\frac{1}{2}$ est pair ou impair.

Tant que p est < 1000, le *Canon arithmeticus* de M. Jacobi donnera une solution très-expéditive. Pour les nombres au delà de 1000 et tels que $\frac{1}{2}\sqrt{\frac{p}{3}} = \sqrt{\frac{p}{12}}$ ne soit pas très-grand, la solution de M. Jacobi (Journal de M. Crelle, tome IX, page 189) sera encore praticable.

Dans son grand Mémoire sur la *Théorie des Nombres*, page 17,

M. Cauchy a donné pour le cas de p premier de forme $4q+3$, la formule

$$1^{\frac{p-1}{2}} + 2^{\frac{p-1}{2}} + 3^{\frac{p-1}{2}} + \ldots + \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p+1}{4}} \cdot \frac{2\left(2^{\frac{p+1}{2}}-1\right)}{2^{\frac{p-1}{2}}} A_{\frac{p+1}{4}},$$

où A_1, A_2, A_3,... représentent les nombres de Bernoulli. Si $A_{\frac{p+1}{4}}$ était connu, cette équation conduirait à la différence $R\frac{1}{2} - N\frac{1}{2}$; et comme on a $R\frac{1}{2} + N\frac{1}{2} = \frac{p-1}{2}$, on en déduirait $R\frac{1}{2}$ et $N\frac{1}{2}$. Mais comme on ne connaît que les premiers des nombres dits de Bernoulli, la solution précédente n'est bonne qu'en théorie.

Comme la parité ou l'imparité de Σa correspond à celle de $N\frac{1}{2}$, je vais indiquer un moyen de calculer Σa ou plutôt de chercher si cette somme est paire ou impaire. Ce moyen serait très-expéditif si l'on avait une table de carrés suffisamment prolongée. J'ai trouvé depuis longtemps cette solution du problème de M. Dirichlet, mais c'est d'après la Note de M. Jacobi, déjà citée, que j'ai su que la parité ou imparité de μ dans la congruence $1.2.3\ldots\frac{p-1}{2} \equiv (-1)^{\mu} (\text{mod}.\, p)$ correspondait à la parité ou à l'imparité de Σa.

Voici en quoi consiste cette règle.

On écrira sur une même ligne les multiples successifs de p moindres que $\left(\frac{p-1}{2}\right)^2$, et au-dessous les carrés entiers immédiatement inférieurs

$$(1) \qquad p, \quad 2p, \quad 3p, \ldots, \; n.p,$$

$$(2) \qquad \alpha^2, \quad \beta^2, \quad \gamma^2, \ldots, \; \nu^2, \; \left(\frac{p-1}{2}\right)^2,$$

on aura

$$\Sigma a = \frac{p.\overline{p-1}}{2}\left(\frac{p+1}{12} - n\right) + (\alpha + \beta + \gamma + \ldots + \nu)p;$$

cela résulte de ce que l'on a

$$S_2 = 1^2 + 2^2 + 3^2 + \ldots + \left(\frac{p-1}{2}\right)^2 = \frac{\overline{p-1}.p.\overline{p+1}}{24}$$

(divisible par 3, sauf pour $p = 3$, cas excepté), et de plus, par l'omission des multiples de p dans les carrés $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$,

$$\Sigma a = S_2 - (\beta - \alpha) p - (\gamma - \beta) 2p - (\delta - \gamma) 3p \ldots - \left(\frac{p-1}{2} - \nu\right) np$$
$$= S_2 - n . \frac{p . p - 1}{2} + (\alpha + \beta + \gamma + \ldots + \nu) p.$$

Pour $p = 4q + 1$ on aura $n = \frac{p-5}{4}$, et par suite

$$\Sigma a = - \frac{p . p - 1 . p - 8}{12} + (\alpha + \beta + \gamma + \ldots \nu) p;$$

par l'omission des multiples de 2 on trouverait facilement

$$\Sigma a \equiv \frac{p-1}{4} + \alpha + \beta + \gamma + \ldots \nu.$$

Pour $p = 4q - 1$ on aura $n = \frac{p-3}{4}$, et par suite

$$\Sigma a = - \frac{p . p - 1 . p - 5}{12} + (\alpha + \beta + \ldots + \nu) p,$$

et par l'omission des multiples de 2,

$$\Sigma a \equiv 1 + \alpha + \beta + \gamma + \ldots \nu.$$

Ainsi tout revient à savoir combien il y a de nombres impairs dans la série $\alpha, \beta, \gamma, \ldots, \nu$.

Pour le cas de $p = 4q - 1$, Σa est pair quand il y a un nombre impair de termes impairs dans la série $\alpha, \beta, \gamma, \ldots, \nu$; Σa est impair dans le cas contraire.

Tout le calcul se réduit donc à la formation des $\frac{p-3}{4}$ premiers multiples de p, et à la recherche des carrés entre lesquels ils tombent, ce qui se trouvera à l'inspection même de la table des carrés. Ce calcul, comme celui de M. Jacobi, deviendra impraticable pour de très-grands nombres.

Il faudrait donc avoir un autre moyen de former Σa. M. Libri a donné des formules pour trouver la somme des racines d'une congruence, et en particulier pour la somme des racines de

$$x^n - 1 \equiv 0 \text{ (mod. } p),$$

qui renferme $x^{\frac{p-1}{2}} - 1 \equiv 0$ (mod. p); mais ces formules ne paraissent pas facilement réductibles en nombres, ce qui est nécessaire pour avoir une solution pratique.

Je ferai observer en finissant que depuis longtemps M. Stern a posé un problème qui revient au suivant :

Trouver la somme des racines de la congruence

$$x^{\frac{p-1}{t}} - 1 \equiv 0 \text{ (mod. } p).$$

(Journal de M. Crelle, tome VII, page 104.)

Pour $t = 2$, la somme cherchée serait Σa, qui conduit, comme nous l'avons vu, à la solution de divers problèmes dont une solution praticable pour tous les cas est encore à désirer.