6.

La loi de réciprocité tireé des formules de Mr. Gauss, sans avoir déterminé préalablement le signe du radical.

(Par Mr. G. *Eisenstein* à Berlin.)

Mr. *Gauss* a déduit la loi de réciprocité entre deux nombres premiers impairs quelconques, des formules remarquables présentées dans son beau mémoire ayant pour titre: „Summatio quarundam serierum singularium." Cette démonstration, qu'on trouve aussi dans un excellent mémoire de Mr. *Dirichlet* *), est maintenant bien connue, et l'on sait que les considérations de Mr. *Gauss* exigent nécessairement *la détermination du signe du radical* qui entre dans les formules citées. Mais la détermination de ce signe est un des problèmes les plus difficiles de la science des nombres, et les recherches préliminaires qu'il y a à faire pour vaincre cette difficulté paraissent diminuer beaucoup la simplicité de cette démonstration. Nous ferons voir ici, comment on peut déduire des formules de Mr. *Gauss*, la loi de réciprocité, *sans avoir déterminé le signe du radical*.

Soient p et q deux nombres premiers impairs, et supposons $q > p$; soit de plus r une racine imaginaire de l'équation $x^p = 1$, et posons pour abréger,

$$\sum_{k=1}^{k=p-1}\left(\frac{k}{p}\right)r^k = S, \qquad \sum_{k=1}^{k=p-1}\left(\frac{k}{p}\right)r^{qk} = S_q.$$

Les formules de Mr. *Gauss* donnent les deux équations suivantes:

$$(\alpha.) \qquad S_q = \left(\frac{q}{p}\right)S,$$

$$(\beta.) \qquad S^2 = (-1)^{\frac{1}{2}(p-1)}p.$$

Si l'on élève la seconde de ces deux équations à la puissance $\frac{1}{2}(q+1)$ et que l'on en retranche la première après l'avoir multipliée par S, on trouve

$$S^{q+1} - SS_q = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q+1)}p^{\frac{1}{2}(q+1)} - \left(\frac{q}{p}\right)S^2.$$

Substituant la valeur du quarré S^2 fournie par l'equation $(\beta.)$, on aura

*) „Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies. Tome XVII. de ce journal.

$$(\gamma.) \qquad S(S^q - S_q) = (-1)^{\frac{1}{2}(p-1)} p \left((-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right)\right).$$

Pour abréger, nous désignerons l'expression à gauche par χ.

En développant la puissance S^q, on voit aisément qu'elle renferme: 1) Les $q$ièmes puissances de tous les termes individuels de la série S, c'est à dire les termes de la forme $\left(\frac{k}{p}\right)^q r^{qk} = \left(\frac{k}{p}\right) r^{qk}$. La somme de ces termes sera $= S_q$. 2) Un nombre de termes dont les coëfficients sont divisibles par q.

On voit donc que l'expression $S(S^q - S_q)$ peut prendre la forme

$$q(A + Br + Cr^2 + \ldots + Kr^{p-2}),$$

où $A, B, C, \ldots K$ sont des entiers réels. Donc on a

$$\chi = q(A + Br + Cr^2 + \ldots + Kr^{p-2}).$$

Comme rien n'empêche de remplacer dans tous ces résultats r par ses autres valeurs

$$r^2, \; r^3, \; r^4, \; \ldots \; r^{p-1},$$

on aura aussi

$$\begin{aligned} \chi &= q(A + Br^2 + Cr^4 + \ldots), \\ \chi &= q(A + Br^3 + Cr^6 + \ldots), \\ &\cdots\cdots\cdots\cdots \\ \chi &= p(A + Br^{p-1} + Cr^{2(p-1)} + \ldots). \end{aligned}$$

La somme de ces $p-1$ équations est

$$(p-1)\chi = q((p-1)A - B - C - \ldots - K),$$

ce qui prouve que $(p-1)\chi$ est divisible par q. De là, $p(p-1)$ n'étant pas divisible par q, on conclut

$$(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} \equiv \left(\frac{q}{p}\right) \pmod{q},$$

$$p^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} \left(\frac{q}{p}\right) \pmod{q},$$

d'où l'on tire

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

ce qu'il s'agissait de prouver.

Nous démontrerons par une analyse semblable le théorème rélatif au nombre 2; c'est à dire la formule $\left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}(q^2-1)}$.

En combinant les deux équations suivantes

$$(\Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^\gamma)^2 = 8, \qquad \Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^{q\gamma} = (-1)^{\frac{1}{8}(q^2-1)} \Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^\gamma,$$

où ζ désigne une racine primitive de l'équation $x^8 = 1$, et où les sommations doivent s'étendre aux quatre entiers γ inférieurs et premiers à 8, on obtient facilement

$$(\Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^\gamma)[(\Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^\gamma)^q - \Sigma(-1)^{\frac{1}{8}(\gamma^2-1)}\zeta^{q\gamma}]$$
$$= 8(8^{\frac{1}{2}(q-1)} - (-1)^{\frac{1}{8}(q^2-1)}).$$

On tire de là par les mêmes considérations comme ci-dessus, que le second membre est divisible par q, ce qui donne la congruence

$$8^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{8}(q^2-1)} \pmod{q},$$

donc

$$\left(\frac{8}{q}\right) = \left(\frac{2}{q}\right) = (-1)^{\frac{1}{8}(q^2-1)}.$$

Berlin, Mai 1844.