NOUVELLES ANNALES DE MATHÉMATIQUES

ZOLOTAREFF

# Nouvelle démonstration de la loi de réciprocité de Legendre

*Nouvelles annales de mathématiques 2^e série*, tome 11 (1872), p. 354-362

<http://www.numdam.org/item?id=NAM_1872_2_11__354_0>

# NOUVELLE DÉMONSTRATION DE LA LOI DE RÉCIPROCITÉ DE LEGENDRE;

PAR M. ZOLOTAREFF,
Privatdocent à l'Université de Saint-Pétersbourg.

Soit $p$ un nombre premier impair. Étant donnée une suite de nombres

$$1,\quad 2,\quad 3,\ldots,\quad p-1, \tag{1}$$

si l'on y permute d'une manière quelconque les éléments, on aura une autre disposition

$$\mu,\quad \mu',\quad \mu'',\ldots. \tag{2}$$

On sait que toutes les $1.2.3\ldots(p-1)$ dispositions possibles se partagent en deux classes, contenant chacune $\frac{1.2.3\ldots(p-1)}{2}$ dispositions. Les dispositions qui forment la première classe se déduisent de (1) au moyen d'un nombre pair de transpositions, et celles qui forment la seconde classe se déduisent de (1) au moyen d'un nombre impair de transpositions. Nous dirons, pour abréger, que le caractère de la disposition est égal à $+1$ ou à $-1$, suivant que cette disposition appartiendra à la première ou à la seconde classe.

Cela posé, nous allons démontrer la proposition suivante :

THÉORÈME I. — *Soit $k$ un nombre entier quelconque non divisible par $p$. Le caractère de la suite*

$$k,\quad 2k,\quad 3k,\ldots,\quad (p-1)k, \tag{3}$$

*si l'on y remplace les éléments par leurs résidus par*

*rapport au module p qui se trouvent dans la série* (1), *est égal à* $\left(\frac{k}{p}\right)$.

*Démonstration.* — Soit $a$ l'une des racines primitives du nombre $p$. La suite des nombres

$$(4) \qquad 1, \quad a, \quad a^2, \ldots, \quad a^{p-2},$$

si l'on y remplace chaque nombre par son résidu positif moindre que $p$, aura les mêmes éléments que la suite (1).

Posons

$$k \equiv a^f \pmod{p},$$

et considérons la suite des nombres

$$(5) \qquad a^f, \quad a^{f+1}, \quad a^{f+2}, \ldots, \quad a^{f+p-2},$$

à laquelle s'applique aussi la remarque qu'on vient de faire par rapport à la suite (4).

On peut évidemment passer de la disposition (4) à celle-ci (5), au moyen de $f$ substitutions circulaires d'ordre $p-1$. En remarquant que toute substitution circulaire d'ordre $p-1$ est équivalente à $p-2$ transpositions, on voit qu'on passe de la suite (4) à la suite (5) au moyen de $(p-2)f$ transpositions. Il s'ensuit qu'en faisant les mêmes transpositions dans la disposition (1), c'est-à-dire en permutant circulairement $f$ fois les nombres de cette suite congrus à $1, a, a^2, \ldots, a^{p-2}$, on arrivera à la disposition (3). En effet, après ces permutations, chaque nombre sera remplacé par un autre égal au premier multiplié par $a^f \equiv k \pmod{p}$, c'est-à-dire que la disposition (1) sera remplacée par la disposition (3). En remarquant que $p-2$ est un nombre impair, on conclut que le nombre $(p-2)f$ sera pair ou impair, suivant que $f$ sera pair ou impair, c'est-à-dire suivant que $k$ sera résidu ou non résidu quadratique de $p$. C. Q. F. D.

Laissant de côté les conséquences qui se déduisent du théorème précédent, relatives au caractère quadratique des nombres $-1$ et $2$, passons à la loi de réciprocité.

Soit $q$ un autre nombre premier impair. Concevons qu'on déduise de la disposition

$$(6) \qquad 1,\ 2,\ 3,\ldots,\ p,\ p+1,\ldots,\ qp-1$$

une nouvelle disposition

$$(7)\ \begin{cases} \lambda_1 p+1,\ \lambda_2 p+2,\ \lambda_3 p+3,\ldots,\ p,\ (\lambda_1+1)p+1, \\ \qquad (\lambda_2+1)p+2,\ldots,\ 2p,\ldots, \end{cases}$$

par le procédé suivant.

On ajoute aux éléments de la série (6), qui sont congrus à 1 par rapport au module $p$, le nombre $\lambda_1 p$; aux éléments congrus à 2, on ajoute $\lambda_2 p$ et ainsi de suite. $\lambda_1$, $\lambda_2,\ldots$ sont des nombres entiers quelconques; enfin les éléments de la suite (6), qui sont multiples de $p$, n'éprouvent aucun changement. Après cela, on remplace les éléments de la suite (7) par leurs résidus positifs par rapport au module $pq$, moindres que $pq$. Ce remplacement étant fait, il est facile de voir que la série (7) aura les mêmes éléments que la série (6), mais disposés dans un ordre différent.

Relativement à cette disposition on a :

THÉORÈME II. — *La série* (7) *se déduit de la suite* (6) *au moyen d'un nombre pair de transpositions.*

En effet, ne considérant d'abord que les nombres de la série (7) congrus à 1 par rapport au module $p$,

$$\lambda_1 p+1,\quad (\lambda_1+1)p+1,\ldots,\quad (\lambda_1+q-1)p+1,$$

on voit qu'au moyen de substitutions circulaires d'ordre $q$, on peut ramener cette disposition à celle-ci

$$1,\quad p+1,\quad 2p+1,\ldots,\quad (q-1)p+1.$$

Toute substitution circulaire d'ordre $q$ étant équivalente à $q-1$ transpositions, c'est-à-dire à un nombre pair de transpositions, il s'ensuit que le nombre de toutes les transpositions relatives aux éléments congrus à 1 sera pair. La même conclusion aura lieu pour les éléments congrus à 2, 3,..., et par conséquent le nombre des transpositions au moyen desquelles on passe de la disposition (6) à la disposition (7) sera pair.

THÉORÈME III. — *Le caractère de la suite*

$$(8)\quad \begin{cases} q, \quad 2q, \ldots, \quad (p-1)q, \quad 1, \quad 1+q, \quad 1+2q, \ldots, \\ \qquad 1+(p-1)q, \quad 2, \quad 2+q, \ldots, \end{cases}$$

*qui se distingue de la suite* (6) *par la disposition de ses éléments, en ce qu'on y trouve d'abord* $p-1$ *nombres congrus à* 0 (mod. $q$), *ensuite* $p-1$ *nombres congrus à* 1, *et ainsi de suite, est égal à* $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Pour démontrer ce théorème, il faut compter le nombre de transpositions au moyen desquelles on passe de la disposition (8) à la disposition (6).

Pour cela, dans la disposition (8), on fait arriver 1 à la première place au moyen de $p-1$ transpositions, ensuite 2 à la seconde place au moyen de $2(p-1)$ transpositions, et ainsi de suite, enfin $q-1$ à la $(q-1)^{ième}$ place au moyen de $(q-1)(p-1)$ transpositions. Ainsi, en faisant

$$p-1+2(p-1)+\ldots+(q-1)(p-1)=\frac{q(q-1)}{2}(p-1)$$

transpositions, on passe de la suite (8) à celle-ci

$$1, \quad 2, \quad 3, \ldots, \quad q-1, \quad q, \quad 2q, \ldots, \quad (p-1)q,$$
$$1+q, \quad 1+2q, \ldots.$$

Après cela, en faisant encore $\frac{q(q-1)}{2}(p-2)$ transpositions, on arrivera à la disposition

$$1,\ 2,\ 3,\ldots,\ q-1,\ q,\ 1+q,\ 2+q,\ldots,$$
$$2q-1,\ 2q,\ 3q,\ldots,\ (p-1)q,\ldots.$$

Donc, en continuant la même marche, on verra qu'après avoir fait

$$\frac{q(q-1)}{2}(p-1+p-2+\ldots+1)=\frac{q(q-1)}{2}\frac{p(p-1)}{2}$$

transpositions, on arrivera à la disposition (6).

Le nombre

$$\frac{q(q-1)}{2}\ \frac{p(p-1)}{2}$$

sera pair ou impair, suivant que $\frac{q-1}{2}\ \frac{p-1}{2}$ sera pair ou impair; par conséquent le théorème est démontré.

Considérons maintenant une suite de nombres

$$(9)\quad \left\{\begin{array}{l} q,\ 2q,\ldots,\ (p-1)q,\ p,\ p+q,\ldots, \\ p+(p-1)q,\ 2p,\ 2p+q,\ldots, \end{array}\right.$$

contenant d'abord $p-1$ nombres divisibles par $q$, ensuite $p$ nombres congrus à $p$ (mod. $q$), $p$ nombres congrus à $2p$, et ainsi de suite, enfin $p$ nombres congrus à $(q-1)p$. Si, au lieu de ces nombres, on prend leurs résidus positifs par rapport au module $pq$, moindres que $pq$, on aura tous les éléments de la suite (6).

Cela posé, nous allons démontrer que le caractère de la disposition (9) est égal à $\left(\frac{q}{p}\right)$.

En effet, les nombres

$$q, \quad 2q, \ldots, \quad (p-1)q$$

peuvent être représentés comme il suit :

$$\begin{aligned} q &= \lambda_1 p + \alpha, \\ 2q &= \lambda_2 p + \alpha_2, \\ &\ldots\ldots\ldots\ldots, \\ (p-1)q &= \lambda_{p-1} p + \alpha_{p-1}, \end{aligned}$$

où $\lambda_1, \lambda_2, \ldots, \lambda_{p-1}$ sont des nombres entiers, et où la suite des nombres $\alpha_1, \alpha_2, \ldots, \alpha_{p-1}$ est la même que la suite

$$1, \quad 2, \quad 3, \ldots, \quad p-1;$$

on y trouve seulement les éléments dans une autre disposition. Le caractère de cette disposition, en vertu du théorème I, est égal à $\left(\frac{q}{p}\right)$.

Désignons par $\sigma$ le nombre des transpositions par lesquelles on passe de la disposition

$$q, \quad 2q, \ldots, \quad (p-1)q$$

à celle-ci

$$\mu_1 p + 1, \quad \mu_2 p + 2, \ldots, \quad \mu_{p-1} p + p - 1,$$

où $\mu_1 = \lambda_i$, si $\alpha_i = 1$, où $\mu_2 = \lambda'_i$, si $\alpha'_i = 2, \ldots$. Il résulte de ce qui précède que $\sigma$ sera un nombre pair ou impair, suivant que $\left(\frac{q}{p}\right) = 1$ ou que $\left(\frac{q}{p}\right) = -1$.

En faisant de nouveau les mêmes transpositions dans la suite

$$p+q, \quad p+2q, \ldots, \quad p+(p-1)q,$$

nous arriverons à la suite

$$(\mu_1+1)p+1, \quad (\mu_2+1)p+2, \ldots, \quad (\mu_{p-1}+1)p+p-1.$$

Le même chose s'applique à la disposition

$$2p+q, \quad 2p+2q\ldots, \quad 2p+(p-1)q$$

et aux autres suites.

Nous avons donc à faire $\sigma q$ transpositions pour passer à la disposition (7), qui nous ramènera à la disposition (6) au moyen d'un nombre pair de transpositions (th. II). Il en résulte que le caractère de la suite (9) dépend de la parité du nombre $\sigma$. Il est donc égal à $\left(\frac{q}{p}\right)$.

On peut trouver une autre expression pour le caractère de la suite (9). Soient

$$(10) \qquad \begin{cases} p = \rho_1 q + \beta_1, \\ 2p = \rho_2 q + \beta_2, \\ \cdots\cdots\cdots\cdots, \\ (q-1)p = \rho_{q-1} q + \beta_{q-1}. \end{cases}$$

La série de nombres

$$\beta_1, \quad \beta_2, \ldots, \quad \beta_{q-1}$$

contient les mêmes éléments que la séric

$$1, \quad 2, \quad 3, \ldots, \quad q-1,$$

mais dans un ordre différent.

D'après ce qui précède, on voit que le caractère de cet ordre est égal à $\left(\frac{p}{q}\right)$. Remarquons que, sans changer le caractère de la suite, il est permis de faire des transpositions entre ses éléments, pourvu que le nombre de ces transpositions soit pair. Ainsi on peut faire des substitutions circulaires d'ordre $q$, puisque ces substitutions sont équivalentes à $q-1$ transpositions.

D'après cela, en considérant d'abord les nombres de la suite (9) congrus à $p$ par rapport au module $q$, et en

remplaçant $p$ par son expression (10), on voit qu'ils peuvent être rangés, au moyen de quelques substitutions circulaires, comme il suit :

$$\beta_1, \quad \beta_1 + q, \quad \beta_1 + 2q, \ldots, \quad \beta_1 + (p-1)q,$$

sans changer le caractère de la suite (9). De même les nombres congrus à $2p$ peuvent être écrits ainsi

$$\beta_2, \quad \beta_2 + q, \quad \beta_2 + 2q, \ldots, \quad \beta_2 + (p-1)q.$$

De sorte qu'au lieu de la disposition (9), on peut considérer la disposition

$$(11) \left\{ \begin{array}{c} q, \ 2q, \ldots, \ (p-1)q, \ \beta_1, \ \beta_1 + q, \ldots, \ \beta_1 + (p-1)q, \\ \beta_2, \ \beta_2 + q, \ldots, \ \beta_2 + (p-1)q, \ldots. \end{array} \right.$$

Afin de déterminer le caractère de cette dernière suite, permutons les nombres

$$\beta_1, \quad \beta_2, \ldots, \quad \beta_{q-1},$$

en laissant les autres à leurs places. Supposons qu'au moyen de $\delta$ transpositions, cette disposition devienne

$$1, \quad 2 \quad 3, \ldots, \quad q-1.$$

En faisant les transpositions correspondantes entre les nombres

$$\beta_1 + q, \quad \beta_2 + q, \ldots, \quad \beta_{q-1} + q,$$

nous arriverons à la disposition

$$1 + q, \quad 2 + q, \ldots, \quad q - 1 + q,$$

et ainsi de suite. En sorte que, après les $\delta p$ transpositions, on aura, au lieu de la suite (11), celle-ci

$$q, \ 2q, \ldots, \ (p-1)q, \ 1+q, \ 2+q, \ldots, \ 1+2q, \ 2+2q, \ldots.$$

Nous avons vu plus haut que le caractère de cette série est égal à $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (th. III).

En remarquant que $\delta$ est pair ou impair, suivant que $\left(\frac{p}{q}\right) = 1$ ou que $\left(\frac{p}{q}\right) = -1$, on en conclura que le caractère de la série (11) ou, ce qui revient au même, de la série (9) est égal à $\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Or on a démontré plus haut que le caractère de la même série est égal à $\left(\frac{q}{p}\right)$; on aura donc

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