Matyáš Lerch

Modification de la troisième démonstration donnée par Gauss de la loi de réciprocité de Legendre

Jornal des sciencias mathematicas e astronomicas, Coimbra, 8 (1887), 137–146

Persistent URL: http://dml.cz/dmlcz/501621

MODIFICATION DE LA TROISIÈME DÉMONSTRATION DONNÉE PAR GAUSS DE LA LOI DE REPROCITÉ DE LEGENDRE

PAR

M. LERCH

(à Prague)

Il y a déjà une foule des démonstrations du célèbre théorème arithmétique appelé la loi de reciprocité de Legendre, et parmi elles plusieures reposent sur le même principe que la troisième parmi les six démonstrations données par Gauss de ce théorème. C'est aussi la démonstration suivante que je vais développer.

Dans cette note je fais usage du symbole $E(x)$ qui représente le plus grand nombre entier contenu dans la quantité x supposée réelle et positive, de sorte que la différence $x - E(x)$ sera ou zéro ou une quantité positive inférieure à l'unité; ensuite, je représente par $R(x)$ le résultat qu'on obtient en retranchant de la quantité réelle x le nombre entier qui lui est le plus approché, de sorte que la quantité $R(x)$ est ou positive ou négative, mais toujours contenue entre les limites $\left(-\frac{1}{2} \ldots \frac{1}{2}\right)$, de sorte qu'on a

$$-\frac{1}{2} \leq R(x) < \frac{1}{2}.$$

Enfin, x étant une quantité différente de zéro, je représente par le symbole sgn. x (lisez signum x) ou $+1$ ou -1, selon que x est positif ou négatif. Ces deux dernières fonctions numériques ont été introduites par M. Kronecker.

1. Soit maintenant p un nombre premier supérieur à 2, q un nombre entier positif non divisible par p, et posons

$$(1) \qquad a_\nu = 2\nu q - p - 2p\,\mathrm{E}\left(\frac{\nu q}{p}\right), \quad \left(\nu = 1, 2, 3, \ldots \frac{p-1}{2}\right).$$

Les nombres $a_1, a_2, \ldots a_{\frac{p-1}{2}}$ sont évidemment tous entiers, positifs ou négatifs, impairs, et en valeur absolue moindres que p. Je vais en premier lieu en déterminer les signes. Comme le nombre a_ν a le même signe que le suivant

$$\frac{a_\nu}{2p} = \frac{\nu q}{p} - \mathrm{E}\left(\frac{\nu q}{p}\right) - \frac{1}{2},$$

il suffit de considérer ce dernier nombre. Or la différence

$$\frac{\nu q}{p} - \mathrm{E}\left(\frac{\nu q}{p}\right)$$

étant le reste positif de la fraction $\frac{\nu q}{p}$, la quantité $\frac{a_\nu}{2p}$ sera positive ou négative selon que

$$\frac{\nu q}{p} - \mathrm{E}\left(\frac{\nu q}{p}\right) > \frac{1}{2} \text{ ou } < \frac{1}{2};$$

et comme on a dans le premier cas $\mathrm{R}\left(\frac{\nu q}{p}\right) < 0$, et $\mathrm{R}\left(\frac{\nu q}{p}\right) > 0$ dans le second, on voit que $\frac{a_\nu}{2p}$ sera positif ou négatif selon que $\mathrm{R}\left(\frac{\nu q}{p}\right)$ sera négatif ou positif.

En d'autres termes on a

$$\mathrm{sgn.}\left(\frac{a_\nu}{2p}\right) = -\mathrm{sgn.}\,\mathrm{R}\left(\frac{\nu q}{p}\right),$$

ou ce qui est la même chose,

$$\text{(2)} \qquad \text{sgn. } a_\nu = -\text{sgn. R}\left(\frac{\nu q}{p}\right).$$

C'est cette formule qui exprime le signe de a_ν par celui de la fonction arithmétique $\text{R}(x)$.

Je dis maintenant que les $\frac{p-1}{2}$ nombres a_ν sont différents même dans leurs valeurs absolues. Car en effet, si a_ρ et a_ν auraient la même valeur absolue, ou devrait avoir ou $a_\nu = a_\rho$ ou $a_\nu = -a_\rho$, c'est-à-dire l'un des deux nombres $a_\nu \pm a_\rho$ devrait s'annuler. Or les nombres ν, ρ étant supposés contenus dans la série $1, 2, 3, \ldots \frac{p-1}{2}$, la valeur absolue du nombre $\nu \pm \rho$ sera moindre que $p-1$; ensuite, on déduit de l'hypothèse $a_\nu \pm a_\rho = 0$ l'équation suivante

$$2(\nu \pm \rho)q = (1 \pm 1)p + 2p\text{E}\left(\frac{\nu q}{p}\right),$$

dont on voit que $(\nu \pm \rho)q$ doit être divisible par p. Or q étant premier avec p, il faut que $\frac{\nu \pm \rho}{p}$ soit un nombre entier, ce qui est impossible, le numérateur étant inférieur à $p-1$. Donc tous les nombres a_ν ont leurs modules différents entre eux.

Cela étant il est clair que les nombres a_ν ne diffèrent que par l'ordre et le signe des nombres de la suite $1, 2, 5, 7, \ldots p-2$, de sorte que le produit $a_1 a_2 a_3 \ldots a_{\frac{p-1}{2}}$ a pour valeur absolue le nombre $1 \cdot 3 \cdot 5 \ldots p-2$, et comme son signe équivant au produit des seconds membres de la formule (2), savoir

$$\Pi\left[-\text{sgn. R}\left(\frac{\nu q}{p}\right)\right] = (-1)^{\frac{1}{2}(p-1)}\,\text{sgn.}\prod_{\nu=1}^{\frac{1}{2}(p-1)}\text{R}\left(\frac{\nu q}{p}\right),$$

on aura évidemment la formule

$$(3)\quad \begin{cases} a_1 a_2 a_3 \ldots a_{\frac{p-1}{2}} \\ = (-1)^{\frac{1}{2}(p-1)} 1.3.5 \ldots (p-2) \operatorname{sgn}. \prod_{\nu=1}^{\frac{1}{2}(p-1)} R\left(\frac{\nu q}{p}\right). \end{cases}$$

Or l'équation (1) montre qu'il subsiste la congruence

$$a_\nu \equiv 2\nu q, \pmod p,$$

de sorte que nous aurons

$$a_1 a_2 \ldots a_{\frac{p-1}{2}} \equiv 1.2.3 \ldots \frac{p-1}{2} . (2q)^{\frac{1}{2}(p-1)}, \pmod p,$$

et l'équation (3) nous donnera, par conséquent, la congruence

$$1.2.3 \ldots \frac{p-1}{2} . (2q)^{\frac{1}{2}(p-1)}$$
$$\equiv (-1)^{\frac{1}{2}(p-1)} 1.3.5 \ldots (p-2) \operatorname{sgn}. \prod_{\nu=1}^{\frac{1}{2}(p-1)} R\left(\frac{\nu q}{p}\right)$$

prise par rapport au même module p.

En multipliant les deux membres de cette congruence par le nombre

$$2.4.6 \ldots (p-1) = 2^{\frac{1}{2}(p-1)} . 1.2.3 \ldots \frac{p-1}{2},$$

il vient

$$(3*)\quad \begin{cases} \left(1.2.3 \ldots \frac{p-1}{2}\right)^2 . (4q)^{\frac{1}{2}(p-1)} \\ \equiv (-1)^{\frac{1}{2}(p-1)} (p-1)! \operatorname{sgn}. \prod R\left(\frac{\nu q}{p}\right). \end{cases}$$

Or le théorème de Wilson exprimé par la formule

$$(p-1)! \equiv -1, \pmod{p}$$

conduit à la congruence

$$\left(1.2.3\ldots\frac{p-1}{2}\right)^2 \equiv -(-1)^{\frac{1}{2}(p-1)}, \pmod{p},$$

puisque les nombres $\frac{p+1}{2}$, $\frac{p+3}{2}$, $\ldots$ $p-1$ sont congrus aux nombres $-\frac{p-1}{2}$, $-\frac{p-3}{2}$, $\ldots$ -1; on a ensuite, d'après le théorème de Fermat,

$$4^{\frac{1}{2}(p-1)} = 2^{p-1} \equiv 1, \pmod{p}.$$

D'après ces trois congruences la formule (3 *) se change en la suivante

$$q^{\frac{1}{2}(p-1)} \equiv \text{sgn.} \prod_{\nu=1}^{\frac{1}{2}(p-1)} \text{R}\left(\frac{\nu q}{p}\right), \pmod{p}.$$

et c'est cette congruence qui joue le rôle capitale dans la démonstration qui nous occupe.

Car en représentant avec Legendre par le symbol $\left(\frac{q}{p}\right)$ ou 1 ou -1 selon que la congruence $x^2 \equiv q$, (mod p) a ou n'a pas de racines, on sait depuis Euler que l'on a

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

ce qui est en même temps le théorème le plus élémentair de la théorie des résidus quadratiques.

D'après cette formule la congruence (4) se change en l'équation

$$(5) \qquad \left(\frac{q}{p}\right) = \text{sgn.} \prod_{\nu=1}^{\frac{1}{2}(p-1)} \mathrm{R}\left(\frac{\nu q}{p}\right)$$

qui se trouve établie dans plusieurs articles fort intéressants de M. Kronecker (*).

3. La formule (5) n'exprime que ce que le symbole $\left(\frac{q}{p}\right)$ équivaut ou à 1 ou à -1, selon que le nombre des termes négatifs de la série

$$(5*) \qquad \mathrm{R}\left(\frac{q}{p}\right), \quad \mathrm{R}\left(\frac{2q}{p}\right), \quad \mathrm{R}\left(\frac{3q}{p}\right), \quad \ldots \quad \mathrm{R}\left[\frac{\frac{1}{2}(p-1)q}{p}\right]$$

est pair ou impair. Cette série peut être remplaçée par d'autres; par exemple, le signe de la quantité $\mathrm{tg}\,\pi x$ ou celui de $\sin 2\pi x$ étant le même que celui de $\mathrm{R}(x)$ on peut considérer les séries

$$\mathrm{tg}\frac{\nu q\pi}{p}, \quad \sin\frac{2\nu q\pi}{p}, \quad \left(\nu = 1, 2, \ldots \frac{p-1}{2}\right)$$

au lieu de la précédante.

Je me borne seulement à remarquer que la somme

$$(6) \qquad \sigma = \sum_{\nu=1}^{\frac{1}{2}(p-1)} \frac{1}{2}\left[1 - \text{sgn.}\,\mathrm{R}\left(\frac{\nu q}{p}\right)\right]$$

est précisément égale au nombre des termes négatifs de la série (5). Car si $\text{sgn.}\,\mathrm{R}\left(\frac{\nu q}{p}\right) = 1$, le terme correspondant de la

(*) Sitzungsberichte der kön. preussischen Akad. d. Wiss; mai et juin 1884, avril et novembre 1885.

somme σ disparaît, tandis qu'il deviendra égal à l'unité en supposant que $R\left(\frac{\nu q}{p}\right)$ soit négatif, c'est-à-dire que $\text{sgn. } R\left(\frac{\nu q}{p}\right) = -1$; on aura donc la formule

$$\left(\frac{q}{p}\right) = (-1)^{\sigma}. \tag{6*}$$

Pour transformer la somme (6) je considère de nouveau les nombres a_ν introduits au commencement. Les nombres a_ν étant affectés du signe $-\text{sgn. } R\left(\frac{\nu q}{p}\right)$ les produits $a_\nu \text{ sgn. } R\left(\frac{\nu q}{p}\right)$ seront négatifs et coïncideront à l'ordre près avec les termes de la série $-1, -3, -5, \ldots -(p-2)$, dont la somme est

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

de sorte qu'il vient

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[2\nu q - p - 2p\,E\left(\frac{\nu q}{p}\right)\right] . \text{sgn. } R\left(\frac{\nu q}{p}\right) = -\left(\frac{p-1}{2}\right)^2;$$

il s'ensuit la formule

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[\nu q - p\,E\left(\frac{\nu q}{p}\right)\right] . \text{sgn. } R\left(\frac{\nu q}{p}\right)$$

$$-\frac{p}{2} \sum_{\nu=1}^{\frac{1}{2}(p-1)} \text{sgn. } R\left(\frac{\nu q}{p}\right) - \frac{1}{2}\left(\frac{p-1}{2}\right)^2;$$

en la retranchant, membre à membre, de l'identité

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[\nu q - p\,E\left(\frac{\nu q}{p}\right)\right] = \frac{p^2-1}{8} q - p \sum_{\nu=1}^{\frac{1}{2}(p-1)} E\left(\frac{\nu q}{p}\right)$$

il vient

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} \left[\nu q - pE\left(\frac{\nu q}{p}\right)\right]\left[1-\text{sgn.}\,R\left(\frac{\nu q}{p}\right)\right]$$

$$-p\sum_{\nu=1}^{\frac{1}{2}(p-1)}\frac{1}{2}\left[1-\text{sgn.}\,R\left(\frac{\nu q}{p}\right)\right]-p\sum_{\nu=1}^{\frac{1}{2}(p-1)}E\left(\frac{\nu q}{p}\right)+\frac{p^2-1}{8}(q-1).$$

Or les facteurs $1-\text{sgn.}\,R\left(\frac{\nu q}{p}\right)$ étant ou zéro ou deux, on voit que le premier membre est un nombre pair, et le nombre p étant impair on voit aisément que le second membre n'est pair que si

$$(7)\qquad \begin{cases} \sum_{\nu=1}^{\frac{1}{2}(p-1)}\frac{1}{2}\left[1-\text{sgn.}\,R\left(\frac{\nu q}{p}\right)\right] \\ \equiv \sum_{\nu=1}^{\frac{1}{2}(p-1)}E\left(\frac{\nu q}{p}\right)+\frac{p^2-1}{8}(q-1), \pmod 2; \end{cases}$$

c'est donc une formule qui permet de remplacer la somme (6) par un nombre de la même parité, ce qui suffit pour notre but.

Prenant alors $q=2$ et se rappelant ce que, dans ce cas, tous les fractions $\frac{2\nu}{p}$ étant moindres que l'unité, on aura $E\left(\frac{2\nu}{p}\right)=0$, de sorte que la formule (7) nous donne

$$\sigma \equiv \frac{p^2-1}{8}, \pmod 2,$$

et par suite l'équation (6 *) devient dans ce cas

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

Soit maintenant q un nombre impair; dans ce cas le nombre $\frac{p^2-1}{8}(q-1)$ sera pair et la congruence (7) deviendra

$$(9) \qquad \sigma \equiv \sum_{\nu=1}^{\frac{1}{2}(p-1)} \mathrm{E}\left(\frac{\nu q}{p}\right), \pmod 2.$$

Cette formule n'exige que ce que le nombre q soit impair et non divisible par le nombre premier p.

Mais si l'on cherche l'expression $\left(\frac{q}{p}\right)$, on doit supposer que même le nombre q soit premier et différent de p.

Cela étant supposé rempli, la règle exprimée par la formule (6*) nous donne

$$(10) \qquad \left(\frac{p}{q}\right) = (-1)^{\sigma'}, \quad \sigma' \equiv \sum_{\rho=1}^{\frac{1}{2}(p-1)} \mathrm{E}\left(\frac{\rho p}{q}\right), \pmod 2.$$

Je vais maintenant prouver la formule

$$(11) \qquad \sum_{\nu=1}^{\frac{1}{2}(p-1)} \mathrm{E}\left(\frac{\nu q}{p}\right) + \sum_{\rho=1}^{\frac{1}{2}(p-1)} \mathrm{E}\left(\frac{\rho p}{q}\right) = \frac{1}{4}(p-1)(q-1).$$

A cet effet je suppose $q<p$ et je considère la droite OP dont l'équation, dans le système cartésien, soit $y=\frac{q}{p}x$; soit P le point de cette droite dont l'abscisse est $x=\frac{1}{2}(p-1)$ et dont l'ordonnée sera donc

$$y = \frac{1}{2}(q-1) + \frac{1}{2}\left[1 - \frac{q}{p}\right],$$

de sorte que

$$\mathrm{E}(y) = \frac{1}{2}(q-1).$$

En représentant par P', P'' les projections du point P sur l'axe des x et des y, j'observe que le triangle rectangle OP'P contient précisément $\sum_{\nu=1}^{\frac{1}{2}(p-1)} E\left(\frac{\nu q}{p}\right)$ points dont les coordonnées sont des nombres entiers positifs, ainsi que le triangle OP''P contient $\sum_{\rho=1}^{\frac{1}{2}(p-1)} E\left(\frac{\rho p}{q}\right)$ des points de cette espèce. Comme le contour de ces triangles ne contient aucun de tels points, on voit que la somme

$$\sum_{\nu=1}^{\frac{1}{2}(p-1)} E\left(\frac{\nu q}{p}\right) + \sum_{\rho=1}^{\frac{1}{2}(p-1)} E\left(\frac{\rho p}{q}\right)$$

équivaut au nombre des points, à coordonnées entières et positives, placés dans le rectangle OP'PP'', et ce nombre étant évidemment le produit $\frac{p-1}{2} \cdot \frac{q-1}{2}$ l'équation (11) est démontrée.

Alors il résulte des formules (6*), (9), (10) et (11) la suivante

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

qui exprime le célèbre théorème de Legendre que nous voulions établir.