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

V.-A. LEBESGUE

Démonstration nouvelle et élémentaire de la loi de réciprocité de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations qui peuvent être tirées du même principe

Journal de mathématiques pures et appliquées 1re série, tome 12 (1847), p. 457-473.
<http://www.numdam.org/item?id=JMPA_1847_1_12__457_0>

Démonstration nouvelle et élémentaire de la loi de réciprocité de Legendre, par M. Eisenstein, précédée et suivie de remarques sur d'autres démonstrations qui peuvent être tirées du même principe;

Par M. V.-A. LEBESGUE,

Correspondant de l'Institut, Professeur à la Faculté des Sciences de Bordeaux.

La démonstration de M. Eisenstein, dont je veux parler ici (car M. Eisenstein en a donné plusieurs), est celle qui a paru en 1844 dans le tome XXVII du Journal de M. Crelle. Il est dit, dans le préambule, que dans l'espace de près de trente ans, on n'avait rien ajouté de nouveau aux six démonstrations de M. Gauss. Désirant connaître le fondement de cette assertion, j'ai relu les six démonstrations de M. Gauss et celles qui sont parvenues à ma connaissance; j'ai été conduit à quelques remarques que je vais exposer brièvement :

1°. La démonstration de M. Jacobi, communiquée à Legendre en 1827, et qui a paru en 1830 dans la troisième édition de la *Théorie des Nombres*, ou, ce qui revient au même, la démonstration donnée par M. Cauchy, en 1829, dans le Bulletin de Férussac, peut être regardée comme une simplification de la sixième démonstration de M. Gauss.

2°. Le principe fondamental de la démonstration nouvelle et élémentaire de M. Eisenstein paraît emprunté à la sixième démonstration de M. Gauss.

En d'autres termes, ces démonstrations emploient le développement suivant :

$$\left\{\sum_{i=1}^{i=p-1}\left(\frac{i}{p}\right)x^i\right\}^q=\xi^q.$$

où le symbole $\left(\frac{i}{p}\right)$ représente $+1$ si i est résidu quadratique du nombre p, premier impair et positif, et -1 si i est non-résidu quadratique de p.

M. Gauss suppose x tout à fait indéterminée.

MM. Jacobi et Cauchy supposent $x^p = 1$, x imaginaire.

M. Eisenstein suppose $x^p = 1$, $x = 1$.

3°. La démonstration que j'ai donnée dans le tome III, page 142 de ce Journal (*Recherches sur les Nombres*), peut être considérablement abrégée par l'emploi du développement indiqué plus haut, ou plutôt par celui-ci,

$$\left\{\sum_{i=1}^{i=p-1} x^{i^2}\right\}^q,$$

qui s'y ramène immédiatement quand $x^p = 1$.

I.

1. La sixième démonstration de M. Gauss dépend du développement de la somme $\xi = \sum_{i=1}^{i=p-1} \left(\frac{i}{p}\right) x^i$ élevée à la puissance q. L'auteur, qui emploie une autre notation, commence par montrer que la quantité

$$\xi^2 - (-1)^{\frac{p-1}{2}} p$$

est divisible par

$$1 + x + x^2 + \ldots + x^{p-1} = \sum_{i=1}^{i=p-1} x^i;$$

le nombre p est supposé positif premier et impair. La quantité x est tout à fait arbitraire.

On voit donc que pour $x^p = 1$, on a

$$\xi^2 - (-1)^{\frac{p-1}{2}} p = 0,$$

ce qui avait été déjà prouvé par le même auteur dans ses *Recherches arithmétiques*.

M. Gauss donne ensuite une double expression de la somme ξ^q, d'où résulte une identité qui conduit à la loi de réciprocité.

2. La rédaction que Legendre a donnée de la démonstration de M. Jacobi n'est pas complétement satisfaisante. D'après une Note qui se trouve à la page 172 du tome XXX du Journal de M. Crelle, la démonstration de M. Jacobi serait celle que M. Eisenstein a exposée dans un article intitulé : « La loi de réciprocité tirée des formules de » M. Gauss, sans avoir préalablement déterminé le signe du radical » (Journal de M. Crelle, tome XXVIII). La démonstration de M. Cauchy n'est qu'indiquée dans le Bulletin de Férussac (septembre 1829) : elle se trouve avec tous les développements nécessaires dans la quatrième Note du Mémoire sur la théorie des nombres (*Mémoires de l'Académie royale des Sciences*, tome XVII).

Voici, avec une légère modification, la rédaction de M. Eisenstein.

Soit

$$S = \sum_{i=1}^{i=p-1} \left(\frac{i}{p}\right) x^i, \qquad \sum_{i=1}^{i=p-1} \left(\frac{i}{p}\right) x^{qi} = S_q = \left(\frac{q}{p}\right) S;$$

comme on a

$$S^2 = (-1)^{\frac{p-1}{2}} p,$$

il en résultera

$$S^{q-1} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}},$$

d'où

$$S.S^q = (-1)^{\frac{p-1}{2}} p.(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}};$$

d'ailleurs

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

donc

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

Mais on reconnaît tout de suite que $S^q - S_q$ se réduit à une somme de termes de la forme qAx^i où A est entier, pourvu que q soit un nombre

premier et impair; il en sera donc de même de $S(S^q - S_q)$, et l'on aura

$$m = (-1)^{\frac{p-1}{2}} p \left\{ (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right) \right\}$$
$$= q(A + Bx + \ldots + Gx^{p-2} + Hx^{p-1}).$$

Soit donc l'équation

$$m = q(A + Bx + \ldots Gx^{p-2} + Hx^{p-1}),$$

où m, q, A, B,..., H sont des nombres entiers; comme on a

$$qH(1 + x + x^2 + \ldots + x^{p-1}) = 0,$$

l'équation précédente deviendra

$$m = q[(A - H) + (B - H)x + \ldots + (G - H)x^{p-2}].$$

Or l'équation

$$1 + x + x^2 + \ldots + x^{p-1} = 0$$

est irréductible : il faut donc qu'on ait

$$B = H, \ldots\ldots, G = H,$$

et

$$m = q(A - H),$$

ce qui montre que q divise m, et, par conséquent aussi,

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

puisque q est premier à p. D'ailleurs

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

est aussi divisible par q; il suit de là que

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

sera également divisible par q, ce qui ne peut arriver que pour

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

ce qui est la loi de réciprocité.

5. Cette démonstration a été donnée comme la plus courte; mais si l'on remarque qu'elle suppose la démonstration de l'équation

$$\xi^2 = (-1)^{\frac{p-1}{2}} p,$$

on reconnaîtra qu'elle est réellement plus longue et d'ailleurs moins simple que la troisième démonstration de M. Gauss. Quand on fait intervenir l'équation $x^p = 1$ dans la démonstration de la loi de réciprocité, la démonstration la plus courte est, ce me semble, celle que M. Liouville a donnée dans ce Journal (février 1847); l'équation

$$\xi^2 = (-1)^{\frac{p-1}{2}} p$$

est remplacée par la suivante, où ρ est une racine imaginaire de l'équation $x^p = 1$,

$$p = (-1)^{\frac{p-1}{2}} (\rho^1 - \rho^{-1})^2 (\rho^2 - \rho^{-2})^2 \dots \left(\rho^{\frac{p-1}{2}} - \rho^{-\frac{p-1}{2}}\right)^2;$$

l'élévation à la puissance $\frac{1}{2}(q-1)$ donne, comme on le voit aisément,

$$p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \Pi\left(\frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}}\right)\left(\begin{matrix}\alpha = 1 \\ \alpha = \frac{p-1}{2}\end{matrix}\right).$$

Cette équation, comparée à celle-ci,

$$\left(\frac{q}{p}\right) = \Pi\left(\frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}}\right),$$

donne immédiatement la loi de réciprocité.

Quant à l'équation fondamentale

$$p = (-1)^{\frac{p-1}{2}} \Pi (\rho^{\alpha} - \rho^{-\alpha})^2,$$

où $\alpha = 1, 2, 3, \dots, \frac{p-1}{2}$, c'est une conséquence presque immédiate de l'identité

$$1 + x + x^2 + \dots + x^{p-1} = (x - \rho)(x - \rho^2) \dots x - \rho^{p-1}).$$

Il est à remarquer que l'équation

$$\left(\frac{q}{p}\right) = \Pi\left(\frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}}\right)$$

revient à

$$\left(\frac{q}{p}\right) = \Pi \frac{\sin \alpha \frac{q\,2\pi}{p}}{\sin \alpha \frac{2\pi}{p}};$$

cette équation, combinée avec cette autre

$$\left(\frac{p}{q}\right) = \Pi \frac{\sin \beta \frac{p\,2\pi}{q}}{\sin \beta \frac{2\pi}{q}} \left(\beta = 1 \quad \beta = \frac{q-1}{2}\right),$$

a conduit M. Eisenstein à une démonstration qui a son analogue dans la théorie des résidus biquadratiques et cubiques.

Voyez son article sur l'application de l'algèbre à l'arithmétique transcendante (Journal de M. Crelle, tome XXIX).

II.

4. La démonstration nouvelle et élémentaire de M. Eisenstein s'appuie sur le calcul de certaines sommes $\psi(\mu, \nu)$, qui se présentent tout naturellement quand on développe

$$\xi^\mu = \left\{\sum \left(\frac{i}{p}\right) x^i\right\}^\mu = \left\{\left(\frac{1}{p}\right) x + \left(\frac{2}{p}\right) x^2 + \ldots + \left(\frac{p-1}{p}\right) x^{p-1}\right\}^\mu$$

dans l'hypothèse de $x^p = 1$.

En supposant p premier, le terme général du développement de ξ^μ sera

$$\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_\mu}{p}\right) x^{a_1 + a_2 + \ldots + a_\mu},$$

en représentant par

$$a_1, \quad a_2, \ldots, \quad a_\mu,$$

des nombres égaux ou non pris dans la série

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

Si donc on pose

$$a_1 + a_2 + \ldots + a_\mu \equiv \nu \pmod{p},$$

et qu'on fasse

$$\sum \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_\mu}{p}\right) = \psi(\mu, \nu),$$

on aura

$$\xi^\mu = \psi(\mu, 0) + \psi(\mu, 1)x + \psi(\mu, 2)x^2 + \ldots + \psi(\mu, \nu)x^\nu + \ldots + \psi(\mu, p-1)x^{p-1}.$$

Or c'est précisément de la considération des sommes $\psi(\mu, \nu)$, définies comme il vient d'être dit, que M. Eisenstein tire sa démonstration.

Pour $x = 1$, $\xi = 0$, il en résultera donc

$$\psi(\mu, 0) + \psi(\mu, 1) + \psi(\mu, 2) + \ldots + \psi(\mu, p-1) = 0.$$

Soient d'ailleurs les congruences

$$a_1 + a_2 + \ldots + a_\mu \equiv K, \quad a_1 \equiv Kb_1, \quad a_2 \equiv Kb_2, \ldots, \quad a_\mu \equiv Kb_\mu \pmod{p},$$

il en résultera, K n'étant pas divisible par p,

$$b_1 + b_2 + \ldots + b_\mu \equiv 1 \pmod{p};$$

et comme

$$\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_\mu}{p}\right) = \left(\frac{K}{p}\right)^\mu \left(\frac{b_1}{p}\right)\left(\frac{b_2}{p}\right)\cdots\left(\frac{b_\mu}{p}\right),$$

on en conclura l'équation

$$\psi(\mu, K) = \left(\frac{K}{p}\right)^\mu \psi(\mu, 1).$$

1°. Soit $\mu = 2\lambda + 1$ ou impair, alors

$$\psi(2\lambda + 1, K) = \left(\frac{K}{p}\right)\psi(2\lambda + 1, 1);$$

de là

$$\psi(2\lambda + 1, 1) + \psi(2\lambda + 1, 2) + \ldots + \psi(2\lambda + 1, p-1) = 0,$$

et, par conséquent,

$$\psi(2\lambda + 1, 0) = 0.$$

2°. Soit $\mu = 2\lambda$ ou pair, alors

$$\psi(2\lambda, K) = \psi(2\lambda, 1);$$

donc

$$\psi(2\lambda, 0) + (p-1)\psi(2\lambda, K) = 0,$$
$$\psi(2\lambda, 0) - \psi(2\lambda, K) = -p\psi(2\lambda, K),$$
$$\psi(2\lambda, 0) - \psi(2\lambda, 1) = -p\psi(2\lambda, 1).$$

Par ce qui précède, on ramène $\psi(\mu, \nu)$ à dépendre de $\psi(\mu, 1)$; on peut aussi faire dépendre $\psi(\mu, \nu)$ de $\psi(\mu - 1, 1)$.

On posera

$$a_1 + a_2 + \ldots + a_{\mu-1} \equiv \nu - a_\mu \pmod{p},$$
$$\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_\mu}{p}\right) = \left(\frac{a_\mu}{p}\right) \times \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_{\mu-1}}{p}\right),$$

et il en résultera

$$\psi(\mu, \nu) = \sum \left(\frac{a_\mu}{p}\right) \psi(\mu - 1, \nu - a_\mu),$$

où il faut donner successivement à a_μ les valeurs $1, 2, \ldots, p-1$.

Pour $\nu = 0$, on a

$$\psi(\mu, 0) = \sum \left(\frac{a_\mu}{p}\right) \psi(\mu - 1, -a_\mu);$$

or pour $\mu = 2\lambda$, on a

$$\psi(\mu - 1, -a_\mu) = \left(\frac{-a_\mu}{p}\right) \psi(\mu - 1, 1),$$

de là

$$\psi(\mu, 0) = \sum \left(\frac{-1}{p}\right)\left(\frac{a_\mu}{p}\right)^2 \psi(\mu - 1, 1),$$

ou bien

$$\psi(\mu, 0) = \left(\frac{-1}{p}\right)(p-1)\psi(\mu - 1, 1),$$

mais, dans ce cas,

$$\psi(\mu, 0) = (1-p)\psi(\mu, 1).$$

On a donc, pour $\mu = 2\lambda$,

$$\psi(\mu, 1) = -\left(\frac{-1}{p}\right)\psi(\mu - 1, 1) = \psi(\mu, \nu).$$

Mais si $\mu = 2\lambda + 1$, on aura

$$\psi(2\lambda+1,\nu) = \left(\frac{\nu}{p}\right)\psi(2\lambda,0) + \begin{Bmatrix}\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\ldots+\left(\frac{\nu-1}{p}\right)\\ +\left(\frac{\nu+1}{p}\right)+\ldots+\left(\frac{p-1}{p}\right)\end{Bmatrix}\psi(2\lambda,1)$$

$$= \left(\frac{\nu}{p}\right)\{\psi(2\lambda,0) - \psi(2\lambda,1)\}$$

$$= -\left(\frac{\nu}{p}\right)p\psi(2\lambda,1).$$

Voici donc le résumé des formules obtenues :

$$\psi(2\lambda+1,0) = 0, \qquad \psi(2\lambda+1,\nu) = -\left(\frac{\nu}{p}\right)p\psi(2\lambda,1),$$

$$\psi(2\lambda,0) = \left(\frac{-1}{p}\right)(p-1)\psi(2\lambda-1,1), \quad \psi(2\lambda,\nu) = -\left(\frac{-1}{p}\right)\psi(2\lambda-1,1)$$

On aura donc, pour $\nu = 1$,

$$\psi(2\lambda+1,1) = -p\psi(2\lambda,1),$$

$$\psi(2\lambda,1) = -\left(\frac{-1}{p}\right)\psi(2\lambda-1,1),$$

$$\psi(2\lambda-1,1) = -p\psi(2\lambda-2,1),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\psi(3,1) = -p\psi(2,1),$$

$$\psi(2,1) = -\left(\frac{-1}{p}\right)\psi(1,1);$$

et comme $\psi(1,1) = 1$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, la multiplication donnera

$$\psi(2\lambda+1,1) = (-1)^{\frac{p-1}{2}\lambda}p^{\lambda}, \qquad \psi(2\lambda+1,\nu) = \left(\frac{\nu}{p}\right)(-1)^{\frac{p-1}{2}\lambda}p^{\lambda},$$

$$\psi(2\lambda+1,0) = 0,$$

$$\psi(2\lambda,1) = \psi(2\lambda,\nu) = -(-1)^{\frac{p-1}{2}\lambda}p^{\lambda-1}, \quad \psi(2\lambda,0) = (-1)^{\frac{p-1}{2}\lambda}(p-1)p^{\lambda-1}.$$

on aura, par exemple,

$$\psi(2,1) = \psi(2,\nu) = -(-1)^{\frac{p-1}{2}}, \qquad \psi(2,0) = (-1)^{\frac{p-1}{2}}(p-1),$$

d'où l'on tirera

$$\xi^2 = (-1)^{\frac{p-1}{2}} p.$$

5. Pour déduire des formules précédentes la loi de réciprocité, on prendra un nombre premier impair q, et l'on aura

$$\psi(q, 1) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} = \sum \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_q}{p}\right),$$

sous la condition

$$a_1 + a_1 + \ldots + a_q \equiv 1 \pmod{p}.$$

Or il y a un terme qui donne

$$a_1 = a_2 = \ldots = a_q,$$

et, par suite,

$$qa_1 \equiv 1 \pmod{p};$$

de là une seule valeur de a_1, telle que $\left(\frac{a_1}{p}\right) = \left(\frac{q}{p}\right)$. La somme $\psi(q, 1)$ contient donc un terme $\left(\frac{a_1}{p}\right)^q = \left(\frac{q}{p}\right)$.

D'ailleurs des nombres $a_1, a_2, \ldots, a_q$, qui ne sont pas tous égaux, donnent, dans le cas de q premier, un nombre d'arrangements multiple de q; on aura donc

$$\sum \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_q}{p}\right) = \left(\frac{q}{p}\right) + \mathrm{M}q,$$

le nombre M étant étant entier. Il suit de là que

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

est divisible par q, et que l'on a, par suite,

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

ce qui est la loi de réciprocité.

III.

6. J'ai montré dans mes Recherches sur les nombres que, étant donnée une formule pour le nombre des solutions de la congruence

$$x_1^2 + x_2^2 + \ldots + x_q^2 \equiv a \pmod{p},$$

on en tirait très-facilement la démonstration de la loi de réciprocité. Voici une rédaction simple et nouvelle de cette démonstration.

Représentons par n_q^a le nombre des solutions de la congruence précédente, ce nombre étant déterminé ainsi qu'il suit. On fera les $(p-1)^q$ arrangements des nombres $1, 2, 3, \ldots, p-1$ pris q à q, le même nombre pouvant être répété. Soit

$$x_1 = a_1, \quad x_2 = a_2, \ldots, \quad x_q = a_q$$

un de ces arrangements; ce sera une solution si l'on a

$$a_1^2 + a_2^2 + \ldots + a_q^2 \equiv a \pmod{p}.$$

Le nombre de solutions ainsi obtenues est celui que l'on représente par n_q^a.

Il faut distinguer trois cas :

1°. $a = 0$, le nombre des solutions est n_q^0.

2°. Soit a un résidu quadratique, on reconnaît de suite que si l'on prend pour a un quelconque des $\frac{p-1}{2}$ résidus quadratiques de p, le nombre de solutions restera le même, ce qui résulte de ce que tous les résidus sont contenus dans la formule ay^2, où a est résidu. On remplacera donc n_q^a par n_q^1 ou n_q.

3°. Si a est un non-résidu quadratique, comme ay^2 sera la formule des non-résidus, n_q^a conservera une même valeur, quel que soit le non-résidu a. Cette valeur sera représentée par n_q'.

De là et de la manière d'obtenir les solutions, on tire l'équation

$$n_q^0 + \frac{p-1}{2}(n_q + n_q') = (p-1)^q.$$

Si l'on voulait admettre o au nombre des valeurs données aux

inconnues, on remplacerait n_q^0, n_q, n_q' par N_q^0, N_q, N_q', et la relation analogue à la précédente serait

$$\mathrm{N}_q^0 + \frac{p-1}{2}(\mathrm{N}_q + \mathrm{N}_q') = p^q,$$

les nombres pris q à q étant ici 0, 1, 2, ..., $p-1$, et, par conséquent, en nombre p.

7. Cela posé, à

$$\xi = \sum \left(\frac{i}{p}\right) x^i = \sqrt{p(-1)^{\frac{p-1}{2}}},$$

ajoutons

$$1 + x + x^2 + \ldots + x^{p-1} = 0,$$

il viendra

$$1 + x^1 + x^4 + \ldots + x^{i^2} + \ldots + x^{(p-1)^2} = \sqrt{p(-1)^{\frac{p-1}{2}}};$$

dans cette équation on a remplacé les exposants par les carrés qui leur sont congrus ou équivalents. Quant au signe du radical, il reste indéterminé; le radical sera représenté par ξ et disparaîtra du résultat final.

L'équation

$$x^1 + x^4 + \ldots + x^{(p-1)^2} = \xi - 1$$

donne, par l'élévation à la puissance q et en vertu des remarques faites plus haut,

$$n_0^q + n_q \Sigma x^a + n_q' \Sigma x^b = (\xi - 1)^q,$$

en représentant par Σx^a la somme des $\frac{p-1}{2}$ termes $x^{a'}$, $x^{a''}$, $x^{a'''}$, ... ayant pour exposants les $\frac{p-1}{2}$ résidus quadratiques, et, de même, par Σx^b la somme des $\frac{p-1}{2}$ termes $x^{b'}$, $x^{b''}$, ..., ayant pour exposants les $\frac{p-1}{2}$ non-résidus quadratiques.

Comme on a

$$\Sigma x^a = \Sigma x^b = \frac{\xi}{\ldots} \quad \text{et} \quad 1 + \Sigma x^a + \Sigma x^b = 0,$$

il en résultera

$$1 + 2\Sigma x^{a} = \xi, \quad 1 + 2\Sigma x^{b} = -\xi;$$

on aura donc

$$(A) \qquad 2n_{q}^{0} - n_{q} - n_{q}' + (n_{q} - n_{q}')\xi = 2(\xi - 1)^{q}.$$

En partant de l'équation

$$1 + x^{1} + x^{2} + \ldots + x^{(p-1)} = \xi,$$

on trouverait tout à fait de la même manière

$$(B) \qquad 2\mathrm{N}_{q}^{0} - \mathrm{N}_{q} - \mathrm{N}_{q}' + (\mathrm{N}_{q} - \mathrm{N}_{q}')\xi = 2\xi^{q}$$

Calcul des nombres N_{q}^{0}, N_{q}, N_{q}'.

1°. Soit $q = 2r$, l'équation (B) devra se partager ainsi :

$$2\mathrm{N}_{q}^{0} - \mathrm{N}_{q} - \mathrm{N}_{q}' = 2\xi^{q}, \quad \mathrm{N}_{q} - \mathrm{N}_{q}' = 0;$$

joignant à ces deux équations celle-ci,

$$\mathrm{N}_{q}^{0} + \frac{p-1}{2}(\mathrm{N}_{q} + \mathrm{N}_{q}') = p^{q},$$

il viendra

$$p\mathrm{N}_{q}^{0} = p^{q} + (p-1)\xi^{q}, \quad \mathrm{N}_{q} = \mathrm{N}_{q}' = \mathrm{N}_{q}^{0} - \xi^{q}$$

ou

$$\xi = \sqrt{(-1)^{\frac{p-1}{2}} p}$$

donne

$$\xi^{q} = (-1)^{\frac{p-1}{2}\cdot\frac{q}{2}} p^{\frac{q}{2}};$$

on a donc

$$\mathrm{N}_{q}^{0} = p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q}{2}}(p-1)p^{\frac{q}{2}-1}, \quad \mathrm{N}_{q} = \mathrm{N}_{q}' = p^{q-1} - (-1)^{\frac{p-1}{2}\cdot\frac{q}{2}} p^{\frac{q}{2}-1}.$$

2°. Soit q impair, l'équation (B) se partagera ainsi :

$$2\mathrm{N}_{q}^{0} - \mathrm{N}_{q} - \mathrm{N}_{q}' = 0, \quad \mathrm{N}_{q} - \mathrm{N}_{q}' = 2\xi^{q-1}$$

D'ailleurs on a

$$\mathrm{N}_{q}^{0} + \frac{p-1}{2}(\mathrm{N}_{q} + \mathrm{N}_{q}') = p^{q};$$

donc

$$N_r^0 = p^{q-1}, \quad N_q = p^{q-1} + \xi^{q-1}, \quad N'_q = p^{q-1} - \xi^{q-1};$$

et comme

$$\xi^{q-1} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}},$$

on aura

$$N_r^0 = p^{q-1}, \quad N_q = p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}}, \quad N'_q = p^{q-1} - (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}}$$

Calcul des nombres n_r^0, n_q, n'_q.

Si q est pair $= 2r$, en posant

$$\xi = \sqrt{p(-1)^{\frac{p-1}{2}}} = \sqrt{pi}, \quad \left[i = (-1)^{\frac{p-1}{2}} \right],$$

le développement $(\xi - 1)^q$ deviendra $(\xi - 1)^q = P - Q\xi$; en posant

$$P = (pi)^r + \frac{q\cdot q-1}{1\cdot 2}(pi)^{r-1} + \ldots + \frac{q\cdot q-1}{1\cdot 2} pi + 1 = 1 + pi.R,$$

$$R = (pi)^{r-1} + \frac{q\cdot q-1}{1\cdot 2}(pi)^{r-2} + \ldots + \frac{q\cdot q-1}{1\cdot 2},$$

$$Q = q(pi)^{r-1} + \frac{q\cdot q-1\cdot q-2}{1\cdot 2\cdot 3}(pi)^{r-2} + \ldots + q,$$

on aura les équations

$$2n_r^0 - (n_q + n'_q) = 2P, \quad n_q - n'_q = -2Q, \quad 2n_q^0 + (p-1)(n_q + n'_q) = 2(p-1)^q,$$

qui donneront

$$n_r^0 = (p-1)\left\{\frac{(p-1)^{q-1}+1}{p} + iR\right\}, \quad n_q = \frac{(p-1)^q - 1}{p} - iR - Q,$$

$$n'_q = \frac{(p-1)^q - 1}{p} - iR + Q.$$

Si q est impair $= 2r + 1$, on aura $(\xi - 1)^q = P\xi - Q$,

$$P = (pi)^r + \frac{q\cdot q-1}{1\cdot 2}(pi)^{r-1} + \ldots + q,$$

$$Q = q(pi)^r + \frac{q\cdot q-1\cdot q-2}{1\cdot 2\cdot 3}(pi)^{r-1} + \ldots + \frac{q\cdot q-1}{1\cdot 2} pi + 1 = 1 + piR,$$

$$R = q(pi)^{r-1} + \frac{q\cdot q-1\cdot q-2}{1\cdot 2\cdot 3}(pi)^{r-2} + \ldots + \frac{q\cdot q-1}{1\cdot 2}$$

On aura, de plus, les équations

$$2n_q^0 - n_q - n_q' = -2Q, \quad n_q - n_q' = 2P, \quad 2n_q^0 + (p-1)(n_q + n_q') = 2(p-1)^q,$$

d'où l'on tire

$$n_q^0 = (p-1)\left\{\frac{(p-1)^{q-1}-1}{p} - iR\right\}, \quad n_q = \frac{(p-1)^q+1}{p} + iR + P,$$

$$n_q' = \frac{(p-1)^q+1}{p} + iR - P.$$

8. Pour tirer des formules précédentes la loi de réciprocité, il faut d'abord remarquer que la congruence

$$x^2 \equiv m \pmod{p}$$

a toujours deux solutions, quand elle est possible : l'une de ces solutions étant $x = z$, l'autre sera $x = p - z$. Il suit de là que les nombres n_q^0, n_q, n_q' sont de la forme

$$2^q S_q^0, \quad 2^q S_q, \quad 2^q S_q',$$

c'est-à-dire multiples de 2^q.

Quand la congruence

$$x_1^2 + x_2^2 + \ldots + x_q^2 \equiv a \pmod{p}$$

est satisfaite par

$$x_1^2 = x_2^2 = \ldots = x_q^2,$$

on a

$$qx_1^2 \equiv a \pmod{p}.$$

Ainsi

$$(qx_1)^2 \equiv aq \pmod{p},$$

aq doit être résidu quadratique de p. Réciproquement, si aq est résidu quadratique, on pourra résoudre

$$qx_1^2 \equiv a \pmod{p},$$

et la congruence sera satisfaite par

$$x_1^2 = x_2^2 = \ldots = x_q^2.$$

Il suit de là que l'on a

$S_q = qQ + 1$ si q est résidu quadratique de p, et

$S_q = qQ$ si q est non-résidu ;

car des nombres $x_1^2, x_2^2, \ldots, x_i^2$ inégaux donnent un nombre de solutions multiple de q, si q est premier.

De même $S'_q = qQ + 1$ si q est non-résidu quadratique de p, et

$$S'_q = qQ \qquad \text{si } q \text{ est résidu quadratique.}$$

D'ailleurs on a

$$n_q \equiv 2S_q, \qquad n'_i \equiv 2S'_q \pmod{q};$$

donc

$$n_q \equiv 1 + \left(\frac{q}{p}\right) \pmod{q},$$

$$n'_q \equiv 1 - \left(\frac{q}{p}\right) \pmod{q}.$$

Pour le cas de q premier impair, l'équation

$$n_q = \frac{(p-1)^q + 1}{p} + iR + P$$

donne

$$n_q \equiv p^{q-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} \pmod{q};$$

d'ailleurs

$$n_q \equiv 1 + \left(\frac{q}{p}\right) \pmod{q},$$

de là

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

ce qui revient à la loi de réciprocité

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

Si l'on voulait employer les valeurs de N_q, il suffirait d'établir la formule

$$N_q = n_q + q n_{q-1} + \frac{q\cdot q-1}{1\cdot 2} n_{q-2} + \ldots + q n_1,$$

d'où

$$n_q = N_q - qN_{q-1} + \frac{q\cdot q-1}{1\cdot 2} N_{q-2} - \ldots \pm qN_1.$$

Pour le cas de q premier, il en résulte

$$\mathrm{N}_q \equiv n_q \pmod{q};$$

ainsi

$$\mathrm{N}_q \equiv 1 + \left(\frac{q}{p}\right).$$

Mais

$$\mathrm{N}_q = q^{p-1} + (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}};$$

la comparaison des deux valeurs de N_q donne, comme plus haut, la loi de Legendre.

Dans mes Recherches sur les nombres, je n'ai donné que les valeurs de

$$\mathrm{N}_q^0, \quad \mathrm{N}_q, \quad \mathrm{N}_q';$$

celles de

$$n_q^0, \quad n_q, \quad n_q',$$

pouvant s'en déduire au moyen de l'équation

$$n_q = \mathrm{N}_q - q\mathrm{N}_{q-1} + \frac{q\cdot q-1}{1\cdot 2}\mathrm{N}_{q-2} + \ldots \pm q\mathrm{N}_1.$$

Le calcul donné plus haut est plus simple.