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

LEJEUNE-DIRICHLET

Sur la première démonstration donnée par Gauss de la loi de réciprocité dans la théorie des résidus quadratiques

Journal de mathématiques pures et appliquées 2^e série, tome 4 (1859), p. 401-420.
<http://www.numdam.org/item?id=JMPA_1859_2_4__401_0>

SUR

LA PREMIÈRE DÉMONSTRATION DONNÉE PAR GAUSS DE LA LOI DE RÉCIPROCITÉ DANS LA THÉORIE DES RÉSIDUS QUADRATIQUES;

PAR M. LEJEUNE-DIRICHLET.

JOURNAL DE CRELLE, TOME XLVII. — TRADUCTION DE M. HOÜEL.

Parmi les nombreuses démonstrations du théorème fondamental de la théorie des congruences du second degré, la plus ancienne, découverte par Gauss dans l'année 1796, et publiée dans les *Disquisitiones Arithmeticæ*, section IV, m'a toujours paru digne d'une attention particulière, tant à cause de la simplicité de l'idée qui lui sert de base, que parce que cette démonstration est la seule, que je sache, où l'on emprunte toutes les considérations à la doctrine des congruences du second degré, à laquelle appartient essentiellement ce théorème; tandis que les principes fondamentaux des autres démonstrations semblent être plus ou moins étrangers à cette doctrine [*]. D'ailleurs si cette belle démonstration laisse à désirer sous le rapport de la brièveté, par laquelle quelques-unes des démonstrations plus récentes se font remarquer à un si haut degré, cette imperfection n'est pas dans l'essence de la méthode: elle a bien plutôt sa source dans cette circonstance accidentelle que, pour représenter certaines relations qui reviennent à chaque instant dans cette manière de procéder, on n'a employé aucun signe approprié au calcul,

[*] Voici le jugement que Gauss lui-même porte de sa première démonstration, dans un Mémoire postérieur (*Comment. Soc. Gott.*, t. XVI, p. 70): Sed omnes hæ demonstrationes, etiamsi respectu rigoris nihil desiderandum relinquere videantur, e principiis nimis heterogeneis derivatæ sunt, prima forsan excepta, quæ tamen per ratiocinia magis laboriosa procedit, operationibusque prolixioribus premitur.

ce qui a mis dans la nécessité de distinguer huit cas différents, dont chacun se partage encore en plusieurs subdivisions. En introduisant le signe dont Legendre a le premier fait usage, avec la signification plus générale que Jacobi lui a donnée depuis, et faisant quelques autres simplifications qui n'altèrent pas sensiblement le fond de la démonstration, celle-ci se trouve réduite à tel point, qu'elle ne semble guère le céder pour la brièveté à aucune des autres, si toutefois on n'oublie pas de remarquer qu'une partie des développements qu'elle contient sont encore indispensables pour la théorie des résidus quadratiques, lors même qu'on choisit un autre mode de démonstration pour la loi de réciprocité. J'ai cru devoir consacrer quelques pages à une nouvelle exposition de ce sujet, simplifiée comme je viens de l'indiquer, d'autant plus que l'expérience m'a toujours fait voir combien la multiplicité des cas différents rendait difficile aux commençants l'intelligence de l'ancienne démonstration.

§ I.

Dans ce premier paragraphe, nous allons exposer quelques propositions élémentaires et quelques définitions, indispensables pour ce qui doit suivre.

Suivant que la congruence

$$x^2 \equiv k \,(\text{mod. } m)$$

(k désignant un nombre entier positif ou négatif) est ou n'est pas possible, k est dit un *résidu* ou un *non-résidu* quadratique du module m, dont le signe est naturellement indifférent. Il est permis, pour le but que nous nous proposons, de supposer toujours k et m sans diviseur commun. Dans le cas particulièrement important où m est un nombre premier impair p, le signe $\left(\frac{k}{p}\right)$ désignera l'unité positive ou négative, suivant que k sera un résidu ou un non-résidu quadratique de p.

La proposition connue, que le produit $k'\,k''\ldots$ est un résidu ou un non-résidu quadratique de p, selon que ceux des facteurs k', k'',... qui sont non-résidus quadratiques de p, se trouvent en nombre pair ou en

nombre impair, sera exprimée, à l'aide de notre notation, par l'équation

$$\left(\frac{k'\,k''\ldots}{p}\right) = \left(\frac{k'}{p}\right)\left(\frac{k''}{p}\right)\ldots.$$

Pour la possibilité de la congruence

$$x^2 \equiv k \,(\text{mod. } p^{\varpi}),$$

ϖ étant > 1, il faut évidemment que l'on ait la condition

$$\left(\frac{k}{p}\right) = 1,$$

et il est facile aussi de démontrer que, dès que cette condition est remplie, la congruence est résoluble pour toute valeur de ϖ. Il en est autrement de la congruence

$$x^2 \equiv k \,(\text{mod. } 2^{\varpi}).$$

Pour $\varpi = 1$, le nombre impair k n'a aucune condition à remplir; au contraire, pour $\varpi = 2$, et pour $\varpi \geqq 3$, les conditions nécessaires et suffisantes pour la résolubilité de la congruence sont que k ait, dans le premier cas, la forme $4\mu + 1$, dans le second, la forme $8\mu + 1$. Si le module, dans notre congruence, est le produit de puissances de différents nombres premiers, il faut et il suffit, pour que la congruence soit possible, qu'elle soit résoluble pour chacune des puissances de nombres premiers.

Nous allons maintenant donner une signification plus générale à la notation $\left(\frac{k}{p}\right)$, définie jusqu'ici pour le cas où p est un nombre premier impair, ne divisant pas le nombre positif ou négatif k; et en supposant que le nombre impair m, dont le signe est indifférent, n'ait avec k aucun diviseur commun, et soit décomposé dans ses facteurs premiers égaux ou inégaux p', p'', p''',..., de sorte qu'on ait

$$m = p'\,p''\,p'''\ldots,$$

nous désignerons par la notation $\left(\frac{k}{m}\right)$ le produit

$$\left(\frac{k}{p'}\right)\left(\frac{k}{p''}\right)\left(\frac{k}{p'''}\right)\cdots$$

Il est aisé de voir que, dans un pareil symbole, on peut remplacer k par un nombre congru avec k suivant le module m, et que, pour ces symboles, on a les deux équations

$$\left(\frac{k}{m}\right)\left(\frac{l}{m}\right)=\left(\frac{kl}{m}\right),\quad \left(\frac{k}{m}\right)\left(\frac{k}{n}\right)=\left(\frac{k}{mn}\right).$$

Mais il ne faut pas oublier que $\left(\frac{k}{m}\right)$ n'a plus avec la congruence

$$x^2\equiv k\,(\text{mod. } m)$$

le même rapport que tout à l'heure, lorsque m était un nombre premier. Si la congruence est résoluble, il s'ensuit bien encore que $\left(\frac{k}{m}\right)=1$, parce qu'alors, d'après ce qui précède, tous les facteurs dont le produit a été désigné par $\left(\frac{k}{m}\right)$ sont égaux à l'unité positive; mais il est évident qu'on ne peut pas, de la condition $\left(\frac{k}{m}\right)=1$, conclure réciproquement la possibilité de la congruence.

Enfin, nous ferons remarquer encore que, m étant toujours supposé impair, de la possibilité de la congruence

$$lx^2\equiv k\,(\text{mod. } m),$$

k et l étant des nombres premiers avec m, résulte l'équation

$$\left(\frac{kl}{m}\right)=1,$$

comme on peut le voir immédiatement, en mettant la congruence sous la forme

$$(lx)^2\equiv kl.$$

§ II.

Passons maintenant à l'objet spécial de ce Mémoire, aux critériums qui servent à distinguer, pour un nombre donné k, positif ou négatif, les modules simples impairs p dont k est résidu quadratique, de ceux dont k est non-résidu. Le caractère distinctif demandé ramenant, d'après la proposition que nous venons de rappeler, à la considération des caractères analogues relatifs aux facteurs premiers de k, nous n'avons que trois cas à examiner, suivant que k est l'un des nombres -1, 2, ou qu'il est égal à un nombre premier impair positif q. Pour ces trois cas, les critériums cherchés sont contenus dans les équations suivantes, où le nombre premier impair p est positif comme q et différent de q :

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

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

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

D'après la première de ces équations, $\left(\frac{-1}{p}\right)$ est égal à $+1$ ou à -1, suivant que p est de la forme $4\mu+1$ ou de la forme $4\mu+3$. D'après la seconde, on a

$$\left(\frac{2}{p}\right) = 1, \qquad \text{pour} \quad p = 8\mu + 1, 7,$$

et, au contraire,

$$\left(\frac{2}{p}\right) = -1, \quad \text{pour} \quad p = 8\mu + 3, 5;$$

et, d'après la troisième, on a toujours

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

excepté lorsque les nombres premiers p, q sont tous les deux de la forme $4\mu + 3$, auquel cas on a

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Les équations (a) et (b) sont faciles à démontrer pour certains cas particuliers. Tel est, pour la première, le cas où p est de la forme $4\mu + 3$, et où, par suite, $\left(\frac{-1}{p}\right)$ doit être égal à -1. Si cette propriété n'avait pas lieu pour tous les nombres premiers $4\mu + 3$, soit p le plus petit de ceux pour lesquels $\left(\frac{-1}{p}\right) = 1$. On peut alors poser $e^2 + 1 = ph$, et si, comme cela est toujours possible, on choisit $e < p$ et en même temps pair, on aura aussi $h < p$ et de la forme $4\mu + 3$. Le nombre h a donc un facteur premier $r < p$, de même forme $4\mu + 3$, pour lequel on a, d'après l'équation,

$$\left(\frac{-1}{r}\right) = 1,$$

ce qui est contraire à notre hypothèse.

En second lieu, pour démontrer que l'on a toujours $\left(\frac{2}{p}\right) = -1$, lorsque p est de l'une des formes $8\mu + 3, 5$, admettons qu'il y ait des nombres premiers de l'une de ces formes, pour lesquels la proposition n'ait point lieu, et désignons le plus petit de ces nombres par p. On peut alors poser

$$e^2 - 2 = ph,$$

et en prenant e impair et en même temps $< p$, il arrivera, à cause de

$$e^2 - 2 = 8\mu + 7,$$

que la valeur de h, correspondante à la forme $8\mu + 3$ ou 5 de p, sera de la forme $8\mu + 5$ ou 3, et de plus $< p$. Or, comme des facteurs premiers, qui seraient tous contenus dans l'une des formes $8\mu + 1, 7$, ne peuvent donner pour produit un nombre $8\mu + 3, 5$, il existe donc un facteur premier r de h, qui est de la forme $8\mu + 3, 5$, et pour le-

quel, d'après l'équation précédente, on aurait, contrairement à notre hypothèse, $\left(\frac{2}{r}\right) = 1$.

La démonstration de l'équation $\left(\frac{-2}{p}\right) = -1$, lorsque p est de l'une des formes $8\mu + 5, 7$, se faisant absolument de la même manière, nous l'omettrons pour abréger. En mettant ce dernier résultat, pour le cas de $p = 8\mu + 7$, sous la forme

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

et remarquant que, d'après ce que nous avons vu, $\left(\frac{-1}{p}\right) = -1$, puisque la forme $8\mu + 7$ est un cas particulier de la forme $4\mu + 3$, il vient, pour les nombres premiers $p = 8\mu + 7$,

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

de sorte que maintenant la proposition (b) est démontrée pour tous les nombres premiers qui ne sont pas de la forme $8\mu + 1$.

§ III.

Avant de pouvoir entreprendre la démonstration générale des propositions énoncées dans le paragraphe précédent, nous allons tirer de ces équations, supposées exactes, quelques conséquences, que nous ferons précéder de la remarque suivante.

Étant donné un produit

$$R = \Pi r$$

de facteurs impairs r, pour déterminer son résidu relatif au diviseur 4, si l'on met chaque facteur sous la forme $(r - 1) + 1$, on peut, dans la multiplication, négliger tous les termes dans lesquels les premières parties de ces binômes sont multipliées entre elles. On a ainsi

$$R \equiv 1 + \sum (r - 1) \pmod 4;$$

en d'autres termes, $\frac{1}{2}(R-1)$ et $\sum\frac{1}{2}(r-1)$ sont de *même espèce*, c'est-à-dire, ou tous deux pairs, ou tous deux impairs.

Pareillement, de l'équation

$$R^2 = \Pi r^2,$$

tout carré impair r^2 étant de la forme $8\mu + 1$, il résulte

$$R^2 \equiv 1 + \sum (r^2 - 1) \pmod{64},$$

d'où l'on conclut encore que les nombres $\frac{1}{8}(R^2-1)$ et $\sum\frac{1}{8}(r^2-1)$ sont de même espèce.

Au moyen de cette remarque, il est maintenant facile de déduire des équations ci-dessus les équations suivantes, plus générales et de même forme, dans lesquelles P et Q désignent deux nombres positifs impairs quelconques, n'ayant entre eux aucun diviseur commun :

$$(a') \qquad \left(\frac{-1}{P}\right) = (-1)^{\frac{1}{2}(P-1)},$$

$$(b') \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{1}{8}(P^2-1)},$$

$$(c') \qquad \left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(Q-1)}.$$

Posons $P = \Pi p$, p désignant chacun des facteurs premiers, égaux ou inégaux, de P; appliquons à chaque facteur p la proposition (a), et multiplions entre elles toutes les équations ainsi obtenues; il vient alors

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

résultat qui se change dans l'équation (a'), en remplaçant l'exposant par le nombre de même espèce $\frac{1}{2}(P-1)$. On mettrait de même en évidence l'exactitude de la proposition (b'). Pour démontrer l'équation

(c'), décomposons aussi Q en ses facteurs simples q. Le premier membre peut alors être considéré comme un produit d'expressions de la forme $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$, chaque nombre p devant être combiné successivement avec chaque nombre q. En remplaçant chacune de ces expressions par sa valeur donnée par l'équation (c), il vient

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

le signe de sommation se rapportant à toutes les combinaisons p, q. La somme est par conséquent le produit des facteurs $\sum \frac{1}{2}(p-1)$ et $\sum \frac{1}{2}(q-1)$, auxquels on peut substituer les nombres respectivement de même espèce $\frac{1}{2}(P-1)$ et $\frac{1}{2}(Q-1)$, et l'on a ainsi l'équation (c').

En multipliant entre elles les équations (a') et (c'), on a

$$\left(\frac{-Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(Q+1)},$$

ou

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

On voit donc que l'équation (c') subsiste encore lorsqu'on l'applique au nombre positif P et au nombre négatif $-Q$, et qu'elle est, pour ce cas, une conséquence de l'équation (a') et de l'équation primitive (c'). De même celle-ci est évidemment une conséquence de (a') et de l'équation (c') appliquée à la combinaison P, $-Q$, et cette même remarque s'applique naturellement aussi aux équations (a) et (c), qui sont contenues comme cas particuliers dans celles dont nous nous occupons.

§ IV.

Actuellement, pour démontrer généralement les propositions (a) et (c), partons de la supposition qu'elles sont vraies l'une et l'autre jusqu'à un certain nombre premier positif impair q exclusivement, c'est-à-dire

que la première est vraie pour tout nombre premier positif, impair et $< q$, et que la seconde est vraie pour deux pareils nombres premiers. Si l'on déduit de cette supposition que l'équation (a) est vraie pour q, et l'équation (c) pour toute combinaison p, q, pourvu seulement que le nombre premier positif impair p soit moindre que q, les deux propositions, qui sont évidemment vraies pour les plus petits nombres premiers, seront alors rendues générales.

Il est aisé de voir que la démonstration qu'il s'agit de donner se réduit à prouver les deux points suivants :

Premièrement, il faut faire voir que si, en prenant $\varpi = \pm p$ avec un signe convenable, on a $\left(\frac{\varpi}{q}\right) = 1$, l'équation (c), appliquée à la combinaison q, ϖ, donnera

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

En second lieu, si q est de la forme $4\mu + 1$, et que l'on ait

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

il faut en déduire

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

et faire voir en même temps que ce second cas a lieu pour toute valeur de q de la forme $4\mu + 1$, c'est-à-dire que, parmi les nombres premiers p, plus petits que q, il y en a toujours au moins un qui est non-résidu quadratique de q.

En effet, si q est de la forme $4\mu + 3$, l'équation (a) est déjà démontrée pour q, et, par conséquent, d'après ce qui a été remarqué à la fin du paragraphe précédent, il est indifférent pour laquelle des deux combinaisons p, q, ou $-p$, q, on démontrera l'exactitude de l'équation (c). Mais de $\left(\frac{-1}{q}\right) = -1$, il résulte $\left(\frac{-p}{q}\right) = -\left(\frac{p}{q}\right)$, c'est-à-dire qu'il y a toujours une de ces combinaisons comprise dans le premier cas.

Si, au contraire, q est de la forme $4\mu + 1$, alors, de la supposition

$\left(\frac{p}{q}\right) = 1$, il résulte, d'après le premier cas (en posant $\varpi = p$),

$$\left(\frac{q}{p}\right) = 1;$$

et de la supposition $\left(\frac{p}{q}\right) = -1$, il résulte, d'après le second cas,

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

comme cela devait être. L'équation

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

se démontre comme il suit. Pour un nombre premier p, appartenant au second cas, on a

$$\left(\frac{p}{q}\right) = -1, \quad \left(\frac{q}{p}\right) = -1.$$

Si l'on avait maintenant

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

et, par suite,

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

il en résulterait, d'après le premier cas,

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

résultat contradictoire avec celui que l'on déduit du second cas.

Avant de passer à la démonstration des deux points que nous venons d'indiquer, il faut remarquer que la supposition faite au commencement du présent paragraphe entraîne évidemment, d'après la manière dont les équations (a'), (c') se déduisent des équations (a), (c) [paragraphe précédent], l'exactitude de l'équation (c') pour deux nombres impairs quelconques premiers entre eux, pourvu qu'ils ne soient pas tous les deux négatifs, et que leurs facteurs premiers soient tous moindres que q.

§ V.

En vertu de l'équation

$$\left(\frac{\varpi}{q}\right) = 1,$$

qui a lieu dans le premier cas, on peut poser

$$e^2 - \varpi = qf.$$

Si l'on suppose dans cette équation, comme on peut toujours le faire, e pair et en même temps $< q$, alors f sera impair, positif [*] (puisque la valeur numérique p de ϖ est moindre que q), et aussi $< q$. Notre équation devra maintenant être traitée différemment, suivant que f sera ou ne sera pas divisible par ϖ.

1. Si f n'est pas divisible par ϖ, on a, d'après le § I,

$$\left(\frac{\varpi}{f}\right) = 1, \quad \left(\frac{qf}{\varpi}\right) = \left(\frac{q}{\varpi}\right)\left(\frac{f}{\varpi}\right) = 1,$$

d'où l'on tire par multiplication, en appliquant l'équation (c') à la combinaison f, ϖ,

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

D'ailleurs il résulte de l'équation précédente que $\frac{1}{2}(f-1)$ et $\frac{1}{2}(q-1)+\frac{1}{2}(\varpi+1)$ sont des nombres de même espèce. En substituant donc, dans les exposants, le second nombre au premier, et supprimant $\frac{1}{4}(\varpi^2-1)$ comme nombre pair, on a, comme cela devait

---

[*] Dans ce qui va suivre, nous désignerons par les caractères italiques des nombres essentiellement positifs, et au contraire par les lettres grecques des nombres qui pourront être positifs ou négatifs.

être,

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

II. Si f contient le facteur ϖ, posons

$$e = \varpi\varepsilon, \quad f = \varpi\varphi,$$

de sorte que ε et φ sont de même signe. De l'équation résultante

$$\varpi\varepsilon^2 - 1 = q\varphi$$

il suit alors que l'on a

$$\left(\frac{\varpi}{\varphi}\right) = 1, \quad \left(\frac{-q\varphi}{\varpi}\right) = \left(\frac{q}{\varpi}\right)\left(\frac{-\varphi}{\varpi}\right) = 1,$$

d'où l'on tire, par multiplication, en appliquant l'équation (c') aux nombres ϖ, $-\varphi$, dont un seul est négatif,

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

ou, puisque $\frac{1}{2}(q-1)$ et $\frac{1}{2}(\varphi+1)$ sont évidemment de même espèce,

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

§ VI.

La supposition relative au second cas

$$\left(\frac{p}{q}\right) = -1, \quad q = 4\mu + 1$$

ne permet pas, comme dans le premier cas, d'établir immédiatement une équation. Il faut démontrer préalablement l'existence d'un nombre premier auxiliaire $p' < q$, satisfaisant à la condition

$$\left(\frac{q}{p'}\right) = -1.$$

Si q est de la forme $8\mu + 5$, cette démonstration ne présente aucune difficulté; car $q - 2$ est alors de la forme $8\mu + 3$, et a par conséquent un facteur premier $p' < q$ de l'une des formes $8\mu + 3, 5$, et pour lequel on a

$$q \equiv 2 \pmod{p'},$$

et partant

$$\left(\frac{q}{p'}\right) = \left(\frac{2}{p'}\right),$$

ou, d'après le § II,

$$\left(\frac{q}{p'}\right) = -1.$$

L'existence de p' n'est pas aussi facile à démontrer lorsque q est de la forme $8\mu + 1$. C'est la nécessité d'étendre aussi la démonstration à ce cas qui constituait peut-être la plus grande difficulté que Gauss ait eu à surmonter dans sa première manière d'établir la loi de réciprocité. Il y est parvenu par une considération où il a fait preuve d'une rare sagacité, et qui revient au fond à la suivante.

Soit $2m + 1 < q$, et supposons que q soit résidu quadratique de tous les nombres premiers impairs qui ne surpassent pas $2m + 1$. D'après le § I, et à cause de $q = 8\mu + 1$, la congruence $x^2 \equiv q$ est alors résoluble pour tout module qui, outre une puissance quelconque de 2, contient seulement des facteurs premiers impairs ne surpassant pas $2m + 1$. Or cette condition est remplie par le produit

$$1.2.3\ldots(2m+1) = \mathrm{M},$$

et l'on peut dès lors poser

$$k^2 \equiv q \pmod{\mathrm{M}},$$

où nous prendrons k positif. On a donc

$$(q-1^2)(q-2^2)\ldots(q-m^2) \equiv (k^2-1^2)(k^2-2^2)\ldots(k^2-m^2) \pmod{\mathrm{M}}.$$

Maintenant le second membre, si on le multiplie par le facteur k, qui est premier avec M, peut s'écrire sous forme de produit continu,

$$(k+m)(k+m-1)\ldots(k-m),$$

lequel produit est un multiple de M, comme on peut le faire voir par des considérations purement arithmétiques, et comme cela résulte aussi de ce que ce nombre, divisé par M, représente un nombre de combinaisons. Il faut donc que le premier membre de l'équation soit aussi divible par M. En donnant au quotient de cette division la forme

$$\frac{1}{m+1}\cdot\frac{q-1^2}{(m+1)^2-1^2}\cdot\frac{q-2^2}{(m+1)^2-2^2}\cdots\frac{q-m^2}{(m+1)^2-m^2},$$

il se manifeste évidemment une contradiction, si l'on choisit pour m le nombre entier immédiatement inférieur à $\sqrt{q}$, parce qu'alors le quotient est un produit de fractions moindres que l'unité. On a ici supposé tacitement que ce choix du nombre m est conforme à la condition $2m+1<q$, qui sert de base à notre raisonnement, ce qui est en effet le cas, puisque

$$2m+1<2\sqrt{q}+1,$$

et qu'évidemment, pour tous les nombres premiers $8\mu+1$, dont le plus petit est 17, on a

$$2\sqrt{q}+1<q.$$

Il est donc démontré qu'il existe toujours un nombre premier $p'<2m+1<q$, et tel qu'on ait

$$\left(\frac{q}{p'}\right)=-1.$$

Remarquons encore que, pour notre nombre premier auxiliaire p', on a

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

car de la supposition

$$\left(\frac{p'}{q}\right)=1,$$

il résulterait, d'après le paragraphe précédent,

$$\left(\frac{q}{p'}\right)=1.$$

En nous occupant maintenant de démontrer que de l'équation

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

(q étant égal à $4\mu + 1$), il résulte toujours

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

nous pouvons considérer p comme différent du nombre premier auxiliaire p', puisque l'on a déjà établi pour celui-ci la simultanéité des équations

$$\left(\frac{p'}{q}\right) = -1, \quad \left(\frac{q}{p'}\right) = -1,$$

à l'aide desquelles nous pourrons représenter notre hypothèse par l'équation

$$\left(\frac{pp'}{q}\right) = 1,$$

et la conséquence qui en doit résulter par

$$\left(\frac{q}{pp'}\right) = 1.$$

D'après la première de ces équations, on peut donc poser

$$e^2 - pp' = q\varphi,$$

e devant être pair et $< q$. Alors φ sera impair, et à cause de $p < q$, $p' < q$, φ sera numériquement moindre que q.

Il y a maintenant trois cas à distinguer : ou φ n'est divisible par aucun des nombres premiers p, p', ou il l'est par un seul, ou enfin il l'est par tous les deux. Comme l'équation précédente et l'équation

$$\left(\frac{q}{pp'}\right) = 1,$$

qu'il s'agit d'en déduire, sont symétriques par rapport à p et à p', le second cas se traitera de la même manière, que ce soit p ou p' que l'on considère comme facteur de φ.

I. Si φ n'est divisible ni par p ni par p', de notre équation il résulte

$$\left(\frac{pp'}{\varphi}\right) = 1, \quad \left(\frac{q\varphi}{pp'}\right) = \left(\frac{q}{pp'}\right)\left(\frac{\varphi}{pp'}\right) = 1,$$

d'où, en multipliant et appliquant la formule (c'),

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

Mais d'après l'équation ci-dessus, dans laquelle $q = 4\mu + 1$, les nombres $\frac{1}{2}(pp'-1)$, $\frac{1}{2}(\varphi-1)$ ne sont pas de même espèce, c'est-à-dire que l'un d'eux est pair; donc on a

$$\left(\frac{q}{pp'}\right) = 1.$$

II. A cause de la symétrie que nous avons déjà remarquée, nous pouvons considérer p' comme étant le diviseur de φ. En posant

$$\varphi = p'\psi, \quad e = p'g,$$

notre équation se change en

$$p'g^2 - p = q\psi,$$

ψ n'étant divisible ni par p ni par p'. De cette dernière équation, on tire

$$\left(\frac{pp'}{\psi}\right) = 1, \quad \left(\frac{p'q\psi}{p}\right) = 1, \quad \left(\frac{-pq\psi}{p'}\right) = 1,$$

d'où, en multipliant,

$$\left(\frac{q}{pp'}\right) = \left(\frac{pp'}{\psi}\right)\left(\frac{\psi}{pp'}\right)\left(\frac{p'}{p}\right)\left(\frac{-p}{p'}\right),$$

ou, en appliquant l'équation (c') aux deux combinaisons pp', ψ et p', $-p$,

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

En remplaçant $\frac{1}{2}(\psi-1)$ par le nombre $\frac{1}{2}(p+1)$ qui, d'après une

équation précédente, est de même espèce que $\frac{1}{2}(\psi - 1)$, et $\frac{1}{2}(pp' - 1)$ par $\frac{1}{2}(p - 1) + \frac{1}{2}(p' - 1)$, l'exposant prend la valeur

$$\frac{1}{2}(p + 1)(p' - 1) + \frac{1}{4}(p^2 - 1),$$

qui est évidemment paire. Donc on a

$$\left(\frac{q}{pp'}\right) = 1.$$

III. En posant, dans le troisième cas,

$$\varphi = pp'\psi, \quad e = pp'g,$$

il vient

$$pp'g^2 - 1 = q\psi,$$

d'où résulte

$$\left(\frac{pp'}{\psi}\right) = 1, \quad \left(\frac{-q\psi}{pp'}\right) = \left(\frac{q}{pp'}\right)\left(\frac{-\psi}{pp'}\right) = 1,$$

et par suite

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)}.$$

Or $\frac{1}{2}(\psi + 1)$ étant évidemment pair, il vient finalement

$$\left(\frac{q}{pp'}\right) = 1.$$

Les équations (a) et (c), ainsi que les équations (a') et (c') qui s'en déduisent, sont donc généralement démontrées.

§ VII.

Il reste encore maintenant à s'occuper du cas de la proposition (b) relatif aux nombres premiers de la forme $8\mu + 1$, et qui nous restait encore à démontrer. Désignons par q un nombre premier quelconque de cette forme, et admettons que la proposition soit vraie pour tous les nombres premiers de cette même forme et $< q$, ou, ce qui revient absolument au même d'après ce qui a été démontré au § II, qu'elle soit vraie pour tous les nombres premiers $< q$. Si de cette hypothèse

ou peut déduire l'équation

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

la proposition sera vraie alors sans restriction. Nous allons maintenant prouver l'exactitude de cette dernière équation, en faisant voir que l'hypothèse de $\left(\frac{2}{q}\right) = -1$ conduit à une contradiction.

Choisissons un nombre premier $p < q$ et tel, que l'on ait

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

On aura, d'après l'hypothèse que nous venons de faire,

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

et l'on peut poser par conséquent

$$e^2 - 2p = q\varphi,$$

où, en supposant e impair et $< q$, φ sera pareillement impair et $< q$, abstraction faite du signe. Il faut maintenant distinguer deux cas, selon que φ n'est pas divisible ou qu'il est divisible par p.

I. Dans le premier cas, on a immédiatement

$$\left(\frac{2p}{q\varphi}\right) = \left(\frac{2}{q}\right)\left(\frac{2}{\varphi}\right)\left(\frac{p}{q\varphi}\right) = 1, \quad \left(\frac{q\varphi}{p}\right) = 1,$$

et, par suite,

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

Or l'équation (b'), dans laquelle le signe de P est indifférent, et qui est une conséquence de l'équation (b), est évidemment applicable au nombre φ, dont tous les facteurs premiers satisfont à l'équation (b). Comme on a, d'après cela,

$$\left(\frac{2}{\varphi}\right) = (-1)^{\frac{1}{8}(\varphi^2-1)},$$

on peut donner à la dernière équation la forme

$$-1 = (-1)^{\frac{1}{8}[2(p-1)(q\varphi-1)+\varphi^2-1]}.$$

L'expression entre crochets variera évidemment d'un multiple de 16, si l'on y remplace $q\varphi - 1$ et φ par d'autres nombres congrus avec eux suivant le module 8. Mais, à cause de

$$e^2 \equiv 1, \quad q \equiv 1 \pmod 8,$$

il résulte immédiatement, d'une équation précédente, qu'on a

$$q\varphi - 1 \equiv -2p, \quad \varphi \equiv 1 - 2p \pmod 8,$$

de sorte que notre expression

$$\equiv -4p(p-1) + (1-2p)^2 - 1 = 0 \pmod{16},$$

et par conséquent le second membre de l'équation ci-dessus est égal à l'unité positive et est différent du premier membre.

II. Si φ est divisible par p, posons

$$\varphi = p\psi, \quad e = pg, \quad \text{d'où} \quad pg^2 - 2 = q\psi.$$

En vertu de cette dernière équation, on a

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

d'où, comme dans le cas précédent,

$$-1 = (-1)^{\frac{1}{8}[2(p-1)(q\psi+1)+p^2+\psi^2-2]}.$$

En remplaçant maintenant les nombres $q\psi + 1$ et ψ par les nombres $p - 1$ et $p - 2$, qui, d'après une équation précédente, leur sont congrus suivant le module 8, on voit que l'expression entre crochets

$$\equiv 2(p-1)^2 + p^2 + (p-2)^2 - 2 = 4(p-1)^2 \equiv 0 \pmod{16},$$

ce qui conduit encore à la même contradiction.