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

PEPIN

Sur un théorème de Legendre

Journal de mathématiques pures et appliquées 3^e série, tome 5 (1879), p. 21-30.
<http://www.numdam.org/item?id=JMPA_1879_3_5__21_0>

Sur un théorème de Legendre;

PAR LE P. PEPIN, S. J.

---

1. Je me propose de compléter la démonstration du théorème par lequel commence le § III de la troisième Partie de la *Théorie des nombres* de Legendre, et dont voici l'énoncé :

Si c est premier ou double d'un nombre premier, deux formes trinaires différentes de c ne pourront répondre à un même diviseur trinaire de la formule $t^2 + cu^2$.

Commençons par résumer rapidement la démonstration de Legendre, afin d'en remarquer le point faible. Nous supposons que les deux formes trinaires

$$c = F^2 + \theta^2(G^2 + H^2), \quad c = F'^2 + \theta'^2(G'^2 + H'^2)$$

correspondent à un même diviseur trinaire Δ et que les deux nombres G, H soient premiers entre eux, ainsi que les deux nombres G', H'; puis, pour abréger, nous faisons

$$G^2 + H^2 = \pi, \quad G'^2 + H'^2 = \pi'.$$

Chacun des deux nombres π, π' sera représenté par le diviseur Δ, de sorte que leur produit $\pi\pi'$ sera représenté par la forme principale. On pourra donc vérifier l'équation

$$\pi\pi' = y^2 + cz^2, \tag{1}$$

sans supposer $z = 0$, tant que l'on n'aura pas $\pi = \pi'$; car, si $\pi = \pi'$,

il peut arriver que l'équation (1) n'admette pas d'autre solution que la solution évidente $y = \pm\pi$, $z = 0$.

En multipliant l'équation (1) par $\theta^2\theta'^2$, et en remplaçant $\theta^2\pi$, $\theta'^2\pi'$ par leurs valeurs $c - F^2$, $c - F'^2$, on obtient l'équation

$$(c - F^2)(c - F'^2) = \theta^2\theta'^2 y^2 + c\theta^2\theta'^2 z^2;$$

d'où l'on déduit que la différence $F^2F'^2 - \theta^2\theta'^2 y^2$ est divisible par c.

Considérant alors que c ou $\frac{1}{2}c$ est premier, et que les deux facteurs $FF' + \theta\theta' y$, $FF' - \theta\theta' y$ sont de même parité, nous concluons que l'un de ces facteurs est divisible par c, et nous posons $FF' - \theta\theta' y = cu$. L'élimination de y entre cette équation et la précédente donne

$$(2) \qquad c - F'^2 = (F - F'u)^2 + (c - F'^2)u^2 + z^2\theta^2\theta'^2.$$

Si z est différent de zéro, cette équation est impossible, à moins que l'on ne fasse $u = 0$. Mais, si z est nécessairement nul, comme cela arrive lorsque, π et π' étant égaux, leur valeur commune est inférieure à $\frac{1}{2}c$, on peut vérifier l'équation (2) en faisant $u = 1$, pourvu que les deux carrés F^2, F'^2 soient égaux, ainsi que θ^2 et θ'^2. Ainsi il est un cas qui échappe au raisonnement de Legendre : c'est celui où les deux formes trinaires considérées sont

$$(3) \qquad c = F^2 + \theta^2(G^2 + H^2), \quad c = F^2 + \theta^2(G'^2 + H'^2),$$

$G^2 + H^2$, $G'^2 + H'^2$ étant deux décompositions d'un même nombre π en une somme de deux carrés premiers entre eux.

Supposons θ pair et F impair. Le raisonnement de Legendre exige que l'on prenne pour F^2 et F'^2 les deux carrés impairs des deux formes trinaires; ici ces deux carrés sont égaux, ainsi que les deux nombres π et π'; et, comme π est inférieur à $\frac{1}{4}c$, on ne peut vérifier l'équation (1) qu'en faisant $y = \pi$ et $z = 0$. L'équation (2) se réduit à une identité, de sorte qu'on ne peut plus en déduire la formule

$$c = F^2 + F'^2 + \theta^2\theta'^2 z^2,$$

nécessaire pour la démonstration.

2. Il reste donc à démontrer le théorème de Legendre, dans le cas où les formes trinaires de c sont données par les formules (3).

Pour faire cette démonstration, nous chercherons d'abord les conditions nécessaires pour que les deux formes trinaires

$$(4)\quad \begin{cases} \Delta = (mx + ny)^2 + (m'x + n'y)^2 + (m''x + n''y)^2, \\ \Delta = (m_1 x + n_1 y)^2 + (m'_1 x + n'_1 y)^2 + (m''_1 x + n''_1 y)^2 \end{cases}$$

d'un même diviseur quadratique

$$\Delta = px^2 + 2qxy + ry^2$$

correspondent respectivement aux deux formes trinaires (3) de

$$c = pr - q^2.$$

Les formes trinaires de c qui correspondent aux deux formes trinaires de Δ sont

$$(5)\quad \begin{cases} c = (m'n'' - m''n')^2 + (m''n - mn'')^2 + (mn' - m'n)^2, \\ c = (m'_1 n''_1 - m''_1 n'_1)^2 + (m''_1 n_1 - m_1 n''_1)^2 + (m_1 n'_1 - m'_1 n_1)^2; \end{cases}$$

et, pour qu'elles soient identiques avec les formes (3), il faut que l'on ait

$$\begin{aligned} &(m'n'' - m''n')^2 + (m'_1 n''_1 - m''_1 n'_1)^2 = \mathrm{F}^2, \\ &(m''n - mn'')^2 + (mn' - m'n)^2 = \theta^2(\mathrm{G}^2 + \mathrm{H}^2) = \theta^2\pi, \\ &(m''_1 n_1 - m_1 n''_1)^2 + (m_1 n'_1 - m'_1 n_1)^2 = \theta^2(\mathrm{G}'^2 + \mathrm{H}'^2) = \theta^2\pi. \end{aligned}$$

Or, en faisant $y = m$, $x = -n$ dans la première forme trinaire de Δ, puis $y = m_1$ et $x = -n_1$ dans la seconde, on trouve

$$(6)\quad \begin{cases} pn^2 - 2qmn + rm^2 = (m'n - n'm)^2 + (m''n - mn'')^2 = \theta^2\pi, \\ pn_1^2 - 2qm_1 n_1 + rm_1^2 = (m'_1 n_1 - n'_1 m_1)^2 + (m''_1 n_1 - m_1 n''_1)^2 = \theta^2\pi; \end{cases}$$

d'ailleurs on a, identiquement,

$$\begin{aligned} &(pn^2 - 2qmn + rm^2)(pn_1^2 - 2qm_1 n_1 + rm_1^2) \\ &\quad = [pnn_1 - q(mn_1 + m_1 n) + rmm_1]^2 + c(m_1 n - mn_1)^2; \end{aligned}$$

donc

$$(\theta^2\pi)^2 = y^2 + cz^2, \quad z = m_1 n - m n_1.$$

Si z est différent de zéro, l'équation obtenue nous montre que l'un des facteurs $\theta^2\pi + y$, ou $\theta^2\pi - y$ doit être divisible par c, puisque c est premier ou double d'un nombre premier. D'ailleurs, $\theta^2\pi$ et y étant inférieurs à c, leur somme ne peut être divisible par c sans être égale à c; on a donc

$$\theta^2\pi + y = c, \quad \theta^2\pi - y = z^2.$$

Puis, en remplaçant $\theta^2\pi$ par sa valeur $c - \mathrm{F}^2$, on déduit de ces équations

$$y = \mathrm{F}^2, \quad c = \mathrm{F}^2 + \mathrm{F}^2 + z^2.$$

Dans ce cas, le raisonnement de Legendre subsiste; car, s'il est nécessaire de prendre pour F^2 et F'^2 les deux carrés égaux des deux formes trinaires de c, l'équation $c = \mathrm{F}^2 + \mathrm{F}'^2 + \theta^2\theta'^2 z^2$, qui n'a pas lieu dans ce cas, se trouve remplacée par une équation équivalente

$$c = \mathrm{F}^2 + \mathrm{F}^2 + z^2,$$

d'où l'on déduira les mêmes conclusions. Il nous suffira donc d'établir le théorème proposé dans le cas où l'on a

$$z = m n_1 - m_1 n = 0.$$

3. Dans cette hypothèse, les deux nombres m_1, n_1 sont respectivement égaux aux deux nombres m et n. D'abord, si l'on suppose $m = 0$, comme n ne peut être nul en même temps, il faut égaler m_1 à zéro, et les formules (6) donnent $pn^2 = \theta^2\pi = pn_1^2$, d'où $n^2 = n_1^2$. Comme le signe de n_1 est arbitraire, nous prendrons $n_1 = n$; on verrait de même que, si $n = 0$, il faut faire $n_1 = 0$ et $m^2 = m_1^2$. Considérons le cas où aucun des deux nombres, m ou n, ne s'évanouit. Soit $\frac{\alpha}{\beta}$ la fraction irréductible à laquelle se réduisent les deux fractions égales $\frac{m}{n}, \frac{m_1}{n_1}$; on aura $m = \lambda\alpha$, $n = \lambda\beta$, $m_1 = \mu\alpha$, $n_1 = \mu\beta$. Les

deux représentations considérées de $\theta^2\pi$ par la forme Δ deviendront

$$\theta^2\pi = \lambda^2(p\beta^2 - 2q\alpha\beta + r\alpha^2) = \mu^2(p\beta^2 - 2q\alpha\beta + r\alpha^2),$$

et l'on en déduira $\lambda^2 = \mu^2$, puis $\lambda = \mu$, parce que l'on peut changer en même temps les signes des deux nombres m_1 et n_1. On a donc $m_1 = m$ et $n = n_1$, ainsi que nous l'avons annoncé, et les deux formes trinaires de Δ sont

$$(5)' \quad \begin{cases} \Delta = (mx + ny)^2 + (m'x + n'y)^2 + (m''x + n''y)^2, \\ \Delta = (mx + ny)^2 + (m'_1x + n'_1y)^2 + (m''_1x + n''_1y)^2. \end{cases}$$

Les équations de condition nécessaires pour l'identité des deux formules sont

$$(7) \quad \begin{cases} m'^2 + m''^2 = m'^2_1 + m''^2_1, \quad n'^2 + n''^2 = n'^2_1 + n''^2_1)^2, \\ m'n' + m''n'' = m'_1n'_1 + m''_1n''_1; \end{cases}$$

de plus, les deux formes trinaires de Δ correspondent respectivement aux deux formes suivantes de c :

$$(8) \quad \begin{cases} c = F^2 + (m''n - mn'')^2 + (mn' - m'n)^2, \\ c = F^2 + (m''_1n - mn''_1)^2 + (mn'_1 - m'_1n)^2. \end{cases}$$

4. Nous allons d'abord résoudre, d'une manière générale, les équations (7). La première, mise sous la forme

$$(m' + m'_1)(m' - m'_1) = (m''_1 + m'')(m''_1 - m''),$$

est équivalente aux formules simultanées

$$m' + m'_1 = ab, \quad m' - m'_1 = cd, \quad m''_1 + m'' = ac, \quad m''_1 - m'' = bd,$$

où a, b, c, d désignent quatre nombres entiers, assujettis à la seule condition de donner des valeurs entières aux formules

$$(A) \quad m' = \frac{ab + cd}{2}, \quad m'_1 = \frac{ab - cd}{2}, \quad m'' = \frac{ac - bd}{2}, \quad m''_1 = \frac{ac + bd}{2};$$

on verrait de même que l'équation $n'^2 + n''^2 = n'^2_1 + n''^2_1$ est résolue de la manière la plus générale par les formules

$$(B) \qquad n' = \frac{\alpha\beta + \gamma\delta}{2}, \quad n'_1 = \frac{\alpha\beta - \gamma\delta}{2}, \quad n'' = \frac{\alpha\gamma - \beta\delta}{2}, \quad n''_1 = \frac{\alpha\gamma + \beta\delta}{2}.$$

La troisième équation de condition, transformée successivement au moyen des formules (A) et (B), prend les deux formes équivalentes

$$(9) \quad \begin{cases} (n' - n'_1)\, ab + c(n'' - n''_1)\, a - d(n'' + n''_1)\, b + cd(n' + n'_1) = 0, \\ (m' - m'_1)\,\alpha\beta + \gamma(m'' - m''_1)\,\alpha - \delta(m'' + m''_1)\,\beta + \gamma\delta(m' + m'_1) = 0. \end{cases}$$

5. Nous allons discuter cette équation, afin d'en déduire les relations qu'elle exige entre les nombres $a, b, c, d, \alpha, \beta, \gamma, \delta$. Supposons que l'on ait en même temps $n' = n'_1$, $m' = m'_1$, les équations (7) ne peuvent être vérifiées que de l'une des deux manières suivantes :

$$\begin{aligned} m'' &= m''_1 \quad \text{et} \quad n'' = n''_1, \\ m'' &= -m''_1 \quad \text{et} \quad n'' = -n''_1. \end{aligned}$$

Dans les deux cas, les formes trinaires (8) de c deviennent identiques, contrairement à l'hypothèse. Nous pouvons donc admettre que l'une, au moins, des deux différences $(m' - m'_1)$, $(n' - n'_1)$ ne s'évanouit pas.

1° Soit $n' - n'_1 \gtrless 0$. L'équation (9), multipliée par $(n' - n'_1)$ se met sous la forme équivalente

$$\begin{aligned} [(n' - n'_1)\, a - d(n'' + n''_1)]\ [(n' - n'_1)\, b + c(n'' - n''_1)] \\ + cd(n''^2 - n''^2_1 + n'^2 - n'^2_1) = 0; \end{aligned}$$

puis, en ayant égard à l'équation $n'^2 + n''^2 = n'^2_1 + n''^2_1$, et aux formules (B), on la réduit à la suivante :

$$\gamma\delta(a\delta - d\alpha)(b\gamma - \beta c) = 0.$$

D'ailleurs, aucun des deux nombres γ, δ ne peut être nul, car alors on aurait $n' = n'_1$, contrairement à l'hypothèse; l'équation obtenue se

réduit donc à l'une des deux suivantes :

$$a\delta = \alpha d, \quad b\gamma = \beta c. \tag{10}$$

2° Soit $n' = n'_1$ et $m' - m'_1 \gtrless 0$. L'équation (9), prise sous sa seconde forme et multipliée par $(m' - m'_1)$, se met sous la forme suivante :

$$[(m' - m'_1)\alpha - \delta(m'' + m''_1)]\,[(m' - m'_1)\beta + \gamma(m'' - m''_1)] + \gamma\delta(m''^2 - m'^2_1 + m'^2 - m''^2_1) = 0,$$

et se réduit à l'équation

$$cd(\alpha d - a\delta)\,(\beta c - b\gamma) = 0,$$

en vertu des formules (A) et de l'équation $m'^2 + m''^2 = m'^2_1 + m''^2_1$. Comme aucun des deux nombres c ou d n'est nul dans l'hypothèse actuelle, on conclut encore que les nombres a, b, c, ... sont assujettis, par la troisième des conditions (7), à vérifier l'une des deux équations (10).

6. Soit d'abord $a\delta = \alpha d$. On peut vérifier cette équation en faisant évanouir les deux membres, ce qui peut s'obtenir des quatre manières suivantes :

$$a = d = 0, \quad \alpha = \delta = 0,$$
$$a = \alpha = 0, \quad d = \delta = 0.$$

Dans les deux premières hypothèses, les nombres m'_1, m''_1, ... ou n'_1, n''_1, ... sont nuls, et les deux formes trinaires (8) de c sont

$$c = 0 + m^2 n'^2 + m^2 n''^2 = 0 + m^2 n'^2_1 + m^2 n''^2_1,$$

ou bien

$$c = 0 + n^2(m'^2 + m''^2) = 0 + n^2(m'^2_1 + m''^2_1),$$

c'est-à-dire qu'elles se réduisent à deux sommes de deux carrés. Mais le nombre c, étant premier ou double d'un nombre premier, n'est décomposable que d'une seule manière en une somme de deux carrés; les deux formes trinaires de c ne peuvent donc différer l'une de

l'autre que par l'ordre des deux derniers carrés, ce qui est contraire à l'hypothèse. Dans les deux derniers cas, les nombres m'_1, m''_1, n'_1, n''_1 sont respectivement égaux à m', m'', n', n'' ou à ces nombres changés de signes; de sorte que les deux formes trinaires de c sont identiques, tandis qu'on les suppose différentes. Nous pouvons donc admettre qu'aucun des quatre nombres a, α, d, δ ne s'évanouit. Désignant alors par f_g la fraction irréductible à laquelle se réduisent les deux fractions $\frac{a}{d}, \frac{\alpha}{\delta}$, on a

$$a = \lambda f, \quad d = \lambda g, \quad \alpha = \mu, \quad \delta = \mu g,$$

λ et μ étant deux nombres entiers.

Les formules (A) et (B) deviennent alors

$$(11)\quad \begin{cases} m' = \lambda \frac{bf + cg}{2}, & m'' = \lambda \frac{cf - bg}{2}, & m'_1 = \lambda \frac{bf - cg}{2}, & m''_1 = \lambda \frac{cf + bg}{2}, \\ n' = \mu \frac{\beta f + \gamma g}{2}, & n'' = \lambda \frac{\gamma f - \beta g}{2}, & n''_1 = \mu \frac{\beta f - \gamma g}{2}, & n''_1 = \mu \frac{\gamma f + \beta g}{2}. \end{cases}$$

Au moyen de ces formules, nous allons montrer que le nombre c est nécessairement composé, à moins que les deux formes trinaires (8) cessent d'être différentes. Pour cela, nous ordonnerons la première de ces formes, par rapport aux nombres arbitraires m, n, ce qui nous donnera

$$(12)\quad c = F^2 + (n'^2 + n''^2)m^2 - 2(m'n' + m''n'')mn + (m'^2 + m''^2)n^2.$$

D'ailleurs, par les formules (11), on trouve

$$\begin{aligned} F^2 = (m'n'' - m''n')^2 &= \frac{\lambda^2\mu^2}{16}(f^2 + g^2)^2 (b\gamma - c\beta)^2, \\ n'^2 + n''^2 &= \frac{\mu^2}{4}(f^2 + g^2)(\beta^2 + \gamma^2), \\ m'^2 + m''^2 &= \frac{\lambda^2}{4}(f^2 + g^2)(b^2 + c^2), \\ m'n' + m''n'' &= \frac{\lambda\mu}{4}(f^2 + g^2)(b\beta + c\gamma). \end{aligned}$$

On ne peut pas supposer $F = 0$, car les deux formes ternaires (8), se

réduisant à des sommes de deux carrés, seraient nécessairement identiques, ainsi que nous l'avons déjà fait remarquer plus haut. Dès lors, les formules précédentes montrent que c est le produit de deux facteurs, dont l'un est (f^2+g^2) ou $\frac{1}{2}(f^2+g^2)$, et dont l'autre est plus grand que $\frac{f^2+g^2}{2}$. Pour que c soit premier ou double d'un nombre premier, il faut que $\frac{f^2+g^2}{2}$ soit égal à 1 ou à 2. D'ailleurs, f et g étant des nombres entiers, premiers entre eux et différents de zéro, l'équation $f^2+g^2=4$ est impossible; on doit donc prendre

$$f^2+g^2=2, \quad f=\pm g=\pm 1.$$

Si l'on a $f=g=\pm 1$, les formules (11) donnent

$$m'=m''_1, \quad m''=-m'_1, \quad n'=n''_1, \quad n''=-n'_1,$$

de sorte que l'on a

$$mn'-m'n=mn''_1-m''_1n, \quad mn''-m''n=-(mn'_1-m'_1n),$$

et les deux formes trinaires de c ne diffèrent que par l'ordre des termes. Si l'on a $f=-g=\pm 1$, les formules (11) donnent

$$m'=-m''_1, \quad m''=m_1, \quad n'=-n''_1, \quad n''=n_1,$$

ce qui donne

$$(mn'-m'n)=-(mn''_1-m''_1n), \quad (mn''-m''n)=mn'_1-m'_1n,$$

et les deux formes trinaires de c sont encore identiques, à l'ordre près des deux derniers carrés. Si donc deux formes trinaires de c, réellement différentes, correspondent à un même diviseur trinaire de la formule t^2+cu^2, le nombre c n'est ni premier ni le double d'un nombre premier.

7. On arriverait encore à la même conclusion si l'on supposait $b\gamma=\beta c$. D'abord on doit exclure les deux hypothèses

$$b=c=0, \quad \beta=\gamma=0,$$

parce qu'elles font évanouir le carré F^2. On doit aussi écarter les deux hypothèses $b = \beta = 0$, $c = \gamma = 0$, parce qu'elles identifient entre elles les deux formes trinaires de c. On pourra donc poser

$$\frac{b}{c} = \frac{\beta}{\gamma} = \frac{f}{g},$$

f et g désignant deux nombres premiers entre eux et différents de zéro, et l'on en déduira $b = \lambda f$, $c = \lambda g$, $\beta = \mu f$, $\gamma = \mu g$; puis, en substituant dans la formule (12) les valeurs qui en résultent pour m', m'', ..., on verrait, comme dans le cas précédent, que c est le produit de deux facteurs, dont le plus petit est $\frac{1}{2}(f^2 + g^2)$, et qu'ainsi il ne peut être premier ou double d'un nombre premier, à moins que l'on n'ait

$$f^2 + g^2 = 2 \quad \text{et} \quad f = \pm g = \pm 1.$$

Or, dans cette hypothèse, les deux formes trinaires de c ne diffèrent l'une de l'autre que par l'ordre des termes.

Ainsi, dans le cas exceptionnel où les deux formes trinaires de c seraient déterminées par les formules (3), il est impossible que ces deux formes correspondent à un même diviseur trinaire de la formule $t^2 + cu^2$, si le nombre c est premier ou double d'un nombre premier. Le théorème proposé de Legendre est donc vrai, sans aucune exception.