

JACOBI

**Sur la division du cercle et son application
à la théorie des nombres**

Nouvelles annales de mathématiques 1^{re} série, tome 15
(1856), p. 337-352

http://www.numdam.org/item?id=NAM_1856_1_15__337_0

© Nouvelles annales de mathématiques, 1856, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

**SUR LA DIVISION DU CERCLE
ET SON APPLICATION A LA THÉORIE DES NOMBRES ;**

PAR JACOBI.

(Extrait des *Comptes rendus mensuels* de l'Académie des Sciences
de Berlin pour l'année 1837.)

(TRADUIT PAR M. E. LAGUERRE-WERLY.)

Soient p un nombre premier, x une racine de l'équation

$$\frac{x^p - 1}{x - 1} = 0,$$

et g une racine primitive de p . Posons en outre

$$F(\alpha) = x + \alpha x^g + \alpha^2 x^{g^2} + \dots + \alpha^{p-2} x^{p^{g^{p-2}}},$$

α désignant une racine de l'équation

$$\frac{\alpha^{p-1} - 1}{\alpha - 1} = 0.$$

On aura

$$F(\alpha) F(\alpha^{-1}) = \alpha^{\frac{p-1}{2}} \cdot p;$$

et si l'on pose

$$F(\alpha^m) F(\alpha^n) = \psi(\alpha) F(\alpha^{m+n}),$$

l'expression $\psi(\alpha)$ sera une fonction entière de α dont les coefficients seront des nombres entiers; on aura de plus

$$\psi(\alpha) \psi(\alpha^{-1}) = p (*).$$

(*) On doit excepter le cas où une ou plusieurs des quantités α^m , α^n , α^{m+n} se réduiraient à l'unité.

Désignons par r une racine primitive de l'équation

$$r^{p-1} - 1 = 0,$$

et dans l'expression

$$\psi(r) = \frac{F(r^{-m}) \cdot F(r^{-n})}{F(r^{-m-n})}$$

remplaçons la quantité r par le nombre g ; il viendra, si m et n sont des nombres positifs plus petits que $p - 1$,

$$\psi(g) \equiv - \frac{\Pi(m+n)}{\Pi(m)\Pi(n)} \pmod{p},$$

équation dans laquelle

$$\Pi(n) = 1 \cdot 2 \cdot 3 \dots n.$$

Mais si $m + n$ est plus grand que $p - 1$, on aura

$$\psi(g) \equiv 0 \pmod{p};$$

cette dernière proposition constitue dans les applications un des théorèmes les plus féconds de la théorie des nombres.

Le cas de $m + n = p - 1$ doit être excepté. Il y a plus de dix ans que j'ai communiqué ces théorèmes à Gauss. Je ferai encore remarquer que si l'on pose

$$2 \equiv g^m, \quad 3 \equiv g^{m'} \pmod{p},$$

on obtient ces deux formules remarquables :

$$(1) \quad F(-1) F(\alpha^2) = \alpha^{2m} F(\alpha) F(-\alpha),$$

$$(2) \quad F(\alpha) F(\gamma\alpha) F(\gamma^2\alpha) = \alpha^{-3m'} p F(\alpha^3).$$

Dans la dernière formule, γ désigne une racine cubique de l'unité. Si λ est un facteur impair de $p - 1$, la première de ces deux formules permet de déterminer les fonctions $F(\alpha)$, dans lesquelles α désigne une racine $2^{\lambda^{i\text{ème}}}$ de l'u-

nité, au moyen de celles où α désigne une racine $\lambda^{\text{ième}}$ de l'unité. On obtient aussi pour $F(-\gamma)$ l'expression

$$F(-\gamma) = \sqrt{p} \sqrt[3]{\gamma^{-B} \frac{A - B\sqrt{-3}}{A + B\sqrt{-3}}},$$

équation dans laquelle

$$A^2 + 3B^2 = p.$$

A l'aide des deux mêmes formules, on trouve que si α est une racine primitive 8^{e} de l'unité et si l'on a

$$\begin{aligned} p &= a^2 + b^2 = c^2 + d^2, \\ a &\equiv c \equiv -1 \pmod{4}, \end{aligned}$$

on aura

$$F(\alpha) = \sqrt{(-1)^{\frac{c+1}{4}} (c + d\sqrt{-2}) \sqrt{(a + b\sqrt{-1})\sqrt{p}}},$$

et de plus

$$F(\alpha) F(\alpha^2) = (-1)^{\frac{c+1}{4} + \frac{p-1}{8}} (a + b\sqrt{-1}) F(\alpha^3),$$

$$F(\alpha) F(\alpha^3) = (-1)^{\frac{p-1}{8}} (c + d\sqrt{-1}) F(-1).$$

On obtient encore la formule suivante où γ et α désignent respectivement des racines imaginaires de l'unité du troisième et du quatrième degré,

$$F(\gamma\alpha) = \frac{F(\alpha) F(\gamma)}{a' + b'\alpha} = \frac{\sqrt{(a + b\alpha)} \sqrt{p} \sqrt[3]{\frac{L + M\sqrt{-3}}{2}} \cdot \sqrt{p}}{a' + b'\alpha},$$

formule dans laquelle

$$p = a^2 + b^2 = a'^2 + b'^2 = \frac{L^2 + 3M^2}{4},$$

$$a \equiv -1 \pmod{4}, \quad a' \equiv -L \equiv -1 \pmod{3},$$

$$M \equiv 0 \pmod{3}, \quad \frac{a'}{b'} \equiv \frac{a}{b} \pmod{p}.$$

Les signes douteux et les valeurs des radicaux seront toujours déterminés par des congruences, ou, s'ils dépendent du choix de la racine primitive g , cette dépendance sera indiquée d'une manière simple. La loi de cette dépendance est le principe le plus fécond dans l'application à la théorie des résidus des puissances. Je ferai encore remarquer que si

$$p = c^2 + 2d^2$$

est de la forme $8n + 1$, C est le résidu minimum par rapport au module p du nombre

$$-\frac{1}{2} \frac{\left(\frac{p+1}{2}\right) \left(\frac{p+3}{2}\right) \dots \frac{5(p-1)}{8}}{1 \cdot 2 \dots \frac{p-1}{8}},$$

et qu'il est toujours positif ou négatif suivant que, abstraction faite du signe, il est de la forme $4n + 3$ ou de la forme $4n + 1$.

Les fonctions $F(\alpha)$, que l'on avait seulement déterminées dans les cas où α était ou une racine carrée ou une racine cubique ou une racine biquadratique de l'unité, sont maintenant déterminées par la formule ci-dessus lorsque α est une racine de l'unité soit du degré 6, soit du degré 8 ou bien encore du degré 12. On peut donc à priori résoudre complètement les équations du sixième, du huitième et du douzième degré qui se présentent dans la division du cercle; on n'a besoin pour cela que de la décomposition du nombre p en les trois formes $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$. J'ai joint à mon travail le tableau de ces décompositions pour tous les nombres premiers compris depuis 5 jusqu'à 12,000.

La formule suivante est d'une grande importance dans l'application de la division du cercle à la théorie des nombres.

Soient p un nombre premier de la forme $n\lambda + 1$, β une racine primitive de l'unité du degré λ , α une racine quelconque de l'équation

$$\alpha^{p-1} = 1 ;$$

soit de plus

$$\lambda \equiv g^m \pmod{p} ;$$

on aura, si λ est impair,

$$F(\alpha) F(\beta\alpha) F(\beta^2\alpha) \dots F(\beta^{\lambda-1}\alpha) = \alpha^{-\lambda m} p^{\frac{\lambda-1}{2}} F(\alpha^\lambda),$$

et si λ est pair,

$$(4) \quad \left\{ \begin{array}{l} F(\alpha) F(\beta\alpha) \dots F(\beta^{\lambda-1}\alpha) \\ = (-1)^{\frac{(p-1)(\lambda-2)}{8}} p^{\frac{\lambda-2}{2}} F(-1) F(\alpha^\lambda) (*). \end{array} \right.$$

La quantité $F(-1)$ qui entre dans cette formule est toujours égale à

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

Les fonctions ψ sont liées intimement avec les coefficients du binôme ou les intégrales eulériennes de première espèce, comme le montre la congruence

$$\psi(g) \equiv - \frac{\Pi(m+n)}{\Pi(m)\Pi(n)} \pmod{p}.$$

La comparaison de cette congruence avec la formule

$$\psi(r) = \frac{F(r^{-m}) \cdot F(r^{-n})}{F(r^{-m-n})}$$

montre qu'il doit exister entre les fonctions F et les inté-

(*) Ce théorème est analogue à un théorème de Gauss sur les intégrales eulériennes, théorème dont récemment Dirichlet a donné une remarquable démonstration
(Jacobi)

grales eulériennes de deuxième espèce un semblable rapport, de telle sorte que $-\frac{1}{\pi(n)}$ corresponde à $F(r^{-n})$. J'ai longtemps cherché ce rapport, et je l'ai enfin trouvé dans le théorème suivant :

Remplaçons dans l'expression $F(\alpha)$ l'exposant g^m par son résidu positif g_m par rapport au module p , en sorte que

$$F(x, \alpha) = x + \alpha x^{g_1} + \alpha^2 x^{g_2} + \dots + \alpha^{p-2} x^{g_{p-2}}.$$

Ne représentons plus par x et α des racines de l'unité; mais soient x une variable indéterminée et α un nombre congru à g^{-m} suivant le module p . Représentons en outre par Y_n l'expression que l'on obtient en développant

$$[\log(1 + y)]^n,$$

et en supprimant dans ce développement les puissances de y supérieures à la $(p - 1)^{\text{ième}}$.

On aura pour une valeur quelconque de α et la valeur de m correspondante,

$$F(1 + y, \alpha) \equiv -\frac{Y_m}{\Pi_m} \pmod{p},$$

congruence qui doit avoir lieu quel que soit y , et, par conséquent, doit être vérifiée isolément par les coefficients de chaque puissance de y . Telle est la relation cherchée; en multipliant ensemble deux fonctions F , on en déduit le rapport indiqué plus haut entre les fonctions ψ et les coefficients binomiaux. Je ferai encore remarquer que dans le développement de la $(2m)^{\text{ième}}$ puissance de $\log(1 + y)$ si p est un nombre premier plus grand que $2m + 1$, le coefficient de y^p réduit à sa plus simple expression contient toujours un multiple de p à son numérateur.

La vraie forme des racines de l'équation

$$x^p = 1,$$

forme que l'on n'a donnée nulle part jusqu'ici , est la suivante :

On peut, comme on sait, former facilement ces racines au moyen des fonctions $F(\alpha)$ et par de simples additions. Si λ est un facteur de $p - 1$ et si

$$\alpha^\lambda = 1,$$

il est aussi connu que $[F(\alpha)]^\lambda$ n'est fonction que de α . Mais on n'a besoin de connaître que les valeurs de $F(\alpha)$, pour lesquelles λ est une puissance d'un nombre premier. Soit par exemple $\lambda\lambda'\lambda''$ un facteur de $p - 1$; supposons que $\lambda, \lambda', \lambda''$ soient des puissances de nombres premiers différents et $\alpha, \alpha', \alpha''$ des racines primitives de l'unité des degrés $\lambda, \lambda', \lambda''$, etc.; on aura

$$F(\alpha\alpha'\alpha''\dots) = \frac{F(\alpha)F(\alpha')F(\alpha'')\dots}{\psi(\alpha, \alpha', \alpha''\dots)},$$

$\psi(\alpha, \alpha', \alpha''\dots)$ étant une fonction rationnelle de $\alpha, \alpha', \alpha'', \dots$, à coefficients entiers. Si donc on regarde la racine $(p - 1)^{i\text{ème}}$ de l'unité comme connue, l'expression de x ne contiendra que des radicaux dont les exposants seront des puissances de nombres premiers, ou des produits de tels radicaux. Si

$$\lambda = \mu^n,$$

μ étant un nombre premier, on trouve les fonctions $F(\alpha)$ de la manière suivante. Posons

$$F(\alpha)F(\alpha^i) = \psi_i(\alpha)F(\alpha^{i+1}),$$

il viendra

$$F(\alpha) = \sqrt[\mu]{\psi_1(\alpha)\psi_2(\alpha)\dots\psi_{\mu-1}(\alpha)F(\alpha^\mu)},$$

$$F(\alpha^\mu) = \sqrt[\mu]{\psi_1(\alpha^\mu)\psi_2(\alpha^\mu)\dots\psi_{\mu-1}(\alpha^\mu)F(\alpha^{2\mu})},$$

.....

et enfin

$$F(\alpha^{\mu^{n-1}}) \\ = \sqrt[n]{\psi_1(\alpha^{\mu^{n-1}}) \psi_2(\alpha^{\mu^{n-1}}) \dots \psi_{\mu-2}(\alpha^{\mu^{n-1}}) (-1)^{\frac{\mu-1}{2}} p.}$$

Les $\mu - 1$ fonctions ψ ne déterminent pas seulement toutes les quantités placées sous les signes radicaux, mais encore la dépendance mutuelle des valeurs des radicaux. Si l'on remplace α par ses différentes puissances, on peut, au moyen des valeurs ainsi obtenues, exprimer rationnellement $F(\alpha^i)$ par les puissances de $F(\alpha)$, puisque tous les $\mu^n - 1$ quotients $\frac{[F(\alpha)]^i}{F(\alpha)^i}$ s'expriment toujours par un produit de plusieurs des $\mu - 1$ fonctions $\psi(\alpha)$. C'est en cela que consiste un des plus grands avantages de la méthode proposée sur celle de Gauss; dans cette dernière méthode, la recherche de la dépendance des différentes valeurs des radicaux exige un travail tout spécial, d'une pratique très-pénible à cause de sa difficulté, même pour de petits nombres premiers; par l'introduction des fonctions ψ , on obtient, au contraire, en même temps, et les quantités placées sous les signes radicaux, et les relations qui lient entre elles les valeurs de ces radicaux. On forme les fonctions ψ par un algorithme très-simple; il exige seulement l'emploi d'une Table donnant les solutions des congruences de la forme

$$g^{m^i} \equiv 1 + g^m \pmod{p}.$$

En suivant ces règles, un de mes auditeurs (*) a dans

(*) A cette occasion, le même géomètre (Rosenhain) a démontré ce remarquable théorème: Si α désigne une racine cubique et γ une racine cinquième de l'unité; si, de plus, p désigne un nombre de la forme $30n + 1$ et si l'on pose

$$24 \equiv g^m \pmod{p},$$

un Mémoire couronné par l'Académie de Berlin donné la résolution complète des équations de la forme $x^p = 1$ pour tous les nombres premiers jusqu'à 103.

Un des théorèmes les plus féconds dans la théorie des nombres est le suivant. Soient $m, m', m'',$ etc., des nombres positifs et plus petits que $p - 1$; désignons par $m_i, m'_i, m''_i,$ les plus petits restes positifs que l'on obtient en divisant $im, im', im'',$ etc., par $p - 1$. Faisons de plus

$$m_i + m'_i + m''_i + \dots = n_i(p - 1) + s_i,$$

où s_i est positif et plus petit que $p - 1$. Si r est le plus petit des nombres n_1, n_2, \dots, n_{p-1} et si l'on pose

$$F(r^{-m}) \cdot F(r^{-m'}) \dots = \chi(r) F(r^{-s}),$$

tous les coefficients de $\chi(r)$ seront des nombres entiers divisibles par p^r et non divisibles par une puissance plus élevée de p ; si l'on pose en outre

$$\chi(r) = p^r \chi'(r),$$

on aura

$$\chi'(g) \equiv \pm \frac{\Pi(s)}{\Pi(m) \Pi(m') \Pi(m'')} \pmod{p}.$$

L'application de cette proposition donne des théorèmes particuliers, dont j'ai donné il y a longtemps dans le *Journal* de Crellé un spécimen concernant le nombre des formes quadratiques réduites des diviseurs de la forme

on aura

$$F(\alpha) F(-\gamma) = \alpha^m \frac{A + B\sqrt{-3}}{2} F(-\alpha\gamma),$$

équation où l'on a

$$A \equiv -2, \quad B \equiv 0 \pmod{5}$$

et

$$4p = A^2 + 3B^2.$$

(Jacobi.)

$y^2 + pz^2$, p étant un nombre premier de la forme $4n + 3$ (*). Quand j'aurai donné à ces théorèmes la généralité dont ils paraissent susceptibles, j'aurai l'honneur de les communiquer à l'Académie. Ils forment un lien entre les deux parties principales de la haute arithmétique, la division du cercle et la théorie des formes quadratiques.

J'ai fait l'application de la division du cercle à la théorie des résidus cubiques et biquadratiques, et l'ai employé

(*) Un théorème analogue a lieu pour les nombres premiers de la forme $4n + 1$; le nombre des résidus quadratiques compris entre 0 et $\frac{1}{4}p$ donne alors le nombre des formes. (Jacobi.)

Le théorème dont Jacobi fait ici mention est ainsi conçu: Tout diviseur quadratique de la forme

$$y^2 + pz^2$$

peut se mettre sous la forme

$$ax^2 + bxy + cy^2$$

ou

$$p = 4ac - b^2,$$

si b est impair, et

$$p = ac - \frac{b^2}{4},$$

si b est pair. On peut faire en sorte que b soit plus petit que a et c . Les formes ainsi obtenues sont alors des formes réduites, et le nombre des classes des diviseurs quadratiques est le même que celui de ces formes réduites. Choisissons ces formes réduites en sorte que, si n est pair, b soit impair et réciproquement. Soit N le nombre de ces formes, P la somme des résidus quadratiques de p , Q la somme des non-résidus, on aura

$$2N - 1 = \frac{Q - P}{A}.$$

On peut conclure de là que l'on a toujours

$$Q > P,$$

si

$$p = 4n + 3,$$

résultat aussi obtenu par M. Dirichlet dans son Mémoire sur les progressions arithmétiques. (Note du Traducteur.)

avec beaucoup de simplicité et de facilité à la démonstration du beau théorème donné par Gauss dans son deuxième Mémoire sur les résidus biquadratiques; il n'en a pas fait connaître jusqu'à présent la démonstration, qu'il désigne comme un *mysterium maxime reconditum*, et il y était parvenu vraisemblablement par un chemin tout différent (*). La loi de réciprocité pour les résidus cubiques est de la plus grande simplicité, et la démonstration découle immédiatement des formules connues de la division du cercle.

Soient

$$\frac{L + M\sqrt{-3}}{2} \quad \text{et} \quad \frac{L' + M'\sqrt{-3}}{2}$$

deux nombres complexes premiers (M et M' sont divisibles par 3 et peuvent être zéro); désignons par

$$\left[\frac{x + y\sqrt{-3}}{\frac{1}{2}(L + M\sqrt{-3})} \right]$$

celle des quantités

$$1, \quad \frac{-1 + \sqrt{-3}}{2}, \quad \frac{-1 - \sqrt{-3}}{2},$$

qui est congrue à la puissance

$$(x + y\sqrt{-3})^{\frac{\frac{1}{2}(L^2 + 3M^2) - 1}{3}}$$

suivant le module $L + M\sqrt{-3}$, on aura

$$\left(\frac{\frac{1}{2}(L' + M'\sqrt{-3})}{\frac{1}{2}(L + M\sqrt{-3})} \right) = \left(\frac{\frac{1}{2}(L + M\sqrt{-3})}{\frac{1}{2}(L' + M'\sqrt{-3})} \right).$$

(*) Ce théorème concerne la réciprocité biquadratique entre deux nombres premiers complexes $a + b\sqrt{-1}$ et $c + d\sqrt{-1}$. M. Dirichlet a démon-

Les démonstrations de ces théorèmes ont pu être communiquées sans difficulté à mes auditeurs dans mes leçons de l'hiver dernier (*).

Quand on cherche au moyen de la loi de réciprocité de Legendre à reconnaître si un nombre premier est résidu quadratique ou non-résidu d'un autre, on est obligé de décomposer en facteurs premiers chacun des restes obtenus et de traiter chacun d'eux en particulier. Gauss a apporté à la théorie des résidus quadratiques un perfectionnement essentiel en ramenant par un théorème spécial cette recherche au développement d'une fraction en fraction continue, sans qu'il soit nécessaire d'effectuer aucune décomposition en facteurs. J'ai complété de même la théorie des résidus cubiques et biquadratiques; c'était une généralisation qui s'offrait d'elle-même. Pour montrer en particulier en quoi consiste cette généralisation pour les résidus quadratiques, soit p un nombre impair quelconque égal à $f, f', f'', \text{etc.}$, où $f, f', f'', \text{etc.}$, sont des nombres premiers égaux ou différents; j'étends de la manière suivante le sens de la belle notation employée

tré le premier théorème de Gauss relatif à la réciprocité quadratique de ces nombres.

(*) Ces démonstrations, connues déjà des professeurs Dirichlet et Kummer, ont été récemment publiées par le Dr Eisenstein dans le XXVII^e volume du *Journal de Crelle*, page 289, et dans le XXVIII^e, page 53. La démonstration de la loi de réciprocité des résidus quadratiques donnés par le même géomètre à la page 41 du XXVIII^e volume est la même que celle que j'ai communiquée à Legendre en 1827, et qu'il a insérée dans la troisième édition de sa *Théorie des nombres*. Les théorèmes donnés ci-dessus sur les formes quadratiques font maintenant partie d'une grande théorie fondée par Dirichlet. (Jacobi, octobre 1845.)

La démonstration de la loi de réciprocité de Legendre dont parle ici Jacobi est aussi identique avec celle qu'a donnée M. Cauchy en 1829 dans le *Bulletin de Ferussac* avant la publication de la troisième édition de la *Théorie des nombres*. M. Serret a introduit la démonstration de Jacobi dans la deuxième édition de son *Algèbre supérieure*.

(Note du Traducteur.)

par Legendre. Si x est un nombre premier, $\left(\frac{x}{p}\right)$ désigne le produit

$$\left(\frac{x}{f}\right) \left(\frac{x}{f'}\right) \left(\frac{x}{f''}\right) \dots$$

Soient p et p' deux nombres impairs premiers entre eux dont un au moins soit positif; on a, comme pour les nombres premiers,

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

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

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

Ces formules donnent la valeur de $\left(\frac{p'}{p}\right)$ au moyen du développement ordinaire de $\frac{p'}{p}$ en fraction continue par une règle simple et essentiellement différente de celle de Gauss. La détermination de $\left(\frac{p'}{p}\right)$ exige seulement que l'on recherche si p et p' sont réellement premiers entre eux comme on l'a supposé. Ceci s'applique aussi aux résidus biquadratiques et cubiques pour lesquels j'ai introduit une notation semblable. L'emploi du symbole général $\left(\frac{x}{p}\right)$ fournit dans la pratique de grandes facilités.

Quant aux résidus du huitième et du cinquième degré, qui exigent des principes tout à fait nouveaux, j'en ai déjà poussé l'étude assez avant; aussitôt que j'aurai amené la loi de réciprocité qui les concerne à la perfection désirable, je les communiquerai à l'Académie. Une de mes premières applications de la division du cercle concerne la résolution du problème de Pell par les fonctions cir-

culaires (*). J'extrais d'un Cours rédigé sous mes yeux par le professeur au gymnase de Dantzig, Czawalina, d'après des leçons que j'ai faites il y a plusieurs années, les théorèmes suivants :

Soit p un nombre premier de la forme $4n + 1$; désignons par a ses résidus quadratiques inférieurs à $\frac{1}{2} p$ et positifs, on aura

$$\sqrt{p(\sqrt{p} \cdot y + x)} = 2^{\frac{p+1}{2}} \Pi \sin^2 \frac{a\Pi}{p},$$

x et y étant des solutions de l'équation

$$x^2 - py^2 = -4,$$

et le signe Π désignant un produit s'étendant à toutes les valeurs de a . Soit q un nombre premier de la forme $8n + 3$; désignons par a ses résidus quadratiques, il viendra

$$x + y\sqrt{q} = \sqrt{2} \Pi \sin \left(\frac{a\Pi}{q} + \frac{\Pi}{4} \right),$$

x et y étant des solutions de l'équation

$$x^2 - qy^2 = -2.$$

Soient q et q' deux nombres premiers de la forme $4n + 3$; supposons en outre q résidu quadratique de q' ; désignons respectivement par a et a' les résidus quadratiques positifs de q et de q' , on aura

$$+ 2^{\frac{q-1}{2} \cdot \frac{q'-1}{2}} \Pi \sin \left(\frac{a\Pi}{q} + \frac{a'\Pi}{q'} \right) = \sqrt{q} \cdot x + \sqrt{q'} \cdot y,$$

(*) Ce problème consiste dans la résolution de l'équation indéterminée

$$x^2 - Dy^2 = 1.$$

Euler (*Algèbre*, tome II) en attribue une solution à Pell.

(Note du Traducteur.)

x et y satisfaisant à l'équation

$$qx^2 - q'y^2 = 4.$$

Si x et y ne sont pas pairs, en cubant les équations

$$x^2 - py^2 = -4 \quad \text{et} \quad qx^2 - q'y^2 = 4,$$

on obtiendra la solution des équations

$$u^2 - pv^2 = -1,$$

$$qu^2 - q'v^2 = +1$$

Note du Traducteur (*). On peut consulter sur cette théorie les *Recherches arithmétiques* de Gauss, septième section; les Mémoires sur la théorie des nombres, publiés par M. Cauchy dans les *Mémoires de l'Institut*, tome X; différents articles du même géomètre dans les *Comptes rendus*, et le Mémoire de M. Kummer sur les nombres complexes (*Journal* de M. Liouville, tome XVI).

M. Lebesgue a donné dans le même journal des démonstrations de quelques-unes des propositions contenues dans le présent Mémoire de Jacobi. M. Cauchy a aussi publié dans le *Bulletin* de Férussac (septembre 1829) un résumé de ses recherches sur cette partie de la théorie des nombres; on y trouve notamment indiquée l'application à la théorie des résidus de tous les degrés. Ce résumé se termine ainsi :

« J'observerai, en finissant, qu'ayant donné à M. Jacobi communication de mes formules, j'ai appris de cet habile géomètre qu'il était parvenu de son côté, et en s'appuyant sur les mêmes principes, à des résultats du même genre. Il a donné quelques-uns de ses résultats, mais sans indiquer la méthode qui les avait fournis, dans le tome II du *Journal* de Crelle. »

(*) Le Traducteur, profond investigateur en géométrie et en analyse, possède un esprit d'abstraction excessivement rare chez des jeunes gens. On ne saurait trop encourager les travaux de ces hommes d'avenir. TM.

On peut encore consulter les *Recherches sur la théorie des nombres* publiées par M. Libri dans le tome IX du *Journal de Crelle*, et depuis réimprimées dans les *Mémoires de l'Institut*.