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

PEPIN

Étude sur la théorie des résidus cubiques

Journal de mathématiques pures et appliquées 3^e série, tome 2 (1876), p. 313-324.
<http://www.numdam.org/item?id=JMPA_1876_3_2__313_0>

Gallica NUMDAM

Article numérisé dans le cadre du programme Gallica de la Bibliothèque nationale de France
http://gallica.bnf.fr/

et catalogué par Mathdoc dans le cadre du pôle associé BnF/Mathdoc
http://www.numdam.org/journals/JMPA

Étude sur la théorie des résidus cubiques;

PAR LE P. PEPIN, S. J.

1. Il n'est pas sans fruit de rechercher quelle a pu être l'origine des grandes découvertes, comment l'esprit des inventeurs a pu s'y trouver conduit par l'étude des travaux antérieurs. Quand même cette divination ferait connaître, non pas la voie suivie par le savant dont on étudie les œuvres, mais une voie différente qu'il aurait pu suivre, elle n'aurait pas moins l'avantage d'exercer l'esprit d'invention et de manifester les liens cachés qui rattachent entre elles les diverses parties d'une même science. En étudiant les points principaux de la théorie des résidus cubiques, nous trouverons une formule dont la généralisation est le théorème fondamental du Mémoire publié par Cauchy dans le *Bulletin de Férussac* (1829) et développé plus tard dans le tome XVII des *Mémoires de l'Académie des Sciences*. D'ailleurs, ce résultat n'est pas le seul capable de recommander ce travail aux géomètres; ils y trouveront, je l'espère, les théorèmes les plus remarquables de la théorie des résidus cubiques démontrés d'une manière plus simple que partout ailleurs.

2. Soit p un nombre premier $3\varpi + 1$. Nous désignerons par t une racine primitive de p, et nous poserons $t^3 \equiv g \pmod{p}$, en sorte que g sera une racine primitive de la congruence $x^\varpi \equiv 1 \pmod{p}$. Tous les nombres entiers non divisibles par p seront congrus respectivement aux termes des trois suites

$$(0) \qquad 1, \quad g, \quad g^2, \quad \ldots, \quad g^{\varpi-1},$$

$$(1) \qquad t, \quad tg, \quad tg^2, \quad \ldots, \quad tg^{\varpi-1},$$

$$(2) \qquad t^2, \quad t^2 g, \quad t^2 g^2, \quad \ldots, \quad t^2 g^{\varpi-1}.$$

Nous appellerons *résidus* de classe (i) relativement au nombre premier p et à la base t celles des racines de la congruence $x^{p-1} \equiv 1 \pmod{p}$ dont les indices relativement à la base t sont de la forme $3x + i$; tous ces résidus de classe (i) sont congrus aux différents termes de la suite (i). Les résidus cubiques du nombre premier p sont donc pour nous les résidus de la classe (0).

3. Nous adopterons pour les résidus cubiques une notation analogue à celle que Gauss a employée dans ses Mémoires sur les résidus biquadratiques; nous désignerons par la lettre α diversement accentuée les résidus cubiques de p, par β, β', ... les résidus de classe (1), et par γ, γ', ... les résidus de classe (2). Si nous ajoutons une unité à chacun des termes $\alpha, \alpha', \alpha'', \ldots$, l'une des sommes sera p, car $p - 1$ est résidu cubique de p; les autres sommes seront des résidus de classe (0), (1) ou (2). Désignons par n, n', n'' les nombres des sommes $1 + \alpha$ qui appartiennent respectivement à ces trois classes; ces nombres sont égaux à ceux des solutions des trois congruences

$$(a) \quad 1 + \alpha + \alpha' \equiv 0, \quad 1 + \alpha + \beta \equiv 0, \quad 1 + \alpha + \gamma \equiv 0 \pmod{p},$$

et ils vérifient évidemment la formule

$$(4) \qquad 1 + n + n' + n'' = \varpi.$$

Si l'on ajoute de même une unité aux résidus de classe (1), toutes les sommes appartiennent à l'une des trois classes (0), (1) ou (2). Le nombre des sommes égales à des résidus cubiques est évidemment le même que celui des solutions de la congruence $1 + \beta + \alpha \equiv 0$ ou $1 + \alpha + \beta \equiv 0 \pmod{p}$; ce nombre est n'. Le nombre de celles qui satisfont à la congruence $(1 + \beta) + \beta' \equiv 0 \pmod{p}$ est égal à n''; car la racine de la congruence $\alpha\beta' \equiv 1 \pmod{p}$ est un nombre γ, et le produit $\gamma\beta$ est un nombre α, en sorte que la congruence précédente, multipliée par γ, devient $\gamma + \alpha + 1 \equiv 0 \pmod{p}$, d'où l'on voit que le nombre de ses solutions est n''. Désignons par n_1 le nombre des solutions de la congruence $1 + \beta + \gamma \equiv 0 \pmod{p}$; on aura

$$n' + n'' + n_1 = \varpi,$$

puisque chacune des ϖ sommes $1+\beta$ est un nombre α, un nombre β ou un nombre γ; et, en comparant cette relation avec la formule (4), on déduit $n_1 = n+1$. Ainsi les nombres de solutions des trois congruences

$$(b) \quad 1+\beta+\alpha \equiv 0, \quad 1+\beta+\beta' \equiv 0, \quad 1+\beta+\gamma \equiv 0 \pmod{p}$$

sont respectivement n', n'', $n+1$.

Enfin, si l'on augmente d'une unité les termes γ, les ϖ sommes obtenues satisferont respectivement aux trois congruences

$$(c) \quad 1+\gamma+\alpha \equiv 0, \quad 1+\gamma+\beta \equiv 0, \quad 1+\gamma+\gamma' \equiv 0 \pmod{p};$$

les deux premières ne sont que la troisième des équations (a) et la troisième des équations (b); les nombres de leurs solutions sont donc respectivement n'', $n+1$. En désignant par n_2 le nombre des solutions de la congruence $1+\gamma+\gamma' \equiv 0 \pmod{p}$, on a

$$n''+n+1+n_2 = \varpi,$$

et la comparaison de ce résultat et de la formule (4) donne $n_2 = n'$. Ainsi les nombres de solutions des congruences (c) sont respectivement n'', $n+1$, n'.

4. Proposons-nous de déterminer la somme des puissances d'une racine primitive θ de l'équation binôme $x^p = 1$, qui ont pour exposants les résidus cubiques de p. Posons pour cela

$$s = \Sigma\theta^{g^i}, \quad s' = \Sigma\theta^{tg^i}, \quad s'' = \Sigma\theta^{t^2 g^i}, \quad (i = 0, 1, 2, \ldots, \varpi - 1).$$

Nous aurons

$$s^2 = \Sigma\theta^{g^i}\Sigma\theta^{g^{i'}} = \Sigma\Sigma\theta^{g^i+g^{i'}}, \quad (i \text{ et } i' = 0, 1, 2, \ldots, \varpi - 1);$$

or, parmi les diverses combinaisons des valeurs de i et de i', les unes rendent l'exposant $g^i + g^{i'}$ divisible par p : ce sont les solutions de la congruence

$$i - i' \equiv \tfrac{1}{2}\varpi \pmod{\varpi},$$

car

$$g^i + g^{i'} = g^{i'}(g^{i-i'} + 1) \quad \text{et} \quad g^{\frac{1}{2}\varpi} \equiv -1 \pmod{p}.$$

Or on peut donner à i' l'une quelconque des ϖ valeurs 0, 1, 2, ..., $\varpi - 1$; à chacune de ces valeurs correspond pour i une valeur unique, déterminée par l'une des équations

$$i = \tfrac{1}{2}\varpi + i' \quad \text{ou} \quad i = i' - \tfrac{1}{2}\varpi,$$

suivant que i' sera inférieur ou supérieur à $\frac{1}{2}\varpi$. Les autres combinaisons des valeurs de i et de i' rendent l'exposant $g^i + g^{i'}$ équivalent à des résidus des trois classes (0), (1) ou (2). Le nombre de ces exposants qui sont congrus à $g^l \pmod{p}$ est le même que celui des solutions de la congruence $g^{i-l+\frac{1}{2}\varpi} + g^{i'-l+\frac{1}{2}\varpi} + 1 \equiv \alpha + \alpha' + 1 \equiv 0 \pmod{p}$: ce nombre est donc égal à n. Ainsi, dans notre somme double $\Sigma\Sigma\theta^{g^i+g^{i'}}$, tous les termes θ^{g^l} de s entrent le même nombre de fois n.

Le nombre de fois que la même somme double s^2 renferme le terme θ^{tg^l} est égal au nombre des solutions de la congruence

$$g^i + g^{i'} \equiv tg^l \quad \text{ou} \quad 1 + g^{i-i'} + tg^{l-i+\frac{\varpi}{2}} \equiv 1 + \alpha + 6 \equiv 0 \pmod{p};$$

ce nombre est n'. De même le nombre des exposants $g^i + g^{i'}$ qui sont équivalents à un même résidu de classe (2) est égal à celui des solutions de la congruence

$$1 + g^{i-i'} + t^2 g^{l-i+\frac{1}{2}\varpi} \equiv 1 + \alpha + \gamma \equiv 0 \pmod{p}.$$

Ce nombre est n''; donc

$$s^2 = \varpi + ns + n's' + n''s''. \tag{5}$$

5. En suivant la même méthode, on trouve

$$ss' = \Sigma\theta^{g^i+tg^{i'}} = n's + n''s' + (n+1)s'', \tag{6}$$

car aucun des exposants $g^i + tg^{i'}$ n'est divisible par p, et le nombre de ceux qui se réduisent à un résidu donné est le même pour tous les résidus de la même classe, savoir n' pour la classe (0), n'' pour la

classe (1), et $n+1$ pour la classe (2). Il est égal à n' pour la classe (0), car la congruence $g^i + tg^{i'} \equiv g^t \pmod{p}$ revient à la congruence

$$1 + tg^{i'-i} + g^{t-i+\frac{1}{2}\varpi} \equiv 1 + \beta + \alpha \equiv 0 \pmod{p}.$$

Or le nombre des solutions de cette congruence est n'. On vérifie de même les coefficients n'' et $n+1$ de s' et de s''.

Dans les équations (5) et (6), on peut remplacer θ par θ^t; cette substitution change s en s', s' en s'' et s'' en s. On obtiendra ainsi les deux groupes de formules

$$(7)\qquad \begin{cases} s^2 = \varpi + ns + n's' + n''s'', \\ s'^2 = \varpi + ns' + n's'' + n''s, \\ s''^2 = \varpi + ns'' + n's + n''s', \end{cases}$$

$$(8)\qquad \begin{cases} ss' = n's + n''s' + (n+1)s'', \\ s's = n's'' + n''s + (n+1)s, \\ s''s'' = n's' + n''s'' + (n+1)s'. \end{cases}$$

6. Considérons la fonction Θ_h de Cauchy, définie par la formule

$$\Theta_h = \theta + \rho^h\theta^t + \rho^{2h}\theta^{t^2} + \ldots + \rho^{(p-2)h}\theta^{t^{p-2}} = \Sigma\rho^{ih}\theta^{ti} \quad (i = 0, 1, 2, \ldots, p-2),$$

où ρ est une racine cubique imaginaire de l'unité.

On peut l'écrire sous la forme suivante :

$$\Theta_h = s + \rho^h s' + \rho^{2h} s''.$$

Toutes les puissances de cette fonction peuvent se réduire à des fonctions linéaires des trois sommes s, s', s'' au moyen des formules (7) et (8). Formons d'abord son carré :

$$\begin{aligned} \Theta_h^2 &= s^2 + \rho^{2h}s'^2 + \rho^h s''^2 + 2\rho^h ss' + 2\rho^{2h} ss'' + 2s's'' \\ &= (s^2 + 2s's'') + \rho^{2h}(s'^2 + 2ss'') + \rho^h(s''^2 + 2ss'). \end{aligned}$$

Or on déduit des formules (7) et (8)

$$\begin{aligned} s^2 + 2s's'' &= \varpi + (3n+2)s + 3n's' + 3n''s'', \\ s'^2 + 2s''s &= \varpi + (3n+2)s' + 3n's'' + 3n''s, \\ s''^2 + 2ss' &= \varpi + (3n+2)s'' + 3n's + 3n''s \end{aligned}$$

On a donc, eu égard à la relation $1+\rho^h+\rho^{2h}=0$,

$$(9)\quad \Theta_h^2=(3n+2+3n'\rho^h+3n''\rho^{2h})(s+\rho^{2h}s'+\rho^h s'')=R_{h,h}\Theta_{2h}.$$

Dans toutes ces formules, h est supposé non divisible par 3; il nous suffit de lui attribuer les deux valeurs 1 et 2, ce qui donne

$$\Theta_1^2=R_{1,1}\Theta_2,\quad \Theta_2^2=R_{2,2}\Theta_4\quad\text{et}\quad(\Theta_1\Theta_2)^2=R_{1,1}R_{2,2}\Theta_2\Theta_4.$$

D'ailleurs $\Theta_4=\Theta_1$; on a donc

$$\Theta_1\Theta_2=R_{1,1}R_{2,2}.$$

Or si l'on prend $\rho=\frac{-1+\sqrt{-3}}{2}$, on a

$$R_{1,1}=\tfrac{1}{2}\left[6n+4-3(n'+n'')+3\sqrt{-3}(n'-n'')\right],$$
$$R_{2,2}=\tfrac{1}{2}\left[6n+4-3(n'+n'')-3\sqrt{-3}(n'-n'')\right],$$

$$(10)\quad 4R_{1,1}R_{1,2}=[6n-3(n'+n''-1)+1]^2+27(n'-n'')^2.$$

D'un autre côté,

$$\begin{aligned}\Theta_1\Theta_2&=(s+\rho s'+\rho^2 s'')(s+\rho^2 s'+\rho s'')\\&=s^2+s'^2+s''^2-ss'-ss''-s's''\\&=3\varpi-(s+s'+s'')=3\varpi+1=p.\end{aligned}$$

On déduit donc de la formule (10) et de l'équation $\Theta_1\Theta_2=R_{1,1}R_{2,2}$

$$(11)\qquad 4p=[6n-3(n'+n''-1)+1]^2+27(n'-n'')^2.$$

Posons

$$(12)\qquad 6n-3(n'+n''-1)+1=L,\quad n'-n''=M;$$

L^2 et M^2 sont connus au moyen de l'équation indéterminée

$$(13)\qquad 4p=L^2+27M^2,$$

qui n'admet qu'une seule solution en nombres entiers et positifs. Le signe de L est déterminé par la congruence $L\equiv 1\pmod 3$; celui de M reste indéterminé, et l'on reconnaît aisément que cette indétermi-

nation est nécessaire, puisque le changement de la base t suffit pour échanger entre elles les deux classes (1) et (2), et conséquemment les deux nombres n', n''. En ajoutant aux relations (12) l'équation (4), on trouve

$$(14)\quad n=\frac{p+\mathrm{L}-8}{9},\quad n'=\frac{2p-4-\mathrm{L}+9\mathrm{M}}{18},\quad n''=\frac{2p-4-\mathrm{L}-9\mathrm{M}}{18}.$$

7. Jacobi a donné une expression curieuse du nombre L, analogue à celle que Gauss avait donnée pour la racine du carré impair, dans la décomposition unique d'un nombre premier $4x+1$ en une somme de deux carrés. On arrive aisément à l'expression de Jacobi par une méthode analogue à celle que Gauss a employée dans ses *Recherches sur les résidus biquadratiques* (*Werke*, t. II, p. 88).

Si, dans les deux équations

$$(1+\alpha)^{\varpi}=1+\alpha^{\varpi}+\Sigma\mathrm{A}_i\alpha^i,\quad (i=1,2,\ldots.\,\varpi-1),$$

$$(1+\alpha)^{2\varpi}=1+\alpha^{2\varpi}+\frac{2\varpi.2\varpi-1\ \ldots\varpi-1}{1.2.3\ldots\varpi}\alpha^{\varpi}+\Sigma\mathrm{A}_i\alpha^i+\Sigma\mathrm{A}_l\alpha^l,$$

$$(i=1,2,\ldots,\varpi-1),\quad (l=\varpi+1,\varpi+2,\ldots,2\varpi-1),$$

nous égalons α aux ϖ résidus cubiques du nombre p, et que nous ajoutions les résultats membre à membre, pour chacune des deux équations, en nous rappelant que $\Sigma\alpha^i(\alpha=1,g,g^2,\ldots)$ est un multiple de p pour toutes les valeurs de i non divisibles par ϖ, et qu'on a

$$\alpha^{\varpi}\equiv\alpha^{2\varpi}\equiv 1\pmod{p},$$

nous obtiendrons les deux relations

$$\Sigma(1+\alpha)^{\varpi}\equiv 2\varpi,\quad \Sigma(1+\alpha)^{2\varpi}\equiv 2\varpi+\varpi\frac{1.2\ 3\ldots 2\varpi}{(1.2.3\ldots\varpi)^2}\pmod{p}.$$

D'un autre côté, nous avons vu que, parmi les ϖ valeurs de la somme $1+\alpha$, une seule est divisible par p; n, n', n'' sont respectivement α', $t\alpha'$, $t^2\alpha'$; on a donc

$$\Sigma(1+\alpha)^{\varpi}\equiv n+n't^{\varpi}+n''t^{2\varpi},\quad \Sigma(1+\alpha)^{2\varpi}\equiv n+n't^{2\varpi}+n''t^{\varpi}\pmod{p};$$

par conséquent les trois nombres n, n', n'' seront déterminés par les formules

$$(16)\qquad \begin{cases} n+n'+n''=\varpi-1, \\ n+n't^{\varpi}+n''t^{2\varpi}\equiv 2\varpi, \\ n+n't^{2\varpi}+n''t^{\varpi}\equiv 2\varpi+\varpi\,\frac{1.2.3\ldots 2\varpi}{(1.2.3\ldots\varpi)^2} \pmod p. \end{cases}$$

Si l'on pose $t^{\varpi}\equiv r \pmod p$, r sera une racine primitive de la congruence $x^3\equiv 1 \pmod p$; on a donc

$$1+t^{\varpi}+t^{2\varpi}\equiv 1+r+r^2\equiv 0 \pmod p,$$

en sorte que l'addition des formules (15) donne

$$3n\equiv 5\varpi-1+\varpi\Pi \pmod p, \quad \text{où} \quad \Pi=\frac{\varpi+1.\varpi+2\ldots 2\varpi}{1.2.3\ldots\varpi},$$

ou bien, en multipliant par 3 et remplaçant 3ϖ par -1,

$$9n\equiv -8-\Pi \pmod{p=3\varpi+1}.$$

En comparant ce résultat avec la première des équations (14), nous trouvons

$$L\equiv -\Pi \pmod p.$$

Comme le nombre L est compris entre $-\frac{1}{2}p$ et $\frac{1}{2}p$, et qu'entre ces limites il n'y a qu'un seul nombre congru, suivant le module p, à $-\Pi$, ce résidu unique est la valeur de L, et l'on conclut de l'équation $9n+8=p+L$ que ce résidu divisé par 3 donne pour reste 1. Nous obtenons ainsi ce théorème de Jacobi :

Soit p un nombre premier $3\varpi+1$, *et posons*

$$4p=L^2+27M^2,$$

ce qui est toujours possible d'une seule manière; L *sera le résidu minimum compris entre* $-\frac{1}{2}p$ *et* $\frac{1}{2}p$ *du nombre*

$$-\frac{\varpi+1.\varpi+2\ldots 2\varpi}{1.2\ldots\varpi}$$

divisé par p, et ce résidu, divisé par 3, *laisse toujours* 1 *pour reste.*

Les formules (15) permettent de déterminer le signe de M en fonction de la base t du système d'indices relatif au nombre p; si on les ajoute après avoir multiplié la deuxième par $t^{2\varpi}$ et la troisième par t^{ϖ} et en ayant égard à la formule $1 + t^{\varpi} + t^{2\varpi} \equiv 0 \pmod{p}$, on trouve

$$3n' \equiv (\varpi - 1) - 2\varpi + \varpi t^{\varpi} \Pi \pmod{p},$$

ou bien, en multipliant par 3,

$$9n' \equiv -4 + 2 - t^{\varpi} \Pi \equiv -(2 + t^{\varpi} \Pi) \pmod{p}.$$

La comparaison de ce résultat avec la deuxième des formules (14) donne, pour déterminer le signe de M,

$$9M \equiv (1 + 2t^{\varpi}) L \pmod{p}, \tag{16}$$

car ce signe est la seule inconnue de cette congruence.

8. Les formules (7) et (8), jointes à l'équation $s + s' + s'' = -1$, déterminent les coefficients de l'équation du troisième degré dont les racines sont les trois quantités s, s', s''; l'addition des formules de chaque groupe donne d'abord

$$s^2 + s'^2 + s''^2 = 3\varpi - (n + n' + n'') = 2\varpi + 1,$$
$$ss' + s's'' + s''s = -(n' + n'' + n + 1) = -\varpi;$$

puis l'addition des équations (8), multipliées respectivement par s'', s, s', conduit aux équations suivantes :

$$3ss's'' = (n' + n'')(ss' + s's'' + s''s) + (n + 1)(s^2 + s'^2 + s''^2)$$
$$= (2\varpi + 1)(n + 1) - \varpi(n' + n'') = (n + 1)p - \varpi^2.$$

La première des formules (14), $n + 1 = \frac{p + L + 1}{9}$ étant combinée avec cette équation, on trouve

$$ss's'' = \frac{p + L + 1}{27} - \frac{(p - 1)^2}{27} = \frac{p(L + 3) - 1}{27}.$$

On a donc

$$(x-s)(x-s')(x-s'') = x^3 + x^2 - \frac{p-1}{3}x - \frac{p(L+3)-1}{27} = 0.$$

En posant $y = 3x+1$, on obtient l'équation plus simple

$$y^3 - 3py - pL = 0, \tag{17}$$

dont les racines sont les trois quantités

$$1+3s, \quad 1+3s', \quad 1+3s''.$$

Du reste, les équations du n° 6 fournissent aisément ces racines. Des deux équations $\Theta_1^2 - R_{1,1}\Theta_2$, $\Theta_1\Theta_2 = p$, on déduit d'abord

$$\Theta_1^3 = pR_{1,1}, \quad \Theta_1 = \sqrt[3]{p}\sqrt[3]{R_{1,1}} \quad \text{et} \quad \Theta_2 = \frac{1}{R_{1,1}}\Theta_1^2.$$

En ajoutant les trois équations

$$s+s'+s'' = -1, \quad s+\rho s'+\rho^2 s'' = \Theta_1, \quad s+\rho^2 s'+\rho s'' = \frac{1}{R_{1,1}}\Theta_1^2,$$

on obtient la formule

$$3s+1 = \Theta_1+\Theta_2 = \Theta_1 + \frac{1}{R_{1,1}}\Theta_1^2,$$

qui représente les trois racines de l'équation (17), à raison des trois valeurs du radical cubique $\Theta_1 = \sqrt[3]{pR_{1,1}}$.

Pour donner une forme réelle à ces racines, qui se présentent ici sous une forme imaginaire, il suffit de calculer l'angle auxiliaire φ déterminé par les formules

$$L = 2\sqrt{p}\cos\varphi, \quad 3\sqrt{3}M = 2\sqrt{p}\sin\varphi;$$

on aura

$$R_{1,1} \text{ ou } \frac{L+3\sqrt{-3}M}{2} = \sqrt{p}\,[\cos(2k\pi+\varphi) + i\sin(2k\pi+\varphi)],$$

$$\Theta_1 = \sqrt[3]{pR_{1,1}} = \sqrt{p}\left[\cos\left(\frac{2k\pi+\varphi}{3}\right) + i\sin\left(\frac{2k\pi+\varphi}{3}\right)\right],$$

$$\Theta_2 = \sqrt{p}\left[\cos\left(\frac{2k\pi+\varphi}{3}\right) - i\sin\left(\frac{2k\pi+\varphi}{3}\right)\right],$$

$$1+3s = 2\sqrt{p}\cos\frac{2k\pi+\varphi}{3};$$

cette formule n'a que trois valeurs distinctes qui correspondent aux valeurs 0, 1 et 2 de k.

Le point délicat, dans cette solution, est de déterminer celle de ces trois valeurs qui convient à la somme $\theta + \theta^{\xi^3} + \theta^{\xi^6} + \ldots + \theta^{\xi^{p-4}}$, dans le cas où θ désigne une racine déterminée $\cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ de l'équation $x^p = 1$. M. Kummer s'est occupé de ce problème dans le tome XXXII du *Journal de Crelle* (*De residuis cubicis disquisitiones nonnullæ*, p. 341), où il ramène la question à celle de déterminer les signes et les grandeurs relatives de trois nombres m, m', m'' définis par les équations

$$\tfrac{1}{24}(p^2-1) - \Sigma\alpha = m, \quad \tfrac{1}{24}(p^2-1) - \Sigma\beta = m', \quad \tfrac{1}{24}(p^2-1) - \Sigma\gamma = m'',$$

où α, β, γ désignent ceux des termes de la suite 1, 2, 3,..., $\frac{p-1}{2}$ qui appartiennent respectivement aux classes (0), (1) et (2), définies plus haut (n° 2). Il reste encore à trouver un moyen pratique de calculer les sommes $\Sigma\alpha$, $\Sigma\beta$ et $\Sigma\gamma$.

9. Gauss a obtenu, avant Jacobi, l'équation (11). Il l'a déduite de la relation

$$n^2 + n'^2 + n''^2 + n - (n+1)(n'+n'') - n'n'' = 0, \tag{18}$$

obtenue en exprimant de deux manières différentes, au moyen des nombres n, n', n'', le nombre de solutions de la congruence $1 + \alpha + \beta + \gamma \equiv 0 \pmod{p}$. Cette relation se déduit aisément des formules (7) et (8), en réduisant le produit $ss's''$ à une fonction linéaire des sommes s, s' et s''; on trouve successivement

$$\begin{aligned} ss' &= -(n+1) + (n'-n-1)s + (n''-n-1)s' \\ ss's'' &= -(n+1)s'' + (n'-n-1)[n's'' + n''s + (n+1)s'] \\ &\qquad + (n''-n-1)[n's' + n''s'' + (n+1)s] \\ &= [n'n'' - (n+1)^2](s+s') \\ &\qquad + [n'(n'-n-1) + n''(n''-n-1) - (n+1)]s''. \end{aligned}$$

Comme dans cette équation θ désigne une racine primitive quelconque de l'équation $x^p = 1$, on peut, sans qu'elle cesse d'être vraie, rem-

placer θ par θ^t, ce qui revient à faire la substitution circulaire (s, s', s''); on a donc

$$ss's'' = [n'n'' - (n+1)^2](s'+s'') + [n''(n'-n-1) + n''(n''-n-1) - (n+1)]s.$$

La comparaison des deux expressions du produit $ss's''$ donne

$$(s-s'')[(n+1)^2 + n'^2 + n''^2 - (n+1)(n'+n''+1) - n'n''] = 0.$$

Comme on n'a pas $s - s'' = 0$, puisque l'équation (17) n'a pas de racines égales, il faut que le second facteur soit nul; on obtient ainsi la formule (18). Pour en déduire l'équation (11), il faut, après l'avoir multipliée par 36, l'ajouter membre à membre à l'équation

$$12(n+n'+n'') + 16 = 4p,$$

et appliquer au résultat la méthode de décomposition en carré

10. Dans une Note publiée en décembre 1874, dans les *Comptes rendus de l'Académie des Sciences*, les valeurs des nombres n, n', n'', données ici par les formules (14), ont été obtenues au moyen des relations qui y sont établies entre ces nombres et les coefficients a_0, a_1, a_2 de la fonction $R_{1,1}$ de Cauchy mise sous la forme $R_{1,1} = a_0 + a_1\rho + a_2\rho^2$. Nous les avons obtenus ici directement en appliquant pour la détermination des sommes s, s', s'' une méthode analogue à celle que Vandermonde a suivie pour la résolution de l'équation $x^{11} = 1$. Cette méthode nous a donné les deux formules

$$\Theta_1\Theta_{-1} = p, \quad \Theta_h\Theta_h = R_{h,h}\Theta_{2h},$$

qui, généralisées, deviennent les formules fondamentales des recherches de Cauchy et de Jacobi sur les applications de la théorie des fonctions circulaires à la théorie des nombres, à savoir

$$\Theta_h\Theta_{-h} = (-1)^{h\varpi}p, \quad \Theta_h\Theta_k = R_{h,k}\Theta_{h+k}.$$

Ainsi Cauchy a pu trouver ces formules en cherchant à simplifier, ainsi que nous venons de le faire, la manière dont Gauss obtient les sommes s, s', s'' à la fin de la septième Section des *Disquisitiones*. Cela explique aussi comment il s'est rencontré avec Jacobi.