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

LEBESGUE

Suite des recherches sur les nombres

Journal de mathématiques pures et appliquées 1re série, tome 4 (1839), p. 9-59.
<http://www.numdam.org/item?id=JMPA_1839_1_4__9_0>

SUITE

DES

RECHERCHES

SUR LES NOMBRES;

PAR M. LEBESGUE,

Professeur à la Faculté des Sciences de Bordeaux (*).

§ IV. *Des Résidus cubiques.*

La considération des racines imaginaires des congruences étant utile dans la théorie des résidus de puissances, ainsi que l'a montré M. Jacobi (*De residuis cubicis commentatio numerosa;* Journal de M. Crelle, tome II), nous exposerons dans un premier article quelques propositions concernant ces racines imaginaires, qu'il importe d'introduire dans la théorie des nombres.

I.

Des racines imaginaires des congruences du second degré.—Résolution de la congruence $x^{p+1} \equiv a \pmod{p = hm - 1}$. *— Conséquences.*

Quand le nombre a n'est pas résidu quadratique du module premier p, la congruence $x^2 \equiv a \pmod{p}$ est impossible; en d'autres termes l'expression $x \equiv \sqrt{a} \pmod{p}$ est imaginaire, ou n'indique

(*) § I, tome II, page 253; § II et III, tome III, page 113 de ce Journal.

rien de réel. Néanmoins ces expressions imaginaires ne sont pas inutiles à considérer, comme nous le reconnaîtrons bientôt. Nous allons donc exposer, d'après M. Jacobi, la résolution de la congruence..... $x^{p+1} \equiv a \pmod{p = hm - 1}$, où p est supposé premier. Mais il faut d'abord dire quelque chose des racines imaginaires de la congruence $x^2 \equiv N \pmod{p}$, où N est un non-résidu quadratique du nombre premier $p = 2p' + 1$.

Si l'on représente par $n_1, n_2 \ldots n_{p'}$, les non-résidus quadratiques de p, les expressions imaginaires $\sqrt{n_1}, \sqrt{n_2}, \ldots \sqrt{n_{p'}} \pmod{p}$, peuvent se ramener à la forme $\alpha\sqrt{n_1}, \beta\sqrt{n_1}, \ldots \pmod{p}$, où $\alpha, \beta, \ldots$ sont des nombres entiers. En effet puisque $n_1 n_2$ produit de deux non-résidus quadratiques est un résidu quadratique, on pourra poser $a^2 \equiv n_1 n_2 \pmod{p}$, d'où $a \equiv \sqrt{n_1}.\sqrt{n_2} \pmod{p}$, et par suite $a\sqrt{n_1} \equiv n_2\sqrt{n_1} \pmod{p}$; si l'on détermine le nombre b de sorte que l'on ait $ab \equiv 1 \pmod{p}$, et qu'on fasse $bn_2 \equiv \alpha \pmod{p}$, il en résultera $\sqrt{n_2} \equiv \alpha\sqrt{n_1} \pmod{p}$, et ainsi des autres. On peut conclure de là que si n est un non-résidu quadratique de p, et que la congruence $x^2 + ax + b \equiv 0 \pmod{p}$ soit impossible, on peut lui trouver deux racines imaginaires de la forme $f \pm g\sqrt{n}$, f et g étant des entiers.

Il n'en est pas cependant des racines imaginaires des congruences comme des racines imaginaires des équations. Si l'on suppose, par exemple, a non-résidu cubique du nombre premier $p = 3h + 1$, la congruence $x^3 \equiv a \pmod{p}$ sera impossible, l'expression $\sqrt[3]{a} \pmod{p}$ sera imaginaire, mais elle ne saurait se réduire à la forme $y + z\sqrt{n}$, où y et z sont des entiers et n un non-résidu quadratique de p. Si cela pouvait être, on aurait

$$y^3 + 3nyz^2 - a + (3y^2z + nz^3)\sqrt{n} \equiv 0 \pmod{p};$$

comme $\sqrt{n} \pmod{p}$ ne saurait avoir une valeur réelle, il faudrait donc poser les deux congruences

$$y^3 + 3nyz^2 - a \equiv 0, \qquad 3y^2z + nz^3 \equiv 0 \pmod{p},$$

et comme on ne peut avoir $z \equiv 0 \pmod{p}$, la seconde donnerait $-nz^2 \equiv 3y^2 \pmod{p}$, ce qui réduirait la première à $(-2y)^3 \equiv a \pmod{p}$, congruence impossible, puisque a est non-résidu cubique. L'expres-

sion imaginaire $\sqrt[3]{a}$ (mod. $p=3h+1$) n'est donc jamais réductible à la forme $f+g\sqrt{n}$ (mod. p).

Néanmoins il est des congruences binomes dont toutes les racines ont la forme $f+g\sqrt{n}$ (mod. p). Soit, par exemple, la congruence $x^{p+1}\equiv a \pmod p$, posant $x\equiv y+z\sqrt{n} \pmod p$, n étant un non-résidu quadratique de p, ce qui suppose $n^{\frac{p-1}{2}}\equiv -1 \pmod p$, on trouvera immédiatement

$$x^p \equiv y^p + n^{\frac{p-1}{2}}.z^p.\sqrt{n} \equiv y - z\sqrt{n} \pmod p,$$

à cause de

$$y^p \equiv y, \quad z^p \equiv z \pmod p.$$

De là encore $$x^{p+1} \equiv y^2 - nz^2 \pmod p$$

et par suite, $$y^2 - nz^2 \equiv a \pmod p.$$

Quand on aura déterminé y et z (nombres entiers réels) par cette congruence qui a $p+1$ solutions, par un théorème du § I de ces *Recherches*, on aura les $p+1$ racines de la congruence $x^{p+1}\equiv a \pmod p$, savoir $x\equiv y+z\sqrt{n} \pmod p$ où y et z peuvent prendre le double signe $\pm$; ainsi les racines s'assemblent quatre à quatre de la manière suivante :

$$x \equiv y \pm z\sqrt{n}, \quad x \equiv -y \pm z\sqrt{n} \pmod p,$$

en supposant y et z positifs. Pour le cas de $z=0$ qui exige que a soit résidu quadratique de p, on a

$$y^2 \equiv a \pmod p, \quad \text{puis} \quad x \equiv \pm y \pmod p$$

et ce sont là les seules racines réelles, puisque pour de telles racines on a toujours

$$x^{p+1} \equiv x^2 \equiv a \pmod p.$$

Les deux racines imaginaires conjuguées

$$x \equiv y + z\sqrt{n} \quad \text{et} \quad x \equiv y - z\sqrt{n} \pmod p$$

donnent le facteur quadratique trinome

$$(x-y)^2 - nz^2 \equiv x^2 - 2yx + a \pmod{p}.$$

Pour $y = 0$, ce facteur se réduit à $x^2 + a$. Ce cas ne peut arriver que pour $-nz^2 \equiv a \pmod{p}$, ou pour $-a$ non-résidu quadratique, et il arrive toujours quand cette condition est remplie. Quant aux deux racines réelles, elles donnent le facteur quadratique $x^2 - a$.

Appliquons ce qui précède à la congruence $x^{p+1} \equiv 1 \pmod{p}$. Il y aura d'abord deux racines réelles $+1$ et -1, puis $p-1$ racines imaginaires de forme $f + g\sqrt{n} \pmod{p}$ sous la relation $f^2 - ng^2 \equiv 1 \pmod{p}$. Or ici, comme pour le cas de la congruence $x^{p-1} \equiv 1 \pmod{p}$, il existe des racines imaginaires primitives $r \equiv f + g\sqrt{n} \pmod{p}$, c'est-à-dire qui sont telles que la suite

$$r,\ r^2,\ r^3, \ldots r^{p-1},\ r^p,\ r^{p+1} \equiv 1 \pmod{p}$$

reproduit les $p+1$ racines de $x^{p+1} \equiv 1 \pmod{p}$, trouvées par la résolution de la congruence $f^2 - ng^2 \equiv 1 \pmod{p}$. On pourrait le prouver ainsi qu'il est dit à la page 258 du tome II de ce Journal, ce qui donnerait la congruence aux racines primitives imaginaires. On peut aussi appliquer au cas présent la démonstration donnée dans les n^os 52—55 des *Recherches arithmétiques* de M. Gauss, en ayant soin de remplacer les $p-1$ racines $1, 2, 3, \ldots p-1$ de la congruence $x^{p-1} \equiv 1 \pmod{p}$, par les $p+1$ racines de la congruence $x^{p+1} \equiv 1 \pmod{p}$.

Cela posé, soit m un diviseur de $p+1$, de sorte qu'on ait $p = hm - 1$, si l'on écrit la congruence

$$x^{p+1} \equiv 1 \pmod{p = hm - 1}$$

sous la forme

$$(x^m)^h \equiv 1 \pmod{p = hm - 1},$$

les racines de $y^h \equiv 1 \pmod{p = hm - 1}$, au nombre de h, seront les résidus de $m^{\text{ième}}$ puissance; quand on aura calculé les valeurs de x, la formule x^m les donnera toutes.

Quant aux non-résidus de m^{e} puissance, si l'on cherche les racines

de $t^m \equiv 1 \pmod{p}$ qui, en représentant par r une racine primitive de la congruence $x^{p+1} \equiv 1 \pmod{p = hm - 1}$, sont

$$r^k,\ r^{mk},\ \ldots r^{(m-1)k},\ r^{mk} \equiv 1 \pmod{p},$$

ou pour abréger,

$$\rho,\ \rho^2,\ \ldots \rho^{m-1},\ \rho^m \equiv 1 \pmod{p}, \quad \text{en faisant} \quad r^k \equiv \rho \pmod{p};$$

une racine R de la congruence $x^{p+1} \equiv 1 \pmod{p}$ sera dite non-résidu de k^e classe, si elle donne $R^k \equiv \rho^k \pmod{p}$. Cette classification est comme l'on voit la même que pour les racines réelles. On doit aussi remarquer que le numérotage des classes de non-résidus peut varier avec la racine primitive ρ de la congruence $t^m \equiv 1 \pmod{p}$, ce qui n'empêche point cette classification d'être fort utile.

Soit pour exemple $m = 3$ et le module $p = 3q - 1$. Ici -3 est non-résidu quadratique de p; les racines de la congruence $x^{p+1} \equiv 1 \pmod{p = 3q - 1}$ sont de forme $y + z\sqrt{-3} \pmod{p}$, sous la relation $y^2 + 3z^2 \equiv 1 \pmod{p}$, et comme les trois racines de la congruence $t^3 \equiv 1 \pmod{p}$ sont $1, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2} \pmod{p}$, on reconnaîtra la classe de $R \equiv f + g\sqrt{-3} \pmod{p}$, racine de la congruence $x^{p+1} \equiv 1 \pmod{p}$, ainsi qu'il suit :

Si l'on a

$$(f + g\sqrt{-3})^q \equiv 1 \pmod{p},$$

la racine R sera un résidu cubique. Ce sera un non-résidu de première classe si l'on a

$$(f + g\sqrt{-3})^q \equiv \frac{-1+\sqrt{-3}}{2} \pmod{p},$$

et un non-résidu de deuxième classe, si l'on a

$$(f + g\sqrt{-3})^q \equiv \frac{-1-\sqrt{-3}}{2} \pmod{p}.$$

Ainsi pour le module $5 = 3 \cdot 2 - 1$, comme la congruence

$f^6+3g^6\equiv 1 \pmod 5$ a les six solutions

$$g=0,\ f=1;\ g=0,\ f=-1;\ g=2,\ f=2;\ g=2,\ f=-2;$$
$$g=-2,\ f=2;\ g=-2,\ f=-2;$$

la congruence $x^6\equiv 1 \pmod 5$ aura les six racines

$$\pm 1,\quad 2\pm 2\sqrt{-3},\quad -2\pm 2\sqrt{-3} \pmod 5;$$

or les racines

$$1,\quad \frac{-1+\sqrt{-3}}{2},\quad \frac{-1-\sqrt{-3}}{2} \pmod 5$$

reviennent à

$$1,\quad 2-2\sqrt{-3},\quad 2+2\sqrt{-3} \pmod 5,$$

d'après cela les résidus cubiques seront $+1$ et -1;
les non-résidus de première classe seront $2+2\sqrt{-3}$, $-2-2\sqrt{-3}$;
les non-résidus de deuxième classe seront $2-2\sqrt{-3}$, $-2+2\sqrt{-3}$.

Soit pour second exemple $m=4$ et $p=4q-1$. Comme ici -1 est non-résidu quadratique de p, les racines de $x^{p+1}\equiv 1 \pmod{p=4q-1}$ seront de forme $f+g\sqrt{-1} \pmod p$, sous la relation $f^2+g^2\equiv 1 \pmod{p=4q-1}$ et comme les quatre racines de la congruence $t^4\equiv 1 \pmod p$ sont ± 1 et $\pm\sqrt{-1} \pmod p$, une racine.... $R\equiv f+g\sqrt{-1} \pmod p$ de la congruence $x^{p+1}\equiv 1 \pmod{p=4q-1}$

sera résidu biquadratique pour $(f+g\sqrt{-1})^q\equiv 1$
non-résidu de 1re classe pour $(f+g\sqrt{-1})^q\equiv +\sqrt{-1}$
non-résidu de 2e classe pour $(f+g\sqrt{-1})^q\equiv -1$
non-résidu de 3e classe pour $(f+g\sqrt{-1})^q\equiv -\sqrt{-1}$
$\pmod p$.

Ainsi, pour $p=11=4\cdot 3-1$, les racines de la congruence $x^{10}\equiv 1 \pmod{11}$, sont

$$\pm 1,\quad \pm\sqrt{-1},\quad +5\pm 3\sqrt{-1},\quad -5\pm 3\sqrt{-1},\quad 3\pm 5\sqrt{-1},$$
$$-3\pm 5\sqrt{-1},$$

et si l'on forme les troisièmes puissances, on trouvera

pour résidus biquadratiques 1 et $5\pm 3\sqrt{-1}$,
pour non-résidus de 1re classe $+\sqrt{-1}$ et $\pm 3-5\sqrt{-1}$,
pour non-résidus de 2e classe -1 et $-5\pm 3\sqrt{-1}$,
pour non-résidus de 3e classe $-\sqrt{-1}$ et $\pm 3+5\sqrt{-1}$.

Si l'on demandait les résidus et non-résidus quadratiques pour le cas de la congruence $x^{p+1}\equiv 1 \pmod{p=4q-1}$ au lieu de former les puissances $2q$ des racines, ce qui donnerait 1 pour les résidus quadratiques et -1 pour les non-résidus, on pourrait poser la règle suivante : « La racine $f+g\sqrt{-1}$ (*) (mod. $p=4q-1$) sera résidu » quadratique pour $2(f+1)$ résidu quadratique de p, et non-résidu » quadratique, pour $2(f-1)$ non-résidu quadratique de p. » Pour le prouver, remarquons d'abord que l'on a

$$2(f+1).2(f-1)\equiv -4g^2 \pmod{p=4q-1},$$

un des nombres $2(f+1)$, $2(f-1)$ est donc résidu quadratique et l'autre non-résidu quadratique de p. Or, si l'on pose

$$f+g\sqrt{-1}\equiv (y+z\sqrt{-1})^2 \pmod{p},$$

l en résulte les deux congruences

$$y^2-z^2\equiv f, \quad 2yz\equiv g \pmod{p},$$

d'où par l'élimination de z,

$$(2y^2-f)^2\equiv 1 \pmod{p},$$

et par suite

$$4y^2\equiv 2(f\pm 1) \pmod{p};$$

or cette congruence est toujours possible en déterminant convenable-

(*) La démonstration ne change pas quand on remplace -1 par un autre non-résidu quadratique de p.

ment le signe du terme ± 1 ; donc y et par suite z sont toujours réels.

Si l'on a $4y^2 \equiv 2(f+1) \pmod{p}$, c'est-à-dire $2(f+1)$ résidu quadratique de p, cette dernière congruence, combinée avec $2y^2 - 2z^2 \equiv 2f \pmod{p}$ donnera $y^2+z^2 \equiv 1 \pmod{p}$, de sorte que $y+z\sqrt{-1}$ étant racine de la congruence $x^{p+1} \equiv 1 \pmod{p}$ $f+g\sqrt{-1}$ sera effectivement résidu quadratique de p. Mais si l'on a $4y^2 \equiv 2(f-1) \pmod{p}$, ou $2(f-1)$ résidu quadratique, il en résultera $y^2+z^2 \equiv -1 \pmod{p}$, de sorte que $y+z\sqrt{-1}$ n'étant pas racine de la congruence $x^{p+1} \equiv 1 \pmod{p}$, $f+g\sqrt{-1}$ ne sera pas résidu quadratique, ou ce qui revient au même sera non-résidu quadratique de p.

Ces notions suffiront pour ce que nous avons à dire des résidus cubiques et biquadratiques.

II.

Caractères des résidus et non-résidus cubiques pour le module $p = 3h+1$.

Les théorèmes des paragraphes précédents suffisent pour la solution du problème général :

« Un nombre décomposé en ses facteurs premiers étant donné, » trouver s'il est résidu ou non-résidu cubique; ou plus généralement, » trouver à quelle classe il appartient. »

M. Jacobi a donné, dans la note citée plus haut, les énoncés de deux théorèmes généraux qui font voir dans quel cas un nombre premier est résidu cubique. De ces théorèmes, il n'était pas difficile de passer au cas général, ce que l'auteur n'a pu manquer de faire. M. Cauchy a donné également des théorèmes fort généraux sur les résidus de puissances; j'ignore s'il en a développé les conséquences relativement aux résidus cubiques et biquadratiques. (Voyez *Bulletin de Férussac, pour les Sciences mathématiques*, année 1829.)

On sait que pour le module $p=3h+1$, si r représente une racine primitive de la congruence $x^3 \equiv 1 \pmod{p}$, tout nombre $a<p$

donne $a^k \equiv 1$, ou $\equiv r$, ou $\equiv r^2 \pmod{p}$, et qu'il est dit résidu cubique pour le premier cas, non-résidu de première classe pour le second, et non-résidu de deuxième classe pour le troisième. Or, comme on aurait pu tout aussi bien, en posant $r^k \equiv S \pmod{p}$, prendre 1, S, S^2 pour racines de la congruence $x^3 \equiv \pmod{p}$, on voit qu'il est impossible de distinguer les classes de non-résidus sans faire quelque nouvelle convention. C'est encore ce qui résulte des valeurs des quantités N_q, N'_q, N''_q qui représentent les nombres respectifs de solutions des congruences

$$\left.\begin{array}{l} x_1^3 + x_2^3 \ldots + x_q^3 \equiv \text{à un résidu cubique} \\ x_1^3 + x_1^3 \ldots + x_q^3 \equiv \text{à un non-résidu cubiq., } 1^{re} \text{ classe} \\ x_1^3 + x_2^3 \ldots + x_q^3 \equiv \text{à un non-résidu cubiq., } 2^e \text{ classe} \end{array}\right\} \pmod{p}.$$

En effet, si l'on suppose $4p = L^2 + 27M^2$ et $L = 3\lambda - 2$, en représentant par y_0, y_1, y_2 les racines de l'équation

$$y^3 + y^2 + \tfrac{1}{3}(1-p)y + \tfrac{1}{27}(1 - 3p + L) = 0,$$

la formule (41) du § 1 donnera

$$(A)\quad \begin{cases} p(N_q - p^{q-1}) = y_0(1+3y_0)^q + y_1(1+3y_1)^q + y_2(1+3y_2)^q, \\ p(N'_q - p^{q-1}) = y_1(1+3y_0)^q + y_2(1+3y_1)^q + y_0(1+3y_2)^q, \\ p(N''_q - p^{q-1}) = y_2(1+3y_0)^q + y_0(1+3y_1)^q + y_1(1+3y_2)^q. \end{cases}$$

On voit de suite que le second membre de la première des équations précédentes est une fonction symétrique des racines de l'équation en y, de sorte que N_q sera déterminé sans ambiguité. Il n'en est pas de même de N'_q et N''_q: selon l'ordre qu'on aura donné aux racines y_0, y_1, y_2 de l'équation en y, N'_q pourra se changer en N''_q et réciproquement.

Pour le voir plus facilement, il suffit de changer $1+3y$ en z, et par suite $1+3y_0$, $1+3y_1$, $1+3y_2$ en z_0, z_1 et z_2; il en résultera

$$\begin{aligned} z^3 - 3pz - pL &= 0, \\ 3p(N_q - p^{q-1}) &= z_0^{q+1} + z_1^{q+1} + z_2^{q+1} - (z_0^q + z_1^q + z_2^q), \\ 3p(N'_q - p^{q-1}) &= z_1 z_0^q + z_2 z_1^q + z_0 z_2^q - (z_0^q + z_1^q + z_2^q), \\ 3p(N''_q - p^{q-1}) &= z_2 z_0^q + z_0 z_2^q + z_1 z_2^q - (z_0^q + z_1^q + z_2^q); \end{aligned}$$

et comme en posant

$$z_1z_0^q + z_2z_1^q + z_0z_2^q = \mathrm{T}, \quad z_2z_0^q + z_0z_1^q + z_1z_2^q = \mathrm{T}',$$

on a les équations

$$\mathrm{T} + \mathrm{T}' = (z_0 + z_1 + z_2)(z_0^q + z_1^q + z_2^q) - (z_0^{q+1} + z_1^{q+1} + z_2^{q+1}),$$
$$\mathrm{T}.\mathrm{T}' = z_0z_1z_2(z_0^{2q-1} + z_1^{2q-1} + z_2^{2q-1}) + z_0^2.z_1^2.z_2^2(z_0^{q-3} + z_1^{q-2} + z_2^{q-2}) + z_0^{q+1}z_2^{q+1} + z_0^{q+1}z_1^{q+1} + z_1^{q+1}z_2^{q+1},$$

dont les seconds membres sont des fonctions symétriques des racines z_0, z_1, z_2, il en résultera que T et T′ sont racines d'une équation du second degré; ils ne différeront donc, aussi bien que N'_q et N''_q, que par le signe d'un radical.

Pour le cas particulier de $q = 2$, on a, en représentant par f_i la somme $z_0^i + z_1^i + z_2^i$, les équations

$$\mathrm{T} + \mathrm{T}' = f_1f_2 - f_3, \quad \mathrm{TT}' = p\mathrm{L}f_3 + 3p^2\mathrm{L}^2 + \tfrac{1}{8}(f_3^2 - f_6),$$

d'où l'on tirera à cause de $f_1 = 0$,

$$(\mathrm{T} - \mathrm{T}')^2 = 2f_6 - f_3^2 - 4p\mathrm{L}f_3 - 12p^2\mathrm{L}^2;$$

mais

$$f_3 = 3p\mathrm{L}, \quad f_6 = 54p^3 + 3p^2\mathrm{L}^2,$$

donc

$$(\mathrm{T} - \mathrm{T}')^2 = 27p^2(4p - \mathrm{L}^2) = (27p\mathrm{M})^2.$$

Ainsi

$$\mathrm{T} + \mathrm{T}' = -3p\mathrm{L}, \quad \mathrm{T} - \mathrm{T}' = \mp 27p\mathrm{M},$$

d'où

$$\mathrm{T} = -3p\left(\frac{\mathrm{L} + 9\mathrm{M}}{2}\right), \quad \mathrm{T}' = -3p\left(\frac{\mathrm{L} - 9\mathrm{M}}{2}\right),$$

en prenant le signe supérieur, ou bien

$$\mathrm{T} = -3p\left(\frac{\mathrm{L} - 9\mathrm{M}}{2}\right), \quad \mathrm{T}' = -3p\left(\frac{\mathrm{L} + 9\mathrm{M}}{2}\right),$$

en prenant le signe inférieur.

Nous emploierons toujours les premières valeurs, c'est-à-dire celles qui répondent à $T - T' = -27pM$.

Si maintenant l'on tire de l'équation en z, $z^3 = F + Gz + Hz^2$, F, G et H étant des fonctions entières des coefficients de l'équation en z, on en déduira

$$z_1 z_0^q + z_2 z_1^q + z_0 z_2^q = -3pG + H(z_1 z_0^2 + z_2 z_1^2 + z_0 z_2^2),$$
$$z_2 z_0^q + z_0 z_1^q + z_1 z_2^q = -3pG + H(z_2 z_0^2 + z_0 z_1^2 + z_1 z_2^2),$$

ou bien

$$z_1 z_0^q + z_2 z_1^q + z_0 z_2^q = -3pG - 3pH\left(\frac{L + 9M}{2}\right),$$
$$z_2 z_0^q + z_0 z_1^q + z_1 z_2^q = -3pG - 3pH\left(\frac{L - 9M}{2}\right).$$

Ainsi c'est toujours au changement de signe de M que tient le changement de N'_q en N''_q et réciproquement.

Si l'on remarque que les trois racines de l'équation en z sont

$$\frac{1}{2}\sqrt[3]{4p(L + 3M\sqrt{-3})} + \frac{1}{2}\sqrt[3]{4p(L - 3M\sqrt{-3})} = \frac{1}{2}(P + Q),$$
$$\frac{1}{2}\left(\frac{-1 + \sqrt{-3}}{2}\right)P + \frac{1}{2}\left(\frac{-1 - \sqrt{-3}}{2}\right)Q,$$
$$\frac{1}{2}\left(\frac{-1 - \sqrt{-3}}{2}\right)P + \frac{1}{2}\left(\frac{-1 + \sqrt{-3}}{2}\right)Q,$$

ou bien

$$\frac{1}{2}(P + Q), \quad \frac{1}{2}(\alpha P + \alpha^2 Q), \quad \frac{1}{2}(\alpha^2 P + \alpha Q),$$

sous l'hypothèse

$$\frac{-1 + \sqrt{-3}}{2} = \alpha, \quad \frac{-1 - \sqrt{-3}}{2} = \alpha^2,$$
$$P = \sqrt[3]{4p(L + 3M\sqrt{-3})}, \quad Q = \sqrt[3]{4p(L - 3M\sqrt{-3})};$$

en posant

$$z_0 = \frac{1}{2}(P + Q), \quad z_1 = \frac{1}{2}(\alpha P + \alpha^2 Q), \quad z_2 = \frac{1}{2}(\alpha^2 P + \alpha Q),$$

on trouvera

$$z_1 z_0^2 + z_2 z_1^2 + z_0 z_2^2 = -3p\left(\frac{L+9M}{2}\right);$$

il faut donc admettre les valeurs précédentes des racines z_0, z_1 et z_2, et convenir que N_q et N_q, données alors par la deuxième équation et par la troisième du système (A), répondront aux non-résidus cubiques de première classe, et aux non-résidus de seconde classe.

Les classes de non-résidus étant ainsi fixées, cherchons la classe du nombre 2.

On trouve sans difficulté

$$N_2 = p - L - 2,\quad N_2' = p - 2 - \frac{L+9M}{2},\quad N_2'' = p - 2 - \frac{L-9M}{2},$$

et par conséquent les équations

$$\begin{aligned} n_2 &= N_2 - 2N_1, & n_2' &= N_2' - 2N_1', & n_2'' &= N_2'' - 2N_1'', \\ N_1 &= 3, & N_1' &= 0, & N_1'' &= 0, \end{aligned}$$

donneront

$$n_2 = p - 8 + L,\quad n_2' = p - 2 - \frac{L+9M}{2},\quad n_2'' = p - 2 - \frac{L-9M}{2}.$$

Pour savoir à quelle classe appartient le nombre 2, il suffira de trouver lequel des trois nombres n_2, n_2', n_2'' est de forme $3^2(2Q+1)$, d'après ce qui a été démontré dans le § III. La division par 9 s'effectue nécessairement, ce qui peut se vérifier facilement, car $L=3\lambda-2$ change $4p = L^2 + 27M^2$ en $4(h+\lambda) = 3\lambda^2 + 9M^2$, d'où l'on doit conclure que $h+\lambda$ est divisible par 3. D'ailleurs $p = 3h+1$, on trouve donc

$$\begin{aligned} n_2 &= 3(h+\lambda) - 9, & 4n_2' &= 6[3h - (h+\lambda)] - 18M, \\ & & 4n_2'' &= 6[3h - (h+\lambda)] + 18M, \end{aligned}$$

ce qui montre que la division par 9 est possible. Il suffit donc de chercher lequel des trois nombres n_2, n_2', n_2'' est impair; en négligeant les

multiples de 2 on trouve

$$n_2 \equiv 1 + L,\ n_2' \equiv 1 - \frac{L+M}{2},\ n_2'' \equiv 1 - \frac{L-M}{2} \pmod 2,$$

d'où la proposition qui suit :

« *Théorème.* Le nombre 2 est résidu cubique du nombre premier » $p = 3h + 1$, pour $M \equiv 0 \pmod 2$, [qui entraîne $L \equiv 0 \pmod 2$] » et réciproquement]. Pour $L \equiv -M \pmod 4$, 2 est non-résidu » cubique de première classe, et pour $L \equiv M \pmod 4$, 2 est non-» résidu cubique de seconde classe. »

On trouvera de même, mais par un calcul un peu plus long,

$$N_3 = p - L + 6p,\quad N_3' = p - L - 3p,\quad N_3'' = p - L - 3p,$$

et au moyen des équations

$$n_3 = N_3 - 3N_2 + 3N_1,\ n_3' = N_2' - 3N_2' + 3N_1',\ n_3'' = N_3'' - 3N_2'' + 3N_1'',$$

il en résultera

$$n_3 = p^2 + 3p + 15 - 4L,$$
$$n_3' = p^2 - 6p + 6 + \tfrac{1}{2}(L + 27M),$$
$$n_3'' = p^2 - 6p + 6 + \tfrac{1}{2}(L - 27M),$$

qui peuvent s'écrire ainsi

$$4(n_3 - 27) = 27\,[(h - \lambda)(\lambda^2 + 3M^2) + 4(h - M^2)],$$
$$32(n_3' - 27) = 27\,[4(3h^2 - 4h) - (h - \lambda)(\lambda^2 + 3M^2) + M^2 + 16(M - 2)],$$
$$32(n_3'' - 27) = 27\,[4(3h^2 - 4h) - (h - \lambda)(\lambda^2 + 3M^2) + M^2 - 16(M + 2)],$$

et pour trouver la classe du nombre 3, il suffira de chercher lequel des nombres n_3, n_3', n_3'', a la forme $3^3(3Q + 1)$, c'est-à-dire qui diminué de 27, donne un reste divisible par 81. On voit donc que cela revient à chercher laquelle des trois quantités entre crochets [ ], est divisible par 3. Or, si l'on néglige les multiples de 3, et que l'on

observe que $(h-\lambda)\lambda^6+h$, à cause de $h+\lambda\equiv 0 \pmod 3$, se réduit à

$$(h-\lambda)\lambda^6+h\equiv -2\lambda^3-\lambda\equiv\lambda^3-\lambda\equiv\lambda(\lambda-1)(\lambda+1)\equiv 0 \pmod 3,$$

il restera à savoir laquelle des quantités M^2, M^2+M+1, M^2-M+1 est multiple de 3, d'où la proposition suivante, en remarquant que l'on a $L=3\lambda-2\equiv 1 \pmod 3$.

« Théorème. Le nombre 3 est résidu cubique du nombre premier » $p=3h+1$, quand on a $M\equiv 0 \pmod 3$. Il est non-résidu de » première classe pour $M\equiv 1 \pmod 3$ [ou $M\equiv L \pmod 3$]. Il est » non-résidu de deuxième classe pour $M\equiv -1 \pmod 3$ [ou » $M\equiv -L \pmod 3$]. »

On pourrait continuer de la même manière pour les nombres premiers 5, 7, 11, 13, etc.; mais les calculs deviendraient de plus en plus longs.

Au reste, on évitera le calcul des quantités N_q, N'_q, N''_q ainsi qu'il suit. L'équation $n_q\equiv N_q-qN_{q-1}+\frac{q.q-1}{1.2}N_{q-2}\ldots\ldots+qN_1$ donne en supposant que q soit premier, $n_q\equiv N_q \pmod q$, et comme $n_q=3^q(qQ+1)$ revient à $n_q\equiv 3 \pmod q$, on a $N_q\equiv 3 \pmod q$, pour exprimer que q est résidu cubique de p. Pareillement $N'_q\equiv 3$, $N''_q\equiv 3 \pmod q$ exprimeront que q est non-résidu cubique de première ou de deuxième classe. Il suffira donc de remplacer N_q, N'_q, N''_q par 3, pour changer les équations (A) en congruences conditionnelles qui feront connaître la classe de q, car de ces trois congruences une seule pourra être satisfaite. Si c'est la première, q sera résidu cubique. Si c'est la seconde, q sera non-résidu cubique de première classe. Si c'est la troisième, q sera non-résidu de deuxième classe.

Pour éviter les fractions, on aura en doublant les racines z_0, z_1, z_2,

$$z_0=P+Q,\quad z_1=\alpha P+\alpha^2 Q,\quad z_2=\alpha^2 P+\alpha Q;$$

et comme il en résulte

$$z_0^q\equiv P^q+Q^q,\quad z_1^q\equiv \alpha P^q+\alpha^2 Q^q,\quad z_2^q\equiv \alpha^2 P^q+\alpha Q^q \pmod q,$$

pour $q = 3q' + 1$, et

$$z_0^q \equiv P^q + Q^q,\ z_1^q \equiv \alpha^2 P^q + \alpha Q^q,\ z_2^q \equiv \alpha P^q + \alpha^2 Q^q \pmod{q},$$

pour $q = 3q' - 1$, on aura dans les deux cas $z_0^q + z_1^q + z_2^q \equiv 0 \pmod{q}$, à cause de $1 + \alpha + \alpha^2 = 0$; les équations (A) se réduiront à

$$\left.\begin{aligned} 24p &\equiv z_0^{q+1} + z_1^{q+1} + z_2^{q+1} \\ 24p &\equiv z_1 z_0^q + z_2 z_1^q + z_0 z_2^q \\ 24p &\equiv z_2 z_0^q + z_0 z_1^q + z_1 z_2^q \end{aligned}\right\} \pmod{q},$$

et si l'on substitue dans ces congruences les valeurs de z_0^q, z_1^q, z_2^q, on trouvera

$$\text{(B)} \qquad \left.\begin{aligned} 2 &\equiv P^{3q'} + Q^{3q'} \\ 2 &\equiv \alpha^2 P^{3q'} + \alpha Q^{3q'} \\ 2 &\equiv \alpha P^{3q'} + \alpha^2 Q^{3q'} \end{aligned}\right\} \pmod{q = 3q' + 1},$$

pour le cas de $q = 3q' + 1$, et

$$\text{(C)} \qquad \left.\begin{aligned} 8p &\equiv P^{3q'} + Q^{3q'} \\ 8p &\equiv \alpha P^{3q'} + \alpha^2 Q^{3q'} \\ 8p &\equiv \alpha^2 P^{3q'} + \alpha Q^{3q'} \end{aligned}\right\} \pmod{q = 3q' - 1},$$

pour le cas de $q = 3q' - 1$.

Si l'on pose en général

$$P^{3q'} = [4p(L + 3M\sqrt{-3})]^{q'} = (4p)^{q'}(R + S\sqrt{-3}),$$

$$R = L^{q'} + K_2(-3)^3 M^2 L^{q'-3} + K_4(-3)^6 M^4 L^{q'-6} \ldots + K_{q'}(-3)^{\frac{3q'}{2}} M^{q'},$$

$$S = 3ML[K_1 L^{q'-1} + K_3(-3)^3 M^2 L^{q'-4} + \ldots + K_{q'-1}(-3)^{\frac{3q'-3}{2}} M^{q'-2}],$$

en représentant par K_2, K_4, ... $K_{q'}$ les coefficients binomiaux $\frac{q'}{1}$, $\frac{q' \cdot q' - 1}{1 \cdot 2}$, etc., on trouvera

$$\text{(D)} \qquad \left.\begin{aligned} 1 &\equiv (4p)^{q'} \cdot R \\ 1 &\equiv (4p)^{q'} \cdot (-R + 3S) \\ 1 &\equiv (4p)^{q'} \cdot (-R - 3S) \end{aligned}\right\} \pmod{q = 3q' + 1},$$

pour le premier cas, et

$$(E)\quad \left\{\begin{array}{l} 1 \equiv (4p)^{q'-1}.R \\ 1 \equiv (4p)^{q'-1}.(-R-3S) \\ 1 \equiv (4p)^{q'-1}.(-R+3S) \end{array}\right. \Big\} (\text{mod. } q=3q'-1),$$

pour le second.

Examinons les deux cas particuliers $L \equiv o$ et $M \equiv o \pmod{q}$, qui tous deux donnent $S \equiv o \pmod{q}$.

Soit d'abord $M \equiv o \pmod{q}$, il en résulte

$$R \equiv L^{q'},\ 4p \equiv L^{2},\ (4p)^{q'} \equiv L^{2q'} \text{ et } (4p)^{q'-1} \equiv L^{2q'-2} \pmod{q},$$

ce qui réduit les systèmes (D) et (E) à

$$\begin{array}{l} 1 \equiv L^{3q'},\quad 2 \equiv -L^{3q'},\quad 2 \equiv -L^{3q'} \pmod{q=3q'+1}, \\ 1 \equiv L^{3q'-2},\ 2 \equiv -L^{3q'-2},\ 2 \equiv -L^{3q'-2} \pmod{q=3q'-1}. \end{array}$$

C'est donc toujours la première congruence qui est satisfaite à cause de $L^{q-1} \equiv 1 \pmod{q}$.

Soit en second lieu $L \equiv o \pmod{q}$, il en résulte

$$R \equiv (-3)^{\frac{3q'}{2}} M^{q'},\ 4p \equiv 27M^{3} \equiv -(-3)^{3} M^{3},\ (4p)^{q'} \equiv (-3)^{3q'} M^{3q'},$$

et

$$(4p)^{q'-1} \equiv -(-3)^{3q'-3} M^{3q'-3} \pmod{q},$$

d'où les congruences

$$1 \equiv (-3)^{3q'+\frac{3q'}{2}} M^{3q'},\ 2 \equiv -(-3)^{3q'+\frac{3q'}{2}} M^{3q'} \pmod{q=3q'+1},$$

$$1 \equiv -(-3)^{3q'-2+\frac{3q'-2}{2}} M^{3q'-3},\ 2 \equiv (-3)^{3q'-2+\frac{3q'-2}{2}} M^{3q'-3} \pmod{q=3q'-1}.$$

Or pour $q=3q'+1$, -3 est toujours résidu quadratique de q; pour ce cas c'est donc la première congruence qui a lieu. Pour $q=3q'-1$, -3 est toujours non-résidu quadratique de q, et c'est encore la première congruence qui est vérifiée.

« Théorème. Pour $L\equiv o$ ou $M\equiv o \pmod{q}$, le nombre premier q » est toujours résidu cubique du nombre premier $p = 3h + 1$. »

Pour autre application prenons $q = 5 = 3.2 - 1$ ou $q' = 2$. Ici $(L + 3M\sqrt{-3})^3 = R + S\sqrt{-3}$ donne $R = L^3 - 27M^3$, $S = 6LM$, on a donc

$$\left.\begin{aligned} 1 &\equiv (L^3 + 27M^3)(L^3 - 27M^3) \\ 2 &\equiv (L^3 + 27M^3)(-L^3 + 27M^3 - 18LM) \\ 2 &\equiv (L^3 + 27M^3)(-L^2 + 27M^2 + 18LM) \end{aligned}\right\} \pmod{5}.$$

En posant $L \equiv Mz \pmod{3}$, ces congruences deviennent à cause de $M^4 \equiv 1 \pmod{5}$ [on met de côté le cas de $M \equiv o \pmod{5}$ déjà traité],

$$z^4 \equiv o,\quad z^4 - 2z^3 + z - 2 \equiv o,\quad z^4 + 2z^3 - z - 2 \equiv o \pmod{5}.$$

La première est satisfaite par $z = o$.

La seconde par $z = -1$ et $z = 2$.

La troisième par $z = +1$ et $z = -2$.

Soit encore $p = 7 = 3.2 + 1$, $q' = 2$; on a les mêmes valeurs de R et de S, d'où les congruences

$$\left.\begin{aligned} 1 &\equiv (z^2 - 1)^3 (z^2 + 1) \\ 2 &\equiv (z^2 - 1)^3 (-z^2 + 1 - 3z) \\ 2 &\equiv (z^2 - 1)^3 (-z^2 + 1 + 3z) \end{aligned}\right\} \pmod{7},$$

en rejetant le cas déjà traité $M \equiv o \pmod{7}$, et posant $M^6 \equiv 1$, $L \equiv Mz \pmod{7}$.

Si l'on rejette aussi la valeur $z = o$, qui répond à $L \equiv o \pmod{q}$, et que l'on pose $z^6 \equiv 1 \pmod{7}$, on trouvera

$$z^4 + z^3 - 1 \equiv o,\quad z^4 + z^3 - 4 - 3z(z^4 - 2z^3 + 1) \equiv o,$$
$$z^4 + z^3 - 4 + 3z(z^4 - 2z^3 + 1) \equiv o \pmod{7}.$$

Aucune valeur de z ne satisfait à la première.

La seconde est satisfaite par $z = -2$ et $z = 3$; et la troisième est résolue par $z = 2$ et $z = -3$; d'où les propositions suivantes :

« Théorème. Le nombre 5 est résidu cubique de $p = 3h + 1$ pour » $L \equiv 0$ ou $M \equiv 0$ (mod. 5). Il est non-résidu de première classe » pour $L \equiv -M$ et pour $L \equiv 2M$ (mod. 5), et non-résidu de « deuxième classe pour $L \equiv M$ et pour $L \equiv -2M$ (mod. 5).

» Théorème. Le nombre 7 est résidu cubique de $p = 3h + 1$, » pour $L \equiv 0$ et pour $M \equiv 0$ (mod. 7). Il est non-résidu de première » classe pour $L \equiv -2M$ et pour $L \equiv 3M$ (mod. 7), et non-résidu » de deuxième classe pour $L \equiv 2M$ et $L \equiv -3M$ (mod. 7). »

Il serait long et d'ailleurs assez peu utile d'énoncer les théorèmes relatifs aux autres petits nombres premiers 11, 13, etc. Il suffit de construire une table renfermant les valeurs de z, qui satisfont à la première congruence, à la seconde ou à la troisième. Les remarques suivantes font voir qu'il suffit de résoudre la deuxième congruence, pour avoir la solution des deux autres.

Si l'on fait le produit

$$(P^{3q'} + Q^{3q'} - 2)(\alpha P^{3q'} + \alpha^2 Q^{3q'} - 2)(\alpha^2 P^{3q'} + \alpha Q^{3q'} - 2),$$

on verra qu'il se réduit à

$$P^{3(q-1)} + Q^{3(q-1)} \equiv 2 \pmod{q = 3q' + 1},$$

ou bien à

$$(F) \quad [4p(L + 3M\sqrt{-3})]^{q-1} + [4p(L - 3M\sqrt{-3})]^{q-1} \equiv 2 \pmod{q}.$$

En posant $L \equiv Mz$, $\beta^2 + 3 \equiv 0 \pmod{q}$, cette congruence se réduira à

$$[4pM(z + 3\beta)]^{q-1} + [4pM(z - 3\beta)]^{q-1} \equiv 2 \pmod{q},$$

où $4p = L^2 + 27M^2$ doit être remplacé par $M^2(z^2 + 27)$. On voit que toute valeur de z satisfera à cette congruence, excepté $z = \pm 3\beta$, qui donne $4p \equiv 0 \pmod{q}$.

Ainsi pour le cas de $q = 3q' + 1$, les valeurs $z = \pm 1, \pm 2, \pm 3 \ldots \pm \frac{1}{2}(q - 1)$, à l'exception de $\pm 3\beta \equiv 3\sqrt{-3} \pmod{q}$, satisfont à quelqu'une des congruences (D) où l'on a posé..... $L \equiv Mz \pmod{q}$.

Si l'on remarque que la puissance $a^{q'}$ satisfait à la congruence $t^3 \equiv 1 \pmod{q}$, puisque $a^{3q'} = a^{q-1} \equiv 1 \pmod{q}$, on voit que $a^{q'}$ ne peut avoir que les valeurs 1, $\frac{-1+\beta}{2}$, $\frac{-1-\beta}{2}$ (mod. q), ou 1, α et α^2, en évaluant $\sqrt{-3}$ pour le module q.

D'après cela les équations (B) étant mises sous la forme

$$(G) \quad \left\{ \begin{array}{l} 2 \equiv [4p(L+3M\beta)]^{q'} + [4p(L-3M\beta)]^{q'} \\ 2 \equiv \alpha^2[4p(L+3M\beta)]^{q'} + \alpha[4p(L-3M\beta)]^{q'} \\ 2 \equiv \alpha[4p(L+3M\beta)]^{q'} + \alpha^2[4p(L-3M\beta)]^{q'} \end{array} \right\} \pmod{q},$$

on voit que la première congruence ne peut être satisfaite qu'en posant

$$[4p(L+3M\beta)]^{q'} \equiv 1, \quad [4p(L-3M\beta)]^{q'} \equiv 1 \pmod{q},$$

ou bien encore

$$\left(\frac{L+3M\beta}{L-3M\beta}\right)^{q'} \equiv 1 \pmod{q},$$

d'où ce théorème général dû à M. Jacobi :

« Théorème. Si p et q sont deux nombres premiers de forme $6K+1$, » q sera résidu cubique de p, si, en supposant $\beta^2 + 3 \equiv 0 \pmod{q}$ » et $4p = L^2 + 27M$, l'on a $4p(L+3M\beta)$ (ou $p \cdot \frac{L+3M\beta}{2}$ en divi- » sant par le cube 8), ou encore $\frac{L+3M\beta}{L-3M\beta} \pmod{q}$, résidu cubique » de q. Autrement q sera non-résidu cubique de p. »

Il sera facile, d'après ce théorème, de calculer les valeurs de z, qui résolvent la première des congruences (G), où l'on fait $L \equiv Mz \pmod{q}$. En représentant par ρ un des résidus cubiques de q, résidus au nombre de $q' = \frac{q-1}{3}$, il faudra poser $\frac{L+3M\beta}{L-3M\beta} \equiv \rho \pmod{q}$, ce qui donne $z \equiv 3\beta \cdot \frac{1+\rho}{\rho-1} \pmod{q}$. Il faut remarquer que ρ peut être pris avec le signe + ou le signe — 1.

Dans tous les cas + 1 et — 1 sont résidus cubiques, $\rho = 1$ exige $M \equiv 0$, et répond à $z \equiv \infty \pmod{q}$, $\rho = -1$ exige $L \equiv 0$ et répond à $z = 0 \pmod{q}$.

Les $\frac{p-1}{3}$ valeurs de z peuvent se grouper 2 à 2, ainsi qu'il suit : on a $z \equiv 3\beta . \frac{1+\rho}{\rho-1} \pmod{q}$ et $z' \equiv 3\beta . \left(\frac{1-\rho}{-\rho-1}\right) \pmod{q}$, d'où $zz' \equiv 9\beta^2 \equiv -27 \pmod{q}$.

Deux valeurs de z qui répondent à des résidus cubiques différents ρ et ρ' ne sauraient être égales, car il faudrait avoir $\frac{1+\rho}{\rho-1} \equiv \frac{1+\rho'}{\rho'-1} \pmod{q}$, ou $\rho \equiv \rho' \pmod{q}$, ce qui est impossible; mais deux valeurs de z peuvent être (et sont toujours deux à deux), égales et de signe contraire. La congruence $\frac{1+\rho}{\rho-1} \equiv -\frac{1+\rho'}{\rho'-1} \pmod{q}$ revient à $\rho\rho' \equiv 1 \pmod{q}$, et il existe toujours deux résidus cubiques de q, qui donnent $\rho . \rho' \equiv 1 \pmod{q}$. Dans le cas de $\rho' = -\rho$ ou de $\rho^2 + 1 \equiv 0 \pmod{q}$, ce qui arrive pour $q = 12q'' + 1$, les deux valeurs de z, répondent à un même couple.

On a donc les conséquences suivantes, déjà énoncées par M. Jacobi. Les valeurs de z sont en nombre $\frac{q-1}{3}$, comprenant $z=0$ et $z=\infty$, $z = \pm a$, $z = \pm b$, etc., elles forment des couples de congruences conditionnelles $L \equiv aM$, $L \equiv bM \pmod{q}$ assujétis à la condition $ab \equiv -27 \pmod{q}$. Dans le cas de $q = 12q'' + 1$, on a pour une valeur de z, $a^2 \equiv -27 \pmod{q}$.

Pour satisfaire à la seconde congruence conditionnelle (G), il faudra poser

$$[4p(L + 3M\beta)]^{q'} \equiv \alpha, \quad [4p(L - 3M\beta)]^{q'} \equiv \alpha^2 \pmod{q},$$

α et α^2 représentant les nombres entiers

$$\frac{-1+\beta}{2}, \quad \frac{-1-\beta}{2} \pmod{q};$$

on aura donc

$$\left(\frac{L+3M\beta}{L-3M\beta}\right)^{q'} \equiv \frac{\alpha}{\alpha^2} \equiv \alpha^2 \pmod{q}.$$

Au contraire pour satisfaire à la troisième congruence conditionnelle (G), il faudra poser

$$[4p(L + 3M\beta)]^{q'} \equiv \alpha^2, \quad 4p(L - 3M\beta)^{q'} \equiv \alpha \pmod{q},$$

d'où

$$\left(\frac{L+3M\beta}{L-3M\beta}\right)^{q'} \equiv \alpha \pmod{q}.$$

Ainsi, en égalant $\frac{L+3M\beta}{L-3M\beta}$ à tous les non-résidus de q, formant une même classe, on aura toutes les valeurs de z qui satisfont à l'une des deux dernières congruences (G), et en égalant $\frac{L+3M\beta}{L-3M\beta} \pmod{q}$, à tous les non-résidus de q, formant la seconde classe, on aura toutes les valeurs de z qui satisfont à l'autre des deux dernières congruences (D). Comme on peut remplacer la congruence

$$\left(\frac{L+3M\beta}{L-3M\beta}\right)^{q'} \equiv \alpha \pmod{q} \quad \text{par} \quad \left(\frac{L-3M\beta}{L+3M\beta}\right)^{q'} \equiv \alpha^2 \pmod{q},$$

on voit de suite que quand on a les valeurs de z satisfaisant à la deuxième congruence, en changeant le signe on aura les valeurs de z qui satisfont à la troisième. On pouvait aussi le voir par les équations (D), mais on pouvait demander si les deux dernières équations (D), n'auraient point des racines communes, satisfaisant à $S \equiv 0 \pmod{q}$. Ce qui précède montre que cela est impossible, car il en résulterait

$$\left(\frac{L+3M\beta}{L-3M\beta}\right)^{q'} \equiv \alpha^2, \quad \left(\frac{L-3M\beta}{L+3M\beta}\right)^{q'} \equiv \alpha^2 \pmod{q},$$

d'où $1 \equiv \alpha \pmod{q}$, ce qui est absurde.

Voici donc la marche à suivre pour former la table donnant les valeurs de z qui satisfont aux trois congruences conditionnelles.

1°. On cherchera les valeurs de z qui satisfont à l'une des deux dernières congruences (G), où l'on a fait $L \equiv Mz \pmod{q}$, en égalant $\frac{L+3M\beta}{L-3M\beta}$ à tous les non-résidus cubiques d'une même classe relativement à q. Or, pour avoir ces non-résidus, il suffit de prendre les restes des cubes $1, 2^3, 3^3, 4^3, \ldots$ ce qui donne les résidus cubiques $r, r', r'' \ldots$ Soit n un non-résidu cubique quelconque, ou un nombre de la série $1, 2, 3, \ldots p-1$, qui ne soit pas contenu dans la série $r, r', r'' \ldots$. Les restes des produits nr, nr', nr'', etc., donne-

ront une classe de non-résidus cubiques, et par exclusion on trouverait l'autre, si elle était nécessaire. Ces valeurs de z donnent les congruences $L \equiv aM$, $L \equiv bM \pmod{q}$, etc., qui peuvent se distribuer par couples. L'essai d'une des valeurs de z, savoir a, b, etc., fera voir si elle satisfait à la deuxième ou à la troisième congruence (D). Il suffit de faire dans la seconde $L \equiv aM \pmod{q}$; si elle n'est pas satisfaite, la troisième le sera nécessairement par la même substitution.

2°. Le changement de signe des valeurs de z donnera toutes celles qui satisfont à celle des deux dernières congruences, non satisfaite par les valeurs précédentes de z.

3°. Si de la série ± 1, ± 2, ± 3, ... $\pm \frac{1}{2}(q-1)$ on exclut d'abord $\pm 3\sqrt{-3} \pmod{q}$, et ensuite les valeurs de z déjà trouvées, il restera les valeurs de z qui satisfont à la première congruence (D) ou (G).

Il reste à parler du cas de $q = 3q' - 1$; on prouverait comme plus haut que toute valeur de z [en supposant $L \equiv Mz \pmod{q}$], satisfait nécessairement à quelqu'une des congruences (E); mais on le verra plus facilement encore, ainsi qu'il suit :

Si la première des congruences (C) est satisfaite, comme $PQ = 4p$ et par suite $P^{q+1}.Q^{q+1} \equiv (4p)^2 \pmod{q}$, on aura $8p \equiv P^{q+1} + Q^{q+1}$ et $P^{q+1}\,Q^{q+1} \equiv 16p^2 \pmod{q}$, ce qui donnera $P^{q+1} \equiv 4p$, $Q^{q+1} \equiv 4p \pmod{q}$, et par conséquent $\left(\frac{P}{Q}\right)^{q+1} = \left(\frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}}\right)^{q'} \equiv 1 \pmod{q}$; en d'autres termes la quantité imaginaire $\frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}} \pmod{q}$, doit être résidu cubique de q. La réciproque est vraie, car si l'on a $\left(\frac{L + 3M\sqrt{-3}}{L - 3M\sqrt{-3}}\right)^{q'} \equiv 1 \pmod{q}$, il en résultera $P^{q+1} \equiv Q^{q+1} \pmod{q}$. et puis $P^{q+1}.Q^{q+1} \equiv 16p^2 \pmod{q}$ donnera $P^{q+1} \equiv Q^{q+1} \equiv 4p \pmod{q}$, et la congruence $8p \equiv P^{q+1} + Q^{q+1} \pmod{q}$ sera satisfaite. On a donc ce second théorème général de M. Jacobi.

« Théorème. Si p est un nombre premier de forme $6n+1$, et q » un nombre premier de forme $6n-1$, q sera résidu cubique du

» nombre premier p toutes les fois que $\frac{L+3M\sqrt{-3}}{L-3M\sqrt{-3}}$ (mod. q) (*), » sera résidu cubique de q; autrement q sera non-résidu cubique » de p. »

Pour satisfaire à la seconde des congruences (C), on fera voir, comme plus haut, qu'il faut poser $\alpha P^{q+1} \equiv \alpha^2 Q^{q+1} \equiv 4p$ (mod. q), où l'on suppose $\alpha \equiv \frac{-1+\sqrt{-3}}{2}$ (mod. q); il en résultera.... $\left(\frac{L+3M\sqrt{-3}}{L-3M\sqrt{-3}}\right)^{q'} \equiv \alpha$ (mod. q). Pareillement, pour satisfaire à la troisième des congruences (C), il faudra poser

$$\alpha^2 P^{q+1} \equiv \alpha Q^{q+1} \equiv 4p \text{ (mod. } q),$$

d'où

$$\left(\frac{L+3M\sqrt{-3}}{L-3M\sqrt{-3}}\right)^{q'} \equiv \alpha^2 \text{ (mod. } q).$$

On doit donc dire pour ce cas tout ce qui a été dit pour le premier; seulement, au lieu de poser $\frac{L+3M\sqrt{-3}}{L-3M\sqrt{-3}}$ congru à une quantité réelle, il faudra écrire

$$\frac{L+3M\sqrt{-3}}{L-3M\sqrt{-3}} \equiv f + g\sqrt{-3} \text{ (mod. } q),$$

$f+g\sqrt{-3}$ étant une racine de la congruence $x^{q+1} \equiv 1$ (mod. q); ce qui suppose la condition $f^2+3g^2 \equiv 1$ (mod. q). On obtient ainsi deux congruences conditionnelles qui se réduisent à $L \equiv \frac{3(f+1)}{g} M$ (mod. q). Il suffit pour cela de réduire une congruence telle que celle-ci

$$A+B\sqrt{-3} \equiv 0 \text{ (mod. } q) \text{ à } A \equiv 0 \text{ et } B \equiv 0 \text{ (mod. } q).$$

Ce qui est indispensable, car autrement $\sqrt{-3}$ (mod. q) prendrait une valeur réelle.

On tirera de la congruence $L \equiv \frac{3(f+1)}{g} M$ (mod. q), différentes conséquences analogues à celles exposées plus haut, pour le cas de $b = 3q'+1$.

(*) Dans le journal de M. Crelle, on lit M au lieu de 3M : la comparaison des deux énoncés suffit pour faire voir qu'il y a faute d'impression.

Chaque congruence conditionnelle est satisfaite par $q' = \frac{q+1}{3}$ valeurs de z; pour la première z prend le double signe, à l'exception des valeurs $z = 0$ et $z \equiv \infty$.

Pour la seconde congruence, z ne prend qu'un signe. Pour la troisième on a les mêmes valeurs de z, au signe près, c'est-à-dire avec un signe contraire.

Deux valeurs de z qui répondent l'une à $f + g\sqrt{-3}$, l'autre à $-f - g\sqrt{-3}$ donnent un produit congru à -27 (mod. q).

Deux racines différentes de $x^{q+1} \equiv 1$ (mod. q), $f + g\sqrt{-3}$ et $f' + g'\sqrt{-3}$ ne sauraient donner la même valeur de z, ni des valeurs de z égales au signe près.

Enfin, pour le cas de $q = 12q'' - 1$, les deux valeurs de z correspondantes aux résidus cubiques $\pm g\sqrt{-3}$, formeront un couple donnant un produit $\equiv -27$ (mod. q).

Le calcul des nombres z se fera donc comme pour le cas de $q = 3q' + 1$, seulement il sera plus long, parce qu'il faudra d'abord résoudre la congruence $x^{q+1} \equiv 1$ (mod. $q = 3q' - 1$), ou ce qui revient au même, celle-ci $f^2 + 3g^2 \equiv 1$ (mod. q); puis former les résidus cubiques, ou les cubes des racines $f + g\sqrt{-3}$; trouver par exclusion un non-résidu cubique; et enfin en déduire une classe de non-résidus. Ces calculs, qu'on peut abréger par divers artifices, donneront la table suivante, qu'il serait facile de prolonger, ce que je me propose de faire dans un autre Mémoire sur la résolution des congruences binomes.

PREMIÈRE TABLE.

$$4p = L^2 + 27M^2, \quad L = 3\lambda - 2,$$

$p =$	7,	13,	19,	31,	37,	43,	61,	67,	73,	79,	97, etc.
$L =$	1,	−5,	7,	4,	−11,	−8,	1,	−5,	7,	−17,	19,
$M =$	1,	1,	1,	2,	1,	2,	3,	3,	3,	1,	1,
$\sqrt{-3} =$	2,	6,	4,	11,	16,	13,	27,	8,	17,	32,	27,

etc.

Valeurs de z : $L \equiv Mz \pmod{q}$,

q											
2	1,	1,	1,	»	1,	»	1,	1,	1,	1,	1,
3	1,	1,	1,	−1,	1,	−1,	∞,	∞,	∞,	1,	1,
5	1,	0,	2,	2,	−1,	1,	2,	0,	−1,	−2,	−1,
7	1,	2,	0,	2,	3,	3,	−2,	3,	0,	−3,	−2,
11	1,	−5,	4,	2,	0,	−4,	5,	2,	−5,	−5,	−3,
13	1,	−5,	6,	2,	2,	−4,	4,	−6,	−2,	−4,	6,
etc.											

$p = 7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97,$ etc.

Valeurs de z ou caractères des non-résidus de première classe :

q						
2	− 1,	caractère des résidus		$M \equiv 0 \pmod{2}$,		
3	1,	caractère des résidus		$M \equiv 0 \pmod{3}$,		
5	− 1,	2,				
7	− 2,	3,				
11	1,	2,	3,	−5,		
13	2,	−3,	−4,	6,		
etc.						

Exemple. Veut-on trouver par le moyen de cette table, la classe du nombre $39 = 3.13$ pour le mod. 43? On cherchera les classes de 3 et de 13. Pour 3 la table donne $z = -1$, et comme on trouve $+1$, pour caractère des non-résidus de première classe, il s'ensuit que 3 est un non-résidu de deuxième classe. Pour 13 on trouve $z = -4$, et -4 est un caractère des non-résidus de première classe. Ainsi 3 et 13 sont respectivement des non-résidus de deuxième et de première classe. La somme des numéros de classe est 3. Donc le produit 39 est un résidu cubique.

Autrement, on a $39 \equiv -4 \equiv -2^2 \pmod{4}$, le facteur -1 est un résidu, $(-1) = (-1)^3$. Comme M est divisible par 2, le nombre 2, et par suite son carré sont résidus cubiques, ainsi 39 est un résidu cubique.

On voit qu'au moyen de cette table il sera toujours facile de trouver la classe d'un nombre composé, puisqu'elle donnera celles de ses facteurs premiers.

Quand on aura trouvé les numéros de classe des petits nombres premiers, de 2, 3, 5, 11, 13, par exemple, ceux des nombres premiers plus grands s'en déduiront très facilement. Il suffira de remplacer leurs multiples, puissances ou multiples de puissances, par des nombres dont on sache trouver la classe, ou n'ayant pas de facteur premier au-dessus de 13. Si l'on veut, par exemple, avoir la classe de 17 pour le module 97, comme $5.17 = 85 = 97 - 12$, la classe de 5.17 sera la même que celle de -12 ou de 12; or la classe des nombres 2 et 3 est 1 (la première des non-résidus). Ainsi 5.17 est résidu cubique; or 5 est de première classe, donc 17 doit être de seconde.

On formera donc très facilement la table suivante, où 0 indique la classe des résidus cubiques, et 1 et 2 les deux classes de non-résidus.

TABLE DEUXIÈME.

$q = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$

p,													
7,	2,	1,											
13,	1,	1,	0,										
19,	1,	1,	1,	0,									
31,	0,	2,	1,	2,	1,	1,							
37,	2,	1,	1,	1,	0,	1,	2,						
43,	0,	2,	2,	1,	0,	1,	1,	2,					
61,	1,	0,	1,	1,	2,	2,	2,	2,	0,				
67,	2,	0,	0,	1,	1,	2,	2,	2,	2,	1,	1,		
73,	2,	0,	1,	0,	1,	2,	0,	1,	2,	0,	2,		
79,	1,	1,	2,	2,	2,	1,	0,	2,	2,	2,	2,	1,	
97,	1,	1,	1,	1,	2,	1,	2,	0,	2,	1,	1,	1,	1, 1, 0.

Cette table est analogue à celle donnée par M. Gauss, pour les résidus quadratiques. Elle indique la possibilité ou l'impossibilité de la congruence $x^3 \equiv a \pmod{p}$, en supposant $p < 100$. Quant à la résolution, elle exige d'autres tables.

§ V.

Des résidus bi-quadratiques.

La question des résidus bi-quadratiques a été traitée par M. Gauss : un premier Mémoire a paru dans les *Commentaires de Gottingue;* j'ignore s'il a été suivi d'autres qui complètent la solution de ce problème général : « Un nombre, décomposé en ses facteurs pre-» miers, étant donné, trouver s'il est résidu ou non-résidu bi-qua-» dratique; ou plus généralement à quelle classe il appartient. » J'en donnerai la solution dans ce paragraphe. J'ai déjà cité les recherches de M. Cauchy sur les résidus, je ne dois pas oublier de mentionner un mémoire de M. Dirichlet sur les diviseurs premiers d'une classe de formules du quatrième degré (Journal de M. Crelle, t. III), j'en parlerai avec détail dans l'article suivant.

I.

Caractères des résidus et non-résidus bi-quadratiques pour le module premier $p = 4h + 1$.

Par rapport au module premier $p = 4h + 1$, les nombres $1, 2, 3, \ldots p - 1$ se distribuent en quatre classes, telles qu'en représentant par r, $r^2 \equiv -1$, $r^3 \equiv -r$, $r^4 \equiv 1 \pmod{p}$, les quatre racines de la congruence $t^4 \equiv 1 \pmod{p}$, tout nombre $a < p$ donne a^4 congru à un des nombres $1, r, -1, -r$, pour le module p. Dans le premier cas a est dit résidu bi-quadratique, et dans les autres non-résidu bi-quadratique de première, deuxième ou troisième classe.

Or, si l'on pose $p = L^2 + 4M^2$, L positif ou négatif ayant la forme $1 + 4\lambda$, et si l'on représente par y_0, y_1, y_2, y_3, les racines de l'équation

$$y^4 + y^3 + \tfrac{1}{2}(pr - 3h)y^2 + \tfrac{1}{4}(2p\lambda + pr - h)y + \tfrac{1}{16}[(pr - h)^2 - 4p\lambda^2] = 0,$$

où $p = 4h + 1$ et $h = 2h' + r$, r étant 0 ou 1; on aura pour dé-

terminer les quantités N_q, N'_q, N''_q, N'''_q, ou les nombres de solutions des congruences ayant pour premier membre la somme..... $x_1^4 + x_2^4 + x_3^4 + \ldots + x_q^4$, et pour second un résidu bi-quadratique, ou un non-résidu de première, deuxième ou troisième classe; on aura, dis-je, pour le cas de $r = 0$, ou de $p = 8h' + 1$, les équations suivantes qui se déduisent de la formule (41) du § I (t. II, p. 290):

$$(H)\begin{cases} p(N_q - p^{q-1}) = \gamma_0(1+4\gamma_0)^q + \gamma_1(1+4\gamma_1)^q + \gamma_2(1+4\gamma_2)^q + \gamma_3(1+4\gamma_3)^q, \\ p(N'_q - p^{q-1}) = \gamma_1(1+4\gamma_0)^q + \gamma_2(1+4\gamma_1)^q + \gamma_3(1+4\gamma_2)^q + \gamma_0(1+4\gamma_3)^q, \\ p(N''_q - p^{q-1}) = \gamma_2(1+4\gamma_0)^q + \gamma_3(1+4\gamma_1)^q + \gamma_0(1+4\gamma_2)^q + \gamma_1(1+4\gamma_3)^q, \\ p(N'''_q - p^{q-1}) = \gamma_3(1+4\gamma_0)^q + \gamma_0(1+4\gamma_1)^q + \gamma_1(1+4\gamma_2)^q + \gamma_2(1+4\gamma_3)^q. \end{cases}$$

Pour le cas de $r = 1$, ou de $p = 8h' + 5$, il faudrait employer la formule (42) du § I, et au lieu des équations (H), on en aurait d'autres qui n'en différeraient que par le changement de N_q en N''_q, de N'_q en N'''_q et réciproquement.

Si l'on pose $1 + 4\gamma = z$, les équations précédentes se simplifient et deviennent

$$(I)\begin{cases} 4p(N_q - p^{q-1}) = z_0^{q+1} + z_1^{q+1} + z_2^{q+1} + z_3^{q+1} - (z_0^q + z_1^q + z_2^q + z_3^q), \\ 4p(N'_q - p^{q-1}) = z_1 z_0^q + z_2 z_1^q + z_3 z_2^q + z^0 z_3^q - (z_0^q + z_1^q + z_2^q + z_3^q), \\ 4p(N''_q - p^{q-1}) = z_2 z_0^q + z_3 z_1^q + z_0 z_2^q + z_1 z_3^q - (z_0^q + z_1^q + z_2^q + z_3^q), \\ 4p(N'''_q - p^{q-1}) = z_3 z_0^q + z_0 z_1^q + z_1 z_2^q + z_2 z_3^q - (z_0^q + z_1^q + z_2^q + z_3^q), \end{cases}$$

pour le cas de $p = 8h' + 1$. Pour celui de $p = 8h' + 5$, il suffira de changer N_q en N'_q et réciproquement, N''_q en N'''_q et réciproquement.

L'équation en γ se décompose en deux facteurs

$$(K)\begin{cases} \gamma^2 + \frac{1}{2}(1 - \sqrt{p})\gamma + \frac{1}{4}(pr - h + 2\lambda\sqrt{p}) = 0, \\ \gamma^2 + \frac{1}{2}(1 + \sqrt{p})\gamma + \frac{1}{4}(pr - h - 2\lambda\sqrt{p}) = 0, \end{cases}$$

d'où l'on tire pour $1 + 4\gamma$ ou z,

$$1 + 4\gamma = z = \quad \sqrt{} \pm \sqrt{2p(-1)^h - 2L\sqrt{p}},$$
$$1 + 4\gamma = z = -\sqrt{p} \pm \sqrt{2p(-1)^h + 2L\sqrt{p}};$$

et d'après la formation des quantités $\gamma_0, \gamma_1, \gamma_2, \gamma_3$, (§ I, p. 288, t. II), γ_0 et γ_2 doivent satisfaire à l'une des équations (K) du second degré en γ, et γ_1, γ_3 doivent satisfaire à l'autre.

On voit donc que N_q et N_q'' seront complétement déterminés au moyen des coefficients des équations (K), mais il n'en sera pas de même de N_q' et N_q'''. On prouverait comme dans le § précédent que N_q' peut se changer en N_q''' et réciproquement, et que ces deux quantités ne diffèrent que par le signe de M.

Prenons pour première application la recherche de la classe du nombre premier 2.

On trouve d'abord

$$\begin{aligned}
&z_0^2 + z_1^2 + z_2^2 + z_3^2 = 4p[1 + 2(-1)^k],\\
&z_0^3 + z_1^3 + z_2^3 + z_3^3 = -24pL,\\
&z_2z_0^2 + z_3z_1^2 + z_0z_2^2 + z_1z_3^2 = 8pL,\\
&z_1z_0^2 + z_2z_1^2 + z_3z_2^2 + z_0z_3^2 = 8pL + 32pM,\\
&z_2z_0^2 + z_0z_1^2 + z_1z_2^2 + z_2z_3^2 = 8pL - 32pM.
\end{aligned}$$

D'après cela, on aura

$$\begin{aligned}
&N_2 - p = -6L - [1 + 2(-1)^k],\\
&N_2' - p = 2L + 8M - [1 + 2(-1)^k],\\
&N_2'' - p = 2L - [1 + 2(-1)^k],\\
&N_2''' - p = 2L - 8M - [1 + 2(-1)^k],
\end{aligned}$$

et comme on a d'ailleurs

$$\begin{aligned}
&N_1 = 4, \quad N_1' = N_1'' = N_1''' = 0,\\
&n_2 = N_2 - 8, \quad n_2' = N_2', \quad n_2'' = N_2'', \quad n_2''' = N_2''',
\end{aligned}$$

il en résultera

$$\begin{aligned}
&n_2 - 16 = p - 6L - 25 - 2(-1)^k,\\
&n_2' - 16 = p + 2L + 8M - 17 - 2(-1)^k,\\
&n_2'' - 16 = p + 2L - 17 - 2(-1)^k,\\
&n_2''' - 16 = p + 2L - 8M - 17 - 2(-1)^k,
\end{aligned}$$

pour le cas de $p = 8h' + 1$. Pour celui de $p = 8h' + 5$, il faudrait changer N_2 en N_2'', N_2' en N_2''', et réciproquement; puis introduire les

quantités n_2, n_2', n_2'', n_2''', ce qui donnerait

$$\begin{aligned}
n_2 - 16 &= p + 2L - 25 - 2(-1)^k,\\
n_2' - 16 &= p + 2L - 8M - 17 - 2(-1)^k,\\
n_2 - 16 &= p - 6L - 17 - 2(-1)^k,\\
n_2''' - 16 &= p + 2L + 8M - 17 - 2(-1)^k.
\end{aligned}$$

Celle des quatre quantités $n_2 - 16$, $n_2' - 16$, $n_2'' - 16$, $n_2''' - 16$, qui sera divisible par 32 fera connaître la classe du nombre 2.

1°. Soit $p = 8h' + 1$ ou h pair; comme 2 est résidu quadratique de p, il ne peut appartenir qu'à la classe des résidus bi-quadratiques, ou à la deuxième classe des non-résidus bi-quadratiques, puisque $2^{4h'} \equiv 1 \pmod{p}$ donne $2^{2h'} \equiv \pm 1 \pmod{p}$. C'est ce qui suit d'ailleurs des équations précédentes, en posant

$$p = 8h' + 1 = (1 + 4\lambda)^2 + 4M^2;$$

elles deviennent

$$n_2 - 16 = 16\left(\lambda^2 - \lambda - 2 + \frac{M^2}{4}\right), \quad n_2'' - 16 = 16\left(\lambda^2 + \lambda - 1 + \frac{M^2}{4}\right),$$

$$n_2' - 16 = 16\left(\lambda^2 + \lambda + \frac{M^2 + 2M}{4} - 1\right), \quad n_2 - 16 = 16\left(\lambda^2 + \lambda + \frac{M^2 - 2M}{2} - 1\right),$$

et comme M est nécessairement pair, et $M^2 \pm 2M$ ou $(M \pm 1)^2 - 1$, divisible par 8 et que d'ailleurs $\lambda^2 \pm \lambda$ est pair, aucun des nombres $n_2' - 16$, $n_2''' - 16$ ne sera divisible par 32, et un seul des nombres $n_2 - 16$, $n_2 - 16$ le sera. Savoir : le premier si M est divisible par 4, et le second si M est divisible seulement par 2.

2°. Soit $p = 4h + 1 = 8h' + 5$, ou h impair, le nombre 2 étant non-résidu quadratique de p, ne peut être que non-résidu bi-quadratique de première ou troisième classe. C'est aussi ce qu'on voit de suite par les valeurs de $n_2 - 16$, $n_2' - 16$, $n_2 - 16$, $n_2 - 16$, qui deviennent

$$n_2 - 16 = 16\left(\lambda^2 + \lambda - 1 + \frac{M^2 - 1}{4}\right), \quad n_2'' - 16 = 16\left(\lambda^2 + \lambda - 1 + \frac{M^2 - 1}{4}\right),$$

$$n_2' - 16 = 16\left[\lambda^2 + \lambda + \left(\frac{M+1}{2}\right)^2 - 1\right], \quad n_2''' - 16 = 16\left[\lambda^2 + \lambda + \left(\frac{M-1}{2}\right)^2 - 1\right].$$

Comme l'équation $p = 8h' + 5 = (1 + 4\lambda)^2 + 4M^2$, fait voir que M est impair, $n_2 - 16$ et $n_2'' - 16$ ne sauraient être divisibles par 32. Des deux quantités $n_2 - 16$ et $n_2''' - 16$, une seule sera divisible par 32; ce sera la première si $\frac{M+1}{2}$ est impair, et la seconde si $\frac{M-1}{2}$ est impair.

Il faut remarquer que les valeurs précédentes de N_2, N_2', N_2'' et N_2''', correspondent à la substitution

$$\begin{aligned}
1 + 4y_0 &= z_0 = \sqrt{p} + \sqrt{2p(-1)^h - 2L\sqrt{p}},\\
1 + 4y_2 &= z_2 = \sqrt{p} - \sqrt{2p(-1)^h - 2L\sqrt{p}},\\
1 + 4y_1 &= z_1 = -\sqrt{p} + \sqrt{2p(-1)^h + 2L\sqrt{p}},\\
1 + 4y_3 &= z_3 = -\sqrt{p} - \sqrt{2p(-1)^h + 2L\sqrt{p}}.
\end{aligned}$$

Le produit

$$\sqrt{2p(-1)^h - 2L\sqrt{p}} \times \sqrt{2p(-1)^h + 2L\sqrt{p}} = 4M\sqrt{p},$$

étant pris avec le signe +. C'est cette substitution qui servira à fixer l'ordre des classes de non-résidus. Cette nouvelle convention faite, nous aurons la proposition suivante :

« Théorème. Soit $p = 4h + 1 = L^2 + 4M^2$, le nombre 2 sera ré-
» sidu bi-quadratique pour $M \equiv 0 \pmod 4$, non-résidu bi-quadratique
» de seconde classe pour $M \equiv 2 \pmod 4$; non-résidu bi-quadratique
» de première classe pour $M \equiv -1 \pmod 4$, et non-résidu de
» troisième classe pour $M \equiv 1 \pmod 4$. »

Comme $L = 1 + 4\lambda$, on voit que ces conditions reviennent à $M \equiv 0$, $M \equiv 2L$, $M \equiv -L$, $M \equiv +L \pmod 4$.

Pour le cas général de $q = 2q' + 1$ nombre premier, on a

$$N_q \equiv n_q, \quad N_q' \equiv n_q', \quad N_q'' \equiv n_q'', \quad N_q''' \equiv n_q''' \pmod q,$$

et selon que des congruences

$$n_q \equiv 4, \quad n_q' \equiv 4, \quad n'' \equiv 4, \quad n_q''' \equiv 4 \pmod q,$$

la première, la seconde, la troisième ou la quatrième sera satisfaite,

le nombre q sera par rapport à p, résidu biquadratique, ou non-résidu de première, deuxième ou troisième classe.

Les équations (I) deviennent d'après cela

$$\left.\begin{aligned} 12p &\equiv z_1^{q+1} + z_1^{q+1} + z_2^{q+1} + z_3^{q+1} - (z_0^q + z_1^q + z_2^q + z_3^q),\\ 12p &\equiv z_1 z_0^q + z_2 z_1^q + z_3 z_2^q + z_0 z_3^q - (z_0^q + z_1^q + z_2^q + z_3^q),\\ 12p &\equiv z_2 z_0^q + z_3 z_1^q + z_0 z_2^q + z_1 z_3^q - (z_0^q + z_1^q + z_2^q + z_3^q),\\ 12p &\equiv z_3 z_0^q + z_0 z_1^q + z_1 z_2^q + z_2 z_3^q - (z_0^q + z_1^q + z_2^q + z_3^q), \end{aligned}\right\} \text{(mod. } q\text{)}.$$

Or, en posant pour abréger

$$R = 2p(-1)^h - 2L\sqrt{p}, \quad S = 2p(-1)^h + 2L\sqrt{p},$$

et par suite

$$RS = 4p(p - L^2) = 16pM^2, \quad \sqrt{RS} = 4M\sqrt{p},$$

on trouvera

$$\left.\begin{aligned} z_0^q &\equiv p^{q'}\sqrt{p} + R^{q'}\sqrt{R}, \quad & z_1^q &\equiv -p^{q'}\sqrt{p} + S^{q'}\sqrt{S}\\ z_2^q &\equiv p^{q'}\sqrt{p} - R^{q'}\sqrt{R}, \quad & z_3^q &\equiv -p^{q'}\sqrt{p} - S^{q'}\sqrt{S} \end{aligned}\right\} \text{(mod. } q\text{)},$$

ce qui donne

$$\left.\begin{aligned} z_0^q + z_1^q + z_2^q + z_3^q &\equiv 0 \text{ (mod. } q\text{)},\\ z_0^{q+1} + z_1^{q+1} + z_2^{q+1} + z_3^{q+1} &\equiv 4p^{q'+1} + 2(R^{q'+1} + S^{q'+1})\\ z_2 z_0^q + z_3 z_1^q + z_0 z_2^q + z_1 z_3^q &\equiv 4p^{q'+1} - 2(R^{q'+1} + S^{q'+1})\\ z_1 z_0^q + z_2 z_1^q + z_3 z_2^q + z_0 z_3^q &\equiv -4p^{q'+1} + 2(R^{q'} - S^{q'})\sqrt{RS}\\ z_3 z_0^q + z_0 z_1^q + z_1 z_2^q + z_2 z_3^q &\equiv -4p^{q'+1} - 2(R^{q'} - S^{q'})\sqrt{RS} \end{aligned}\right\} \text{(mod. } q\text{)},$$

et par conséquent, en ayant égard à la transposition relative au cas de h impair, on aura les congruences

$$\text{(M)} \quad \left\{\begin{aligned} 12p &\equiv 4p^{q'+1} + 2(-1)^h(R^{q'+1} + S^{q'+1})\\ 12p &\equiv -4p^{q'+1} - 2(-1)^h(S^{q'} - R^{q'})\sqrt{RS}\\ 12p &\equiv 4p^{q'+1} - 2(-1)^h(R^{q+1} + S^{q'+1})\\ 12p &\equiv -4p^{q'+1} + 2(-1)^h(S^{q'} - R^{q'})\sqrt{RS} \end{aligned}\right\} \text{(mod. } q\text{)};$$

et comme l'on a

$$\begin{aligned} R^{q'+1} + S^{q'+1} &= R^{q'}[2p(-1)^k - 2L\sqrt{p}] + S^{q'}[2p(-1)^k + 2L\sqrt{p} \\ &= 2p(-1)^k (R^{q'} + S^{q'}) + 2L\sqrt{p}(S^{q'} - R^{q'}), \end{aligned}$$

elles deviendront

$$(N) \left\{ \begin{array}{l} 1\,2p \equiv 4p^{q'+1} + 4p(R^{q'} + S^{q'}) + 4L\sqrt{p}(S^{q'} - R^{q'})(-1)^k \\ 1\,2p \equiv -4p^{q'+1} - 8M\sqrt{p}(S^{q'} - R^{q'})(-1)^k \\ 1\,2p \equiv 4p^{q'+1} - 4p(R^{q'} + S^{q'}) - 4L\sqrt{p}(S^{q'} - R^{q'})(-1)^k \\ 1\,2p \equiv -4p^{q+1} + 8M\sqrt{p}(S^{q'} - R^{q'})(-1)^k \end{array} \right\} (\text{mod. } q).$$

Soit maintenant

$$R^{q'} = \varphi - \Psi\sqrt{p}, \quad S^{q'} = \varphi + \Psi\sqrt{p},$$

d'où

$$R^{q'} + S^{q'} = 2\varphi, \quad S^{q'} - R^{q'} = 2\Psi\sqrt{p} :$$

en représentant par k_1, k_2, k_3... les coefficients binomiaux

$$\frac{q'}{1}, \quad \frac{q'.q'-1}{1.2}, \quad \frac{q'.q'-1.q'-2}{1.2.3}, \quad \text{etc.}$$

et en supposant

$$\begin{aligned} \varphi_1 &= p^{q'} + k_2 p^{q'-1} L^2 + k_4 p^{q'-2} L^4 + \ldots, \\ \Psi_1 &= k_1 p^{q'-1} + k_3 p^{q'-2} L^2 + k_5 p^{q'-3} L^4 + \ldots, \end{aligned}$$

on aura

$$\varphi = (-1)^{kq'} . 2^{q'} \varphi_1, \quad \Psi(-1)^k = (-1)^{kq'} . 2^{q'} \Psi_1,$$

et les congruences (N) deviendront, en divisant les deux membres, par $4p$,

$$(O) \left\{ \begin{array}{l} 3 \equiv p^{q'} + 2^{q'+1}(-1)^{kq'}(\varphi_1 + L^2\Psi_1) \\ 3 \equiv -p^{q'} - 2^{q'+2}(-1)^{kq'} . M\Psi L_1 \\ 3 \equiv p^{q'} - 2^{q'+1}(-1)^{kq'}(\varphi_1 + L^2\Psi_1) \\ 3 \equiv -p^{q'} + 2^{q'+2}(-1)^{kq'} LM\Psi_1 \end{array} \right\} (\text{mod. } q),$$

d'où L, M et p disparaîtront quand on posera

$$L \equiv Mz (\text{mod. } q).$$

Pour première application, cherchons quelle est la classe du nombre q, quand on a

$$M \equiv 0 \quad \text{ou} \quad L \equiv 0 \pmod{q}.$$

Comme l'équation $p = L^2 + 4M^2$

donne alors

$$p \equiv L^2 \quad \text{ou} \quad p \equiv 4M^2 \equiv (2M)^2 \pmod{q},$$

on a toujours $p^{q'} \equiv 1 \pmod{q}$.

Ainsi la deuxième et la quatrième des congruences (O) se réduisant à $4 \equiv 0 \pmod{q}$ sont impossibles. Le nombre q est donc résidu biquadratique, ou non-résidu biquadratique de deuxième classe. C'est ce que l'on distinguera au moyen de la première et de la troisième des congruences (O), qui deviennent

$$1 \equiv 2^{q'}(-1)^{hq'}(\varphi_1 + L^2\Psi_1), \quad 1 \equiv -2^{q'}(-1)^{hq'}(\varphi_1 + L^2\Psi_1) \pmod{q}.$$

1°. Soit d'abord $M \equiv 0 \pmod{q}$, il en résulte $L^2 \equiv p \pmod{q}$ et par conséquent

$$\left.\begin{aligned} \varphi_1 &= p^{q'}(1 + k_2 + k_4 + \ldots) \equiv 2^{q'-1}, \\ \psi_1 &= p^{q'}(k_1 + k_3 + k_5 + \ldots) \equiv 2^{q'-1}, \end{aligned}\right\} \pmod{q},$$

et par suite,

$$\varphi_1 + L^2\psi_1 \equiv 2^{q'} \pmod{q},$$

ce qui réduit la première et la troisième des congruences (O) à

$$1 \equiv (-1)^{hq'}, \quad 1 \equiv -(-1)^{hq'} \pmod{q}.$$

« Théorème. Soit $M \equiv 0 \pmod{q}$, on aura

» pour $p = 8h' + 1$ (h pair), q résidu biquadratique,
» pour $q = 4q'' + 1$ (q' pair), q résidu biquadratique,
» pour $p = 8h' + 5$ et $q = 4q'' - 1$ (ou h et q' impairs)

» q non-résidu biquadratique de seconde classe. »

2°. Soit $L \equiv 0 \pmod{q}$, il en résulte $\varphi_1 \equiv p^{q'} \equiv 1 \pmod{q}$, ce qui réduit la première et la troisième des congruences (0) à

$$1 \equiv 2^{q'}(-1)^{hq'}, \qquad 1 \equiv -2^{q'}(-1)^{hq'} \pmod{q}.$$

Comme l'on a $2^{q'} \equiv 1 \pmod{q}$ pour $q = 8q'' \pm 1$ et $2^{q'} \equiv -1 \pmod{q}$ pour $q = 8q'' \pm 3$, voici les conclusions à tirer :

« Théorème. Soit $L \equiv 0 \pmod{q}$, on aura

» pour $p = 8h' + 1$ et $q = 8q'' \pm 1$

» et pour $p = 8h' + 5$ et $q = 8q'' + 1$ ou $8q'' + 3$,

» le nombre p résidu bi-quadratique;

» pour $p = 8h' + 1$ et $q = 8q'' \pm 3$,

» et pour $p = 8h' + 5$ et $q = 8q'' + 5$ ou $q = 8q'' + 7$,

» le nombre q non-résidu biquadratique de seconde classe. »

Examinons le cas de $q = 2q' + 1 = 3$, d'où $q' = 1$. En posant

$L \equiv Mz \pmod{3}$, ce qui donne $p \equiv M^2(z^2 + 1) \pmod{3}$,

on trouve, en laissant de côté le cas de $M \equiv 0 \pmod{3}$,

$$\varphi_1 \equiv z^2 + 1 \pmod{3}, \quad L^2\downarrow_1 \equiv z^2 \pmod{3}, \quad LM\downarrow_1 \equiv z \pmod{3},$$

et les congruences (0) deviennent

$$\left.\begin{array}{ll} 1^{re}..3 \equiv z^2+1+(-1)^h(2z^2+1), & 2^e..3 \equiv -z^2-1+(-1)^h z \\ 3^e...3 \equiv z^2+1-(-1)^h(2z^2+1), & 4^e..3 \equiv -z^2-1-(-1)^h z \end{array}\right\} \pmod{3}.$$

Savoir pour h pair,

$1^{re}...0 \equiv 2 \pmod{3}$, impossible;

$2^e...0 \equiv -z^2 + z - 1 \pmod{3}$, solution $z = -1$;

$3^e....0 \equiv -z^2 \pmod{3}$, solution $z = 0$;

$4^e....0 \equiv -z^2 - z - 1 \pmod{3}$, solution $z = 1$;

et pour h impair,

$$\begin{aligned}
&1^{re}\ldots 0 \equiv -z^3 \pmod 3, \text{ solution } z = 0;\\
&2^{e}\ldots 0 \equiv -z^3 - z - 1 \pmod 3, \text{ solution } z = 1;\\
&3^{e}\ldots 0 \equiv 2 \pmod 3, \text{ impossible};\\
&4^{e}\ldots 0 \equiv -z^3 + z - 1 \pmod 3, \text{ solution } z = -1.
\end{aligned}$$

On aura donc la proposition suivante :

« Théorème. Le nombre 3 sera, en supposant $p = 8h' + 1$,
» résidu biquadratique pour $M \equiv 0 \pmod 3$,

» non-résidu biquadrat. de 1re classe pour $L \equiv -M \pmod 3$,
» non-résidu biquadrat. de 2e classe pour $L \equiv 0$ *idem*,
» non-résidu biquadrat. de 3e classe pour $L \equiv M$ *idem*,

» Si l'on suppose au contraire $p = 8h' + 5$, alors 3 sera

» résidu biquadratique de p pour $L \equiv 0 \pmod 3$,
» non-résidu biquadrat. de 1re classe pour $L \equiv M$ *idem*,
» non-résidu biquadrat. de 2e classe pour $M \equiv 0$ *idem*,
» non-résidu biquadrat. de 3e classe pour $L \equiv M$ *idem*. »

Soit encore

$$q = 2q' + 1 = 5, \quad q' = 2, \quad L \equiv Mz \pmod 5,$$

et

$$p \equiv M^4(z^4 - 1) \pmod 5,$$

il en résultera

$$\varphi_1 \equiv (z^4-1)^4 + (z^4-1)z^4,\ L^4\downarrow_1 \equiv 2(z^4-1)z^4,\ LM\downarrow_1 \equiv 2(z^4-1)z \pmod 5,$$

ou bien en laissant de côté le cas de $M \equiv 0 \pmod 5$ et celui de $z = 0$, ou $L \equiv 0 \pmod 5$, c'est-à-dire en supposant $z^4 \equiv 1 \pmod 5$, on aura plus simplement

$$\varphi_1 \equiv 2z^4 - 2, \quad L^4\downarrow_1 \equiv 2 - 2z^4, \quad LM\downarrow_1 \equiv 2z^3 - 2z \pmod 5,$$

et par conséquent les congruences (0) deviendront

$$\begin{aligned}
&1^{re}\ldots\ 1 \equiv -2z^3 \pmod 5 \text{ impossible},\\
&2^{e}\ldots\ 0 \equiv z^3 - z(z^4 - 1) \pmod 5 \text{ solution } z = -2,
\end{aligned}$$

$3^e \ldots\ 1 \equiv -2z^2 \pmod 5$ impossible,
$4^e \ldots\ 0 \equiv z^2 + 2(z^2 - 1) \pmod 5$ solution $z = +2$.

De là le théorème qui suit

« Théorème. Pour le nombre $p = 4h + 1$, le nombre 5 est résidu
» biquadratique pour $M \equiv 0 \pmod 5$,
» non-résidu biquadrat. de 1re classe pour $L \equiv 2M$ *idem*,
» non-résidu biquadrat. de 2e classe. pour $L \equiv 0$ *idem*,
» non-résidu biquadrat. de 3e classe pour $L \equiv 2M$ *idem*. »

On voit que pour ce cas de $p=5$, il n'est pas nécessaire d'examiner séparément le cas de $p = 8h' + 1$ et celui de $p = 8h' + 5$. Il en est de même toutes les fois que q a la forme $4q'' + 1$, parce que le facteur $(-1)^{hq'}$ se réduit à 1, quel que soit p.

Si l'on traite semblablement les cas de $p = 7, = 11, = 13$, etc., on formera facilement une table semblable à celle concernant les résidus cubiques. Mais ces calculs pourront s'abréger au moyen des propositions suivantes, qui sont des lois de réciprocité.

Reprenons les congruences (N) en laissant de côté le cas de $M \equiv 0 \pmod q$, qui exige qu'on ait $R \equiv 0$ ou $S \equiv 0 \pmod q$, à cause de $RS = 16pM^2$.

Soit d'abord q résidu quadratique de p, comme p est de forme $4h + 1$, il en résultera p résidu quadratique de q. Ainsi les quantités R et S données par la formule $2p(-1)^h \pm 2L\sqrt{p}$ seront des nombres réels, tous deux résidus ou non-résidus quadratiques de q, à cause de $RS = 16pM^2$. Pour les obtenir, il suffira de résoudre la congruence $z^2 \equiv p \pmod q$.

Puisque l'on a

$$p^{q'} \equiv 1 \quad \text{et} \quad R^{q'} \equiv S^{q'} \equiv \pm 1 \pmod q,$$

les congruences (N) deviendront

$$2 \equiv \pm 2, \quad 16 \equiv 0, \quad 2 \equiv \pm 2, \quad 16 \equiv 0 \pmod q,$$

d'où l'on voit, comme on le savait déjà, que q ne peut être que résidu biquadratique, ou non-résidu biquadratique de seconde classe, ce que l'on distingue ainsi :

« Théorème. Le nombre premier q résidu quadratique du nombre » premier $p = 4h + 1 = L^2 + 4M^2$, en sera aussi résidu biquadra- » tique si l'on a $2p(-1)^k \equiv 2L\sqrt{p} \pmod{q}$ résidus quadratiques de q. » Dans le cas contraire, q sera non-résidu biquadratique de 2e classe. »

Ce théorème a beaucoup d'analogie avec un théorème de M. Dirichlet, et qui se déduit facilement du précédent, ainsi que nous le montrerons plus bas.

Au moyen du théorème précédent, il est facile de former les valeurs de z qui satisfont aux congruences conditionnelles (O). On posera

$$p \equiv \gamma^2 L^2 \pmod{q},$$

il faudra avoir, par conséquent,

$$2(\gamma^2 - \gamma)(-1)^k \quad \text{et} \quad 2(\gamma^2 + \gamma)(-1)^k,$$

résidus quadratiques de q. L'équation $p = L^2 + 4M^2$ donnera

$$M \equiv \pm L\sqrt{\frac{\gamma^2 - 1}{4}} \equiv \pm zL \pmod{q},$$

en supposant

$$\gamma^2 \equiv 4z^2 + 1 \pmod{q}.$$

La congruence précédente pourra être réduite à $L \equiv \pm z'M$, en posant $zz' \equiv \pm 1 \pmod{q}$. Comme l'on a $4(\gamma^4 - \gamma^2) \equiv 16\gamma^2 z^2 \pmod{q}$, il suffira donc de satisfaire à la congruence $\gamma^2 \equiv 4z^2 + 1 \pmod{q}$, en rendant de plus $2(\gamma^2 - \gamma)(-1)^k$ résidu quadratique de q. Ainsi il faudra faire

$$\gamma^2 - \gamma \text{ résidu quadratique de } q,$$

1°. pour $p = 8h' + 1$ et $q = 8q'' \pm 1$;
2°. pour $p = 8h' + 5$ et $q = 8q'' + 1$ ou $8q'' + 3$;

$$\text{et } \gamma^2 - \gamma \text{ non-résidu quadratique de } \gamma,$$

1°. pour $p = 8h' + 1$ et $q = 8q'' \pm 3$;
2°. pour $p = 8h' + 5$ et $q = 8q'' + 5$ ou $8q'' +$

Voici un exemple de ce calcul pour $p=8h'+1$ et $q=13=8+5$. Il faut avoir ici y^2-y non-résidu quadratique de 13,

Valeurs de z,	1,	2,	3,	4,	5,	6,
de z^2,	1,	4,	−4,	3,	−1,	−3,
de $y^2=4z^2+1$,	5,	4,	−2,	0,	−3,	2,
de y		2,		0,	6,	
de y^2-y,		2*		0,	4.	

Le nombre 2, valeur de y^2-y étant non-résidu quadratique de 13, on aura donc $M\equiv\pm 2L \pmod{13}$, ou bien $L\equiv\pm 6M \pmod{13}$, c'est cette dernière qui sera employée dans les tables.

On formerait tout-à-fait de la même manière les congruences $L\equiv\pm zM \pmod{q}$ relatives au cas du nombre q non-résidu biquadratique de seconde classe relativement à p. Il faut alors avoir $2(y^2-y)(-1)^h$ non-résidu quadratique de q. Donc dans le cas de l'exemple précédent, au lieu de considérer la valeur de y^2-y qui est non-résidu quadratique de 13, il faudra prendre celle qui est résidu quadratique, c'est-à-dire 4, d'où résulte

$$M\equiv\pm 5L \pmod{13} \text{ ou } L\equiv\pm 5M \pmod{13}.$$

Quant à la valeur $y^2-y\equiv 0$, elle répond au cas de $M\equiv 0 \pmod{13}$, si $y=1$; si $y=0$, elle répond au cas de q résidu biquadratique puisqu'on a $R\equiv S\equiv 0 \pmod{q}$.

Le théorème de M. Dirichlet, cité plus haut, revient à ceci :

« Soit $p=L^2+4M^2$, si L est divisible par q, le nombre » $\pm q=4q''+1$ sera résidu biquadratique ou non-résidu biquadra- » tique de seconde classe, selon que $\pm q$ sera de forme $8m+1$ ou » $8m+5$. Si L n'est pas divisible par q, le nombre $\pm q$ sera résidu » biquadratique de seconde classe, selon que $p\pm 2M\sqrt{p}$ seront » résidus ou non-résidus quadratiques de q. ($\pm q$ est supposé résidu » quadratique de p.)

Après avoir démontré le théorème précédent, M. Dirichlet ajoute : « On a sans doute remarqué que les énoncés des théorèmes I et II » (donnés plus haut en un seul) sont tels qu'il n'y entre que la racine » du carré impair que l'on obtient en décomposant p en deux carrés.

» Il serait facile de modifier ces énoncés de manière à ce qu'ils ne » renfermassent plus que la racine du carré impair. On y parvien- » drait en suivant une marche entièrement semblable à celle que nous » avons exposée dans ce qui précède. »

On retomberait alors sur le théorème précédemment démontré. Au reste, voici la manière d'obtenir le théorème de M. Dirichlet. D'abord la partie relative à L divisible par q, a été démontrée plus haut. Quant à la seconde partie, soit $\theta^2 \equiv p \pmod{q}$ ou bien $\theta^2 \equiv L^2 + 4M^2 \pmod{q}$. On aura

$$(\theta+L+2M)^2 \equiv 2[\theta^2+\theta(L+2M)+2LM] \equiv 2(\theta+L)(\theta+2M) \pmod{q}.$$

Ainsi $2(\theta+L)$ et $(\theta+2M)$ sont à la fois résidus quadratiques, ou non-résidus quadratiques de q, et comme l'on a $\theta^2 - L^2 \equiv 4M^2$, $\theta^2 - 4M^2 \equiv L^2 \pmod{q}$, il en sera de même de $2(\theta-L)$ et $(\theta-2M)$. Ainsi en multipliant chaque nombre par θ, on aura $2(\theta^2 \pm L\theta)$ et $(\theta^2 \pm 2M\theta)$ ou bien encore $2p \pm 2L\sqrt{p}$ et $p \pm 2M\sqrt{p} \pmod{q}$, à la fois résidus ou non-résidus quadratiques de q.

1°. Soit h pair ou $p = 8h' + 1$, les nombres $+q$ et $-q$ sont de la même classe et comme $(-1)^{\frac{1}{4}} = 1$, on voit que

$$2p(-1)^{\frac{1}{4}} + 2L\sqrt{p} \pmod{q} \quad \text{et} \quad p + 2M\sqrt{p} \pmod{q}$$

sont à la fois résidus quadratiques ou non-résidus quadratiques de q. D'où suit immédiatement le théorème de M. Dirichlet.

2°. Soit h impair, ou $p = 4h + 1 = 8h' + 5$; pour ce cas l'on a

$$-[2p(-1)^{\frac{1}{4}} + 2L\sqrt{p}] \quad \text{et} \quad p + 2M\sqrt{p} \pmod{q}$$

tous deux résidus ou tous deux non-résidus quadratiques de q. Si l'on a $q = 4q'' + 1$, on pourra changer le signe de la première quantité, et l'on retombera sur

$$2p(-1)^{\frac{1}{4}} + 2L\sqrt{p} \quad \text{et} \quad p + 2M\sqrt{p} \pmod{q},$$

tous deux résidus ou non-résidus quadratiques de q, d'où le théorème de M. Dirichlet.

3°. Soit enfin h impair et $q = 4q'' - 1$, comme q et $-q$ sont de classes différentes, pour appliquer la règle à $-q$, il faudra rem-

placer $-[2p(-1)^k+2L\sqrt{p}]$ par $+[2p(-1)^k+2L\sqrt{p}]$ et l'on voit encore que les quantités

$$2p(-1)^k+2L\sqrt{p} \quad \text{et} \quad p+2M\sqrt{p} \pmod{q}$$

sont toutes deux résidus quadratiques ou toutes deux non-résidus quadratiques de q : on aura donc le théorème de M. Dirichlet, dans sa dernière partie qui s'applique à $-(4q''-1)=-4q''+1=-q$.

Soit maintenant q non-résidu quadratique de p et par suite p non-résidu quadratique de q. Les quantités R et S ou $2p(-1)^k \pm 2L\sqrt{p}$ (mod. q) sont donc imaginaires. Il faudra, dans ce cas, considérer les congruences (M). Comme $q=2q'+1$ est nécessairement non-résidu biquadratique de première ou troisième classe, elles doivent aussi le faire voir. Or c'est ce qui arrive, car puisque $p^{q'} \equiv -1 \pmod{q}$, en développant $[2p(-1)^k - 2L\sqrt{p}]^{q+1} = R^{q+1}$ et ne conservant que les deux premiers et les deux derniers termes, tous les autres étant des multiples de q, on trouvera facilement $R^{q+1} \equiv 16pM^2 \pmod{q}$. De plus $(RS)^{\frac{q+1}{2}} = (16pM^2)^{\frac{q+1}{2}} \equiv -16pM^2 \pmod{q}$, donc..... $R^{\frac{q+1}{2}}(R^{\frac{q+1}{2}}+S^{\frac{q+1}{2}}) \equiv 0 \pmod{q}$ et par conséquent $R^{\frac{q+1}{2}}+S^{\frac{q+1}{2}} \equiv 0 \pmod{q}$, en laissant de côté le cas de $R \equiv 0 \pmod{q}$. D'après cela les première et troisième des congruences (M) deviennent $16p \equiv 0 \pmod{q}$. donc elles ne sont jamais satisfaites. Les deuxième et quatrième congruences (M) se réduisent à

$$8p \equiv -2(-)^k(S^{q'}-R^{q'})\sqrt{RS}, \quad 8p \equiv +2(-1)^k(S^{q'}-R^{q'})\sqrt{RS} \pmod{q},$$

dont l'une est nécessairement satisfaite. Car $R^{q'+1}+S^{q'+1} \equiv 0 \pmod{q}$ donne $R^{q'} \equiv -S^{q'}\frac{S}{R}$ et $\frac{R^{q'}}{S^{q'}} \equiv -\frac{S}{R} \pmod{q}$, de là $S^{q'}-R^{q'} \equiv S^{q'}\frac{S+R}{R}$ $\equiv Lp(-1)^k . RS^{q'}$: donc $(S^{q'}-R^{q'})\sqrt{RS} \equiv 4p(-1)^k S^{q'}\sqrt{\frac{S}{R}} \equiv 4p(-1)^{kq'}$ $\sqrt{-\frac{R^{q'}}{S^{q'}}} \equiv 4p(-1)^k\sqrt{-R^{q'}.S^{q'}} \pmod{q}$; ou bien, à cause de $R^{q'}.S^{q'} \equiv (16pM^2)^{q'} \equiv p^{q'} \equiv -1 \pmod{q}$, $(S^{q'}-R^{q'})\sqrt{RS} \equiv \pm 4p(-1)^k \pmod{q}$. On a par conséquent $8p \equiv \mp 8p$, et $8p \equiv \pm 8p \pmod{q}$

pour les congruences deuxième et quatrième du système (M), de sorte que l'une d'elles est satisfaite et l'autre non.

D'après ce qui a été dit dans l'article I du § IV, sur les racines imaginaires de la congruence $x^{q+1} \equiv 1 \pmod{q}$, on voit que parmi les racines $f+g\sqrt{p} \pmod{q}$ satisfaisant à la condition $f^2-pg^2 \equiv 1 \pmod{q}$, les non-résidus biquadratiques satisfont à la congruence..... $x^{\frac{q+1}{2}}+1 \equiv 0 \pmod{q}$. Or la condition $R^{q'+1}+S^{q'+1} \equiv 0 \pmod{q}$ revient à

$$1+\left(\frac{R}{S}\right)^{\frac{q+1}{2}} \equiv 0 \text{ ou } 1+\left(\frac{S}{R}\right)^{\frac{q+1}{2}} \equiv 0 \pmod{q}.$$

Par conséquent les expressions

$$\frac{2p(-1)^h-2L\sqrt{p}}{2p(-1)^h+2L\sqrt{p}} \quad \text{et} \quad \frac{2p(-1)^h+2L\sqrt{p}}{2p(-1)^h-2L\sqrt{p}} \pmod{q}$$

sont des non-résidus quadratiques imaginaires de q. Soit donc $f+g\sqrt{p} \pmod{q}$ un de ces non-résidus, on écrira

$$\frac{2p(-1)^h-2L\sqrt{p}}{2p(-1)^h+2L\sqrt{p}} \equiv f+g\sqrt{p} \pmod{q},$$

ce qui donnera les deux congruences

$$L \equiv \frac{(1-f)(-1)^h}{g}, \quad L \equiv \frac{-pg(-1)^h}{1+f} \pmod{q},$$

qui s'accordent parce que l'on a $f^2-pg^2 \equiv 1 \pmod{q}$. Au moyen de l'équation $p=L^2+4M^2$, on en déduira facilement

$$L \equiv \pm \sqrt{2(f-1)}.M \equiv Mz. \pmod{q},$$

où z est réel d'après ce qui a été dit dans l'article des racines imaginaires.

Le changement de signe de L, qui répond à celui de q, n'apprendrait rien de plus, et ce qui précède ne donne point le moyen de séparer les valeurs de z, relatives au cas pour lequel q est un non-

résidu biquadratique de première classe de celui pour lequel q est un non-résidu biquadratique de troisième classe. Tout ce que l'on peut voir, c'est que les valeurs de z relatives à ces deux cas ne diffèrent que par le signe. Il faudra donc pour former les tables analogues à celles de l'article précédent, employer les congruences (O), et c'est peut-être même ce qu'il y a de plus simple à faire, d'autant plus qu'il suffit de considérer un petit nombre de valeurs de q. Par exemple, 2, 5, 7, 11, 13.

Voici les deux petites tables pour les modules premiers, moindres que 100.

TABLE I.

$$p = L^2 + 4M^2, \quad L = 1 + 4\lambda, \quad L \equiv Mz \pmod{q}.$$

$p =$	5,	13,	17,	29,	37,	41,	53,	61,	73,	89,	97,
$L =$	1,	— 3,	1,	5,	1,	5,	— 7,	5,	3,	5,	— 9,
$M =$	1,	1,	2,	1,	3,	2,	1,	3,	4,	4,	2,

Valeurs de z.

q									
3,	1,	0,	— 1,	— 1,	∞,	1,	— 1,	∞,	0,	— 1,	0,
5,	1,	2,	— 2,	0,	2,	0,	— 2,	0,	— 2,	0,	— 2,
7,	1,	3,	— 3,	— 2,	— 2,	— 1,	0,	— 3,	1,	3,	— 1,
11,	1,	3,	— 5,	5,	4,	— 3,	4,	— 2,	2,	4,	1,
13,	1,	3,	— 6,	5,	— 4,	— 4,	6,	6,	— 4,	— 2,	2.

etc.

Caract. des résidus biquadratiques.

3.... ∞ : (0),
5.... ∞,
7.... ∞, 0 : ($\pm$ 2),
11.... ∞, $\pm$ 4 : (0, $\pm$ 1),
13.... ∞, $\pm$ 6,
etc.

Caract. des non-résidus biquadratiq. de 1re classe.

3.... — : 1 (+ 1),
5.... — 2,
7.... 1, 3 : (— 1, — 3),
11.... 2, 3, 5 : (2, —3, —5),
13.... 1, 2, 4,
etc.

Remarques. — 1°. L'analogie porte à conclure que le nombre des valeurs de z pour chaque classe de nombres est $\frac{q \mp 1}{4}$ en posant

$q = 4q' \pm 1$. Pour le prouver, il faudrait distinguer plusieurs cas. Pour plusieurs la démonstration se présente immédiatement. Les autres paraissent exiger quelques recherches préliminaires dont nous ne nous occuperons pas ici.

2°. Selon que l'on a $M \equiv 0$, $M \equiv -1$, $M \equiv 2$ ou $M \equiv 1 \pmod 4$. Le nombre 2 est résidu bi-quadratique ou non résidu de première, deuxième ou troisième classe.

3°. Les valeurs de z entre parenthèses se rapportent au cas de $p = 8h' + 5$, et les autres au cas de $p = 8h' + 1$.

4°. En changeant le signe des valeurs de z relatives aux non-résidus de première classe, on a celles relatives aux non-résidus biquadratiques de troisième classe.

5°. L'exclusion donnera les valeurs de z relatives aux cas des non-résidus de deuxième classe (en supposant prouvé le théorème énoncé dans la première remarque).

Il faut remarquer que l'équation $p = L^2 + 4M^2$ donnant la valeur de z, il suffit de savoir qu'elle ne satisfait pas à trois des congruences, pour conclure qu'elle doit satisfaire à la quatrième.

6°. L'usage de cette table est tout-à-fait semblable à celui de la table de l'article précédent. Il faut remarquer ici que dans les nombres composés $\pm 2a^\alpha b^\beta c^\gamma, \ldots$ il ne faut pas négliger le facteur -1. Le nombre -1 est résidu biquadratique pour $p = 8h' + 1$ et non-résidu biquadratique de deuxième classe pour $p = 8h' + 5$.

Au moyen de la table précédente, on formera très promptement la suivante qui est d'un usage plus commode. Les chiffres 0, 1, 2, 3 indiquent que les facteurs premiers q (y compris -1 et 2) sont résidus biquadratiques ou non-résidus de première, deuxième ou troisième classe.

TABLE II.

p	— 1, 2, 3, 5, 7	11, 13, 17, 19, 23	29, 31, 37, 41, 43, 47.
5	2, 3,		
13	2, 3, 0, 3, 3		
17	0, 2, 1, 1, 3		
29	2, 3, 3, 2, 0	3, 2	
37	2, 1, 2, 3, 0	2, 3, 3	
41	0, 2, 3, 2, 3	3, 3, 1, 1	
53	2, 3, 3, 1, 2	2, 0, 2, 3, 1	
61	2, 1, 2, 2, 1	3, 0, 3, 2, 1	3
73	0, 0, 2, 1, 1	3, 3, 1, 2, 2	3, 3
89	0, 0, 1, 2, 1	0, 3, 2, 3, 1	3, 3, 3, 1, 2
97	0, 2, 2, 1, 3	2, 1, 1, 1, 1	1, 2, 3, 1, 0, 0.

Exemple. Quelle est la classe de 91 pour le module 97^2.

Solution. On a $91 \equiv -6 \equiv -1.2.3 \pmod{97}$.

La classe du facteur — 1 est marquée par le nombre . . . 0
Celle du facteur 2 est la. . . . . 2^2
Celle du facteur 3 est la. . . . . 2^2
La somme est. . . . . 4.

Multiple de 4, donc 91 est un résidu bi-quadratique. En effet, l'on a $11^4 \equiv 91 \pmod{97}$.

II.

Comment l'équation $bp = T^2 \pm aU^2$ *fait voir si le nombre quelconque a, résidu quadratique du nombre premier* $p = 4h + 1$, *est résidu ou non-résidu bi-quadratique du même nombre.*

On voit par l'article précédent que c'est par la forme des nombres L et M de l'équation $p = L^2 + 4M^2$, que l'on peut distinguer si un nombre donné, est résidu ou non-résidu bi-quadratique d'un nombre premier donné $p = 4h + 1$. Cette équation $p = L^2 + 4M^2$, n'est pas la seule qui puisse servir au même objet. M. Dirichlet a employé

dans le mémoire cité plus haut, l'équation $ps^2 = T^2 \pm aU^2$ en supposant $\pm a = 4k + 1$ et premier. Le théorème de M. Dirichlet est un cas particulier d'un autre plus général que nous allons donner, après avoir rappelé quelques propositions connues.

On sait que tous les nombres premiers diviseurs de $x^2 - Am^2$, où A est sans diviseur carré, sont compris dans certaines formules $Az+r$ ou $4Az + r$, et que les nombres premiers qui ne peuvent diviser $x^2 - Am^2$, ou pour abréger les non-diviseurs de $x^2 - Am^2$, sont compris dans d'autres formules $Az + n$ ou $4Az + n$. On a donc des formules de *diviseurs* et des formules de *non-diviseurs*. On trouve les premières dans les tables III — VII de la théorie des nombres de Legendre, sous le nom de *diviseurs linéaires impairs*.

Quand un nombre composé impair est contenu dans une forme de non-diviseurs, il est par là même non-diviseur; car il contient nécessairement un nombre impair de facteurs premiers non-diviseurs. Quand un nombre composé impair est contenu dans une forme de diviseurs, il y a parmi ses facteurs premiers un nombre pair de non-diviseurs, ou bien il n'y en a aucun. On ne peut donc conclure qu'il soit diviseur. (V. *Rech. Arith.* de M. Gauss, sect. IV.)

Pour ne pas multiplier les énoncés nous ferons les conventions suivantes. Dans l'équation $bp = T^2 \pm aU^2$, nous supposerons T et U premiers entre eux, nous représenterons par t et u leurs plus grands diviseurs impairs, et par 2^m la plus haute puissance de 2 qui divise celui des deux nombres T, U qui est pair. D'ailleurs nous supposerons toujours $\mp a$ résidu quadratique du nombre premier $p = 4h+1$, sans quoi l'équation $bp = T^2 \pm aU^2$ serait impossible. Mais le nombre a sera quelconque, premier ou composé, et c'est en cela, aussi bien que dans l'indétermination du nombre b, que consiste la généralisation du théorème. Cela posé, nous dirons que la solution de l'équation $bp = T^2 \pm aU^2$ est de *première espèce* dans les cas suivants :

1°. $p = 8h' + 1$ quel que soit m et le signe de a;
2°. $p = 8h' + 5$ et m impair avec $+a$,
ou $p = 8h' + 5$ et m pair avec $-a$.

Et au contraire que la solution est de *seconde espèce* dans le cas suivant :

3°. $p = 8h' + 5$ et m impair avec $-a$;
ou $p = 8h' + 5$ et m pair avec $+a$.
Ceci convenu on a le théorème suivant :

« THÉORÈME I. Soit p un nombre premier de forme $4h+1$, ayant » $\mp a$ pour résidu quadratique. Pour les solutions de première es- » pèce de l'équation $bp = T^2 \pm aU^2$, a sera résidu bi-quadratique » de p dans les deux cas suivants :

» 1°. u étant dans les formes de diviseurs de $x^2 - b$, et t dans » les formes de diviseurs de $x^2 \mp ab$, ou 2°. u étant dans les » formes de non-diviseurs de $x^2 - b$, et t dans les formes de non- » diviseurs de $x^2 \mp ab$, c'est-à-dire quand u et t seront contenus » dans des formules de même espèce, de diviseurs ou de non-divi- » seurs.

» Au contraire a sera non-résidu bi-quadratique, quand u et t » seront compris dans des formules d'espèce différente ; t par exem- » ple étant dans les formes de diviseurs de $x^2 \pm ab$, et u dans les » formes de non-diviseurs de $x^2 - b$.

» Quand la solution sera de seconde espèce, il suffira de renver- » ser la conclusion. Le nombre a sera résidu bi-quadratique de p, » si u et t sont l'un dans les formes de diviseurs et l'autre dans les » formes de non-diviseurs de $x^2 - b$ et $x^2 \mp ab$ respectivement. » Dans le cas contraire a sera non-résidu biquadratique de p. »

Démonstration I De l'équation $bp = T^2 \pm aU^2$, l'on tire $aU^4 \equiv \mp U^2T^2 \pmod{p}$, et par conséquent en élevant à la puissance $\frac{p-1}{4}$ et remarquant que l'on a $U^{p-1} \equiv 1 \pmod{p}$, il viendra $a^{\frac{p-1}{4}} \equiv (\mp 1)^{\frac{p-1}{4}} (UT)^{\frac{p-1}{2}} \equiv (\mp 1)^{\frac{p-1}{4}} (2^{\frac{p-1}{2}})^m (ut)^{\frac{p-1}{2}} \pmod{p}$; savoir : pour les solutions de première espèce $a^{\frac{p-1}{4}} \equiv (ut)^{\frac{p-1}{2}} \pmod{p}$, et pour celles de deuxième espèce $a^{\frac{p-1}{4}} \equiv -(ut)^{\frac{p-1}{2}} \pmod{p}$. Comme $(ut)^{\frac{p-1}{2}} \pmod{p}$, est nécessairement congru à $+1$ ou -1 et que pour $a^{\frac{p-1}{4}} \equiv 1 \pmod{q}$, a est résidu bi-quadratique, tandis qu'il est non-résidu pour $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$, le premier cas aura donc lieu

quand t et u seront tous deux résidus quadratiques de p, ou tous deux non-résidus, en supposant la solution de première espèce. Mais pour les solutions de seconde espèce, on devra avoir au contraire l'un des nombres t, u résidu quadratique de p, et l'autre non-résidu. Pour exprimer que a doit être non-résidu biquadratique, il suffira de renverser les conclusions.

II. L'équation $T^s - pb = \mp aU^s$ montre que out diviseur premier impair de u, le nombre v par exemple, est diviseur de $T^s - pb$, c'est-à-dire que pb sera résidu quadratique de v, il faudra donc avoir simultanément b résidu quadratique de v, p résidu de v et alors v est dans les formes de diviseurs de $x^s - b$ et de $x^s - p$; ou bien b non-résidu quadratique de v et p, aussi non-résidu quadratique de v, et alors v serait dans les formes de non-diviseurs de $x^s - b$ et de $x^s - p$.

De même comme l'on a $(aU)^s \mp abp = \mp aT^s$, en représentant par θ un diviseur premier impair de T, on verra que θ est compris dans les formes de diviseurs de $x^s \mp ab$ et de $x^s - p$; ou bien dans les formes de non-diviseurs des mêmes quantités.

III. Or pour les solutions de première espèce, quand a sera résidu biquadratique, on devra avoir t et u résidus quadratiques de p, ou bien t et u non-résidus quadratiques de p. Dans le premier cas u devra contenir un nombre pair de facteurs non-résidus quadratiques de p. Par la loi de réciprocité p sera non-résidu quadratique de ces facteurs et résidu des autres, il y a donc dans u un nombre pair de facteurs non-diviseurs de $x^s - p$, ainsi u est dans les formes de diviseurs de $x^s - p$, par conséquent d'après (II), u sera aussi dans les formes de diviseurs de $x^s - b$. On prouvera semblablement que t est dans les formes de diviseurs de $x^s - p$ et par suite dans les formes de diviseurs de $x^s \mp ab$. Quand t et u seront tous deux non-résidus quadratiques de p, il s'ensuivra pareillement que t et u seront dans les formes de non-diviseurs de $x^s - p$, et d'après (II), t et u seront par conséquent aussi dans les formes de non-diviseurs de $x^s \mp ab$ et $x^s - b$ respectivement.

Pour les solutions de seconde espèce, on verra par un raisonnement tout-à-fait semblable que l'un des nombres t et u est dans les

formes de diviseurs de $x^2 - p$, et l'autre dans les formes de non-diviseurs. Donc d'après (II) t et u seront, l'un dans les formes de diviseurs, et l'autre dans les formes de non-diviseurs de $x^2 \mp ab$ et $x^2 - b$ respectivement.

Remarque. Quand b est un carré, le théorème se simplifie, car alors u est toujours dans les formes de diviseurs de $x^2 - b$; on a donc le théorème suivant.

« THÉORÈME II. Ayant l'équation $c^2 p = T^2 \pm aU^2$, pour les solu-
» tions de première espèce, a sera résidu ou non-résidu quadratique
» de p, selon que t sera dans les formes de diviseurs ou de non-
» diviseurs de $x^2 \mp a$. Pour les solutions de deuxième espèce, ce
» sera le contraire. »

Si a est premier, le théorème se simplifie encore, et fournit les deux suivants qui renferment le théorème de M. Dirichlet.

« THÉORÈME III. Soit $c^2 p = T^2 \pm aU^2$, en supposant $\pm a = 4k + 1$
» premier, pour les solutions de première espèce, a sera résidu ou
» non-résidu biquadratique de p, selon que t sera résidu ou non-
» résidu quadratique de p. — Pour les solutions de deuxième espèce,
» ce sera le contraire. »

» THÉORÈME IV. Si $\pm a = 4k + 3$, la même conclusion a encore
» lieu si t est de forme $4t' + 1$, mais il faudra prendre la conclusion
» opposée, si t est de forme $4t' + 3$. »

Cette dernière simplification résulte de ces propositions connues :

Quand A est un nombre premier dont les résidus quadratiques sont r, r', r'', etc., et les non-résidus n, n', n'', etc., les formes de diviseurs et de non-diviseurs se trouvent ainsi qu'il suit,

Soit $\pm A = 4A' + 1$; les diviseurs de $x^2 - (\pm A)$ sont contenus dans $Az + r$, $Az + r'$, $Az + r''$, ... et les non-diviseurs dans $Az + n$, $Az + n'$, $Az + n''$, etc....

Soit $\pm A = 4A' + 3$; la même chose aura encore lieu pour les diviseurs $4k+1$; pour ceux $4k+3$, ce sera précisément le contraire.

Voici quelques applications.

Les formes de diviseurs de $x^2 - 2$ étant $8k \pm 1$ et celles de $x^2 + 2$

étant $8k+1$ et $8k+3$, le th. II donne les deux suivants relatifs au nombre 2 : l'un est de M. Gauss et l'autre de M. Dirichlet.

« Théorème. Si p est un nombre premier de forme $8h'+1$ et » qu'on pose $p = T^2 + 2U^2$, ce qui est toujours possible ; on aura » 2 résidu biquadratique de p, si T est de forme $8k \pm 1$; au con- » traire 2 sera non-résidu biquadratique, si T est de forme $8k \pm 3$. »

« Théorème. Si l'on a dans le même cas $p = T^2 - 2U^2$, ce qui est » toujours possible ; 2 sera résidu biquadratique de p, si T est de » forme $8k+1$ ou $8k+3$, et non-résidu biquadratique dans le cas » contraire. »

Les nombres premiers de forme $4q+1$, qui ont 3 pour résidu quadratique, sont de forme $12q+1$; pour ces nombres on a la proposition qui suit :

« Théorème. Soit $p = T^2 + 3U^2$, p étant de forme $12q+1$, 3 » sera résidu biquadratique de p, si T est de forme $12k \pm 1$, et non- » résidu dans le cas contraire. »

C'est une conséquence du th. II, et de ce que les formes de diviseurs de $x^2 - 3$ sont $12k \pm 1$. Il en est de même des suivants.

« Théorème. Si p est un nombre de forme $4q+1$, ayant 5 pour » résidu quadratique, c'est-à-dire de forme $20n+1$ et $20n+9$, on » pourra toujours poser $p = T^2 + 5U^2$; le nombre 5 sera résidu biqua- » dratique si T est de forme $20n \pm 1$, $20n \pm 9$. Dans le cas con- » traire 5 sera non-résidu biquadratique. Ceci suppose la solution » de première espèce, c'est le contraire qui a lieu si elle est de » deuxième. »

« Théorème. Si le nombre premier $p = 4q+1$ peut avoir 7 pour » résidu quadratique, ce qui arrive quand p a l'une des formes » $28n+1$, $+9$, $+25$, on pourra toujours poser $p = T^2 + 7U^2$; » alors 7 sera résidu ou non-résidu biquadratique selon que T sera » ou non de forme $28n+1$, $+9$, $+25$. »

Au-delà de 7, pour parvenir à un caractère complet, on est forcé de considérer l'équation $bp = T^2 \pm aU^2$ et les théorèmes deviennent moins simples. En voici deux pour le nombre 11. Le premier offre le caractère complet.

« Théorème. Soit $p = 4h + 1$ un nombre premier ayant 11 pour » résidu quadratique, ou de forme $44q+1$, 5, 9, 25, 27; on pourra » toujours poser $p = T^2 + 11U^2$ ou $4p = T^2 + 11U^2$; alors 11 sera » résidu biquadratique, si t est de forme $44k \pm 1$, ± 5, ± 7, ± 9, » ± 19, et non-résidu biquadratique dans le cas contraire. Cela a » lieu pour les solutions de première espèce. C'est le contraire pour » celles de deuxième espèce.

Quand l'équation $p = T^2 + 11U^2$ n'est pas possible, $3p = T^2 + 11U^2$ l'est toujours. Cette équation aurait donné le théorème suivant, qui est moins simple. »

« Théorème. Soit $3p = T^2 + 11U^2$, les formes de diviseurs de » $x^2 - 3$ sont $12k \pm 1$ (D). Les formes de diviseurs de $x^2 - 33$ sont » $132k \pm 1$, ± 17, ± 25, ± 29, ± 31, ± 35, ± 37, ± 41, » ± 49, ± 65, (D′). Le nombre 11 sera résidu biquadratique de p, » si u et t sont respectivement des formes (D), (D′); ou bien si ni u, » ni t ne sont contenues dans les formes (D), (D′). Dans tous les » autres cas le nombre 11 sera non-résidu biquadratique. »

Il serait superflu de multiplier les applications qui se déduiront en grand nombre des tables de la théorie des nombres de Legendre.

C'est en égalant $ps^2 = (\varphi^2 + \psi^2)s^2$ à $ps^2 = T^2 \pm aU^2$, que M. Dirichlet a établi le théorème général dont nous avons parlé dans l'article précédent.

Je ne connaissais pas le Mémoire de M. Dirichlet, quand j'ai trouvé la démonstration du théorème général (I) donné plus haut, mais j'avais lu ce qu'on en dit dans le *Bulletin des Sciences Mathématiques* de M. Férussac.
