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

ÉMILE MATHIEU

Mémoire sur la théorie des résidus biquadratiques

Journal de mathématiques pures et appliquées 2^e série, tome 12 (1867), p. 377-438.
<http://www.numdam.org/item?id=JMPA_1867_2_12__377_0>

MÉMOIRE

SUR

LA THÉORIE DES RÉSIDUS BIQUADRATIQUES;

PAR M. ÉMILE MATHIEU.

INTRODUCTION.

Je vais indiquer les résultats auxquels je suis arrivé dans ce Mémoire; mais auparavant il est utile de rappeler les premières recherches qui ont été faites sur la théorie des résidus biquadratiques fondée par Gauss.

D'abord, soit N un nombre quelconque; il est résidu quadratique du nombre premier p si on peut poser

$$N = a^2 + Mp \quad \text{ou} \quad N \equiv a^2 \pmod{p};$$

si de plus on peut poser

$$N = b^4 + Mp \quad \text{ou} \quad N \equiv b^4 \pmod{p},$$

N est dit *résidu biquadratique* de p, et il est évident que tout résidu biquadratique est aussi résidu quadratique.

Mais l'inverse a lieu aussi, comme il est très-aisé de le voir, lorsque le module est de la forme $4n + 3$, de sorte que tout résidu quadratique d'un nombre premier de la forme $4n + 3$ est également un résidu biquadratique; et il en résulte qu'il suffit d'étudier le caractère biquadratique des nombres par rapport aux nombres premiers p de la forme $4n + 1$; nous supposerons donc désormais que le module ait cette forme.

Désignons par g une racine primitive quelconque du nombre premier $p = 4n + 1$, et formons les résidus des nombres

$$g^0,\ g,\ g^2,\ldots,\ g^{p-2};$$

puis partageons-les en quatre groupes correspondant aux quatre groupes des puissances de g :

$$\begin{aligned} &g^0,\ g^4,\ g^8,\ g^{12},\ldots,\\ &g,\ g^5,\ g^9,\ g^{13},\ldots,\\ &g^2,\ g^6,\ g^{10},\ g^{14},\ldots,\\ &g^3,\ g^7,\ g^{11},\ g^{15},\ldots, \end{aligned}$$

et désignons ces groupes respectivement par les lettres A, B, C, D. Les nombres du groupe A sont les résidus biquadratiques de p; ceux du groupe C sont les résidus quadratiques qui ne sont pas en même temps biquadratiques; enfin les nombres des groupes B et D sont des non-résidus quadratiques, et à plus forte raison des non-résidus biquadratiques.

Les deux groupes A et C ne dépendent en aucune façon de la racine primitive que l'on a choisie; mais les deux groupes B et D peuvent s'échanger l'un dans l'autre par un changement de cette racine, et, pour qu'ils soient parfaitement déterminés, il faut donc spécifier la racine primitive que l'on choisit; pour cet effet, nous supposerons que l'on adopte toujours pour g la plus petite racine primitive.

p, étant de la forme $4n + 1$, est décomposable en la somme de deux carrés $a^2 + b^2$ et d'une seule manière; mais comme il faut que a et b soient parfaitement déterminés, on désigne par a le nombre impair et par b celui qui est pair; enfin il convient de choisir les signes de a et b de manière que le nombre impair

$$a \text{ soit } \equiv 1 \pmod 4$$

et

$$b \equiv a g^{\frac{p-1}{4}} \pmod p,$$

g étant, comme nous l'avons dit, la plus petite racine primitive de p.

Cela posé, pour déterminer le caractère biquadratique d'un nombre quelconque N par rapport au nombre-premier p, on peut suivre une méthode analogue à celle qui permet de trouver son caractère quadratique. On décompose encore le nombre donné en ses facteurs premiers ; mais on ne regarde plus comme premiers tous ceux qui sont ainsi désignés ordinairement dans l'arithmétique ; car les nombres premiers réels de la forme $4n+1$ sont considérés comme décomposables en deux nombres $c+di$, $c-di$, qui sont dits *nombres premiers complexes*. Enfin, décomposant le module en les deux facteurs $a+bi$, $a-bi$, il suffit de chercher le caractère du nombre N par rapport au nombre premier complexe $a+bi$.

Parmi les quatre nombres

$$c+di, \quad -d+ci, \quad -c-di, \quad d-ci,$$

qui sont dits *associés* et qui ne diffèrent que par le facteur i, -1 ou $-i$, il y en a un qui est $\equiv 1 \pmod{2+2i}$ et qui est appelé nombre *primaire*. Or on a à chercher le caractère biquadratique de chaque facteur de N par rapport à $a+bi$; il sera aisé de ramener cette recherche à ne s'effectuer que sur des nombres premiers primaires, et chacune de ces déterminations s'opérera par l'application à ces nombres du théorème fondamental (*Theoria residuorum biquadraticorum*, § 67), théorème tout à fait analogue à la loi de réciprocité de la théorie des résidus quadratiques.

Toutefois l'application du théorème fondamental peut être facilitée par la remarque suivante, due à Jacobi :

Soit l un nombre complexe quelconque et m un autre nombre semblable, mais premier. On désigne par $\left[\frac{l}{m}\right]$ les quantités 1, i, -1 ou $-i$, suivant que

$$l^{\frac{\mu-1}{4}} \text{ est congru à } 1,\ i,\ -1 \text{ ou } -i \pmod{m},$$

μ étant la norme de m, et si l'on pose

$$\left[\frac{l}{m}\right] = i^{\lambda},$$

λ désigne le caractère du nombre l par rapport au nombre premier m.

Si de plus, lorsque n est un nombre composé $tt't''\ldots$, où t, t', t'',... sont premiers, on convient que $\left[\frac{l}{n}\right]$ représente le produit

$$\left[\frac{l}{t}\right]\left[\frac{l'}{t'}\right]\left[\frac{l''}{t''}\right]\cdots,$$

alors on a le théorème suivant : « *Si* $A+Bi$ *et* $C+Di$ *sont deux entiers complexes premiers entre eux* $\equiv 1 \pmod{2+2i}$, *on a*

$$\left[\frac{A+Bi}{C+Di}\right]=\left[\frac{C+Di}{A+Bi}\right](-1)^{\frac{A-1}{2}\frac{C-1}{2}};$$

ce qui se réduit au théorème fondamental, lorsque $A+Bi$ et $C+Di$ sont deux nombres premiers.

Quant au théorème fondamental, Eisenstein en a donné deux démonstrations différentes dans le tome XXVIII du *Journal de Crelle*.

Mais Gauss indique une autre méthode pour déterminer le caractère biquadratique d'un nombre N par rapport à un nombre premier $p=4n+1$; supposons encore p décomposé en la somme de deux carrés a^2+b^2, les signes de a et b étant déterminés comme nous avons dit ci-dessus. Gauss a reconnu par induction que le caractère biquadratique d'un nombre premier $\pm q$, le signe $\pm$ ayant lieu suivant que $q=4n\pm 1$, dépend uniquement de la valeur de $\frac{b}{a} \pmod{q}$. Ainsi soient deux nombres premiers $p=a^2+b^2$, $p'=a'^2+b'^2$, a' et b' étant déterminés comme a et b; si $\frac{b}{a}$ et $\frac{b'}{a'}$ sont congrus suivant le module q, $\pm q$ a le même caractère par rapport à p et à p'. Mais il ne nous apprend rien sur la possibilité de reconnaître quels sont ceux des rapports $\frac{b}{a}$ qui appartiennent aux quatre classes correspondant respectivement aux groupes A, C ou B et D, et qui sont propres à indiquer si $\pm q$ est résidu biquadratique, résidu simplement quadratique ou non-résidu.

Dans les *Comptes rendus de l'Académie des Sciences* du 18 mars 1867, j'ai donné la loi qui distingue les quatre classes, et de laquelle Gauss avait dit : *At lex hujus distributionis abstrusior videtur, etiamsi*

quædam generalia prompte animadvertantur [*]. Je donnerai dans ce Mémoire la démonstration de la solution de cette question. Mais voici d'abord de cette solution une forme géométrique qui en facilite le souvenir et qui me semble fort curieuse, encore que cette forme ne soit pas celle qui convient à l'application du calcul.

Considérons séparément les cas de $q = 4n + 1$ et de $q = 4n + 3$.

1° Si q est de la forme $4n + 1$, divisons la demi-circonférence π en $q - 1$ parties égales et considérons les tangentes des arcs

$$0, \quad \frac{\pi}{q-1}, \quad 2\frac{\pi}{q-1}, \quad 3\frac{\pi}{q-1}, \ldots, \quad (q-2)\frac{\pi}{q-1}.$$

On sait que ces tangentes sont exprimables par radicaux; et de plus il est remarquable que ces radicaux, pris suivant le module q, sont toujours des nombres entiers réels, de sorte que les expressions de ces tangentes, prises suivant le module q, représentent elles-mêmes des nombre entiers réels. Or q appartiendra au groupe A, B, C ou D, selon que $\frac{b}{a}$ sera congru suivant le module q à la tangente d'un des arcs commençant à l'origine de la demi-circonférence et terminés aux points de division 0, 4, 8,..., ou 1, 5, 9,..., ou 2, 6, 10,..., ou 3, 7, 11,....

2° Si q est de la forme $4n + 3$, divisons la demi-circonférence $-\pi$ en $q + 1$ parties égales et considérons les tangentes des arcs

$$0, \quad -\frac{\pi}{q+1}, \quad -2\frac{\pi}{q+1}, \quad -3\frac{\pi}{q+1}, \ldots, \quad -q\frac{\pi}{q+1},$$

qui commencent à l'origine de la circonférence et se terminent à des points de division que nous marquerons 0, -1, -2,.... Non-seulement les tangentes de ces arcs sont exprimables par radicaux, mais leurs expressions prises suivant le module q sont des nombres entiers réels. Et le nombre $-q$ appartient au groupe A, B, C ou D, selon que $\frac{b}{a}$ est congru suivant le module q à la tangente d'un arc terminé aux points de division 0, -4, -8,..., ou -1, -5, -9,..., ou -2, -6, -10,..., ou -3, -7, -11,....

[*] *Höhere Arithmetik*, p 100.

On peut encore donner à ce théorème une forme plus concise en réunissant les cas de $q = 4n+1$ et de $q = 4n+3$. En effet, si l'on pose $\pm q = \tau$, on a le théorème suivant :

Considérons les tangentes des arcs

$$0, \quad \frac{\pi}{\tau-1}, \quad 2\frac{\pi}{\tau-1}, \quad 3\frac{\pi}{\tau-1}, \ldots;$$

elles sont exprimables par radicaux, et leurs expressions prises suivant le module q sont des nombres entiers. Posons

$$\alpha = \operatorname{tang} 0, \quad \operatorname{tang} 4\frac{\pi}{\tau-1}, \quad \operatorname{tang} 8\frac{\pi}{\tau-1}, \ldots,$$

$$\beta = \operatorname{tang}\frac{\pi}{\tau-1}, \quad \operatorname{tang} 5\frac{\pi}{\tau-1}, \quad \operatorname{tang} 9\frac{\pi}{\tau-1}, \ldots,$$

$$\gamma = \operatorname{tang} 2\frac{\pi}{\tau-1}, \quad \operatorname{tang} 6\frac{\pi}{\tau-1}, \quad \operatorname{tang} 10\frac{\pi}{\tau-1}, \ldots,$$

$$\delta = \operatorname{tang} 3\frac{\pi}{\tau-1}, \quad \operatorname{tang} 7\frac{\pi}{\tau-1}, \quad \operatorname{tang} 11\frac{\pi}{\tau-1}, \ldots;$$

suivant que $\frac{b}{a}$ sera congru suivant le module q à l'un des nombres α, β, γ ou δ, τ appartiendra respectivement à A, B, C ou D.

Par exemple, s'agira-t-il du caractère biquadratique de $q = 5$, divisant la demi-circonférence en $q-1 = 4$ parties égales, on voit que l'on a

$$\operatorname{tang} 0 = 0, \quad \operatorname{tang}\frac{\pi}{4} = 1, \quad \operatorname{tang}\frac{\pi}{2} = \infty, \quad \operatorname{tang}\frac{3\pi}{4} = -1 \equiv 4 \pmod 5.$$

On en conclut que 5 appartient au groupe A, B, C ou D, par rapport à p, selon que $\frac{b}{a}$ est congru suivant le module 5 à 0, 1, ∞ ou 4.

Ces théorèmes de la théorie des résidus biquadratiques fournissent immédiatement ceux-ci, qui sont nouveaux aussi, quoiqu'ils rentrent dans le domaine de la théorie des résidus quadratiques :

1° Soient p et q deux nombres premiers de la forme $4n+1$, dont l'un p soit égal à $a^2 + b^2$, et ici il n'est besoin d'avoir égard aux signes de a et b, ni même à leur ordre de parité. Divisons la demi-circonfé-

rence en $q-1$ parties égales et menons les tangentes de tous les arcs qui commencent à l'origine de la demi-circonférence et se terminent aux différents points de division. Si la valeur de $\frac{b}{a}$ est congrue suivant le module q à l'expression de la tangente d'un des arcs terminés à un point de division d'ordre pair 0, 2, 4, 6..., le nombre premier p est résidu quadratique de q et q résidu quadratique de p; mais si $\frac{b}{a}$ correspond à une divison impaire, p et q sont non-résidus l'un de l'autre.

2° Si p et q sont deux nombres premiers, dont l'un q est de la forme $4n+3$, tandis que l'autre p est de la forme $4n+1$, on divisera la demi-circonférence en $q+1$ parties égales et on obtiendra les mêmes conséquences que dans le cas précédent.

Ici nous devons faire une réflexion importante sur le choix que nous avons fait de la racine primitive prise pour base. Après avoir distingué, par rapport au module p, tous les nombres non divisibles par p en les quatre groupes A, B, C, D, nous avons dit que, afin de ne laisser aucune ambiguïté sur les groupes B et D, nous supposerons que l'on prenne toujours pour base la plus petite racine primitive g de p. Or il est à remarquer que ce choix n'a pas été fait au hasard, mais en vue de simplifier la théorie, et que par exemple on aurait des résultats plus compliqués si on remplaçait la plus petite par la plus grande racine primitive.

En effet, nous avons dit comment de la loi de réciprocité des résidus biquadratiques donnée par Gauss pour les nombres complexes on peut tirer le caractère biquadratique d'un nombre réel N par rapport à un nombre premier réel $p=a^2+b^2$, et, pour que cette méthode soit applicable, il faut absolument que l'on prenne pour base la plus petite racine primitive g de p. Et de même la méthode que nous avons donnée pour déterminer le caractère biquadratique de p par rapport à $p=a^2+b^2$ au moyen du nombre $\frac{b}{a}\pmod{q}$ exige encore ce choix.

Considérations des quatre périodes de $\frac{p-1}{4}$ *racines de la congruence* $\frac{x^p-1}{x-1} \equiv 0 \pmod{q}$. — *Démonstration simple et nouvelle de la loi de réciprocité de la théorie des résidus quadratiques.* — *Théorème nouveau de cette théorie.*

1. Nos recherches sur la théorie des résidus biquadratiques seront entièrement fondées sur l'étude des quatre périodes formées des racines de la congruence

$$\frac{x^p-1}{x-1} \equiv 0 \pmod{q}, \tag{1}$$

dans laquelle p est un nombre premier positif de la forme $4n+1$; en désignant par x une quelconque de ces racines, elles sont représentées par

$$\omega \equiv \sum x^A, \quad \omega' \equiv \sum x^B, \quad \omega'' \equiv \sum x^C, \quad \omega''' \equiv \sum x^D \pmod{q},$$

le signe sommatoire $\sum$ se rapportant aux différents nombres A, B, C, D, et, d'après ce qui a été dit dans l'Introduction, les quatre groupes A, B, C, D sont les résidus des nombres des quatres lignes

$$\begin{aligned} &g^0, g^4, g^8, \ldots, g^{p-5}, \\ &g, g^5, g^9, \ldots, g^{p-4}, \\ &g^2, g^6, g^{10}, \ldots, g^{p-3}, \\ &g^3, g^7, g^{11}, \ldots, g^{p-2}, \end{aligned}$$

pris par rapport au module p, g désignant la plus petite racine primitive de p.

Désignons par m le plus petit nombre pour lequel est satisfaite la congruence

$$q^m - 1 \equiv 0 \pmod{p},$$

les racines de la congruence (1) appartiennent toutes à la congruence

$$x^{q^m-1} \equiv 1 \pmod{q},$$

dont l'étude des racines a été faite rigoureusement pour la première fois par M. Serret dans son *Algèbre supérieure*.

Comme l'examen de ces quatre périodes demande une étude longue et attentive, nous commencerons, pour mieux faire comprendre les principes qui nous serviront, à les appliquer à la théorie beaucoup plus simple des résidus quadratiques.

2. Nous considérerons alors les deux périodes de $\frac{p-1}{2}$ racines de la congruence

$$\frac{x^p-1}{x-1} \equiv 0 \pmod{q},$$

qui ont pour valeurs

$$\Omega \equiv \sum x^a, \quad \Omega' \equiv \sum x^b,$$

x désignant une quelconque des racines et le signe $\sum$ se rapportant aux lettres a et b, dont la première désigne un résidu quadratique de p, et la seconde un non-résidu. On suppose ici que p peut être indistinctement de la forme $4n \pm 1$, et on sait (*Disquisitiones arithmeticæ*, 356) que la congruence qui donne ces deux périodes est

$$x^2 + x \mp n \equiv 0 \pmod{q}.$$

Si on élève Ω et Ω' à la puissance q, il est aisé de voir, puisqu'on doit négliger les multiples de q, que l'on aura.

$$\Omega^q \equiv \sum x^{aq}, \quad \Omega'^q \equiv \sum x^{bq} \pmod{q}.$$

Tous les exposants aq et tous les exposants bq sont différents entre eux selon le module p, et de plus, si q est résidu quadratique de p, tous les nombres aq sont des résidus quadratiques, et les nombres bq des non-résidus, et, au contraire, si q est non-résidu quadratique de p, tous les nombres aq sont des non-résidus, et les nombres bq des résidus quadratiques de p.

On en conclut que si q est résidu quadratique on a

$$\Omega^q \equiv \Omega, \quad \Omega'^q \equiv \Omega',$$

et que par conséquent les deux périodes sont réelles, puisqu'elles satisfont à la congruence

$$x^q \equiv x \pmod{q};$$

mais si q est non-résidu de p, on a

$$\Omega^q \equiv \Omega', \quad \Omega'^q \equiv \Omega,$$

et les deux périodes sont imaginaires; car si Ω était réel, on aurait $\Omega^q \equiv \Omega$ et par suite $\Omega \equiv \Omega'$, tandis que la congruence du second degré ci-dessus ne peut avoir ses racines égales.

Or, d'autre part, les racines de cette congruence sont

$$\equiv \frac{-1 \pm \sqrt{\pm p}}{2} \pmod{q},$$

et sont par conséquent réelles ou imaginaires, selon que $\pm p$ est résidu ou non-résidu quadratique de q. On en conclut ce théorème (où l'on adopte, soit tous les signes supérieurs, soit tous les signes inférieurs) :

Si le nombre premier q est résidu quadratique du nombre premier $p = 4n \pm 1$, $\pm p$ est résidu quadratique de q; mais si q est non-résidu quadratique de p, $\pm p$ est lui-même non-résidu de q.

Enfin, en s'appuyant sur ce que -1 est résidu ou non-résidu quadratique de q, suivant que $q = 4n+1$ ou $4n-1$, on en conclut la loi de réciprocité :

Le nombre premier p est résidu ou non-résidu quadratique du nombre premier q, selon que q est lui-même résidu ou non-résidu de p, toutes les fois que l'un au moins de ces deux nombres est de la forme $4n+1$; mais si tous les deux sont de la forme $4n+3$, l'un étant résidu quadratique de l'autre, le second est non-résidu du premier.

Ces considérations peuvent également servir à déterminer le caractère quadratique du nombre 2. Nous avons vu tout à l'heure que, q désignant un nombre premier, si q est résidu quadratique de p, la congruence qui donne les deux périodes a ses racines réelles, mais que si q est non-résidu de p, cette congruence a ses racines imagi-

naires, et le raisonnement qui nous a servi est applicable au cas où q est égal à 2.

Supposons que p soit de la forme $8l \pm 1$, nous devons faire $n = 2l$, et la congruence qui donne les deux périodes prises suivant le module $q = 2$ devient

$$x^2 + x \mp 2l \equiv 0 \pmod 2$$

ou

$$x^2 + x \equiv 0 \pmod 2,$$

elle a ses deux racines réelles qui sont 0 et 1; donc 2 est résidu quadratique de p.

Mais si p est de la forme $8l + 5$ ou $8l + 3$, nous devons faire $n = 2l + 1$, et la congruence se réduit à

$$x^2 + x + 1 \equiv 0 \pmod 2;$$

comme 0 et 1 ne sont pas racines de cette congruence, elle est irréductible, et ses deux racines doivent être regardées comme imaginaires; 2 est donc non-résidu quadratique de p.

3. Revenons à l'expression des deux périodes, lorsque p est de la forme $4n + 1$; il faut prendre sous le radical le signe $+$, et elles sont données par la formule

$$\frac{-1 \pm \sqrt{p}}{2} \pmod q;$$

le nombre premier p est décomposable en la somme de deux carrés $a^2 + b^2$ et d'une seule manière, et, regardant a^2 comme le carré impair et b^2 comme le carré pair, nous pouvons écrire, au lieu de la formule précédente, la suivante

$$\frac{-1 \pm \sqrt{a^2 + b^2}}{2}$$

ou

$$-\frac{1}{2} \pm \frac{a}{2}\sqrt{\frac{b^2}{a^2} + 1} \pmod q,$$

et, suivant que ces deux expressions sont réelles ou imaginaires, q est

résidu quadratique ou non-résidu de p. Donc si on désigne par α le nombre entier moindre que q qui est représenté par

$$\frac{b}{a} \pmod{q},$$

q sera résidu quadratique de p ou non-résidu, selon que

$$\alpha^2 + 1$$

sera résidu quadratique de q ou en sera un non-résidu.

Ainsi le caractère de q par rapport à p ne dépend que de la valeur de $\frac{b}{a} \pmod{q}$, ou plutôt de son carré, en sorte que si nous désignons par α ce nombre, et que p' soit un autre nombre premier de la forme $4n+1$ décomposable en la somme de deux carrés $a'^2 + b'^2$, q aura le même caractère par rapport à p' que par rapport à p, si on a

$$\frac{b'}{a'} \equiv \pm \alpha \pmod{q},$$

et il en sera encore de même si on a

$$\frac{b'}{a'} \equiv \pm \frac{1}{\alpha} \pmod{q};$$

car $\frac{1}{\alpha^2} + 1$ ou $\frac{\alpha^2+1}{\alpha^2}$ a par rapport au module q le même caractère que $\alpha^2 + 1$.

Mais nous allons montrer, ce qui est extrêmement curieux, comment on peut embrasser tout d'un coup par une même formule les deux classes de l'expression

$$\frac{b}{a} \pmod{q},$$

la première renfermant ceux de ces nombres pour lesquels q est résidu quadratique de p, et la seconde ceux pour lesquels q est un non-résidu, et ces deux formules nous apprendront que chacune des deux classes renferme la même quantité de nombres au-dessous du module q.

Il faut considérer séparément les cas de $q = 4n+1$ et de $q = 4n+3$.

Supposons d'abord $q = 4n+1$; -1 étant résidu quadratique de q, on peut satisfaire à la congruence

$$\varphi^2 \equiv -1 \pmod{q},$$

dont nous retenons l'une des racines ; désignons par A un résidu quadratique quelconque de q, et par B un non-résidu de q : je dis que toutes les valeurs de $\frac{b}{a} \pmod{q}$ pour lesquelles q est résidu quadratique de p, et qui forment la première classe, sont données par la formule

$$\alpha_1 \equiv \varphi \frac{1-A}{1+A} \pmod{q},$$

et que toutes les valeurs de $\frac{b}{a} \pmod{q}$ de la seconde classe sont données par

$$\alpha_2 \equiv \varphi \frac{1-B}{1+B} \pmod{q},$$

En effet, posons

$$\alpha = \varphi \frac{1-L}{1+L},$$

et nous aurons

$$1+\alpha^2 \equiv 1 - \frac{(1-L)^2}{(1+L)^2} \equiv \frac{4L}{(1+L)^2} \pmod{q},$$

et $1+\alpha^2$ sera résidu quadratique de q ou non-résidu, en même temps que L.

On voit aussi, d'après les formules précédentes, que les deux classes renferment la même quantité de nombres.

Supposons ensuite $q = 4n+3$; les formules précédentes ne sont plus admissibles, car φ serait imaginaire et par suite aussi les expressions de α_1 et α_2 ; mais on peut former celles qui sont applicables à ce cas par analogie et d'après une considération semblable à celle que M. Serret a employée (*Comptes rendus de l'Académie des Sciences*, 17 janvier 1859).

Posons $i = \sqrt{-1}$ et divisons les racines de la congruence

$$(a) \qquad z^{q+1} \equiv 1 \pmod{q}$$

en deux classes : celles qui satisfont à

$$z^{\frac{q+1}{2}} \equiv 1,$$

que nous désignerons en général par $\mathfrak{A}$, et celles qui satisfont à

$$z^{\frac{q+1}{2}} \equiv -1,$$

que nous désignerons par $\mathfrak{B}$. Toutes les valeurs de $\frac{b}{a} \pmod q$ qui appartiennent à la première classe, sont données par la formule

$$\alpha_1 \equiv i\,\frac{1-\mathfrak{A}}{1+\mathfrak{A}} \pmod q,$$

et toutes celles qui appartiennent à la seconde classe par

$$\alpha_2 \equiv i\,\frac{1-\mathfrak{B}}{1+\mathfrak{B}} \pmod q.$$

D'abord il faut reconnaître que ces expressions sont réelles, quoiqu'elles renferment des quantités imaginaires. Or la condition pour qu'une quantité soit réelle suivant le module q est qu'elle satisfasse à la congruence

$$X^q \equiv X \pmod q.$$

Élevons donc à la puissance q la quantité

$$\alpha \equiv i\,\frac{1-\xi}{1+\xi},$$

où ξ représente une racine de (a), et on aura en effet

$$\alpha^q \equiv i^q\,\frac{1-\xi^q}{1+\xi^q} \equiv i^{4n+3}\,\frac{1-\frac{1}{\xi}}{1+\frac{1}{\xi}} \equiv i\,\frac{1-\xi}{1+\xi} \equiv \alpha,$$

ce qui prouve que les expressions précédentes sont réelles.

Formons ensuite la quantité $1+\alpha^2$; elle est

$$1+\alpha^2 \equiv \frac{4\xi}{(1+\xi)^2}.$$

Si ξ est un nombre $\mathfrak{A}$ il est le carré d'un des nombres complexes n qui satisfont à la congruence (a); donc on a

$$1+\alpha^2 \equiv \left(\frac{2n}{1+n^2}\right)^2,$$

et par la méthode qui précède, on reconnaît que $\frac{2n}{1+n^2}$ est réel; donc $1+\alpha^2$ est un résidu quadratique. Au contraire, si ξ est un des nombres $\mathfrak{B}$, il est évident que $1+\alpha^2$ est un non-résidu, et l'exactitude de nos formules est démontrée.

4. Revenons maintenant aux quatre périodes de la congruence

$$\frac{x^p-1}{x-1} \equiv 0 \pmod{q},$$

dans laquelle on suppose que p est un nombre premier de la forme $4n+1$. Les valeurs de ces périodes sont

$$\omega \equiv x^{A'} + x^{A''} + x^{A'''} + \ldots,$$
$$\omega' \equiv x^{B'} + x^{B''} + x^{B'''} + \ldots,$$
$$\omega'' \equiv x^{C'} + x^{C''} + x^{C'''} + \ldots,$$
$$\omega''' \equiv x^{D'} + x^{D''} + x^{D'''} + \ldots,$$

A′, A″, A‴, ... étant ce que nous avons appelé les nombres A; B′, B″, B‴, ... les nombres B, etc. Si nous élevons ces quantités à la puissance q, comme nous ne considérons que leurs valeurs suivant le module q, il nous suffit d'élever chacun des termes à la puissance q, de sorte que nous obtenons

$$\omega^q \equiv \sum x^{Aq}, \quad \omega'^q \equiv \sum x^{Bq}, \quad \omega''^q \equiv \sum x^{Cq}, \quad \omega'''^q \equiv \sum x^{Dq}.$$

Or, supposons que q soit résidu biquadratique de p, les nombres de

chacune des quatre lignes

$$\begin{aligned} &A'q,\ A''q,\ A'''q,\ldots,\\ &B'q,\ B''q,\ B'''q,\ldots,\\ &C'q,\ C''q,\ C'''q,\ldots,\\ &D'q,\ D''q,\ D'''q,\ldots, \end{aligned}$$

sont tous différents entre eux selon le module p, et les nombres de la première ligne sont congrus dans un certain ordre aux nombres A', A'', A''',..., ceux de la seconde aux nombres B', B'', B''',..., etc.; donc, puisque x^p est $\equiv 1$, on a

$$\sum x^{Aq} \equiv \sum x^{A}, \quad \sum x^{Bq} \equiv \sum x^{B}, \ldots \quad (\mathrm{mod.}\, q),$$

et

$$\omega^q \equiv \omega, \quad \omega'^q \equiv \omega', \quad \omega''^q \equiv \omega'', \quad \omega'''^q \equiv \omega''',$$

c'est-à-dire que ω, ω', ω'', ω''' sont réels.

Quand un nombre q est donné, on sait comment on peut reconnaître s'il est résidu quadratique du nombre premier $p = 4n + 1$ ou s'il ne l'est pas, et par conséquent si q appartient aux groupes A et C ou aux groupes B et D, et il résulte de ce qui précède que, au cas où q est résidu quadratique de p, on pourra reconnaître si q appartient à A ou à C en examinant si les quatre périodes ω, ω', ω'', ω''' sont toutes les quatre réelles ou ne le sont pas.

Nous allons donc déterminer la congruence qui donne les quatre périodes de la congruence

$$\frac{x^p - 1}{x - 1} \equiv 0 \quad (\mathrm{mod.}\, q),$$

ou, ce qui revient au même, l'équation du quatrième degré qui a pour racines les quatre périodes de l'équation

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

et lorsque nous les aurons obtenues, il nous sera aisé de reconnaître si q est résidu biquadratique, résidu simplement quadratique ou non-résidu, et nous aurons fait un premier pas vers la solution de la recherche du caractère biquadratique de q. Plus tard, nous verrons comment on peut discerner si q appartient à B ou à D par rapport à p.

Formation des périodes de $\frac{p-1}{4}$ *racines de l'équation* $\frac{x^p-1}{x-1}=0$.

5. Désignons par g la plus petite racine primitive du nombre premier p de la forme $4m+1$; les quatre périodes de $\frac{p-1}{4}$ racines pour l'équation

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

sont, en désignant par x une racine quelconque,

$$\omega = x + x^{g^4} + x^{g^8} + \ldots + x^{g^{p-5}},$$
$$\omega' = x^g + x^{g^5} + x^{g^9} + \ldots + x^{g^{p-4}},$$
$$\omega'' = x^{g^2} + x^{g^6} + x^{g^{10}} + \ldots + x^{g^{p-3}},$$
$$\omega''' = x^{g^3} + x^{g^7} + x^{g^{11}} + \ldots + x^{g^{p-2}}.$$

Supposons que l'équation qui donne ces quatre périodes soit

$$x^4 - Ax^3 + Bx^2 - Cx + D = 0,$$

on aura

$$A = \omega + \omega' + \omega'' + \omega''', \quad B = \omega\omega' + \omega'\omega'' + \omega''\omega''' + \omega'''\omega + \omega\omega'' + \omega'\omega''',$$
$$C = \omega\omega'\omega'' + \omega'\omega''\omega''' + \omega\omega'\omega''' + \omega\omega''\omega''', \quad D = \omega\omega'\omega''\omega'''.$$

On obtient sur-le-champ, pour le premier coefficient, $A = -1$.

Désignons par (00) la quantité des nombres $1, g^4, g^8, \ldots, g^{p-5}$, ou plutôt la quantité des nombres A, leurs résidus minima qui, augmentés d'une unité, donnent des nombres A; puis désignons par (01), (02), (03) la quantité des nombres A qui, augmentés d'une unité, donnent des nombres B, C ou D. Pareillement, représentons par (10), (11), (12), (13) la quantité des nombres B qui, augmentés d'une unité, donnent des nombres A, B, C ou D. Enfin on voit clairement ce que l'on doit entendre par les seize quantités de la figure

$$S \begin{cases} (00), (01), (02), (03), \\ (10), (11), (12), (13), \\ (20), (21), (22), (23), \\ (30), (31), (32), (33), \end{cases}$$

que nous appellerons la figure S.

Représentons, en général, x^l par $[l]$; alors nous aurons

$$\omega' = [g] + [g^5] + [g^9] + [g^{13}] + \ldots,$$
$$\omega = [1] + [g^4] + [g^6] + [g^{12}] + \ldots,$$

et en multipliant ces deux expressions nous obtenons

$$\begin{aligned}\omega\omega' = &[g + 1] + [g^5 + 1] + [g^9 + 1] + \ldots \\ &+ [g^5 + g^4] + [g^9 + g^4] + [g^{13} + g^4] + \ldots \\ &+ [g^9 + g^8] + [g^{13} + g^8] + \ldots \\ &\ldots\ldots\ldots\end{aligned}$$

Les termes qui se trouvent dans une même ligne verticale forment une période, et l'on en déduit facilement

$$\omega\omega' = (10)\,\omega + (11)\,\omega' + (12)\,\omega'' + (13)\,\omega''';$$

on obtient ensuite (*Disquis. Arithm.*, n° 345), d'après cette formule,

$$\omega'\omega'' = (10)\,\omega' + (11)\,\omega'' + (12)\,\omega''' + (13)\,\omega,$$
$$\omega''\omega''' = (10)\,\omega'' + (11)\,\omega''' + (12)\,\omega + (13)\,\omega',$$
$$\omega'''\omega = (10)\,\omega''' + (11)\,\omega + (12)\,\omega' + (13)\,\omega'',$$

si on multiple ω'' par ω, on obtient aussi facilement

$$\begin{aligned}\omega\omega'' &= (20)\,\omega + (21)\,\omega' + (22)\,\omega'' + (23)\,\omega''' \quad \text{si} \quad p = 8n+1, \\ &= (20)\,\omega + (21)\,\omega' + (22)\,\omega'' + (23)\,\omega''' + 2n + 1 \ \text{si} \ p = 8n+5,\end{aligned}$$

et, d'après le n° 345 des *Disquisitiones*, on en tire

$$\begin{aligned}\omega'\omega''' &= (20)\,\omega' + (21)\,\omega'' + (22)\,\omega''' + (23)\,\omega \quad \text{si} \quad p = 8n+1, \\ &= (20)\,\omega' + (21)\,\omega'' + (22)\,\omega''' + (23)\,\omega + 2n + 1 \ \text{si} \ p = 8n+5;\end{aligned}$$

mais d'après le même principe appliqué à cette dernière formule nous avons

$$\begin{aligned}\omega''\omega &= (20)\,\omega'' + (21)\,\omega''' + (22)\,\omega + (23)\,\omega' \quad \text{si} \quad p = 8n+1, \\ &= (20)\,\omega'' + (21)\,\omega''' + (22)\,\omega + (23)\,\omega' + 2n + 1 \ \text{si} \ p = 8n+5.\end{aligned}$$

Comparant les deux valeurs de $\omega\omega''$, nous obtenons

$$(20) = (22), \quad (21) = (23).$$

En calculant $\omega\omega'''$ comme on a obtenu $\omega\omega''$, on trouve encore

$$\omega\omega''' = (30)\,\omega + (31)\,\omega' + (32)\,\omega'' + (33)\,\omega''',$$

et en comparant cette valeur avec celle que nous avons trouvée ci-dessus, on a

$$(11) = (30), \quad (12) = (31), \quad (13) = (32), \quad (10) = (33),$$

ce qui prouve que les deuxième et quatrième lignes de S sont composées de termes égaux.

Distinguons les deux cas de $p = 8n + 1$ et de $p = 8n + 5$.

6. Supposons d'abord que l'on ait

$$p = 8n + 1.$$

D'après la *Theoria residuorum biquadraticorum*, les termes de la figure S peuvent être ainsi écrits :

$$\begin{array}{cccc} h, & i, & k, & l, \\ i, & l, & m, & m, \\ k, & m, & k, & m, \\ l, & m, & m, & i, \end{array}$$

et se réduisent à cinq quantités.

Posons

$$p = a^2 + b^2,$$

en regardant a comme impair et par suite b comme pair; puis choisissons le signe de a de manière que l'on ait $a \equiv 1 \pmod 4$ et le signe de b de manière que l'on ait $b \equiv af \pmod p$, et f la valeur de $\sqrt{-1} \pmod p$ donnée par

$$f \equiv g^{\frac{p-1}{4}} \pmod p.$$

Alors les cinq quantités précédentes se déduisent des formules suivantes données par Gauss :

$$\begin{cases} 8h = 4n - 3a - 5, \\ 8i = 4n + a - 2b - 1, \\ 8k = 4n + a - 1, \\ 8l = 4n + a + 2b - 1, \\ 8m = 4n - a + 1. \end{cases}$$

Dans le cas actuel, les produits de deux périodes deviennent

$$\begin{aligned} \omega\omega' &= i\omega + l\omega' + m\omega'' + m\omega''', \\ \omega'\omega'' &= m\omega + i\omega' + l\omega'' + m\omega''', \\ \omega''\omega''' &= m\omega + m\omega' + i\omega'' + l\omega''', \\ \omega'''\omega &= l\omega + m\omega' + m\omega'' + i\omega''', \\ \omega\omega'' &= k\omega + m\omega' + k\omega'' + m\omega''', \\ \omega'\omega''' &= m\omega + k\omega' + m\omega'' + k\omega''', \end{aligned}$$

et on en conclut

$$\begin{aligned} B = \sum \omega\omega' &= (i + k + l + 3m)(\omega + \omega' + \omega'' + \omega''') \\ &= -(i + k + l + 3m) = -3n. \end{aligned}$$

La somme des périodes étant égale à -1, en l'élevant au carré, on a

$$\sum \omega^2 + 2\sum \omega\omega' = 1,$$

puis

$$\sum \omega^2 = 6n + 1.$$

Formons le produit de $\omega\omega''$ par $\omega'\omega'''$ et nous aurons

$$\begin{aligned} D = \omega\omega'\omega''\omega''' = mk\sum \omega^2 &+ 2mk(\omega\omega'' + \omega'\omega''') \\ &+ (m^2 + k^2)(\omega\omega' + \omega\omega''' + \omega''\omega''' + \omega'\omega''); \end{aligned}$$

or on a

$$\omega\omega' + \omega\omega''' + \omega''\omega''' + \omega'\omega'' = -(i + l + 2m) = -2n,$$
$$\omega\omega'' + \omega'\omega''' = -(k + m) = -n,$$

on en conclut pour D

$$D = mk(6n + 1) - 2mkn - 2n(m^2 + k^2) = -2n^3 + mk(8n + 1)$$

ou

$$D = -2n^3 + mkp.$$

Cherchons maintenant le coefficient C. En multipliant $\omega'\omega''$ par ω, on obtient

$$\begin{aligned}\omega\omega'\omega'' &= m\omega^2 + i\omega\omega' + l\omega\omega'' + m\omega\omega''' \\ &= m(h\omega + i\omega' + k\omega'' + l\omega''' + 2n) + i(i\omega + l\omega' + m\omega'' + m\omega''') \\ &\quad + l(k\omega + m\omega' + k\omega'' + m\omega''') + m(l\omega + m\omega' + m\omega'' + i\omega''')\end{aligned}$$

ou

$$\begin{aligned}\omega\omega'\omega'' = {} & (hm + i^2 + kl + ml)\omega + (mi + il + ml + m^2)\omega' \\ & + (mk + mi + kl + m^2)\omega'' + (2ml + 2mi)\omega''' + 2mn.\end{aligned}$$

Écrivons, pour abréger,

$$\omega\omega'\omega'' = M\omega + N\omega' + P\omega'' + Q\omega''' + 2mn,$$

nous aurons aussi

$$\begin{aligned}\omega'\omega''\omega''' &= M\omega' + N\omega'' + P\omega''' + Q\omega + 2mn, \\ \omega''\omega'''\omega &= M\omega'' + N\omega''' + P\omega + Q\omega' + 2mn, \\ \omega'''\omega\omega' &= M\omega''' + N\omega + P\omega' + Q\omega'' + 2mn,\end{aligned}$$

et en ajoutant ces quatre expressions, on a

$$C = -(M + N + P + Q) + 8mn.$$

Ensuite on a

$$\begin{aligned}M + N + P + Q &= hm + i^2 + il + 2kl + 4ml + 4mi + 2m^2 + mk \\ &= m(h + k) + i(i + l) + 2kl + 4m(i + l) + 2m^2,\end{aligned}$$

et en s'appuyant sur les égalités $h + k = 2m - 1$, $i + l = 2k$

$$\begin{aligned} M + N + P + Q &= m(2m - 1) + 2k(i + l) + 8mk + 2m^2 \\ &= 4m^2 - m + 4k^2 + 8mk = 4(m + k)^2 - m \\ &= 4n^2 - m, \end{aligned}$$

et on en conclut enfin

$$C = -(4n^2 - m) + 8mn = -4n^2 + mp.$$

Donc l'équation qui donne les quatre périodes lorsque p est de la forme $8n + 1$ est

$$(A) \qquad x^4 + x^3 - 3nx^2 + (4n^2 - mp)x - 2n^3 + mkp = 0.$$

7. Supposons maintenant

$$p = 8n + 5.$$

Les termes de la figure S se réduisent encore à cinq, et peuvent s'écrire

$$\begin{matrix} h, & i, & k, & l, \\ m, & m, & l, & i, \\ h, & m, & h, & m, \\ m, & l, & i, & m. \end{matrix}$$

On pose

$$p = a^2 + b^2,$$

a étant impair et b pair, et on détermine les signes de a et b comme dans le premier cas. Alors on a les formules suivantes :

$$\begin{aligned} 8h &= 4n + a - 1, \\ 8i &= 4n + a + 2b + 3, \\ 8h &= 4n - 3a + 3, \\ 8l &= 4n + a - 2b + 3, \\ 8m &= 4n - a + 1. \end{aligned}$$

D'après le n° 5, on a pour les produits de deux périodes

$$\begin{aligned}
\omega\omega' &= m\omega + m\omega' + l\omega'' + i\omega''',\\
\omega'\omega'' &= i\omega + m\omega' + m\omega'' + l\omega''',\\
\omega''\omega''' &= l\omega + i\omega' + m\omega'' + m\omega''',\\
\omega'''\omega &= m\omega + l\omega' + i\omega'' + m\omega''',\\
\omega\omega'' &= h\omega + m\omega' + h\omega'' + m\omega''' + 2n + 1,\\
\omega'\omega''' &= m\omega + h\omega' + m\omega'' + h\omega''' + 2n + 1,
\end{aligned}$$

et on en conclut

$$B = -(i + l + h + 3m) + 4n + 2 = -(3n + 1) + 4n + 2 = n + 1.$$

Les carrés de ω, ω', ω'', ω''' sont

$$\begin{aligned}
\omega^2 &= h\omega + i\omega' + k\omega'' + l\omega''',\\
\omega'^2 &= l\omega + h\omega' + i\omega'' + k\omega''',\\
\omega''^2 &= k\omega + l\omega' + h\omega'' + i\omega''',\\
\omega'''^2 &= i\omega + k\omega' + l\omega'' + h\omega''',
\end{aligned}$$

et leur somme est égale à $-(h + i + k + l) = -(2n + 1)$.

Faisons le produit de $\omega\omega''$ par $\omega'\omega'''$, et nous aurons

$$\begin{aligned}
D = \omega\omega'\omega''\omega''' = {} & mh(\omega^2 + \omega'^2 + \omega''^2 + \omega'''^2)\\
& + (m^2 + h^2)(\omega\omega' + \omega'\omega'' + \omega''\omega''' + \omega'''\omega)\\
& + 2mh(\omega\omega'' + \omega'\omega''')\\
& + (2n + 1)(h + m)(\omega + \omega' + \omega'' + \omega''') + (2n + 1)^2,
\end{aligned}$$

et comme on a

$$\begin{aligned}
\omega\omega' + \omega'\omega'' + \omega''\omega''' + \omega'''\omega &= -2n - 1,\\
\omega\omega'' + \omega'\omega''' &= 3n + 2,
\end{aligned}$$

il en résulte, en s'appuyant sur l'égalité $m + h = n$,

$$\begin{aligned} D &= -mh(2n+1) - (m^2+h^2)(2n+1) \\ &\quad + 2mh(3n+2) - (2n+1)(h+m) + (2n+1)^2 \\ &= -(2n+1)(m+h)^2 + (8n+5)mh - (2n+1)n + (2n+1)^2 \\ &= (2n+1)(-n^2+n+1) + (8n+5)mh \\ &= pmh - (2n+1)(n^2-n-1). \end{aligned}$$

Il reste à déterminer le coefficient C. Pour cela, multiplions $\omega\omega'$ par ω'', et nous aurons

$$\begin{aligned} \omega\omega'\omega'' &= m\omega\omega'' + m\omega'\omega'' + l\omega''^2 + i\omega''\omega''' \\ &= m(h\omega + m\omega' + h\omega'' + m\omega''' + 2n + 1) \\ &\quad + m(i\omega + m\omega' + m\omega'' + l\omega''') + l(k\omega + l\omega' + h\omega'' + i\omega''') \\ &\quad + i(l\omega + i\omega' + m\omega'' + m\omega''') \end{aligned}$$

ou

$$\begin{aligned} \omega\omega'\omega'' = {} & (mh + mi + lk + il)\,\omega + (2m^2 + l^2 + i^2)\,\omega' \\ & + (mh + m^2 + lh + im)\,\omega'' \\ & + (m^2 + ml + il + mi)\,\omega''' + m(2n+1). \end{aligned}$$

Au lieu de cette formule, écrivons, pour abréger,

$$\omega\omega'\omega'' = M\omega + N\omega' + P\omega'' + Q\omega''' + (2n+1)m,$$

et nous en déduisons aisément

$$C = -(M + N + P + Q) + 4m(2n+1).$$

On a ensuite

$$M + N + P + Q = 2mh + 2im + m(i+l) + (i+l)^2 + 4m^2 + l(k+h),$$

et en se fondant sur les égalités $i + l = 1 + 2h$, $k + h = 2m$, on a

$$M + N + P + Q = 4mh + 2m(i+l) + m + 4h^2 + 4m^2 + 4h + 1,$$

et, en remplaçant $i + l$ par $1 + 2h$,

$$M + N + P + Q = [2(m+h) + 1]^2 - m = (2n+1)^2 - m.$$

Donc on a

$$\begin{aligned} C &= -(2n+1)^2 + m + 4m(2n+1) \\ &= -(2n+1)^2 + m(8n+5) = -(2n+1)^2 + mp, \end{aligned}$$

et l'équation qui donne les quatre périodes, lorsque p est de la forme $8n+5$, est

$$(B) \quad \left\{ \begin{aligned} &x^4 + x^3 + (n+1)x^2 + [(2n+1)^2 - mp]x \\ &\qquad + pmh - (2n+1)(n^2 - n - 1) = 0. \end{aligned} \right.$$

8. Résolvons les équations (A) et (B); mais auparavant exprimons les coefficients au moyen des seuls nombres a et b.

Dans le cas où $p = 8n+1$, on a

$$n = \frac{a^2-1}{8} + \frac{b^2}{8}, \quad 8m = 4n - a + 1 = \frac{(a-1)^2 + b^2}{2},$$
$$8k = 4n + a - 1 = \frac{(a-1)(a+3) + b^2}{2},$$

et l'équation (A) par des transformations convenables devient

$$\begin{aligned} &(4x - a + 1)^3 (4x + 3a + 1) \\ &\quad - \frac{3b^2}{8}\left(x - \frac{a-1}{4}\right)^2 - \frac{ab^2}{16}\left(x - \frac{a-1}{4}\right) + \frac{b^4}{256} = 0. \end{aligned}$$

Posons

$$x - \frac{a-1}{4} = y,$$

et nous aurons l'équation plus simple

$$y^4 + ay^3 - \frac{3b^2}{8}y^2 - \frac{ab^2}{16}y + \frac{b^4}{256} = 0.$$

Faisons

$$\frac{b}{a} = \mu, \quad \frac{y}{a} = z,$$

et nous aurons l'équation

$$z^4 + z^3 - \frac{3}{8}\mu^2 z^2 - \frac{\mu^2}{16}z + \frac{\mu^4}{256} = 0;$$

en posant $\sqrt{1+\mu^2}=\varepsilon$, on en conclut facilement pour les quatre racines

$$z=\frac{-1\pm\varepsilon}{4}\pm\frac{1}{4}\sqrt{2\varepsilon^2\mp 2\varepsilon},$$

expressions dans lesquelles il faut prendre en avant des deux ε des signes contraires, et on en conclut

$$x=\frac{-1\pm a\varepsilon}{4}\pm\frac{a}{4}\sqrt{2\varepsilon^2\mp 2\varepsilon},$$

pour les quatre périodes de l'équation $\frac{x^p-1}{x-1}=0$, lorsque p est de la forme $8n+1$. Si on s'occupe de la congruence

$$\frac{x^p-1}{x-1}\equiv 0 \pmod{q},$$

toutes les équations précédentes doivent être changées en des congruences suivant le module q, et on a pour l'expression des quatre périodes

$$x\equiv\frac{-1\pm a\varepsilon}{4}\pm\frac{a}{4}\sqrt{2\varepsilon^2\mp 2\varepsilon} \pmod{q}.$$

Si a est $\equiv 0$, la congruence qui donne y devient

$$y^4-\frac{3b^2}{8}y^2+\frac{b^4}{256}\equiv 0 \pmod{q},$$

et on en conclut

$$y\equiv\pm\frac{b}{4}(1\pm\sqrt{2}),\quad x\equiv\frac{-1}{4}\pm\frac{b}{4}(1\pm\sqrt{2}).$$

Dans le cas où $p=8n+5$, on a

$$p=a^2+b^2,\quad m=\frac{(a-1)(a+3)+b^2}{16},\quad h=\frac{a^2+2a-7+b^2}{16},$$
$$n=\frac{a^2-5}{8}+\frac{b^2}{8},$$

et l'équation (B) se change par la substitution de ces nombres en la

suivante

$$\left(x+\frac{a+1}{4}\right)^2\left[\left(x-\frac{a-1}{4}\right)^2+\frac{a^2}{4}\right]$$
$$+\frac{b^2}{8}\left(x+\frac{a+1}{4}\right)^2+\frac{ab^2}{16}\left(x+\frac{a+1}{4}\right)+\frac{a^2b^2}{32}+\frac{9b^4}{256}=0.$$

Posons

$$x+\frac{a+1}{4}=y,$$

et nous avons

$$y^4-ay^3+\frac{4a^2+b^2}{8}y^2+\frac{ab^2}{16}y+\frac{a^2b^2}{32}+9\frac{b^4}{256}=0.$$

Faisons

$$\frac{b}{a}=\mu,\quad \frac{y}{a}=z,$$

et nous aurons l'équation

$$z^4-z^3+\frac{4+\mu^2}{8}z^2+\frac{\mu^2}{16}z+\frac{1}{32}\left(\mu^2+\frac{9\mu^4}{8}\right)=0,$$

dont les racines sont, en posant encore $\sqrt{1+\mu^2}=\varepsilon$,

$$z=\frac{1\pm\varepsilon}{4}\pm\frac{1}{4}\sqrt{2\varepsilon^2\pm 2\varepsilon}\sqrt{-1},$$

et les quatre périodes sont renfermées dans l'expression

$$x=\frac{-1\mp a\varepsilon}{4}\pm\frac{a}{4}\sqrt{2\varepsilon^2\mp 2\varepsilon}\sqrt{-1}.$$

Toutes ces équations doivent être changées en congruences suivant le module q, si on s'occupe des périodes de la congruence

$$\frac{x^p-1}{x-1}\equiv 0 \pmod{q}.$$

Si a est $\equiv 0$, la congruence en y se réduit à

$$y^4+\frac{b^2}{8}y^2+\frac{9b^4}{256}\equiv 0,$$

ou à

$$y \equiv \pm \frac{b}{4}(1 \pm \sqrt{-2}),$$

et on obtient pour les périodes

$$x \equiv -\frac{1}{4} \pm \frac{b}{4}(1 \pm \sqrt{-2}) \pmod{q}.$$

Comment on peut reconnaître si le nombre premier q appartient à A *ou à* C *par rapport à p.*

9. Supposons d'abord p de la forme $8n + 1$; les périodes de la congruence binôme ont pour valeurs

$$\frac{-1 \pm a\varepsilon}{4} \pm \frac{a}{4}\sqrt{2\varepsilon^2 \mp 2\varepsilon} \pmod{q}, \tag{1}$$

et se réduisent dans le cas particulier de $a \equiv 0$ à

$$\frac{-1}{4} \pm \frac{b}{4}(1 \pm \sqrt{2}). \pmod{q}.$$

Donc, toutes les fois que a est $\equiv 0$, les périodes seront réelles si 2 est résidu quadratique de q, ou lorsque q est de la forme $8n \pm 1$, et les périodes sont imaginaires dans le cas contraire. Au reste ce cas peut être regardé comme renfermé dans le cas général en faisant $a \equiv 0$ et $a\varepsilon \equiv b$.

Disons maintenant dans quels cas l'expression (1) est réelle. Il faut d'abord que $\varepsilon \equiv \sqrt{1 + \mu^2} \pmod{q}$ soit réel; ce qui aura lieu toutes les fois que q sera résidu quadratique de p (n° **3**).

Cette condition étant supposée remplie, il faut de plus pour la réalité des périodes que les deux quantités

$$2\varepsilon^2 \pm 2\varepsilon$$

soient des résidus quadratiques de q; ce qui a toujours lieu quand

l'une d'elles l'est, puisque leur produit

$$(2\varepsilon^2 + 2\varepsilon)(2\varepsilon^2 - 2\varepsilon) \equiv 4\varepsilon^2\mu^2$$

est un résidu quadratique.

Alors rappelons-nous que la condition pour que q soit résidu biquadratique de p est que les quatre périodes soient réelles, et on en conclut le théorème suivant :

Si le nombre q est résidu quadratique de $p = 8n + 1 = a^2 + b^2$; posons $\frac{b}{a} \equiv \mu$, $1 + \mu^2$ sera un résidu quadratique $\equiv \varepsilon^2 \pmod{q}$ et ε étant l'une des deux valeurs de $\sqrt{1 + \mu^2} \pmod{q}$, la condition pour que q soit résidu biquadratique de p est que $2\varepsilon^2 + 2\varepsilon$ soit résidu quadratique de q. En particulier q est résidu biquadratique de p toutes les fois que b est $\equiv 0$, et toutes les fois que a étant $\equiv 0$, q est de la forme $8n \pm 1$.

Supposons ensuite p de la forme $8n + 5$. Les périodes de la congruence binôme ont pour valeurs

$$\frac{-1 \pm a\varepsilon}{4} \pm \frac{a}{4}\sqrt{2\varepsilon^2 \pm 2\varepsilon}\sqrt{-1} \pmod{q}.$$

Si q est de la forme $4n + 1$, -1 est résidu quadratique de q, donc $\sqrt{-1} \pmod{q}$ est réel. Pour que les périodes soient réelles, il faut que $1 + \mu^2$ soit un résidu quadratique $\equiv \varepsilon^2$ et que la quantité $2\varepsilon^2 + 2\varepsilon$ soit aussi résidu quadratique de q. Alors q sera résidu biquadratique de p.

Si q est de la forme $4n + 3$, considérons le caractère biquadratique de $-q$. Comme -1 est non résidu quadratique de q, $\sqrt{-1}$ est imaginaire; q et par suite $-q$ étant supposés résidus quadratiques de p, $1 + \mu^2$ est un résidu de q, $\equiv \varepsilon^2 \pmod{q}$. Pour que q soit résidu biquadratique de p, il faudra que les périodes soient réelles ou que $-(2\varepsilon^2 + 2\varepsilon)$ soit un résidu quadratique, ou encore que $2\varepsilon^2 + 2\varepsilon$ soit un non résidu de q. Donc comme -1 appartient à C par rapport à p, $-q$ appartient à A ou à C par rapport à p suivant que $2\varepsilon^2 + 2\varepsilon$ est résidu quadratique ou non résidu par rapport à q.

Donc en observant que $+q$ et $-q$ appartiennent tous deux à A ou

tous deux à C, lorsque p est de la forme $8n+1$, on en conclut le théorème suivant : Si on prend dans $\pm q$ le signe $+$ ou le signe $-$ suivant que $q=4n+1$ ou $4n-1$; $\pm q$ est résidu quadratique du nombre premier $p=a^2+b^2$, lorsque, en désignant par μ la quantité $\frac{b}{a}\,(\text{mod. } q)$, $1+\mu^2$ est un résidu quadratique de q, $\equiv \varepsilon^2\,(\text{mod. } q)$, et $\pm q$ sera résidu biquadratique ou simplement quadratique par rapport à p, suivant que $2\varepsilon^2+2\varepsilon$ est résidu ou non-résidu quadratique de q.

A cela on peut ajouter que si a est $\equiv 0\,(\text{mod. } q)$, $\pm q$ est résidu biquadratique de p ou simplement résidu selon que q est de la forme $8n\pm 1$ ou $8n\pm 3$. C'est ce que nous avons vérifié quand p est de la forme $8n+1$, et ce qui est aussi aisé à reconnaître pour $p=8n+5$.

Formules qui donnent les classes du rapport $\frac{b}{a}\,(\text{mod. } q)$.

10. Nous venons de voir comment les valeurs de $\frac{b}{a}\,(\text{mod. } q)$ peuvent servir à distinguer si un nombre premier q appartient à A ou à C ou aux groupes B et D suivant le module p. Mais on peut aller plus loin; car on peut exprimer par une même formule les classes du rapport $\frac{b}{a}\,(\text{mod. } q)$, pour lesquelles q est résidu biquadratique, simplement résidu, ou non-résidu de p.

Nous avons déjà montré (n° **3**) comment on peut distinguer les deux classes qui se rapportent aux groupes A et C des deux classes qui se rapportent aux groupes B et D; il nous faut maintenant séparer les deux premières.

Supposons d'abord $p=4n+1$; ces deux classes sont données par la formule

$$\frac{b}{a}\equiv\mu\equiv\varphi\,\frac{1-\mathrm{L}}{1+\mathrm{L}}\quad(\text{mod. } q),$$

où l'on prend pour L un résidu quadratique $\equiv l^2$, et pour φ une valeur de $\sqrt{-1}\,(\text{mod. } q)$. On a

$$1+\mu^2\equiv 1-\frac{(1-l^2)^2}{(1+l^2)^2}\equiv\frac{4l^2}{(1+l^2)^2}.$$

Posons

$$\frac{2l}{1+l^2} \equiv \varepsilon,$$

et nous aurons

$$2(\varepsilon^2+\varepsilon) \equiv 4l\frac{(1+l)^2}{(1+l^2)^2} \pmod{q};$$

et cette expression sera résidu quadratique ou non en même temps que l.

Il résulte donc de ce que nous avons prouvé dans le numéro précédent, que q appartient au groupe A ou C, selon que L est résidu biquadratique de q ou simplement résidu.

Désignons par G la plus petite racine primitive de q, adoptons pour φ

$$\varphi \equiv G^{\frac{p-1}{4}},$$

et désignons par α, β, γ, δ les valeurs de $\frac{b}{a} \pmod{q}$ pour lesquelles q appartient aux groupes A, B, C, D; nous aurons

$$\alpha \equiv \varphi\frac{1-G^{4e}}{1+G^{4e}}, \quad \gamma \equiv \varphi\frac{1-G^{4e+2}}{1+G^{4e+2}},$$

formules où il suffira de donner à e les valeurs 0, 1, 2,..., $\frac{q-5}{4}$, de sorte que l'on aura $\frac{q-1}{4}$ nombres α, $\frac{q-1}{4}$ nombres γ, et il restera $\frac{q-1}{2}$ nombres pour les classes β et δ.

Passons au cas où q est de la forme $4n+3$; les deux classes α et γ sont données par la formule

$$\mu \equiv i\frac{1-H}{1+H},$$

dans laquelle i représente $\sqrt{-1}$, et H une des racines de la congruence

$$(a) \qquad z^{\frac{q+1}{2}} \equiv 1 \pmod{q}.$$

Désignons par j une racine primitive de la congruence binôme

$$(b) \qquad z^{q+1} \equiv 1 \pmod{q};$$

toutes les racines sont congrues aux nombres

$$1, j, j^2, \ldots, j^q;$$

disposons-les sur quatre lignes

$$\begin{aligned} &1, j^4, j^8, \ldots, j^{q-3}, \\ &j, j^5, j^9, \ldots, \\ &j^2, j^6, j^{10}, \ldots, \\ &j^3, j^7, j^{11}, \ldots, \end{aligned}$$

Toutes ces quantités sont des nombres complexes de la forme $A + Bi$, car elles appartiennent à la congruence

$$z^{q^2-1} \equiv 1 \pmod{q},$$

dont les racines imaginaires satisfont à des congruences irréductibles du second degré, et, q étant de la forme $4n + 3$, elles sont de la forme $A + Bi$. Nous distinguerons tous ces nombres complexes en disant qu'ils appartiennent aux groupes A, B, C ou D, suivant qu'ils seront dans la première ligne, dans la deuxième, la troisième ou la quatrième.

Les nombres complexes des groupes A ou C sont les racines de la congruence (a), et nous pouvons dans l'expression de μ remplacer H par l^2 et nous en conclurons

$$1 + \mu^2 \equiv \frac{4l^2}{(1+l^2)^2} \equiv \left(\frac{2l}{1+l^2}\right)^2;$$

posons

$$\frac{2l}{1+l^2} \equiv \varepsilon,$$

ε sera réel; comme nous l'avons vu (n° 3).

Nous avons ensuite

$$2(\varepsilon^2+\varepsilon)\equiv 4l\frac{(1+l)^2}{(1+l^2)^2}\pmod{q}.$$

Si l appartient à A ou à C, le second membre est le carré du nombre complexe

$$2l\frac{1+l}{1+l^2},$$

et en l'élevant à la puissance p, on le reconnaît réel; donc $2(\varepsilon^2+\varepsilon)$ est un résidu quadratique. Mais si l appartient à B ou à D, le second membre n'est pas congru au carré d'un nombre complexe qui renferme le nombre réel comme cas particulier; donc $2(\varepsilon^2+\varepsilon)$ est un non-résidu quadratique.

De ce qui précède et de la fin du n° 9, nous concluons que les classes α et γ de la quantité $\frac{b}{a}\pmod{q}$ sont données par les formules

$$\alpha\equiv i\frac{1-j^{4e}}{1+j^{4e}},\quad \gamma\equiv i\frac{1-j^{4e+2}}{1+j^{4e+2}},$$

dans lesquelles il suffit de donner à e les valeurs $0, 1, 2, \ldots, \frac{q-3}{4}$.

Formules qui donnent trois nombres consécutifs qui ont le même caractère quadratique par rapport à un nombre premier q.

11. D'après ce que nous avons vu précédemment, il est facile de déterminer un nombre qui soit précédé et suivi de deux nombres ayant un même caractère quadratique identique ou différent à celui du nombre intermédiaire. Afin d'éviter les longueurs inutiles, donnons seulement les formules qui déterminent trois nombres consécutifs qui ont le même caractère quadratique.

Nous avons déterminé les nombres ε qui jouissent de la propriété que les deux expressions $2\varepsilon(\varepsilon\pm 1)$ soient des résidus quadratiques, et alors 2ε, $\varepsilon+1$, $\varepsilon-1$ ont tous trois le même caractère quadratique.

Supposons q de la forme $8n+1$ ou de la forme $8n+7$, 2 est

résidu quadratique de q, et $\varepsilon - 1$, ε, $\varepsilon + 1$ sont trois nombres qui ont le même caractère quadratique. Si q est de la forme $8n + 1$, cette forme étant comprise dans $4n + 1$, on a, d'après la formule du n° **10**, pour le nombre du milieu,

$$(a) \qquad \varepsilon \equiv \pm \frac{2G^{2e}}{1 + G^{4e}} \pmod{q}.$$

Si q est de la forme $8n + 7$, qui est renfermée dans $4n + 3$, on a

$$(b) \qquad \varepsilon \equiv \pm \frac{2j^{2e}}{1 + j^{4e}}.$$

Nous avons aussi déterminé des nombres ε qui jouissent de la propriété que $2\varepsilon(\varepsilon \pm 1)$ représentent deux non-résidus. Alors 2ε a un caractère quadratique contraire à celui de $\varepsilon + 1$ et de $\varepsilon - 1$; donc si 2 est un non-résidu, ce qui a lieu pour $q = 8n + 3$ et $8n + 5$, les trois nombres $\varepsilon - 1$, ε, $\varepsilon + 1$ ont le même caractère quadratique. Si $q = 8n + 5$, le nombre intermédiaire est donné par la formule

$$(c) \qquad \varepsilon \equiv \pm \frac{2G^{2e+1}}{1 + G^{4e+2}},$$

et si $q = 8n + 3$, par

$$(d) \qquad \varepsilon \equiv \pm \frac{2j^{2e+1}}{1 + j^{4e+2}}.$$

Proposons-nous de déterminer combien il y a de résidus quadratiques suivis et précédés d'un résidu quadratique. Si q est de la forme $4n + 3$, on doit remarquer que de deux nombres qui ne diffèrent que par le signe, l'un seulement est résidu de q; donc on doit prendre les formules (b) et (d) avec e quelconque, mais en choisissant l'un des deux signes; donc le nombre cherché est $\frac{q+1}{8}$.

Si q est de la forme $4n + 1$, les nombres considérés sont donnés par les formules (a) et (c), mais avec la condition que $G^{4e} + 1$ ou $G^{4e+2} + 1$ soient des résidus quadratiques. Posons

$$q = A^2 + B^2,$$

A^2 étant le carré impair, B^2 le carré pair et le signe de A choisi de manière que $A \equiv 1 \pmod 4$; si nous adoptons les notations du n° **6**, on voit que si $q = 8n + 1$, le nombre cherché est égal à

$$(00) + (02) = \frac{q-1}{8} - \frac{A+3}{4},$$

et que si $q = 8n + 5$, il a pour valeur

$$(20) + (22) = \frac{q-5}{8} + \frac{A+3}{4}.$$

Distinction des groupes A, B, C, D.

12. On reconnaît par induction que si p est un nombre premier $4n + 1$ égal à $a^2 + b^2$ (a et b étant choisis comme il a été dit n° **6**), le caractère biquadratique du nombre premier $\pm q$ par rapport au nombre p dépend uniquement de la valeur du rapport $\frac{b}{a}$ prise suivant le module q. Et déjà nous savons comment on peut reconnaître si le rapport $\frac{b}{a}$ caractérise un résidu biquadratique, un résidu simplement quadratique ou un non-résidu, et par conséquent si $\pm q$ appartient aux groupes A, C ou au deux groupes B et D réunis ensemble.

Mais jusqu'à présent nous n'avons rien dit qui permît de distinguer les deux groupes B et D. La détermination des valeurs des quatre périodes de la congruence $\frac{x^p - 1}{x - 1} \equiv 0 \pmod q$ nous avait suffi pour résoudre la première partie de la question, et nous allons montrer que la seconde se résoudra facilement dès que l'on sera parvenu à déterminer l'ordre des quatre périodes.

Ces quatre périodes sont

$$\omega \equiv x + x^{a'} + x^{a''} + x^{a'''} + \ldots,$$
$$\omega' \equiv x^{b'} + x^{b''} + x^{b'''} + \ldots,$$
$$\omega'' \equiv x^{c'} + x^{c''} + x^{c'''} + \ldots,$$
$$\omega''' \equiv x^{d'} + x^{d''} + \ldots,$$

1, a', a'',... étant les nombres A selon le module p; b', b'', b''',... les nombres B; c', c'',... les nombres C; d', d'',... les nombres D.

Ces périodes ne sont pas complétement déterminées, car nous n'avons pas assigné une valeur à la racine x qui peut être l'une quelconque; mais si, ayant pris pour x une racine, on en prend ensuite une autre, il est aisé de voir que l'ordre circulaire ne sera pas changé. Ainsi divisons un cercle en quatre parties égales, puis, tournant dans un sens déterminé, plaçons-y les périodes ω, ω', ω'', ω''' successivement aux points de division que l'on rencontre; quelle que soit la racine x, l'ordre des périodes sur ce cercle restera le même.

Si q est résidu biquadratique de p, comme nous l'avons déjà observé, en élevant les périodes à la puissance q, elles ne changent pas et par conséquent elles sont réelles. Supposons maintenant que q appartienne aux groupes C, B ou D par rapport à p.

Si q appartient à C, on a

$$\omega^q \equiv x^q + x^{a'q} + x^{a''q} + \ldots \equiv \omega'',$$
$$\omega'^q \equiv x^{b'q} + x^{b''q} + \ldots \equiv \omega''', \quad \omega''^q \equiv \omega, \quad \omega'''^q \equiv \omega'.$$

Si q appartient à B, on a

$$\omega^q \equiv \omega', \quad \omega'^q \equiv \omega'', \quad \omega''^q \equiv \omega''', \quad \omega'''^q \equiv \omega.$$

Enfin, si q appartient à D, on obtient

$$\omega^q \equiv \omega''', \quad \omega'^q \equiv \omega, \quad \omega''^q \equiv \omega', \quad \omega'''^q \equiv \omega''.$$

Il résulte de là que, pour la recherche qui nous occupe, il suffit d'examiner dans quel ordre se suivent sur le cercle les valeurs des quatre périodes, et c'est la question qui va nous occuper.

Introduction d'un angle v dans l'expression des quatre périodes de l'équation $\frac{x^p - 1}{x - 1} = 0$.

13. Reprenons les valeurs des quatre périodes; mais, au lieu de supposer qu'il s'agisse des racines de la congruence binôme, commençons

par nous occuper des périodes relatives aux racines de l'équation

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

D'abord si p est de la forme $8n + 1$, nous savons que les périodes ont pour valeurs

$$\frac{-1 \pm a\varepsilon}{4} \pm \frac{a}{4}\sqrt{2\varepsilon^2 \mp 2\varepsilon}.$$

Posons

$$\frac{b}{a} = \operatorname{tang} v,$$

b et a étant déterminés comme nous avons vu, $\frac{b}{a}$ est un nombre positif ou négatif, et il nous suffira de faire varier v entre zéro et π, c'est-à-dire entre zéro et $\frac{\pi}{2}$ ou entre $\frac{\pi}{2}$ et π, suivant que $\frac{b}{a}$ sera positif ou négatif.

On aura

$$\varepsilon = \sqrt{1 + \frac{b^2}{a^2}} = \sqrt{1 + \operatorname{tang}^2 v} = \pm \frac{1}{\cos v}.$$

Prenons par exemple

$$\varepsilon = -\frac{1}{\cos v},$$

et il en résultera

$$2\varepsilon^2 - 2\varepsilon = 2\,\frac{1 + \cos v}{\cos^2 v} = \frac{4\cos^2\frac{v}{2}}{\cos^2 v},$$

$$\sqrt{2\varepsilon^2 - 2\varepsilon} = \pm \frac{2\cos\frac{v}{2}}{\cos v};$$

de même on a

$$\sqrt{2\varepsilon^2 + 2\varepsilon} = \pm \frac{2\sin\frac{v}{2}}{\cos v},$$

et on en conclut que les périodes ont les valeurs suivantes :

$$\frac{-1}{4} - \frac{a\left(1+2\cos\frac{v}{2}\right)}{4\cos v}, \quad \frac{-1}{4} - \frac{a\left(1-2\cos\frac{v}{2}\right)}{4\cos v},$$

$$-\frac{1}{4} + \frac{a\left(1-2\sin\frac{v}{2}\right)}{4\cos v}, \quad -\frac{1}{4} + \frac{a\left(1+2\sin\frac{v}{2}\right)}{4\cos v}.$$

On sait que les quatre périodes sont toutes exprimables par l'une d'entre elles. Pour obtenir ω' au moyen de ω, employons les formules du n° **6**

$$\omega + \omega' + \omega'' + \omega''' = -1,$$

$$\omega\omega' = i\omega + l\omega' + m(\omega'' + \omega'''),$$

et l'on en tire

$$\omega' = \frac{(i-m)\omega - m}{\omega - l + m}$$

ou

$$\omega' = \frac{4(a-b-1)\omega - a^2 - b^2 + 2a - 1}{16\omega - 4(a+b-1)}.$$

Puisque nous pouvons prendre pour ω la période que nous voulons, posons

$$\omega = -\frac{1}{4} - \frac{a\left(1+2\cos\frac{v}{2}\right)}{4\cos v},$$

et déduisons-en l'expression de ω' en fonction de v. Désignons par N et D le numérateur et le dénominateur, nous aurons

$$D = 4(4\omega - a - b + 1) = -\frac{4a}{\cos v}\left(\sin v + 2\cos^2\frac{v}{2} + 2\cos\frac{v}{2}\right),$$

$$N = (a - a\operatorname{tang} v - 1)\left(-1 - a\frac{1+2\cos\frac{v}{2}}{\cos v}\right) - \frac{a^2}{\cos^2 v} + 2a - 1$$

$$= -\frac{a^2}{\cos v}\left[\sin v + 2\cos^2\frac{v}{2} + 2\cos\frac{v}{2} - \operatorname{tang} v\left(-\sin v + 2\cos^2\frac{v}{2} + 2\cos\frac{v}{2}\right)\right]$$

$$+ \frac{a}{\cos v}\left(\sin v + 2\cos^2\frac{v}{2} + 2\cos\frac{v}{2}\right).$$

On en tire

$$\omega' = \frac{N}{D} = \frac{a-1}{4} - \frac{a}{4}\operatorname{tang}\upsilon \frac{-\sin\upsilon + 2\cos^2\frac{\upsilon}{2} + 2\cos\frac{\upsilon}{2}}{\sin\upsilon + 2\cos^2\frac{\upsilon}{2} + 2\cos\frac{\upsilon}{2}}.$$

Or, on a

$$-\frac{\operatorname{tang}\upsilon}{4}\frac{-\sin\upsilon + 2\cos^2\frac{\upsilon}{2} + 2\cos\frac{\upsilon}{2}}{\sin\upsilon + 2\cos^2\frac{\upsilon}{2} + 2\cos\frac{\upsilon}{2}} = \frac{\sin\upsilon}{4\cos\upsilon}\frac{\sin\frac{\upsilon}{2} - \cos\frac{\upsilon}{2} - 1}{\sin\frac{\upsilon}{2} + \cos\frac{\upsilon}{2} + 1}$$

$$= \frac{1}{2\cos\upsilon}\left(\sin^2\frac{\upsilon}{2} - \sin\frac{\upsilon}{2}\right);$$

et il en résulte enfin

$$\omega' = -\frac{1}{4} + \frac{a\left(1 - 2\sin\frac{\upsilon}{2}\right)}{4\cos\upsilon}.$$

ω' se déduit donc de ω par le changement de υ en $\upsilon + \pi$; ω'' doit évidemment se déduire par le même changement de ω' et ω''' de ω'', et on a par conséquent

$$\omega = -\frac{1}{4} - \frac{a\left(1 + 2\cos\frac{\upsilon}{2}\right)}{4\cos\upsilon}, \quad \omega'' = -\frac{1}{4} - \frac{a\left(1 + 2\cos\frac{\upsilon}{2}\right)}{4\cos\upsilon},$$

$$\omega' = -\frac{1}{4} + \frac{a\left(1 + 2\sin\frac{\upsilon}{2}\right)}{4\cos\upsilon}, \quad \omega''' = -\frac{1}{4} + \frac{a\left(1 + 2\sin\frac{\upsilon}{2}\right)}{4\cos\upsilon},$$

et ces quatre formules sont renfermées dans la suivante

$$\omega^{(k)} = -\frac{1}{4} - \frac{a\left(1 + 2\cos\frac{\upsilon + k\pi}{2}\right)}{4\cos(\upsilon + k\pi)}.$$

14. Passons au cas où p est de la forme $8n + 5$. Les quatre périodes ont pour valeurs

$$\frac{-1 \pm a\varepsilon}{4} \pm \frac{a}{4}\sqrt{2\varepsilon^2 \pm 2\varepsilon}\sqrt{-1}.$$

Faisons encore $\frac{b}{a} = \operatorname{tang} v$, et les quatre périodes ont pour valeurs

$$(B)\quad \begin{cases} \omega = -\frac{1}{4} + \frac{a}{4\cos v}\left(1 + 2\sqrt{-1}\cos\frac{v}{2}\right), \\ \omega' = -\frac{1}{4} - \frac{a}{4\cos v}\left(1 - 2\sqrt{-1}\sin\frac{v}{2}\right), \\ \omega'' = -\frac{1}{4} + \frac{a}{4\cos v}\left(1 - 2\sqrt{-1}\cos\frac{v}{2}\right), \\ \omega''' = -\frac{1}{4} - \frac{a}{4\cos v}\left(1 + 2\sqrt{-1}\sin\frac{v}{2}\right); \end{cases}$$

mais il faut prouver que ces formules donnent aussi leur ordre. On pourrait employer un calcul analogue à celui qui nous a servi dans le cas de $p = 8n + 1$. Mais ce calcul étant assez long, on peut l'éviter par la remarque suivante.

Que p soit égal à $8n + 1$ ou à $8n + 5$, les expressions des périodes restent dans le même ordre pour toutes les valeurs de p de l'une de ces deux formes; de sorte que, si on le détermine pour une valeur particulière $p = 5$, cette recherche sera faite en même temps pour toutes les valeurs de p de la forme $8n + 5$.

Calculons donc directement les périodes pour $p = 5$.

Les nombres des groupes A, B, C, D par rapport à 5 se réduisent à un seul; 2 est la plus petite racine primitive de 5, et on a

$$A = 1, \quad B = 2, \quad C = 4, \quad D = 3.$$

Soit x une racine quelconque de $\frac{x^5 - 1}{x - 1} = 0$, les périodes se réduisent à un seul terme, et ont pour valeurs

$$\omega = x, \quad \omega' = x^2, \quad \omega'' = x^4, \quad \omega''' = x^3,$$

et si nous prenons pour x

$$\cos\frac{2\pi}{5} + \sqrt{-1}\sin\frac{2\pi}{5},$$

nous aurons

$$\omega = \cos\frac{2\pi}{5} + \sqrt{-1}\sin\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4} + \frac{1}{4}\sqrt{10+2\sqrt{5}}\sqrt{-1},$$

$$\omega' = \cos\frac{4\pi}{5} + \sqrt{-1}\sin\frac{4\pi}{5} = -\frac{\sqrt{5}+1}{4} + \frac{1}{4}\sqrt{10-2\sqrt{5}}\sqrt{-1},$$

$$\omega'' = \cos\frac{8\pi}{5} + \sqrt{-1}\sin\frac{8\pi}{5} = \frac{\sqrt{5}-1}{4} - \frac{1}{4}\sqrt{10+2\sqrt{5}}\sqrt{-1},$$

$$\omega''' = \cos\frac{6\pi}{5} + \sqrt{-1}\sin\frac{6\pi}{5} = -\frac{\sqrt{5}+1}{4} - \frac{1}{4}\sqrt{10-2\sqrt{5}}\sqrt{-1}.$$

Employons ensuite les formules (B), et nous avons $p = 1+4$ et $a \equiv 1 \pmod 4 = 1$, $b \equiv 2 \pmod 5 = 2$; donc $\operatorname{tang} v = 2$, et, en supposant que v varie de zéro à π, nous avons pour $\sin v$ et $\cos v$ les valeurs

$$\sin v = \frac{2}{\sqrt{5}}, \quad \cos v = \frac{1}{\sqrt{5}}.$$

La partie réelle de la première expression (B) est donc

$$-\frac{1}{4} + \frac{a}{4\cos v} = \frac{\sqrt{5}-1}{4},$$

et le coefficient de $\sqrt{-1}$ est

$$\frac{a}{2\cos v}\cos\frac{v}{2} = \frac{a}{2\cos v}\sqrt{\frac{1+\cos v}{2}} = +\frac{1}{4}\sqrt{10+2\sqrt{5}}.$$

La partie réelle de la seconde expression (B) est

$$-\frac{1}{4} - \frac{a}{4\cos v} = -\frac{\sqrt{5}+1}{4},$$

et le coefficient de $\sqrt{-1}$ est

$$\frac{a\sin\frac{v}{2}}{2\cos v} = \frac{a}{2\cos v}\sqrt{\frac{1-\cos v}{2}} = \frac{1}{4}\sqrt{10-2\sqrt{5}};$$

on reconnaît par conséquent l'exactitude des formules (B), que l'on peut réduire à la suivante

$$\omega^{(k)} = -\frac{1}{4} + \frac{a}{4\cos(v + k\pi)}\left(1 + 2\sqrt{-1}\cos\frac{v + k\pi}{2}\right).$$

Sur les racines de la congruence $x^{q-1} \equiv 1$ *ou* $x^{q+1} \equiv 1 \pmod{q}$, *suivant que* q *est de la forme* $4n + 1$ *ou* $4n - 1$.

15. La division de la circonférence en n parties égales dépend de la résolution de l'équation

$$x^n = 1,$$

dont les racines sont renfermées dans la formule

$$\cos\frac{2k\pi}{n} + \sqrt{-1}\sin\frac{2k\pi}{n},$$

k étant susceptible des valeurs $0, 1, 2, \ldots, n-1$.

La théorie de la division du cercle permet de calculer les sinus, cosinus et tangentes d'un arc sous-multiple de la circonférence entière sous la forme algébrique, c'est-à-dire sous la forme d'expressions qui ne sont irrationnelles que par les radicaux. Il suit évidemment de là que les lignes trigonométriques des multiples de cet arc sont elles-mêmes exprimables sous la forme algébrique; prenons ces expressions suivant le module q, et représentons-les par les formules

$$\sin\frac{2k\pi}{n} \pmod{q}, \quad \cos\frac{2k\pi}{n} \pmod{q}, \quad \operatorname{tang}\frac{2k\pi}{n} \pmod{q}.$$

Or, si cherchant à déterminer suivant le module q tous les radicaux dans l'ordre où ils se présentent dans le calcul de ces quantités, on peut successivement les remplacer par des nombres entiers qui leur sont congrus, de sorte que l'on obtienne en définitive pour l'expression complète un nombre entier, nous devrons regarder cette expression comme réelle; mais dans le cas contraire elle doit être considérée comme imaginaire.

D'après cela, étudions les valeurs des expressions des lignes trigono-

métriques de l'arc $\frac{2\pi}{2(q-1)}$ prises suivant le module premier $q = 4n+1$; nous sommes conduit à considérer la congruence

$$x^{2(q-1)} \equiv 1 \pmod{q}, \tag{1}$$

et, d'après les réflexions qui précèdent, on peut représenter les racines par

$$\cos\frac{k\pi}{q-1} + \sqrt{-1}\sin\frac{k\pi}{q-1} \pmod{q}, \tag{2}$$

k ayant les valeurs 0, 1, 2,..., $2q-3$, et $\sqrt{-1}$, à cause de la forme du module, est une quantité réelle que nous désignerons par φ.

La congruence peut se décomposer en les deux suivantes

$$x^{q-1} \equiv 1, \tag{3}$$

$$x^{q-1} \equiv -1. \tag{4}$$

La congruence (3) a toutes ses racines réelles qui sont 1, 2,..., $q-1$, et on peut aussi les représenter par l'expression

$$u \equiv \cos\frac{2k\pi}{q-1} + \varphi\sin\frac{2k\pi}{q-1} \pmod{q}.$$

Les deux parties qui composent u sont elles-mêmes réelles; car deux des racines sont données par

$$\cos\frac{2k\pi}{q-1} \pm \varphi\sin\frac{2k\pi}{q-1},$$

et, puisqu'elles sont toutes deux réelles, il s'ensuit que

$$\sin\frac{2k\pi}{q-1}, \quad \cos\frac{2k\pi}{q-1}, \quad \operatorname{tang}\frac{2k\pi}{q-1}$$

sont réels. Nous pouvons ensuite observer que

$$1 + \operatorname{tang}^2\frac{2k\pi}{q-1}$$

est un résidu quadratique, car cette expression est équivalente à

$$\frac{1}{\cos^2 \frac{2k\pi}{q-1}} \pmod{q},$$

qui est un résidu quadratique, puisque $\cos \frac{2k\pi}{q-1}$ est un entier réel. Posons

$$\frac{1}{\cos \frac{2k\pi}{q-1}} \equiv \varepsilon,$$

et nous aurons pour l'expression de $2(\varepsilon^2 \pm \varepsilon)$

$$\frac{4\cos^2 \frac{k\pi}{q-1}}{\cos^2 \frac{2k\pi}{q-1}}, \quad \frac{4\sin^2 \frac{k\pi}{q-1}}{\cos^2 \frac{2k\pi}{q-1}},$$

qui sont des résidus quadratiques dans le cas où k est pair; mais ces expressions sont au contraire des non-résidus si k est impair, parce que $\sin \frac{k\pi}{q-1}$ et $\cos \frac{k\pi}{q-1}$ sont imaginaires, comme on le reconnait par l'expression générale des racines de la congruence (4) qui est

$$\nu \equiv \cos \frac{(2l+1)\pi}{q-1} + \varphi \sin \frac{(2l+1)\pi}{q-1} \pmod{q};$$

car il est clair que toutes ces racines sont imaginaires, puisque la congruence (4) n'a pas de racine commune avec la congruence (3).

Démontrons maintenant que les tangentes de tous les arcs $0, \frac{\pi}{q-1}, 2\frac{\pi}{q-1}, 3\frac{\pi}{q-1}, \cdots, (q-2)\frac{\pi}{q-1}$, sont incongrues suivant le mod. q. Soit m une racine quelconque de (1); en désignant par α un des arcs précédents, on a

$$\cos\alpha + \varphi \sin\alpha \equiv m,$$

et ensuite

$$\cos\alpha - \varphi \sin\alpha \equiv \frac{1}{m};$$

donc

$$\operatorname{tang}\alpha \equiv \varphi \frac{1-m^2}{1+m^2}.$$

Il est aisé d'en conclure que toutes ces tangentes sont incongrues et peuvent représenter tous les nombres 0, 1, 2, . . . , $q-1$, excepté $+\varphi$ et $-\varphi$.

Si α est de la forme $\frac{2k\pi}{q-1}$, m est réel et m^2 résidu quadratique; si α a au contraire la valeur $\frac{(2k+1)\pi}{q-1}$, m est racine de (4) et m^2 est un nombre réel, mais non-résidu.

16. Étudions ensuite les valeurs des lignes trigonométriques de l'arc $\frac{2\pi}{2(q+1)}$ prises suivant le module premier $q=4n+3$. Nous considérerons la congruence

$$x^{2(q+1)} \equiv 1 \pmod{q}, \tag{1}$$

dont les racines peuvent être représentées par

$$\cos\frac{k\pi}{q+1} + \sqrt{-1}\sin\frac{k\pi}{q+1} \pmod{q};$$

mais ici $\sqrt{-1}$ est imaginaire, et nous le remplacerons par la lettre i.

Décomposons la congruence (1) en les suivantes :

$$x^{q+1} - 1 \equiv 0, \tag{3}$$

$$x^{q+1} + 1 \equiv 0. \tag{4}$$

La congruence (3) a toutes ses racines imaginaires, excepté 1 et -1. Ses racines sont données par

$$u \equiv \cos\frac{2k\pi}{q+1} + i\sin\frac{2k\pi}{q+1} \pmod{q};$$

celles de (4) sont

$$v \equiv \cos\frac{(2l+1)\pi}{q+1} + i\sin\frac{(2l+1)\pi}{q+1}.$$

Remarquons que si on élève les racines v au carré, on obtiendra la moitié des racines u, celles pour lesquelles k est impair.

Soit $u = m + ni$ une racine de (3) autre que 1 et -1, elle satisfait à une congruence irréductible du second degré

$$x^2 + 2ax + b \equiv 0 \pmod{q};$$

or u étant racine, u^q, qui est congru à $m - ni$, est la seconde, et puisque leur produit est $\equiv 1$ d'après (3), b est $\equiv 1$ et la congruence devient

$$x^2 + 2ax + 1 \equiv 0;$$

$a^2 - 1$ est donc un non-résidu, et par suite $1 - a^2$ un résidu. Écrivons donc les racines sous la forme

$$x = -a \pm \sqrt{1 - a^2}\, i.$$

Or, on peut disposer les racines u par couples, tels que

$$\cos\frac{2k\pi}{q+1} + i\sin\frac{2k\pi}{q+1}, \quad \cos\frac{2k\pi}{q+1} - i\sin\frac{2k\pi}{q+1},$$

dont le produit est congru à 1. De ces deux manières de grouper les racines, qui sont évidemment identiques, on conclut que $\cos\frac{2k\pi}{q+1}$ et $\sin\frac{2k\pi}{q+1}$ sont deux nombres entiers réels.

Les racines v appartiennent aussi deux à deux à des congruences irréductibles du second degré, dont les coefficients sont réels; mais accouplons-les autrement et de manière que le produit des deux racines réunies soit congru à l'unité; on aura pour l'un des couples

$$v_1 \equiv \cos\frac{(2l+1)\pi}{q+1} + i\sin\frac{(2l+1)\pi}{q+1},$$
$$v_2 \equiv \cos\frac{(2l+1)\pi}{q+1} - i\sin\frac{(2l+1)\pi}{q+1};$$

ces racines satisfont à la congruence du second degré

$$x^2 + 2ax + 1 \equiv 0 \pmod{q},$$

dans laquelle a n'est pas réel; car s'il l'était, ν étant racine, ν^q serait la seconde, et puisque leur produit est congru à l'unité, on aurait $\nu^{q+1} \equiv 1$, ce qui est absurde; donc $\cos \frac{(2l+1)\pi}{q+1}$ est imaginaire, et nous allons prouver que le sinus l'est aussi.

Posons

$$\operatorname{tang} \frac{2r\pi}{q+1} = b,$$

nous aurons

$$\operatorname{tang} \frac{r\pi}{q+1} \equiv \frac{-1 \pm \sqrt{1+b^2}}{b};$$

or, on a

$$1 + b^2 \equiv \frac{1}{\cos^2 \frac{2r\pi}{q+1}};$$

donc puisque $\cos \frac{2r\pi}{q+1}$ est réel, $\operatorname{tang} \frac{r\pi}{q+1}$ l'est aussi. Posons

$$\sqrt{1+b^2} \equiv \varepsilon,$$

et nous aurons

$$\sin \frac{r\pi}{q+1} \equiv \frac{-1+\varepsilon}{\sqrt{2\varepsilon^2 + 2\varepsilon}}, \quad \cos \frac{r\pi}{q+1} \equiv \frac{b}{\sqrt{2\varepsilon^2 + 2\varepsilon}}.$$

Si r est impair, le cosinus est imaginaire d'après ce que nous avons dit ci-dessus; donc aussi le sinus. Comme nous savons que si r est pair le sinus et le cosinus sont réels, $2\varepsilon^2 + 2\varepsilon$ est résidu ou non suivant que r est pair ou impair.

Désignons par N une racine de la congruence (1), nous pourrons poser

$$\mathrm{N} \equiv \cos \frac{k\pi}{q+1} + i \sin \frac{k\pi}{q+1},$$

et nous en tirerons

$$\operatorname{tang} \frac{k\pi}{q+1} \equiv \varphi \frac{1-\mathrm{N}^2}{1+\mathrm{N}^2}$$

ou

$$\operatorname{tang} \frac{k\pi}{q+1} \equiv \varphi \frac{1-\mathrm{M}}{1+\mathrm{M}},$$

M désignant l'une quelconque des racines de (3); il en résulte que les tangentes des arcs o, $\frac{\pi}{q+1}$, $2\frac{\pi}{q+1}$, $\cdots$, $q\frac{\pi}{q+1}$ sont toutes incongrues suivant le module q.

Propriétés des nombres goniométriques des arcs $\frac{k\pi}{2(q\pm 1)}$.

17. Nous désignons par nombres goniométriques les expressions des lignes trigonométriques d'un multiple d'une partie aliquote du cercle, prises suivant un module q.

Supposons que q soit un nombre premier de la forme $4n+1$. Désignons par G la plus petite racine primitive de la congruence

$$(a) \qquad z^{q-1} \equiv 1 \pmod{q},$$

et posons $\varphi \equiv G^{\frac{q-1}{4}}$, cette plus petite racine primitive peut être représentée par la formule

$$G \equiv \cos\frac{2\pi}{q-1} + \varphi \sin\frac{2\pi}{q-1},$$

et on obtient les nombres entiers qui appartiennent aux groupes A, B, C, D par rapport à q, en élevant G respectivement aux puissances $4n$, $4n+1$, $4n+2$, $4n+3$. D'ailleurs les puissances de G s'obtiennent en multipliant l'argument par l'exposant de la puissance, de sorte que l'on a

$$G^l \equiv \cos\frac{2l\pi}{q-1} + \varphi \sin\frac{2l\pi}{q-1}.$$

Actuellement considérons des expressions de même genre, mais dans lesquelles l'argument, au lieu d'être un multiple de $\frac{2\pi}{q-1}$, soit un multiple du quart de cet argument. La quantité

$$L \equiv \cos\frac{l\pi}{2(q-1)} + \varphi \sin\frac{l\pi}{2(q-1)},$$

est l'une de ces expressions, elle est racine de

$$z^{4(q-1)} \equiv 1,$$

et en l'élevant à la puissance q, on a

$$L^q \equiv \left[\cos\frac{l\pi}{2(q-1)} + \varphi \sin\frac{l\pi}{2(q-1)}\right]^q \equiv \cos\frac{lq\pi}{2(q-1)} + \varphi \sin\frac{lq\pi}{2(q-1)}$$
$$\equiv \cos\left[\frac{l\pi}{2(q-1)} + \frac{l\pi}{2}\right] + \varphi \sin\left[\frac{l\pi}{2(q-1)} + \frac{l\pi}{2}\right].$$

Mais si l'on observe que l'on a $\varphi^q \equiv \varphi$, puisque $\varphi^4 \equiv 1$ et que q est de la forme $4n+1$, on a aussi

$$L^q \equiv \left[\cos\frac{l\pi}{2(q-1)}\right]^q + \varphi\left[\sin\frac{l\pi}{2(q-1)}\right]^q;$$

et en comparant les deux expressions de L^q, et observant que leur égalité subsisterait encore si on y changeait φ en $-\varphi$, on a

$$\cos^q\frac{l\pi}{2(q-1)} \equiv \cos\left[\frac{l\pi}{2(q-1)} + \frac{l\pi}{2}\right],$$
$$\sin^q\frac{l\pi}{2(q-1)} \equiv \sin\left[\frac{l\pi}{2(q-1)} + \frac{l\pi}{2}\right].$$

Supposons ensuite que q soit de la forme $4n+3$; l'une des racines primitives de

$$(b) \qquad z^{q+1} \equiv 1 \pmod{q},$$

peut être représentée par la formule

$$k \equiv \cos\frac{2\pi}{q+1} + i\sin\frac{2\pi}{q+1},$$

et nous obtiendrons quatre groupes de nombres complexes A, B, C, D, en élevant k aux puissances de la forme $4n$, $4n+1$, $4n+2$, $4n+3$, et nous servant de la formule

$$k^l \equiv \cos\frac{2l\pi}{q+1} + i\sin\frac{2l\pi}{q+1}.$$

Considérons ensuite l'expression semblable

$$N \equiv \cos\frac{l\pi}{2(q+1)} + i\sin\frac{l\pi}{q+1},$$

mais dont l'argument, au lieu d'être un multiple de $\frac{2\pi}{q+1}$, soit un multiple du quart de cet argument ; en l'élevant à la puissance q, on a

$$\begin{aligned} N^q &\equiv \cos\frac{lq\pi}{2(q+1)} + i\sin\frac{lq\pi}{2(q+1)} \\ &\equiv \cos\left[\frac{-l\pi}{2(q+1)} + \frac{l\pi}{2}\right] + i\sin\left[\frac{-l\pi}{2(q+1)} + \frac{l\pi}{2}\right], \end{aligned}$$

et puisqu'on a $i^q \equiv i^{4n+3} \equiv -i$, on a aussi

$$N^q \equiv \cos^q\frac{l\pi}{2(q+1)} - i\sin^q\frac{l\pi}{2(q+1)},$$

et en comparant les deux expressions de N^q, on obtient

$$\begin{aligned} \cos^q\frac{l\pi}{2(q+1)} &\equiv \cos\left[\frac{l\pi}{2(q+1)} - \frac{l\pi}{2}\right], \\ \sin^q\frac{l\pi}{2(q+1)} &\equiv \sin\left[\frac{l\pi}{2(q+1)} - \frac{l\pi}{2}\right]. \end{aligned}$$

Mais afin d'arriver à l'uniformité dans les résultats, nous adopterons pour base la racine primitive

$$h \equiv \cos\frac{2\pi}{q+1} - i\sin\frac{2\pi}{q+1} \equiv \cos\frac{-2\pi}{q+1} + i\sin\frac{-2\pi}{q+1},$$

pour laquelle on a

$$h^{\frac{q+1}{4}} \equiv -i.$$

Élevons h à la puissance l, nous aurons

$$h^l \equiv \cos\frac{-2l\pi}{q+1} + i\sin\frac{-2l\pi}{q+1},$$

et pour avoir toutes les racines de la congruence (b), on donnera à l les valeurs 0, 1, 2,..., q, et cette racine appartient aux groupes A, B, C ou D suivant que l est de la forme $4n$, $4n+1$, $4n+2$ ou $4n+3$. Ensuite si on élève à la puissance q les nombres goniométriques de

l'arc $-\frac{2\pi}{2(q+1)}$, on voit que l'argument s'accroît de $\frac{l\pi}{2}$; et on a

$$\cos^q \frac{-l\pi}{2(q+1)} \equiv \cos\left[\frac{-l\pi}{2(q+1)} + \frac{l\pi}{2}\right],$$
$$\sin^q \frac{-l\pi}{2(q+1)} \equiv \sin\left[\frac{-l\pi}{2(q+1)} + \frac{l\pi}{2}\right].$$

On conclut de là : *soit l'arc* $\pm\frac{l\pi}{2(q\mp 1)}$ *où l'on prend les signes supérieurs ou les signes inférieurs, selon que* $q = 4n+1$ *ou* $4n+3$, *si on élève les sinus et cosinus goniométriques de cet arc à la puissance* q, *on ne fait qu'accroître l'argument de* $\frac{l\pi}{2}$.

Introduction de l'angle υ *dans l'expression des quatre périodes de la congruence* $\frac{x^p-1}{x-1} \equiv 0 \pmod{q}$.

18. Nous avons introduit dans l'expression des périodes de l'équation

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

un arc υ incommensurable avec la circonférence, et dont la tangente est rationnelle et déterminée par l'équation

$$\operatorname{tang}\upsilon = \frac{b}{a}.$$

Dans le cas de $p = 8n+1$, les quatre périodes, avec leur ordre circulaire, sont données par la formule

$$(1) \qquad \omega^{(k)} = -\frac{1}{4} - \frac{a}{4\cos(\upsilon+k\pi)}\left(1+2\cos\frac{\upsilon+k\pi}{2}\right),$$

et si p est de la forme $8n+5$, leurs expressions sont

$$(2) \qquad \omega^{(k)} = -\frac{1}{4} + \frac{a}{4\cos(\upsilon+k\pi)}\left(1+2\sqrt{-1}\cos\frac{\upsilon+k\pi}{2}\right).$$

Or, d'après les conventions que nous avons faites et l'adoption des nombres goniométriques, on peut employer les mêmes expressions pour les périodes de la congruence

$$\frac{x^p - 1}{x - 1} \equiv 0 \pmod{q}.$$

Considérons d'abord un module q de la forme $4n + 1$. Le nombre $\frac{b}{a} \pmod{q}$ peut avoir pour valeur un des nombres $0, 1, 2, \ldots, q-1, \infty$, excepté $\pm\varphi$; car si l'on avait

$$\frac{b}{a} \equiv \pm\varphi \pmod{q},$$

on en conclurait

$$b^2 + a^2 \equiv 0 \pmod{q},$$

et p ne serait pas premier. Or les expressions algébriques des tangentes des arcs

$$0, \quad \frac{\pi}{q-1}, \quad 2\frac{\pi}{q-1}, \quad 3\frac{\pi}{q-1}, \ldots, \quad (q-2)\frac{\pi}{q-1},$$

prises suivant le module q, représentent tous ces nombres d'après le n° **15**; donc, v étant un de ces arcs, on peut poser

$$\frac{b}{a} \equiv \operatorname{tang} v \pmod{q}, \quad v = \frac{l\pi}{q-1},$$

et si l'on fait

$$M \equiv \cos 2v + \varphi \sin 2v,$$

M sera l'un quelconque des nombres $1, 2, \ldots, q-1$ d'après le même numéro, et l'on aura

$$\frac{b}{a} \equiv \varphi \frac{1 - M}{1 + M}. \tag{3}$$

Si nous considérons la période ω, pour laquelle k est nul, nous avons

$$\omega \equiv -\frac{1}{4} - \frac{a}{4\cos v}\left(1 + 2\cos\frac{v}{2}\right) \quad \text{si} \quad p = 8n + 1,$$

$$\omega \equiv -\frac{1}{4} + \frac{a}{4\cos v}\left(1 + 2\varphi\cos\frac{v}{2}\right) \quad \text{si} \quad p = 8n + 5,$$

Or, d'après le numéro précédent, on a

$$\left(\cos\frac{\upsilon}{2}\right)^q \equiv \cos\left(\upsilon + \frac{l\pi}{2}\right), \quad (\cos\upsilon)^q \equiv \cos(\upsilon + l\pi);$$

donc, dans les deux cas, en remarquant que φ^q est $\equiv \varphi$, on a

$$\omega^q \equiv -\frac{1}{4} - \frac{a}{4\cos(\upsilon + l\pi)}\left(1 + 2\cos\frac{\upsilon + l\pi}{2}\right),$$

$$\omega^q \equiv -\frac{1}{4} - \frac{a}{4\cos(\upsilon + l\pi)}\left(1 + 2\varphi\cos\frac{\upsilon + l\pi}{2}\right),$$

et par suite

$$\omega^q \equiv \omega^{(l)}.$$

On en conclut, d'après le n° **12**, que q *appartient à* A, B, C *ou* D *par rapport à* p, selon que l est de la forme $4n$, $4n+1$, $4n+2$, $4n+3$, ou *selon que le nombre entier* (n° **17**)

$$\mathrm{M} \equiv \cos\frac{2l\pi}{q-1} + \varphi\sin\frac{2l\pi}{q-1},$$

de la formule (3), *appartient à* A, B, C *ou* D *par rapport à* q.

Passons à un module premier de la forme $4n+3$. Les expressions algébriques des tangentes des arcs 0, $\frac{\pi}{q+1}$, $2\frac{\pi}{q+1}$, ..., $q\frac{\pi}{q+1}$, prises suivant le module q, représentent tous les nombres 0, 1, 2, ..., $q-1$, ∞ ; et il en est de même des tangentes des arcs 0, $-\frac{\pi}{q+1}$, $-2\frac{\pi}{q+1}$, ..., $-\frac{q\pi}{q+1}$: donc υ étant un certain arc de la forme

$$\upsilon = -\frac{l\pi}{q+1},$$

dans lequel l est un nombre entier compris de zéro à q, on peut poser

$$(n) \qquad \frac{b}{a} \equiv \operatorname{tang}\upsilon,$$

et si l'on écrit

$$\cos 2\upsilon + i\sin 2\upsilon \equiv \mathrm{M} \pmod{q},$$

M sera l'une quelconque des racines de

$$z^{q+1} \equiv 1,$$

et en prenant pour base la racine primitive

$$h \equiv \cos \frac{-2\pi}{q+1} + i \sin \frac{-2\pi}{q+1},$$

pour laquelle on a

$$h^{\frac{q+1}{4}} \equiv -i,$$

M appartient (n° **17**) aux groupes A, B, C ou D, suivant que l est de la forme $4n$, $4n+1$, $4n+2$ ou $4n+3$, et par l'introduction de ce nombre dans la formule (n) on a

$$\frac{b}{a} \equiv i \frac{1-M}{1+M}. \tag{4}$$

q étant de la forme $4n+3$, distinguons les cas de $p = 8n+1$ et de $p = 8n+5$.

Si p est de la forme $8n+1$, on aura en élevant ω à la puissance q, d'après le théorème qui termine le n° **17**,

$$\omega^q \equiv -\frac{1}{4} - \frac{a}{4\cos(v+l\pi)}\left(1+2\cos\frac{v+l\pi}{2}\right)$$
$$\equiv \omega^{(l)}.$$

et on a le même résultat que lorsque q est de la forme $4n+1$; ainsi q appartient à A, B, C ou D par rapport à p, selon que l est de la forme $4n$, $4n+1$, $4n+2$ ou $4n+3$, ou selon que le nombre M de la formule (4) appartient aux groupes A, B, C ou D. Et dans cet énoncé on peut substituer $-q$ à $+q$, en remarquant que ces deux nombres ont le même caractère biquadratique par rapport à p.

Mais si p est de la forme $8n+5$, en élevant à la puissance $q^{ième}$ la période

$$\omega \equiv -\frac{1}{4} + \frac{a}{4\cos v}\left(1+2i\cos\frac{v}{2}\right),$$

et observant que i^q est $\equiv -i$, on obtient

$$\begin{aligned}\omega^q &\equiv -\frac{1}{4} + \frac{a}{4\cos(v+l\pi)}\left(1 - 2i\cos\frac{v+l\pi}{2}\right)\\ &\equiv -\frac{1}{4} + \frac{a}{4\cos[v+(l+2)\pi]}\left[1 + 2i\cos\frac{v+(l+2)\pi}{2}\right]\\ &\equiv \omega^{(l+2)}.\end{aligned}$$

Donc, suivant que l est de la forme $4n$, $4n+1$, $4n+2$, $4n+3$, ω^q est équivalent à ω'', ω''', ω ou ω', et q appartient, suivant le module p, à C, D, A ou B, et comme -1 appartient à C, $-q$ est respectivement un des nombres A, B, C ou D.

Donc enfin *toutes les fois que q est de la forme* $4n+3$, $-q$ *appartient à* A, B, C *ou* D *par rapport à p, suivant que le nombre* M *de la formule* (4) *appartient lui-même aux groupes* A, B, C *ou* D *des racines de la congruence* $z^{q+1} \equiv 1$.

Il résulte de là que les formules (3) et (4) détermineront dans tous les cas le caractère biquadratique de $\pm q$ par rapport à p.

Sur les quatre classes α, β, γ, δ *de valeurs de* $\frac{b}{a}$ (mod. q).

19. G étant la plus petite racine primitive du nombre premier $q = 4n+1$, il résulte de ce qui précède que les quatre classes de valeurs du rapport $\frac{b}{a}$ (mod. q) sont données par les formules

$$(1)\begin{cases}\alpha \equiv \varphi\frac{1-G^{4e}}{1+G^{4e}}, \quad \beta \equiv \varphi\frac{1-G^{4e+1}}{1+G^{4e+1}}, \quad \gamma \equiv \varphi\frac{1-G^{4e+2}}{1+G^{4e+2}}, \quad \delta \equiv \varphi\frac{1-G^{4e+3}}{1+G^{4e+3}},\\ \varphi \equiv G^{\frac{q-1}{4}},\end{cases}$$

où il suffit de donner à e les valeurs $0, 1, 2, \ldots, \frac{q-5}{4}$.

Si au contraire q est de la forme $4n+3$, alors parmi deux racines primitives conjuguées quelconques $r+si$ et $r-si$ de la congruence

$$z^{q+1} \equiv 1 \pmod{q},$$

choisissons celle h pour laquelle on a

$$h^{\frac{q+1}{4}} = -i,$$

et nous avons pour les nombres des classes α, β, γ, δ

$$(2)\quad \alpha \equiv i\frac{1-h^{4e}}{1-h^{4e}},\quad \beta \equiv i\frac{1-h^{4e+1}}{1+h^{4e+1}},\quad \gamma \equiv i\frac{1-h^{4e+2}}{1+h^{4e+2}},\quad \delta \equiv i\frac{1-h^{4e+3}}{1-h^{4e+3}},$$

en donnant à e les valeurs $0, 1, 2, \ldots, \frac{q-3}{4}$.

Si nous avons à distinguer les nombres α, β, γ, δ les uns des autres, nous représenterons les expressions (1) par α_e, β_e, γ_e, δ_e; ainsi l'on a

$$\alpha_k \equiv \varphi\frac{1-G^{4k}}{1+G^{4k}},\quad \alpha_l \equiv \varphi\frac{1-G^{4l}}{1+G^{4l}},\quad \alpha_{k+l} \equiv \varphi\frac{1-G^{4(k+l)}}{1+G^{4(k+l)}},$$

et l'on vérifie sans peine que l'on a

$$\frac{\alpha_k+\alpha_l}{1-\alpha_k\alpha_l} \equiv \alpha_{k+l},$$

formule qui rappelle la tangente de la somme de deux arcs k et l.

Désignons par la lettre μ des nombres (1) appartenant à la même classe, et posons

$$\mu_e \equiv \varphi\frac{1-G^{4e+j}}{1+G^{4e+j}},$$

e étant variable et j fixe; nous aurons

$$(3)\qquad \frac{\mu_k+\alpha_l}{1-\mu_k\alpha_l} \equiv \mu_{k+l}.$$

Considérons l'expression

$$\theta(\mu) \equiv \frac{\mu+\alpha_1}{1-\alpha_1\mu},$$

et posons les notations

$$\theta\theta(t) = \theta^2(t),\quad \theta\theta^2(t) = \theta^3(t),\ \ldots,$$

il est aisé de voir qu'on aura en général

$$\theta^n(\mu) \equiv \frac{\mu + \alpha_n}{1 - \alpha_n \mu},$$

et par conséquent, en formant successivement les nombres $\theta(\mu)$, $\theta^2(\mu)$, $\theta^3(\mu)$, etc., on aura une suite de nombres appartenant à la même classe que le premier μ d'où l'on est parti. Comme $\alpha_{\frac{q-1}{4}} \equiv 0$, on a

$$\theta^{\frac{q-1}{4}}(\iota) \equiv \iota,$$

et dès la $\left(\frac{q-1}{4}\right)^{ième}$ opération, on retrouve les mêmes nombres; mais on aura obtenu tous les nombres de la classe à laquelle μ appartient.

On a donc une méthode pour calculer les nombres (1) autre que celle qui résulte directement des valeurs posées.

20. Cette méthode est aussi applicable aux nombres (2), et offre alors beaucoup d'avantage sur le calcul direct, qui serait compliqué d'opérations sur des nombres imaginaires.

En effet, si l'on pose

$$\alpha_l \equiv i\,\frac{1 - h^{2l}}{1 + h^{2l}}, \quad \mu_k \equiv i\,\frac{1 - h^{4k+j}}{1 + h^{4k+j}},$$

j étant égal à 0, 1, 2 ou 3, mais ayant une valeur fixe; on a encore la formule (3), et si l'on pose de plus

$$\alpha_1 \equiv i\,\frac{1 - h^4}{1 + h^4}, \quad \theta(\mu) \equiv \frac{\mu + \alpha_1}{1 - \alpha_1 \mu},$$

on aura encore

$$\theta^n(\mu) \equiv \frac{\mu + \alpha_n}{1 - \alpha_n \mu}$$

On a $\alpha_{\frac{q+1}{4}} \equiv 0$; donc la suite

$$\mu,\ \theta(\mu),\ \theta^2(\mu),\ldots,\ \theta^{\frac{q-3}{4}}(\mu)$$

donne les $\frac{q+1}{4}$ nombres qui appartiennent à la même classe que μ.

Ayant calculé cette série, on peut prendre un des nombres 0, 1, 2,..., $q-1$ qui ne s'y trouvent pas et former une seconde suite

$$\nu,\ \theta(\nu),\ \theta^2(\nu),\ldots,\ \theta^{\frac{q-3}{4}}(\nu),$$

qui donnera tous les nombres d'une même classe. On pourra de même obtenir les deux autres séries, et il ne restera plus qu'à les distinguer; or la classe α contient le nombre zéro, et la classe γ, comme la classe α, est composée de nombres égaux et de signe contraire selon le module q; de sorte qu'il n'y a plus à distinguer que la série β de la série δ, et on arrivera à cette dernière séparation en calculant

$$\beta_1 = i\,\frac{1-h}{1+h}.$$

Disons maintenant comment on déterminera α_1 et β_1 qui entrent dans ce calcul.

h, racine primitive de $z^{q+1} \equiv 1 \pmod{q}$, appartient à une congruence irréductible du second degré de la forme

$$h^2 - 2rh + 1 \equiv 0 \pmod{q},$$

la congruence étant irréductible, $r^2 - 1$ est un non-résidu quadratique et par conséquent $1 - r^2$ un résidu. Posons

$$h = r + si,$$

en choisissant pour s celle des deux valeurs de $\sqrt{1-r^2}$ pour laquelle on a

$$h^{\frac{q+1}{4}} \equiv -i.$$

Alors on aura pour β_1

$$\beta_1 \equiv i\,\frac{1-r-si}{1+r+si} \equiv i\,\frac{(1-r-si)(1+r-si)}{(1+r+si)(1+r-si)} \equiv i\,\frac{(1-si)^2-r^2}{(1+r)^2+s^2}.$$

Si l'on opère les réductions en se rappelant que $s^2 \equiv 1 - r^2$, on a

$$\beta_1 \equiv \frac{s}{1+r}.$$

On a ensuite, en élevant h à la quatrième puissance,

$$h^4 \equiv 8r^4 - 8r^2 + 1 + 4rs(2r^2 - 1)i;$$

donc

$$\alpha_1 \equiv 2ir\frac{-2r^3 + 2r - s(2r^2-1)i}{(2r^2-1)(2r^2-1+2rsi)} \equiv 2r\frac{s(2r^2-1) + 2r(1-r^2)i}{(2r^2-1)(2r^2-1+2rsi)}$$

$$\equiv 2r\frac{s(2r^2-1) + 2rs^2 i}{(2r^2-1)(2r^2-1+2rsi)} \equiv \frac{2rs}{2r^2-1},$$

et les deux quantités α_1 et β_1 sont obtenues, dégagées de toutes les imaginaires.

Applications. — 1° Soit $q = 5$; la plus petite racine primitive de 5 est $G = 2$; on a donc $\varphi \equiv 2$, puis

$$\alpha = 0, \quad \beta = 1, \quad \gamma = \infty, \quad \delta = 4;$$

donc 5 appartient à A, B, C ou D, selon le module p, suivant que $\frac{b}{a}$ est congru à 0, 1, ∞ ou 4 suivant le module 5.

2° Soit $q = 13$; on a $G = 2$, $\varphi \equiv 8$ et

$$\alpha = 0, \quad 9, \quad 4; \qquad \beta = 6, \quad 11, \quad 12;$$
$$\gamma = 3, \quad \infty, \quad 10; \qquad \delta = 1, \quad 2, \quad 7.$$

On en conclut le caractère de 13.

Les nombres précédents sont de la forme $4n + 1$; considérons des nombres de la forme $4n + 3$.

3° Si q est égal à 3, on a $h \equiv -i$ qui satisfait à la condition

$$h^{\frac{q+1}{4}} \equiv h \equiv -i \pmod{3},$$

et on en conclut $\alpha_1 = 0$, $\beta_1 = 2$; on a donc

$$\alpha = 0, \quad \beta = 2, \quad \gamma = \infty, \quad \delta = 1.$$

Ainsi -3 appartient à A, B, C ou D, selon le module p, suivant que $\frac{b}{a}$ est congru à 0, 2, ∞ ou 1 suivant le module 3.

4° Soit $q = 7$; $h = -2 + 2i$ est racine primitive de la congruence

$$h^8 \equiv 1 \pmod{7},$$

et satisfait de plus à la condition $h^2 \equiv -i$; on a donc $\alpha_1 = \infty$, $\beta_1 = 5$; puis

$$\alpha = 0, \infty; \quad \beta = 5, 4; \quad \gamma = 1, 6; \quad \delta = 3, 2.$$

5° Soit $q = 11$; $h = -3 + 5i$ est racine primitive de

$$h^{12} \equiv 1 \pmod{11},$$

et l'on a $h^{\frac{q+1}{4}} = h^3 \equiv -i$; donc $\alpha_1 = 6$, $\beta_1 = 3$, et l'on obtient

$$\alpha = 0, 6, 5; \qquad \beta = 3, 4, 1;$$
$$\gamma = \infty, 2, 9; \qquad \delta = 8, 7, 10.$$

Le caractère biquadratique des nombres premiers suivants est indiqué par les tableaux ci-dessous :

$$q = 17.$$

$$\alpha = 0, 1, 16, \infty; \qquad \beta = 2, 6, 8, 14;$$
$$\gamma = 5, 7, 10, 12; \qquad \delta = 3, 9, 11, 15.$$

$$-q = -19.$$

$$\alpha = 0, 2, 5, 14, 17; \qquad \beta = 3, 7, 11, 13, 18;$$
$$\gamma = 4, 9, 10, 15, \infty; \qquad \delta = 1, 6, 8, 12, 16.$$

$$-q = -23.$$

$$\alpha = 0, 7, 10, 13, 16, \infty; \qquad \beta = 2, 3, 4, 11, 15, 17;$$
$$\gamma = 1, 5, 9, 14, 18, 22; \qquad \delta = 6, 8, 12, 19, 20, 21.$$

$$q = 29.$$

$\alpha = 0,\ 9,\ 11,\ 14,\ 15,\ 18,\ 20;$
$\beta = 7,\ 19,\ 23,\ 24,\ 25,\ 26,\ 28;$
$\gamma = 2,\ 8,\ 13,\ 16,\ 21,\ 27,\ \infty;$
$\delta = 1,\ 3,\ 4,\ 5,\ 6,\ 10,\ 22.$

$$-q = -31.$$

$\alpha = 0,\ 1,\ 7,\ 9,\ 22,\ 24,\ 30,\ \infty;$
$\beta = 5,\ 6,\ 8,\ 11,\ 12,\ 14,\ 18,\ 27;$
$\gamma = 2,\ 3,\ 10,\ 15,\ 16,\ 21,\ 28,\ 29;$
$\delta = 4,\ 13,\ 17,\ 19,\ 20,\ 23,\ 25,\ 26.$

$$q = 37.$$

$\alpha = 0,\ 10,\ 12,\ 14,\ 15,\ 22,\ 23,\ 25,\ 27;$
$\beta = 1,\ 2,\ 7,\ 9,\ 13,\ 16,\ 19,\ 20,\ 33;$
$\gamma = 3,\ 5,\ 8,\ 11,\ 26,\ 29,\ 32,\ 34,\ \infty;$
$\delta = 4,\ 17,\ 18,\ 21,\ 24,\ 28,\ 30,\ 35,\ 36.$

$$q = 41.$$

$\alpha = 0,\ 2,\ 11,\ 15,\ 20,\ 21,\ 26,\ 30,\ 39,\ \infty;$
$\beta = 4,\ 5,\ 8,\ 10,\ 13,\ 16,\ 22,\ 23,\ 24,\ 29;$
$\gamma = 1,\ 3,\ 6,\ 7,\ 14,\ 27,\ 34,\ 35,\ 38,\ 40;$
$\delta = 12,\ 17,\ 18,\ 19,\ 25,\ 28,\ 31,\ 33,\ 36,\ 37.$

$$-q = -43.$$

$\alpha = 0,\ 10,\ 11,\ 12,\ 14,\ 15,\ 28,\ 29,\ 31,\ 32,\ 33;$
$\beta = 1,\ 2,\ 5,\ 7,\ 16,\ 19,\ 22,\ 26,\ 34,\ 35,\ 37;$
$\gamma = 3,\ 4,\ 13,\ 18,\ 20,\ 23,\ 25,\ 30,\ 39,\ 40,\ \infty;$
$\delta = 6,\ 8,\ 9,\ 17,\ 21,\ 24,\ 27,\ 36,\ 38,\ 41,\ 42.$

$$-q=-47.$$

$$\alpha=0,\quad 1,\quad 4,\quad 10,\quad 12,\quad 14,\quad 33,\quad 35,\quad 37,\quad 43,\quad 46,\quad \infty;$$
$$\beta=3,\quad 13,\quad 15,\quad 18,\quad 19,\quad 21,\quad 24,\quad 25,\quad 31,\quad 38,\quad 42,\quad 45;$$
$$\gamma=6,\quad 7,\quad 8,\quad 11,\quad 17,\quad 20,\quad 27,\quad 30,\quad 36,\quad 39,\quad 40,\quad 41;$$
$$\delta=2,\quad 5,\quad 9,\quad 16,\quad 22,\quad 23,\quad 26,\quad 28,\quad 29,\quad 32,\quad 34,\quad 44.$$

FIN DU TOME DOUZIÈME (2^{e} SÉRIE).

PARIS. — IMPRIMERIE DE GAUTHIER-VILLARS, SUCCESSEUR DE MALLET-BACHELIER,
Rue de Seine-Saint-Germain, 10, près l'Institut.