96

MÉMOIRE

SUR

La détermination des fonctions Y *et* Z *qui satisfont à l'équation* $4(x^n-1)=(x-1)(Y^2\pm nZ^2)$, n *étant un nombre premier* $4i\mp 1$.

PAR M. LEGENDRE.

Lu à l'Académie, le 11 octobre 1830.

DANS les articles 511 et 512 de ma Théorie des nombres, troisième édition, j'ai donné des règles fort simples pour calculer les coefficients de la fonction Y qui satisfait à l'équation $4X=Y^2\pm nZ^2$, où l'on désigne par n le nombre premier $4i\mp 1$ et par X le quotient de x^n-1 divisé par $x-1$. Ces règles sont fondées sur la supposition que les coefficients des différents termes de la fonction Y sont moindres que $\frac{1}{2}n$, en les prenant avec le signe convenable; cette propriété a lieu en effet pour toutes les valeurs de n comprises dans le tableau de l'art. 512, et elle se vérifierait également pour quelques-unes des valeurs suivantes, mais elle cesse d'avoir lieu pour des valeurs plus grandes et il arrive au contraire que les coefficients de x dans la fonction Y, loin d'être plus

petits que $\frac{1}{2}n$, deviennent progressivement plus grands que n, à mesure que n augmente, même plus grands que n^2, n^3, etc. Les règles dont nous parlons ne font donc plus connaître les vrais coefficients de Y, mais seulement les restes de ces coefficients divisés par n, ce qui peut être utile pour vérifier les valeurs calculées par d'autres méthodes, et il en résulte toujours, conformément à ce qui a été dit dans l'article 511, que le polynome Y, dont les premiers termes sont $2x^m + x^{m-1} + \frac{3 \mp n}{4} x^{m-2} + \text{etc.}$ contient nécessairement tous ses termes au nombre de $m+1$ sans qu'aucun d'eux puisse devenir nul, ce qui n'a pas toujours lieu pour le polynome Z du degré $m-1$, qui peut être complet ou incomplet suivant les différents cas. Voici maintenant une méthode sûre et exacte pour déterminer, dans tous les cas, les polynomes Y et Z qui satisfont à l'équation $4X = Y^2 \pm nZ^2$.

Soit d'abord $n = 4i+1$ ou $m = 2i$, valeur qui répond à l'équation $4X = Y^2 - nZ^2$, si on fait en général

$$Y + Z\sqrt{n} = 2x^m + A_1 x^{m-1} + A_2 x^{m-2} + A_3 x^{m-3} + \text{etc.}$$

la forme connue des polynomes Y et Z étant

$$Y = 2x^m + x^{m-1} + a_2 x^{m-2} + a_3 x^{m-3} + \text{etc.}$$
$$Z = \qquad x^{m-1} + b_2 x^{m-2} + b_3 x^{m-3} + \text{etc.},$$

on aura les relations suivantes entre les coefficients A, a, b:

$$A_1 = 1 + \sqrt{n}, \quad A_2 = a_2 + b_2\sqrt{n}, \quad A_3 = a_3 + b_3\sqrt{n},$$

et en général $A_i = a_i + b_i\sqrt{n}$; ainsi pour avoir les valeurs des fonctions Y et Z, il suffira de connaître celles des coefficients A_2, A_3, etc.

Soit g l'une des racines primitives du nombre premier n : si l'on désigne par α l'un des termes de la suite

$$1, g^1, g^2, g^3 \ldots\ldots g^{n-3}, \qquad (1)$$

et par ϵ l'un des termes de la suite

$$g, g^3, g^5, g^7 \ldots\ldots g^{n-2},$$

on sait que ces deux suites de nombres, diminués des multiples de n qu'ils peuvent contenir, donnent par leur réunion la suite des nombres naturels $1, 2, 3 \ldots\ldots n-1$; on sait de plus que r étant l'une quelconque des racines imaginaires de l'équation $r^n - 1 = 0$, le produit de tous les facteurs $x - r^\alpha$, sera égal à l'un des deux polynomes $\frac{1}{2}(Y + Z\sqrt{n})$, $\frac{1}{2}(Y - Z\sqrt{n})$, et le produit de tous les facteurs $x - r^\epsilon$ sera égal à l'autre polynome; d'ailleurs comme le signe de $\sqrt{n}$ peut être pris à volonté, on pourra supposer généralement

$$(x-r)(x-r^{g^2})(x-r^{g^4}) \ldots (x-r^{g^{n-3}})$$
$$= x^n + \tfrac{1}{2}A_1 x^{n-1} + \tfrac{1}{2}A_2 x^{n-2} + \tfrac{1}{2}A_3 x^{n-3} + \text{etc.}$$

Appelons S_1 la somme des racines r^α, S_2 la somme de leurs carrés $r^{2\alpha}$, S_3 la somme de leurs cubes $r^{3\alpha}$, etc.; ces sommes étant supposées connues, on pourra déterminer les coefficients A_1, A_2, A_3, etc., au moyen des équations suivantes:

---

(1) La suite des valeurs de α est aussi représentée dans un autre ordre, par celle des carrés $1, 4, 9, 16 \ldots m^2$, diminués des multiples de n qu'ils peuvent contenir.

$$
\begin{aligned}
&-\tfrac{1}{2}A_0 = S_0\\
&-2\cdot\tfrac{1}{2}A_1 = S_1 + S_0\cdot\tfrac{1}{2}A_0\\
(1)\quad &-3\cdot\tfrac{1}{2}A_2 = S_2 + S_1\cdot\tfrac{1}{2}A_1 + S_0\cdot\tfrac{1}{2}A_0\\
&-4\cdot\tfrac{1}{2}A_3 = S_3 + S_2\cdot\tfrac{1}{2}A_1 + S_1\cdot\tfrac{1}{2}A_2 + S_0\cdot\tfrac{1}{2}A_3\\
&-5\cdot\tfrac{1}{2}A_4 = S_4 + S_3\cdot\tfrac{1}{2}A_1 + S_2\cdot\tfrac{1}{2}A_2 + S_1\cdot\tfrac{1}{2}A_3 + S_0\cdot\tfrac{1}{2}A_4\\
&\quad\text{etc.}
\end{aligned}
$$

A l'égard de la somme désignée en général par S_k, elle ne peut avoir que l'une des deux valeurs $-\frac{1}{2}+\frac{1}{2}\sqrt{n}, -\frac{1}{2}-\frac{1}{2}\sqrt{n}$.

On peut supposer $S_0 = -\frac{1}{2}-\frac{1}{2}\sqrt{n}$, et alors on aura

$S_k = -\frac{1}{2}-\frac{1}{2}\sqrt{n}$, si k appartient à la série des nombres α;

et

$S_k = -\frac{1}{2}+\frac{1}{2}\sqrt{n}$, si k appartient à la série des nombres ϵ.

Dans le premier cas, le nombre k serait un résidu quadratique de n, et on aurait, suivant la notation ordinaire, $\left(\frac{k}{n}\right) = 1$; dans le second cas, le nombre k serait un non-résidu et on aurait $\left(\frac{k}{n}\right) = -1$; donc dans tous les cas on aura, au moyen du symbole $\left(\frac{k}{n}\right)$,

$$(2)\qquad S_k = -\tfrac{1}{2}-\tfrac{1}{2}\sqrt{n}\cdot\left(\frac{k}{n}\right).$$

Étant donnés n et k, on pourra toujours déterminer *a priori* celle des deux valeurs $+1$ et -1 qui convient au symbole $\left(\frac{k}{n}\right)$. Ainsi on connaîtra successivement toutes les sommes S_0, S_1, S_2, etc., ce qui permettra de déterminer les coefficients A_0, A_1, A_2, par le moyen des équations (1). Ensuite la fonction $2x^n + A_0x^{n-1} + A_1x^{n-2} + A_2x^{n-3} +$ etc. prendra la forme

$$2x^n + (1+\sqrt{n})x^{n-1} + (a_1+b_1\sqrt{n})x^{n-2} + (a_2+b_2\sqrt{n})x^{n-3} + \text{etc.}$$

d'où l'on tire les valeurs séparées des fonctions Y et Z, savoir :

$$Y = 2x^n + x^{n-1} + a_1x^{n-2} + a_2x^{n-3} + \text{etc.}$$
$$Z = \quad x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \text{etc.}$$

Telle est la méthode par laquelle on trouvera les fonctions Y et Z qui satisfont à l'équation $4X = Y^2 - nZ^2$, lorsque le nombre premier n est de la forme $4i+1$; elle servira également à résoudre l'équation $4X = Y^2 + nZ^2$, lorsque le nombre premier n est de la forme $4i-1$. Il suffira pour cela de mettre $-n$ à la place de n dans la valeur de S_1, c'est-à-dire, de prendre $S_1 = -\frac{1}{2} - \frac{1}{2}\sqrt{-n}$; on déterminera ensuite généralement S_k au moyen de la formule $S_k = -\frac{1}{2} - \frac{1}{2}\sqrt{-n}\cdot\left(\frac{k}{n}\right)$ en y substituant la valeur particulière de $\left(\frac{k}{n}\right)$ qu'on peut toujours trouver *a priori*. Alors connaissant par les équations (1) les valeurs des coefficients A, A_1, A_2, etc. qui seront tous de la forme $a + b\sqrt{-n}$, on en déduira comme ci-dessus la valeur de la fonction $2x^n + A_1x^{n-1} + A_2x^{n-2} + \text{etc.}$, et ensuite celles des fonctions Y et Z.

Exemple I.

Pour continuer le tableau de l'art. 512, prenons $n = 31$. Comme les diverses valeurs de S_k ne peuvent être que P et Q, savoir $P = -\frac{1}{2} - \frac{1}{2}\sqrt{n}$, $Q = -\frac{1}{2} + \frac{1}{2}\sqrt{n}$, ayant déja fait $S_1 = P$, nous déterminerons les sommes suivantes S_2, S_3, S_4, etc. au moyen des symboles $\left(\frac{2}{n}\right)$, $\left(\frac{3}{n}\right)$, $\left(\frac{4}{n}\right)$, $\left(\frac{5}{n}\right)$, etc.

Or on trouve par les principes connus

$$\left(\frac{2}{31}\right)=1,\left(\frac{3}{31}\right)=-\left(\frac{31}{3}\right)=-1,\left(\frac{4}{31}\right)\text{ ou en général }\left(\frac{c^2}{31}\right)=1,$$
$$\left(\frac{5}{31}\right)=\left(\frac{31}{5}\right)=1,\left(\frac{6}{31}\right)=\left(\frac{2}{31}\right)\cdot\left(\frac{3}{31}\right)=-1,\left(\frac{7}{31}\right)=-\left(\frac{31}{7}\right)$$
$$=-\left(\frac{3}{7}\right)=\left(\frac{7}{3}\right)=1,\ \left(\frac{8}{31}\right)=\left(\frac{2c^2}{31}\right)=\left(\frac{2}{31}\right)=1,\left(\frac{9}{31}\right)=1,$$
$$\left(\frac{10}{31}\right)=\left(\frac{2}{31}\right)\cdot\left(\frac{5}{31}\right)=1,\text{ etc.,}$$

on a donc

$$S_1=S_2=S_4=S_5=S_7=S_8=S_9=S_{10}=P$$
$$S_3=S_6=Q.$$

Ensuite par l'application des équations (1) on trouvera

$$A_1=1+\sqrt{-n}$$
$$A_2=-7+\sqrt{-n}$$
$$A_3=-11-\sqrt{-n}$$
$$A_4=2-2\sqrt{-n}$$
$$A_5=8$$
$$A_6=-3+\sqrt{-n}$$
$$A_7=-5-\sqrt{-n}$$
$$A_8=5-\sqrt{-n}.$$

Arrivé aux termes moyens A_7 et A_8 on peut se dispenser d'aller plus loin, car il est facile de voir qu'on doit changer simplement le signe de la partie réelle dans les coefficients précédents à compter de A_7, ce qui donnera

$$A_9 = 3 + \sqrt{-n}$$
$$A_{10} = -8$$
$$A_{11} = -2 - 2\sqrt{-n}$$
$$A_{12} = 11 - \sqrt{-n}$$
$$A_{13} = 7 + \sqrt{-n}$$
$$A_{14} = -1 + \sqrt{-n}$$
$$A_{15} = -2.$$

C'est une suite nécessaire de ce que l'équation $4X = Y^2 + nZ^2$ ne doit pas changer de forme en mettant $\frac{1}{x}$ à la place de x, propriété sur laquelle nous reviendrons ci-après.

Connaissant les coefficients A qui servent à composer la fonction

$$Y + Z\sqrt{-n} = 2x^{15} + A_1 x^{14} + A_2 x^{13} + A_3 x^{12} + \text{etc.},$$

on en déduira les valeurs des polynomes Y et Z, savoir :

$$Y = 2x^{15} + x^{14} - 7x^{13} - 11x^{12} + 2x^{11} + 8x^{10} - 3x^9 - 5x^8 + 5x^7 + 3x^6 - 8x^5 - 2x^4 + 11x^3 + 7x^2 - x - 2$$
$$Z = x^{14} + x^{13} - x^{12} - 2x^{11} + x^9 - x^8 - x^7 + x^6 - 2x^4 - x^3 + x^2 + x.$$

Exemple II.

Soit $n = 37$, on aura

$$\left(\frac{2}{n}\right) = -1, \left(\frac{3}{n}\right) = 1, \left(\frac{4}{n}\right) = 1, \left(\frac{5}{n}\right) = -1, \left(\frac{6}{n}\right) = -1$$
$$\left(\frac{7}{n}\right) = 1, \left(\frac{8}{n}\right) = -1, \left(\frac{9}{n}\right) = 1, \left(\frac{10}{n}\right) = 1.$$

Delà

$$A_9 = 3 + \sqrt{-n}$$
$$A_{10} = -8$$
$$A_{11} = -2 - 2\sqrt{-n}$$
$$A_{12} = 11 - \sqrt{-n}$$
$$A_{13} = 7 + \sqrt{-n}$$
$$A_{14} = -1 + \sqrt{-n}$$
$$A_{15} = -2.$$

C'est une suite nécessaire de ce que l'équation $4X = Y^2 + nZ^2$ ne doit pas changer de forme en mettant $\frac{1}{x}$ à la place de x, propriété sur laquelle nous reviendrons ci-après.

Connaissant les coefficients A qui servent à composer la fonction

$$Y + Z\sqrt{-n} = 2x^{15} + A_1 x^{14} + A_2 x^{13} + A_3 x^{12} + \text{etc.},$$

on en déduira les valeurs des polynomes Y et Z, savoir :

$$Y = 2x^{15} + x^{14} - 7x^{13} - 11x^{12} + 2x^{11} + 8x^{10} - 3x^9 - 5x^8 + 5x^7 + 3x^6 - 8x^5 - 2x^4 + 11x^3 + 7x^2 - x - 2$$
$$Z = x^{14} + x^{13} - x^{12} - 2x^{11} + x^9 - x^8 - x^7 + x^6 - 2x^4 - x^3 + x^2 + x.$$

Exemple II.

Soit $n = 37$, on aura

$$\left(\frac{2}{n}\right) = -1, \left(\frac{3}{n}\right) = 1, \left(\frac{4}{n}\right) = 1, \left(\frac{5}{n}\right) = -1, \left(\frac{6}{n}\right) = -1$$
$$\left(\frac{7}{n}\right) = 1, \left(\frac{8}{n}\right) = -1, \left(\frac{9}{n}\right) = 1, \left(\frac{10}{n}\right) = 1.$$

Delà

$$S_1=S_3=S_4=S_7=S_9=S_{10}=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{n}$$
$$S_2=S_5=S_6=S_8=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{n},$$

et la substitution de ces valeurs dans les équations (1) donnera

$$A_1=1+\sqrt{n},\ A_2=10,\ A_3=-4+2\sqrt{n},\ A_4=15-\sqrt{n},$$
$$A_5=-5+3\sqrt{n},\ A_6=17-\sqrt{n},\ A_7=-8+2\sqrt{n},$$
$$A_8=11-\sqrt{n},\ A_9=-4+2\sqrt{n},\ A_{10}=11-\sqrt{n}.$$

Le terme moyen étant A_9, il est inutile d'aller plus loin, et les coefficients qui suivent A_9 seront égaux à ceux qui le précèdent à intervalles égaux, de sorte qu'on aura

$$A_{10}=A_8=11-\sqrt{n},\ A_{11}=A_7=-8+2\sqrt{n},\ \text{etc.};$$

et on en déduit les valeurs suivantes des fonctions Y et Z,

$$\begin{aligned}Y=&\,2x^{18}+x^{17}+10x^{16}-4x^{15}+15x^{14}-5x^{13}+17x^{12}-8x^{11}\\&+11x^{10}-4x^9+11x^8-8x^7+17x^6-5x^5+15x^4-4x^3\\&+10x^2+x+2\end{aligned}$$
$$\begin{aligned}Z=&\,x^{17}+2x^{15}-x^{14}+3x^{13}-x^{12}+2x^{11}-x^{10}+2x^9\\&-x^8+2x^7-x^6+3x^5-x^4+2x^3+x,\end{aligned}$$

lesquelles satisfont à l'équation $4X=Y^2-37Z^2$.

Dans ces deux exemples les coefficients des fonctions Y et Z sont encore plus petits que $\frac{1}{2}n$; mais à compter de $n=41$, on trouve des coefficients plus grands, ce qui devient encore plus marqué, lorsque franchissant un plus grand intervalle on prend $n=61$. Voici les résultats de ces calculs qui feront suite au tableau de l'article 512.

n	*Valeurs des polynomes* Y *et* Z.
31	$Y = 2x^{15} + x^{14} - 7x^{13} - 11x^{12} + 22x^{11} + 8x^{10} - 3x^9 - 5x^8$ $+ 5x^7 + 3x^6 - 8x^5 - 22x^4 + 11x^3 + 7x^2 - x - 2$ $Z = x^{14} + x^{13} - x^{12} - 2x^{11} + x^9 - x^8 - x^7 + x^6 - 2x^4 - x^3 + x^2 + x$
37	$Y = 2x^{18} + x^{17} + 10x^{16} - 4x^{15} + 15x^{14} - 5x^{13} + 17x^{12} - 8x^{11} + 11x^{10} - 4x^9$ $+ 11x^8 - 8x^7 + 17x^6 - 5x^5 + 15x^4 - 4x^3 + 10x^2 + x + 2$ $Z = x^{17} + 2x^{15} - x^{14} + 3x^{13} - x^{12} + 2x^{11} - x^{10} + 2x^9$ $- x^8 + 2x^7 - x^6 + 3x^5 - x^4 + 2x^3 + x$
41	$Y = 2x^{20} + x^{19} + 11x^{18} + 16x^{17} + 14x^{16} + 29x^{15} + 30x^{14}$ $+ 22x^{13} + 36x^{12} + 34x^{11} + 20x^{10} + 34x^9 + 36x^8 + 22x^7$ $+ 30x^6 + 29x^5 + 14x^4 + 16x^3 + 11x^2 + x + 2$ $Z = x^{19} + x^{18} + 2x^{17} + 4x^{16} + 3x^{15} + 4x^{14} + 6x^{13} + 4x^{12} + 4x^{11}$ $+ 6x^{10} + 4x^9 + 4x^8 + 6x^7 + 4x^6 + 3x^5 + 4x^4 + 2x^3 + x^2 + x$
61	$Y = 2x^{30} + x^{29} + 16x^{28} - 7x^{27} + 32x^{26} - 20x^{25} + 63x^{24} - 33x^{23}$ $+ 72x^{22} - 54x^{21} + 89x^{20} - 62x^{19} + 88x^{18} - 89x^{17} + 95x^{16}$ $- 81x^{15} + \text{etc.}$ $Z = x^{29} + 3x^{27} - 2x^{26} + 6x^{25} - 3x^{24} + 9x^{23} - 6x^{22} + 10x^{21}$ $- 7x^{20} + 12x^{19} - 10x^{18} + 11x^{17} - 11x^{16} + 13x^{15} - \text{etc.}$

On voit dans ce tableau que pour le nombre 61 plusieurs des coefficients de Y sont plus grands que n, mais pour avoir une idée de la progression suivant laquelle les coefficients augmentent lorsque n est un nombre premier un peu grand, prenons par exemple $n = 2521$, nous aurons

$$\left(\frac{2}{n}\right) = 1, \left(\frac{3}{n}\right) = 1, \left(\frac{4}{n}\right) = 1, \left(\frac{5}{n}\right) = 1, \left(\frac{6}{n}\right) = 1, \left(\frac{7}{n}\right) = 1, \text{ etc.},$$

ce qui donne

$$S_1 = S_2 = S_3 = S_4 = S_5 = S_6 = S_7 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{n}.$$

Substituant ces valeurs dans les équations (1), on en tire

$$\begin{aligned} A_1 &= 1 + \sqrt{n} & A_5 &= 84001 + 3613\sqrt{n} \\ A_2 &= 631 + \sqrt{n} & A_6 &= 836032 + 10312\sqrt{n} \\ A_3 &= 946 + 106\sqrt{n} & A_7 &= 2633212 + 69292\sqrt{n} \\ A_4 &= 34231 + 211\sqrt{n} & &\text{etc.} \end{aligned}$$

Ainsi les premiers termes des fonctions Y et Z seront, en faisant $1260 = m$

$$\begin{aligned} Y = 2x^m + x^{m-1} &+ 631x^{m-2} + 946x^{m-3} \\ &+ 34231x^{m-4} + 84001x^{m-5} \\ &+ 836032x^{m-6} + 2633212x^{m-7} + \text{etc.} \\ Z = x^{m-1} + x^{m-2} &+ 106x^{m-3} + 211x^{m-4} \\ &+ 3613x^{m-5} + 10312x^{m-6} \\ &+ 69292x^{m-7} + \text{etc.} \end{aligned}$$

On voit avec quelle rapidité les coefficients croissent dans l'une et l'autre fonction, mais cet accroissement n'a lieu que jusqu'au terme moyen; ensuite il fait place à un décroissement semblable, puisque les coefficients doivent être égaux à égale distance des extrêmes.

C'est en effet la loi à laquelle sont assujéties les fonctions Y et Z, puisque la substitution de x^{-1} à la place de x dans l'équation $4X = Y^2 - nZ^2$, n'y doit apporter aucun changement, après qu'on a fait disparaître le dénominateur commun. On voit par là que dans chaque fonction les coefficients des termes extrêmes ou également éloignés des extrêmes, doivent être égaux; mais ces coefficients sont-ils précédés du même signe ou de signes différents? c'est ce qu'il faut examiner.

Soit 1° $n=4i-1$ ou $m=\frac{1}{2}(n-1)=2i-1$: puisque la fonction Z doit rester la même, ou du moins ne faire que changer de signe, en mettant x^{-1} à la place de x et multipliant le tout par x^m, cette fonction ne pourra avoir que l'une des deux valeurs suivantes :

$$\text{I.}\quad Z=\begin{cases} x^{m-1}+b_1x^{m-2}+b_2x^{m-3}\ldots.+b_{i-1}x^i \\ +x+b_1x^2 \quad +b_2x^3 \quad \ldots.+b_{i-1}x^{i-1} \end{cases}$$

$$\text{II.}\quad Z=\begin{cases} x^{m-1}+b_1x^{m-2}+b_2x^{m-3}\ldots.+b_{i-1}x^i \\ -x-b_1x^2 \quad -b_2x^3 \quad \ldots.+b_{i-1}x^{i-1}. \end{cases}$$

Or si la seconde valeur avait lieu, la supposition $x=1$ donnerait $Z=0$, et comme en même temps on aurait $X=\frac{x^n-1}{x-1}=n$, l'équation $4X=Y^2+nZ^2$ deviendrait $4n=Y^2$, équation impossible, puisque $4n$ n'est point un carré, donc la forme I a lieu nécessairement.

Cela posé cette forme I de la fonction Z doit être combinée avec l'une des deux formes que pourrait avoir la fonction Y, lesquelles sont

$$\text{I.}\quad Y=\begin{cases} 2x^m+x^{m-1}+a_1x^{m-2}+a_2x^{m-3}\ldots.+a_{i-1}x^i \\ +2+x \quad +a_1x^2 \quad +a_2x^3 \quad \ldots.+a_{i-1}x^{i-1} \end{cases}$$

$$\text{II.}\quad Y=\begin{cases} 2x^m+x^{m-1}+a_1x^{m-2}+a_2x^{m-3}\ldots.+a_{i-1}x^i \\ -2-x \quad -a_1x^2 \quad -a_2x^3 \quad \ldots.-a_{i-1}x^{i-1}. \end{cases}$$

Or si la forme I avait lieu, la supposition $x=-1$ donnerait $Y=0$, et comme alors on aurait $X=1$, l'équation $4X=Y^2+nZ^2$ deviendrait $4=nZ^2$, équation impossible ; donc la forme II de Y est celle qui a lieu nécessairement.

Donc lorsqu'on a $n=4i-1$, les fonctions Y et Z qui satisfont à l'équation $4X=Y^2+nZ^2$ ont nécessairement la

forme ici déterminée

$$Y = \begin{cases} 2x^m + x^{m-1} + a_1 x^{m-2} + a_2 x^{m-3} \ldots + a_{i-1} x^i \\ -2 - x \quad - a_1 x^2 \quad - a_2 x^3 \quad \ldots - a_{i-1} x^{i-1} \end{cases}$$

$$Z = \begin{cases} x^{m-1} + b_1 x^{m-2} + b_2 x^{m-3} \ldots + b_{i-1} x^i \\ +x + b_1 x^2 \quad + b_2 x^3 \quad \ldots + b_{i-1} x^{i-1}. \end{cases}$$

Le tableau que nous avons donné de ces fonctions pour quelques-unes des plus simples valeurs de n s'accorde avec ce résultat, mais il était nécessaire de démontrer l'existence de cette propriété indépendamment de toute induction.

Soit 2° $n = 4i + 1$ ou $m = 2i$, nous allons faire voir que la valeur de Z ne peut être que de la forme

$$Z = \begin{cases} x^{m-1} + b_1 x^{m-2} + b_2 x^{m-3} \ldots + b_{i-1} x^{i+1} + b_i x^i \\ +x + b_1 x^2 \quad + b_2 x^3 \quad \ldots + b_{i-1} x^{i-1} \end{cases}$$

qui ne changera pas en mettant x^{-1} à la place de x et multipliant le tout par x^m. Car si après le terme moyen $b_i x^i$ tous les signes changeaient, en sorte qu'on eût

$$Z = \begin{cases} x^{m-1} + b_1 x^{m-2} + b_2 x^{m-3} \ldots + b_{i-1} x^{i+1} + b_i x^i \\ -x - b_1 x^2 \quad - b_2 x^3 \quad \ldots - b_{i-1} x^{i-1}, \end{cases}$$

la substitution de x^{-1} au lieu de x, donnerait, après avoir multiplié le tout par $-x^m$,

$$Z = \begin{cases} x^{m-1} + b_1 x^{m-2} + b_2 x^{m-3} \ldots + b^{i-1} x^{i+1} - b_i x^i \\ -x + b_1 x^2 \quad - b_2 x^3 \quad \ldots - b_{i-1} x^{i-1}, \end{cases}$$

valeur qui ne pourrait être égale à la précédente qu'en supposant $b_i = 0$. Mais alors la supposition $x = 1$ donnerait $Z = 0$ et l'équation $4X = Y^2 + nZ^2$ deviendrait $4n = Y^2$, équation

impossible. Donc la forme que nous avons donnée à la valeur de Z est la seule admissible.

Maintenant cette valeur de Z doit être combinée avec l'une ou l'autre de ces deux valeurs de Y

$$\text{I.}\quad Y=\begin{cases} 2x^n+x^{n-1}+a_2x^{n-2}+a_3x^{n-3}\ldots+a_{i-1}x^{i+1}+a_ix^i \\ +2+x\quad+a_2x^2\quad+a_3x^3\quad\ldots+a_{i-1}x^{i-1} \end{cases}$$

$$\text{II.}\quad Y=\begin{cases} 2x^n+x^{n-1}+a_2x^{n-2}+a_3x^{n-3}\ldots+a_{i-1}x^{i+1}+a_ix^i \\ -2-x\quad-a_2x^2\quad-a_3x^3\quad\ldots-a_{i-1}x^{i-1}. \end{cases}$$

Or si la seconde forme avait lieu, il faudrait qu'elle ne changeât pas, ou qu'elle changeât seulement de signe, en mettant x^{-1} à la place de x et multipliant tout par x^n, ce qui exigerait qu'on eût $a_i=0$. Mais cette condition ne peut être remplie, puisqu'on sait qu'aucune des puissances de x ne peut manquer dans le polynome Y; d'ailleurs si le coefficient a_i était zéro, la supposition $x=1$ dans la seconde forme donnerait $Y=0$, et alors l'équation $4X=Y^2-nZ^2$ deviendrait $4n=-nZ^2$ équation impossible; donc par cette double raison la première forme de Y est la seule admissible; donc dans le cas de $n=4i+1$ les fonctions Y et Z qui satisfont à l'équation $4X=Y^2-nZ^2$ seront toujours des formes suivantes:

$$Y=\begin{cases} 2x^n+x^{n-1}+a_2x^{n-2}+a_3x^{n-3}\ldots+a_{i-1}x^{i+1}+a_ix^i \\ +2+x\quad+a_2x^2\quad+a_3x^3\quad\ldots+a_{i-1}x^{i-1} \end{cases}$$

$$Z=\begin{cases} x^{n-1}+b_2x^{n-2}+b_3x^{n-3}\ldots+b_{i-1}x^{i+1}+b_ix^i \\ +x+b_2x^2\quad+b_3x^3\quad\ldots+b_{i-1}x^{i-1}, \end{cases}$$

résultat qui s'accorde avec tous les exemples compris dans notre tableau.

La méthode que nous avons donnée pour calculer les va-

leurs des fonctions Y et Z, ne laisse rien à désirer quand il s'agit de l'appliquer à une valeur particulière du nombre premier n; mais pour parvenir à quelques résultats généraux, il sera bon de considérer la valeur de n sous une forme indéterminée qui la rende applicable à une infinité de nombres premiers. Et parce que les formules relatives aux nombres premiers $4i-1$, se déduisent aisément des formules relatives aux nombres premiers $4i+1$, nous allons nous occuper exclusivement de ceux-ci.

Observons d'abord que la forme $4i+1$ se divise en quatre autres, savoir :

$$24\lambda+1,\quad 24\lambda+5,\quad 24\lambda+13,\quad 24\lambda+17,$$

ce qui offre quatre cas à considérer.

Premier cas $n=24\lambda+1$.

Alors on aura $\left(\frac{2}{n}\right)=1$, $\left(\frac{3}{n}\right)=\left(\frac{n}{3}\right)=1$, $\left(\frac{4}{n}\right)$ ou en général $\left(\frac{c^2}{n}\right)=1$. Nous nous arrêterons là, parce que pour aller plus loin, il faudrait connaître le reste que donne λ divisé par 5, ce qui exigerait une nouvelle subdivision. Au moyen de ces valeurs de $\left(\frac{4}{n}\right)$, on trouvera

$$S_0=S_1=S_3=-\tfrac{1}{4}-\tfrac{1}{4}\sqrt{n};$$

ensuite par les équations (1), on aura

$$A_0=1+\sqrt{n}$$
$$A_1=1+6\lambda+\sqrt{n}$$
$$A_2=1+9\lambda+(1+\lambda)\sqrt{n}$$
$$A_4=1+11\lambda+3\lambda^2+(1+2\lambda)\sqrt{n}.$$

Second cas $n=24\lambda+5$.

Alors on aura $\left(\frac{2}{n}\right)=-1$, $\left(\frac{3}{n}\right)=\left(\frac{5}{3}\right)=-1$, $\left(\frac{4}{n}\right)=1$; ce qui donne

$$S_1=S_4=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{n},\ S_2=S_3=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{n},$$

et par l'application des équations (1), on aura

$$A_1=1+\sqrt{n}$$
$$A_2=2+6\lambda$$
$$A_3=-3\lambda+\lambda\sqrt{n}$$
$$A_4=-2\lambda+3\lambda'-\lambda\sqrt{n}.$$

Troisième cas, $n=24\lambda+13$.

Alors on aura $\left(\frac{2}{n}\right)=-1$, $\left(\frac{3}{n}\right)=1$, $\left(\frac{4}{n}\right)=1$, ensuite

$$S_1=S_3=S_4=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{n},\ S_2=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{n},$$

et par l'application des équations (1) on trouve

$$A_1=1+\sqrt{n}$$
$$A_2=4+6\lambda$$
$$A_3=-1-3\lambda+(1+\lambda)\sqrt{n}$$
$$A_4=4+8\lambda+3\lambda'-\lambda\sqrt{n}.$$

Quatrième cas, $n=24\lambda+17$.

Alors on aura $\left(\frac{2}{n}\right)=1$, $\left(\frac{3}{n}\right)=-1$, $\left(\frac{4}{n}\right)=1$; de là

$$S_1=S_2=S_4=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{n},\ S_3=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{n},$$

et en vertu des équations (1);

$$A_1 = 1 + \sqrt{n}$$
$$A_2 = 5 + 6\lambda + \sqrt{n}$$
$$A_3 = 7 + 9\lambda + (1+\lambda)\sqrt{n}$$
$$A_4 = 4 + 7\lambda + 3\lambda^2 + (2+2\lambda)\sqrt{n}.$$

Ces formules pour les nombres premiers $4i+1$, considérés sous les quatre formes $24\lambda+1$, $+5$, $+13$, $+17$, dont ils sont susceptibles, s'appliquent aux nombres premiers $4i-1$, considérés également sous leurs quatre formes $24\lambda-1$, -5, -13, -17. Il suffit pour cela de changer le signe de λ dans les formules précédentes et en même temps le signe de n dans l'équation $4X = Y^2 - nZ^2$ relative aux nombres premiers $4i+1$; on aura ainsi les valeurs de A qui satisfont à l'équation $4X = Y^2 + nZ^2$ relative aux nombres premiers $4i-1$; nous les avons réunies dans le tableau suivant :

n	A_1	A_2	A_3	A_4
$24\lambda-1$	$1+\sqrt{-n}$	$1-6\lambda+\sqrt{-n}$	$1-9\lambda+(1-\lambda)\sqrt{-n}$	$1-11\lambda+3\lambda^2+(1-2\lambda)\sqrt{-n}$
$24\lambda-5$	$1+\sqrt{-n}$	$2-6\lambda$	$3\lambda-\lambda\sqrt{-n}$	$2\lambda+3\lambda^2+\lambda\sqrt{-n}$
$24\lambda-13$	$1+\sqrt{-n}$	$4-6\lambda$	$-1+3\lambda+(1-\lambda)\sqrt{-n}$	$4-8\lambda+3\lambda^2+\lambda\sqrt{-n}$
$24\lambda-17$	$1+\sqrt{-n}$	$5-6\lambda+\sqrt{-n}$	$7-9\lambda+(1-\lambda)\sqrt{-n}$	$4-7\lambda+3\lambda^2+(2-2\lambda)\sqrt{-n}$

Ainsi on voit que pour tout nombre premier $n = 24\lambda - 1$, les premiers termes des valeurs de Y et de Z seront

$$Y = 2x^n + x^{n-1} + (1-6\lambda)x^{n-2} + (1-9\lambda)x^{n-3} + (1-11\lambda+3\lambda^2)x^{n-4} + \text{etc.}$$
$$Z = x^{n-1} + x^{n-2} + (1-\lambda)x^{n-3} + (1-2\lambda)x^{n-4} + \text{etc.}$$

Et dans cette formule on remarquera que les quatre premiers coefficients de Y, savoir $2, 1, 1-6\lambda, 1-9\lambda$, sont toujours moindres que $\frac{1}{2}n$, mais le coefficient suivant $1-11\lambda+3\lambda^2$, qui est de l'ordre $3\lambda^2$ ou $\frac{n^2}{192}$, devient bientôt plus grand que n; ainsi faisant $\lambda=13$ ou $n=311$, on a $1-11\lambda+3\lambda^2=365$.

Ces deux premiers tableaux pour les nombres premiers $4i+1$ et $4i-1$, ne s'étendent pas au-delà de A_4 qui donne les coefficients de x^{n-4} dans Y et Z; pour aller plus loin, il faut subdiviser chacune des valeurs $n=24\lambda+1, 5, 13, 17$, en quatre autres par la substitution des cinq valeurs $\lambda=5\mu$, $5\mu+1, 5\mu+2, 5\mu+3, 5\mu+4$, dont une doit être rejetée, comme ne donnant pas pour n des nombres premiers; voici ces subdivisions :

Valeur principale de n.	*Ses quatre sous-divisions.*
$24\lambda+1$	$120\mu+1$, $120\mu+49$, $120\mu+73$, $120\mu+97$
$24\lambda+5$	$120\mu+29$, $120\mu+53$, $120\mu+77$, $120\mu+101$
$24\lambda+13$	$120\mu+13$, $120\mu+37$, $120\mu+61$, $120\mu+109$
$24\lambda+17$	$120\mu+17$, $120\mu+41$, $120\mu+89$, $120\mu+113$

Appliquant notre méthode à ces différents cas, on trouvera pour chacun d'eux l'expression générale du coefficient A_5 et celle de A_6, l'une renfermant des termes affectés de μ^2 et $\mu^2\sqrt{n}$, l'autre des termes affectés de $\mu^2\sqrt{n}$ et μ^3; on en conclura que le coefficient de x^{n-6} dans Y, étant de l'ordre μ deviendra bientôt plus grand que n^2, ce qui manifeste l'augmentation progressive des coefficients de Y. On voit en même temps que le nombre et la complication des formules augmen-

tent rapidement avec la valeur de n, ce qui les rend peu propres à la solution des cas particuliers. C'est pourquoi il suffira de développer ici les formules relatives à l'une de nos subdivisions; nous choisirons pour cet effet la valeur $n = 120\mu + 61$.

On trouve alors, comme dans le cas de $n = 24\lambda + 13$ dont cette subdivision fait partie

$$S_1 = S_3 = S_4 = -\tfrac{1}{5} - \tfrac{1}{5}\sqrt{n},\quad S_2 = -\tfrac{1}{5} + \tfrac{1}{5}\sqrt{n}.$$

On aura de plus $\left(\frac{5}{n}\right) = \left(\frac{61}{5}\right) = 1$, $\left(\frac{6}{n}\right) = 1$, ce qui donne $S_5 = S_1$ et $S_6 = S_2$.

Cela posé dans le cas principal $n = 24\lambda + 13$, on a trouvé les valeurs de A_1, A_2, A_3, A_4, dans lesquelles il faudra substituer la valeur $\lambda = 5\mu + 2$, ce qui donnera, pour la division $n = 120\mu + 61$, les valeurs

$$\begin{aligned} A_1 &= 1 + \sqrt{n} \\ A_2 &= 16 + 30\mu \\ A_3 &= -7 - 15\mu + (3 + 5\mu)\sqrt{n} \\ A_4 &= 32 + 100\mu + 75\mu^2 - (2 + 5\mu)\sqrt{n}. \end{aligned}$$

Au moyen de ces valeurs on trouvera par les équations (1):

$$\begin{aligned} A_5 &= -20 - \tfrac{195}{2}\mu - \tfrac{225}{2}\mu^2 + \left(6 + \tfrac{29}{2}\mu + \tfrac{15}{2}\mu^2\right)\sqrt{n} \\ A_6 &= 63 + 246\mu + 280\mu^2 + 75\mu^3 - (3 + 14\mu + 15\mu^2)\sqrt{n}, \end{aligned}$$

Et l'on voit que le terme $75\mu^3$ qui fait partie de A_6 deviendra plus grand que n^2 si on a $n > \frac{(120)^3}{75}$ ou $n > 23040$.

Pour aller plus loin, c'est-à-dire pour trouver les valeurs

de A_1 et A_5, il faudrait au lieu de μ substituer l'une des six valeurs $7\nu, 7\nu+1, 7\nu+3, 7\nu+4, 7\nu+5, 7\nu+6$, c'est-à-dire il faudrait subdiviser la forme $n=120\mu+61$ en six autres

$$n=840\nu+61, 181, 421, 541, 661, 781;$$

alors A_1 contiendrait un terme de l'ordre $\mu^3\sqrt{n}$, et A_5 un terme de l'ordre μ^4. Il est inutile d'entrer dans de plus grands détails; nous déduirons seulement des valeurs précédentes de $A_1, A_2, \ldots A_6$ celles des fonctions Y et Z développées jusqu'à la puissance x^{n-6}; elles donnent pour le nombre premier $n=120\mu+61$,

$$Y=2x^n+x^{n-1}+(16+30\mu)x^{n-2}-(7+15\mu)x^{n-3}$$
$$+(32+100\mu+75\mu^2)x^{n-4}-\left(20+\frac{195}{2}\mu+\frac{225}{2}\mu^2\right)x^{n-5}$$
$$+(63+246\mu+280\mu^2+75\mu^3)x^{n-6}-\text{etc.}$$
$$Z=x^{n-1}+(3+5\mu)x^{n-3}-(2+5\mu)x^{n-4}$$
$$+\left(6+\frac{29}{2}\mu+\frac{15}{2}\mu^2\right)x^{n-5}-(3+14\mu+15\mu^2)x^{n-6}$$
$$-\text{etc.}$$

On en déduirait pour le cas de $n=120\mu-61$, les formules suivantes qui satisfont à l'équation $4X=Y^2+nZ^2$,

$$Y=2x^n+x^{n-1}+(16-30\mu)x^{n-2}-(7-15\mu)x^{n-3}$$
$$+(32-100\mu+75\mu^2)x^{n-4}-\left(20-\frac{195}{2}\mu+\frac{225}{2}\mu^2\right)x^{n-5}$$
$$+(63-246\mu+280\mu^2-75\mu^3)x^{n-6}-\text{etc.}$$
$$Z=x^{n-1}+(3-5\mu)x^{n-3}-(2-5\mu)x^{n-4}$$
$$+\left(6-\frac{29}{2}\mu+\frac{15}{2}\mu^2\right)x^{n-5}-(3-14\mu+15\mu^2)x^{n-6}-\text{etc.}$$

Dans les deux cas on a fait $m=\frac{1}{2}(n-1)$.