ANNALES SCIENTIFIQUES DE L'É.N.S.

A. LEFÉBURE

Mémoire sur la composition de polynômes entiers qui n'admettent que des diviseurs premiers d'une forme déterminée

Annales scientifiques de l'É.N.S. 3^e série, tome 1 (1884), p. 389-404

<http://www.numdam.org/item?id=ASENS_1884_3_1__389_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1884, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

MÉMOIRE

SUR LA

COMPOSITION DE POLYNOMES ENTIERS

QUI N'ADMETTENT

QUE DES DIVISEURS PREMIERS D'UNE FORME DÉTERMINÉE,

PAR M. A. LEFÉBURE,

DOCTEUR ÈS SCIENCES, INSPECTEUR D'ACADÉMIE HONORAIRE.

Je me propose de déterminer des polynômes entiers qui n'admettent que des nombres premiers de la forme $H'T+1$, T désignant un nombre entier d'une valeur arbitraire.

PREMIÈRE PARTIE.

Je suppose d'abord que T ne contient qu'un facteur premier. Soient

$T=n^t$;

n un nombre premier quelconque;

t un exposant quelconque également.

Je recherche, dans cette première Partie, des polynômes dont les diviseurs premiers soient de la forme $H'n^t+1$.

Le polynôme $A^{n-1}+A^{n-2}B+A^{n-3}B^2+\ldots+A^2B^{n-3}+AB^{n-2}+B^{n-1}$ ou son équivalent $\frac{A^n-B^n}{A-B}$, dans lequel A, B sont des nombres entiers quelconques premiers entre eux, n'admet que des diviseurs premiers de la forme $Hn+1$; n est néanmoins diviseur également, si $A-B$ est divisible par n; j'en ai donné une démonstration. Je vais établir d'abord que ces diviseurs, à l'exception de n, sont nécessairement de la forme $H'n^2+1$, quand A et B sont des puissances $n^{\text{ièmes}}$.

Je rappelle un théorème que j'ai démontré dans un Mémoire sur les résidus des puissances $n^{\text{ièmes}}$, et sur lequel je m'appuierai.

p désignant un nombre premier de la forme $Hn+1$, les résidus des puissances $n^{\text{ièmes}}$ des nombres, obtenus par le diviseur p, sont au nombre de H. Si je considère la suite des $p-1$ premiers nombres 1, 2, 3, ..., $(p-1)$, cette suite peut se partager en H séries de n nombres chacune, de telle sorte que les nombres d'une même série, élevés à la puissance $n^{\text{ième}}$, conduisent à un même résidu, et que leur somme soit un multiple de p. J'ai démontré de plus qu'il se présente toujours l'un des deux cas suivants : 1° les n nombres sont tous résidus dans plusieurs séries, et dans les autres aucun d'eux n'est résidu; 2° dans chaque série il y a un résidu, mais un seul.

Exemples. — Soient $p=19$, $H=6$, $n=3$; les 18 premiers nombres forment les six séries suivantes :

Résidus.	
1	$1+7+11=19$
18	$8+12+18=19\times 2$
7	$4+6+9=19$
12	$10+13+15=19\times 2$
8	$2+3+14=19$
11	$5+16+17=19\times 2$

les six résidus composent les deux premières séries. Dans les autres il n'y a pas de résidus.

Soient encore $p=41$, $H=8$, $n=5$.

On obtient les huit séries suivantes :

Résidus.	
1	$1+10+16+18+37=41\times 2$
3	$11+12+28+34+38=41\times 3$
9	$5+8+9+21+39=41\times 2$
14	$15+22+24+27+35=41\times 3$
40	$40+31+25+23+4=41\times 3$
38	$30+29+13+7+3=41\times 2$
32	$36+33+32+20+2=41\times 3$
27	$26+19+17+14+6=41\times 2$

dans chacune de ces séries un seul des nombres est résidu.

Lorsque le premier cas a lieu, H est nécessairement divisible par n, car le nombre des résidus est un multiple de n, et H représente ce nombre; p est alors de la forme $H'n^2+1$.

Cela posé, je représente le polynôme $A^{n-1}+A^{n-2}B+\ldots+AB^{n-2}+B^{n-1}$ par la fonction $F_n(A,B)$. Soit p un diviseur premier quelconque de $F_n(A,B)$, diviseur nécessairement de la forme $Hn+1$; je ne considère pas le facteur n qui peut se rencontrer. Soit $A=C^n$, et d'abord $B=1$, il vient

$$F_n(C^n,1)\equiv 0 \pmod p$$

et, par suite,

$$(C^n)^n-1\equiv 0 \pmod p;$$

soit α le résidu de C^n divisé par p, de sorte que

$$C^n\equiv\alpha \pmod p,\quad \alpha^n-1\equiv 0 \pmod p.$$

α ne peut être l'unité, car alors

$$F_n(C^n,1)\equiv 0 \pmod p$$

donnerait

$$n\equiv 0 \pmod p,$$

en vertu de

$$C^n\equiv 1 \pmod p,$$

ce qui est impossible.

Soient r et s des nombres tels que leur différence $r-s$ soit moindre que n, les résidus obtenus par les divisions de α^r, α^s par p sont différents entre eux; en effet, supposons qu'ils puissent être égaux, on aura

$$\alpha^r\equiv\alpha^s \pmod p,\quad \alpha^s(\alpha^{r-s}-1)\equiv 0 \pmod p,\quad \alpha^h-1\equiv 0 \pmod p;$$

en posant $r-s=h$, on a déjà

$$\alpha^n-1\equiv 0 \pmod p.$$

Soit $n=h\rho+h'$, il vient, en remplaçant n par sa valeur dans $\alpha^n-1\equiv 0 \pmod p$,

$$(\alpha^h)^\rho\alpha^{h'}-1\equiv 0 \pmod p,\quad \text{d'où}\quad \alpha^{h'}-1\equiv 0 \pmod p,$$

en vertu de

$$\alpha^h-1\equiv 0 \pmod p.$$

Comme n et h sont premiers entre eux, on arrive, en opérant sur h

et h' comme sur n et h, et ainsi de suite, à un dernier reste égal à l'unité; par suite on obtient

$$\alpha - 1 \equiv 0 \pmod{p},$$

ce qui est impossible, puisqu'on a vu que α, moindre que p, est différent de l'unité. Ainsi α^r, α^s, divisés par p, donnent des résidus différents. De plus, si l'on élève ces résidus à la puissance $n^{\text{ième}}$, ils conduisent à un même résidu, au résidu 1; en effet, on a

$$\alpha^n - 1 \equiv 0 \pmod{p}, \quad \text{d'où} \quad (\alpha^r)^n - 1 \equiv 0 \pmod{p}, \quad (\alpha^s)^n - 1 \equiv 0 \pmod{p}.$$

On est donc dans le premier des deux cas indiqués précédemment, car on a deux résidus qui, élevés à la puissance $n^{\text{ième}}$, donnent un même résidu. Il en résulte que p est de la forme $\mathrm{H}'n^2 + 1$.

Nous avons supposé $\mathrm{B} = 1$, soit plus généralement $\mathrm{B} = \mathrm{D}^n$; $\mathrm{F}_n(\mathrm{A}, \mathrm{B})$ devient

$$\mathrm{F}_n(\mathrm{C}^n, \mathrm{D}^n) \equiv 0 \pmod{p}, \quad \text{d'où} \quad (\mathrm{C}^n)^n - (\mathrm{D}^n)^n \equiv 0 \pmod{p}.$$

Posons

$$\mathrm{D}^n \equiv \mathrm{C}^n \mathrm{R}^n \pmod{p},$$

ce qui est toujours possible d'après les propriétés des résidus des puissances $n^{\text{ièmes}}$, il vient, en remplaçant D^n par sa valeur dans les fonctions précédentes, et en supprimant les facteurs $\mathrm{C}^{n(n-1)}$, $(\mathrm{C}^n)^n$ qui n'admettent pas le diviseur p,

$$\mathrm{F}_n(\mathrm{R}^n, 1) \equiv 0 \pmod{p}, \quad (\mathrm{R}^n)^n - 1 \equiv 0 \pmod{p};$$

on est donc ramené au cas précédent; p est donc de la forme $\mathrm{H}'n^2 + 1$, ce qu'il fallait établir.

Applications. — Soient $n = 3$, $\mathrm{A} = \mathrm{L}^3$, $\mathrm{B} = 1$; on a

$$\mathrm{F}_3(\mathrm{L}^3, 1) = \mathrm{L}^6 + \mathrm{L}^3 + 1 = 3 \times 19 \times 73,$$

19 et 73 sont de la forme $\mathrm{H}'n^2 + 1$. On trouve de plus le facteur 3, parce que $\mathrm{A} - \mathrm{B}$ est divisible par 3.

Soient $n = 5$, $\mathrm{A} = 2^5$, $\mathrm{B} = -1$; on a

$$\mathrm{F}_5(2^5, 1) = 2^{20} - 2^{15} + 2^{10} - 2^5 + 1 = 1016801,$$

nombre premier de la forme $\mathrm{H}'n^2 + 1$.

Soient $n = 3$, $A = 3^3$, $B = 2^3$; il vient

$$F_3(3^3, 2^3) = 3^6 + 3^3 . 2^3 + 2^6 = 1009,$$

nombre premier de la forme $H'n^2 + 1$.

Considérons le cas plus général où A et B seraient des puissances $n^{\text{ièmes}}$ de puissances $n^{\text{ièmes}}$. Posons

$$A = C^{n^{t-1}}, \quad B = D^{n^{t-1}},$$

je démontre que les diviseurs premiers de la fonction $F_n(C^{n^{t-1}}, D^{n^{t-1}})$ sont de la forme $H'n^t + 1$.

Je dois entrer d'abord dans quelques explications.

J'ai établi que les H résidus des puissances $n^{\text{ièmes}}$ des nombres, obtenus par le diviseur p de la forme $Hn + 1$, n désignant un nombre premier, peuvent toujours être exprimés par les puissances d'un seul nombre. Ainsi, soit a ce nombre, auquel on peut donner le nom de *base,* la suite a^1, a^2, a^3, ..., a^H, où les exposants sont la suite des nombres de 1 à H, donne tous les résidus, après avoir divisé par p chacune de ces puissances. Il en résulte que tous les résidus satisfont à la relation

$$a^m \equiv a_m \pmod{p},$$

en donnant à m successivement toutes les valeurs de 1 à H, et en convenant de désigner par a affecté de l'indice m le résidu auquel a^m conduit. On remarquera que l'on a toujours

$$a_H = 1.$$

Il existe une règle très simple pour la composition des indices, et dont la démonstration est facile. Ainsi le produit de deux ou plusieurs résidus conduit à un résidu dont l'indice est la somme des indices des facteurs. Une puissance d'un résidu donne un résidu qui s'obtient en multipliant son indice par le degré de la puissance. Dans les calculs, on sera souvent conduit à écrire un indice de résidu qui dépasse H, alors on peut le diminuer d'un multiple de H tel qu'il ne dépasse plus H : on ne changera pas le résidu. En effet, on a

$$a^H \equiv 1 \pmod{p}, \quad \text{d'où} \quad a^{H\varepsilon} \equiv 1 \pmod{p},$$

quel que soit ε, par suite

$$a^{m+H\varepsilon} \equiv a^m \pmod{p}, \quad a_{m+H\varepsilon} = a_m.$$

Cela posé, soient p un nombre premier de la forme $\mathrm{H}n+1$; r un diviseur quelconque premier de H; a l'une des bases des résidus des puissances $n^{\text{ièmes}}$ des nombres déterminés par p; la relation

$$a^{\mathrm{H}}-1\equiv 0 \pmod p$$

donne

$$\left(a^{\frac{\mathrm{H}}{r}}\right)^r-1\equiv 0 \pmod p, \quad \text{d'où} \quad \left(a^{\frac{\mathrm{H}}{r}}-1\right)\mathrm{F}_r\left(a^{\frac{\mathrm{H}}{r}},1\right)\equiv 0 \pmod p,$$

mais $a^{\frac{\mathrm{H}}{r}}-1$ n'est pas divisible par p, puisque l'exposant $\frac{\mathrm{H}}{r}$, moindre que H, ne peut être un multiple de H; donc on a

$$\mathrm{F}_r\left(a^{\frac{\mathrm{H}}{r}},1\right)\equiv 0 \pmod p,$$

et si, dans cette dernière relation, on remplace les exposants de a par les indices correspondants, il vient

$$1+a_{\frac{\mathrm{H}}{r}}+a_{2\frac{\mathrm{H}}{r}}+\ldots+a_{(r-1)\frac{\mathrm{H}}{r}}\equiv 0 \pmod p.$$

Je multiplie les deux membres de cette dernière relation successivement par les résidus $a_1, a_2, \ldots, a_{\frac{\mathrm{H}}{r}}$, et j'obtiens

$$\begin{aligned}
&a_1+a_{1+\frac{\mathrm{H}}{r}}+a_{1+2\frac{\mathrm{H}}{r}}+\ldots+a_{1+(r-1)\frac{\mathrm{H}}{r}}\equiv 0 \pmod p,\\
&a_2+a_{2+\frac{\mathrm{H}}{r}}+a_{2+2\frac{\mathrm{H}}{r}}+\ldots+a_{2+(r-1)\frac{\mathrm{H}}{r}}\equiv 0 \pmod p,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&a_{\frac{\mathrm{H}}{r}}+a_{2\frac{\mathrm{H}}{r}}+a_{3\frac{\mathrm{H}}{r}}+\ldots+a_{\mathrm{H}}\equiv 0 \pmod p.
\end{aligned}$$

Tous les résidus se groupent ainsi en $\frac{\mathrm{H}}{r}$ séries, contenant chacune r résidus. Si l'on compte les indices par colonnes verticales, on reconnaît qu'ils forment la suite des nombres de 1 à H. Tous ces résidus sont différents entre eux, puisque leurs indices, qui ne dépassent pas H, sont différents; de plus, les résidus d'une même série, élevés à la puissance r, conduisent à un même résidu. Ces résidus sont, pour les diverses séries, $a_r, a_{2r}, \ldots, a_{\mathrm{H}}$. Ils sont différents entre eux, puisque leurs indices, qui ne dépassent pas H, sont différents; de plus, le dernier est l'unité. Il

n'y a donc que les résidus de la dernière série qui, élevés à la puissance de r, donnent l'unité.

Je considère actuellement le polynôme $F_n(C^{n^{t-1}}, 1)$, et je démontre que ses diviseurs sont de la forme $H'n^t + 1$. Soit p un diviseur quelconque de ce polynôme. Il est de la forme $Hn + 1$; de plus, comme $C^{n^{t-1}}$ est une puissance $n^{\text{ième}}$, H est divisible par n, comme on l'a démontré. Les résidus des puissances $n^{\text{ièmes}}$ des nombres par rapport à ce diviseur p peuvent donc, comme précédemment, se grouper en séries. On les obtient en remplaçant, dans les séries précédentes, r par n et en désignant la base par a. Les n résidus de la dernière série $a_{\frac{H}{n}}$, $a_{2\frac{H}{n}}$, ..., a_H sont les seuls qui, élevés à la puissance $n^{\text{ième}}$, conduisent au résidu 1.

On a les relations

$$F_n(C^{n^{t-1}}, 1) \equiv 0 \pmod{p}, \quad C^{n^t} - 1 \equiv 0 \pmod{p}.$$

Soit a_s le résidu auquel C^n conduit, de sorte que $C^n \equiv a_s \pmod{p}$, il vient

$$\begin{aligned} C^{n^{t-1}} &\equiv a_{sn^{t-2}} \pmod{p}, \\ C^{2n^{t-1}} &\equiv a_{2sn^{t-2}} \pmod{p}, \\ &\cdots\cdots\cdots\cdots\cdots, \\ C^{(n-1)n^{t-1}} &\equiv a_{(n-1)sn^{t-2}} \pmod{p}. \end{aligned}$$

Si l'on remplace $C^{n^{t-1}}$, $C^{2n^{t-1}}$, ... par leurs valeurs dans les deux relations qui précèdent, on obtient

$$a_{(n-1)sn^{t-2}} + a_{(n-2)sn^{t-2}} + \ldots + a_{sn^{t-2}} + 1 \equiv 0 \pmod{p}, \quad a_{sn^{t-1}} - 1 \equiv 0 \pmod{p}.$$

Considérons l'un quelconque des résidus de la première de ces deux relations, $a_{sn^{t-2}}$ par exemple. Il ne peut être l'unité, car alors cette relation donnerait $n \equiv 0 \pmod{p}$, ce qui est impossible; mais, élevé à la puissance $n^{\text{ième}}$, il conduit au résidu 1, en vertu de $a_{sn^{t-1}} - 1 \equiv 0 \pmod{p}$. $a_{sn^{t-2}}$ est donc nécessairement l'un des résidus de la série $a_{\frac{H}{n}}$, $a_{2\frac{H}{n}}$, ..., $a_{(n-1)\frac{H}{n}}$, a_H; moins le dernier a_H qui est l'unité, on peut donc poser $a_{sn^{t-2}} = a_{\alpha\frac{H}{n}}$, α étant un nombre moindre que n. Deux résidus égaux, formés avec la même base, ont même indice, ou bien a différence de

leurs indices est un multiple de H, il en résulte l'égalité

$$S n^{t-2} = \alpha \frac{H}{n} + H\varepsilon, \quad \text{d'où} \quad S n^{t-1} = (\alpha + n\varepsilon) H;$$

mais $\alpha + n\varepsilon$ est premier avec n^{t-1}, puisque α est moindre que n : donc il faut que H soit divisible par n^{t-1} ; par suite, p est de la forme $H' n^t + 1$.

On a supposé $B = 1$. Soient, plus généralement, $A = C^{n^{t-1}}$, $B = D^{n^{t-1}}$; je pose

$$D^n \equiv C^n R^n \pmod{p},$$

on en déduit

$$D^{n^{t-1}} \equiv C^{n^{t-1}} R^{n^{t-1}} \pmod{p}, \quad \text{d'où} \quad B \equiv AL \pmod{p}$$

en désignant $R^{n^{t-1}}$ par L. Les relations

$$F_n(A, B) \equiv 0 \pmod{p} \quad \text{et} \quad A^n - B^n \equiv 0 \pmod{p}$$

deviennent, en remplaçant B par sa valeur et en supprimant les facteurs A^{n-1}, A^n, qui ne sont pas divisibles par p,

$$F_n(L, 1) \equiv 0 \pmod{p}, \quad L^n - 1 \equiv 0 \pmod{p};$$

on est ainsi ramené au cas précédent. Les diviseurs de $F_n(A, B)$ sont donc de la forme $H' n^t + 1$, quand A et B sont des puissances affectées de l'exposant n^{t-1}, ce qu'il fallait démontrer.

Applications. — Soient $n = 3$, $A = 2^{3^2}$, $B = 1$; on a

$$F_3(3^2, 1) = 2^{18} + 2^9 + 1 = 262657;$$

que ce nombre soit premier ou qu'il ne le soit pas, il doit être de la forme $H' 3^3 + 1$, ce qui a lieu.

Soient $n = 3$, $A = 2^{3^3}$, $B = 1$; on a

$$F_3(2^{3^3}, 1) = 2^{54} + 2^{27} + 1 = 180143986436997 13;$$

ce nombre, premier ou non, doit être de la forme $H' 3^4 + 1$, ce qui a lieu.

DEUXIÈME PARTIE.

Je considère, dans cette seconde Partie, le cas où T a deux facteurs premiers quelconques. Soient $T = n^t m^h$; n, m des nombres premiers; t, h des exposants d'une valeur arbitraire. Je recherche des polynômes dont les diviseurs premiers soient de la forme $H' n^t m^h + 1$.

J'établis d'abord que les deux expressions $\frac{R^{vs} - S^{vs}}{R - S}$, $\frac{R^{us} - S^{us}}{R - S}$, où R, S sont des nombres quelconques premiers entre eux, ont $\frac{R^s - S^s}{R - S}$ pour plus grand commun diviseur, si s est le plus grand commun diviseur des exposants vs, us.

Supposons u et v premiers entre eux, $\frac{R^v - S^v}{R - S}$ $\frac{R^u - S^u}{R - S}$ sont aussi premiers entre eux. En effet, admettons que ces expressions puissent avoir un diviseur commun; soit r l'un quelconque de leurs diviseurs premiers communs, on aura

$$R^v - S^v \equiv 0 \pmod{r}, \quad R^u - S^u \equiv 0 \pmod{r}.$$

Posons $u = v\rho + v'$, il vient, en substituant,

$$R^{v\rho} R^{v'} - S^{v\rho} S^{v'} \equiv 0 \pmod{r}, \quad \text{d'où} \quad R^{v'} - S^{v'} \equiv 0 \pmod{r},$$

en vertu de $R^v - S^v \equiv 0 \pmod{r}$; mais on peut opérer sur

$$R^v - S^v \equiv 0 \pmod{p}, \quad R^{v'} - S^{v'} \equiv 0 \pmod{p}$$

comme sur

$$R^u - S^u \equiv 0 \pmod{r}, \quad R^v - S^v \equiv 0 \pmod{r},$$

et ainsi de suite; u et v étant premiers entre eux, on arrivera nécessairement à un dernier exposant égal à l'unité, d'où

$$R - S \equiv 0 \pmod{r}.$$

On a

$$R^u - S^u = (R - S) F_u(R, S),$$
$$R^v - S^v = (R - S) F_v(R, S);$$

$R - S$ et $F_u(R, S)$ ne peuvent avoir pour diviseurs communs que des

diviseurs de u; de même $R - S$ et $F_v(R, S)$ n'ont pour diviseurs communs que des diviseurs de v. Il en résulte que si r n'est pas diviseur de u, comme il divise $R - S$, il ne pourra diviser $F_u(R, S)$, c'est-à-dire $\frac{R^u - S^u}{R - S}$, ce qui est contraire à la supposition. Il faut donc que r soit diviseur de u; mais, si r est diviseur de u, il ne le sera pas de v qui est premier avec u; divisant $R - S$, il ne pourra donc diviser $F_v(R, S)$, c'est-à-dire $\frac{R^v - S^v}{R - S}$, ce qui est contre la supposition. Ainsi on ne peut admettre que r soit diviseur de u et qu'il ne le soit pas; il n'existe donc pas, $\frac{R^u - S^u}{R - S}$, $\frac{R^v - S^v}{R - S}$ sont donc premiers entre eux.

Reprenons actuellement $\frac{R^{us} - S^{us}}{R - S}$, $\frac{R^{vs} - S^{vs}}{R - S}$; je pose $R^s = K$, $S^s = L$, il vient, en substituant,

$$\frac{K^u - L^u}{R - S} = \frac{K^u - L^u}{K - L} \times \frac{K - L}{R - S}, \quad \frac{K^v - L^v}{R - S} = \frac{K^v - L^v}{K - L} \times \frac{K - L}{R - S}.$$

Comme $\frac{K^u - L^u}{K - L}$ et $\frac{K^v - L^v}{K - L}$ sont premiers entre eux, puisque les exposants u et v sont premiers entre eux, il en résulte que $\frac{K - L}{R - S}$, c'est-à-dire $\frac{R^s - S^s}{R - S}$ est le plus grand commun diviseur de $\frac{R^{us} - S^{us}}{R - S}$ et $\frac{R^{vs} - S^{vs}}{R - S}$.

Cela posé, considérons la fonction $F_n(u^m, v^m)$, où u et v ont pour valeur respectivement $C^{m^{h-1}n^{t-1}}$, $D^{m^{h-1}n^{t-1}}$, C, D désignant des nombres quelconques premiers entre eux; m, n des nombres premiers; h, t des exposants arbitraires. On a les égalités suivantes :

$$u^{mn} - v^{mn} = (u^m - v^m) F_n(u^m, v^m), \quad u^{mn} - v^{mn} = (u^n - v^n) F_m(u^n, v^n).$$

De ces égalités on déduit la suivante, en égalant les seconds membres et en les divisant par $u - v$,

$$\frac{u^m - v^m}{u - v} F_n(u^m, v^m) = \frac{u^n - v^n}{u - v} F_m(u^n, v^n); \tag{1}$$

$\frac{u^m - v^m}{u - v}$ et $\frac{u^n - v^n}{u - v}$ sont premiers entre eux, puisque les exposants m, n

sont premiers entre eux; il en résulte, d'après l'égalité (1), que $F_n(u^m, v^m)$ est divisible par $\frac{u^n - v^n}{u - v}$, c'est-à-dire par $F_n(u, v)$; on peut donc écrire l'égalité suivante, dans laquelle Π représente une quantité entière

$$F_n(u^m, v^m) = F_n(u, v)\Pi. \tag{2}$$

Comme u et v sont des nombres affectés de l'exposant n^{t-1}, il résulte du théorème établi dans la première Partie que les diviseurs premiers de $F_n(u^m, v^m)$ sont de la forme $H'n^t + 1$ et, par suite, qu'il en est de même pour le polynôme Π, facteur du second membre de l'égalité (2).

Je vais démontrer que les diviseurs de Π sont aussi de la forme $H'm^h + 1$.

Je multiplie par $u^m - v^m$ les deux membres de l'égalité (2); elle devient, après avoir remplacé $F_n(u, v)$ par la valeur $\frac{u^n - v^n}{u - v}$,

$$u^{mn} - v^{mn} = (u^n - v^n)\frac{u^m - v^m}{u - v}\Pi;$$

d'où, en remarquant que l'on a

$$u^{mn} - v^{mn} = (u^n - v^n)F_m(u^n, v^n), \qquad \frac{u^m - v^m}{u - v} = F_m(u, v)$$

et en supprimant le facteur commun $u^n - v^n$, on déduit

$$F_m(u^n, v^n) = F_m(u, v)\Pi.$$

Les diviseurs premiers de $F_m(u^n, v^n)$ sont de la forme $H'm^h + 1$; en effet, u et v sont des nombres affectés de l'exposant m^{h-1} : donc les diviseurs de Π, facteur du second membre, sont également de la forme $H'm^h + 1$.

Les diviseurs de Π étant de la forme $H'n^t + 1$, $H'm^h + 1$ sont de la forme $H'm^h n^t + 1$. Π est donc le polynôme que l'on s'est proposé de déterminer. Il a pour valeur l'une ou l'autre des expressions suivantes, en désignant Π par Π_{mn},

$$\Pi_{mn} = \frac{F_m(u^n, v^n)}{F_m(u, v)}, \qquad \Pi_{mn} = \frac{F_n(u^m, v^m)}{F_n(u, v)},$$

puisque u et v sont symétriques par rapport à m^h et n^t.

En vertu de la formule

$$F_n(A, B) = \frac{A^n - B^n}{A - B},$$

ces deux expressions de Π_{mn} peuvent s'écrire comme il suit :

$$\Pi_{mn} = \frac{(u^{mn} - v^{mn})(u - v)}{(u^n - v^n)(u^m - v^m)}.$$

Applications. — Soient $m = 3$, $n = 5$; il vient

$$\Pi_{3,5} = \frac{u^{10} + u^5 v^5 + v^{10}}{u^2 + uv + v^2} = u^8 - u^7 v + u^5 v^3 - u^4 v^4 + u^3 v^5 - uv^7 + v^8.$$

Soient $h = 3$, $t = 1$, $C = 2$, $D = 1$; d'où $u = 2^{3^2}$, $v = 1$, on obtient

$$\Pi_{3,5} = 2^{72} - 2^{63} + 2^{45} - 2^{36} - 2^{27} - 2^9 + 1 = 47131431459485772672 01,$$

que ce nombre soit premier ou non, il doit être de la forme $H' m^h n^t + 1$, c'est-à-dire $H' . 3^3 . 5 + 1$, ce qui a lieu : il est égal à

$$34912171451470942720 \times 3^3 . 5 + 1.$$

TROISIÈME PARTIE.

Je suppose que T contient trois facteurs premiers; soit $T = n^t m^h s^h$.

Je considère la fonction $F_n(u^{ms}, v^{ms})$, dans laquelle $u = C^{n^{t-1} m^{h-1} s^{h-1}}$, $v = D^{n^{t-1} m^{h-1} s^{h-1}}$, et je pose $u^s = R_1$, $v^s = S_1$; $F_n(u^{ms}, v^{ms})$ devient $F_n(R_1^m, S_1^m)$ et la relation (2) donne, si l'on opère sur $F_n(R_1^m, S_1^m)$ comme sur la fonction $F_n(u^m, v^m)$ de la deuxième Partie,

$$F_n(R_1^m S_1^m) = F_n(R_1 S_1) \varphi_{nm}, \tag{3}$$

où φ_{nm} représente une quantité entière dont les diviseurs sont de la forme $H' m^h n^t + 1$.

Je pose $u^m = R_2$, $v^m = S_2$; la fonction $F_n(u^{ms}, v^{ms})$ devient $F_n(R_2^s, S_2^s)$ et l'on a pareillement

$$F_n(R_2^s, S_2^s) = F_n(R_2, S_2) \psi_{ns}, \tag{4}$$

où ψ_{ns} a pour diviseurs des nombres de la forme $H' s^h n^t + 1$. Comme les

premiers membres des égalités (3), (4) sont égaux à $F_n(u^{ms}, v^{ms})$ et, par conséquent, égaux entre eux, les seconds membres sont aussi égaux, et il vient

$$F_n(u^s, v^s)\varphi_{nm} = F_n(u^m, v^m)\psi_{ns}, \tag{5}$$

$$\frac{u^{ns} - v^{ns}}{u^s - v^s}\varphi_{nm} = \frac{u^{mn} - v^{mn}}{u^m - v^m}\psi_{ns}; \tag{6}$$

les expressions $\frac{u^{ns} - v^{ns}}{u - v}$, $\frac{u^{nm} - v^{nm}}{u - v}$ ont $\frac{u^n - v^n}{u - v}$ pour plus grand commun diviseur, puisque n est le plus grand commun diviseur des exposants ns, nm.

Je divise ces deux expressions par leur plus grand commun diviseur, les quotients seront premiers entre eux. Ces deux quotients, divisés respectivement par $\frac{u^s - v^s}{u - v}$, $\frac{u^m - v^m}{u - v}$, seront nécessairement premiers entre eux; ainsi les quantités suivantes seront premières entre elles :

$$\frac{\dfrac{u^{sn} - v^{sn}}{u - v}}{\dfrac{u^n - v^n}{u - v} \times \dfrac{u^s - v^s}{u - v}}, \qquad \frac{\dfrac{u^{mn} - v^{mn}}{u - v}}{\dfrac{u^n - v^n}{u - v} \times \dfrac{u^m - v^m}{u - v}}.$$

Il est facile de reconnaître que ces quantités sont entières; en effet, considérons, par exemple, la première. Le numérateur $\frac{u^{sn} - v^{sn}}{u - v}$ est divisible par chacun des facteurs $\frac{u^n - v^n}{u - v}$, $\frac{u^s - v^s}{u - v}$ du dénominateur, et ces deux facteurs sont premiers entre eux, puisque n et s sont des nombres premiers; le numérateur est donc divisible par leur produit.

Je multiplie les deux membres de l'égalité (6) par $u - v$, je les divise par $u^n - v^n$ et j'obtiens la relation suivante :

$$\frac{(u^{sn} - v^{sn})(u - v)}{(u^n - v^n)(u^s - v^s)}\varphi_{nm} = \frac{(u^{mn} - v^{mn})(u - v)}{(u^n - v^n)(u^m - v^m)}\psi_{ns}. \tag{7}$$

Comme on vient de le voir, le premier facteur du premier membre de l'égalité (7) est premier avec le premier facteur du second membre; φ_{nm} est donc divisible par le premier facteur du second membre, et

l'on est conduit aux égalités suivantes :

$$(8)\qquad \varphi_{nm}=\frac{(u^{mn}-v^{mn})(u-v)}{(u^{t}-v^{n})(u^{m}-v^{m})}\Pi,\quad \psi_{ns}=\frac{(u^{sn}-v^{sn})(u-v)}{(u^{n}-v^{n})(u^{s}-v^{s})}\Pi.$$

Π est une quantité entière dont les diviseurs sont de la forme $H'n^{t}m^{h}+1$, comme ceux de φ_{nm}, et de la forme $H'n^{t}s^{k}+1$, comme ceux de ψ_{ns}; donc ils sont de la forme $H'n^{t}m^{h}s^{k}+1$. Π est donc le polynôme que je m'étais proposé de déterminer : je le désigne par Π_{nms}.

Pour l'obtenir, je remplace dans l'égalité (3) φ_{nm} par sa valeur tirée de l'égalité (8). Il vient, en remplaçant R_1, S_1 par leur valeur u^{s}, v^{s},

$$(9)\qquad \Pi_{nms}=\frac{F_n(u^{ms},v^{ms})\,F_n(u,v)}{F_n(u^{m},v^{m})\,F_n(u^{s},v^{s})},\quad u=C^{nt-1}m^{h-1}s^{k-1},\quad v=D^{nt-1}m^{h-1}s^{k-1}.$$

On peut encore écrire comme il suit le polynôme Π_{nms}, à l'aide de la formule $F_n(A,B)=\dfrac{A^{n}-B^{n}}{A-B}$,

$$(10)\qquad \Pi_{nms}=\frac{(u^{msn}-v^{msn})(u^{m}-v^{m})(u^{s}-v^{s})(u^{n}-v^{n})}{(u^{ms}-v^{ms})(u^{mn}-v^{mn})(u^{sn}-v^{sn})(u-v)}.$$

On voit que les exposants de u et v dans les facteurs qui composent Π_{nms} sont formés des trois nombres m, s, n qui y entrent tous, soit isolément, soit dans toutes leurs combinaisons 2 à 2, 3 à 3.

Applications. — Soient $n=3$, $m=5$, $s=7$, $v=1$, il vient

$$\Pi_{3,5,7}=\frac{u^{70}+u^{35}+1}{u^{6}+u^{7}+1}:\frac{u^{10}+u^{5}+1}{u^{2}+u+1}=\frac{u^{36}-u^{19}+u^{35}-u^{28}+u^{21}-u^{7}+1}{u^{8}-u^{7}+u^{5}-u^{4}+u^{3}-u+1},$$

d'où

$$\begin{aligned}\Pi_{3,5,7}=u^{48}&+u^{47}+u^{46}-u^{43}-u^{42}-2u^{41}-u^{40}-u^{39}+u^{36}+u^{35}+u^{34}\\&+u^{33}+u^{32}+u^{31}-u^{28}-u^{26}-u^{24}-u^{22}-u^{20}+u^{17}+u^{16}\\&+u^{15}+u^{14}+u^{13}+u^{12}-u^{9}-u^{8}-2u^{7}-u^{6}-u^{5}+u^{2}+u+1.\end{aligned}$$

Soient $t=1$, $h=1$, $k=1$, $c=2$, d'où $u=2$, les diviseurs de $\Pi_{3,5,7}$ doivent être de la forme $H'_{3,5,7+1}$; il vient, en effet,

$$\Pi_{3,5,7}=4734746899199\,11,$$
$$\Pi_{3,5,7}=45092827611\,42\times 3\times 5\times 7+1.$$

La composition du polynôme Π_{nms} que l'on vient d'indiquer est

générale ; elle se retrouve, quel que soit le nombre des facteurs de T, dans H'T + 1. La démonstration de cette proposition est analogue aux précédentes, mais elle exige quelques développements.

Soit $T = n^t m^h s^k \dots r^v$, soit $\Pi_{nms\dots r}$ un polynôme dont tous les diviseurs sont de la forme H'T + 1; si l'on pose

$$u = C^{n^{t-1} m^{h-1} s^{k-1} \dots r^{v-1}}, \quad v = D^{n^{t-1} m^{h-1} s^{k-1} \dots r^{v-1}},$$

le polynôme $\Pi_{nms\dots r}$ aura la forme indiquée par l'égalité (10). Les exposants de u et v seront composés des facteurs premiers $n, m, s, \dots, r$ qui y entreront tous soit isolément, soit dans toutes leurs combinaisons 2 à 2, 3 à 3, ..., λ à λ, si λ est le nombre des facteurs $n, m, s, \dots, r$. Il convient de remarquer que ces combinaisons se placent alternativement au numérateur et au dénominateur.

QUATRIÈME PARTIE.

Les polynômes Π, fonctions de u, v, que l'on vient de déterminer, sont indépendants des exposants $t, h, k, \dots$ de $n, m, s, \dots$. Leur calcul reste donc le même quels que soient ces exposants. Il n'y a que u et v qui varient avec eux.

Ces polynômes sont symétriques et homogènes par rapport à u et v; leurs degrés sont respectivement

$$n-1, \ (n-1)(m-1), \ (n-1)(m-1)(s-1), \ \dots,$$

selon que leurs diviseurs sont de la forme $H'n^t + 1$, $H'n^t m^h + 1$, $H'n^t m^h s^k + 1$, ...

Le polynôme Π_{mn}, qui a pour expression $\frac{F_n(u^m, v^m)}{F_n(u, v)}$, peut s'obtenir par une règle assez simple, qui trouve également son emploi dans la recherche des polynômes $\Pi_{nms\dots r}$.

Je suppose le polynôme Π_{mn} ordonné par rapport aux puissances croissantes de v; $(n-1)(m-1)$ est le plus fort exposant de v. Soit $r = (n-1)(m-1)$; Π_{mn} peut s'écrire comme il suit :

$$h_0 u^r + h_1 u^{r-1} v + h_2 u^{r-2} v^2 + \dots + h_{r-1} u v^{r-1} + h_r v^r.$$

Je multiplie ce polynôme par le dénominateur $F_n(u, v)$, je dois retrouver le numérateur $F_n(u^m, v^m)$. On obtient ainsi $r+1$ équations, dont la résolution est facile, en égalant 2 à 2 les coefficients. On peut ainsi déterminer $h_0, h_1, \ldots, h_r$. On arrive à la règle suivante pour obtenir ces coefficients, en supposant que l'on ait pris pour n le plus petit des deux nombres m, n, ce qui est toujours possible.

Les deux premiers coefficients h_0, h_1 sont 1, -1; les $n-2$ suivants sont nuls. Pour les autres, ils satisfont à l'égalité $h_\alpha = h_{\alpha-n}$, il y a exception quand l'indice α de h_α est un multiple de m, ou bien quand il est un multiple de m augmenté de l'unité. On a alors

$$h_{\varepsilon m} = 1 + h_{\varepsilon m - n}, \quad h_{\varepsilon m+1} = -1 + h_{\varepsilon m+1-n}.$$

Il résulte de cette règle que les n premiers coefficients $h_0, h_1, h_2, \ldots$ sont 1, -1, 0, ..., et que les suivants s'en déduisent très facilement. On peut démontrer qu'ils sont tous 1, -1 ou 0.

Les coefficients à égale distance des extrêmes sont égaux et de même signe. Ainsi soit $\gamma u^\lambda v^\mu$ un terme de $\frac{F_n(u^m, v^m)}{F_n(u, v)}$, comme ce polynôme ne change pas de valeur quand on y remplace u par v et réciproquement, il en résulte que $\gamma u^\mu v^\lambda$ est encore l'un de ses termes. Or $\gamma u^\lambda v^\mu$, $\gamma v^\lambda u^\mu$ sont des termes à égale distance des extrêmes : leurs coefficients sont donc égaux.

Application. — Si l'on suppose $n=3, m=5$, d'où $(n-1)(m-1)=8$, l'application de la règle précédente donne

$$h_0 = 1, \quad h_1 = -1, \quad h_2 = 0, \quad h_3 = h_0 = 1, \quad h_4 = h_1 = -1, \quad h_5 = 1 + h_2 = 1,$$
$$h_6 = -1 + h_3 = 0, \quad h_7 = h_4 = -1, \quad h_8 = h_5 = 1;$$

d'où

$$\Pi_{3,5} = \frac{F_3(u^5, v^5)}{F_3(u, v)} = u^8 - u^7 v + u^5 v^3 - u^4 v^4 + u^3 v^5 - u v^7 + v^8,$$

résultat déjà obtenu par le calcul direct de la division.