A. LEFÉBURE

Sur la composition de polynômes entiers, qui n'admettent que des diviseurs premiers d'une forme déterminée (suite)

Annales scientifiques de l'É.N.S. 3e série, tome 2 (1885), p. 113-122

<http://www.numdam.org/item?id=ASENS_1885_3_2__113_0>

MÉMOIRE

SUR LA

COMPOSITION DE POLYNOMES ENTIERS

QUI N'ADMETTENT

QUE DES DIVISEURS PREMIERS D'UNE FORME DÉTERMINÉE

(Suite);

PAR M. A. LEFÉBURE,

DOCTEUR ÈS SCIENCES, INSPECTEUR D'ACADÉMIE HONORAIRE.

CINQUIÈME PARTIE.

Les polynômes $\Pi_{nms\ldots r}$ peuvent être compris dans une formule générale. Soient toujours

$$R = nms\ldots r, \qquad T = n^t m^h s^k \ldots r^\gamma,$$
$$U = C^{n^{t-1} m^{h-1} s^{k-1} \ldots r^{\gamma-1}}, \quad V = D^{n^{t-1} m^{h-1} s^{k-1} \ldots r^{\gamma-1}},$$

λ le nombre des facteurs de R; C, D des nombres quelconques premiers entre eux. Désignons par $P_{\rho,R}(U,V)$ le produit de facteurs représentés par $U^\mu - V^\mu$, dans lesquels μ exprime successivement toutes les combinaisons ρ à ρ des λ facteurs de R. Ainsi l'on a

$$P_{2,nmr}(U,V) = (U^{nm} - V^{nm})(U^{nr} - V^{nr})(U^{mr} - V^{mr}),$$
$$P_{1,nmr}(U,V) = (U^{n} - V^{n})(U^{m} - V^{m})(U^{r} - V^{r}),$$
$$P_{0,nmr}(U,V) = U - V.$$

Les polynômes Π_R sont donnés par la formule suivante :

$$(11) \qquad \Pi_R = \frac{P_{\lambda,R}(U,V)\ldots P_{3,R}(U,V)\,P_{1,R}(U,V)}{P_{(\lambda-1),R}(U,V)\ldots P_{2,R}(U,V)\,P_{0,R}(U,V)}.$$

Les indices λ, λ, 2, ..., 3, 1 des facteurs du numérateur sont de même parité, il en est de même pour le dénominateur. Pour fixer les idées, j'ai supposé λ impair, de sorte que les indices impairs sont au numérateur, et les indices pairs au dénominateur.

Lorsque T est impair dans les diviseurs $H'T+1$ qui composent Π_R, on obtient de nouveaux polynômes dont les diviseurs sont toujours de même forme, si l'on change V en $-V$ dans la formule (11).

La démonstration de cette proposition est analogue à celle qui a conduit à cette formule. Elle présente seulement quelques modifications dans le cas où T ne contient qu'un seul facteur n^t; cas qui a été l'objet de la première Partie de ce Mémoire. Je vais m'y arrêter.

On a démontré, dans cette première Partie, que les diviseurs premiers de la fonction $F_n(U,V)$, c'est-à-dire de

$$U^{n-1}+U^{n-2}V+\ldots+UV^{n-2}+V^{n-1},$$

dans laquelle $U=C^{n^{t-1}}$, $V=D^{n^{t-1}}$, sont de la forme $H'n^t+1$. Je me propose d'établir que le polynôme $U^{n-1}-U^{n-2}V+\ldots-UV^{n-2}+V^{n-1}$, que je représente par $F_n(U,-V)$, a pour diviseurs premiers des nombres de même forme $H'n^t+1$.

Je suppose $D=1$, d'où $V=1$; le cas général, où D aurait toute autre valeur, s'en déduirait, comme on l'a vu dans la première Partie.

Soit p un diviseur premier quelconque de $F_n(U,-V)$, il est de la forme $Hn+1$; je démontre d'abord que H est un multiple de n. En effet, on a

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

Cette dernière relation s'obtient en multipliant $F_n(U,-1)$ par $U+1$. U est une puissance $n^{\text{ième}}$; soit a_m le résidu de U divisé par p, a désignant la base des résidus, on a

$$U\equiv a_m \pmod{p},\quad a_{mn}=p-1.$$

Cette valeur du résidu a_{mn} se déduit de la relation $U^n+1\equiv 0 \pmod{p}$. a_m ne peut être le résidu négatif -1, ou, en d'autres termes, $p-1$, car $F_n(U,-1)\equiv 0 \pmod{p}$ donnerait $n\equiv 0 \pmod{p}$, ce qui est impossible. Ainsi l'on ne peut avoir $m=\frac{H}{2}$; a_m ne peut être l'unité, car, en l'élevant à la puissance $n^{\text{ième}}$, le résidu a_{mn}, que l'on obtiendrait, serait encore l'unité, et l'on a vu que ce résidu est $p-1$. On n'a donc pas $m=\mathrm{H}$.

Désignons par r et s deux nombres de même parité, pairs par exemple, et dont la différence soit 2; a_{ms}, a_{mr} sont des résidus différents. En effet, s'ils sont égaux, il faut que leurs indices soient égaux, ou que la différence de ces indices soit un multiple de H. Les indices ms, mr ne sont pas égaux, puisque s et r sont des nombres différents. Il faut donc que

$$ms-mr=\varepsilon\mathrm{H},\quad m(s-r)=\varepsilon\mathrm{H},\quad 2m=\varepsilon\mathrm{H}.$$

Comme m est moindre que H, il faut que 2 soit plus grand que ε, d'où $\varepsilon=1$, $m=\frac{\mathrm{H}}{2}$, ce qui n'a pas lieu, comme on l'a vu. Ainsi a_{ms}, a_{mr} sont des résidus différents. De plus, élevés à la puissance $n^{\text{ième}}$, ils donnent deux résidus a_{msn}, a_{mrn} égaux, égaux à l'unité, puisque r et s sont pairs, et en vertu de $a_{mn}=p-1$. On est donc dans le premier des deux cas dont il est fait mention dans la première Partie; donc H est divisible par n et p est de la forme $\mathrm{H}'n^2+1$.

Nous nous sommes appuyé sur ce que l'indice du résidu négatif -1 est $\frac{\mathrm{H}}{2}$. En effet, si dans les $\frac{\mathrm{H}}{r}$ groupes de r résidus, qui comprennent tous les résidus des puissances $n^{\text{ièmes}}$ des nombres divisés par p dont il est fait mention dans la première Partie du Mémoire, on fait $r=2$, ces groupes deviennent

$$a_1+a_{1+\frac{\mathrm{H}}{2}}=p,\quad a_2+a_{2+\frac{\mathrm{H}}{2}}=p,\quad \ldots,\quad a_{\frac{\mathrm{H}}{2}}+a_{\mathrm{H}}=p.$$

Il en résulte que les indices de deux résidus égaux et de signes contraires ont toujours $\frac{\mathrm{H}}{2}$ ou un multiple de $\frac{\mathrm{H}}{2}$ pour différence. Comme a_{H} représente le résidu 1, $a_{\frac{\mathrm{H}}{2}}$ est donc le résidu négatif -1 ou, en d'autres termes, $p-1$.

Je remplace U par sa valeur $\mathrm{C}^{n^{t-1}}$ dans $\mathrm{F}_n(\mathrm{U},-1)$ et dans U^n+1, il vient

$$\mathrm{F}_n(\mathrm{C}^{n^{t-1}},-1)\equiv 0 \pmod{p},\quad \mathrm{C}^{n^t}+1\equiv 0 \pmod{p}.$$

Je désigne par a_s le résidu déterminé par C^n, de sorte que l'on a

$$\mathrm{C}^n\equiv a_s \pmod{p},\quad \mathrm{C}^{n^{t-1}}\equiv a_{sn^{t-2}} \pmod{p},\quad \mathrm{C}^{n^t}\equiv a_{sn^{t-1}} \pmod{p},\quad a_{sn^{t-1}}\equiv -1.$$

La dernière relation se déduit de $C^{n^t}+1\equiv 0 \pmod{p}$. Le résidu $a_{sn^{t-2}}$ ne peut être le résidu négatif -1, car, s'il était -1, la relation

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

donnerait

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

ce qui est impossible. Mais, si on l'élève à la puissance $n^{\text{ième}}$, il conduit au résidu -1, en vertu des $a_{sn^{t-1}}=-1$. Donc $a_{sn^{t-2}}$ est l'un des résidus de la série

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

Cette série fait partie des $\frac{H}{r}$ séries mentionnées à la première Partie, qui comprennent tous les résidus, et dans lesquels on fait $r=n$. C'est celle dont les termes, élevés à la puissance $n^{\text{ième}}$, donnent le résidu -1. En effet, on a

$$\left(a_{\frac{H}{2n}+\alpha\frac{H}{n}}\right)^n\equiv a_{\frac{H}{2}+\alpha H} \pmod{p},\quad a_{\frac{H}{2}+\alpha H}=-1.$$

Il résulte de ce qui précède que l'on doit avoir

$$a_{sn^{t-2}}=a_{\frac{H}{2n}+\alpha\frac{H}{n}},\quad s_{n^{t-2}}=\frac{H}{2n}+\frac{\alpha H}{n}+\varepsilon H,\quad 2sn^{t-1}=H(1+2\alpha+2\varepsilon n).$$

En désignant par α un nombre qui ne peut dépasser $n-1$; $1+2\alpha$ ne peut être divisible par n, car la plus grande valeur de α étant $n-1$, celle de $1+2\alpha$ est $2n-1$. Donc, si $1+2\alpha$ était divisible par n, on aurait

$$1+2\alpha=n$$

et, par suite, il viendrait

$$a_{sn^{t-2}}=a_{\frac{H}{2}},\quad a_{sn^{t-2}}=-1,$$

égalités qui n'ont pas lieu, car on a établi précédemment que $a_{sn^{t-2}}$ ne peut être le résidu -1. Ainsi $1+2\alpha$ n'est pas divisible par n : il résulte donc de l'égalité $2sn^{t-1}=H(1+2\alpha+2\varepsilon n)$ que H est divisible par n^{t-1}, et, par suite, que p est de la forme $H'n^t+1$, ce qu'il fallait démontrer.

Nous avons supposé, dans ce qui précède, T impair, et nous venons de voir qu'en changeant V en $-V$ dans la formule (11), on obtient encore des polynômes dont les diviseurs sont de la forme $H'T+1$.

Quand T est pair, la formule (11) donne aussi des polynômes dont les diviseurs sont de la forme $H'T+1$, mais en y introduisant une modification; R dans cette formule ne devra pas comprendre le facteur 2. Posons

$$R = 2R_1, \quad R_1 = ms\ldots r,$$

les nouveaux polynômes seront donnés par la formule suivante :

$$(12)\qquad \left\{\begin{aligned} &\Pi_R = \frac{P_{(\lambda-1),R_1}(U,-V)\ldots P_{2,R_1}(U,-V)\,P_{0,R_1}(U,-V)}{P_{(\lambda-2),R_1}(U,-V)\ldots P_{1,R_1}(U,-V)},\\ &U = C^{2^{t-1}m^{h-1}s^{k-1}\ldots r^{\gamma-1}}, \quad V = D^{2^{t-1}m^{h-1}s^{k-1}\ldots r^{\gamma-1}}.\end{aligned}\right.$$

En effet, comme R_1 est impair, il résulte de ce qui précède que le second membre de la relation (12), et par conséquent Π_R, a pour diviseurs des nombres de la forme $H'm^h s^k\ldots r^\gamma+1$. Il reste à établir qu'ils sont aussi de la forme $H'.2^t+1$: ils seront alors de la forme $H'.2^t m^h s^k\ldots r^\gamma+1$, $H'T+1$.

De la relation (12) on déduit l'égalité

$$U^{R_1}+V^{R_1} = L\Pi_R,$$

en appelant L le multiplicateur de Π_R, et en remarquant que

$$P_{(\lambda-1),R_1}(U,-V)$$

est égal à

$$U^{R_1}+V^{R_1}.$$

L est un polynôme entier, comme on le reconnaitra plus loin.

Je pose

$$C^{m^h s^k\ldots r^\gamma} = C_1, \quad D^{m^h s^k\ldots r^\gamma} = D_1, \quad \text{d'où} \quad U^{R_1} = C_1^{2^{t-1}}, \quad V^{R_1} = D_1^{2^{t-1}},$$

on en déduit

$$C_1^{2^{t-1}}+D_1^{2^{t-1}} = L\Pi_R;$$

$C_1^{2^{t-1}}+D_1^{2^{t-1}}$ est la fonction $F_n(C_1^{n^{t-1}}, D_1^{n^{t-1}})$ dans laquelle on a $n=2$; on a vu dans la première Partie que les diviseurs de cette fonction sont de la forme $H'n^t+1$: donc les diviseurs de $C_1^{2^{t-1}}+D_1^{2^{t-1}}$ sont de la forme $H'.2^t+1$. Comme la démonstration qui a été donnée se modifie pour le cas particulier de n égal à 2, je vais entrer dans quelques détails à ce sujet.

Je suppose $D_1 = 1$: le cas où D_1 aurait une valeur quelconque s'en déduit.

Soit p un diviseur quelconque de $C_1^{2^{t-1}}+1$; il est de la forme $H.2+1$, comme tous les nombres premiers impairs, et ici je ne m'occupe pas du diviseur 2. On a

$$C_1^{2^{t-1}}+1 \equiv 0 \pmod{p}.$$

H est divisible par 2; en effet, soit a_u le résidu du carré $C_1^{2^{t-1}}$, obtenu en divisant ce carré par p, on a

$$a_u + 1 \equiv 0 \pmod{p}.$$

En vertu de $C_1^{2^{t-1}}+1 \equiv 0 \pmod{p}$, a_u est donc le résidu négatif -1. On a vu, dans la première Partie, comment les $p-1$ premiers nombres $1, 2, \ldots, (p-1)$ se groupent en H séries de n nombres chacune, et telles que les puissances $n^{\text{ièmes}}$ des n nombres d'une même série donnent lieu à un même résidu. Ici, pour $n=2$, chaque série est composée de deux nombres dont la somme est p, et ces deux nombres sont nécessairement situés à égale distance des extrêmes de la suite $1, 2, \ldots, (p-1)$. L'une de ces séries est donc $1+(p-1)=p$. Elle est formée de deux résidus, puisque l'unité est toujours résidu, et $(p-1)$ est le résidu a_u. Comme les deux termes de cette série sont résidus, il en résulte que H est divisible par 2, et, par suite, que p est de la forme $H'.2^2+1$.

Soit actuellement a_s le résidu que l'on obtient en divisant C_1^2 par p; on en déduit

$$C_1^2 \equiv a_s \pmod{p}, \quad C_1^{2^{t-1}} \equiv a_{s.2^{t-2}} \pmod{p}, \quad a_{s.2^{t-2}} \equiv -1 \pmod{p}.$$

Cette dernière relation s'obtient en vertu de $C_1^{2^{t-1}}+1 \equiv 0 \pmod{p}$; $a_{s.2^{t-2}}$ est donc le résidu négatif -1, qui a pour expression $a_{\frac{H}{2}}$. On a donc les inégalités suivantes :

$$a_{s.2^{t-2}} = a_{\frac{H}{2}}, \quad s.2^{t-2} = \frac{H}{2} + \varepsilon H, \quad s.2^{t-1} = H(1+2\varepsilon).$$

Comme $1+2\varepsilon$ est impair, il résulte de ces égalités que H est divisible par 2^{t-1}, et par suite que p est de la forme $H'.2^t+1$.

Ainsi les diviseurs de $C_1^{2^{t-1}}+D_1^{2^{t-1}}$ sont de la forme $H'.2^t+1$; il en est donc de même pour ceux de Π_R, en vertu de la relation $C_1^{2^{t-1}}+D_1^{2^{t-1}}=L\Pi_R$ indiquée plus haut. Les diviseurs de Π_R dans la relation (12) sont donc de la forme $H'T+1$, ce qu'il fallait établir.

SIXIÈME PARTIE.

Je me propose de rechercher la composition des polynômes de la forme U^R-V^R, dans lesquels on a

$$U=C^{n^{t-1}m^{h-1}s^{k-1}\ldots r^{\gamma-1}},\quad V=D^{n^{t-1}m^{h-1}s^{k-1}\ldots r^{\gamma-1}},\quad R=nms\ldots r.$$

Désignons par λ le nombre des facteurs de R; l'égalité (11) donne, en vertu de $P_{\lambda,R}(U,V)=U^R-V^R$,

$$U^R-V^R=\frac{P_{(\lambda-1),R}(U,V)\ldots P_{2,R}(U,V)\,P_{0,R}(U,V)}{P_{(\lambda-2),R}(U,V)\ldots P_{1,R}(U,V)}\,\Pi_R. \tag{13}$$

Si l'on considère les cas de $\lambda=2$, $R=nm$; $\lambda=3$, $R=nmr$, on a

$$\begin{aligned}U^{nm}-V^{nm}&=\frac{P_{1,nm}(U,V)}{P_{0,nm}(U,V)}\,\Pi_{nm},\\ P_{1,nm}(U,V)&=(U^n-V^n)(U^m-V^m),\\ P_{0,nm}(U,V)&=U-V;\end{aligned}$$

d'où l'on déduit

$$U^{nm}-V^{nm}=\frac{(U^n-V^n)(U^m-V^m)}{U-V}\,\Pi_{nm},\quad U^{nm}-V^{nm}=(U-V)\,\Pi_n\Pi_m\Pi_{nm}.$$

On a également

$$\begin{aligned}U^{nmr}-V^{nmr}&=\frac{P_{2,nmr}(U,V)\,P_{0,nmr}(U,V)}{P_{1,nmr}(U,V)}\,\Pi_{nmr},\\ P_{0,nmr}(U,V)&=U-V,\\ P_{1,nmr}(U,V)&=(U-V)^3\Pi_n\Pi_m\Pi_r,\\ P_{2,nmr}(U,V)&=(U-V)^3\Pi_n^2\Pi_m^2\Pi_r^2\Pi_{nm}\Pi_{nr}\Pi_{mr},\end{aligned}$$

ce qui conduit à

$$U^{nmr}-V^{nmr}=(U-V)\,\Pi_n\Pi_m\Pi_r\Pi_{nm}\Pi_{nr}\Pi_{mr}\Pi_{nmr}.$$

Représentons d'une manière générale par $P_{\mu,R}\Pi$ le produit de facteurs de la forme Π_ρ, où l'indice ρ exprime successivement toutes les combinaisons μ à μ des facteurs $nms\ldots r$ de R. On a ainsi, par exemple,

$$P_{1,nmr}\Pi = \Pi_n \Pi_m \Pi_r, \quad P_{2,nmr}\Pi = \Pi_{nm}\Pi_{nr}\Pi_{mr};$$

en adoptant cette notation, la valeur de $U^{nmr} - V^{nmr}$ peut s'écrire comme il suit :

$$U^{nmr} - V^{nmr} = (U - V)(P_{1,nmr}\Pi)(P_{2,nmr}\Pi)(P_{3,nmr}\Pi).$$

La forme de ce développement du polynôme $U^R - V^R$, où R contient trois facteurs, se retrouve quel que soit le nombre des facteurs de R : c'est ce que je vais établir.

Soit $R = nms\ldots r$; λ le nombre des facteurs de R. Je suppose qu'il ait été démontré que cette forme de développement s'applique à toute expression, telle que $U^\mu - V^\mu$, où le nombre des facteurs de μ serait moindre que λ; je démontre que $U^R - V^R$, où le nombre des facteurs de R est λ, se compose de la même manière. Alors, comme la proposition est vraie quand le nombre des facteurs de μ est 1, 2, 3, elle sera encore vraie pour quatre facteurs, pour cinq facteurs, et ainsi de suite.

Pour obtenir les égalités qui suivent, je fais usage des nombres de combinaisons que donnent successivement λ, $\lambda - 1$, $\lambda - 2$, ... lettres, prises 2 à 2, 3 à 3, ... Je désigne par $1, \lambda, \lambda_1, \lambda_2, \ldots, \lambda_2, \lambda_1, \lambda, 1$ les coefficients du binôme $(\alpha + \beta)^\lambda$; pareillement par $1, a, a_1, \ldots, a_1, a, 1$; par $1, b, b_1, \ldots, b_1, b, 1$; par $1, c, c_1, \ldots, c_1, c, 1, \ldots$, ceux des binômes $(\alpha + \beta)^a$, $(\alpha + \beta)^b$, $(\alpha + \beta)^c$, ... Pour fixer les idées, je suppose λ impair. On est conduit aux égalités suivantes :

$$\left\{\begin{array}{l}
P_{0,R}(U,V) = (U - V)^1, \\
P_{1,R}(U,V) = (U - V)^\lambda (P_{1,R}\Pi)^1, \\
P_{2,R}(U,V) = (U - V)^{\lambda_1} (P_{1,R}\Pi)^a (P_{2,R}\Pi)^1, \\
P_{3,R}(U,V) = (U - V)^{\lambda_2} (P_{1,R}\Pi)^{a_1} (P_{2,R}\Pi)^b (P_{3,R}\Pi)^1, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
P_{(\lambda-3),R}(U,V) = (U - V)^{\lambda_2} (P_{1,R}\Pi)^{a_2} (P_{2,R}\Pi)^{b_2} (P_{3,R}\Pi)^{c_2}, \\
P_{(\lambda-2),R}(U,V) = (U - V)^{\lambda_1} (P_{1,R}\Pi)^{a_1} (P_{2,R}\Pi)^{b_1} (P_{3,R}\Pi)^{c_1} \ldots (P_{(\lambda-2),R}\Pi)^1, \\
P_{(\lambda-1),R}(U,V) = (U - V)^\lambda (P_{1,R}\Pi)^a (P_{2,R}\Pi)^b (P_{3,R}\Pi)^c \ldots (P_{(\lambda-2),R}\Pi)^2 (P_{(\lambda-1),R}\Pi)^1.
\end{array}\right.$$

La suite des exposants de U — V est formée de coefficients du binôme $(\alpha+\beta)^\lambda$, si l'on excepte le dernier coefficient qui est l'unité. Pareillement l'ensemble des exposants de $P_{1,R}\Pi$, $P_{2,R}\Pi$, $P_{3,R}\Pi$, ... représente respectivement les coefficients des binômes $(\alpha+\beta)^a$, $(\alpha+\beta)^b$, $(\alpha+\beta)^c$, . . ., moins les derniers coefficients. Si je remplace, dans l'expression du polynôme $U^R - V^R$ donné par l'égalité (13), $P_{0,R}(U,V)$, $P_{1,R}(U,V)$, ... par leurs valeurs déduites des égalités (14), on reconnaît que, dans le développement de $U^R - V^R$ ainsi obtenu, $U-V$, $P_{1,R}\Pi$, $P_{2,R}\Pi$, $P_{3,R}\Pi$, ... ont respectivement pour exposants

$$\lambda - \lambda_1 + \lambda_2 \ldots \lambda_1 - \lambda + 1,\quad a - a_1 + a_2 + \ldots + a - 1,$$
$$b - b_1 + b_2 - \ldots - b + 1,\quad c - c_1 + c_2 + \ldots + c - 1,\quad \ldots$$

Dans les différents binômes $(\alpha-\beta)^\lambda$, $(\alpha-\beta)^a$, $(\alpha-\beta)^b$, $(\alpha-\beta)^c$, ... je fais $\alpha=\beta=1$; ces binômes deviennent nuls et conduisent aux égalités suivantes, en remarquant que λ, b, ... sont impairs, et que a, c, ... sont pairs :

$$1 = \lambda - \lambda_1 + \lambda_2 - \ldots - \lambda + 1,\quad 1 = a - a_1 + \ldots + a - 1,$$
$$1 = b - b_1 - \ldots - b + 1,\qquad 1 = c - c_1 + \ldots + c - 1,\quad \ldots;$$

les seconds membres sont les exposants de $U-V$, $P_{1,R}\Pi$, $P_{2,R}\Pi$, ... Donc ces exposants sont l'unité, et l'on obtient ainsi

$$U^R - V^R = (U-V)(P_{1,R}\Pi)(P_{2,R}\Pi)\ldots(P_{(\lambda-1),R}\Pi)(P_{\lambda,R}\Pi). \tag{15}$$

Telle est la forme générale du développement de $U^R - V^R$.

Dans ce développement, les diviseurs de $P_{1,R}\Pi$, $P_{2,R}\Pi$. . ., $P_{\lambda,R}\Pi$ sont respectivement, comme il a été dit, de la forme

$$\Pi' n^t + 1,\ \Pi' m^h + 1,\ \ldots;\ \Pi' n^t m^h + 1,\ \Pi' n^t s^k + 1,\ \ldots;$$
$$\Pi' n^t m^h s^k \ldots r^q + 1,\ \Pi' T + 1.$$

L'égalité (13) donne un développement analogue du polynôme $U^R + V^R$, quand R est impair : il suffit d'y remplacer V par $-V$. Les mêmes raisonnements y conduisent. Ces raisonnements s'appliquent également à la relation (12), où R_1 est impair. Dans l'égalité $U^{R_1} + V^{R_1} = L\Pi_R$ qui s'en déduit, $L\Pi_R$ présente une composition pareille.

SEPTIÈME PARTIE.

La suite des nombres premiers de la forme $H'T+1$ est illimitée, quel que soit le nombre entier que T représente.

Cette proposition a été déjà démontrée par M. Genocchi d'une manière différente.

Si T est impair, il résulte des théorèmes exposés dans ce Mémoire que les polynômes $U^R - V^R$, $U^R + V^R$ ont tous deux, parmi leurs diviseurs, des diviseurs de la forme $H'T+1$.

Supposons T pair, les polynômes $U^R - V^R$, $U^{R_1} + V^{R_1}$ ont aussi nécessairement des diviseurs de la forme $H'T+1$; $U^{R_1} + V^{R_1}$ est donné par la formule (12) qui a conduit à $U^{R_1} + V^{R_1} = L\Pi_R$. Dans cette formule, C et D sont quelconques, pourvu qu'ils soient premiers. Je puis donc y remplacer C et D par C^2 et D^2, et, par suite, U et V par U^2 et V^2; la relation $U^{R_1} + V^{R_1} = L\Pi_R$ prendra la forme $U^R + V^R = L'\Pi'_R$, puisque $R = 2R_1$. Ainsi, si T est pair, les deux polynômes $U^R - V^R$, $U^R + V^R$ ont encore des diviseurs de la forme $H'T+1$.

Cela posé, considérons les polynômes $U^R - V^R$, $U^R + V^R$, dans lesquels R est pair ou impair; ils ne peuvent avoir que 2 pour facteur commun; en effet, leur somme $2U^R$ et leur différence $2V^R$ n'ont que 2 pour diviseur commun, puisque U et V sont premiers entre eux. Donc les diviseurs premiers de la forme $H'T+1$ de $U^R - V^R$ et $U^R + V^R$ sont différents entre eux. Il en résulte que le produit $(U^R - V^R)(U^R + V^R)$ ou, en d'autres termes, $(U^2)^R - (V^2)^R$, contient au moins deux diviseurs de la forme $H'T+1$.

Les deux polynômes $(U^2)^R - (V^2)^R$, $(U^2)^R + (V^2)^R$ ont, comme les précédents, des diviseurs de la forme $H'T+1$, puisque, d'après les explications qui précèdent, C et D peuvent être remplacés par C^2, D^2 dans $U^R + V^R$, sans altérer la forme de ses diviseurs. Le produit $[(U^2)^R - (V^2)^R][(U^2)^R + (V^2)^R]$, c'est-à-dire $(U^{2^2})^R - (V^{2^2})^R$ a donc au moins trois diviseurs de la forme $H'T+1$, et ainsi de suite. Plus α, dans l'expression $(U^{2^\alpha})^R - (V^{2^\alpha})^R$, augmentera, plus le nombre de ses diviseurs de la forme $H'T+1$ sera considérable, et, comme rien ne limite α, la suite des nombres $H'T+1$ est aussi sans limites.