Il s'ensuit de là que si Aa est la somme de quatre carrés, Aa' sera aussi la somme de quatre carrés, a' étant plus petit que $\frac{b}{2}+\frac{1}{b}$ et $a=b\rho$; ainsi si a est plus grand que 1, a' sera nécessairement plus petit que a; et, si a' est encore plus grand que 1, on prouvera de la même manière que Aa'' sera aussi la somme de quatre carrés, a'' étant plus petit que a'; et ainsi de suite; donc comme les nombres a, a', a'',... sont des nombres entiers, dont aucun ne peut être égal à zéro (à cause que ces nombres sont des diviseurs des nombres $1+\alpha^2+\beta^2$, $1+\alpha'^2+\beta'^2$,... qui, comme on voit, ne peuvent jamais devenir nuls), et que ces nombres vont en diminuant, il est clair qu'on parviendra nécessairement à un de ces nombres qui sera égal à l'unité, et alors on aura A égal à la somme de quatre carrés entiers.

COROLLAIRE. — *Si un nombre premier quelconque est un diviseur de la somme de quatre carrés qui n'aient point de commun diviseur, ce nombre sera aussi la somme de quatre carrés.*

Car nommant, comme ci-dessus, A le nombre premier donné et $p^2+q^2+r^2+s^2$ le nombre composé de quatre carrés qui est divisible par A, il est clair que, si chacune des racines p, q, r, s était moindre que $\frac{A}{2}$, on aurait

$$p^2+q^2+r^2+s^2<4\left(\frac{A}{2}\right)^2<A^2;$$

de sorte que A serait plus grand que $\sqrt{p^2+q^2+r^2+s^2}$ comme on l'a supposé dans le Théorème précédent; donc, etc.

Or je dis que quels que soient les nombres p, q,..., on peut toujours les réduire à être moindres que $\frac{A}{2}$; car soit, par exemple, $p>\frac{A}{2}$, il est visible que si $p^2+q^2+r^2+s^2$ est divisible par A, $(p-mA)^2+q^2+r^2+s^2$ le sera aussi, de même que $(mA-p)^2+q^2+r^2+s^2$, quel que soit le nombre m; or on peut toujours prendre m tel que $p-mA$ ou $mA-p$ soit moindre que $\frac{A}{2}$; donc il n'y aura qu'à mettre au lieu de p le nombre

$p - m\mathrm{A}$ ou $m\mathrm{A} - p$; et l'on fera la même chose par rapport aux autres nombres s'ils se trouvent plus grands que $\frac{\mathrm{A}}{2}$.

Si p était divisible par A on aurait

$$p - m\mathrm{A} = 0;$$

de sorte que dans ce cas il faudrait mettre 0 à la place de p; il en serait de même à l'égard de q s'il était aussi divisible par A, et ainsi des autres; mais comme on suppose que p, q, r et s n'ont aucun diviseur commun, ils ne peuvent pas être tous divisibles à la fois par A, et même il ne pourra pas y en avoir plus de deux qui le soient; autrement il faudrait que tous quatre le fussent; de sorte qu'il n'y a pas à craindre que, par ces réductions, le dividende $p^2 + q^2 + r^2 + s^2$ devienne nul.

Remarque. — Au reste il est clair que la démonstration du Théorème précédent n'en subsistera pas moins si l'on suppose qu'un ou deux des quatre carrés qui composent le dividende soient nuls; d'ailleurs il peut aussi arriver qu'un ou deux des quatre carrés qu'on trouvera pour le diviseur A soient nuls; donc, en général, *tout nombre premier qui divisera la somme de quatre ou d'un moindre nombre de carrés entiers, pourvu qu'ils n'aient entre eux aucun diviseur commun, sera nécessairement égal à la somme de quatre ou d'un moindre nombre de carrés entiers.*

Théorème II.

Si A *est un nombre premier et que* B *et* C *soient des nombres quelconques positifs ou négatifs non divisibles par* A, *je dis qu'on pourra toujours trouver deux nombres p et q tels que le nombre* $p^2 - \mathrm{B}q^2 - \mathrm{C}$ *soit divisible par* A.

Car : 1° Si l'on peut trouver un nombre q tel que $\mathrm{B}q^2 + \mathrm{C}$ soit divisible par A, il n'y aura alors qu'à prendre p divisible par A, ou bien $p = 0$;

2° S'il n'y a aucun nombre qui étant pris pour q puisse rendre $\mathrm{B}q^2 + \mathrm{C}$ divisible par A, faisons, pour abréger, $\mathrm{B}q^2 + \mathrm{C} = b$, et supposant

$$\mathrm{P} = p^{\mathrm{A}-3} + bp^{\mathrm{A}-5} + b^2 p^{\mathrm{A}-7} + \ldots + b^{\frac{\mathrm{A}-3}{2}},$$

on aura

$$(p^2 - Bq^2 - C)P = p^{A-1} - b^{\frac{A-1}{2}} = p^{A-1} - 1 - \left(b^{\frac{A-1}{2}} - 1\right);$$

multiplions cette équation par $b^{\frac{A-1}{2}} + 1$ que nous supposerons égal à Q, et l'on aura

$$(p^2 - Bq^2 - C)PQ = Q(p^{A-1} - 1) - (b^{A-1} - 1).$$

Or, par le Théorème connu de Fermat, que M. Euler a démontré dans les *Commentaires de Pétersbourg*, on sait que si A est un nombre premier quelconque et a un autre nombre quelconque non divisible par A, $a^{A-1} - 1$ sera toujours divisible par A. Donc, si l'on suppose que p ne soit pas divisible par A, on aura les deux nombres $p^{A-1} - 1$ et $b^{A-1} - 1$ divisibles à la fois par A, à cause que b n'est jamais divisible par A, quel que soit q (hypothèse). Donc le nombre $(p^2 - Bq^2 - C)PQ$ sera divisible par A, de sorte que, si ni P ni Q n'étaient divisibles par A, il faudrait que $p^2 - Bq^2 - C$ le fût, à cause que A est un nombre premier par l'hypothèse. Ainsi la difficulté se réduit à prouver que l'on peut toujours prendre p et q tels que ni P ni Q ne soient pas divisibles par A, p ne l'étant pas non plus.

Pour cela je remarque d'abord que, quelle que soit la valeur de q, on peut toujours trouver une valeur de p plus petite que A et par conséquent non divisible par A, telle que P ne soit pas divisible par A. Car si l'on substitue successivement dans l'expression de P les nombres 1, 2, 3,... jusqu'à A − 2 inclusivement à la place de p, et qu'on nomme P′, P″, P‴,..., $P^{(A-2)}$ les valeurs résultantes de P, on aura, par la théorie connue des différences,

$$P' - (A-3)P'' + \frac{(A-3)(A-4)}{2}P''' - \ldots + P^{(A-2)} = 1.2.3.4\ldots(A-3).$$

Or, si tous les nombres P′, P″, P‴,... jusqu'à $P^{(A-2)}$ étaient divisibles par A, il faudrait que le nombre $1.2.3\ldots(A-3)$ le fût aussi; ce qui ne pouvant être à cause que A est premier, il s'ensuit que parmi les nombres P′, P″,..., $P^{(A-2)}$ il s'en trouvera nécessairement quelqu'un qui ne sera pas divisible par A; donc, etc.

Ainsi il ne reste plus qu'à prouver que l'on peut toujours prendre q tel que Q ou $(Bq^2+C)^{\frac{A-1}{2}}+1$ ne soit pas divisible par A.

Soit, pour plus de simplicité, $\frac{A-1}{2}=m$, et l'on aura

$$Q=B^m q^{A-1}+mB^{m-1}q^{A-3}C+\frac{m(m-1)}{2}B^{m-2}q^{A-5}C^2+\ldots+mBq^2C^{m-1}+C^m+1.$$

Or si C^m+1 n'est pas divisible par A, il est clair qu'il n'y aura qu'à prendre q divisible par A, ou bien $q=0$; car alors Q ne sera pas divisible par A.

Mais si C^m+1 est divisible par A, alors pour que Q ne le soit pas, il faudra que q ne le soit pas, et que la quantité

$$B^m q^{A-3}+mB^{m-1}q^{A-5}C+\frac{m(m-1)}{2}B^{m-2}q^{A-7}C^2+\ldots+mBC^{m-1}$$

ne le soit pas non plus; or on peut démontrer, comme plus haut, qu'il doit nécessairement exister une valeur de q plus petite que A et par conséquent non divisible par A, telle que la quantité dont il s'agit ne le soit pas. Car nommant R cette quantité, et désignant par R′, R″, R‴,..., $R^{(A-2)}$ les valeurs de R qui résulteraient de la substitution des nombres 1, 2, 3,..., A − 2 à la place de q, on aura

$$R'-(A-3)R''+\frac{(A-3)(A-4)}{2}R'''-\ldots+R^{(A-2)}=1.2.3\ldots(A-3)B^m.$$

Or comme A est premier et que B n'est pas divisible par A, il est clair que le nombre $1.2.3\ldots(A-3)B^m$ ne le sera pas non plus; donc, etc.

Corollaire I. — Si l'on fait $B=-1$ et $C=-1$, on aura le nombre p^2+q^2+1 qui sera divisible par A; d'où il s'ensuit qu'*étant donné un nombre premier quelconque on peut toujours trouver un nombre égal à la somme de trois carrés entiers dont l'un soit même l'unité, lequel soit divisible par le nombre premier donné.*

Ce Théorème a déjà été démontré par M. Euler d'une autre manière, dans le tome V des *Nouveaux Commentaires de Pétersbourg;* mais pour

ne rien laisser à désirer à nos lecteurs nous avons cru devoir le démontrer de nouveau, d'autant plus que notre démonstration a l'avantage d'avoir une très-grande généralité.

COROLLAIRE II. — Combinant donc le Théorème précédent avec celui de la Remarque qui est après le Théorème I, on en déduira celle-ci : que *tout nombre premier est nécessairement égal à la somme de quatre ou d'un moindre nombre de carrés entiers*. D'où il est aisé de conclure que *tout nombre entier est aussi égal à la somme de quatre ou d'un moindre nombre de carrés entiers;* car on sait que le produit de deux, ou de plusieurs nombres égaux chacun à la somme de quatre, ou d'un moindre nombre de carrés, est aussi nécessairement égal à la somme de quatre, ou d'un moindre nombre de carrés; en effet on a

$$\begin{aligned}&(p^2+q^2+r^2+s^2)(p'^2+q'^2+r'^2+s'^2)\\&\quad=(pp'-qq'-rr'+ss')^2+(pq'+qp'-rs'-sr')^2\\&\quad+(pr'+qs'+rp'+sq')^2+(qr'-ps'+sp'-rq')^2,\end{aligned}$$

et même plus généralement

$$\begin{aligned}&(p^2-\mathrm{B}q^2-\mathrm{C}r^2+\mathrm{BC}s^2)(p'^2-\mathrm{B}q'^2-\mathrm{C}r'^2+\mathrm{BC}s'^2)\\&\quad=[pp'+\mathrm{B}qq'\pm\mathrm{C}(rr'+\mathrm{B}ss')]^2-\mathrm{B}[pq'+qp'\pm\mathrm{C}(rs'+sr')]^2\\&\qquad-\mathrm{C}[pr'-\mathrm{B}qs'\pm(rp'-\mathrm{B}sq')]^2+\mathrm{BC}[qr'-ps'\pm(sp'-rq')]^2.\end{aligned}$$