DÉMONSTRATION

D'UN

THÉORÈME D'ARITHMÉTIQUE.

(*Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin*, année 1770[1].)

C'est un Théorème connu depuis longtemps que *tout nombre entier non carré peut toujours se décomposer en duex, ou trois, ou quatre carrés entiers ;* mais personne, que je sache, n'en a encore donné la démonstration. M. Bachet de Méziriac est le premier qui ait fait mention de ce Théorème ; il paraît qu'il y a été conduit par la question 31^{e} du IV^{e} Livre de Diophante, où le Théorème dont nous parlons est en quelque sorte tacitement supposé ; mais M. Bachet s'est contenté de s'assurer de la vérité de ce Théorème par induction, en examinant successivement tous les nombres entiers depuis 1 jusqu'à 325 ; et quant à la démonstration générale, il avoue qu'il n'avait pas encore pu y parvenir. ≪ *Mihi sane* (dit-il dans son Commentaire à la question citée) *perfecta id demonstratione assequi nondum licuit, quam qui proferet maximas ei habebo gratias, præsertim cum non solum in hac quæstione sed et in nonnullis libri quinti hoc supponere videatur Diophantus.* ≫ Je ne connais, jusqu'à présent, que deux Auteurs qui se soient appliqués à cette recherche, savoir M. Fermat et M. Euler. Dans les Notes que le premier a ajoutées au Commentaire de Bachet sur Diophante, il annonce un grand Ouvrage qu'il avait dessein de composer sur la théorie des nombres, et il promet d'y démontrer cette proposition générale : que tout nombre est, ou triangulaire, ou composé de deux ou de trois nombres triangulaires ; qu'il est, ou carré, ou composé de deux, ou de trois, ou de quatre carrés, et ainsi de suite ; mais cet Ouvrage n'a jamais paru, et dans tout ce qui nous reste des écrits de ce grand Géomètre, on ne trouve absolument rien qui puisse fournir la moindre lumière pour la démonstration dont il s'agit. A l'égard de M. Euler, si son travail sur ce sujet n'a pas eu tout le succès qu'on pourrait désirer, on lui a du moins l'obligation d'avoir ouvert la route qu'il faut suivre dans ces sortes de recherches. On peut voir dans le tome V des *Nouveaux Commentaires de Pétersbourg* le résultat des tentatives ingénieuses que ce grand Géomètre a faites pour parvenir à démontrer le Théorème de M. Bachet.

M. Euler fait voir que le produit de deux, ou de plusieurs nombres, dont chacun serait composé de quatre carrés entiers, sera aussi toujours composé de quatre, ou d'un moindre nombre de carrés entiers ; d'où il suit d'abord que si la Théorème proposé peut être démontré pour tous les nombres premiers, il le sera aussi pour tous les autres nombres. M. Euler démontre, de plus, qu'un nombre premier quelconque étant proposé, on peux toujours trouver deux ou trois nombres carrés dont la somme soit divisible par ce nombre sans que chacun des carrés en particulier le soit, et que ces nombres carrés peuvent toujours être supposés tels que le quotient de la division de leur somme par le nombre premier donné soit moindre que ce même nombre. De là M. Euler conclut, avec raison, que le Théorème en question serait démontré pour tous les nombres premiers si l'on pouvait seulment démontrer cette autre proposition, savoir, que lorsque le produit de deux nombres est la somme de quatre ou d'un moindre nombre de carrés, et que l'un des nombres produisants est pareillement la somme de quatre ou d'un moindre nombre de carrés, l'autre produisant le sera de même. ≪ *Si summa quatuor quadratorum* (dit-il, page 55 du volume cité) $a^2+b^2+c^2+d^2$ *fuerit divisibilis per summam quatuor quadratorum* $p^2+q^2+r^2+s^2$, *tum quotum non solum in fractis sed etiam in integris esse summam quatuor quadratorum, est Theorma elegantissimum Fermatii, cujus demonstratio cum ipso nobis est erepta ; fateor me adhuc hanc demonstrationem invenire non potuisse,* etc. ≫

C'est donc cette dernière proposition seule qu'il s'agit de démontrer. Or pour cela nous n'aurons pas besoin de supposer que le diviseur soit aussi représenté par la somme de quatre carrés, et nous démontrerons, en général, que tout nombre premier qui est diviseur d'un nombre quelconque composé de quatre ou d'un moindre nombre de carrés, sans l'être de chacun des carrés en particulier, est nécessairement aussi composé de quatre ou d'un moindre nombre de carrés ; après quoi il n'y aura plus rien à désirer pour la démonstration complète du Théorème général de Bachet, que nous nous sommes proposé de donner dans ce Mémoire.

Lemme.

Les nombres qui sont la somme de deux carrés premiers entre eux n'admettent d'autres diviseurs que ceux qui sont pareillement la somme de deux carrés.

Cette proposition, qui est de M. Fermat, a été démontrée par M. Euler dans un Mémoire imprimé dans le tome IV des *Nouveaux Commentaires de Pétersbourg.*

Corollaire I. — *Si deux nombres égaux chacun à la somme de deux carrés, tels que* p^2+q^2 *et* r^2+s^2, *sont divisibles par un même nombre* ρ, *et que les quatre carrés* p^2, q^2, r^2, s^2 *n'aient aucun diviseur commun, je dis que les deux quotients* $\frac{p^2+q^2}{\rho}$ *et* $\frac{r^2+s^2}{\rho}$ *seront aussi chacun égaux à la somme de deux carrés.*

[1] *Œuvres de Lagrange,* t. III, p. 189.

Car soit m la plus grande commune mesure de p et q, et n la plus grande commune mesure de r et s, de sorte qu'en faisant

$$p = mp', \quad q = mq', \quad r = nr', \quad s = ns'$$

les nombres p' et q' soient premiers entre eux, comme aussi les nombres r' et s' entre eux ; on aura donc les deux nombres $m^2(p'^2 + q'^2)$ et $n^2(r'^2 + s'^2)$ qui seront divisibles à la fois par ρ. Or je remarque d'abord que m et n seront premiers entre eux ; autrement les quatre nombres p, q, r et s auraient une commune mesure, ce qui est contre l'hypothèse. Maintenant soit μ la plus grande commune mesure entre m^2 et ρ, en sorte que l'on ait $\rho = \mu\rho'$, et que ρ' soit premier à $\frac{m^2}{\mu}$; donc m^2 sera divisible par μ, et il faudra que $p'^2 + q'^2$ le soit par ρ', de sorte qu'on aura

$$\frac{p^2 + q^2}{\rho} = \frac{m^2}{\mu}\frac{p'^2 + q'^2}{\rho'};$$

or p' et q' étant premiers entre eux, il suit du Lemme précédent que tant le diviseur ρ' que le quotient seront la somme de deux carrés ; ainsi l'on aura

$$\frac{p'^2 + q'^2}{\rho'} = \alpha^2 + \beta^2.$$

Soit de plus ν^2 le plus grand facteur carré du nombre μ, en sorte que $\mu = \nu^2\mu'$, μ' étant un nombre qui ne soit divisible par aucun carré, et il est clair que m^2 ne pourra être divisible par μ à moins que m ne le soit par $\nu\mu'$; soit donc $m = \mathrm{K}\nu\mu'$, et l'on aura

$$\frac{m^2}{\mu} = \mathrm{K}^2\mu'.$$

Or $n^2(r'^2 + s'^2)$ doit être aussi divisible par $\rho = \mu\rho'$; donc μ divisera $n^2(r'^2 + s'^2)$; mais μ divise déjà m^2 ; donc, puisque m^2 et n^2 sont premiers entre eux, il s'ensuit que μ sera aussi premier à n^2 ; par conséquent il faudra que μ divise $r'^2 + s'^2$; et comme $\mu = \nu^2\mu'$, μ' sera aussi un diviseur de $r'^2 + s'^2$; donc, puisque r' et s' sont premiers entre eux, le diviseur μ' sera égal à la somme de deux carrés par le Lemme. Faisant donc $\mu' = \gamma^2 + \delta^2$, on aura

$$\frac{m^2}{\mu} = \mathrm{K}^2(\gamma^2 + \delta^2);$$

et de là

$$\frac{p^2 + q^2}{\rho} = \mathrm{K}^2(\gamma^2 + \delta^2)(\alpha^2 + \beta^2) = \mathrm{K}^2(\gamma\alpha + \delta\beta)^2 + \mathrm{K}^2(\gamma\beta - \delta\alpha)^2,$$

c'est-à-dire égal à la somme de deux carrés. On démontrera de la même manière que le quotient $\frac{r^2+s^2}{\rho}$ sera aussi égal à la somme de deux carrés.

Corollaire II. — *Si la somme de deux carrés est divisible par une autre somme de deux carrés, le quotient sera toujours égal à la somme de deux carrés.*

Car soit $a^2 + b^2$ divisible par $c^2 + d^2$, et si les nombres a, b, c, d ont une commune mesure, dénotons-la par l, en sorte que l'on ait

$$a = lp, \quad b = lq, \quad c = lr, \quad d = ls,$$

et que p, q, r, s n'aient aucun commun diviseur ; donc on aura

$$\frac{a^2 + b^2}{c^2 + d^2} = \frac{p^2 + q^2}{r^2 + s^2},$$

de sorte que $p^2 + q^2$ sera divisible par $r^2 + s^2$; or, faisant $r^2 + s^2 = \rho$, on aura par le Corollaire précédent $\frac{p^2+q^2}{\rho}$ égal à la somme de deux carrés ; donc, etc.

Théorème I.

Si la somme de quatre carrés est divisible par un nombre premier plus grand que la racine carrée de la même somme, ce nombre sera nécessairement égal à la somme de quatre carrés.

Car soit $p^2 + q^2 + r^2 + s^2$ divisible par A, A étant un nombre premier, en sorte que l'on ait

$$\mathrm{A}a = p^2 + q^2 + r^2 + s^2,$$

et comme on suppose que le diviseur A est plus grand que

$$\sqrt{p^2 + q^2 + r^2 + s^2},$$

il est clair que le quotient a sera plus petit que la même racine, de sorte qu'on aura $a < \mathrm{A}$.

Cela posé, si les nombres p, q, r et s ont un diviseur commun d, il est clair que la somme de leurs carrés sera divisible par d^2, et qu'ainsi il faudra que $\mathrm{A}a$ le soit aussi ; or d^2 étant plus petit que $\mathrm{A}a$, d sera plus petit que $\sqrt{\mathrm{A}a} < A$, à cause de $\mathrm{A} < a$; donc, puisque A est premier (hypothèse), il est clair que A et d seront premiers entre eux ; d'où il s'ensuit que $\mathrm{A}a$ ne pourra être divisible par d^2 à moins que a ne le soit ; ainsi, divisant tant le nombre a que chacun des carrés p^2, q^2,... par d^2, on aura une équation de la même forme que la précédente, où le coefficient a sera toujours plus petit que A et où les quatre carrés p^2, q^2, r^2, s^2 n'auront plus de commun diviseur.

Considérons donc l'équation

$$\mathrm{A}a = p^2 + q^2 + r^2 + s^2$$

comme déjà réduite à cet état, et si le nombre $p^2 + q^2$ n'est pas premier à a, soit ρ leur plus grande commune mesure, en sorte que l'on ait

$$a = b\rho \quad \text{et} \quad p^2 + q^2 = t\rho,$$

b et t étant premiers entre eux ; on aura donc

$$\mathrm{A}b\rho = t\rho + r^2 + s^2,$$

d'où l'on voit que $r^2 + s^2$ doit être aussi divisible par ρ, de sorte que, nommant le quotient u, l'équation deviendra

$$\mathrm{A}b = t + u;$$

or, puisque ρ divise tant $p^2 + q^2$ que $r^2 + s^2$, et que p, q, r et s n'ont aucun diviseur commun, il s'ensuit du Corollaire I du Lemme précédent que les quotients $\frac{p^2+q^2}{\rho} = t$ et $\frac{r^2+s^2}{\rho} = u$ seront l'un et l'autre la somme de deux carrés ; ainsi l'on aura

$$t = m^2 + n^2 \quad \text{et} \quad u = h^2 + l^2;$$

donc, multipliant toute l'équation par t, on aura

$$\mathrm{A}bt = t^2 + tu,$$

ou bien, en faisant $x = mh + nl$ et $y = ml - nh$, en sorte que $tu = x^2 + y^2$, on aura cette équation-ci

$$\mathrm{A}bt = t^2 + x^2 + y^2.$$

Maintenant, comme b et t sont premiers entre eux, on peut toujours trouver deux multiples de b et t tels que leur somme ou leur différence soit égale à un nombre quelconque donné, et de plus on peut supposer que l'un de ces multiples soit moindre que $\frac{bt}{2}$ [*voyez* le Lemme I du Mémoire sur les Problèmes indéterminés, qui est imprimé dans le tome XXIV des *Mémoires de l'Académie royale des Science et Belles-Lettres de Berlin,* pour l'année 1768[2]] ; ainsi l'on peut faire

$$x = \alpha t + \gamma b \quad \text{et} \quad y = \beta t + \delta b,$$

α, β, γ et δ étant des nombres entiers positifs ou négatifs, et l'on peut supposer en même temps que α et β, pris positivement, soient l'un et l'autre plus petits que $\frac{b}{2}$. Qu'on fasse donc cette substitution dans l'équation précédente, elle deviendra

$$\mathrm{A}bt = t^2(1 + \alpha^2 + \beta^2) + 2\alpha\gamma tb + 2\beta\delta tb + \gamma^2 b^2 + \delta^2 b^2,$$

où l'on voit que tous les termes sont multipliés par b, à l'exception de ceux-ci

$$t^2(1 + \alpha^2 + \beta^2);$$

ainsi, pour cette équation puisse subsister en nombres entiers comme il le faut, il est nécessaire que $t^2(1 + \alpha^2 + \beta^2)$ soit aussi divisible par b ; mais b et t sont premiers entre eux, donc il faudra que b divise $1 + \alpha^2 + \beta^2$, de sorte qu'en nommant le quotient a' on aura

$$a'b = 1 + \alpha^2 + \beta^2;$$

et comme α et β sont chacun plus petits que $\frac{b}{2}$, $1 + \alpha^2 + \beta^2$ sera plus petit que $\frac{b^2}{2} + 1$; par conséquent a' sera plus petit que $\frac{b}{2} + \frac{1}{b}$.

Or, mettant dans l'équation ci-dessus $a'b$ à la place de $1 + \alpha^2 + \beta^2$, et divisant ensuite par b, on aura

$$\mathrm{A}t = a't^2 + 2\alpha\gamma t + 2\beta\delta t + (\gamma^2 + \delta^2)b,$$

où je remarque encore que tous les termes étant multipliés par t, excepté ceux-ci

$$(\gamma^2 + \delta^2)b,$$

[2] *Œuvres de Lagrange,* t. II, p. 659.

il faudra que le nombre $(\gamma^2+\delta^2)b$ soit divisible par t, et comme b et t sont premiers entre eux, il faudra que $\gamma^2+\delta^2$ soit divisible par t.

Si l'on multiplie léquation que nous venons de trouver par a', elle pourra se mettre sous cette forme

$$\mathrm{A}a't = (a't+\alpha\gamma+\beta\delta)^2 + (\gamma^2+\delta^2)a'b - (\alpha\gamma+\beta\delta)^2,$$

ou bien sous celle-ci

$$\mathrm{A}a't = (a't+\alpha\gamma+\beta\delta)^2 + \gamma^2(a'b-\alpha^2) + \delta^2(a'b-\beta^2) - 2\alpha\beta\gamma\delta;$$

mais on a

$$a'b = 1+\alpha^2+\beta^2,$$

donc l'équation précédente deviendra

$$\mathrm{A}a't = (a't+\alpha\gamma+\beta\delta)^2 + \gamma^2(1+\beta^2) + \delta^2(1+\alpha^2) - 2\alpha\beta\gamma\delta,$$

c'est-à-dire

$$\mathrm{A}a't = (a't+\alpha\gamma+\beta\delta)^2 + (\beta\gamma-\alpha\delta)^2 + \gamma^2 + \delta^2.$$

Or nous avons dit ci-dessus que $\gamma^2+\delta^2$ doit être divisible par t, donc il faudra aussi que le nombre

$$(a't+\alpha\gamma+\beta\delta)^2 + (\beta\gamma-\alpha\delta)^2$$

le soit ; mais on a

$$t = m^2+n^2,$$

donc, par le Corollaire II du Lemme, chacun des deux quotients sera nécessairement la somme de deux carrés ; de sorte qu'on aura

$$\gamma^2+\delta^2 = t(p'^2+q'^2) \quad \text{et} \quad (a't+\alpha\gamma+\beta\delta)^2 + (\beta\gamma-\alpha\delta)^2 = t(r'^2+s'^2).$$

Donc on aura, après avoir divisé toute l'équation par t,

$$\mathrm{A}a' = p'^2+q'^2+r'^2+s'^2.$$

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 $\frac{\mathrm{A}}{2}$, on aurait

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

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 $\frac{\mathrm{A}}{2}$; car soit, par exemple, $p > \frac{\mathrm{A}}{2}$, il est visible que si $p^2+q^2+r^2+s^2$ est divisible par A, $(p-m\mathrm{A})^2+q^2+r^2+s^2$ le sera aussi, de même que $(m\mathrm{A}-p)^2+q^2+r^2+s^2$, quel que soit le nombre m ; or on peut toujours prendre m tel que $p-m\mathrm{A}$ ou $m\mathrm{A}-p$ soit moindre que $\frac{\mathrm{A}}{2}$; 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 nobmres 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 divisible 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

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

on aura

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

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

$$(p^2 - \mathrm{B}q^2 - C)\mathrm{PQ} = \mathrm{Q}(p^{\mathrm{A}-1} - 1) - (b^{\mathrm{A}-1} - 1).$$

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, $a^{\mathrm{A}-1} - 1$ sera toujours divisible par A. Donc, si l'on suppose que p ne soit pas divisible par A, on aura les deux nombres $p^{\mathrm{A}-1} - 1$ et $b^{\mathrm{A}-1} - 1$ divisible à la fois par A, à cause que b n'est jamais divisible par A, quel que soit q (hypothèse). Donc le nombre $(p^2 - \mathrm{B}q^2 - \mathrm{C})\mathrm{PQ}$ sera divisible par A, de sorte que, ni P ni Q n'étaient divisible par A, il faudrait que $p^2 - \mathrm{B}q^2 - \mathrm{C}$ 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 $\mathrm{A} - 2$ inclusivement à la place de p, et qu'on nomme P′, P″, P‴,..., $P^{(\mathrm{A}-2)}$ les valeurs résultantes de P, on aura, par la théorie connue des différences,

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

Or, si tous les nombres P', P'', P''',... jusqu'à $\mathrm{P}^{(A-2)}$ étaient divisible par A, il faudrait que le nombre $1.2.3\ldots(\mathrm{A}-3)$ le fût aussi ; ce qui ne pouvant être à cause que A est premier, il s'ensuit que parmi les nombres P', P'',..., $P^{(\mathrm{A}-2)}$ 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 $(\mathrm{B}q^2 + \mathrm{C})^{\frac{\mathrm{A}-1}{2}} + 1$ ne soit pas divisible par A.

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

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

Or si $\mathrm{C}^m + 1$ 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 $\mathrm{C}^m + 1$ est divisible par A, alors pour Q ne le soit pas, il faudra que q ne le soit pas, et que la quantité

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

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‴,..., $\mathrm{R}^{(\mathrm{A}-2)}$ les valeurs de R qui résulteraient de la substitution des nombres 1, 2, 3,..., $\mathrm{A} - 2$ à la place de q, on aura

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

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

Corollaire I. — Si l'on fait $\mathrm{B}=-1$ et $\mathrm{C}=-1$, 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 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

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