où $\varphi(\omega)$, $\psi(\omega)$ sont des fonctions quelconques de $\omega$; mais les quantités $\lambda$, $\mu$, $\nu$ seront égales aux cosinus des arcs AP, BP, CP, de même que $l$, $m$, $n$ aux cosinus des arcs AQ, BQ, CQ.

(Au verso, de la main de Lagrange :
*Répondu dans une Lettre à M. Euler du 15 juillet 1773.*)

---

## 28.

## EULER A LAGRANGE.

Saint-Pétersbourg, $\frac{\text{24 septembre}}{\text{5 octobre}}$ 1773 (¹).

Monsieur et très honoré Confrère,

Ayant enfin reçu la traduction française de mon Algèbre, j'ai l'honneur de vous témoigner ma très parfaite reconnaissance de la peine que vous vous êtes donnée d'y ajouter vos très profondes recherches sur l'Analyse indéterminée, et je vous prie de vouloir bien présenter tant à M. Bernoulli qu'aux libraires mes très humbles remerciements.

J'ai lu avec la plus grande satisfaction les excellents Mémoires dont vous venez d'enrichir les *Mémoires de l'Académie royale de Berlin;* les belles démonstrations que vous y donnez du théorème de M. Waring (²) m'ont causé un très grand plaisir, et j'en ai aussi trouvé une démonstration fondée sur des principes tout à fait différents.

Soit $2p+1$ le nombre premier dont il s'agit, et il est certain qu'il y a toujours une infinité de nombres $a$, tels que les puissances $1.a.a^2.a^3\ldots$ jusqu'à $a^{2p-1}$, étant divisées par $2p-1$, produisent des restes tout différents entre eux, de sorte que $a^{2p}$ soit la première puissance après l'unité qui reproduise le reste 1, d'où il s'ensuit que la puissance $a^p$ donne $-1$ pour reste. Comme donc tous les restes mentionnés sont

(¹) Ms. in-4°, f° 40. — *Opera postuma,* t. I, p. 583.
(²) Édouard Waring, né à Shrewsbury en 1734, mort en 1798.

inégaux entre eux, leur nombre étant $2p$, tous les nombres $1.2.3.4\ldots 2p$ y seront compris. Soit maintenant M le produit de tous ces nombres $1.2.3.4\ldots 2p$, et il est clair que ce produit M, étant divisé par $2p+1$, laissera le même reste que le produit de toutes les puissances rapportées; or ce produit est ouvertement $a^{p(2p-1)}$, que je représente par ce produit $a^{2p(p-1)}a^p$, dont le premier facteur $a^{2p(p-1)}$ étant une puissance de $a^{2p}$ laissera l'unité pour reste, mais l'autre facteur $a^p$ donnera le reste $-1$; d'où il est clair que le reste qui résulte de cette puissance entière sera égal à $-1$, de sorte qu'aussi le produit M doit donner le même reste, d'où il s'ensuit que la formule $M+1$ sera divisible par le nombre proposé $2p+1$.

Or, pour ce qui regarde le nombre $a$, il faut qu'il soit tel que la formule $x^2-a$ ne puisse jamais devenir divisible par le nombre premier $2p+1$; ainsi, par rapport à chaque nombre premier $2p+1$, tous les nombres se partagent en deux classes : la première de ceux que je nommerai $b$, d'où la formule $x^2-b$ peut devenir divisible par $2p+1$, et l'autre classe contient les nombres $a$ dont je viens de parler. Pour trouver dans chaque cas ces deux classes de nombres indiqués par les lettres $b$ et $a$, j'ai trouvé, par hasard, une règle très facile, qui mérite d'autant plus d'attention que je ne suis pas en état d'en donner une démonstration rigoureuse.

Pour cet effet, il faut diviser les nombres premiers en deux classes : l'une de la forme $4n-1$ et l'autre de la forme de $4n+1$. Soit donc, premièrement, le nombre premier proposé de la forme $4n-1$, et j'en forme une progression contenue dans ce terme général $n+z^2+z$, laquelle sera par conséquent

$$n,\quad n+2,\quad n+6,\quad n+12,\quad n+20,\quad n+30,\quad n+42,\quad n+56,\quad n+72,\quad \ldots,$$

et je puis démontrer que tous les termes de cette série sont compris dans la classe des nombres marqués par $b$, de sorte qu'une formule $x^2-b$ puisse devenir divisible par $4n-1$, ou bien tous ces nombres sont aussi tels que la formule $b^{2n-1}-1$ soit toujours divisible par $4n-1$, d'où il faut pourtant excepter les cas où $b$ serait égal à $4n-1$

ou un multiple; mais, pour ce que je ne puis pas encore démontrer, c'est que, non seulement tous les termes de cette progression, mais aussi tous les diviseurs de chacun, appartiennent à la classe des nombres $b$; et, en effet, on observera toujours que, si $d$ est un diviseur de quelques-uns de ces termes, on rencontrera toujours dans la même progression un terme de la forme $dk^2$ qui est équivalent au nombre $d$.

Soit, par exemple, le nombre premier proposé $4n - 1 = 71$, et partant $n = 18 = 2.3^2$, et la progression sera

$$18,\ 20,\ 24,\ 30,\ 38,\ 48,\ 60,\ 74,\ 90,\ 108,\ \ldots,$$

et l'on voit d'abord que les nombres de la classe $b$ sont

$$2,\ 3,\ 5,\ 19,\ 37,\ 87.$$

Pour le nombre 2 la chose est claire, puisqu'il se trouve déjà dans le premier terme, multiplié par le carré 9; et le nombre 3 se trouve, multiplié par le carré 16, dans le terme 48; ensuite le second terme 20 renferme le nombre 5 multiplié par le carré 4.

Pour les nombres premiers de la forme $4n + 1$, je forme d'abord la progression de cette formule $n - x - x^2$, qui sera

$$n,\ n-2,\ n-6,\ n-12,\ n-20,\ n-30,\ n-42,\ n-56,\ n-72,\ \ldots;$$

et, lorsque ces termes deviennent négatifs, on n'a qu'à les traiter comme positifs, puisque si $b$ est un tel nombre, non seulement la formule $x^2 - b$, mais aussi $x^2 + b$ pourra devenir divisible par $4n + 1$. Ici la même propriété a lieu que non seulement tous les termes de cette progression, mais aussi tous leurs diviseurs, fournissent des nombres de la classe $b$, et tous les nombres qui ne s'y trouvent pas sont ceux qui constituent la classe $a$; ainsi, prenant pour exemple $4n + 1 = 89$ ou bien $n = 22$, notre progression sera

$$22,\ 20,\ 16,\ 10,\ 2,\ 8,\ 20,\ 34,\ 50,\ 68,\ 88,\ 110,\ 134,\ 160,\ \ldots;$$

d'où l'on voit d'abord que la classe des nombres $b$ contient

$$2,\ 11,\ 17,\ 67,\ \ldots,$$

où il est clair que le nombre 2 se rencontre lui-même dans cette série; et pour le nombre 11, en prenant $x = 33$, le terme de la progression sera $1100 = 11.10^2$; mais il est ici très remarquable que cette belle propriété n'a lieu que si le nombre $4n - 1$ ou $4n + 1$ est premier, car, prenant par exemple $4n - 1 = 35$ ou $n = 9$, la progression sera

$$9, \ 11, \ 15, \ 21, \ 29, \ 39, \ 51, \ 65, \ 81, \ 99, \ 119, \ 141, \ 165, \ \ldots$$

ici, quoique 3 divise plusieurs de ces termes, cependant il ne s'y trouvera aucun qui ait la forme $3k^2$, et il en est de même des nombres 5.7 et d'autres qui sont multipliés par 3.

Je suis fort assuré que la considération de ces circonstances pourra conduire à des découvertes très importantes.

Vous aurez vu, Monsieur, dans mon Algèbre, que le problème de trouver 4 nombres dont les produits 2 à 2, en y ajoutant l'unité, deviennent des nombres carrés, m'a fort embarrassé; et je n'ai pu même assigner, en général, des nombres entiers satisfaisants, quoique je me sois presque souvenu que ce problème a été résolu par Ozanam; mais l'occasion m'a manqué de faire des recherches là-dessus. Or, depuis, j'ai trouvé cette solution assez générale :

Ayant pris à volonté deux nombres $m$ et $n$, tels que $mn + 1 = l^2$, les quatre nombres cherchés seront

$$\begin{array}{llll} (\mathrm{I}) & m, & (\mathrm{III}) & m + n + 2l, \\ (\mathrm{II}) & n, & (\mathrm{IV}) & 4l(l + m)(l + n), \end{array}$$

où le nombre $l$ peut être pris tant négatif que positif. Peut-être que cette solution se trouve dans l'Algèbre d'Ozanam (¹); mais je n'aurais jamais cru que l'Analyse fût suffisante d'étendre (²) cette question jusqu'à cinq nombres, et je fus ces jours-ci très agréablement surpris lorsque je rencontrai les cinq nombres suivants

$$A = 1, \qquad B = 3, \qquad C = 8, \qquad D = 120 \qquad \text{et} \qquad E = \frac{777480}{(2879)^2},$$

(¹) *Nouveaux éléments d'Algèbre*. Amsterdam, 1702, in-8°.

(²) C'est-à-dire qu'au moyen de l'Analyse, on pût étendre....

qui satisfont aux dix conditions prescrites de la manière suivante :

| | | | |
|---|---|---|---|
| (I) | $AB + 1 = 2^2$, | (VI) | $CD + 1 = 31^2$, |
| (II) | $AC + 1 = 3^2$, | (VII) | $AE + 1 = \left(\frac{3011}{2879}\right)^2$, |
| (III) | $AD + 1 = 11^2$, | (VIII) | $BE + 1 = \left(\frac{3259}{2879}\right)^2$, |
| (IV) | $BC + 1 = 5^2$, | (IX) | $CE + 1 = \left(\frac{3809}{2879}\right)^2$, |
| (V) | $BD + 1 = 19^2$, | (X) | $DE + 1 = \left(\frac{10079}{2879}\right)^2$; |

et de là je suis parvenu, mais par une méthode très indirecte que je ne saurais expliquer clairement, à donner une solution assez générale; car ayant établi, par les formules données, les quatre premiers nombres A, B, C, D, je fais

$$A + B + C + D = p, \qquad AB + AC + AD + BC + BD + CD = q,$$
$$ABC + ABD + ACD + BCD = r, \qquad ABCD = s,$$

et alors le cinquième nombre sera

$$E = \frac{4r + 2p(s+1)}{(s-1)^2},$$

et, par rapport à ces nombres, cette propriété est fort remarquable, qu'on aura toujours

$$1 + q + s = \tfrac{1}{4}p^2.$$

Cette matière paraît bien digne d'être mise dans tout son jour, mais je m'en sens incapable.

La résolution de la formule $ax^2 + 1 = y^2$ m'a causé autrefois bien de la peine, par rapport aux nombres $a$ qui demandent de très grands nombres pour $x$ et $y$, comme 61 et 109; mais je viens de trouver un théorème qui conduit d'abord à la solution de ces cas et d'autres semblables.

Connaissant pour le nombre $a$ les valeurs $r$ et $s$, telles que

$$ar^2 - 4 = s^2,$$

qu'on prenne

$$p = rs \quad \text{et} \quad q = s^2 + 2,$$

et ensuite

$$x = \tfrac{1}{2}p^2(q^2 - 1) \quad \text{et} \quad y = \tfrac{1}{2}q(q^2 - 3),$$

et il y aura certainement

$$ax^2 + 1 = y^2,$$

où il faut remarquer que, puisque $r$ est par sa nature un nombre impair, ces deux expressions pour $x$ et $y$ donneront des nombres entiers; ainsi, pour le cas $a = 61$, on aura d'abord $r = 5$, $s = 39$, et de là on tire les grands nombres $x$ et $y$ rapportés dans ma Table.

M. Lexell et moi venons de remettre à M. le chevalier Triquet quelques Mémoires pour les *Actes de l'Académie royale de Turin;* il m'a assuré avant son départ que vous y serez incessamment rappelé, et que Sa Majesté le Roi régnant veut remettre son Académie dans son premier état florissant; dans ce cas, l'Académie de Berlin serait bien à plaindre.

Vous voyez, Monsieur, que je vous ai découvert mon cœur tout entier, et je vous prie de me continuer l'honneur de votre amitié en vous assurant que je serai toujours avec le plus inviolable attachement,

Monsieur,

Votre très humble et très obéissant serviteur,

LÉONARD EULER.

---

## 29.

## EULER A LAGRANGE.

DOMINO CELEBERRIMO *de Lagrange* S. P. D. LEONARDUS EULER (1),

Sequens theorema attentione geometrarum haud indignum, et analysin prorsus singularem postulare videtur.

(1) Ms. in-4°, f° 43. — *Opera postuma,* t. II, p. 585.