JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

E. PROUHET

Note sur les arcs de cercle dont la tangente est rationnelle

Journal de mathématiques pures et appliquées 2e série, tome 1 (1856), p. 215-222.

<http://www.numdam.org/item?id=JMPA_1856_2_1__215_0>

NOTE

SUR

LES ARCS DE CERCLE DONT LA TANGENTE EST RATIONNELLE;

PAR M. E. PROUHET.

La Note qu'on va lire est extraite d'un Mémoire présenté à l'Académie des Sciences le 25 août 1851 et relatif au nombre des solutions de l'équation indéterminée

$$x^2 + y^2 = N.$$

Ayant reconnu depuis que ce sujet pouvait être traité d'une manière beaucoup plus simple que je ne l'avais fait, je n'ai conservé de mon travail que quelques propositions sur les arcs de cercle dont la tangente est rationnelle. Ces propositions ne paraîtront peut-être pas tout à fait indignes de l'attention des géomètres, soit à cause d'un tour particulier de raisonnement susceptible d'être étendu à d'autres questions du même genre, soit parce qu'elles offrent un nouvel exemple de cette correspondance singulière remarquée depuis longtemps entre les propriétés du cercle et celles des nombres premiers.

1. Lorsqu'un nombre entier N est la somme de deux carrés a^2 et a'^2, j'appelle *argument* de N tout arc dont la tangente trigonométrique a pour valeur l'un des rapports suivants:

$$\frac{a}{a'}, \quad -\frac{a}{a'}, \quad +\frac{a'}{a}, \quad -\frac{a'}{a}.$$

2. Parmi les arcs en nombre infini que cette définition comprend, il en existe un et un seul dans l'intervalle de o à $\frac{\pi}{4}$: je lui donnerai le nom d'*argument principal*. Si on le désigne par α, tous les arguments seront donnés par l'expression $k\frac{\pi}{2} \pm \alpha$, k étant un nombre entier positif, négatif ou nul.

3. Le nombre N peut être de plusieurs manières la somme de deux carrés. Dans ce cas, je dirai que deux arguments du nombre N sont *équivalents* ou *distincts* suivant qu'ils correspondront à la même décomposition en deux carrés, ou à des décompositions différentes.

On voit par ce que nous avons dit plus haut que deux arguments α et α' seront équivalents si l'on a

$$\alpha \pm \alpha' \equiv 0 \quad \left(\text{mod.}\ \frac{\pi}{2}\right).$$

Un nombre N aura autant d'arguments distincts qu'il y aura de manières de le décomposer en deux carrés.

4. Un nombre premier de la forme $4n+1$ n'a qu'un seul argument, puisqu'un pareil nombre n'est décomposable que d'une seule manière en deux carrés.

L'argument principal du nombre 2 est $\frac{\pi}{4}$.

L'argument principal d'un carré a^2, considéré comme égal à $a^2 + 0^2$, est 0.

Il n'y a pas lieu de considérer d'arguments dans les nombres premiers de la forme $4n-1$, qui ne peuvent, comme on sait, être la somme de deux carrés. Les produits composés exclusivement de facteurs premiers de cette forme, ne peuvent avoir pour argument principal que 0, et seulement dans le cas où ils sont des carrés parfaits.

Il est bon de remarquer que si un nombre N est la somme de deux carrés, on ne modifiera ni le nombre ni la grandeur de ses arguments en le multipliant par un carré m^2, si m n'a que des diviseurs premiers de la forme $4n-1$.

5. Théorème I. — *Toute somme algébrique des arguments de plusieurs nombres est un argument du produit de ces nombres.*

Soient d'abord deux nombres

$$N = a^2 + a'^2, \quad P = b^2 + b'^2,$$

et posons

$$\frac{a}{a'} = \text{tang}\,\alpha,\quad \frac{b}{b'} = \text{tang}\,\beta.$$

On a identiquement

$$\text{NP} = (ab' \pm ba')^2 + (a'b' \mp ab)^2.$$

Aux deux modes de décomposition de NP, compris dans cette formule, correspondent des arguments ayant pour tangentes

$$\frac{ab' \pm ba'}{a'b' \mp ab} = \frac{\frac{a}{a'} \pm \frac{b}{b'}}{1 \mp \frac{a}{a'}\frac{b}{b'}} = \frac{\text{tang}\,\alpha \pm \text{tang}\,\beta}{1 \mp \text{tang}\,\alpha\,\text{tang}\,\beta} = \text{tang}(\alpha \pm \beta).$$

Donc le produit NP a pour arguments

$$\alpha + \beta \quad \text{et} \quad \alpha - \beta. \qquad \text{C. Q. F. D.}$$

6. Le principe étant démontré pour le cas de deux facteurs, il est facile de l'étendre au cas d'un nombre quelconque de facteurs.

Soient, par exemple, trois nombres, et α, β, γ leurs arguments respectifs. Désignons ces nombres par les symboles $[\alpha]$, $[\beta]$, $[\gamma]$: nous aurons (5)

$$[\alpha][\beta] = [\alpha + \beta] = [\alpha - \beta],$$

d'où

$$[\alpha][\beta][\gamma] = [\alpha + \beta][\gamma] = [\alpha - \beta][\gamma],$$

et, par suite,

$$\begin{aligned}[\alpha][\beta][\gamma] &= [\alpha + \beta + \gamma] = [\alpha + \beta - \gamma] \\ &= [\alpha - \beta + \gamma] = [\alpha - \beta - \gamma].\end{aligned}$$

7. Théorème II. — Réciproquement, *Un nombre décomposable en deux carrés ne peut avoir pour arguments que les sommes algébriques des arguments de ses facteurs premiers.*

Soit

$$\text{N} = a^2 + a'^2 = [\alpha]$$

un nombre décomposable en deux carrés, et que nous supposerons débarrassé de ses facteurs premiers de la forme $4n - 1$, qui ne peuvent influer sur les valeurs de ses arguments. On sait que si un nombre premier

$$p = b^2 + b'^2 = [\beta]$$

divise N, on doit avoir

$$ab' + ba' = ep, \quad a'b' - ab = e'p,$$

ou bien

$$ab' - ba' = ep, \quad a'b' + ab = e'p,$$

e et e' désignant des nombres entiers. D'où l'on conclut ensuite, dans l'un et l'autre cas,

$$\frac{\mathrm{N}}{p} = e^2 + e'^2.$$

Si donc on pose

$$e^2 + e'^2 = [\varepsilon],$$

on aura

$$\operatorname{tang} \varepsilon = \frac{e}{e'} = \frac{ab' \pm ba'}{a'b' \mp ba} = \operatorname{tang}[\alpha \pm \beta],$$

et, par suite,

$$\varepsilon \equiv \alpha \pm \beta \quad \left(\text{mod. } \frac{\pi}{2}\right),$$

ou

$$\alpha \equiv \varepsilon \pm \beta \quad \left(\text{mod. } \frac{\pi}{2}\right).$$

Ainsi α sera équivalent à $\varepsilon + \beta$ ou à $\varepsilon - \beta$. De même, si $q = [\gamma]$ est un diviseur premier de $e^2 + e'^2$, on aura

$$\varepsilon \equiv \eta \pm \gamma,$$

et, par suite,

$$\alpha \equiv \eta \pm \beta \pm \gamma.$$

En continuant ainsi, on finira par arriver à un quotient qui sera un nombre premier. L'argument α est donc une somme algébrique composée avec les arguments des facteurs premiers de N.

8. Corollaire. — *Le nombre des solutions de l'équation*

$$x^2 + y^2 = [\alpha]^{\mathrm{a}} [\beta]^{\mathrm{b}} \ldots [\lambda]^{\mathrm{l}},$$

où α, β,..., λ désignent des arguments de nombres premiers, est égal au nombre des sommes algébriques distinctes que l'on peut former avec a *termes égaux en valeur absolue à α,* b *termes égaux en valeur absolue à β,..., et enfin* l *termes égaux en valeur absolue à λ.*

9. Théorème III. — *Les arguments de deux nombres premiers sont incommensurables entre eux.*

Soient

$$p = [\alpha], \quad q = [\beta]$$

deux nombres premiers différents, et supposons, si c'est possible,

$$\frac{\alpha}{\beta} = \frac{m}{n},$$

m et n étant deux nombres premiers entre eux. Le produit $p^n q^m$ aura pour l'un de ses arguments

$$n\alpha - m\beta,$$

c'est-à-dire o. Donc $p^n q^m$ serait un carré parfait, ce qui est impossible, puisque l'un au moins des exposants est impair.

10. Corollaire. — Comme l'argument de 2 est $\frac{\pi}{4}$, on voit que les *arguments de tous les nombres premiers de la forme $4n + 1$ sont incommensurables avec la circonférence.*

11. Théorème IV. — *Une somme composée d'un nombre fini d'arguments de nombres premiers, multipliés par des coefficients rationnels, ne peut être nulle.*

Soient, par exemple,

$$p = [\alpha], \quad q = [\beta], \quad r = [\gamma]$$

trois nombres premiers distincts, et admettons, si c'est possible, que l'on ait

$$t\alpha - s\beta + u\gamma = 0,$$

t, s, u étant des nombres rationnels, qu'on peut toujours supposer entiers et sans facteur commun. Le produit

$$p^t q^s r^u$$

aura pour l'un de ses arguments

$$t\alpha - s\beta + u\gamma,$$

c'est-à-dire o. Donc ce produit serait un carré, ce qui est impossible, puisque l'un au moins des trois exposants est impair.

12. Corollaire. — *La circonférence ne peut être égale à la somme des arguments de plusieurs nombres premiers de la forme $4n+1$, ni à une somme de ces arguments multipliés par des nombres rationnels.*

13. Théorème V. — *Tout arc dont la tangente est commensurable avec le rayon*, $\frac{\pi}{4}$ excepté, *est incommensurable avec la circonférence.*

Soit

$$\frac{a}{a'} = \operatorname{tang} \alpha,$$

α étant différent de $\frac{\pi}{4}$, et désignons par

$$[\beta], \quad [\gamma], \quad [\delta], \ldots,$$

les facteurs premiers de

$$a^2 + a'^2 :$$

α devra être composé des arguments β, γ, δ, en sorte qu'on aura

$$\alpha \equiv t\beta + r\gamma + s\delta + \ldots \quad \left(\text{mod. } \frac{\pi}{2}\right),$$

t, r, s étant des nombres entiers positifs ou négatifs, qui ne peuvent être tous nuls à moins que α ne soit nul.

Dès lors, si le rapport de α à π ou à $\frac{\pi}{4}$ pouvait être rationnel, on aurait

$$\frac{\pi}{4} = \frac{m}{n}(t\beta + r\gamma + \ldots),$$

c'est-à-dire que l'argument du nombre premier 2 serait une fonction rationnelle et linéaire des arguments d'autres nombres premiers, ce qui est contraire au théorème précédent.

14. Corollaire. — *Le carré est parmi les polygones réguliers circonscrits au cercle, le seul dont le périmètre soit commensurable avec le rayon.*

15. *Remarque.* — Pour savoir si deux arcs dont les tangentes rationnelles sont $\frac{a}{a'}$, $\frac{b}{b'}$, ont un rapport commensurable, il faudra chercher les facteurs premiers des nombres

$$a^2 + a'^2, \quad b^2 + b'^2.$$

Si les facteurs premiers ainsi obtenus ne sont pas les mêmes, les arcs sont incommensurables.

Si ces facteurs sont les mêmes, mais que leurs exposants ne soient pas proportionnels, les arcs sont encore incommensurables.

D'où il est aisé de conclure que le rapport $\dfrac{\text{arc tang}\,\frac{a}{a'}}{\text{arc tang}\,\frac{b}{b'}}$ ne peut être rationnel que si l'on a

$$(a^2 + a'^2)^m = (b^2 + b'^2)^n.$$

16. Théorème VI. — *Si* $[\alpha], [\beta], [\gamma], \ldots, [\lambda]$ *sont des nombres premiers différents de la forme* $4n + 1$, *et* a, b, $c, \ldots$, *des nombres entiers sans diviseur commun, aucune partie aliquote de l'arc*

$$a\alpha + b\beta + c\gamma + \ldots + l\lambda,$$

ne peut avoir une tangente rationnelle.

Ce théorème, conséquence très-simple des propositions précédentes, peut être regardé comme le résumé et le complément d'une théorie ingénieuse exposée par Lambert dans un très-beau Mémoire, inséré parmi ceux de l'Académie de Berlin pour l'année 1761.

Dans ce Mémoire, Lambert appelle *tangente première* toute tangente rationnelle telle, qu'aucune partie aliquote de son arc n'ait une tangente rationnelle, et à l'aide d'une analyse pleine d'originalité, il établit les propositions suivantes :

1°. La tangente de l'arc $\frac{\pi}{4}$ est première ;

2°. Les arcs de deux tangentes premières sont incommensurables ;

3°. Il existe une infinité de tangentes premières ;

4°. Si tang ω et tang φ sont deux tangentes premières, m et n deux nombres premiers entre eux, la tangente de l'arc $m\omega + n\varphi$ sera première.

On voit par notre théorie que les arcs qui ont une tangente première sont de deux sortes, savoir, des arguments de nombres premiers ou des sommes de ces arguments respectivement multipliés par des nombres entiers sans diviseur commun. Mais cette distinction essentielle, qui tient aux propriétés des nombres premiers de la forme $4n+1$, ne pouvait être faite par Lambert dont l'analyse était uniquement fondée sur la règle donnée par Euclide pour trouver la plus grande commune mesure de deux grandeurs.

17. Je remarquerai en terminant que les théorèmes démontrés dans cet article s'étendent aux arcs dont la tangente est $\frac{a}{b}\sqrt{m}$, toutes les fois que les nombres de la forme ma^2+b^2 ne peuvent résulter que de la multiplication de nombres premiers de la même forme. C'est ainsi qu'on arriverait à ce théorème : *La circonférence ne peut être obtenue en combinant par voie d'addition ou de soustraction un nombre fini d'arcs dont les tangentes sont de la forme*

$$\frac{a}{b}\sqrt{3},$$

a et b étant des entiers, et

$$3a^2+b^2$$

un nombre premier.