JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

J.-A. SERRET

Sur un théorème relatif aux nombres entiers

Journal de mathématiques pures et appliquées 1re série, tome 13 (1848), p. 12-14.
<http://www.numdam.org/item?id=JMPA_1848_1_13__12_0>

SUR UN THÉORÈME RELATIF AUX NOMBRES ENTIERS;

PAR M. J.-A. SERRET.

En cherchant une démonstration élémentaire de ce théorème connu : *Tout nombre premier* $4k + 1$ *est la somme de deux carrés*, je suis parvenu aux propositions suivantes qui me semblent dignes d'être signalées.

THÉORÈME I. *Si* -1 *est résidu quadratique par rapport à* p, *en sorte qu'on ait*

$$q^2 \equiv -1 \pmod{p},$$

q *étant pris inférieur à* p, *et que l'on réduise en fraction continue la fraction* $\frac{p}{q}$, *en s'arrangeant de manière que le nombre des quotients soit pair, ce qui est toujours possible, puisque, si ce nombre est impair, on peut diminuer le dernier quotient d'une unité et prendre un quotient de plus égal à* 1, *les termes également distants des extrêmes dans la suite des quotients seront égaux entre eux.*

En effet, si l'on désigne par q_0 le quotient de $q^2 + 1$ par p, on aura

$$pq_0 - qq = 1,$$

d'où il suit que $\frac{q}{q_0}$ est la fraction convergente qui précède $\frac{p}{q}$; par conséquent, en développant $\frac{q}{q_0}$ en fraction continue, on trouvera les quotients de $\frac{p}{q}$, sauf le dernier. Mais, d'un autre côté, des relations connues entre les dénominateurs des diverses fractions convergentes on déduit que les quotients de $\frac{q}{q_0}$, réduite en fraction continue, sont les mêmes

que ceux de $\frac{p}{q}$, sauf le premier, mais en ordre inverse; d'où il suit évidemment que, dans la suite des quotients de $\frac{p}{q}$, les termes également distants des extrêmes sont égaux.

COROLLAIRE. *Tout nombre premier* $4k+1$, *ou plus généralement, tout nombre qui divise une somme de deux carrés, est lui-même la somme de deux carrés.*

Si p divise une somme de deux carrés, -1 est résidu quadratique par rapport à p; et en posant

$$q^2 \equiv -1 \pmod{p},$$

avec $q < p$, la suite des quotients dans le développement de $\frac{p}{q}$ sera, d'après le théorème précédent, disposée comme il suit :

$$\alpha,\ \beta,\ldots,\ \mu,\ \omega,\ \omega,\ \mu,\ldots,\ \beta,\ \alpha.$$

Soient $\frac{m}{n}$ la fraction convergente qui comprend les quotients de la première moitié de la suite, $\frac{m_0}{n_0}$ la précédente, il est évident que $\frac{m}{m_0}$ sera la valeur de la fraction continue ayant pour quotients ceux de la seconde moitié de la suite. D'ailleurs, la fraction convergente qui suit $\frac{m}{n}$ a pour valeur $\frac{m\omega+m_0}{n\omega+n_0}$, et en y remplaçant ω par $\frac{m}{m_0}$, on aura la valeur de $\frac{p}{q}$, savoir,

$$\frac{p}{q} = \frac{m\frac{m}{m_0}+m_0}{n\frac{m}{m_0}+n_0} = \frac{m^2+m_0^2}{mn+m_0n_0}.$$

Donc

$$p = m^2 + m_0^2. \qquad C.\ Q.\ F.\ D.$$

THÉORÈME II. *Si l'on a*

$$q^2 \equiv 1 \pmod{p},$$

q étant pris inférieur à p, et que l'on réduise en fraction continue la fraction $\frac{p}{q}$, *en s'arrangeant de manière que le nombre des quotients soit*

impair, ce qui est toujours possible, les termes également distants des extrêmes dans la suite des quotients seront égaux entre eux.

La démonstration est identique à celle du théorème I.

Legendre a donné dans sa *Théorie des nombres* une démonstration du corollaire de notre théorème I, qui est fondée sur la considération du développement en fraction continue de la racine carrée d'un nombre entier. Cette démonstration présente quelque analogie avec la nôtre, analogie qui résulte de ce que les quotients d'une période dans le développement de la racine d'un nombre entier sont précisément disposés comme ceux des fractions ordinaires que nous considérons dans les théorèmes I et II.

J'énoncerai, à ce sujet, une dernière proposition dont la démonstration ne présente aucune difficulté.

Si l'on développe en fraction continue la racine carrée d'un nombre entier A, et que a soit la racine du plus grand carré contenu dans A, le dernier quotient de chaque période sera, comme on sait, $2a$; et les autres formeront une suite telle que

$$\alpha, \beta, \ldots, \beta, \alpha,$$

composée d'un nombre pair ou impair de termes, et dans laquelle les termes également distants des extrêmes sont égaux. Appelons, pour abréger, *fraction correspondante* au nombre A la fraction ordinaire $\frac{p}{q}$ qui donnerait lieu aux quotients $\alpha, \beta, \ldots, \beta, \alpha$; on peut trouver très-aisément tous les nombres entiers ayant la même fraction correspondante $\frac{p}{q}$, problème qui ne pourra être impossible que si p est un nombre pair.

Cela posé, on a le théorème suivant :

THÉORÈME III. Lorsqu'une suite *symétrique,* telle que

$$\alpha, \beta, \ldots, \beta, \alpha,$$

ne donne pas lieu à une fraction *correspondante,* en supprimant le terme du milieu s'il y en a un, ou en en mettant un quelconque s'il n'y en a pas, on obtiendra une nouvelle suite de quotients donnant lieu à une fraction correspondante.