172. *Une démonstration géométrique de la loi de réciprocité quadratique*

Par Pierre KAPLAN
Maison Franco-Japonaise, Kanda, Tokyo

(Comm. by Zyoiti SUETUNA, M. J. A., Nov. 12, 1969)

Dans l'article (1) Eisenstein démontre la loi de réciprocité quadratique en utilisant les fonctions circulaires, il se sert en particulier du fait que $\frac{\sin nx}{\sin x}$ est un polynôme de degré $n-1$ en sin x. Mais à la fin de cet article il remarque que l'on pourrait faire cette démonstration de manière purement arithmétique, sans utiliser de propriété des fonctions circulaires.

La but de cette note est d'indiquer comment cela peut se faire.

Cette démonstration est basée sur un lemme de Gauss bien connu: Soit p un nombre premier impair, a un entier premier à p, r le nombre des entiers $a, 2a, \cdots, \frac{p-1}{2}a$ congru modulo p à un entier de l'intervalle $\left(\frac{p+1}{2}, p-1\right)$. Alors $\left(\frac{a}{p}\right)=\left(-1\right)^r$.

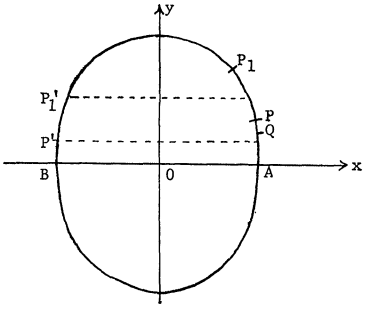

Fig. 1

Dans la suite p et q désignent deux nombres impairs premiers entre eux. Considérons dans un plan rapporté à deux axes rectangulaires une coube (C), rectifiable, symétrique par rapport aux axes, définie dans le premier quadrant par une fonction $x(y)$ décroissante. Soient A et B les points d'intersection de (C) avec O_x. Désignons par P (respectivement Q) les points de division de (C) en p (respectivement q) parties de longueur égale: A étant l'un d'eux, pris pour origine des

abscisses curvilignes sur (C), orientée dans le sens positif. La hauteur d'un point de (C) est son ordonnée y.

Le point essentiel est la remarque suivante: p et q étant impairs, la hauteur du milieu d'un intervalle de devision en p (respectivement en q) est égale à celle d'un point de division en p (respectivement en q), son symétrique par rapport à O_y.

Soit μ le nombre des entiers $p\times 1, \cdots, p\times\frac{q-1}{2}$ congrus modulo q à un entier de l'intervalle $\left(\frac{q+1}{2}, \cdots, q-1\right)$, ν le nombre analogue obtenu en échangeant p et q. Les entiers $1, \cdots, \frac{q-1}{2}$ correspondant aux points d'abscisse curviligne $\frac{1}{q}\cdots\frac{q-1}{2}\cdot\frac{1}{q}$, c'est à dire aux points de division en q situés sur la moitié supérieure de C. Un tel point Q_0 contribue pour 1 à μ si, après multiplication de son abscisse curviligne par p, il vient sur la moitié inférieure de (C), donc si, avant, il était sur la *deuxième moitié* d'un intervalle de division en p, donc, d'après la remarque, si il y a un nombre impair de points P de hauteur positive" au dessous de lui, c'est à dire si

$$\prod_{\substack{P\\ y(P)>0}} (y(P)-y(Q_0))<0.$$

$(-1)^\mu$ a donc le signe de $\prod_{\substack{P,Q\\ y(P),y(Q)>0}} [y(P)-y(Q)]$

et $(-1)^\nu$ celui de $\prod_{\substack{P,Q\\ y(P),y(Q)>0}} [y(Q)-y(P)]$.

Comme il y a $\frac{p-1}{2}\cdot\frac{q-1}{2}$ couples P, Q de hauteurs positives,

$$(-1)^{\mu+\nu}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \qquad \text{C.Q.F.D.}$$

Remarques. (1) Cette démonstration s'expose le plus commodément en utilisant un langage géométrique. Pour ne parler que de nombres entiers il suffit de prendre pour C la coube aplatie sur O_y, de longueur totale $8pq$.

(2) Il serait intéressant de trouver la démonstration "analogue mais plus compliquée" de la loi de réciprocité biquadratique (voir (1) p. 128).

Référence

[1] G. Eisenstein: Applications de l'Algebre a l'Arithmetique transcendante. Mathematische Abhandlungen, 121–128. Georg Olms (1967).