Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 9 (1907)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR LES CONGRUENCES DU TROISIÈME DEGRÉ
Autor: Mirimanoff, D.
DOI: https://doi.org/10.5169/seals-10158

8. Composition de deux translations rectilignes de directions différentes.

Par une translation parallèle à la direction Δ et de grandeur AA′ un segment de droite AB de la figure mobile est venu en A′B′, ce qui donne le parallélogramme AA′B′B. Par une autre translation de directrice Δ' égale à A′A″ le segment de droite A′B′ est venu en A″B″ et on a le parallélogramme A′A″B″B′.

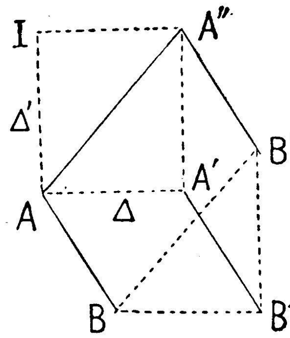

Fig. 10.

Or on sait que A″B″ est égal et parallèle à AB, donc la figure AA″ B″ B est également un parallélogramme. On pourra par conséquent par une translation *unique* égale et parallèle à AA″ amener le segment de droite AB sur A″B″.

Or le déplacement du segment AB entraîne celui des divers points de la figure et on peut observer que : *La translation unique AA″ est la diagonale du parallélogramme AA′A″I dont les côtés AA′ et AI représentent les directions et les grandeurs des translations rectilignes composantes.*

V. Hioux (Paris).

SUR LES CONGRUENCES DU TROISIÈME DEGRÉ[1]

Dans le chapitre IX de son Etude des fonctions arithmétiques M. Arnoux établit, à l'aide de sa méthode graphique, les propriétés caractéristiques des congruences du troisième degré. Ces propriétés ne sont pas nouvelles, mais je les crois peu connues ; et il ne serait peut-être pas inutile de rappeler qu'elles se déduisent très simplement d'un théorème impor-

[1] A propos du livre de M. G. Arnoux : « Introduction à l'étude des fonctions arithmétiques ». — (Voir l'analyse de l'ouvrage dans le précédent n°, p. 326-329. *Réd.*).

tant de M. L. Stickelberger, retrouvé par M. Voronoï et généralisé par M. Hensel.

Supposons que le module soit un nombre premier p supérieur à 3.

La congruence générale du 3e degré se ramène alors à la forme

$$x^3 + bx + a \equiv 0 \pmod{p}, \tag{1}$$

a et b étant deux nombres entiers.

M. Arnoux pose

$$R \equiv \frac{a^2}{4} + \frac{b^3}{27}.$$

Voici alors comment s'énoncent les propriétés retrouvées par M. Arnoux :

(1er cas) p est de la forme $3k - 1$.

Si $R \equiv 0$, la congruence (1) a trois racines réelles dont deux égales.

Si R est un résidu quadratique, il y a une seule racine réelle.

Si R est un non-résidu, le nombre des racines réelles est égal tantôt à trois et tantôt à zéro.

(2me cas) p est de la forme $3k + 1$.

Si $R \equiv 0$, la congruence a encore trois racines réelles, dont deux égales.

Si R est un résidu quadratique, le nombre des racines réelles est égal tantôt à trois et tantôt à zéro.

Si R est un non-résidu, il y a une seule racine réelle.

On voit que les fonctions R se comportent d'une manière inverse, suivant qu'on a $p \equiv -1$ ou $p \equiv 1 \pmod{3}$. Mais la différence dans les énoncés ne tient pas à la nature des choses : elle disparaît, si à la place de R on introduit le discriminant de l'équation. Soit D ce discriminant. On a

$$D = -4b^3 - 27a^2,$$

d'où

$$D = -3 \cdot 6^2 R.$$

Or -3 est un non-résidu pour les nombres p de la forme $3k-1$ et un résidu pour les nombres p de la forme $3k+1$.

On aura donc dans les deux cas :

Si $D \equiv 0$, la congruence (1) a trois racines réelles, dont deux égales.

Si D est un résidu quadratique, le nombre des racines réelles est égal à 3 ou à 0.

Si D est un non-résidu, il y a une seule racine réelle.

La première de ces trois propriétés se démontre immédiatement. En effet, lorsque $D \equiv 0$, la congruence (1) admet les racines $x_1 \equiv -\frac{3a}{2b}$ et $x_2 \equiv \frac{3a}{b}$ et la première de ces racines est double.

Je supposerai donc que D n'est pas divisible par p.

Voici maintenant en quoi consiste le théorème de Stickelberger-Voronoï. Soit

$$f(x) \equiv 0 \pmod{p}$$

une congruence d'un degré quelconque n. Soient D son discriminant, ν le nombre des facteurs irréductibles de $f(x)$ (mod. p). Je supposerai $p > 2$. On a alors

$$\left(\frac{D}{p}\right) = (-1)^{n-\nu}.$$

$\left(\frac{D}{p}\right)$ étant le symbole de Legendre.

Or dans le cas d'une congruence du 3^e degré, $n = 3$. Si donc D est un résidu, l'exposant $3-\nu$ est pair, par conséquent $\nu = 3$ ou 1 ; dans le premier cas le nombre des racines réelles est égal à trois, dans le second à zéro. Si au contraire D est un non-résidu, $3-\nu$ est impair, d'où $\nu = 2$, et par conséquent le nombre des racines réelles est égal à 1.

Je tiens à ajouter que ces résultats avaient été établis d'une manière différente par M. Voronoï dans une thèse publiée en 1894 (v. Verhandlungen des III. intern. math. Kongr., p, 189).

Une question se pose : Quelle est la valeur de ν dans le cas où le discrim. D est un résidu quadratique ? Est-elle égale à 1 ou à 3 ? Une difficulté analogue se présente dans le cas d'une congruence du 4^e degré. Pour trouver la valeur de ν, on pourrait se servir d'une propriété des congruences irréductibles que je voudrais rappeler.

Soient $f(x) \equiv 0 \pmod{p}$ une congruence irréductible de degré n et x_0 l'une de ses racines (imaginaires)[1]. Les n racines de la congruence sont alors x_0, $x_1 = x_0^p$, $x_2 = x_0^{p^2}$, ..., $x_{n-1} = x_0^{p^{n-1}}$.

Il en résulte immédiatement que toute fonction cyclique entière et à coefficients entiers de ces racines est congrue à un nombre entier (mod. p), pourvu que les substitutions cycliques correspondantes soient des puissances quelconques de $(x_0 x_1 x_2 \ldots x_{n-1})$.

Soit maintenant $n = 3$ et posons $D \equiv d^2$. Considérons la fonction

$$M = (x_0 + \alpha x_1 + \alpha^2 x_2)^3 ,$$

α étant une racine $\neq 1$ de $z^3 - 1 \equiv o$ (mod. p). Supposons d'abord que $p \equiv 1$ (mod. 3); α est alors un nombre entier, M une fonction cyclique à coefficients entiers; si donc $\nu = 1$, M est congrue à un nombre entier; si $\nu = 3$, la somme $x_0 + \alpha x_1 + \alpha^2 x_2$ est un entier et M est un résidu cubique. Et l'on retombe sur le critérium de M. Arnoux: $\nu = 3$, si le nombre M ou

$$\frac{3}{2}\left[-9a + (\alpha - \alpha^2)\, d\right] \quad \text{ou} \quad \frac{3}{2}\left[-9a + \sqrt{-3}\,.\,d\right]$$

est un résidu cubique (mod. p).

Supposons maintenant que $p \equiv -1$ (mod. 3). M est une fonction cyclique dans le domaine $[\sqrt{-3}]$. Pour que $\nu = 3$, il faut qu'on ait

$$M^{\frac{p^2-1}{3}} \equiv 1 \quad (\text{mod. } p) .$$

Ces résultats peuvent du reste être établis d'une manière directe (comp. l'ouvrage de M. Arnoux).

Dans le cas d'une congruence du 4e degré on pourrait se servir de la fonction cyclique $(x_0 - x_1 + x_2 - x_3)^2$.

D. MIRIMANOFF (Genève).

[1] On peut supposer par exemple que x_0 est une des racines de l'équation $f(x) = 0$.