NOUVELLES ANNALES DE MATHÉMATIQUES

MIRIMANOFF

Sur l'équation $(x+1)^l - x^l - 1 = 0$

Nouvelles annales de mathématiques 4^e série, tome 3 (1903), p. 385-397

<http://www.numdam.org/item?id=NAM_1903_4_3__385_0>

[A3i]

SUR L'ÉQUATION $(x+1)^l - x^l - 1 = 0$;

PAR M. MIRIMANOFF.

1. On connaît la démonstration qu'Euler a donnée du célèbre théorème de Fermat relatif à la congruence

$$x^l - x \equiv 0 \pmod{l},$$

l étant un nombre premier.

Elle s'appuie sur ce fait que dans le polynome

$$P(x) = (x+1)^l - x^l - 1,$$

tous les coefficients sont divisibles par l, et que, par conséquent, on a identiquement

$$(x+1)^l - (x+1) \equiv x^l - x \pmod{l}.$$

On rencontre le polynome $P(x)$ dans l'étude de questions moins élémentaires.

Considérons, par exemple, le quotient

$$q = \frac{a^l - a}{l}.$$

Si a est entier, q est entier. On peut se proposer de calculer le reste de $q \pmod{l}$. Le polynome $P(x)$ joue un rôle important dans la solution de ce problème (1).

On le rencontre encore dans l'étude de la fameuse équation de Fermat

$$\xi^l + \eta^l + \zeta^l = 0.$$

(1) P. BACHMANN, *Niedere Zahlentheorie*, t. I, p. 161 (*Teubner's Sammlung von Lehrbüchern*).

Dans ces problèmes, on envisage tantôt le polynome même, tantôt la congruence identique $P(x) \equiv 0$, tantôt la congruence

$$\frac{P(x)}{l} \equiv 0 \qquad (\mathrm{mod}\, l).$$

Le polynome et la congruence possèdent des propriétés curieuses qui sont étroitement liées à celles de l'équation

$$P(x) = 0. \tag{1}$$

Peut-être y aurait-il quelque intérêt à faire une étude directe de cette équation. Essayons d'en établir les propriétés les plus caractéristiques.

2. Supposons $l > 3$. Observons d'abord que le polynome $P(x)$ s'annule pour $x = 0$ et pour $x = -1$.

D'autre part, l'équation

$$\frac{dP}{dx} = l x^{l-1}\left[\left(\frac{x+1}{x}\right)^{l-1} - 1\right] = 0 \tag{2}$$

n'a qu'une seule racine réelle, $x = -\frac{1}{2}$.

Par conséquent, l'équation $P(x) = 0$ a deux racines réelles et $l - 3$ racines imaginaires.

L'équation (1) a-t-elle des racines multiples?

Toute racine multiple annule la dérivée $P'(x)$, elle est racine de

$$(x+1)x^{l-1} - x^l - 1 = 0$$

ou de

$$x^{l-1} - 1 = 0$$

et de

$$(x+1)^{l-1} - 1 = 0.$$

Par conséquent, x et $x+1$ sont figurées par deux points situés sur la circonférence de rayon 1 dont le centre est à l'origine, et l'on voit que les racines multiples de (1) sont racines de $x^2 + x + 1 = 0$.

D'autre part, elles annulent $x^{l-1} - 1$, d'où l'on conclut que $l - 1$ doit être divisible par 3.

Mais le polynome $P(x)$ est divisible par $x^2 + x + 1$ pour tout $l > 3$.

Si donc $l - 1$ est divisible par 3, l'équation (1) a deux racines doubles, $P(x)$ est divisible par

$$x(x+1)(x^2+x+1)^2.$$

Si, au contraire, $l - 1$ n'est pas divisible par 3, l'équation (1) n'a pas de racines multiples, $P(x)$ est divisible par

$$x(x+1)(x^2+x+1).$$

3. Divisons l'équation (1) par l; elle deviendra

$$(3)\quad \left\{ x^{l-1} + \frac{l-1}{1.2}x^{l-2} + \frac{(l-1)(l-2)}{1.2.3}x^{l-3} + \ldots + \frac{l-1}{1.2}x^2 + x = 0. \right.$$

C'est une équation réciproque.

D'autre part, le polynome $P(x)$ ne varie pas lorsqu'on remplace x par $-1-x$. Soit α une racine de (1). Il résulte de la remarque que nous venons de faire que l'équation (1) admet aussi les racines

$$\frac{1}{\alpha},\quad -1-\alpha,\quad -\frac{1}{1+\alpha},\quad -1-\frac{1}{\alpha},\quad -\frac{\alpha}{1+\alpha}.$$

Mais ces racines ne sont pas nécessairement distinctes.

Elles se réduisent à deux :

1° Lorsque α est égal à 0 ou à -1;

2° Lorsque α est racine de $x^2 + x + 1 = 0$.

Elles se réduisent à trois :

3° Lorsque α est égal à l'un des trois nombres suivants : $1, -2, -\frac{1}{2}$.

Dans tous les autres cas les six racines sont distinctes.

Mais le troisième cas ne peut pas se présenter. D'autre part, $P(x)$ est toujours divisible, pour $l > 3$, par $x(x+1)$ et x^2+x+1.

Si donc on pose

$$E(x) = \frac{1}{l}\,\frac{P(x)}{x(x+1)(x^2+x+1)^{\varepsilon}},$$

l'exposant ε étant égal à 1, lorsque $l-1 \not\equiv 0 \pmod 3$, et à 2, lorsque $l-1 \equiv 0 \pmod 3$, l'équation

$$E(x) = 0 \tag{4}$$

n'a que des racines imaginaires inégales qui peuvent être divisées en groupes comprenant chacun six racines.

Soit k le nombre des groupes; le degré de (4) est égal à $6k$.

Si $l-1 \not\equiv 0 \pmod 3$,

$$k = \frac{l-5}{6}.$$

Si $l-1 \equiv 0 \pmod 3$,

$$k = \frac{l-7}{6}.$$

A chaque groupe de six racines correspond un polynome du sixième degré $e_i(x)$ et l'on peut écrire

$$E(x) = e_1(x)\,e_2(x)\ldots e_k(x).$$

4. Dans l'équation (1), posons $x = -z$, elle devient

$$(-z+1)^l + z^l - 1 = 0.$$

Le premier membre ne varie pas lorsqu'on remplace z par $1-z$; de plus, l'équation est réciproque. Si donc elle est vérifiée en posant $z = \alpha$, elle admet aussi les racines

$$\frac{1}{\alpha},\quad 1-\alpha,\quad \frac{-1+\alpha}{\alpha},\quad \frac{1}{1-\alpha},\quad \frac{-\alpha}{1-\alpha}.$$

Posons $\alpha = k^2(\omega)$, k étant le module d'une intégrale elliptique, ω le rapport des périodes.

Les six racines du groupe sont respectivement égales à

$$k^2, \quad \frac{1}{k^2}, \quad k'^2, \quad -\frac{k'^2}{k^2}, \quad \frac{1}{k'^2}, \quad -\frac{k^2}{k'^2},$$

$k'(\omega)$ étant le module complémentaire.

Ce sont les six valeurs du carré du module qui se déduisent de $k^2(\omega)$ par les transformations du premier degré.

On voit que la théorie de l'équation (1) peut être rattachée à celle des fonctions elliptiques.

Nous nous bornerons à cette remarque.

5. Reprenons l'équation $E(x) = 0$. Le coefficient de son premier terme étant égal à l'unité, ses racines sont des nombres algébriques entiers et même des unités complexes, puisque le dernier terme de $E(x)$ est aussi égal à 1.

Il en résulte que les coefficients des polynomes $e_i(x)$ sont des nombres algébriques entiers. Je montrerai qu'ils sont tous réels. Pour que les coefficients d'un polynome $e_i(x)$ soient réels, il faut et il suffit que les racines de $e_i(x) = 0$ forment trois couples de racines imaginaires conjuguées.

On en déduit la condition suivante :

Les racines de l'un des couples ont l'unité pour module.

Reprenons l'équation

$$P(x) = 0.$$

Posons

$$x = \cos\varphi + i\sin\varphi.$$

A chaque valeur réelle de φ correspond une racine de module 1. Le nombre des couples de module 1 est égal à celui des racines φ comprises entre 0 et π.

Mais l'équation $P(x) = 0$ devient

$$2^{l-1}\left(\cos\frac{\varphi}{2}\right)^l = \cos\frac{l\varphi}{2}$$

ou

$$2^{l-1}(\cos\omega)^l = \cos l\omega,$$

en posant

$$\frac{\varphi}{2} = \omega.$$

Considérons les courbes

$$(a) \qquad y = 2^{l-1}(\cos\omega)^l,$$

$$(b) \qquad y = \cos l\omega,$$

ω étant l'abscisse et y l'ordonnée.

Les deux courbes passent par les points $\omega = \frac{\pi}{3}$, $y = \frac{1}{2}$ et $\omega = \frac{\pi}{2}$, $y = 0$. Considérons la partie du plan comprise entre les parallèles $\omega = \frac{\pi}{3}$ et $\omega = \frac{\pi}{2}$.

Lorsque l'abscisse ω croît de $\frac{\pi}{3}$ à $\frac{\pi}{2}$, la courbe (a) se rapproche de plus en plus de l'axe des ω, tandis que l'ordonnée de (b) oscille entre $+1$ et -1 $\left(\text{elle a } \frac{2\pi}{l}\right.$ pour période$\left.\right)$. On en déduit facilement que le nombre des points d'intersection distincts situés à l'intérieur du domaine considéré est égal à $k+2$, k étant le nombre des polynomes $e_i(x)$. Mais les points extrêmes correspondent aux racines de $x+1=0$ et de $x^2+x+1=0$. On doit les écarter.

Il en résulte que chacune des équations $e_i(x) = 0$ admet un couple de racines de module 1. On voit en

même temps qu'il est inutile de considérer l'intervalle compris entre o et $\frac{\pi}{3}$, puisque le nombre des points d'intersection situés entre les parallèles $\omega = 0$ et $\omega = \frac{\pi}{2}$ ne saurait être supérieur à $k+2$. Le théorème est démontré.

Considérons l'une des équations $e_i(x) = 0$. Soit

$$\alpha_i = \cos\varphi_i + i\sin\varphi_i$$

celle de ses racines de module 1 qui est située dans la partie supérieure du plan. D'après ce qui précède, l'argument φ_i est compris entre $\frac{2\pi}{3}$ et π. Rangeons les racines α_i dans l'ordre des arguments croissants. A chacune des racines α_i correspond un polynome déterminé $e_i(x)$.

Les racines α_i sont situées sur la circonférence de rayon 1 dont le centre est à l'origine. On pourra les construire à l'aide des deux courbes (a) et (b).

Mais chacune des équations $e_i(x) = 0$ admet six racines imaginaires qui s'expriment très simplement en fonction de α_i. Soient α_i' la racine $-\frac{1}{\alpha_i+1}$, α_i'' la racine $-\frac{\alpha_i+1}{\alpha_i}$.

Menons la droite D représentée par l'équation

$$x = -\frac{1}{2}.$$

Soit D_1 la droite passant par le point α_i et le point $e^{\pi i}$. Les droites D et D_1 se coupent au point α_i'. Le point α_i'' est le symétrique de α_i par rapport à la droite D.

Les trois autres racines du groupe sont les conjuguées imaginaires de α_i, α_i' et α_i''.

On voit qu'il est facile, à l'aide des courbes (a) et (b), de construire les $6k$ racines de l'équation $E(x) = 0$.

6. *Quelle est la forme des polynomes $e_i(x)$?*

Ces polynomes appartiennent à la catégorie des polynomes du sixième degré qui possèdent les propriétés suivantes :

1° Les termes équidistants des extrêmes ont les mêmes coefficients ;

2° Le coefficient du premier terme est égal à 1 ;

3° Le polynome ne varie pas lorsqu'on remplace x par $-1-x$.

On constate facilement que ces polynomes sont de la forme

$$x^6+3x^5+tx^4+(2t-5)x^3+tx^2+3x+1,$$

t étant un paramètre.

A chacun des polynomes $e_i(x)$ correspond une valeur déterminée t_i du paramètre t.

Nous savons que t_i est un nombre algébrique entier réel; t_i est lié à une racine quelconque x de $e_i(x)=0$ par la relation

$$t_i-6=-\frac{(x^2+x+1)^3}{x^2(x+1)^2}; \tag{5}$$

et, pour $x=\alpha_i$,

$$t_i-6=\frac{\left(1-4\cos^2\frac{\varphi_i}{2}\right)^3}{4\cos^2\frac{\varphi_i}{2}}, \tag{6}$$

φ_i étant l'argument de α_i.

Si, dans l'équation $e_i(x)=0$, on pose $x=-k^2(\omega)$, comme dans le n° 4, on trouve

$$t_i-6=-\frac{27g_2^3}{4(g_2^3-27g_3^2)}=-\frac{27}{4}\,\mathrm{I}(\omega), \tag{7}$$

g_2 et g_3 étant les invariants de Weierstrass et $\mathrm{I}(\omega)$ l'invariant de Klein.

Supposons que $l-1$ ne soit pas divisible par 3 et soit α une racine de $x^2+x+1=0$. En prenant la dérivée du polynome $\frac{P(x)}{l}$, on trouve, pour $x=\alpha$,

$$\frac{1}{l}\frac{dP}{dx}=\alpha(\alpha+1)(2\alpha+1)E(\alpha);$$

or,

$$e_i(\alpha)=t_i-6.$$

On en conclut

$$(8)\qquad (t_1-6)(t_2-6)\ldots(t_k-6)=1;$$

t_i-6 est dans ce cas une unité complexe.

Mais il n'en est plus ainsi lorsque $l-1\equiv 0 \pmod 3$. On a alors

$$(8')\qquad (t_1-6)(t_2-6)\ldots(t_k-6)=\frac{l-1}{6}.$$

On trouve de même que dans le premier cas

$$(9)\qquad \Sigma t_i=\frac{(l+17)(l-5)}{24}\qquad (i=1,2,\ldots,k)$$

et dans le second

$$(9')\qquad \Sigma t_i=\frac{(l+19)(l-7)}{24}.$$

Pour former l'équation qui a pour racines $t_1, t_2, \ldots, t_k$, on peut se servir de la méthode classique qui est exposée dans le Tome II du *Cours d'Algèbre supérieure* de J.-A. Serret (p. 544 de la 5e édit.).

7. Une dernière question se pose :

L'équation $E(x)=0$ *est-elle réductible* (*dans le domaine des nombres entiers ordinaires*)?

Soit $D(x)$ un diviseur irréductible de $E(x)$. Les coefficients de $D(x)$ étant entiers et, par conséquent,

réels, si l'équation $D(x) = 0$ admet une racine de $e_i(x) = 0$, elle admet aussi sa conjuguée.

Mais les racines de $e_i(x) = 0$ forment trois couples :

1° Le couple

$$\alpha_i \quad \text{et} \quad \frac{1}{\alpha_i}$$

(couple de première espèce);

2° Le couple

$$\alpha'_i = -\frac{1}{\alpha_i + 1} \qquad \text{et} \qquad -1 - \alpha'_i = -\frac{\alpha_i}{\alpha_i + 1}$$

(couple de deuxième espèce);

3° Le couple

$$\alpha''_i = -\frac{\alpha_i + 1}{\alpha_i} \qquad \text{et} \qquad -\frac{\alpha''_i}{\alpha''_i + 1} = -1 - \alpha_i$$

(couple de troisième espèce).

Supposons que l'équation $D(x) = 0$ admette deux couples de racines de $e_i(x) = 0$; je dis qu'elle les admet tous les trois. Supposons, par exemple, qu'elle admette les couples 1° et 2°. Le polynome

$$F(x) = D(-1 - x)$$

s'annule pour $x = \alpha'_i$. $F(x)$ admet donc toutes les racines de $D(x) = 0$. Par conséquent,

$$F(\alpha_i) = 0,$$

d'où

$$D(-1 - \alpha_i) = 0,$$

et l'on voit que $D(x) = 0$ admet les racines de troisième espèce. Les autres cas se traitent de la même manière.

Reste à voir si le nombre des couples communs à $D(x) = 0$ et à $e_i(x) = 0$ peut être égal à 1.

Toute racine de $D(x) = 0$ vérifie l'une des k équa-

tions $e_i(x) = 0$. Soient $e_{i_1}(x) = 0$, $e_{i_2}(x) = 0$, ..., $e_{i_m}(x) = 0$ celles d'entre elles qui ont des racines communes avec $D(x) = 0$. Je dis que chacune de ces m équations fournit à $D(x) = 0$ un même nombre de couples. Si donc $D(x)$ n'était pas égal au produit

$$\pi(x) = e_{i_1}(x)\, e_{i_2}(x) \ldots e_{i_m}(x),$$

le nombre des couples fournis par chacune des m équations serait égal à 1. De plus, ces m couples appartiendraient tous à la même espèce (la démonstration est exactement semblable à celle que nous avons indiquée au commencement de ce Paragraphe).

Le polynome $\Pi(x)$ se décomposerait en un produit de trois facteurs irréductibles tels que $D(x)$, correspondant aux couples de première, de deuxième et de troisième espèce.

Considérons celui de ces facteurs dont les racines sont toutes de première espèce. Nous nous appuierons sur le théorème suivant :

Une unité complexe de module 1 *dont toutes les conjuguées ont l'unité pour module est une racine de l'unité* (1).

En vertu de ce théorème, les racines de notre facteur sont des racines de l'unité.

D'autre part, aucune des racines de $E(x) = 0$ n'est une racine de l'unité. On en conclut que tout diviseur irréductible de $E(x)$ est égal au produit d'un certain nombre de polynomes $e_i(x)$.

Si donc $E(x)$ se décompose en facteurs, l'équation en t est réductible.

---

(1) KRONECKER, *Journal für die reine und angewandte Mathematik*, t. LIII.

Tout porte à penser que l'équation en t [et, par suite, l'équation $E(x) = 0$] est irréductible dans le domaine des nombres entiers.

8. *Exemples.* — Soit $l = 11$:

$$\frac{(x+1)^{11} - x^{11} - 1}{11} = x(x+1)(x^2+x+1)\,E(x);$$

la formule (8) donne

$$t - 6 = 1,$$

d'où

$$E(x) = x^6 + 3x^5 + 7x^4 + 9x^3 + 7x^2 + 3x + 1$$

(le coefficient de $x^3 = 2t - 5$).

L'équation $E(x) = 0$ est irréductible.

Soit maintenant $l = 13$:

$$\frac{(x+1)^{13} - x^{13} - 1}{13} = x(x+1)(x^2+x+1)^2\,E(x).$$

La formule (8′) donne

$$t - 6 = \frac{12}{6} = 2,$$

d'où

$$E(x) = x^6 + 3x^5 + 8x^4 + 11x^3 + 8x^2 + 3x + 1;$$

l'équation $E(x) = 0$ est irréductible.

Soit enfin $l = 17$:

$$\frac{(x+1)^{17} - x^{17} - 1}{17} = x(x+1)(x^2+x+1)\,E(x),$$

$$E(x) = e_1(x)\,e_2(x).$$

Les formules (8) et (9) donnent

$$(t_1 - b)(t_2 - b) = 1,$$

$$t_1 + t_2 = 17.$$

L'équation $E(x) = 0$ est irréductible.

P. S. — Je viens d'apprendre que M. Bendz, à Upsal, s'est occupé du même sujet. Dans un opuscule intitulé : *Öfver diophantiska ekvationen* $x^n + y^n = z^n$ (Upsala, Lindequistska bokhandeln, 1902), le géomètre suédois établit une partie des résultats que je fais connaître dans cette Note. Comme moi, il considère les deux courbes $y = 2^{l-1}\left(\cos\frac{\varphi}{2}\right)^l$ et $y = \cos\frac{l\varphi}{2}$, mais l'analogie ne va pas plus loin. Je tiens à signaler à l'attention des lecteurs des *Nouvelles Annales* le travail de M. Bendz.