NOUVELLES ANNALES DE MATHÉMATIQUES

ZOLOTAREFF

Sur l'équation $Y^2 - (-1)^{\frac{p-1}{2}} pZ^2 = 4X$

Nouvelles annales de mathématiques 2^e série, tome 11 (1872), p. 539-549

<http://www.numdam.org/item?id=NAM_1872_2_11__539_1>

SUR L'ÉQUATION $Y^2 - (-1)^{\frac{p-1}{2}} pZ^2 = 4X$;

PAR M. ZOLOTAREFF,
Privatdocent à l'Université de Saint-Petersbourg.

Soient

$$r, \quad r^2, \quad r^3, \ldots, \quad r^{p-1}$$

les $p - 1$ racines de l'équation

$$X = x^{p-1} + x^{p-2} + x^{p-3} + \ldots + x + 1 = \frac{x^p - 1}{x - 1} = 0,$$

p étant un nombre premier, et

$$r = \cos\frac{2\pi}{p} + i \sin\frac{2\pi}{p}.$$

Ces racines, comme on sait, peuvent être distribuées en deux groupes (*) : les racines

$$r, \quad r^\alpha, \quad r^{\alpha'}, \ldots,$$

dont les exposants $1, \alpha, \alpha', \ldots$ sont résidus quadratiques par rapport à p, forment le premier groupe, et celles

$$r^\beta, \quad r^{\beta'}, \ldots,$$

où $\beta, \beta', \ldots$ sont non-résidus, forment le second groupe. Le nombre des racines dont chaque groupe se compose

(*) *Voir* GAUSS, *Disquisitiones arithmeticæ*, ou SERRET, *Cours d'Algèbre supérieure*; 3e édition.

est égal à $\frac{p-1}{2} = m$. On sait aussi comment, à l'aide de ces groupes, on forme deux fonctions entières, Y et Z, à coefficients entiers, satisfaisant à l'équation

$$Y^2 - (-1)^{\frac{p-1}{2}} pZ^2 = 4X.$$

Quant à ces fonctions Y et Z, Gauss s'exprime comme il suit : « Terminos duos summos functionis Y semper fieri $2x^m + x^{m-1}$, summumque functionis Z x^{m-1} facile perspicietur; coefficientes reliqui autem, qui manifesto omnes erunt integri, variant pro diversa indole numeri p, nec formulæ analyticæ generali subjici possunt. »

Lejeune-Dirichlet (*) généralisa l'équation

$$Y^2 - (-1)^{\frac{p-1}{2}} pZ^2 = 4X$$

pour le cas où p est un nombre composé impair, n'ayant pas de diviseurs carrés plus grands que l'unité.

Dans cette Note, je me propose de démontrer que les polynômes Y et Z se trouvent au moyen des fractions continues. En outre, je donne les équations linéaires d'après lesquelles se trouvent aussi les coefficients de la fonction Z. Nous verrons que, après avoir trouvé la fonction Z, on peut facilement déterminer la fonction Y. Je me suis borné au cas où p est un nombre premier.

Considérons en premier lieu la fonction

$$S(x) = \sum_{1}^{p-1} \left(\frac{i}{p}\right) x^i$$
$$= \left(\frac{1}{p}\right) x + \left(\frac{2}{p}\right) x^2 + \ldots + \left(\frac{p-1}{p}\right) x^{p-1},$$

(*) Voir *Vorlesungen über Zahlentheorie*, §§ 138, 139, 140.

où $\left(\frac{i}{p}\right)$ est le symbole connu de Legendre. On sait que, pour les valeurs de x égales à une des racines r^i de l'équation $X = \frac{x^p - 1}{x - 1} = 0$,

$$S(r^i) = \pm\sqrt{(-1)^{\frac{p-1}{2}} p}. \tag{1}$$

Quant au signe qu'on doit prendre pour le second membre de cette équation, il doit être le même pour toutes les valeurs de i qui sont résidus quadratiques, et le signe contraire pour les autres valeurs de i. En effet, cela résulte de l'équation connue

$$S(r^i) = \left(\frac{i}{p}\right) S(r).$$

Gauss et Dirichlet ont démontré que c'est le signe $+$ qui correspond aux résidus quadratiques; mais cette détermination du signe n'est pas nécessaire pour l'objet que nous avons en vue.

Développons maintenant $\frac{S(x)}{X}$ en fraction continue et cherchons les fractions convergentes

$$\frac{f_0(x)}{\psi_0(x)}, \quad \frac{f_1(x)}{\psi_1(x)}, \quad \frac{f_2(x)}{\psi_2(x)}, \ldots.$$

Soit

$$\frac{S(x)}{X} = \pm 1 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots}};$$

nous aurons

$$\begin{aligned} f_0(x) &= \pm 1, & \psi_0(x) &= 1, \\ f_1(x) &= \pm q_1 + 1, & \psi_1(x) &= 1, \\ f_2(x) &= f_1(x) q_2 + f_0(x), & \psi_2(x) &= \psi_1(x) q_2 + \psi_0(x), \end{aligned}$$

et, en général,

$$f_{i+1}(x) = f_i(x)\,q_{i+1} + f_{i-1}(x), \quad \psi_{i+1}(x) = \psi_i(x)\,q_{i+1} + \psi_{i-1}(x).$$

Cela posé, soit $\frac{f_\mu(x)}{\psi_\mu(x)}$ la dernière des fractions convergentes, dont le dénominateur est de degré inférieur à $\frac{p-1}{2} = m$; nous allons établir que la différence

$$S(x)\psi_\mu(x) - f_\mu(x)\,X,$$

que nous désignerons par $\varphi_\mu(x)$, est de degré non supérieur à m. En effet, de nos conventions il résulte

$$\frac{S(x)}{X} - \frac{f_\mu(x)}{\psi_\mu(x)} = \frac{\varphi_\mu(x)}{X\psi_\mu(x)}; \tag{2}$$

mais on sait, par la théorie des fractions continues, que le premier membre de l'équation (2) est de degré non supérieur à celui de la fonction

$$\frac{1}{\psi_\mu(x)\psi_{\mu+1}(x)}.$$

Il s'ensuit que la fonction $\varphi_\mu(x)$ est de degré non supérieur à celui de la fonction

$$\frac{X}{\psi_{\mu+1}(x)},$$

c'est-à-dire non supérieur à m, en vertu de ce que X est de degré $p-1$ et $\psi_{\mu+1}(x)$ de degré non inférieur à $\frac{p-1}{2}$.

En posant dans l'équation

$$S(x)\psi_\mu(x) - X f_\mu(x) = \varphi_\mu(x)$$

successivement

$$x = r, \quad r^2, \ldots, \quad r^i, \ldots, \quad r^{p-1},$$

nous aurons

$$\begin{aligned}
S(r)\psi_\mu(r) &= \varphi_\mu(r),\\
S(r^2)\psi_\mu(r^2) &= \varphi_\mu(r^2),\\
&\cdots\cdots\cdots\cdots\cdots,\\
S(r^i)\psi_\mu(r^i) &= \varphi_\mu(r^i),\\
&\cdots\cdots\cdots\cdots\cdots,
\end{aligned}$$

ou, ce qui revient au même,

$$\begin{aligned}
\varphi_\mu(r) &= \pm\sqrt{(-1)^{\frac{p-1}{2}}p}\,\psi_\mu(r),\\
\varphi_\mu(r^2) &= \pm\sqrt{(-1)^{\frac{p-1}{2}}p}\,\psi_\mu(r^2),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
\varphi_\mu(r^i) &= \pm\sqrt{(-1)^{\frac{p-1}{2}}p}\,\psi_\mu(r^i),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots,
\end{aligned}$$

où, comme nous avons dit plus haut, on doit prendre le radical $\sqrt{(-1)^{\frac{p-1}{2}}p}$ avec le même signe pour toutes les valeurs de i qui sont résidus quadratiques, et avec le signe contraire pour les autres valeurs de i.

En désignant par ε l'unité avec le signe qui correspond aux résidus quadratiques, on voit donc que l'équation

$$(3)\qquad \varphi_\mu(x) - \varepsilon\sqrt{(-1)^{\frac{p-1}{2}}p}\,\psi_\mu(x) = 0$$

admet les racines

$$x = r,\quad x = r^\alpha,\quad x = r^{\alpha'},\ldots,$$

et l'équation

$$(4)\qquad \varphi_\mu(x) + \varepsilon\sqrt{(-1)^{\frac{p-1}{2}}p}\,\psi_\mu(x) = 0$$

les racines

$$r^\beta,\quad r^{\beta'},\ldots.$$

Ainsi les équations (3) et (4) ont chacune au moins m racines. En remarquant, d'un autre côté, que le degré de la fonction $\psi_\mu(x)$ est inférieur à m et que celui de $\varphi_\mu(x)$ ne surpasse pas m, on voit que les équations (3) et (4) ne peuvent admettre chacune plus de m racines; donc elles n'admettent que m racines et le degré de $\varphi_\mu(x)$ est égal par conséquent à m. Il suit de là que la fonction

$$\varphi_\mu(x) - \varepsilon\sqrt{(-1)^{\frac{p-1}{2}}p}\,\psi_\mu(x)$$

est égale, à un facteur constant près, à celle-ci

$$W = (x-1)(x-r^\alpha)(x-r^{\alpha'})\ldots.$$

En désignant par $\frac{\lambda}{2}$ ce facteur constant, on a

$$2W = \lambda\varphi_\mu(x) - \varepsilon\sqrt{(-1)^{\frac{p-1}{2}}p}\,\lambda\psi_\mu(x);$$

or, d'un autre côté,

$$2W = Y \pm \sqrt{(-1)^{\frac{p-1}{2}}p}\,Z$$

(voir *Disquisitiones arithmeticæ*); donc

$$Y \pm \sqrt{(-1)^{\frac{p-1}{2}}p}\,Z = \lambda\varphi_\mu(x) - \varepsilon\sqrt{(-1)^{\frac{p-1}{2}}p}\,\lambda\psi_\mu(x).$$

On détermine la constante λ de telle manière que le premier terme de $\lambda\varphi_\mu(x)$ soit égal à $2x^m$; il s'ensuit que λ est un nombre rationnel, et, par conséquent, on a

$$Y = \lambda\varphi_\mu(x), \quad Z = \pm\lambda\psi_\mu(x).$$

Il résulte de l'équation (2) que $f_\mu(x)$ est le quotient et $\varphi_\mu(x)$ le reste de la division de $S(x)\psi_\mu(x)$ par X; on trouvera donc $\varphi_\mu(x)$, lorsque $\psi_\mu(x)$ sera connu.

Nous allons maintenant déduire les équations linéaires

auxquelles satisfont les coefficients de la fonction $\psi_\mu(x)$. Décomposons à cet effet la fraction $\frac{\varphi_\mu(x)S(x)}{X}$ en fractions simples, après avoir séparé préalablement la partie entière, nous aurons

$$\frac{\psi_\mu(x)S(x)}{X} = f_\mu(x) + \sum \frac{A_i}{x - r^i},$$

où

$$A_i = \frac{\psi_\mu(r^i)S(r^i)}{X_i'},$$

X_i' étant la valeur de la dérivée de X pour $x = r^i$, ou bien

$$\frac{\psi_\mu(x)S(x)}{X} - f_\mu(x) = \frac{\varphi_\mu(x)}{X} = \sum \frac{A_i}{x - r^i}.$$

En remarquant que la fonction $\frac{\varphi_\mu(x)}{X}$ est de degré $-m$, on voit que le développement de la fonction

$$\sum \frac{A_i}{x - r^i},$$

suivant les puissances descendantes de x, ne doit pas contenir les termes

$$x^{-1}, \quad x^{-2}, \ldots, \quad x^{-m+1};$$

on a donc les conditions

$$(5) \qquad \begin{cases} \Sigma A_i = 0, \\ \Sigma r^i A_i = 0, \\ \Sigma r^{2i} A_i = 0, \\ \cdots\cdots\cdots, \\ \Sigma r^{(m-2)i} A_i = 0. \end{cases}$$

Nous allons maintenant transformer l'expression A_i. On a d'abord

$$X' = \frac{d}{dx}\frac{x^p - 1}{x - 1} = \frac{(p-1)x^p - p x^{p-1} + 1}{(x-1)^2},$$

et, par suite, pour $x = r^i$,

$$X'_i = \frac{p(1 - r^{i(p-1)})}{(r^i - 1)^2} = \frac{p}{r^i(r^i - 1)};$$

on a ensuite

$$S(r^i) = \left(\frac{i}{p}\right) S(r) \ldots; \tag{6}$$

ainsi

$$A_i = \frac{S(r)}{p}\left(\frac{i}{p}\right) r^i (r^i - 1)\psi_\mu(r^i).$$

Si l'on remplace dans les équations (5) A_i par sa valeur, elles deviennent

$$\sum \left(\frac{i}{p}\right) r^i (r^i - 1)\psi_\mu(r^i) = 0,$$

$$\sum \left(\frac{i}{p}\right) r^{2i} (r^i - 1)\psi_\mu(r^i) = 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$\sum \left(\frac{i}{p}\right) r^{(m-1)i} (r^i - 1)\psi_\mu(r^i) = 0.$$

En posant

$$\psi_\mu(x) = C_0 + C_1 x + C_2 x^2 + \ldots + C_{m-1} x^{m-1},$$

c'est-à-dire

$$\psi_\mu(r^i) = C_0 + C_1 r^i + C_2 r^{2i} + \ldots + C_{m-1} r^{(m-1)i},$$

et ayant égard à la formule (6), on arrive aux équations

$$(7)\quad \begin{cases} \left[\left(\frac{2}{p}\right)-\left(\frac{1}{p}\right)\right]C_0+\left[\left(\frac{3}{p}\right)-\left(\frac{2}{p}\right)\right]C_1+\dots \\ \qquad\qquad +\left[\left(\frac{m+1}{p}\right)-\left(\frac{m}{p}\right)\right]C_{m-1}=0, \\ \left[\left(\frac{3}{p}\right)-\left(\frac{2}{p}\right)\right]C_0+\left[\left(\frac{4}{p}\right)-\left(\frac{3}{p}\right)\right]C_1+\dots \\ \qquad\qquad +\left[\left(\frac{m+2}{p}\right)-\left(\frac{m+1}{p}\right)\right]C_{m-1}=0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots, \\ \left[\left(\frac{m}{p}\right)-\left(\frac{m-1}{p}\right)\right]C_0+\left[\left(\frac{m+1}{p}\right)-\left(\frac{m}{p}\right)\right]C_1+\dots \\ \qquad\qquad +\left[\left(\frac{2m-1}{p}\right)-\left(\frac{2m-2}{p}\right)\right]C_{m-1}=0. \end{cases}$$

On voit, d'après ce qui précède, qu'en supposant $C_{m-1}=1$ et en déterminant les autres coefficients au moyen des équations (7), on a

$$Z=\psi_\mu(x).$$

Voici quelques exemples :

1. $$p=3,\quad m=1,\quad \psi_\mu(x)=1,$$

$$S(x)=\left(\frac{1}{3}\right)x+\left(\frac{2}{3}\right)x^2=x-x^2.$$

Le reste de la division de $S(x)\psi_\mu(x)$ par x^2+x+1 est

$$2x+1;$$

donc

$$\varphi_\mu(x)=Y=2x+1.$$

2. $$p=5,\quad \psi_\mu(x)=C_0+x,$$

où C_0 se détermine par l'équation

$$\left[\left(\frac{2}{5}\right)-\left(\frac{1}{5}\right)\right]C_0+\left[\left(\frac{3}{5}\right)-\left(\frac{2}{5}\right)\right]=0;$$

par conséquent $C_0=0$,

$$S(x)=x-x^2-x^3+x^4.$$

Le reste de la division de $S(x)\psi_{\mu}(x)$ par

$$x^4+x^3+x^2+x+1$$

est

$$2x^2+x+2;$$

donc, dans ce cas, on aura

$$Y=2x^2+x+2, \quad Z=x.$$

3. $p=7, \quad m=3, \quad \psi_{\mu}(x)=C_0+C_1x+x^2,$

où, pour déterminer C_0 et C_1, on a les équations

$$\left[\left(\frac{2}{7}\right)-\left(\frac{1}{7}\right)\right]C_0+\left[\left(\frac{3}{7}\right)-\left(\frac{2}{7}\right)\right]C_1+\left[\left(\frac{4}{7}\right)-\left(\frac{3}{7}\right)\right]=0,$$
$$\left[\left(\frac{3}{7}\right)-\left(\frac{2}{7}\right)\right]C_0+\left[\left(\frac{4}{7}\right)-\left(\frac{3}{7}\right)\right]C_1+\left[\left(\frac{5}{7}\right)-\left(\frac{4}{7}\right)\right]=0,$$

c'est-à-dire les équations

$$-C_1+1=0, \quad -C_0+C_1-1=0,$$

d'où

$$C_0=0, \quad C_1=1,$$

$$\psi_{\mu}(x)=x^2+x=Z, \quad S(x)=x+x^2-x^3-x^4-x^5-x^6.$$

Le reste de la division de $S(x)\psi_{\mu}(x)$ par X est

$$2x^3+x^2-x-2;$$

donc

$$Y=2x^3+x^2-x-2.$$

4. $p=11, \quad m=5,$

$$\psi_{\mu}(x)=C_0+C_1x+C_2x^2+C_3x^3+x^4.$$

Les équations par lesquelles on détermine C_0, C_1, C_2 sont

$$\left[\left(\frac{2}{11}\right)-\left(\frac{1}{11}\right)\right]C_0+\left[\left(\frac{3}{11}\right)-\left(\frac{2}{21}\right)\right]C_1$$
$$+\left[\left(\frac{4}{11}\right)-\left(\frac{3}{11}\right)\right]C_2+\left[\left(\frac{5}{11}\right)-\left(\frac{4}{11}\right)\right]C_3$$
$$+\left[\left(\frac{6}{11}\right)-\left(\frac{5}{11}\right)\right]=0,$$

$$\left[\left(\frac{3}{11}\right)-\left(\frac{2}{11}\right)\right]C_0+\left[\left(\frac{4}{11}\right)-\left(\frac{3}{11}\right)\right]C_1$$
$$+\left[\left(\frac{5}{11}\right)-\left(\frac{4}{11}\right)\right]C_2+\left[\left(\frac{6}{11}\right)-\left(\frac{5}{11}\right)\right]C_3$$
$$+\left[\left(\frac{7}{11}\right)-\left(\frac{6}{11}\right)\right]=0,$$

$$\left[\left(\frac{4}{11}\right)-\left(\frac{3}{11}\right)\right]C_0+\left[\left(\frac{5}{11}\right)-\left(\frac{4}{11}\right)\right]C_1$$
$$+\left[\left(\frac{6}{11}\right)-\left(\frac{5}{11}\right)\right]C_2+\left[\left(\frac{7}{11}\right)-\left(\frac{6}{11}\right)\right]C_3$$
$$+\left[\left(\frac{8}{11}\right)-\left(\frac{7}{11}\right)\right]=0,$$

$$\left[\left(\frac{5}{11}\right)-\left(\frac{4}{11}\right)\right]C_0+\left[\left(\frac{6}{11}\right)-\left(\frac{5}{11}\right)\right]C_1$$
$$+\left[\left(\frac{7}{11}\right)-\left(\frac{6}{11}\right)\right]C_2+\left[\left(\frac{8}{11}\right)-\left(\frac{7}{11}\right)\right]C_3$$
$$+\left[\left(\frac{9}{11}\right)-\left(\frac{8}{11}\right)\right]=0,$$

c'est-à-dire

$$-C_0+C_1-1=0,\quad C_0-C_3=0,\quad -C_2=0,\quad -C_1+1=0,$$

d'où l'on a

$$C_0=0,\quad C_1=0,\quad C_2=0,\quad C_3=0,$$
$$\psi_\mu(x)=x^4+x=Z.$$

Le reste de la division de $\psi_\mu(x)S(x)$ par X sera

$$Y=2x^5+x^4+2x^2-x-2.$$