Polynômes de Cassels P_N et Q_N et résultant.

Références :
Cassels J., *A note on the division values of $\wp(u)$.* Proc. Cambridge Philos. Soc. 45, (1949), 167–172.
Lang S., *Elliptic curves and Diophantine analysis.* Springer, 1978.
Silverman J., *Arithmetic of elliptic curves.* Springer, 1986.

Soit E une courbe elliptique donnée par une équation de Weierstrass générale $f = 0$ de la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

à laquelle est associée (par Tate) les quantités

$b_2 = a_1^2 + 4a_2$, $\quad b_4 = 2a_4 + a_1a_3$, $\quad b_6 = a_3^2 + 4a_6$, $\quad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$

$c_4 = b_2^2 - 24b_4$, $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ et surtout

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Les quantités sont reliées par $c_4^3 - c_6^2 = 1728\Delta$ et l'invariant de la courbe se calcule par $j = c_4^3/\Delta$. L'équation $(*)$ homogeneisée en z i.e. $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$ définit une courbe projective irréductible (avec un unique point à l'infini $O_E = (0, 1, 0)$ qui est non singulier et a pour tangente $z = 0$) qui est lisse si et seulement si $\Delta \neq 0$.

On introduit les anneaux

$$R_0 := \mathbf{Z}[a_1, a_2, a_3, a_4, a_6] \quad \text{et} \qquad R := R_0[x, y] = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6, x, y]/(f).$$

Ecrivons $\pi : E \to \mathbf{P}^1$ le morphisme $(x, y) \mapsto x$. Le morphisme π identifie les points $P = (x, y)$ et $[-1](P) = (x, -y - a_1x - a_3)$. Comme $[-1]$ commute avec $[N]$, on dispose d'un morphisme F_N tel que le diagramme suivant commute:

$$\begin{array}{ccc} E & \xrightarrow{[N]} & E \\ \pi \downarrow & & \downarrow \pi \\ \mathbf{P}^1 & \xrightarrow{F_N} & \mathbf{P}^1 \end{array}$$

On sait, au moins depuis Cassels, exprimer par des formules de récurrence F_N comme une fraction rationnelle en x et écrire donc

$$x \circ [N] = \frac{P_N(x)}{Q_N(x)}$$

Les polynômes P_N et Q_N étant premiers entre eux si $\Delta \neq 0$.

Des considérations de factorisation dans R_0, $R_0[x]$, $R_0[x, y]$ et R (notamment le fait que $R_0^* = R^* = \{\pm 1\}$) montrent qu'il existe P_N, R_N et $\psi_N \in R$ tels que

$$[n](x, y) = \left(\frac{P_N}{\psi_N^2}, \frac{R_N}{\psi_N^3}\right).$$

Ceux-ci sont uniques si on impose la coprimalité et choisit disons +1 comme signe du coefficient "dominant" de ψ_N. Pour les déterminer on va partir de la formule (qui s'obtient par procédé de corde et tangente) :

$$x(P_1+P_2)-x(P_1-P_2)=-\frac{(2y_1+a_1x_1+a_3)(2y_2+a_1x_2+a_3)}{(x_2-x_1)^2}$$

et l'appliquer à $P_1=[m](P)$ et $P_2=[n](P)$, ce qui donne :

$$\frac{P_{m+n}}{\psi_{m+n}^2}-\frac{P_{m-n}}{\psi_{m-n}^2}=-\frac{\left(2\frac{R_m}{\psi_m^3}+a_1\frac{P_m}{\psi_m^2}+a_3\right)\left(2\frac{R_n}{\psi_n^3}+a_1\frac{P_n}{\psi_n^2}+a_3\right)}{\left(\frac{P_m}{\psi_m^2}-\frac{P_n}{\psi_n^2}\right)^2}$$

On en tire (en réduisant les numérateurs et dénominateurs) :

$$\begin{cases}\psi_{m+n}\psi_{m-n}=P_n\psi_m^2-P_m\psi_n^2 & \text{pour } m>n\\ P_{m-n}\psi_{m+n}^2-P_{m+n}\psi_{m-n}^2=\psi_n\psi_m(2R_m+a_1P_m\psi_m+a_3\psi_m^3)(2R_n+a_1P_n\psi_n+a_3\psi_n^3)\end{cases}$$

Le signe dans la première équation est choisi grâce aux conventions : en effet le coefficient dominant (voir plus loin) du membre de droite est m^2-n^2. Prenons $n=1$ dans la première équation, comme $P_1=x$ et $\psi_1=1$, on en tire

$$P_m=x\psi_m^2-\psi_{m+1}\psi_{m-1}.$$

Si l'on reporte les valeurs de P_m et P_n on obtient la relation de récurrence suivante

$$\psi_{m+1}\psi_{m-1}\psi_n^2-\psi_{n+1}\psi_{n-1}\psi_m^2=\psi_{m+n}\psi_{m-n}$$

qui entraîne les deux suivantes (choisir $m=N+1$, $n=N$, puis $m=N+1$, $n=N-1$) :

$$\left.\begin{array}{rcl}\psi_{2N+1} & = & \psi_{N+2}\psi_N^3-\psi_{N-1}\psi_{N+1}^3\\ \psi_2\psi_{2N} & = & \psi_N\left(\psi_{N+2}\psi_{N-1}^2-\psi_{N-2}\psi_{N+1}^2\right)\end{array}\right\}\quad\text{pour } N\geq 2$$

Ainsi, ayant calculé $\psi_1=1$, $\psi_2=2y+a_1x+a_3$, $\psi_3=3x^4+b_2x^3+3b_4+3b_6+b_8$, et

$$\psi_4=\psi_2\left(2x^6+b_2x^5+5b_4x^4+10b_6x^3+10b_8x^2+(b_2b_8-b_4b_6)x+(b_4b_8-b_6^2)\right)$$

on en tirera tous les autres (on peut aussi poser par convention $\psi_0=0$). On peut utiliser la formule $\psi_3=xQ_2-P_2$ pour obtenir ψ_3 à partir de la formule de duplication donnée par

$$x\circ[2]=\frac{P_2}{Q_2}=\frac{P_2}{(2y+a_1x+a_3)^2}=\frac{x^4-b_4x^2-2b_6x-b_8}{4x^3+b_2x^2+2b_4x+b_6}$$

Enfin si on exploite l'autre relation en fixant $n=1$ (donc $R_1=y$) on obtient

$$\begin{aligned}\psi_m(2R_m+a_1P_m\psi_m+a_3\psi_m^3)(2y+a_1x+a_3) &= -P_{m+1}\psi_{m+1}^2+P_{m-1}\psi_{m+1}^2\\ &= \psi_m(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2)\end{aligned}$$

d'où une équation permettant de calculer les R_N dans l'anneau R :

$$(2R_m + a_1P_m\psi_m + a_3\psi_m^3)\psi_2 = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2$$

On peut préciser si ces "polynômes", *a priori* dans R, sont en fait dans $R_0[x]$ ou $\psi_2 R_0[x]$ et calculer leurs coefficients dominants. Ainsi $\psi_m \in R$ et plus précisément $\psi_m = mx^{\frac{m^2-1}{2}} + \ldots \in R_0[x]$ (pour m impair) et $\psi_m = \psi_2(\frac{m}{2}x^{\frac{m^2}{2}-2} + \ldots) \in \psi_2 R_0[x]$ (pour m pair). Alors $P_N := x\psi_N^2 - \psi_{N+1}\psi_{N-1} = x^{N^2} + \ldots \in R_0[x]$ et $Q_N = \psi_N^2 = N^2x^{N^2-1} + \ldots \in R_0[x]$. Quant à R_N, posons $\tilde{R}_N := 2R_N + a_1P_N\psi_N + a_3\psi_N^3$, on trouve $\tilde{R}_N = 2x^{\frac{3N^2}{2}} + \ldots \in R_0[x]$ (pour N pair) et $\tilde{R}_N = \psi_2\left(x^{\frac{3(N^2-1)}{2}} + \ldots\right) \in \psi_2 R_0[x]$ (pour N impair).

On a aussi "N divise M implique ψ_N divise ψ_M" dans R, en effet $\psi_N = 0$ ou $P_N = \psi_N^2 = 0$ donne l'équation sans multiplicité des points de torsion non nuls et annulés par N, les racines de P_N sont donc aussi racines de P_M et ψ_N^2 divise ψ_M^2 dans $R_0[x]$ donc ψ_N divise ψ_M dans R; en particulier $\psi_{2N} = \psi_2\tilde{\psi}_{2N}$. On peut en déduire une "factorisation":

$$\psi_N = \prod_{d\,|\,N} \psi_d^* \qquad \text{et bien sûr} \quad P_N = \prod_{d\,|\,N} P_N^*.$$

Si on note μ la fonction de Moebius, $\psi_d^* \in R$ peut être défini par $\psi_N^* := \prod_{d\,|\,N} \psi_d^{\mu(N/d)}$ et bien sûr $P_N^* = \psi_N^*$.

Revenons au calcul de R_N en définissant U_N, $V_N \in R_0[x]$ par

$$R_N := U_N + yV_N.$$

En se souvenant de la factorisation $\psi_{2M} = \psi_2\tilde{\psi}_{2M}$ et la formule donnant $\tilde{R}_N$ on obtient

$$\begin{aligned} U_N &= \frac{1}{2}\left\{\tilde{\psi}_{N+2}\psi_{N-1}^2 - \tilde{\psi}_{N-2}\psi_{N+1}^2 - (a_1P_N + a_3Q_N)\tilde{\psi}_N\right\} \\ V_N &= -\tilde{\psi}_N\,(a_1P_N + a_3Q_N) \end{aligned} \qquad \text{pour } N \text{ pair}$$

ainsi que

$$\begin{aligned} U_N &= \frac{1}{2}\left\{\left(\psi_{N+2}\tilde{\psi}_{N-1}^2 - \psi_{N-2}\tilde{\psi}_{N+1}^2\right)(a_1x + a_3) - (a_1P_N + a_3Q_N)\psi_N\right\} \\ V_N &= -\tilde{\psi}_N(a_1P_N + a_3Q_N) \end{aligned} \qquad \text{pour } N \text{ impair}$$

En particulier

$$\begin{aligned} U_2 &= \frac{1}{2}\left(\tilde{\psi}_4 - (a_1P_2 + a_3Q_2)(a_1x + a_3)\right) \\ &= x^6 + 2a_2x^5 + 5a_4x^4 + C_6x^3 + D_8x^2 + E_{10}x + F_{12} \\ V_2 &= -a_1P_2 - a_3Q_2 \\ &= -a_1x^4 - 4a_3x^3 - (a_3b_2 - a_1b_4)x^2 - 2(a_3b_4 - a_1b_6)x - (a_3b_6 - a_1b_8) \end{aligned}$$

avec

$$\begin{aligned}
C_6 &:= 3a_3^2 + 4a_6 - 2a_1a_2a_3 + a_1^2a_4,\\
D_8 &:= 5b_8 - a_1(a_3b_4 - a_1b_6) - a_3(2a_2a_3 - a_1a_4),\\
E_{10} &:= a_3(a_3b_4 - a_1b_6) + b_8(2a_2 + a_1^2) - b_6(a_4 + a_1a_3),\\
F_{12} &:= b_8(a_4 + a_1a_3) - 2b_6(a_6 + a_3^2).
\end{aligned}$$

Homogéneïté. On attribue le poids i à a_i, 2 à x et 3 à y, alors toutes les formules deviennent homogènes : l'équation $(*)$ est de poids 6, Δ est de poids 12, ψ_N est de poids N^2-1, $P_N = x^{N^2} + \ldots$ est de poids $2N^2$, alors que $Q_N = N^2X^{N^2-1} + \ldots + q_{N,0}$ est de poids $2(N^2-1)$ et R_N de poids $3N^2$. Ces considérations permettent de calculer par exemple le *résultant* de P_N et Q_N.

Proposition. *On a la formule suivante (pour $N \geq 1$)*

$$\mathrm{Res}(P_N, Q_N) = \pm\Delta^{\lambda(N)}$$

où $\lambda(N) = N^2(N^2-1)/6$.

Remarque. En particulier si $a_1 = a_2 = a_3 = 0$ et le modèle de Weierstrass s'écrit $y^2 = x^3 + Ax + B$, on obtient $\Delta = -2^4(4A^3 + 27B^2)$ et

$$\mathrm{Res}(P_N, Q_N) = 2^{\frac{2N^2(N^2-1)}{3}} \left(4A^3 + 27B^2\right)^{\frac{N^2(N^2-1)}{6}}.$$

La preuve de la proposition résulte du fait que le membre de gauche est nul si et seulement si $\Delta = 0$ (pour chaque valeur des a_i), que c'est un polynôme en les a_i, i.e. un élément de R_0, que c'est un élément homogène si on attribue le poids i à a_i, le poids est celui de chacun des termes du développement du déterminant "résultant" donc par exemple celui de $q_{N,0}^{N^2}$ c'est-à-dire $2N^2(N^2-1)$. On en tire $\mathrm{Res}(P_N, Q_N) = c\Delta^{\lambda(N)}$ avec donc $2N^2(N^2-1) = 12\lambda(N)$. Enfin la formule obtenu devant être valable pour toute spécialisation, y compris en caractéristique p; on voit que c, *a priori* entier non nul, est en fait inversible et donc $c = \pm 1$.