

Quelques exemples de factorisations de fonctions zêta

Philippe GOUTET

exposé donné le 21 février 2007 ; version remaniée du 8 juin 2011

Résumé. Étant donné $f \in \mathbb{F}_q[x_1, \dots, x_n]$, on cherche à calculer le nombre de zéros de f sur tous les $\mathbb{F}_{q^r}$ d'un seul coup. Cela est par exemple possible si on peut calculer explicitement la fonction zêta de l'hypersurface $f = 0$. Après avoir donné quelques exemples où ce calcul explicite est possible et après avoir rappelé les conjectures de Weil (qui décrivent la forme générale des fonctions zêta), on s'intéressera à l'apparition, dans une fonction zêta donnée, de facteurs provenant d'autres fonctions zêta sur les exemples des courbes de Fermat $x^d + y^d = z^d$ et des hypersurfaces de Dwork $x_1^n + \dots + x_n^n - n\psi x_1 \dots x_n = 0$ où ψ est un paramètre.

1 Notion de fonction zêta

Soit $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$. On note $X : f(x_1, \dots, x_n) = 0$ l'hypersurface correspondante. Par définition, le nombre de points de X sur $\mathbb{F}_{q^r}$ est le nombre de zéros de f dans $\mathbb{F}_{q^r}^n$ (ou dans $\mathbb{P}_{\mathbb{F}_{q^r}}^n$ si f est homogène) ; on le note $|X(\mathbb{F}_{q^r})|$. La fonction zêta de l'hypersurface X est définie par :

$$Z_{X/\mathbb{F}_q}(t) = \exp\left(\sum_{r=1}^{+\infty} |X(\mathbb{F}_{q^r})| \frac{t^r}{r}\right).$$

Elle est simplement reliée à la fonction génératrice du nombre de zéros de f dans les $\mathbb{F}_{q^r}$ par la formule :

$$\frac{d}{dt} \left(\log Z_{X/\mathbb{F}_q}(t) \right) = G_{X/\mathbb{F}_q}(t) \quad \text{où} \quad G_{X/\mathbb{F}_q}(t) = \sum_{r=1}^{+\infty} |X(\mathbb{F}_{q^r})| t^{r-1}.$$

La raison pour laquelle on s'intéresse à la fonction zêta plutôt qu'à la fonction génératrice est que la fonction zêta vérifie un certain nombre de propriétés supplémentaires (conjectures de Weil, aujourd'hui démontrées ; voir § 3).

2 Exemples de fonctions zêta

On commence par deux exemples triviaux (espace affine et espace projectif) puis on donne quatre exemples plus évolués (courbes elliptiques, courbes projectives lisses, grassmanniennes et hypersurfaces diagonales). Pour plus de détails sur l'histoire des conjectures de Weil, voir [Hou02].

Fonction zêta de l'espace affine. Si on veut rester dans le cadre précédent des fonctions zêta d'hypersurfaces, on peut voir l'espace affine comme l'hypersurface définie par le polynôme identiquement nul et :

$$|\mathbb{A}_{\mathbb{F}_{q^r}}^n| = (q^r)^n.$$

Par suite :

$$\begin{aligned} Z_{\mathbb{A}_{\mathbb{F}_q}^n}(t) &= \exp\left(\sum_{r=1}^{+\infty} (q^r)^n \frac{t^r}{r}\right) = \exp\left(\sum_{r=1}^{+\infty} \frac{(q^n t)^r}{r}\right) = \exp\left(-\log(1 - q^n t)\right) \\ &= \frac{1}{1 - q^n t}. \end{aligned}$$

Fonction zêta de l'espace projectif. Rappelons que l'espace projectif $\mathbb{P}^n$ est défini par $\mathbb{P}^n = (\mathbb{A}^{n+1} \setminus \{0\})/\mathbb{F}_q^*$. Comme pour l'espace affine, si on veut rester dans le cadre des hypersurfaces décrit précédemment, on peut considérer l'espace projectif comme correspondant à l'hypersurface définie par le polynôme identiquement nul, mais on compte le nombre de points projectivement (c'est-à-dire qu'on identifie tous les points non nuls sur une même droite) et donc :

$$|\mathbb{P}_{\mathbb{F}_{q^r}}^n| = \frac{(q^r)^{n+1} - 1}{q^r - 1} = 1 + q^r + (q^r)^2 + \dots + (q^r)^n,$$

Ainsi :

$$\begin{aligned} Z_{\mathbb{P}_{\mathbb{F}_q}^n}(t) &= \exp\left(\sum_{r=1}^{+\infty} (1 + q^r + (q^r)^2 + \dots + (q^r)^n) \frac{t^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{+\infty} \frac{t^r}{r}\right) \exp\left(\sum_{r=1}^{+\infty} \frac{(qt)^r}{r}\right) \dots \exp\left(\sum_{r=1}^{+\infty} \frac{(q^n t)^r}{r}\right) \\ &= \exp\left(-\log(1 - t)\right) \exp\left(-\log(1 - qt)\right) \dots \exp\left(-\log(1 - q^n t)\right) \\ &= \frac{1}{(1 - t)(1 - qt) \dots (1 - q^n t)}. \end{aligned}$$

Fonction zêta d'une courbe elliptique. Soit E une courbe elliptique sur $\mathbb{Q}$ (donc une courbe projective et non singulière), disons donnée par une équation affine explicite $y^2 = x^3 + ax + b$ où $a, b \in \mathbb{Q}$. Il existe un nombre fini de p premiers divisant le dénominateur de a et b (écrits sous forme irréductible). Cela a donc un sens de considérer E sur $\mathbb{F}_p$ pour une infinité de nombre premier p .

Pour de tels nombres premiers, Hasse [Has36] a montré en 1936 que la fonction zêta de E était de la forme suivante :

$$Z_{E/\mathbb{F}_q}(t) = \frac{1 - a_q t + q t^2}{(1 - t)(1 - qt)} = \frac{(1 - \pi_q t)(1 - \bar{\pi}_q t)}{(1 - t)(1 - qt)},$$

où $\pi_q, \bar{\pi}_q \in \mathbb{C}$ sont des nombres algébriques conjugués de valeur absolue $\sqrt{q}$ et donc :

$$\left| |E(\mathbb{F}_q)| - (q + 1) \right| = |a_q| \leq 2\sqrt{q}. \quad (\text{majoration de Hasse-Weil})$$

Il a récemment été montré que, lorsque $q = p$, ce coefficient a_p était en fait le p -ième coefficient de Fourier d'une forme modulaire de poids 2. On verra d'autres exemples de phénomènes de modularité au § 4.

Fonction zêta d'une courbe. Soit $\mathcal{C}$ une courbe projective non singulière de genre g définie sur $\mathbb{F}_q$. Weil a montré en 1940 (voir [Wei40] pour l'annonce et le livre [Wei48] pour une démonstration complète) que la fonction zêta de $\mathcal{C}$ était de la forme :

$$Z_{\mathcal{C}/\mathbb{F}_q}(t) = \frac{P(t)}{(1 - t)(1 - qt)},$$

où le polynôme $P(t)$ est dans $1 + t\mathbb{Z}[t]$, a pour degré $2g$ et les inverses de ses racines ont pour valeur absolue $\sqrt{q}$. On en déduit la majoration suivante :

$$\left| |\mathcal{C}(\mathbb{F}_q)| - (q+1) \right| \leq 2g\sqrt{q}. \quad (\text{majoration de Hasse-Weil})$$

Fonction zêta d'une grassmannienne. La grassmannienne $G_{n,r}(\mathbb{F}_q)$ est la variété composée des sous-espaces de dimension r dans l'espace affine de dimension n . Contrairement aux exemples précédents, on ne peut pas considérer que c'est une hypersurface, mais la fonction zêta se définit de la même manière ; le nombre de points de cette variété est juste le nombre de sous-espaces vectoriels de dimension r dans $\mathbb{F}_q^n$:

$$|G_{n,r}(\mathbb{F}_q)| = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{r-1})}{(q^r - 1)(q^r - q) \dots (q^r - q^{r-1})}.$$

Par exemple :

$$|G_{4,2}(\mathbb{F}_q)| = \frac{(q^4 - 1)(q^3 - q)}{(q^2 - 1)(q^2 - q)} = (q^2 + 1)(q^2 + q + 1) = q^4 + q^3 + 2q^2 + q + 1.$$

En fait, on peut montrer que $|G_{n,r}(\mathbb{F}_q)|$ est toujours un polynôme en q ; pour cela, il suffit d'utiliser la relation de récurrence suivante :

$$|G_{n,r}(\mathbb{F}_q)| = |G_{n-1,r}(\mathbb{F}_q)| + q^{n-r} |G_{n-1,r-1}(\mathbb{F}_q)|,$$

puis raisonner par récurrence pour obtenir :

$$|G_{n,r}(\mathbb{F}_q)| = b_0 + b_1 q + \dots + b_{n(n-r)} q^{n(n-r)}.$$

En fait, le coefficient b_i est égal au nombre de r -uplets $0 \leq k_1 \leq \dots \leq k_r \leq n - r$ tels que $k_1 + \dots + k_r = i$ (voir [And76, § 3.3 p. 35-34 et § 13.2 p. 212-214]). On reconnaît les nombres de Betti de la grassmannienne complexe tels qu'ils ont été calculés par Ehresmann [Ehr34, théorème p. 409]. À titre d'exemple, on peut écrire explicitement les partitions correspondant aux différents entiers b_i de $G_{4,2}(\mathbb{F}_q)$:

NOMBRES DE BETTI	$b_0 = 1$	$b_1 = 1$	$b_2 = 2$	$b_3 = 1$	$b_4 = 1$
PARTITIONS	(0,0)	(0,1)	(0,2),(1,1)	(1,2)	(2,2)

Fonction zêta d'une hypersurface diagonale. Dans son célèbre article de 1949 [Wei49] (c'est l'article où il énonce ce que l'on appelle aujourd'hui les conjectures de Weil), Weil détermine la fonction zêta des hypersurfaces diagonales $D_\alpha : \alpha_1 x_1^d + \dots + \alpha_n x_n^d = 0$ lorsque $q \equiv 1 \pmod{d}$:

$$Z_{D_\alpha/\mathbb{F}_q}(t) = \frac{\prod_{\substack{1 \leq s_i \leq d-1 \\ n|s_1+\dots+s_n}} \left(1 - (-1)^{n-1} \chi^{-s_1}(\alpha_1) \dots \chi^{-s_n}(\alpha_n) J(\chi^{s_1}, \dots, \chi^{s_n}) t \right)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^{n-2}t)},$$

où $J(\chi^{s_1}, \dots, \chi^{s_n})$ est la somme de Jacobi

$$J(\chi^{s_1}, \dots, \chi^{s_n}) = \sum_{\substack{x_1, \dots, x_n \in \mathbb{F}_q \\ x_1 + \dots + x_n = 1}} \chi^{s_1}(x_1) \dots \chi^{s_n}(x_n),$$

le symbole χ désignant un caractère multiplicatif d'ordre d de $\mathbb{F}_q^*$ (prolongé par $\chi(0) = 0$). Une propriété importante des sommes de Jacobi précédentes est que $|J(\chi^{s_1}, \dots, \chi^{s_n})| = \sqrt{q^{n-2}}$ (le caractère χ étant supposé à valeurs dans $\mathbb{C}$). Si on calcule le degré du numérateur, on trouve $\frac{(d-1)^n + (-1)^n(d-1)}{d}$. Guidé par les exemples précédents, Weil a demandé à Dolbeault de calculer les nombres de Betti de l'hypersurface complexe $\alpha_1 x_1^d + \dots + \alpha_n x_n^d = 0$. Comme on peut s'y attendre, ces nombres sont $b_{n-2} = \frac{(d-1)^n + (-1)^n(d-1)}{d}$ et $b_i = 1$ ou 0 sinon (selon que $i \neq n-2$ est pair ou impair).

3 Conjectures de Weil

Les exemples précédents ont amené Weil à formuler les conjectures suivantes (voir [Wei49]).

Énoncé des conjectures de Weil. Soit X une variété algébrique projective lisse de dimension m définie sur $\mathbb{F}_q$. Il existe (*propriété de Lefschetz*) $2m + 1$ polynômes $P_0, \dots, P_{2m} \in 1 + t\mathbb{Z}[t]$ tels que :

$$Z_{X/\mathbb{F}_q}(t) = \frac{P_1(t)P_3(t) \dots P_{2m-1}(t)}{P_0(t)P_2(t) \dots P_{2d-2}(t)P_{2m}(t)},$$

où $P_0(t) = 1 - t$, $P_{2m}(t) = 1 - q^m t$ et, si on écrit $P_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{i,j}t)$ avec $\alpha_{i,j} \in \mathbb{C}$, les $\alpha_{i,j}$ vérifient l'hypothèse de Riemann suivante :

$$|\alpha_{i,j}| = q^{\frac{i}{2}}.$$

De plus, si on pose $\chi = \sum_{i=0}^{2m} (-1)^i b_i$ (où $b_i = \deg P_i$), la fonction zêta vérifie l'équation fonctionnelle suivante :

$$Z_{X/\mathbb{F}_q}\left(\frac{1}{q^m t}\right) = \pm q^{\frac{m\chi}{2}} t^\chi Z_{X/\mathbb{F}_q}(t).$$

Finalement, si X provient d'une variété complexe (par exemple, X est une hypersurface à coefficients entiers), les b_i sont les nombres de Betti de la variété complexe correspondante (et donc χ en est la caractéristique d'Euler-Poincaré).

REMARQUES. La rationalité a été montrée par Dwork en 1960 [Dwo60] pour des variétés quelconques (affines ou projectives, singulières ou non) grâce à des techniques p -adiques ; voir [Kob77, chap. 5]. La propriété de Lefschetz, l'équation fonctionnelle et l'interprétation des nombres de Betti ont été démontrées par Grothendieck et Michael Artin en 1963 ; voir [Gro64, Gro66]. Finalement, Deligne a montré l'hypothèse de Riemann en 1974 ; voir [Del74].

Cas d'une hypersurface. Dans le cas d'une hypersurface projective non singulière, on peut préciser un peu les conjectures de Weil. Soit X l'hypersurface de $\mathbb{P}^{n-1}$ définie par l'équation $f = 0$ avec $f \in \mathbb{F}_q[x_1, \dots, x_n]$ homogène de degré d et non singulier ; la dimension de X est $m = n - 2$. Dans ces conditions, Dwork [Dwo62, Dwo64] a montré qu'il existait un polynôme $P(t) \in 1 + t\mathbb{Z}[t]$ de degré $\frac{(d-1)^n + (-1)^n(d-1)}{d}$ tel que :

$$Z_{X/\mathbb{F}_q}(t) = \frac{P(t)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^{n-2}t)}.$$

L'hypothèse de Riemann permet de montrer que les inverses des racines de P sont toutes de valeur absolue $q^{\frac{n-2}{2}}$.

4 Quelques exemples du phénomène de factorisation

Concernant les fonctions zêta, disons d'hypersurfaces, un phénomène intéressant peut se produire : le polynôme $P(t)$ peut être produit de polynômes du type $P_1(q^{n_1}t), \dots, P_k(q^{n_k}t)$ où $P_1, \dots, P_k$ proviennent eux-mêmes de fonctions zêta d'autres hypersurfaces. On va voir trois exemples de ce phénomène : les courbes de Fermat, les hypersurfaces de Dwork, et une famille de surfaces K3.

Les courbes de Fermat. Considérons les courbes de Fermat $\mathcal{F}_d : x^d + y^d = z^d$; ce sont des hypersurfaces diagonales donc on connaît leurs fonctions zêta. Pour simplifier, on suppose que $q \equiv 1 \pmod{d}$. Commençons par examiner le cas $d = 4$; pour simplifier un peu le résultat, on considère la courbe projective $C : x^4 + y^4 + z^4 = 0$ plutôt que $x^4 + y^4 = z^4$. Sa fonction zêta est :

$$Z_{C/\mathbb{F}_q}(t) = \frac{(1 - a_q t + q t^2)^3}{(1 - t)(1 - q t)} \quad \text{avec} \quad Z_{E/\mathbb{F}_q}(t) = \frac{1 - a_q t + q t^2}{1 - q t},$$

où E est la courbe elliptique d'équation affine $y^2 = x^3 + x$; ce résultat est valable pour tout q , mais lorsque $q \equiv 3 \pmod{4}$, on a $a_q = 0$. Pour une démonstration de ce résultat, on pourra consulter [Sch03]; les méthodes utilisées sont complètement élémentaires (uniquement des sommes de Gauss, des sommes de Jacobi et quelques transformations géométriques).

Le point le moins évident dans ce genre de problème de facteurs de fonction zêta provenant d'autres hypersurfaces est de trouver de manière explicite les hypersurfaces qui interviennent. Dans ce cas précis (voir [Sch03]), si on regarde ce qui se passe sur $\mathbb{F}_5$, on trouve que le numérateur de la fonction zêta de $C : x^4 + y^4 + z^4 = 0$ est $(1 - 2t + 5t^2)^3$; cela suggère déjà que le numérateur est le cube du numérateur d'une certaine courbe elliptique. Pour trouver les candidats possibles, on regarde dans des tables et on voit que seules les courbes elliptiques d'équations affines $y^2 = x^3 + x$ et $y^2 = x^3 + x + 2$ ont pour numérateur de leur fonction zêta $1 - 2t + 5t^2$. Le calcul explicite des zéros de $y^2 = x^3 + x$ et de $x^4 + y^4 + z^4 = 0$ grâce aux sommes de Jacobi montre que c'est $y^2 = x^3 + x$ qui intervient et pas $y^2 = x^3 + x + 2$.

Revenons à la courbe $\mathcal{F}_d : x^d + y^d = z^d$. En général, il n'y a aucune raison que le numérateur de la fonction zêta de $\mathcal{F}_d$ soit un produit de numérateurs de fonctions zêta de courbes elliptiques; par exemple, si on fait les calculs explicites pour $d = 7$ et $q = 29$, on trouve :

$$\begin{aligned} Z_{\mathcal{F}_7/\mathbb{F}_{29}}(t) &= \frac{(1 + t - 27t^2 - 69t^3 - 783t^4 + 841t^5 + 24389t^6)^3(1 - 2t + 29t^2)^6}{(1 - t)(1 - 29t)} \\ &= \frac{P(t)^3 Q(t)^6}{(1 - t)(1 - 29t)}. \end{aligned}$$

Le polynôme P de degré 6 est irréductible sur $\mathbb{Q}$, donc ne provient pas d'une courbe elliptique. Par contre, c'est le cas du polynôme Q de degré 2 (voir ci-dessous).

Une chose remarquable dans le cas des courbes de Fermat est que l'on peut donner des équations explicites pour tous les facteurs composant le numérateur de la fonction zêta. Plus précisément, lorsque d est premier, Faddeev a montré que, sur $\mathbb{C}$, la jacobienne de $x^d + y^d = z^d$ est isogène au produit des jacobienes de courbes du type

$$H_{r,s} : y^d = x^r(1 - x)^s,$$

où r et s sont des entiers entre 1 et d tels que $r + s \not\equiv 0 \pmod{d}$ (voir [Roh78]). Ce résultat se transpose sur $\mathbb{F}_q$ (en supposant toujours que d est premier) : le numérateur de la fonction zêta se factorise en un produit de numérateurs de fonctions zêta de courbes du type précédent (lorsque d n'est pas premier, il faut faire un peu plus attention, car on peut devoir diviser par certains des facteurs). Pour trouver les entiers r et s qui interviennent, on procède comme suit (voir [GR78, p. 202]). On énumère, à permutation près, l'ensemble des (s_1, s_2, s_3) tels que $1 \leq s_i \leq d - 1$ et $s_1 + s_2 + s_3 \equiv 0 \pmod{d}$. Une fois fait, on les regroupe sous l'action de $(\mathbb{Z}/d\mathbb{Z})^\times$ définie par $k \cdot (s_1, s_2, s_3) = (ks_1, ks_2, ks_3)$. À chaque classe d'équivalence $[s_1, s_2, s_3]$ correspond la courbe

$$y^d = x^{s_1}(1 - x)^{s_2}.$$

Quitte à choisir le représentant de $[s_1, s_2, s_3]$, on peut toujours supposer que $s_1 = 1$.

EXEMPLE. Considérons le cas $d = 7$. On trouve :

$[s_1, s_2, s_3]$	NOMBRE DE PERMUTATIONS	ÉQUATION
$[1, 1, 5]$	3	$y^7 = x(1 - x)$
$[1, 2, 4]$	6	$y^7 = x(1 - x)^2$

Les techniques de sommes de Jacobi exposées dans [GR78, p. 202] permettent de montrer que les fonctions zêta de $H_{1,1} : y^7 = x(1 - x)$ et $H_{1,2} : y^7 = x(1 - x)^2$ sont

$$Z_{H_{1,1}/\mathbb{F}_q}(t) = \frac{P(t)}{1 - qt} \quad \text{et} \quad Z_{H_{1,2}/\mathbb{F}_q}(t) = \frac{Q(t)^3}{1 - qt},$$

où $P(t)$ est de degré 6 et $Q(t)$ de degré 2. Comme on s'y attend, le facteur $Q(t)$ provient d'une courbe elliptique sur $\mathbb{Q}$. Pour le voir, on peut remarquer que $H_{1,2} : y^7 = x(1 - x)^2$ est birationnelle à la courbe de Klein $x^3y + y^3z + z^3x = 0$ (voir [Elk99, p. 67]) ; on obtient alors la courbe elliptique en question comme un quotient (voir [Elk99, p. 68]). L'équation affine que l'on trouve pour cette courbe elliptique est $y^2 = 4x^3 + 21x^2 + 28x$. Il reste ensuite à montrer que $Q(t)$ est bien le numérateur de la fonction zêta de la courbe elliptique en question.

REMARQUE. Le phénomène d'apparition de facteurs provenant de courbes elliptiques dans les courbes de Fermat qu'on a constaté pour $d = 4$ et $d = 7$ peut être complètement décrit. Koblitz [Kob78] a élucidé les cas pour lesquels la jacobienne des courbes de Fermat sur $\overline{\mathbb{Q}}$ font apparaître des facteurs provenant de courbes elliptiques et il est facile d'adapter ces résultats aux corps finis. Plus précisément, on peut ainsi montrer qu'il existe un facteur qui provient d'une courbe elliptique uniquement pour les courbes de Fermat dont le degré est un multiple d'un des nombres suivants :

3, 4, 6, 7, 8, 12.

(Les nombres de la liste précédente correspondent aux cas primitifs ; par exemple, $x^{21} + y^{21} = z^{21}$ héritera des courbes elliptiques de $x^3 + y^3 = z^3$ et $x^7 + y^7 = z^7$; quant à $x^{12} + y^{12} = z^{12}$, en plus des courbes elliptiques héritées de $x^3 + y^3 = z^3$ et $x^4 + y^4 = z^4$, elle en aura de nouvelles.)

La famille X_ψ : $x_1^n + \dots + x_n^n - n\psi x_1 \dots x_n = 0$. Cette famille de variété a été étudiée par Wan [Wan04] ; on suppose que $n \geq 3$. En tant qu'hypersurface, sa fonction zêta a pour forme

$$Z_{X_\psi/\mathbb{F}_q}(t) = \frac{P(t)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^{n-2}t)},$$

où $P \in 1 + t\mathbb{Z}[t]$ est un polynôme de degré $\frac{(n-1)^n + (-1)^n(n-1)}{n}$ dont les inverses des racines ont pour valeur absolue $\sqrt{q^{n-2}}$. Pour trouver la factorisation de $P(t)$, on quotiente X_ψ . Plus précisément, soit G le groupe $\{(\zeta_1, \dots, \zeta_n) \in \mu_n^n \mid \zeta_1 \dots \zeta_n = 1\} / \{(\zeta, \dots, \zeta)\}$ qui agit de manière naturelle sur X_ψ via

$$(\zeta_1, \dots, \zeta_n) \cdot (x_1, \dots, x_n) = (\zeta_1 x_1, \dots, \zeta_n x_n).$$

Notons Y_ψ le quotient de X_ψ par G . C'est une variété singulière mais on peut calculer sa fonction zêta (voir [Wan04, éq. (14)]) :

$$Z_{Y_\psi/\mathbb{F}_q}(t) = \frac{Q(t)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^{n-2}t)},$$

où $Q \in 1 + t\mathbb{Z}[t]$ est un polynôme de degré $n - 1$ dont les inverses des racines ont pour valeurs absolues $\sqrt{q^{n-2}}$. Lorsque $n|q - 1$ (voir [Wan04, th. 7.3]) ou lorsque n est premier (voir [Hae04, th. 9.5]), on peut montrer que :

$$\frac{P(t)}{Q(t)} = R(qt),$$

où $R \in 1 + t\mathbb{Z}[t]$ est un polynôme de degré $\frac{(n-1)^n + (-1)^n(n-1)}{n} - (n-1)$ dont les inverses des racines ont pour valeur absolue $\sqrt{q^{n-4}}$ (si $n \geq 4$). Il semblerait donc naturel que R proviennent de « numérateurs » de fonctions zêta de variétés de dimension $\leq n-3$. Wan dresse l'état des connaissances en la matière.

CAS $n = 3$. Le facteur R est de degré $\frac{2^3 + (-1)^3 2}{3} - 2 = 0$ donc est égal à 1. Le seul facteur de la fonction zêta est donc le miroir. En fait, on est en présence d'une courbe de genre 1, c'est-à-dire d'une courbe elliptique. On peut la mettre sous une forme un peu plus usuelle, à savoir

$$y^2 - 3\psi xy + 9y = x^3 - 27(\psi^3 + 1).$$

Il n'y a pas de phénomène de factorisation car la fonction zêta est celle d'une courbe elliptique sur $\mathbb{Q}$:

$$Z_{X_\psi/\mathbb{F}_q}(t) = \frac{1 - a_q t + q t^2}{(1-t)(1-qt)}, \quad \text{avec } a_q \in \mathbb{Z}.$$

CAS $n = 4$. Le facteur R est de degré $\frac{3^4 + (-1)^4 3}{4} - 3 = 21 - 3 = 18$ et devrait normalement provenir de variétés de dimension 0 (c'est-à-dire de points). C'est bien le cas, comme Dwork l'a montré [Dwo69, § 6.j], p. 75] : le polynôme R est un produit de facteurs linéaires $(1 \pm t)$. Kadir [Kad04, § 6.1 p. 109-116] a fait des calculs explicites pour $p \leq 41$. Par exemple, lorsque $p \equiv 1 \pmod{4}$ et $\psi = 0$, on peut montrer que :

$$Z_{X_\psi/\mathbb{F}_p}(t) = \frac{1}{(1-t)(1-pt)(1-p^2t)} \cdot \frac{1}{(1-pt)(1-ap_t+p^2t^2)(1-(-1)^{(p^2-1)/8}pt)(1-p^2t^2)^{12}}.$$

Les calculs de Kadir semblent indiquer que le coefficient a_p provient d'une forme modulaire de poids 3 et de niveau 16. Voir http://modular.fas.harvard.edu/cgi-bin/mfd/mfe_eigenvalues.py?code=16k3A%5B1,0%5D1 pour les 100 premiers coefficients.

CAS $n = 5$. Cette fois-ci, R est de degré 200. Candelas, de la Ossa et Rodriguez-Villegas [CdlORV03] ont trouvé numériquement une correspondance entre ce facteur et un produit $P_{\mathcal{A}}^{10} P_{\mathcal{B}}^{15}$ (lorsque $\psi \neq 0$) où $P_{\mathcal{A}}$ et $P_{\mathcal{B}}$ sont des polynômes de degré 8 provenant du numérateur des deux courbes dont les équations sont $\mathcal{A} : y^5 = x^2(1-x)^3(1 - \frac{1}{\psi^5}x)^2$ et $\mathcal{B} : y^5 = x^2(1-x)^4(1 - \frac{1}{\psi^5}x)$ respectivement :

$$Z_{\mathcal{A}/\mathbb{F}_q}(t) = \frac{P_{\mathcal{A}}(t)}{1-qt} \quad \text{et} \quad Z_{\mathcal{B}/\mathbb{F}_q}(t) = \frac{P_{\mathcal{B}}(t)}{1-qt}.$$

De plus, lorsque $\psi^5 = 1$ (c'est-à-dire que l'hypersurface est singulière), alors un résultat de Schoen [Sch86] permet de montrer (voir [CdlORV03]) que, lorsque $q = p$, $Q(t) = (1 - \varepsilon pt)(1 - a_p t + p^3 t^2)$ où $\varepsilon = (\frac{5}{p})$ (symbole de Legendre) et où a_p est le p -ième terme du développement de Fourier d'une la forme modulaire de poids 4 et de niveau 25 que l'on peut exprimer en termes de la fonction η de Dedekind (voir [CdlORV03, § 12.1] et [Sch86, p. 109-110]) :

$$\begin{aligned} f(q) &= \eta(q^5)^4 \left(\eta(q)^4 + 5\eta(q)^3 \eta(q^{25}) + 20\eta(q)^2 \eta(q^{25})^2 + 25\eta(q) \eta(q^{25})^3 + 25\eta(q^{25})^4 \right) ; \\ &= q + q^2 + 7q^3 - 7q^4 + 7q^6 + 6q^7 - 15q^8 + 22q^9 - 43q^{11} - 49q^{12} - 28q^{13} \\ &\quad + 6q^{14} + 41q^{16} + 91q^{17} + 22q^{18} - 35q^{19} + 42q^{21} - 43q^{22} + 162q^{23} - 105q^{24} \\ &\quad - 28q^{26} - 35q^{27} - 42q^{28} + 160q^{29} + 42q^{31} + 161q^{32} - 301q^{33} + 91q^{34} \\ &\quad - 154q^{36} - 314q^{37} - 35q^{38} - 196q^{39} - 203q^{41} + 42q^{42} + 92q^{43} + 301q^{44} \\ &\quad + 162q^{46} + 196q^{47} + 287q^{48} - 307q^{49} + 637q^{51} + 196q^{52} + 82q^{53} + \dots \end{aligned}$$

Schoen a montré ce résultat en montrant que la fonction L du H^3 de l'hypersurface était la fonction L de la forme modulaire en question.

CAS GÉNÉRAL. La question de trouver les variétés dont le facteur R provient pour $n \geq 6$ est mentionnée comme ouverte par Wan.

Une surface K3. Voici maintenant un exemple dû à Ahlgren, Ono et Penniston [AOP02]. Ils ont montré que la fonction zêta (affine) de $S_\lambda : z^2 = xy(x+1)(y+1)(x+\lambda y)$ est de la forme

$$Z_{S_\lambda/\mathbb{F}_p}(t) = \frac{1}{(1-p^2t)(1-\varepsilon pt)(1-\varepsilon\pi^2t)(1-\varepsilon\bar{\pi}^2t)},$$

où $\varepsilon = (\frac{\lambda+1}{p})$ (symbole de Legendre), et le nombre algébrique π intervient au numérateur de la fonction zêta de la courbe elliptique $\mathcal{E}_\lambda$ d'équation affine $y^2 = (x-1)(x^2 - \frac{1}{\lambda+1})$:

$$Z_{\mathcal{E}_\lambda/\mathbb{F}_q}(t) = \frac{(1-\pi t)(1-\bar{\pi}t)}{1-qt}.$$

Ils montrent également que lorsque $\lambda \in \mathbb{Q} \setminus \{0, -1\}$, la surface S_λ est modulaire si et seulement si

$$\lambda \in \{1, 8, \frac{1}{8}, -4, -\frac{1}{4}, -64, -\frac{1}{64}\}.$$

Beukers et Stienstra ont montré que la surface singulière S_{-1} est également modulaire.

REMARQUE. Pour plus de précisions sur comment le lien entre la surface K3 S_λ et la courbe elliptique $\mathcal{E}_\lambda$ a été découvert, on renvoie à [BEW98, notes du chapitre 13, p. 467]. Ce problème est relié au calcul de certaines sommes de caractères appelées sommes de Brewer.

Références

- [And76] ANDREWS (George E.) – *The Theory of Partitions*, addison-wesley éd., Encyclopedia of Mathematics and its Applications, vol. 2, 1976.
- [AOP02] AHLGREN (Scott), ONO (Ken) et PENNISTON (David) – « Zeta functions of an infinite family of K3 surfaces », *Amer. J. Math.* **124** (2002), p. 353-368, disponible sur : <http://www.math.wisc.edu/~ono/reprints/065.pdf>.
- [BEW98] BERNDT (Bruce C.), EVANS (Ronald J.) et WILLIAMS (Kenneth S.) – *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 21, John Wiley & Sons, Inc., New-York, 1998.
- [CdLORV03] CANDELAS (Philip), DE LA OSSA (Xenia) et RODRIGUEZ-VILLEGAS (Fernando) – « Calabi-Yau Manifolds Over Finite Fields, II », *Calabi-Yau Varieties and Mirror Symmetry* (Toronto, July, 23-29 2001) (YUI (Noriko) et LEWIS (J. D.), eds.), Fields Institute Comm. Series, vol. 38, Fields Institute, AMS, 2003, p. 121-157, disponible sur : <http://www.arxiv.org/hep-th/0402133>.
- [Del74] DELIGNE (Pierre) – « La conjecture de Weil : I », *Pub. Math. IHES* **43** (1974), p. 273-307, disponible sur : http://www.numdam.org/item?id=PMIHES_1974__43__273_0.
- [Del80] ———, « La conjecture de Weil : II », *Pub. Math. IHES* **52** (1980), p. 137-252, disponible sur : http://www.numdam.org/item?id=PMIHES_1980__52__137_0.
- [Dwo60] DWORK (Bernard M.) – « On the rationality of the zeta function of an algebraic variety », *Amer. J. Math.* **82** (1960), p. 631-648.
- [Dwo62] ———, « On the zeta function of a hypersurface I », *Pub. Math. IHES* **12** (1962), p. 5-68, disponible sur : http://www.numdam.org/item?id=PMIHES_1962__12__5_0.
- [Dwo64] ———, « On the zeta function of a hypersurface II », *Ann. of Math.* **80** (1964), p. 227-299.
- [Dwo69] ———, « p -adic cycles », *Pub. Math. IHES* **37** (1969), p. 27-115, disponible sur : http://www.numdam.org/item?id=PMIHES_1969__37__27_0.
- [Ehr34] EHRESMANN (Charles) – « Sur la topologie de certains espaces homogènes », *Ann. of Math.* **35** (1934), no. 2, p. 396-443.
- [Elk99] ELKIES (Noam) – « The Klein Quartic in Number Theory », *The Eightfold Way: The Beauty of Klein's Quartic Curve* (LEVY (Silvio), éd.), MSRI, Cambridge University Press, 1999, disponible sur : <http://www.msri.org/communications/books/Book35/files/elkies.pdf>.

- [GR78] GROSS (Benedict H.) et ROHRLICH (David E.) – « Some Results on the Mordell-Weil Group of the Jacobian of the Fermat Curve », *Invent. Math.* **44** (1978), p. 201-224, disponible sur : http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN356556735_0044.
- [Gro78] GROSS (Benedict H.) – « On the Periods of Abelian Integrals and a Formula of Chowla and Selberg », *Invent. Math.* **45** (1978), p. 193-211, disponible sur : http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN356556735_0045.
- [Gro64] GROTHENDIECK (Alexandre) (éd.) – *Théorie des topos et cohomologie étale des Schémas (SGA 4)*, Springer, 1963-64, Lecture notes in mathematics, vol. 269, 270 et 305, Séminaire de Géométrie Algébrique du Bois-Marie, disponible sur : <http://modular.fas.harvard.edu/sga/sga/pdf/index.html>.
- [Gro66] ——— (éd.) – *Cohomologie ℓ -adique et fonction L (SGA5)*, 1965-66, Lecture notes in mathematics, vol. 589, Séminaire de Géométrie Algébrique du Bois-Marie, disponible sur : <http://modular.fas.harvard.edu/sga/sga5/index.html>.
- [Hae04] HAESSIG (C. Douglas) – « Mirror Symmetry For Zeta Functions – Appendix », (2004), prépublication, appendice à [Wan04], disponible sur : <http://www.math.uci.edu/~dwan/mirror.pdf>.
- [Has36] HASSE (Helmut) – « Ueber die Riemannsche Vermutung im Funktionenkörpern », *Congrès international d'Oslo* (1936).
- [Hou02] HOUZEL (Christian) – « La géométrie algébrique – Recherches historiques », ch. XIII, Albert Blanchard, Paris, 2002.
- [Kad04] KADIR (Shabnam N.) – « The Arithmetic of Calabi-Yau Manifolds and Mirror Symmetry », Thèse, Oxford University, 2004, disponible sur : <http://www.arxiv.org/hep-th/0409202>.
- [Kob77] KOBLITZ (Neal) – *p -adic Numbers, p -adic Analysis, and Zeta-Functions*, second edition éd., GTM, vol. 58, Springer, Berlin, 1977.
- [Kob78] ———, « Gamma Function Identities and Elliptic Differentials on Fermat Curves », *Duke Mathematical Journal* **45** (1978), no. 1, p. 87-99.
- [Roh78] ROHRLICH (David E.) – « The Periods of the Fermat curves », *Invent. Math.* **45** (1978), p. 208-211, Appendix to [Gro78], disponible sur : http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN356556735_0045.
- [Sch86] SCHOEN (Chad) – « On the geometry of a special determinantal hypersurface associated to the Mumford-Horrocks vector bundle », *J. Reine Angew. Math.* **364** (1986), p. 85-111, disponible sur : http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN243919689_0364.
- [Sch03] SCHWERTFEGER (Berndt E.) – « The zeta-function of $x^4 + y^4 + z^4 = 0$ », (2003), disponible sur : <http://berndt-schwerdtfeger.de/v4/v4.pdf>.
- [Wan04] WAN (Daqing) – « Mirror Symmetry For Zeta Functions », *prépublication* (2004), disponible sur : <http://www.math.uci.edu/~dwan/mirror.pdf>.
- [Wei40] WEIL (André) – « Sur les fonctions algébriques à corps de constantes fini », *Comptes rendus de l'Académie des Sciences de Paris* **210** (1940), p. 592-594.
- [Wei48] ———, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités scientifiques et industrielles, vol. 1041, Hermann, 1948.
- [Wei49] ———, « Numbers of solutions of equations in finite fields », *Bull. Amer. Math. Soc.* **55** (1949), p. 497-508, disponible sur : <http://berndt-schwerdtfeger.de/v4/nf.pdf>.