Séminaire Bourbaki du vendredi Novembre 2022
6e année, 2022–2023, no ?

LES CONJECTURES DE WEIL : ORIGINES, APPROCHES, GÉNÉRALISATIONS

par **Antoine Chambert-Loir**

***Résumé.* —** Je retracerai l'histoire des conjectures de Weil sur le nombre de solutions d'équations polynomiales dans un corps fini et quelques unes des approches qui ont été proposées pour les résoudre.

***Abstract* (The Weil conjectures: origins, approaches, generalizations)**
I recount the history of the conjectures by Weil on the number of solutions of polynomial equations in finite fields, and some of the approaches that have been proposed to solve them.

1. PROLOGUE : GAUSS

Dans ses *Disquisitiones arithmeticae*, Gauss ([1801] 1863) démontrait plusieurs théorèmes qui dénombrent les solutions de certaines équations en congruences modulo un nombre premier.

Il prouve par exemple que le nombre de couples (x, y) d'entiers modulo p tels que $x^2 + y^2 \equiv 1 \pmod{p}$ est donné par

$$\mathrm{N}(x^2 + y^2 = 1) = p - \left(\frac{-1}{p}\right),$$

où $\left(\frac{\cdot}{p}\right)$ désigne le « symbole de Legendre » modulo p, défini par $\left(\frac{a}{p}\right) = 0$ si p divise a, 1 si a est un carré modulo p (l'expression était « résidu quadratique »), et -1 sinon. Il utilisait cette formule pour établir la « loi complémentaire » de sa *loi de réciprocité quadratique* (theorema aureum) disant que $\left(\frac{2}{p}\right)$ vaut 1 si $p \equiv \pm 1 \pmod{8}$ et -1 si $p \equiv \pm 3 \pmod{8}$.

La dernière entrée de son agenda, publié par Klein (1903), est une affirmation du même genre :

> Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta si $a+bi$ est numerus primus, $a-1+bi$ per $2+2i$ divisibilis, multitudo omnium solutionum congruentiae
>
> $$1 \equiv xx + yy + xxyy \pmod{a + bi}$$
>
> inclusis
>
> $$x = \infty, \quad y = \pm i; \qquad x = \pm i, \quad y = \infty$$

fit

$$= (a-1)^2 + bb.$$

1814 Iul. 9.

Autrement dit, on considère un nombre premier p congru à 1 modulo 4. D'après Fermat, il s'écrit sous la forme $a^2 + b^2$ (de sorte que $\pi = a + bi$ est un premier de l'anneau $\mathbf{Z}[i]$ des entiers de Gauss). Quitte à échanger a et b, on suppose que a est impair et b est pair ; quitte à remplacer a par $-a$, on peut supposer que $a + b \equiv 1 \pmod 4$; alors, $a - 1 + bi$ est divisible par $2 + 2i$ dans $\mathbf{Z}[i]$. De manière équivalente, on impose que $(a-1)^2 + b^2$ est divisible par 8, d'où $p - 2a + 1 \equiv 0 \pmod 8$; lorsque $p \equiv 1 \pmod 8$, on a donc $a \equiv 1 \pmod 4$, tandis que lorsque $p \equiv 5 \pmod 8$, on a $a \equiv 3 \pmod 4$. Gauss affirme alors que le nombre de couples (x, y) dans $\mathbf{Z}$ tels que $x^2 + y^2 + x^2y^2 = 1$ modulo p est égal à $(a-1)^2 + b^2 - 4 = p - 2a - 3$.

C'est toutefois une *conjecture* que Gauss énonce ici — *observatio per inductionem facta gravissima* — et plusieurs mathématiciens après lui en proposeront des démonstrations : Herglotz (1921); Chowla (1949).

Pourtant, ainsi que le rappelle Weil (1949), Gauss avait démontré des résultats analogues pour les congruences cubiques

$$ax^3 - by^3 \equiv 1 \pmod p$$

(Gauss (1863, §358)) et biquadratiques

$$ax^4 - by^4 \equiv 1 \pmod p, \qquad y^2 \equiv ax^4 - b \pmod p$$

(Gauss ([1801] 1863, §23)) On a par exemple

$$\mathrm{N}(y^2 = 1 - x^4) = \begin{cases} 2 & \text{si } p = 2\,; \\ p - 1 & \text{si } p \equiv 3 \pmod 4\,; \\ p - 1 - 2a & \text{si } p \equiv 1 \pmod 4, \end{cases}$$

où l'on a écrit $p = a^2 + b^2$ avec $a \equiv p \pmod 8$.

2. ESTIMATION ET DÉNOMBREMENT

Hasse & Davenport (1935) et Weil (1949) généralisent ces formules à toutes les équations de la forme

$$\sum_{i=1}^{m} a_i x_i^{n_i} = 1$$

non seulement en congruences modulo un nombre premier p, c'est-à-dire dans le corps fini $\mathbf{Z}/p\mathbf{Z}$, mais dans un corps fini arbitraire. Leur solution est exprimée en termes de sommes de Gauss ou de Jacobi (introduites par Gauss) et met en évidence de très grandes régularités.

Ces questions, et notamment la réflexion de Weil, sont nées de la fusion de deux motivations assez différentes.

Dans sa thèse, Artin (1924*a*,*b*) avait poursuivi l'analogie entre corps de nombres et corps de fonctions entamée par Dedekind (1857) en mettant en vis-à-vis le corps $\mathbf{Q}$ des nombres rationnels et les corps de fractions rationnelles $\mathbf{F}_p(x)$ en une indéterminée x à coefficients dans $\mathbf{Z}/p\mathbf{Z}$. Il met en regard l'anneau $\mathbf{Z}$ des entiers relatifs et celui $\mathbf{F}_p[x]$ des polynômes, tous deux des anneaux principaux, les nombres premiers correspondent aux polynômes irréductibles unitaires, les unités ± 1 aux polynômes constants non nuls et les entiers strictement positifs aux polynômes unitaires. En observant que pour $n > 0$, on a $n = \mathrm{Card}(\mathbf{Z}/(n))$ tandis que pour un polynôme unitaire P, on a $\mathrm{Card}(\mathbf{F}_p[x]/(\mathrm{P})) = p^{\deg(\mathrm{P})}$, l'analogue de la fonction zêta de Riemann

$$\zeta_{\mathbf{Z}}(s) = \sum_{n\neq 0} n\frac{1}{n^s} = \prod_{p \text{ premier}} \frac{1}{1-p^{-s}}$$

est la série

$$\zeta_{\mathbf{F}_p[x]}(s) = \sum_{0\neq \mathrm{I}\subseteq \mathbf{F}_p[x]} \frac{1}{\mathrm{Card}(\mathbf{F}_p[x]/\mathrm{I})^s} = \prod_{\mathrm{P\ irréductible\ unitaire}} \frac{1}{1-p^{s\deg(\mathrm{P})}}.$$

Artin poursuivait donc cette analogie des nombres rationnels aux corps quadratiques en étudiant l'arithmétique des corps de la forme $\mathbf{F}_p(x)(\sqrt{f(x)})$ obtenus en adjoignant à $\mathbf{F}_p(x)$ une racine carrée d'un polynôme sans facteur carré f. Il introduisait en particulier leur fonction zêta et démontrait que c'est une fraction rationnelle de q^{-s}, établissait leur équation fonctionnelle, vérifiait la « formule analytique du nombre de classes », les utilisait pour étudier l'analogue des théorèmes des nombres premiers et de la progression arithmétique. Il vérifiait aussi, mais seulement dans un petite nombre de cas (§23), l'analogue de l'*hypothèse de Riemann*, c'est-à-dire que les zéros de ces fonctions zêta soient des nombres complexes de partie réelle $1/2$; il avait apparemment en vue la finitude de l'ensemble des corps de ce type dont le nombre de classes est donné. En des termes géométriques encore anachroniques, dont la nécessité n'apparaîtra que peu à peu, il étudie la courbe affine hyperelliptique d'équation $y^2 = f(x)$.

En Grande-Bretagne, Davenport (1933), alors élève de L. J. Mordell, tentait d'estimer des « sommes exponentielles » analogues aux sommes de Gauss, du genre

$$\sum_{x\in(\mathbf{Z}/p\mathbf{Z})} \left(\frac{f(x)}{p}\right)$$

où f est un polynôme. C'est une somme de p termes égaux à ± 1, et parfois 0; guidé par l'heuristique qu'elle devrait être de l'ordre de $\sqrt{p}$, il obtenait une majoration non triviale, en $\mathrm{O}(p^{3/4})$ lorsque f est unitaire de degré 4. En observant que $1 + \left(\frac{f(x)}{p}\right)$ est le nombre de solutions dans $\mathbf{Z}/p\mathbf{Z}$ de l'équation $y^2 = f(x)$, on a

$$\sum_{x\in(\mathbf{Z}/p\mathbf{Z})} \left(\frac{f(x)}{p}\right) = \mathrm{N}(y^2 = f(x)) - p$$

faisant un lien entre les deux questions.

Peu après sa thèse, Artin avait étendu son étude en remplaçant $\mathbf{Z}/p\mathbf{Z}$ par un corps fini arbitraire. Ainsi, il a pu montrer que la validité de son hypothèse de Riemann était inchangée si l'on étendait le corps fini, sans modifier le polynôme f et en déduire des familles de polynômes pour lesquelles l'hypothèse est vérifiée. Selon Roquette (2018), il semble que ce soit cette vérification qui lui ait permis de croire en la véracité de l'hypothèse de Riemann. Roquette explique cependant comment l'attitude quelque peu « mandarinale » de Hilbert lors de son exposé à Göttingen a conduit Artin à abandonner subitement ce sujet. Dans les années suivantes, M. Deuring et F.K. Schmidt ont mis en place la théorie des courbes sur un corps fini, notamment leurs fonctions zêta. C'est cependant Artin qui a expliqué à H. Hasse, lors d'une visite à Hamburg en 1932, le lien entre le problème de majoration de sommes d'exponentielles et l'analogue de l'hypothèse de Riemann, convaincant le second de s'y attaquer : en 1935, Hasse résoudra le cas des courbes elliptiques, c'est-à-dire lorsque le polynôme f a degré 3 ou 4.

3. LES CONJECTURES DE WEIL

Pour énoncer les conjectures générales de Weil, nous adoptons désormais un langage géométrique. Considérons donc un corps fini k et une variété algébrique V sur k, c'est-à-dire, suivant son goût, un schéma de type fini sur k, ou bien un système d'équations polynomiales $\{f_1(x_1, \dots, x_m) = \cdots = f_r(x_1, \dots, x_m) = 0\}$ à coefficients dans k.

L'ensemble $\mathrm{V}(k)$ des points k-rationnels de V correspond aux solutions dans k^m du système $\{f_1 = \cdots = f_m = 0\}$; comme le corps k est fini, c'est un ensemble fini et on note $\mathrm{N}(\mathrm{V})$ son cardinal.

Soit q le cardinal de k. La théorie des corps finis apprend que q est une puissance de la caractéristique p de k et qu'inversement, toute puissance de p est le cardinal d'un corps fini, unique à isomorphisme près. Ainsi, toute puissance q^n de q est le cardinal d'un corps fini k_n qui est l'unique extension de degré n de k. On notera $\mathrm{N}_n(\mathrm{V})$ le cardinal de $\mathrm{V}(k_n)$.

Introduisant une indéterminée t, Weil (1949) définit alors la série formelle à coefficients rationnels

$$\mathrm{Z}_v(t) = \exp\Big(\sum_{n=1}^{\infty} \tfrac{1}{n}\mathrm{N}_n(\mathrm{V})t^n\Big).$$

Motivée par les calculs que Weil avait faits au début de son article, cette formule peut-être étrange généralise les définitions de Dedekind et Artin. En effet, les points fermés x du schéma V correspondent aux idéaux maximaux M de l'anneau $\mathrm{A} = k[x_1, \dots, x_m]/(f_1, \dots, f_r)$, ou aux solutions $(x_1, \dots, x_m)$ du système $\{f_1, \dots, f_r\}$ dans une clôture algébrique fixée $\overline{k}$ de k ; le corps résiduel $\kappa(x)$ correspond au corps

résiduel A/M et aussi à l'extension finie de k engendrée par $x_1, \dots, x_m$; on note $\deg(x)$ le degré de cette extension. Alors, on a

$$\mathrm{Z_V}(t) = \prod_{x \in |\mathrm{V}|} \frac{1}{1 - t^{\deg(x)}},$$

une formule qui prouve que $\mathrm{Z_V}(q^{-s}) = \zeta_{\mathrm{V}}(s)$ dans les cas considérés par Dedekind et Artin. Elle montre aussi que $\mathrm{Z_V}(t)$ est à coefficients entiers

Dans le cas de Dedekind, $\mathrm{V} = \mathbf{A}^1$ est la droite affine, on a $\mathrm{N}_n(\mathrm{V}) = q^n$ et on obtient

$$\mathrm{Z}_{\mathbf{A}^1}(t) = \exp\Big(\sum_{n=1}^{\infty} \tfrac{1}{n} q^n t^n\Big) = \frac{1}{1 - qt}.$$

Les cas de l'espace affine et de l'espace projectif sont également élémentaires, on trouve

$$\mathrm{Z}_{\mathbf{A}^d}(t) = \frac{1}{1 - q^d t} \quad \text{et} \quad \mathrm{Z}_{\mathbf{P}_d}(t) = \frac{1}{(1-t)(1-qt)\dots(1-q^d t)}.$$

Weil (1949) considère aussi le cas des grassmanniennes ; il observe dans tous ces cas, ainsi que celui des hypersurfaces « diagonales » d'équation $a_1 x_1^{n_1} + \dots + a_m x_m^{n_m} = 1$ (ou leur version homogène), un lien entre le résultat obtenu et le polynôme de Poincaré de l'espace affine, l'espace projectif, la grassmannienne ou l'hypersurface diagonale complexe analogue.

La première conjecture de Weil énonce que $\mathrm{Z_V}(t)$ *est une fraction rationnelle.*

L'analogie avec la situation géométrique classique peut même être poursuivie. Pour cela, il convient de faire l'hypothèse supplémentaire que V est un schéma propre, lisse et géométriquement connexe, soit d sa dimension ; sa compagne en géométrie complexe est alors une variété différentielle compacte et connexe de dimension (réelle) $2d$. Weil suggère en effet qu'on peut écrire $\mathrm{Z_V}$ sous la forme

$$\mathrm{Z_V}(t) = \frac{\mathrm{P}_1(t) \dots \mathrm{P}_{2d-1}(t)}{\mathrm{P}_0(t) \dots \mathrm{P}_{2d}(t)}$$

où $\mathrm{P}_0, \dots, \mathrm{P}_{2d}$ sont des polynômes de terme constant 1 et de degré les *nombres de Betti* $b_0, \dots, b_{2d}$ de la compagne complexe de V.

Les seconde et troisième conjectures se placent encore sous cette hypothèse.

Weil postule l'existence d'une *équation fonctionnelle* du type

$$\mathrm{Z_V}(1/q^d t) = \varepsilon q^{\chi d/2} t^{\chi} \mathrm{Z_V}(t),$$

où $\varepsilon = \pm 1$ et $\chi = b_0 - b_1 + b_2 - \dots$ est la caractéristique d'Euler-Poincaré de V.

Enfin, la troisième conjecture affirme que les inverses des racines de P_i sont des entiers algébriques de valeur absolue $q^{i/2}$.

Dans son exposé (Weil, 1956) au Congrès international d'Amsterdam, il précisera son intuition géométrique, dans le cas des courbes, d'une façon qui orientera définitivement les études ultérieures.

4. COHOMOLOGIES DE WEIL

Considérons un schéma propre, lisse, géométriquement intègre V sur un corps fini k de cardinal q. Dans le contexte des courbes elliptiques, Hasse avait introduit le morphisme de Frobenius de V. Ici, c'est un morphisme de schémas $\phi_{\mathrm{V}}\colon \mathrm{V} \to \mathrm{V}$ qui est l'identité sur les points mais, du point de vue des anneaux locaux de V, est donné par l'élévation à la puissance q. Chaque ouvert affine U de V est stable par ϕ_{V}, et sur l'anneau A de U, ϕ_{V} est donné par le morphisme de k-algèbres $a \mapsto a^q$.

Si l'on étend les scalaires de k à une clôture algébrique $\overline{k}$ de k, le morphisme ϕ_{V} devient un morphisme de schémas $\phi_{\overline{\mathrm{V}}}\colon \overline{\mathrm{V}} \to \overline{\mathrm{V}}$ et $\mathrm{V}(k)$ apparaît comme l'ensemble des *points fixes* de $\phi_{\overline{\mathrm{V}}}$ agissant sur $\overline{\mathrm{V}}$.

Comme l'explique Weil (1956), la formule des traces de Lefschetz en topologie algébrique suggère alors une expression

$$\mathrm{N}(\mathrm{V}) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}\left(\phi_{\overline{\mathrm{V}}}^{*} \mid \mathrm{H}_i(\overline{\mathrm{V}})\right)$$

où les $\mathrm{H}^i(\overline{\mathrm{V}})$ seraient les groupes d'homologie de $\overline{\mathrm{V}}$, définis fonctoriellement en $\overline{\mathrm{V}}$.

Notons que dans la formule précédente, les points fixes sont comptés avec multiplicité 1. En effet, comme la dérivée du polynôme T^q, égale à $q\mathrm{T}^{q-1}$, est nulle dans $k[\mathrm{T}]$, la « différentielle » de $\phi_{\overline{\mathrm{V}}}$ est nulle, et en particulier, son graphe dans $\overline{\mathrm{V}} \times \overline{\mathrm{V}}$ est transverse à la diagonale.

Appliquant cette idée aux puissances $\phi_{\overline{\mathrm{V}}}^{n}$ de $\phi_{\overline{\mathrm{V}}}$, on obtient une formule

$$\mathrm{N}_n(\mathrm{V}) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}\left((\phi_{\overline{\mathrm{V}}}^{n})^{*} \mid \mathrm{H}_i(\overline{\mathrm{V}})\right),$$

qui conduit à l'expression

$$\mathrm{Z}_{\mathrm{V}}(t) = \frac{\mathrm{P}_1(t)\mathrm{P}_3(t)\ldots\mathrm{P}_{2d-1}(t)}{\mathrm{P}_0(t)\mathrm{P}_2(t)\ldots\mathrm{P}_{2d}(t)}$$

où

$$\mathrm{P}_i(t) = \det\left(1 - t\phi_{\overline{\mathrm{V}}} \mid \mathrm{H}_i(\overline{\mathrm{V}})\right).$$

Dans cette analogie, l'équation fonctionnelle traduirait la dualité de Poincaré $\mathrm{H}_i(\overline{\mathrm{V}}) \leftrightarrow \mathrm{H}_{2d-i}(\overline{\mathrm{V}})$.

Ces idées suggèrent également des formes d'uniformité pour des familles de variétés. Un théorème d'Ehresmann énonce qu'une submersion propre de variétés différentielles est localement triviale, une fibre est difféomorphe aux fibres voisines. En géométrie algébrique, cela suggère que si $\mathcal{V} \to \mathrm{S}$ est un morphisme propre et lisse de schémas, à fibres géométriquement connexes, les espaces d'homologie $\mathrm{H}_i(\overline{\mathcal{V}_s})$ devraient être de dimension constante, lorsque s parcourt S. Lorsque $\kappa(s)$ est un sous-corps de $\mathbf{C}$, la variété $\mathcal{V}_s$ peut être considérée comme une variété complexe, et on voudrait également que les espaces d'homologie soient reliés à ceux donnés par la topologie.

Les années 1960 ont vu le début d'une quête des « cohomologies[1] de Weil ». Les constructions de Weil (1948*b*) éclairent le cas des courbes. Dans le cas topologique, l'espace d'homologie $H_1(V)$ d'une courbe V (projective, lisse, connexe) de genre g est un $\mathbf{Q}$-espace vectoriel de dimension $2g$ et les travaux de Weil suggèrent, lorsque V est une telle courbe sur un corps k qu'on puisse prendre pour $H_1(V)$ un espace vectoriel de dimension $2g$, non pas sur $\mathbf{Q}$, mais sur le corps $\mathbf{Q}_\ell$ des nombres ℓ-adiques, où ℓ est un nombre premier distinct de la caractéristique de k. Chez Weil, cet espace vectoriel est construit à partir du « module de Tate » ℓ-adique de la jacobienne J de V, c'est-à-dire la limite

$$\varprojlim_n J[\ell^n]$$

des groupes des points d'ordre une puissance de ℓ de la variété abélienne J. Comme $V[\ell^n]$ est isomorphe $(\mathbf{Z}/\ell^n\mathbf{Z})^{2g}$, ce module est un $\mathbf{Z}_\ell$-module libre de rang $2g$, dont on peut prendre le produit tensoriel par $\mathbf{Q}$.

Dès le début, cette quête est néanmoins placée sous l'ombre d'une mise en garde de Serre quant au type d'espaces vectoriels que l'on peut espérer obtenir. Supposons en effet que V soit une courbe elliptique *supersingulière*. l'anneau des endomorphismes de V qu'avait introduit Hasse, est alors un ordre d'une algèbre de quaternions A sur $\mathbf{Q}$ et la fonctorialité de l'homologie fournit un plongement de cette algèbre A dans l'anneau des matrices 2×2 à coefficients dans F. Cela impose que $A \otimes F$ soit isomorphe à l'algèbre $M_2(F)$, ce qui est effectivement le cas lorsque $F = \mathbf{Q}_\ell$ pour ℓ différent de la caractéristique, mais n'a pas lieu pour $F = \mathbf{R}$ ou $F = \mathbf{Q}_p$. En particulier, la quête d'une cohomologie de Weil à valeurs « $\mathbf{Q}$-espaces vectoriels » est illusoire.

Parmi les quelques exemples de cohomologies de Weil maintenant à notre disposition, citons :

1. La *cohomologie étale* définie par Grothendieck et développée avec plusieurs collaborateurs, dont M. Artin, J.-L. Verdier et P. Deligne au sein des *Séminaires de géométrie algébrique* (volumes 4, 5 et 7 en particulier). Sa définition repose sur la notion de revêtement en géométrie algébrique ; qu'elle donne le résultat attendu utilise le calcul des revêtements des courbes en termes de jacobiennes, ainsi qu'un théorème de M. Artin selon lequel les variétés algébriques complexes ont une base d'ouverts qui sont des $K(\pi, 1)$, c'est-à-dire dont le type d'homotopie est gouverné par leur groupe fondamental.
2. Les *cohomologies cristalline* et *rigide* définies par Berthelot sur le modèle d'une construction par Grothendieck de la cohomologie de De Rham. Le modèle est la théorie des équations différentielles.

En quelque sorte ces deux cohomologies sont les deux pôles de la correspondance de Riemann–Hilbert.

De nombreuses questions restent cependant ouvertes : on ne sait par exemple pas si la dimension des groupes de cohomologie étale dépend du choix du nombre premier ℓ !

[1] Je ne sais pas bien comment l'on est passé de l'homologie au point de vue dual de la cohomologie.

5. APPROCHES DES CONJECTURES DE WEIL (RATIONALITÉ ET ÉQUATION FONCTIONNELLE)

Il y a essentiellement trois preuves de la rationalité des fonctions zêta de Weil.

1) La première, limitée au cas des courbes, est due à Schmidt (1931) et repose sur le théorème de Riemann–Roch. Donnons-en le principe. Lorsqu'on développe la formule exprimant $Z_V(t)$ comme un produit sur les points fermés de V, on obtient une formule

$$Z_V(t) = \sum_n \mathrm{Card}(\mathrm{Div}_n^+(V))t^n,$$

où $\mathrm{Div}_n^+(V)$ désigne l'ensemble des diviseurs effectifs de degré n sur V, c'est-à-dire des combinaisons linéaires formelles de points fermés dont la somme des degrés vaut n. Admettons qu'il existe un diviseur de degré 1, D_0, sur V (Schmidt (1931) le déduit de l'analyse ci-dessous ; sinon, la fonction zêta de V sur une extension convenable de k n'aurait pas un pôle simple en 1 et $1/q$) et associons à un diviseur $D \in \mathrm{Div}_n^+(V)$ la classe $[D - nD_0]$ de $D - nD_0$ dans la jacobienne de V. Pour tout diviseur E de degré 0, on trouve les diviseurs effectifs D tels que $[D - nD_0] = E$ en considérant l'espace de Riemann–Roch $\mathcal{L}(E + nD_0)$: les fonctions rationnelles sur V dont le diviseur f vérifie $\mathrm{div}(f) + E + nD_0 \geq 0$; alors $D = \mathrm{div}(f) + E + nD_0$ est un diviseur effectif de degré n sur V et $D - nD_0$ a même classe que E. Cela permet de calculer le cardinal des éléments de $\mathrm{Div}_n^+(V)$ de classe [E] :

$$\frac{q^{h(E+nD_0)} - 1}{q - 1},$$

où $h(E + nD_0) = \dim(\mathcal{L}(E + nD_0))$. D'après le théorème de Riemann–Roch, cette dimension vaut $n + 1 - g$ si $n > 2g - 2$; en ajoutant les contributions de chaque classe de diviseur E de degré 0, on obtient que $(1 - t)(1 - qt)Z_V(t)$ est un polynôme de degré $2g$.

Le théorème de Riemann–Roch affirme plus précisément que $h(E+nD_0) = n+1-g+h(K_V - E - nD_0)$, où K_V est un diviseur canonique sur V. En termes plus modernes, le théorème de Riemann–Roch calcule une caractéristique d'Euler-Poincaré $h^0(E + nD_0) - h^1(E + nD_0) = n + 1 - g$, on a $h = h^0$ et la « dualité de Serre » exprime $h^1(E + nD_0) = h^0(K_V - E - nD_0)$.

2) Dwork (1960) a démontré la rationalité des fonctions zêta en toute dimension par une méthode très originale. Il se ramène d'abord au cas où V est une hypersurface d'équation $f = 0$ dans un tore $(\mathbf{A}^1 \setminus \{0\})^m$ et récrit $Z_V(t)$ comme une somme exponentielle. Par des arguments d'analyse p-adique, il prouve que cette série est le quotient de deux séries entières dont le rayon de convergence p-adique est infini ; en particulier, $Z_v(t)$ apparaît comme une *fonction méromorphe* définie sur tout $\mathbf{Z}_p$. En utilisant que $\mathrm{Card}(V(k_n)) \leq q^{nm}$, on constate que cette même série définit une fonction holomorphe sur le disque ouvert de rayon q^{-m} dans $\mathbf{C}$. En adaptant le critère de rationalité de Borel (1894), Dwork en déduit que $Z_v(t)$ est le développement de Taylor d'une fraction rationnelle.

3) Comme esquissé au paragraphe précédent, les cohomologies de Weil fournissent une démonstration de la rationalité des fonctions zêta. Il y a en particulier une démonstration par voie étale (SGA 5) et une démonstration par voie cristalline.

L'équation fonctionnelle des fonctions zêta se déduit alors de la dualité de Poincaré.

6. APPROCHES DES CONJECTURES DE WEIL (HYPOTHÈSE DE RIEMANN)

6.1. Le cas des courbes

Au delà de quelques familles d'exemples dans l'article initial d'Artin (1924*b*) et dans une étude qu'il avait abandonnée à l'automne 1921 (voir Ullrich (2000)), la première démonstration concerne le cas des courbes elliptiques pour lesquelles Hasse a offert deux preuves.

La première reposait sur la théorie de la multiplication complexe, à savoir la construction d'une courbe elliptique complexe dont les endomorphismes soient un ordre d'un corps quadratique imaginaire et telle qu'en en « réduisant modulo p » l'équation de Weierstrass, on obtienne la courbe elliptique initiale V sur k. L'endomorphisme de Frobenius de V correspond alors à un nombre quadratique imaginaire π tel que $\pi\overline{\pi} = q$ et le cardinal de $V(k)$ est égal à $|1 - \pi|^2 = 1 - \mathrm{Tr}(\pi) + q$. D'une certaine manière, cette preuve est dans la lignée des calculs de Gauss : la courbe d'équation $y^2 = 1 - x^4$ est en effet une courbe elliptique à multiplication complexe par $\mathbf{Z}[i]$.

La seconde démonstration (Hasse, 1936) repose sur une étude plus algébrique de l'anneau des endomorphismes de V. Hasse démontre que le degré d'un tel endomorphisme fournit une forme quadratique définie positive et les égalités $N(V) = \deg(1 - \phi_V)$ et $\deg(\phi_V) = q$, puis en déduit l'inégalité $|N(V) - 1 - q| \leq 2\sqrt{q}$.

La démonstration générale est due à Weil. L'anneau des endomorphismes d'une courbe elliptique est remplacé par celui des *correspondances* qu'avait introduit Deuring. Weil démontre une formule $N(V) = 1 - \mathrm{Tr}(\phi_V) + q$, où $\mathrm{Tr}(\phi_V)$ désigne la trace de l'action de ϕ_V sur ce qu'on appelle aujourd'hui le module de Tate ℓ-adique de la jacobienne de V. De fait, la note (Weil, 1940) établissait cette formule sous l'hypothèse que la jacobienne de V possède, pour tout entier n premier à la caractéristique de k, précisément n^{2g} points α tels que $n\alpha = 0$, de sorte que ce module de Tate est de rang 2 sur l'anneau des entiers ℓ-adiques. L'année suivante, Weil (1941) fournirait les détails d'une preuve de cette formule.

Presque dix années furent nécessaire à la rédaction détaillée de cette preuve, pour laquelle Weil dut développe une « géométrie algébrique abstraite », sur un corps arbitraire et en particulier indépendante de toute considération topologique (Weil, 1946, 1948*b*,*a*).

Le cœur de l'hypothèse de Riemann apparaît comme la positivité d'une trace : si C est une correspondance sur la courbe V, c'est-à-dire une somme formelle de courbes tracées sur la surface $V \times V$, l'hypothèse de Riemann apparaît comme conséquence de l'inégalité $\mathrm{Tr}(C \circ C') > 0$, que Weil démontre via l'étude des endomorphismes de la jacobienne de V.

Mattuck & Tate (1958) et Grothendieck (1958) reprouvent cette inégalité de façon plus directe, sans recours à la jacobienne, via le théorème de Riemann–Roch pour la surface $V \times V$. C'est le théorème de l'indice de Hodge qui apparaît alors comme source de l'inégalité cruciale.

Dans le cas des courbes hyperelliptiques, Stepanov (1969) a proposé une démonstration encore plus élémentaire, en ce qu'elle se place sur la courbe elle-même et n'utilise que le théorème de Riemann–Roch. Elle a été généralisée indépendamment par Schmidt (1976) et Bombieri (1974). L'idée est de construire une fonction rationnelle f non nulle sur la courbe V de degré contrôlé et qui, par construction, s'annule automatiquement en chaque point de $V(k)$; il en résulte une inégalité de la forme $N(V) \leq q + 1 + O(\sqrt{q})$. En utilisant cette inégalité pour des courbes auxiliaires convenables V′, on obtient une inégalité dans l'autre sens $N(V) \geq q + 1 - O(\sqrt{q})$. Un argument simple fondé sur la rationalité de Z_V permet alors de conclure.

6.2. Estimées partielles en dimension supérieure

Pendant près de 25 ans, la seule estimée générale était due à Lang & Weil (1954). Pour une sous-variété $V \subset \mathbf{P}_n$, de dimension d et géométriquement irréductible, ils démontrent une majoration du type

$$\left|N(V) - q^d\right| \leq c_1 q^{d-\frac{1}{2}} + c_2 q^{d-1},$$

où $c_1 = (\deg(V) - 1)(\deg(V) - 2)$ et c_2 est un nombre réel non explicite, mais qui ne dépend que de n et de $\deg(V)$.

Modulo l'utilisation de l'hypothèse de Riemann pour les courbes, leur démonstration est très simple : elle consiste à considérer les intersections $V \cap H$ de V avec un sous-espace projectif variable H de dimension $n + 1 - d$. Supposons pour simplifier que V ne soit pas contenue dans un sous-espace projectif non trivial. Par un théorème de type Lefschetz, ces intersections $V \cap H$ sont le plus souvent des courbes géométriquement irréductibles, de genre arithmétique $g = (\deg(V) - 1)(\deg(V) - 2)$. Quitte à prendre garde à leurs singularités, elles donnent toutes lieu à une estimation du type

$$|N(V \cap H) - q| \leq g\sqrt{q} + c,$$

où c est un nombre réel qui ne dépend pas de H. Par des arguments de géométrie algébrique les sous-espaces projectifs H pour lesquels $V \cap H$ n'est pas géométriquement irréductible figurent parmi une sous-variété de la variété grassmannienne adéquate ; dans leur cas, on se contente d'une majoration $N(V \cap H) \leq \deg(V)$. Il reste à sommer ces estimations lorsque H varie ; celles du premier type dominent l'asymptotique et fournissent le premier terme $c_1 q^{d-\frac{1}{2}}$, les secondes donnent lieu au terme d'erreur.

6.3. Conjectures standard

Dans son exposé au Congrès international, Weil (1956) avait expliqué une démonstration de la positivité $\mathrm{Tr}(C \circ C') > 0$ qui utilise la géométrie algébrique complexe (et ne permet donc pas de prouver le théorème de Weil).

Serre (1960) a ensuite élaboré cet argument en dimension supérieure pour démontrer un *analogue kählérien*. Alors, V est une variété projective compacte munie d'un endomorphisme $f : V \to V$ tel que l'image inverse f^*H d'une section hyperplane H soit numériquement équivalente à qH, pour un nombre réel $q > 0$. Serre démontre alors que les valeurs propres de f^* agissant sur l'espace de cohomologie $H^i(V)$ sont de module $q^{i/2}$. Sa preuve utilise de façon cruciale le théorème de Lefschetz difficile et la signature de la forme d'intersection en restriction à la cohomologie primitive. Pour la transposer aux variétés sur les corps finis, il faut disposer de l'analogue de ces deux résultats pour une cohomologie de Weil. Si le théorème de Lefschetz difficile est actuellement connu (mais comme *conséquence* des conjectures de Weil), la signature des formes d'intersection est une question largement ouverte.

Dans une lettre à Serre datée du 27 août 1965, Grothendieck présente un faisceau de conjectures, inspiré par la démonstration de Serre, qui entraîneraient les conjectures de Weil. Un aspect important est que ces conjectures ne font plus référence à une cohomologie de Weil mais s'expriment uniquement en termes des cycles algébriques sur la variété V et leurs intersections : ce sont les *conjectures standard*, et je renvoie à Grothendieck (1969) et Kleiman (1968, 1994) pour une présentation.

6.4. Le cas général

La démonstration générale de l'hypothèse de Riemann pour les variétés sur un corps fini est due à Deligne (1974). Il m'est impossible de décrire cette preuve qui repose sur la machinerie de la cohomologie étale ℓ-adique, mais d'une façon moins « statique » que les approches antérieures. En particulier, intervient l'idée d'exploiter qu'une famille de sections hyperplanes donne lieu à une grosse monodromie.

Deligne généralisera ses arguments pour établir une propriété de stabilité fondamentale des *poids* en cohomologie étale, voir Deligne (1980).

7. APPLICATIONS

Il est probablement impossible de faire la liste de toutes les applications des conjectures de Weil. Je vais donner quelques indications dans trois directions différentes : arithmétique, géométrie et théorie des modèles.

7.1. Arithmétique

Comme je l'ai déjà évoqué, l'hypothèse de Riemann sur les corps finis est intimement liée à de bonnes majorations de sommes d'exponentielles. Dans le cas des courbes, l'article de Weil (1948*b*) détaille ce que l'on peut obtenir. En dimension supérieure, Deligne (1974, §8.4) expose une majoration générale, due à Bombieri dont voici une simplification lorsque $k = \mathbf{F}_p$: si $f \in \mathbf{Z}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ est un polynôme de degré d dont la partie homogène modulo p définit une hypersurface lisse de degré d de $\mathbf{P}_{n-1}$, alors

$$\left| \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^n} \exp\left(2i\pi \frac{f(x)}{p}\right) \right| \leq (d-1)^n p^{n/2}.$$

Le livre de Katz (1980) présente une introduction à l'utilisation de la cohomologie étale pour les sommes d'exponentielles.

Une autre application importante est liée à la théorie des formes modulaires. Le produit infini

$$\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24}, \qquad q = \exp(2i\pi z)$$

définit une forme modulaire de poids 12 pour le groupe $\mathrm{SL}(2, \mathbf{Z})$; explicitement, on a

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z).$$

Si l'on note

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n,$$

Généralisant des idées de Kuga et Shimura, Deligne (1971) a déduit de l'hypothèse de Riemann une démonstration de l'inégalité conjecturée par Ramanujan (1916) : pour tout nombre premier p, on a

$$|\tau(p)| < 2p^{11/2}.$$

La raison d'être de cette inégalité est que $\tau(p)$ s'écrit $\alpha_p + \beta_p$, où α_p et β_p sont deux des valeurs propres de l'endomorphisme de Frobenius ϕ_V agissant sur un espace d'homologie $\mathrm{H}_1 1(\mathrm{V})$ d'une variété lisse. Les détails sont évidemment un peu plus compliqués...

Citons une application de ces majorations de Ramanujan par Lubotzky *et al.* (1988) à une construction optimale de graphes expanseurs.

7.2. Géométrie

La première application géométrique de la démonstration de l'hypothèse de Riemann est peut-être la démonstration de l'analogue en cohomologie étale du théorème de Lefschetz difficile (Deligne, 1980, Théorème 4.1.1). C'est un énoncé pour les variétés algébriques sur un corps algébriquement clos, si bien qu'il convient peut-être d'expliquer comment il peut bien être lié à un énoncé sur le nombre de points de variétés sur un corps fini.

De fait, il y a plusieurs procédés de réduction pour étudier la géométrie des variétés sur un corps k. On peut notamment observer que la définition de ces variétés et des divers objets géométriques qui interviennent dans un énoncé donné ne font intervenir qu'un nombre fini de polynômes ; voyant les coefficients de ces polynômes comme des indéterminées, la situation apparaît comme une spécialisation d'un énoncé « en famille ». Le principe est alors que souvent, la validité du théorème en vue est uniforme dans la famille, si bien qu'il suffirait de le prouver pour de bonnes spécialisations.

Une extension de ce principe est au cœur de la démonstration du « théorème de décomposition » de Beĭlinson *et al.* ([1982] 2018). Une application récente de ce principe est due à Batyrev (1999) : si deux variétés algébriques complexes de type Calabi-Yau (projectives, lisses, à fibré canonique trivial) sont birationnelles, elles ont mêmes nombres de Betti. Citons aussi l'article d'exposition de Serre (2009).

Mentionnons enfin que Katz & Messing (1974) ont déduit du théorème de Deligne que le théorème de Lefschetz difficile valait pour *toute* cohomologie de Weil. Ils ont aussi prouvé que le polynôme caractéristique des endomorphismes de Frobenius de variétés projectives lisses ne dépendait pas du choix de cette cohomologie de Weil. Ils obtiennent en particulier que la dimension de ces espaces (dans le cas projectif lisse) ne dépend pas du choix de la cohomologie de Weil.

7.3. Théorie des modèles

Ax (1968) a déduit de l'hypothèse de Riemann, plus précisément, des estimées de Lang & Weil (1954) une caractérisation remarquable des corps finis de « grand cardinal ».

Il se place en théorie des modèles c'est-à-dire qu'il s'intéresse aux *formules* qui sont vraies dans un corps fini. Les formules qu'il considère utilisent le « langage des anneaux » : elles sont écrites à l'aide des symboles + (addition), − (soustraction), · (multiplication), 0 et 1 (zéro et un), de symboles de variables et de quantificateurs $\exists$ (il existe), $\forall$ (pour tout), $\neg$ (négation). Par exemple, $\exists x, x^2+1 = 0$ est une telle formule, à condition d'écrire $x^2 = x \cdot x$, mais $\exists x \exists n, x^n = 2$ n'en est pas une car on ne dispose pas de symbole de puissance entière. Si une telle formule ϕ n'a pas de variable libre et si k est un corps, on dit qu'elle est vérifiée dans ce corps (on note $k \models \phi$) si son interprétation évidente est vraie lorsqu'on lit les quantificateurs $\exists x$ comme « il existe $x \in k$ », etc. Par exemple, si p est un nombre premier, la formule « $\exists x, x^2 + 1 = 0$ » est vérifiée dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si p n'est pas congru à 3 modulo 4 ; elle est vérifiée dans $\mathbf{C}$, mais pas dans $\mathbf{R}$ ni dans $\mathbf{Q}(i\sqrt{3})$.

Avec un peu de travail en géométrie algébrique, on peut écrire à l'aide d'une telle formule le contexte de l'estimation de Lang & Weil (1954) : il s'agit d'exprimer l'expression « soit V une variété algébrique affine géométriquement intègre et de dimension d » en termes concrets : V est définie par une famille finie $(f_1, \ldots, f_r)$ de polynômes de degrés $\leq$ D, et il s'agit d'exprimer que V est géométriquement intègre et de dimension d par une formule $\phi_{d,r,\mathrm{D}}$ du langage des anneaux en les coefficients de ces polynômes.

Les entiers d, r, D étant fixés, le théorème de Lang & Weil (1954) fournit une estimation uniforme

$$\left|\mathrm{Card}(\mathrm{V}(k)) - q^d\right| \leq c_{d,r,\mathrm{D}} q^{d-\frac{1}{2}}$$

dès que k est un corps fini de cardinal q. En particulier, si $q > c_{d,r,\mathrm{D}}^2$, on en déduit que $\mathrm{V}(k) \neq \emptyset$. En particulier, la formule $\phi'_{d,r,\mathrm{D}}$ qui exprime que pour toute telle V, l'ensemble $\mathrm{V}(k)$ n'est pas vide est vraie pour tout corps fini k de cardinal assez grand.

Le théorème principal d'Ax (1968) est qu'à l'inverse, une formule ϕ est vraie dans tout corps fini de cardinal assez grand si et seulement si elle se déduit des formules $\phi'_{d,r,\mathrm{D}}$.

8. AU DELÀ DES BORNES DE WEIL

Malgré leur importance, il n'est peut-être pas inutile de signaler que les majorations qu'entraînent les conjectures de Weil pour le nombre de solutions d'équations dans les corps finis sont loin d'épuiser ce qu'on voudrait savoir de ce nombre.

Je donne deux exemples.

a) Tout d'abord, déjà dans le cas d'une courbe projective lisse de genre g, la majoration $|\mathrm{N}(\mathrm{V}) - q - 1| \leq 2g\sqrt{q}$ n'est pas forcément applicable à une question donnée, notamment lorsqu'il s'agit de faire varier V.

Si l'on cherche une minoration de $\mathrm{N}(\mathrm{V})$, l'inégalité

$$\mathrm{N}(\mathrm{V}) \geq q + 1 - 2g\sqrt{q}$$

est par exemple inutile lorsque g est trop grand. De fait, il est possible d'avoir $\mathrm{N}(\mathrm{V}) = 0$.

Étant donnée une suite de courbes (V_g) de genres tendant vers l'infini, définies sur un même corps fini k à q éléments, la majoration de Weil entraîne

$$\overline{\lim} \frac{1}{2g} \mathrm{Card}(\mathrm{V}_g(k)) \leq \sqrt{q}.$$

Lorsque q est un carré parfait, on sait produire une suite de courbes qui réalise cette limite supérieure ; dans le cas contraire, on ne sait pas s'il en existe.

b) Plutôt que des majorations/minorations, on peut avoir besoin de congruences pour l'entier $\mathrm{N}(\mathrm{V})$, dans l'esprit du classique théorème de Chevalley–Warning, voir Chevalley (1935); Warning (1935).

La cohomologie étale fournit en principe de telles congruences modulo les nombres premiers ℓ qui ne divisent pas la caractéristique p de k, mais elle en donne peu car ces congruences sont rares. Dans le cas des formes modulaires, voir par exemple Serre (1973).

On dispose en revanche de congruences p-adiques, démontrées soit par des méthodes de type Dwork, par exemple (Ax, 1964), soit par l'étude précise de la cohomologie cristalline, cf. (Mazur, 1972, 1973, 1975). Un exemple récent d'application de ces idées à l'*existence* de points rationnels est le théorème d'Esnault (2003) : si V est une variété projective lisse, géométriquement rationnellement connexe, sur un

corps fini k de cardinal q, alors $\mathrm{V}(k)$ n'est pas vide ; plus précisément, $\mathrm{Card}(\mathrm{V}(k)) \equiv 1 \pmod{q}$. (Cela s'applique en particulier aux variétés de Fano.)

BIBLIOGRAPHIE

E. Artin (1924*a*), « Quadratische Körper im Gebiete der höheren Kongruenzen. I. » *Mathematische Zeitschrift*, **19** (1), p. 153–206.

E. Artin (1924*b*), « Quadratische Körper im Gebiete der höheren Kongruenzen. II. » *Mathematische Zeitschrift*, **19** (1), p. 207–246.

J. Ax (1964), « Zeroes of polynomials over finite fields ». *American Journal of Mathematics*, **86**, p. 255–261.

J. Ax (1968), « The Elementary Theory of Finite Fields ». *The Annals of Mathematics*, **88** (2), p. 239.

V. V. Batyrev (1999), « Stringy Hodge numbers of varieties with Gorenstein canonical singularities ». *Integrable Systems and Algebraic Geometry*, p. 1–32, World Sci. Publ., Kobe/Kyoto.

A. A. Beĭlinson, J. Bernstein, P. Deligne & O. Gabber ([1982] 2018), « Faisceaux pervers ». *Analyse et Topologie Sur Les Espaces Singuliers, I (Luminy, 1981)*, Astérisque **100**, p. 5–171, Soc. Math. France, Paris, 2$^{\mathrm{e}}$ édition.

E. Bombieri (1974), « Counting points on curves over finite fields ». *Séminaire Bourbaki Vol. 1972/73 Exposés 418–435*, Lecture Notes in Mathematics, p. 234–241, Springer, Berlin, Heidelberg.

É. Borel (1894), « Sur une application d'un théorème de M. Hadamard ». *Bull. Sc. Math.*, **18**, p. 22–25.

C. Chevalley (1935), « Démonstration d'une hypothèse de M. Artin ». *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, **11** (1), p. 73–75.

S. Chowla (1949), « The Last Entry in Gauss's Diary ». *Proceedings of the National Academy of Sciences of the United States of America*, **35** (5), p. 244–246.

H. Davenport (1933), « On certain exponential sums ». *Journal für die reine und angewandte Mathematik*, **169**, p. 158–176.

R. Dedekind (1857), « Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus. » *Journal für Mathematik*, **54** (1), p. 1–26.

P. Deligne (1971), « Formes modulaires et représentations ℓ-adiques ». *Séminaire Bourbaki 1968/69*, Lecture Notes in Math. **175**, p. Exposé 355, 139–172, Springer.

P. Deligne (1974), « La conjecture de Weil. I ». *Publications mathématiques de l'IHÉS*, **43** (1), p. 273–307.

P. Deligne (1980), « La Conjecture de Weil. II ». *Publications mathématiques de l'IHÉS*, **52** (1), p. 137–252.

B. Dwork (1960), « On the rationality of the zeta function of an algebraic variety ». *American Journal of Mathematics*, **82** (3), p. 631–648.

H. Esnault (2003), « Varieties over a finite field with trivial Chow group of 0-cycles have a rational point ». *Inventiones mathematicae*, **151** (1), p. 187–191.

C. F. Gauss ([1801] 1863), *Werke I. Disquisitiones Arithmeticae*, Königlichen Gesellschaft der Wissenschaften zu Göttingen, Göttingen.

C. F. Gauss (1863), *Werke II. Höhere Arithmetik*, Königlichen Gesellschaft der Wissenschaften zu Göttingen, Göttingen.

A. Grothendieck (1958), « Sur une note de Mattuck-Tate. » *Journal für die reine und angewandte Mathematik*, **200**, p. 208–215.

A. Grothendieck (1969), « Standard conjectures on algebraic cycles ». *Algebraic Geometry. 1968, 193-199 (1969).*, p. 193–199, Bombay, 1968.

H. Hasse (1936), « Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. » *jreia*, **175** (4), p. 193–208.

H. Hasse & H. Davenport (1935), « Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. » *Journal für die reine und angewandte Mathematik*, **172**, p. 151–182.

G. Herglotz (1921), « Zur letzten Eintragung im Gaußschen Tagebuch ». *Ber. Math. Phys. Kl. Sächs. Akad. Wiss. Leipzig*, **73**, p. 271–276.

N. M. Katz (1980), *Sommes exponentielles. Cours à Orsay, automne 1979. Redige par Gerard Laumon, preface par Luc Illusie*, Astérisque **79**, Société Mathématique de France (SMF), Paris.

N. M. Katz & W. Messing (1974), « Some consequences of the Riemann hypothesis for varieties over finite fields ». *Inventiones mathematicae*, **23** (1), p. 73–77.

S. L. Kleiman (1968), « Algebraic cycles and the Weil conjectures ». *Dix Exposés Sur La Cohomologie Des Schémas*, Adv. Stud. Pure Math. **3**, p. 359–386, North-Holland, Amsterdam.

S. L. Kleiman (1994), « The standard conjectures ». *Motives. Proceedings of the Summer Research Conference on Motives, Held at the University of Washington, Seattle, WA, USA, July 20-August 2, 1991*, p. 3–20, American Mathematical Society, Providence, RI.

F. Klein (1903), « Gauß' wissenschaftliches Tagebuch 1796–1814 ». *Mathematische Annalen*, **57** (1), p. 1–34.

S. Lang & A. Weil (1954), « Number of points of varieties in finite fields ». *American Journal of Mathematics*, **76**, p. 819–827.

A. Lubotzky, R. Phillips & P. Sarnak (1988), « Ramanujan graphs ». *Combinatorica*, **8** (3), p. 261–277.

A. Mattuck & J. Tate (1958), « On the inequality of Castelnuovo-Severi : To Emil Artin on his 60th birthday ». *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, **22** (1), p. 295–299.

B. Mazur (1972), « Frobenius and the Hodge filtration ». *Bulletin of the American Mathematical Society*, **78** (5), p. 653–667.

B. Mazur (1973), « Frobenius and the Hodge filtration (estimates) ». *Annals of Mathematics. Second Series*, **98**, p. 58–95.

B. Mazur (1975), « Eigenvalues of Frobenius acting on algebraic varieties over finite fields ». *Proc. Symp. Pure Math.*, **29**, p. 231–261, American Mathematical Society,

Arcata.
J. S. Milne (2016), « The Riemann hypothesis over finite fields : From Weil to the present day ». *Notices of the International Congress of Chinese Mathematicians*, **4** (2), p. 14–52.
F. Oort & N. Schappacher (2016), « Early History of the Riemann Hypothesis in Positive Characteristic ». *The Legacy of Bernhard Riemann After One Hundred and Fifty Years*, édité by L. Ji, F. Oort & S.-T. Yau, **35**, p. 595–631, Higher Education Press and International Press, Beijing–Boston.
S. Ramanujan (1916), « On certain arithmetical functions ». *Transactions of the Cambridge Philosophical Society*, **22**, p. 159–184.
P. Roquette (2018), *The Riemann Hypothesis in Characteristic p in Historical Perspective*, Lecture Notes in Mathematics **2222**, Springer International Publishing, Cham.
F. K. Schmidt (1931), « Analytische Zahlentheorie in Körpern der Charakteristikp ». *Mathematische Zeitschrift*, **33** (1), p. 1–32.
W. M. Schmidt (1976), *Equations over Finite Fields An Elementary Approach*, Lecture Notes in Mathematics **536**, Springer Berlin Heidelberg, Berlin, Heidelberg.
J.-P. Serre (1960), « Analogues kählériens de certaines conjectures de Weil ». *Annals of Mathematics. Second Series*, **71**, p. 392–394.
J.-P. Serre (1973), « Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer) ». *Séminaire Bourbaki 1971/72*, Lecture Notes in Mathematics **317**, p. Exposé 416, 319–338.
J.-P. Serre (2009), « How to use finite fields for problems concerning infinite fields ». *Arithmetic, Geometry, Cryptography and Coding Theory*, Contemp. Math. **487**, p. 183–193, Amer. Math. Soc., Providence, RI.
S. A. Stepanov (1969), « On the number of points of a hyperelliptic curve over a finite prime field ». *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, **33**, p. 1171–1181.
P. Ullrich (2000), « Emil Artin's unpublished generalization of his dissertation ». *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, **19**, p. 173–194.
E. Warning (1935), « Bemerkung zur vorstehenden Arbeit von Herrn Chevalley ». *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, **11** (1), p. 76–83.
A. Weil (1940), « Sur les fonctions algébriques à corps de constantes fini ». *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Paris*, **210**, p. 592–594.
A. Weil (1941), « On the Riemann Hypothesis in Function-Fields ». *Proceedings of the National Academy of Sciences*, **27** (7), p. 345–347.
A. Weil (1946), *Foundations of Algebraic Geometry*, Colloq. Publ., Am. Math. Soc. **29**, American Mathematical Society (AMS), Providence, RI.
A. Weil (1948*a*), « Sur les courbes algébriques et les variétés qui s'en déduisent ».
A. Weil (1948*b*), *Variétés Abéliennes et Courbes Algébriques*, Actualités Sci. Ind. **1064**, Hermann & Cie., Paris.
A. Weil (1949), « Number of solutions of equations in finite fields ». *Bull. Amer. Math. Soc.*, **55**, p. 397–508.

A. Weil (1956), « Abstract versus classical algebraic geometry ». *Proceedings of the International Congress of Mathematicians 1954. Amsterdam, September 2–9. Vol. III. Stated Addresses in Sections. Symposia*, Erven P. Noordhoff N. V.; Amsterdam : North-Holland Publishing Co., Groningen.

Antoine Chambert-Loir

Université Paris Cité
IMJ-PRG
F-75013, Paris, France
E-mail : antoine.chambert-loir@u-paris.fr