Nombres de solutions des équations dans les corps finis

Par André Weil

Les équations à considérer sont celles du type

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \ldots + a_rx_r^{n_r} = b. \tag{1}$$

De telles équations ont une histoire intéressante. Dans l'art. 358 des *Disquisit*iones [1a][1], Gauss détermine les sommes gaussiennes (qu'on appelle "périodes" cyclotomiques) d'ordre 3, pour un nombre premier de la forme $p = 3n + 1$, et il obtient en même temps le nombre de solutions de toutes les congruences $ax^3 - by^3 \equiv 1 \pmod{p}$. Il attire l'attention sur l'élégance de sa méthode, ainsi que sur sa large étendue ; ce n'est que beaucoup plus tard, cependant, viz. dans son premier mémoire sur les résidus biquadratiques [1b], qu'il a fourni par écrit une autre application de la même méthode ; alors il traite le prochain cas plus élevé, trouve le nombre de solutions de toute congruence $ax^4 - by^4 \equiv 1 \pmod{p}$, pour un nombre premier de la forme $p = 4n + 1$, et il déduit de cela le caractère biquadratique de 2 mod p, ceci étant l'objectif visible de toute cette recherche ingénieuse et complexe. Comme conséquence accidentelle ("*coronidis loco*," p. 89), il fournit également en substance le nombre de solutions de toute congruence $y^2 \equiv ax^4 - b \pmod{p}$; ce résultat inclut comme cas particulier le théorème énoncé comme une conjecture ("*observatio per inductionem facta gravissima*") dans la dernière entrée de son *Tagebuch*[2] [1c][3] ; et cela implique la vérité de ce qui est devenu plus tard connu comme l'hypothèse de Riemann, pour le corps de fonctions défini par cette équation sur le corps premier à p éléments.

La procédure de Gauss est entièrement élémentaire, et elle n'utilise pas les sommes gaussiennes, puisque son but est davantage de l'appliquer pour déterminer de telles sommes. Si on essaie de l'appliquer à des cas plus généraux, pourtant, les calculs deviennent vite incroyables et on réalise la nécessité d'inverser cela en prenant les sommes gaussiennes comme points de départ. Les moyens de faire cela ont été fournis, aussi tôt qu'en 1827, par Jacobi, dans une lettre à Gauss [2a] (cf. [2b]). Mais Lebesgue, qui en 1837 consacra deux articles [3a, b] au cas $n_0 = \ldots = n_r$ de l'équation (1), n'a pas réussi a amener de résultat saisissant. Le problème dans son entièreté semble alors avoir été oublié jusqu'à ce qu'Hardy et Littlewood trouvent nécessaire d'obtenir des formules pour le nombre de solutions de la congruence $\sum_i x_i^n \equiv b \pmod{p}$ dans

Reçu par les éditeurs le 2 octobre 1948.

Transcription en Latex et traduction : Denise Vella-Chemla, août 2022.

[1]Les nombres entre crochets réfèrent à la bibliographie en fin d'article.

[2]trad : agenda.

[3]Il est surprenant que cela ait été négligé par Dedekind et d'autres auteurs qui ont discuté de cette conjecture (cf. M. Deuring, Abh. Math. Sem. Hamburgischen Univ. vol. 14 (1941) p. 197-198).

leur travail sur les séries singulières pour le problème de Waring [4] ; ils firent cela au moyen de sommes gaussiennes. Plus récemment, Davenport et Hasse [5] ont appliqué la même méthode au cas $r = 2, b = 0$ de l'équation (1) ainsi qu'à d'autres équations similaires ; pourtant, comme ils étaient principalement concernés par d'autres aspects du problème, et en particulier par sa relation à l'hypothèse de Riemann dans les corps de fonctions[4], le caractère vraiment élémentaire de leur traitement n'apparaît pas clairement.

Comme les équations du type (1) ont à nouveau récemment été le sujet de quelques discussions (cf. e.g. [6]), il peut être utile de donner ici une exposition brève mais complète du sujet. Cet exposé ne contiendra rien de nouveau, excepté peut-être dans le mode de présentation des résultats finaux, qui amèneront à l'établissement de quelques conjectures concernant les nombres de solutions des équations sur les corps finis, et leur relation aux propriétés topologiques des variétés définies par les équations correspondantes sur le corps des nombres complexes.

On considère l'équation (1) sur un corps fini k à q éléments ; les a_i sont dans k, et sont non nuls ; les n_i sont des entiers, que nous supposons être > 0 (seules quelques modifications insignifiantes seraient nécessaires si certains étaient < 0). On va d'abord discuter le cas $b = 0$.

Soit donc N le nombre de solutions dans k de l'équation

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \ldots + a_r x_r^{n_r} = 0$$

Pour chaque i, soit $d_i = (n_i, q-1)$ le p.g.c.d. des n_i et de $q-1$; pour chaque i et pour chaque u dans k, soit $N_i(u)$ le nombre de solutions de l'équation $x^{n_i} = u$; $N_i(u)$ est égal à 1 pour $u = 0$, et sinon, il est égal à d_i ou à 0 selon que u est ou n'est pas une $d_i^{\text{ième}}$ puissance dans k. Posons $L(u) = \sum_{i=0}^{r} a_i u_i$; on a

$$N = \sum_{L(u)=0} N_0(u_0) \ldots N_r(u_r), \tag{2}$$

où la somme est prise sur tous les ensembles de valeurs pour les u_i satisfaisant $L(u) = 0$, ou, comme on peut le dire, sur tous les points $(u) = (u_0, \ldots, u_r)$ dans la variété linéaire définie par $L(u) = 0$ dans l'espace vectoriel de dimension $r+1$ sur k.

Si k^* est le groupe multiplicatif de tous les éléments non nuls dans k, on dénotera par la lettre χ tout caractère de k^* ; comme k^* est cyclique d'ordre $q-1$, un tel caractère

[4]Pour cela, cf. H. Hasse, J. Reine Angew. Math. vol. 172 (1935) p. 37-54. Je regrette de n'avoir mentionné aucun de ces articles, dans lesquels la connexion avec les différentes sortes de sommes exponentielles et l'hypothèse de Riemann est assez clairement exprimée, dans ma note récente sur ce même sujet, Proc. Nat. Acad. Sci. U.S.A. vol. 34 (1948) P. 204-207.

est complètement déterminé si on assigne sa valeur à un élément générateur w de k^* (une "racine primitive"), et la valeur peut être n'importe quelle valeur des racines $(q-1)^{\text{ièmes}}$ de l'unité. En choisissant un tel élément w une fois pour toutes, on dénotera par χ_α le caractère de k^* déterminé par $\chi_\alpha(w) = e^{2\pi i\alpha}$, où α est un nombre rationnel satisfaisant $(q-1)\alpha \equiv 0 \pmod 1$. On pose également $\chi_\alpha(0) = 0$ pour $\alpha \not\equiv 0 \pmod 1$ et $\chi_\alpha(0) = 1$ pour $\alpha \equiv 0 \pmod 1$. Alors on a

$$N_i(u) = \sum_\alpha \chi_\alpha(u) \qquad (d_i\alpha \equiv 0 \pmod 1, 0 \leqq \alpha < 1).$$

En fait, pour $u = 0$, les deux côtés de l'équation ont pour valeur 1 ; pour $u \neq 0$, le côté droit peut s'écrire $\sum_{\nu=0}^{d_i-1} \zeta^\nu$, avec $\zeta = \chi_{1/d_i}(u)$; et ζ est alors la $d_i^{\text{ième}}$ racine de l'unité, égale à 1 si et seulement si u est une $d_i^{\text{ième}}$ puissance dans k^*.

En utilisant cela dans (2), on obtient :

$$N = \sum_{u,\alpha} \chi_{\alpha_0}(u_0)\ldots\chi_{\alpha_r}(u_r) \qquad (L(u) = 0\ ;\ d_i\alpha_i \equiv 0 \pmod 1,\ \ 0 \leqq \alpha_i < 1).$$

Comme il y a q^r points dans $L(u) = 0$, les termes dans la somme ci-dessus qui correspondent à $\alpha_0 = \ldots = \alpha_r = 0$, étant tous égaux à 1, ont pour somme q^r. Nous montrons maintenant que ces termes pour lesquels quelques-uns, mais non tous, des α_i valent 0, ont pour somme 0. En fait, considérons e.g. ceux pour lesquels $\alpha_0, \ldots, \alpha_{s-1}$ ont des valeurs données, autres que 0, et $\alpha_s = \ldots = \alpha_r = 0$, avec $s \leqq r$; comme il y a q^{r-s} points (u) dans la variété $L(u) = 0$ pour lesquels $u_0, \ldots, u_{s-1}$ ont des valeurs arbitrairement assignées, la somme de ces termes est

$$q^{r-s} \prod_{i=0}^{s-1} \left(\sum_{u_i} \chi_{\alpha_i}(u_i) \right),$$

et elle est nulle puisque chacun des facteurs est nul. Cela donne

$$N = q^r + \sum_{u,\alpha} \chi_{a_0}(u_0)\ldots\chi_{a_r}(u_r) \qquad (L(u) = 0\ ;\ d_i\alpha_i \equiv 0 \pmod 1,\ \ 0 < \alpha_i < 1).$$

Dans cette expression, on remplace les u_i, respectivement, par u_i/a_i, et on obtient

$$N = q^r + \sum_a \chi'_{a_0} a_0^{-1})\ldots\chi_{a_r}(a_r^{-1}).S(\alpha) \qquad (d_i\alpha_i \equiv 0 \pmod 1,\ \ 0 < \alpha_i < 1),$$

si on pose, pour toutes les valeurs de α_i vérifiant $(q-1)\alpha_i \equiv 0 \pmod 1, \alpha_i \not\equiv 0 \pmod 1$:

$$S(\alpha) = S(\alpha_0, \ldots, \alpha_r) = \sum_{\sum u_i = 0} \chi_{\alpha 0}(u_0)\ldots\chi_{\alpha_r}(u_r).$$

Comme pour la dernière somme, les termes pour lesquels $u_0 = 0$ valent 0, et nous pouvons les exclure ; on peut alors poser $u_i = u_0 v_i$ $(1 \leqq i \leqq r)$; les termes, dans notre somme, correspondant à des valeurs données des v_i (satisfaisant $1+\sum_{i=1}^{r} v_i = 0$) donnent

$$\chi_{\alpha_1}(v_1) \dots \chi_{\alpha_r}(v_r) \sum_{u_0 \neq 0} \chi_\beta(u_0),$$

avec $\beta = \sum_{i=0}^{r} \alpha_i$, et cette dernière somme est égale à $q-1$ pour $\beta \equiv 0 \pmod 1$, et 0 sinon, de telle façon que dans le dernier cas $S(\alpha)$ vaut 0.

Définissons alors, pour tout ensemble des α_i satisfaisant les conditions

$$(q-1)\alpha_i \equiv 0, \qquad \alpha_i \not\equiv 0, \qquad \sum_{i=0}^{r} \alpha_i \equiv 0 \pmod 1,$$

un nombre $j(\alpha)$ par la relation

$$\begin{aligned} j(\alpha) &= \sum_{1+v_1+\dots+v_r=0} \chi_{\alpha_1}(v_1) \dots \chi_{\alpha_r}(v_r) \\ &= \frac{1}{q-1} \sum_{u_0+\dots+u_r=0} \chi_{\alpha_0}(u_0) \dots \chi_{\alpha_r}(u_r) \end{aligned}$$

En fonction des $j(\alpha)$, on voit maintenant que le nombre N des solutions de $\sum_{i=0}^{r} a_i x_i^{n_i} = 0$ est donné par

$$N = q^r + (q-1) \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \dots \chi_{\alpha_r}(a_r^{-1}) \cdot j(\alpha) \qquad (3)$$
$$(d_i \alpha_i \equiv 0 \ ; \ \textstyle\sum \alpha_i \equiv 0 \pmod 1 \ ; 0 < \alpha_i < 1).$$

Les $j(\alpha)$ peuvent être appelés les sommes de Jacobi pour le corps k ; ils ont été d'abord introduits et étudiés, dans le cas d'un corps premier, par Jacobi [2a, b], plus tard par Stickelberger [7], et plus récemment par Davenport et Hasse [5]. Ils sont intimement liés aux sommes de Gauss pour k :

$$g(\chi) = \sum_{x \in k} \chi(x)\psi(x),$$

où ψ est un caractère pour le groupe additif de k, choisi une fois pour toutes, et non partout égal à 1, et où χ est n'importe quel caractère multiplicatif défini ci-dessus, autre que χ_0. Pour la commodité du lecteur, nous rappellerons brièvement quelques-unes des propriétés connues de ces sommes. En premier lieu, dans les sommes qui définissent $g(\chi)$, on peut, comme χ n'est pas égal à χ_0, contraindre x à être $\neq 0$. Alors on obtient

$$g(\chi)\overline{g}(\chi) = \sum_{y \neq 0} \sum_{x \neq 0} \chi(xy^{-1})\psi(x-y),$$

où on peut substituer xy à x dans la somme pour x, et alors intervertir l'ordre des sommations :

$$g(\chi)\overline{g}(\chi) = \sum_{x\neq 0} \chi(x) \sum_{y\neq 0} \psi[(x-1)y],$$

Comme la somme de toutes les valeurs de ψ sur k est 0, la seconde somme a pour valeur $q-1$ pour $x=1$, et -1 pour $x\neq 1$; comme la somme de toutes les valeurs de χ sur k^* est 0, cela donne

$$g(\chi)\overline{g}(\chi) = q. \tag{4}$$

Maintenant, dans la définition de $g(\chi)$, écrivons tx pour x avec n'importe quel $t\neq 0$ dans k ; cela donne

$$g(\chi) = \chi(t) \sum_x \chi(x)\psi(tx),$$

par conséquent, en utilisant (4), et en échangeant x et t :

$$\chi(x) = \frac{g(\chi)}{q} \sum_t \overline{\chi}(t)\overline{\psi}(tx),$$

qui est également vrai pour $x=0$; ceci est l'expansion de Fourier de $\chi(x)$ sur k selon les caractères additifs de k. En utilisant cela dans la définition de $j(\alpha)$, on obtient

$$(q-1)j(\alpha) = q^{-r-1} \cdot g(\chi_{\alpha_0}) \dots g(\chi_{\alpha_r}) \sum_t \overline{\chi}_{\alpha_0}(t_0) \dots \overline{\chi}_{\alpha_r}(t_r) \sum_{\sum u_i = 0} \overline{\psi}\left(\sum_i t_i u_i\right).$$

Mais, dans le groupe additif de tous les vecteurs $(u) = (u_0, \dots, u_r)$, les vecteurs satisfaisant $\sum u_i = 0$ forment un sous-groupe de q^r éléments, sur lequel $\overline{\psi}(\sum t_i u_i)$ est un caractère ; la somme des valeurs de ce caractère sur le sous-groupe doit donc être soit q^r, si le caractère a la valeur constante 1, soit 0 sinon. Le premier cas advient si et seulement si tous les t_i sont égaux, puisque sinon, on peut résoudre les équations $\sum u_i = 0, \sum t_i u_i = z$, où z est n'importe quel élément de k, e.g. un élément tel que $\psi(z)\neq 1$. Comme on a $\sum \alpha_i \equiv 0 \pmod 1$ par la définition de $j(\alpha)$, cela donne

$$j(\alpha) = \frac{1}{q} g(\chi_{\alpha_0}) \dots g(\chi_{\alpha_r}).$$

Comme conséquence, on a

$$j(\alpha)\overline{j}(\alpha) = q^{r-1},$$

et donc

$$|N - q^r| \leqq M(q-1)q^{(r-1)/2},$$

où M est le nombre de systèmes de nombres rationnels α_i satisfaisant

$$n_i\alpha_i \equiv 0, \quad \sum \alpha_i \equiv 0 \pmod 1, \quad 0 < \alpha_i < 1,$$

et est donc un entier dépendant seulement des n_i.

Des résultats ci-dessus, on peut facilement déduire le nombre N_1 de solutions de l'équation $\sum_{i=0}^{r} a_i x_i^{n_i} + 1 = 0$. En fait, soit N, comme précédement, le nombre de solutions de $\sum_{i=0}^{r} a_i x_i^{n_i} = 0$, et soit N' le nombre de solutions de $\sum_{i=0}^{r} a_i x_i^{n_i} + x_{r+1}^{q-1} = 0$. Les résultats précédents s'appliquent à la dernière équation, avec $d_{r+1} = n_{r+1} = q-1$. Mais, puisque x_{r+1}^{q-1} a la valeur 1, sauf pour $x_{r+1} = 0$, on a

$$N' = (q-1)N_1 + N.$$

Cela donne immédiatement une expression pour N_1 ; pour écrire cela plus convenablement, on définira le symbole $j(\alpha)$ même dans le cas où certains, mais pas tous parmi les α_i, valent 0. Soit β_j les nombres satisfaisant $(q-1)\beta_j \equiv 0, \sum_j \beta_j \equiv 0 \pmod 1$, et non tous $\equiv 0 \pmod 1$; supposons que s d'entre eux soient $\equiv 0 \pmod 1$, et appelons $\alpha_0, \ldots, \alpha_r$, les autres, dans n'importe quel ordre ; alors on pose $j(\beta) = (-1)^s j(\alpha)$. Cela étant, la formule pour N_1 peut s'écrire

$$N_1 = q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \ldots \chi_{\alpha_r}(a_r^{-1})\; j\left(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^{r} \alpha_i\right)$$

$$(d_i\alpha_i \equiv 0 \pmod 1, 0 < \alpha_i < 1),$$

et l'on obtient, comme précédemment :

$$|N_1 - q^r| \leqq M_1 q^{r/2},$$

où M_1 est maintenant donné par

$$M_1 = (d_0 - 1)\ldots(d_r - 1) < n_0 n_1 \ldots n_r.$$

C'est d'un intérêt considérable d'être capable de comparer le nombre de solutions d'une équation (ou, plus généralement, le nombre de points rationnels d'une variété algébrique) dans un corps fini donné, et dans toutes les extensions de degré fini de ce corps. Cela peut être fait facilement, pour le type d'équations qui sont considérées dans cet article, si l'on utilise une relation, due à Davenport et Hasse [5], entre les sommes gaussiennes dans un corps fini et ses extensions. Nous donnerons d'abord un bref compte-rendu, en langage élémentaire, de la preuve de Davenport et Hasse de cette relation.

Soit k' une extension de k, de degré ν ; pour y dans k', dénotons par $N(y)$ et $T(y)$ la norme et la trace de y, respectivement, sur k. Si w dénote, comme précédemment, un générateur du groupe multiplicatif k^*, il y a des générateurs de k'^*, tels que $N(z) = w$; alors, si on dénote, comme précédemment, par $\chi'_\alpha(y)$ le caractère multiplicatif sur k' déterminé par $\chi'_\alpha(z) = e^{2\pi i\alpha}$, on a, pour $(q-1)\alpha \equiv 0 \pmod 1$, $\chi'_\alpha(y) = \chi_\alpha[N(y)]$. On pose également $\psi'(y) = \psi[T(y)]$; c'est un caractère additif de k', non partout égal à 1 puisqu'on sait que $T(y)$ envoie k' sur k. Soit maintenant $g'(\chi'_\alpha)$ la somme gaussienne dans k' :

$$g'(\chi'_\alpha) = \sum_{y \in k'} \chi'_\alpha(y)\psi'(y).$$

Le théorème de Davenport et Hasse s'énonce ainsi :

$$-g'(\chi'_\alpha) = [-g(\chi_\alpha)]^\nu. \tag{5}$$

Dans le but de prouver cela, considérons les polynômes à coefficients dans k, et de plus haut coefficient 1 ; à chacun de ces polynômes

$$F(X) = X^n + c_1X^{n-1} + \ldots + c_n,$$

de degré $n \geqq 1$, on associe le nombre

$$\lambda(F) = \chi_\alpha(c_n)\psi(c_1).$$

Pour deux tels polynômes F_1, F_2, on a $\lambda(F_1F_2) = \lambda(F_1)\lambda(F_2)$. Si l'on dénote également par $n(F)$ le degré d'un tel polynôme F, et par U une indéterminée, cela donne l'identité formelle

$$1 + \sum_F \lambda(F) \cdot U^{n(F)} = \prod_P [1 - \lambda(P) \cdot U^{n(P)}]^{-1},$$

où la somme du côté gauche est prise sur *tous les* polynômes F sur k, de degré $\geqq 1$, de plus haut coefficient 1, et le produit du côté droit est pris sur tous les polynômes *irréductibles* P sur k, de plus haut coefficient 1. Comme d'habitude, cela découle immédiatement du fait que tout F peut s'exprimer de manière unique comme un produit de puissances de polynômes irréductibles.

Dans la somme du côté gauche, considérons d'abord les termes qui correspondent aux polynômes $F(X) = X + c$ de degré 1 ; la somme de ces termes est égale à $g(\chi_\alpha)U$. Comme pour la somme des termes correspondant à n'importe quel degré donné $n > 1$, elle est égale à 0, puisque, avec les notations ci-dessus, elle est égale à

$$q^{n-2} \sum_{c_n} \chi_\alpha(c_n) \sum_{c_1} \psi(c_1) \cdot U^n,$$

où les deux sommes sont prises sur k et valent donc 0. Cela donne

$$1 + g(\chi_\alpha)U = \prod_P [1 - \lambda(P) \cdot U^{n(P)}]^{-1}. \tag{6}$$

De façon similaire, si $F'(X) = X^n + d_1 X^{n-1} + \ldots + d_n$ est un polynôme sur k', on écrit

$$\lambda'(F') = \chi'_\alpha(d_n)\psi'(d_1),$$

et, en prenant une autre indéterminée U', on obtient l'identité formelle

$$1 + g'(\chi'_\alpha)U' = \prod_{P'} [1 - \lambda'(P') \cdot U'^{n(P')}]^{-1} \tag{6'}$$

où le produit est pris sur tous les polynômes irréductibles P' sur k', de plus haut coefficient 1.

Maintenant soit P comme ci-dessus ; soit P' l'un des facteurs irréductibles de P sur k' ; soit $-\xi$ l'une des racines de P'. Alors ξ engendre sur k une extension $k(\xi)$ de degré $n = n(P)$, et sur k' une extension $k'(\xi)$ de degré $n' = n(P')$; comme $k'(\xi)$ est le composé de $k(\xi)$ et de k', son degré sur k doit être le p.p.c.m. des degrés n de $k(\xi)$ sur k, et du degré ν de k' sur k, i.e. égal à $n\nu/d$ si on a $d = (n, \nu)$. Cela donne $n' = n/d$; par conséquent P a sur k' exactement d facteurs irréductibles, tous de degré n/d. De plus, si a et b sont respectivement la norme et la trace de ξ, prises dans $k(\xi)$ relativement à k, on a

$$P(X) = X^n + bX^{n-1} + \ldots + a,$$

et donc

$$\lambda(P) = \chi_\alpha(a)\psi(b).$$

De façon similaire, si a' et b' sont la norme et la trace de ξ, prises dans $k'(\xi)$ relativement à k', on a

$$\lambda'(P') = \chi'_\alpha(a')\psi'(b') = \chi_\alpha(Na')\psi(Tb'),$$

où Na' et Tb' sont la norme de a' et la trace de b', prises dans k' relativement à k ; donc Na' et Tb' sont respectivement égales à la norme et à la trace de ξ, prises dans $k'(\xi)$ relativement à k. On peut donc également obtenir Na' en prenant la norme de ξ dans $k'(\xi)$ relativement à $k(\xi)$, celle-ci étant égale à $\xi^{\nu/d}$, et alors la norme de ceci dans $k(\xi)$ relativement à k, qui est $a^{\nu/d}$. Donc on a $Na' = a^{\nu/d}$, et de façon similaire $Tb' = (\nu/d)b$, et par conséquent

$$\lambda'(P') = \lambda(P)^{\nu/d}.$$

Maintenant, du côté droit de (6'), on peut mettre ensemble les d facteurs correspondant à tous les facteurs irréductibles de P sur k' ; si, de plus, on remplace U' par U^ν, on obtient

$$[1 - \lambda(P)^{\nu/d} U^{\nu n/d}]^{-d},$$

qui peut également s'écrire

$$\prod_{\rho=0}^{\nu-1} [1 - \lambda(P) \cdot (\zeta^\rho U)^n]^{-1}$$

où ζ est n'importe quelle $\nu^{\text{ième}}$ racine de l'unité. Cela donne

$$\begin{aligned} 1 + g'(\chi'_\alpha) U^\nu &= \prod_{\rho=0}^{\nu-1} \prod_P [1 - \lambda(P) \cdot (\zeta^\rho U)^{n(P)}]^{-1} \\ &= \prod_{\rho=0}^{\nu-1} (1 + g(\chi_\alpha) \zeta^\rho U) \\ &= 1 + (-1)^{\nu+1} g(\chi_\alpha)^\nu U^\nu, \end{aligned}$$

ce qui prouve (5).

Maintenant, N_ν étant le nombre de solutions d'une équation de type (1), avec ou sans terme constant, sur l'extension de degré ν du corps de base k, il est facile, en utilisant les résultats ci-dessus, de donner une expression simple de la "série de puissances génératrice" pour N_ν, i.e. pour la série de puissances formelle $\sum_1^\infty N_\nu U^\nu$; cela s'avère être l'expansion d'une certaine fonction rationnelle dans U. Nous illustrerons, cependant, l'idée en considérant le cas de l'équation homogène

$$a_0 x_0^n + \ldots + a_r x_r^n = 0, \tag{7}$$

considérée comme l'équation d'une variété (sans point singulier) dans l'espace projectif P^r de dimension r sur k. Le nombre $\overline{N}$ des points rationnels sur k, sur cette variété, est relié au nombre N de solutions de la même équation dans l'espace affine par $N = 1 + (q-1)\overline{N}$, de telle façon que, en posant $d = (n, q-1)$, on obtient, à partir de nos résultats précédents :

$$\overline{N} = 1 + q + \ldots + q^{r-1} + \sum_\alpha \overline{\chi}_{\alpha_0}(a_0) \ldots \overline{\chi}_{\alpha_r}(a_r) \cdot j(\alpha)$$
$$(d\alpha_i \equiv 0,\ \textstyle\sum \alpha_i \equiv 0 \pmod 1\ ;\ 0 < \alpha_i < 1).$$

Maintenant appelons $\overline{N}_\nu$ le nombre de points rationnels, sur la variété définie par (7), sur l'extension k_ν de k de degré ν ; nous calculerons la série $\sum_1^\infty \overline{N}_\nu U^{\nu-1}$.

Dans le but de faire cela, considérons n'importe quel ensemble de nombres rationnels $\alpha_0, \ldots, \alpha_r$ satisfaisant $n\alpha_i \equiv 0$, $\sum \alpha_i \equiv 0 \pmod 1$, $0 < \alpha_i < 1$. Pour cet ensemble, posons $\mu = \mu(\alpha)$ le plus petit entier, tel que $(q^\mu - 1)\alpha_i \equiv 0 \pmod 1$ pour $0 \leqq i \leqq r$; alors les extensions k_ν de k telles que $(q^\nu - 1)\alpha_i \equiv 0 \pmod 1$ sont celles pour lesquelles ν est un multiple de μ, et celles-ci seulement. En choisissant une racine primitive dans k_μ, on peut maintenant, comme précédemment, définir dans k_μ les caractères χ_{α_i}, les sommes gaussiennes $g(\chi_{\alpha_i})$, et la somme de Jacobi

$$j(\alpha) = \frac{1}{q} g(\chi_{\alpha_0}) \ldots g(\chi_{\alpha_r}).$$

De plus, si l'on dénote par $\chi'_{\alpha_i}, g'(\chi'_{\alpha_i})$ et $j'(\alpha)$ les caractères correspondants et les sommes pour l'extension $k' = k_{\lambda\mu}$ de k de degré $\lambda\mu$, où λ est n'importe quel entier, on obtient de nos résultats précédents :

$$\chi'_{\alpha_i}(a_i) = \chi_{\alpha_i}(a_i)^\lambda, \quad g'(\chi'_{\alpha_i}) = (-1)^{\lambda-1} g(\chi_{\alpha_i})^\lambda, \quad j'(\alpha) = (-1)^{(\lambda-1)(r-1)} j(\alpha)^\lambda.$$

Alors on obtient :

$$\sum_1^\infty \overline{N}_\nu U^{\nu-1} = -\sum_{h=0}^{r-1} \frac{d}{dU} \log (1 - q^h U)$$

$$+ (-1)^r \sum_\alpha \frac{1}{\mu(\alpha)} \frac{d}{dU} \log [1 - C(\alpha) \cdot U^{\mu(\alpha)}] \tag{8}$$

$$(n\alpha_i \equiv 0, \quad \textstyle\sum \alpha_i \equiv 0 \pmod 1 \ ; \quad 0 < \alpha_i < 1)$$

où on a posé

$$C(\alpha) = (-1)^{r-1} \overline{\chi}_{\alpha_0}(a_0) \ldots \overline{\chi}_{\alpha_r}(a_r).j(\alpha).$$

De plus, il est facile de voir que $C(q\alpha) = C(\alpha)$, puisque $x \to x^q$ est un automorphisme de k_μ qui laisse les a_i invariants. Donc, dans la dernière somme dans (8), les termes $\mu(\alpha)$ correspondant à l'ensemble $(\alpha) = (\alpha_0, \ldots, \alpha_r)$ et aux ensembles $(q^\rho \alpha)$ pour $1 \leqq \rho \leqq \mu - 1$ sont tous égaux, de telle façon que, en les mettant ensemble, on peut faire disparaître le dénominateur $\mu(\alpha)$.

Soit A le nombre de solutions, en nombres rationnels α_i, du système $n\alpha_i \equiv 0, \sum \alpha_i \equiv 0 \pmod 1, 0 < \alpha_i < 1$. Alors on trouve[5] que le polynôme de Poincaré (au sens de la topologie combinatoire) de la variété définie, dans l'espace projectif P^r sur les nombres complexes, par une équation de la forme

$$c_0 x_0^n + \ldots + c_r x_r^n = 0$$

[5]Comme cela m'a été obligeamment communiqué par P. Dolbeault à Paris.

est égal à

$$\sum_{h=0}^{r-1} X^{2h} + A \cdot X^{r-1}.$$

Ceci, et d'autres exemples dont nous ne pouvons discuter ici, semble apporter quelque soutien aux assertions conjecturales suivantes, qui sont connues comme étant vraies pour les courbes, mais que je n'ai pas été jusque-là capable de prouver pour des variétés de dimension plus grande.

Soit V une variété sans point singulier, de dimension n, définie sur un corps fini k à q éléments. Soit N_ν le nombre de points rationnels sur V sur l'extension k_ν de k de degré ν. Alors on a

$$\sum_{1}^{\infty} N_\nu U^{\nu-1} = \frac{d}{dU} \log Z(U),$$

où $Z(U)$ est la fonction rationnelle en U, satisfaisant l'équation fonctionnelle

$$Z\left(\frac{1}{q^n U}\right) = \pm q^{n\chi/2} U^\chi Z(U),$$

avec χ égal à la caractéristique d'Euler-Poincaré de V (nombre d'intersections de la diagonale avec elle-même sur le produit $V \times V$).

De plus, on a :

$$Z(U) = \frac{P_1(U) P_3(U) \dots P_{2n-1}(U)}{P_0(U) P_2(U) \dots P_{2n}(U)},$$

avec $P_0(U) = 1 - U, P_{2n}(U) = 1 - q^n U$, et, pour $1 \leqq h \leqq 2n-1$:

$$P_h(U) = \prod_{i=1}^{B_h} (1 - \alpha_{hi} U)$$

où les α_{hi} sont les entiers algébriques de valeur absolue $q^{h/2}$.

Finalement, appelons les degrés B_h des polynômes $P_h(U)$ les *nombres de Betti* de la variété V ; la caractéristique d'Euler-Poincaré χ est alors exprimée par la formule habituelle $\chi = \sum_h (-1)^h B_h$. La preuve à portée de main semble suggérer que, si $\overline{V}$ est une variété sans points singuliers, définie sur un corps K de nombres algébriques, les nombres de Betti des variétés $V_\mathfrak{p}$, déduits de $\overline{V}$ par réduction modulo un idéal premier $\mathfrak{p}$ dans K, sont égaux aux nombres de Betti de $\overline{V}$ (considérés comme une variété sur les nombres complexes) au sens de la topologie combinatoire, pour tous, sauf au plus un nombre fini, les idéaux premiers $\mathfrak{p}$. Par exemple, considérons la variété grassmanienne $G_{m,r}$, dont les points sont les variétés linéaires r-dimensionnelles dans

un espace projectif m-dimensionnel, sur un corps à q éléments. On voit facilement que le nombre de points rationnels sur la variété est égal à $F(q)$, où F est le polynôme défini par

$$F(X) = \frac{(X^{m+1}-1)(X^{m+1}-X)\dots(X^{m+1}-X^r)}{(X^{r+1}-1)(X^{r+1}-X)\dots(X^{r+1}-X^r)}.$$

Alors, si les conjectures ci-dessus sont vraies, le polynôme de Poincaré de la variété grassmanienne $G_{m,r}$ sur les nombres complexes doit être $F(X^2)$. Il en est effectivement ainsi, comme cela peut être aisément vérifié à partir des résultats bien connus de Ehresmann [8] [6].

Références

1. C. F. Gauss, *Werke* : (a) vol. I, p. 445-449; (b) vol. II, p. 67-92; (c) vol. Xi, p. 571.
2. C. G. Jacobi, *Gesammelte Werke*: (a) vol. VII, p. 393-400; (b) vol. VI, p. 254-274.
3. V. A. Lebesgue: (a) J. Math. Pures Appl. vol. 2 (1837) p. 253-292; (b) J. Math. Pures Appl. vol. 3 (1838) p. 113-144.
4. G. H. Hardy and J. E. Littlewood, Math. Zeit. vol. 12 (1922) p. 161-188.
5. H. Davenport and H. Hasse, J. Reine Angew. Math. vol. 172 (1935) p. 151-182.
6. L. K. Hua and H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A. vol. 34 (1948) p. 258-263.
7. L. Stickelberger, Math. Ann. vol. 37 (1890) p. 321-367.
8. Ch. Ehresmann, Ann. of Math. vol. 35 (1934) p. 396-443.

Université de Chicago

[6] Ajouté à la preuve. Les résultats, substantiellement identiques à notre formule (3), viennent juste d'être publiés par L. K. Hua et H. S. Vandiver, Proc. Nat. Acad. Sci. U.S.A. vol. 35 (1949) p. 94-99.