I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a été consacré à la question suivante :

Quel est le nombre maximum de points rationnels que peut avoir une courbe algébrique de genre g sur un corps fini $\mathbf{F}_q$ *?*

Notons $N_q(g)$ ce maximum. D'après un théorème classique de Weil, on a

(1) $$N_q(g) \leqslant q + 1 + 2gq^{1/2}.$$

Cette inégalité peut souvent être améliorée, comme l'ont montré entre autres Stark, Ihara et Drinfeld-Vladut. On dispose de plusieurs méthodes :

1. *Utilisation des « formules explicites »*

Cette méthode, inspirée de celles de Ihara et Drinfeld-Vladut, avait été exposée dans le Séminaire 1982-1983 (voir aussi *C.R. Acad. Sci. Paris,* t. 296, mars 1983, p. 397-402). La borne qu'elle fournit pour $N_q(g)$ dépend d'un polynôme trigonométrique auxiliaire :

$f(\theta) = 1 + \sum_{n \geqslant 1} u_n \cos n\theta$, avec $u_n \geqslant 0$ et $f(\theta) \geqslant 0$ pour tout θ.

Elle s'écrit :

(2) $$N_q(g) \leqslant 1 + (2g + \sum_{n \geqslant 1} u_n q^{n/2})/(\sum_{n \geqslant 1} u_n q^{-n/2}).$$

2. *Utilisation des traces d'entiers algébriques totalement positifs*

Soit C une courbe algébrique (lisse, projective, absolument irréductible) de genre g sur $\mathbf{F}_q$, et soit N(C) le nombre de ses points rationnels. D'après Weil, on a

(5) $$N(C) = q + 1 - \Sigma\,(\pi_i + \bar{\pi}_i), \text{ avec } |\pi_i| = q^{1/2},$$

où les π_i, $\bar{\pi}_i$ $(1 \leqslant i \leqslant g)$ sont les valeurs propres de l'endomorphisme de Frobenius de C. Soit $m = [2q^{1/2}]$ la partie entière de $2q^{1/2}$. Posons :

(6) $$x_i = m + 1 + \pi_i + \bar{\pi}_i \qquad (1 \leqslant i \leqslant g).$$

Les x_i sont des entiers algébriques > 0, et la famille des x_i est stable par conjugaison sur $\mathbf{Q}$. En particulier, Πx_i est un entier > 0. D'où :

$$\frac{1}{g}\,\Sigma\, x_i \geqslant (\Pi x_i)^{1/g} \geqslant 1,$$

et l'on en déduit :

(7.1) $$\Sigma x_i \geqslant g\ ;$$

(7.2) *Si* $\Sigma x_i = g$, *on a* $(x_1, \ldots, x_g) = (1, 1, \ldots, 1)$.

En utilisant un théorème de Siegel (*Ges. Abh.*, III, n° 48), on peut aller plus loin, et déterminer dans quels cas la somme des x_i est égale à $g + 1$, ou $g + 2$ (des calculs sur ordinateur de C.J. Smyth permettent même d'aller jusqu'à $g + 6$). Pour $g + 1$, on trouve :

(7.3) *Si* $\Sigma x_i = g + 1$, *deux cas seulement sont possibles* (à permutation près des indices $1, \ldots, g$) :

$$(x_1, \ldots, x_g) = (2, 1, 1, \ldots, 1)$$

et

$$(x_1, \ldots, x_g) = (\varepsilon, \varepsilon', 1, \ldots, 1) \text{ où } \varepsilon = (3 + \sqrt{5})/2,\ \varepsilon' = (3 - \sqrt{5})/2.$$

En combinant (5), (6) et (7.1), on obtient :

(8) $$N(C) \leqslant q + 1 + gm,$$

d'où évidemment :

(9) $$N_q(g) \leqslant q + 1 + gm \qquad (\text{avec } m = [2q^{1/2}]),$$

ce qui est plus précis que (1) lorsque q n'est pas un carré.

De plus, (7.2) montre que, s'il y a égalité dans (8), tous les $\pi_i + \bar{\pi}_i$ sont égaux à $-m$ (ce qui donne un précieux renseignement sur la jacobienne de la courbe C). Quant à (7.3), on peut l'utiliser pour prouver que $N(C) = q + gm$ entraîne $g \leqslant 2$.

Remarque. De façon plus générale, si π est l'endomorphisme de Frobenius de la cohomologie (en dimension $r \geqslant 0$) d'une variété projective lisse sur $\mathbf{F}_q$, on a

(10) $$|\mathrm{Tr}(\pi)| \leqslant \frac{b}{2}\,[2q^{r/2}],$$

4. *Autres déterminations des* $N_q(g)$

Le cours s'est terminé par une brève discussion du cas $g = 3$. Une difficulté nouvelle apparaît, liée à l'ambiguïté de signe du théorème de Torelli (dans le cas non hyperelliptique) : une variété abélienne de dimension 3, munie d'une polarisation principale indécomposable, n'est pas toujours une jacobienne *sur le corps de base* donné ; il peut être nécessaire de la « tordre » par une extension quadratique. Une telle torsion remplace l'endomorphisme de Frobenius par son opposé : à la place d'une courbe ayant beaucoup de points rationnels, on en obtient une qui en a très peu. Cette difficulté a empêché de donner une détermination générale de $N_q(3)$; il a fallu se borner à $q < 23$.

Le tableau suivant résume les résultats obtenus :

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27
$N_q(1)$	5	7	9	10	13	14	16	18	21	25	26	28	33	36	38
$N_q(2)$	6	8	10	12	16	18	20	24	26	33	32	36	42	46	48
$N_q(3)$	7	10	14	16	20	24	28	28	32	38	40	44	?	56	?
$N_q(4)$	8	12	15	18	?	?	?	?	?	?	?	?	?	66	?

Missions

Exposés

— *Problems on modular forms,* Durham, juillet 1983 (2 exposés) ;

— *On Faltings' proof of Mordell conjecture,* Durham, juillet 1983 ; Institute for Advanced Study, Princeton, novembre 1983 ;

— *Number of points of curves over finite fields,* Noordwijkerhout, Pays-Bas, juillet 1983 ; Harvard, septembre 1983 ; Johns Hopkins University, octobre 1983 ; Berkeley (M.S.R.I.), octobre 1983 ; Institute for Advanced Study, Princeton, octobre-novembre 1983 (8 exposés) ; Lehigh University, décembre 1983 ; British Mathematical Colloquium, Bristol, avril 1984 ; Leningrad, avril 1984 ; Moscou, avril 1984 (4 exposés) ;

— *Rational points on algebraic varieties,* Berkeley, octobre 1983 ; Pitcher lectures, Lehigh University, décembre 1983 (3 exposés) ;

— *Opening adress,* Armand Borel Colloquium, Institute for Advanced Study, Princeton, octobre 1983 ;

— *An algebraic application of the second Stiefel-Whitney class,* John C. Moore Colloquium, Princeton University, novembre 1983 ;

où b est le nombre de Betti correspondant. Cela se démontre de la même manière, en remplaçant le théorème de Weil par celui de Deligne.

3. *Détermination de* $N_q(g)$ *pour* $g = 1$ *et* $g = 2$

On conserve les notations ci-dessus ; en particulier, m désigne la partie entière de $2q^{1/2}$. On note p la caractéristique de $\mathbf{F}_q$; on a $q = p^e$, avec $e \geqslant 1$.

3.1. *Le cas* $g = 1$

Ce cas est bien connu (Deuring, Tate, Waterhouse). On trouve que $N_q(1)$ est égal à $q + 1 + m$ (i.e. la borne (9) est atteinte), *sauf* si e est impair $\geqslant 3$ et m est divisible par p, auquel cas $N_q(1)$ est égal à $q + m$.

(La plus petite valeur exceptionnelle de q est $q = 128$, qui correspond à $p = 2$, $e = 7$, $m = 22$, $N_q(1) = 150$. Autres exemples : $q = 2^{11}, 2^{15}, 3^7, 5^9, 7^5, \ldots$).

3.2. *Le cas* $g = 2$

Ce cas a occupé la plus grande partie du cours. Le résultat obtenu est analogue à celui du genre 1 :

$N_q(2)$ est « en général » égal à la borne (9), i.e. $q + 1 + 2m$. Les valeurs exceptionnelles de q sont :

$q = 4, 9$;
q non carré, et m divisible par p ;
q non carré, de la forme $x^2 + 1$, $x^2 + x + 1$ ou $x^2 + x + 2$, avec $x \in \mathbf{Z}$.

Pour de tels q, $N_q(2)$ est égal, soit à $q + 2m$, soit à $q + 2m - 1$, soit à $q + 2m - 2$ (ce cas ne se produit que pour $q = 4$).

L'un des points essentiels de la démonstration consiste à construire des courbes de genre 2 ayant beaucoup de points rationnels. Indiquons par exemple comment on procède quand q n'est pas un carré, et n'est pas exceptionnel. On part d'une courbe elliptique E sur $\mathbf{F}_q$ ayant $q + 1 + m$ points, et dont l'anneau d'endomorphismes R soit réduit à $\mathbf{Z}[\pi]$, où π est l'endomorphisme de Frobenius. L'anneau R est un ordre d'un corps quadratique imaginaire, de discriminant $d = m^2 - 4q$; comme q n'est pas exceptionnel, on a $d < -7$. On choisit alors un module hermitien unimodulaire P sur R, projectif de rang 2, positif non dégénéré, et indécomposable (il en existe du fait que $d < -7$). Soit $A = P \otimes_R E$; c'est une variété abélienne de dimension 2, isogène à $E \times E$. La structure hermitienne de P munit A d'une polarisation principale, qui est indécomposable. Il en résulte (théorème de Torelli en dimension 2) que A est la jacobienne d'une courbe C de genre 2, et il est immédiat que $N(C) = q + 1 + 2m$; on a donc bien $N_q(2) = q + 1 + 2m$ dans ce cas. (Cette construction de courbes de genre 2 au moyen de formes hermitiennes est due à Hayashida-Nishi dans le cas complexe.)

La détermination du meilleur choix de f est un problème de programmation linéaire, résolu par J. Oesterlé pour $q \geqslant 3$ (exposé au Séminaire 1982-1983 - non publié). Pour $g \leqslant (q - q^{1/2})/2$, le meilleur choix est $f(\theta) = 1 + \cos\theta$, ce qui redonne la borne de Weil (1). Cette méthode ne conduit donc à des résultats nouveaux que lorsque $g > (q - q^{1/2})/2$, autrement dit lorsque g est « grand » relativement à q (c'est d'ailleurs le cas le plus intéressant pour la théorie des codes, d'après Goppa).

Le cours s'est borné à rappeler ces résultats, et à donner deux exemples liés aux *groupes de Suzuki et de Ree* :

(a) En prenant $f(\theta) = \dfrac{1}{2}(1 + \sqrt{2}\cos\theta)^2 = 1 + \sqrt{2}\cos\theta + \dfrac{1}{2}\cos 2\theta$, on obtient, grâce à (2) :

$$N_q(g) \leqslant q^2 + 1 \quad \text{si} \quad g \leqslant b(q) = (q^{3/2} - q^{1/2})/\sqrt{2}. \tag{3}$$

Lorsque q est de la forme 2^e, avec e impair, la courbe de Deligne-Lusztig associée au groupe de Suzuki ${}^2B_2(q)$ est de genre $b(q)$ et a $q^2 + 1$ points rationnels (après adjonction de ses points à l'infini) ; cela montre que (3) est optimal dans ce cas.

(b) En prenant $f(\theta) = \dfrac{1}{3}\cos^2\theta\,(\sqrt{3} + 2\cos\theta)^2$, on obtient :

$$N_q(g) \leqslant q^3 + 1 \quad \text{si} \quad g \leqslant g(q) = \frac{\sqrt{3}}{2}(q^{5/2} - q^{1/2}) + \frac{1}{2}(q^2 - q). \tag{4}$$

Lorsque $q = 3^e$, avec e impair, la courbe de Deligne-Lusztig associée au groupe de Ree ${}^2G_2(q)$ est de genre $g(q)$ et a $q^3 + 1$ points rationnels ; cela montre que (4) est optimal dans ce cas.

D'autres applications de (2) avaient été données dans le Séminaire 1982-1983 :

(c) *Résultats asymptotiques*

Soit $A(q) = \limsup N_q(g)/g$ pour $g \to \infty$ (q étant fixé). On a $A(q) \leqslant q^{1/2} - 1$ (Drinfeld-Vladut), et il y a égalité lorsque q est un carré (Ihara, Tsfasman-Vladut-Zink). Lorsque q n'est pas un carré, on ignore la valeur de $A(q)$; on peut seulement prouver (au moyen de tours de corps de classes) que $A(q) \geqslant c \log q$, où c est une constante absolue > 0.

(d) *Détermination de* $N_q(g)$ *pour* $q = 2$, *et* g *assez petit* :

g	0	1	2	3	4	5	6	7	8	9	15	19	21	39	50
$N_2(g)$	3	5	6	7	8	9	10	10	11	12	17	20	21	33	40

— *Applications of symmetric powers to eigenvalues of Hecke operators,* Institute for Advanced Study, Princeton, novembre 1983 ;

— *Minkowski, Smith, et l'Académie des Sciences,* Séminaire d'Histoire des Mathématiques, Paris, février 1984 ;

— *L'invariant de Witt de la forme* $Tr(x^2)$, Zürich, février 1984 ;

— *The Ramanujan Function,* Leningrad, avril 1984 ;

— *Kajdan's Property, and Groups acting on Trees,* Séminaire Gelfand, Moscou, avril 1984 ;

— ℓ*-adic representations,* Arbeitstagung, Bonn, juin 1984.