GÉOMÉTRIE ALGÉBRIQUE. — *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini.* Note (*) de **Jean-Pierre Serre,** Membre de l'Académie.

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

$$N \leqq q+1+2gq^{1/2}.$$

Nous montrons comment on peut préciser cette inégalité dans divers cas particuliers, complétant ainsi des résultats antérieurs de Stark, Ihara et Drinfeld-Vladut. Nous déterminons notamment le maximum de N lorsque $g=2$ (et q est premier), et aussi lorsque $q=2$ (et $g \leqq 9$, ou $g=15$, 19, 21, 39, 50).

ALGEBRAIC GEOMETRY. — On the Number of Rational Points of an Algebraic Curve over a Finite Field.

Let C *be an algebraic curve of genus* g *over* $\mathbf{F}_q$, *and let* N *be the number of its rational points. By Weil's inequality, we have:*

$$N \leqq q+1+2gq^{1/2}.$$

Recent results of Stark, Ihara and Drinfeld-Vladut show that this bound can often be sharpened. We give some more results in that direction. For instance, we determine the maximum of N *when* $g=2$ (*and* q *is prime*), *and when* $q=2$ (*and* $g \leqq 9$, *or* $g=15$, 19, 21, 39, 50).

NOTATIONS. — On pose $q=p^e$, avec p premier, $e \geqq 1$. Par une *courbe* sur $\mathbf{F}_q$ on entend une courbe projective, lisse, et absolument irréductible. Si C est une telle courbe, on note $g=g(C)$ son *genre*, et $N=N(C)$ le *nombre de ses points rationnels* (sur $\mathbf{F}_q$).

Dans [11], Weil démontre l'inégalité :

$$|N-(q+1)| \leqq 2gq^{1/2}. \tag{1}$$

UNE MAJORATION ÉLÉMENTAIRE. — Notons, comme d'habitude, $[x]$ la partie entière d'un nombre réel x. La majoration (1) peut se récrire :

$$|N-(q+1)| \leqq [2gq^{1/2}]. \tag{2}$$

En voici une amélioration :

THÉORÈME 1. — *On a :*

$$|N-(q+1)| \leqq g[2q^{1/2}]. \tag{3}$$

[Par exemple, pour $g=2$, $q=23$, (2) donne $|N-24| \leqq 19$, alors que (3) donne $|N-24| \leqq 18$, qui est optimal, *cf.* th. 2 ci-après.]

Le théorème 1 se déduit d'un résultat général (et facile) sur les variétés abéliennes : si A est une telle variété, définie sur $\mathbf{F}_q$, et si π est son endomorphisme de Frobenius, on a :

$$|\mathrm{Tr}(\pi)| \leqq g[2q^{1/2}] \qquad \text{avec} \quad g=\dim A. \tag{4}$$

De plus, on ne peut avoir égalité que si le polynôme caractéristique de π est égal à $(X^2 \pm mX+q)^g$, où $m=[2q^{1/2}]$.

DÉFINITION DE $N_q(g)$. — Pour g et q fixés, on note $N_q(g)$ le maximum de $N(C)$, lorsque C parcourt les courbes de genre g sur $\mathbf{F}_q$. D'après (3), on a :

$$N_q(g) \leqq q+1+g[2q^{1/2}]. \tag{5}$$

LES CAS $g=1$ ET $g=2$. — On suppose, pour simplifier, que $e=1$, *i. e.* que $q=p$.

Lorsque $g=1$, on sait (*cf.* [10], th. 4.1) que $N(C)$ peut prendre toutes les valeurs entières satisfaisant à (1). En particulier :

$$N_p(1)=p+1+[2p^{1/2}]. \tag{6}$$

Lorsque $g=2$, la situation est moins simple. Pour énoncer le résultat, convenons de dire que p est *exceptionnel* s'il est, soit de la forme n^2+1, soit de la forme n^2+n+1, avec $n\in\mathbb{Z}$. Lorsque p n'est pas exceptionnel, la borne (5) est exacte. Plus précisément :

THÉORÈME 2. — *On a :*

$$N_p(2)=\begin{cases} 6 & si \quad p=2, \\ p-1+2[2p^{1/2}] & si \quad p \text{ est exceptionnel}, p\geqq 3 \\ p+1+2[2p^{1/2}] & si \quad p \text{ n'est pas exceptionnel.} \end{cases}$$

La démonstration utilise [2] et [8]. Pour $p\geqq 3$, le résultat peut se reformuler en disant que $N_p(2)=p+1+2[\sqrt{4p-5}]$.

COROLLAIRE. — *Le nombre minimal de points rationnels d'une courbe de genre 2 sur* $\mathbf{F}_p$ *est :*

$$\begin{cases} 0 & si \quad p\leqq 11, \\ p+3-2[2p^{1/2}] & si \quad p \text{ est exceptionnel}, p\geqq 3, \\ p+1-2[2p^{1/2}] & si \quad p \text{ n'est pas exceptionnel.} \end{cases}$$

En effet, un argument de « torsion » montre que ce minimum est égal à $2p+2-N_p(2)$.

TABLEAU

p	$N_p(2)$	p	$N_p(2)$	p	$N_p(2)$
2	6	13	26	31	52
3	8	17	32	37	60
5	12	19	36	41	66
7	16	23	42	43	68
11	24	29	50	47	74

(Noter le cas $p=13$, déjà traité par Stark [7] au moyen d'une variante de la méthode de Stepanov.)

UTILISATION DES « FORMULES EXPLICITES » DE WEIL. — Revenons à une courbe C de genre g sur $\mathbf{F}_q$. Pour tout entier $d\geqq 1$, notons $a_d=a_d(C)$ le *nombre de points de degré d* de C (précisons qu'il s'agit de *points fermés* du $\mathbf{F}_q$-schéma C) ; on a $N(C)=a_1(C)$. La fonction zêta de C est donnée par le produit eulérien :

$$Z(T)=\prod_{d\geqq 1} 1/(1-T^d)^{a_d}. \tag{7}$$

D'après Weil [11], on a :

$$Z(T)=L(T)/(1-T)\,(1-qT), \tag{8}$$

où L(T) est un polynôme de degré $2g$, que l'on peut écrire sous la forme :

$$L(T)=\prod_{\alpha=1}^{\alpha=g}(1-z_\alpha T)\,(1-\bar{z}_\alpha T), \tag{9}$$

avec :

$$z_\alpha=q^{1/2}\,e^{i\theta_\alpha}, \qquad \theta_\alpha\in\mathbf{R}.$$

Soit d'autre part :

$$f(\theta)=1+2\sum_{n\geq 1} c_n\cos n\theta, \tag{10}$$

un polynôme trigonométrique pair, à coefficients réels, dont le terme constant est égal à 1. Si d est un entier $\geqq 1$, définissons un polynôme $\psi_d(t)$ par :

$$\psi_d(t)=\sum_{n\geq 1} c_{dn}\,t^{dn}. \tag{11}$$

En particulier :

$$\psi_1(t)=\sum_{n\geq 1} c_n\,t^n. \tag{12}$$

On vérifie immédiatement la « formule explicite » (au sens de Weil [12]) que voici :

$$\sum_{\alpha=1}^{\alpha=g} f(\theta_\alpha)+\sum_{d\geq 1} da_d\,\psi_d(q^{-1/2})=g+\psi_1(q^{-1/2})+\psi_1(q^{1/2}). \tag{13}$$

Supposons maintenant que f satisfasse aux deux conditions :

(*a*) $f(\theta)\geqq 0$ *pour tout* $\theta\in\mathbf{R}$;

(*b*) $c_n\geqq 0$ *pour tout* $n\geqq 1$;

ce que nous écrirons $f\gg 0$. On déduit de (13) l'inégalité suivante, valable pour tout entier $k\geqq 1$:

$$(N-1)\,\psi_1(q^{-1/2})+\sum_{2\leqq d\leqq k} da_d\,\psi_d(q^{-1/2})\leqq g+\psi_1(q^{1/2}). \tag{14}$$

En particulier, pour $k=1$:

$$N\leqq a_f g+b_f, \tag{15}$$

avec :

$$a_f=1/\psi_1(q^{-1/2}) \qquad \text{et} \qquad b_f=1+\psi_1(q^{1/2})/\psi_1(q^{-1/2}).$$

Grâce à (15), tout $f\gg 0$ donne une majoration de N, donc aussi une majoration de $N_q(g)$. Ainsi, $f(\theta)=1+\cos\theta$ conduit à la majoration de Weil. Lorsque $g>(q-q^{1/2})/2$, d'autres choix de f donnent de meilleures majorations; il existe d'ailleurs des choix « optimaux », qui ont été déterminés par J. Oesterlé (au moins pour $q\geqq 3$). La situation est analogue à celle des *minorations de discriminants* de corps de nombres (*cf.* [6]), l'analogie fonctionnant de la manière suivante :

corps de nombres	$\Leftrightarrow$	courbe algébrique
degré	...	nombre de points
$\log\lvert discr.\rvert$	...	genre
géométrie des nombres	...	théorie des codes

APPLICATION : MAJORATIONS ASYMPTOTIQUES. — Soit $\{ C^\lambda \}$ ($\lambda = 1, 2, \ldots$) une suite de courbes sur $\mathbf{F}_q$ dont les genres g^λ tendent vers $+\infty$. Notons a_d^λ le nombre de points de C^λ de degré d ($d = 1, 2, \ldots$). Fixons un entier $k \geqq 1$.

THÉORÈME 3. — *On a :*

$$\limsup \frac{1}{g^\lambda} \sum_{d=1}^{k} d a_d^\lambda / (q^{d/2} - 1) \leqq 1 \quad (\textit{pour } \lambda \to \infty). \tag{16}$$

Pour $k = 1$, ce théorème est dû à Drinfeld-Vladut [1]. Le cas général se démontre de la même manière : on applique (14) à une suite de fonctions $f \gg 0$ tendant vers la mesure de Dirac à l'origine sur $\mathbf{R}/2\pi\mathbf{Z}$; les c_n tendent vers 1, et $\psi_d(q^{-1/2})$ tend vers $1/(q^{d/2} - 1)$; en passant à la limite, on obtient (16).

Comme application, on a le résultat suivant, dû à Ihara [4] :

COROLLAIRE. — *Soient* C *une courbe de genre* g *sur* $\mathbf{F}_q$ *et* S *un ensemble non vide de points de* C. *Supposons qu'il existe des revêtements non ramifiés* $C^\lambda \to C$, *de degrés* n^λ *tendant vers* $+\infty$, *tels que tout point de* S *se décompose complètement dans chacun des* C^λ. *On a alors :*

$$\sum_{P \in S} \deg(P)/(q^{\deg(P)/2} - 1) \leqq g - 1. \tag{17}$$

On peut supposer S fini. On applique alors (16) aux C^λ, en prenant $k \geqq \deg(P)$ pour tout $P \in S$; comme $g^\lambda = 1 + n^\lambda (g-1)$ et $a_d^\lambda \geqq n^\lambda \sum_{\deg(P)=d} 1$, on obtient bien (17).

LE NOMBRE $A(q)$. — On le définit (*cf.* [1], [3], [5]) par la formule :

$$A(q) = \limsup N_q(g)/g \quad \text{pour} \quad g \to \infty. \tag{18}$$

D'après Drinfeld-Vladut [1], on a :

$$A(q) \leqq q^{1/2} - 1 \quad (\textit{cf.} \text{ th. 3, avec } k = 1). \tag{19}$$

Lorsque q est un carré, Ihara [3] a montré que $A(q)$ *est égal à* $q^{1/2} - 1$ (*voir* aussi [9]). Lorsque q n'est pas un carré (i. e. $q = p^e$, avec e impair), on ne connaît pas la valeur de $A(q)$. On peut toutefois démontrer :

THÉORÈME 4. — *On a* $A(q) > 0$.

La démonstration utilise des « tours de corps de classes » à la Golod-Šafarevič. Elle prouve en fait un résultat un peu plus précis, à savoir *l'existence d'une constante* $c > 0$ *telle que* :

$$A(q) \geqq c \log q \quad \text{pour tout } q. \tag{20}$$

Exemple. — Si $q = 2$, la borne de Weil (1) donne $A(2) \leqq 2\sqrt{2} = 2{,}828\ldots$; la borne (3) donne $A(2) \leqq 2$, et la borne de Drinfeld-Vladut (19) donne $A(2) \leqq \sqrt{2} - 1 = 0{,}414\ldots$ D'autre part, une construction de « tour » convenable permet de montrer que $A(2) \geqq 8/39 = 0{,}205\ldots$

LE CAS DU CORPS $\mathbf{F}_2$. — Il est possible de déterminer $N_2(g)$ pour certaines valeurs de g :

THÉORÈME 5. — *Les valeurs de* $N_2(g)$ *pour* $g \leqq 9$, *et pour* $g = 15, 19, 21, 39, 50$ *sont données par le tableau suivant :*

TABLEAU

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

Dans chaque cas (celui de $g=7$ excepté), on *majore* $N = N_2(g)$ au moyen de la formule (15) appliquée à un polynôme trigonométrique $f \geqslant 0$ convenable. On peut, par exemple, prendre f de la forme

$$f(\theta) = c^{-1}(1 + 2x_1 \cos\theta + 2x_2 \cos 2\theta + \ldots)^2,$$

avec $x_i \geqq 0$ et $c = 1 + 2\sum x_i^2$.

Ainsi, le choix :

$$x_1 = 1; \qquad x_2 = 0{,}7; \qquad x_3 = 0{,}2; \qquad x_4 = x_5 = \ldots = 0$$

conduit à :

$$N \leqq 0{,}83\,g + 5{,}35, \tag{21}$$

qui donne les bornes voulues pour $g = 3, 4, 5, 6, 8, 9, 15$.

De même, le choix :

$$x_1 = 1; \qquad x_2 = 0{,}8; \qquad x_3 = 0{,}6; \qquad x_4 = 0{,}4; \qquad x_5 = 0{,}1; \qquad x_6 = x_7 = \ldots = 0$$

conduit à :

$$N \leqq 0{,}6272\,g + 9{,}562, \tag{22}$$

qui, pour $g = 50$, donne $N \leqq 40{,}922$ d'où $N \leqq 40$.

Le cas $g = 7$ est spécial. La formule (15), avec le meilleur choix possible de f, donne seulement $N \leqq 11$ (et non $N \leqq 10$) ; il faut une étude directe pour montrer que $N = 11$ est impossible.

En ce qui concerne les *minorations*, elles se font en construisant des courbes ayant le nombre de points imposé. Pour $g \leqq 4$, on se sert d'équations explicites. Ainsi, pour avoir une courbe de genre 3 sur $\mathbf{F}_2$ ayant 7 points rationnels, on prend la quartique plane d'équation homogène :

$$x^3y + y^3z + z^3x + x^2y^2 + y^2z^2 + z^2x^2 + x^2yz + xy^2z = 0;$$

cette quartique est non singulière (donc de genre 3), et passe par les 7 points du plan projectif, d'où $N = 7$. Pour $g \geqq 5$, cette méthode est difficilement applicable ; il est plus commode d'utiliser des revêtements abéliens de courbes déjà construites, revêtements dont l'existence est assurée par la théorie du corps de classes.

Par exemple, soit E une courbe de genre 1 ayant 5 points rationnels, et soit P_n un point de E de degré $n \geqq 5$. On prouve facilement l'existence d'un revêtement abélien $C \to E$, de degré 2^{n-4}, ramifié seulement en P_n (l'exposant du conducteur étant 2), et dans lequel les 5 points rationnels de E se décomposent complètement. On a $g(C) = 1 + n(2^{n-4} - 1)$ et $N(C) = 5.2^{n-4}$. Pour $n = 5$, 6 ou 7, cette construction fournit des courbes de genre 6, 19 ou 50 ayant 10, 20 ou 40 points rationnels.

(*) Remise le 14 février 1983.

[1] V. G. DRINFELD et S. G. VLADUT, *Sur le nombre de points d'une courbe algébrique* [en russe], *Anal. fonct. et appl.*, 17, 1983, (à paraître).

[2] T. HAYASHIDA et M. NISHI, *Existence of Curves of Genus two on a Product of two Elliptic Curves, J. Math. Soc. Japan*, 17, 1965, p. 1-16.

[3] Y. IHARA, *Some Remarks on the Number of Rational Points of Algebraic Curves over Finite Fields, J. Fac. Sc. Tokyo*, 28, 1981, p. 721-724.

[4] Y. IHARA, *How Many Primes Decompose Completely in an Infinite Unramified Galois Extension of a Global Field?*, Tokyo, 1982 (prépublication).

[5] Y. MANIN, *What is the Maximum Number of Points on a Curve over* F_2*?, J. Fac. Sc. Tokyo*, 28, 1981, p. 715-720.

[6] G. POITOU, *Minorations de discriminants* (*d'après A. M. Odlyzko*), Sém. Bourbaki 1975/1976, exposé 479, *Lect. Notes in Math.* n° 567, 1977, p. 136-153 (*voir* aussi Sém. DPP 1976/1977, exposé n° 6).

[7] H. STARK, *On the Riemann Hypothesis in Hyperelliptic Function Fields, Proc. A.M.S. Symp. Pure Math.*, 24, 1973, p. 285-302.

[8] J. TATE, *Endomorphisms of Abelian Varieties over Finite Fields, Inv. math.*, 2, 1966, p. 134-144.

[9] M. A. TSFASMAN, S. G. VLADUT et T. ZINK, *Modular Curves, Shimura Curves, and Goppa Codes Better than Warshamov-Gilbert Bound, Math. Nach.*, 109, 1983 (à paraître).

[10] W. C. WATERHOUSE, *Abelian Varieties over Finite Fields, Ann. Sc. E.N.S.*, (4), 2, 1969, p. 521-560.

[11] A. WEIL, *Variétés abéliennes et courbes algébriques*, Hermann, Paris, 1948.

[12] A. WEIL, *Sur les « formules explicites » de la théorie des nombres premiers, Comm. Lund*, 1952, p. 252-265 (=*Oeuvres Sc.*, II, p. 48-61).

Collège de France, 75231 *Paris Cedex* 05.