SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

M. PERRET

Nombre maximum de points rationnels d'une courbe sur un corps fini

Séminaire de Théorie des Nombres de Bordeaux, tome 3, n° 2 (1991), p. 261-274

<http://www.numdam.org/item?id=JTNB_1991__3_2_261_0>

© Université Bordeaux 1, 1991, tous droits réservés.

L'accès aux archives de la revue « Séminaire de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire de Théorie des Nombres,
Bordeaux **3** *(1991), 261-274*

Nombre maximum de points rationnels d'une courbe sur un corps fini.

par M. PERRET

Soit $\mathbb{F}_q$ le corps fini à q éléments. Une courbe projective irréductible $C \subset \mathbb{P}^n_{\overline{\mathbb{F}_q}}$ est le lieu des zéros de s polynômes homogènes indépendants en $n+1$ variables à coefficients dans $\mathbb{F}_q$, tels que l'idéal $P_1, \cdots, P_s) \subset \overline{\mathbb{F}_q}[X_0, \cdots, X_n]$ soit un idéal premier de hauteur $n-1$. Elle est dite lisse si la matrice Jacobienne de ces s polynômes est de rang $n-1$ en tout point de la courbe. A une telle courbe, on associe un entier positif g, appelé le genre de C.

L'objet de cet exposé est de montrer de quelle façon cet invariant g gouverne le nombre de points rationnels de C sur $\mathbb{F}_q$ (c'est à dire le nombre de points de la courbe à coordonnées dans $\mathbb{F}_q$), noté $C(\mathbb{F}_q)$. Le premier paragraphe est consacré aux bornes valables pour toutes les valeurs de g : borne de Weil (améliorée par Serre), et borne relative à un revêtement. Dans le second paragraphe, on donne les valeurs $N_q(g)$ du nombre maximum de points rationnels sur $\mathbb{F}_q$ d'une courbe de genre g lorsque celui-ci est connu, c'est à dire seulement dans les cas $g = 0$, 1 et 2. On donne aussi un exemple de construction d'une courbe de petit genre ayant beaucoup de points rationnels. Enfin, le dernier paragraphe est consacré à l'étude de la quantité $A(q) = \limsup_{g \to \infty} N_q(g)/g$. On construit par la théorie du corps de classes une suite de courbes, et on conjecture un critère de non finitude de celle-ci, conjecture démontrée dans le cas des revêtements non ramifiés. On applique alors cette construction pour donner plusieurs minorations de $A(q)$.

I. Estimations générales.

1. La borne de Weil.

On considère la fonction Zêta de C :

$$Z_C(T) \stackrel{def}{=} \exp\left(\sum_{i=1}^{\infty} \sharp C(\mathbb{F}_{q^n}) \frac{T^n}{n}\right),$$

qui est en fait une fraction rationnelle :

Manuscrit reçu le 28.06.1991 .

THÉORÈME 1 (WEIL, 1948, [14]). *Il existe un polynôme unitaire $P_C(T) \in \mathbb{Z}[T]$, de degré $2g$, tel que*

$$Z_C(T) = \frac{P_C(T)}{(1-T)(1-qT)}.$$

De plus, les racines inverses ω_i de P_C sont des nombres algébriques conjugués deux à deux, de modules $|\omega_i| = \sqrt{q}$.

La dernière assertion est connue sous le nom d'hypothèse de Riemann. Ainsi,

$$Z_C(T) = \prod_{i=1}^{g} \frac{(1-\omega_i T)(1-\overline{\omega_i} T)}{(1-T)(1-qT)}.$$

On en déduit

$$\frac{Z_C'(T)}{Z_C(T)} = \frac{1}{1-T} + \frac{q}{1-qT} - \sum_{i=1}^{g} \left(\frac{\omega_i}{1-\omega_i T} + \frac{\overline{\omega_i}}{1-\overline{\omega_i} T} \right),$$

d'où, pour $T = 0$:

$$\sharp C(\mathbb{F}_q) = \frac{Z_C'(0)}{Z_C(0)} = q + 1 - \sum_{i=1}^{g} (\omega_i + \overline{\omega_i}).$$

Compte tenu du théorème 1, on en déduit aussitôt l'inégalité de Weil :

THÉORÈME 2 (WEIL, 1948, [14]).

$$|\sharp C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Remarques. **1.** Cela peut se reformuler comme suit :

$$|\sharp C(\mathbb{F}_q) - \sharp \mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_q)| \leq 2(g_C - g_{\mathbb{P}^1_{\mathbb{F}_q}})\sqrt{q},$$

inégalité que l'on compare à celle du théorème 3.

2. Cette inégalité entraîne à son tour la conjecture de Riemann (voir par exemple [2], exercice 5.7, page 458).

En fait, on peut être un peut plus précis :

PROPOSITION 1 (SERRE, 1983). *Soit* $n \in \mathbb{N}^*$, *et*

$$P(T) = \prod_{i=1}^{n}(1 - \alpha_i T)(1 - \overline{\alpha}_i T)$$

un polynôme à coefficients entiers. On suppose que pour tout i, α_i *est de module* $\sqrt{q}$. *Alors*

$$|\sum_{i=1}^{n}(\alpha_i + \overline{\alpha}_i)| \leq n[2\sqrt{q}],$$

où $[x]$ *désigne la partie entière du reel* x.

Démonstration. On pose $x_i = [2\sqrt{q}]+1+\alpha_i+\overline{\alpha}_i \in \overline{\mathbb{Q}}\cap\mathbb{R}_+^*$. Alors $\prod_{i=1}^{n} x_i$ est un entier naturel non nul, et par l'inégalité arithmético-géométrique,

$$\frac{1}{n}\sum_{i=1}^{n} x_i > \left(\prod_{i=1}^{n} x_i\right)^{\frac{1}{n}} \geq 1,$$

d'où $\sum_{i=1}^{n} x_i \geq n$, c'est à dire

$$\sum_{i=1}^{n}(\alpha_i + \overline{\alpha}_i) \geq -n[2\sqrt{q}].$$

En faisant le même raisonnement avec $y_i = [2\sqrt{q}] + 1 - \alpha_i - \overline{\alpha}_i$, on trouve

$$\sum_{i=1}^{n}(\alpha_i + \overline{\alpha}_i) \leq n[2\sqrt{q}].$$

COROLLAIRE (SERRE, 1983).

$$|\sharp C(\mathbb{F}_q) - (q+1)| \leq g[2\sqrt{q}].$$

Cette inégalité est meilleure que celle de Weil lorsque q n'est pas un carré. Elle est d'autant meilleure que le genre est grand. Signalons que ces deux inégalités sont utilisées pour l'estimation des paramètres des codes de Goppa (voir par exemple [4], [15] et [16]).

2. Situation relative.

Soient X et Y deux courbes algébriques projectives lisses irréductibles définies sur $\mathbb{F}_q$, de genres respectivement g_X et g_Y, et $\pi : Y \longrightarrow X$ un revêtement de Y sur X, définit sur $\mathbb{F}_q$ (cela signifie que si $X \subset \mathbb{P}^n_{\mathbb{F}_q}$ et $Y \subset \mathbb{P}^m_{\mathbb{F}_q}$, on peut localement écrire $\pi = (\pi_0, \cdots, \pi_n)$, où les π_i sont des polynômes homogènes de même degrés en $m+1$ variables à coefficients dans $\mathbb{F}_q$). A un tel revêtement, il correspond une extension des corps de fonctions $\mathbb{F}_q(X) \overset{\pi^\star}{\hookrightarrow} \mathbb{F}_q(Y)$, donnée par $\pi^\star(f)(Q) \overset{def}{=} f(\pi(Q))$ pour $f \in \mathbb{F}_q(X)$ et $Q \in Y(\overline{\mathbb{F}_q})$. Le revêtement π est dit Galoisien (resp.Abélien, de Kummer ou d'Artin-Schreier), si l'extension $\pi^\star$ l'est.

THÉORÈME 3 ([5], [8]). *Supposons que le revêtement π soit d'Artin-Schreier, ou de Kummer. Alors*

$$|\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq 2(g_Y - g_X)\sqrt{q}.$$

Là aussi, on peut remplacer le majorant par $(g_Y - g_X)[2\sqrt{q}]$. La preuve de ce théorème utilise la théorie des fonctions L : on écrit le quotient $Z_Y(T)/Z_X(T)$ comme un produit de fonctions L Abéliennes, ces dernières étant des polynômes. Le polynôme $P_X(T)$ divise donc $P_Y(T)$. On écrit alors $Z_Y(T)/Z_X(T) = \exp(\sharp Y(\mathbb{F}_q) - \sharp X(\mathbb{F}_q))T^n/n$, et on compare les coefficients de T.

CONJECTURE 1. *Le théorème 3 est vrai pour tout revêtement.*

Lors d'un récent colloque à Marseille, J.P. Serre m'a signalé que l'on peut démontrer cette conjecture en faisant un raisonnement analogue à celui ci dessus soit en considérant les Jacobiennes des deux courbes, soit en faisant appel à la cohomologie ℓ-adique.

II. Le cas des petits genres.

Dans tout ce qui suit, on note $N_q(g)$ le nombre maximum de points rationnels sur $\mathbb{F}_q$ d'une courbe de genre g, définie sur $\mathbb{F}_q$. D'après l'inégalité de Serre, on a

$$N_g(q) \leq q + 1 + g[2\sqrt{q}].$$

1. Les cas g = 0, 1, et 2.

Dans ces trois cas seulement, la valeur de $N_q(g)$ est connue explicitement. Pour $g = 0$, c'est à dire pour les courbes rationnelles, le théorème 2 montre qu'une telle courbe à toujours $q + 1$ points rationnels. Le cas des courbes elliptiques (ce sont les courbes de genre 1) est moins trivial ; il est connu depuis Hasse et Deuring :

THÉORÈME 4 (HASSE, DEURING). *Soit $q = p^n$ avec p premier, et posons $m = [2\sqrt{q}]$. Alors*

$$N_q(1) = \begin{cases} q + m & \text{si } p \text{ divise } m, \text{ et si } n \geq 3, \\ q + 1 + m & \text{sinon.} \end{cases}$$

Le cas $g = 2$ a été entièrement résolu par Serre (1983). L'énoncé est plus long :

Soit $q = p^e$ une puissance du nombre premier p, et notons $m = [2\sqrt{q}]$. On dit que q est spécial si e est impair, et si q vérifie l'une des conditions suivantes :

- p divise m
- Il existe $x \in \mathbb{Z}$, tel que $q = x^2 + 1$
- Il existe $x \in \mathbb{Z}$, tel que $q = x^2 + x + 1$
- Il existe $x \in \mathbb{Z}$, tel que $q = x^2 + x + 2$.

THÉORÈME 5 (SERRE, 1983, [11]).

- Si q est un carré, $q \neq 4, 9$, alors $N_q(2) = q + 1 + 4\sqrt{q}$; de plus, $N_4(2) = 10$ et $N_9(2) = 20$.

- Si e est est impair (c'est à dire si q n'est pas un carré), alors

$$N_q(2) = \begin{cases} q + 1 + 2m & \text{si } q \text{ n'est pas spécial} \\ \begin{cases} q + 2m & \text{si } q \text{ est spécial, et si } 2\sqrt{q} - [2\sqrt{q}] > \dfrac{\sqrt{5} - 1}{2} \\ q + 2m - 1 & \text{si } q \text{ est spécial, et si } 2\sqrt{q} - [2\sqrt{q}] \leq \dfrac{\sqrt{5} - 1}{2}. \end{cases} \end{cases}$$

2. Minorations de $N_q(g)$ par constructions explicites.

Dans cette section, on va montrer sur un exemple comment on peut exhiber, par une méthode due à Serre ([12]), une courbe de petit genre ayant

beaucoup de points rationnels. Construisons par exemple une courbe sur $\mathbb{F}_2$ de genre 6, ayant 10 points rationnels. On rappelle les résultats suivants (on trouvera un exposé plus détaillé dans [9]). Soit X une courbe projective lisse irreductible definie sur $\mathbb{F}_q$. Si S est un ensemble fini de points fermés de X, on appelle diviseur sur X porté par S une combinaison linéaire formelle

$$m = \sum_{P \in S} m_P P,$$

où pour tout $P \in S$, m_P est un entier relatif. On dit qu'une fonction $f \in \mathbb{F}_q(X)$ est congrue à 1 $mod^* m$ si $v_P(1-f) \geq m_P$ pour tout $P \in S$. On définit alors le groupe des classes de diviseurs étrangers à S *modulo*m* :

$$P_m = \frac{\left\{D = \sum_{P \notin S} d_P P \ ; \ d_P \in \mathbb{Z}\right\}}{\left\{(f) \ ; \ f \in \mathbb{F}_q(X)^* \ ; \ v_P(1-f) \geq m_P \ \forall P \in S\right\}}.$$

La théorie du corps de classes montre que P_m gouverne les revêtements Abéliens de X, de conducteur $\leq m$. Plus précisément, il y a une bijection

$$\left\{ \begin{array}{c} \text{revêtements Abéliens de } X \\ \text{de conducteur } \leq m. \end{array} \right\} \xleftrightarrow{\sim} \{ \text{ quotients finis de } P_m \}$$

Si de plus le revêtement $Y \longrightarrow X$ correspond au sous-groupe K d'indice fini de P_m, les places associées aux diviseurs irréductibles P, tels que $P \bmod^* m \in K$, sont totalement décomposées dans Y.

Revenons à la construction d'une courbe sur $\mathbb{F}_2$ de genre 6 ayant 10 points rationnels. On part d'une courbe elliptique E ayant 5 points $P_1, \cdots, P_5$ rationnels sur $\mathbb{F}_2$ (courbe dont l'existence est assurée par le théorème 4) et d'un point Q de E de degré 5 (c'est à dire un point rationnel sur $\mathbb{F}_{2^5}$, mais pas sur $\mathbb{F}_2$). Un tel point existe car d'après le théorème 2, le nombre de points rationnels de E sur $\mathbb{F}_{2^5}$ est $\geq 2^5 + 1 - 2 \times 1 \times \sqrt{2^5} > 5 =$ nombre de points rationnels de E sur $\mathbb{F}_2$. En considèrant le diviseur $m = 2Q$, on a, en notant t une uniformisante de la place Q :

$$P_m = \frac{\left\{D = \sum_{P \neq Q} d_P P \ ; \ d_P \in \mathbb{Z}\right\}}{\left\{(f) \ ; \ f \in \mathbb{F}_q(X)^* \ ; \ v_Q(1-f) \geq 2\right\}}$$

$$\simeq \mathbb{Z} \times \left\{ f = 1 + \alpha t \ (mod\ t^2) \ ; \ \alpha \in \mathbb{F}_{2^5} \right\}$$

$$\simeq \mathbb{Z} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^5.$$

Ainsi,

$$\frac{P_m}{2P_m} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^6.$$

Il y a donc une surjection de P_m dans $\left(\mathbb{Z}/2\mathbb{Z}\right)^6$, donnée par

$$P_m \xrightarrow{surj.} \frac{P_m}{2P_m} \xrightarrow{\sim} \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \right)^6.$$

Notons, pour $1 \leq i \leq 5$, $\sigma_i \in \left(\mathbb{Z}/2\mathbb{Z}\right)^6$ l'image de $P_i \bmod^* m$ par cette application. Il existe une forme linéaire non nulle ϕ de $\left(\mathbb{Z}/2\mathbb{Z}\right)^6$ contenant les σ_i dans son noyau. Cette forme linéaire induit un isomorphisme $P_m/Ker\phi \simeq \mathbb{Z}/2\mathbb{Z}$; le noyau K de ϕ définit donc un revêtement quadratique X de E, de discriminant $2Q$. Son genre est donné par la formule de Hurwitz :

$$2g_X - 2 = 2(2g_E - 2) + deg\ 2Q = 10,$$

soit $g_X = 6$. D'autre part, les 5 points $P_i \in E(\mathbb{F}_2)$ sont dans K, donc se décomposent totalement, et donnent chacun naissance à 2 points de X rationnels sur $\mathbb{F}_2$, d'où $\sharp X(\mathbb{F}_2) \geq 10$. Enfin, les formules explicites discrètes montrent, avec un bon choix de polynôme trigonométrique, que $N_2(6) \leq 10$. La courbe X a donc exactement 10 points rationnels sur $\mathbb{F}_2$, et est maximale.

III. Résultats asymptotiques.

1. La quantité A(q).

Les résultats de la section **II.1.** montrent que, à q fixé, l'inégalité de Serre est optimale pour les petites valeurs du genre ($g = 0, 1, 2$). Nous allons voir dans ce paragraphe qu'il n'en est rien pour les grandes valeurs de g. Pour cela, posons

$$A(q) \stackrel{def}{=} \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

Remarque. Cette quantité joue un rôle important dans les questions asymptotiques de la théorie des codes correcteurs d'erreurs (voir par exemple [4], [7], [13]).

La proposition 1 montre que $A(q) \leq [2\sqrt{q}]$. En fait, on peut montrer (en utilisant des formules explicites discrètes à la Weil) le théorème suivant :

THÉORÈME 6 (DRINFEL'D, VLADUT, 1983, [1]).

$$A(q) \leq \sqrt{q} - 1.$$

D'autre part, Ihara, Tsfasman, Vladut et Zink ont montré dans [3] et [13] que les courbes de Shimura atteignent cette borne lorsque q est un carré. cela montre que $A(q^2) = q - 1$, et on conjecture que c'est vrai dans tous les cas :

CONJECTURE 2. *Pour tout* q, $A(q) = \sqrt{q} - 1$.

Afin de démontrer cette conjecture, il s'agit (en vertue du théorème 6) de construire explicitement une suite $(X_n)_{n \in \mathbb{N}}$ de courbes de genre g_n tendant vers l'infini, telles que $\lim_{n \to \infty} \sharp X_n(\mathbb{F}_q)/g_n = \sqrt{q} - 1$. Dans la section suivante, nous allons donner une méthode de construction de suites de courbes ayant asymptotiquement un nombre de points proche de la conjecture 2.

2. Minorations de A(q) par constructions explicites de tours de corps de classes.

a. Construction de la tour et critère de non finitude.

Afin de construire une telle suite de courbes, on se place du point de vue arithmétique, en utilisant la correspondance

$$\left\{ \begin{array}{c} \text{Courbes algébriques } X \text{ projectives lisses} \\ \text{irréductibles définies sur } \mathbb{F}_q \end{array} \right\} \stackrel{\sim}{\longleftrightarrow} \left\{ \begin{array}{c} \text{Corps globaux } K \\ \text{contenant } \mathbb{F}_q \end{array} \right\}$$

Explicitement, une courbe X est associée à son corps de fonctions $K = \mathbb{F}_q(X)$. Dans cette correspondance, les places de degré n sur $\mathbb{F}_q$ de K correspondent aux points rationnels de X sur $\mathbb{F}_{q^n}$, non rationnels sur $\mathbb{F}_{q^d}$ pour $d|n$, $d \neq n$, et le genre de K est égal au genre de X.

On va construire la suite de corps comme suit : on considère un corps de base K (global, contenant $\mathbb{F}_q$) , deux ensembles finis disjoints $S \neq \emptyset$ et R de places de K, un nombre premier ℓ, ainsi qu'un module $m = \sum_{P \in R} m_P P$ de K porté par R. On considère alors la plus grande extension Abélienne K_a de K, d'exposant 1 ou ℓ, où les places de S se décomposent totalement, et de conducteur $\leq m$. En d'autres termes, K_a est le corps de classes du groupe de normes $W_{m,S}/W^{\ell}_{m,S}$, où

$$W_{m,S} = \prod_{P \in S} K_P^{\star} \times \prod_{P \in R} U_P^{m_P} \times \prod_{P \notin S \cup R} U_P.$$

On note alors S_a (resp.R_a) l'ensemble des places de K_a au dessus de S (resp.R), et $m_a = \sum_{P \in R} \sum_{\substack{Q \in R_a \\ Q|P}} m_P Q$. On peut alors itérer cette construction en posant

$$K_0 = K,\ S_0 = S,\ R_0 = R,\ m_0 = m,$$

et pour tout $n \geq 0$,

$$K_{n+1} = (K_n)_a,\ S_{n+1} = (S_n)_a,\ R_{n+1} = (R_n)_a,\ \text{et } m_{n+1} = (m_n)_a.$$

On a donc construit une suite $(K_n, S_n, R_n, m_n, \ell)_{n \in \mathbb{N}}$, appellée la ℓ-tour de corps de classes au dessus de (K, S, R, m). On montre alors le théorème suivant :

THÉORÈME 7 (7). *Si la tour $(K_n, S_n, R_n, m_n, \ell)_{n \in \mathbb{N}}$ est infinie, et si, pour tout $n \in \mathbb{N}$, les places de R_n sont totalement ramifiées dans K_{n+1} (ce qui est le cas si $R_0 = \emptyset$, ou si $\ell = p = car K$ et $\sharp R_0 = 1$), alors*

$$A(q) \geq \frac{\sharp S_0}{g_0 - 1 + \frac{1}{2} deg\ m}.$$

Il s'agit donc de donner un critère de non-finitude pour ces ℓ-tours, puis d'expliciter un quadruplet (K, S, R, m) tel que sa ℓ-tour de corps de classes associée soit infinie. Posons $G_1 = Gal(K_1/K_0)$, et notons d le nombre minimum de générateurs du ℓ-groupe G_1.

CONJECTURE 3. *Si $d+\sharp S \leq d^2/4$, alors la ℓ-tour au dessus de (K,S,R,m) est infinie.*

THÉORÈME 8 (SERRE, 1983, [12]). *La conjecture 3 est vraie si $R=\emptyset$.*

La conjecture 3 est liée au théorème de Golod-Shafarevich, amélioré par Gaschütz et Vinberg (si d est le nombre minimum de générateurs d'un ℓ-groupe fini G, et si r est le nombre minimum de relations entre d générateurs de G, alors $r \leq d^2/4$), et au multiplicateur de Schür $H_3(G,\mathbb{Z})$ d'un groupe fini G. Signalons enfin que cette construction, ainsi que les théorèmes et conjectures qui lui sont attachées, est valable pour les corps de nombres, pourvu que S contienne les places à l'infini de K.

b. Minorations indépendantes de la conjecture 3.

On considère le corps $k=\mathbb{F}_q(T)$, et on se donne deux parties non vides disjointes A et B de $\mathbb{F}_q$. Soit $K=k(y)$ avec $y^\ell=\prod_{\alpha\in A}(T-\alpha)$, et posons

$$S=\left\{\text{places de K au dessus des places } (T-\beta)\ ,\ \beta\in B\right\} \text{ et } R=\emptyset.$$

On montre que si $q\equiv 1\ (mod\ \ell)$, si $pgcd(\sharp A,\ell)=1$, et si tous les éléments de $B-A$ sont des puissances $\ell^{ièmes}$ dans $\mathbb{F}_q$, alors $d(G_1)\geq \sharp A-1$. Il résulte alors des théorèmes 7 et 8 la proposion suivante (cf [12] dans le cas $\ell=2$) :

PROPOSITION 2. *Soit ℓ un nombre premier tel que $q\equiv 1\ (mod\ \ell)$. Si on peut trouver deux parties non vides disjointes A et $B\subset \mathbb{F}_q$, avec*
i) $\sharp A\geq 2$, $\sharp B\geq 1$,
ii) $B-A\subset \mathbb{F}_q^{*\ell}$,
iii) $pgcd\ (\sharp A,\ell)=1$,
alors

$$A(q)\geq \frac{2\ell\sharp B}{(\sharp A-1)(\ell-1)}.$$

COROLLAIRE 1 (SERRE, 1983, [12]). *Il existe une constante $c>0$, telle que pour tout q, on ait $A(q)>c\log q$. En particulier, $A(q)>0$ pour tout q. De plus, $A(2)>\frac{2}{9}$.*

COROLLAIRE 2([7]). *Supposons que* $q > 4\ell + 1$. *Soit* k *un entier non nul, tel que* q *soit une racine primitive* $k^{ième}$ *de l'unité dans* $\mathbb{F}_\ell$. *Alors*

$$A(q^\ell) \geq \frac{\sqrt{\ell(q-1)} - 2\ell}{\ell - 1} \quad \text{si } k = 1,$$

$$A(q^k) \geq \frac{\sqrt{\ell(q-1)} - 2\ell}{\ell - 1} \quad \text{sinon.}$$

Le corollaire 1 provient d'un lemme combinatoire. Le corollaire 2, quant à lui, provient du fait que si $q \equiv 1 \ (mod\ \ell)$, tous les éléments de $\mathbb{F}_q$ sont des puissances $\ell^{ièmes}$ dans $\mathbb{F}_{q^\ell}$, et que si $pgcd\ (\ell, q-1) = 1$, tous les éléments de $\mathbb{F}_q$ sont des puissances $\ell^{ièmes}$ dans $\mathbb{F}_q$, donc aussi dans $\mathbb{F}_{q^k}$. Dans ces deux cas, on prend pour couple (A, B) une partition de $\mathbb{F}_q$, et on applique la proposition 2 à q^ℓ (resp. q^k).

c. Minorations de A(q) sous la conjecture 3.

On se place maintenant dans le cas où $\ell = p$. On se donne encore deux parties non vides disjointes A et B de $\mathbb{F}_q$, où $\sharp B$ est une puissance de p. On considère le corps $K = k(z)$, avec $k = \mathbb{F}_q(T)$ et

$$z^p - z = \Big(\prod_{\beta \in B} (T - \beta)\Big) \times \Big(\sum_{\alpha \in A} \frac{1}{(T-\alpha)^{\sharp B}}\Big).$$

On pose

$$S = \Big\{\text{places de } K \text{ au dessus des places } (T-\beta), \beta \in B \text{ de } k\Big\},$$

$$R = \{P_\infty\} = \Big\{\text{la place de } K \text{ au dessus de la place } \Big(\frac{1}{T}\Big) \text{ de } k\Big\},$$

$m = 2P_\infty$, et on considère la p-tour de corps de classes au dessus de (K, S, R, m). On montre alors que $d(G_1) \geq \sharp A - 1$, et que la condition de la conjecture 4 est vérifiée dès que $\sharp A = 3 + \lceil 2\sqrt{q+1} \rceil$ (partie entière par excès) et $\sharp B = q/p$; on peut choisir deux telles parties disjointes dans $\mathbb{F}_q$ si et seulement si $3 + \lceil 2\sqrt{q+1} \rceil + q/p \leq q$, c'est à dire si q n'est pas trop petit vis à vis de p. La conjecture 3 et le théorème 7 permettent donc d'énoncer

THÉORÈME 9 ([7]). *Sous la conjecture 3, si* $q = p^n$, $n \geq 2$, *et* $q \neq 4, 8, 9,$ *et 16, on a*

$$A(q) \geq \frac{\sqrt{q+1}-2}{2(p-1)}.$$

De façon similaire, on peut montrer en considérant des places de la forme $(T^2 - \beta)$ pour $\beta \in \mathbb{F}_q$, $\beta \notin \mathbb{F}_q^2$:

THÉORÈME 9' ([7]). *Sous la conjecture 3, si* $q = p^n$, p *impair*, $n \geq 2$, *et* $q \neq 9, 25, 27, 49, 81, 121,$ *et 169, alors*

$$A(q) \geq \frac{\sqrt{pq+1}-2}{4(p-1)}.$$

Remarque. Comme me l'a fait remarquer Tsfasman, on peut obtenir par cette méthode une minoration de $A(q)$ pour q pair en considérant des places de la forme $(T^2 - T - \beta)$ pour $\beta \in \mathbb{F}_q$, $\beta \neq b^2 - b \ \forall b \in \mathbb{F}_q$.

De ces deux théorèmes et de la proposition 2, corollaire 1, on déduit

COROLLAIRE. *Sous la conjecture 3, pour tout nombre premier* p, *il existe une constante* $c(p) > 0$ *telle que, pour toute puissance* q *de* p, *on ait*

$$A(q) \geq c(p)(\sqrt{q} - 1).$$

Si de plus on suppose q *distinct des valeurs écartées dans les théorèmes 9 et 9', on peut choisir* $c(2) = 1/3$ *et* $c(p) = 1/(p-1)$ *si* p *est impair.*

d. Comparaison avec le cas des corps de nombres.

Soit K un corps de nombre, et δ_K son discriminant absolu. Les méthodes utilisées pour l'étude asymptotique de la quantité $(\log \delta_K)/[K : \mathbf{Q}]$ sont similaires à celles employées ici. En effet, l'inégalité $\limsup_{g \to \infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1$ s'obtient via l'hypothèse de Riemann (démontée dans ce cas) et des formules explicites discrètes à la Weil, alors que l'inégalité $\liminf_{[K:\mathbf{Q}] \to \infty} (\log \delta_K)/[K : \mathbf{Q}] \geq \log 44,763$ s'obtient sous GRH et les formules explicites de Weil (par la méthode de Stark-Odlyzko).

De même, c'est en utilisant une construction analogue à celle de la section **III.2.b.** (avec $k = \mathbf{Q}$, $K = k(y)$, et $y^2 = 3.5.7.11.13.17.19$), que

Shafarevich a montré le premier l'existence d'une tour (non ramifiée) infinie de corps de nombres telle que

$$(\log \delta_K)/[K : \mathbf{Q}] = \text{ constante.}$$

Le record dans cette direction est actuellement détenu par Martinet (cf. [6]), qui a montré l'existence d'une tour infinie (non ramifiée) de corps, avec $(\log \delta_K)/[K : \mathbf{Q}] = \log 92,368\cdots$. Dans cet esprit, on peut espérer (après avoir démontré la conjecture 3) construire une tour ramifiée infinie de corps de nombres, ayant asymptotiquement un rapport $(\log \delta_K)/[K : \mathbf{Q}]$ plus petit.

RÉFÉRENCES.

[1] V.G. Drinfel'd et S.G. Vladut, *Number of points of an algebraic curve*, Funktsional'nyi Analiz i Ego Prilozheniya **17** (1983), 53-54.

[2] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer (1977).

[3] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, Journ. Fac. Sc. Tokyo, sec. 1. A, **28** (1982), 721-724..

[4] G. Lachaud, *Les codes géométriques de Goppa*, Séminaire Bourbaki 1884/85, exp. **641**, Astérisque **133-134** (1986), p. 189-207.

[5] G. Lachaud, *Artin-Shreier curves, exponential sums and the Carlitz-Uchiyama bound for geometric codes*, Journ. of Numb. Theory, vol **39**, (1991), 18-40.

[6] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Mathematicae (1978), 65-73.

[7] M. Perret, *Tours ramifiées infinies de corps de classes*, Journ. of Numb. Theory, vol **38**, (1991), 300-322.

[8] M. Perret, *Multiplicative character sums and Kummer coverings*, Acta Arith. **59** n **3** (1991), 75-86.

[9] J.P. Serre, *Groupes algebriques et corps de classes*, Hermann, Paris, 1959.

[10] J.P. Serre, *Zeta and L functions*, Arithmetical Algebraic Geometry, Harper and Row, New York (1965), p. 82-92 ; = Oeuvres, t. II, n **64**, p. 249-259, *Springer*, Berlin, 1986.

[11] J.P. Serre, *Nombre de points des courbes algebriques sur* $\mathbb{F}_q$, Séminaire de Théorie des nombres de Bordeaux, 1982/83 ; = Oeuvres, t. III, n **129**, p. 664-668, *Springer*, Berlin, 1986.

[12] J.P. Serre, cours au collège de France 1982/83 (non publié), notes de M. Waldschmidt.

[13] M.A. Tsfasman, S.G. Vladut, T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound*, Math. Nachr **109** (1982), p. 21-28.

[14] A. Weil, *Variétés Abéliennes et courbes algébriques*, Hermann, Paris, 1948.

[15] J. Wolfmann, *Nombre de points rationnels sur les courbes algébriques sur les corps finis associés à des codes cycliques*, Comptes Rendus de l'Académie des Sciences de Paris **305**, Ser. I (1987), p. 345-348.

[16] J. Wolfmann, *Polynomial description of binary linear codes and related topics*, à paraître au *journal of AAECC*, Springer.

M. PERRET
Equipe "Arithmétique et Théorie de l'Information"
C.I.R.M., Luminy, Case 916
13288 - Marseille Cedex 9
France