Literatur

[1] G. Kolesnik, *On the number of Abelian groups of a given order*, J. Reine Angew. Math. 329 (1981), 164–175.
[2] E. Krätzel, *Lattice Points*, VEB Deutscher Verlag der Wissenschaften, Berlin 1988.
[3] W. Recknagel, *Ein Mittelwertsatz im asymmetrischen dreidimensionalen Gitterpunktproblem*, Mitt. Math. Semin. Gießen 175 (1981), 1–17.
[4] P. G. Schmidt, *Zur Anzahl abelscher Gruppen gegebener Ordnung*, J. Reine Angew. Math. 229 (1968), 34–42.
[5] E. C. Titchmarsh, *On Epstein's Zeta-function*, Proc. London Math. Soc. (2) 36 (1934), 485–500.

PHILIPPS-UNIVERSITÄT
Lahnberge
D-3550 Marburg, F.R.G.

Eingegangen am 6.4.1989
und in revidierter Form am 4.7.1989 (1921)

ACTA ARITHMETICA
LVI (1990)

Nombre de points des jacobiennes sur un corps fini

par

GILLES LACHAUD (Marseille)

et

MIREILLE MARTIN-DESCHAMPS (Paris)

Introduction. Dans l'analogie entre corps de nombres et corps de fonctions sur un corps fini, le nombre de classes correspond au nombre de points de la jacobienne. Nous donnons dans cet article une borne inférieure du nombre de points d'une jacobienne sur un corps fini. Depuis les résultats de Weil ([9], [10]), il y a eu beaucoup de travaux consacrés au nombre de points des courbes sur un corps fini, mais peu d'entre eux concernent explicitement le nombre de points des jacobiennes (cf. [1], [2], [5], [6]). Signalons que récemment S. G. Vladut a abordé ce problème pour l'appliquer à la théorie des codes correcteurs d'erreurs (cf. [8]).

Le § 1 fixe la terminologie, les notations, et rappelle les résultats de Weil; le § 2 établit les estimations classiques qui découlent immédiatement de ces résultats. Nous établissons au § 3 une identité (théorème 1) entre le nombre de diviseurs positifs de degré n sur une courbe, le nombre de points de sa jacobienne, et les racines inverses du numérateur de sa fonction zêta. Cette identité résulte d'une formule (lemme 2) qui est l'expression algébrique d'un théorème classique pour les fonctions zêta des corps de nombres: la formule de Hecke.

Nous donnons au § 4 une minoration (théorème 2) du nombre h de points d'une jacobienne qui résulte du théorème 1, et nous améliorons ainsi les minorations standard comme le montrent les tableaux en annexe. Ces minorations nous permettent d'obtenir des conditions sur q et g pour qu'il existe des courbes de genre g sur $\boldsymbol{F}_q$ avec $h = 1$ ou $h = 2$; dans le cas $h = 1$, nous retrouvons des résultats de Madan et Queen [6].

Nous tenons à remercier J. P. Serre pour les remarques qu'il a faites sur ce travail.

1. Fonction zêta d'une courbe algébrique. Soit X une courbe algébrique projective irréductible et lisse de genre g définie sur le corps fini $\boldsymbol{F}_q$; on suppose que le corps des constantes du corps des fonctions rationnelles sur X est égal à $\boldsymbol{F}_q$, ce qui revient à dire que X est géométriquement irréductible sur $\boldsymbol{F}_q$. On

désigne par $\mathrm{Div}^+(X; F_q)$ (resp. $\mathrm{Div}_n^+(X; F_q)$) l'ensemble des diviseurs positifs (resp. des diviseurs positifs de degré n) de X rationnels sur F_q. A un diviseur $\mathfrak{a} \in \mathrm{Div}^+(X; F_q)$, on associe sa *norme*

$$N(\mathfrak{a}) = q^{\deg(\mathfrak{a})}.$$

La *fonction zêta* (*minuscule*) de la courbe X est

$$\zeta_X(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \sum_{n=0}^{\infty} \frac{D_n}{q^{ns}}$$

où $\mathfrak{a}$ parcourt l'ensemble $\mathrm{Div}^+(X; F_q)$, et où D_n est le nombre de diviseurs positifs de degré n. On peut aussi l'écrire

$$\zeta_X(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \prod_{d \geqslant 0} \left(1 - \frac{1}{q^{ds}}\right)^{-a_d}$$

où le premier produit porte sur tous les points fermés $\mathfrak{p}$ du schéma X, et où a_d est le nombre de points fermés de degré d.

La *fonction zêta* (*majuscule*) de la courbe X est

$$Z_X(T) = \exp \sum_{n=1}^{\infty} \frac{T^n}{n} |X(F_{q^n})|.$$

On a $\zeta_X(s) = Z_X(q^{-s})$, ce qui s'écrit aussi, en posant $T = q^{-s}$:

$$Z_X(T) = \sum_{n=0}^{\infty} D_n T^n.$$

On pose

$$P_X(T) = Z_X(T)(1-T)(1-qT).$$

Les résultats de Weil (cf. [9], [7], p. 207, [10], p. 130) sont les suivants:

(i) (*rationalité*) la fonction $P_X(T)$ est un polynôme de $\mathbf{Z}[T]$ de degré $2g$; on a

$$P_X(0) = 1 \quad \text{et} \quad P_X(1) = h = |J_X(F_q)|$$

où J_X est la jacobienne de X;

(ii) (*équation fonctionnelle*) on a

$$P_X(1/qT) = q^{-g} T^{-2g} P_X(T);$$

(iii) (*hypothèse de Riemann*) écrivons

$$P_X(T) = \prod_{i=1}^{2g} (1 - \pi_i T),$$

on a $|\pi_i| = \sqrt{q}$ pour $1 \leqslant i \leqslant 2g$.

Il résulte de (iii) que l'application $\pi_i \mapsto \bar{\pi}_i = q/\pi_i$ est une permutation des racines π_i.

En fait, on peut aussi écrire:

$$P_X(T) = \prod_{i=1}^{g} (1 - \pi_i T)(1 - \bar{\pi}_i T);$$

autrement dit, les racines éventuelles réelles sont de multiplicité paire. Sinon, le polynôme $P_X(T)$ serait de la forme

$$P_X(T) = (1 - \sqrt{q}T)(1 + \sqrt{q}T) \prod_{i=1}^{g-1} (1 - \pi_i T)(1 - \bar{\pi}_i T)$$

et on aurait

$$P_X(1) = h = (1-q) \prod_{i=1}^{g-1} (1 - \pi_i)(1 - \bar{\pi}_i) < 0.$$

Il s'ensuit que le coefficient de T^{2g} dans $P_X(T)$ est égal à q^{2g}.

2. Estimations standard du nombre de classes. Il résulte de la relation

$$P(1) = h = \prod_{i=1}^{g} (1 - \pi_i)(1 - \bar{\pi}_i)$$

que l'on a

$$(\sqrt{q} - 1)^{2g} \leqslant h \leqslant (1 + \sqrt{q})^{2g};$$

puisque

$$(1 + \sqrt{q})^{2g} = \sum_{n=0}^{2g} \binom{2g}{n} q^{n/2},$$

on a

$$(1 + \sqrt{q})^{2g} \leqslant q^g + q^{g-(1/2)} \sum_{n=1}^{2g} \binom{2g}{n} = q^g + (2^{2g} - 1) q^{g-(1/2)}$$

et

$$|h - q^g| \leqslant (2^{2g} - 1) q^{g-(1/2)};$$

plus précisément, on a

$$(1 + \sqrt{q})^{2g} \leqslant q^g + 2g \cdot q^{g-(1/2)} + q^{g-1} \sum_{n=2}^{2g} \binom{2g}{n}$$

$$= q^g + 2g \cdot q^{g-(1/2)} + (2^{2g} - 2g - 1) q^{g-1}$$

et donc

$$|h - q^g| \leqslant 2g \cdot q^{g-(1/2)} + (2^{2g} - 2g - 1) q^{g-1}.$$

Ces majorations s'appliquent en fait à toute variété abélienne et non seulement à une jacobienne.

3. Relation entre le nombre de classes et le nombre de diviseurs positifs. On désigne par $J_n(X; F_q)$ l'ensemble des classes d'isomorphisme de faisceaux inversibles de degré n de X. C'est un espace homogène principal sous $J(X; F_q)$. Pour tout entier n, il y a un diviseur de degré n sur X (cf. [10], p. 126), donc l'ensemble $J_n(X; F_q)$ est non vide et son cardinal est égal à h. Pour tout faisceau inversible L de degré n on note $\mathrm{cl}\,L$ sa classe dans $J_n(X; F_q)$, $H^0(X, L)$ l'espace vectoriel de ses sections, $h^0(X, L)$ la dimension de $H^0(X, L)$ sur F_q, et ω le faisceau des formes différentielles de X. Le résultat suivant est bien connu:

LEMME 1. *Si $n \geqslant 0$, on a l'égalité*

$$D_n = q^{n+1-g} D_{2g-2-n} + h\frac{q^{n+1-g}-1}{q-1}. \tag{1}$$

Démonstration. A tout diviseur positif sur X, on associe un faisceau inversible de la façon usuelle. On définit ainsi une application de $\mathrm{Div}_n^+(X; F_q)$ dans $J_n(X; F_q)$. Puisque l'image réciproque de la classe d'un faisceau inversible L est l'espace projectif $P(H^0(X, L))$, on a

$$D_n = \sum_{\mathrm{cl}L \in J_n(X;F_q)} \frac{q^{h^0(X,L)}-1}{q-1}.$$

D'après le théorème de Riemann–Roch, on a

$$h^0(X, L) = n+1-g+h^0(X, \omega \otimes L^{-1}),$$

par suite

$$\begin{aligned}(q-1)D_n &= \sum_{\mathrm{cl}L \in J_n(X;F_q)} q^{n+1-g+h^0(X,\omega\otimes L^{-1})}-1 \\ &= h(q^{n+1-g}-1)+q^{n+1-g}\sum_{\mathrm{cl}L\in J_n(X;F_q)} q^{h^0(X,\omega\otimes L^{-1})}-1.\end{aligned}$$

Quand $\mathrm{cl}\,L$ parcourt $J_n(X; F_q)$, la classe du faisceau $\omega \otimes L^{-1}$ parcourt l'espace $J_{2g-2-n}(X; F_q)$, donc

$$(q-1)D_{2g-2-n} = \sum_{\mathrm{cl}L\in J_n(X;F_q)} q^{h^0(X,\omega\otimes L^{-1})}-1,$$

d'où l'égalité cherchée.

En particulier, pour $n \geqslant 2g-1$, on a $D_{2g-2-n} = 0$, donc

$$D_n = h\frac{q^{n+1-g}-1}{q-1}. \tag{2}$$

LEMME 2. *Pour $g \geqslant 2$, on a*

$$\sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} = \frac{P_X(T)}{(1-T)(1-qT)} + h\frac{T^{g-1}}{q-1}\left(\frac{1}{1-T}-\frac{1}{1-qT}\right).$$

Démonstration. En utilisant (1) et (2), on obtient

$$\begin{aligned}Z_X(T) &= \sum_{n=0}^{\infty} D_n T^n \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=g-1}^{2g-2} q^{n+1-g} D_{2g-2-n} T^n + h\sum_{n=g-1}^{\infty} \frac{q^{n+1-g}}{q-1} T^n \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} + h\frac{T^{g-1}}{q-1}\sum_{n=0}^{\infty}(q^n-1)T^n \\ &= \sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} + h\frac{T^{g-1}}{q-1}\left(\frac{1}{1-qT}-\frac{1}{1-T}\right),\end{aligned}$$

d'où le lemme.

Remarque. Le lemme 2 est la version algébrique d'une formule intégrale pour la fonction $\zeta_K(s)$, qui est la *formule de Hecke* dans le cas des corps de nombres (cf. [3], thm. 15, p. 300).

THÉORÈME 1. *Soient X une courbe algébrique projective, géométriquement irréductible et lisse de genre $g \geqslant 2$ sur F_q, D_n le nombre de diviseurs positifs de degré n sur X, et $(\pi_i, \bar{\pi}_i)_{1\leqslant i\leqslant g}$ les couples de racines inverses du numérateur de la fonction $Z_X(T)$; alors*

$$\sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n = h\sum_{i=1}^{g}\frac{1}{|1-\pi_i|^2}. \tag{3}$$

Démonstration. Posons $P(T) = P_X(T)$ et faisons $T = 1$ dans les deux membres de l'égalité du lemme 2; pour cela, il nous faut introduire la fonction auxiliaire

$$F(T) = \frac{P(T)}{1-qT} + h\frac{T^{g-1}}{q-1}$$

qui s'annule pour $T = 1$. Avec cette notation:

$$\sum_{n=0}^{g-2} D_n T^n + \sum_{n=0}^{g-1} q^{g-1-n} D_n T^{2g-2-n} = \frac{F(T)}{1-T} - h\frac{T^{g-1}}{(q-1)(1-qT)},$$

d'où

$$\sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n = -F'(1) + h\frac{1}{(q-1)^2}.$$

D'après la définition de F, on a

$$F'(T) = \frac{P'(T)}{1-qT} + q\frac{P(T)}{(1-qT)^2} + h(g-1)\frac{T^{g-2}}{q-1},$$

$$F'(1) = \frac{P'(1)}{1-q} + q\frac{P(1)}{(1-q)^2} + h(g-1)\frac{1}{q-1}.$$

Pour achever le calcul, il faut donc déterminer $P'(1)$ et $F'(1)$, ce que nous allons faire maintenant. On a successivement

$$P(T) = \prod_{i=1}^{g} (1-\pi_i T)(1-\bar{\pi}_i T),$$

$$\frac{P'(T)}{P(T)} = -\sum_{i=1}^{g} \frac{\pi_i}{1-\pi_i T} + \frac{\bar{\pi}_i}{1-\bar{\pi}_i T} = -\sum_{i=1}^{g} \frac{\pi_i + \bar{\pi}_i - 2qT}{(1-\pi_i T)(1-\bar{\pi}_i T)},$$

et

$$\frac{P'(1)}{P(1)} = \sum_{i=1}^{g} \frac{2q-(\pi_i+\bar{\pi}_i)}{|1-\pi_i|^2}.$$

En vertu des égalités

$$P(1) = h, \quad (1-\pi_i)(1-\bar{\pi}_i)+q-1 = 2q-(\pi_i+\bar{\pi}_i),$$

on peut écrire

$$\frac{P'(1)}{h} = g + \sum_{i=1}^{g} \frac{q-1}{|1-\pi_i|^2},$$

$$F'(1) = \frac{gh}{1-q} - h\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2} + q\frac{h}{(1-q)^2} + h(g-1)\frac{1}{q-1}$$

$$= \frac{h}{(1-q)^2} - h\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2},$$

ce qui démontre le théorème 1.

4. Nouvelles minorations du nombre de classes. La proposition précédente va nous permettre de minorer h. Pour cela, nous devons majorer la somme

$$\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2}.$$

Puisque $|\pi_i| = \sqrt{q}$, on obtient immédiatement deux inégalités:

$$|1-\pi_i|^2 \geqslant (\sqrt{q}-1)^2, \quad |1-\pi_i^2|^2 \geqslant (q-1)^2,$$

et la deuxième s'écrit

$$|(1-\pi_i)(1+\pi_i)|^2 \geqslant (q-1)^2,$$

donc

$$|1-\pi_i|^2 \geqslant \frac{(q-1)^2}{|1+\pi_i|^2}.$$

On en déduit les deux majorations suivantes: d'une part

$$\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2} \leqslant \frac{g}{(\sqrt{q}-1)^2}; \tag{4}$$

d'autre part

$$\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2} \leqslant \frac{1}{(q-1)^2} \sum_{i=1}^{g} (1+q+\pi_i+\bar{\pi}_i)$$

$$= \frac{1}{(q-1)^2}(g(q+1)+1+q-|X(F_q)|),$$

d'où

$$\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2} \leqslant \frac{1}{(q-1)^2}((g+1)(q+1)-|X(F_q)|), \tag{5}$$

car on déduit immédiatement des formules de Weil

$$|X(F_q)| = 1+q-\sum_{i=1}^{g} (\pi_i+\bar{\pi}_i).$$

Puisque $1+q-2g\sqrt{q} \leqslant |X(F_q)|$, la majoration (5) est meilleure que (4). On peut aussi remarquer directement que l'inégalité

$$|1-\pi_i|^2 \geqslant (q-1)^2/|1+\pi_i|^2$$

est toujours meilleure que l'inégalité

$$|1-\pi_i|^2 \geqslant (\sqrt{q}-1)^2,$$

puisque $|1+\pi_i|^2 \leqslant (\sqrt{q}+1)^2$.

Le résultat principal de cet article est le suivant:

THÉORÈME 2. *Soit X une courbe algébrique projective, géométriquement irréductible et lisse de genre $g \geqslant 1$ définie sur F_q; soit J_X la jacobienne de X, et $h = |J_X(F_q)|$.*

1) *On a*

$$h \geqslant q^{g-1}\frac{(q-1)^2}{(q+1)(g+1)};$$

2) *On a aussi*

$$h \geqslant (\sqrt{q}-1)^2 \frac{q^{g-1}-1}{g} \frac{|X(F_q)|+q-1}{q-1};$$

3) *Si $g > \sqrt{q}/2$ et si X a au moins un point rationnel sur F_q, alors*

$$h \geqslant (q^g-1)\frac{q-1}{q+g+gq}.$$

Démonstration. Posons $\Sigma(X) = 1$ si $g = 1$ et

$$\Sigma(X) = \sum_{n=0}^{g-2} D_n + \sum_{n=0}^{g-1} q^{g-1-n} D_n$$

si $g \geqslant 2$; l'égalité (3) du théorème 1 se réécrit

$$\Sigma(X) = h\sum_{i=1}^{g} \frac{1}{|1-\pi_i|^2}$$

et cette égalité est vraie pour $g \geqslant 1$. Pour $n > 0$, on peut minorer D_n par $|X(F_q)|$; compte tenu de ce que $D_0 = 1$, il vient pour $g \geqslant 2$

$$\Sigma(X) \geqslant 1 + q^{g-1} + |X(F_q)| \sum_{n=1}^{g-1} q^{g-1-n},$$

et donc

$$\Sigma(X) \geqslant q^{g-1}$$

si $g \geqslant 1$; l'inégalité (5) donne alors l'inégalité 1). On a aussi, pour $g \geqslant 1$,

$$\Sigma(X) \geqslant (q^{g-1}-1)\frac{|X(F_q)|+q-1}{q-1},$$

et l'inégalité (4) donne l'inégalité 2). Si $|X(F_q)| \geqslant 1$, on a, pour $g \geqslant 2$,

$$\Sigma(X) \geqslant 1 + q^{g-1} + \sum_{n=1}^{g-1} q^{g-1-n} = 1 + q^{g-1} + \frac{q^{g-1}-1}{q-1} = 1 + \frac{q^g-1}{q-1} > \frac{q^g-1}{q-1},$$

ce qui établit le résultat annoncé en 3) en utilisant l'inégalité (5).

Remarque. Au paragraphe 2, on avait mentionné la minoration standard

$$h \geqslant (\sqrt{q}-1)^{2g};$$

la minoration de l'assertion 1) du théorème 2 sera meilleure que la minoration standard si

$$\frac{(\sqrt{q}-1)^2}{g} q^{g-1} \geqslant (\sqrt{q}-1)^{2g},$$

autrement dit si

$$\frac{g-1}{\log g} \geqslant \frac{1}{\log\left(q/(\sqrt{q}-1)^2\right)} = v(q);$$

l'inégalité précédente sera satisfaite si $g \geqslant g_0(q)$, où $g_0(q)$ est la solution de l'équation

$$\frac{g-1}{\log g} = v(q)$$

qui tend vers l'infini avec q; puisque $v(q) \sim \sqrt{q}/2$, on a

$$g_0(q) \sim \frac{\sqrt{q}}{2} \log \frac{\sqrt{q}}{2}.$$

Quand $g \geqslant g_0(q)$, ces nouvelles minorations sont bien meilleures, comme le montrent les tableaux du paragraphe 6; mais elles ne valent que pour les jacobiennes, et non pour les variétés abéliennes quelconques.

On obtient immédiatement d'après les tableaux du paragraphe 6 les résultats suivants:

COROLLAIRE. *Soit X une courbe de genre $g \geqslant 1$ sur F_q (resp. ayant au moins un point rationnel). Si $h = 1$, on est dans l'un des cas suivants:*

$$q = 2 \quad et \quad g \leqslant 5 \quad (resp.\ g \leqslant 3),$$
$$q = 3 \quad et \quad g = 1,$$
$$q = 4 \quad et \quad g = 1;$$

si $h = 2$, on est dans l'un des cas suivants:

$$q = 2 \quad et \quad g \leqslant 6 \quad (resp.\ g \leqslant 5),$$
$$q = 3 \quad et \quad g \leqslant 2,$$
$$q = 4 \quad et \quad g = 1,$$
$$q = 5 \quad et \quad g = 1.$$

Le cas $h = 1$ se trouve déjà dans les travaux de Madan et Queen [6], qui généralisent ceux de MacRae [4].

5. L'analogue du théorème de Brauer–Siegel. On garde les notations précédentes, et on pose

$$D = q^{2g-2}.$$

Ce nombre joue le même rôle que la valeur absolue du discriminant d'un corps de nombres. En fait, la valeur absolue du discriminant d'un corps de nombres est la norme de la différente de son anneau d'entiers; dans le cas d'une extension de $F_q(x)$ avec $[K: F_q(x)] = n$, la formule de Hurwitz (cf. [10], p. 157) implique que le degré de la différente $\mathfrak{d}$ est égal à

$$\deg(\mathfrak{d}) = 2g-2+2n,$$

d'où $N(\mathfrak{d}) = q^{2n} D$.

Soit K le corps des fonctions rationnelles sur X; le corps K est une extension de degré n d'une extension transcendante pure $F_q(x)$ si et seulement s'il y a un morphisme non constant $X \to \mathbf{P}^1$ de degré n.

Le résultat suivant est une conséquence du lemme 2.

LEMME 3. *Supposons qu'il y ait un morphisme non constant $X \to \mathbf{P}^1$ de degré $n \geqslant 1$; alors, pour $s > 1$, on a*

$$h < q^{gs} \zeta_{\mathbf{P}^1}(s)^{n-1}.$$

Démonstration. Soit $\mathfrak{q}$ un point fermé de $\mathbf{P}^1$; si $\mathfrak{p}$ est un point fermé de X au-dessus de $\mathfrak{q}$, on a $N(\mathfrak{p}) = N(\mathfrak{q})^f$ avec $f \geqslant 1$, et

$$\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \leqslant \left(1 - \frac{1}{N(\mathfrak{q})^s}\right)^{-f};$$

s'il y a r points fermés au-dessus de q, on obtient

$$\prod_{p|q}\left(1-\frac{1}{N(p)^s}\right)^{-1} \leqslant \left(1-\frac{1}{N(q)^s}\right)^{-fr};$$

puisque $fr \leqslant n$, il vient pour $s>1$

$$\zeta_X(s) \leqslant \zeta_{\mathbf{P}^1}(s)^n.$$

D'autre part la formule du lemme 2 se réécrit

$$Z_X(T) = hT^g Z_{\mathbf{P}^1}(T)+Q(T),$$

où $Q(T)$ est un polynôme de degré $2g-2$ dont les coefficients sont des entiers positifs; si $T>0$, on a donc

$$Z_X(T) > hT^g Z_{\mathbf{P}^1}(T),$$

et en prenant $T=q^{-s}$,

$$\zeta_X(s) > hq^{-gs}\zeta_{\mathbf{P}^1}(s)^n,$$

d'où le résultat.

THÉORÈME 3. *Si K parcourt une suite d'extensions de $\mathbf{F}_q(x)$ telle que $[K:\mathbf{F}_q(x)] \leqslant n$, il y a des constantes explicites C_1 et C_2 telles que*

$$C_1\frac{\sqrt{D}}{\log D} \leqslant h \leqslant C_2\sqrt{D}(\log\sqrt{D})^{n-1}.$$

Démonstration. Le théorème 2 implique

$$h \geqslant \frac{(\sqrt{q}-1)^2}{g}q^{g-1}, \tag{6}$$

d'où l'on déduit la première inégalité. D'autre part si on pose

$$s = 1+\frac{1}{g\log q},$$

on a $q^{gs} = eq^g$ (où e est le nombre tel que $\log e = 1$), et

$$\zeta_{\mathbf{P}^1}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})} \leqslant \frac{2}{1-e^{-1/g}} \leqslant \frac{e^{1/2g}}{\operatorname{sh}(1/(2g))} \leqslant 2g\,e^{1/2g} \leqslant 2g\sqrt{e},$$

(la troisième inégalité car $\operatorname{sh} x \geqslant x$), par suite

$$h \leqslant e(2g\sqrt{e})^{n-1}\sqrt{D},$$

d'où la deuxième inégalité grâce au lemme 3, et le résultat.

Remarque. Si K parcourt une suite d'extensions de $\mathbf{F}_q(x)$ telle que

$$[K:\mathbf{F}_q(x)]/\log D \to 0,$$

alors

$$\log h \sim \log\sqrt{D}.$$

En effet, il résulte du lemme 3 et de (6) que pour tout $\varepsilon>0$, il y a des constantes $C_1(\varepsilon)$ et $C_2(\varepsilon)$ ne dépendant que de ε tel que

$$C_2(\varepsilon)(\sqrt{D})^{1-\varepsilon} \leqslant h \leqslant C_2(\varepsilon)^{n-1}(\sqrt{D})^{1+\varepsilon}.$$

Ces résultats sont l'analogue du théorème de Brauer–Siegel (cf. [3], Ch. XVI) pour les corps de fonctions, établi par Inaba [2]; cf. aussi Gogia et Luthar [1], Madan et Madden [5]; nous avons obtenu ici un résultat plus précis comme conséquence du théorème 2.

6. Tableaux numériques. On note $\lceil x \rceil$ le plus grand entier supérieur ou égal au nombre x.

1. *Variétés abéliennes*

$$h_{VA} = \lceil(\sqrt{q}-1)^{2g}\rceil$$

$g\backslash q$	2	3	4	5	7	9	11	13	16
1	1	1	1	2	3	4	6	7	9
2	1	1	1	3	8	16	29	47	81
3	1	1	1	4	20	64	155	313	729
4	1	1	1	6	54	256	830	2125	6561
5	1	1	1	9	146	1024	4453	14422	59049
6	1	1	1	13	395	4096	23893	97903	531441
7	1	1	1	20	1070	16384	128228	664653	4782969

2. *Jacobiennes*

$$h_{JO} = \left\lceil q^{g-1}\frac{(q-1)^2}{(q+1)(g+1)}\right\rceil$$

$g\backslash q$	2	3	4	5	7	9	11	13	16
1	1	1	1	2	3	4	5	6	7
2	1	1	3	5	11	20	31	45	71
3	1	3	8	17	56	130	253	435	848
4	1	6	24	67	309	934	2219	4520	10843
5	1	14	77	278	1801	6999	20335	48962	144565
6	2	35	264	1191	10805	53988	191728	545574	1982602
7	3	92	922	5209	66178	425153	1845377	6205898	27756424

3. *Jacobiennes de courbes ayant au moins un point rationnel*

$$h_{J1} = \left\lceil (q^g-1)\frac{q-1}{q+g+gq}\right\rceil$$

$g\backslash q$	2	3	4	5	7	9	11	13	16
1	1	1	1	2	3	4	5	6	7
2	1	2	4	6	13	23	35	50	77
3	1	4	10	22	67	150	283	480	917
4	2	9	32	87	370	1072	2482	4967	11703
5	2	22	106	358	2146	8007	22684	53681	155729
6	4	54	362	1525	12835	61617	213441	597131	2132697
7	6	142	1261	6649	78433	484352	205128	26783624	29826162

Bibliographie

[1] S. K. Gogia and I. S. Luthar, *The Brauer–Siegel theorem for algebraic function fields*, J. Reine Angew. Math. 299 (1978), 28–37.
[2] E. Inaba, *Number of divisor classes in algebraic function fields*, Proc. Japan Acad. 26 (1950), 1–4.
[3] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading 1970.
[4] R. E. MacRae, *On unique factorization in certain rings of algebraic functions*, J. Algebra 17 (1971), 243–261.
[5] M. L. Madan and D. J. Madden, *On the theory of congruence function fields*, Comm. Algebra 8 (17) (1980), 1687–1697.
[6] M. L. Madan and C. S. Queen, *Algebraic function fields of class number one*, Acta Arith. 20 (1972), 423–432.
[7] D. Mumford, *Abelian Varieties*, Tata Inst. of Fund. Res. Stud. in Math., Bombay, Oxford University Press, Bombay 1970.
[8] S. G. Vladut, *An exhaustion bound for algebraic-geometric codes*, Problemy Peredachi Informatsii 23 (1987), 28–41; = Problems Inform. Transmission 23 (1987), 22–38.
[9] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent, Variétés abéliennes et courbes algébriques*, Pub. Math. Univ. Strasbourg VII et VIII, Act. Sci. Ind. n° 1041 et 1064, Hermann & Cie, Paris 1948.
[10] — *Basic Number Theory*, Grundlehren Math. Wiss. 144, Springer, New York 1967.

EQUIPE C.N.R.S. "ARITHMÉTIQUE ET THÉORIE DE L'INFORMATION"
C.I.R.M.
Luminy Case 916
13288 Marseille Cedex 9, France
D.M.I.
ÉCOLE NORMALE SUPÉRIEURE
45, rue d'Ulm
75230 Paris Cedex 05, France

Reçu le 15.5.1989 (1932)

ACTA ARITHMETICA
LVI (1990)

On the splitting of primes in an arithmetic progression, II

by

M. Bhaskaran (Duncraig) and S. Venkataraman (Madras)

1. Introduction. Let k be a number field and suppose $p \in \mathbb{Q}$ is tamely ramified in k: $p = P_1^{e_1} P_2^{e_2} \dots P_r^{e_r}$, $p \nmid e_i$. In this paper we show that there exists a set of rational primes with positive density in an arithmetic progression whose splitting in k depends on the ramification indices and residue class degrees of the P_i's. This is an extension of the result in [1].

2. Some preliminary results

LEMMA 1. *Let k be a number field and suppose K is the narrow class field of the normal closure $\bar{k}$. Let P be a prime in K and suppose $I = I(P|P \cap \mathbb{Q})$ is the inertia group of P over $\mathbb{Q}$. If Q is any prime unramified in K such that $\left[\frac{K/\mathbb{Q}}{Q}\right] \in I$, then $q = \mathbb{Q} \cap Q$ splits into positive principal prime divisors.* (This means that the prime ideals have generators whose images under all real embeddings of k are positive.)

This is proved for (Hilbert) class field in [4] (also in [2]).
This easily carries over to narrow class-fields.

THEOREM A. *Let k be a normal number field in which a prime p ramifies with ramification index $e_p = p^r e'_p$, $p \nmid e'_p$. Let a be a primitive root modulo p^l. Then there is a t_0, $0 \leqslant t_0 \leqslant r$, with the following property: The set of primes $q \equiv a \pmod{p^l}$ which have degree $e'_p p^{t_0}$ and which split into positive principal prime ideals in k has positive density.*

Proof. Let P be a prime ideal lying over p in the narrow class-field K of k. Let $I = I(P|p)$ be the inertia group of P over p and T the fixed field of the inertia group. Let V_1 be as usual,

$$V_1 = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) |\ \sigma(\alpha) \equiv \alpha \pmod{P^2}\}.$$

Then V_1 is a normal subgroup of I and I/V_1 is cyclic. Let K' be the fixed field of V_1. Since V_1 is the p-Sylow subgroup of I, K'/T is a cyclic extension of degree e'_p. Let ζ denote a primitive p^l-th root of unity. Since T and $\mathbb{Q}(\zeta)$ are linearly disjoint,

$$\mathrm{Gal}(T(\zeta)/T) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}).$$