



## Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis

Aubry, Yves; Haloui, Safia; Lachaud, Gilles

*Published in:*  
Comptes Rendus Mathématique

*Link to article, DOI:*  
[10.1016/j.crma.2012.10.001](https://doi.org/10.1016/j.crma.2012.10.001)

*Publication date:*  
2012

*Document Version*  
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

*Citation (APA):*  
Aubry, Y., Haloui, S., & Lachaud, G. (2012). Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis. *Comptes Rendus Mathématique*, 350(19-20), 907-910.  
<https://doi.org/10.1016/j.crma.2012.10.001>

---

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



ELSEVIER

Contents lists available at SciVerse ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com



Géométrie algébrique

## Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis

*On the number of points on abelian and Jacobian varieties over finite fields*

Yves Aubry<sup>a,b</sup>, Safia Haloui<sup>a,c</sup>, Gilles Lachaud<sup>a</sup>

<sup>a</sup> Institut de mathématiques de Luminy, Aix-Marseille université-CNRS, campus de Luminy, case 907, 163, avenue de Luminy, 13009 Marseille, France

<sup>b</sup> Institut de mathématiques de Toulon, université du Sud Toulon-Var, avenue de l'université, 83957 La Garde cedex, France

<sup>c</sup> Department of Mathematics, Technical University of Denmark, Matematiktorvet 303 B, DK-2800 Kgs. Lyngby, Denmark

### INFO ARTICLE

Historique de l'article :

Reçu le 31 août 2012

Accepté le 2 octobre 2012

Disponible sur Internet le 24 octobre 2012

Présenté par Jean-Pierre Serre

### RÉSUMÉ

Nous établissons de nouvelles majorations et minorations pour le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur un corps fini. Nous déterminons de plus les nombres maximum et minimum de points rationnels des surfaces Jacobiennes sur un corps fini donné.

© 2012 Publié par Elsevier Masson SAS pour l'Académie des sciences.

### ABSTRACT

We give upper and lower bounds for the number of points on abelian and Jacobian varieties over finite fields. We also determine the values for the maximum and minimum number of points on Jacobian surfaces on a given finite field.

© 2012 Publié par Elsevier Masson SAS pour l'Académie des sciences.

### 1. Variétés abéliennes

Soit  $A$  une variété abélienne de dimension  $g$  sur le corps fini  $\mathbf{F}_q$ , avec  $q = p^e$ . Le polynôme de Weil  $f_A(t)$  de  $A$  est le polynôme caractéristique de son endomorphisme de Frobenius  $F_A$ . On note  $\omega_1, \dots, \omega_g, \bar{\omega}_1, \dots, \bar{\omega}_g$  les racines de  $f_A(t)$ , et  $|\omega_i| = q^{1/2}$ . Pour  $1 \leq i \leq g$ , on pose  $x_i = -(\omega_i + \bar{\omega}_i)$ , et on dit que  $A$  est de type  $[x_1, \dots, x_g]$ . Le type de  $A$  dépend uniquement de sa classe d'isogénie. On note  $\tau = \tau(A) = -\sum_{i=1}^g (\omega_i + \bar{\omega}_i) = \sum_{i=1}^g x_i$  l'opposé de la trace de  $F_A$  et on dit que  $A$  est de trace  $-\tau$ . Le nombre de points rationnels de  $A$  sur  $\mathbf{F}_q$  est

$$|A(\mathbf{F}_q)| = f_A(1) = \prod_{i=1}^g (q + 1 + x_i). \quad (1)$$

Puisque  $|x_i| \leq 2q^{1/2}$ , on déduit de (1) les bornes classiques :

$$(q + 1 - 2q^{1/2})^g \leq |A(\mathbf{F}_q)| \leq (q + 1 + 2q^{1/2})^g.$$

Ces bornes peuvent être améliorées :

Adresses e-mail : yves.aubry@univ-tln.fr (Y. Aubry), s.haloui@mat.dtu.dk (S. Haloui), lachaud@univ-amu.fr (G. Lachaud).

**Théorème 1.1.** Soit  $A$  une variété abélienne sur  $\mathbf{F}_q$  de dimension  $g$ , et posons  $m = \lfloor 2\sqrt{q} \rfloor$ . Alors

$$(q + 1 - m)^g \leq |A(\mathbf{F}_q)| \leq (q + 1 + m)^g$$

avec égalité à droite (resp. à gauche) si et seulement si  $A$  est de type  $[m, \dots, m]$  (resp.  $[-m, \dots, -m]$ ).

On peut être plus précis en introduisant la trace :

**Théorème 1.2.** Soit  $A$  une variété abélienne sur  $\mathbf{F}_q$  de dimension  $g$  et de trace  $-\tau$ . Alors

$$|A(\mathbf{F}_q)| \leq \left( q + 1 + \frac{\tau}{g} \right)^g,$$

avec égalité si et seulement si  $A$  est de type  $[\tau/g, \dots, \tau/g]$ .

Ce résultat a été démontré par H.G. Quebbemann [5] pour les Jacobiennes et par M. Perret [4] pour les variétés de Prym. On dit que  $A$  (ou  $\tau$ ) est de défaut  $d$  si  $\tau = gm - d$ . On a :

**Proposition 1.3.** Si  $A$  est de défaut  $d$ , avec  $d = 1$  ou  $d = 2$ , alors

$$|A(\mathbf{F}_q)| \leq (q + m)^d (q + 1 + m)^{g-d}.$$

Le résultat suivant donne une minoration pour  $|A(\mathbf{F}_q)|$ , qui est symétrique de la borne supérieure du Théorème 1.2, et qui dépend du quotient de Specht [6] défini pour  $h \geq 1$  par

$$S(h) = \frac{h^{1/(h-1)}}{e \log h^{1/(h-1)}}, \quad S(1) = 1.$$

**Théorème 1.4.** Si  $q \geq 2$ , posons  $h(q) = ((q^{1/2} + 1)/(q^{1/2} - 1))^2$  et  $M(q) = 1/S(h(q))$ . Soit  $A$  une variété abélienne définie sur  $\mathbf{F}_q$  de dimension  $g$  et de trace  $-\tau$ . Alors

$$|A(\mathbf{F}_q)| \geq M(q)^g \left( q + 1 + \frac{\tau}{g} \right)^g.$$

De plus  $M(2) \geq 0.261$  et  $M(q) \geq 1 - (2/q)$ .

**Théorème 1.5.** Soit  $A$  une variété abélienne sur  $\mathbf{F}_q$  de dimension  $g$  et de trace  $-\tau$ . Alors

$$|A(\mathbf{F}_q)| \geq (q + 1 - m)^g + (q - m)^{g-1} (gm + \tau).$$

En utilisant les méthodes de convexité de M. Perret [4], on obtient :

**Proposition 1.6.** Posons  $r = \lfloor (g + \lfloor \omega \rfloor)/2 \rfloor$  et  $s = \lfloor (g - 1 - \lfloor \omega \rfloor)/2 \rfloor$ , où  $\omega = \tau/(2q^{1/2})$ . Alors

$$|A(\mathbf{F}_q)| \geq (q + 1 + \tau - 2(r - s)q^{1/2})(q + 1 + 2q^{1/2})^r (q + 1 - 2q^{1/2})^s.$$

On note  $\eta(A)$  la moyenne harmonique des nombres  $q + 1 + x_i$  :

$$\frac{1}{\eta(A)} = \frac{1}{g} \sum_{i=1}^g \frac{1}{q + 1 + x_i} = \frac{1}{g} \sum_{i=1}^g \frac{1}{|1 - \omega_i|^2}.$$

Il est possible de minorer  $|A(\mathbf{F}_q)|$  en fonction de  $\eta(A)$  :

**Théorème 1.7.** Soit  $A$  une variété abélienne sur  $\mathbf{F}_q$  de dimension  $g$ . Alors  $|A(\mathbf{F}_q)| \geq \eta(A)^g$ .

On démontre que si  $q \geq 8$ , alors  $\eta(A) \geq q + 1 - m$ . Le Théorème 1.7 est donc plus précis que le Théorème 1.1 si  $q \geq 8$ . Notons que si  $q \leq 7$ , on peut avoir  $\eta(A) < q + 1 - m$ .

## 2. Jacobiennes

Par une courbe sur  $\mathbf{F}_q$ , on entend une courbe algébrique projective, lisse, et absolument irréductible définie sur  $\mathbf{F}_q$ . Si  $C$  est une telle courbe, on note  $J_C$  sa Jacobienne et  $N = |C(\mathbf{F}_q)|$  le nombre de ses points sur  $\mathbf{F}_q$ . Les résultats de la Section 1 s'appliquent évidemment aux Jacobiennes ; en particulier, le Théorème 1.4 implique :

**Proposition 2.1.** *Si  $C$  est une courbe sur  $\mathbf{F}_q$  de genre  $g$ , alors :*

$$|J_C(\mathbf{F}_q)| \geq M(q)^g \left( q + 1 + \frac{N - (q + 1)}{g} \right)^g.$$

Les Propositions 1.5 et 1.6 fournissent des bornes sur les Jacobiennes de la même manière. Si  $A$  est une variété abélienne sur  $\mathbf{F}_q$  de dimension  $g$ , on note  $P(t) = P_A(t)$  le polynôme réciproque de  $f_A(t)$ . On définit d'abord la fonction zêta virtuelle de numérateur  $P(t)$  comme la série formelle :

$$Z(t) = \frac{P(t)}{(1-t)(1-qt)} \in \mathbf{Z}[[t]],$$

et on introduit ensuite trois suites d'entiers  $(A_n)$ ,  $(B_n)$ ,  $(N_n)$  par les identités suivantes :

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n = \exp \sum_{n=1}^{\infty} N_n \frac{t^n}{n} = \prod_{n=1}^{\infty} (1 - t^n)^{-B_n}. \tag{2}$$

Comme démontré dans [3] pour une Jacobienne, on a

**Théorème 2.2.** *Supposons  $g \geq 2$ . Avec les notations précédentes,*

$$\frac{g}{\eta(A)} |A(\mathbf{F}_q)| = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n. \quad \square$$

Si  $A = J_C$  est la Jacobienne d'une courbe  $C$  sur  $\mathbf{F}_q$ , alors  $A_n$  (resp.  $B_n$ ) représentent respectivement les nombres de diviseurs rationnels effectifs (resp. premiers) de degré  $n$  de  $C$ , et  $N_n = |C(\mathbf{F}_{q^n})|$ . Dans ce cas, les deux conditions suivantes sont vérifiées :

$$B_n \geq 0 \quad \text{si} \quad 1 \leq n \leq 2g, \tag{B}$$

$$N_n \geq N_1 \geq 0 \quad \text{si} \quad 1 \leq n \leq 2g. \tag{N}$$

En fait, ces conditions sont vérifiées pour tout  $n \geq 1$ . La proposition suivante, qui améliore certains résultats de N. Elkies et al. [1], montre que les conditions (B) et a fortiori (N) ne sont propres aux Jacobiennes que si  $g$  est suffisamment grand devant  $q$ .

**Proposition 2.3.** *Soit  $A$  une variété abélienne sur  $\mathbf{F}_q$  de dimension  $g \geq 1$ . Si  $n \geq 2$ , alors*

$$nB_n \geq (q^{n/4} + 1)^2 ((q^{n/4} - 1)^2 - 2g).$$

Le théorème suivant s'applique évidemment aux Jacobiennes.

**Théorème 2.4.** *Soit  $A$  une variété abélienne définie sur  $\mathbf{F}_q$  de dimension  $g \geq 2$ . Si la condition (B) est vérifiée, alors*

$$|A(\mathbf{F}_q)| \geq \frac{q-1}{q^g-1} \left[ \binom{N+2g-2}{2g-1} + \sum_{n=0}^{2g-3} B_{2g-1-n} \binom{N+n-1}{n} \right].$$

Si la condition (N) est vérifiée, alors

$$|A(\mathbf{F}_q)| \geq \frac{\eta(A)}{g} \left[ \binom{N+g-2}{g-2} + \sum_{n=0}^{g-1} q^{g-1-n} \binom{N+n-1}{n} \right].$$

Si la condition (N) est vérifiée, et si  $N \geq g(q^{1/2} - 1) + 1$ , alors

$$|A(\mathbf{F}_q)| \geq \binom{N+g-1}{g} - q \binom{N+g-3}{g-2}.$$

### 3. Surfaces Jacobiennes

On pose

$$j_q(g) = \min_C |J_C(\mathbf{F}_q)|, \quad J_q(g) = \max_C |J_C(\mathbf{F}_q)|,$$

où  $C$  parcourt l'ensemble des courbes sur  $\mathbf{F}_q$  de genre  $g$ . Le résultat suivant s'appuie sur la détermination des classes d'isogénies des surfaces abéliennes qui contiennent une Jacobienne, voir E. Howe, E. Nart, et C. Ritzenthaler [2]. Rappelons que le nombre  $q = p^e$ , où  $e$  est impair, est *spécial* si  $p|m$ , ou bien s'il existe une solution entière à l'une des équations  $q = x^2 + 1$ ,  $q = x^2 + x + 1$ ,  $q = x^2 + x + 2$ .

**Théorème 3.1.** *On a*

$$j_q(2) = (q + 1 - m)^2, \quad J_q(2) = (q + 1 + m)^2,$$

sauf dans les cas particuliers suivants :

$j_q(2)$	$q = 4$	5
	$q = 9$	25
$q$ spécial	$\{2q^{1/2}\} \geq \varphi_1$	$(q + 1 - m - \varphi_1)(q + 1 - m - \varphi_2)$
	$\sqrt{2} - 1 \leq \{2q^{1/2}\} < \varphi_1$	$(q + 2 - m + \sqrt{2})(q + 2 - m - \sqrt{2})$
	$\{2q^{1/2}\} < \sqrt{2} - 1, p \nmid m, q \neq 7^3$	$(q + 1 - m)(q + 3 - m)$
	sinon	$(q + 2 - m)^2$
$J_q(2)$	$q = 4$	55
	$q = 9$	225
$q$ spécial	$\{2q^{1/2}\} \geq \varphi_1$	$(q + 1 + m + \varphi_1)(q + 1 + m + \varphi_2)$
	$\{2q^{1/2}\} < \varphi_1, p \neq 2$ ou $p m$	$(q + m)^2$
	sinon	$(q + 1 + m)(q - 1 + m)$

Ici  $\varphi_1 = (-1 + \sqrt{5})/2, \varphi_2 = (-1 - \sqrt{5})/2$  et on a noté  $\{x\}$  la partie fractionnaire d'un nombre réel  $x$ .

Les résultats présentés dans cette Note sont développés et démontrés dans un article à paraître dans la revue Acta Arithmetica.

### Références

- [1] Noam D. Elkies, Everett W. Howe, Andrew Kresch, Poonen Bjorn, Joseph L. Wetherell, Michael E. Zieve, Curves of every genus with many points, II: Asymptotically good families, Duke Math. J. 122 (2) (2004) 399–422.
- [2] Everett Howe, Enric Nart, Christophe Ritzenthaler, Jacobians in isogeny classes of abelian surfaces over finite fields, Ann. Inst. Fourier 59 (2009) 239–289.
- [3] Gilles Lachaud, Mireille Martin-Deschamps, Nombre de points des jacobiniennes sur un corps fini, Acta Arithmetica 16 (1990) 329–340.
- [4] Marc Perret, Number of points of Prym varieties over finite fields, Glasgow Math. J. 48 (2006) 275–280.
- [5] Heinz-Georg Quebbemann, Lattices from curves over finite fields, Preprint, April 1989.
- [6] Wilhelm Specht, Zur Theorie der elementaren Mittel, Math. Zeitschr. 74 (1960) 91–98.