Glasgow Math. J. **48** (2006) 275–280.
doi:10.1017/S0017089506003065. Printed in the United Kingdom

NUMBER OF POINTS OF PRYM VARIETIES OVER FINITE FIELDS

MARC PERRET

GRIMM, Université de Toulouse 2 – Le Mirail, 5, allées A. Machado, 31 058 Toulouse – France
e-mail: perret@univ-tlse2.fr

(Received 15 September, 2005; accepted 10 February, 2006)

Abstract. We establish some upper and lower bounds for the number of rational points of Prym varieties defined over finite fields. They are better than the usual Weil bounds valid for any abelian varieties defined over such fields.

2000 *Mathematics Subject Classification.* 14G15, 14K15, 11G10, 11G25.

I. Introduction. Let $\pi : Y \to X$ be a covering of smooth algebraic irreducible projective curves defined over a field k of zero or odd characteristic. Then the Jacobian J_X of X is isogenous to a sub-abelian variety of the Jacobian J_Y of Y. If we suppose moreover that π has degree 2, then the non-trivial involution σ of this covering induces an involution σ^* on J_Y.

DEFINITION AND PROPOSITION 1. *The Prym variety $Pr = Pr_\pi$ associated to the unramified double cover $\pi : Y \to X$ of a curve X of genus $g \geq 2$ is defined as $Pr := \mathrm{Im}(\sigma^* - id)$. It is an abelian subvariety of J_Y of dimension $g - 1$, isogenous to a direct factor of J_X in J_Y.*

For more details, see [**1**] or [**4**]. The computation of the dimension follows from the Riemann-Hurwitz Theorem. It is known that Prym varieties are in general *not* jacobian varieties. For instance, it has been proved by Beauville in [**1**] that any abelian variety of dimension less than 5 is a degeneration of Prym varieties, at least on algebraically closed fields.

Suppose from now on that k is the finite field $\mathbf{F}_q$ with q elements. Being an abelian variety of dimension $g - 1$, we can apply to Pr the following theorem. (See the historical source [**6**] for instance.)

THEOREM (WEIL). *Let A be an abelian variety of dimension d defined over $\mathbf{F}_q$. Then there exists $\theta_1, \ldots, \theta_d \in \mathbf{R}/2\pi\mathbf{Z}$ such that, for any $n \geq 1$, the number of rational points of A over $\mathbf{F}_{q^n}$ is given by*

$$\text{(i)} \qquad \sharp A(\mathbf{F}_{q^n}) = \prod_{i=1}^{d} (q^n + 1 - 2\sqrt{q^n} \cos n\theta_i).$$

In particular,

$$\text{(ii)} \qquad (q + 1 - 2\sqrt{q})^d \leq \sharp A(\mathbf{F}_q) \leq (q + 1 + 2\sqrt{q})^d.$$

(iii) *If in addition A is the jacobian of a curve C of genus g, then $d = g$ and the θ_i's are also related to the number of rational points of C over $\mathbf{F}_{q^n}$ by*

$$\sharp C(\mathbf{F}_{q^n}) = q^n + 1 - 2\sqrt{q^n}\left(\sum_{i=1}^{g} \cos n\theta_i\right).$$

Part (ii) of Weil's theorem for the prymian variety Pr_π of a double unramified cover π of a curve X of genus g reads as follows.

$$(q + 1 - 2\sqrt{q})^{g-1} \leq \sharp Pr_\pi(\mathbf{F}_q) \leq (q + 1 + 2\sqrt{q})^{g-1}. \tag{1}$$

The upper and lower bounds in (1) are the "best possible" in the sense that both can be reached. Indeed, it is known that any elliptic curve is a Prymian variety. Now, suppose that E is chosen so that it reaches the upper bound (resp. the lower bound) of Weil's inequality (ii). Such an elliptic curve does exist if q is a square; see [**5**]. Then E reaches the upper (resp. the lower) bound of (1).

The existence of such an elliptic curve E also proves, of course, that part (ii) of Weil's theorem for the Jacobian variety J_X of a curve X

$$(q + 1 - 2\sqrt{q})^{g} \leq \sharp J_X(\mathbf{F}_q) \leq (q + 1 + 2\sqrt{q})^{g} \tag{2}$$

is also the "best possible", at least for $g = 1$. Nevertheless, several sharper lower bounds and an upper bound were proved in [**3**] for Jacobians. For instance:

THEOREM (G. LACHAUD AND M. MARTIN-DESCHAMPS). *Let J_X be the jacobian variety of a genus g curve X defined over $\mathbf{F}_q$, and $\sharp X(\mathbf{F}_q)$ be the number of rational points of X. Then*

$$(\sqrt{q} - 1)^2 \frac{q^{g-1} - 1}{g} \frac{\sharp X(\mathbf{F}_q) + q - 1}{q - 1} \leq \sharp J_X(\mathbf{F}_q). \tag{3}$$

If X admits a map of degree d onto the projective line, then one has also

$$\sharp J_X(\mathbf{F}_q) \leq \frac{e}{q}(2g\sqrt{e})^{d-1} q^g. \tag{3 \textit{bis}}$$

The aim of this paper is to prove some Lachaud-Martin Deschamps type bounds for prymian varieties (see Theorem 2). The method used is different from theirs. It also gives some bounds for jacobians (Theorem 5), but they are not always as good as (3) and (3 *bis*); see remark 3 below.

II. Bounds for prymian varieties. If C is an algebraic curve defined over a finite field k with q elements, we denote by $\sharp C(\mathbf{F}_q)$ the number of $\mathbf{F}_q$-rational points of C.

The main result of this paper is as follows.

THEOREM 2. *Let X be an absolutely irreducible projective smooth algebraic curve defined over the finite field k of odd characteristic with q elements. Let g be the genus of X, and let $\pi\colon Y \to X$ be an unramified covering of degree 2. Then*

(i) $$\left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^{\frac{\sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q)}{2\sqrt{q}} - 2\delta} (q-1)^{g-1} \leq \sharp Pr(\mathbf{F}_q)$$

https://doi.org/10.1017/S0017089506003065 Published online by Cambridge University Press

with $\delta = 1$ if $\frac{\sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q)}{2\sqrt{q}} \notin \mathbf{Z}$, and $\delta = 0$ otherwise.

(ii) $$\sharp Pr(\mathbf{F}_q) \leq \left(q + 1 + \frac{\sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q)}{g-1}\right)^{g-1}.$$

(iii) If X admits a degree d map onto $\mathbf{P}^1_{\mathbf{F}_q}$, then

$$\left(\frac{\sqrt{q}-1}{\sqrt{q}+1}\right)^{d\frac{q+1}{2\sqrt{q}}+2}(q-1)^{g-1} \leq \sharp Pr(\mathbf{F}_q) \leq e^d(q+1)^{g-1}.$$

Proof of Theorem 2. We use Lemmas 3 and 4 that follow, whose proofs are postponed to the end of this section.

LEMMA 3. *Let* $a > 1$, $\gamma \in \mathbf{N}$, $b \in \mathbf{R}$ *and* P *be the polytope* $P = \{(x_1, \ldots, x_\gamma) \in [-1, 1]^\gamma \mid \sum_{k=1}^{\gamma} x_k = b\}$. *Suppose that* $|b| \leq \gamma$. *Then*

$$\inf_{(x_1,\ldots,x_\gamma)\in P} \prod_{k=1}^{\gamma}(a - x_k) \geq \left(\sqrt{\frac{a-1}{a+1}}\right)^{b+2\delta}(\sqrt{a^2-1})^\gamma,$$

where $\delta = 0$ *if* $b \in \mathbf{Z}$, $\delta = 1$ *otherwise.*

LEMMA 4. *In the situation of Lemma* 3, *we have*

$$\sup_{(x_1,\ldots,x_\gamma)\in P} \prod_{k=1}^{\gamma}(a - x_k) = \left(a - \frac{b}{\gamma}\right)^\gamma.$$

We now return to the proof of Theorem 2. Since Pr is isogenous to a direct factor of J_X in J_Y by Proposition 1, we have

$$\sharp Pr(\mathbf{F}_q) = \frac{\sharp J_Y(\mathbf{F}_q)}{\sharp J_X(\mathbf{F}_q)}. \tag{4}$$

We need the more precise form of Weil's theorem as in the introduction. Let F_C be the Frobenius endomorphism acting on the Tate module $T_\ell(J_C)$ of the Jacobian J_C of a smooth projective curve C over $\mathbf{F}_q$. It is well known that $\dim T_\ell(J_C) = 2g_C$ where g_C denotes the genus of C. If *Spec* F_C is the spectrum with multiplicities of this endomorphism, then Weil's theorem asserts that

$$\sharp C(\mathbf{F}_q) = q + 1 - \sum_{\omega \in Spec\ F_C} \omega, \tag{5}$$

$$\sharp J_C(k) = \prod_{\omega \in Spec\ F_C} (1 - \omega), \tag{6}$$

and $|\omega| = \sqrt{q}$ for all $\omega \in$ *Spec* F_C.

Now, J_X is a $Gal(\bar{k}/k)$-invariant subvariety of J_Y, so that $T_\ell(J_X)$ is an F_Y-invariant submodule of $T_\ell(J_Y)$, and F_X is the restriction of F_Y to $T_\ell(J_X)$. Moreover, $\dim T_\ell(J_Y) - \dim T_\ell(J_X) = 2g - 1 - g = g - 1$ by the Riemann-Hurwitz formula. Hence, there exists some numbers $\theta_1, \ldots, \theta_{g-1} \in \mathbf{R}/2\pi\mathbf{Z}$, such that

$$Spec\ F_Y = Spec\ F_X \cup \left\{\sqrt{q}\exp(\pm i\theta_1), \cdots, \sqrt{q}\exp(\pm i\theta_{q-1})\right\}.$$

https://doi.org/10.1017/S0017089506003065 Published online by Cambridge University Press

This implies, together with (5) applied to both X and Y :

$$\sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q) = -2\sqrt{q}\sum_{k=1}^{g-1}\cos\theta_k, \tag{7}$$

and together with (4) and (6) applied to both J_X and J_Y :

$$\sharp Pr_\pi(k) = \prod_{k=1}^{g-1}(q+1-2\sqrt{q}\cos\theta_k). \tag{8}$$

Notice that from (7) we have

$$-(g-1) \le \sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q) \le g-1.$$

One then deduces part (i) of Theorem 2 (resp. part (ii)) from (7), (8) and Lemma 3 (resp. Lemma 4) with $C = X$ and Y, $a = \frac{q+1}{2\sqrt{q}}$, $b = -\frac{\sharp Y(\mathbf{F}_q)-\sharp X(\mathbf{F}_q)}{2\sqrt{q}}$, and $\gamma = g-1$. Part (iii) follows then from the inequalities

$$-d(q+1) \le -\sharp X(\mathbf{F}_q) \le \sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q) \le \sharp X(\mathbf{F}_q) \le d(q+1).$$

The proof of the theorem will be complete if we prove both Lemma 3 and 4.

Proof of Lemma 3. Up to logarithm, we need to calculate the minimum of the function

$$F(x_1,\dots,x_\gamma) = \sum \log(a-x_k).$$

This is a strictly concave function. Hence its minimum on the compact convex domain P is reached on an extremal point of P; that is a point $x \in P$, such that $[a,b] \subset P$ implies that $x \notin]a,b[$.

Suppose that $x = (x_1, x_2, x_3, \dots, x_\gamma) \in P$ has at least two coordinates, x_1 and x_2 for simplicity, lying in $]-1,1[$. Then for ε sufficiently small, one also has $(x_1+t, x_2-t, x_3, \dots, x_\gamma) \in P$ for any $t \in]-\varepsilon,\varepsilon[$, which implies that x is not extremal on P. It follows that an extremal point $a = (a_1,\dots,a_\gamma) \in P$ satisfies

$$\begin{cases} a_k = 1 & \text{for } n \text{ values of } k \in \{1,\dots,\gamma\},\\ a_k = -1 & \text{for } m \text{ values of } k \in \{1,\dots,\gamma\},\\ \text{eventually } a_k = \pm\{b\} \text{ or } \pm(\{b\}-1) & \text{for } \delta \in \{0,1\},\ \text{value of } k \in \{1,\dots,\gamma\}. \end{cases}$$

Here, $\{b\}$ denotes the fractional part of the real number b, so that $\{b\} \in [0,1[$ and $b - \{b\} \in \mathbf{Z}$. Hence, we have $\delta = 0$ if $b \in \mathbf{Z}$, and $\delta = 1$ otherwise.

In the case $b \notin \mathbf{Z}$, that is $\delta = 1$, let us denote by β the unique coordinate of the extremal point $a = (a_1,\dots,a_\gamma)$ of P, lying in $]-1,1[$. Up to permutation of the entries, these extremal points then have the shape

$$\begin{cases} (1,\dots,1,-1,\dots,-1) & \text{if } b \in \mathbf{Z},\\ (1,\dots,1,-1,\dots,-1,\beta) & \text{if } b \notin \mathbf{Z}. \end{cases}$$

Now, the equations

$$\begin{cases} n+m+\delta = \gamma,\\ n-m+\delta\beta = b \end{cases} \tag{9}$$

https://doi.org/10.1017/S0017089506003065 Published online by Cambridge University Press

give the values of n and m in terms of the parameters γ, b and δ. We obtain:

$$\begin{aligned}\min \exp F(x_1, \ldots, x_\gamma) &= \exp F(a_1, \ldots, a_\gamma) \\ &= (a-\beta)^\delta (a-1)^n (a+1)^m \\ &= (a-\beta)^\delta (a^2-1)^{\frac{m+n}{2}} \left(\frac{a-1}{a+1}\right)^{\frac{n-m}{2}} \\ &= (a-\beta)^\delta (a^2-1)^{\frac{\gamma-\delta}{2}} \left(\frac{a-1}{a+1}\right)^{\frac{b-\delta\beta}{2}}\end{aligned}$$

by (9). But $a-\beta \geq a-1$ and $b-\delta\beta \leq b+\delta$. Hence Lemma 3 follows.

Proof of Lemma 4. We now have to calculate the maximum of the strictly concave function F given in the beginning of the proof of Lemma 3. It is a maximum on the compact set P. Since F is strictly concave on its range of definition, this is also a maximum on the larger set characterized by $\sum x_k = b$. By differential calculus, this maximum of F on the whole hyperplane whose equation is $\sum x_k = b$ is reached at the point $x = (x_1, \ldots, x_\gamma)$ provided that $grad\, F(x) = (-\frac{1}{a-x_1}, \ldots, -\frac{1}{a-x_\gamma})$ is colinear to $grad\, (\sum x_k - b) = (1, \ldots, 1)$; that is for $x_1 = \ldots = x_\gamma = \frac{b}{\gamma}$. Since $|b| \leq \gamma$ by assumption, this point lies on P, so that Lemma 4 follows.

REMARK 1. Let $\pi : Y \to X$ be a Galois covering of curves of any degree, and with possible ramifications. The Galois group G acts on the Jacobian J_Y and on its Tate module. For each irreducible character χ of G, there is an isotypic sub-abelian variety P_χ of J_Y. For the trivial character 1, we have $P_1 = J_X$. One could hope to apply the method of this paper to obtain bounds on the number of rationnal points of these P_χ. Unfortunately, they depend on the dimension of P_χ, which cannot in general be expressed in terms of simple invariants. The point made in the present paper is that in the degree two case, there is a unique non-trivial χ, and if moreover the covering is unramified, then one can compute by Riemann-Roch the dimension of J_Y in terms of the genus g of X, so that the dimension of the Prym variety $Pr_\pi = P_\chi$ for the unique non-trivial χ is known.

However, these dimensions can be computed when $\pi : Y \to X$ is a Galois covering of order prime to the characteristic p, whose group G has only rational representations (note that this is the case if G is a Weyl group). The reader is refered to [**2**]. The proofs therein also work in finite characteristic if one works with the Tate modules instead of the cohomology groups $H^0(X, \omega_X)$.

REMARK 2. Since Pr has dimension $g-1$, we have seen in the introduction that

$$(q+1-2\sqrt{q})^{g-1} \leq \sharp Pr(k) \leq (q+1+2\sqrt{q})^{g-1}$$

by Weil's theorem. On the other hand, (6) implies

$$-2(g-1)\sqrt{q} \leq \sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q) \leq 2(g-1)\sqrt{q}.$$

Hence, our bounds in Theorem 2 are always "better" than Weil's one (in the sense that for instance our upper bound is smaller than Weil's one).

https://doi.org/10.1017/S0017089506003065 Published online by Cambridge University Press

Moreover, one can observe that the closer $|\sharp Y(\mathbf{F}_q) - \sharp X(\mathbf{F}_q)|$ is to its maximal possible value $2(g-1)\sqrt{q}$, the "sharper" (in the sense that the ratio of our upper bound by our lower bound is smaller) are our bounds in Theorem 2. But for fixed $\pi : Y \to X$ over $\mathbf{F}_q$ and large n, it is expected by Tchebotarev that about half of the rational points in $X(\mathbf{F}_{q^n})$ split in Y, and half remain inert, so that $\sharp Y(\mathbf{F}_{q^n}) - \sharp X(\mathbf{F}_{q^n})$ should be less than $2(g-1)\sqrt{q^n}$. Consequently, it can be expected that our bound is rather good for large q^n.

REMARK 3. Of course, one can also give upper and lower bouds for the number of rational points of J_X in the same way. We obtain the following result.

THEOREM 3. *Let J_X be the Jacobian variety of the projective smooth irreducible curve X of genus g defined over $\mathbf{F}_q$. Then*

(i) $$\left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^{\frac{\sharp X(\mathbf{F}_q)-(q+1)}{2\sqrt{q}}-2\delta}(q-1)^g \leq \sharp J_X(\mathbf{F}_q)$$

with $\delta = 1$ if $\frac{\sharp X(\mathbf{F}_q)-q-1}{2\sqrt{q}} \notin \mathbf{Z}$, and $\delta = 0$ otherwise.

(ii) $$\sharp J_X(\mathbf{F}_q) \leq \left(q+1+\frac{\sharp X(\mathbf{F}_q)-q-1}{g}\right)^g.$$

Proof of Theorem 5. It follows from (5), (6), and Lemmas 3 and 4 with $\gamma = g$, $a = \frac{q+1}{2\sqrt{q}}$ and $b = -\frac{\sharp X(\mathbf{F}_q)-q-1}{2\sqrt{q}}$.

Let us compare this theorem with that of Lachaud and Martin-Deschamps stated in the introduction. Roughly speaking, their upper and lower bounds, say for fixed q and large g, both grow like q^g. The bounds of Theorem 5 can be better if $\sharp X(\mathbf{F}_q)$ is sufficiently small. However, suppose that X has a degree d map onto the projective line. Then $\sharp X(\mathbf{F}_q) \leq d(q+1)$, and the upper bound of Proposition 5 implies that

$$\sharp J_X(\mathbf{F}_q) \leq (q+1)^g\left(1+\frac{d-1}{g}\right)^g \leq \exp(d-1)(q+1)^g,$$

growing like $(q+1)^g$, which is not as good as (3 *bis*).

REMERCIEMENTS. Ce travail a été élaboré dans une grande mesure lors de discutions avec Emmanuel Hallouin et Thierry Henocq. L'auteur tient à les remercier vivement.

REFERENCES

1. A. Beauville, Prym varieties and the Schottky problem, *Inv. Math.* **41** (1977), 149–196.

2. A. Ksir, Dimensions of Prym varieties, *Internet. J. Math. Math. Sci.* **26** (2001), 107–116.

3. G. Lachaud and M. Martin-Deschamps, Nombre de points des jacobiennes sur un corps fini, *Acta Arith.* **16** (1990), 329–340.

4. D. Mumford, Prym varieties. I. in *Contributions to Analysis* (Academic Press, 1974), 325–350.

5. W. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. Éc. Norm. Sup* (4) **2** (1969), 521–560.

6. A. Weil, *Courbes algebriques et variétés abéliennes* (Hermann, Paris, 1948).