Glasgow Math. J. **58** (2016) 55–68.
doi:10.1017/S0017089515000063.

ON THE NUMBER OF RATIONAL POINTS ON PRYM VARIETIES OVER FINITE FIELDS

YVES AUBRY

Institut de Mathématiques de Toulon, Université de Toulon, 83 957 La Garde, France and Institut de Mathématiques de Marseille, Aix-Marseille Université, 13 288 Marseille, France
e-mail: yves.aubry@univ-tln.fr

and SAFIA HALOUI

Department of Mathematics, Technical University of Denmark, Lyngby, Denmark
e-mail: s.haloui@mat.dtu.dk

(Received 16 July 2014; accepted 3 October 2014; first published online 21 July 2015)

Abstract. We give upper and lower bounds for the number of rational points on Prym varieties over finite fields. Moreover, we determine the exact maximum and minimum number of rational points on Prym varieties of dimension 2.

2000 *Mathematics Subject Classification.* 14H40, 14G15, 14K15, 11G10, 11G25.

1. Introduction. Prym varieties are abelian varieties that come from unramified double covers of curves.

Let $\pi : Y \longrightarrow X$ be an unramified cover of degree 2 of a smooth algebraic irreducible projective curve defined over $\mathbb{F}_q$ with $q = p^e$, where p is an odd prime number. Let σ be the non-trivial involution of this cover and σ^* the induced involution on the Jacobian J_Y of Y. The *Prym variety* P_π (we will often drop the subscript π when it is clear from the context) associated to π is defined as

$$P_\pi = \mathrm{Im}(\sigma^* - \mathrm{id}).$$

It is also the connected component of the kernel of $\pi_* : J_Y \longrightarrow J_X$, which contains the origin of J_Y. It is an abelian subvariety of J_Y such that J_Y is isogenous to $J_X \times P_\pi$. If X has genus $g + 1 \geq 2$, then Y has genus $2g + 1$ by the Riemann–Hurwitz formula, and P_π has dimension g.

Prym varieties form a special class of principally polarized abelian varieties. Let us denote by $\mathcal{A}_g$ the moduli space of principally polarized abelian varieties of dimension g, by $\mathcal{J}_g$ the Jacobian locus in $\mathcal{A}_g$, by $\mathcal{P}_g$ the subset of $\mathcal{A}_g$ corresponding to Prym varieties, and by $\overline{\mathcal{P}}_g$ its closure. Then $\overline{\mathcal{P}}_g$ is an irreducible subvariety of $\mathcal{A}_g$ of dimension $3g$ (for $g \geq 5$) containing $\mathcal{J}_g$; for $g \leq 5$ one has $\overline{\mathcal{P}}_g = \mathcal{A}_g$ (see [3]).

We are interested in the maximum and minimum number of rational points on Prym varieties over finite fields. In [8], Perret proved that if X has genus $g + 1$, $\pi : Y \longrightarrow X$ is a double unramified cover over $\mathbb{F}_q$, and $N(X)$ and $N(Y)$ are the respective numbers of rational points on X and Y, then the number of rational points $\#P(\mathbb{F}_q)$ on

the associated Prym variety P satisfies

$$\#P(\mathbb{F}_q) \leq \Big(q+1+\frac{N(Y)-N(X)}{g}\Big)^g, \tag{1}$$

and

$$\#P(\mathbb{F}_q) \geq \Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)^{\frac{N(Y)-N(X)}{2\sqrt{q}}-2\delta}(q-1)^g, \tag{2}$$

where $\delta = 0$ if $\frac{N(Y)-N(X)}{2\sqrt{q}}+g$ is an even integer, and $\delta = 1$ otherwise (here we have corrected the value of δ given in [**8**]).

The aim of this paper is to give new upper and lower bounds on the number of rational points on Prym varieties over finite fields.

In Section 2, we recall some methods (from [**1**, **2**]) to estimate the number of rational points on an abelian variety if we know its trace. We also explain how to derive the Perret bounds (1) and (2) in this setting.

In Section 3, we study the trace of a Prym variety. We prove that the trace $-\tau(P)$ of a Prym variety P defined over $\mathbb{F}_q$ satisfies the following bound dependent of $N(X)$ (see Proposition 6):

$$\tau(P)^2 \leq g(q^2-1) - \frac{g(N(X)-q-1)^2}{g+1} - 2g(N(X)-q-1) + 4g^2q.$$

Then we prove the following new bounds on $\#P(\mathbb{F}_q)$ (see Corollary 8):

$$m(-N(X)) \leq \#P(\mathbb{F}_q) \leq M(N(X)),$$

where

$$M(\tau) = \left(q+1+\frac{\tau}{g}\right)^g,$$

and

$$m(\tau) = (q+1+\tau-2(r(\tau)-s(\tau))\sqrt{q})(q+1+2\sqrt{q})^{r(\tau)}(q+1-2\sqrt{q})^{s(\tau)},$$

with $r(\tau) = [\frac{g+[\frac{\tau}{2\sqrt{q}}]}{2}]$ and $s(\tau) = [\frac{g-1-[\frac{\tau}{2\sqrt{q}}]}{2}]$.

Furthermore, if $|\tau(P)| \geq q-g$ (for instance, this condition is satisfied when $g \geq q$), then we get the following bound on the trace depending only on g and q (see Proposition 9):

$$|\tau(P)| \leq \frac{g}{2g+1}\Big(q-g+\sqrt{(q-g)^2+(2g+1)(4gq+q^2+6q+1)}\Big).$$

Finally, for $g \geq q$, we prove the following new bounds on $\#P(\mathbb{F}_q)$ (see Theorem 11):

$$(q+1-2\sqrt{q})^g \leq m(-\psi) \leq \#P(\mathbb{F}_q) \leq M(\psi) \leq (q+1+2\sqrt{q})^g,$$

where

$$\psi = \frac{g}{2g+1}\Big(q-g+\sqrt{(q-g)^2+(2g+1)(4gq+q^2+6q+1)}\Big).$$

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

The last section is devoted to the study of Prym surfaces. The main result of this section is that any product $E_1 \times E_2$ of elliptic curves defined over $\mathbb{F}_q$ is isomorphic (with the product polarization) to a Prym variety except if one of the conditions below is satisfied:

- $q = 7$, E_1 and E_2 have full 2-torsion over $\mathbb{F}_q$, $\#E_1(\mathbb{F}_q) \neq \#E_2(\mathbb{F}_q)$ and $\#E_1(\mathbb{F}_q)$ or $\#E_1(\mathbb{F}_q)$ is equal to 8,
- $q = 5$, E_1 and E_2 have full 2-torsion over $\mathbb{F}_q$,
- $q = 3$, E_1 or E_2 has full 2-torsion over $\mathbb{F}_q$.

This enable us (Corollary 17) to find exact formulas for the maximum and the minimum number of points on Prym surfaces.

2. Bounding the number of rational points on an abelian variety depending on its trace. Let A be an abelian variety of dimension g defined over a finite field $\mathbb{F}_q$. The *Weil polynomial* $f_A(t)$ of A is the characteristic polynomial of its Frobenius endomorphism. It is a monic polynomial with integer coefficients and the set of its roots (with multiplicity) consists of couples of conjugated complex numbers of modulus $\sqrt{q}$.

Let $\omega_1, \ldots, \omega_g, \overline{\omega}_1, \ldots, \overline{\omega}_g$ be the roots of $f_A(t)$. For $1 \leq i \leq g$, we set $x_i = -(\omega_i + \overline{\omega}_i)$. We say that A is of *type* $[x_1, \ldots, x_g]$. The *trace* of A is defined to be the trace of its Frobenius endomorphism. We denote by $\tau(A)$ the opposite of the trace of A, more explicitly

$$\tau(A) = -\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = \sum_{i=1}^{g} x_i.$$

This is an integer, and since $|x_i| \leq 2\sqrt{q}$, $i = 1, \ldots, g$, we have $|\tau(A)| \leq 2g\sqrt{q}$.

In the case where the abelian variety is the Jacobian J_X of a smooth projective absolutely irreducible curve X defined over $\mathbb{F}_q$, its trace can be easily expressed in terms of the number $N(X)$ of rational points on X. Indeed, we have

$$\tau(J_X) = N(X) - (q + 1), \tag{3}$$

which follows from the fact that the numerator of the zeta function of X is the reciprocal polynomial of the Weil polynomial $f_{J_C}(t)$.

Now let P be a Prym variety and $\pi : Y \longrightarrow X$ be an unramified double cover that gives rise to P. The map $\pi_* \times (\sigma^* - \mathrm{id}) : J_Y \longrightarrow J_X \times P$ has finite kernel and sends the ℓ^n-torsion points of J_Y in to those of $J_X \times P$, for any prime number ℓ distinct from the characteristic of $\mathbb{F}_q$. Then, taking the tensor product of the Tate modules with $\mathbb{Q}_\ell$, we get an isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$T_\ell(J_Y) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \longrightarrow T_\ell(J_X \times P) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = T_\ell(J_X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \times T_\ell(P) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

which commutes with the action of the Frobenius. Therefore, we have

$$f_{J_Y}(t) = f_{J_X}(t) f_P(t).$$

It follows that

$$\tau(J_Y) = \tau(J_X) + \tau(P),$$

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

and using (3), we get

$$\tau(P) = N(Y) - N(X). \tag{4}$$

Let us come back to general abelian varieties. With the same notations as before, we can write

$$f_A(t) = \prod_{i=1}^{g}(t-\omega_i)(t-\overline{\omega}_i) = \prod_{i=1}^{g}(t^2 + x_i t + q).$$

It is well known that the number of rational points on A is

$$\#A(\mathbb{F}_q) = f_A(1) = \prod_{i=1}^{g}(q+1+x_i). \tag{5}$$

Since $|x_i| \leq 2\sqrt{q}$, one deduces from (5) the classical *Weil bounds*

$$(q+1-2\sqrt{q})^g \leq \#A(\mathbb{F}_q) \leq (q+1+2\sqrt{q})^g. \tag{6}$$

Now, for $\tau \in [-2g\sqrt{q}; 2g\sqrt{q}]$, define

$$M(\tau) = \left(q+1+\frac{\tau}{g}\right)^g, \tag{7}$$

and

$$m(\tau) = (q+1+\tau-2(r(\tau)-s(\tau))\sqrt{q})(q+1+2\sqrt{q})^{r(\tau)}(q+1-2\sqrt{q})^{s(\tau)}, \tag{8}$$

where $r(\tau) = [\frac{g+[\frac{\tau}{2\sqrt{q}}]}{2}]$ and $s(\tau) = [\frac{g-1-[\frac{\tau}{2\sqrt{q}}]}{2}]$ (for a real number x, we denote by $[x]$ its integer part).

We have the following estimation of $\#A(\mathbb{F}_q)$ (see [**1**, **2**]):

THEOREM 1. *If A is an abelian variety defined over $\mathbb{F}_q$ of dimension g, we have*

$$m(\tau(A)) \leq \#A(\mathbb{F}_q) \leq M(\tau(A)).$$

Notice that in the case of Prym varieties, the upper bound of Theorem 1 together with (4) gives the Perret upper bound (1). The lower bound (2) comes from the fact (proved by Perret in the case of Prym varieties) that for any abelian variety, we have

$$\#A(\mathbb{F}_q) \geq \left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right)^{\frac{\tau(A)}{2\sqrt{q}}-2\delta}(q-1)^g,$$

where $\delta = 0$ if $\frac{\tau(A)}{2\sqrt{q}} + g$ is an even integer and $\delta = 1$ otherwise. The lower bound (2) is always less precise than the lower bound from Theorem 1 (for more details, see [**2**]).

In the next section, we shall use Theorem 1 without knowing the value of $\tau(A)$ (but having an estimation). In order to do so, we need some basic results on the functions M and m defined by (7) and (8). These results are summarized in the following proposition:

PROPOSITION 2. *The functions M and m are continuous and increasing on the interval* $[-2g\sqrt{q}; 2g\sqrt{q}]$.

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

Proof. The function M is obviously continuous, and it is increasing because for $\tau \in [-2g\sqrt{q}; 2g\sqrt{q}]$, we have $q + 1 + \tau/g \geq q + 1 - 2\sqrt{q} > 0$.

Now, we focus on m. First, notice that the functions r and s are piecewise constant, and therefore m is piecewise an affine function with leading coefficient $(q + 1 + 2\sqrt{q})^{r(\tau)}(q + 1 - 2\sqrt{q})^{s(\tau)} > 0$. Hence, the fact that m is increasing will follow from its continuity.

We now prove that m is continuous. Let $k \in \{-g, \ldots, g-2\}$ be an integer which has the *same parity* as g, and $\alpha \in [0; 2[$. As $[\alpha] \in \{0, 1\}$ and $g + k$ and $g - k$ are non-negative even integers, we have

$$r(2\sqrt{q}(k + \alpha)) = \left[\frac{g + k + [\alpha]}{2}\right] = \frac{g + k}{2} + \left[\frac{[\alpha]}{2}\right] = \frac{g + k}{2},$$

and

$$s(2\sqrt{q}(k + \alpha)) = \left[\frac{g - 1 - k - [\alpha]}{2}\right] = \frac{g - k}{2} + \left[\frac{-1 - [\alpha]}{2}\right] = \frac{g - k}{2} - 1.$$

In particular, the functions r and s are constant on any interval of the form $[2k\sqrt{q}; 2(k + 2)\sqrt{q}[$, where $k \in \{-g, \ldots, g-2\}$ has the same parity as g, and thus m is continuous (in fact affine) on these intervals.

It remains to check that

$$\lim_{\substack{\alpha \to 2 \\ \alpha < 2}} m(2\sqrt{q}(k + \alpha)) = m(2\sqrt{q}(k + 2)).$$

The previous computations show us that

$$r(2\sqrt{q}(k + \alpha)) - s(2\sqrt{q}(k + \alpha)) = k + 1,$$

and thus the first factor in the expression of m is

$$q + 1 + 2\sqrt{q}(k + \alpha) - 2(r(2\sqrt{q}(k + \alpha)) - s(2\sqrt{q}(k + \alpha)))\sqrt{q} = q + 1 + 2\sqrt{q}(\alpha - 1).$$

We deduce that

$$m(2\sqrt{q}(k + \alpha)) = (q + 1 + 2\sqrt{q}(\alpha - 1))(q + 1 + 2\sqrt{q})^{\frac{g+k}{2}}(q + 1 - 2\sqrt{q})^{\frac{g-k}{2}-1},$$

and as

$$m(2\sqrt{q}(k + 2)) = (q + 1 - 2\sqrt{q})(q + 1 + 2\sqrt{q})^{\frac{g+k}{2}+1}(q + 1 - 2\sqrt{q})^{\frac{g-k}{2}-2},$$

we have

$$m(2\sqrt{q}(k + \alpha)) = \frac{(q + 1 + 2\sqrt{q}(\alpha - 1))}{(q + 1 + 2\sqrt{q})} m(2\sqrt{q}(k + 2)),$$

and the result follows. □

Notice that we have

$$m(-2g\sqrt{q}) = (q + 1 - 2\sqrt{q})^g \text{ and } M(2g\sqrt{q}) = (q + 1 + 2\sqrt{q})^g,$$

in particular, the bounds of Theorem 1 are at least as precise as the Weil bounds (6) (but require more information on A).

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

3. On the trace of Prym varieties. As before, let A be an abelian variety defined over $\mathbb{F}_q$ of dimension g, $f_A(t)$ be its Weil polynomial, $\omega_1, \ldots, \omega_g, \overline{\omega}_1, \ldots, \overline{\omega}_g$ be the complex roots of $f_A(t)$, $x_i = -(\omega_i + \overline{\omega}_i)$, $1 \leq i \leq g$, and

$$\tau(A) = -\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = \sum_{i=1}^{g} x_i,$$

be the opposite of the trace of A. For $k \geq 1$, we also define $\tau_k(A)$ to be the opposite of the trace of $A \times_{\mathbb{F}_q} \mathbb{F}_{q^k}$, that is,

$$\tau_k(A) = -\sum_{i=1}^{g}(\omega_i^k + \overline{\omega}_i^k).$$

Hence, we have $\tau_1(A) = \tau(A)$.

We recall the following classical upper bound for $\tau_2(A)$ (see [**6**]), which is a direct consequence of the Cauchy–Schwartz inequality:

$$\tau_2(A) = -\sum_{i=1}^{g} x_i^2 + 2gq \leq -\frac{1}{g}\Big(\sum_{i=1}^{g} x_i\Big)^2 + 2gq = \frac{-\tau(A)^2}{g} + 2gq. \tag{9}$$

Now let P be a Prym variety and $\pi : Y \longrightarrow X$ be an unramified double cover that gives rise to P. We denote by $N_k(X)$ and $N_k(Y)$ the respective numbers of rational points on X and Y over $\mathbb{F}_{q^k}$ for $k \geq 1$. The results from Section 2 tell us that

$$N_k(X) = q^k + 1 + \tau_k(J_X),$$

and

$$N_k(Y) = q^k + 1 + \tau_k(J_X) + \tau_k(P) = N_k(X) + \tau_k(P).$$

REMARK 3. As π is unramified and of degree 2, the number of rational points on Y must be even (it is twice the number of splitting rational points on X). Of course, this holds for any finite extension of the base field, and therefore, for $k \geq 1$, the numbers $N_k(Y)$ are even, or in other words (recall that q is supposed to be odd), we have

$$\tau_k(P) \equiv \tau_k(J_X) \mod 2.$$

Now, we give estimations of $\tau(P)$ that are independent from Y. We start by the following lemma:

LEMMA 4. *With the notations above, we have*

$$0 \leq N(Y) \leq 2N(X) \leq N_2(Y).$$

Proof. The first inequality is obvious. For the second one, we use the fact that the image of a rational point is a rational point, and the number of points in the preimage of a point is at most 2. For the third one, if we denote by $B_d(Y)$ the number of points on Y of degree d, we have

$$N_2(Y) = B_1(Y) + 2B_2(Y).$$

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

The set $X(\mathbb{F}_q)$ can be partitioned into two subsets: the rational points which are split and those which are inert in the cover $Y \longrightarrow X$. Denote respectively their cardinality by s and i, we have $B_1(Y) \geq 2s$ and $B_2(Y) \geq i$. Hence, $N_2(Y) \geq 2s + 2i = 2N(X)$. □

The two first inequalities of Lemma 4 give us immediately the following result, which is stated in [**8**]:

PROPOSITION 5 (Perret). *We have*

$$|\tau(P)| \leq N(X).$$

Notice that the bound of Proposition 5 is sharp when X has few points (in particular, if X has no rational points, then we get the exact value of τ).

The third inequality of Lemma 4 gives us the following proposition:

PROPOSITION 6. *We have*

$$\tau(P)^2 \leq g(q^2-1) - \frac{g(N(X)-q-1)^2}{g+1} - 2g(N(X)-q-1) + 4g^2q.$$

Proof. We have

$$\begin{aligned} 2(q+1+\tau(J_X)) = 2N_1(X) &\leq N_2(Y) \\ &= q^2 + 1 + \tau_2(J_X) + \tau_2(P) \\ &\leq q^2 + 1 - \tau(J_X)^2/(g+1) + 2(g+1)q - \tau(P)^2/g + 2gq, \end{aligned}$$

where the last inequality comes from (9). Rearranging the terms, we find

$$\frac{\tau(P)^2}{g} \leq q^2 - 1 - \frac{\tau(J_X)^2}{g+1} - 2\tau(J_X) + 4gq,$$

and using the fact that $\tau(J_X) = N(X) - q - 1$, the result follows once we notice that the second term in the previous inequality is necessarily non-negative. □

REMARK 7. The third inequality of Lemma 4 is sharp when X has many points. Indeed, we have

$$2N(X) \leq N_2(Y) \leq 2N_2(X).$$

The last inequality is just the second inequality of Lemma 4 applied after a quadratic extension of the base field, and according to (9), a curve with many points over $\mathbb{F}_q$ must have few points over $\mathbb{F}_{q^2}$.

Now, recall that we have defined

$$M(\tau) = \left(q + 1 + \frac{\tau}{g}\right)^g,$$

and

$$m(\tau) = (q+1+\tau - 2(r(\tau)-s(\tau))\sqrt{q})(q+1+2\sqrt{q})^{r(\tau)}(q+1-2\sqrt{q})^{s(\tau)},$$

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

where $r(\tau) = [\frac{g+[\frac{\tau}{2\sqrt{q}}]}{2}]$ and $s(\tau) = [\frac{g-1-[\frac{\tau}{2\sqrt{q}}]}{2}]$. Theorem 1 and Proposition 2 give us the following result:

COROLLARY 8. *We have*

$$m(-N(X)) \leq \#P(\mathbb{F}_q) \leq M(N(X)),$$

and

$$m\left(-\varphi(N(X))\right) \leq \#P(\mathbb{F}_q) \leq M\left(\varphi(N(X))\right),$$

where

$$\varphi(N(X)) = \left(g(q^2-1) - g(N(X)-q-1)^2/(g+1) - 2g(N(X)-q-1) + 4g^2q\right)^{1/2}.$$

By combining Propositions 5 and 6, we can eliminate the variable $N(X)$:

PROPOSITION 9. *If $|\tau(P)| \geq q-g$ (for instance, this condition is satisfied when $g \geq q$), then we have*

$$|\tau(P)| \leq \frac{g}{2g+1}\left(q-g+\sqrt{(q-g)^2+(2g+1)(4gq+q^2+6q+1)}\right).$$

Proof. The last inequality in the proof of Proposition 6 can be rewritten as

$$\frac{\tau(J_X)^2}{g+1} + 2\tau(J_X) + \tau(P)^2/g - q^2 - 4gq + 1 \leq 0. \tag{10}$$

Considering the left hand side of (10) as a polynomial equation in $\tau(J_X)$ and computing the roots, we find

$$\tau(J_X) \leq -(g+1) + \sqrt{(g+1)(q^2+g+4gq-\tau(P)^2/g)}.$$

But Proposition 5 tells us that $\tau(J_X) \geq |\tau(P)| - (q+1)$, and therefore, we have

$$|\tau(P)| + g - q \leq \sqrt{(g+1)(q^2+g+4gq-\tau(P)^2/g)}. \tag{11}$$

Under the assumptions of the proposition, the left hand side of (11) is non-negative, so we can square everything. We get

$$(|\tau(P)| + g - q)^2 \leq (g+1)\left(q^2+g+4gq-\frac{\tau(P)^2}{g}\right),$$

so that

$$\begin{aligned}\tau(P)^2 + 2(g-q)|\tau(P)| + g^2 - 2gq + q^2 \leq\ & gq^2 + g^2 + 4g^2q \\ & - \tau(P)^2 + q^2 + g + 4gq - \tau(P)^2/g.\end{aligned}$$

Hence

$$-(2g+1)\tau(P)^2 - 2g(g-q)|\tau(P)| + g^2(4gq+q^2+6q+1) \geq 0. \tag{12}$$

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

Considering the left hand side of (12) as a polynomial equation in $|\tau(P)|$ and computing the roots, we get the result. □

The bound of Proposition 9 is sharper than the Weil bound $|\tau(P)| \leq 2g\sqrt{q}$ if

$$2g\sqrt{q} \geq \Big(q - g + \sqrt{(q-g)^2 + (2g+1)(4gq + q^2 + 6q + 1)}\Big)g/(2g+1), \quad (13)$$

and since the right hand side of (13) is the greatest root of the polynomial in $|\tau(P)|$ defined by the left hand side of (12), and the smallest root must be smaller than $2g\sqrt{q}$, the inequality (13) is equivalent to

$$0 \leq (2g+1)(2g\sqrt{q})^2 + 2g(g-q)2g\sqrt{q} - g^2(4gq + q^2 + 6q + 1),$$

which is equivalent to

$$0 \leq (2g+1)4q + 4(g-q)\sqrt{q} - 4gq - q^2 - 6q - 1,$$

and which is finally equivalent to

$$g \geq (q^2 + 4q\sqrt{q} + 2q + 1)/(4q + 4\sqrt{q}) = (q\sqrt{q} + 3q - \sqrt{q} + 1)/(4\sqrt{q}).$$

Notice that this last condition is satisfied when $g \geq q$.

REMARK 10. According to the results of Ihara [**6**], the number of rational points of a (smooth, projective, absolutely irreducible) curve of genus $(g+1)$ over $\mathbb{F}_q$ is at most

$$\frac{1}{2}\Big(2q - g + 1 + \sqrt{(8q+1)(g+1)^2 + (4q^2 - 4q)(g+1)}\Big), \quad (14)$$

so using Proposition 5, we get another bound for $|\tau(P)|$. However, it is easy to check that the quantity (14) is always (for any q and g) greater than the right hand side of the inequality of Proposition 9.

As in Corollary 8, we can derive some bounds on $\#P(\mathbb{F}_q)$ depending only on g and q.

THEOREM 11. *If $g \geq q$, we have*

$$(q + 1 - 2\sqrt{q})^g \leq m(-\psi) \leq \#P(\mathbb{F}_q) \leq M(\psi) \leq (q + 1 + 2\sqrt{q})^g,$$

where

$$\psi = \frac{g}{2g+1}\Big(q - g + \sqrt{(q-g)^2 + (2g+1)(4gq + q^2 + 6q + 1)}\Big).$$

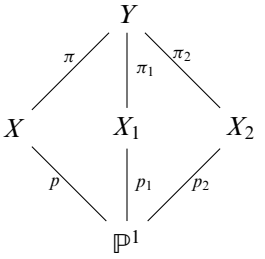
4. Prym varieties of dimension 2. In this section, we focus on Prym surfaces. According to the Weil Theorem, any principally polarized abelian surface A defined over $\mathbb{F}_q$ is either a Jacobian, or the restriction of scalars of a polarized elliptic curve over $\mathbb{F}_{q^2}$, or a product of two polarized elliptic curves. In the two first cases, it is known that A is a Prym variety; it follows easily from the Legendre construction described below (for the second case, see [**4**]). We shall deal with the third case and give an explicit description of the set of products of two elliptic curves which are isomorphic (with the polarization) to a Prym variety.

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

We start by recalling the Legendre construction, more details can be found in [**7**, **4**]. Let X be an hyperelliptic curve of genus g, let $p : X \longrightarrow \mathbb{P}^1$ be an associated double cover and $\{z_1, \ldots, z_{2g+2}\}$ be the set of branch points. Then all unramified double covers $\pi : Y \longrightarrow X$ over $\bar{\mathbb{F}}_q$ arise as follows:

(1) Separate the branch points into two nonempty groups of even cardinality: $\{1, 2, \ldots, 2g+2\} = I_1 \cup I_2, \#I_1 = 2h+2, \#I_2 = 2k+2, I_1 \cap I_2 = \emptyset$ (hence $h + k + 1 = g$).
(2) Consider the degree 2 maps $p_1 : X_1 \longrightarrow \mathbb{P}^1$ and $p_2 : X_2 \longrightarrow \mathbb{P}^1$ with respective sets of branch points $\{z_i\}_{i\in I_1}$ and $\{z_i\}_{i\in I_2}$.
(3) Let Y be the normalization of $X \times_{\mathbb{P}^1} X_1$.

Then we have such a diagram



In this situation, the Prym variety P_π associated to the cover $\pi : Y \longrightarrow X$ is isomorphic to the product of the Jacobians of X_1 and X_2,

$$P_\pi \simeq J_{X_1} \times J_{X_2}.$$

The isomorphism is given by $\pi_1^* + \pi_2^* : J_{X_1} \times J_{X_2} \longrightarrow P_\pi$, see [**4**].

Moreover, if I_1 and I_2 are chosen to be stable under the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ then all the curves and maps involved in this construction will be defined over $\mathbb{F}_q$.

In particular, we have the following result.

PROPOSITION 12 (Legendre construction). *Let X_1 and X_2 be two hyperelliptic (or elliptic) curves. The product $J_{X_1} \times J_{X_2}$ of polarized abelian varieties is isomorphic to the Prym variety of a double cover of an hyperelliptic curve if and only if there exist two degree 2 maps $p_1 : X_1 \longrightarrow \mathbb{P}^1$ and $p_2 : X_2 \longrightarrow \mathbb{P}^1$ with disjoint sets of ramified points.*

Proposition 12 has the following direct consequence:

COROLLARY 13. *A Jacobian of dimension 2 is isomorphic to a Prym variety.*

Proof. A Jacobian of dimension 2 is the Jacobian of a (necessarily hyperelliptic) genus 2 curve C and the associated double cover $p : C \longrightarrow \mathbb{P}^1$ is ramified at exactly 6 points. Since $\#\mathbb{P}^1(\mathbb{F}_{q^2}) = q^2 + 1 \geq 3^2 + 1 = 10$, there exist unramified points $z_1, z_2 \in \mathbb{P}^1(\mathbb{F}_{q^2})$ such that the set $\{z_1, z_2\}$ is invariant under the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Now we consider a double cover $p_1 : C_1 \longrightarrow \mathbb{P}^1$ which is ramified at z_1 and z_2 (note that C_1 is a genus zero curve) and we apply Proposition 12. □

In order to apply Proposition 12 to the product of two elliptic curves, we shall use the following Lemma:

LEMMA 14. *Let $A = \{a_0, a_1, a_2, a_3\}$ and $B = \{b_0, b_1, b_2, b_3\}$ be two subsets of $\mathbb{P}^1(\bar{\mathbb{F}}_q)$ with four elements. Suppose that $a_0, b_0 \in \mathbb{P}^1(\mathbb{F}_q)$ and that A and B are invariant under*

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

the action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$*, then there exists an automorphism* φ *of* $\mathbb{P}^1$ *defined over* $\mathbb{F}_q$ *such that* $\varphi(A)\cap B=\emptyset$*, except possibly if* $q=5,7$ *and* A *and* B *are contained in* $\mathbb{P}^1(\mathbb{F}_q)$*, or if* $q=3$ *and* A *or* B *is contained in* $\mathbb{P}^1(\mathbb{F}_q)$*.*

Proof. We start by recalling that by the Fundamental Theorem of Projective Geometry: for any two subsets $\{x_1,x_2,x_3\}$ and $\{z_1,z_2,z_3\}$ of $\mathbb{P}^1(\bar{\mathbb{F}}_q)$ with three elements, there exists a unique automorphism $\varphi\in\mathrm{Aut}_{\bar{\mathbb{F}}_q}(\mathbb{P}^1)$ such that $\varphi(x_i)=z_i$, $i=1,2,3$. In particular, we have

$$\#\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1)=(q+1)q(q-1)=q^3-q,$$

because for $\{x_1,x_2,x_3\}\subseteq\mathbb{P}^1(\mathbb{F}_q)$ we have $(q+1)$ possible choices for the image of x_1, q for the image of x_2 and $(q-1)$ for the image of x_3, and the obtained automorphisms commute with the Frobenius since they do at x_1,x_2,x_3, thus they are defined over $\mathbb{F}_q$. Now, let

$$S=\left\{\varphi\in\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1),\quad \varphi(A)\cap B\neq\emptyset\right\}.$$

We would like to prove that under the conditions of the lemma, the quantity

$$\Psi=\#\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1)-\#S=q^3-q-\#S,$$

is positive. In order to do so, we consider the sets

$$T_{U,V}=\left\{\varphi\in\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1),\quad \varphi(U)\subseteq V\right\},$$

where $U\subseteq A$ and $V\subseteq B$. We also denote by $\mathcal{P}(i,j)$ the assertion

$$\#A\cap\mathbb{P}^1(\mathbb{F}_q)=i\quad\text{and}\quad\#B\cap\mathbb{P}^1(\mathbb{F}_q)=j.$$

Notice that $\mathcal{P}(i,j)$ can be true only if $i,j\in\{1,2,4\}$. Moreover, if the lemma is true under $\mathcal{P}(i,j)$, then it is true as well under $\mathcal{P}(j,i)$ (switch A and B and exchange automorphisms by their inverse).

If $\mathcal{P}(4,4)$ is satisfied, we have

$$S=\bigcup_{i=0}^{3}T_{\{a_i\},B},$$

so using the Inclusion-Exclusion Principle, we deduce that

$$\begin{aligned}\#S&=\sum_{i=0}^{3}\#T_{\{a_i\},B}-\sum_{0\le i<j\le 3}\#T_{\{a_i,a_j\},B}+\sum_{0\le i<j<k\le 3}\#T_{\{a_i,a_j,a_k\},B}-\#T_{A,B}\\&\le\sum_{i=0}^{3}\#T_{\{a_i\},B}-\sum_{0\le i<j\le 3}\#T_{\{a_i,a_j\},B}+\sum_{0\le i<j<k\le 3}\#T_{\{a_i,a_j,a_k\},B}.\end{aligned}$$

For $\{i,j,k\}\subseteq\{0,1,2,3\}$, we have $\#T_{\{a_i\},B}=4q(q-1)$, $\#T_{\{a_i,a_j\},B}=2\binom{4}{2}(q-1)=12(q-1)$ and $\#T_{\{a_i,a_j,a_k\},B}=3!\binom{4}{3}=24$, thus

$$\#S\le 16q(q-1)-12(q-1)\binom{4}{2}+24\binom{4}{3}=16q^2-88q+168,$$

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

hence

$$\Psi \geq q^3 - 16q^2 + 87q - 168 = (q-7)(q^2 - 9q + 24).$$

Using the same trick, we check that Ψ is:

- equal to $(q-1)(q-3)(q-4)$ under $\mathcal{P}(2,4)$,
- equal to $q(q-1)(q-3)$ under $\mathcal{P}(1,4)$,
- greater than or equal to $q^3 - 4q^2 + 3q + 4$ under $\mathcal{P}(2,2)$,
- equal to $q(q-1)^2$ under $\mathcal{P}(1,2)$,
- greater than or equal to $q^3 - q^2 - 3$ under $\mathcal{P}(1,1)$.

We deduce that Ψ is positive under $\mathcal{P}(4,4)$ for $q > 7$ (since the polynomial $t^2 - 9t + 24$ has no real root), under $\mathcal{P}(2,4)$ or $\mathcal{P}(1,4)$ for $q > 4$ and under $\mathcal{P}(2,2)$, $\mathcal{P}(1,2)$ or $\mathcal{P}(1,1)$ for any q (since the roots of the polynomials $t^3 - 4t^2 + 3t + 4$ and $t^3 - t^2 - 3$ are smaller than 2). This concludes the proof. □

Now, we can solve the problem of deciding which product of elliptic curves is isomorphic to a Prym variety:

PROPOSITION 15. *Let E_1 and E_2 be two elliptic curves defined over $\mathbb{F}_q$. Then $E_1 \times E_2$ is isomorphic (with the polarization) to a Prym variety if and only if the conditions below are not satisfied:*

- *$q = 7$, E_1 and E_2 have full 2-torsion over $\mathbb{F}_q$, $\#E_1(\mathbb{F}_q) \neq \#E_2(\mathbb{F}_q)$ and $\#E_1(\mathbb{F}_q)$ or $\#E_1(\mathbb{F}_q)$ is equal to 8,*
- *$q = 5$, E_1 and E_2 have full 2-torsion over $\mathbb{F}_q$,*
- *$q = 3$, E_1 or E_2 has full 2-torsion over $\mathbb{F}_q$.*

Proof. According to [**4**], the Prym varieties associated to double covers of non-hyperelliptic curves are always polarized Jacobians. Therefore, $E_1 \times E_2$ is a Prym variety if and only if the conditions of Proposition 12 are satisfied.

For $i = 1, 2$, let $y^2 = f_i(x)$ be a Weierstrass equation for E_i, p_i be the associated degree 2 map and A_i the set of ramified points. In this case, the 2-torsion points of E_i correspond to the elements of $A_i \setminus \{\infty\}$.

If $q > 7$ or if $q = 5, 7$ and E_1 or E_2 has not full 2-torsion over $\mathbb{F}_q$ or if $q = 3$ and E_1 and E_2 have not full 2-torsion over $\mathbb{F}_q$, then Lemma 14 ensures that there exists $\varphi \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1)$ such that $\varphi(A_1) \cap A_2 = \emptyset$. The maps $\varphi \circ p_1$ and p_2 satisfy the conditions of Proposition 12.

For $q = 3, 5$, if one of the exceptional conditions of Proposition 15 holds, it is clear that the conditions of Proposition 12 cannot be satisfied, since $\mathbb{P}^1(\mathbb{F}_q)$ does not have enough elements.

Finally, suppose that $q = 7$ and $A_1 \cup A_2 \subseteq \mathbb{P}^1(\mathbb{F}_7)$. We shall use the fact (easy to check) that the data of the set of ramified points of a (necessarily separable) degree 2 map $p : X \longrightarrow \mathbb{P}^1$ over $\mathbb{F}_7$ determines the curve X up to quadratic twist. The proof of Lemma 14 (the part where $\mathcal{P}(4,4)$ is assumed) shows that the conclusion of the lemma holds under our assumptions if and only if $\#T_{A_1,A_2} > 0$, i.e. there exists an automorphism $\varphi \in \mathrm{Aut}_{\mathbb{F}_7}(\mathbb{P}^1)$ such that $\varphi(A_1) = A_2$. Taking in account the Weil bounds, an elliptic curve with full 2-torsion over $\mathbb{F}_7$ must have 4, 8 or 12 rational points. For $k = 4, 8, 12$, let R_k be the set of elliptic curves with full 2-torsion over $\mathbb{F}_7$ and with k rational points. We check (using Magma) that the action of $\mathrm{Aut}_{\mathbb{F}_7}(\mathbb{P}^1)$ on the set of 4 elements subsets of $\mathbb{P}^1(\mathbb{F}_7)$ has exactly two orbits, which must correspond to R_8 and $R_4 \cup R_{12}$ (the quadratics twists of curves in R_4 lie in R_{12} and conversely). We deduce that the conditions of Proposition 12 are satisfied if and only if E_1 and E_2

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

are both in R_8 or E_1 and E_2 are both in $R_4 \cup R_{12}$. This gives the conditions in the first point of the proposition and concludes the proof. □

COROLLARY 16. *Let E_1 and E_2 be two elliptic curves defined over $\mathbb{F}_q$. Then $E_1 \times E_2$ is isogenous to a Prym variety.*

Proof. If $q > 7$, by Proposition 15, the result is obvious. Otherwise, according to Rück's work [**9**], for $i = 1, 2$, there exists an elliptic curve E_i' which is isogenous to E_i, and such that $E_i'(\mathbb{F}_q)$ has a cyclic group structure. Applying Proposition 15 to E_1' and E_2', we get the result. □

For any power of an odd prime q and any integer $g \geq 1$, we define the quantities

$$\mathrm{Pr}_q(g) = \max_{\pi} \#P_\pi(\mathbb{F}_q) \quad \text{and} \quad \mathrm{pr}_q(g) = \min_{\pi} \#P_\pi(\mathbb{F}_q),$$

where π runs over the set of unramified double covers of genus $(g+1)$ curves defined over $\mathbb{F}_q$.

Notice that Theorem 11 gives us bounds on $\mathrm{Pr}_q(g)$ and $\mathrm{pr}_q(g)$ when $g \geq q$.

The proof of Corollary 13 can be easily adapted to prove that Prym varieties of dimension 1 are elliptic curves. Therefore, the value of $\mathrm{Pr}_q(1)$ and $\mathrm{pr}_q(1)$ can be derived directly from the Deuring–Waterhouse theorem [**5**, **13**]. Recall that we have set $q = p^e$ where p is an odd prime number and $m = [2\sqrt{q}]$. Then we have $\mathrm{Pr}_q(1) = q + 1 + m$ (respectively $\mathrm{pr}_q(1) = q + 1 - m$) if $e = 1$, e is even or $p \not| m$ and $\mathrm{Pr}_q(1) = q + m$ (resp. $\mathrm{pr}_q(1) = q + 2 - m$) otherwise.

The same idea works for abelian surfaces. Indeed, according to the classic results [**10**, **11**, **12**] (some detailed explanations can also be found in [**2**]), an abelian surface over $\mathbb{F}_q$ which has a maximum number of rational points is of type: $[m, m]$ if $e = 1$, or e even or $p \not| m$; $[m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}]$ if $e \neq 1$, e odd, $p|m$ and the fractional part $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$; and $[m-1, m-1]$ otherwise.

In the same way, an abelian surface over $\mathbb{F}_q$, which has a minimum number of rational points is of type: $[-m, -m]$ if $e = 1$, or e even or $p \not| m$; $[-m - \frac{-1+\sqrt{5}}{2}, -m - \frac{-1-\sqrt{5}}{2}]$ if $e \neq 1$, e odd, $p|m$ and $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$; $[-m+1+\sqrt{2}, -m+1-\sqrt{2}]$ if $e \neq 1$, e odd, $p|m$ and $\sqrt{2} - 1 \leq \{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$; and $[-m+1, -m+1]$ otherwise.

Taking into account the results from this section, we get the value of $\mathrm{Pr}_q(2)$ and $\mathrm{pr}_q(2)$:

COROLLARY 17. *Let $q = p^e$ where p is an odd prime number and $m = [2\sqrt{q}]$.*

(1) *$Pr_q(2)$ is equal to:*
- *$(q+1+m)^2$ if $e = 1$, or e even or $p \not| m$;*
- *$(q+1+m-\frac{1+\sqrt{5}}{2})(q+1+m-\frac{1-\sqrt{5}}{2})$ if $e \neq 1$, e odd, $p|m$ and $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$;*
- *$(q+m)^2$ otherwise.*

(2) *$pr_q(2)$ is equal to:*
- *$(q+1-m)^2$ if $e = 1$ or e even, or $p \not| m$;*
- *$\left(q+1-m+\frac{1+\sqrt{5}}{2}\right)\left(q+1-m+\frac{1-\sqrt{5}}{2}\right)$ if $e \neq 1$, e odd, $p|m$ and $\{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}$;*

https://doi.org/10.1017/S0017089515000063 Published online by Cambridge University Press

- $(q+2-m-\sqrt{2})(q+2-m+\sqrt{2})$ *if* $e \neq 1$, *e odd,* $p|m$ *and* $\sqrt{2}-1 \leq \{2\sqrt{q}\} < \frac{\sqrt{5}-1}{2}$;
- $(q+2-m)^2$ *otherwise.*

REMARK 18. We can define $N_k(P) = q^k + 1 + \tau_k(P)$: these are the "virtual numbers of rational point" of P. If $q \leq 9$, then $q+1-2m = -2$ and Proposition 15 asserts that there exist Prym surfaces of type $[-m, -m]$. This gives us examples of Prym varieties with $N_1(P) < 0$. In particular, the bounds announced in [**1**] and proved in [**2**] concerning the number of rational points on abelian varieties with non-negative virtual numbers of rational points do not apply.

ACKNOWLEDGEMENTS. The authors would like to thank Marc Perret for plenty of discussions on Prym varieties and the anonymous referee for his suggestions which enabled us to extend the results of the last section.

REFERENCES

1. Y. Aubry, S. Haloui and G. Lachaud, Sur le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur les corps finis, *C. R. Acad. Sci. Paris*, Ser. I **350** (2012), 907–910.

2. Y. Aubry, S. Haloui and G. Lachaud, On the number of points on abelian and Jacobian varieties over finite fields, *Acta Arithmetica* **160**(3) (2013), 201–241.

3. A. Beauville, Prym varieties: A survey, in *Proc. Symposia in Pure Math.*, **49** (1989).

4. N. Bruin, The arithmetic of Prym varieties in genus 3, *Compos. Math.* **144** (2008), 317–338.

5. M. Deuring, Die typen der multiplikatorenringe elliptischer funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.

6. Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28**(3) (1981), 721–724.

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

8. M. Perret, Number of points of Prym varieties over finite fields, *Glasgow Math. J.* **48** (2006), 275–280.

9. H. G. Rück, A note on elliptic curves over finite fields, *Math. Comp.* **49** (1987), 301–304.

10. H. G. Rück, Abelian surfaces and Jacobian varieties over finite fields, *Compositio Math.* **76** (1990), 351–366.

11. J.-P. Serre, Rational points on curves over finite fields, Lectures at Harvard University, Notes by F. Gouvea, 1985.

12. C. Smyth. Totally positive algebraic integers of small trace. *Ann. Inst. Fourier*, 34(3) (1984), 1–28.

13. W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sc. E.N.S.* **2**(4) (1969), 521–560.