Indian J. Pure Appl. Math., **51**(2): 761-776, June 2020

DOI: 10.1007/s13226-020-0429-1

A PROOF OF THE HASSE-WEIL INEQUALITY FOR GENUS 2 *à la* MANIN

Eduardo Ruíz Duarte[1] and Jaap Top

Bernoulli Institute, University of Groningen, The Netherlands

e-mails: rduarte@ciencias.unam.mx; j.top@rug.nl

(*Received* 15 *October* 2018; *accepted* 17 *April* 2019)

We prove the Hasse-Weil inequality for genus 2 curves given by an equation of the form $y^2 = f(x)$ with f a polynomial of degree 5, using arguments that mimic the elementary proof of the genus 1 case obtained by Yu. I. Manin in 1956.

Key words : Hasse-Weil inequality; hyperelliptic curve; genus two curve.

2010 Mathematics Subject Classification : 11G10, 11G20, 14G10, 14G15.

1. Manin's Proof of the Hasse Inequality for Genus One

Recall the following theorem:

***Theorem* 1.1** — *(Hasse-Weil). Let C be an algebraic curve of genus g over $\mathbb{F}_q$ then*

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

The Hasse-Weil inequality for an elliptic curve $E/\mathbb{F}_q$ (so the case of genus one), was obtained in an elementary way by Manin for char $\mathbb{F}_q \neq 2, 3$ in [8] (see [9] for an English translation). Adjustments of these elementary arguments to the remaining genus one cases are presented in [3] and [12]. Our goal is to extend these ideas to the case of genus 2 curves. To facilitate this, we very briefly summarize in this first section Manin's argument in the genus one situation. Throughout the paper, we restrict to finite fields of odd characteristic.

Let $E/\mathbb{F}_q$ be an elliptic curve given by an equation $y^2 = f(x)$ where f is a polynomial of degree 3. Consider $\phi, [n] \in \mathrm{End}_{\mathbb{F}_q}(E)$ where ϕ is the q-th Frobenius and $[n]$ the multiplication by n. Consider

[1] This author was supported by CONACyT México through the agreement CVU-440153

$\psi_n := \phi + [n] \in \mathrm{End}_{\mathbb{F}_q}(E)$. If ψ_n is non-trivial then it is of the form $(x, y) \mapsto \left(\frac{u_{1,n}(x)}{u_{2,n}(x)}, y\frac{v_1(x)}{v_2(x)}\right)$, with $u_{1,n}, u_{2,n}, v_1, v_2 \in \mathbb{F}_q[x]$ such that $\gcd(u_{1,n}, u_{2,n}) = 1$ (see [14, §2.9]). The Hasse-Weil inequality for E follows from the claim that $d_n := \deg(\psi_n)$ satisfies

$$0 \le d_n = \begin{cases} \deg(u_{1,n}) & (\text{if } \ \psi_n \neq 0) \\ 0 & (\text{if } \ \psi_n = 0) \end{cases} = n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q. \tag{1}$$

Here for $\psi_n \neq 0$ by definition $\deg(\psi_n) = [\mathbb{F}_q(E) : \psi_n^* \mathbb{F}_q(E)]$, and $\deg(u_{1,n})$ is the degree of the polynomial $u_{1,n} \in \mathbb{F}_q[x]$ (and $\deg(0) := 0$).

The leftmost equality in (1) for $\psi_n \neq 0$ follows from the elementary observation $\deg(\psi_n) = [\mathbb{F}_q(x) : \mathbb{F}_q(\frac{u_1,n(x)}{u_2,n(x)})] = \max\{\deg(u_{1,n}(x)), \deg(u_{2,n}(x))\}$ (see [14, §2.9]) or [12, Lemma 6.2]), together with $\deg(u_{1,n}(x)) > \deg(u_{2,n}(x))$. The latter follows from $\psi_n(\infty) = \infty$, implying $v_\infty(\frac{u_{1,n}(x)}{u_{2,n}(x)}) < 0$. The rightmost equality in (1) is shown by induction on n using the *basic identity* $d_{n-1} + d_{n+1} = 2d_n + 2$ (see [2, Lemma 8.5]).

Finally the non-negativity of $d_n = n^2 + (q + 1 - \#E(\mathbb{F}_q))n + q$ yields that the discriminant of this quadratic polynomial in n is non-positive, implying the Hasse inequality.

In order to extend these ideas to genus 2 curves, we introduce an analogous δ_n which also satisfies a *basic identity*, namely $\delta_{n-1} + \delta_{n+1} = 2\delta_n + 4$, in the genus 2 case.

2. An Analogous δ_n for Genus 2

Let $k := \mathbb{F}_q$ be a finite field of odd cardinality q, and let $\mathcal{H}$ be a hyperelliptic curve of genus 2 over k. Throughout, we assume that $\mathcal{H}$ is given by the equation $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$. By $\mathcal{J}$ we denote the Jacobian variety associated to $\mathcal{H}$. The points of $\mathcal{J}$ correspond to divisor classes $[D] \in \mathrm{Pic}^0(\mathcal{H})$.

Fix the point $\infty \in \mathcal{H}$ and consider the Abel-Jacobi map $\iota \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ given by $P \mapsto [P - \infty]$. We have that $\Theta := \mathrm{Im}\ \iota$ is the *theta divisor* of $\mathcal{J}$ and $\Theta \cong \mathcal{H}$. Consider the q-th power Frobenius map $\phi \in \mathrm{End}_k(\mathcal{J})$ and the morphism $\Phi := \phi \circ \iota \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$. Since $\mathrm{Mor}_k(\mathcal{H}, \mathcal{J}) \cong \mathcal{J}(k(\mathcal{H}))$ is an Abelian group, we define $\Psi_n := \Phi + n \cdot \iota \in \mathrm{Mor}_k(\mathcal{H}, \mathcal{J})$ and $\Theta_n := \mathrm{Im}\ \Psi_n \subset \mathcal{J}$.

Similar to $d_n = \deg(\psi_n)$ in (1), we will define the ‘complexity’ (height) of Ψ_n and denote this by δ_n.

Consider the generic point of $\mathcal{J}$ given by $\mathfrak{g} := [(x_1, y_1) + (x_2, y_2) - 2\infty]$ and the function field of $\mathcal{J}$ denoted by $k(\mathcal{J}) \cong k(x_1 + x_2, x_1x_2, \frac{y_1 - y_2}{x_1 - x_2}, \frac{x_2y_1 - x_1y_2}{x_1 - x_2})$. The Riemann-Roch space $\mathcal{L}(\in\times) \subset \|(\mathcal{J})$ has dimension 4; a basis is given by $\{\kappa_1, \kappa_2, \kappa_3, \kappa_4\}$ with $\kappa_1 := 1, \kappa_2 := x_1 + x_2, \kappa_3 :=$

$x_1x_2, \kappa_4 := \frac{F_0(x_1+x_2, x_1x_2)-2y_1y_2}{(x_1-x_2)^2}$ where $F_0(A,B) := 2a_0 + a_1A + 2a_2B + a_3AB + 2a_4B^2 + AB^2$ (see [1, Chapter 2] and [4, Page 5]). This basis is used to define a singular surface $\mathcal{K} \subset \mathbb{P}^3$ birational to the Kummer surface associated to $\mathcal{J}$, as the closure of the image of

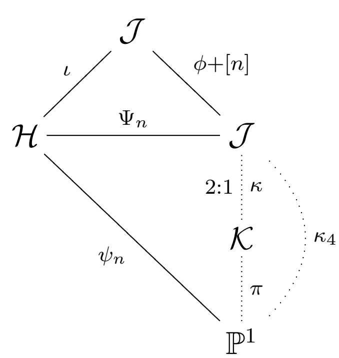
$$\kappa : \mathcal{J} \setminus \Theta \to \mathbb{P}^3,$$
$$D \mapsto [\kappa_1(D) : \kappa_2(D) : \kappa_3(D) : \kappa_4(D)].$$

As a remark, let $[-1] \in \mathrm{Aut}(\mathcal{J})$ be the involution on $\mathcal{J}$ given by $[-1]\mathfrak{g} = [(x_1, -y_1) + (x_2, -y_2) - 2\infty] = -\mathfrak{g}$.

Note that $[-1]^* : k(\mathcal{J}) \to k(\mathcal{J})$ is the trivial map on $\mathcal{L}(\in\times) \subset \|(\mathcal{J})$. Particularly for all $D \in \mathcal{J} \setminus \Theta$ we have that $\kappa_i(D) = \kappa_i(-D)$.

Using the previous remark, suppose that $\Theta_n := \mathrm{Im}\ \Psi_n \not\subset \Theta$ and Θ_n is not a zero of κ_4. Let $(x,y) \in \mathcal{H}$ be generic, then we have that $\psi_n(x,y) := (\kappa_4 \circ \Psi_n)(x,y) = (\kappa_4 \circ \Psi_n)(x,-y)$. Hence $\psi_n(x,y) \in k(x)$, that is, $\psi_n(x,y) =: \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)}$ is a rational function in one variable x, which is the one that we will use to define δ_n.

Our geometric situation is described in the following diagram:



Here π is a projection and $\kappa_4 = \pi \circ \kappa$. Since Θ_n is not a zero or a pole of κ_4, we define $\delta_n := \deg \mu_{1,n}$.

There are two situations left to define δ_n for every $n \in \mathbb{Z}$. The first is when Ψ_n is constant (hence equal to the zero map). In this case $\Theta_n \subset \mathcal{J}$ is a point and we define $\delta_n := 0$. The second is when $\{0\} \neq \Theta_n$ is a curve which is a zero or a pole of κ_4, that is $\Theta_n \in \mathrm{Supp\ div}(\kappa_4)$. In the following section (Formula (11)) we will define δ_n for this special situation. We show that if Ψ_n is non-constant but $\kappa_4(\Psi_n(x,y)) = c$ is constant then c can only be 0 or ∞, that is, the curve $\Theta_n = \mathrm{Im}\Psi_n$ is a zero or a pole of κ_4 respectively (see Lemma 3.12).

Further, if Θ_n is not a zero or a pole of κ_4, we show in the next section that $\frac{\deg \psi_n}{2} = \max \{\deg \mu_{1,n}, \deg \mu_{2,n}\}$.

In the case Θ_n is a zero or a pole of κ_4, a similar equality will be shown taking a translation of Θ_n by a 2-torsion point of $\mathcal{J}$ in order to avoid the pole and zero divisor of $\mathcal{J}$.

Finally, we show the *basic identity* $\delta_{n-1} + \delta_{n+1} = 2\delta_n + 4$. The same strategy also employed by Manin for genus one will then lead to a proof of the Hasse-Weil inequality in this case.

3. PROOF OF THE HASSE-WEIL INEQUALITY FOR GENUS 2

We use the notations $\mathcal{H}/\mathbb{F}_q, \Theta, \Theta_n$ etc. introduced in the previous section.

Lemma 3.1 — Let $(x, y) \in \mathcal{H}/\mathbb{F}_q$ be generic. Suppose that $\Theta_n \subset \mathcal{J}$ is a curve that is not a zero nor a pole of κ_4. Then $\psi_n(x, y) = \frac{\mu_{1,n}(x)}{\mu_{2,n}(x)}$ for some coprime polynomials $\mu_{1,n}, \mu_{2,n}$. Moreover $\frac{\deg \psi_n}{2} = \max\{\deg \mu_{1,n}(x), \deg \mu_{2,n}(x)\}$.

PROOF : Since Θ_n is not a zero or a pole of κ_4 and $\kappa_4 \in \mathcal{L}(\in\times)$, the function $\psi_n(x, y) = \kappa_4(\Psi_n(x, y))$ is defined and non-zero. In the previous section we saw that $\psi_n(x, y) = \psi_n(x, -y)$, and hence $\psi_n(x, y) \in \mathbb{F}_q(x)$. This shows the existence of the coprime $\mu_{1,n}, \mu_{2,n} \in \mathbb{F}_q[x]$.

Now,

$$\deg(\psi_n) = [\mathbb{F}_q(x, y) : \mathbb{F}_q(\tfrac{\mu_{1,n}(x)}{\mu_{2,n}(x)})] = [\mathbb{F}_q(x, y) : \mathbb{F}_q(x)] \cdot [\mathbb{F}_q(x) : \mathbb{F}_q(\tfrac{\mu_{1,n}(x)}{\mu_{2,n}(x)})]$$

and the lemma follows. □

It can happen that Ψ_n is the zero map, which implies $\Theta_n = \mathrm{Im}\Psi_n$ is a point. For example consider the hyperelliptic curve $Y^2 = X^5 + 5X$ over $\mathbb{F}_{49}$. An explicit MAGMA computation shows that $\psi_7 := \Phi + 7\iota \in \mathrm{Mor}_{\mathbb{F}_{49}}(\mathcal{H}, \mathcal{J}) \cong \mathcal{J}(\mathbb{F}_{49}(\mathcal{H}))$ is the zero map:

```
> p := 7; q := p^2; F := FiniteField(q);
> P<x> := PolynomialRing(F);
> H := HyperellipticCurve(x^5+5*x);
> FH<X,Y> := FunctionField(H); HE := BaseExtend(H,FH);
> JE := Jacobian(HE); M<t> := PolynomialRing(FH);
> Phi := JE![t-X^q, Y^q];
> GPt := JE![t-X,   Y];
> -7*GPt;
(x + 6*X^49, (X^120 + X^116 + 5*X^112 + 6*X^108 + X^92 + X^88 + 5*X^84 + 6*X^80 + 5*X^64 +
5*X^60 + 4*X^56 + 2*X^52 + 6*X^36 + 6*X^32 + 2*X^28 + X^24)*Y, 1)
> Phi;
(x + 6*X^49, (X^120 + X^116 + 5*X^112 + 6*X^108 + X^92 + X^88 + 5*X^84 + 6*X^80 + 5*X^64 +
5*X^60 + 4*X^56 + 2*X^52 + 6*X^36 + 6*X^32 + 2*X^28 + X^24)*Y, 1)
> Phi+7*GPt;
(1, 0, 0)
```

In this example $\mathcal{J}$ is isogenous to the square of a supersingular elliptic curve and the ground field has $p^2 = 49$ elements. The characteristic polynomial of Frobenius $\phi \in \mathrm{End}_{\mathbb{F}_{49}}(\mathcal{J})$ is given by $\chi_\phi(X) := (X+7)^4$ which is the main reason of this behavior.

A general construction of curves having Jacobian isogenous to a square of a supersingular elliptic curve was achieved by Moret-Bailly in [11].

The following proposition and lemma isolates a special case for our final proof of the Hasse-Weil inequality for genus 2. Note that the example discussed above illustrates this special case.

Proposition 3.2 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2, given by an equation $y^2 = f(x)$ with f of degree 5. Let $\mathcal{J}$ be the Jacobian of $\mathcal{H}$ and $\iota\colon \mathcal{H} \to \mathcal{J}$ the map $P \mapsto [P - \infty]$. Suppose that there is an $n \in \mathbb{Z}$ such that $\Psi_n = (\phi + [n]) \circ \iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is constant. Then q is a perfect square and $\#\mathcal{H}(\mathbb{F}_q) = q + 1 + 4n = q + 1 \pm 4\sqrt{q}$.

PROOF : First, we show that if $\Psi_n = (\phi + [n]) \circ \iota$ is constant, then $\phi = -[n]$.
We have that $\Psi_n = (\phi + [n]) \circ \iota$ is constant and $0 \in \mathrm{Im}\Psi_n$, hence $\Psi_n = 0$; this is equivalent to $(\phi + [n])(\Theta) = 0$ since $\Theta = \iota(\mathcal{H})$. Moreover, Θ generates $\mathcal{J}$, that is $\mathcal{J} = \{D_1 + D_2 : D_1, D_2 \in \Theta\}$. So if any $\varphi \in \mathrm{End}(\mathcal{J})$ is zero on Θ then it is the zero map. Hence $\phi = -[n] \in \mathrm{End}(\mathcal{J})$.

Note that $\phi = -[n]$ implies $q^2 = \deg(\phi) = \deg([-n]) = n^4$. Hence $q = n^2$ is a perfect square and $n = \pm\sqrt{q}$.

Now we proceed to count $\#\mathcal{H}(\mathbb{F}_q)$. Using that $\phi = -[n]$ we have that:

$$\#\mathcal{J}(\mathbb{F}_q) = \#\mathrm{Ker}(\phi - [1]) = \#\mathrm{Ker}(-[n+1]) = (n+1)^4. \tag{2}$$

(Here we used that $n+1$ is not a multiple of $\mathrm{char}(\mathbb{F}_q)$). Moreover, an easy counting argument (see [1, Chapter 8, §2]) shows:

$$\#\mathcal{J}(\mathbb{F}_q) = \frac{(\#\mathcal{H}(\mathbb{F}_q))^2 + \#\mathcal{H}(\mathbb{F}_{q^2})}{2} - q. \tag{3}$$

Consider the quadratic twist of $\mathcal{H}$ denoted by $\mathcal{H}^{\mathrm{TW}}$ and its Jacobian $\mathcal{J}^{tw}$, then:

$$\#\mathcal{J}^{tw}(\mathbb{F}_q) = \#\mathrm{Ker}(\phi + [1]) = \#\mathrm{Ker}(-[n] + 1) = (n-1)^4. \tag{4}$$

Similarly as in (4) and using that $\#\mathcal{H}(\mathbb{F}_q) + \#\mathcal{H}^{tw}(\mathbb{F}_q) = 2q + 2 = 2n^2 + 2$ and $\mathcal{H}^{tw}(\mathbb{F}_{q^2}) \cong$

$\mathcal{H}(\mathbb{F}_{q^2})$, we have that:

$$\begin{aligned}\#\mathcal{J}(\mathbb{F}_q) &= \frac{\#\mathcal{H}(\mathbb{F}_q)^2 + \#\mathcal{H}(\mathbb{F}_{q^2})}{2} - q \\ &= \frac{(2n^2+2-\#\mathcal{H}(\mathbb{F}_q))^2 + \#\mathcal{H}(\mathbb{F}_{q^2})}{2} - q = (n-1)^4\end{aligned} \tag{5}$$

Subtracting (6) from (4) yields:

$$\begin{aligned}\#\mathcal{H}(\mathbb{F}_q)^2 - (2n^2+2-\#\mathcal{H}(\mathbb{F}_q))^2 &= 2\big((n+1)^4 - (n-1)^4\big) \\ &= 16n(n^2+1),\end{aligned} \tag{6}$$

which can be rewritten as $\#\mathcal{H}(\mathbb{F}_q) = n^2+4n+1 = q+1\pm 4\sqrt{q}$. □

Corollary 3.3 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by an equation $Y^2 = f(X)$ with f of degree 5. Let $\mathcal{J}$ be its Jacobian and suppose that $\Psi_n = (\phi + [n]) \circ \iota$ is constant. Then Im $\Psi_{n-1} =$ Im $\Psi_{n+1} = \Theta \in$ Div$(\mathcal{J})$.

PROOF : By the Proposition (3.2) $\phi = -[n]$, hence $\Psi_{n\pm1} = \pm[1]\circ\iota = \pm\iota \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H},\mathcal{J})$. Further, Im $\iota =$ Im $-\iota = \Theta$ since $\Theta \cong \mathcal{H}$ (here we used that Θ is symmetric with respect of the hyperelliptic involution under ι). □

Lemma 3.4 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by $Y^2 = f(X)$ with $\deg f(X) = 5$ and let $\mathcal{J}$ be the Jacobian of $\mathcal{H}$. Let $(x,y) \in \mathcal{H}$ be generic, then $-\Psi_n(x,y) = \Psi_n(x,-y)$.

PROOF : Using $[(a,b)-\infty] = [\infty - (a,-b)]$ for any $(a,b) \in \mathcal{H}$ one finds

$$\begin{aligned}-\Psi_n(x,y) &= -\phi([(x,y)-\infty]) - n[(x,y)-\infty] \\ &= [\infty - (x^q,y^q)] + n[\infty-(x,y)] \\ &= [(x^q,-y^q)-\infty] + n[(x,-y)-\infty] = \Psi_n(x,-y).\square\end{aligned}$$

Now we calculate some values of δ_n.

Proposition 3.5 — Let $\mathcal{H}/\mathbb{F}_q :\ Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 =: f(X)$ be a genus 2 curve (q odd). Then $\delta_{-1} = \#\mathcal{H}(\mathbb{F}_q) + q + 1$.

PROOF : For $(x,y) \in \mathcal{H}$ generic, $\Psi_{-1}(x,y) = [(x^q, yf(x)^{\frac{q-1}{2}}) + (x,-y) - 2\infty]$. Lemma **??** shows that δ_{-1} equals the degree of $\psi_{-1}(x,y) = \kappa_4(\Psi_{-1}(x,y)) \in \mathbb{F}_q(x)$. This degree is the maximum of the polynomial degrees of the numerator and the denominator, assuming these are coprime. Here

$$\psi_{-1}(x,y) = \frac{x^{3q+2}+x^{2q+3}+2a_4x^{2q+2}+a_3(x^{2q+1}+x^{q+2})+2a_2x^{q+1}+a_1(x^q+x)+2a_0+2f(x)^{\frac{q+1}{2}}}{(x^q-x)^2}. \tag{7}$$

Let $\nu(x)$ and $\eta(x)$ be respectively the numerator and denominator of (8) before cancellation of common factors. Note that $\deg(\eta) = 2q$ and that every $\alpha \in \mathbb{F}_q$ is a double root of $\eta(x)$. Furthermore, $\deg(\nu(x)) = 3q + 2 > 2q$, hence $\delta_{-1} = 3q + 2 - \deg(\gcd(\nu(x), \eta(x)))$.

Since $\psi_{-1}(x, y) \in \mathbb{F}_q(\mathcal{H})$, the common factors $(x - \alpha)$ of ν and η occur at the points $(\alpha, \beta) \in \mathcal{H}$ such that $\alpha \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$ or $\beta \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ or $\beta = 0$. Hence, we have three possibilities for cancellations:

Case : $\beta \in \mathbb{F}_q^*$.

In this case $(\alpha, \beta) \in \mathcal{H}(\mathbb{F}_q)$ and therefore $f(\alpha)$ is a square in $\mathbb{F}_q^*$. Hence $f(\alpha)^{\frac{q-1}{2}} = 1$. Moreover, $\alpha^q = \alpha$. Using this, the last term of $\nu(\alpha)$ is $2f(\alpha)^{\frac{q+1}{2}} = 2f(\alpha)f(\alpha)^{\frac{q-1}{2}} = 2f(\alpha)$ and

$$\nu(\alpha) = 4f(\alpha).$$

Since $\beta \neq 0$ there is no cancellation of a factor $(x - \alpha)$ in this case.

Case : $\beta = 0$.

We have that $f(\alpha) = 0$ and $\alpha^q = \alpha$, so the numerator of (8) is $2f(\alpha) = 0$. Therefore $\nu(x)$ and $\eta(x)$ share the linear factor $x - \alpha$ with multiplicity one or two. The multiplicity in fact equals one since $\frac{d}{dx}\nu(x) \mid_\alpha = 4f'(\alpha) \neq 0$ as $f(x)$ does not have repeated zeros.

Case $\beta \notin \mathbb{F}_q$.

In this case $f(\alpha)$ is nonzero and is not a square in $\mathbb{F}_q^*$. Therefore $f(\alpha)^{\frac{q-1}{2}} = -1$ by Euler's criterion. Moreover $\alpha^q = \alpha$ and $\nu(\alpha)$ is in this case

$$2(\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) - 2f(\alpha) = 0.$$

To find the multiplicity of α as a zero of $\nu(x)$, note that

$$\begin{aligned}
\frac{d}{dx}\nu(x) \mid_\alpha &= 2\alpha^{3q+1} + 3\alpha^{2q+2} + 4a_4\alpha^{2q+1} + a_3(\alpha^{2q} + 2\alpha^{q+1}) + 2a_2\alpha^q + a_1 - f'(\alpha) \\
&= 5\alpha^4 + 4a_4\alpha^3 + 3a_3\alpha^2 + 2a_2\alpha + a_1 - f'(\alpha) \\
&= f'(\alpha) - f'(\alpha). \\
&= 0.
\end{aligned}$$

This tells us that the factor $(x - \alpha)^2$ appears in ν and then it cancels with the denominator.

Combining the cases, one concludes $\deg(\gcd(\nu(x), \eta(x))) = 2q + 1 - \#\mathcal{H}(\mathbb{F}_q)$ and therefore $\deg(\kappa_4(\Psi_{-1}(x, y))) = q + 1 + \#\mathcal{H}(\mathbb{F}_q)$. □

Proposition 3.6 — With notations as in Proposition 3.5 one has

$$\delta_1 = 3(q+1) - \#\mathcal{H}(\mathbb{F}_q).$$

PROOF : Note that

$$\kappa_4(\Psi_1(x,y)) = \frac{x^{3q+2}+x^{2q+3}+2a_4x^{2q+2}+a_3(x^{2q+1}+x^{q+2})+2a_2x^{q+1}+a_1(x^q+x)+2a_0-2f(x)^{\frac{q+1}{2}}}{(x^q-x)^2}.$$

This expression differs from (8) only at the sign of the last term of the numerator, namely $2f(x)^{\frac{q+1}{2}}$. An analogous argument as the one given in Proposition 3.5 proves the proposition. □

We will use the following definition in order to interpret δ_n in the case where Θ_n is a curve that is a zero or a pole of κ_4. The case $\Theta_n = \Theta$ (which is a pole of κ_4) occurs, e.g., for $n = 0$.

Let $D_1, D_2 \in$ Div$(\mathcal{J})$. By $D_1 \bullet D_2$ we denote the intersection number of the divisors D_1 and D_2 on the surface $\mathcal{J}$.

For details and properties of this see, e.g., [6, Appendix C or Chapter V].

Lemma 3.8 — Suppose that Im$\Psi_n = \Theta_n \not\subset \Theta$ and that $\psi_n = \kappa_4 \circ \Phi_n \circ \iota \colon \mathcal{H} \to \mathbb{P}^1$ is nonconstant, where $\Phi_n := \phi + [n] \in$ End$(\mathcal{J})$. Then

$$2\Theta \bullet \Theta_n = \deg \psi_n = 2\Phi_n^*\Theta \bullet \Theta.$$

PROOF : Let $(x,y) \in \mathcal{H}$ be generic. Since Im$\Psi_n = \Theta_n \not\subset \Theta$ and since $\kappa_4 \in \mathbb{F}_q(\mathcal{J})$ has divisor $D - 2\Theta$ for some effective divisor $D \in$ Div$(\mathcal{J})$, we have that $\psi_n(x,y) = \kappa_4(\Psi_n(x,y)) \in \mathbb{F}_q(x)$ by Lemma 3.1. Moreover by assumption this rational function is nonconstant. Therefore $\deg \psi_n = \deg\left((\kappa_{4|\Theta_n})^*\infty\right) = 2\Theta \bullet \Theta_n$ which shows the first equality.

For the second, note that $\Phi_n^{-1}(\Theta) = \{D \in \mathcal{J} : \Phi_n(D) \in \Theta\}$ and Θ is the locus where κ_4 has a pole (in fact a double pole). Since $\deg(\psi_n) = \deg(\kappa_4 \circ \Phi_{n|\Theta})$ we conclude $\deg \psi_n = 2\Phi_n^{-1}(\Theta) \bullet \Theta$. Applying [5, Lemma 1.7.1] this equals $2\Phi_n^*\Theta \bullet \Theta$. □

We will deal with the cases where $\Theta_n = \Theta$ by using a linear equivalent divisor $\Theta_n' \in$ Div$(\mathcal{J})$ and Lemma 3.8.

First we show that $\Theta \bullet \Theta = 2$ using the pole divisor of κ_4. To achieve this we use (see [6, Chapter V. Theorem 1.1]) that if $\Theta \sim \Theta'$ as divisors ($\sim$ denoting linear equivalence), then $\Theta \bullet \Theta = \Theta \bullet \Theta'$. A suitable divisor Θ' will be constructed as a symmetric translation of $\Theta \subset \mathcal{J}$ (with respect of $[-1] \in$ Aut$(\mathcal{J})$).

Remark 3.9 : The following lemmas use that for divisors D, D' on $\mathcal{J}$ and any point $\xi \in \mathcal{J}$, denoting by t_ξ the translation over ξ, we have $D \bullet D' = D \bullet t_\xi^* D'$. Indeed, the fact that D' and $t_\xi^* D'$ are algebraically equivalent is a special case of [7, I §2 Proposition 2], and the fact that algebraically equivalent cycles are numerically equivalent can be found in [5, 19.3.1].

Lemma 3.10 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 =: f(X)$ and consider its Jacobian $\mathcal{J}$. Then $\Theta = \iota(\mathcal{H}) \subset \mathcal{J}$ satisfies $\Theta \bullet \Theta = 2$.

PROOF : Let $(w, 0) \in \mathcal{H}(\overline{\mathbb{F}}_q)$ be a Weierstrass point and consider $\iota_w \in \mathrm{Mor}(\mathcal{H}, \mathcal{J})$ given by $P \mapsto [P + (w, 0) - 2\infty]$. Let $(x, y) \in \mathcal{H}$ be the generic point. We have that $\Theta' := \mathrm{Im}\ \iota_w \subset \mathcal{J}$ is a translation of Θ, and therefore $\Theta' \sim \Theta$ in $\mathrm{Div}(\mathcal{J})$. Since $\kappa_4 \circ [-1] = \kappa_4$ and $[(x, -y) + (w, 0) - 2\infty] = 2\infty - (x, y) - (w, 0)]$ it follows that $\kappa_4(\iota_w(x, y)) \in \mathbb{F}_q(x)$. Analogous to the proof of Lemma 3.8 one obtains $\Theta \bullet \Theta = \Theta' \bullet \Theta = \deg \kappa_4(\iota_w(x, y))$ where deg denotes the degree of the given element of $\mathbb{F}_q(x)$ (which is half the degree of the map $\kappa_4 \circ \iota_w : \mathcal{H} \to \mathbb{P}^1$). Note that

$$\kappa_4(\iota_w(x, y)) = \tfrac{2a_0 + a_1(x+w) + 2a_2xw + a_3(x+w)xw + 2a_4(xw)^2 + (x+w)(xw)^2}{(x-w)^2} \tag{8}$$

One observes that both the numerator and denominator here are divisible by $(x - w)$ and the derivative w.r.t. x of the numerator, evaluated at $x = w$, equals $f'(w) \neq 0$. Hence $\deg \kappa_4(\iota_w(x, y)) = 2$ which proves the lemma.

Lemma 3.10 also follows using the *adjunction formula* ([6, Chapter V, 1.5]).

Let $\Phi_n := \phi + [n] \in \mathrm{End}(\mathcal{J})$. Using an analogous argument, we calculate $(\Phi_0)_*\Theta \bullet \Theta = \Theta \bullet \Phi_0^*\Theta$; the equality of these intersection numbers is a consequence of the 'projection formula' [5, Proposition 2.3(c)]. In fact, in the present case equality is also established by computing both numbers directly.

Lemma 3.11 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 =: f(X)$ and consider its Jacobian $\mathcal{J}$. With notations as before, we have $(\Phi_0)_*\Theta \bullet \Theta = 2q = \Theta \bullet \Phi_0^*\Theta$.

PROOF : As $\Phi_0 : \mathcal{J} \to \mathcal{J}$ is the qth power Frobenius morphism, its restriction to Θ maps Θ to itself and has degree q. As a consequence $(\Phi_0)_*\Theta = q\Theta$ and therefore Lemma 3.10 implies the first equality. For the second equality, let $(x, y) \in \mathcal{H}$ be generic. By a similar argument the one presented in Lemma 3.10 we translate $\Psi_0 \in \mathrm{Mor}(\mathcal{H}, \mathcal{J})$ by $\iota(w, 0) \in \mathcal{J}(\overline{\mathbb{F}}_q)$, namely $\Psi_{0,w}(x, y) = [(x^q, yf(x)^{\frac{q-1}{2}}) + [(w, 0) - 2\infty]$. Then, since $\mathrm{Im}\Psi_0 = \Phi_0(\Theta)$ we define $\Phi_{0,w} := \Phi_0 + \iota(w, 0)$ and we have that $\Theta \bullet \Phi_0^*\Theta = \Theta \bullet \Phi_{0,w}^*\Theta$. The latter intersection number equals the degree of

$$\kappa_4(\Psi_{0,w}(x,y)) = \frac{2a_0+a_1(x^q+w)+2a_2x^qw+a_3(x^q+w)x^qw+2a_4(x^qw)^2+(x^q+w)(x^qw)^2}{(x^q-w)^2} \tag{9}$$

(considered as a morphism $\mathbb{P}^1 \to \mathbb{P}^1$). Take $v \in \overline{\mathbb{F}}_q$ with $v^q = w$, then the denominator in the right-hand-side of (10) equals $(x-v)^{2q}$. The numerator equals $(2a_0 + a_1(x+v) + 2a_2xv + a_3(x+v)xv + 2a_4(xv)^2 + (x+v)xv)^q$. Evaluating the numerator at $x = v$ yields $(2f(v))^q = 0$, hence the numerator is divisible by $(x-v)^q$. Since the derivative of $2a_0 + a_1(x+v) + 2a_2xv + a_3(x+v)xv + 2a_4(xv)^2 + (x+v)xv$ evaluated at $x = v$ equals $f'(v) \neq 0$ it follows that the rational function (10) has degree $2q$. □

Lemma 3.12 — Suppose that $\Theta_n \subset \mathcal{J}$ is a curve. If $\kappa_4(\Psi_n(x,y)) = c$ is constant then $c \in \{0, \infty\}$.

PROOF : Let $\Theta_n = \mathrm{Im}\Psi_n \in$ Supp div(κ_4) then $\kappa_4(\Psi_n(x,y)) \in \{0,\infty\}$ depending on Θ_n being a zero or a pole of κ_4.

Suppose that $\kappa_4(\Psi_n(x,y)) = c \in \mathbb{F}_q^*$. Since $\kappa_4 \in \mathcal{L}(\in\times)$ and $\deg \kappa_4(\Psi_n(x,y)) = \Theta_n \bullet \Theta = 0$ (note that here we use $c \neq 0, \infty$), this contradicts the fact that the curves Θ_n and Θ intersect in $0 \in \mathcal{J}$. With this we have that $c \in \{0, \infty\}$.

Lemma 3.12 (rather, its proof) provides a geometric reason for the fact that $\kappa_4 \in \mathcal{L}(\in\times)$ cannot be constant $\neq 0, \infty$ when restricted to the curves Θ_n: these curves will always intersect Θ and therefore they will have a positive intersection number (degree of $\kappa_4(\Psi_n(x,y))$. However, if the curve Θ_n equals Θ or is contained in the zero-locus of κ_4, then of course $\kappa_4|_{\Theta_n}$ is the constant map ∞ or 0, respectively.

Note that when Θ_n has dimension zero, then $\Theta_n = \{0\} \subset \mathcal{J}$ (compare the proof of Proposition 3.2). This case is treated separately in the definition of δ_n given below.

Using Lemma 3.12, it follows that the only cases where δ_n is not defined yet, is the situation where Θ_n is a pole or a zero of κ_4. The following property of κ_4 will be useful.

Lemma 3.13 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve given by an equation $Y^2 = f(X)$ where f has degree 5 and consider its Jacobian $\mathcal{J}$. Then the function κ_4 on $\mathcal{J}$ has a divisor of zeros $D_0 =$ div$_0(\kappa_4)$ such that its support consists of at most four irreducible curves.

PROOF : Let div$(\kappa_4) = D_0 - 2\Theta$ with D_0 effective. We have that $D_0 = \sum C_i$ where the $C_i \subset \mathcal{J}$ are irreducible curves. Then

$$4 = 2\Theta \bullet \Theta = \left(\sum C_i\right) \bullet \Theta = \sum (C_i \bullet \Theta).$$

As Θ is ample, $C_i \bullet \Theta > 0$ (see [6, Chapter V, Theorem 1.10]) which implies that the support of the zero divisor of κ_4 consists of four or less irreducible curves in $\mathcal{J}$.

Lemma 3,.14 — Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve of genus 2 given by $Y^2 = X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = f(X)$ and let $\mathcal{J}$ be its Jacobian. Assume Im $\Psi_n = \Theta_n \subset \mathcal{J}$ is a curve that is a zero or a pole of κ_4. Let $(w, 0) \in \mathcal{H}(\overline{\mathbb{F}}_q)$ be some Weierstrass point. Define $\Phi_{n,w} := \Phi_n + \iota(w, 0)$ where $\Phi_n = \phi + [n] \in$ End$(\mathcal{J})$ and consider $\Psi_{n,w} := \Psi_n + \iota(w, 0) \in$ Mor$_{\overline{\mathbb{F}}_q}(\mathcal{H}, \mathcal{J})$. Take the generic point $(x, y) \in \mathcal{H}$, then $\kappa_4(\Psi_{n,w}(x, y)) =: \frac{\mu^w_{1,n}(x)}{\mu^w_{2,n}(x)} \in \overline{\mathbb{F}}_q(x)^*$ for coprime $\mu^w_{1,n}, \mu^w_{2,n} \in \overline{\mathbb{F}}_q[x]$ and $\Phi_{n,w}{}^*\Theta \bullet \Theta = \max\{\deg \mu^w_{1,n}, \deg \mu^w_{2,n}\}$.

PROOF : Suppose that $\Psi_n(\mathcal{H}) = \Theta_n = \Theta$ (is a pole of κ_4), it follows that $\Theta^w_n :=$ Im$\Psi_{n,w} \not\subset \Theta$. We want Θ^w_n to avoid the support of κ_4. We do this in order to have a well defined degree of κ_4 restricted to the symmetric divisor Θ^w_n (see Remark 3.9).

If the curve $\Theta^w_n \subset \mathcal{J}$ would be a zero of κ_4, then by Lemma 3.13 there are at most four possible curves $\{C_1, C_2, C_3, C_4\}$ in the zero locus κ_4. Further, there are exactly five affine Weierstrass points in $\mathcal{H}$, and then for at least one of them say $(\hat{w}, 0) \in \mathcal{H}$ we have that $\Theta^{\hat{w}}_n \notin \{C_1, C_2, C_3, C_4\}$.

As a result, $\kappa_4(\Psi_{n,\hat{w}}(x, y))$ is well defined and non-constant since $\Theta^{\hat{w}}_n \notin$ Supp div(κ_4) (see Lemma 3.12). Further, Im$\Psi_{n,\hat{w}}$ is symmetric with respect to $[-1] \in$ Aut$(\mathcal{J})$ since $\Psi_n(x, y) + \iota(\hat{w}, 0)$ is. Hence $\kappa_4(\Psi_{n,\hat{w}}(x, y)) = \kappa_4(\Psi_{n,\hat{w}}(x, -y)) \in \overline{\mathbb{F}}_q(x)^*$.

By Remark 3.9 and Lemma 3.8, as in the previous lemmas,

$$\Phi^*_{n,w}\Theta \bullet \Theta = \deg \kappa_4(\Psi_{n,w}(x, y)) = \max\{\deg \mu^w_{1,n}, \deg \mu^w_{2,n}\},$$

which proves the lemma for Θ_n a pole of κ_4. Similarly if Θ_n is a zero of κ_4 one can translate Θ_n by some Weierstrass point of $\mathcal{H}$ in order to avoid the zero or the pole divisor of κ_4. Therefore the degree of $\kappa_4(\Psi^w_n(x, y))$ is well defined. □

Using the previous Lemmas, we know that there is always a $(w, 0) \in \mathcal{H}$ such that the value $\Theta_n \bullet \Theta$ can be obtained using the degree of the rational function κ_4 restricted to the generic point of Θ^w_n. Further, we know that if Ψ_n is non-constant but $\kappa_4(\Psi_n(x, y))$ is constant then it must be 0 or ∞ and $\Theta_n =$ Im$\Psi_n \in$ Supp div(κ_4) by Lemma 3.12. Hence we have a definition of δ_n for all $n \in \mathbb{Z}$:

$$\delta_n := \begin{cases} 0 & \text{if } \Psi_n : \mathcal{H} \to \mathcal{J} \text{ is constant;} \\ \max\{\deg(\mu^w_{1,n}), \deg(\mu^w_{2,n})\} & \text{if } \Theta_n \in \text{Supp div}(\kappa_4); \\ \max\{\deg(\mu_{1,n}), \deg(\mu_{2,n})\} & \text{otherwise.} \end{cases} \tag{10}$$

Before proving our *basic identity* for genus 2, namely $\delta_{n-1} + \delta_{n+1} = 2\delta_n + 4$ to obtain the Hasse-Weil inequality in this case *à la* Manin, we recall an additional result.

***Theorem* 3.15** — *(Theorem of the cube for Abelian varieties). Let $\mathcal{A}$ be an Abelian variety, $\alpha, \beta, \gamma \in \mathrm{End}_k(\mathcal{A})$ and $D \in$ Div$(\mathcal{A})$, then*

$$(\alpha+\beta+\gamma)^*D-(\alpha+\beta)^*D-(\alpha+\gamma)^*D-(\beta+\gamma)^*D+\alpha^*D+\beta^*D+\gamma^*D \sim 0$$

where $\sim$ denotes linear equivalence.

PROOF : See [10, Corollary 5.3]. □

Corollary 3.16 — Let $\Theta \in \mathrm{Div}(\mathcal{J})$ and consider the multiplication-by-n map $[n] \in \mathrm{End}(\mathcal{J})$. Then $[n]^*\Theta \sim n^2\Theta \in \mathrm{Div}(\mathcal{J})$.

PROOF : This is an application of Theorem 3.15 with $\alpha = [1], \beta = [-1]$ and $\gamma = [n]$ together with induction w.r.t. n. For details, see [10, Corollary 5.4] and use that in the present case $[-1]^*\Theta = \Theta$.

The next proposition (see also [10, Cor. 6.6]) will be used in the final induction process for our *basic identity*.

Corollary 3.17 — Let $\mathcal{A}$ be an Abelian variety and $[n] \in \mathrm{End}_k(\mathcal{A})$. If $\mathcal{L} \in \mathrm{Div}(\mathcal{A})$ then

$$[n]^*\mathcal{L} \sim \frac{\backslash\in+\backslash}{\in}\mathcal{L} + [-\infty]^*\frac{\backslash\in-\backslash}{\in}\mathcal{L}$$

PROOF : See [2].

In particular, let $\mathcal{A} = \mathcal{J}$ and $\mathcal{L} = \times$. Take $\mathfrak{t} \in \mathrm{Aut}_{\mathfrak{k}}(\mathcal{H})$ the hyperelliptic involution. We have that $\mathfrak{t}(\mathcal{H}) = \mathcal{H} \cong \mathfrak{f} = \iota(\mathfrak{t}(\mathcal{H}))$, hence Θ is symmetric, i.e., $[-1]^*\Theta = \Theta$. Applying Corollary 3.16 yields $[n]^*\Theta \sim n^2\Theta \in \mathrm{Div}(\mathcal{J})$.

***Theorem* 3.17** — *Let $\mathcal{H}$ be a hyperelliptic curve of genus 2 over $\mathbb{F}_q$ with one rational point at infinity, then:*

$$\delta_{n-1} + \delta_{n+1} = 2\delta_n + 4. \tag{11}$$

Moreover, $\delta_n = 2n^2 + n(q+1-\#\mathcal{H}(\mathbb{F}_q)) + 2q$.

PROOF : As before, we denote $\Phi_m := \phi + [m] \in \mathrm{End}(\mathcal{J})$ where ϕ is the q-th Frobenius map. We begin with some cases when either Ψ_n or $\Psi_{n\pm1}$ is constant.

Suppose that Ψ_n is constant, then by definition (11) we have that $\delta_n = 0$. By Corollary 3.3 we have that $\Theta_{n\pm1} = \Theta$ and $\Psi_{n\pm1} = \pm[1] \circ \iota$. It follows by Lemma 3.10 and the symmetry of Θ with respect to $[-1]$ that $\delta_{n\pm1} = [\pm1]^*\Theta \bullet \Theta = \Theta \bullet \Theta = 2$ and the lemma follows.

Now suppose that Ψ_{n-1} is constant. Then $\delta_{n-1} = 0$ and by Corollary 3.3 we have that $\Theta_n = \Theta$ and $\Psi_n = \iota$. An analogous argument as in the previous case shows that $\delta_n = 2$.

To prove that $\delta_{n+1} = 8$, note that by Proposition 3.2 we have that $\phi = -[n-1] \in \mathrm{End}(\mathcal{J})$. Therefore $\Phi_{n+1} := \phi + [n+1] = [2]$ which means that $\Psi_{n+1} = \Phi_{n+1} \circ \iota = [2] \circ \iota$. Hence by Corollary 3.16 and Lemma 3.8 we obtain $\delta_{n+1} = \Phi_{n+1}^* \Theta \bullet \Theta = [2]^* \Theta \bullet \Theta = 4\Theta \bullet \Theta = 8$.

The case that Ψ_{n+1} is constant is similar to the previous case: one uses the symmetry of Θ with respect to $[-1] \in \mathrm{End}(\mathcal{J})$ to obtain $\delta_{n-1} = [-2]^* \Theta \bullet \Theta = [2]^* \Theta \bullet \Theta = 8$.

Now we assume that $\Psi_{n\pm1}$ and Ψ_n are non-constant. In the case that $\Theta_n \in \mathrm{Supp\ div}(\kappa_4)$, by Lemma 3.14there is a $(w, 0) \in \mathcal{H}$ such that $\delta_n = \Phi_{n,w}^* \Theta \bullet \Theta = \deg \kappa_4(\Psi_n^w(x, y))$. Using Remark 3.9 and Lemma 3.8, the latter integer equals $\Phi_n^* \Theta \bullet \Theta$. Note that also in the case that $\Theta_n \notin \mathrm{Supp\ div}(\kappa_4)$ we have $\delta_n = \Phi_n^* \Theta \bullet \Theta$ (see Lemma 3.8). We will finish the proof by studying these intersection numbers.

Using Theorem 3.15, let $D := \Theta \in \mathrm{Div}(\mathcal{J})$ and take $\alpha := \phi + [n], \beta = [1], \gamma := -[1] \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{J})$. The Theorem of the cube (3.15) implies:

$$2\Phi_n^* \Theta - \Phi_{n+1}^* \Theta - \Phi_{n-1}^* \Theta + 2\Theta \sim 0,$$

or equivalently:

$$2\Phi_n^* \Theta + 2\Theta \sim \Phi_{n-1}^* \Theta + \Phi_{n+1}^* \Theta. \tag{12}$$

Intersecting both sides of the equivalence with Θ proves the first part of the theorem. To be more precise, we use Lemma 3.8 together with Lemma 3.10 to deduce $2\delta_n + 4 = \delta_{n-1} + \delta_{n+1}$.

The explicit formula for δ_n now follows by induction, noting (Proposition 3.11) that $\delta_1 = 3(q + 1) - \#\mathcal{H}(\mathbb{F}_q)$ and (Lemma 3.11) that $\delta_0 = 2q$. □

Corollary 3.18 — (Hasse-Weil for $g = 2$). Let $\mathcal{H}/\mathbb{F}_q$ be a hyperelliptic curve with one rational point at infinity and $\mathrm{char}(\mathbb{F}_q) \neq 2$, then:

$$|q + 1 - \#\mathcal{H}(\mathbb{F}_q)| \leq 4\sqrt{q}. \tag{13}$$

PROOF : Consider the polynomial in n appearing in the previous Theorem 3.17. The polynomial has the form $\delta(x) := 2x^2 + Tx + 2q$ with $T := q + 1 - \#\mathcal{H}(\mathbb{F}_q)$. Its discriminant is

$$\Delta_\delta := T^2 - 16q.$$

We want to prove that $\Delta_\delta \leq 0$ since that would imply that $|T| \leq 4\sqrt{q}$, which is exactly the statement of the Hasse-Weil inequality for $g = 2$.

We already proved in Proposition 3.2 that if $n \in \mathbb{Z}$ exists such that $\Psi_n \in \mathrm{Mor}_{\mathbb{F}_q}(\mathcal{H}, \mathcal{J})$ is constant, then $\Psi_n = 0$, $q = n^2$ is a perfect square and $\#\mathcal{H}(\mathbb{F}_q) = q + 1 \pm 4\sqrt{q}$. Hence from the existence of such n, the Hasse-Weil inequality over $\mathbb{F}_q$ for the curve in question follows. So from now on we will suppose that Ψ_n is non-constant for every $n \in \mathbb{Z}$. By Theorem 3.17 this implies that $\delta_n = \Phi_n^*\Theta \bullet \Theta$ for all $n \in \mathbb{Z}$.

It is clear that $\delta_n > 0$ for all $n \in \mathbb{Z}$ by definition. This is since Ψ_n is non-constant, hence $\Theta_n \subset \mathcal{J}$ is a curve, implying that δ_n is the degree of the rational function $\kappa_4(\Psi_{n,w}(x, y)) \in \mathbb{F}_q(x)^*$ or $\kappa_4(\Psi_n(x, y)) \in \mathbb{F}_q(x)^*$ depending on Θ_n being in Supp div(κ_4) or not.

Another fast and not very elementary argument for this uses that the divisor Θ is ample, hence by the Nakai-Moishezon criterion for ampleness on surfaces (see [6, Chapter V, Theorem 1.10]), its intersection number with any curve is positive.

Now from Theorem 3.17 we have that $\delta_n = 2n^2 + (q + 1 - \#\mathcal{H}(\mathbb{F}_q))n + 2q$. Consider $\delta(x) = 2x^2 + (q + 1 - \#\mathcal{H}(\mathbb{F}_q))x + 2q$. We claim that $\delta(x)$ is non-negative for all $x \in \mathbb{R}$, hence it has non-positive discriminant Δ_δ. This will imply the Hasse-Weil inequality for this case.

Suppose that the Hasse-Weil inequality for genus 2 is false. This is equivalent to the statement $\Delta_\delta > 0$. In this case $\delta(x)$ has two different real zeros $\alpha < \beta$. We have that Δ_δ in terms of α and β is given by:

$$\Delta_\delta = 4(\alpha - \beta)^2 = T^2 - 16q.$$

The integer Δ_δ is assumed to be positive, so we conclude $4(\alpha - \beta)^2 \geq 1$. Moreover, recall $\delta(n) > 0$ for every $n \in \mathbb{Z}$. Since for any $x_0 \in (\alpha, \beta)$ we have that $\delta(x_0) < 0$, it follows that (α, β) contains no integers. This implies that $\beta - \alpha < 1$ and then $1 \leq 4(\alpha - \beta)^2 < 4$.

So we have just three situations for positive discriminant: $T^2 - 16q \in \{1, 2, 3\}$. Each of these possibilities results in a contradiction as we will see below.

Case : $T^2 - 16q = 3$. There are no integers (T, q) satisfying this, as one checks by reducing modulo 4.

Case : $T^2 - 16q = 2$. Again reducing modulo 4 implies that no integral solutions (T, q) exist.

Case $T^2 - 16q = 1$. Then

Subcase : (i) $T = 8w + 1 = q + 1 - \#\mathcal{H}(\mathbb{F}_q)$, $q = 4w^2 + w = p^n$.

Since p is the only prime dividing $q = w(4w + 1)$ and since gcd$(w, 4w + 1) = 1$, it follows that $w = \pm 1$ or $4w + 1 = \pm 1$. We proceed to check all possibilities.

If $4w+1=+1$ then $w=0$ and $q=0$ which is not possible.

If $4w+1=-1$ then $w=-\frac{1}{2}$ which is absurd since w is an integer.

If $w=+1$ then $q=5$ and $T=9$. However $9=5+1-\#\mathcal{H}(\mathbb{F}_5)$ is impossible.

If $w=-1$ then $q=3$ and $T=-7$. However $\mathcal{H}(\mathbb{F}_3)$ has at most $2\cdot 3+2$ rational points, hence $T\geq 3+1-8=-4$.

Subcase : (ii) $T=8w+7=q+1-\#\mathcal{H}(\mathbb{F}_q)$, $q=4w^2+7w+3=p^n$.

Again p is the only prime dividing $q=4w^2+7w+3=(w+1)(4w+3)$. Moreover these two factors are coprime since $4(w+1)-(4w+3)=1$. Therefore one of the factors must be ± 1. Again we check all possibilities.

If $w+1=1$ then $q=3$ and $T=7$. However any curve $C/\mathbb{F}_3$ has at least 0 rational points, hence $T=3+1-\#C(\mathbb{F}_3)\leq 4$.

If $w+1=-1$ then $q=5$ and $T=-9$. Any hyperelliptic $\mathcal{H}/\mathbb{F}_5$ satisfies $\#\mathcal{H}(\mathbb{F}_5)\leq 2\cdot(5+1)$, hence $T\geq 6-12=-6$.

The case $4w+3=1$ is impossible since w is assumed to be an integer.

Finally, $4w+3=-1$ leads to $q=0$ which is absurd.

This shows that assuming $\Delta_\delta=T^2-16q>0$ leads to a contradiction. Therefore $|T|\leq 4\sqrt{q}$ which is the Hasse-Weil inequality for this case. □

Remark : Note that our *definition* of the integers δ_n is elementary and completely analogous to the definition by Manin of the integers d_n. However, whereas Manin also succeeded in presenting a completely elementary proof of the basic identity for the d_n, we used the interpretation of the δ_n as intersection numbers in order to show an analogous basic identity in the genus two case. To obtain a fully elementary proof also in genus two, it therefore suffices to replace this intersection theory argument by a calculation in the spirit of what Manin did. We do not know whether this is a feasible task.

REFERENCES

1. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230. Cambridge University Press, (1996).

2. J. S. Chahal, Chapter 8: Equations over finite fields, In: *Topics in Number Theory*, pages 147-162. Plenum Press, New York, (1988).

3. J. S. Chahal, A. Soomro, and J. Top, A supplement to Manin's proof of the Hasse inequality, *Rocky Mountain Journal of Mathematics*, **44**(5) (2014), 1457-1470.

4. E. V. Flynn, The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field, In: *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 107, pages 425-441, (1990).

5. W. Fulton, *Intersection theory*, volume 2 of Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, Berlin, (1984).

6. R. Hartshorne, Algebraic Geometry, volume 52 of Graduate Texts in Mathematics. Springer Verlag, New York, (1977).

7. S. Lang, Abelian Varieties, volume 7 of Interscience Tracts in Pure and Applied Mathematics. Interscience Publishers, New York, (1959).

8. Yu. I. Manin, On cubic congruences to a prime modulus, *Izv. Akad. Nauk SSSR. Ser. Mat.*, **20** (1956), 673-678.

9. Yu. I. Manin, . On cubic congruences to a prime modulus, *Amer. Math. Soc. Transl.*, **13**(2) (1960), 1-7.

10. J. S. Milne, *Abelian varieties (v2.00)*, http: //www. jmilne. org/math/, pages=166+vi.

11. L. Moret-Bailly, *Families de courbes et de varietes abeliennes sur PI. Sem. sur les pinceaux de courbes de genre au mains deux*, (ed. L. Szpiro). Asterisques, 86 (1981).

12. M. Soeten, *Hasse's Theorem on Elliptic Curves*, Rijksuniversiteit Groningen, http://fse.studenttheses.ub.rug.nl/id/eprint/10999 (Master's thesis), (2013).

13. M. A. Soomro, *Algebraic curves over finite fields*, Rijksuniversiteit Groningen, http://hdl.handle.net/11370/024430b9-3e8e-497f-8374-326f014a26e7 (PhD Thesis), (2013).

14. L. C. Washington, *Elliptic curves Number theory and cryptography*, *Discrete Mathematics and its Applications*, Chapman Hall / CRC, Boca Raton, second edition, (2008).