EQUIDISTRIBUTION QUESTIONS FOR UNIVERSAL EXTENSIONS

NICHOLAS M. KATZ

1. Introduction

We will discuss in detail some equidistribution questions arising from the study of the universal extension of an elliptic curve by a vector group. We will also indicate analogous questions in the case of the universal extension of a Jacobian by a vector group, cf. [Mes] for the basic facts about the universal extension.

2. The overall setting

Let k be a field, C/k a proper, smooth, geometrically connected curve of genus $g \geq 1$ given with a marked rational point $0 \in C(k)$, $J_C/k := Pic^0_{C/k}$ its Jacobian. Concretely, the group $J_C(k)$ is the group (under tensor product) of isomorphism classes of invertible sheaves $\mathcal{L}$ on C of degree zero.

Given a point $P \in C(k)$, we denote by $I(P) \subset \mathcal{O}_C$ the ideal sheaf of functions vanishing at P. Given $P_1, ..., P_r$ a finite, possibly empty, list of distinct points in $C(k)$, and $D := \sum_i n_i[P_i]$ a divisor of degree zero (i.e., $\sum_i n_i = 0$) supported at these points, we have the invertible sheaf $\mathcal{L}_D := \otimes_i I(P_i)^{\otimes n_i}$. [This $\mathcal{L}_D$ is denoted $\mathcal{L}(-D)$ in Riemann-Roch notation, and called $\mathcal{O}_C(-D)$ classically.] If the list is empty, i.e. if $D = 0$ is the zero divisor, we take $\mathcal{L}_0 := \mathcal{O}_C$. Although not every point in $J_C(k)$ need be the isomorphism class of such an $\mathcal{L}_D$ built of rational points (unless either $g = 1$ or k is algebraically closed), those that are form a subgroup of $J_C(k)$, namely the subgroup generated by all elements of the form $I(P) \otimes I(0)^{-1}$ with $P \in C(k)$. For $g = 1$, i.e. when C/k is an elliptic curve E/k with origin 0, every element of $J_E(k)$ is uniquely of this form (and this bijection of $J_E(k)$ with $E(k)$ is what gives $E(k)$ its group structure).

Given an invertible sheaf $\mathcal{L}$ on C which has degree zero, one has the notion of a connection ∇ on $\mathcal{L}$, namely a k-linear map

$$\nabla : \mathcal{L} \to \mathcal{L} \otimes \Omega^1_{C/k}$$

which satisfies the Leibniz rule

$$\nabla(f\ell) = f\nabla(\ell) + \ell \otimes df.$$

Any $\mathcal{L}$ of degree zero admits a connection, and two connections differ by an $\mathcal{O}_C$ linear map, i.e. by a map of the form $\ell \mapsto \ell \otimes \omega$, for some $\omega \in H^0(C, \Omega^1_{C/k})$. One can tensor together such pairs $(\mathcal{L}, \nabla)$, by the rule

$$(\mathcal{L}_1, \nabla_1) \otimes (\mathcal{L}_2, \nabla_2) = (\mathcal{L}_1 \otimes \mathcal{L}_2, \quad \nabla_1 \otimes id_2 + id_1 \otimes \nabla_2).$$

The inverse (or dual) of an object $(\mathcal{L}, \nabla)$ is $(\mathcal{L}^{-1}, \nabla^\vee)$, where the dual connection $\nabla^\vee$ on $\mathcal{L}^{-1} = \mathcal{L}^\vee$ is defined by the requirement that for local sections ℓ of $\mathcal{L}$ and $\ell^\vee$ of $\mathcal{L}^\vee$, and $(,) : \mathcal{L} \times \mathcal{L}^\vee \to \mathcal{O}_C$ the canonical duality pairing, we have the formula

$$d(\ell, \ell^\vee) = (\nabla\ell, \ell^\vee) + (\ell, \nabla^\vee\ell^\vee).$$

The group of isomorphism classes of such pairs $(\mathcal{L}, \nabla)$ is denoted $J^\#_C(k)$. "Forgetting" the connection thus defines a surjection homomorphism $J^\#_C(k) \twoheadrightarrow J_C(k)$. Its kernel is the space of connections on the structure sheaf $\mathcal{O}_C$. One connection on $\mathcal{O}_C$ is exterior differentiation d, so any other is $d + \omega$ for some $\omega \in H^0(C, \Omega^1_{C/k})$. So we may view $H^0(C, \Omega^1_{C/k})$ as the space of connections on $\mathcal{O}_C$. Thus we have a short exact sequence

$$0 \to H^0(C, \Omega^1_{C/k}) \to J^\#_C(k) \to J_C(k) \to 0,$$

which is (the k-valued points of) the universal extension of the title, cf. [Mes].

Concretely, if $\mathcal{L}$ is the invertible sheaf $\mathcal{L}_D := \otimes_i I(P_i)^{\otimes n_i}$ attached to a divisor $D := \sum_i n_i[P_i]$ of degree $0 = \sum_i n_i$, then a connection of $\mathcal{L}_D$ is given by meormorphic differential ω_D, holomorphic outside the support of D, which has only simple poles at the points P_i, with residue n_i at P_i. [In the classical literature, such a differential is called a "differential of the third kind (in the strict sense)".] The corresponding connection is given by $\nabla(f) = df - f\omega_D$. Indeed, if f is a section over an open set U, so that f has $ord_{P_i}(f) \geq n_i$ at each P_i in U, then although df has $ord_{P_i}(f) \geq n_i - 1$ at each P_i in U, $df - f\omega_D$ again has $ord_{P_i}(df - f\omega_D) \geq n_i$ at each P_i in U, so $df - f\omega_D$ is a section of $\mathcal{L} \otimes \Omega^1_{E/k}$ over U.

In particular, if the divisor D above is principal, say $D = (g)$, then there is a canonical choice of ω_D, namely $\omega_{(g)} = dg/g$, well defined because g is determined by its divisor up to a $k^\times$ factor.

3. A construction in the hyperelliptic case, compare [Ka-Eis, Appendix C.2.1]

Suppose now that 2 is invertible in the field k, and that C/k is a hyper elliptic curve of genus $g \geq 1$, given as the complete nonsingular model of the affine curve defined by an equation of the form

$$y^2 = f(x)$$

with $f(x) \in k[x]$ of degree $2g+1$ with $2g+1$ distinct roots in $\overline{k}$. There is precisely one point in $C(k)$ not on the affine curve, the point $\infty \in C(k)$, which we take as marked point in $C(k)$.

Lemma 3.1. *Given a point $P \neq \infty$ in $C(k)$, say $P = (a, b)$, the differential*

$$\omega_{[P]-[\infty]} := (1/2)((y+b)/(x-a))dx/y$$

has simple poles at P and ∞ (and no other poles), with residues 1 *and* -1 *respectively.*

Proof. By an additive translation of the x coordinate, we may assume $a = 0$. Suppose first that $b = 0$. Then our differential is $(1/2)dx/x$. The function x has a double pole at ∞, and (because $b = 0$) it has a double zero at P, so the statement is obvious in this case.

In the remaining case, $a = 0, b \neq 0$, our differential $\omega_{[P]-[\infty]}$ is

$$(1/2)((y+b)/x)dx/y = (1/2)((y+b)/y)dx/x.$$

The differential dx/y is holomorphic at finite distance (because f has all distinct roots) and has a zero of order $2g = 2$ at ∞ (because x has a double pole at ∞ and y has a pole of order $2g+1$ at ∞). Since the degree of the canonical bundle is $2g-2$, dx/y has no zero or pole at finite distance. So the only possible pole of our differential $\omega_{[P]-[\infty]}$ is at the zeroes of x. The function x has a simple zero at each of the two points $P = (0, b)$ and $-P := (0, -b)$. The function $y + b$ vanishes at $-P$. Hence the function $(y+b)/x$ is holomorphic at $-P$, and its only finite pole is a simple pole at P. At P, x is a parameter, and the function $(y+b)/y = 1+b/y$ takes the invertible value 2 at P. Thus our differential $\omega_{[P]-[\infty]}$ near P is of the form $(2 + ...)dx/x$, so has residue 1 there. At ∞, the function $(y+b)/x$ has a pole of order $2g-1$, so our differential $\omega_{[P]-[\infty]}$ has a simple pole at ∞. As the sum of the residues is 0, our differential must have residue -1 at ∞. □

Corollary 3.2. *Given a point $P \neq \infty$ in $C(k)$ with $P \neq -P$, say $P = (a, b)$ with $b \neq 0$, the differential*

$$\omega_{[P]-[-P]} := bdx/(x-a)y$$

has simple poles at P *and* $-P$ *(and no other poles), with residues* 1 *and* -1 *respectively.*

Proof. Indeed, this differential is just the difference $\omega_{[P]-[\infty]} - \omega_{[-P]-[\infty]}$. $\square$

Suppose now that 2 is invertible in k, but that our hyperelliptic curve C/k of genus $g \geq 1$ is the complete nonsingular model of the affine curve defined by an equation of the form

$$y^2 = f(x)$$

with $f(x) \in k[x]$ of degree $2g+2$ with $2g+2$ distinct roots in $\overline{k}$. There are now two points in $C(\overline{k})$ not on the affine curve. Let us call them ∞_+ and ∞_-. If the leading coefficient of $f(x)$ is a square in k, these two points are both in $C(k)$; otherwise they are galois conjugate points in $C(k_2)$, for k_2/k the quadratic extension. We have the following lemma, whose proof is left to the reader.

Lemma 3.3. *Let* $P = (a, b), b \neq 0$ *be a finite point in* $C(k)$*, and denote by* $-P$ *the point* $(a, -b)$*. The differential*

$$((y+b)/(x-a))dx/y$$

has simple poles at the points P, ∞_+, ∞_- *with residues* $2, -1, -1$ *respectively, and no other poles. The differential*

$$bdx/(x-a)y$$

has simple poles at the points $P, -P$ *with residues* $1, -1$ *respectively, and no other poles.*

4. The situation over a base scheme

Let S be a scheme, and $\mathcal{C}/S$ a proper smooth curve, structural map $f : \mathcal{C} \to S$, with geometrically connected fibres of genus $g \geq 1$, given with a marked section $0 \in \mathcal{C}(S)$. Denote by $J_{\mathcal{C}/S} := Pic^0_{\mathcal{C}/S}$ its Jacobian, an abelian scheme over S. The group $J_{\mathcal{C}/S}(S)$ is the group of equivalence classes of invertible sheaves $\mathcal{L}$ on $\mathcal{C}$ which are fibre-by-fibre of degree zero, under tensor product. Two such invertible sheaves $\mathcal{L}_1$ and $\mathcal{L}_2$ are equivalent if their ratio $\mathcal{L}_1 \otimes \mathcal{L}_2^{-1}$ is isomorphic to $f^\star(\mathcal{M})$ for some invertible sheaf $\mathcal{M}$ on the base S.

Given an $\mathcal{L}$ as above, we have the notion of an S-linear connection ∇ on $\mathcal{L}$, namely an S-linear map

$$\nabla : \mathcal{L} \to \mathcal{L} \otimes \Omega^1_{\mathcal{C}/S}$$

which satisfies the Leibniz rule. The tensor product of such pairs $(\mathcal{L}, \nabla)$ is defined as above, namely

$$(\mathcal{L}_1, \nabla_1) \otimes (\mathcal{L}_2, \nabla_2) = (\mathcal{L}_1 \otimes \mathcal{L}_2, \quad \nabla_1 \otimes id_2 + id_1 \otimes \nabla_2).$$

One knows that when S is affine, any $\mathcal{L}$ which is fibre-by-fibre of degree zero admits an S-linear connection, cf. [Maz-Mes, page 46], and the difference of any two is a global one-form $\omega \in H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/S})$. Just as above, we have the notion of the inverse, or dual, of an object $(\mathcal{L}, \nabla)$, defined by

$$(\mathcal{L}, \nabla)^{-1} := (\mathcal{L}^{-1}, \nabla^{\vee}).$$

We say that two objects $(\mathcal{L}_1, \nabla_1)$ and $(\mathcal{L}_2, \nabla_2)$ are equivalent if their ratio $(\mathcal{L}_1, \nabla_1) \otimes (\mathcal{L}_2, \nabla_2)^{-1}$ is isomorphic to an object of the form $(f^{\star}(\mathcal{M}), d_{\mathcal{C}/S})$, with $\mathcal{M}$, i.e., an invertible sheaf on the base S together with the trivial connection on its pullback. The group of equivalence classes of such pairs is denoted $J^{\#}_{\mathcal{C}/S}(S)$. When S is affine, we thus have a short exact sequence

$$0 \to H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/S}) \to J^{\#}_{\mathcal{C}/S}(S) \to J_{\mathcal{C}/S}(S) \to 0,$$

In the special case when we are given a finite list of pairwise disjoint sections $P_1, .., P_r \in \mathcal{C}(S)$, and integers $n_1, ..., n_r$ with $\sum_i n_i = 0$, a connection on $\otimes_i I(P_i)^{\otimes n_i}$ is given by a differential in $H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/S}(\log(\sum_i P_i))$ having log poles along the P_i, with residue n_i along P_i for each i.

5. The hyperelliptic construction over a base scheme

Let A be a ring in which 2 is invertible. Suppose $S = Spec(A)$, and that $\mathcal{C}/S$ is a hyperelliptic curve of genus $g \geq 1$ (whose affine part is) given by an equation of the form

$$y^2 = f(x)$$

with $f(x) \in A[x]$ a monic polynomial of degree $2g + 1$ whose discriminant $\Delta(f)$ is a unit in A.

Exactly as in the case when A is a field, we have the following lemma.

Lemma 5.1. *Let $P = (a, b)$ be a finite point, with b a unit in A (to insure that $I(P) \otimes I(\infty)^{-1}$ is everywhere disjoint from the scheme-theoretic kernel of multiplication by 2 on the Jacobian). Then the differential*

$$\omega_{[P]-[\infty]} := (1/2)((y + b)/(x - a))dx/y$$

gives a connection on $I(P) \otimes I(\infty)^{-1}$, and the differential

$$\omega_{[P]-[-P]} := bdx/(x - a)y$$

gives a connection on $I(P) \otimes I(P)^{-1}$.

6. Formulation of a conjecture

We begin with $C/\mathbb{Q}$ a hyperelliptic curve over $\mathbb{Q}$ given by an equation $y^2 = f(x)$ with $f(x) \in \mathbb{Z}[x]$ monic of degree $2g+1$, with $2g+1$ distinct zeroes in $\mathbb{C}$, and an integer point $P = (a,b)$ with $b \neq 0$. We denote by $-P$ the point $(a,-b)$.

Denote by $\Delta(f) \in \mathbb{Z}$ the discriminant of the integer polynomial f. Thus over the ring $A := \mathbb{Z}[1/2b\Delta(f)]$ we have the following structures:

1. a hyperelliptic curve $\mathcal{C}/A$, defined by the equation $y^2 = f(x)$,
2. pairwise disjoint sections P, $-P$, and ∞ in $\mathcal{C}(A)$,
3. the point $\mathbb{P}$ in $J_{\mathcal{C}/A}(A)$ which is the class of $I(P) \otimes I(\infty)^{-1}$,

3bis. the point $2\mathbb{P}$ in $J_{\mathcal{C}/A}(A)$ which is the class of $I(P) \otimes I(-P)^{-1}$,

4. the connection on $\mathbb{P}$ given by $\omega_{[P]-[\infty]}$,

4bis. the connection on $2\mathbb{P}$ given by $\omega_{[P]-[-P]}$,

5. the point $\mathbb{P}^\# := (\mathbb{P}, \omega_{[P]-[\infty]})$ in $J^\#_{\mathcal{C}/A}(A)$, which lies over the point $\mathbb{P}$ in in $J_{\mathcal{C}/A}(A)$,

5bis. the point $(2\mathbb{P})^\# := (2\mathbb{P}, \omega_{[P]-[-P]})$ in $J^\#_{\mathcal{C}/A}(A)$, which lies over the point $2\mathbb{P}$ in in $J_{\mathcal{C}/A}(A)$.

For each odd prime p not dividing $b\Delta(f)$, we can reduce all of this data mod p. We will indicate the reductions with a subscript p. Thus we have the hyperelliptic curve $\mathcal{C}_p/\mathbb{F}_p$, the point P_p on it, the point $\mathbb{P}_p$ in $J_{\mathcal{C}_p}(\mathbb{F}_p)$ and the point $\mathbb{P}_p^\#$ in $J^\#_{\mathcal{C}_p}(\mathbb{F}_p)$ lying over it.

We also have the point $2\mathbb{P}_p$ in $J_{\mathcal{C}_p}(\mathbb{F}_p)$ and the point $(2\mathbb{P}_p)^\#$ in $J^\#_{C_p}(\mathbb{F}_p)$ lying over it.

Denote by n_p the cardinality of $J_{C_p}(\mathbb{F}_p)$. If we multiply the point $\mathbb{P}_p^\#$ by n_p, we get a point which lies over the origin in $J_{C_p}(\mathbb{F}_p)$, i.e., we get a point in $H^0(\mathcal{C}_p, \Omega^1_{\mathcal{C}_p/\mathbb{F}_p})$; let us call it

$$\omega_p(\mathbb{P}^\#).$$

Concretely, the invertible sheaf $n\mathbb{P}_p := (I(P_p)^{n_p} \otimes I(\infty_p)^{-n_p}$ is trivial on $\mathcal{C}_p$, i.e. there is a meromorphic function g_p on $\mathcal{C}_p$ whose divisor is $n_p([P_p] - [\infty_p])$. Then dg_p/g_p is **another** connection on $n\mathbb{P}_p$. The difference $n_p\omega_{[P_p]-[\infty_p]} - dg_p/g_p$ is the differential $\omega_p(\mathbb{P}^\#)$.

We can play this same game instead with the point $(2\mathbb{P}_p)^\#$; then $n_p(2\mathbb{P}_p)^\#$ is an element

$$\omega_p(2\mathbb{P}^\#)$$

in $H^0(\mathcal{C}_p, \Omega^1_{\mathcal{C}_p/\mathbb{F}_p})$.

In our hyperelliptic case, $H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/A})$ has an "obvious" A-basis, namely the g differentials $x^i dx/xy$ for $i = 1, ..., g$. We will denote by $\mathbb{H}$ the free $\mathbb{Z}$-module with this basis. Thus $H^0(\mathcal{C}, \Omega^1_{\mathcal{C}/A})$ is $\mathbb{H} \otimes_{\mathbb{Z}} A$, and for each odd prime p not dividing $b\Delta(f)$, $H^0(\mathcal{C}_p, \Omega^1_{\mathcal{C}_p/\mathbb{F}_p})$ is $\mathbb{H}/p\mathbb{H}$.

For each odd prime p not dividing $b\Delta(f)$, we have the isomorphism $\mathbb{H}/p\mathbb{H} \cong (1/p)\mathbb{H}/\mathbb{H}$ given by multiplication by $1/p$. We denote by

$$\omega_p(\mathbb{P}^\#)/p,\ \omega_p(2\mathbb{P}^\#)/p \in (1/p)\mathbb{H}/\mathbb{H}$$

the images of $\omega_p(\mathbb{P}^\#)$ and $\omega_p(2\mathbb{P}^\#)$ respectively in $(1/p)\mathbb{H}/\mathbb{H}$. Via the inclusion

$$(1/p)\mathbb{H}/\mathbb{H} \subset \mathbb{H} \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z}$$

we view these elements $\omega_p(\mathbb{P}^\#)/p$, $\omega_p(2\mathbb{P}^\#)/p$ as lying in the g-dimensional compact real torus $\mathbb{H} \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \cong (\mathbb{R}/\mathbb{Z})^g$.

Conjecture 6.1. *Suppose the cyclic subgroup generated by $\mathbb{P}$ is Zariski dense in $J_{\mathcal{C}/A} \otimes_A \mathbb{C}$. Then both of the sequences $\{\omega_p(\mathbb{P}^\#)/p\}_p$ and $\{\omega_p(2\mathbb{P}^\#)/p\}_p$, indexed by odd primes p not dividing $b\Delta(f)$, are equidistributed in the compact real torus $\mathbb{H} \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z}$ for its Haar measure of total mass one.*

Remark 6.2. When can we be sure that the cyclic subgroup generated by $\mathbb{P}$ is Zariski dense in $J_{\mathcal{C}/A} \otimes_A \mathbb{C}$? The simplest case is when the Jacobian is geometrically a simple abelian variety, in which case the condition is simply that $\mathbb{P}$ not be a point of finite order. This geometric simplicity holds when $g = 1$, or when $C/\mathbb{Q}$ is of either of the following two forms:

1. (CM case) an equation $y^2 = x^\ell + a$, ℓ an odd prime, any $a \in \mathbb{Q}^\times$, cf. [Ka-Wief, 9.1]
2. (Big Galois case) an equation $y^2 = f(x)$ with f of degree $d = 2g + 1 \geq 5$ having Galois group either S_d or A_d (Zarhin's theorem), cf. [Zarhin] or [Ka-Wief, section 10].

To check that the point $\mathbb{P}$ is not of finite order in $J_{\mathcal{C}_p}(A)$, it suffices to exhibit two distinct odd primes p_1 and p_2, both prime to $b\Delta(f)$, such that the images of $\mathbb{P}$ in the two groups $J_{\mathcal{C}/A}(\mathbb{F}_{p_1})$ and $J_{\mathcal{C}/A}(\mathbb{F}_{p_2})$ have different orders, cf. [Ka-Gal, Appendix].

We have the following lemma over $\mathbb{C}$. We formulate it for a Jacobian, but it remains valid, with the same proof, for the universal extension of $Pic^0(A)$,

$$0 \to H^0(A, \Omega^1_{A/\mathbb{C}}) \to Pic^0(A)^\#(\mathbb{C}) \to Pic^0(A)(\mathbb{C}) \to 0,$$

for $A/\mathbb{C}$ any complex abelian variety.

Lemma 6.3. *Let $C/\mathbb{C}$ be a proper smooth connected curve of genus $g \geq 1$, $\mathbb{P}$ a point in $J_C(\mathbb{C})$ and $\mathbb{P}^\#$ a point in $J_C^\#(\mathbb{C})$ lying over $\mathbb{P}$.*

Suppose that the cyclic group generated by $\mathbb{P}$ is Zariski dense in J_C. Then the cyclic group generated by $\mathbb{P}^\#$ is Zariski dense in $J_C^\#$.

Proof. This results formally from the universal extension property. More precisely, recall that

$$\mathrm{Ext}^1(J_C, \mathbb{G}_a) \cong H^1(J_C, \mathcal{O}_{J_C}) \cong H^1(C, \mathcal{O}_C),$$

in such a way that the nontrivial extensions of J_C by $\mathbb{G}_a$ are precisely the push-outs of

$$0 \to H^0(C, \Omega^1_{C/\mathbb{C}}) \to J_C^\#(\mathbb{C}) \to J_C(\mathbb{C}) \to 0,$$

by nonzero elements of $H^1(C, \mathcal{O}_C) \cong \mathrm{Hom}_{\mathbb{C}}(H^0(C, \Omega^1_{C/\mathbb{C}}), \mathbb{C})$.

Denote by $G \subset J_C^\#$ the Zariski closure of the subgroup generated by $\mathbb{P}^\#$. By hypothesis, G maps onto J_C, so G itself is an extension of the form

$$0 \to \mathbb{V} \to G \to J_C \to 0,$$

with $\mathbb{V}$ some vector subspace of $H^0(C, \Omega^1_{C/\mathbb{C}})$. If $\mathbb{V}$ is the entire space $H^0(C, \Omega^1_{C/\mathbb{C}})$, we are done. If not, we get a contradiction as follows. Choose a surjective homomorphism ϕ from $H^0(C, \Omega^1_{C/\mathbb{C}})$ to $\mathbb{C}$ whose kernel contains $\mathbb{V}$. This extension is simultaneously split (because ϕ kills $\mathbb{V}$) and nontrivial (by the universal extension property). $\square$

7. Relation, in the elliptic case, to another conjecture

We begin with $E/\mathbb{Q}$ an elliptic curve over $\mathbb{Q}$ given by an equation $y^2 = f(x)$ with $f(x) \in \mathbb{Z}[x]$ a squarefree monic cubic, and an integer point $P = (a, b)$ with $b \neq 0$. We denote by $\Delta(f)$ the discriminant of f. We work over the ring $A := \mathbb{Z}[1/2b\Delta(f)]$. So we have an elliptic curve $\mathcal{E}/A$, and a line bundle $\mathcal{L} := I(P) \otimes I(\infty)^{-1}$ on $\mathcal{E}$, fibrewise of degree zero. For each good prime p, i.e. for each prime p not dividing $2b\Delta(f)$, we denote $n_p := \#\mathcal{E}(\mathbb{F}_p)$. We assume that n_p is prime to p for all good p. [This is automatic if $E(\mathbb{Q})$ contains a nontrivial point of order 2, at least for good primes $p \geq 7$, cf. [Ka-Alg, 7.5.2].] For each good p, the divisor $n_p([P] - [\infty])$ on $\mathcal{E}_p := \mathcal{E} \otimes_A \mathbb{F}_p$ is principal, so the divisor of some function g_p on $\mathcal{E}_p$. Then $(1/n_p)dg_p/g_p$ is a connection on $\mathcal{L}_p := I(P) \otimes I(\infty)^{-1}|\mathcal{E}_p$. In [Ka-Alg, Conjecture 7.5.11], we suppose chosen a connection ∇ on $\mathcal{L}$. In terms of the connection

$$\omega_{[P]-[\infty]} := (1/2)((y + b)/(x - a))dx/y,$$

such a choice is of the form

$$\nabla = \omega_{[P]-[\infty]} + a dx/y$$

for some $a \in A$. We denote by ∇_p its restriction to $\mathcal{L}_p$.

We then consider, for each good prime p, the difference

$$\nabla_p - (1/n_p)dg_p/g_p,$$

which is necessarily of the form $b_p dx/y$ for some $b_p \in \mathbb{F}_p$. We consider the sequence $\{b_p\}_{\text{good p}}$ in $\prod_{\text{good p}} \mathbb{F}_p$. If we change the choice of ∇, say to $\nabla + Bdx/y$ for some $B \in A$, we change this sequence to $\{B + b_p\}_{\text{good p}}$. So given the point P, we get a well defined element of the quotient group $(\prod_{\text{good p}} \mathbb{F}_p)/A$, where A is embedded diagonally. In [Ka-Alg, Conjecture 7.5.11], we conjecture that if this element in $(\prod_{\text{good p}} \mathbb{F}_p)/A$ vanishes, then P is a point of finite order in $E(\mathbb{Q})$.

Lemma 7.1. *If Conjecture 6.1 holds for E/Q, then* [Ka-Alg, Conjecture 7.5.11] *holds.*

Proof. We argue by contradiction. Suppose P is a point of infinite order, but it gives rise to zero in the quotient group. This means that for some $b \in A$, if we use the connection $\nabla = \omega_{[P]-[\infty]} - bdx/y$, then for each good p we have

$$\omega_{[P]-[\infty]} - bdx/y = (1/n_p)dg_p/g_p,$$

i.e., we have

$$n_p \omega_{[P]-[\infty]} = dg_p/g_p + n_p bdx/y.$$

In other words, denoting by $b_p \in \mathbb{F}_p = A/pA$ the reduction mod p of b, we have

$$\omega_p(P^{\#}) = n_p b_p dx/y.$$

According to Conjecture 6.1, the sequence $\{n_p b_p/p\}_{\text{good p}}$ is equidistributed in $\mathbb{R}/\mathbb{Z}$ for Haar measure. If $b = 0$, this is obviously false. If $b \in A$ is nonzero, denote by N its denominator, say

$$b = B/N,$$

with B, N nonzero integers. Recall that if a sequence $\{x_i\}_i$ is equidistributed in $\mathbb{R}/\mathbb{Z}$ for Haar measure, then so is the sequence $\{Nx_i\}_i$, cf. [Ka-Wief, 5.1]. Hence the sequence $\{n_p B/p\}_{\text{good p}}$ is equidistributed. This too is false, for if we write $n_p = p + 1 - a_p$, then we have the Hasse bound $|a_p| < 2\sqrt{p}$. Thus mod $\mathbb{Z}$, $n_p B/p$ is $(1 - a_p)B/p$, a fraction bounded in absolute value by $B(1 + 2\sqrt{p})/p$. As B is fixed and p is growing, this sequence tends to 0 in $\mathbb{R}/\mathbb{Z}$, so certainly is not equidistributed for Haar measure. $\square$

8. Numerical evidence, in the elliptic case

It is only in the $g = 1$ case that we have performed numerical experiments. We took the curve

$$y^2 = (x^2 - 1)(x - 4)$$

and the point

$$P := (0, 2).$$

The only bad primes are $2, 3, 5$. We calculated both $\omega_p(\mathbb{P}^{\#})/p$ and $\omega_p(2\mathbb{P}^{\#})/p$ for the first 330000 primes starting with 7, i.e., for all primes $7 \le p \le 4716091$, and found excellent agreement, as measured by the Kolmogorov-Smirnov statistic, with the conjecture.

We also took the CM curve

$$y^2 = x^3 + 3$$

and the point

$$P := (1, 2).$$

The only bad primes are $2, 3$. We calculated $\omega_p(\mathbb{P}^{\#})/p$ for the first 180000 primes starting with 7, i.e. for all primes $7 \le p \le 2454631$ and here also found excellent agreement, as measured by the Kolmogorov-Smirnov statistic, with the conjecture.

Let us recall the definition of this statistic. Given a sequence of length N of points in $\mathbb{R}/\mathbb{Z}$, one takes their representatives in $[0, 1)$, one sorts them into increasing order, say $0 \le x_1 \le x_2 ... \le x_N < 1$, one computes the maximum over $i \in [1, N]$ of the absolute value of $x_i - i/N$, and one multiplies this maximum by the square root of N. See [Gnedenko, pp. 450-451] and [PFTV, pp. 490-492] for a discussion of the significance of this statistic.

We also did some equicharacteristic experiments. For several large primes p, the largest of which was 3497861, we looked at the curves E_t over $\mathbb{F}_p$ given by

$$E_t : y^2 = (x^2 - 1)(x - t^2),$$

for $t \in \mathbb{F}_p$ with $t(t^4 - 1) \neq 0$. On E_t we took the point $P_t := (0, t)$, and calculated the point $\omega_p(\mathbb{P}_t^{\#})/p$ (respectively the point $\omega_p(2\mathbb{P}_t^{\#})/p$) and its ratios to dx/y. We found that in both cases as t varies, these $p - 5$, resp. $p - 3$ (if p is 1, resp. 3, mod 4) points in $(1/p)\mathbb{Z}/\mathbb{Z}$ were approximately equidistributed in $\mathbb{R}/\mathbb{Z}$, again as measured by the Kolmogorov-Smirnov statistic.

9. How we did the calculations

Let p be an odd prime, $E/\mathbb{F}_p$ an elliptic curve given by an equation $y^2 = f(x)$ with $f(x)$ a monic cubic polynomial which is squarefree. We are given a divisor of degree zero, $D := \sum_i e_i[P_i]$ with all $P_i \in E(\mathbb{F}_p)$, and a differential ω_D which is holomorphic except at the points P_i, and has simple poles at the Pi with $res_{Pi}(\omega_D) = e_i$. We denote

$$n_p := \#E(\mathbb{F}_p).$$

Then the divisor n_pD is principal, say $n_pD = (g_p)$. Hence the difference $n_p\omega_D - dg_p/g_p$ is everywhere holomorphic, so some $\mathbb{F}_p$ multiple of dx/y:

$$n_p\omega_D = dg_p/g_p + c_p dx/y$$

for some $c_p \in \mathbb{F}_p$. Our task is to calculate c_p.

Lemma 9.1. *Suppose $n_p := \#E(\mathbb{F}_p)$ is prime to p. Denote by $\mathcal{C}$ the Cartier operator. Then*

$$(1 - \mathcal{C})(\omega_D) = c_p dx/y.$$

Proof. The Cartier operator fixes logarithmic differentials, and preserves holomorphicity at any given point. Now ω_D is, near each P_i, the sum of a holomorphic (at P_i) form and a logarithmic one, so $(1-\mathcal{C})(\omega_D)$ is everywhere holomorphic. Applying $1-\mathcal{C}$ to both sides of the equation

$$n_p\omega_D = dg_p/g_p + c_p dx/y,$$

we get

$$n_p(1 - \mathcal{C})(\omega_D) = c_p(1 - \mathcal{C})(dx/y).$$

But one knows that

$$\mathcal{C}(dx/y) = a_p dx/y,$$

for

$$a_p := p + 1 - n_p.$$

So the above identity reads

$$n_p(1 - \mathcal{C})(\omega_D) = c_p(1 - a_p)(dx/y).$$

As n_p is congruent to $1 - a_p$ mod p and is invertible mod p, we may cancel to get the asserted identity $(1 - \mathcal{C})(\omega_D) = c_p dx/y$. □

Remark 9.2. In fact, the identity

$$(1 - \mathcal{C})(\omega_D) = c_p dx/y$$

remains valid even when $p|n_p$. In an appendix, we will give a proof of this.

We now work out the special cases when D is $[P]-[\infty]$ or $[P]-[-P]$, with P a finite point (a,b) with $b\neq 0$. By an additive translation of x, we reduce to the case when P is $(0,b)$, with $b\neq 0$.

Lemma 9.3. *Suppose n_p is prime to p, and $P\in E(\mathbb{F}_p)$ is $(0,b)$ with $b\neq 0$. Write $f(x)=A_0+A_1x+A_2x^2+x^3$, with coefficients $A_i\in\mathbb{F}_p$. Write*

$$f(x)^{(p-1)/2}=\sum_i B_i x^i.$$

Then

$$\omega([P]-[-P])=-bB_p dx/y$$

and

$$\omega([P]-[\infty])=(1/2)\omega([P]-[-P])=(-bB_p/2)dx/y.$$

Proof. We first explain the factor 1/2. The differential $\omega_{[P]-[\infty]}$ is

$$\omega_{[P]-[\infty]}=(1/2)(y+b)dx/xy=(1/2)dx/x+(1/2)bdx/xy.$$

The differential $\omega_{[P]-[-P]}$ is

$$\omega_{([P]-[-P]}=bdx/xy.$$

But $1-\mathcal{C}$ kills dx/x, so we have

$$(1-\mathcal{C})(\omega_{[P]-[\infty]}=(1/2)(1-\mathcal{C})(\omega_{[P]-[-P]}),$$

and we apply the previous lemma.

It remains to compute $(1-\mathcal{C})(\omega_{[P]-[-P]}=b(1-\mathcal{C})(dx/xy)$. For this, we follow the classical computation. We write

$$dx/xy=y^{p-1}dx/xy^p=f(x)^{(p-1)/2}dx/xy^p.$$

In terms of Dwork's Ψ operator on $\mathbb{F}_p$-polynomials

$$\Psi(\sum_n e_nx^n):=\sum_n e_{pn}x^n,$$

we have

$$\mathcal{C}(f(x)^{(p-1)/2}dx/xy^p)=\Psi((f(x)^{(p-1)/2})dx/xy.$$

Thus

$$(1-\mathcal{C})(dx/xy)=(1-\Psi((f(x)^{(p-1)/2}))dx/xy=\Psi(1-f(x)^{(p-1)/2})dx/xy.$$

Because $P=(0,b)$ is an $\mathbb{F}_p$ point point on E with $b\neq 0$, we have $f(0)=b^2$, and hence $f(x)^{(p-1)/2}$ has constant term 1. Thus $1-f(x)^{(p-1)/2}$ has no constant term. As its degree is $3(p-1)/2<2p$, we have $\Psi(1-f(x)^{(p-1)/2})=-B_px$, and hence

$$(1-\mathcal{C})(dx/xy)=-B_pdx/y,\quad (1-\mathcal{C})(bdx/xy)=-bB_pdx/y.$$

$\square$

We now explain our method of computing B_p. In $\mathbb{F}_p$, we have the identity

$$\sum_{x\in\mathbb{F}_p^\times} x^d = -1 \text{ if } (p-1)|d, \quad = 0 \text{ if not.}$$

Because $f(x)^{(p-1)/2}$ has degree $< 2(p-1)$, we have

$$\sum_{x\in\mathbb{F}_p^\times} (1/x)f(x)^{(p-1)/2} = -B_1 - B_p.$$

So

$$-bB_p = bB_1 + b\sum_{x\in\mathbb{F}_p^\times} (1/x)f(x)^{(p-1)/2}.$$

On the other hand, in terms of the linear term $b^2 + A_1x$ of $f(x)$, we have

$$B_1 = ((p-1)/2)(b^2)^{(p-3)/2}A_1 = -b^{p-3}A_1/2 = -A_1/2b^2.$$

For χ_2 the quadratic character of $\mathbb{F}_p^\times$, extended to $\mathbb{F}_p$ by $\chi_2(0) = 0$, and viewed as having values in $\mathbb{F}_p$, we have

$$\chi_2(f(x)) = f(x)^{(p-1)/2}$$

for each $x \in \mathbb{F}_p$. So we get

Lemma 9.4. *We have*

$$-bB_p = -A_1/2b + b\sum_{x\in\mathbb{F}_p^\times} (1/x)\chi_2(f(x)).$$

In some of our experiments, we took curves of the form $y^2 = (x^2 - 1)(x - b^2)$. For such a curve, $A_1 = -1$. All the points of order 2 are rational, so n_p is divisible by 4. Hence n_p is prime to p; if not, the strictly positive integer n_p would be divisible by $4p$ and hence we would have $n_p \geq 4p$. This contradicts the completely elementary estimate $n_p \leq 2(p+1)$ which results from viewing an elliptic curve as a double cover of $\mathbb{P}^1$.

For the CM curve $y^2 = x^3 + 3$, P the point $(1, 2)$, and D the divisor $[P] - [\infty]$,there were 43 primes p with $p|n_p$ (or equivalently $p = n_p$) in our test range $7 \leq p \leq 2454631$. For each of these we checked by computer that

$$(1 - \mathcal{C})(\omega_D) = c_p dx/y,$$

or equivalently (since $0 = n_p\omega_D = dg/g + c_p dx/y$) that $dg/g = (\mathcal{C} - 1)(\omega_D)$ for g the function whose divisor is n_pD. [We used a Magma program kindly provided by Bradley Brock to compute the function g with divisor n_pD, and the differential dg/g.] Of course, once we know that Lemma 9.1 remains valid when $p|n_p$, as we show in the appendix, such computer checking is no longer necessary.

10. Computational problems in the higher genus case

We now consider a (proper, smooth, geometrically connected) curve $C/\mathbb{F}_p$ of genus $g \geq 1$, a divisor D of degree zero on C. Choose any differential of the third kind in the strict sense ω_D with simple poles at (some of) the points of D and no other poles, whose residue divisor is congruent mod p to D. With $n_p := \#Jac(C/\mathbb{F}_p)(\mathbb{F}_p)$, we know that n_pD is the divisor of a function g, and our problem is to compute the holomorphic one-form

$$n_p\omega_D - dg/g.$$

Equivalently, our problem is to compute dg/g for the function g, unique up to a $k^\times$ factor, whose divisor is n_pD.

To do this, we consider the action of the Cartier operator $\mathcal{C}$ on $H^0(C, \Omega^1_{C/\mathbb{F}_p})$, and denote by $F(T) \in \mathbb{F}_p[T]$ its characteristic polynomial:

$$F(T) := \det(T\mathrm{Id} - \mathcal{C}|H^0(C, \Omega^1_{C/\mathbb{F}_p})).$$

Lemma 10.1. *If n_p is prime to p, and the function g has divisor n_pD, then*

$$F(\mathcal{C})(\omega_D) = dg/g.$$

Proof. We first remark that $F(\mathcal{C})(\omega_D)$ is independent of the particular choice of ω_D. Indeed, that choice is indeterminate up to adding an element of $H^0(C, \Omega^1_{C/\mathbb{F}_p})$. By the Cayley-Hamilton theorem, the operator $F(\mathcal{C})$ kills the space $H^0(C, \Omega^1_{C/\mathbb{F}_p})$. We next remark that the formation of $F(\mathcal{C})(\omega_D)$ is additive in D; if we have chosen ω_{D_i} for $i = 1, 2$, then $\omega_{D_1} \pm \omega_{D_2}$ is an ω_{D_3} for $D_3 := D_1 \pm D_2$. We have the same additivity for dg/g as a function of D.

Thus the construction

$$D \mapsto F(\mathcal{C})(\omega_D) - dg/g$$

is an additive map from the group $Div^0(C)$ of divisors of degree zero on C to the space $H^0(C, \Omega^1_{C/\mathbb{F}_p})$. This map kills principal divisors. For if $D = (h)$, then one choice of an ω_D is dh/h. Then n_pD is the divisor of $g := h^{n_p}$, and hence dg/g is n_pdh/h. So the assertion is that

$$F(\mathcal{C})(dh/h) - n_pdh/h = 0.$$

But $\mathcal{C}$ fixes logarithmic differentials, so $F(\mathcal{C})(dh/h) = F(1)dh/h$, and $F(1) = \det(1 - \mathcal{C})$ is n_p mod p.

Summing up, the construction

$$D \mapsto F(\mathcal{C})(\omega_D) - dg/g$$

defines a group homomorphism from $Jac(C/\mathbb{F}_p)(\mathbb{F}_p)$ to $H^0(C, \Omega^1_{C/\mathbb{F}_p})$. The target is a p-group, so this homomorphism must vanish when its source has order prime to p, and in general factors through the quotient group $Jac(C/\mathbb{F}_p)(\mathbb{F}_p)/pJac(C/\mathbb{F}_p)(\mathbb{F}_p)$. □

Corollary 10.2. *If n_p is prime to p, and the function g has divisor $n_p D$, then*

$$n_p D - dg/g = (F(1) - F(\mathcal{C}))(\omega_D).$$

Remark 10.3. When $g = 1$, then $F(T) = T - A$ for A the Hasse invariant, and the difference $F(1) - F(\mathcal{C})$ is $1 - \mathcal{C}$.

Remark 10.4. Just as in the elliptic case, where we are able to prove it, we believe that the formula

$$F(\mathcal{C})(\omega_D) = dg/g$$

remains valid even when p divides n_p. In any case, we universally have the "decomposition"

$$n_p D = F(\mathcal{C}))(\omega_D) + (F(1) - F(\mathcal{C}))(\omega_D).$$

The first term, $F(\mathcal{C})(\omega_D)$, is always logarithmic, because it is killed by $1 - \mathcal{C}$. Indeed,

$$(1 - \mathcal{C})F(\mathcal{C})(\omega_D) = F(\mathcal{C})(1 - \mathcal{C})(\omega_D).$$

But $(1-\mathcal{C})(\omega_D)$ is an everywhere holomorphic form, and $F(\mathcal{C})$ kills all such. The second term, $(F(1)-F(\mathcal{C}))(\omega_D)$, is everywhere holomorphic, because the operator $F(1)-F(\mathcal{C})$ is divisible by $1-\mathcal{C}$, and $(1-\mathcal{C})(\omega_D)$ is everywhere holomorphic. [When n_p is prime to p, an expression as the sum of a logarithmic form and a holomorphic one is unique. This amounts to the fact that if a nonzero logarithmic form dh/h is everywhere holomorphic, then there is a rational point of order p on the Jacobian. The divisor of h is of the form pD, and the nonvanishing of dh/h means that D is not principal, although pD is.]

To examine a bit the computational issues, we consider the special case of a hyperelliptic curve $C/\mathbb{F}_p$ of genus $g \geq 2$ over $\mathbb{F}_p$, p odd, of equation $y^2 = f(x)$ with $f(x)$ a monic, squarefree polynomial of degree $2g + 1$. We suppose that $(0, b), b \neq 0$, is a point $P \in C(\mathbb{F}_p)$ on our curve, and we define $-P := (0, -b)$. With D taken to be $[P] - [\infty]$ or $[P] - [-P]$, then a choice of $\omega_{[P]-[\infty]}$ is

$$\omega_{[P]-[\infty]} = (1/2)(y + b)dx/xy = (1/2)dx/x + (1/2)bdx/xy,$$

and a choice of $\omega_{[P]-[-P]}$ is

$$\omega_{([P]-[-P]} = bdx/xy.$$

In view of the preceding general discussion, we will need first to compute the characteristic polynomial $F(T)$, then to compute the action of the powers $\mathcal{C}, \mathcal{C}^2, ..., \mathcal{C}^g$ on bdx/xy. For the first step, we can proceed as follows. For each $i \geq 1$ we have the mod p congruence

$$\#C(\mathbb{F}_{p^i}) \equiv 1 - \mathrm{Trace}(\mathcal{C}^i).$$

In characteristic $p > g$, these traces (Newton sums of eigenvalues) for $1 \leq i \leq g$ determine the elementary symmetric functions $\mathrm{Trace}(\Lambda^i(\mathcal{C}))$, which are, up to sign, the coefficients of $F(T)$.

This second step is theoretically straightforward, as we have the following lemma, the higher genus version of Lemma 9.3.

Lemma 10.5. *For $q = p^i, i \geq 1$ any power of p, write*

$$f(x)^{(q-1)/2} = \sum_i B_{i,q} x^i.$$

Then $B_{0,q} = 1$, and

$$\mathcal{C}^i(dx/xy) = B_{0,q} dx/xy + \sum_{j=1}^{g} B_{jq,q} x^j dx/y.$$

Proof. That $B_{0,q} = 1$ results from the hypothesis that the constant term b^2 of f is a square. Fix $i \geq 1$, write $q := p^i$, and write

$$dx/xy = y^{q-1} dx/xy^q = f(x)^{(q-1)/2} dx/xy^q = (\sum_i B_{i,q} x^i) dx/xy^q.$$

Applying $\mathcal{C}$ once, we get

$$\mathcal{C}(dx/xy) = (\sum_i B_{ip,q} x^i) dx/xy^{q/p}.$$

Continuing to apply $\mathcal{C}$ to both sides of the above equality, we find successively that for each j in the interval $1 \leq j \leq i$, we have

$$\mathcal{C}^j(dx/xy) = (\sum_i B_{ip^j,q} x^i) dx/xy^{q/p^j}.$$

□

Combining Corollary 10.2 with this result, we get a method of calculation, but one which is computationally unpleasant. For $D = [P] - [\infty]$, with $P = (0, b)$, and

$$F(1) - F(T) = \sum_{i=0}^{g} d_i T^i,$$

we find

$$(F(1) - F(\mathcal{C}))(\omega_D) = (\sum_{i=0}^{g} d_i \mathcal{C}^i)((1/2)dx/x + (b/2)dx/xy) =$$

$$= \sum_{j=1}^{g} \mathbb{A}_i x^j dx/xy,$$

with

$$\mathbb{A}_j = (b/2) \sum_{i=0}^{g} d_i B_{jp^i,p^i}.$$

[The $\mathbb{A}_0$ term vanishes, because each $B_{0,p^i} = 1$, and $\sum_i d_i = 0$.]

In the case $g = 2$ we can compute $F(1) - F(\mathcal{C})$ in a simpler way. We know that $1 - \mathrm{Trace}(\mathcal{C}) \equiv \#C(\mathbb{F}_p) \bmod p$. So we get

$$F(1) - F(\mathcal{C}) = (1 - \mathrm{Trace}(\mathcal{C}) + \det(\mathcal{C})) - (\mathcal{C}^2 - \mathrm{Trace}(\mathcal{C})\mathcal{C} + \det(\mathcal{C})) =$$

$$= -\mathcal{C}^2 + (1 - \#C(\mathbb{F}_p))\mathcal{C} + \#C(\mathbb{F}_p).$$

11. Appendix

In this appendix, we show that the conclusion of Lemma 9.1 remains valid without the assumption that n_p is prime to p. Because it may be of use in other situations, we will work in a slightly more general situation. We take an odd prime p, a finite extension field $\mathbb{F}_q$ of $\mathbb{F}_p$, and an elliptic curve $E/\mathbb{F}_q$, with $\#E(\mathbb{F}_q)$ denoted n_q. We give ourselves a point $P \in E(\mathbb{F}_q)$ with $P \neq -P$. We choose a Weierstrass equation for our curve, $y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ a monic, squarefree cubic, so that our point P is $(0, b)$. We take for D the divisor $[P] - [0]$ on E, and for ω_D the differential of the third kind in the strong sense,

$$\omega_D := (1/2)(y + b)dx/xy,$$

which has simple poles only at P and 0, with residues 1 and -1 respectively. We know that the divisor $n_q D$ is principal, say $n_q D = (g)$ for some function g on E, and so the difference $n_q\omega_D - dg/g$ has no poles. In other words, we can write

$$n_q\omega_D = dg/g + \omega(D)$$

with $\omega(D)$ a differential of the first kind on E, say $\omega(D) = c_q dx/y$ with $c_q \in \mathbb{F}_q$.

For $d := \deg(\mathbb{F}_q/\mathbb{F}_p)$, we denote by $\mathcal{C}_q$ the d'th iterate $\mathcal{C}_p^d$ of the Cartier operator. This is an $\mathbb{F}_q$-linear operator on the space of meromorphic one-forms on E which fixes logarithmic differentials, kills exact differentials, and preserves holomorphicity at any given point. We denote by $a_q \in \mathbb{F}_q$ the effect of $\mathcal{C}_q$ on the one-dimensional space $H^0(E, \Omega^1_{E/\mathbb{F}_q})$:

$$\mathcal{C}_q(dx/y) = a_q dx/y.$$

We have the mod p congruence

$$n_q \equiv 1 - a_q \bmod p,$$

which shows that in fact a_q lies in the prime field.

Theorem 11.1. *In the situation of the Appendix we have the formulas*

$$dg/g = (\mathcal{C}_q - a_q)(\omega_D), \quad \omega(D) = (1 - \mathcal{C}_q)(\omega_D).$$

Corollary 11.2. *Let $E/\mathbb{F}_q$ be an elliptic curve, D a divisor of degree zero on E, and g a nonzero function on E whose divisor is $n_q D$. Then for* **any** *differential ω_D of the third kind in the strict sense whose residue divisor is D, dg/g is given by the formula*

$$dg/g = (\mathcal{C}_q - a_q)(\omega_D).$$

Proof. For given D, a choice of ω_D is indeterminate up to adding a differential of the first kind on E. But any such is killed by $\mathcal{C}_q - a_q$, so we may choose ω_D conveniently. We treat three cases separately.

If D is linearly equivalent to zero, say $D = (h)$, then a convenient choice of ω_D is dh/h. In this case, $n_q D$ is the divisor of $g := h^{n_q}$. In this case, $dg/g = n_q dh/h$, and the assertion is that $(\mathcal{C}_q - a_g)(dh/h) = n_q dh/h$. This holds because $n_q \equiv 1 - a_q \bmod p$ while $\mathcal{C}_q$ fixes dh/h.

If D is linearly equivalent to $D_0 := [P] - [0]$ for a point P in $E(\mathbb{F}_q)$ of order 2, let h be a function whose divisor is $2[P] - 2[0]$. Because p is odd, $(1/2)dh/h$ is a choice of ω_D. With this choice, $(\mathcal{C}_q - a_q)(\omega_D)$ is $(1 - a_q)(1/2)dh/h = (n_q/2)dh/h = dg/g$ for $g := h^{n_q/2}$. This g has divisor $n_q D$.

If D is linearly equivalent to $D_0 := [P] - [0]$ for a point P in $E(\mathbb{F}_q)$, with $P \neq -P$, write $D = [P] - [0] + (h)$, for some nonzero function h on E. Then a convenient choice of ω_D is $\omega_{D_0} + dh/h$. Write $n_q D_0 = (g_0)$. Then $n_q D = (g_0 h^{n_q})$, and the assertion is that $(\mathcal{C}_q - a_q)(\omega_{D_0} + dh/h) = dg_0/g_0 + n_q dh/h$, which results from Theorem 11.1, together with the first case treated above. □

We now turn to the proof of the theorem.

Proof. The two formulas are equivalent, because

$$n_q \omega_D = dg/g + \omega(D),$$

and $n_q \equiv 1 - a_g \bmod p$.

When n_q is prime to p, the argument is the one used in proving Lemma 9.1. We apply the operator $1-\mathcal{C}_q$ to both sides of the displayed formula. This operator kills dg/g, so we get

$$n_q(1-\mathcal{C}_q)\omega_D = (1-\mathcal{C}_q)\omega(D) = (1-a_q)\omega(D).$$

Because $n_q \equiv 1 - a_g \bmod p$ is prime to p, we may divide and get $(1-\mathcal{C}_q)\omega_D = \omega(D)$.

More generally, if the divisor class D has order n_D prime to p, say $n_D D = (h)$, then we write

$$n_D\omega_D = dh/h + \omega_0(D).$$

Multiplying by n_q/n_D, we see that

$$\omega(D) = (n_q/n_D)\omega_0(D).$$

But if we apply $1-\mathcal{C}_q$ to both sides of $n_D\omega_D = dh/h + \omega_0(D)$, we get

$$n_D(1-\mathcal{C}_q)\omega_D = (1-a_q)\omega_0(D) = n_q\omega_0(D).$$

Dividing through by n_D gives the result.

Suppose now that p divides n_q, or equivalently that a_q is 1 mod p. Then certainly E is ordinary. We denote by $\mathbb{E}/W(\mathbb{F}_q)$ its canonical lifting in the sense of Serre-Tate. There are two key properties of the canonical lifting we will make use of, cf. [Mes-BT, Ch. V, 2.3, 2.3.6, 3.3, 3.4 and Appendix, 1.2]

The first is that the torsion subgroup of $\mathbb{E}(W(\mathbb{F}_q))$ maps by reduction mod p isomorphically to the group $E(\mathbb{F}_q)$. This is true for the prime to p parts for any lifting. It is true for the p-power parts for the canonical lifting because the p-divisible group of $\mathbb{E}$ is the product of the étale group $E(\overline{\mathbb{F}_q})[p^\infty]$ with the dual twisted form of μ_{p^∞}. Because p is odd, the second factor has no (nontrivial) unramified points, so none with values in $W((\overline{\mathbb{F}_q})$, and a fortiori none with values in $W(\mathbb{F}_q)$.

The second property we will use is that the q'th power Frobenius endomorphism $Frob_q$ of E lifts to an endomorphism $\mathbb{F}$ of $\mathbb{E}$. Any endomorphism of $\mathbb{E}$, in particular $\mathbb{F}$, maps the torsion subgroup of $\mathbb{E}(W(\mathbb{F}_q))$ to itself. As $Frob_q$ fixes each element of $E(\mathbb{F}_q)$, it follows that $\mathbb{F}$ fixes each torsion point in $\mathbb{E}(W(\mathbb{F}_q))$. [If $\mathbb{P}$ is a torsion point upstairs, $\mathbb{P}$ and $\mathbb{F}(\mathbb{P})$ have the same reduction, so must be equal.]

Let us denote by $A_q \in W(\mathbb{F}_q)$ the action of $\mathbb{F}$ on the free $W(\mathbb{F}_q)$-module of rank one $H^1(\mathbb{E}, \mathcal{O}_{\mathbb{E}})$, and by $B_q \in W(\mathbb{F}_q)$ the action of $\mathbb{F}$ on the free $W(\mathbb{F}_q)$-module of rank one $H^0(\mathbb{E}, \Omega^1_{\mathbb{E}/W(\mathbb{F}_q)})$. One knows that A_q mod p is a_q, so A_q is a p-adic unit, one knows that $B_q = q/A_q$, and one knows that

$$n_q = q + 1 - A_q - B_q.$$

Let us denote by $\mathbb{P} \in \mathbb{E}(W(\mathbb{F}_q))$ the unique torsion point lifting $P \in E(\mathbb{F}_q)$. On $\mathbb{E}$, we have the divisor $\mathbb{D} := [\mathbb{P}] - [0_{\mathbb{E}}]$, and now $n_q\mathbb{D}$ is principal. So there exists an invertible function $\mathbb{G}$ on $\mathbb{E} \setminus \{0_E, \mathbb{P}\}$ which is a $W(\mathbb{F}_q)$-basis of the free $W(\mathbb{F}_q)$-module of rank one

$$H^0(E, (I(\mathbb{P}) \otimes I(0_{\mathbb{E}})^{-1})^{\otimes n_q}).$$

We now choose a torsion point $\mathbb{P}_1$ in $\mathbb{E}(W(\mathbb{F}_q))$ other than $\mathbb{P}$ or $0_{\mathbb{E}}$. For example, we could take $\mathbb{P}_1$ to be $-\mathbb{P}$. We further choose a uniformizing parameter T at $\mathbb{P}_1$, so the formal completion $\mathbb{E}^\vee$ of $\mathbb{E}$ along $\mathbb{P}_1$ is the formal Spec of $W(\mathbb{F}_q))[[T]]$. Because $\mathbb{P}_1$ is everywhere disjoint from both $\mathbb{P}$ and $0_{\mathbb{E}}$, we can choose $\mathbb{G}$ so that its formal expansion along $\mathbb{P}_1$ lies in $1 + W(\mathbb{F}_q))[[T]]$.

In terms of a Weierstrass equation for $\mathbb{E}$ lifting that of E, we have the differential of the third kind $\omega_{\mathbb{D}}$, and we know that $n_q\omega_{\mathbb{D}} - dG/G$ is everywhere holomorphic on $\mathbb{E}$, say

$$n_q\omega_{\mathbb{D}} = dG/G + \omega(\mathbb{D}).$$

We now work in the group $H^1_{DR}(\mathbb{E}^\vee, (p))$ defined as the cokernel of p times the exterior differentiation map

$$pd : TW(\mathbb{F}_q))[[T]] \to \Omega^1_{\mathbb{E}^\vee/W(\mathbb{F}_q)} = TW(\mathbb{F}_q))[[T]]dT/T,$$

cf. [Ka-CrCohDMJS, Thm. 5.1.6 with I there the ideal (p)]. Because the point $\mathbb{P}_1$ is fixed by $\mathbb{F}$, $\mathbb{F}$ is a pointed endomorphism of $\mathbb{E}^\vee$, and so $\mathbb{F}$ acts on this cohomology group. However, it will be convenient to consider instead the pointed endomorphism $\mathbb{F}_1$ of $\mathbb{E}^\vee$ given by $T \mapsto T^q$. According to [Ka-CrCohDMJS, Thm. 5.1.6], the two maps $\mathbb{F}$ and $\mathbb{F}_1$, being congruent mod p, induce the **same** map on this cohomology group.

We now introduce another map, $\mathbb{V}$, on the terms of the de Rham complex, given by

$$\mathbb{V}(\sum_{n\geq 1} a_n T^n) := \sum_{n\geq 1} a_{nq} T^n dT/T,$$

$$\mathbb{V}(\sum_{n\geq 1} a_n T^n dT/T) := \sum_{n\geq 1} a_{nq} T^n dT/T.$$

We have the following lemma, whose proof is left to the reader.

Lemma 11.3. *For any $f \in TW(\mathbb{F}_q))[[T]]$, we have*

$$\mathbb{V}(df) = qd(\mathbb{V}(f)).$$

This map $\mathbb{V}$ is an ad hoc formal lifting of the Cartier operator $\mathcal{C}_q$. [It is **not** a lifting of the Verschiebung V_q of E. Indeed, from the relation $V_q Frob_q = q$, we see that V_q acts on $E(\mathbb{F}_q)$ as multiplication by q, so only the points in $E(\mathbb{F}_q)$ of order dividing $q-1$ are fixed by V_q. Our problematic points P in $E(\mathbb{F}_q)$ are those of p-power order, so are certainly not fixed by V_q. So although V_q **does** lift to an endomorphism of $\mathbb{E}$, this lifting will in general not even act on our $\mathbb{E}^\vee$.]

Choose a $W(\mathbb{F}_q)$-basis ω of $H^0(\mathbb{E}, \Omega^1_{\mathbb{E}/W(\mathbb{F}_q)})$. Then we have the identity of differential forms on $\mathbb{E}$

$$\mathbb{F}^\star(\omega) = (q/A_q)\omega.$$

So in $H^1_{DR}(\mathbb{E}^\vee, (p))$, we have this same relation.On this cohomology group, $\mathbb{F}_1$ induces the same map as $\mathbb{F}$, so we have the relation

$$\mathbb{F}_1^\star(\omega) = (q/A_q)\omega \text{ in } H^1_{DR}(\mathbb{E}^\vee, (p)).$$

Lemma 11.4. *We have the relation*

$$\mathbb{V}(\omega) = A_q\omega \text{ in } H^1_{DR}(\mathbb{E}^\vee, (p)).$$

Proof. Indeed, write the formal expansion of ω along $\mathbb{P}_1$, say

$$\omega = \sum_{n\geq 1} a_n T^n dT/T, \quad \text{coefficients } a_n \in W(\mathbb{F}_q).$$

Its pullback by $\mathbb{F}_1$ is

$$\mathbb{F}_1^\star(\omega) = q\sum_{n\geq 1} a_n T^{nq} dT/T.$$

So the assertion that $\mathbb{F}_1^\star(\omega) = (q/A_q)\omega$ in $H^1_{DR}(\mathbb{E}^\vee, (p))$ means that

$$(q/A_q)\sum_{n\geq 1} a_n T^n dT/T - q\sum_{n\geq 1} a_n T^{nq} dT/T$$

is d of some series in $pTW(\mathbb{F}_q)[[T]]$. If we look at the coefficient of nq, the exactness means precisely that

$$(q/A_q)a_{nq} - qa_n \text{ lies in } pqnW(\mathbb{F}_q).$$

Because A_q is a p-adic unit, we may rewrite this as a congruence

$$a_{nq} \equiv A_q a_n \bmod pnW(\mathbb{F}_q).$$

These congruences means precisely that

$$\mathbb{V}(\omega) = A_q\omega \text{ in } H^1_{DR}(\mathbb{E}^\vee, (p)).$$

$\square$

Lemma 11.5. *For any function* $G \in 1+TW(\mathbb{F}_q)[[T]]$, *writing* $\mathrm{dlog}(G) := dG/G$, *we have the relation*

$$(1-\mathbb{V})(\mathrm{dlog}(G)) = 0 \text{ in } H^1_{DR}(\mathbb{E}^\vee, (p)).$$

Proof. Write G as an infinite product

$$G = \prod_{n \geq 1} \frac{1}{1 - b_n T^n}, \quad \text{coefficients } b_n \in W(\mathbb{F}_q).$$

Then $\mathrm{dlog}(G)$ is the sum

$$\mathrm{dlog}(G) = \sum_{n \geq 1} \sum_{d \geq 1} n(b_n)^d T^{nd} dT/T.$$

Since the space of exact forms is T-adically complete, it suffices to show that for each $n \geq 1$, and for any $b \in W(\mathbb{F}_q)$, $1 - \mathbb{V}$ kills $\mathrm{dlog}(1/(1 - bT^n))$, i.e., that

$$((1 - \mathbb{V})(\sum_{d \geq 1} nb^d T^{nd} dT/T) = 0 \text{ in } H^1_{DR}(\mathbb{E}^\vee, (p)).$$

Equivalently, we must show that for the series

$$\sum_{a \geq 1} c_a T^a := \sum_{d \geq 1} nb^d T^{nd} - \sum_{d \geq 1 \ \text{such that } q|nd} nb^d T^{nd/q},$$

its coefficients satisfy the congruences

$$c_a \equiv 0 \mod paW(\mathbb{F}_q).$$

There are two cases to consider. Suppose first that a can be written as $a = ne$. Then a can be written uniquely as nd/q, with $d = qe$.Then

$$c_a = nb^e - nb^d.$$

Here $d = qe$, $pa = pne$, and we must show that

$$nb^e - nb^{qe} \equiv 0 \bmod pneW(\mathbb{F}_q).$$

If e is prime to p, it suffices to show that for any $b \in W(\mathbb{F}_q)$ (here our b^e), we have

$$b \equiv b^q \bmod pW(\mathbb{F}_q),$$

which is obviously true, since $W(\mathbb{F}_q)/pW(\mathbb{F}_q)$ is $\mathbb{F}_q$. If p divides e, write $e = e_0 p^f$ with e_0 prime to p. In this case it suffices to show that for any $b \in W(\mathbb{F}_q)$ (here our b^{e_0}), we have

$$b^{p^f} \equiv b^{qp^f} \bmod p^{f+1}W(\mathbb{F}_q).$$

If b is divisible by p, both sides vanish mod $p^{f+1}W(\mathbb{F}_q)$, this is just the statement that $p^f \geq f + 1$. If b is a unit in $W(\mathbb{F}_q)$, write is as the product $\zeta_{q-1}(1 + pc)$ of its Teichmuller part $\zeta_{q-1} \in \mu_{q-1}(W(\mathbb{F}_q))$ with a principal unit $1 + pc \in 1 + pW(\mathbb{F}_q)$. The Teichmuller parts of b^{p^f} and of b^{qp^f} agree, so we may divide through by them and reduce to the case when b is $1 + pc$. Now successively use the fact that for any $n \geq 1$,

p'power maps $1 + p^n W(\mathbb{F}_q)$ to $1 + p^{n+1} W(\mathbb{F}_q)$ (in fact isomorphically for $p \geq 3$). So both sides lie in $1 + p^{f+1} W(\mathbb{F}_q)$, and we are done.

Suppose next that $a = nd/q$ but a cannot be written as ne. Then $c_a = nb^d$, and we must show that

$$nb^d \equiv 0 \bmod p(nd/q)W(\mathbb{F}_q),$$

or equivalently

$$qb^d \equiv 0 \bmod pdW(\mathbb{F}_q).$$

To say that a cannot be written as ne is to say that q does not divide d, which is to say that $\mathrm{ord}_p(q) > \mathrm{ord}_p(d)$. But in this case $\mathrm{ord}_(q) \geq \mathrm{ord}_p(pd)$, i.e., $q \equiv 0 \bmod pdW(\mathbb{F}_q)$, so again the assertion is obvious. □

With these preliminaries, we now finish the proof of the theorem. We start with the identical relation

$$n_q \omega_{\mathbb{D}} = dG/G + \omega(\mathbb{D}).$$

We apply $1 - \mathbb{V}$ to it, and view the result in $H^1_{DR}(\mathbb{E}^\vee, (p))$. There are f and g in $TW(\mathbb{F}_q)[[T]]$ such that we have the identical relations

$$(1 - \mathbb{V})(dG/G) = pdf, \quad \mathbb{V}(\omega(\mathbb{D})) = A_q \omega(\mathbb{D}) + pdg.$$

So we have an identical relation

$$n_q(1 - \mathbb{V})(\omega_{\mathbb{D}}) = (1 - \mathbb{V})(dG/G) + (1 - \mathbb{V})(\omega(\mathbb{D})) =$$
$$= pdf + (1 - A_q)\omega(\mathbb{D}) - pdg.$$

Now apply $\mathbb{V}$ to this relation. We get

$$n_q \mathbb{V}(1 - \mathbb{V})(\omega_{\mathbb{D}}) = p\mathbb{V}(df) - p\mathbb{V}(dg) + (1 - A_q)(A_q \omega(\mathbb{D}) + pdg).$$

As we have already remarked, $V(df) = qd(\mathbb{V}(f))$, $V(dfg = qd(\mathbb{V}(g))$, so we have

$$n_q \mathbb{V}(1 - \mathbb{V})(\omega_{\mathbb{D}}) = pqd(\mathbb{V}(f - g)) + (1 - A_q)A_q \omega(\mathbb{D}) + (1 - A_q)pdg.$$

Remember that A_q is a p-adic unit. From the formula

$$n_q := \#E(\mathbb{F}_q) = (1 - A_q)(1 - q/A_q)$$

we see that n_q and $1 - A_q$ have the same ord_p; their ratio is the p-adic unit $1 - q/A_q$. Moreover, from the Hasse bound we see that n_q cannot be divisible by pq. In other words, pq/n_q lies in $pW(\mathbb{F}_q)$. So dividing through by n_q, we get

$$\mathbb{V}(1 - \mathbb{V})(\omega_{\mathbb{D}}) = (pq/n_q)d(\mathbb{V}(f - g)) + ((1 - A_q)/n_q)A_q \omega(\mathbb{D}) + ((1 - A_q)/n_q)pdg.$$

Remember that $(1 - A_q)/n_q = 1/(1 - q/A_q)$ is 1 mod p. So when we reduce mod p, we get a relation of differential forms on $\mathbb{F}_q[[T]]$,

$$\mathcal{C}_q(1 - \mathcal{C}_q)(\omega_D) = a_q \omega(D).$$

Recalling that $(1 - \mathcal{C}_q)(\omega_D)$ is itself everywhere holomorphic on E, we have

$$\mathcal{C}_q(1 - \mathcal{C}_q)(\omega_D) = a_q(1 - \mathcal{C}_q)(\omega_D).$$

As a_q is nonzero in $\mathbb{F}_q$ (in fact it is 1), we may divide through by it to get

$$(1 - \mathcal{C}_q)(\omega_D) = \omega(D).$$

As this equality of global forms on E holds in the formal completion at P_1, it holds identically. □

References

[Gnedenko] Gnedenko, B. V. The theory of probability. Translated from the fourth Russian edition by B. D. Seckler. Chelsea Publishing Co., New York, 1967. 529 pp.

[Ka-Alg] Katz, N., Algebraic solutions of differential equations (p-curvature and the Hodge filtration). Inv. Math. 18 (1972), 1-118.

[Ka-CrCohDMJS] Katz, N., Crystalline cohomology, Dieudonné modules, and Jacobi sums. Automorphic forms, representation theory and arithmetic (Bombay, 1979), pp. 165246, Tata Inst. Fund. Res. Studies in Math., 10, Tata Inst. Fundamental Res., Bombay, 1981.

[Ka-Eis] Katz, N., The Eisenstein measure and p-adic interpolation. Amer. J. Math. 99 (1977), no. 2, 238-311.

[Ka-Gal] Katz, N.,Galois properties of torsion points on abelian varieties. Invent. Math. 62 (1981), no. 3, 481-502.

[Ka-Wief] Katz, N., Wieferich past and future.

[Maz-Mes] Mazur, B. and Messing, W., Universal Extensions and One Dimensional Crystalline Cohomoiogy, Springer Lecture Notes in Mathematics 370, 1974.

[Mes] Messing, W., The universal extension of an abelian variety by a vector group. Symposia Mathematica, Vol. XI (Convegno di Geometria, INDAM, Rome, 1972), pp. 359-372. Academic Press, London, 1973.

[Mes-BT] Messing, W., The Crystals Associated to Barsotti-Tate Groups: with Applications to Abelian Schemes, Springer Lecture Notes in Mathematics 264, 1972.

[PFTV] Press, W., Flannery, B., Teukolsky, S., Vetterling, W., Numerical recipes in C. The art of scientific computing. Cambridge University Press, Cambridge, 1988. xxii+735 pp.

[Zarhin] Zarhin, Yuri G., Very simple 2-adic representations and hyperelliptic Jacobians, Mosc. Math. J. 2 (2002), no. 2, 403-431.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu