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 $0 \in C(k)$, $J_{C/k} := \text{Pic}^0_{C/k}$ 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 $P_1, \ldots, P_r$ 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 $\nabla$ on $\mathcal{L}$, namely a $k$-linear map

$$\nabla : \mathcal{L} \to \mathcal{L} \otimes \Omega^1_{C/k}$$
which satisfies the Liebnitz 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
\[ (\mathcal{L}_1, \nabla_1) \otimes (\mathcal{L}_2, \nabla_2) = (\mathcal{L}_1 \otimes \mathcal{L}_2, \ nabla_1 \otimes \text{id}_2 + \text{id}_1 \otimes \nabla_2). \]

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 \(\ell\) 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 \(J_C(k) \to J_C(k)\). 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 \(\mathcal{L}_D := \otimes_i I(P_i)^{n_i}\) 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 meromorphic differential \(\omega_D\), holomorphic outside the support of \(D\), which has only simple poles at the points \(P_i\), with residue \(n_i\) at \(P_i\). 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 \(\text{ord}_{P_i}(f) \geq n_i\) at each \(P_i\) in \(U\), then although \(df\) has \(\text{ord}_{P_i}(f) \geq n_i - 1\) at each \(P_i\) in \(U\), \(df - f\omega_D\) again has \(\text{ord}_{P_i}(df - f\omega_D) \geq n_i\) 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 \(\omega_D\), 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 \( \bar{k} \). 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 \( \infty \) (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 \( \infty \), 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 \( \infty \) (because \( x \) has
a double pole at \( \infty \) and \( y \) has a pole of order \( 2g + 1 \) at \( \infty \)). 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 \( \infty \), the function \((y + b)/x\) has a pole of order \( 2g - 1 \), so our
differential \( \omega_{[P]-[\infty]} \) has a simple pole at \( \infty \). As the sum of the residues
is 0, our differential must have residue \(-1\) at \( \infty \). \( \square \)

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 \( \omega_{P-\infty} - \omega_{-P-\infty} \).

\( \square \)

4. **The situation over a base scheme**

Let \( S \) be a scheme, and \( C/S \) a proper smooth curve, structural map \( f: C \rightarrow S \), with geometrically connected fibres of genus \( g \geq 1 \), given with a marked section \( 0 \in C(S) \). Denote by \( J_{C/S} := Pic_{C/S}^0 \) its Jacobian, an abelian scheme over \( S \). The group \( J_{C/S}(S) \) is the group of equivalence classes of invertible sheaves \( \mathcal{L} \) on \( C \) 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 \( f^*\mathcal{M} \) 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 \( \nabla \) on \( \mathcal{L} \), namely an \( S \)-linear map

\[
\nabla: \mathcal{L} \rightarrow \mathcal{L} \otimes \Omega^1_{C/S}
\]

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

\[
(\mathcal{L}_1, \nabla_1) \otimes (\mathcal{L}_2, \nabla_2) = (\mathcal{L}_1 \otimes \mathcal{L}_2, \ n_1 \otimes id_2 + id_1 \otimes \nabla_2).
\]

One knows that when \( S \) is affine, any \( \mathcal{L} \) which is fibre-by-fibre of degree zero admits an \( S \)-linear connection [REFERENCE FOR THIS!!], and the difference of any two is a global one-form \( \omega \in H^0(C, \Omega^1_{C/S}) \). 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 \((f^*\mathcal{M}, d_{C/S})\), 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 \( J^\#_{C/S}(S) \). When \( S \) is affine, we thus have a short exact sequence

\[
0 \rightarrow H^0(C, \Omega^1_{C/S}) \rightarrow J^\#_{C/S}(S) \rightarrow J_{C/S}(S) \rightarrow 0,
\]

In the special case when we are given a finite list of pairwise disjoint sections \( P_1, ..., P_r \in C(S) \), and integers \( n_1, ..., n_r \) with \( \sum_i n_i = 0 \), a connection on \( \otimes_i f_i(P_i)^{\otimes_n} \) is given by a differential in \( H^0(C, \Omega^1_{C/S}(\log(\sum_i P_i))) \) 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 \( S = \text{Spec}(A) \), and that \( C/S \) 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

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

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 \( A := \mathbb{Z}[1/2\Delta(f)] \) we have the following structures:

1. a hyperelliptic curve \( C/A \), defined by the equation \( y^2 = f(x) \),
2. pairwise disjoint sections \( P, -P, \) and \( \infty \) in \( C(A) \),
3. the point \( \mathbb{P} \) in \( J_{C/A}(A) \) which is the class of \( I(P) \otimes I(\infty)^{-1} \),
4. the connection on \( \mathbb{P} \) given by \( \omega_{[P] - [\infty]} \),
5. the point \( \mathbb{P}^\# := (\mathbb{P}, \omega_{[P] - [\infty]}) \) in \( J_{C/A}^\#(A) \), which lies over the point \( \mathbb{P} \) in in \( J_{C/A}(A) \),
6. the point \( (2\mathbb{P})^\# := (2\mathbb{P}, \omega_{[P] - [-P]}) \) in \( J_{C/A}^\#(A) \), which lies over the point \( 2\mathbb{P} \) in in \( J_{C/A}(A) \).

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 \( C_p/\mathbb{F}_p \), the point \( P_p \) on it, the point \( \mathbb{P}_p \) in \( J_{C_p}^\#(\mathbb{F}_p) \), and the point \( \mathbb{P}_p^\# \) in \( J_{C_p}^\#(\mathbb{F}_p) \) lying over it.
We also have the point $2\mathbb{P}_p$ in $J_{C_p}(\mathbb{F}_p)$ 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 $H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})$; let us call it

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

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

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

$$\omega_p(2\mathbb{P}_p^\#)$$
in $H^0(C_p, \Omega^1_{C_p/\mathbb{F}_p})$.

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

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

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

$$(1/p)\mathbb{H}/\mathbb{H} \subseteq \mathbb{H} \otimes_\mathbb{Z} \mathbb{R}/\mathbb{Z}$$
we view these elements $\omega_p(\mathbb{P}_p^\#)/p, \omega_p(2\mathbb{P}_p^\#)/p$ as lying in the $g$-dimensional compact real torus $\mathbb{H} \otimes_\mathbb{Z} \mathbb{R}/\mathbb{Z}$.

**Conjecture 6.1.** Suppose the cyclic subgroup generated by $\mathbb{P}$ is Zariski dense in $J_{C/A} \otimes_\mathbb{A} \mathbb{C}$. Then both of the sequences $\{\omega_p(\mathbb{P}_p^\#)/p\}_p$ and $\{\omega_p(2\mathbb{P}_p^\#)/p\}_p$, 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 $J_{C/A} \otimes_\mathbb{A} \mathbb{C}$? 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 $y^2 = x^\ell + a$, $\ell$ 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 $P$ is not of finite order in $J_{C}(A)$, it suffices to exhibit two distinct odd primes $p_1$ and $p_2$, both prime to $b\Delta(f)$, such that the images of $P$ in the two groups $J_{C/A}(\mathbb{F}_{p_1})$ and $J_{C/A}(\mathbb{F}_{p_2})$ 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 $g \geq 1$, $P$ a point in $J_{C}(\mathbb{C})$ and $P^\#$ a point in $J_{C}^\#(\mathbb{C})$ lying over $P$. Suppose that the cyclic group generated by $P$ is Zariski dense in $J_{C}$. Then the cyclic group generated by $P^\#$ is Zariski dense in $J_{C}^\#$.

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

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

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 $H^1(C, \mathcal{O}_C) \cong \text{Hom}_{\mathbb{C}}(H^0(C, \Omega^1_{C/\mathbb{C}}), \mathbb{C})$.

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

$$0 \to V \to G \to J_{C} \to 0,$$

with $V$ some vector subspace of $H^0(C, \Omega^1_{C/\mathbb{C}})$. If $V$ 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 $\phi$ from $H^0(C, \Omega^1_{C/\mathbb{C}})$ to $\mathbb{C}$ whose kernel contains $V$. This extension is simultaneously split (because $\phi$ kills $V$) and nontrivial (by the universal extension property). \qed
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 \( E/A \), 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 \( n_p := \#E(\mathbb{F}_p) \). 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 prime \( p \), the divisor \( n_p([P] - [\infty]) \) on \( E_p := \mathcal{E} \otimes_A \mathbb{F}_p \) is principal, so the divisor of some function \( g_p \) on \( E_p \). Then \((1/n_p)dg_p/g_p\) is a connection on \( \mathcal{L}_p := I(P) \otimes I(\infty)^{-1}|E_p \). In [Ka-Alg, Conjecture 7.5.11], we suppose chosen a connection \( \nabla \) 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 \( \nabla = \omega_{[P]-[\infty]} + adx/y \) for some \( a \in A \). We denote by \( \nabla_p \) 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 \( b_pdx/y \) 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 \( \nabla \), 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 \( E/\mathbb{Q} \), 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

\[
n_p\omega_{[P]-[\infty]} = dg_p/g_p + n_pbdx/y.
\]
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 \( \{N x_i\}_i \), 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.

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 \( \omega_p(P^\#)/p \) and \( \omega_p(2P^\#)/p \) for the first 330000 primes starting with 7, i.e., for all primes \( 7 \leq p \leq 4716091 \), and 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 \( 0 \leq x_1 \leq x_2 \ldots \leq x_N < 1 \), 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 \( \omega_p(P_t^\#)/p \) (respectively the point \( \omega_p(2P_t^\#)/p \))
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 $\omega_D$ which is holomorphic except at the points $P_i$, and has simple poles at the $P_i$ with $\text{res}_{P_i}(\omega_D) = e_i$. 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 $\omega_D$ 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 $(1 - \mathcal{C})(\omega_D) = c_p dx/y$.  \qed
Remark 9.2. In the higher genus case, with \( n_p := \# J_C(\mathbb{F}_p) \), we have \( n_p \omega_D = d g_p / g_p + \omega(D) \) for some holomorphic differential \( \omega(D) \). The above argument gives
\[
n_p(1 - C)(\omega_D) = (1 - C)(\omega(D)).
\]
If we know how to compute \((1 - C)(\omega_D)\), then we know \((1 - C)(\omega(D))\). If \( n_p \) is prime to \( p \), we can proceed as follows. On the one hand, \( n_p \mod p \) is the determinant \( \text{det}(1 - C| H^0(C, \Omega^1_C)) \), and so \( 1 - C \) on \( H^0(C, \Omega^1_C) \) is invertible. So we can compute \( (\omega_D) \) (because we know \((1 - C)(\omega(D))\)).

Thus we have two computational problems, first to compute \((1 - C)(\omega_D)\) on a given differential of the third kind, namely \( \omega_D \), and second to invert \((1 - C)(\omega_D)\) on the space \( H^0(C, \Omega^1_C) \) of differentials of the first kind. We will discuss these problems further in the next section.

We now return to the elliptic case, and 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 nonzero, and \( P \in E(\mathbb{F}_p) \) is \((0, b)\) with \( b \neq 0 \). Write \( f(x) = A_0 + A_1 x + A_2 x^2 + x^3 \), with coefficients \( A_i \in \mathbb{F}_p \). Write
\[
f(x)^{(p-1)/2} = \sum_i B_i x^i.
\]
Then
\[
\omega([P] - [-P]) = -b B_p dx/y
\]
and
\[
\omega([P] - [\infty]) = (1/2) \omega([P] - [-P]) = (-b B_p/2) dx/y.
\]

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 \( 1 - C \) kills \( dx/x \), so we have
\[
(1 - C)(\omega_{[P] - [\infty]} = (1/2)(1 - C)(\omega_{[P] - [-P]}),
\]
and we apply the previous lemma.

It remains to compute \((1 - C)(\omega_{[P] - [-P]} = b(1 - C)(dx/xy)\). 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 $\Psi$ operator on $\mathbb{F}_p$-polynomials

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

we have

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

Thus

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

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 $\Psi(1-f(x)^{(p-1)/2}) = -B_p x$, and hence

$$(1-C)(dx/xy) = -B_p dx/y, \quad (1-C)(bdx/xy) = -bB_p dx/y.$$

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 $b^2 + A_1 x$ 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 $\chi_2$ 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 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 \( \mathbb{P}^1 \).

10. Computational problems in the higher genus case

We now consider 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 \( D \) either \([P] - [\infty] \) or \([P] - [-P] \), we have

\[
n_p \omega_D = dg/g + \omega(D).
\]

As \( 1 - C \) kills \( dg/g \), we still have

\[
n_p(1 - C)(\omega_{[P] - [\infty]}) = (1 - C)(\omega([P] - [\infty])),
\]

\[
n_p(1 - C)(\omega_{[P] - [-P]}) = (1 - C)(\omega([P] - [-P])).
\]

The differential \( \omega_{[P] - [\infty]} \) is

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

and the differential \( \omega_{[P] - [-P]} \) is

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

Thus

\[
(1 - C)(\omega_{[P] - [\infty]}) = (1/2)b(1 - C)(dx/xy),
\]

\[
(1 - C)(\omega_{[P] - [-P]}) = b(1 - C)(dx/xy).
\]

Exactly as in the proof of Lemma 8.3, we have

**Lemma 10.1.** Write

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

For \( C \) the Cartier operator, we have

\[
(1 - C)(dx/xy) = -\sum_{j=1}^g B_{jp} x^j dx/xy.
\]

So we get
Corollary 10.2. We have the formulas

\[(1 - C)(\omega([P] - [\infty])) = -n_p (b/2) \left( \sum_{j=1}^{g} B_{jp} x^j dx/xy \right),\]

\[(1 - C)(\omega([P] - [-P])) = -n_p b \left( \sum_{j=1}^{g} B_{jp} x^j dx/xy \right).

If \(n_p\) is nonzero mod \(p\), we have the formulas

\[(1/n_p)(1 - C)(\omega([P] - [\infty])) = -(b/2) \left( \sum_{j=1}^{g} B_{jp} x^j dx/xy \right),\]

\[(1/n_p)(1 - C)(\omega([P] - [-P])) = -b \left( \sum_{j=1}^{g} B_{jp} x^j dx/xy \right).

Here \(n_p\) mod \(p\) is \(\det(1 - C|H^0(C, \Omega^1_C))\). So if \(n_p\) is prime to \(p\), then \(1 - C\) is invertible on \(H^0(C, \Omega^1_C)\), and the inverse of \((1/n_p)(1 - C)\) on that space is, matricially, the transpose of the matrix of cofactors of \((1 - C)\) on that space.

Recall the standard computation of the Cartier operator on \(H^0(C, \Omega^1_C)\), in the basis \(\{x^i dx/xy\}_{i=1,...,g}\).

Lemma 10.3. For \(i = 1,...,g\), we have

\[C(x^i dx/xy) = \sum_{j=1}^{g} B_{j-p} x^j dx/xy.\]

The upshot is that when \(g \geq 2\), and under the assumption that \(n_p\) is prime to \(p\), we can in principle compute \(\omega([P] - [\infty])\) and \(\omega([P] - [-P])\). But to do this, it seems that we need to compute the \(g(g+1)\) coefficients \(B_{j-p}\) for \(j = 1,...,g, i = 0,...,g\), and to compute the transpose of the matrix of cofactors of the \(g \times g\) matrix \(Id_g - (B_{j-p})_{i,j=1,...,g}\). We do not know how to do this efficiently.

References


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