LINEAR INDEPENDENCE IN LINEAR SYSTEMS ON ELLIPTIC CURVES

BRADLEY W. BROCK, BRUCE W. JORDAN, BJORN POONEN, ANTHONY J. SCHOLL, AND JOSEPH L. WETHERELL

Abstract. Let $E$ be an elliptic curve, with identity $O$, and let $C$ be a cyclic subgroup of odd order $N$, over an algebraically closed field $k$ with char $k \nmid N$. For $P \in C$, let $s_P$ be a rational function with divisor $N \cdot P - N \cdot O$. We ask whether the $N$ functions $s_P$ are linearly independent. For generic $(E, C)$, we prove that the answer is yes. We bound the number of exceptional $(E, C)$ when $N$ is a prime by using the geometry of the universal generalized elliptic curve over $X_1(N)$. The problem can be recast in terms of sections of an arbitrary degree $N$ line bundle on $E$.

1. Introduction

Fix $N \geq 1$ and an algebraically closed field $k$ such that char $k \nmid N$. Let $E$ be an elliptic curve over $k$. Let $C \subset E$ be a cyclic subgroup of order $N$.

Let $\mathcal{L}$ be a degree $N$ line bundle on $E$. Since Pic$^0(E)$ is divisible, there exist points $P \in E$ such that $\mathcal{O}(N \cdot P) \simeq \mathcal{L}$, or equivalently, such that there exists a global section $s_P$ of $\mathcal{L}$ whose divisor of zeros is $N \cdot P$. The set of such $P$ is a coset $E[N]'$ of $E[N]$. Let $C' \subset E[N]'$ be a coset of $C$. Then $\#C' = N$. On the other hand, dim $\Gamma(E, L) = N$ by the Riemann-Roch theorem.

Question 1.1. Are the sections $s_P$ for $P \in C'$ linearly independent in $\Gamma(E, L)$?

The answer is sometimes yes, sometimes no.

Example 1.2. Let $O \in E(k)$ be the identity. Let $\mathcal{L} = \mathcal{O}(N \cdot O)$ and $C' = C$. Then $s_P$ is a rational function on $E$ with divisor $(s_P) = N \cdot P - N \cdot O$. Question 1.1 asks whether the $s_P$ for $P \in C$ are linearly independent, i.e., whether they form a basis of $\Gamma(E, \mathcal{O}(N \cdot O))$.

Proposition 1.3. The answer to Question 1.1 depends only on $(E, C)$, not on the choice of degree $N$ line bundle $\mathcal{L}$ or coset $C'$ or $s_P$ for $P \in C'$. More precisely, the codimension of $\text{Span}\{s_P : P \in C'\}$ in $\Gamma(E, \mathcal{L})$ depends only on $(E, C)$.

We will prove Proposition 1.3 in Section 3.

The pair $(E, C)$ corresponds to a $k$-point on the classical modular curve $Y_0(N)$.

Theorem 1.4. Let $N$ be an odd positive integer such that char $k \nmid N$. Then for all but finitely many $(E, C) \in Y_0(N)(k)$, Question 1.1 has a positive answer.
We next work towards a quantitative version of Theorem 1.4, at least for prime $N$. Let $c_{(E,C)}$ be the codimension in Proposition 1.3, and let $D = \sum_{(E,C)} c_{E,C} (E, C) \in \text{Div} Y_0(N)$.

**Theorem 1.5.** Let $N > 3$ be a prime with $\text{char } k \nmid N$. There exist effective divisors $D_1$ and $D_2$ on $Y_0(N)$ such that $D = D_1 + 2D_2$ with

\[
\deg D_1 \leq (N^2 - 1)/24 \\
\deg D_2 \leq (N - 3)(N^2 - 1)/48.
\]

**Conjecture 1.6.** If $\text{char } k = 0$, then $D_1$ and $D_2$ are reduced and disjoint, and the inequalities in Theorem 1.5 are equalities.

**Remark 1.7.** Conjecture 1.6 is equivalent to the claim that for prime $N > 3$ and $\text{char } k = 0$, there are exactly $(N^2 - 1)/24$ points $(E, C) \in Y_0(N)(k)$ with $c_{E,C} = 1$, exactly $(N - 3)(N^2 - 1)/48$ points with $c_{E,C} = 2$, and no points with $c_{E,C} > 2$.

The primes $N > 3$ for which the genus of $X_0(N)$ is 0 are 5, 7, and 13; for these we checked that Conjecture 1.6 is true, using methods to be described in Section 10. There we will also show that Conjecture 1.6 sometimes fails when $\text{char } k > 0$.

2. Notation

Let $\mu$ be the group of roots of unity in $k$. Fix a primitive $N$th root of unity $\zeta \in k$.

If $C$ is a finite abelian group with $\text{char } k \nmid \#C$, and $V$ is a $k$-representation of $C$, and $\chi : C \to k^\times$ is a character, define the $\chi$-isotypic subspace

\[ V^\chi := \{ v \in V : cv = \chi(c) v \text{ for all } c \in C \}. \]

Let $X$ be a regular $k$-variety. Let $\text{Div} X$ be its divisor group. Now suppose in addition that $X$ is integral. Let $k(X)$ be its function field. If $f \in k(X)^\times$, let $(f)_X = (f) \in \text{Div} X$ be its divisor. For each irreducible divisor $Z$ on $X$, let $v_Z$ be the associated valuation. A finite morphism of regular integral curves $\phi : X \to Y$ induces a homomorphism $\phi_* : \text{Div} X \to \text{Div} Y$ (sending each point to its image) compatible with the norm homomorphism $\phi_* : k(X)^\times \to k(Y)^\times$.

3. Codimension is independent of choices

**Proof of Proposition 1.3.** Fix $(E, C)$. Once $\mathcal{L}$ and $C'$ are also fixed, each $s_P$ is determined up to scaling by an element of $k^\times$, which does not change the span.

For each $Q \in E(k)$, let $\tau_Q : E \to E$ be the morphism sending $x$ to $x + Q$. Pulling back by $\tau_Q$ shows that the codimension for $(\mathcal{L}, C')$ is the same as for $(\tau_Q^* \mathcal{L}, \tau_Q^{-1}(C'))$. If $Q \in E[N]$, then $\tau_Q^* \mathcal{L} \cong \mathcal{L}$ but $\tau_Q^{-1}(C')$ can be any other coset of $C'$ in $E[N]$; thus the codimension is independent of $C'$.

As $Q$ ranges over $E(k)$, the line bundle $\tau_Q^* \mathcal{L}$ ranges over all degree $N$ line bundles; thus the codimension is independent of $\mathcal{L}$ too. \qed

4. Normalized functions

If $f \in k(E)^\times$ has divisor supported on $E[N]$, then $[N]_s(f) = 0$, so $[N]_s f \in k^\times$. Multiplying $f$ by a constant $\alpha \in k^\times$ multiplies $[N]_s f$ by $\alpha^{\deg[N]} = \alpha^{N^2}$. Call $f \in k(E)^\times$ normalized if there exists $N \geq 1$ such that $[N]_s f \in \mu$. In that case, $[N]_s f \in \mu$ for all multiples $N'$ of $N$. Therefore the normalized functions form a subgroup of $k(E)^\times$. Given a principal divisor
supported on torsion points, there exists a normalized function with that divisor, uniquely
determined up to multiplication by a root of unity. In particular, a normalized constant
rational function is an element of $\mu$. If $f$ is normalized and $P$ is a torsion point on $E$, then
$\tau_P^*f$ is normalized too.

5. Character-weighted combinations

From now on, we assume that $N$ is odd. View $C$ as a degree $N$ divisor on $E$. Choose
$\mathcal{L} := \mathcal{O}(C)$. The group $C$ acts on $\mathcal{L}$: each $P$ acts as $\tau_P^*$ on sections of $\mathcal{L}$. Since $N$ is odd,
$\mathcal{L} \simeq \mathcal{O}(N \cdot O)$. Choose $C' = C$. Choose sections $s_P$ as in Section \[1\]

If we view $s_O$ as a rational function on $E$, then $(s_O) = N \cdot O - C$. Assume that $s_O$
is normalized. For $P \in C' = C$, we may assume that $s_P := \tau_P^*s_O$. Then $\text{Span}\{s_P : P \in C\}$ is
the image of a $kC$-module homomorphism $kC \to \Gamma(E, \mathcal{L})$, so it decomposes as a direct sum of distinct
distinct characters. For each character $\chi: C \to k^\times$, the projection of $\text{Span}\{s_P : P \in C\}$
onto $\Gamma(E, \mathcal{L})^\chi$ is spanned by

$$g_\chi := \left(\sum_{P \in C} \chi(P)\tau_P^*\right)s_O = \sum_{P \in C} \chi(P)s_P.$$ 

Then $c_{E,C} = \#\{\chi: g_\chi = 0\}$.

**Lemma 5.1.** We have $[-1]^*s_O = s_O$.

**Proof.** The divisor $(s_O)$ is fixed by $[-1]^*$, so $s_O$ is an eigenvector of $[-1]^*$, with eigenvalue
$\pm 1$. Since $v_O(s_O)$ is even, the eigenvalue is 1. \(\square\)

**Lemma 5.2.** For each $\chi$, we have $[-1]^*g_\chi = g_{\chi^{-1}}$.

**Proof.** Apply

$$[-1]^*\left(\sum_{P \in C} \chi(P)\tau_P^*\right) = \left(\sum_{P \in C} \chi(P)\tau_P^*\right)[-1]^* = \left(\sum_{Q \in C} \chi(Q)\tau_Q^*\right)[-1]^*$$

to $s_O$ and use Lemma 5.1. \(\square\)

**Lemma 5.3.** We have $\prod_{P \in C} s_P \in \mu$.

**Proof.** It is a normalized rational function whose divisor is 0. \(\square\)

6. An almost canonical basis

Fix $(E, C)$. Let $\phi: E \to E'$ be an isogeny with kernel $C$. Let $\hat{\phi}: E' \to E$ be the dual
isogeny. The Weil pairing

$$e_\phi: \ker \phi \times \ker \hat{\phi} \to k^\times$$

is nondegenerate, so choosing $Q \in \ker \hat{\phi}$ is equivalent to choosing a character $\chi: C \to k^\times$, related via $\chi(P) = e_\phi(P, Q)$ for all $P \in C$. Let $C_\chi = \phi^*Q \in \text{Div} E$. Let $h_\chi$ be a normalized
function with $(h_\chi) = C_\chi - C$.

**Lemma 6.1.** For $P \in C$, we have $\tau_P^*h_\chi = \chi(P)h_\chi$.

**Proof.** This is the definition of $e_\phi(P, Q)$, which equals $\chi(P)$; see \cite{Sil09} Exercise 3.15(a). \(\square\)
Thus $0 \neq h_\chi \in \Gamma(E, \mathcal{L})^\chi$ for all $\chi$, but $\bigoplus_\chi \Gamma(E, \mathcal{L})^\chi$ is $N$-dimensional, so $\Gamma(E, \mathcal{L})^\chi = kh_\chi$. In particular, $g_\chi/h_\chi \in k$. Now
\[(1) \quad c_{E,C} = \#\{\chi : g_\chi = 0\} = \#\{\chi : g_\chi/h_\chi = 0\}.
\]

**Lemma 6.2.** For each $\chi$, we have $[-1]^*h_\chi \equiv h_{\chi^{-1}} \pmod{\mu}$.

**Proof.** Compare divisors, and observe that both sides are normalized. □

**Lemma 6.3.** For any $\chi$, we have $g_\chi/h_\chi \equiv g_{\chi^{-1}}/h_{\chi^{-1}} \pmod{\mu}$.

**Proof.** By Lemmas \[5.2\] and \[6.2\] $[-1]^*(g_\chi/h_\chi) \equiv g_{\chi^{-1}}/h_{\chi^{-1}} \pmod{\mu}$. On the other hand, $g_\chi/h_\chi$ is constant on $E$, so $[-1]^*(g_\chi/h_\chi) = g_\chi/h_\chi$. □

7. The universal elliptic curve

Given an elliptic curve $E$ over $k$ and a point $P \in E(k)$ of exact order $N$, we define $C$ as the subgroup generated by $P$. For $m \in \mathbb{Z}/NZ$, let $\chi : C \to k^\times$ be the character such that $\chi(P) = \zeta^m$, and set $g_m := g_\chi$ and $h_m := h_\chi$. We may assume that $h_0 = 1$.

Suppose that $N > 3$ and char $k \nmid N$. Then the moduli space $Y_1(N)$ parametrizing pairs $(E, P)$ is a fine moduli space (it can be viewed as an étale quotient of the affine curve $Y(N)$ constructed by Igusa [Igu59], because a pair $(E, P)$ consisting of an elliptic curve and a point of exact order $N > 3$ has no nontrivial automorphisms). Thus there is a universal elliptic curve $\mathcal{E} \to Y_1(N)$. The construction of $s_0$ makes sense on $\mathcal{E}$, except that normalizing it may require taking an $N$th root of an invertible function on $Y_1(N)$. Thus $s_0$ is a rational function not on the elliptic surface $\mathcal{E} \to Y_1(N)$, but on a pullback $\mathcal{E}' \to Y_1(N)'$ by some finite étale cover $Y_1(N)' \to Y_1(N)$. Then $s_0^n$ for some $n \geq 1$ lies in $k(\mathcal{E})^\times$, and $s_0$ itself may be identified with $1/n \otimes s_0^n \in \mathbb{Q} \otimes k(\mathcal{E})^\times$. Its divisor $(s_0)$ is then an element of $\mathbb{Q} \otimes \text{Div} \mathcal{E}$. Given $m \in \mathbb{Z}/NZ$, we may also define $g_m, h_m \in k(\mathcal{E})^\times$ and consider them as elements of $\mathbb{Q} \otimes k(\mathcal{E})^\times$. Its divisor on $Y_1(N)$ lies in $\text{Div} Y_1(N)$, not just $\mathbb{Q} \otimes \text{Div} Y_1(N)$, since $Y_1(N)' \to Y_1(N)$ is finite étale.

8. The universal generalized elliptic curve

We continue to assume $N > 3$. Complete $Y_1(N)$ to a smooth projective curve $X_1(N)$ over $k$. One can recover from [DR73] IV.4.14 and VI.2.7 that $\mathcal{E} \to Y_1(N)$ can be completed to a “universal generalized elliptic curve” $\pi : \mathcal{E} \to X_1(N)$. The following description of the cusps of $X_1(N)$ and the associated Tate curves is well-known; see [DR73] VII.2 and [FJ95] §3.1.

The cusps on $X_1(N)$ are in bijection with
\[
\prod_{d|N} \frac{(\mathbb{Z}/d\mathbb{Z})^\times \times (\mathbb{Z}/e\mathbb{Z})^\times}{\{±1\}},
\]
where $e = N/d$ in each term. The integer $e$ equals the ramification index of $X_1(N) \to X(1)$ at the cusp, and is called the width of the cusp. The cusp represented by $(d, a, b)$, where $0 \leq a < d$ and $0 < b < e$ and $\gcd(a, d) = \gcd(b, e) = 1$, has a uniformizer $q$ and a punctured formal neighborhood $\text{Spec} k((q))$ above which is the Tate curve analytically isomorphic to $(\mathbb{G}_m/q^\mathbb{Z}, \zeta^aq^b) \in Y_1(N)(k((q)))$. This Tate curve specializes above the cusp itself to an $e$-gon consisting of irreducible components $Z_i \simeq \mathbb{P}^1$ indexed by $i \in \mathbb{Z}/e\mathbb{Z}$ such that $0 \in Z_i$ is
attached to $\infty \in \mathbb{Z}_{i+1}$ for all $i$. We choose the coordinate $t: \mathbb{Z}_i \rightarrow \mathbb{P}^1$ for each $i$ such that a point $t_iq^j + \sum_{j>i} t_j q^j \in \mathbb{G}_m/q^\mathbb{Z}$ with $t_i \in k^\times$ specializes to $t_i \in \mathbb{G}_m \subseteq \mathbb{P}^1 \simeq \mathbb{Z}_i \subset \pi^{-1}(y)$. For each cusp $y$, define $F_y := \pi^*y = \sum_i Z_i \in \text{Div} \mathcal{F}$. 

9. Divisors 

Given a rational function $f$ on $\mathcal{F}$ whose divisor on $\mathcal{F}$ is known, the divisor of $f$ on $\mathcal{F}$ is determined up to addition of a linear combination of the $F_y$. We now explain how to compute it, modulo the ambiguity. Fix a cusp $y$ of $X_1(N)$, and let $q$ be a uniformizer at $y$, and let $Z_0, \ldots, Z_{e-1}$ be the components of $\pi^{-1}(y)$. The valuations $n_i := v_{Z_i}(f)$ can be simultaneously computed, modulo addition of a constant independent of $i$, by the relations $(f/q^u_i).Z_i = 0$ for all $i$, which amount to linear equations in the $n_i$. Let us make these equations explicit. In the case where the zeros and poles of $f$ specialize to smooth points of $\pi^{-1}(y)$, let $r_i$ be the number of them specializing to a point of $Z_i$, counted with multiplicity, with poles counted as negative. In the equation $(f/q^u_i).Z_i = 0$, only $Z_{i+1}, Z_{i-1}$, and the horizontal divisors in $(f)$ meet $Z_i$, so the equation says 

$$(n_{i+1} - n_i) + (n_{i-1} - n_i) + r_i = 0.$$ 

There is one such equation for each $i$. Solving this system of $e$ equations yields all the $n_i$ up to a common additive constant, since the solutions to the corresponding homogeneous system are the arithmetic progressions that are periodic modulo $N$, i.e., constant sequences. If in addition, $f$ is normalized, then $\sum n_i = 0$; now the $n_i$ are uniquely determined.

The above procedure can be applied also to any $f \in \mathbb{Q} \otimes k(\mathcal{F})^\times$, and in particular to the functions $s_p, g_m,$ and $h_m$. 

Lemma 9.1. For $f = s_O$, 

(a) At a cusp of $X_1(N)$ above $\infty \in X_0(N)$, we have $e = 1$, $n_0 = 0$, and $s_O|Z_0 = (1-t)^N/(1-t^N)$ in $\mathbb{Q} \otimes k(\mathcal{F})^\times$.

(b) At a cusp of $X_1(N)$ above $0 \in X_1(N)$, we have $e = N$, $n_i = (N^2 - 1)/12 - i(N-1)/2$ for $0 \leq i < N$, and $\left(q^{(N^2-1)/2} s_O\right)|_{Z_{(N-1)/2}}$ has a zero at $\infty$ and not at $0$, while $\left(q^{(N^2-1)/24} s_O\right)|_{Z_{(N-1)/2}}$ has a zero at $0$ and not at $\infty$.

Proof.

(a) A cusp above $\infty$ has a punctured neighborhood above which is the Tate curve $\mathbb{G}_m/q^\mathbb{Z}$ with cyclic subgroup $\mu_N$, specializing to a 1-gon. In fact, the relation $\prod_{R \in C} \tau_{R}s_O = 1$ in $\mathbb{Q} \otimes k(\mathcal{F})^\times$ from Lemma 5.3 implies $N n_0 = 0$, so $n_0 = 0$.

The order $N$ zero of $s_O$ specializes to 1, and the $N$ poles of $s_O$ specialize to the $N$th roots of unity, so $s_O|Z_0$ is a nonzero scalar times $(1-t)^N/(1-t^N)$.

Since $s_O$ is normalized, $[N]s_O \in \mu$. On the other hand, the morphism $[N]$ specializes to the $N$th power map on $Z_0 \simeq \mathbb{P}^1$, which pushes $(1-t)^N/(1-t^N)$ forward to the norm $\prod_{\omega \in \mu_N} (1-\omega t)^N/(1-(\omega t)^N) = (1-t)^N/(1-t^N)^N = 1$. By the previous two sentences, the scalar of the previous paragraph is in $\mu$.

(b) A cusp above $0$ has a punctured neighborhood above which is the Tate curve $\mathbb{G}_m/q^{N\mathbb{Z}}$ with cyclic subgroup generated by $q$. The $N$ zeros specialize to $Z_0$, but the $N$ poles specialize to different $Z_i$, one pole per $Z_i$. Thus $r_0 = N-1$ and $r_i = -1$ for $i \neq 0$.

On the other hand, $\prod_{R \in C} \tau_{R}s_O = 1$ implies $\sum n_i = 0$. Together these imply that
$n_i = (N^2 - 1)/12 - i(N - i)/2$ for $0 \leq i < N$. The most negative of these are $n_{(N-1)/2}$ and $n_{(N+1)/2}$, which are both $-(N^2 - 1)/24$.

The divisor of \( q^{(N^2 - 1)/24} s_0 \) on $Z_{(N-1)/2}$ is
\[
(n_{(N+1)/2} - n_{(N-1)/2})(0) + (n_{(N-3)/2} - n_{(N-1)/2})(\infty) - (1) = (\infty) - (1).
\]

Similarly, the divisor of \( q^{(N^2 - 1)/24} s_0 \) on $Z_{(N+1)/2}$ is
\[
(n_{(N+3)/2} - n_{(N+1)/2})(0) + (n_{(N-1)/2} - n_{(N+1)/2})(\infty) - (1) = (0) - (1). \quad \square
\]

**Corollary 9.2.**
(a) At the cusp above $\infty \in X_0(N)$ given by \( \langle G_m/q^z, \zeta \rangle \), we have $g_0|z_0 = N$, and for $m \neq 0$ we have $g_m|z_0 = (-1)^m N(1 - t^N) t^m/(1 - t^{2N})$, in $\mathbb{Q} \otimes k(z_0)^\times$.

(b) At a cusp above $0$, for any $m, i \in \mathbb{Z}/N\mathbb{Z}$, we have $v_{Z_i}(g_m) = -(N^2 - 1)/24$.

**Proof.**
(a) Up to a root of unity which may be ignored, $s_0|z_0 = (1 - t)^N/(1 - t^{2N})$ by Lemma 9.1(a).
Translation by $P$ restricts to multiplication by $\zeta$ on $z_0$, so
\[
s_{jP}|z_0 = \tau_{-jP}^* s_0|z_0 = (1 - \zeta^{-j} t)^N/(1 - (\zeta^{-j} t)^N)
= \frac{1}{1 - tN} \sum_{i=0}^N \binom{N}{i} (-1)^i \zeta^{-ij} t^i
= \sum_{j=0}^{N-1} \zeta^{mj} \frac{1}{1 - tN} \sum_{i=0}^N \binom{N}{i} (-1)^i \zeta^{-ij} t^i
= \frac{1}{1 - tN} \sum_{i=0}^N (-1)^i \binom{N}{i} t^i \sum_{j=0}^{N-1} \zeta^{(m-i)j}
= \frac{1}{1 - tN} \sum_{i=0}^N (-1)^i \binom{N}{i} t^i \begin{cases} N, & \text{if } m - i \equiv 0 \pmod{N}; \\ 0, & \text{otherwise}. \end{cases}
\]

If $m = 0$, then only the terms with $i = 0$ or $i = N$ are nonzero, and the sum becomes $(1 - t^N)N$. If $m \neq 0$, then only the term with $i = m$ is nonzero, and the sum becomes $(-1)^m N(m) t^m N$.

(b) The translation action of $C$ acts simply transitively on the set of components $Z_i$ above the cusp. Thus the numbers $v_{Z_i}(s_{jP})$ for $j = 0, \ldots, N - 1$ equal the numbers $v_{Z_i}(s_0)$ for $i' = 0, \ldots, N - 1$ in some order, which are described by Lemma 9.1(b). Hence in the sum $g_m = \sum_{j=0}^{N-1} \zeta^{mj} s_{jP}$ there are exactly two terms with the most negative valuation along $Z_i$, so $v_{Z_i}(\zeta^{mj} s_{jP}) = -(N^2 - 1)/24$ for $j = j_1$ and $j = j_2$, say. The last two claims in Lemma 9.1(b) imply that one of the functions $(q^{(N^2 - 1)/24} \zeta^{mj} s_{jP})|z_i$ for $j = j_1$ and $j = j_2$ has a zero at $\infty$ and not at $0$, while the other has a zero and not at $\infty$, so their sum is nonzero on $Z_i$. Thus $v_{Z_i}(g_m) = -(N^2 - 1)/24$ too. \quad \square

**Proof of Theorem 1.4.** We may work on the finite cover $Y_1(N)'$ of $Y_0(N)$ defined in Section 7. By Corollary 9.2(b), no $g_m$ is identically zero. Hence each function $g_m/h_m$ on $Y_1(N)'$ has
only finitely many zeros. Equation (1) shows that outside the union of these zeros, \( c_{E,C} = 0 \); i.e., the \( f_p \) are linearly independent.

Let \( G := g_1g_2\cdots g_{N-1} \) and \( H := h_1h_2\cdots h_{N-1} \) in \( \mathbb{Q} \otimes \kappa(\mathcal{E})^\times \). The divisor of \( H \) on \( \mathcal{E} \) is \( \mathcal{E}[N] - NC \).

**Lemma 9.3.** For \( f = H \)

(a) At a cusp of \( X_1(N) \) above \( \infty \in X_0(N) \), we have \( e = 1 \) and \( n_0 = -(N^2 - 1)/12 \).

(b) At a cusp of \( X_1(N) \) above \( 0 \in X_0(N) \), we have \( n_i = 0 \) for all \( i \).

**Proof.** We work on the universal generalized elliptic curve over \( X(N) \), whose degenerate fibers are all \( N \)-gons, so that the zeros and poles of \( H \) do not specialize to the singular points of fibers. As usual, let \( Z_0, \ldots, Z_{N-1} \) be the components above a cusp; let \( n'_i = v_{Z_i}(H) \). The normalization implies that the product of all translates of \( H \) by \( N \)-torsion points is in \( \mu \), so \( \sum n_i = 0 \).

(a) We have \( r_0 = -N(N - 1) \) and \( r_i = N \) for \( i \neq 0 \). The \( r_i \) here are \( -N \) times the \( r_i \) in the proof of Lemma 9.1(b), so the resulting \( n'_i \) are also multiplied by \( -N \); that is, \( n'_i = -N(N^2 - 1)/12 + Ni(N - i)/2 \) for \( 0 \leq i < N \). Finally, \( X(N) \rightarrow X_1(N) \) has ramification index \( N \) at cusps above \( \infty \), so \( n_0 = n'_0 / N \).

(b) Each \( h_m \) has one zero and one pole specializing to each \( Z_i \); so \( r_i = 0 \) for all \( i \). Thus \( n'_i = 0 \) for all \( i \), so \( n_i = 0 \) for all \( i \). □

**Lemma 9.4.** Let \( N > 3 \) be prime.

(a) The element \( g_0 = g_0 / h_0 \in \mathbb{Q} \otimes \kappa(\mathcal{E})^\times \) lies in \( \mathbb{Q} \otimes \kappa(X_0(N))^\times \), its valuations at the cusps of \( X_0(N) \) are \( v_\infty(g_0) = 0 \) and \( v_0(g_0) = -(N^2 - 1)/24 \), and its divisor on \( Y_0(N) \) is effective and of degree \( (N^2 - 1)/24 \).

(b) The \( G/H = \prod_{m=1}^{N-1}(g_m/h_m) \in \mathbb{Q} \otimes \kappa(\mathcal{E})^\times \) lies in \( \mathbb{Q} \otimes \kappa(X_0(N))^\times \), with \( v_\infty(G/H) \geq (N^2 - 1)/12 \) and \( v_0(G/H) = -(N - 1)(N^2 - 1)/24 \). The divisor of \( G/H \) on \( Y_0(N) \) is of degree \( (N^2 - 1)(N^2 - 1)/24 \), and it is twice an effective divisor on \( Y_0(N) \).

**Proof.** Each \( g_m/h_m \) is constant on each elliptic curve fiber, so \( g_m/h_m \) lies in \( \mathbb{Q} \otimes \kappa(X_1(N))^\times \). The Galois group of \( X_1(N) \rightarrow X_0(N) \) fixes \( g_0 / h_0 \) and permutes the \( g_m/h_m \), so \( g_0 / h_0 \) and \( G/H \) are in \( \mathbb{Q} \otimes \kappa(X_0(N))^\times \).

(a) The valuations \( v_\infty(g_0) \) and \( v_0(g_0) \) are determined by Corollary 9.2. On the other hand, (a power of) \( g_0 = g_0 / h_0 \) is regular on \( Y_0(N) \), and its divisor on the projective curve \( X_0(N) \) has degree 0.

(b) The valuation of \( G/H \) along the component \( Z_0 \) above a cusp of \( X_1(N) \) above \( \infty \) is \( \!\!\geq \left( \sum_{m=1}^{N-1} 0 \right) - \left( -(N^2 - 1)/12 \right) = (N^2 - 1)/12 \), by Corollary 9.2(a) and Lemma 9.3(a); thus \( v_\infty(G/H) \geq (N^2 - 1)/12 \). The valuation of \( G/H \) along any component \( Z_i \) above a cusp above 0 is \( \left( \sum_{m=1}^{N-1} -(N^2 - 1)/24 \right) - 0 = -(N - 1)(N^2 - 1)/24 \) by Corollary 9.2(b) and Lemma 9.3(b); thus \( v_0(G/H) = -(N - 1)(N^2 - 1)/24 \).

Since the divisor of \( G/H \) on \( X_0(N) \) has degree 0, its divisor on \( Y_0(N) \) has degree at most \( -(N^2 - 1)/12 + (N - 1)(N^2 - 1)/24 = (N - 3)(N^2 - 1)/24 \).

That it is twice an effective divisor can be checked on the étale cover \( Y_1(N)' \) of Section 7. There, each \( g_m/h_m \) is regular, and Lemma 6.3 shows that \( g_m/h_m = g_m/h_m \), so \( G/H \) is a square. □
Proof of Theorem 1.5. Let $D_{Y_1(N)}$ be the pullback of $D$ under $Y_1(N) \to Y_0(N)$. Let $(g_m/h_m)_{\text{red}} \in \text{Div} Y_1(N)$ be the reduced divisor whose support equals the divisor of $g_m/h_m$ on $Y_1(N)$. Equation (1) says that $D_{Y_1(N)} = \sum_{m=0}^{N-1} (g_m/h_m)_{\text{red}}$. The divisors $D_{Y_1(N),1} := (g_0/h_0)_{\text{red}}$ and $D_{Y_1(N),2} = \sum_{m=1}^{(N-1)/2} (g_m/h_m)_{\text{red}} = \frac{1}{2} \sum_{m=1}^{N-1} (g_m/h_m)_{\text{red}}$ are invariant under the Galois group of $Y_1(N) \to Y_0(N)$, so they are pullbacks of divisors $D_1$ and $D_2$ on $Y_0(N)$. We have $D_{Y_1(N)} = D_{Y_1(N),1} + 2D_{Y_1(N),2}$, so $D = D_1 + 2D_2$.

The degree of $D_1$ is bounded by the degree of $g_0/h_0$ on $Y_0(N)$, which is $(N^2 - 1)/24$ by Lemma 9.4(a). Similarly, the degree of $2D_2$ is bounded by the degree of $G/H$ on $Y_0(N)$, which is at most $(N - 3)(N^2 - 1)/24$ by Lemma 9.4(b). \hfill \Box

10. Examples

Let $N > 3$ be prime. On the Tate curve over $k((q))$ analytically isomorphic to $\mathbb{G}_m/q^Z$, we can write down a function with prescribed divisor in terms of theta functions in $u$ and $q$, where $u$ is the coordinate on $\mathbb{G}_m$. In this way, we express the elements $s_p$, $g_m$, and $h_m$ in terms of $u$ and $q$ and we compute the $q$-expansions of the rational functions $g_0/h_0$ and $G/H$ on $X_0(N)$.

Now suppose in addition that the genus of $X_0(N)$ is 0; that is, $N \in \{5,7,13\}$. Let $\eta(q) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$. Then the function $(N^{1/2}\eta(q^N)/\eta(q))^{24/(N-1)}$ is the $q$-expansion of a rational function $t$ on $X_0(N)$ with $k(t) = k(X_0(N))$ such that $t$ has a zero at the cusp $\infty$ and a pole at the cusp 0. Because of Lemma 9.4, this lets us compute $g_0/h_0$ and $G/H$ as polynomials $f_1(t)$ and $t^{(N^2-1)/2} f_2(t)$ whose zeros with $t \neq 0$ give the points $(E,C) \in Y_0(N)$ with $c_{E,C} > 0$; call these points exceptional. Moreover, in these cases, using an expression for $j$ in terms of $t$, we may take the $k(t)/k(j)$ norm and take numerators to obtain polynomials $F_1(j)$ and $F_2(j)$ (determined up to scalar multiple) whose zeros are the $j$-invariants of the $E$ such that $c_{E,C} > 0$ for some $C \subset E$.

For $N \in \{5,7,13\}$, we found that the polynomials $f_1(t)$ and $f_2(t)$ are of degrees $(N^2 - 1)/24$ and $(N - 3)(N^2 - 1)/48$ and have disjoint distinct roots in $\overline{Q}$ (in fact, they are irreducible over $Q$); this verifies Conjecture 1.6 for these values of $N$. In fact, $F_1(j)$ and $F_2(j)$ had the same properties.

Example 10.1. Let $N = 5$. Then

\[ f_1(t) = t + 5 \]
\[ f_2(t) = t + 10 \]
\[ F_1(j) = j - 1600 \]
\[ F_2(j) = 2j + 25. \]

Each of $f_1$ and $f_2$ has a unique zero, and these zeros are distinct, and they avoid the cusps (where $t = 0$ and $t = \infty$), except in characteristic 2 (we always exclude characteristic 5). Thus in characteristics $\neq 2,5$, we have $c_{E,C} = 0$ except for one $(E,C)$ with $c_{E,C} = 1$ and one $(E,C)$ with $c_{E,C} = 2$, so the conclusion of Conjecture 1.6 for $N = 5$ holds in characteristics $\neq 2,5$. In characteristic 2, we have $c_{E,C} = 0$ except for one $(E,C)$ with $c_{E,C} = 1$, so the conclusion of Conjecture 1.6 fails.

Moreover, in characteristics $\neq 2,5$, the two exceptional $(E,C)$ have $j$-invariants 1600 and $-25/2$, which are distinct except in characteristics 3 and 43. In characteristics 3 and 43, we
find that $c_{E,C} = 0$ always except that the $E$ with $j(E) = 1600 = -25/2$ has two exceptional subgroups $C_1$ and $C_2$, with $c_{E,C_1} = 1$ and $c_{E,C_2} = 2$.

**Example 10.2.** Let $N = 7$. Then

$$
\begin{align*}
f_1(t) &= t^2 + 7t + 7 \\
f_2(t) &= t^4 + 21t^3 + 168t^2 + 588t + 735 \\
F_1(j) &= j^2 - 1104j - 288000 \\
F_2(j) &= 15j^4 - 28857j^3 + 20163177j^2 - 5403404499j - 141176604743
\end{align*}
$$

and the constant terms, discriminants, and resultants factor as follows:

$$
\begin{align*}
f_1(0) &= 7 \\
f_2(0) &= 3 \cdot 5 \cdot 7^2 \\
\text{Disc}(f_1) &= 3 \cdot 7 \\
\text{Disc}(f_2) &= -3^3 \cdot 7^6 \\
\text{Res}(f_1, f_2) &= 7^4 \\
\text{Disc}(F_1) &= 2^8 \cdot 3^3 \cdot 7^3 \\
\text{Disc}(F_2) &= -3 \cdot 7^{18} \cdot 43^2 \cdot 139^2 \cdot 421^2 \cdot 591751^2 \\
\text{Res}(F_1, F_2) &= 5 \cdot 7^{12} \cdot 47 \cdot 3491 \cdot 5939 \cdot 244603.
\end{align*}
$$

The values of $f_1(0)$, $f_2(0)$, $\text{Disc}(f_1)$, $\text{Disc}(f_2)$ show that in all characteristics $\neq 3, 5, 7$, we have $c_{E,C} = 0$ except for two $(E, C)$ with $c_{E,C} = 1$ and four with $c_{E,C} = 2$, so the conclusion of Conjecture 1.6 for $N = 7$ holds in characteristics $\neq 3, 5, 7$. In characteristic 3, we have $c_{E,C} = 0$ except that $c_{E,C} = 1$ for one $(E, C)$ (corresponding to the double root $t = 1$ of $f_1$, where $j(E) = 0$). In characteristic 5, we have $c_{E,C} = 0$ except for two $(E, C)$ with $c_{E,C} = 1$ and only three $(E, C)$ with $c_{E,C} = 2$.

Moreover, excluding characteristic 7 as always, the exceptional $(E, C)$ have distinct values of $j(E)$ except in characteristics 2, 43, 47, 139, 241, 3491, 5939, 244603, and 591751, for which there are exactly two exceptional $(E, C)$ sharing the same $j(E)$. In characteristic 2, these two have $c_{E,C} = 1$ (since 2 divides $\text{Disc}(F_1)$ but not $\text{Disc}(f_1)$). In characteristics 43, 139, 241, and 591751, these two have $c_{E,C} = 2$ (since these primes divide $\text{Disc}(F_2)$ but not $\text{Disc}(f_2)$). In characteristics 47, 5939, and 244603, these two have $c$-values 1 and 2, respectively (since these primes divide $\text{Res}(F_1, F_2)$ but not $\text{Res}(f_1, f_2)$).

**Example 10.3.** Let $N = 13$. Then $\deg f_1 = \deg F_1 = 7$ and $\deg f_2 = \deg F_2 = 35$, and each of the four polynomials has distinct zeros in $\overline{\mathbb{Q}}$. The analysis is similar to that for $N = 5$ and $N = 7$, except that we were unable to factor $\text{Disc}(F_2)$ completely.

**Acknowledgment**

We thank Hyuk Jun Kweon for a comment on a draft of the article.
REFERENCES

[DR73] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349 (French). MR0337993

[FJ95] Gerd Faltings and Bruce W. Jordan, Crystalline cohomology and GL(2, Q), Israel J. Math. 90 (1995), no. 1-3, 1–66, DOI 10.1007/BF02783205. MR1336315

[Igu59] Jun-ichi Igusa, Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves, Amer. J. Math. 81 (1959), 453–476, DOI 10.2307/2372751. MR104669

[Sil09] Joseph H. Silverman, The arithmetic of elliptic curves, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540-1966, USA
Email address: bwbrock@idaccr.org

Department of Mathematics, Baruch College, The City University of New York, One Bernard Baruch Way, New York, NY 10010-5526, USA
Email address: bruce.jordan@baruch.cuny.edu

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: poonen@math.mit.edu
URL: http://math.mit.edu/~poonen/

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
Email address: a.j.scholl@dpmms.cam.ac.uk

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121-1969, USA