COMPOSITIO MATHEMATICA

DAVID A. COX
WALTER R. PARRY

Torsion in elliptic curves over $k(t)$

Compositio Mathematica, tome 41, nº 3 (1980), p. 337-354
<http://www.numdam.org/item?id=CM_1980__41_3_337_0>

COMPOSITIO MATHEMATICA, Vol. 41, Fasc. 3, 1980, pag. 337–354.

TORSION IN ELLIPTIC CURVES OVER $k(t)$

David A. Cox and Walter R. Parry

Let k be a field of characteristic $p \geq 0$, $p \neq 2, 3$, and let t be transcendental over k. The purpose of this paper is to study the groups

$$E(k(t))'_{\text{tor}} = \{x \in E(k(t))_{\text{tor}} : p \text{ does not divide the order of } x\}$$

where E is an elliptic curve over $k(t)$ with nonconstant j-invariant. Since $E(k(t))$ is finitely generated (the Mordell–Weil theorem), $E(k(t))'_{\text{tor}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ where n and m are positive integers with $p \nmid n$ and $m \mid n$. A complete description of the possible groups is given in Theorem 5.1.

We approach this problem in a classical way, using the subgroups $\Gamma_m(n)$, $m|n$, of $\mathrm{SL}(2, \mathbb{Z})$ defined by

$$\Gamma_m(n) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod n,\, b \equiv 0 \bmod m\right\}.$$

$\Gamma_m(n)$ acts on the upper half plane $\mathfrak{H}$ as usual, and the quotient $Y_m(n) = \Gamma_m(n)\backslash\mathfrak{H}$ is related to moduli problems of elliptic curves containing a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ (we make this precise in §1). The basic idea is that the possible groups $E(\mathbb{C}(t))_{\text{tor}}$ are those $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ for which $X_m(n) = \Gamma_m(n)\backslash\mathfrak{H}^*$ has genus 0. The methods of Deligne and Rapoport then allow us to generalize to an arbitrary field k of characteristic not 2 or 3.

The first section defines a level (n, m) structure on an elliptic curve over a base, and uses [2] to solve the resulting (coarse) moduli problem and relate it to $\Gamma_m(n)$. §2 is preliminary to §3, which is a

0010-437X/80/060337-18 $00.20/0

catalog of the properties of $\Gamma_m(n)$, and §4 applies this to the fine moduli problem, studying the universal curves for level (n, m) structures (these exist in most cases). Then §5 puts this all together to prove the classification theorem. An appendix contains a theorem, used in §4, which is a nice extension of a representability result in [2, VI.2].

The usual ways of writing $\Gamma_n(n)$, $Y_n(n)$ and $X_n(n)$ are $\Gamma(n)$, $Y(n)$ and $X(n)$, and we will use the latter. Note that when $m = 1$, our notation agrees with standard notation.

We would like to thank Barry Mazur for several useful suggestions.

§1

In this section we make extensive use of [2]. Let n and m be positive integers with $n \geq 2$ and $m \mid n$. A level (n, m) structure on a generalized elliptic curve $E \to S$ (see [2, II.1.12] for a definition) is an S-inclusion of groups

$$\alpha : \mathbb{Z}/n\mathbb{Z} \times C_m \to E$$

such that:

1. C_m is locally, in the étale topology, isomorphic to $(\mathbb{Z}/m\mathbb{Z})_S$, and
2. the image of α meets every irreducible component of every geometric fiber of $E \to S$.

To relate this to [2], let H be the subgroup of $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ defined by:

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & * \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}) : b \equiv 0 \bmod m \right\}.$$

Then, from [2, IV.3], we get the algebraic stack $\mathcal{M}_H^0[1/n]$ and its compactification (relative to $\mathbb{Z}[1/n]$) $\mathcal{M}_H[1/n]$. These objects have the following interpretation:

Proposition 1.1: *$\mathcal{M}_H^0[1/n]$ (resp. $\mathcal{M}_H[1/n]$) is the algebraic stack classifying equivalence classes of level (n, m) structures on elliptic curves E over S (resp. generalized elliptic curves E over S), where two level (n, m) structures $\alpha : \mathbb{Z}/n\mathbb{Z} \times C_m \to E$ and $\alpha' : \mathbb{Z}/n\mathbb{Z} \times C'_m \to E$ are equivalent if there is an S-isomorphism $\eta : C_m \to C'_m$ such that $\alpha = \alpha' \circ (1 \times \eta)$.*

Proof: We first treat $\mathcal{M}_H^0[1/n]$. From [2, IV.3.2], a level H structure on E is an element α of $F_H(S)$, where F_H is the étale sheaf $H\backslash\underline{\mathrm{Iso}}_S(E_n, (\mathbb{Z}/n\mathbb{Z})^2_S)$. Such an α thus consists of an étale cover $\{S_i \to S\}_{i\in I}$ of S and isomorphisms $\alpha_i: (E_n)_{S_i} \to (\mathbb{Z}/n\mathbb{Z})^2_{S_i}$ such that for $i, j \in I$, there is an $h_{ij} \in \mathrm{Hom}(S_{ij}, H)$ ($S_{ij} = S_i \times_S S_j$) and a commutative diagram:

$$\begin{tikzcd} & (\mathbb{Z}/n\mathbb{Z})^2_{S_{ij}} \arrow[d, "h_{ij}"] \\ (E_n)_{S_{ij}} \arrow[ur, "\alpha_i"] \arrow[r, "\alpha_j"'] & (\mathbb{Z}/n\mathbb{Z})^2_{S_{ij}}. \end{tikzcd}$$

Let C be the subgroup of $(\mathbb{Z}/n\mathbb{Z})^2$ generated by $(0, n/m)$. Since

$$(1) \qquad H = \{h \in \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}): h(1,0) = (1,0), h(C) = C\},$$

the $\alpha_i^{-1}(1,0)$ (resp. the $\alpha_i^{-1}(C)$) patch to give us a map $(\mathbb{Z}/n\mathbb{Z})_S \to E$ (resp. an S-group scheme C_m and a map $C_m \to E$). Together, these define a level (n, m) structure whose equivalence class is well defined. Then, using (1), one sees that $F_H(S)$ is the set of equivalence classes of level (n, m) structures on E, as desired.

With this interpretation of $\mathcal{M}^0_H[1/n]$, the technique used in the proof of Construction 4.13 of [2, IV.4] easily gives us the desired interpretation of $\mathcal{M}_H[1/n]$. ∎

Let $M^0_H[1/n]$ and $M_H[1/n]$ denote the underlying algebraic spaces of $\mathcal{M}^0_H[1/n]$ and $\mathcal{M}_H[1/n]$ (i.e., they are coarse moduli spaces for the underlying functors of $\mathcal{M}^0_H[1/n]$ and $\mathcal{M}_H[1/n]$). As we will most often be working over a field k, we introduce the notation:

$$\mathcal{M}^0_k = \mathcal{M}^0_H[1/n] \times_{\mathbb{Z}} k$$

$$\mathcal{M}_k = \mathcal{M}_H[1/n] \times_{\mathbb{Z}} k$$

$$M^0_k = M^0_H[1/n] \times_{\mathbb{Z}} k$$

$$M_k = M_H[1/n] \times_{\mathbb{Z}} k.$$

(We are assuming that the characteristic of k does not divide n.) If there is any danger of confusion, we will write $\mathcal{M}^0_{n,m,k}$, $\mathcal{M}_{n,m,k}$, etc.

We can say the following about M^0_k and M_k:

PROPOSITION 1.2: *If k is a field whose characteristic does not divide n, then*:

1. *M_k is a smooth, geometrically connected curve whose genus is independent of k.*
2. *When $k = \mathbb{C}$,* there are isomorphisms:

$$M^0_{\mathbb{C}} \simeq Y_m(n) = \Gamma_m(n)\backslash\mathfrak{H}$$

$$M_{\mathbb{C}} \simeq X_m(n) = \Gamma_m(n)\backslash\mathfrak{H}^*.$$

($\Gamma_m(n)$ is defined in the introduction.)

PROOF: The map

$$M_H[1/n] \to \mathrm{Spec}(\mathbb{Z}[1/n])$$

is smooth and proper by [2, VI.6.7] and has connected geometric fibers by [2, IV.5.5] (note that $\det: H \to (\mathbb{Z}/n\mathbb{Z})^*$ is surjective). So we need only show that $M^0_{\mathbb{C}} \simeq \Gamma_m(n)\backslash\mathfrak{H}$. But this follows from [2, IV.5.3] since $\det: H \to (\mathbb{Z}/n\mathbb{Z})^*$ is surjective and $\Gamma_m(n)$ is the inverse image of $H \cap \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ in $\mathrm{SL}(2, \mathbb{Z})$. ■

A level (n, m) structure has a simple form when the base has a primitive mth root of unity:

PROPOSITION 1.3: *Let $\alpha: (\mathbb{Z}/n\mathbb{Z}) \times C_m \to E$ be a level (n, m) structure over S, where n is invertible on S and S has a primitive* mth *root of unity. Then there is an isomorphism $C_m \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})_S$ over S.*

PROOF: Pick an étale cover $\{S_i \to S\}_{i \in I}$ so that $(C_m)_{S_i}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})_{S_i}$. Let $e_n: E_n \times E_n \to \mu_n$ be the usual pairing, and let ζ_m be a primitive mth root of unity on S. Over each S_i there is a unique section u_i of C_m such that u_i generates C_m and $e_n(\alpha(1, 0), \alpha(0, u_i)) = \zeta_m$. Then the u_i patch to give an isomorphism $(\mathbb{Z}/m\mathbb{Z})_S \to C_m$ over S. ■

Thus, whenever S has a primitive mth root of unity, we will write a level (n, m) structure as

$$\alpha: (\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z})_S \to E.$$

§2

For every prime p, let Γ_p be the intersection of $\mathrm{SL}(2, \mathbb{Z})$ with an open subgroup of $\mathrm{SL}(2, \mathbb{Z}_p)$ such that $\Gamma_p = \mathrm{SL}(2, \mathbb{Z})$ for almost all p.

Let

$$\Gamma = \bigcap_p \Gamma_p,$$

which will be fixed throughout this section. Γ is a congruence subgroup of $\mathrm{SL}(2, \mathbb{Z})$, and let n be its level (so that $\Gamma(n) \subseteq \Gamma$). We also fix the subgroup

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\} \subseteq \mathrm{SL}(2, \mathbb{Z})$$

For our purposes, the way to understand Γ is to reduce modulo $\Gamma(n)$. We will use the well-known isomorphisms:

$$\mathrm{SL}(2, \mathbb{Z})/\Gamma(\mathrm{n}) \simeq \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z}) \simeq \prod_p \mathrm{SL}(2, \mathbb{Z}/p^{v_p(n)}\mathbb{Z})$$

induced by the natural maps, where v_p is the usual p-adic valuation. ϕ will denote map $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$, and ϕ_p will denote the map $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/p^{v_p(n)}\mathbb{Z})$.

We see that $\Gamma(p^{v_p(n)}) \subseteq \Gamma_p$, and it then follows that

$$\phi(\Gamma) \xrightarrow{\sim} \prod_p \phi_p(\Gamma_p)$$

is an isomorphism. We also have an isomorphism:

$$\phi(N) \xrightarrow{\sim} \prod_p \phi_p(N).$$

Combining all of this, we get a bijection

$$\phi(\Gamma)\backslash \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\phi(N) \simeq \prod_p \phi_p(\Gamma_p)\backslash \mathrm{SL}(2, \mathbb{Z}/p^{v_p(n)}\mathbb{Z})/\phi_p(N),$$

which, combined with the bijection

$$\Gamma\backslash \mathrm{SL}(2, \mathbb{Z})/N \xrightarrow{\sim} \phi(\Gamma)\backslash \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\phi(N), \tag{2}$$

shows that the natural map

$$\Gamma\backslash \mathrm{SL}(2, \mathbb{Z})/N \xrightarrow{\sim} \prod_p \Gamma_p \backslash \mathrm{SL}(2, \mathbb{Z})/N \tag{3}$$

is bijective.

The cusps of Γ can be identified with the set

$$\Gamma\backslash\mathrm{SL}(2,\mathbb{Z})/\pm N.$$

Every cusp has one or two preimages in $\Gamma\backslash\mathrm{SL}(2,\mathbb{Z})/N$, and this leads us to define the sets

$$C^{+}(\Gamma)=\{\text{cusps with two preimages in } \Gamma\backslash\mathrm{SL}(2,\mathbb{Z})/N\}$$

$$C^{-}(\Gamma)=\{\text{cusps with one preimage in } \Gamma\backslash\mathrm{SL}(2,\mathbb{Z})/N\}.$$

Since a double coset $\Gamma\sigma(\pm N)$ is in $C^{-}(\Gamma)$ if and only if $-\sigma$ is in $\Gamma\sigma N$, we see that:

$$\Gamma\sigma(\pm N)\in C^{-}(\Gamma) \text{ if and only if } \sigma^{-1}\Gamma\sigma\cap(-N)\neq\emptyset. \tag{4}$$

This proves the first two assertions of the following:

LEMMA 2.1:

1. *If $-1\notin\Gamma$, then $C^{+}(\Gamma)$ is the set of regular cusps and $C^{-}(\Gamma)$ is the set of irregular cusps (see* [3, *p.* 29)].
2. *If $-1\in\Gamma$, then $C^{+}(\Gamma)=\emptyset$.*
3. *If $-1\notin\Gamma$ and the level of Γ is odd, then $C^{-}(\Gamma)=\emptyset$.*

PROOF: To prove 3, assume that $C^{-}(\Gamma)\neq\emptyset$. By (4), there exist $\sigma\in\mathrm{SL}(2,\mathbb{Z})$ and $\gamma\in\Gamma$ so that $-\sigma^{-1}\gamma^{n}\sigma\in\Gamma(n)$, and this implies $-\gamma^{n}\in\Gamma(n)\subseteq\Gamma$. It follows that $-1\in\Gamma$. ∎

Let $\nu_\infty^{+}(\Gamma)=\#C^{+}(\Gamma)$ and $\nu_\infty^{-}(\Gamma)=\#C^{-}(\Gamma)$. Then $\nu_\infty(\Gamma)=\nu_\infty^{+}(\Gamma)+\nu_\infty^{-}(\Gamma)$ is the number of cusps of Γ, and

$$\#(\Gamma\backslash\mathrm{SL}(2,\mathbb{Z})/N)=2\nu_\infty^{+}(\Gamma)+\nu_\infty^{-}(\Gamma). \tag{5}$$

We can now compute $\nu_\infty(\Gamma)$ in terms of the Γ_p's:

THEOREM 2.2: *For each odd prime p, define $\epsilon(p)$ so that*

$$\epsilon(p)=\begin{cases}1 & \text{if } -1\in\Gamma_p\\ 2 & \text{if } -1\notin\Gamma_p.\end{cases}$$

Then

$$\nu_\infty(\Gamma) = \begin{cases} \prod_p \nu_\infty(\Gamma_p) & \text{if } -1 \in \bigcap_{p \text{ odd}} \Gamma_p \\ (\nu_\infty^+(\Gamma_2) + \frac{1}{2}\nu_\infty^-(\Gamma_2)) \prod_{p \text{ odd}} \epsilon(p)\nu_\infty(\Gamma_p) & \text{if } -1 \notin \bigcap_{p \text{ odd}} \Gamma_p. \end{cases}$$

PROOF: If $-1 \in \bigcap_{p \text{ odd}} \Gamma_p$, then we have an isomorphism

$$\phi(\pm\Gamma) \xrightarrow{\sim} \prod_p \phi_p(\pm\Gamma_p)$$

which then gives a bijection:

$$\phi(\pm\Gamma)\backslash \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\phi(N) \to \prod_p \phi_p(\pm\Gamma_p)\backslash \mathrm{SL}(2, \mathbb{Z}/p^{v_p(n)}\mathbb{Z})/\phi_p(N).$$

Interpreting this in terms of cusps (via the analog of (2) for $\pm\Gamma$ and $\pm\Gamma_p$) gives the desired formula.

When $-1 \notin \bigcap_{p \text{ odd}} \Gamma_p$, the last assertion of Lemma 2.1 implies that $C^-(\Gamma_p) = \emptyset$ for some odd prime p, and then $C^-(\Gamma) = \emptyset$. The result now follows from (3), (5) and the last two assertions of Lemma 2.1. ■

§3

We will study the group $\Gamma_m(n)$ of the introduction. We will assume $n \geq 2$.

LEMMA 3.1: *The index* $\mu(\Gamma_m(n)) = [\mathrm{SL}(2, \mathbb{Z}) : \pm\Gamma_m(n)]$ *is given by*:

$$\mu(\Gamma_m(n)) = \begin{cases} 3 & \text{if } (n, m) = (2, 1) \\ 6 & \text{if } (n, m) = (2, 2) \\ \dfrac{mn^2}{2} \prod_{p \mid n} (1 - 1/p^2) & \text{otherwise.} \end{cases}$$

PROOF: The index of $\Gamma(n)$ in $\Gamma_m(n)$ is n/m, and the index of $\pm\Gamma(n)$ in $\mathrm{SL}(2, \mathbb{Z})$ is well-known (see [3, p. 22]). ■

We next want to determine the number of cusps of $\Gamma_m(n)$. The first step is to prove:

PROPOSITION 3.2:

$$\#(\Gamma_m(n)\backslash \mathrm{SL}(2, \mathbb{Z})/N) = \prod_{p \mid n} (p-1)p^{v_p(nm)-2}(p + 1 + (p-1)v_p(n/m)).$$

PROOF: Identify $SL(2, \mathbb{Z})/N$ with the set

$$\left\{\begin{pmatrix} a \\ c \end{pmatrix} : a, c \in \mathbb{Z}, \gcd(a, c) = 1\right\}$$

via the map sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. Using [3, Lemma 1.41], it is easy to see that $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right)$ as above represent the same double coset of $\Gamma_m(n)\backslash SL(2, \mathbb{Z})/N$ if and only if

$$\begin{aligned} a &\equiv a' \bmod \gcd(n, mc) \\ c &\equiv c' \bmod n. \end{aligned} \tag{6}$$

Note that $\Gamma_m(n)$ has the form of the Γ in §2, i.e.,

$$\Gamma_m(n) = \bigcap_p \Gamma_p,$$

where each Γ_p equals $\Gamma_{p^r}(p^s)$ for some r and s, $r \leq s$. By (3), we are reduced to the case $n = p^s$, $m = p^r$.

For every i between 0 and s there are $\varphi(p^{s-i})$ different c's between 1 and p^s with $\gcd(c, p^s) = p^i$ (φ is the Euler φ-function). By (6), for every such c there are

$$\#\{a \in \mathbb{Z} : \gcd(a, c) = 1, 1 \leq a \leq \gcd(p^s, p^{r+i})\}$$
$$= \begin{cases} p^r & \text{if } i = 0 \\ \varphi(\gcd(p^s, p^{r+1})) & \text{if } 1 \leq i \leq s \end{cases}$$

double cosets represented by $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ for some a. Forming the appropriate sum over i and simplifying yields the formula:

$$\#(\Gamma_{p^r}(p^s)\backslash SL(2, \mathbb{Z})/N) = (p-1)p^{r+s-2}(p + 1 + (p-1)(s-r)). \quad \blacksquare$$

The next step is to determine $\nu_\infty^-(\Gamma_m(n))$:

PROPOSITION 3.3:

$$\nu_\infty^-(\Gamma_1(2)) = 2 \quad \nu_\infty^+(\Gamma_1(2)) = 0$$
$$\nu_\infty^-(\Gamma(2)) = 3 \quad \nu_\infty^+(\Gamma(2)) = 0$$
$$\nu_\infty^-(\Gamma_1(4)) = 1 \quad \nu_\infty^+(\Gamma_1(4)) = 2$$

and

$$\nu_\infty^-(\Gamma_m(n)) = 0 \quad \textit{in all other cases.}$$

PROOF: Let $\binom{a}{c}$, $\gcd(a, c) = 1$, represent a cusp in $C^-(\Gamma_m(n))$. Then $\binom{a}{c}$ and $-\binom{a}{c}$ represent the same double coset in $\Gamma_m(n)\backslash \mathrm{SL}(2, \mathbb{Z})/N$, so that

$$-a \equiv a \bmod \gcd(n, mc)$$
$$-c \equiv c \bmod n$$

by (6). Using the second congruence to simplify the first, we see that $n = 2$ or 4. It is easy to compute ν^+ and ν^- in these cases to complete the proof. ■

Propositions 3.2 and 3.3, together with the results of §2, give an immediate proof of:

PROPOSITION 3.4: *The number of cusps of $\Gamma_m(n)$ is given by*

$$\nu_\infty(\Gamma_1(2)) = 2$$
$$\nu_\infty(\Gamma(2)) = 3$$
$$\nu_\infty(\Gamma_1(4)) = 3$$

and in all other cases,

$$\nu_\infty(\Gamma_m(n)) = \tfrac{1}{2} \prod_{p \mid n} (p-1)p^{v_p(nm)-2}(p + 1 + (p-1)v_p(n/m)). \qquad ■$$

Next, we consider elements of finite order in $\Gamma_m(n)$:

PROPOSITION 3.5:
1. $\Gamma_1(2)$ *has exactly two conjugacy classes of elliptic elements, all of which have order* 4.
2. $\Gamma_1(3)$ *has exactly two conjugacy classes of elliptic elements, all of which have order* 3.
3. *For* $(n, m) \neq (2, 1)$ *or* $(3, 1)$, $\Gamma_m(n)$ *has no elliptic elements.*

Since -1 is in $\Gamma_m(n)$ if and only if $n = 2$, we get:

COROLLARY 3.6: *$\Gamma_m(n)$ is torsion-free if and only if* $(n, m) \neq (2, 1)$, $(2, 2)$ *or* $(3, 1)$.

PROOF OF PROPOSITION 3.5: By [3, §1.4], every elliptic element of $\mathrm{SL}(2, \mathbf{Z})$ is conjugate to one of the following:

$$\pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \pm\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \pm\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Trace considerations now show that $\Gamma_m(n)$ has no elliptic elements for $n > 3$. Also, none of the above elements is congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ modulo 2 or 3, so that $\Gamma(2)$ and $\Gamma(3)$ have no elliptic elements. This leaves only $\Gamma_1(2)$ and $\Gamma_1(3)$, and it is easy to determine their elliptic elements. ∎

Knowing μ, ν_∞ and the elliptic elements for $\Gamma_m(n)$ enables us to compute the genus of $X_m(n)$ by applying the formula of [3, Proposition 1.40]. Then we can prove:

PROPOSITION 3.7: *$X_m(n)$ has genus 0 if and only if (n, m) is one of the 18 following ordered pairs:*

$$\begin{gathered} (2,1), (3,1), \ldots, (10,1), (12,1) \\ (2,2), (4,2), (6,2), (8,2) \\ (3,3), (6,3), (4,4), (5,5). \end{gathered} \tag{7}$$

PROOF: The genus formula referred to above shows that $X_m(n)$ does have genus 0 for the pairs listed in (7). Conversely, assume that $X_m(n)$ has genus 0. The maps $X_m(n) \to X_1(n)$ and $X_m(n) \to X(m)$ show that both $X_1(n)$ and $X(m)$ have genus 0. As is well-known, this implies $2 \le n \le 10$ or $n = 12$ and $1 \le m \le 5$. The pairs (n, m) with $m \mid n$ satisfying these inequalities consist of the 18 listed in (7) and 7 more: $(10,2)$, $(12,2)$, $(9,3)$, $(12,3)$, $(8,4)$, $(12,4)$ and $(10,5)$. In each of these 7 cases, one computes that $X_m(n)$ has genus ≥ 1. ∎

We now study the ramification of the natural map from $X(n)$ to $X_m(n)$:

PROPOSITION 3.8: *The ramification index of the map*

$$X(n) \to X_m(n)$$

above a cusp of $X_m(n)$ represented by $\binom{a}{c}$ is $\gcd(n/m, c)$, except that when $(n, m) = (4, 1)$, the ramification index above $\binom{1}{2}$ is 4.

PROOF: From (6) it is evident that the number of double cosets in $\Gamma(n)\backslash\mathrm{SL}(2,\mathbb{Z})/N$ which are contained in the double coset of $\Gamma_m(n)\backslash\mathrm{SL}(2,\mathbb{Z})/N$ represented by $\binom{a}{c}$ is $n/\gcd(n, mc)$. Proposition 3.3 shows but for the case $(n, m) = (4, 1)$ that this is equal to the number of cusps of $X(n)$ mapping to $\binom{a}{c}$ in $X_m(n)$. Because $\Gamma(n)$ is normal in $\Gamma_m(n)$, the degree n/m of the map is the product of the ramification index and the number of preimages. This together with an examination of the exceptional case gives the result. ■

Proposition 1.2 in §1 shows that $X_m(n)$ can be regarded as the complex points of a variety $M_{\mathbb{Q}}$ defined over $\mathbb{Q}$. We want to determine the field of rationality of each cusp. Using [2, VI.5], the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on the cusps can be described as follows. The cusps are rational over $\mathbb{Q}(\zeta_n)$. Let $\binom{a}{c}$ represent a cusp, and take $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If u is an integer relatively prime to c and n whose image in $(\mathbb{Z}/n\mathbb{Z})^*$ corresponds to σ, then σ takes $\binom{a}{c}$ to $\binom{au}{c}$. Using this, we can prove:

PROPOSITION 3.9: *Let $\binom{a}{c}$ represent a cusp of $X_m(n)$, and let*

$$r = \frac{\gcd(n, mc)}{\gcd(m, a)}.$$

The field of rationality of $\binom{a}{c}$ is the maximal real subfield of $\mathbb{Q}(\zeta_r)$ if $c \equiv 0$ or $n/2 \bmod n$, and $\mathbb{Q}(\zeta_r)$ otherwise.

PROOF: Lift the above action of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ on the cusps of $X_m(n)$ to $\Gamma_m(n)\backslash\mathrm{SL}(2,\mathbb{Z})/N$. Let u be an integer relatively prime to c and n. Then (6) implies that $\binom{au}{c}$ represents the same double coset as $\binom{a}{c}$ if and only if

$$au \equiv a \bmod \gcd(n, mc), \text{ equivalently,}$$

$$\frac{a}{\gcd(m, a)}(u-1) \equiv 0 \bmod r.$$

Since $a/\gcd(m, a)$ and r are relatively prime, the last congruence is equivalent to

$$u \equiv 1 \bmod r.$$

The passage from the above double cosets to cusps is straightforward and concludes the proof of the proposition. ■

§4

Let n and m be as usual. In this section k will denote a field of characteristic $p \geq 0$, where:

1. $p \nmid n$ and $p \neq 2, 3$
2. k contains a primitive mth root of unity.

Assume that $(n, m) \neq (2, 1)$, $(2, 2)$, $(3, 1)$ or $(4, 1)$. Then $\Gamma_m(n)$ is torsion-free (Corollary 3.6) and all of its cusps are regular (Proposition 3.3), so by Theorem A.1, M_k represents $\mathcal{M}_k$, i.e., there is a universal level (n, m) structure

$$\alpha_k : (\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z})_{M_k} \to E_k \tag{8}$$

on some generalized elliptic curve E_k over M_k (note that we're using Proposition 1.3).

The part of E_k lying over M_k^0 is a smooth elliptic curve E_k^0 over M_k^0. The complement $M_k - M_k^0$, when k is algebraically closed, can be identified with the set

$$\Gamma_m(n)\backslash \mathrm{SL}(2, \mathbb{Z})/\pm N.$$

We can prove the following:

Proposition 4.1: *Let n and m be as above.*

1. *If k is algebraically closed, the fiber of $E_k \to M_k$ over the cusp represented by $\binom{a}{c}$ is of type I_b, where $b = n/\gcd(n/m, c)$.*
2. *$E_k \to M_k$ is the Néron model of $E_k^0 \to M_k^0$.*
3. *The group of sections of $E_k \to M_k$ having finite order is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.*
4. *$E_{\mathbb{C}} \to M_{\mathbb{C}}$ is isomorphic to the elliptic modular surface for $\Gamma_m(n)$ (see [4, §4]).*

Since all sections of an elliptic modular surface are torsion (see [4, Theorem 5.1] or [1, 3.20]), we get an immediate corollary:

Corollary 4.2: *If k has characteristic 0 (and a primitive mth root of unity), then the group of sections of $E_k \to M_k$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.*

Proof of Proposition 4.1: We will use the notation of the appendix (in particular, the group $\phi(N)$ of §2 is written U). The cusp represented by $\binom{a}{c}$ is a double coset

$$H \cap \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})\alpha(\pm U), \quad \alpha = \begin{pmatrix} a & * \\ c & * \end{pmatrix} \text{ in } \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z}).$$

The fiber of $E_k \to M_k$ over this cusp is of type I_b, where b is the unique positive integer dividing n such that

$$\alpha^{-1}H\alpha \cap U = \left\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \equiv 0 \bmod b\right\}$$

(see (10) in the appendix). It is easy to calculate that $b = n/\gcd(n/m, c)$, as desired.

To prove the second assertion, we first compute the order of $j: M_k \to \mathbb{P}^1_k$ at $\binom{a}{c}$. Using [2, VI.5.3] and the proof of Proposition 3.8, we see that $j: M_{n,n,k} \to \mathbb{P}^1_k$ has a pole of order n at every cusp. Then Proposition 3.8 shows that j has a pole of order $b = n/\gcd(n/m, c)$ at $\binom{a}{c}$. Since E_k has sections which hit every irreducible component of the fiber over $\binom{a}{c}$, it follows that E_k is the Néron model of $E_k^0 \to M_k^0$ at $\binom{a}{c}$.

The third assertion is now easy to prove. We can assume that k is algebraically closed, and let G be the group of sections of $E_k \to M_k$. The map α_k (see (8)) gives an injection

$$\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \hookrightarrow G.$$

The fiber over the cusp represented by $\binom{1}{0}$ is of type I_m by 1, so that [4, Remark 1.10] gives an injection

$$G_{\mathrm{tor}} \hookrightarrow k^* \times \mathbb{Z}/m\mathbb{Z}.$$

It also follows from 1 that for σ in G, $n\sigma$ hits the zero component of every fiber. Thus, by [4, Proposition 1.6], $nG_{\mathrm{tor}} = 0$. From this we immediately see that $G_{\mathrm{tor}} \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

To prove the last assertion, let $X \to X_m(n)$ be the elliptic modular surface for $\Gamma_m(n)$. Note that X is an algebraic surface. Let $f: X^0 \to Y_m(n)$ be the restriction of this over $Y_m(n)$. For $\tau \in \mathfrak{H}$, the fiber of f over $[\tau] \in Y_m(n)$ is the elliptic curve $X_\tau = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, and the maps sending $[\tau]$ to $[1/n]$ and $[\tau/m]$ in X_τ give holomorphic sections of f which define a holomorphic injection:

$$\tilde{\alpha}: (\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z})_{Y_m(n)} \to X^0.$$

We want to show that $\tilde{\alpha}$ is algebraic.

X_n^0, the kernel of multiplication by n, is an algebraic curve (being étale over $Y_m(n)$), and so X_n, its closure in X, is finite over $X_m(n)$. Thus we have a finite map $X_n \to X_m(n)$ and holomorphic sections (given by $\tilde{\alpha}$) over $Y_m(n)$. These clearly extend and hence are algebraic.

Then, using the fact that $\mathcal{M}_{\mathbb{C}}^0$ is represented by $Y_m(n)$, there is a map $\beta : Y_m(n) \to Y_m(n)$ and a cartesian diagram:

$$\begin{tikzcd} X^0 \arrow[r] \arrow[d] & E_{\mathbb{C}}^0 \arrow[d] \\ Y_m(n) \arrow[r, "\beta"] & Y_m(n). \end{tikzcd}$$

Suppose $\beta([\tau_1]) = \beta([\tau_2])$, $\tau_i \in \mathfrak{H}$. Then $\tilde{\alpha}_{\tau_i} : \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \hookrightarrow X_{\tau_i}$ ($i = 1, 2$) are isomorphic level (n, m) structures. From this it is easy to find $\gamma \in \Gamma_m(n)$ with $\gamma(\tau_1) = \tau_2$. Thus β is injective and hence an isomorphism. This proves our assertion. ∎

Let us briefly discuss the cases $(n, m) = (4, 1)$ and $(3, 1)$.

$\Gamma_1(4)$ is torsion-free, so that M_k^0 represents $\mathcal{M}_k^0$ by [2, VI.2.7]. Thus, there is a universal level (4, 1) structure on an elliptic curve

$$E_k^0 \to M_k^0.$$

For k algebraically closed, the Néron model of $E_k^0 \to M_k^0$ has fibers of types I_1, I_4 and I_1^* over the cusps $\binom{1}{0}$, $\binom{0}{1}$ and $\binom{1}{2}$ (the irregular cusp), and for any k, its group of sections of finite order is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Also, the elliptic modular surface for $\Gamma_1(4)$ is the Néron model of $E_{\mathbb{C}}^0 \to M_{\mathbb{C}}^0$, and $E_k^0 \to M_k^0$ has only torsion sections when k has characteristic zero.

$\Gamma_1(3)$ has an elliptic element, so that $\mathcal{M}_k^0$ is not representable. This corresponds to the fact that over $\bar{k}$ there is a unique level (3, 1) structure α_0 with a nontrivial automorphism (over $\mathbb{C}$, it is given by $[(1-\omega)/3] \in \mathbb{C}/\mathbb{Z} + \mathbb{Z}\omega$, $\omega = e^{2\pi i/3}$). But the functor $\tilde{\mathcal{M}}_k^0$ defined by

$$\tilde{\mathcal{M}}_k^0(S) = \{\alpha \in \mathcal{M}_k^0(S) ; \alpha \text{ never equals } \alpha_0 \text{ over } \bar{k}\}$$

is representable by $\tilde{M}_k^0 \subseteq M_k^0$. Thus there is a universal level (3, 1) structure on an elliptic curve

$$\tilde{E}_k^0 \to \tilde{M}_k^0.$$

If k is algebraically closed, then $\tilde{M}_k^0 = M_k^0 - \{\alpha_0\}$, and the Néron model of $\tilde{E}^0_k \to \tilde{M}^0_k$ has bad fibers of types I_1, I_3 and IV^* over $\binom{1}{0}$, $\binom{0}{1}$ and α_0. For any k, the group of sections is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Also, the Néron model of $E^0_{\mathbb{C}} \to M^0_{\mathbb{C}}$ is the elliptic modular surface for $\Gamma_1(3)$, and all sections are torsion when k has characteristic zero.

§5

Now we come to the main result of the paper. For any field k, $k(t)$ will denote the field of rational functions in a variable t.

THEOREM 5.1: *Let k be a field of characteristic $p \geq 0$, and assume that $p \neq 2, 3$. Let n and m be positive integers with $m \mid n$, and set $G = \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$. Then the following are equivalent:*

1. *There is an elliptic curve E over $k(t)$ with nonconstant j-invariant such that $G \simeq E(k(t))'_{\text{tor}}$, the rational points of finite order not divisible by p.*
2. *p does not divide n, k contains a primitive* mth *root of unity, and G is one of the following* 19 *groups:*

$$\begin{gathered} 0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \ldots, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \\ (\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \\ (\mathbb{Z}/3\mathbb{Z})^2, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z})^2, (\mathbb{Z}/5\mathbb{Z})^2. \end{gathered} \tag{9}$$

For $k = \mathbb{Q}$ or $\mathbb{C}$, this means:

COROLLARY 5.2: *If E is an elliptic curve over $\mathbb{C}(t)$ (resp. $\mathbb{Q}(t)$) with nonconstant j-invariant, then $E(\mathbb{C}(t))_{\text{tor}}$ (resp. $E(\mathbb{Q}(t))_{\text{tor}}$) must be one of the* 19 *groups of* (9) *(resp. one of the* 15 *groups on the first two lines of* (9)*). Furthermore, all of these do occur.* ∎

PROOF OF THEOREM 5.1: $1 \Rightarrow 2$. Certainly $p \nmid n$, and since $(\mathbb{Z}/m\mathbb{Z})^2 \subseteq G \subseteq E(k(t))$, k must have a primitive mth root of unity (this is a well-known consequence of the existence of the pairing $e_m : E_m \times E_m \to \mu_m$). By Propositions 3.7 and 1.2, we only have to prove that M_k has genus 0.

But $G \subseteq E(k(t))$ gives a level (n, m) structure on E, so that we get a commutative diagram:

$$\begin{tikzcd} \mathrm{Spec}(k(t)) \arrow[r, "u"] \arrow[dr, "j"'] & M_k^0 \subseteq M_k \arrow[d] \\ & \mathbb{A}_k^1 \end{tikzcd}$$

where $j = j(E)$ is the j-invariant of E. Since j is dominating, u must be dominating. Thus the function field of M_k injects into $k(t)$, which shows that M_k has genus 0.

$2 \Rightarrow 1$. First, assume that $G \neq 0$, $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$. Let K be the function field of $M_{n,m,k}$. Then Proposition 4.1 and the discussion of level (3, 1) and level (4, 1) structures give us an elliptic curve E over K with nonconstant j-invariant such that $E(K)'_{\mathrm{tor}} = G$.

In §3 we described the Galois action on the cusps of $X_m(n)$. Construction 5.3 of [2, VI.5] shows that this description also applies to the cusps of M_k. It is then easy to see that the cusp represented by $\binom{0}{1}$ is rational over k. Since M_k has genus 0 (Propositions 3.7 and 1.2), we see that $M_k \simeq \mathbb{P}_k^1$. Thus $K \simeq k(t)$.

To show that the groups 0, $\mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ can occur, consider the following elliptic curves over $k(t)$, defined by the equations:

$$y^2 = 4x^3 - 3x - t$$

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

$$y^2 = x(x-1)(x-t).$$

Each of these equations has a Néron model over $\mathbb{P}_k^1$. The bad fibers are of types I_1, I_1 and II^* for the first equation, I_1, I_2 and III^* for the second and I_2, I_2 and I_2^* for the third. Then, working over $\bar{k}$ and using [4, Proposition 1.6] as in §4, one easily sees that the group of torsion solutions is 0, $\mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ respectively. ∎

Appendix

Let H be a subgroup of $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. The algebraic stack $\mathcal{M}_H^0[1/n]$ has a compactification $\mathcal{M}_H[1/n]$ relative to $\mathbb{Z}[1/n]$ (see [2, IV.3]), and we set $\mathcal{M}_H^\infty[1/n] = \mathcal{M}_H[1/n] - \mathcal{M}_H^0[1/n]$.

Let Γ be the inverse image of $H \cap \mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})$ in $\mathrm{SL}(2, \mathbb{Z})$. The purpose of this appendix is to relate the representability of $\mathcal{M}_H[1/6n]$ and $\mathcal{M}_H^\infty[1/n]$ to some well-known properties of Γ. Specifically, we will prove:

THEOREM A.1: *$\mathcal{M}_H[1/6n]$ is an algebraic space if and only if Γ is torsion-free and all of its cusps are regular.*

THEOREM A.2: *$\mathcal{M}_H^\infty[1/n]$ is an algebraic space if and only if $C^-(\Gamma) = \emptyset$ (see §2).*

The first theorem follows from the second using Lemma 2.1 and [2, VI.2.7]. To prove the second, we use the interpretation of $\mathcal{M}_H^\infty[1/n]$ given in [2, IV.6]. Let k be an algebraically closed field whose characteristic does not divide n, and let C be a Néron polygon with b sides, $b \mid n$, over k.

A level H structure on C is described as follows. Let $C^0 = C^{\text{reg}} = \mathbb{G}_{m,k} \times \mathbb{Z}/b\mathbb{Z}$, and let $\tilde{C}^0 = \mathbb{G}_{m,k} \times \mathbb{Z}/n\mathbb{Z}$. There is a natural inclusion $C^0 \subseteq \tilde{C}^0$. An isomorphism $\mu_{n,k} \simeq \mathbb{Z}/n\mathbb{Z}$ defines an isomorphism $s : \tilde{C}^0_n \to (\mathbb{Z}/n\mathbb{Z})^2$, and let B be the image of C^0_n under s. In $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$, define the subgroups:

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}; a \in \mathbb{Z}/n\mathbb{Z} \right\}$$

$$U(B) = \{g \in U : g = 1 \text{ on } B\}.$$

Then, from [2, IV.6], a level H structure on C is a double coset $H\alpha U(B)$, $\alpha \in \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$, such that

$$\alpha^{-1} H \alpha \cap U = U(B). \tag{10}$$

Next we describe how automorphisms of $(C, +)$ (see [2, II.1]) act on level H structures on C. Let U_0 be the image of the map $\mathrm{Aut}(C, +) \to \mathrm{Aut}(C^0_n)$. Every automorphism of C^0_n extends to an automorphism of $\tilde{C}^0_n$, and using [2, II.1.10], we get an exact sequence

$$1 \to U(B) \to \pm U \to U_0 \to 1.$$

Then an automorphism ϕ of $(C, +)$ takes a level H structure $H\alpha U(B)$ to the level H structure $H\alpha u U(B)$, where u in $\pm U$ and ϕ map to the same thing in U_0.

LEMMA A.3: *A level H structure $H\alpha U(B)$ on C has a nontrivial automorphism if and only if*

$$\alpha^{-1} H \alpha \cap (-U) \neq \emptyset.$$

Proof: The case $n = 2$ is trivial. When $n \geq 3$, the lemma is an easy consequence of (10) and the fact that U_0 is isomorphic to $\mathrm{Aut}(C, +)$. ∎

Now Theorem A.2 follows easily. An element in $C^-(\Gamma)$ gives us, via (4) in §2, an element $\sigma \in \mathrm{SL}(2, Z/nZ)$ such that

$$\sigma^{-1}(H \cap \mathrm{SL}(2, Z/nZ))\sigma \cap (-U) \neq \emptyset. \tag{11}$$

By the above lemma, $H\sigma U(B)$ has a nontrivial automorphism. Conversely, again using Lemma A.3, suppose we have $\alpha^{-1}h\alpha \in -U$ for some $\alpha \in \mathrm{GL}(2, Z/nZ)$ and $h \in H$. Note that h lies in $H \cap \mathrm{SL}(2, Z/nZ)$. Let $\beta = \left(\begin{smallmatrix}1 & 0\\ 0 & r\end{smallmatrix}\right)$, where $r = \det(\alpha)^{-1}$. Then $\sigma = \alpha\beta$ is in $\mathrm{SL}(2, Z/nZ)$ and satisfies (11). From (4) in §2, we get an element of $C^-(\Gamma)$. ∎

REFERENCES

[1] D. Cox and S. Zucker: Intersection numbers of sections of elliptic surfaces. *Inventiones math.*, *53* (1979) 1–44.

[2] P. Deligne and M. Rapoport: Les schemas de modules de courbes elliptiques, in *Modular functions of one variable II.* Lecture Notes in Math. 349, Springer-Verlag, Berlin–Heidelberg–New York, 1973.

[3] G. Shimura: *Arithmetic theory of automorphic functions.* Princeton U. Press, Princeton, 1971.

[4] T. Shioda: Elliptic modular surfaces. *J. Math. Soc. Japan*, *24* (1972) 20–59.

(Oblatum 12–XII–1978)

Department of Mathematics
Rutgers University
New Brunswick
New Jersey 08903

Current Addresses:
D. Cox
Department of Mathematics
Amherst College
Amherst, Mass. 01002

W. Parry
Department of Mathematics
SUNY at Stony Brook
Stony Brook, N.Y. 11794