Stable reduction of modular curves

Irene I. Bouw   Stefan Wewers

Abstract

We determine the stable reduction at p of all three point covers of the projective line with Galois group $\mathrm{SL}_2(p)$. As a special case, we recover the results of Deligne and Rapoport on the reduction of the modular curves $X_0(p)$ and $X_1(p)$. Our method does not use the fact that modular curves are moduli spaces. Instead, we rely on results of Raynaud and the authors which describe the stable reduction of three point covers whose Galois group is strictly divisible by p.

Introduction

Modular curves are quotients of the upper half plane by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The most prominent examples are $X_0(N)$, $X_1(N)$ and $X(N)$, for $N \geq 1$. Modular curves are also moduli spaces for elliptic curves endowed with a level structure. Therefore, they are defined over small number fields and have a rich arithmetic structure. Deligne and Rapoport [4] determine the reduction behavior of $X_0(p)$ and $X_1(p)$ at the prime p. Using this result, they prove a conjecture of Shimura saying that the quotient of the Jacobian of $X_1(p)$ by the Jacobian of $X_0(p)$ acquires good reduction over $\mathbb{Q}(\zeta_p)$. Both the reduction result and its corollary have been generalized by Katz and Mazur [9] to arbitrary level N and various level structures.

The basic method employed in [4] and [9] is to generalize the moduli problem defining the modular curve in question, in such a way that it makes sense in arbitrary characteristic. By general results on representability of moduli problems one then obtains a model of the modular curve over the ring of integers of a subfield of $\mathbb{Q}(\zeta_N)$. This model has bad reduction at all primes dividing N, and it is far from being semistable, in general. In spite of the very general results of [9], it remains an unsolved problem to describe the stable reduction of $X_0(N)$ at p if p^3 divides N (see [5] for the case $p^2||N$).

In this note we suggest a different approach to study the reduction of modular curves. Our starting point is the observation that the j-invariant

$$X(N) \longrightarrow X(1) \cong \mathbb{P}^1$$

presents the modular curve $X(N)$ as a Galois cover of the projective line (with Galois group $\mathrm{PSL}_2(\mathbb{Z}/N)$) which is branched only at the three rational points 0, 1728 and ∞. Let us call a Galois covers of the projective line branched only at three points a *three point cover*. In [11] Raynaud studies the stable reduction of three point covers under the assumption that the residue characteristic p strictly divides the order of the Galois group. His results have been sharpened in [15] and [16]. In the present paper we determine the stable reduction of all three point covers with Galois group $\mathrm{PSL}_2(p)$, using the results of [16]. As a corollary we obtain a new proof of the results of Deligne and Rapoport on the reduction of $X_0(p)$ and $X_1(p)$. Somewhat surprisingly, our proof does not use the modular interpretation of these curves. On the other hand, the determination of the stable reduction of some of the $\mathrm{PSL}_2(p)$-covers which are not modular curves does use the fact that they are moduli spaces of a certain kind. Here we build on the results of [2].

What is so special about the group $\mathrm{PSL}_2(p)$? From our point of view there are two main aspects. The first is *rigidity*. Let G be a finite group and $\mathbf{C} = (C_1, C_2, C_3)$ a triple of conjugacy classes of G. Suppose that there exists a triple $\mathbf{g} = (g_1, g_2, g_3)$ of generators of G with $g_i \in C_i$ and $g_1 g_2 g_3 = 1$. The triple $\mathbf{g}$ corresponds to a G-cover $Y \to \mathbb{P}^1$ with three branch points. If G equals $\mathrm{PSL}_2(p)$, such a triple $\mathbf{g}$ is unique, up to uniform conjugation in $\mathrm{PGL}_2(p)$. Therefore there exists at most one three point cover with a given branch cycle description $\mathbf{C}$, up to isomorphism.

We use rigidity as follows. By a result of [16] we can construct three point G-covers $Y \to \mathbb{P}^1$ with bad reduction at p by lifting a certain type of 'stable G-cover' $\bar{Y} \to \bar{X}$ from characteristic p to characteristic zero. Here $\bar{Y} \to \bar{X}$ is a finite map between semistable curves in characteristic p together with some extra structure (g, ω) which we call the *special deformation datum*. In the case of the modular curve $X(p)$ (where $G = \mathrm{PSL}_2(p)$) one can construct $\bar{Y} \to \bar{X}$ very explicitly; the special deformation datum (g, ω) corresponds to a solution of a hypergeometric differential equation. (A similar phenomenon occurs in Ihara's work on congruence relations [7].) The $\mathrm{PSL}_2(p)$-cover $Y \to \mathbb{P}^1$ resulting from the lifting process has branch cycle description $(3A, 2A, pA)$. By rigidity, $Y \to \mathbb{P}^1$ is isomorphic to $X(p) \to X(1)$. In particular, the stable reduction of $X(p)$ is isomorphic to $\bar{Y}$.

The other nice thing about $\mathrm{PSL}_2(p)$ is that p strictly divides its order. The results of [11] and [16] which describe the stable reduction of a given G-cover require that p strictly divides the order of G, whereas the Sylow p-subgroup of $\mathrm{PSL}_2(\mathbb{Z}/p^n)$ is rather big for $n > 1$. This is the main obstruction for extending the method of the present paper to modular curves of higher p-power level. There are partial results of the authors generalizing some of the results of [11] and [16] to groups G with a cyclic or an elementary abelian Sylow p-subgroup (unpublished). It seems hopeless to obtain general results beyond these cases. But maybe a combination of the methods presented in the present paper with the modular approach might shed some light on the stable reduction of modular curves of higher p-power level.

The organization of this paper is as follows. In Section 1 we define special deformation data and explain how to associate a special deformation datum to a three point cover with bad reduction. We recall a result from [16] which essentially says that we can reverse this process. In Section 2 we introduce hypergeometric deformation data. These are special deformation data satisfying an addition condition (Definition 2.1). We classify all hypergeometric deformation data by showing that they correspond to the solution in characteristic p of some hypergeometric differential equation. In Sections 3 and 4 we use these results to give a new proof of the stable reduction of the modular curves $X(p)$ and $X_0(p)$. In Section 5 we generalize these results to all three point covers with Galois group $\mathrm{SL}_2(p)$.

1 The special deformation datum

Let k be an algebraically closed field of characteristic $p > 2$. Let H be a finite group of order prime to p. Fix a character $\chi : H \to \mathbb{F}_p^\times$. Let $g : Z_k \to \mathbb{P}^1_k$ be an H-Galois cover and ω be a meromorphic differential on Z_k. We assume that ω is logarithmic (i.e. can be written as $\omega = \mathrm{d}u/u$) and

$$\beta^*\omega = \chi(\beta) \cdot \omega, \qquad \text{for all } \beta \in H.$$

Let $\xi \in Z_k$ be a closed point and τ its image in $\mathbb{P}^1_k$. Denote by H_ξ the stabilizer of ξ in H. Define

$$m_\tau := |H_\xi|, \qquad h_\tau := \mathrm{ord}_\xi(\omega) + 1, \qquad \sigma_\tau = h_\tau / m_\tau. \tag{1}$$

Since ω is logarithmic, we have $h_\tau \geq 0$. We say that τ is a *critical point* of the differential ω if $(m_\xi, h_\xi) \neq (1,1)$. Let $(\tau_i)_{i \in \mathbb{B}}$ be the critical points of ω, indexed by a finite set $\mathbb{B}$. For $i \in \mathbb{B}$, we write m_i, h_i, σ_i instead of $m_{\tau_i}, h_{\tau_i}, \sigma_{\tau_i}$. For every i, choose a point $\xi_i \in Z_k$ above τ_i and write $H(\xi_i) \subset H$ for its stabilizer. Define $\mathbb{B}_{\mathrm{wild}} := \{\, i \in \mathbb{B} \mid h_i = 0 \,\}$.

Definition 1.1 *A* special deformation datum *of type (H, χ) is a pair (g, ω), where $g : Z_k \to \mathbb{P}^1_k$ is an H-Galois cover and ω is a logarithmic differential on Z_k such that the following holds.*

(i) *We have*
$$\beta^*\omega = \chi(\beta)\cdot\omega, \qquad \text{for all } \beta \in H. \tag{2}$$

(ii) *For every* $i \in \mathbb{B} - \mathbb{B}_{\rm wild}$, *we have that* $0 < \sigma_i \leq 2$.

(iii) *Define* $\mathbb{B}_{\rm prim} = \{i \in \mathbb{B} \,|\, 0 < \sigma_i \leq 1\}$. *Then* $|\mathbb{B}_{\rm prim} \cup \mathbb{B}_{\rm wild}| = 3$.

Write $\mathbb{B}_0 = \mathbb{B}_{\rm wild} \cup \mathbb{B}_{\rm prim}$ and $\mathbb{B}_{\rm new} = \mathbb{B} - \mathbb{B}_0$. See [16] for more details and an explanation of the terminology. If $\sigma_i \neq 1, 2$ for all i, the above definition coincides with [16, Definition 2.7].

Definition 1.2 *Let G be a finite group. A G-*tail cover *is a (not necessarily connected) G-Galois cover $f_k : Y_k \to \mathbb{P}^1_k$ such that f_k is wildly branched at ∞ of order pn with n prime to p and tamely branched at no more than one other point. We say that f is a* primitive tail cover *if it is branched at two points. Otherwise, we call f a* new tail cover.

If the group G is understood, we talk about tail covers instead of G-tail covers. To a G-tail cover $f_k : Y_k \to \mathbb{P}^1_k$ we associate its *ramification invariant* $\sigma(f) = h/n$, where h is the conductor of f_k at ∞ and n the order of the prime-to-p ramification, as in Definition 1.2. The ramification invariant is the jump in the filtration of higher ramification groups in the upper numbering.

Three point covers with bad reduction give rise to a special deformation datum and a set of tail covers. Essentially, the stable reduction of the cover is determined by these data. Proposition 1.3 states that given a special deformation datum and a set of tail covers satisfying some compatibility conditions, there exists a three point cover in characteristic zero which gives rise to the given datum.

To be more precise, let R be a complete discrete valuation ring with fraction field K of characteristic zero and residue field an algebraically closed field k of characteristic p. Let G be a finite group and let $f : Y \to X = \mathbb{P}^1_K$ be a G-Galois cover branched at three points x_1, x_2, x_3. We assume that the points x_1, x_2, x_3 specialize to pairwise distinct points on the special fiber $\mathbb{P}^1_k$. Denote the ramification points of f by $y_1, \ldots, y_s$. We consider the y_i as markings on Y. After replacing K by a finite extension, there exists a unique extension $(Y_R; y_i)$ of $(Y; y_i)$ to a stably marked curve over R. The action of G extends to Y_R; write X_R for the quotient of Y_R by G. The map $f_R : Y_R \to X_R$ is called the *stable model* of f; its special fiber $\bar{f} : \bar{Y} \to \bar{X}$ is called the *stable reduction* of f, [16, Definition 1.1].

We say that f has *good reduction* if $\bar{f}$ is separable. This is equivalent to $\bar{X}$ being smooth. If f does not have good reduction, we say it has *bad reduction*.

Suppose that f has bad reduction and that p strictly divides the order of G. Then $\bar{X}$ is a 'comb', see [16, Theorem 2.6] and Figure 1. The central component $\bar{X}_0 \subset \bar{X}$ is canonically isomorphic to $\mathbb{P}^1_k$. Choose a component $\bar{Y}_0$ of $\bar{Y}$ above $\bar{X}_0$. Let $G_0 \subset G$ denote the decomposition group of the component $\bar{Y}_0$ and $I_0 \lhd G_0$ the inertia group. Then $I_0 \cong \mathbb{Z}/p$. Therefore, the restriction of $\bar{f}$ to $\bar{Y}_0$ factors as $\bar{Y}_0 \to \bar{Z}_0 \to \bar{X}_0$, with $g : \bar{Z}_0 \to \bar{X}_0$ a separable Galois cover of prime-to-p order and $\bar{Y}_0 \to \bar{Z}_0$ purely inseparable of degree p. The map $\bar{Y}_0 \to \bar{Z}_0$ is generically endowed with the structure of a $\boldsymbol{\mu}_p$-torsor. This structure is encoded in a logarithmic differential ω. Define $H := \mathrm{Gal}(\bar{Z}_0/\bar{X}_0)$; then G_0 is an extension of H by I_0. The action of H on I_0 by conjugation gives rise to a character $\chi : H \to \mathbb{F}_p^\times$. It is proved in [16, Proposition 2.15] that (g, ω) is a special deformation datum of type (H, χ).

The irreducible components of $\bar{X}$ different from the central component $\bar{X}_0$ are called the *tails* of $\bar{X}$. The tails are parameterized by $i \in \mathbb{B} - \mathbb{B}_{\rm wild}$, [16, Proposition1.7]. For $i \in \mathbb{B} - \mathbb{B}_{\rm wild}$, write $\bar{X}_i$ for the corresponding tail of $\bar{X}$ and write $\bar{f}_i : \bar{Y}_i \to \bar{X}_i$ for the restriction of $\bar{f}$ to $\bar{X}_i$. The map $\bar{f}_i$ is a primitive tail cover if $i \in \mathbb{B}_{\rm prim}$ and a new tail cover if $i \in \mathbb{B}_{\rm new}$, [16, Lemma 1.4]. We say that $\bar{X}_i$ is a *primitive* (resp. *new*) tail of $\bar{X}$ if $i \in \mathbb{B}_{\rm prim}$ (resp. $i \in \mathbb{B}_{\rm new}$).

The three branch points specialize as follows. If p divides the ramification index of x_j, then x_j specializes to $\tau_i \in \bar{X}_0$ for a unique $i \in \mathbb{B}_{\rm wild}$. Otherwise, x_j specializes to one of the primitive tails

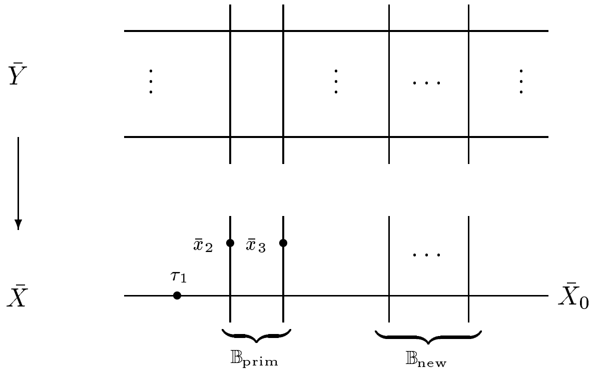

Figure 1: The stable reduction of $f : Y \to \mathbb{P}^1$

$\bar{X}_i$, for $i \in \mathbb{B}_{\rm prim}$. From now on, we will identify the set $\mathbb{B}_0 = \mathbb{B}_{\rm prim} \cup \mathbb{B}_{\rm wild}$ with $\{1, 2, 3\}$ such that $i \in \mathbb{B}_{\rm wild}$ if and only if p divides the order of the ramification index at x_i. For $i \in \mathbb{B}_{\rm prim}$ we denote by $\bar{x}_i \in \bar{X}_i$ the specialization of x_i.

The special deformation datum (g, ω) and the tail covers $\bar{f}_i$ satisfy the following compatibility condition. For every $i \in \mathbb{B} - \mathbb{B}_{\rm wild}$, there exists a point $\xi_i \in \bar{Z}_0$ above τ_i and a point $\eta_i \in \bar{Y}_i$ which is wildly ramified in $\bar{f}_i$ such that

$$I(\eta_i) \subset G_0, \qquad I(\eta_i) \cap H = H(\xi_i). \tag{3}$$

Here $I(\eta_i) \subset G$ (resp. $H(\xi_i) \subset H$) denotes the stabilizer of η_i (resp. of ξ_i). Furthermore, the ramification invariant $\sigma(\bar{f}_i)$ of the tail cover $\bar{f}_i$ is equal to σ_i as in Definition 1.1.

Proposition 1.3 *Let G be a finite group. Fix a subgroup $G_0 \simeq \mathbb{Z}/p \rtimes_\chi H$ of G, where H has order prime-to-p and acts on $\mathbb{Z}/p$ via a character $\chi : H \to \mathbb{F}_p^\times$. Let (g, ω) be a special deformation datum of type (H, χ). Let $\mathbb{B}$, τ_i and $\sigma_i = h_i/m_i$ be as in Definition 1.1.*

For $i \in \mathbb{B}_{\rm prim}$ (resp. $i \in \mathbb{B}_{\rm new}$), suppose we are given a primitive (resp. new) G-tail cover $\bar{f}_i : \bar{Y}_i \to \bar{X}_i = \mathbb{P}^1_k$ with ramification invariant σ_i. Suppose furthermore that there exists a point $\xi_i \in Z_k$ above $\tau_i \in \mathbb{P}^1_k$ and a point $\eta_i \in \bar{Y}_i$ which is wildly ramified in $\bar{f}_i$ such that (3) *holds.*

Let K_0 be the fraction field of $W(k)$ (the Witt vectors over k) and let K/K_0 be the (unique) tame extension of degree

$$N := (p-1) \cdot \operatorname*{lcm}_{i \notin \mathbb{B}_{\rm wild}} (h_i). \tag{4}$$

There exists a G-Galois cover $f : Y \to X = \mathbb{P}^1_K$ over K, branched at 0, 1 and ∞, which gives rise to the special deformation datum (g, ω) and the tail covers $\bar{f}_i$.

Proof. The datum $(g, \omega, \bar{f}_i)$ together with the choice of the points ξ_i and η_i is called a *special G-deformation datum* in [16, Definition 2.13]. Hence the proposition follows from [16, Corollary 4.6]. $\square$

In this paper, the group G is either $\mathrm{SL}_2(p)$ or $\mathrm{PSL}_2(p)$. Therefore, the group H is cyclic and $H(\xi_i)$ only depends on i and not on the choice of ξ_i.

The G-cover $f : Y \to \mathbb{P}^1_K$ in Proposition 1.3 which gives rise to the datum $(g, \omega, \bar{f}_i)$ is not unique. In [16, Theorem 4.5] one finds an explicit parameterization of the the set of isomorphism classes of all such G-covers.

2 Hypergeometric deformation data

In this section we classify a certain type of special deformation data which we call *hypergeometric*. A hypergeometric (special) deformation datum corresponds to a polynomial solution of a hypergeometric differential equation. For this reason it is possible to find all such deformation data. The definition of hypergeometricity looks very restrictive, but we show in Section 5 that the special deformation datum corresponding to a three point cover with Galois group $\mathrm{PSL}_2(p)$ or $\mathrm{SL}_2(p)$ is hypergeometric. In particular, this holds for the $\mathrm{PSL}_2(p)$-cover $X(p) \to X(1) \simeq \mathbb{P}^1_j$.

Definition 2.1 *A* hypergeometric deformation datum *is a special deformation datum* (g, ω) *with* $\sigma_i = (p+1)/(p-1)$ *for all* $i \in \mathbb{B}_{\mathrm{new}}$.

Let (g, ω) be a hypergeometric deformation datum. Recall that $\mathbb{B}_0 = \{1, 2, 3\}$, by assumption. In this section we assume $x_1 = 0, x_2 = 1, x_3 = \infty$. In particular, $\tau_i \neq \infty$ for all $i \in \mathbb{B}_{\mathrm{new}}$. For $i \in \mathbb{B}$, we define integers $0 \leq a_i < p-1$ such that

$$a_i \equiv (p-1)\sigma_i \mod p-1.$$

In particular, $a_i = 2$ for $i \in \mathbb{B}_{\mathrm{new}}$.

To $g : Z_k \to \mathbb{P}^1_k$ we associate the (not necessarily connected) $\mathbb{F}_p^\times$-Galois cover

$$g' : Z'_k := \mathrm{Ind}_{\mathrm{Im}(\chi)}^{\mathbb{F}_p^\times}(Z_k/\mathrm{Ker}\,\chi) \to \mathbb{P}^1_k.$$

It follows easily from Definition 2.1 and the expansion of ω into local coordinates that Z'_k is the complete nonsingular curve defined by

$$z^{p-1} = x^{a_1}(x-1)^{a_2} \prod_{i \in \mathbb{B}_{\mathrm{new}}} (x - \tau_i)^2, \tag{5}$$

where $\beta^* z = \chi(\beta) \cdot z$. We call (a_1, a_2, a_3) the *signature* of the hypergeometric deformation datum (g, ω).

We may identify the differential ω on Z_k with a differential on Z'_k which we also denote by ω. Definition 1.1(i) and (1) imply that

$$\omega = \epsilon \frac{z\,\mathrm{d}x}{x(x-1)}, \tag{6}$$

for some $\epsilon \in k^\times$. The condition that ω is logarithmic imposes a strong condition on $u := \prod_{i \in \mathbb{B}_{\mathrm{new}}}(x - \tau_i)$. Proposition 2.2 below states that the differential (6) is logarithmic if and only if u is the solution to a certain hypergeometric differential equation.

It follows from (1) and the Riemann–Roch Theorem applied to ω that

$$|\mathbb{B}_{\mathrm{new}}| = (p - 1 - a_1 - a_2 - a_3)/2. \tag{7}$$

In particular, $a_1+a_2+a_3$ is an even integer between 0 and $p-1$. Note that if $a_1+a_2+a_3 = p-1$ then $\deg(u) = |\mathbb{B}_{\mathrm{new}}| = 0$. Therefore, we exclude this case in Proposition 2.2.(i). However, Proposition 2.2.(ii) applies also if $a_1 + a_2 + a_3 = p - 1$.

Proposition 2.2 *(i) Let* (g, ω) *be a hypergeometric deformation datum. Let* (a_1, a_2, a_3) *be its signature, and suppose that* $a_1 + a_2 + a_3 < p - 1$. *Then* $u(x) := \prod_{i \in \mathbb{B}_{\mathrm{new}}}(x - \tau_i)$ *is a solution to the hypergeometric differential equation*

$$x(x-1)u'' + [(A + B + 1)x - C]u' + ABu = 0,$$

where $A = (1 + a_1 + a_2 + a_3)/2$, $B = (1 + a_1 + a_2 - a_3)/2$ *and* $C = 1 + a_1$. *The degree of* u *in* x *is* $d := (p - 1 - a_1 - a_2 - a_3)/2$.

(ii) Let $0 \leq a_1, a_2, a_3 < p-1$ be integers with $a_1+a_2+a_3 \leq p-1$. We assume that $a_1+a_2+a_3$ is even. Let $H = \mathbb{Z}/m$, where $m = (p-1)/2$ if a_1, a_2, a_3 are all even and $m = p-1$ otherwise. Choose an injective character $\chi : H \to \mathbb{F}_p^\times$. There exists a hypergeometric deformation datum (g, ω) of signature (a_1, a_2, a_3) and type (H, χ). The deformation datum (g, ω) is uniquely determined by (a_1, a_2, a_3), up to multiplying the differential ω by an element of $\mathbb{F}_p^\times$.

Proof. The following proof is inspired by [1, Lemma 3]. A similar argument can be found in [7, Theorem 5]. Write

$$Q = x^{1+a_1}(x-1)^{1+a_2}, \qquad F = \epsilon \frac{z}{x(x-1)} = \frac{\epsilon z^p}{Qu^2}.$$

It is well known that the fact that $\omega = F\,\mathrm{d}x$ is logarithmic is equivalent to $D^{p-1}F = -F^p$, where $D := \mathrm{d}/\mathrm{d}x$. Since $D^{p-1}F = \epsilon z^p D^{p-1}[1/(Qu^2)]$, we find

$$D^{p-1}\frac{1}{Qu^2} = -\epsilon^{p-1}\frac{1}{x^p(x-1)^p}. \tag{8}$$

Choose $i \in \mathbb{B}_{\mathrm{new}}$ and write

$$\frac{1}{Qu^2} = \sum_{n \geq -2} a_n (x-\tau_i)^n.$$

Then

$$D^{p-1}\frac{1}{Qu^2} = -\left[\frac{a_{-1}}{(x-\tau_i)^p} + a_{p-1} + \cdots\right] = -\epsilon^{p-1}\frac{1}{x^p(x-1)^p}.$$

We conclude that $a_{-1} = 0$.

Write

$$\begin{aligned} Qu^2 &= [Q(\tau_i) + Q'(\tau_i)(x-\tau_i)\cdots][u'(\tau_i)(x-\tau_i) + \frac{1}{2}u''(\tau_i)(x-\tau_i)^2 + \cdots]^2 \\ &= (x-\tau_i)^2\,[\,Q(\tau_i)u'(\tau_i) + (\,Q'(\tau_i)u'(\tau_i) + Q(\tau_i)u''(\tau_i)\,)\,(x-\tau_i) + \cdots]. \end{aligned}$$

We see that $-a_{-1} = u'(\tau_i)[\,Q'(\tau_i)u'(\tau_i) + Q(\tau_i)u''(\tau_i)\,]$. Since $u'(\tau_i) \neq 0$, we have that $Q'(\tau_i)u'(\tau_i) + Q(\tau_i)u''(\tau_i) = 0$ for all $i \in \mathbb{B}_{\mathrm{new}}$.

Define $G = Q'u' + Qu''$. This is a polynomial of degree less than or equal to $e := \deg(Q) + \deg(u) - 2 = |\mathbb{B}_{\mathrm{new}}| + a_1 + a_2$. The coefficient of x^e in G is $g_e = \deg(u)(\deg(Q) + \deg(u) - 1)$. Since $\deg(Q) \geq 2$ and $\deg(u) \neq 0$, the coefficient g_e is nonzero. The polynomial G is obviously divisible by $x^{a_1}(x-1)^{a_2}$, and $G(\tau_i) = 0$, for all $i \in \mathbb{B}_{\mathrm{new}}$. Therefore $G = g_e x^{a_1}(x-1)^{a_2}u$. Dividing by $x^{a_1}(x-1)^{a_2}$, we find that u is a solution to the hypergeometric differential equation

$$P_0 u'' + P_1 u' + P_2 u = 0, \tag{9}$$

where $P_0 = x(x-1)$, $P_1 = P_0 Q'/Q = (2+a_1+a_2)x - (1+a_1)$, and $P_2 = -g_e = ((1+a_1+a_2)^2 - a_3^2)/4$. Part (i) of the proposition follows. The proof also shows that

$$\epsilon^{p-1} = (-1)^{a_1}\binom{p-1-a_2}{a_1}. \tag{10}$$

To prove (ii), let $0 \leq a_1, a_2, a_3 < p-1$ be integers such that $a_1 + a_2 + a_3$ is even and less than or equal to $p-1$. Define $d = (p-1-a_1-a_2-a_3)/2$. We claim that the differential equation (9) has a unique polynomial solution $u = \sum_i u_i x^i \in k[x]$ of degree d with $u_d = 1$.

Suppose that $u = \sum_{i \in \mathbb{Z}} u_i x^i$ is a solution of (9). Put $A_i = (i+1)(i+a_1+1)$ and $B_i = (i + (1+a_1+a_2+a_3)/2)(i + (1+a_1+a_2-a_3)/2)$. The differential equation gives a recursion

$$A_i u_{i+1} = B_i u_i \tag{11}$$

for the coefficients of u. One checks that A_i and B_i are nonzero for all $0 \leq i < d$ and that $A_{-1} = B_d = 0$ and $A_d \cdot B_{-1} \neq 0$. Therefore there is a unique polynomial solution u of degree d with $u_d = 1$. This implies the claim.

Let m be as in the statement of the proposition. Let Z'_k be the complete nonsingular curve defined by

$$z^{p-1} = u^2 x^{a_1}(x-1)^{a_2}$$

and let Z_k be a connected component of Z'_k. Write $g : Z_k \to \mathbb{P}^1_k$ for the m-cyclic cover defined by $(x, z) \mapsto x$. We may identify H with $\mathrm{Gal}(Z_k/\mathbb{P}^1_k)$ such that H acts on z via some chosen character $\chi : H \to \mathbb{F}_p^\times$. Let

$$\omega = \frac{\epsilon\, z\, \mathrm{d}x}{x(x-1)}.$$

Since u is the solution to a hypergeometric differential equation, it has at most simple zeros outside 0 and 1. We know that $u(0) = u_0 = \prod_{i=0}^{d-1}(B_i/A_i) \neq 0$. Therefore u does not have a zero at $x = 0$. We claim that u does not have a zero at 1, also. To see this, let $t = 1 - x$ be a new coordinate on $\mathbb{P}^1_k$ and write $\tilde{u}(t) = u(1-t)$. The coefficients of $\tilde{u}$ satisfy a recursion similar to (11), but with a_1 and a_2 interchanged. The same argument as above applied to $\tilde{u}$ shows now that $\tilde{u}(0) = u(1) \neq 0$. We conclude that u has exactly d zeros different from 0 and 1. Analogous to the proof of (i), one shows that for ϵ as in (10) the differential ω is logarithmic. It is clear that (g, ω) is a special deformation datum. The uniqueness statement is obvious. □

3 The reduction of $X(p)$

In the rest of the paper we suppose that $p \geq 5$. Choose a primitive $(p-1)$th root of unity $\zeta \in \mathbb{F}_p$ and a primitive $(p+1)$th root of unity $\tilde{\zeta} \in \mathbb{F}_{p^2}$. Define

$$C(l) \;=\; \{A \in \mathrm{SL}_2(p) \mid \mathrm{tr}(A) = \zeta^l + \zeta^{-l}\}, \qquad \text{for } 0 < l \leq (p-1)/2$$

and

$$\tilde{C}(l) \;=\; \{A \in \mathrm{SL}_2(p) \mid \mathrm{tr}(A) = \tilde{\zeta}^l + \tilde{\zeta}^{-l}\}, \qquad \text{for } 0 < l < (p+1)/2.$$

These are the conjugacy classes of $\mathrm{SL}_2(p)$ of nontrivial elements of order prime to p. We write pA and pB for the two conjugacy classes of elements of order p. Note that the elements of order p have trace 2.

Let $\mathbf{C} = (C_1, C_2, C_3)$ be a triple of conjugacy classes of $\mathrm{SL}_2(p)$. In the rest of this section, we suppose that the C_i do not contain $\pm I$. We write $\mathrm{Ni}_3^{\mathrm{in}}(\mathbf{C})$ for the set of isomorphism classes of $\mathrm{SL}_2(p)$-covers $Y \to \mathbb{P}^1$ branched at $0, 1, \infty$ with class vector $\mathbf{C}$. This means that the canonical generator of some point of Y above $x_i \in \{0, 1, \infty\}$ with respect to the chosen roots of unity is contained in the conjugacy class C_i. In this paper, we call two G-covers $f_i : Y_i \to X$ isomorphic if there exists a G-equivariant automorphism $\phi : Y_1 \to Y_2$ such that $f_1 = f_2 \circ \phi$.

Proposition 3.1 (Linear rigidity) *Let* $\mathbf{C} = (C_1, C_2, C_3)$ *be a triple of conjugacy classes of* $\mathrm{SL}_2(p)$.

(i) Suppose that the elements of C_i *have prime-to-p order. Then* $\#\,\mathrm{Ni}_3^{\mathrm{in}}(\mathbf{C}) \in \{0, 2\}$.

(ii) Otherwise, $\#\,\mathrm{Ni}_3^{\mathrm{in}}(\mathbf{C}) \in \{0, 1\}$.

Proof. See [13]. The difference between the two cases comes from the fact that the outer automorphism group of G has order two and interchanges the two conjugacy classes of order p but fixes all other conjugacy classes. □

In the following we denote by $2A$ (resp. $3A$) the unique conjugacy classes in $\mathrm{PSL}_2(p)$ of elements of order 2 (resp. 3). Note that elements of $2A$ (resp. elements of $3A$) lift to elements of order 4 (resp. of order 3 or 6) in $\mathrm{SL}_2(p)$. Furthermore, we denote by pA and pB the images in $\mathrm{PSL}_2(p)$ of the conjugacy classes of $\mathrm{SL}_2(p)$ with the same name.

Let $X(N)$ be the modular curve parameterizing (generalized) elliptic curves with full level N-structure [4]. Consider the cover $X(2p) \to X(2) \simeq \mathbb{P}^1_\lambda$. This is a Galois cover with Galois group $\mathrm{PSL}_2(p)$ which is branched at $0, 1, \infty$ of order p and unbranched elsewhere. One easily checks as in [14, Lemma 3.27] that there are no $\mathrm{PSL}_2(p)$-covers with class vector (pA, pA, pB). After renaming the conjugacy classes, the class vector of $X(2p) \to X(2)$ is therefore $\mathbf{C} = (pA, pA, pA)$.

Proposition 3.1 implies that the triple $\mathbf{C} = (pA, pA, pA)$ is rigid, i.e. there is a unique $\mathrm{PSL}_2(p)$-cover of $\mathbb{P}^1$ whose class vector is $\mathbf{C}$, up to automorphism. Since $\mathrm{PSL}_2(p)$ has trivial center, it follows that the $\mathrm{PSL}_2(p)$-cover $X(2p) \to X(2)$ has a unique model $X(2p)_K \to X(2)_K = \mathbb{P}^1_K$ over any field K of characteristic zero containing $\sqrt{p^*}$, [12, Chapter 7]. Let K_0 be the fraction field of the ring of Witt vectors over $k = \bar{\mathbb{F}}_p$, and let K/K_0 be a sufficiently large finite extension. We define the stable reduction of $X(2p) \to X(2)$ at p as the stable reduction of $X(2p)_K \to \mathbb{P}^1_K$.

The cover $X(2p) \to X(2)$ may be considered as a variant with ordered branch points of the cover $X(p) \to X(1) \simeq \mathbb{P}^1_j$. We find it easier to first compute the stable reduction of the former and then deduce the stable reduction of the latter.

Proposition 3.2 *Let $\bar{Y} \to \bar{X}$ be the stable reduction of $X(2p) \to X(2)$ at p. Then $\bar{X}$ has $(p-1)/2$ new tails with ramification invariant $\sigma = (p+1)/(p-1)$. The points $\tau_i \in \mathbb{P}^1_k$, $i \in \mathbb{B}_{\mathrm{new}}$ (where the new tails occur) are precisely the zeros of the polynomial*

$$u \;=\; \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j}^2 x^j. \tag{12}$$

Moreover, the stable reduction occurs over the (unique) tame extension K/K_0 of degree $(p^2-1)/2$.

The polynomial u is known as the *Hasse invariant*. It has the property that the elliptic curve given by $y^2 = x(x-1)(x-\lambda)$ is supersingular in characteristic p if and only if λ is a zero of u. It is a solution to the hypergeometric differential equation with parameters $(1/2, 1/2, 1)$. The relation between this differential equation and the reduction of elliptic curves is well understood, see for example [8].

Proof. Let $a_1 = a_2 = a_3 = 0$ and $m = (p-1)/2$. Choose an injective character $\chi : \mathbb{Z}/m \to \mathbb{F}_p^\times$. Let (g, ω) be the special deformation datum of signature $(0,0,0)$ constructed in Proposition 2.2.(ii). Recall that we associate to the triple $(a_1, a_2, a_3) = (0,0,0)$ the hypergeometric differential equation with parameters $A = B = 1/2$ and $C = 1$. Using the recursion (11) one checks that the polynomial u defined by (12) is a solution in characteristic p to this differential equation. This differential equation has a unique monic solution of degree $(p-1)/2$. Therefore, u is the same as in Proposition 2.2 (ii).

Let $Y'_k \to \mathbb{P}^1_k$ be a connected and new $\mathrm{PSL}_2(p)$-tail cover with ramification invariant $\sigma = (p+1)/(p-1)$. The existence of such a tail cover is proved in Lemma 3.3 below. The inertia group of a point above ∞ has order $p(p-1)/2$. For every $i \in \mathbb{B}_{\mathrm{new}}$, we let $\bar{f}_i : \bar{Y}_i \to \bar{X}_i$ be a copy of $Y'_k \to \mathbb{P}^1_k$. Let $\eta_i \in \bar{Y}_i$ be the point whose inertia group consists of the upper triangular matrices in $\mathrm{PSL}_2(p)$. Then the condition of Proposition 1.3 is satisfied. Therefore, there exists a $\mathrm{PSL}_2(p)$-cover $f_K : Y_K \to \mathbb{P}^1_K$ branched at three points of order p whose stable reduction gives rise to the special deformation datum (g, ω) and the tail covers $\bar{f}_i$. This cover is defined and has stable reduction over the tame extension K/K_0 of degree $(p^2-1)/2$. It follows from rigidity that f_K is isomorphic to $X(2p)_K \to X(2)_K$. This proves the proposition. □

Lemma 3.3 *There exist a connected new $\mathrm{SL}_2(p)$-tail cover $h : Y_k \to X_k = \mathbb{P}^1_k$, with inertia group of order $p(p-1)$ and ramification invariant $\sigma = (p+1)/(p-1)$.*

Proof. Let Y_k be the complete nonsingular curve defined by

$$y^{p+1} = x^p - x.$$

The group $\mathrm{SL}_2(p)$ acts on Y_k as follows. For

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(p), \qquad \text{define } Ax = \frac{ax+b}{cx+d}, \quad Ay = \frac{y}{cx+d}.$$

It is easy to check that the quotient map $h : Y_k \to X_k \simeq \mathbb{P}^1_k$ is branched at exactly one point which we may assume to be ∞. The inertia group of some point above ∞ has order $p(p-1)$ and $\sigma = (p+1)/(p-1)$. □

Let $X(p) \to X(1) \simeq \mathbb{P}^1_j$ be the projection of the modular curve $X(p)$ to the j-line. This is a $\mathrm{PSL}_2(p)$-cover with branch cycle description $(3A, 2A, pA)$, which we may assume to be branched at $x_1 = 0, x_2 = 1728, x_3 = \infty$. By Proposition 3.1, it has a unique model $X(p)_K \to \mathbb{P}^1_K$ over any field K of characteristic 0 containing $\sqrt{p^*}$. As before, we take K/K_0 a sufficiently large finite extension and define the stable reduction of $X(p) \to X(1)$ at p as the stable reduction of the model $X(p)_K \to \mathbb{P}^1_K$.

Corollary 3.4 *Define $\alpha = \lfloor p/12 \rfloor$. Let $\bar{Y}' \to \bar{X}'$ be the stable reduction of $X(p) \to X(1)$. Then $\bar{X}'$ has two primitive tails and α new tails. For $i = 1, 2$, denote by $\bar{X}_i$ the primitive tail to which x_i specializes. Then*

$$\sigma_i = \begin{cases} \dfrac{p+1}{p-1} & \text{if } i \in \mathbb{B}_{\mathrm{new}}, \\ \dfrac{\lceil (p-1)/3 \rceil}{p-1} & \text{if } i = 1, \\ \dfrac{2\lceil (p-1)/4 \rceil}{p-1} & \text{if } i = 2. \end{cases}$$

Moreover, the stable reduction occurs over the tame extension K/K_0 of degree $(p^2-1)/2$.

Proof. Consider the commutative diagram

$$\begin{array}{ccc} X(2p)_K & \longrightarrow & X(p)_K \\ \downarrow & & \downarrow \\ X(2)_K & \longrightarrow & X(1)_K. \end{array}$$

The horizontal arrows are Galois covers whose Galois group is the symmetric group S_3 on three letters. Let Y_R be the stable model of $X(2p)_K$. The action of S_3 extends to Y_R and $Y_R/S_3 := Y_R^*$ is a semistable curve, [10, Appendice].

Since S_3 acts on Y_R it follows that the set of new tails of $\bar{X}_0$ is stable under the action of S_3. We claim that the action of S_3 on the set of new tails of $\bar{X}$ has α orbits of length six, one orbit of length three if $p \equiv 3 \bmod 4$ and one orbit of length two if $p \equiv 2 \bmod 3$. Since $\bar{X}_0$ has genus zero, an element of order three in S_3 has two fixed points in $\bar{X}_0 - \{0, 1, \infty\}$. An element of order two in S_3 fixes one of the points $0, 1, \infty$ and has therefore one fixed point in $\bar{X}_0 - \{0, 1, \infty\}$. The claim now follows by distinguishing the four possibilities for $p \bmod 12$.

The curve $X_R^* := Y_R^*/G$ is almost equal to X_R'. The special fiber $\bar{X}^*$ has a tail at zero (resp. 1728) if and only if $p \equiv -1 \bmod 3$ (resp. $p \equiv -1 \bmod 4$), i.e. exactly when zero (resp. 1728) is supersingular. To obtain X_R' one has to perform a suitable blow up centered at the point $j = 0$ (resp. $j = 1728$) on $\bar{X}^*$ if $p \equiv 1 \bmod 3$ (resp. $p \equiv 1 \bmod 4$.) The corollary follows, by analyzing the ramification of $\bar{Y}_0^* \to \bar{X}_0^*$. For future reference, we note that a connected component of $\bar{Y}_1'$ has decomposition group $\mathrm{PSL}_2(p)$ if $p \equiv -1 \bmod 3$ and the nonabelian group of order $3p$ if $p \equiv 1 \bmod 3$. A connected component of $\bar{Y}_2'$ has decomposition group $\mathrm{PSL}_2(p)$ if $p \equiv -1 \bmod 4$ and the dihedral group of order $2p$ if $p \equiv 1 \bmod 3$. □

The hypergeometric differential equation corresponding to $X(p) \to X(1)$ is

$$x(x-1728)u'' + [(2+a_1+a_2)x - 1728(1+a_1)]u' + (1+a_1+a_2)^2 u/4,$$

where $a_1 = \lceil (p-1)/3 \rceil$ and $a_2 = 2\lceil (p-1)/4 \rceil$. The polynomial

$$u = (1728)^\alpha \sum_{n=0}^{\alpha} \binom{a_1+\alpha}{\alpha-n}\binom{\alpha}{n}\left(\frac{x}{1728}\right)^n \in k[x]$$

is a solution to this differential equation. Recall that $j \in k$ is *supersingular* if and only if the corresponding elliptic curve over k is supersingular. It follows that $j \neq 0, 1728$ is supersingular if and only if $u(j) = 0$.

4 The reduction of $X_0(p)$

Let $X_0(p)$ denote the modular curve parameterizing (generalized) elliptic curves with a $\Gamma_0(p)$-structure [4]. We may and will identify $X_0(p)$ with the quotient curve $X(p)/G_0$, where $G_0 \subset G := \mathrm{PSL}_2(p)$ is the standard Borel group, modulo $\pm I$. The G-cover $X(p) \to X(1) = \mathbb{P}^1_j$ gives rise to a non-Galois cover $X_0(p) \to \mathbb{P}^1_j$ which we call the *j-invariant*. We claim that the curve $X_0(p)$ has a *unique* $\mathbb{Q}$-model $X_0(p)_\mathbb{Q}$ such that the j-invariant descends to a cover $X_0(p)_\mathbb{Q} \to \mathbb{P}^1_\mathbb{Q}$. (Of course, the existence of such a $\mathbb{Q}$-model is also a consequence of the modular interpretation of $X_0(p)$.)

To prove the claim, let $G \hookrightarrow S_{p+1}$ denote the standard permutation representation of G coming from the natural action on $\mathbb{P}^1(\mathbb{F}_p)$. Note that G_0 is precisely the stabilizer of ∞. It is well known that the normalizer of G in S_{p+1} is equal to $\mathrm{PGL}_2(p) = \mathrm{Aut}(G)$. In particular, the centralizer of G in S_{p+1} is trivial. Let $\mathbf{C} = (3A, 2A, pA)$ denote the triple of conjugacy classes of G corresponding to the G-cover $X(p) \to X(1)$, as in the previous section. Let $\mathbf{C}'$ denote the image of $\mathbf{C}$ in $\mathrm{PGL}_2(p)$. Then $\mathbf{C}'$ is rigid and rational. Hence the claim follows from standard Galois theory.

For any field K of characteristic zero we denote by $X_0(p)_K$ the K-model of $X_0(p)$ obtained from $X_0(p)_\mathbb{Q}$ by base change. In [4, VI.6.16] Deligne and Rapoport prove the following result.

Theorem 4.1 *Let $X_0(p)_{\mathbb{Z}_p}$ denote the normalization of $\mathbb{P}^1_{\mathbb{Z}_p}$ inside $X_0(p)_{\mathbb{Q}_p}$. Set $k := \bar{\mathbb{F}}_p$.*

(i) *The $\mathbb{Z}_p$-curve $X_0(p)_{\mathbb{Z}_p}$ is semistable (and stable if $g(X_0(p)) > 1$).*

(ii) *The geometric special fiber $X_0(p)_k := X_0(p)_{\mathbb{Z}_p} \otimes k$ is the union of two smooth curves $\bar{W}_0'$, $\bar{W}_0''$ of genus 0. The induced map $\bar{W}_0' \to \mathbb{P}^1_k$ (resp. $\bar{W}_0'' \to \mathbb{P}^1_k$) is an isomorphism (resp. purely inseparable of degree p). The components $\bar{W}_0'$ and $\bar{W}_0''$ intersect precisely in the* supersingular points*, i.e. the points of $X_0(p)_k$ with supersingular j-invariant.*

(iii) *Let $x \in X_0(p)_k$ be a supersingular point, with j-invariant $j_x \in k$. If $j_x \equiv 0$ then $X_0(p)_{\mathbb{Z}_p}$ has a singularity of type A_3 at x. If $j_x \equiv 1728$ then x presents a singularity of type A_2. Otherwise, x is a regular point of $X_0(p)_{\mathbb{Z}_p}$.*

We give a proof of this theorem using the results of the previous section.

Proof. Let $R_0 := W(k)$ denote the ring of Witt vectors and K_0 the fraction field of R_0. Note that

$$X_0(p)_{R_0} \;:=\; X_0(p)_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} R_0$$

is equal to the normalization of $\mathbb{P}^1_{R_0}$ in the function field of $X_0(p)_{K_0}$. Hence it suffices to prove the theorem with the ring $\mathbb{Z}_p$ replaced by R_0.

Let K/K_0 be the tame extension of degree $(p^2-1)/2$. By Corollary 3.4 the $\mathrm{PSL}_2(p)$-cover $Y_K := X(p)_K \to X_K := \mathbb{P}^1_K$ extends to a stable model $Y_R \to X_R$ over the ring of integers R of K. As before, we denote by $\bar{Y} \to \bar{X}$ the special fiber of $Y_R \to X_R$.

Set $W_R := Y_R/G_0$. By [10, Appendice], W_R is a semistable curve over R with generic fiber $W_K = X_0(p)_K$. By construction, we have a finite map $W_R \to X_R$. Let $\bar{W}$ denote the special fiber of W_R. The formation of the quotient Y_R/G_0 does not commute with base change, in general. However, the canonical map $\bar{Y}/G_0 \to \bar{W}$ is a homeomorphism. Let V be an irreducible component of $\bar{Y}$ and U its image in $\bar{W}$. Let $D(V) \subset G$ (resp. $I(V) \subset G$) denote the decomposition group (resp. the inertia group) of V. Then the natural map $V/(D(V) \cap G_0) \to U$ is purely inseparable of degree $|I(V) \cap G_0|$. Using Corollary 3.4 and the description of the stable reduction in Section 1, we see that $\bar{W}$ has four different types of components (see Figure 2 for the case $p = 29$). In the description below we call an irreducible component of $\bar{W}$ *horizontal* if it is mapped to the central component $\bar{X}_0$ of $\bar{X}$ and *vertical* otherwies, cf. Figure 1.

(a) A horizontal component $\bar{W}_0'$ which is the image of the (unique) horizontal component $\bar{Y}_0 \subset \bar{Y}$ with decomposition group G_0. The natural map $\bar{W}_0' \to \bar{X}_0 = \mathbb{P}^1_k$ is an isomorphism.

(b) Another horizontal component $\bar{W}_0''$ which is the image of the set of horizontal components of $\bar{Y}$ different from $\bar{Y}_0$. Note that if $\bar{Y}'' \neq \bar{Y}_0$ is such a horizontal component, with decomposition group D'', then $D'' \cap G_0$ is a cyclic group of order $(p-1)/2$ (a split torus). Therefore, the natural map $\bar{W}_0'' \to \bar{X}_0$ is purely inseparable of degree p.

(c) For $i \in \mathbb{B}_{\rm new} \cup \mathbb{B}_{\rm prim}$ we let $\bar{W}_i$ be the image of the tail cover $\bar{Y}_i$. Suppose that i is supersingular, i.e. that the tail $\bar{X}_i$ intersects $\bar{X}_0 = \mathbb{P}^1_k$ in a supersingular point. Then $\bar{Y}_i$ and — hence $\bar{W}_i$ as well — is connected. The curve $\bar{W}_i$ intersects each of the horizontal components $\bar{W}_0$ and $\bar{W}_0'$ in a unique point.

(d) With notation as in (c), suppose that i is not supersingular (in particular, $i \in \mathbb{B}_{\rm prim}$). Then $\bar{Y}_i$ is not connected, and the decomposition group of any connected component is isomorphic to $\mathbb{Z}/p \rtimes \mathbb{Z}/2$ or $\mathbb{Z}/p \rtimes \mathbb{Z}/3$ (depending on whether $x_i \equiv 1728$ or $x_i \equiv 0$). It follows that $\bar{W}_i$ has exactly two connected components $\bar{W}_i'$ and $\bar{W}_i''$. The curve $\bar{W}_i'$ (resp. $\bar{W}_i''$) intersects $\bar{W}_0'$ (resp. $\bar{W}_0''$) in a unique point. (See the end of the proof of Corollary 3.4.)

In the modular picture, the component $\bar{W}_0'$ (resp. $\bar{W}_0''$) corresponds generically to ordinary elliptic curves together with a subgroup scheme isomorphic to $\boldsymbol{\mu}_p$ (resp. to $\mathbb{Z}/p$), see [4, VI.6]. The vertical components have no easy modular interpretation. Note that every component of $\bar{W}$ has genus 0.

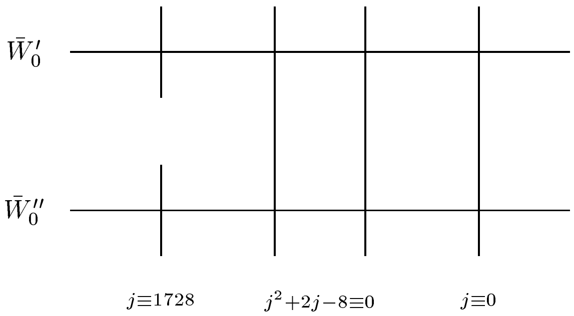

Figure 2: The curve $\bar{W}$ for $p = 29$

Let W_R' be the curve obtained from W_R by contracting all vertical components of $\bar{W}$. Since these vertical components have genus zero and self-intersection number -1 or -2, the curve W_R'

is semistable. In particular, W'_R is a normal scheme. Recall that the curve obtained from X_R by contracting the tails $\bar{X}_i$ is equal to $\mathbb{P}^1_R$. Therefore the finite map $W_R \to X_R$ gives rise to a finite map $W'_R \to \mathbb{P}^1_R$. We conclude that W'_R is the normalization of $\mathbb{P}^1_R$ inside the function field of $W_K = X_0(p)_K$.

Let $\Gamma := \mathrm{Gal}(K/K_0) \cong \mathbb{Z}/N$, and recall that $N = (p^2-1)/2$ is prime to p. Since $W_K = X_0(p)_{K_0} \otimes_{K_0} K$, the group Γ acts naturally on W_K. Since W'_R is the normalization of $\mathbb{P}^1_R$ in W_K this action extends to the R-model W'_R and

$$X_0(p)_{R_0} \;=\; W'_R/\Gamma. \tag{13}$$

Since the order of Γ is prime to p, formation of the quotient commutes with base change. In particular, we have

$$X_0(p)_k \;=\; \bar{W}'/\Gamma. \tag{14}$$

It is clear that the action of Γ commutes with the map $\bar{W}' \to \mathbb{P}^1_k$ coming from the j-invariant. Since this map is an isomorphism on one and purely inseparable of degree p on the other component, Γ acts trivially on $\bar{W}'$. Now Parts (i) and (ii) of the theorem follow from (14) and the description of the components of $\bar{W}$ given above.

It remains to prove Part (iii) of the theorem. Let $x \in X_0(p)_k = \bar{W}'$ be a supersingular point, with j-invariant $j_x \in k$. Let v denote the valuation on K, normalized such that $v(p) = 1$. Since x is an ordinary double point of $\bar{W}'$, the local ring of $X_0(p)_{R_0}$ at x is of the form $R_0[[u, v \mid uv = \pi]]$, with $\pi \in R_0$. We define the *thickness* of $X_0(p)_{R_0}$ at x as the rational number $e(x) := v(\pi)$. We have to show that $e(x)$ is equal to 3 if $j_x \equiv 1728$, equal to 2 if $j_x \equiv 0$ and equal to 1 otherwise.

We assume that $j_x \not\equiv 0, 1728$. The other cases follow in the same manner. Let $x' \in \bar{W}'$ be the unique point lying above x. Also, let x'' and x''' be the two double points on $\bar{W}$ lying above x'. We assume that $x'' \in \bar{W}'_0$ and $x''' \in \bar{W}''_0$. It is easy to see that

$$e(x) \;=\; e(x') \;=\; e(x'') + e(x'''). \tag{15}$$

Let $y'', y''' \in \bar{Y}$ be points above x'', x'''. Recall that $W_R = Y_R/G_0$. By [10, Appendice], we have $e(x'') = |\mathrm{Stab}_{G_0}(y'')| \cdot e(y'')$ and $e(x''') = |\mathrm{Stab}_{G_0}(y''')| \cdot e(y''')$. Using (15) and our knowledge of the G-action on $\bar{Y}$, we see that

$$e(x) \;=\; \frac{p(p-1)}{2} \cdot e(y'') + \frac{p-1}{2} \cdot e(y'''). \tag{16}$$

It is proved in [16] that the thickness of any double point $y \in \bar{Y}$ is equal to $(h_i(p-1))^{-1}$ if y lies on the tail $\bar{Y}_i$ and h_i denotes the conductor of the tail cover $\bar{Y}_i \to \bar{X}_i$ at ∞. Since we assumed that $j_x \not\equiv 0, 1728$ we have $y'', y''' \in \bar{Y}_i$ for some $i \in \mathbb{B}_{\mathrm{new}}$. By Corollary 3.4 we have $h_i = (p+1)/2$ for $i \in \mathbb{B}_{\mathrm{new}}$. With (16) we conclude that

$$e(x) \;=\; \frac{p}{p+1} + \frac{1}{p+1} \;=\; 1.$$

This finishes the proof of the theorem. □

One can analyze the natural R_0-model of $X_1(p)$ in an entirely analogous manner. This would give a new proof of the result of [4] that $J_1(p)/J_0(p)$ has good reduction over $\mathbb{Q}(\zeta_p)$. One can also derive this result directly from our knowledge of the stable reduction of $X(p)$.

5 Three point covers with Galois group $\mathrm{SL}_2(p)$

In this section we compute the stable reduction of all $\mathrm{SL}_2(p)$-covers of $\mathbb{P}^1$ branched at three points. In particular, we obtain an explicit formula for the number of such covers with good reduction

(Theorem 5.6). To prove this we use the results of the previous sections. In addition, we use the fact that some $\mathrm{SL}_2(p)$-covers have a modular interpretation as a *Hurwitz space*.

Let us give an outline of the proof of Theorem 5.6. We first show that the $\mathrm{SL}_2(p)$-covers of $\mathbb{P}^1$ branched at three points of order p, p, n are essentially Hurwitz spaces. These covers have bad reduction to characteristic p; their stable reduction is described in [2]. By considering the (unique) primitive tail of the stable reduction, we obtain one primitive tail cover for every noncentral conjugacy class of $\mathrm{SL}_2(p)$ whose order is prime to p. Proposition 5.5 states that every primitive $\mathrm{SL}_2(p)$-tail cover with group $\mathrm{SL}_2(p)$ arises in this way. Then we show (Proposition 5.3) that the only new tail cover that occurs is the cover constructed in Lemma 3.3. This implies that the special deformation datum of an $\mathrm{SL}_2(p)$-cover branched at three points is hypergeometric (Definition 2.1). Therefore, Proposition 1.3 allows to construct all $\mathrm{SL}_2(p)$-covers with bad reduction at p, by lifting. This also gives a formula for the number of covers with good reduction. Passing to the quotient modulo $-I$, one obtains similar result for three point covers with Galois group $\mathrm{PSL}_2(p)$.

In this section, R is a complete mixed characteristic discrete valuation ring which contains $\sqrt{p^*}$ and whose residue field is an algebraically closed field k of characteristic p. We let K denote the fraction field of R.

Lemma 5.1 *Let $D \in \{C(l), \tilde{C}(l)\}$. Let $f : Y \to \mathbb{P}^1_K$ be an $\mathrm{SL}_2(p)$-Galois cover with class vector $\mathbf{C}_1 = (pA, pA, D)$ or $\mathbf{C}_2 = (pA, pB, D)$. Let $\bar{Y} \to \bar{X}$ be the stable reduction of f. The curve $\bar{X}$ has exactly one primitive tail, with ramification invariant*

$$\sigma = \begin{cases} \dfrac{p-1-2l}{p-1} & \text{if } D = C(l), \\ \dfrac{p+1-2l}{p-1} & \text{if } D = \tilde{C}(l). \end{cases}$$

The inertia group of the primitive tail has order $p(p-1)/\gcd(p-1, l)$ if $D = C(l)$ and $p(p-1)/\gcd(p-1, l-1)$ otherwise. The new tails have ramification invariant $\sigma = (p+1)/(p-1)$ and an inertia group of order $p(p-1)$.

For $\mathrm{SL}_2(p)$-covers with ramification of order n, one can prove a strengthening of Proposition 3.1, cf. [14, Lemma 3.29]. Either there exists a cover with class vector $\mathbf{C}_1$ or there exists a cover with class vector $\mathbf{C}_2$. In both cases, there is a unique such cover. The outer automorphism of $\mathrm{SL}_2(p)$ conjugates the cover with class vector $\mathbf{C}_1$ (resp. $\mathbf{C}_2$) to a cover with class vector (pB, pB, D) (resp. (pB, pA, D)). Therefore, in both cases, there are exactly two covers with ramification (p, p, D), up to isomorphism.

Proof. The case $D = C(l)$ is treated in [2, Section 8]. The idea of the proof is as follows. Define $m = (p-1)/\gcd(p-1, l)$. For $\lambda \in \mathbb{P}^1 - \{0, 1, \infty\}$, let W_λ be a connected component of the nonsingular projective curve corresponding to

$$w^{p-1} = x^l (x-1)^l (x-\lambda)^{p-1-l}.$$

This defines a family of m-cyclic covers $g_\lambda : W_\lambda \to \mathbb{P}^1$, branched at four points. Fix an injective character $\chi : \mathbb{Z}/m \to \mathbb{F}_p^\times$ and let $N = \mathbb{Z}/p \rtimes_\chi \mathbb{Z}/m$. Define the Hurwitz space $\mathbb{H}$ parameterizing N-Galois covers branched at $0, 1, \lambda, \infty$ of order prime to p which factor via g_λ. Define $\mathbb{H} \to \mathbb{P}^1_\lambda$ by mapping an N-cover to the branch point λ and let $f : \tilde{\mathbb{H}} \to \mathbb{P}^1_\lambda$ its Galois closure. The Galois group of f is either $\mathrm{SL}_2(p)$ or $\mathrm{PSL}_2(p)$. If it is $\mathrm{SL}_2(p)$, the class vector of f is (D_1, D_2, D), with $D_1, D_2 \in \{pA, pB\}$. Otherwise, there exists a unique lift of f to a cover with such a class vector. Therefore, f is isomorphic to the cover of the statement of the proposition. In [2], the stable reduction of f is computed, by using the moduli interpretation of $\mathbb{H}$.

The proof for $D = \tilde{C}(l)$ is analogous. (Take $m|(p+1)$ and $N \simeq (\mathbb{Z}/p)^2 \simeq \mathbb{Z}/m$.) □

The following lemma is due to R. Pries (unpublished).

Lemma 5.2 *Let G be a finite group. Let $\varphi : W \to \mathbb{P}^1_k$ be a new G-tail cover with ramification invariant σ and inertia group I of order pn. Suppose $1 < \sigma < 2$. Then there exists a G-cover $f : Y \to \mathbb{P}^1_K$ with signature (p,p,n) such that φ occurs as the unique new tail of the stable reduction of f.*

If $\sigma = 2$ then φ can be lifted to a cover in characteristic zero which is branched at three points of order p, [3, Section 3.2].

Proof. Write $n = m_1 m_2$, where m_2 is the order of the prime-to-p part of the center of I. Then m_1 divides $p-1$ and $\sigma - 1 = a/m_1$ for some $0 < a < m_1$. Write $\alpha = (p-1)/m_1$. Choose $\lambda \in k - \{0,1\}$ such that $(1-\lambda)^{\alpha a} = 1$. Note that $\sigma \neq p/(p-1)$, since conductors are prime to p. Therefore, $\alpha a \neq 1$ and it is possible to choose λ as asserted.

Let $g_0 : \bar{Z}_0 \to \bar{X}_0$ be the m_1-cyclic cover where $\bar{Z}_0$ is defined by $z^{m_1} = x^{-a}(x-\lambda)^a$. Let $g : \bar{Z} \to \mathbb{P}^1_k$ be the n-cyclic cover branched only at 0 and λ which has g_0 as a quotient. Define the differential

$$\omega \;=\; \frac{\epsilon\, z\, \mathrm{d}x}{x(x-1)}$$

on $\bar{Z}$, with ϵ as in (10). A straightforward computation, as in the proof of Proposition 2.2, shows that (g,ω) is a special deformation datum. There is one primitive critical point at zero and one new critical point at λ.

Define a primitive I-tail cover $\psi' : \bar{Y}' \to \mathbb{P}^1_k$ which is totally ramified at ∞ with ramification invariant $\sigma = (m_1 - a)/m_1$ and branched of order n at 0. Let $\psi := \mathrm{Ind}_I^G \psi'$. One checks that the datum (g,ω,ψ,φ) satisfies the conditions of Proposition 1.3. We conclude that there exists a G-Galois cover $f : Y \to \mathbb{P}^1_K$ which is branched at three points with ramification of order (p,p,n) such that its stable reduction gives rise to (g,ω,ψ,φ). This proves the lemma. □

It follows from rigidity that the special deformation datum associated to an $\mathrm{SL}_2(p)$-cover with bad reduction is uniquely determined by the invariants h_i and m_i. On the other hand, the special deformation datum (g,ω) in the proof of Lemma 5.2 depends also on the choice of $\lambda \in k - \{0,1\}$ with $(1-\lambda)^{\alpha a} = 1$. It follows that we have $\alpha a = 2$ in case $G = \mathrm{SL}_2(p)$. This statement is also a consequence of the next proposition.

Proposition 5.3 *Suppose that G is either $\mathrm{SL}_2(p)$ or $\mathrm{PSL}_2(p)$. Let $\varphi : W \to \mathbb{P}^1_k$ be a new G-tail cover with ramification invariant σ. Suppose that $1 < \sigma \leq 2$. Then $\sigma = (p+1)/(p-1)$. The order of the inertia group is $p(p-1)$ if $G = \mathrm{SL}_2(p)$ and $p(p-1)/2$ if $G = \mathrm{PSL}_2(p)$. Furthermore, the cover φ is unique, up to isomorphism.*

Proof. If there exists a new $\mathrm{SL}_2(p)$-tail cover φ with $\sigma \neq 2$, Lemma 5.2 implies that φ occurs as the restriction to a new tail of the stable reduction of a $\mathrm{SL}_2(p)$-cover with signature (p,p,n) for some n prime-to-p. Therefore Lemma 5.1 implies that $\sigma = (p+1)/(p-1)$.

Similarly, one shows that every $\mathrm{SL}_2(p)$-cover of $\mathbb{P}^1_k$ branched at one point, with $\sigma = 2$, can be lifted to a cover of $\mathbb{P}^1_K$ which is branched at three points of order p. The proposition follows in this case from Proposition 3.2 and Proposition 3.1, cf. [3, Corollary 3.2.2].

Since every $\mathrm{PSL}_2(p)$-cover of $\mathbb{P}^1_K$ with ramification of order p,p,n' can be lifted to an $\mathrm{SL}_2(p)$-cover with ramification of order p,p,n (where n is n' or $2n'$), the proposition also follows for $G = \mathrm{PSL}_2(p)$. □

Corollary 5.4 *Let G be $\mathrm{SL}_2(p)$ or $\mathrm{PSL}_2(p)$. Let $f : Y \to \mathbb{P}^1_K$ be a G-Galois cover branched at three points. Suppose that f has bad reduction. Then the special deformation datum corresponding to f is hypergeometric.*

Proof. $f : Y \to \mathbb{P}^1_K$ be a G-Galois cover branched at three points. Suppose that f has bad reduction. Proposition 5.3 implies that $\sigma_i = (p+1)/(p-1)$ for $i \in \mathbb{B}_{\rm new}$. Therefore the corollary follows from Definition 2.1. □

Proposition 5.5 *(i) Let $\varphi : W \to \mathbb{P}^1_k$ be a (possibly nonconnected) primitive* $\mathrm{SL}_2(p)$*-tail cover defined over k, with ramification invariant σ. Suppose that $0 < \sigma < 1$. Denote by D the conjugacy class in* $\mathrm{SL}_2(p)$ *of the canonical generator of a point of W above 0, with respect to the fixed roots of unity. Then*

$$\sigma = \begin{cases} \dfrac{p-1-2l}{p-1} & \text{if } D = C(l), \\ \dfrac{p+1-2l}{p-1} & \text{if } D = \tilde{C}(l). \end{cases}$$

(ii) The decomposition group of an irreducible component of W is $\mathrm{SL}_2(p)$ *if $D = \tilde{C}(l)$ and is a semidirect product of order $p(p-1)/gcd(p-1,l)$ if $C = C(l)$.*

Proof. Write $\sigma = a/(p-1)$. The normalizer $N_G(P)$ of a Sylow p-subgroup P in $\mathrm{SL}_2(p)$ has order $p(p-1)$. Since the center of $N_G(P)$ has order two, it follows that a is even. Therefore $(p-1-a)/2$ is a positive integer.

Proposition 2.2 (ii) shows that there exists a hypergeometric deformation datum (g', ω') of signature $(0,0,a)$, where $g' : Z'_k \to \mathbb{P}^1_k$ is a $(p-1)/2$-cyclic cover, given by

$$z'^{(p-1)/2} = \prod_{i \in \mathbb{B}_{\rm new}} (x - \tau_i).$$

We define $g : Z_k \to \mathbb{P}^1_k$ to be the $(p-1)$-cyclic cover given by

$$z^{p-1} = \prod_{i \in \mathbb{B}_{\rm new}} (x - \tau_i).$$

Let ω be the pull back of ω' to Z_k. Then (g, ω) is a special deformation datum. Note that $|\mathbb{B}_{\rm prim}| = 1$ and $|\mathbb{B}_{\rm new}| = (p-1-a)/2$, with $a = p-1-2l$ if $D = C(l)$ and $a = p+1-2l$ if $D = \tilde{C}(l)$. The primitive critical point is at ∞, where the cover g is branched of order $(p-1)/(p-1,l)$ if $D = C(l)$ and of order $(p-1)/(p-1,l-1)$ otherwise.

Let h be the $\mathrm{SL}_2(p)$-tail cover constructed in Lemma 3.3. For every $i \in \mathbb{B}_{\rm new}$, let $\bar{f}_i$ be a copy of h. Proposition 1.3 shows that there exists an $\mathrm{SL}_2(p)$-cover $f : Y \to \mathbb{P}^1_K$ whose stable reduction gives rise to the special deformation datum (g, ω), the new tail covers $\bar{f}_i$ and the primitive tail cover φ. By construction, the class vector of f is (D_1, D_2, D) with $D_1, D_2 \in \{pA, pB\}$. Therefore f is isomorphic to a cover described in Lemma 5.1. Part (i) of the proposition follows from this.

Let N denote the decomposition group of an irreducible component of W. Suppose $D = \tilde{C}(l)$, for some $l < (p-1)/2$. Then N contains an element of order p and an element of order $(p+1)/\gcd(p+1,l) > 2$. Therefore, $N = \mathrm{SL}_2(p)$, [6, Section II.8].

Next suppose that $D = C(l)$. Put $n_l = (p-1)/\gcd(p-1,l)$. It is easy to construct a primitive tail cover with Galois group $\mathbb{Z}/p \rtimes \mathbb{Z}/n_l$ which is branched at zero of order n_l and has ramification invariant $\sigma = (p-1-2l)/(p-1)$. Let φ' be the primitive $\mathrm{SL}_2(p)$-tail cover obtained by induction. Using again Proposition 1.3, we see that there exists an $\mathrm{SL}_2(p)$-cover $f' : Y' \to \mathbb{P}^1_K$ whose stable reduction gives rise to the special deformation datum (g, ω), the new tail covers $\bar{f}_i$ and the primitive tail cover φ'. Note that f' has the same branch cycle description as f. It follows from Proposition 3.1 that f and f' are outer isomorphic, i.e. become isomorphic as $\mathrm{SL}_2(p)$-covers after twisting by an outer automorphism of $\mathrm{SL}_2(p)$. We conclude that N is an extension of $\mathbb{Z}/n_l$ by $\mathbb{Z}/p$. □

Theorem 5.6 *Let* $\mathbf{C} = (C_1, C_2, C_3)$ *be a triple of conjugacy classes of* $\mathrm{SL}_2(p)$*, where we suppose that the elements of the* C_i *are not contained in the center.*

(a) If C_i *contains an element of order* p *for some* i*, all covers with class vector* $\mathbf{C}$ *have bad reduction.*

(b) Suppose $C_i \in \{C(l), \tilde{C}(l)\}$ *and put* $a_i = p-1-2l$ *if* $C_i = C(l)$ *and* $a_i = p+1-2l$ *otherwise. Write*

$$\mathrm{Ni}_3^{\mathrm{bad}}(\mathbf{C}) \;=\; \{\, f \in \mathrm{Ni}_2^{\mathrm{in}}(\mathbf{C}) \mid \, f \textit{ has bad reduction.} \,\}.$$

Then

$$|\,\mathrm{Ni}_3^{\mathrm{bad}}(\mathbf{C})| \;=\; \begin{cases} 2 & \textit{if } a_1+a_2+a_3 < p-1, \\ 2 & \textit{if } a_1+a_2+a_3 = p-1 \textit{ and } C_i = \tilde{C}(l) \textit{ for some } i, . \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Let $f : Y \to \mathbb{P}^1_K$ be an $\mathrm{SL}_2(p)$-cover with class vector $\mathbf{C} = (C_1, C_2, C_3)$. If p divides one of the ramification indices of f, then f has bad reduction, so (a) is obvious.

Suppose that p does not divide the ramification indices of f. If f has bad reduction, then (7) implies that $a_1 + a_2 + a_3 \leq p-1$. If $a_1 + a_2 + a_3 = p-1$, there are no new tails. Since $\bar{Y}$ is connected, at least one of the primitive tails has decomposition group $\mathrm{SL}_2(p)$. Therefore Proposition 5.5 implies that $C_i = \tilde{C}(l)$, for some i. This shows that if there exists a cover with bad reduction, then either $a_1 + a_2 + a_3 < p-1$ or $a_1 + a_2 + a_3 = p-1$ and $C_i = \tilde{C}(l)$ for some i.

Now suppose that C_1, C_2, C_3 are conjugacy classes of noncentral elements of order prime to p such that the condition of the theorem is satisfied. Let a_1, a_2, a_3 be as in the statement of the theorem. Recall that a_i is even and different from $p-1$. Let (g', ω') be the hypergeometric deformation datum of signature (a_1, a_2, a_3) constructed in Proposition 2.2 (ii). The cover $g' : Z'_k \to \mathbb{P}^1_k$ is the $(p-1)/2$-cyclic cover defined by

$$z'^{(p-1)/2} \;=\; x^{a_1/2}(x-1)^{a_2/2} \prod_{i \in \mathbb{B}_{\mathrm{new}}} (x - \tau_i), \quad (z, x) \mapsto x.$$

We define a $(p-1)$-cyclic cover $g : Z_k \to \mathbb{P}^1_k$, factoring through g' by

$$z^{p-1} \;=\; x^{b_1}(x-1)^{b_2} \prod_{i \in \mathbb{B}_{\mathrm{new}}} (x - \tau_i), \quad (z, x) \mapsto x,$$

where $b_i = a_i/2 + (p-1)/2$, i.e. $b_i = p-1-l$ if $C_i = C(l)$ and $b_i = p-l$ otherwise. Then (g, ω) is a special deformation datum.

We define a set of tail covers, as follows. For $i \in \mathbb{B}_{\mathrm{new}}$, we define $\bar{f}_i \simeq h$, where h is the new $\mathrm{SL}_2(p)$-tail cover of $\mathbb{P}^1_k$ with $\sigma = (p+1)/(p-1)$ from Lemma 3.3. For $i \in \mathbb{B}_{\mathrm{prim}} = \{1, 2, 3\}$, we let $\bar{f}_i$ be the primitive $\mathrm{SL}_2(p)$-tail cover with $\sigma = a_i/(p-1)$ whose existence is guaranteed by Lemma 5.1. As in the proof of Lemma 5.2, one checks that the datum $(g, \omega; \bar{f}_i)$ satisfies the conditions of Proposition 1.3. Hence there exists an $\mathrm{SL}_2(p)$-cover $f : Y \to \mathbb{P}^1_K$ with class vector $\mathbf{C} = (C_1, C_2, C_3)$ whose stable reduction gives rise to the datum $(g, \omega; \bar{f}_i)$.

Since the outer automorphism group of $\mathrm{SL}_2(p)$ has order two, the number of liftings, up to isomorphism, is at least two. Proposition 3.1 implies that the number of elements of $\mathrm{Ni}_3^{\mathrm{in}}(\mathbf{C})$ is at most two. We conclude that the number of liftings is exactly two. This proves that all $\mathrm{SL}_2(p)$-covers over K with class vector $\mathbf{C}$ have bad reduction to characteristic p. □

Institut für Experimentelle Mathematik
Universität GH Essen
Ellernstr. 29

Max–Planck–Institut für Mathematik
Vivatsgasse 7
53111 Bonn, Germany

45326 Essen, Germany
bouw@exp-math.uni-essen.de

wewers@mpim-bonn.mpg.de

References

[1] F. Beukers. On Dwork's accessory parameter problem. Preprint, 2002.

[2] I. I. Bouw. Reduction of metacyclic covers and their Hurwitz spaces. arXiv:math.AG/020403, 2002.

[3] I. I. Bouw and R. J. Pries. Rigidity, reduction, and ramification. To appear in *Math. Ann.*

[4] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, number 349 in LNM, pages 143–316. Springer-Verlag, 1972.

[5] B. Edixhoven. Minimal resolution and stable reduction of $X_0(N)$. *Ann. Inst. Fourier*, 40(1):31–67, 1990.

[6] B. Huppert. *Endliche Gruppen I.* Number 134 in Grundlehren. Springer-Verlag, 1967.

[7] Y. Ihara. On the differentials associated to congruence relations and Schwarzian equations defining uniformizations. *J. Fac. Sci. Univ. Tokyo, Sect. IA Math.*, 21:309–332, 1974.

[8] N. M. Katz. Expansion-coefficients as approximate soluations of differential equations. In *p-adic cohomology*, Astérisque, 119-120, pages 183–189, 1984.

[9] N. M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves.* Number 108 in Annals of Mathematical Studies. Princeton Univ. Press, 1985.

[10] M. Raynaud. p-groupes et réduction semi-stable des courbes. In P. Cartier, editor, *Grothendieck Festschrift III*, number 88 in Progress in Math., pages 179–197. Birkhäuser, 1990.

[11] M. Raynaud. Spécialisation des revêtements en caractéristique $p > 0$. *Ann. Sci. École Norm. Sup.*, 32(1):87–126, 1999.

[12] J.-P. Serre. *Topics in Galois Theory.* Research notes in mathematics, 1. Jones and Bartlett Publishers, 1992. Lecture notes prepared by Henri Darmon.

[13] K. Strambach and H. Völklein. On linear rigid triples. *J. Reine Angew. Math.*, 510:57–62, 1999.

[14] H. Völklein. *Groups as Galois Groups.* Number 53 in Cambridge Studies in Adv. Math. Cambridge Univ. Press, 1996.

[15] S. Wewers. Reduction and lifting of special metacyclic covers. To appear in: *Ann. Sci. École Norm. Sup.*

[16] S. Wewers. Three point covers with bad reduction. arXiv:math.AG/0205026, 2002.