Finite Fields and Their Applications **7,** 415–420 (2001)
doi: 10.1006/ffta.2001.0319, available online at http://www.idealibrary.com on IDEAL®

Singularities of the Modular Curve

Alexander Klyachko and Orhun Kara

Department of Mathematics, Bilkent University, 06533 Ankara, Turkey
E-mail: klyachko@fen.bilkent.edu.tr, okara@fen.bilkent.edu.tr

Communicated by Michael Tsfasman

Received April 13, 1999; revised January 4, 2000; published online June 11, 2001

Let $X_0(\ell)$ be the modular curve, parameterizing cyclic isogenies of degree ℓ, and $Z_0(\ell)$ be its plane model, given by the classical modular equation $\Phi_\ell(X, Y) = 0$. We prove that all singularities of $Z_0(\ell)$, except two cusps, are intersections of smooth branches, and evaluate the order of contact of these branches. © 2001 Academic Press

1. INTRODUCTION

The family of classical modular curves $X_0(\ell)$, parameterizing cyclic isogenies of elliptic curves $\rho: E \to E'$ of degree ℓ, provides the first known example which attains the Drinfeld–Vladuţ bound (see [6], where one can also find another such example based on Drinfeld curves). Since then only one essentially different construction was discovered by Garcia and Stichtenoth [3]. So the modular curves are still interesting for coding theory.

The simplest code associated with the modular curve comes from configuration of its rational points via canonical embedding $X_0(\ell) \hookrightarrow \mathbb{P}(\Omega)$. To realize this construction one needs a description of the space of regular differentials Ω. For a plane *nonsingular* curve $X: F(x, y, z) = 0$ of degree d the regular differentials are of the form

$$\omega = p\,\frac{xdy - ydx}{F_z} = p\,\frac{ydz - zdy}{F_x} = p\,\frac{zdx - xdz}{F_y}, \tag{1}$$

where $p = p(x, y, z)$ is a homogeneous polynomial of degree $d - 3$. This description may be easily modified for a *singular* curve X by adding some local restrictions on p at singularities (see Remark 1.1 below).

1071-5797/01 $35.00

This observation motivates our interest to singularities of the *plane model* $Z_0(\ell)$ of $X_0(\ell)$. It comes from the projection $\pi: X_0(\ell) \to \mathbb{P}^2$, given in affine coordinates by $\rho \mapsto (j(E),\ j(E'))$, and may be defined explicitly by the classical modular equation

$$Z_0(\ell): \Phi_\ell(X, Y) = 0 \tag{2}$$

of degree 2ℓ. Henceforth we suppose ℓ to be a prime, not equal to the characteristic p.

We prove (Proposition 2.2) that for $p \neq 2,3$ the projection $\pi: X_0(\ell) \to \mathbb{P}^2$ is immersion outside of two cusps $0, \infty \in X_0(\ell)$, and at the cusps the plane model $Z_0(\ell)$ has singularities analytically equivalent to that of equation $x^\ell = y^{\ell-1}$ at the origin.

Hence all noncuspidal singularities of $Z_0(\ell)$ are intersections of smooth branches. The main results of the paper describe them in positive characteristic $p > 3$. It may be stated as follows.

THEOREM 1.1. *Let $\sigma, \rho: E \to E'$ be two nonequivalent isogenies of degree ℓ, $\alpha = \rho^*\sigma \in \mathrm{End}(E)$, and $m(\sigma, \rho)$ be the order of contact of the corresponding smooth branches of the plane model at the point $(E, E') \in Z_0(\ell)$. Then*

$$m(\sigma, \rho) = \begin{cases} p^\nu, & \text{if } p \text{ splits in } \mathbb{Q}(\alpha), \\ 2 + 2p + \cdots + 2p^{\nu-1} + p^\nu, & \text{if } p \text{ is inert in } \mathbb{Q}(\alpha), \\ 2 + 2p + \cdots + 2p^\nu, & \text{if } p \text{ is ramified in } \mathbb{Q}(\alpha). \end{cases}$$

Here $\rho^*: E' \to E$ is the dual isogeny, and p^ν is the p-part of conductor of α (i.e., index of $\mathbb{Z}[\alpha]$ in the ring of integers of the imaginary quadratic field $\mathbb{Q}(\alpha)$).

In the first case, which deals with *ordinary* elliptic curves, the result is known to a number of experts, see, for example, [5].[1] It is also plain that in characteristic zero all singularities of $Z_0(\ell)$, except the cusps, are simple nodes.

Remark 1.1. The singularity at an ordinary point $(E, E') \in Z_0(\ell)$ consists of two branches with order of contact equal to p-part of conductor of α. The local equation on differential (1) for such a singularity reduces to vanishing of all derivatives of $p(x, y, z)$ in the tangent direction to the branches up to the order of contact. For a supersingular point the number of branches may be more then two, but the corresponding local equation on p again amounts to vanishing of all derivatives in direction of each branch up to *sum* of its orders of contact with the other branches.

[1] We are grateful to the referee for this remark.

2. GENERALITIES

We first consider the cusps.

PROPOSITION 2.1. *Over a field of characteristic $p \neq \ell$ the singularities of the plane model $Z_0(\ell)$ at cusps are analytically equivalent to that of equation $y^\ell = z^{\ell-1}$ at the origin.*

Proof. The two cusps are permuted by Fricke involution, which on $Z_0(\ell)$ acts as $(j(E), j(E')) \mapsto (j(E'), j(E))$. So it suffices to consider the cusp at ∞, with local parameter q and formal series expansion

$$j(q) = \frac{1}{q} + 744 + 196884q + \cdots = \frac{1}{q} + \sum_{n \geq 0} c_n q^n, \qquad c_n \in \mathbb{Z}.$$

At the cusp $q = 0$ the curve $Z_0(\ell)$ has parametrization $(j(q) : j(q^\ell) : 1) = (q^{\ell-1}u : 1 : q^\ell v)$ where $u = u(q)$, and $v = v(q)$ are power series with leading term 1. Put $x = q^{\ell-1}u$ and $z = q^\ell v$. Then

$$z^{\ell-1} = q^{\ell(\ell-1)}v^{\ell-1} = x^\ell u^{-\ell} v^{\ell-1} = y^\ell,$$

where $y = xu^{-1}v^{1-1/\ell}$ is a well defined power series over a field of characteristic $p \neq \ell$. Hence the cusp singularity is analytically equivalent to that of equation $y^\ell = z^{\ell-1}$. ■

COROLLARY 2.1. *The index of the singularity at a cusp is $(\ell-1)(\ell-2)/2$.*

The structure of the singularity at a noncuspidal point is bounded by the following observation.

PROPOSITION 2.2. *Over a field of characteristic $p \neq 2, 3$ the projection $\pi : X_0(\ell) \to \mathbb{P}^2$ is an immersion outside of two cusps $0, \infty \in X_0(\ell)$.*

Proof. Let us consider the mapping

$$\varphi : X_0(\ell) \xrightarrow{\pi} Z_0(\ell) \xrightarrow{\tau} \mathbb{P}^1 \tag{3}$$

given at noncuspidal points by $(E \xrightarrow{\rho} E') \mapsto (j(E), j(E')) \mapsto j(E)$. The projection φ is unramified outside the cusps and curves E with nontrivial automorphism group. Hence the differential $d\varphi$ does not vanish for $j(E) \neq 0, 12^3$, and therefore $d\pi \neq 0$. The remaining case $j(E) = 0, 12^3$ may be treated in a similar way by taking the pull back of the diagram (3) with respect to the moduli space $Y \to \mathbb{P}^1$ of elliptic curves with full structure of level $M \geq 3$. Then the morphism $\varphi' : X \times_{\mathbb{P}^1} Y \to Y$ is étale at all noncuspidal points, and as before gives rise to a smooth parametrization of $Z_0(\ell) \times_{\mathbb{P}^1} Y$, which in turn may be descent to a parametrization of $Z_0(\ell)$ by factorisation over ramification group at $j(E) = 0, 12^3$. ∎

Corollary 2.2. *All noncuspidal singularities of the plane model $Z_0(\ell)$ are intersections of smooth branches.*

3. MULTIPLICITIES

To determine the structure of singularity at $(E, E') \in Z_0(\ell)$ it remains to evaluate the order of contact of the branches through (E, E'). A common strategy for this is to perturb the curve in such a way that the singularity splits into simple nodes, and then count the nodes. We apply this geometric idea in the arithmetical setting, treating the modular curve $Z_0(\ell)$ in characteristic zero as a generic deformation of $Z_0(\ell) \otimes \mathbb{F}_p$. The deformation principle works in this situation since the scheme $X_0(\ell)$ is flat over $\mathbb{Z}$ (see [1]), and the intersection indices are preserved in flat families.

To proceed we need first the following fact.

Proposition 3.1. *All noncuspidal singularities of $Z_0(\ell)$ over $\mathbb{C}$ are simple nodes. They are parametrized by similarity classes of lattices $L \subset \mathbb{C}$ with complex multiplication by α, where $\alpha\bar{\alpha} = \ell^2$, and α/ℓ is not a root of unity.*

Proof. Let $\sigma, \rho : E \to E'$ be two nonequivalent isogenies, corresponding to two points of $X_0(\ell)$ with the same projection $(E, E') \in Z_0(\ell)$. Writing $E = \mathbb{C}/L$ and $E' = \mathbb{C}/L'$ we identify the isogenies with complex numbers σ, ρ such that $\sigma L \subset L'$ and $\rho L \subset L'$ are different sublattices of index ℓ. Then there exists a basis ω_1, ω_2 of L' such that

$$L' = \langle \omega_1, \omega_2 \rangle, \qquad \sigma L = \langle \ell\omega_1, \omega_2 \rangle, \qquad \rho L = \langle \omega_1, \ell\omega_2 \rangle.$$

Near the point $z_0 = \omega_1/\omega_2$ the two branches of $Z_0(\ell)$ have parametrizations

$$(j(\ell z), j(z)) \qquad \text{and} \qquad (j(\varphi(z/\ell)), j(z)), \quad \varphi(z_0/\ell) = z_0\ell,$$

where $\varphi \in \mathrm{PSL}(2,\mathbb{Z})$ is given by the matrix of isomorphism $\rho/\sigma : \sigma L \to \rho L$. Taking derivatives we get tangent vectors to the branches

$$(\ell j'(\ell z_0), j'(z_0)), \qquad \text{and} \qquad \left(\frac{\ell\sigma^2}{\rho^2} j'(\ell z_0), j'(z_0)\right),$$

which are noncollinear provided $\sigma^2 \neq \rho^2$, and curves E, E' have no extra automorphisms. The curves with automorphisms may be treated in a similar way by taking an appropriate local parameter instead of z (notice that $\mathrm{Aut}(E) = \mathrm{Aut}(E')$ for any selfintersection point $(E, E') \in Z_0(\ell)$).

Since the whole picture depends only on the ratio σ/ρ, it is convenient to describe the branches by element $\alpha = \sigma\ell/\rho$, which induces a complex multiplication in L. ■

Let $\alpha = (t + f\sqrt{-D})/2$, where $-D = \mathrm{Disc}(\mathbb{Q}(\alpha))$. Then the number of lattices L with complex multiplication by α is equal to $\sum_{d|f} h(-d^2D)$, and the number of pairs (L, α), $\alpha\bar{\alpha} = \ell^2$ is given by $\sum_{t,m} h((t^2 - 4\ell^2)/m^2)$. To get the number of nodes we have to count isomorphism classes of (L, α), depending on the ideal (α), rather then element α, and disregard the ideal $(\alpha) = (\ell)$. As a result we get the formula.

COROLLARY 3.1. *The number of nodes of $Z_0(\ell)$ is equal to*

$$\sum_{0 < t < 2\ell,\ t \neq \ell} H(t^2 - 4\ell^2),$$

where $H(-f^2D) = \sum_{d|f} 2h(-d^2D)/w(-d^2D)$ is the Hurwitz class function.

The proposition, along with the above deformation principle, gives the following reduction of the multiplicity problem.

COROLLARY 3.2. *The order of contact of two branches of $Z_0(\ell) \otimes \mathbb{F}_p$, defined by isogenies $\sigma, \rho : E \to E'$, is equal to the number of liftings of the endomorphism $\alpha = \rho^*\alpha : E \to E$ in characteristic zero.*

To prove Theorem 1.1 it remains to evaluate the number of liftings of the endomorphism $\alpha : E$.

PROPOSITION 3.2. *Let $\alpha : E$ be an endomorphism over $\overline{\mathbb{F}}_p$ of discriminant $D(\alpha) = p^{2v} D_p(\alpha)$, where p^v is p-part of the conductor. Then the number of its liftings in characteristic zero is equal to*

$$e_p \frac{H(D(\alpha))}{H(D_p(\alpha))} = \begin{cases} p^v, & \text{if } p \text{ splits in } \mathbb{Q}(\alpha), \\ 2 + 2p + \cdots + 2p^{v-1} + p^v, & \text{if } p \text{ isinert in } \mathbb{Q}(\alpha), \\ 2 + 2p + \cdots + 2p^v, & \text{if } p \text{ is ramified in } \mathbb{Q}(\alpha). \end{cases}$$

Here e_p is the ramification index of p in $\mathbb{Q}(\alpha)$.

Proof. Let W be a complete valuation ring of characteristic zero with residue field $\overline{\mathbb{F}}_p$. We need the following result from [4, Lemma 2.7]. Let $\beta : E$ be an endomorphism over $\overline{\mathbb{F}}_p$ of conductor coprime to p. Then the number of its liftings to an endomorphism $\tilde{\beta}: \tilde{E}$ over W is equal to the number of solutions in W of the equation

$$x^2 + ax + b = 0, \qquad x \equiv \beta_0 \bmod p, \tag{4}$$

where $x^2 + ax + b$ is the characteristic polynomial of β, and the differential of β is multiplication by $\beta_0 \in \bar{\mathbb{F}}_p$. Notice that in [4] the result is stated only for *fundamental* discriminants, but the proof holds for any conductor coprime to p. For an ordinary curve E this amounts to the Deuring lifting theorem [2].

It is well known [2] that the conductor of the integer closure of $\mathbb{Z}[\alpha]$ in $\mathrm{End}(E)$ is coprime to p. Hence there exists unique ring $\alpha \in \mathbb{Z}[\beta] \subset \mathrm{End}(E)$, with discriminant $D(\beta) = D_p(\alpha)$, and any curve over $\bar{\mathbb{F}}_p$ with multiplication by α admits also multiplication by β. By ((4)) each endomorphism $\beta: E$ has e_p liftings. By calculation similar that of Corollary 3.1, there are $H(D(\beta)) = H(D_p(\alpha))$ curves in characteristic zero with complex multiplication by β; hence there are $H(D_p(\alpha))/e_p$ of such curves over $\bar{\mathbb{F}}_p$ (curve E counted with weight $2/|\mathrm{Aut}(E)|$). On the other hand the number of curves in characteristic zero with complex multiplication by α is $H(D(\alpha))$, and the result follows. ■

REFERENCES

1. P. Deligne and M. Rapoport, Schemas des modules de courbes elliptiques, *in* "Lecture Notes in Math.", Vol. 349, pp. 163–315.
2. M. Deuring, Die Typen der Multiplikatorenringe elliptischer Functionenkörper, *Abh. Math. Sem. Hamburg* **14** (1941), 197–272.
3. A. Garcia and H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining Drinfeld–Vladuţ bound, *Invent. Math.* **121** (1995), 211–222.
4. B. H. Gross and D. Zagier, On singular moduli, *J. Reine Angew. Math.* **355** (1985), 191–220.
5. F. Hirzebruch, Kurven auf Hilbertschen Modulflächen und Klassenzalrelationen, *in* "Gesammelte Abhandlungen," pp. 361–393, Springer-Verlag, Berlin/New York, 1987.
6. M. A. Tsfasman and S. G. Vladuţ, "Algebraic Geometric Codes," Kluwer Academic, Dordrecht, 1991.