JOURNAL OF NUMBER THEORY 44, 255–259 (1993)

On Modular Elliptic Curves

DINO J. LORENZINI*

Department of Mathematics, Harvard University,
Cambridge, Massachusetts 02138

Communicated by K. A. Ribet

Received October 24, 1991; revised December 17, 1991

The number of isogeny classes of elliptic curves $E/\mathbf{Q}_p$, having potentially good reduction at p, and which are quotients of the jacobian $J_0(p^2)$, is bounded by $(p/4+4)$.

Let $J_0(N)/\mathbf{Q}$ denote the Jacobian of the modular curve $X_0(N)/\mathbf{Q}$. Fix a prime $p \geqslant 5$, and let K denote the maximal unramified extension of $\mathbf{Q}_p$. Let

$$j\colon J_0(N) \to \prod_{i=1}^{n} A_i$$

be an isogeny, defined over K, and such that all factors A_i/K are simple abelian varieties. To obtain an upper bound on the number of factors A_i in $\prod A_i$ that have dimension 1, we proceed as follows. Recall that given an abelian variety A/K, the connected component of zero of the special fiber of its Néron model is an extension of an abelian variety of dimension $a_K(A)$ by the product of a torus of dimension $t_K(A)$ and an unipotent group of dimension $u_K(A)$. The integers a_K, t_K, and u_K are invariant under isogeny [Gro, IX, 2.2.7]. Recall also that an elliptic curve E/K with additive reduction over the ring of integers $\mathcal{O}_K$ achieves semi-stable reduction after an extension K_d/K of degree $d \in I := \{2, 3, 4, 6\}$.

Let S_d denote the set of elliptic curves in $\prod A_i$ having semi-stable reduction over K_d. The above discussion shows that

$$|S_d| \leqslant t_{K_d}(J_0(N)) + a_{K_d}(J_0(N)).$$

The integers $t_{K_d}(J_0(N))$ and $a_{K_d}(J_0(N))$ can be computed using a regular model of $X_0(N)/K_d$. We have done so for some values of N and have obtained the following result.

* Research supported by a grant from the Fond national suisse de la recherche scientifique.
Present address: Department of Mathematics, University of Georgia, Athens, GA 30602.

0022-314X/93 $5.00

THEOREM. *Let $p \geqslant 5$ be a prime, and let $N = p^2$. The number of factors A_i in $\prod A_i$ that have dimension one and do not have semi-stable reduction over K is bounded by $(p/3+4)$. The number of such factors having potentially good reduction is bounded by $(p/4+4)$.*

It is likely that this bound is not best possible. Indeed, there is no reason to believe that, in general, the only simple factors of $J_0(N)$ that achieve semi-stable reduction after an extension of degree $d \in I$ are the factors of dimension 1.

Let us recall now how to compute the integers t_K and a_K associated to the jacobian of a curve. Let K be any complete field with respect to a discrete valuation. Let $\mathcal{O}_K$ be its ring of integers and let k be its residue field, assumed to be algebraically closed. Let X/K be a smooth proper geometrically irreducible curve, and let A/K denote its jacobian. Let $\mathcal{X}/\mathcal{O}_K$ be a regular model of X/K. Its special fiber $\mathcal{X}_k$ is an effective Cartier divisor and, as such, we write it as

$$\mathcal{X}_k = \sum_{i=1}^{n} r_i C_i,$$

where r_i is the multiplicity of the irreducible component C_i. We call a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K a *good* model if the following additional properties hold:

- The components C_i are smooth of genus $g(C_i)$.
- If $i \neq j$, the intersection number $(C_i \cdot C_j)$ is equal to zero or one.

To $\mathcal{X}$ we associate a graph G defined as follows: the vertices of G are the curves C_i, and C_i is linked to C_j by $(C_i \cdot C_j)$ edges. We let $\beta(G)$ denote the first Betti number of G. When X has a K-rational point, Raynaud (see [BLR, Theorem 4 on p. 267, and Propositions 9 and 10 on pp. 248–249]) has shown that, if $\mathcal{X}/\mathcal{O}_K$ is a good model of X/K, then

$$\sum_{i=1}^{n} g(C_i) = a_K(A),$$

and

$$\beta(G) = t_K(A).$$

Let K_q/K be a *tame* extension of prime order q. Given a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K, it is possible to describe a regular model $\mathcal{Z}/\mathcal{O}_{K_q}$ of X_{K_q}/K_q, and, hence, to compute the integers t_{K_q} and a_{K_q}. Let $\mathcal{Y}/\mathcal{O}_{K_q}$ denote the normalization of the scheme

$$\mathcal{X} \times_{\operatorname{Spec}(\mathcal{O}_K)} \operatorname{Spec}(\mathcal{O}_{K_q}).$$

Let

$$\pi : \mathcal{Y} \to \mathcal{X}$$

denote the natural map; let $\mathcal{Z}/\mathcal{O}_{K_q}$ denote the minimal desingularization of $\mathcal{Y}/\mathcal{O}_{K_q}$. Let

$$R_q = \bigcup_{q \nmid r_i} C_i.$$

The map π is ramified over R_q. If $\mathcal{X}$ is a good model, then $\mathcal{Y}$ is a (good) regular model of X_{K_q}/K_q if and only if R_q is a nonsingular scheme, i.e., if and only if $R_q = \bigsqcup_{q \nmid r_i} C_i$. The reader will find a proof of this fact in the complex case in [BPV, Theorem 5.2]. One easily checks that when $q = 2$ or 3, one can always find a regular model $\mathcal{X}/\mathcal{O}_K$ such that R_q is nonsingular.

The map π can be described as follows.

- If $q \nmid r_i$, then $\pi^{-1}(C_i) =: D_i$ is irreducible, and the restricted map

$$\pi_{|D_i} : D_i \to C_i$$

is an isomorphism. The curve D_i has multiplicity r_i in $\mathcal{Y}_k$.

- If $q \mid r_i$ and $C_i \cap R_q \neq \emptyset$, then $\pi^{-1}(C_i) =: D_i$ is irreducible, and the restricted map

$$\pi_{|D_i} : D_i \to C_i$$

is a morphism of degree q ramified over $|C_i \cap R_q|$ points of C_i. The curve D_i has multiplicity r_i/q in $\mathcal{Y}_k$. Its genus is computed using the Riemann–Hurwitz formula.

- If $q \mid r_i$ and $C_i \cap R_q = \emptyset$, then

$$\pi : \pi^{-1}(C_i) \to C_i$$

is an etale map, and each irreducible component of $\pi^{-1}(C_i)$ has multiplicity r_i/q in $\mathcal{Y}_k$. Note that when C_i is a rational curve, then $\pi^{-1}(C_i) = D_1 \sqcup \cdots \sqcup D_q$ is equal to the disjoint union of q rational curves, and each restricted map

$$\pi_{|D_j} : D_j \to C_i$$

is an isomorphism.

When $\gcd(N, 6) = 1$, Edixhoven ([Edi], 1.5) has computed a regular model of $X_0(N)/K$. Using his description of a regular model for $X_0(N)/K$ and the facts recalled above, one can compute the integers $t_{K_d}(J_0(N))$ and $a_{K_d}(J_0(N))$, for $d \in I$. We have computed these integers when $N = p^2$, with $p \geqslant 5$, and our computations are summarized in the tables below. The above theorem is an immediate consequence of these computations.

TABLE I

	$p=12k+1$	$p=12k+5$	$p=12k+7$	$p=12k+11$
Genus of $X_0(p)$	$k-1$	k	k	$k+1$
Genus of $X_0(p^2)$	$12k^2-3k-1$	$12k^2+5k$	$12k^2+9k+1$	$12k^2+17k+6$

TABLE II

	$p=12k+1$	$p=12k+5$	$p=12k+7$	$p=12k+11$
Toric rank of $J_0(p)$ over K	$k-1$	k	k	$k+1$
Toric rank of $J_0(p^2)$ over K	$2(k-1)$	$2k$	$2k$	$2(k+1)$
Toric rank of $J_0(p^2)$ over K_2 (or K_4, K_6)	$3(k-1)$	$3k$	$3k$	$3(k+1)$

TABLE III

$J_0(p^2)$, $p=12k+1$	$6\mid k$	$2\nmid k$, $3\mid k$	$2\mid k$, $3\nmid k$	$2\nmid k$, $3\nmid k$
Abelian rank/K_4	$k-2$	$k-1$	$k-2$	$k-1$
Abelian rank/K_6	$2(k-2)$	$2(k-2)$	$2(k-1)$	$2(k-1)$

TABLE IV

$J_0(p^2)$, $p=12k+5$	$2\nmid k$, $3\nmid k-1$	$2\mid k$, $3\nmid k-1$	$2\nmid k$, $3\mid k-1$	$2\mid k$, $3\mid k-1$
Abelian rank/K_4	$k-1$	k	$k-1$	k
Abelian rank/K_6	$2(k-2)$	$2(k-2)$	$2(k-1)$	$2(k-1)$

TABLE V

$J_0(p^2)$, $p=12k+7$	$2\nmid k$, $3\mid k-1$	$2\mid k$, $3\mid k-1$	$2\nmid k$, $3\nmid k-1$	$2\mid k$, $3\nmid k-1$
Abelian rank/K_4	k	$k+1$	k	$k+1$
Abelian rank/K_6	$2(k-1)$	$2(k-1)$	$2k$	$2k$

TABLE VI

$J_0(p^2)$, $p=12k+11$	$2\mid k$, $3\nmid k+1$	$2\nmid k$, $3\nmid k+1$	$2\mid k$, $3\mid k+1$	$2\nmid k$, $3\mid k+1$
Abelian rank/K_4	$k+1$	$k+2$	$k+1$	$k+2$
Abelian rank/K_6	$2(k+1)$	$2(k+1)$	$2(k+2)$	$2(k+2)$

It follows from Table II and Table III that there are no modular elliptic curves of conductor $(13)^2$.

The genus of $X_0(11^2)$ is equal to 6, and it is known that $J_0(11^2)$ is isogenous to a product of 6 elliptic curves [Lig].

REFERENCES

[BLR] S. BOSCH, W. LÜTKEBOHMERT, AND M. RAYNAUD, "Néron Models," Springer-Verlag, New York/Berlin, 1990.

[BPV] W. BARTH, C. PETERS, AND A. VAN DE VEN, "Compact Complex Surfaces," Springer-Verlag, New York/Berlin, 1984.

[Edi] B. EDIXHOVEN, Minimal resolution and stable reduction of $X_0(N)$, *Ann. Inst. Fourier* **40**, No. 1 (1990), 31–67.

[Gro] A. GROTHENDIECK, Séminaire de géometrie algébrique SGA 7, I, *in* "Lecture Notes in Math.," Vol. 288, Springer-Verlag, New York/Berlin, 1970.

[Lig] G. LIGOZAT, Courbes modulaires de niveau 11, *in* "Modular Functions of One Variable, V," Lecture Notes in Math., Vol. 601, Springer-Verlag, New York/Berlin, 1977.