PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 112, Number 2, June 1991

BIELLIPTIC CURVES AND SYMMETRIC PRODUCTS

JOE HARRIS AND JOE H. SILVERMAN

(Communicated by William Adams)

ABSTRACT. We show that the twofold symmetric product of a nonhyperelliptic, nonbielliptic curve does not contain any elliptic curves. Applying a theorem of Faltings, we conclude that such a curve defined over a number field K has only finitely many points over all quadratic extensions of K. We illustrate our theory with the modular curves $X_0(N)$, $X_1(N)$, $X(N)$.

A smooth, projective curve C is called *hyperelliptic* (respectively *bielliptic*) if it admits a map $\phi: C \to X$ of degree 2 onto a curve X of genus zero (respectively one). In this case the symmetric product

$$C^{(2)} = \frac{C \times C}{\mathscr{S}_2}$$

contains a copy of X via the natural map $x \to \phi^{-1}(x)$. Conversely, if $C^{(2)}$ contains a curve X of genus 0, then it is easy to see that C is hyperelliptic. (The image of X in the Jacobian of C consists of a single point, so C contains a nontrivial g_2^1.) In this note we deal with the case that $C^{(2)}$ contains a curve of genus 1. Specifically, we show that C is necessarily either hyperelliptic or bielliptic; and if the genus of C is at least 9, then C is actually bielliptic.

Next, using our geometric result and Faltings' theorem [2] describing rational points on subvarieties of abelian varieties, we will show that if a curve C defined over a number field K is neither hyperelliptic nor bielliptic, then the set of quadratic points on C,

$$\{P \in C(\overline{K}): [K(P): K] \leq 2\},$$

is finite.

To illustrate the general theory, we use a method of Ogg to show that if N is sufficiently large (specifically if $N \geq 345$), then the curves $X_0(N)$, $X_1(N)$, and $X(N)$ are neither hyperelliptic nor bielliptic. In particular, they have only finitely many quadratic points. This generalizes results of Frey [3] and Hindry

Received by the editors February 20, 1990 and, in revised form, May 14, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G30; Secondary 14H05.
The first author was supported by an NSF research grant.
The second author was supported by NSF grant DMS-8913113 and a Sloan Foundation Fellowship.

0002-9939/91 $1.00 + $.25 per page

[4], who dealt with the case that N is prime and $K = \mathbb{Q}$. Recently, Kamienny has announced a proof that if $K = \mathbb{Q}$ and N is sufficiently large, then the only quadratic points on $X_1(N)$ are the cusps. Kamienny's proof, which is based on methods pioneered by Mazur, uses very different methods from those used in this paper.

We begin with a proposition which describes the image of a bielliptic curve.

Proposition 1. *If Γ is a bielliptic curve, and if $\Gamma \to C$ is a finite map, then C is either bielliptic or hyperelliptic.*

Proof. To begin with, denote by $\phi: \Gamma \to E$ a map of degree 2 from Γ to an elliptic curve, and let $V \subset H^0(K_\Gamma)$ be the subspace of holomorphic differentials which are anti-invariant under the involution of Γ exchanging the sheets over E.

Now, let $\alpha: \Gamma \to C$ be a map of Γ to a curve C of genus g. We claim that C is bielliptic or hyperelliptic. Since this is immediate if $g \leq 2$, we will assume $g \geq 3$. Let $W \subset H^0(K_C)$ be the subspace of differentials on C that pull back under the map α to differentials in the space V, that is,

$$W = ((\alpha^*)^{-1}(V)) \subset H^0(K_C).$$

Note that W has codimension at most 1 in $H^0(K_C)$.

Next, let B be the image of C under the map $\psi = \psi_W$ associated to the linear series W. This map cannot be birational onto its image—in fact, for any point $p \in E$ with $\phi^{-1}(p) = \{q, r\} \subset \Gamma$, we have

$$\psi(\alpha(q)) = \psi(\alpha(r)).$$

So we have a (nonconstant) map of the elliptic curve to the symmetric fiber square

$$C *_B C = \frac{C \times_B C - \Delta}{\sigma}$$

of C with itself over B. (This is defined to be the union of the irreducible components of the ordinary product other than the diagonal, modulo the involution exchanging the factors.) This also shows that B must have genus 0 or 1. Also, since ψ is not birational, if W were all of $H^0(K_C)$, then C would be hyperelliptic; so we may assume that W has codimension exactly 1 in $H^0(K_C)$.

Now, given that ψ is not birational, a key question is what its degree may be. To bound this, we use the fact that B, being an irreducible, nondegenerate curve in $\mathbb{P}^{g-2}$, must have degree at least $g - 2$. Thus, if the degree of ψ is m, we have

$$2g - 2 \geq m \cdot \deg(B) \geq m(g - 2);$$

and it follows that $m \leq 4$. Of course, if $m = 2$, then we are done, since B is either elliptic or rational. We can similarly dispense with the possibility $m = 3$; in this case the symmetric fiber square $C *_B C$ is isomorphic to C itself, which we have assumed has genus $g \geq 3$.

The case $m = 4$ is more subtle, and requires that we consider the monodromy group $G \subset \mathscr{S}_4$ of the cover $\psi: C \to B$. We consider the possibilities for G in turn.

To begin with, if $G = \{\sigma\}$ is the cyclic group $\mathbb{Z}/4$, then $C *_B C$ will have two components, one a copy of C itself (consisting of pairs of the form $p + \sigma p$) and the other a copy of the quotient $C/(\sigma^2)$ (consisting of pairs $p + \sigma^2 p$). E must then map to the latter, so that the two-to-one map $C \to C/(\sigma^2)$ makes C bielliptic or hyperelliptic. Likewise, if G is the Klein group $\mathbb{Z}/2 \times \mathbb{Z}/2$, then $C *_B C$ will have three components isomorphic to the quotients of C by the subgroups of order 2 in G, so again we are done.

Next, G could be the dihedral group $\mathscr{D}_4$ of order 8. Here $C *_B C$ will consist of two components, one of degree 2 over B and one of degree 4. The first of these is the quotient of C by the square of an element of order 4 in G, and if E maps to this one we are done as before. But comparing the branching of $C *_B C$ over B, we see that the other component will have genus greater than or equal to that of C; it has the same monodromy as C at a branch point of $C \to B$ with monodromy (1234) or (13)(24), and one more ramification point over a branch point of $C \to B$ with monodromy (12). Thus E must map to the first component.

In the remaining cases $G = \mathscr{A}_4$ and $\mathscr{S}_4$, so $C *_B C$ will be irreducible. We claim in either case that the genus of $C *_B C$ will be at least $g - 1 \geq 2$, which will complete the argument. This assertion also follows from an examination of the possible branching of C over B and the corresponding branching of $C *_B C$ over B. Specifically, an inspection of the various types of branch points shows that $C *_B C$ will have strictly greater total ramification index than C over each branch point of $C \to B$ except a point with monodromy type (12)(34), where it will be the same.

This proves that $g(C *_B C) \geq g$ if B has positive genus. On the other hand, if B is rational, then at least two of the branch points of C over B will not be of this type. It follows that the degree r' of the ramification divisor of $C *_B C$ over B will be at least two greater than the degree r of the ramification divisor of C over B. We calculate (note $g(B) = 0$)

$$\begin{aligned} 2g(C *_B C) - 2 &= 6(2g(B) - 2) + r' \geq -12 + r + 2 \\ &= \{4(2g(B) - 2) + r\} - 2 = 2g - 4. \end{aligned}$$

Hence $g(C *_B C) \geq g - 1$, and we are done.

Theorem 2. *Let C be a smooth, projective curve.*

(a) *If the symmetric product $C^{(2)}$ contains a curve of genus 1, then C is either bielliptic or hyperelliptic.*

(b) *If in addition the genus of C is at least 9, then C is bielliptic.*

Proof. The proof of (a) will use Proposition 1. For (b) we give an independent proof, interesting in its own right, using intersection theory on the (ordinary) product C^2.

Assume that $C^{(2)}$ contains a curve of genus 1. Let E be the normalization of that curve, and let $i: E \to C^{(2)}$ be the natural map. Let $\pi: C^2 \to C^{(2)}$ be the usual projection, and let

$$\tilde{\Gamma} = \pi^*(i_*E) \in \mathrm{Div}(C^2)$$

be the pullback of $i(E)$ via π. We claim first that $\tilde{\Gamma}$ is irreducible. Note that in any case there is a rational map $\tilde{\Gamma} \to E$ of degree 2; and, since π is finite, every component of $\tilde{\Gamma}$ must map onto E. Hence if $\tilde{\Gamma}$ is not irreducible, then any component $\tilde{\Gamma}_1 \subset \tilde{\Gamma}$ admits a map $\tilde{\Gamma}_1 \to E$ of degree 1. It follows that $\tilde{\Gamma}_1$ has genus 1, so C^2 contains a curve of genus 1. But that is not possible, since C has genus at least 2. (For example, the projections $p_1, p_2: C^2 \to C$ map $\tilde{\Gamma}_1 \to C$, so would have to be constant, which would imply that $\tilde{\Gamma}_1$ is a single point.) This proves that $\tilde{\Gamma}$ is an irreducible curve on C^2.

Let Γ be the normalization of $\tilde{\Gamma}$, and $j: \Gamma \to C^2$ the natural map. Then we have a commutative diagram

$$\begin{array}{ccccc} \Gamma & \xrightarrow{\text{birat.}} & \tilde{\Gamma} & \longrightarrow & C^2 \\ & \phi \searrow & \downarrow & & \downarrow \pi \\ & & E & \xrightarrow{i} & C^{(2)} \end{array}$$

Notice $\deg \phi = \deg \pi = 2$, so Γ is bielliptic. We consider the compositions

$$\Gamma \xrightarrow{j} C^2 \xrightarrow{p_1 \text{ or } p_2} C.$$

(Notice that they are the same map.) We check that each $p_i \circ j$ is not constant. Let $\sigma: C^2 \to C^2$ be the map $\sigma(x, y) = (y, x)$ interchanging the fibers of π. From the definition of Γ it is clear that $\sigma(j\Gamma) = j\Gamma$, so

$$p_1(j\Gamma) = p_1 \circ \sigma \circ j(\Gamma) = p_2(j\Gamma).$$

Since j is not constant, this shows that $p_1 \circ j$ and $p_2 \circ j$ are not constant.

Applying Proposition 1 to the bielliptic curve Γ and the finite map $p_1 \circ j: \Gamma \to C$, we conclude that C is either hyperelliptic or bielliptic. This concludes the proof of (a).

(b) The idea of the proof is to show that if $g = \mathrm{genus}(C)$ is sufficiently large (i.e. $g \geq 9$), then the map $p_1 \circ j: \Gamma \to C$ has degree 1. Thus C will be isomorphic to the bielliptic curve Γ.

Fix a basepoint $x_0 \in C$. We set the following notation:

$$\begin{aligned} \Delta &= \mathrm{diagonal}(C^2) \in \mathrm{Div}(C^2), \\ H &= p_1^*(x_0) + p_2^*(x_0) \in \mathrm{Div}(C^2), \\ \gamma &= \mathrm{genus}(\Gamma). \end{aligned}$$

Clearly H is ample, and we have intersection indices

$$H^2 = H \cdot \Delta = 2 \quad \text{and} \quad \Delta^2 = 2 - 2g. \tag{1}$$

From above, the maps $p_i \circ j$ are not constant. Since they have the same degree, we find

$$\deg(p_1 \circ j) = \tfrac{1}{2}\deg(j^*H). \tag{2}$$

It is convenient to define two quantities:

$$\begin{aligned} A &= \frac{1}{2g}\deg(j^*\Delta) = \frac{1}{2g}(\tilde{\Gamma}\cdot\Delta), \\ B &= \frac{1}{2}\deg(j^*H) = \frac{1}{2}(\tilde{\Gamma}\cdot H). \end{aligned} \tag{3}$$

(Note that $\tilde{\Gamma} = j_*\Gamma$.) Since H is ample, we can apply the Hodge Index Theorem to the three divisors $H, \Delta, \tilde{\Gamma}$. This yields

$$\begin{aligned} 0 \geq -\det\begin{pmatrix} H^2 & H\cdot\Delta & H\cdot\tilde{\Gamma} \\ \Delta\cdot H & \Delta^2 & \Delta\cdot\tilde{\Gamma} \\ \tilde{\Gamma}\cdot H & \tilde{\Gamma}\cdot\Delta & \tilde{\Gamma}^2 \end{pmatrix} &= -\det\begin{pmatrix} 2 & 2 & 2B \\ 2 & 2-2g & 2gA \\ 2B & 2gA & \tilde{\Gamma}^2 \end{pmatrix} \\ &= 4\{g\tilde{\Gamma}^2 + 2g^2A^2 - 4gAB - (g-1)B^2\}. \end{aligned} \tag{4}$$

To calculate $\tilde{\Gamma}^2$ we use adjunction. Note that

$$K_{C^2} = p_1^*K_C + p_2^*K_C \overset{\text{alg. equiv.}}{\equiv} (2g-2)H. \tag{5}$$

Hence

$$\begin{aligned} \tilde{\Gamma}^2 &= (2p_a(\tilde{\Gamma}) - 2) - \tilde{\Gamma}\cdot K_{C^2} \geq (2\gamma - 2) - (2g-2)\tilde{\Gamma}\cdot H \\ &= (2\gamma - 2) - 4(g-1)B. \end{aligned}$$

(Note that $p_a \geq g$ for any effective divisor on a smooth surface.) Substituting this into (4) gives

$$\begin{aligned} 0 &\geq 2g(\gamma-1) - 4g(g-1)B + (gA - B)2gA - 2gAB - 2(g-1)B^2 \\ &= 2g(\gamma-1) + 2gA(gA - 2B) - 2(g-1)B(B+2g). \end{aligned} \tag{6}$$

It remains to estimate γ and A in terms of B. This involves two applications of the Riemann-Hurwitz genus formula. First, from the nonconstant map $p_1 \circ j: \Gamma \to C$ we find

$$2\gamma - 2 \geq \deg(p_1 \circ j)(2g-2) = B(2g-2), \quad \text{so} \quad \gamma - 1 \geq (g-1)B. \tag{7}$$

Second, we observe that the map $\phi: \Gamma \to E$ has degree 2 and is ramified only at points in the support of $j^*\Delta$. (Note that $\pi: C^2 \to C^{(2)}$ is ramified exactly along Δ.) Hence

$$\begin{aligned} 2\gamma - 2 &= (\deg\phi)(2g(E) - 2) + \deg(\text{ramification divisor of } \phi) \\ &\leq \#\text{Support } j^*\Delta \leq \deg j^*\Delta = 2gA. \end{aligned}$$

Combining this with (7) gives

$$gA \geq \gamma - 1 \geq (g-1)B. \tag{8}$$

Now we substitute (8) into (6) to eliminate A and γ. (If we assume that $g \geq 3$, then (8) shows that $gA \geq 2B$, so it is all right to substitute (8) into the term $2gA(gA - 2B)$.) This yields

$$\begin{aligned} 0 &\geq 2g(g-1)B + 2(g-1)B((g-1)B - 2B) - 2(g-1)B(B+2g) \\ &= 2(g-1)B\{(g-4)B - g\}. \end{aligned}$$

Hence

$$g \geq 5 \Rightarrow B \leq \frac{g}{g-4} = 2 - \frac{g-8}{g-4}.$$

But $B = \deg(p_1 \circ j)$ is an integer, so

$$g \geq 9 \Rightarrow B = 1 \Rightarrow p_1 \circ j : \Gamma \to C \text{ is an isomorphism.}$$

Since $\phi : \Gamma \to E$ exhibits Γ as a double cover of an elliptic curve, we conclude that if $g \geq 9$, then C is bielliptic.

Corollary 3. *Let K be a number field, and let C/K be a curve of genus at least 2. Assume that C is neither hyperelliptic nor bielliptic. Then the set*

$$C(K, 2) = \{P \in C(\overline{K}) : [K(P) : K] \leq 2\}$$

of quadratic points on C/K is finite.

Proof. If $C(K, 2)$ is empty, there is nothing to prove. Otherwise, fix a base-point $p_0 \in C(K, 2)$. Let p_0' be the $\overline{K}/K$ conjugate of p_0. (If p_0 is actually in $C(K)$, we let $p_0' = p_0$.) Then there is a natural map

$$\mu : C^{(2)} \to J = \mathrm{Jac}(C), \qquad (p) + (q) \mapsto \mathrm{class}[(p) + (q) - (p_0) - (p_0')].$$

Since C is not hyperelliptic, the map μ is injective. (C has no nontrivial g_2^1's.) Hence $C^{(2)} \cong \mu(C^{(2)}) \subset J$. Further, since the divisor $(p_0) + (p_0')$ is defined over K, the map μ is defined over K. Hence

$$C^{(2)}(K) \cong \mu(C^{(2)})(K).$$

Next, since C is not bielliptic, we know from Theorem 2 that $C^{(2)}$ contains no curves of genus one. Also, since $C^{(2)}$ itself is not an abelian surface, we see that $\mu(C^{(2)})$ does not contain a translate of an abelian subvariety of J. From Faltings' theorem [2], we conclude that $C^{(2)}(K)$ is finite.

Finally, we note that there is an (at most) two-to-one map of sets

$$C(K, 2) \to C^{(2)}(K), \qquad p \mapsto (p) + (p').$$

(As above, p' is either the $\overline{K}/K$ conjugate of p, or else is equal to p if $p \in C(K)$.) Therefore $C(K, 2)$ is finite, which completes the proof of Corollary 3.

Ogg [5] has shown that if $N \geq 72$, then the modular curve $X_0(N)$ is not hyperelliptic. We will now show that if $N \geq 344$, then $X_0(N)$ is also not bielliptic. This provides an interesting class of examples to which one can apply Corollary 3. Our bound 344 is not sharp. It would be of interest to perform

a more detailed analysis, as Ogg does in the hyperelliptic case, so as to give a complete list of N for which $X_0(N)$ is bielliptic. For prime values of N, Hindry [4] has shown that there are exactly eight values of N for which $X_0(N)$ is bielliptic of genus at least 2, the largest such N being 131. See also Frey [3] for a somewhat weaker result.

Theorem 4. *If $N \geq 344$, then the modular curves $X_0(N)$, $X_1(N)$, and $X(N)$ are neither hyperelliptic nor bielliptic.*

Proof. As mentioned above, Ogg [5] has shown that $X_0(N)$ is not hyperelliptic if $N \geq 72$. This implies the same for $X_1(N)$ and $X(N)$. [For example, if f is a function of degree 2 on $X_1(N)$, and if $\pi: X_1(N) \to X_0(N)$ is the natural projection, then $\pi_* f$ will be a function of degree 2 on $X_0(N)$.] Similarly, Proposition 1 shows that it suffices to deal with $X_0(N)$ in the bielliptic case. So we will prove that if $X_0(N)$ is bielliptic, then $N \leq 343$.

If a curve C is hyperelliptic, then the g_2^1 on C is unique, which implies that C is hyperelliptic over its field of definition. We begin with a similar result for bielliptic curves.

Lemma 5. *Let C/K be a geometrically bielliptic curve of genus at least 6. Then there is a genus 1 curve B/K and a map $\psi: C \to B$ of degree 2 defined over K (i.e. C is bielliptic over K).*

Proof. By assumption, there is a curve $E/\overline{K}$ of genus 1 and a map $\phi: C \to E$ of degree 2 (defined over $\overline{K}$). For each $\sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$ we obtain a second map $\phi^\sigma: C \to E^\sigma$, also of degree 2. Consider the map

$$\phi \times \phi^\sigma: C \to E \times E^\sigma.$$

Let $X = (\phi \times \phi^\sigma)(C)$ be the image. If C is birational to X, then [1, VIII.C-1] says that

$$\text{genus } C \leq (\deg \phi - 1)(\deg \phi^\sigma - 1) + (\deg \phi)(\text{genus } E) + (\deg \phi^\sigma)(\text{genus } E^\sigma) = 5.$$

Since we have assumed that C has genus at least 6, it follows that the map $C \to X$ has degree at least 2. But the composition

$$C \xrightarrow{\phi \times \phi^\sigma} X \xrightarrow{\text{proj}_1} E$$

is the map ϕ, which has degree 2. It follows that X is birational to E. Similarly, using the second projection, we find that X is birational to E^σ. Hence $E \cong E^\sigma$ for all $\sigma \in G_K$.

This proves that E is isomorphic (over $\overline{K}$) to a curve of genus 1 defined over K. (For example, $E \cong \mathrm{Jac}(E)$, and $\mathrm{Jac}(E)$ is defined over K.) Replacing E by this new curve and changing ϕ, we now have C and E defined over K, but the map $\phi: C \to E$ may not be defined over K.

For any $\sigma \in G_K$, the argument given above shows that the maps $\phi: C \to E$ and $\phi^\sigma: C \to E$ differ by an automorphism of E. Thus there is a map

$$\alpha: G_K \to \mathrm{Aut}(E), \quad \text{such that } \phi^\sigma = \alpha_\sigma \circ \phi \text{ for all } \sigma \in G_K.$$

(N.B. $\mathrm{Aut}(E)$ includes "translations." This is the group denoted by $\mathrm{Isom}(E)$ in [6, X §2].) It is easily seen that α_σ is a cocycle in $H^1(G_K, \mathrm{Aut}(E))$, so by [6, X.2.2] it corresponds to a twist of E. Hence there is a curve B/K of genus 1 and an isomorphism $\lambda: B \to E$ defined over $\overline{K}$ such that $\alpha_\sigma = \lambda^\sigma \circ \lambda^{-1}$ for all $\sigma \in G_K$. Now the composition

$$\lambda^{-1} \circ \phi: C \to B$$

is the desired map of degree 2 defined over K from C to a curve of genus 1 defined over K.

Next we use methods from Ogg's paper to prove the bielliptic analogue of his hyperelliptic estimates [5, Theorem 3].

Lemma 6. *For any integer N, let*

$$\nu(N) = \#\text{ of distinct prime divisors of } N,$$
$$\mu(N) = \deg(X_0(N) \to X(1)) = N \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

For any prime p, let

$$s(p) = \sum_{\substack{E/\mathbb{F}_p \\ E \text{ super-singular}}} \frac{1}{|\mathrm{Aut}(E)|}.$$

Assume that $X_0(N)$ is either bielliptic or hyperelliptic. Then

$$2^{\nu(N)} + 2s(p)\mu(N) \le \max\{2(p+1)^2, p^2 + 10p + 1\} \quad \textit{for all } p \nmid N.$$

In particular,

$$2^{\nu(N)} + \tfrac{1}{12}\mu(N) \le 25, \quad \textit{if } 2 \nmid N,$$
$$2^{\nu(N)} + \tfrac{1}{6}\mu(N) \le 40, \quad \textit{if } 3 \nmid N,$$
$$2^{\nu(N)} + \tfrac{1}{3}\mu(N) \le 76, \quad \textit{if } 5 \nmid N,$$
$$2^{\nu(N)} + \tfrac{1}{2}\mu(N) \le 128, \quad \textit{if } 7 \nmid N,$$
$$2^{\nu(N)} + \tfrac{5}{6}\mu(N) \le 288, \quad \textit{if } 11 \nmid N.$$

Proof. If $X_0(N)$ is hyperelliptic, then Ogg [5, Theorem 3] essentially proves this result (with the better upper bound $2p^2 + 2$). We will henceforth assume that $X_0(N)$ is bielliptic.

Let $p \nmid N$ be a prime. Then Ogg essentially shows that

$$\#X_0(N)(\mathbb{F}_{p^2}) \ge 2^{\nu(N)} + 2s(p)\mu(N).$$

The first term is clear, since $X_0(N)$ has at least $2^{\nu(N)}$ cusps. For the second term, Ogg notes that if $E/\mathbb{F}_p$ is supersingular, then its Frobenius endomorphism π_p satisfies $\pi_p^2 = -p \in \mathbb{Z}$. Hence any cyclic subgroup $C \subset E$ of order N will be

defined over $\mathbb{F}_{p^2}$, yielding a point $(E, C) \in X_0(N)(\mathbb{F}_{p^2})$. There are $\mu(N)$ such subgroups of order N, yielding $\mu(N)$ points. However, if $\alpha \in \mathrm{Aut}(E)$, then (E, C) and $(E, \alpha C)$ correspond to the same point of $X_0(N)$. Since $[-1]C = C$, this means that we obtain at least $2\mu(N)/\#\mathrm{Aut}(E)$ distinct, noncuspidal points in $X_0(N)(\mathbb{F}_{p^2})$. Summing over all supersingular $E/\mathbb{F}_p$ gives the stated lower bound for $X_0(N)(\mathbb{F}_{p^2})$.

To find an upper bound, we consider two cases. First, if $X_0(N)$ has genus at most 5, then Weil's estimate gives

$$\#X_0(N)(\mathbb{F}_{p^2}) \leq p^2 + 1 + 2g(X_0(N))p \leq p^2 + 10p + 1.$$

Second, if $g(X_0(N)) \geq 6$, then we can apply Lemma 5 to find a curve $B/\mathbb{Q}$ of genus 1 and a map $\psi: X_0(N) \to B$ of degree 2 defined over $\mathbb{Q}$. It follows that

$$\#X_0(N)(\mathbb{F}_{p^2}) \leq 2\#B(\mathbb{F}_{p^2}) \leq 2(p+1)^2.$$

We have now proven in all cases that

$$\#X_0(N)(\mathbb{F}_{p^2}) \leq \max\{2(p+1)^2,\ p^2 + 10p + 1\}.$$

Combining this upper bound with the lower bound given above proves the first part of Lemma 6.

The specific bounds for small values of p can be obtained by explicitly calculating $s(p)$. For example, if every supersingular curve in characteristic p is defined over $\mathbb{F}_p$ (which is true for $p \leq 31$), then the mass formula of Deuring and Eichler [6, Ex. 5.9] says that $s(p) = (p-1)/24$. This suffices for the particular cases considered in Lemma 6.

Proof of Theorem 4 (Conclusion). We suppose that $X_0(N)$ is bielliptic. Applying Lemma 6 (with the trivial estimates $N < \mu(N)$ and $\nu(N) \geq 1$) gives

$$\begin{aligned}
&N < 276, && \text{if } 2 \nmid N,\\
&N < 228, && \text{if } 3 \nmid N,\\
&N < 222, && \text{if } 5 \nmid N,\\
&N < 252, && \text{if } 7 \nmid N,\\
&N < 343\tfrac{1}{5}, && \text{if } 11 \nmid N.
\end{aligned}$$

If $N \leq 343$, we are done; so from the above list we may assume that N is divisible by $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Write

$$N = N_2 N_3 N_5 N_7 N_{11} M,$$

where N_p is the largest power of p dividing N.

Since there are finite maps $X_0(N) \to X_0(N/N_p)$, Proposition 1 says that the curves $X_0(N/N_p)$ are either hyperelliptic or bielliptic. Since p does not divide N/N_p (for $p = 2, 3, 5, 7, 11$), we can apply Lemma 6 to $X_0(N/N_p)$ and the

prime p. Noting that $\nu(N/N_p) \geq 4$, this yields

$$\begin{aligned}
N/N_2 &\leq \tfrac{3}{4} \cdot \tfrac{5}{6} \cdot \tfrac{7}{8} \cdot \tfrac{11}{12}\mu(N/N_2) \leq 54\tfrac{9}{64}, \\
N/N_3 &\leq \tfrac{2}{3} \cdot \tfrac{5}{6} \cdot \tfrac{7}{8} \cdot \tfrac{11}{12}\mu(N/N_3) \leq 64\tfrac{1}{6}, \\
N/N_5 &\leq \tfrac{2}{3} \cdot \tfrac{3}{4} \cdot \tfrac{7}{8} \cdot \tfrac{11}{12}\mu(N/N_5) \leq 72\tfrac{3}{16}, \\
N/N_7 &\leq \tfrac{2}{3} \cdot \tfrac{3}{4} \cdot \tfrac{5}{6} \cdot \tfrac{11}{12}\mu(N/N_7) \leq 85\tfrac{5}{9}, \\
N/N_{11} &\leq \tfrac{2}{3} \cdot \tfrac{3}{4} \cdot \tfrac{5}{6} \cdot \tfrac{7}{8}\mu(N/N_{11}) \leq 119.
\end{aligned}$$

Multiplying these estimates gives

$$N^4 \leq N^5/(N_2N_3N_5N_7N_{11}) \leq 2,553,229,906,$$

and so $N < 225$.

Acknowledgment

After completing this research, the authors became aware of earlier work by Bob Accola and Alan Landman. Accola and Landman proved Proposition 1 by essentially the same method, but never published their results. The second author would also like to thank Bill McCallum and Paul Vojta for pointing out an error in his original proof of Theorem 2.

References

1. E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves*, vol. I, Springer-Verlag, New York, 1985.
2. G. Faltings, *Diophantine approximation on Abelian varieties*, preprint.
3. G. Frey, *A remark about isogenies of elliptic curves over quadratic fields*, Compositio Math. **58** (1986), 133–134.
4. M. Hindry, *Points quadratiques sur les courbes*, C. R. Acad. Sci. Paris Sér. I **305** (1987), 219–221.
5. A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.
6. J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138

Department of Mathematics, Brown University, Providence, Rhode Island 02912