Experimental Mathematics, 21(2):103–116, 2012

ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2012.645780

Taylor & Francis
Taylor & Francis Group

A Local Version of Szpiro's Conjecture

Michael A. Bennett and Soroosh Yazdani

CONTENTS

Szpiro's conjecture asserts the existence of an absolute constant $K > 6$ such that if E is an elliptic curve over $\mathbb{Q}$, the minimal discriminant $\Delta(E)$ of E is bounded above in modulus by the Kth power of the conductor $N(E)$ of E. An immediate consequence of this is the existence of an absolute upper bound on $\min\{v_p(\Delta(E)) : p \mid \Delta(E)\}$. In this paper, we will prove this *local* version of Szpiro's conjecture under the (admittedly strong) additional hypotheses that $N(E)$ is divisible by a "large" prime p and that E possesses a nontrivial rational isogeny. We will also formulate a related conjecture that if true, we prove to be sharp. Our construction of families of curves for which $\min\{v_p(\Delta(E)) : p \mid \Delta(E)\} \geq 6$ provides an alternative proof of a result of Masser on the sharpness of Szpiro's conjecture. We close the paper by reporting on recent computations of examples of curves with large Szpiro ratio.

1. INTRODUCTION

If E is an elliptic curve over $\mathbb{Q}$, two classical invariants attached to E that measure the primes of bad reduction of E are the conductor of E and the minimal discriminant of E, denoted in this paper by $N(E)$ and $\Delta(E)$, respectively. These have the property that a prime p divides $N(E)$ or $\Delta(E)$ precisely when E has bad reduction at p. Furthermore, either quantity can be calculated locally by studying $E/\mathbb{Q}_p$. They are related via the following result.

Proposition 1.1. (Ogg's Formula.) *Let $L/\mathbb{Q}_p$ be a local field, E/L an elliptic curve, and set*

- $v(\Delta) =$ *the valuation of the minimal discriminant of E/L,*
- $f(E/L) =$ *the exponent of the conductor of E/L,*
- $m(E/L) =$ *the number of components of the special fiber of E/L.*

Then

$$v(\Delta) = f(E/L) + m(E/L) - 1.$$

Using Ogg's formula, it is immediate that $N(E)$ divides $\Delta(E)$ and in particular, that $N(E) \leq |\Delta(E)|$. A

2000 AMS Subject Classification: 11G0S, 14H5Z
Keywords: elliptic curves, Szpiro's conjecture

Conductor	Cremona label	Szpiro ratio
12735814	–	9.01996406836501
1290	h1	8.90370022470358
9510	e1	8.84312822607337
2526810	–	8.81194357194048
9690	m2	8.80159647164269
3990	ba1	8.79237406416090
32658	b1	8.78266784426543
858	k2	8.75731614557112
89150698	–	8.69894197172524
167490523410	–	8.68896770822104

TABLE 1. Top-ten largest known Szpiro ratios.

well-known conjecture of Szpiro provides a bound in the other direction.

Conjecture 1.2. (Szpiro's conjecture.) *Given $\epsilon > 0$, there exists a constant C_ϵ such that for every elliptic curve $E/\mathbb{Q}$,*

$$|\Delta(E)| \leq C_\epsilon N(E)^{6+\epsilon}.$$

This conjecture lies very deep and is (nearly) equivalent to the *abc* conjecture of Masser and Oesterlé. An immediate consequence of Szpiro's conjecture is that the *Szpiro ratio*

$$S(E) = \frac{\log(|\Delta(E)|)}{\log(N(E))}$$

is absolutely bounded as E ranges over all elliptic curves over $\mathbb{Q}$. The example we know with $S(E)$ largest corresponds to

$$E : y^2 + xy = x^3 - 4241517626670033585 18x - 6292273164116612928531204122716,$$

which has minimal discriminant

$$\Delta(E) = -2^{33} \cdot 7^{18} \cdot 13^{27} \cdot 19^3 \cdot 29^2 \cdot 127$$

and conductor

$$N(E) = 2 \cdot 7 \cdot 13 \cdot 19 \cdot 29 \cdot 127,$$

and hence $S(E) = 9.01996\ldots$. In Table 1, we list some data on the largest Szpiro ratios known to us (information on coefficients for Weierstrass models of these curves will be tabulated later).

An immediate corollary of Conjecture 1.2 is the following.

Proposition 1.3. *Assume that Szpiro's conjecture is true for some $\epsilon < 1$ and C_ϵ. Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor N (so that N is square-free). Then if there exists a prime $p \mid N$ for which $p > C_\epsilon^{1/6} N^{(5+\epsilon)/6}$, we may conclude that $v_p(\Delta(E)) \leq 6$.*

This proposition suggests the following, to which we will henceforth refer as the *local Szpiro conjecture*.

Conjecture 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N(E)$ and minimal discriminant $\Delta(E)$. Then there is a prime $p \mid N(E)$ for which*

$$v_p(\Delta(E)) \leq 6\, v_p(N(E)).$$

In particular, if E is semistable, there exists a prime $p \mid N(E)$ with $v_p(\Delta(E)) \leq 6$.

Using Ogg's formula, one can reword this conjecture in terms of the size of the component group of the special fiber of $E/\mathbb{Q}_p$. Alternatively, for large enough p (so that $E[p]$ is irreducible), $v_p(\Delta(E))$ is closely related to level lowering of the modular form attached to E (see [Ribet 91]). As such, Proposition 1.3 can be restated in terms of congruences between modular forms of levels M and N, where $M \mid N$.

The goal of this paper is to study Proposition 1.3, without the assumption of Szpiro's conjecture. We can, in fact, deduce a like conclusion (with different bounds on p) under the additional assumption that $E(\mathbb{Q})$ has a nontrivial rational isogeny.

Theorem 1.5. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor $N(E) = Mp$ and minimal discriminant $\Delta(E)$. Assume that there is an integer $n > 1$ such that E possesses a rational n-isogeny. Then there exists a constant $C = C(M)$ such that if $p \geq C$, then $v_p(\Delta(E)) \leq 6$.*

Optimistically, one might view this as evidence for the validity of Szpiro's conjecture (although the property of having a nontrivial rational isogeny is admittedly rather special).

We now give a brief outline of the paper. The general approach for the proof of Theorem 1.5 is to study universal elliptic curves associated to standard modular curves and exploit the fact that they have correspondingly "nice" discriminant formulas. We begin, in Section 2, by considering the case of elliptic curves having more than three rational torsion points. In Section 3, we carry out a similar analysis for elliptic curves with a rational N-isogeny, and finally, in Section 4, we deal with elliptic curves with rational 2- or 3-isogeny. The results of these three sections combine to prove Theorem 1.5. In Section 5, we apply the results of Section 2 to prove Szpiro's

conjecture when the ramification of elliptic curves is limited (see Theorem 5.1). In Section 6, we reinterpret Theorem 1.5 in terms of level lowering, and suggest some other problems that seem related to the subject at hand.

Section 7 is devoted to a construction that produces infinitely many curves $E/\mathbb{Q}$ for which $\min\{v_p(\Delta(E)) : p \mid \Delta(E)\} \geq 6$ (whereby Conjecture 1.4, if true, is necessarily sharp). This provides an alternative proof to that given in [Masser 90] that the same is true for Szpiro's conjecture. Finally, in Section 8, we extend some of the computations of [Nitaj 98] to find more examples of elliptic curves with large Szpiro ratio.

2. ELLIPTIC CURVES WITH RATIONAL *N*-TORSION

Let X/K be a moduli space of elliptic curves with some given level structure. Assume that X is a genus-0 curve, and note that any such curve will have a natural map $j : X \to X(1)$.[1] The set $j^{-1}(\infty)$ is the set of cusps of X, and the ramification index of each cusp is the multiplicity of the cusp in this preimage. The goal of this section is to prove the following theorem.

Theorem 2.1. *Let X be a modular curve of genus zero. Assume that the cusps of X are in g distinct Galois orbits with $g \geq 3$, and let $e_1, e_2, \ldots, e_g$ be the ramification indices of the cusps in each Galois orbit. Then for any integer M, there exists a constant $C = C(M)$ such that if*

(a) *$E/\mathbb{Q}$ is an elliptic curve of conductor $Mp_1p_2\cdots p_{g-2}$ and minimal discriminant Δ_E, where the p_i are distinct primes for $1 \leq i \leq g-2$,*

(b) *$\min(p_1, p_2, \ldots, p_{g-2}) > C$, and*

(c) *there is $\tau \in X(\mathbb{Q})$ such that $j(\tau) = j(E)$,*

then the multiset $\{v_{p_i}(\Delta_E)\}$ is a multisubset of $\{e_1, e_2, \ldots, e_g\}$.

The main application of the above theorem for us is to prove a small result toward the local Szpiro conjecture for elliptic curves having $\#E(\mathbb{Q})_{\text{tors}} > 3$. Specifically, we have the following sharpening of Theorem 1.5.

Corollary 2.2. *Given M and $N > 3$, there is an effectively computable constant $C = C(M)$ such that if*

$$p_1, p_2, \ldots, p_{[N/2]-1}$$

is a set of primes with $p_i > C$ for each i, and $E/\mathbb{Q}$ is an elliptic curve with conductor $Mp_1p_2\cdots p_{[N/2]-1}$ and minimal discriminant Δ_E having a rational N-torsion point, then we have $v_{p_i}(\Delta_E) \mid N$ for all i, and $v_{p_j}(\Delta_E) \leq 6$ for some j.

Proof of Corollary 2.2. If $E(\mathbb{Q})$ has an N-torsion point, then $j(E)$ is in the image of $j : X \to X(1)$, where $X = X_1(N)$ is one of the modular curves in Table 2 (with, we note, at least three distinct Galois orbits of three rational cusps, since $N > 3$).

The result now follows immediately by studying the ramification indices of each Galois orbit and applying Theorem 2.1. □

We will prove Theorem 2.1 using effective methods from Diophantine approximation for solving Thue–Mahler and S-unit equations. Throughout this section, we denote by K a finite extension of $\mathbb{Q}$, by $\mathcal{O}_K$ the ring of integers of K, by S a finite collection of primes of $\mathcal{O}_K$, by $\mathcal{O}_{K,S}$ the set of S-integers in K, and by $\mathcal{S}$ the set of S-units in $\mathcal{O}_K$ (i.e., the set of $x \in \mathcal{O}_K$ such that $v_\pi(x) = 0$ for all primes $\pi \notin S$). Furthermore, let $N(\pi)$ be the norm of the ideal π, and let $\|x\|$ be the maximum modulus of the image of x for all embeddings $K \to \mathbb{C}$.

Proposition 2.3. (Thue–Mahler equations.) *Let $f(x, y) \in \mathcal{O}_K[x, y]$ be a binary form (i.e., a homogeneous polynomial) of degree n. Assume that $f(X, 1)$ has at least three distinct roots in $\overline{K}$. Then for every solution of $f(a, b) = z$ in $a, b \in \mathcal{O}_K$, $z \in \mathcal{S}$, with $N(a\mathcal{O}_K + b\mathcal{O}_K) = 1$, there is a unit $\epsilon \in \mathcal{O}_K$ such that*

$$\max(\|\epsilon a\|, \|\epsilon b\|) < C,$$

where C is an effectively computable constant that depends only on K, S, and f.

Proof. See [Shorey and Tijdeman 86, Theorem 7.6]. □

Proposition 2.4. (S-unit equations.) *Let $f(x, y) \in \mathcal{O}_K[x, y]$ be a binary form such that the polynomial $f(x, 1)$ has no repeated roots in $\mathbb{C}$. Then there exist at most finitely many $a, b \in \mathcal{S}$ such that the equation*

$$f(a, b) = uz^r$$

has solutions with $u \in \mathcal{S}$, $z \in \mathcal{O}_K$, and $r \in \mathbb{N}$, $r \geq 2$.

Proof. This is standard, and one can find the argument for the case $r = 2$ in, for example, [Silverman 92, Theorem 4.3]. We will present a proof here for the benefit of the reader. We begin by extending K so that f splits into

[1] We can extend our results to any genus-0 curve X/K with a map $j : X \to X(1)$; we will, however, state our results only for modular curves.

X	Number of Galois orbits of cusps	Ramification data
$X(1)$	1	1
$X_1(2)$	1, 1	2, 1
$X_1(3)$	1, 1	3, 1
$X_1(4)$	1, 1, 1	4, 1, 1
$X_1(5)$	1, 1, 2	5, 5, 1
$X_1(6)$	1, 1, 1, 1	6, 3, 2, 1
$X_1(7)$	1, 1, 1, 3	7, 7, 7, 1
$X_1(8)$	1, 1, 1, 1, 2	8, 8, 4, 2, 1
$X_1(9)$	1, 1, 1, 2, 3	9, 9, 9, 3, 1
$X_1(10)$	1, 1, 1, 1, 2, 2	10, 10, 5, 5, 2, 1
$X_1(12)$	1, 1, 1, 1, 2, 2, 2	12, 12, 6, 2, 4, 3, 1
$X(2)$	1, 1, 1	2, 2, 2
$X(2) \times_{X_1(2)} X_1(4)$	1, 1, 1, 1	4, 4, 2, 2
$X(2) \times_{X_1(2)} X_1(6)$	1, 1, 1, 1, 1, 1	6, 6, 6, 2, 2, 2
$X(2) \times_{X_1(2)} X_1(8)$	1, 1, 1, 1, 2, 2, 2	8, 8, 8, 8, 4, 2, 2

TABLE 2. $X_1(N)$ and $X(2) \times_{X_1(2)} X_1(2N)$ data.

linear factors

$$f(x,y) = A(x-\alpha_1 y)(x-\alpha_2 y)\cdots(x-\alpha_n y)$$

and subsequently enlarge S so that

(a) $A \in \mathcal{S}$,

(b) $\alpha_i \in \mathcal{S}$ for all i,

(c) $\alpha_i - \alpha_j \in \mathcal{S}$ for all $i \neq j$, and

(d) $\mathcal{O}_{K,S}$ is a principal ideal domain.

It follows that we may write $x - \alpha_i y = u_i z_i^r$, and after changing variables, we arrive at the equation $x - y = z_i^r$ with $x, y \in \mathcal{S}$. This equation, however, has only finitely many solutions for $r \geq 2$, via, for example, [Shorey and Tijdeman 86, Theorem 9.4]. □

We can appeal to the preceding two propositions to prove the following result.

Proposition 2.5. *Let $g \geq 3$, $F_1, F_2, \ldots, F_g \in \mathcal{O}_K[x,y]$ be distinct irreducible binary forms and let $e_1, e_2, \ldots, e_g$ be positive integers. Furthermore, assume that $\mathcal{O}_{K,S}$ is a unique factorization domain. Then there is an effectively computable constant C such that if $a, b \in \mathcal{O}_{K,S}$ satisfy*

$$F_1(a,b)^{e_1} F_2(a,b)^{e_2} \cdots F_g(a,b)^{e_g} = u p_1^{r_1} p_2^{r_2} \cdots p_{g-2}^{r_{g-2}} \tag{2–1}$$

for some $u \in \mathcal{S}$ and some collection of primes $p_1, \ldots, p_{g-2}$ with $\|p_i\| > C$ for all i, then $\{r_1, r_2, \ldots, r_{g-2}\}$ is a multisubset of $\{e_1, e_2, \ldots, e_g\}$.

Proof. Since we assume that the F_i are distinct irreducible forms, for any pair of integers $a, b \in \mathcal{O}_K$ we have $\gcd(F_i(a,b), F_j(a,b)) \mid R$, where R is the product of the resultants of each pair F_i and F_j with $i \neq j$. Let C_1 be large enough that if $\|p_i\| > C_1$, then p_i fails to divide R.

Consider the set of solutions $(a, b, \{p_i\})$ to equation (2–1) with $\min(\|p_i\|) > C_1$. First, let us assume that for some i, there exist j_1 and j_2 such that $p_{j_1} p_{j_2} \mid F_i(a,b)$. Then, by the pigeonhole principle, there are three polynomials (say F_1, F_2, and F_3) such that $F_1(a,b)F_2(a,b)F_3(a,b) = v$ for some $v \in \mathcal{S}$. Since $F_1F_2F_3$ has degree at least three, it follows by Proposition 2.3 that $\max(\|\epsilon a\|, \|\epsilon b\|) < C_2$ for some S-unit ϵ. Therefore, $F_i(a,b)$ will take only finitely many possible prime values in this case. Let C_3 be the larger of the largest prime value that divides $F_i(a,b)$ and C_1.

If we choose $\min(\|p_i\|) > C_3$, then the equation $\prod F_i(a,b)^{e_i} = u \prod p_j^{r_j}$ implies that each F_i has at most one prime p_j dividing it. Without loss of generality, we may therefore assume that $p_i^{r_i} \mid F_i(a,b)^{e_i}$, for $i = 1, 2, \ldots, g-2$, and that

$$F_{g-1}(a,b)^{e_{g-1}} F_g(a,b)^{e_g} = v, \quad v \in \mathcal{S}.$$

Furthermore, F_{g-1} and F_g must both be linear, and after a linear change of variables, we may assume $F_{g-1}(x,y) = x$ and $F_g(x,y) = y$.

We conclude that $a, b \in \mathcal{S}$ and hence may write

$$F_i(a,b) = v_i p_i^{r_i/e_i}, \tag{2–2}$$

where now $a, b, v_i \in \mathcal{S}$. By Proposition 2.4, there are only finitely many solutions to (2–2) with $r_i \notin \{0, e_i\}$. Choosing C_4 large enough, it follows that if $\min(\|p_i\|) > C_4$, then $r_i \in \{0, e_i\}$ for $i = 1, 2, \ldots, g-2$, as desired. □

Interpreting the above proposition geometrically finishes the proof of Theorem 2.1. Specifically, let $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. Then each element of $\mathbb{P}^1(K)$ has a representative $[a : b] \in K^2 \setminus \{[0 : 0]\}$, with the point at infinity represented by $[1 : 0]$. Note that any point $z = [a : b] \in \mathbb{A}^1$ corresponds to a rational number $a/b \in K$.

Therefore, any valuation on K extends naturally to a valuation on $\mathbb{P}^1(K)$, specifically $v([a : b]) = v(a) - v(b)$. Note that $v([0 : 1]) = -\infty$ and $v([1 : 0]) = \infty$. Furthermore, given any pair of K-rational points P and Q, there is a K-rational isomorphism that will send P to $[0 : 1]$ and Q to $[1 : 0]$ (since we can map any three given rational points to any other three rational points).

Let $j : X \to X(1)$ be a K-rational map. Then we can write this down explicitly as

$$[a : b] \mapsto [G(a, b), F(a, b)]$$

for F and G homogeneous polynomials with rational coefficients of the same degree. We may assume, without loss of generality, that F and G are coprime and have coefficients in $\mathcal{O}_K$. We define the degree of ϕ to be the degree of F (or G). Note that

$$\phi^{-1}(\infty) = \{[a : b] \in \mathbb{P}^1 : F(a, b) = 0\}.$$

We can factor $F(a, b) = \prod_{i=1}^{g} F_i(a, b)^{e_i}$, where each F_i is K-irreducible and every pair F_i and F_j are coprime. Note that the points $P_i = \{[a : b] : F_i(a, b) = 0\}$ form a Galois orbit of a point in $\phi^{-1}(\infty)$, and g is the number of Galois orbits of $\phi^{-1}(\infty)$. We also have $\sum_{i=1}^{g} \deg(F_i)$, $e_i = \deg(\phi)$. This completes the proof of Theorem 2.1.

3. ELLIPTIC CURVES WITH RATIONAL *N*-ISOGENIES

The methods in the previous section do not seem amenable to studying the local Szpiro conjecture for elliptic curves with a rational N-isogeny (but without rational N-torsion). Specifically, $X_0(N)$ has, for N prime, only two cusps, which necessitates a modification of our approach. If, however, we consider ramification data over $j = 0$ and 1728, we arrive at the following result.

Theorem 3.1. *Let X be a modular curve of genus zero. Assume that X has g cusps, all rational, and let e_i be the ramification index of these cusps. Furthermore, assume that there are two unramified points above $j = 1728$ or $j = 0$. Then for any integer M, there exists a constant $C = C(M)$ such that if*

(a) *$E/\mathbb{Q}$ is an elliptic curve of conductor $Mp_1p_2 \cdots p_{g-1}$ and minimal discriminant Δ_E,*

(b) *$\min(p_i) > C$,*

(c) *there is $\tau \in X(\mathbb{Q})$ such that $j(\tau) = j(E)$,*

then the points above $j = 0$ are all ramified and the multiset $\{v_{p_i}(\Delta_E)\}$ is a multisubset of $\{e_1, e_2, \ldots, e_g\}$.

An immediate corollary of the above theorem is the following.

Corollary 3.2. *Given positive integers M and $N > 3$, there is an effectively computable constant $C = C(M)$ such that for any prime $p > C$ and any elliptic curve $E/\mathbb{Q}$ possessing a rational N-isogeny with conductor Mp and minimal discriminant Δ_E, we have $v_p(\Delta_E) \mid N$ and $v_p(\Delta_E) \leq 6$.*

Proof of Corollary 3.2. Note that with finitely many exceptions, all rational elliptic curves having a rational N-isogeny and no complex multiplication arise from rational points on $X_0(N)$, where N has genus 0. We know that if E has complex multiplication, then E has potentially good reduction everywhere, and hence it cannot have multiplicative reduction at p. Therefore, E arises from a rational point on one of the curves in Table 3.

When N is prime, we can apply Theorem 3.1 to obtain the desired result. For the other cases, there are sufficiently many Galois orbits of cusps to apply Theorem 2.1. □

The following lemma is the main ingredient for proving Theorem 3.1. For simplicity, we assume that $K = \mathbb{Q}$ and S is a finite set of primes including 2 and 3. As such, $\mathcal{O}_{K,S} = \mathbb{Z}[1/S]$.

Lemma 3.3. *Let $j = g/f$ and $j - 1728 = h/f$ with $f, g, h \in \mathcal{O}_{K,S}$ coprime S-integers, $gh \neq 0$. Then*

(a) *the elliptic curve E_j given by the model $y^2 = x^3 - 3ghx + 2gh^2$ has $j(E_j) = j$ and discriminant $1728^2 f g^2 h^3$;*

(b) *if for $p \notin S$, we have either $3 \nmid v_p(g)$ or $2 \nmid v_p(h)$, and if $E/\mathbb{Q}$ is any elliptic curve with $j(E) = j$, then E has additive reduction at p.*

Proof. The first part of the lemma is a straightforward calculation. For the second part, note that any elliptic curve with the same j-invariant is a quadratic twist of E_j, which we can write explicitly as

$$y^2 = x^3 - 3ghr^2x + 2gh^2r^3.$$

If $3 \nmid v_p(g)$ or $2 \nmid v_p(h)$, then any such twist will still have additive reduction at p. □

X	Number of Galois orbits of cusps	Ramification data	Number of unramified points above $j=0$ and $j=1728$
$X_0(2)$	$1,1$	$2,1$	$0,1$
$X_0(3)$	$1,1$	$3,1$	$1,0$
$X_0(4)$	$1,1,1$	$4,2,1$	$0,0$
$X_0(5)$	$1,1$	$5,1$	$0,2$
$X_0(6)$	$1,1,1,1$	$6,3,2,1$	$0,0$
$X_0(7)$	$1,1$	$7,1$	$2,0$
$X_0(8)$	$1,1,1,1$	$8,4,2,1$	$0,0$
$X_0(9)$	$1,1,1$	$9,3,1$	$0,0$
$X_0(10)$	$1,1,1,1$	$10,5,2,1$	$0,2$
$X_0(12)$	$1,1,1,1,1,1$	$12,6,4,3,2,1$	$0,0$
$X_0(13)$	$1,1$	$13,1$	$2,2$
$X_0(16)$	$1,1,1,1,1$	$16,8,4,2,1$	$0,0$
$X_0(18)$	$1,1,1,1,1,1$	$18,9,6,3,2,1$	$0,0$
$X_0(25)$	$1,2,1$	$25,5,1$	$0,2$

TABLE 3. $X_0(N)$ data.

Now let $j : X \to X(1)$ be as before, given by $j = [G, F]$, where G and F are homogeneous polynomials of the same degree with no common factor. Let $j - 1728 = [H, F]$ (that is, $G - H = 1728F$). Let $G = G_{\mathrm{u}} G_{\mathrm{r}}^3$ and $H = H_{\mathrm{u}} H_{\mathrm{r}}^2$. Note that the degree of G_{u} (respectively H_{u}) is the number of unramified points above the point $j = 0$ (respectively $j = 1728$). Assume that E is an elliptic curve such that $j(E) = j([a : b])$ for some $[a : b] \in X(\mathbb{Q})$. By Lemma 3.3, if E has semistable reduction outside S, then

$$G_{\mathrm{u}}(a, b) = ug^3, \quad H_{\mathrm{u}}(a, b) = vh^2,$$

where $u, v \in \mathcal{S}$ and $g, h \in \mathbb{Z}$. Since S is a finite set of primes, any such elliptic curve corresponds to solutions to a finite number of such Diophantine equations. We will focus on the case that G_{u} and H_{u} are of degree 2 or 0 (when $X = X_0(N)$, this is satisfied for $N > 3$ prime). The following lemma is well known.

Lemma 3.4. *Let $Q(x, y)$ be a binary quadratic form in $\mathbb{Q}[x, y]$, and let $r \geq 1$. Then there exists a finite number of pairs of homogeneous polynomials A_i, B_i of degree r such that $(A_i(\alpha, \beta), B_i(\alpha, \beta))$ is a solution to $Q(a, b) = c^r$ for all coprime α, β, and all solutions to $Q(a, b) = c^r$, with a and b coprime integers, belong to one of the above families.*

Proof. The above Diophantine equation is just a twist of the Diophantine equation $x^2 - y^2 = z^r$, which gives us the desired result (see [Darmon and Granville 95]). □

We are now ready to prove Theorem 3.1. Specifically, since we are assuming that there is a pair of unramified points above either $j = 0$ or $j = 1728$, it follows that either G_{u} or H_{u} is a binary quadratic form. When H_{u} (respectively G_{u}) is a binary quadratic form, Lemma 3.4 tells us that if $j(E) = j([a, b])$, then $(a, b) = (A(\alpha, \beta), B(\alpha, \beta))$ for some A and B of degree two (respectively degree three) coming from a finite list of possibilities.

On the other hand, since we assume that X has precisely g (rational) cusps, it follows that

$$F(a, b) = \prod_{i=1}^{g} F_i(a, b)^{e_i} = u \prod_{i=1}^{g-1} p_i^{r_i},$$

where the F_i are linear forms. Substituting $(A(\alpha, \beta), B(\alpha, \beta))$ for (a, b), we may write

$$\prod_{i=1}^{g} \overline{F_i}(\alpha, \beta)^{e_i} = u \prod_{i=1}^{g-1} p_i^{r_i},$$

where $\overline{F_i}$ is a homogeneous polynomial of degree two (respectively three). If we choose the p_i large enough, then for some i, we must have $\overline{F_i}(\alpha, \beta) = u$, where $u \in \mathcal{S}$. Assume without loss of generality that $i = g$. When the

degree of $\overline{F_g}$ equals three, then from Proposition 2.4, it follows that there are only finitely many such solutions. Assume that the degree of $\overline{F_g}$ is 2. First consider the case $p_{j_1}p_{j_2} \nmid \overline{F_i}(\alpha,\beta)$. Then, possibly after reordering labels, we deduce the following system of equations:

$$\overline{F_i}(\alpha,\beta) = u_i p_i^{r_i/e_i}, \quad 1 \le i \le g-1, \quad \overline{F_g}(\alpha,\beta) = u_g,$$

where $u_i \in \mathcal{S}$. Such a system of Diophantine equations has been studied in [Shorey and Stewart 83], where it is shown that if $r_i/e_i \neq 1$, then there are only finitely many solutions to the above equation, the heights of which can be bounded effectively. Therefore, by choosing our constant C large enough, we conclude that if $\min(p_i) > C$, then $r_i = e_i$, as desired. If $p_{j_1}p_{j_2} \mid \overline{F_i}(\alpha,\beta)$, then necessarily $\overline{F_{i'}}(\alpha,\beta)$ is an S-unit for some $i' \neq g$. Assume without loss of generality that $i' = 1$, whereby

$$\overline{F_1}(\alpha,\beta) = u_1, \quad \overline{F_g}(\alpha,\beta) = u_g.$$

Again, by the results of [Shorey and Stewart 83], such equations have at most finitely many solutions. This finishes the proof of Theorem 3.1.

4. $X_0(N)$ FOR $N = 2, 3$

The final case we wish to consider is that of elliptic curves with rational 2- (or 3-) isogenies. Our methods of earlier sections do not apply in these cases. We can, however, prove the following result.

Proposition 4.1. *Given an integer M, there exists a constant C such that for any elliptic curve $E/\mathbb{Q}$ with a rational 2- (respectively 3-) isogeny of conductor Mp with $p > C$, we have $v_p(\Delta_E) \in \{1,2,4\}$ (respectively $v_p(\Delta_E) \in \{1,3\}$).*

Proof. Let

$$E_2 : uy^2 = x(x + ax + b),$$
$$E_3 : uy^2 = x^3 + \frac{a^2}{4}x^2 + \frac{ab}{2}x + \frac{b^2}{4}.$$

Then for any elliptic curve E with a rational 2- (respectively 3-) isogeny, we can find integers a, b and a square-free integer u such that $E \simeq E_2(a,b,u)$ (respectively $E \simeq E_3(a,b,u)$). Furthermore, if E has semistable reduction at a given prime $q > 3$, then we can demand that $q \nmid u\gcd(a,b)$, which ensures that the model for E_2 (respectively E_3) is minimal at q.

As before, let S be the set of primes dividing M, together with 2 and 3, and let $\mathcal{S}$ be the set of S-units in $\mathbb{Z}$. If $E = E_l(a,b,u)$ for $l = 2$ or 3, with conductor Mp, then we may assume without any loss of generality that $u \in \mathcal{S}$. Let Δ_l be the discriminant of E_l, and note that

$$\Delta_2 = 2^4 u^6 b^2 (a^2 - 4b),$$
$$\Delta_3 = u^6 b^3 (a^3 - 27b).$$

Assuming $p > M$, we may suppose that E has multiplicative reduction at p, and in particular, that $p \nmid u$ and $p \nmid \gcd(a,b)$.

Write $\Delta_E = \Delta' p^r$, where $\Delta' \in \mathcal{S}$. Assume first that $p \nmid ab$. Then $b \in \mathcal{S}$ and

$$\delta p^r = \begin{cases} a^2 - 4b, & l = 2, \\ a^3 - 27b, & l = 3, \end{cases}$$

where $\delta \in \mathcal{S}$. We are thus led to the Diophantine equation

$$a^l - \delta p^r = \beta$$

in variables a, p, and r, where $\beta, \delta \in \mathcal{S}$. Appealing to [Shorey and Tijdeman 86, Theorem 12.2], we deduce the existence of an effectively computable constant C, depending only on S, such that if $p > C$, then necessarily $lr \le 4$. From this conclusion, it follows that $r = 1$ when $l = 3$, and $r = 1$ or 2 when $l = 2$, which proves the theorem in this case.

Now assume that $p \mid ab$ (so that $p \mid b$, since otherwise, from the fact that $p \nmid \gcd(a,b)$, we would have $p \nmid \Delta_E$). We may thus write $b = \beta p^\rho$, where $\beta \in \mathcal{S}$. Note that in this case, $v_p(\Delta_E) = l\rho = r$. Furthermore, we have that

$$\delta = \begin{cases} a^2 - 4b, & l = 2, \\ a^3 - 27b, & l = 3, \end{cases}$$

where $\delta \in \mathcal{S}$. This leads to the Diophantine equation

$$a^l - \beta' p^\rho = \delta,$$

in a, p, ρ, where $\beta', \delta \in \mathcal{S}$. Again by [Shorey and Tijdeman 86, Theorem 12.2], we may conclude, for $p > C$, that $r = l\rho \le 4$. It follows that $(l,r) \in \{(2,2),(2,4),(3,3)\}$, as claimed. □

Combining Corollaries 2.2 and 3.2 with the above proposition immediately yields Theorem 1.5. We remark here that for E of conductor Mp having a rational N-isogeny with $N > 2$, we may conclude that $v_p(\Delta_E) \mid N$, provided that p is suitably large relative to M. We are unable to prove a similar result for $N = 2$. This is partly because the family of elliptic curves with rational 2-torsion naturally contains elliptic curves with a rational 4-torsion point, and there are infinitely many elliptic curves with conductor Mp arising from the latter family.

5. APPLICATIONS TO SZPIRO'S CONJECTURE

In this section we apply Theorem 2.1 to deduce Szpiro's conjecture for certain families of elliptic curves with limited ramification. Specifically, we prove the following.

Theorem 5.1. *Let $j : X \to X(1)$ be a modular curve of genus 0 over K, and let d be the degree of j, f the number of cusps of X, and g the number of Galois orbits of cusps. Assume that $g \geq 3$ and*[2]

$$(f-2) \geq \frac{d}{6}. \tag{5–1}$$

Then for any integer M and any $\epsilon > 0$, there are only finitely many elliptic curves E/K such that

(a) $j(E) = j(z)$ *for some* $z \in X(K)$,

(b) $N(E) = Mp_1p_2 \cdots p_{g-2}$ *for any collection of primes* p_i,

(c) $\|N(E)\|^{6+\epsilon} < \|\Delta(E)\|$.

We note that inequality (5–1) is satisfied for all the curves in Table 2 except for $X_1(2)$ and $X_1(3)$. As an immediate corollary of Theorem 5.1, we have the following.

Corollary 5.2. *For any integer M and real number $\epsilon > 0$, there are only finitely many elliptic curves $E/\mathbb{Q}$ such that*

(a) $N(E) = Mp_1p_2 \cdots p_l$ *for* $p_1, \ldots, p_l$ *prime,*

(b) $N(E)^{6+\epsilon} > |\Delta(E)|$,

(c) $E(\mathbb{Q})$ *has a rational* $(2l+2)$*-torsion point.*

To prove this theorem, we appeal to estimates for linear forms in logarithms, in order to bound the primes p_i. As usual, let K be a number field and S a finite set of primes. For the remainder of this section, we fix an embedding of K in the complex numbers and suppose that $|\cdot|$ is the usual complex norm. We will appeal to the following two results.

Proposition 5.3. (Linear forms in complex logarithms.) *There exists a positive constant C_1 depending on K and S such that for any $a, b \in \mathcal{S}$, we have*

$$|a-b| > \max(|a|,|b|)B^{-C_1},$$

where $B = B(a,b) = \max_{p\in S} |v_p(a/b)|$.

Proof. This is almost immediate from [Baker 73]; see also [Shorey and Tijdeman 86, Theorem B.2]. □

Proposition 5.4. (Linear forms in p-adic logarithms.) *There is a constant C_2 depending on K and S such that for any coprime $a, b \in \mathcal{S}$,*

$$v_q(a-b) < C_2 \log(B),$$

for any $q \in S$, where $B = B(a,b) = \max_{p\in S} |v_p(a/b)|$.

Proof. This is proved in [Van der Poorten 77] (see also [Shorey and Tijdeman 86, Theorem B.4]). □

We can apply this latter proposition to bound the absolute value of the S-unit part of $a-b$.

Corollary 5.5. *There is a constant C_3 depending on K and S such that for any triple $a, b, c \in \mathcal{S}$ and $z \in \mathcal{O}_K$ satisfying*

$$a - b = cz,$$

we have $|c| < B^{C_3}$.

Combining Corollary 5.5 and Proposition 5.3, it follows that if $a - b = cz$ with $a, b, c \in \mathcal{S}$, then

$$\max(|a|,|b|)\, B^{C_1} < |a-b| < |z|\, B^{C_3},$$

whereby

$$|z| > \max(|a|,|b|)\, B(a,b)^{C_4}. \tag{5–2}$$

We can actually prove a similar bound for a general homogeneous polynomial.

Corollary 5.6. *Let $F \in \mathcal{O}_K$ be a binary form of degree n such that the polynomial $F(x,1)$ has no repeated roots in $\mathbb{C}$, and let S be a finite set of primes. Then there exist constants C (possibly negative) depending on F, K, and S such that for any solution to the equation*

$$F(a,b) = up,$$

with $a, b, u \in \mathcal{S}$ and p prime, we have

$$|p| > \max(|a|,|b|)^n\, B(a,b)^C.$$

Proof. Let K' be the splitting field of F, so that

$$F(x,y) = \prod_{i=1}^{n} (\alpha_i x - \beta_i y).$$

Enlarge S to contain all primes dividing α_i and β_i, for each $i = 1, \ldots, n$, and so that $\mathcal{O}_{K,S}$ is a unique factorization domain. Assuming that p is large enough, we may

[2] Note that when all the points above $j = 0$ and $j = 1728$ are ramified to order 3 and 2 respectively, then Hurwitz's theorem implies that $f - 2 = d/6$.

thus write

$$\alpha_i a - \beta_i b = u_i \mathfrak{p}_i$$

for $i = 1, 2, \ldots, n$. From equation (5–2), it follows that

$$|\mathfrak{p}_i| > \max(|\alpha_i a|, |\beta_i b|) B(\alpha_i a, \beta_i b)^{C_1},$$

where C_1 depends upon K' and S. Let $m = \max(|a|, |b|)$. Note that

$$\max(|\alpha_i a|, |\beta_i b|) \geq m \min(|\alpha_i|, |\beta_i|) \geq C_2 m,$$

for some constant C_2 depending on F. Similarly,

$$B(\alpha_i a, \beta_i b) \geq B(a, b) + C_3.$$

We thus have

$$|\mathfrak{p}_i| > C_2 m (B(a, b) + C_3)^{C_1} > m\, B(a, b)^{C_4},$$

for each i, and hence the existence of C such that

$$|p| > m^n\, B(a, b)^C.$$

□

We note that by considering all possible embeddings of K in $\mathbb{C}$, we actually obtain

$$\|p\| > \max(\|a\|, \|b\|)^n B(a, b)^C.$$

Setting $m = \max(\|a\|, \|b\|)$, and noting that we can find κ such that $\|q\| > \kappa > 1$ for all $q \in S$, we thus have $B(a, b) > \log_\kappa(m)$, and so

$$\|p\| > m^n \log_\kappa(m)^C.$$

We will use this inequality to prove the main theorem of this section.

Proof of Theorem 5.1. Given M, let C_1 be the constant from Theorem 2.1. As in Section 2, we have that if E is a semistable elliptic curve of conductor $Mp_1p_2 \cdots p_{g-2}$ with $\|p_i\| > C_1$ such that $j(E) = j(z)$ for some $z \in X(K)$, then

$$\Delta(E) = a^{e_g} b^{e_{g-1}} \prod_{i=1}^{g-2} F_i(a, b)^{e_i},$$

with $a, b \in \mathcal{S}$ and $F_i(a, b) = u_i p_i$. From Corollary 5.6, there exists a constant C_2 such that

$$\|p_i\| > m^{f_i} \log_\kappa(m)^{C_2},$$

where $f_i = \deg F_i$. Let $f = \sum f_i$ be the number of cusps of X, and let $d = \sum f_i e_i$ be the degree of j. We thus have

$$\|N(E)\| > \|M\|\, m^{f-2} \log_\kappa(m)^{C_3},$$

for some C_3. On the other hand, by the triangle inequality, there is a constant C_4, depending only on F, such that

$$\|\Delta(E)\| = \|F(a, b)\| \leq C_4 m^d.$$

Now assume that E does not satisfy the inequality

$$\|N(E)\|^{6+\epsilon} > \|\Delta(E)\|. \tag{5–3}$$

Then

$$\|M\|^{6+\epsilon} m^{(f-2)(6+\epsilon)} \log_\kappa(m)^{C_3(6+\epsilon)} < C_4 m^d,$$

and so

$$m^{(f-2)(6+\epsilon)-d} < C_5 \log_\kappa(m)^{C_6}.$$

Since we suppose $f > 2$ and $6(f-2) \geq d$, it follows that

$$m^{C_7 \epsilon} < C_5 \log_\kappa(m)^{C_6},$$

whence there exists a constant $C_8 > 0$ such that

$$m = \max(\|a\|, \|b\|) < C_8.$$

This implies that there are only finitely many elliptic curves that do not satisfy the inequality (5–3), as desired. □

6. MODULAR FORMS

In this section, we will interpret our preceding results in terms of modular forms and Galois representations. Recall that attached to an elliptic curve $E/\mathbb{Q}$ and integer n, we have a Galois representation

$$\rho_{E,n} : G_\mathbb{Q} \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n),$$

where $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let E have conductor N and let l be prime. Assume for simplicity that $p \,\|\, N$ and that $p \neq l$. Then $\rho_{E,l}$ is unramified at p if and only if $l \mid v_p(\Delta(E))$.

Corollary 6.1. *Let E be an elliptic curve of conductor Mp with $p > C(M)$, as in Theorem 1.5. Assume that $E(\mathbb{Q})$ has a nontrivial torsion point. Then for $l > 2$ prime, $\rho_{E,l}$ is either ramified at p or reducible at p.*

In terms of modular forms, we know by [Wiles 95] and [Taylor and Wiles 95], for example, that there is a modular newform $f_E \in S_2(\Gamma_0(N))$ with integer coefficients attached to E. If $l \mid v_p(\Delta(E))$ is an odd prime and if $\rho_{E,l}$ is surjective, by [Ribet 91], for example, there exist a modular form $g \in S_2(\Gamma_0(N/p))$, say $g \in \mathcal{O}[[q]]$, and a prime $\lambda \subset \mathcal{O}$ such that $f_E \equiv g \pmod{\lambda}$.

Corollary 6.1 thus implies that if $N = Mp$ with $p > C(M)$, then (modulo some technicalities) there is no congruence with the p-old subspace of $S_2(\Gamma_0(N))$. This is

somewhat surprising, since we have the following level-raising result.

Proposition 6.2. *Let $g = \sum b_n q^n \in S_2(\Gamma_0(M))$ be a modular eigenform of level M. Let $l \mid a_p^2 - (p+1)^2$. Then there is a modular form $f \in S_2(\Gamma_0(Mp)^{p\text{-new}}$ such that $f \equiv g \pmod{\lambda}$ for some $\lambda \mid l$.*

In this context, our result implies that when one performs level raising for a suitably large prime p, then the form f cannot arise from an elliptic curve with nontrivial $E(\mathbb{Q})_{\text{tors}}$.

What about the corresponding situation for other modular forms? It is tempting to suppose that for any newform f of weight 2 and level N, there exists $p \mid N$ such that for any prime ideal λ of characteristic larger than 6, we have that $\rho_{f,\lambda}$ is either ramified at p or reducible. This is false, however, since there exists a modular form f of level 407, with Fourier coefficients in a field of degree 12 over $\mathbb{Q}$, that is congruent modulo a prime above 41 to a modular form attached to the elliptic curve 11A, and also modulo a prime above 17 to a form attached to the elliptic curve 37A. One might guess that for any modular eigenform f with coefficients defined over K_f, there exist a $p \mid N$ and a constant C, depending only on the degree of $K_f/\mathbb{Q}$, such that for any prime ideal λ of characteristic larger than C, $\rho_{f,\lambda}$ is necessarily unramified at p. Unfortunately, we have little data to support such a hypothesis.

7. THE LOCAL SZPIRO CONJECTURE: SHARPNESS

Our goal in this section is to show that Conjecture 1.4, if true, is sharp. We will restrict our attention to the case of semistable $E/\mathbb{Q}$, where we conjecture the existence of a prime of bad reduction p such that $v_p(\Delta_E) \leq 6$. Note that $v_p(\Delta_E) = -v_p(j(E))$ when E is semistable. We remark that searching through Cremona's tables of elliptic curves of conductor $N \leq 230000$, one finds no elliptic curve for which this bound is achieved, tempting one to suppose that it might be possible to replace the upper bound of 6 here with 5. In this section, we will show that there are in fact infinitely many semistable elliptic curves such that

$$\min_{p \mid \Delta_E} v_p(\Delta_E) = 6.$$

To prove this, we start by considering a semistable elliptic curve E with minimal discriminant $p^r M^n$. If n is a prime number and $E[n]$ is irreducible, then by [Ribet 91], one can find a modular form g of level p such that g is congruent to f_E. If g has integral coefficients, then for some elliptic curve F of conductor p, we have $F[n] \simeq E[n]$ as symplectic Galois modules. Conversely, given $F/\mathbb{Q}$ an elliptic curve of conductor p, assuming that $E/\mathbb{Q}$ is a semistable elliptic curve such that $F[n] \simeq E[n]$, then E will have minimal discriminant of the form $p^r M^n$ (we don't need n to be prime here). Therefore, if we are interested in semistable elliptic curves with minimal discriminant $p^r M^6$, it is natural to study the pairs (E, ϕ), where E is an elliptic curve and $\phi : E[6] \to F[6]$ is a symplectic isomorphism. This moduli problem is representable by the curve $X_F(6)$ over the rationals, a twist of the modular curve $X(6)$. This curve is itself an elliptic curve and has positive Mordell–Weil rank for almost all F (see [Rubin and Silverberg 99]). Instead of working with elliptic curves with prime conductor, we can (and will) work with any semistable elliptic curve with good reduction at 2 and 3.

Let F be any elliptic curve with square-free conductor N coprime to 6. We will find points on $X_F(6)$ where the p-adic valuation of the minimal discriminant of the corresponding elliptic curve is larger than 6 for all primes $p \mid N$.

First, note that $X_F(6)$ is birationally isomorphic to $X_F(2) \times_{X(1)} X_F(3)$ in a natural way, where the map $X_F(n) \to X(1)$ is just $(E, \phi) \mapsto E$. When $n = 2, 3$, and 5, this map has been studied in [Rubin and Silverberg 95] and [Rubin and Silverberg 01].

Let $F : Y^2 = X^3 + aX + b$ be an elliptic curve with minimal discriminant D. Then the map $X_F(2) \to X(1)$ can be written as

$$J(u, v) = \frac{(3au^2 + 9buv - a^2v^2)^3\, j(F)}{(3a)^3(u^3 + auv^2 + bv^3)^2},$$

where $[u : v]$ are the coordinates of $X_F(2)$ and $J(u, v)$ is the j-invariant map. Similarly, there is a concrete formula for $X_F(3) \to X(1)$, and we can verify that the image is $j(F)$ times a perfect cube. Therefore, the map $X_F(6) \to X_F(2)$ factors through the curve $C : u^3 + auv^2 + bv^3 = z^3$. The map $C \to X_F(2)$ is of degree 3, and therefore $X_F(6) \to C$ is of degree 4.

Notice that both C and $X_F(6)$ are genus-1 curves without a rational 2-isogeny for a generic choice of a and b (it is shown in [Rubin and Silverberg 99] that the equation for $X_F(6)$ is given by $Y^2 = X^3 - 16(4a^3 + 27b^2)$). Therefore, by choosing appropriate base points, the map $X_F(6) \to C$ is just multiplication by 2. Using $(b, -a, b)$ as a base point for C, we find that C is birationally isomorphic to $C' : Y^2 = X^3 - 16(4a^3 + 27b^2)$ under the map

$$\psi(x, y, z) = (\psi_1(x, y, z), \psi_2(x, y, z), \psi_3(x, y, z)),$$

where

$$\psi_1(x,y,z) = ax^2 - 8a^2xz - 6byz + 16a^3 + 216b^2z^2,$$
$$\psi_2(x,y,z) = -36bxz + 6ayz - 72abz^2,$$
$$\psi_3(x,y,z) = ax^2 + 4a^2xz - 6byz - 32a^3 - 216b^2z^2.$$

Note that the above argument provides us with explicit rational maps $\pi : X_F(6) \to X_F(2)$ and $\pi' : C' \to X_F(2)$.

We can now use the explicit maps π and π' to prove the following results.

Lemma 7.1. *Let F be a semistable elliptic curve of conductor N coprime to 6. Then any rational point P on $X_F(6)$ that reduces to a nonsingular point modulo $p \mid N$ satisfies $v_p(J(\pi(P))) \le v_p(j(F))$.*

Proof. Assume that

$$F : Y^2 = X^3 + aX + b.$$

If $v_p(J(\pi(P))) > v_p(j(F))$, then we must have $p \mid 3au^2 + 9buv - a^2v^2$ on $X_F(2)$. Since $p \mid 4a^3 + 27b^2$, this implies that

$$\frac{u}{v} \equiv \frac{-3b}{2a} \pmod{p},$$

which corresponds to the rational points on C that reduce to the singular point of C modulo p. □

Lemma 7.2. *f Let $F : Y^2 = X^3 + aX + b$ be a model for a semistable elliptic curve of conductor N coprime to 6. Assume, without loss of generality, that $\gcd(a,b,N) = 1$. Then for any rational point P of*

$$C' : zy^2 = x^3 - 16(4a^3 + 27b^2)z^3$$

in the domain of π' that reduces to

$$\left(9^2ab^2, -9^3b^3, a^3\right) \quad \text{modulo } p \mid N,$$

we have $v_p(J(\pi'(P))) < v_p(j(F))$.

Proof. For the inequality $v_p(J(u,v)) < v_p(j(F))$ to hold, we must have u/v congruent to either

$$\frac{-3b}{2a} \quad \text{or} \quad \frac{-3b}{a} \quad \text{modulo } p.$$

The former corresponds to a singular point on C', and the latter to a point that reduces to the desired congruence class. □

Lemma 7.3. *Let $F : Y^2 = X^3 + aX + b$ be a semistable elliptic curve of conductor N coprime to 6. Assume that $\gcd(a,b,N) = 1$, and let $C' : zy^2 = x^3 - 16(4a^3 + 27b^2)z^3$. Let $C'_{ns}(\mathbb{F}_p)$ be the set of nonsingular points of C' modulo p. Then we have that $C'(\mathbb{Q})$ surjects onto $\prod_{p|N} C'_{ns}(\mathbb{F}_p)$.*

Proof. We know that $C'_{ns}(\mathbb{F}_p) \simeq \mathbb{G}_a(\mathbb{F}_p) = \mathbb{Z}/p\mathbb{Z}$ as an abelian group, and in this model we can write this isomorphism explicitly as $(x,y,z) \mapsto x/y$. Appealing to the Chinese remainder theorem, we find that $\prod_{p|N} C'_{ns}(\mathbb{F}_p) \simeq \mathbb{Z}/N\mathbb{Z}$. It suffices, therefore, to show that there is a rational point on $C'(\mathbb{Q})$ that reduces to a generator of $\mathbb{Z}/N\mathbb{Z}$. From [Rubin and Silverberg 99], we have that

$$P = \left(4a\left(a^3 + 9b^2\right), -36b\left(a^3 + 6b^2\right), a^3\right)$$

is a rational point on C' that does not reduce to a singular point on $C'(\mathbb{F}_p)$ for any $p \mid N$. In particular, P is mapped to

$$\frac{4a(a^3 + 9b^2)}{-36b(a^3 + 6b^2)} \equiv \frac{a}{3b} \in \mathbb{Z}/N\mathbb{Z}.$$

Since we are assuming that $\gcd(a,b,N) = 1$ and since $3 \nmid N$, this point generates $\prod_{p|N} C'_{ns}(\mathbb{F}_p)$. □

Proposition 7.4. *Let F be a semistable elliptic curve of conductor N coprime to 6 and minimal discriminant Δ_F. Then there are infinitely many rational points on $(E,\phi) \in X_F(6)(\mathbb{Q})$ such that E is semistable with minimal discriminant Δ_E such that for any prime $p \mid \Delta_E$, we have $v_p(\Delta_E) = 6k + v_p(\Delta_F)$ for some $k > 0$. In particular, $\min_{p|\Delta_E} v_p(\Delta_E) \ge 6$.*

Proof. We know that $X_F(6) \to C$ is just the multiplication-by-2 map. It follows that if we can find a point on $2\,C'(\mathbb{Q})$ that reduces to $(9^2ab^2, -9^3b^3, a^3)$ modulo N, we will have the desired result. However, by Lemma 7.3, we know that $C'(\mathbb{Q})$ surjects onto $\prod_{p|N} C'_{ns}(\mathbb{F}_p) \simeq \mathbb{Z}/N\mathbb{Z}$. Since $(9^2ab^2, -9^3b^3, a^3)$ is a nonsingular point modulo all primes $p \mid N$, and since N is odd, there is necessarily a point in $2\,C'(\mathbb{Q})$ that reduces to the desired congruence class, which proves the proposition. □

We remark that the point

$$\left(4a(a^3 + 9b^2)\right, -36b\left(a^3 + 6b^2\right), a^3\right) \in C'(\mathbb{Q})$$

reduces to

$$\frac{a}{3b} \in \mathbb{Z}/N\mathbb{Z} \simeq \prod_{p|N} C'_{ns}(\mathbb{F}_p),$$

which happens to be -3 times the residue class of interest.

We now use MAGMA to find such points explicitly. Let F be the elliptic curve 11a3 from Cremona's table. This

Cremona label	Szpiro ratio
1290h1	8.90370022470358
9510e1	8.84312822607337
9690m2	8.80159647164269
3990ba1	8.79237406416090
32658b1	8.78266784426543
858k2	8.75731614557112
28530v1	8.53865571757066
128310bw4	8.52531149126014
3870u1	8.51754395179071
97974g1	8.51666093397246
229449b1	8.51571265800695
29070bb2	8.50211900205277

TABLE 4. Largest Szpiro ratios in Cremona's tables.

curve has a short Weierstrass model

$$F : y^2 = x^3 - 432x + 8208,$$

which means that our corresponding curve C is given by the homogeneous equation

$$C : z^3 = u^3 - 432uv^2 + 8208v^3.$$

From Magma, we find that C is isomorphic to the elliptic curve $Y^2 = X^3 - 11$, which has rank 2 over $\mathbb{Q}$, generated by $P_1 = (3, -4)$ and $P_2 = (9/4, 5/8)$. We can check that for any pair of integers A and B, the point $-3P_1 + 11AP_1 + B(P_2 - 4P_1)$ maps to a point on C with $11 \mid z$, which in turn corresponds to an elliptic curve with minimal discriminant $11^r M^6$ with $r > 6$. As a particular example, consider the point $2P_2$, which gives rise to the point $[9225759, -125710, 8904159] \in C(\mathbb{Q})$. This point corresponds to an elliptic curve with j-invariant

$$j = -\frac{2^{12}\, 97^3\, 227^3\, 86063249^3}{11^7\, 53^6\, 1697^6}.$$

The elliptic curve

$$E : y^2 + y = x^3 - x^2 - 631675559910x - 247424709035468556$$

has the above j-invariant, and is semistable of minimal discriminant $11^7 53^6 1697^6$.

We remark that any rational point $P \in C'(\mathbb{Q})$ that satisfies the congruences in Lemma 7.2 and is in the image of $X_F(6)(\mathbb{Q}) \to C'(\mathbb{Q})$ will lead to an elliptic curve with a Szpiro ratio strictly greater than 6. In particular, the preceding argument provides a rather different proof of a result of [Masser 90], to the effect that Szpiro's conjecture, if true, is necessarily sharp. Masser goes further, proving, given $\delta > 0$, the existence of infinitely many elliptic curves $E/\mathbb{Q}$ for which

$$|\Delta(E)| \geq N(E)^6 \times \exp\left((24 - \delta)\,(\log N(E))^{1/2} (\log\log N(E))^{-1}\right). \tag{7–1}$$

From our construction, it appears to be somewhat difficult to deduce lower bounds of the flavor of (7–1).

8. TABLES: EXAMPLES OF $E/\mathbb{Q}$ WITH LARGE SZPIRO RATIO

We conclude our paper by reporting on a number of computations related to Szpiro's conjecture. We begin by listing all $E/\mathbb{Q}$ with conductor $N(E) \leq 230\,000$ and having a Szpiro ratio exceeding 8.5; these are found by simply searching through Cremona's tables. Table 4 shows the largest Szpiro ratios in Cremona's tables.

The remainder of our search for examples of elliptic curves with large Szpiro ratio primarily followed arguments from [Nitaj 98], restricting attention to curves with nontrivial rational torsion or isogeny structure. We

Curve	Model	Δ
E_2	$y^2 = x(x^2 + ax + b)$	$2^4 b^2 (a^2 - 4b)$
E_2'	$y^2 = x(x^2 - 2ax + (a^2 - 4t))$	$2^8 b(a^2 - 4b)^2$
E_3	$y^2 + by = x(x^2 + \frac{a^2}{4}x + \frac{ab}{2})$	$b^3(a^3 - 27b)$
E_3'	$y^2 + by = x^3 + \frac{a^2}{4}x^2 - \frac{9ab}{2}x - b(a^3 + 7b)$	$b(a^3 - 27b)^3$
E_5	$y^2 + (a-b)xy - a^2 by = x^3 - abx^2$	$a^5 b^5 (a^2 - 11ab - b^2)$
E_5'	$\cdots$	$ab(a^2 - 11ab - b^2)^5$
E_7	$y^2 - (a^2 - ab - b^2)xy - a^2 b^3 (a-b)y = x^3 - a^2 b(a-b)x^2$	$a^7 b^7 (a-b)^7 (a^3 - 8a^2 b + 5ab^2 + b^3)$
E_7'	$\cdots$	$ab(a-b)(a^3 - 8a^2 b + 5ab^2 + b^3)^7$
E_{22}	$y^2 = x(x-a)(x+b)$	$2^4 a^2 b^2 (a-b)^2$
E_{22}'	$y^2 = x(x^2 + 2(a+b)x + (a-b)^2)$	$2^8 ab(a-b)^4$

TABLE 5. Families of elliptic curves and their discriminants.

Curve	(a, b)	d	Szpiro Ratio
E_3'	$-2 \cdot 5 \cdot 107 \cdot 191, -2^{36} \cdot 29^2 \cdot 127$	1	9.01996406836501
E_{22}'	$-13 \cdot 19^6, 2^{30} \cdot 5$	1	8.81194357194048
E_2	$2 \cdot 1087 \cdot 3187, 3^{17} \cdot 17^3 \cdot 19$	1	8.80159647164269
E_7'	$-3^2, 2$	1	8.75731614557112
E_3'	$-2 \cdot 5 \cdot 107 \cdot 191, -2^{36} \cdot 29^2 \cdot 127$	-7	8.69894197172524
E_2'	$-2^4 \cdot 5 \cdot 17^2 \cdot 2127165978817991, 2^{77} \cdot 17^4 \cdot 101^2 \cdot 491$	1	8.66221765946058
E_{22}'	$2^{10} \cdot 5^2 \cdot 7^{15}, 3^{18} \cdot 23 \cdot 2269$	1	8.68896770822104
E_3	$-2 \cdot 5 \cdot 107 \cdot 191, -2^{36} \cdot 29^2 \cdot 127$	1	8.62243074548933
E_{22}'	$-13 \cdot 19^6, 2^{30} \cdot 5$	-3	8.61692936402403
E_3'	$-2 \cdot 5 \cdot 107 \cdot 191, -2^{36} \cdot 29^2 \cdot 127$	13	8.61065865983309
E_3'	$2 \cdot 811 \cdot 3089, -2^8 \cdot 41^8 \cdot 1069$	1	8.59658011129187
E_{22}'	$2^{10} \cdot 5^2 \cdot 7^{15}, 3^{18} \cdot 23 \cdot 2269$	-3	8.57932311185482
E_3'	$-2 \cdot 5 \cdot 107 \cdot 191, -2^{36} \cdot 29^2 \cdot 127$	-19	8.55933774170168
E_2'	$-2^4 \cdot 5 \cdot 17^2 \cdot 2127165978817991, 2^{77} \cdot 17^4 \cdot 101^2 \cdot 491$	-3	8.54579452396547
E_{22}'	$-2^7 \cdot 23^8, 19^9 \cdot 857^2$	1	8.53729295364890
E_{22}'	$3^{22} \cdot 13 \cdot 47^2, 2^7 \cdot 23^8$	1	8.53728818586093
E_{22}'	$-13 \cdot 19^6, 2^{30} \cdot 5$	5	8.53517775868216
E_{22}'	$5^{14} \cdot 19, -2^5 \cdot 3 \cdot 7^{13}$	1	8.53180512280382
E_{22}'	$2^{10} \cdot 5^2 \cdot 7^{15}, 3^{18} \cdot 23 \cdot 2269$	-5	8.53133002997689
E_3'	$2 \cdot 811 \cdot 3089, -2^8 \cdot 41^8 \cdot 1069$	29	8.50447784478959
E_2	$2 \cdot 1087 \cdot 3187, 3^{17} \cdot 17^3 \cdot 19$	-3	8.50211900205277
E_{22}'	$-2^4 \cdot 5^{16} \cdot 97 \cdot 919, 7^3 \cdot 29^5 \cdot 151^2$	1	8.50127729380151
E_{22}'	$2^{10} \cdot 5^2 \cdot 7^{15}, 3^{18} \cdot 23 \cdot 2269$	-7	8.50068162668746
E_3'	$19 \cdot 4211, 13^5 \cdot 17239$	1	8.49294029016210
E_5'	$-2^7 \cdot 3727, 3^{10} \cdot 7$	1	8.48609917814708

TABLE 6. Top Szpiro ratios found via computer search.

tabulate the results of our computations as follows. First, in Table 5, we list models of $E/\mathbb{Q}$ with given rational torsion and isogeny structures. To do this, we denote by E_N the universal elliptic curve over $X_1(N)$, and by E_N' the elliptic curve $E_N/\langle P\rangle$, where P is the point of order N. We also write E_{22} for a parameterization of elliptic curves with full rational two-torsion, and $E_{22}' = E_{22}/\langle P\rangle$ for one of these points. The formulas for E_N', when $N = 5$ or 7, can be found in [Nitaj 98], where they are denoted by E_{18} and E_{39}, respectively.

Our final table, Table 6, lists the results of our search within the families given in Table 5; in this table, the quantity d indicates that the curve under consideration is the d-quadratic twist of one of our models from Table 5. We have restricted attention to those examples with Szpiro ratio larger than 8.486 (which is the cutoff we needed to include elliptic curves with a rational 5-torsion point). More extensive data are available from the authors upon request.

REFERENCES

[Baker 73] A. Baker. "A Sharpening of the Bounds for Linear Forms in Logarithms. II." *Acta Arith.* 24 (1973), 33–36.

[Darmon and Granville 95] H. Darmon and A. Granville. "On the Equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$." *Bull. London Math. Soc.* 27 (1995), 513–543.

[Masser 90] D. W. Masser. "Note on a Conjecture of Szpiro." In *Les pinceaux de courbes elliptiques*, Semin., Paris/Fr. 1988, Asterisque 183, pp. 19–23. Paris: Société Mathématique de France, 1990.

[Nitaj 98] A. Nitaj. "Détermination de courbes elliptiques pour la conjecture de Szpiro." *Acta Arith.* 85 (1998), 351–376.

[Van der Poorten 77] A. J. Van der Poorten. "Linear Forms in Logarithms in the p-adic Case." In *Transcendence Theory: Advances and Applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)*, pp. 29–57. London: Academic Press, 1977.

[Ribet 91] K. A. Ribet. "On Modular Representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ Arising from Modular Forms." *Invent. Math.* 100 (1990), 431–476.

[Rubin and Silverberg 95] K. A. Rubin and A. Silverberg. "Families of Elliptic Curves with Constant mod p Representations." In *Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Hong Kong, 1993)*, Ser. Number

Theory, I, pp. 148–161. Cambridge, MA: Int. Press, 1995.

[Rubin and Silverberg 99] K. A. Rubin and A. Silverberg. "Mod 6 Representations of Elliptic Curves." In *Automorphic Forms, Automorphic Representations, and Arithmetic (Fort Worth, TX, 1996)*, Proc. Sympos. Pure Math. 66, pp. 213–220. Providence: Amer. Math. Soc., 1999.

[Rubin and Silverberg 01] K. A. Rubin and A. Silverberg. "Mod 2 Representations of Elliptic Curves." *Proc. Amer. Math. Soc.* 129 (2001), 53–57.

[Shorey and Stewart 83] T. N. Shorey and C. L. Stewart. "On the Diophantine Equation $ax^{2t} + bx^t y + cy^2 = d$ and Pure Powers in Recurrence Sequences." *Math. Scand.* 52 (1983), 24–36.

[Shorey and Tijdeman 86] T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics 87. Cambridge, UK: Cambridge University Press, 1986.

[Silverman 92] J. H. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, corrected reprint of the 1986 original. New York: Springer, 1992.

[Taylor and Wiles 95] R. Taylor and A. Wiles. "Ring-Theoretic Properties of Certain Hecke Algebras." *Ann. of Math.* 141 (1995) 553–572.

[Wiles 95] A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem." *Ann. of Math* 141 (1995), 443–551.

Michael A. Bennett, Department of Mathematics, University of British Columbia, Vancouver, BC, Canada V6T 1Z2 (bennett@matn.ubc.ca)

Soroosh Yazdani, Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, Canada T1K 3M4 (soroosh.yazdani@uleth.ca)

Received January 6, 2011; accepted November 3, 2011