Compositio Mathematica **127**: 23–54, 2001.

On the Density of Elliptic Curves

SIMAN WONG
Department of Mathematics, Brown University. Providence, RI 02912, U.S.A.[⋆]

(Received: 24 June 1999; accepted: 10 March 2000)

Abstract. We show that 17.9% of all elliptic curves over **Q**, ordered by their exponential height, are semistable, and that there is a positive density subset of elliptic curves for which the root numbers are uniformly distributed. Moreover, for any $\alpha > 1/6$ (resp. $\alpha > 1/12$) the set of Frey curves (resp. all elliptic curves) for which the generalized Szpiro Conjecture $|\Delta(E)| \ll_\alpha N_E^{12\alpha}$ is false has density zero. This implies that the ABC Conjecture holds for almost all Frey triples. These results remain true if we use the logarithmic or the Faltings height. The proofs make use of the fibering argument in the square-free sieve of Gouvêa and Mazur. We also obtain conditional as well as unconditional lower bounds for the number of curves with Mordell–Weil rank 0 and $\geqslant 2$, respectively.

Mathematics Subject Classifications (2000). 11G05, 11N36.

Key words. elliptic curves, height, quadratic twists, ranks, root numbers, square-free sieve

1. Introduction

Denote by $\Delta(E)$ and N_E the minimal discriminant and the conductor of an elliptic curve $E/\mathbf{Q}$. The Szpiro Conjecture [20] asserts that for every $\varepsilon > 0$ there exists a constant $C_1(\varepsilon) > 0$ such that

$$|\Delta(E)| < C_1(\varepsilon) N_E^{6+\varepsilon}. \tag{1}$$

This statement is optimal, in that for any constant $C_1(0) > 0$ there exists infinitely many curves $E/\mathbf{Q}$ for which (1) is false with $\varepsilon = 0$ [14]. The Szpiro Conjecture is closely related to the ABC Conjecture, which asserts that for any $\varepsilon > 0$ there exists a constant $C_2(\varepsilon) > 0$ such that, for any pairwise coprime integers A, B, C with $A + B + C = 0$,

$$\max(|A|, |B|, |C|) < C_2(\varepsilon) \prod_{p|ABC} p^{1+\varepsilon}. \tag{2}$$

These two conjectures are related through a special family of elliptic curves. An

[⋆]Current address: Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003-4515, U.S.A. e-mail: siman@math.umass.edu

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

integer triple (A, B, C) is called a *Frey triple* if

$$\begin{aligned}&(A, B) = 1, A + B + C = 0, \qquad C > 0,\\ &\text{and } A \equiv 0 \pmod{16}, B \equiv -1 \pmod 4.\end{aligned} \tag{3}$$

Given a such a triple, Frey [6] showed that the curve $E_{A,B,C}\colon y^2 = x(x + A)(x - B)$ is semistable. Such curves are called *Frey curves.* It is known that the ABC Conjecture is true if and only if (1) is true for all Frey curves (which in turn is true if and only if (1) is true for all elliptic curves; resp. all semistable curves [15]). In particular, the Szpiro Conjecture is true if and only if the ABC Conjecture is true (where in the 'only if' direction, the exponent $1 + \varepsilon$ in (2) is to be replaced by $6/5 + \varepsilon$; cf. [15, §3]). In this paper we show that the Szpiro Conjecture is true for the set of all elliptic curves over $\mathbf{Q}$ (resp. Frey curves) except for a set of density zero, by deriving asymptotic formulae for various collections of elliptic curves of bounded height. It follows that the ABC Conjecture holds for almost all Frey triples (with the weaker exponent $6/5 + \varepsilon$). We also apply these asymptotic results to study questions about equidistribution of root numbers, and to derive lower bounds for the number of elliptic curves of rank 0 and $\geqslant 2$, respectively.

Denote by $c_4(E), c_6(E)$ and $j(E)$ the usual quantities associated to a minimal Weierstrass equation of $E/\mathbf{Q}$. Then the *exponential height* and the *logarithmic height* of $E/\mathbf{Q}$ are defined to be

$$h_e(E) = \max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6}) \quad \text{and} \quad h_l(E) = \log h_e(E),$$

respectively. Choose τ in the upper half complex plane such that $E(\mathbf{C}) \simeq \mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$. Denote by $\delta_{12}(\tau)$ the usual normalized weight 12 cusp form. Then the *Faltings height* of $E/\mathbf{Q}$ is defined to be

$$h_F(E) = \frac{1}{12}(\log|\Delta(E)| - \log|\delta_{12}(\tau)\mathrm{im}(\tau)^6|).$$

We have the following crucial relation ([19, p. 259]; cf. the remark at the end of Section 10):

$$h_F(E) + \mathrm{O}(1) \leqslant h_l(E) \leqslant h_F(E) + \mathrm{O}(\log h_l(E)). \tag{4}$$

Given a real number $x > 0$, define

$$\begin{aligned}S(x) &= \{E/\mathbf{Q}\colon h_e(E) \leqslant x\},\\ S_s(x) &= \{E \in S(x)\colon \text{E is semistable}\},\\ S'(x) &= \{E \in S_s(x)\colon \text{E has good reduction at 2 and 3}\}.\end{aligned}$$

Let δ_E be the product of the odd prime divisors of $\Delta(E)$. For any integer D, denote by

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

E_D the twist of E by $\mathbf{Q}(\sqrt{D})$. For $t = \pm 1$, define

$$S_t(x) = \left\{ E \in S(x)\colon \begin{array}{c} E \text{ is semistable at all } p > 2, \text{ both } E \\ \text{and } E_{-1} \text{ are additive at } 2,\ j(E) \text{ is} \\ \text{a 2-adic unit, and } \delta_E \equiv t \pmod 4 \end{array} \right\}.$$

Clearly $\#S'(x) \leqslant \#S_s(x) \leqslant \#S(x)$, and $\#S(x) \leqslant 4x^{10}$. While not every pair of integers (c_4, c_6) with $|c_4| < x^4$, $|c_6| < x^6$ gives rise to a minimal Weierstrass equation over $\mathbf{Q}$, one would expect that a positive portion of them do, and hence one would expect that $\#S(x) \gg\ll x^{10}$. It is not so clear what to expect for the size of $S_s(x)$. Our first result states that there are indeed asymptotic formula for the size of all four sets above.

THEOREM 1. *With respect to the exponential height,* 17.9% *of all elliptic curves over* $\mathbf{Q}$ *are semistable. More precisely,*

$$\begin{aligned} \#S(x) &= \frac{5\cdot 7\cdot 11^4\cdot 13^2\cdot 31\cdot 61\cdot 233\cdot 727}{2^{21}3^{17}\pi^{10}}x^{10} + \mathrm{O}\left(\frac{x^{10}}{\log x}\right) \sim \\ &\sim 1.094\times 10^{-3}x^{10}, \\ \#S_s(x) &= \frac{5}{2^5 3^4\pi^2}x^{10} + \mathrm{O}\left(\frac{x^{10}}{\log x}\right) \sim 1.954\times 10^{-4}x^{10}, \\ \#S'(x) &= \frac{5\cdot 7}{2^5 3^6\pi^2}x^{10} + \mathrm{O}\left(\frac{x^{10}}{\log x}\right) \sim 1.520\times 10^{-4}x^{10}, \\ \#S_t(x) &= \frac{5}{2^{20}3^5\pi^2}x^{10} + \mathrm{O}\left(\frac{x^{10}}{\log x}\right) \sim 1.988\times 10^{-9}x^{10}, \quad \textit{for } t = \pm 1. \end{aligned}$$

For any positive real numbers α, C and any semistable curve $E/\mathbf{Q}$, consider the following statement:

$$SZ(\alpha, C)\colon \quad h_F(E) \leqslant \alpha \log N_E + C \log\log N_E.$$

For any $\alpha > 1/2$ (and replacing $\log\log N_E$ by 1) this is equivalent to the Szpiro Conjecture [20].

The first part of the following theorem is essentially [7, Thm. 2] (cf. Section 7).

THEOREM 2. (a) *For any real number* $\alpha > 1/12$ *there exists a constant* $C_\alpha > 0$ *depending only on* α, *such that*

$$\#\{E \in S_s(x)\colon SZ(\alpha, C_\alpha) \textit{ is false for } E\} = o_\alpha(x^{10}).$$

(b) *If* $\alpha < 1/12$, *then for any constant* C, *the set of semistable curves for which* $SZ(\alpha, C)$ *is false has positive density.*

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

Define

$$F(x) = \{E \in S_s(x) \colon E \text{ is a Frey curve}\}.$$

While the Szpiro Conjecture is true for all elliptic curves over $\mathbf{Q}$ (resp. all semistable curves) if and only if it is true for all Frey curves,the method in [7] does not seem to yield for Frey curves an analog of Theorem 2(a). By sieving lattice points in homogeneous expanding domains we obtain the following result.

THEOREM 3. (a) *There exists a constant $\delta > 0$ such that*

$$\#F(x) = \delta x^4 + \mathrm{O}(x^4 \log^{-1/2} x).$$

Numerically, $\delta = 0.01148$.

(b) *There exists an absolute constant $c > 0$, such that for any number $\alpha > 1/6$ there exists a constant C_α depending on α only, such that*

$$\#\left\{E \in F(x) : \begin{array}{c} SZ(\alpha, C_\alpha) \textit{ is} \\ \textit{false for } E \end{array} \right\} = \mathrm{O}\left(\frac{x^4}{\log^{\frac{1}{12}} x} + \frac{x^4}{2^{c(1-\frac{1}{6\alpha})\log^{1/2} x}}\right).$$

(c) *If $\alpha < 1/6$, then for any constant C, the set of Frey curves for which $SZ(\alpha, C)$ is false has positive density.*

Utilizing Theorem 3 we can deduce that the ABC Conjecture with a weaker exponent holds for almost all Frey triples. More precisely, for any positive numbers $\alpha, \gamma > 0$ and any coprime integers A, B, C with $A + B + C = 0$, consider the following statement

$$ABC(\lambda, \gamma)\colon \quad \max(|A|, |B|, |C|) < \gamma \prod_{p|ABC} p^{\lambda}.$$

For any $\alpha > 1$ this gives the ABC Conjecture.

COROLLARY 1. *For any $\lambda > 6/5$ there exists a constant $C_\lambda > 0$ depending on λ only, such that the number of Frey triples (A, B, C) for which $ABC(\lambda, C_\lambda)$ fails and with* $\max(|A|, |B|, |C|) < x$, *is $\ll_\lambda x^2/\log^{1/12} x$.*

We now study the question of equidistribution of root numbers. Following Rohrlich [16], we denote by $W(E)$ the global root number of $E/\mathbf{Q}$. It takes the value ±1, and it is equal to the sign of the functional equation of the L-function of the (modular) elliptic curve $E/\mathbf{Q}$.

Let $S_{+1} = \bigcup_{x>0} S_{+1}(x)$. For any elliptic curve $E/\mathbf{Q}$, denote by E_{-1} the quadratic twist of E by $\mathbf{Q}(\sqrt{-1})$.

THEOREM 4. (a) *Suppose* $E \in S_+$. *Then* $E_{-1} \in S_+$ *as well. Both* E *and* E_+ *have the same exponential height, and* $W(E) + W(E_{-1}) = 0$. *Consequently,*

$$\sum_{\substack{E \in S_+ \\ h_e(E)=x}} W(E) = 0.$$

(b) *Denote by* $\omega(E)$ *the number of distinct prime divisors of* $\Delta(E)$. *Then*

$$\sum_{E \in S'(x)} (-1)^{\omega(E)} W(E) = \mathrm{O}(x^{10} \log^{-1/2} x).$$

COROLLARY 2. *Let* $\varepsilon = \pm 1$; *then*

$$\#\{E \in S_{+1}(x)\colon W(E) = \varepsilon\} = \frac{\#S_{+1}(x)}{2},$$

$$\#\{E \in S'(x)\colon (-1)^{\omega(E)} W(E) = \varepsilon\} = \frac{\#S'(x)}{2} + \mathrm{O}(x^{10} \log^{-1/2} x).$$

In particular, a positive portion of all elliptic curves over $\mathbf{Q}$ *have root number* $+1$ (*resp.* -1).

Assuming the generalized Riemann hypothesis for the L-function of elliptic curves plus the modularity conjecture, Brumer [1] showed that the average analytic rank of elliptic curves over $\mathbf{Q}$, ordered by their Faltings height, is $\leqslant 2.3$; Brumer informed us that Heath-Brown has improved this to $\leqslant 2.0$ (unpublished). However, from these conditional results we still cannot deduce that a positive portion of the curves have rank zero. By working with quadratic twists we have the following partial results. Denote by $\mathrm{rank}_{MW}(E)$ and $\mathrm{rank}_{an}(E)$ the Mordell–Weil rank and analytic rank of $E/\mathbf{Q}$, respectively. Recall that by the work of Kolyvagin *et al.*, these two quantities coincide if E is modular and $\mathrm{rank}_{an}(E) \leqslant 1$.

THEOREM 5. *We have the unconditional estimate*

$$\#\{E/\mathbf{Q}\colon h_e(E) \leqslant X, \mathrm{rank}_{an}(E/\mathbf{Q}) = 0\} \gg \#S(X)^{1/3}.$$

Assume the Riemann hypothesis for the zeta functions of the Rankin–Selberg convolutions of the weight 3/2-*modular forms associated to semi-stable elliptic curves by the Shintani–Shimura lift. Then we have the lower bound*

$$\#\{E/\mathbf{Q}\colon h_e(E) \leqslant X, \mathrm{rank}_{an}(E/\mathbf{Q}) = 0\} \gg_\varepsilon \#S(X)^{1-\varepsilon}.$$

In view of their computations with curves of prime conductors, Brumer and McGuiness [2] asked if for every nonnegative integer n there exists a positive portion of elliptic curves with rank n. Little seems to have been proved in this direction; for the record we state the following result.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

THEOREM 6. *We have the unconditional estimate*

$$\#\{E/\mathbf{Q}: h_e(E) \leqslant X, \operatorname{rank}_{MW}(E/\mathbf{Q}) \geqslant 2\} \gg \#S(X)^{1/2},$$

In view of the crucial relation (4), we get

COROLLARY 3. *The six Theorems above plus Corollary* 2 *remain true if we use the logarithmic or Faltings height instead of the exponential height, and if were place* x^{10} *and* $\log x$ *by* e^{10x} *and* x*, respectively.*

We now give an outline of the paper. In Section 2, we give for any prime p (including 2 and 3) sufficient and necessarily conditions for a given $\mathbf{Z}$-Weierstrass equation W to be minimal at p. These conditions involve congruence of $c_4(W)$ and $c_6(W)$ modulo $p^{n(p)}$ with $n(p) < 12$. This allows us to count elliptic curves by counting pairs of integers satisfying conditions conducive to sieving arguments; cf. for instance the proof of Theorem 1 in Sections 3 and 4. In Sections 5 and 6, we apply the fibering argument of Gouvêa and Mazur [9] to bound the number of pairs of integers c_4, c_6 such that $c_4^3 - c_6^2$ have large prime divisors; cf. Proposition 5. This estimate yields the zero-density statements in Theorems 2 and 3; the positive density statements follow from the square-free sieve of nonhomogeneous (resp. homogeneous) cubics. In Section 9, we combine Proposition 5 with Rohrlich's root number calculation [16] and character sums estimates to derive the equidistribution statements in Theorem 4. Finally, in Section 11 we prove Theorem 5 by applying nonvanishing theorems of quadratic twists of L-functions associated to elliptic curves with *square-free* discriminants; and we prove Theorem 6 by constructing a family of elliptic curves with two independent $\mathbf{Q}$-rational nontorsion points, by lifting to $\mathbf{Z}$ elliptic curves over $\mathbf{F}_3$ whose groups of $\mathbf{F}_3$-rational points are not cyclic.

There are two equidistribution statements in Theorem 4. The first one is arithmetic in nature. The second statement is more analytic, involving the square-free sieve and character sums estimates. Now, one might object to averaging over $(-1)^{\omega(E)} W(E)$ as being unnatural, and in any case we expect that the stronger equidistribution statements

$$\sum_{E \in S'(x)} (-1)^{\omega(E)} \overset{?}{=} \mathrm{o}(x^{10}) \quad \text{and} \quad \sum_{E \in S'(x)} W(E) \overset{?}{=} \mathrm{o}(x^{10}) \tag{5}$$

to be true. The analytic argument in Section 10 can be adapted to show that the second part of (5) follows from the first part. But this first part seems to be a very deep problem in analytic number theory: consider the related problem of establishing (5) for curves with square-free discriminants; our argument for Theorem 4 also carries over to this case. The analog of the first part of (5) then becomes (for c_4

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

and c_6 lying in certain congruence classes modulo powers of 2 and 3)

$$\sum_{\substack{|c_4|<x^4\\|c_6|<x^6}} \mu\left(\frac{c_4^3-c_6^2}{1728}\right)?{=}\mathrm{o}(x^{10}), \tag{19}$$

where μ is the Möbius function. On the other hand, even the much simpler assertion

$$\sum_{n\leqslant x} \mu(n) = \mathrm{o}(x)$$

is equivalent to the prime number theorem; more precisely, the nonvanishing of the Riemann zeta function on the line $\mathrm{Re}(s) = 1$ [5, §3.1.4]. It would be interesting to relate (6) to questions about nonvanishing of L-functions.

2. Minimal Weierstrass Equation

In this section we determine those pairs of integers c_4, c_6 which arise from the minimal Weierstrass equations of elliptic curves over $\mathbf{Q}$. Denote by $c_4(W), c_6(W)$ and $\Delta(W)$ the quantities corresponding to a Weierstrass equation W over $\mathbf{Z}$. We will make repeated use of the basic relation

$$c_4(W)^3 - c_6(W)^2 = 1728\Delta(W). \tag{7}$$

Our starting point is the following result of Kraus [13] (independently discovered by Mestre).

PROPOSITION 1. *Let c_4, c_6 and Δ be integers such that $c_4^3 - c_6^2 = 1728\Delta \neq 0$. Then there exists a Weierstrass equation W over $\mathbf{Z}$ with $c_4(W) = c_4$ and $c_6(W) = c_6$ if and only if the following conditions hold:*

- *$v_3(c_6) \neq 2$, and*
- *either $c_6 \equiv -1 \pmod 4$, or both $v_2(c_4) \geqslant 4$ and $c_6 \equiv 0$ or $8 \pmod{32}$.* □

In view of this result, our task is to give conditions on c_4 and c_6 such that

(1) $c_4^3 - c_6^2 \equiv 0 \pmod{1728}$;
(2) c_4 and c_6 satisfy the hypothesis of Proposition 1, and hence correspond to some Weierstrass equation;
(3) this equation is minimal over $\mathbf{Z}$.

The first requirement is achieved by imposing congruence conditions; for future references we will also determine the corresponding reduction type. We will make repeated use of the following standard fact.

LEMMA 1. *If an elliptic curve $E/\mathbf{Q}$ has bad reduction at p (including 2 and 3), then the reduction type is multiplicative if and only if $p \nmid c_4(E)$.*

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

Proof. Cf. [17, p. 180]. □

PROPOSITION 2. *For two integers* c_4, c_6, *we have* $c_4^3 - c_6^2 \equiv 0 \pmod{1728}$ *precisely when, for each of* $p = 2$ *and* 3, *one of the following conditions hold:*

$p = 3$:

(a) $v_3(c_4) \geqslant 2$ *and* $v_3(c_6) \geqslant 3$ (*additive or not minimal at* 3); *or*

(b) $v_3(c_4) = 1$ *and* $v_3(c_6) \geqslant 3$ (*good*);

(c) $c_4 = 1 + 3\alpha$, $c_6 = 1 + 9\beta$, *with* $\alpha \equiv \beta \pmod 3$. *The reduction type is either good or multiplicative, with the former type precisely when*

$$\begin{array}{ll} \alpha \not\equiv 2\beta \pmod 9 & \textit{if } \alpha \not\equiv 2 \pmod 3; \ \textit{or} \\ \alpha - 2\beta + 6 \not\equiv 0 \pmod 9 & \textit{if } \alpha \equiv 2 \pmod 3. \end{array}$$

$p = 2$:

(d) $v_2(c_4) \geqslant 4$ *and* $v_2(c_6) = 3$ (*good*); *or*

(e) $v_2(c_4) \geqslant 4$ *and* $v_2(c_6) \geqslant 5$ (*additive or not minimal at* 2); *or*

(f) $c_4 = 1 + 16\alpha$, $c_6 = -1 + 8\beta$, *with* $\alpha \equiv \beta \pmod 4$. *The reduction type is either good or multiplicative, with the former type precisely when* $\alpha \not\equiv \beta \pmod 8$; *or*

(g) $c_4 = 1 + 8\alpha$, $c_6 = -1 + 4\beta$, *with the following choices for* $\alpha, \beta 1 \pmod{16}$:

$$\begin{array}{ll} \textit{good reduction}: & (1, 15), (9, 7), (3, 9), (11, 1), (5, 11), (13, 3), \\ & (7, 13), (15, 5); \\ \textit{multiplicative}: & (1, 7), (9, 15), (3, 1), (11, 9), (5, 3), (13, 11), \\ & (7, 5), (15, 13). \end{array}$$

Proof. We give the argument for $p = 2$; the case $p = 3$ is similar and simpler.

If c_4 is even, then cases (d) and (e) follows immediately from Proposition 1. Now, suppose c_4 is odd, and hence so is c_6 by (7). Then $c_6^2 \equiv 1 \pmod 8$, whence $c_4 \equiv 1 \pmod 8$ by (7). Write $c_4 = 1 + 8\alpha$, $c_6 = -1 + 4\beta$. Then (7) becomes

$$3\alpha \equiv -\beta + 2\beta^2 \pmod 8. \tag{8}$$

If α is even, then so is β, and (21) becomes $3(\alpha/2) \equiv -(\beta/2) \pmod 4$. Moreover, we have bad reduction (necessarily multiplicative, by Lemma 1) precisely when (8) holds modulo 16. These give case (f) of the Proposition.

Now, suppose α is odd. From (8) we see that the choices for $\alpha, \beta \pmod 8$ are $(1, 7), (3, 1), (5, 3), (7, 5)$. Moreover, we have bad (multiplicative) reduction if and only if $3\alpha + 3 \cdot 2^3\alpha^2 \equiv -\beta + 2\beta^2 \pmod{16}$.

These give case (g) of the Proposition. □

Any pair c_4, c_6 in Proposition 2 already satisfies Proposition 1, and, hence, comes from some Weierstrass equation over **Z**. It remains to decide if this equation is minimal over **Z**.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

PROPOSITION 3. *Let c_4, c_6 be as in Proposition 2. Then the corresponding Weierstrass equation is minimal over* **Z** *if and only if the following conditions are satisfied for every prime* p:

$p > 3$:

(a) $v_p(c_4) < 4$ *or* $v_p(c_6) < 6$;

$p = 3$:

(b) c_4, c_6 *are prime to* 3 *and are as given by Proposition* 2(c); *or*

(c) $v_p(c_4) = 1$ *and* $v_p(c_6) \geqslant 3$ (*good*); *or*

(d) $v_p(c_4) = 2, 3$ *and* $v_p(c_6) \geqslant 3$ (*additive*); *or*

(e) $v_p(c_4) = 4$ *and*

- $v_p(c_6) = 3, 4, 5, 7, 8$*; or*
- $v_p(c_6) = 6$ *and* $(c_4/3^4, c_6/3^6)$ *does not satisfy Proposition* 2(c)*;*

Such pairs give rise to additive reduction.

(f) $v_p(c_4) > 4$ *and* $v_p(c_6) = 3, 4, 5, 6, 7, 8$ (*additive*).

$p = 2$:

(g) c_4, c_6 *are prime to* 2 *and are as given by Proposition* 2(f,g);

(h) $v_p(c_4) \geqslant 4$ *and* $v_p(c_6) = 3$ (*good*); *or*

(i) $v_p(c_4) \geqslant 4$ *and* $v_p(c_6) = 5$ (*additive*); *or*

(j) $v_p(c_4) = 4$, $v_p(c_6) = 6$, *and* $(c_4/2^4, c_6/2^6)$ *does not satisfy Proposition* 2(f,g).
Such pairs give rise to additive reduction.

(k) $4 < v_p(c_4) < 8$ *and* $v_p(c_6) \geqslant 6$ (*additive*); *or*

(l) $v_p(c_4) \geqslant 8$ *and* $v_p(c_6) = 6, 7, 8, 10$ (*additive*).

Proof. Given a Weierstrass equation W, any **Z**-change of variables scales $c_4(W)$ and $c_6(W)$ by a factor of r^{-4} and r^{-6} respectively for some integer $r \neq 0$. The conditions for $p > 3$ then follow from Proposition 1. Moreover,we can assume that for $p = 2$ and 3, either $v_p(c_4) < 8$ or $v_p(c_6) < 12$. The rest now follows from Proposition 2. □

LEMMA 2. *Suppose $E/\mathbf{Q}_p$ has bad reduction over $\mathbf{Q}_p$. Then for any nonzero $D \in \mathbf{Z}_p$, E has good reduction over $\mathbf{Q}_p(\sqrt{D})$ if and only if E_D (the quadratic twist of E by D) has good reduction over $\mathbf{Q}_p$.*

Proof. Since good reduction is preserved by field extensions, the 'if' part of the Lemma is clear. So suppose E has good reduction over $K = \mathbf{Q}_p(\sqrt{D})$. Unramified extensions do not affect reduction types and $E/\mathbf{Q}_p$ has bad reduction, so $K/\mathbf{Q}_p$ is ramified. By the Néron–Ogg–Shafarevich criterion [17, Thm. 7.1], we need to show that the l-adic representation $\rho_{E_D,l}$ of $G = G_{\mathbf{Q}_p}$ associated to E_D is unramified for some prime $l \neq p$.

By Hensel's lemma we can assume that D is an integer; replacing D by $D - p^n$ with n sufficiently large, we can further assume that D is a negative integer. Thus the nontrivial coset of G_K in G is generated by the image in G of the complex conjugation

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

τ. In particular, τhas order 2 in G, and hence $t = \rho_{E,l}(\tau)$ is either $\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Since τ generates the Galois group of the ramified extension $K/\mathbf{Q}_p$ and since E has good reduction over K, the image under $\rho_{E,l}$ of the inertia subgroup of G is generated by t. Thus if t is not scalar, then det$\rho_{E,l}$ is ramified, contradicting the fact that the l-adic cyclotomic character over $\mathbf{Q}_p$ is unramified if $p \neq l$. If $t = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then $\rho_{E,l}$ is unramified, and hence E has good reduction over $\mathbf{Q}_p$, a contradiction. Finally, if $t = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then, denoting by χ_D the quadratic character of G associated to $K/\mathbf{Q}_p$, we get$\rho_{E_D,l}(\tau) = (\rho_{E,l} \otimes \chi_D)(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so E_D has good reduction over $\mathbf{Q}_p$, as desired. □

PROPOSITION 4. *Suppose $E/\mathbf{Q}_2$ has additive reduction at* 2, *and that its j-invariant is a* 2-*adic unit. Then E acquires good reduction over a quadratic extension $L/\mathbf{Q}_2$, and the local root number of $E/\mathbf{Q}_2$ depends on L only. This extension L is determined by the following congruence conditions:*

$L = \mathbf{Q}_2(\sqrt{-1})$ *or* $\mathbf{Q}_2(\sqrt{3})$:

$c_4 = 2^4\gamma_4$, $c_6 = 2^6\gamma_6$ *with* $\gamma_4 \pmod{2^7}$, $\gamma_6 \pmod{2^6}$ *given by*
$(1, 33), (9, 5), (17, 25), (25, 29), (33, 17), (41, 53), (49, 9), (57, 13), (65, 1),$
$(73, 37), (81, 57), (89, 61), (97, 49), (105, 21), (113, 41), (121, 45).$

In this case the local root number is -1.

$L = \mathbf{Q}_2(\sqrt{2})$ *or* $\mathbf{Q}_2(\sqrt{10})$:

$c_4 = 2^6\gamma_4$, $c_6 = 2^9\gamma_6$ *with* $\gamma_4 \pmod{2^7}$, $\gamma_6 \pmod{2^6}$ *given by*
$(1, 31), (9, 59), (17, 39), (25, 35), (33, 47), (41, 11), (49, 55), (57, 51), (65, 63),$
$(73, 27), (81, 7), (89, 3), (97, 15), (105, 43), (113, 23), (121, 19).$

In this case the local root number is $+1$.

$L = \mathbf{Q}_2(\sqrt{-2})$ *or* $\mathbf{Q}_2(\sqrt{-10})$:

$c_4 = 2^6\gamma_4$, $c_6 = 2^9\gamma_6$ *with* $\gamma_4 \pmod{2^7}$, $\gamma_6 \pmod{2^6}$ *given by*
$(1, 33), (9, 5), (17, 25), (25, 29), (33, 17), (41, 53), (49, 9), (57, 13), (65, 1),$
$(73, 37), (81, 57), (89, 61), (97, 49), (105, 21), (113, 41), (121, 45).$

In this case the local root number is -1.

Proof. Since $j(E)$ is a 2-adic unit, $E/\mathbf{Q}_2$ has potentially good reduction, and the automorphism group of the reduced curve (over $\overline{\mathbf{F}}_2$) has order 2 [17, p. 325]. From ([16], bottom of p. 127) and the reference therein we see that $E/\mathbf{Q}_2$ acquires good reduction over an extension of $\mathbf{Q}_2$ of degree $\leqslant 2$. Suppose further that $E/\mathbf{Q}_2$ is additive. The hypothesis that $j(E)$ is a 2-adic unit means that $3v_2(c_4(E)) = v_2(\Delta(E))$, while by [17, Exer. 7.2] we have $v_2(\Delta(E)) < 24$. Combine Proposition 3 with the relation (7), we see that

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

(i) $2^6 || (\gamma_4^3 - \gamma_6^2)$, where $\gamma_4 = c^4$ and γ_6 denote the odd part of c_4 and c_6, respectively; and

(ii) in either $v_2(c_4(E)) = 4$ and $v_2(c_6(E)) = 6$, or $v_2(c_4(E)) = 6$ and $v_2(c_6(E)) = 9$.

Set

$$n = \frac{v_2(c_4(E)) - 4}{2}.$$

Then a routine application of Tate's algorithm shows that

$$y^2 = x^3 - 27\gamma_4 2^{2n} x - 54\gamma_6 2^{3n}$$

is a minimal Weierstrass equation of $E/\mathbf{Q}_2$. Condition (i) is satisfied by specifying $\gamma_4 \pmod{2^7}$ and $\gamma_6 \pmod{2^6}$. Note that if $\gamma_4' \equiv \gamma_4 \pmod{2^7}$ and $\gamma_6' \equiv \gamma_6 \pmod{2^6}$, then by Tate's algorithm the reduction type over $\mathbf{Q}_2$ of the two corresponding curves are identical; moreover, the same holds if we twist the two curves by the same quadratic field. Thus to determine the quadratic extension $L/\mathbf{Q}_2$ over which E has good reduction, it suffices to pick any pair $\gamma_4 \pmod{2^7}$ and $\gamma_6 \pmod{2^6}$ and then check each of the six ramified quadratic extensions of $\mathbf{Q}_2$ using Lemma 2. Finally, the root number computation follows immediately from [16, Prop. 2(iii)]. This completes the proof of the Proposition. □

3. Counting Elliptic Curves: Conditions at $p > 3$

Let a_1, a_2, M_1 and M_2 be integers. Define three sets

$$T_0(x, y, a_1, a_2, M_1, M_2) = \left\{ (\alpha, \beta)\colon \begin{array}{c} |\alpha| \leqslant x, \alpha \equiv a_1 \pmod{M_1}, \\ |\beta| \leqslant y, \beta \equiv a_2 \pmod{M_2} \end{array} \right\},$$

$$T(x, y, a_1, a_2, M_1, M_2) = \left\{ \begin{array}{c} (\alpha, \beta) \in T_0(x, y, a_1, a_2, M_1, M_2)\colon \text{for all} \\ p > 3,\ \text{either } v_p(\alpha) < 4 \text{ or } v_p(\beta) < 6 \end{array} \right\},$$

$$T'(x, y, a_1, a_2, M_1, M_2) = \left\{ \begin{array}{c} (\alpha, \beta) \in T_0(x, y, a_1, a_2, M_1, M_2)\colon \\ p \nmid \gcd(\alpha, \beta) \text{ for any } p > 3 \end{array} \right\}.$$

LEMMA 3. *For $y \geqslant x > e^{M_1 M_2}$, we have the estimates*

$$\#T(x, y, a_1, a_2, M_1, M_2) = \frac{xy}{M_1 M_2 \zeta(10)} \prod_{p | 6M_1M_2} \frac{1}{1 - p^{-10}} + \mathrm{O}\left(\frac{xy}{\log x}\right),$$

$$\#T'(x, y, a_1, a_2, M_1, M_2) = \frac{xy}{M_1 M_2 \zeta(2)} \prod_{p | 6M_1M_2} \frac{1}{1 - p^{-2}} + \mathrm{O}\left(\frac{xy}{\log x}\right).$$

Proof. To simplify the notations, write T_0 for $T_0(x, y, a_1, a_2, M_1, M_2)$, etc. Define

$$T_1 = \{(\alpha, \beta) \in T_0 \colon p^4 | \alpha \Rightarrow p^6 \nmid \alpha \text{ for all } p \text{ with } 3 < p < \log x\},$$
$$T_2 = \{(\alpha, \beta) \in T_0 \colon v_p(\alpha) \geqslant 4 \text{ and } v_p(\beta) \geqslant 6 \text{ for some } p \geqslant \log x\}.$$

Then

$$\#T_1 - \#T_2 \leqslant \#T \leqslant \#T_1. \tag{9}$$

To estimate $\#T$ it then suffices to estimate $\#T_1$ and $\#T_2$.

Let n runs through all integers including 1 which are $\leqslant xy$, prime to M_1M_2, and whose prime divisors are all $< \log x$. Let

$$N_n = \#\{(\alpha, \beta) \in T_0 \colon n^4|\alpha \text{ and } n^6|\beta\}$$

Denote by μ the Möbius function. Then

$$\begin{aligned}\#T_1 = \sum_n \mu(n)\#N_n &= \sum_n \mu(n)\left(\frac{xy}{n^{10}M_1M_2} + \mathrm{O}(1)\right)\\ &= \frac{xy}{M_1M_2}\sum_n \frac{\varphi(n)}{n^{10}} + \mathrm{O}\left(\sum_n 1\right)\end{aligned}$$

The O-term is bounded in terms of the number of integers $\leqslant xy$ whose prime divisors are all $< \log x$. By [21, p. 359], this quantity is

$$\ll xye^{-\log(xy)/2\log\log x} = (xy)^{1-1/2\log\log x} \ll xy/\log x.$$

On the other hand, if $x > e^{6M_1M_2}$, then

$$\prod_{\substack{p>\log x\\ p\nmid 6M_1M_2}} (1 - p^{-10}) = 1 + \mathrm{O}\left(\sum_{m>\log x} m^{-10}\right) = 1 + \mathrm{O}(\log^{-9} x),$$

so the inverse of the left side above is also $1 + \mathrm{O}(\log^{-9} x)$. Consequently,

$$\#T_1 = \frac{xy}{M_1M_2\zeta(10)} \prod_{p|6M_1M_2} (1 - p^{-10})^{-1} + \mathrm{O}(xy/\log x),$$

where the O-constant is absolute. On the other hand,

$$\#T_2 \ll \sum_{x^{1/4}>p\geqslant\log x} \left(\frac{xy}{p^{10}} + \mathrm{O}(1)\right) \ll xy/\log^9 x + x^{1/4}/\log x.$$

Combine these two estimates with (9) then yields the first part of the Lemma. To handle the second part, we work with the sets

$$\begin{aligned}T_1' &= \{(\alpha, \beta) \in T_0 \colon p \nmid \alpha\beta \text{ for every } p \text{ such that } 3 < p < \log x\},\\ T_2' &= \{(\alpha, \beta) \in T_0 \colon p|(\alpha, \beta) \text{ for some } p \geqslant \log x\}\end{aligned}$$

and repeat the arguments as before. □

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

4. Counting Elliptic Curves: Conditions at 2 and 3

To compute $S(x) := \#\{E/\mathbf{Q}: h_e(E) \leqslant x\}$, we need to count the number of pairs (c_4, c_6) in the set $T(x^4, x^6, 1, 1, 1, 1)$ which satisfy one of conditions $\{b, c, d, e, f\}$ in Proposition 3 and one of conditions $\{g, h, i, j, k, l\}$ there. Let $\varepsilon = \zeta(10)(1-2^{-10})^{-1}(1-3^{-10})^{-1}$. As u runs through the labels $\{b, c, d, e, f\}$, Lemma 3 furnishes a positive constant $t_{3,u}$ such that

$$\#\left\{\begin{array}{l}(\alpha, \beta) \in T(x^4, x^6, 1, 1, 1, 1): (\alpha, \beta) \\ \text{satisfies condition } (u) \text{ in Prop. 3}\end{array}\right\} = \frac{4t_{3,u}x^{10}}{\varepsilon} + \mathrm{O}(x^{10}/\log^4 x).$$

For $w \in \{g, h, i, j, k, l\}$ we define $t_{2,w}$ analogously. Note that

$$\#T(x^4, x^6, 1, 1, 1, 1) = \frac{4x^{10}}{\varepsilon} + \mathrm{O}(x^{10}/\log x).$$

Thus $\#S(x)$ is equal to

$$\begin{aligned}&\frac{4x^{10}}{\varepsilon}\left(1 - (1 - \sum_u t_{3,u}) - (1 - \sum_w t_{2,w}) + (1 - \sum_u t_{3,u})(1 - \sum_w t_{2,w})\right) + \\ &\quad + \mathrm{O}(x^{10}/\log^4 x) \\ &= \frac{4x^{10}}{\varepsilon}\left(\sum_u t_{3,u}\right)\left(\sum_w t_{2,w}\right) + \mathrm{O}(x^{10}/\log^4 x).\end{aligned}$$

The first part of Theorem 1 then follows an elementary computation of the t's via Lemma 3. We summarize the results as follow:

u	b	c	d	e	f
$t_{3,u}$	$1/3^4$	$2/3^5$	$26/3^7$	$1502/3^{14}$	$1/3^8$

w	g	h	i	j	k	l
$t_{2,w}$	$1/2^9$	$1/2^8$	$1/2^{10}$	$511/2^{19}$	$15/2^{15}$	$27/2^{19}$

To count $S_s(x)$ we proceed as before, with ε replaced by $\zeta(2)(1-2^{-2})^{-1}(1-3^{-2})^{-1}$, the set $T(x^4, x^6, 1, 1, 1, 1)$ replaced by $T'(x^4, x^6, 1, 1, 1, 1)$, and that for $p = 3$ we have only conditions (b, c) of Proposition 3; and for $p = 2$ only conditions (g, h).Note that the constants $t_{3,u}$ and $t_{2,w}$ so obtained are the same as the previous ones. The calculation for $S'(x)$ is similar to that for $S_s(x)$, but this time $t_{3,b} = 8/3^6$ and $t_{2,g} = 1/2^{10}$.

Finally, to count $S_t(x)$ we use the set $T'(x^4, x^6, 1, 1, 1)$ for the semistable condition at $p > 3$. At $p = 3$ we use conditions (b, c) of the table above. The conditions for $p = 2$ are determined by the second and the third case of Proposition 4. Note that among those pairs (γ_4, γ_6) that are congruent to any one of the pairs in Proposition 4, exactly half of them satisfy $2^{-6}(\gamma_4^3 - \gamma_6^2) \equiv 1 \pmod 4$ (resp. $-1 \pmod 4$). The

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

asymptotic constant is then equal to

$$\frac{4x^{10}}{\zeta(2)(1-2^{-2})(1-3^{-2})}\left(\frac{1}{3^4}+\frac{2}{3^5}\right)\left(32\times\frac{1}{2}\times\frac{1}{2^{13}}\times\frac{1}{2^{15}}\right).$$

This completes the proof of Theorem 1.

5. Local Densities

For any integer $m > 1$, define

$$\rho(m) = \begin{cases}\text{number of integer pairs } (\alpha, \beta) \text{ incongruent mod } m, \text{ such}\\ \text{that } \alpha^3 - \beta^2 \equiv 0 \pmod{m}, \text{ and that } \gcd(m, \alpha, \beta) = 1.\end{cases}$$

Let $M > 1$ be an integer divisible only by powers of 2 and 3, and let a, b be integers prime to M. Define $\rho(m, a, b, M)$ as we did with $\rho(m)$ above with the additional conditions that $\alpha \equiv a \pmod{M}$ and $\beta \equiv b \pmod{M}$.

Denote by φ the Euler φ-function, and by $[c]$ (resp. $\langle c\rangle$) the largest integer $\leqslant c$ (resp. $< c$).

The following is an extension to the *non-homogeneous* cubic $c_4^3 - c_6^2$ of [9, Lem. 1].

LEMMA 4. (a) *Let* $p \leqslant 3$. *For any integer* $v \geqslant 1$ *and any* a, b *prime to* 6, *we have*

$$\rho(p^v, a, b, M) \leqslant \rho(p^v) = O(p^{7v/6}).$$

(b) *Let* $p > 3$, *and let* $\rho_1(p)$ *be the number of solutions of* $x^6 - 1 \equiv 0 \pmod{p}$. *Then for any* $v \geqslant 1$ *and any* a, b *prime to* 6, *we have the equality*

$$\rho(p^v) = \rho(p^v, a, b, M) = \rho_1(p)\sum_{l=0}^{\langle v/6\rangle}\varphi(p^{v-6l}).$$

Proof. Note that $\rho(p^v, a, b, M) \leqslant \rho(p^v)$, and that the congruence conditions are irrelevant if $p > 3$. Thus it suffices to prove the Lemma for $\rho(p^v)$ only.

Let (α, β) be a pair of integer solution of $c_4^3 - c_6^2 \equiv 0 \pmod{p^v}$, such that if $p > 3$ then $p \not| (\alpha, \beta)$, but without the extra congruence mod M. Then

(i) if either $v_p(\alpha) < v/3$ or $v_p(\beta) < v/2$, then $3v_p(\alpha) = 2v_p(\beta)$. Call this common value λ the ord of this solution. Note that $\lambda < v$ and $6|\lambda$.

(ii) any pair of integers (α, β) with both $v_p(\alpha) \geqslant v/3$ and $v_p(\beta) \geqslant v/2$ is a solution of$c_4^3 - c_6^2 \equiv 0 \pmod{p^v}$.

These two cases are clearly disjoint, and the type (ii) solution contributes to $\rho(p^v)$ only if $p \leqslant 3$, in which case the contribution is $p^{[v/2]+[2v/3]}$. We now count the type (i) solutions according to their ord.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

Let (α, β) be a solution of ord λ. Then $\alpha = \alpha_1 p^{\lambda/3}, \beta = \beta_1 p^{\lambda/2}$ with

$$p \nmid \alpha_1\beta_1 \text{ and } \alpha_1^3 - \beta_1^2 \equiv 0 \ (\mathrm{mod}\ p^{v-\lambda}). \tag{10}$$

First, suppose $p = 3$. If $v - \lambda = 1$, then there are 3 solutions. Suppose inductively that there are 3^n solutions mod 3^n. Let (a_1, b_1) one such solution; then

$$(a_1 + 3^n x)^3 - (b_1 + 3^n y)^2 \equiv a_1^3 - b_1^2 - 6yb_1 \ (\mathrm{mod}\ 3^{n+1}).$$

If we set the equation above to 0 (mod 3^{n+1}), then y (mod 3) is uniquely determined since $3 \nmid b_1$. Thus every 1 (mod 3^n) solutions lifts to exactly three 1 (mod 3^{n+1}) solutions. By induction we see that there are 3^n type (i) solutions 1 (mod 3^n) for every n. Together with the type (ii) solutions we then obtained part (a). The same argument takes care of the case $p = 2$.

Now, suppose $p > 3$. From (10) we get

$$\alpha_1 \equiv \alpha_2^2 \ (\mathrm{mod}\ p^{v-\lambda}) \text{ and } \beta_1 \equiv \beta_2^2 \ (\mathrm{mod}\ p^{v-\lambda})$$

with

$$\alpha_2^6 - \beta_6 \equiv 0 \ (\mathrm{mod}\ p^{v-\lambda}) \text{ and } p \nmid \alpha_2\beta_2.$$

We can rewrite this as

$$b_2 \equiv a_2 x \ (\mathrm{mod}\ p^{v-\lambda}) \text{ with } x^6 \equiv 1 \ (\mathrm{mod}\ p^{v-\lambda}), p \nmid a_2 b_2. \tag{11}$$

Since $p > 3$ and $v > \lambda$, the number of solutions 1 (mod $p^{v-\lambda}$) to $x^6 = 1$ is $\rho_1(p)$, so the number of solutions 1 (mod $p^{v-\lambda}$) to (11) is $\rho_1(p)\varphi(p^{v-\lambda})$. The Lemma then follows. □

Following Gouvêa and Mazur, a real-valued function h defined on the set of all prime powers p^v for all p and $v > 0$ is called a prime-power function. Extending h multiplicatively to a function on the positive integers, it then makes sense to speak of the Dirichlet series associated to h. Also, we say that h is negligible if there exists positive constants $c > 1, \sigma < 1$, and $A > 1$ such that

$$\left| \log\left(1 + \sum_{v \geqslant 1} |h(p^v)| p^{-vs} \right) \right| \leqslant A p^{-c}$$

for all real $s \geqslant \sigma$ and all primes p.

Let t' be the prime-power function whose associated Dirichlet series is three times that of the Dedekind zeta function of $\mathbf{Q}(\sqrt{-3})$. Also, define three prime-power functions as follow:

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

	$\alpha(p^\nu, a, b, M)$	$\gamma(p^\nu, a, b, M)$	$t(p^\nu, a, b, M)$
$p > 3$	0	$\rho_1(p)\sum_{l=0}^{\langle \nu/6\rangle}\varphi(p^{\nu-6l})p^{-\nu}$	$\rho(p^\nu, a, b, M)p^{-\nu}$
$p \leqslant 3$	$\rho(p^\nu, a, b, M)p^{-\nu}$	0	$\rho(p^\nu, a, b, M)p^{-\nu}$

Since $\alpha(p^\nu) = 0$ if $p > 3$ and is $\mathrm{O}(p^{\nu/6})$ if $p \leqslant 3$, it follows that α is negligible. We claim that $\gamma - t'$ is also negligible. Since $\alpha + \gamma - t' = t - t'$ by Lemma 4(b), it follows that $t - t'$ is negligible.

To verify the claim, take $p > 3$ and write $\gamma(p^\nu, a, b, M)$ as

$$\begin{aligned}&\rho_1(p)\varphi(p)/p + \rho_1(p)\sum_{l=1}^{\langle \nu/6\rangle}\varphi(p^{\nu-6l})p^{-\nu}\\ &\quad = \rho_1(p) - \rho_1(p)/p + \mathrm{O}\left(\rho_1(p)\sum_{l=1}^{\langle \nu/6\rangle}p^{-6l}\right)\\ &\quad = \rho_1(p) - \rho_1(p)/p + \mathrm{O}\big(\rho_1(p)/p^5\big).\end{aligned} \tag{12}$$

Let $\gamma'(p^\nu, a, b, M)$ be $\rho_1(p)$ if $\nu = 1$ and is 0 otherwise. It follows from (12) that $\gamma - \gamma'$ is negligible, and that the Dirichlet series associated to $\gamma' - t'$ converges for any $s > 0$. The latter implies that $\gamma' - t'$ is negligible, and hence so is $\gamma - t' = (\gamma - \gamma') + (\gamma' - t')$, as claimed.

For any integer $m > 0$, define $\sigma_{-1/2}(m)$ to be the sum of the $-\frac{1}{2}$th power of the positive divisors of n.

LEMMA 5. *For any a, b and M as before, we have the estimate*

$$\sum_{m \leqslant x}\sigma_{-1/2}(m)\rho(m, a, b, M)/m = \mathrm{O}(x).$$

Proof. Note that $\sigma_{-1/2}(m) < 1$ for all m, so $(t - t')\sigma_{-1/2}$ is also negligible. The Lemma then follows by combining [9, Lem. 6] applied to $t - t'$, with the Tauberian theorem applied to the Dirichlet series associated to t' (i.e. the zeta function of $\mathbf{Q}(\sqrt{-3})$). □

6. A Fibering Argument

The following estimate is the backbone of our subsequent sieve arguments.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

PROPOSITION 5. *Let c_4 and c_6 run through all pairs of integers with $|c_4| \leqslant x^4$, $|c_6| \leqslant x^6$ and with no common prime divisor > 3. Write $\Delta = c_4^3 - c_6^2$. Then*

$$\sum_{\frac{\log x}{10} < p < x^6} \sum_{\substack{c_4, c_6 \\ p^2 | \Delta}} 1 \ll x^{10} \log^{-1/2} x. \tag{13}$$

Proof. For $p > 3$, the number of integer pairs (α, β) which are incongruent mod p^2 such that $p \not| \alpha\beta$ and $\alpha^3 - \beta^2 \equiv 0 \pmod{p^2}$, is $p(p-1)$.Thus the contribution to (13) from primes $p \leqslant x^4\sqrt{\log x}$ is bounded from the above by

$$\begin{aligned}
&\sum_{\frac{\log x}{10} < p \leqslant x^4\sqrt{\log x}} \left(p(p-1) \left(\frac{2x^4}{p^2} + \mathrm{O}(1) \right) \left(\frac{2x^6}{p^2} + \mathrm{O}(1) \right) \right) \\
&\ll \sum_{\frac{\log x}{10} < p \leqslant x^4\sqrt{\log x}} (x^{10}/p^2 + x^6) \\
&\ll x^{10} \sum_{n > \log x} 1/n^2 + \frac{x^4 \log^{-1/2} x}{\log x} x^6 \\
&\ll x^{10} \log^{-1/2} x.
\end{aligned}$$

It remains to work with those primes $p > x^4\sqrt{\log x}$.

Given any integer $m \neq 0$, define

$$\begin{aligned}
\Upsilon(c_6, m) &= \# \left\{ |c_4| \leqslant x^4 \colon \begin{array}{l} c_4^3 - c_6^2 = mp^2 \text{ for some prime } p \\ \text{such that } x^4 \log^{-1/2} x < p < x^6 \end{array} \right\}, \\
\rho_{c_6}(m) &= \#\{c_4 \ (\mathrm{mod}\ m) \colon c_4^3 - c_6^2 \equiv 0 \ (\mathrm{mod}\ m)\}.
\end{aligned}$$

Using the method of large sieve plus the Riemann hypothesis for curves, Hooley [11, §4.3] showed that, for $m < A_3 x^4 \log^{-4/3} x$ (A_3 a constant),

$$\Upsilon(c_6, m) = \mathrm{O}(\sigma_{-1/2}(m) \rho_{c_6}(m) \sqrt{x^4/m}). \tag{14}$$

Moreover, Gouvêa and Mazur [9, Lem. 11] showed that the O-constant is independent of c_6.

Remark. Gouvêa and Mazur assumed that both m and c_6 are positive; a quick inspection of their argument shows that this hypothesis was not invoked. Also, note that the proof the Sublemma there makes no use of the fact that the polynomial $f_b(u)$ there is homogeneous in u and b.

The contribution to (13) from primes $p > x^4\sqrt{\log x}$ is then

$$\sum_{x^4\sqrt{\log x} < p < x^6} \sum_{\substack{c_4, c_6 \\ p^2 | \Delta}} 1 \ll \sum_{|c_6| \leqslant x^6} \sum_{\substack{|m| \leqslant \\ x^4/\log x}} \Upsilon(c_6, m),$$

where on the right side we sum over all c_6 and (in Υ) c_4, with no divisibility condition on (c_4, c_6). Interchange the order of summation and invoke Hooley's estimate (14) as

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

in [9, p. 19], we get

$$\begin{aligned}\sum_{\substack{|m| \leqslant \\ x^4/\log x}} \sum_{|c_6| \leqslant x^6} \Upsilon(c_6, m) &\leqslant \sum_{|m| \leqslant x^4/\log x} \frac{x^6}{m} \sum_{0 \leqslant |c_6| < m} \Upsilon(c_6, m) \\ &\ll \sum_{|m| \leqslant x^4/\log x} \frac{x^6}{m} \left(\sqrt{\frac{x^4}{m}} \sigma_{-1/2}(m) \sum_{0 \leqslant |c_6| < m} \rho_{c_6}(m) \right) \\ &\ll x^8 \sum_{|m| \leqslant x^4/\log x} \frac{1}{\sqrt{m}} \sigma_{-1/2}(m) \frac{\rho(m)}{m}.\end{aligned}$$

Combine Lemma 5 with partial summation, we see that the contribution to (13) from $p > x^4\sqrt{\log x}$ is

$$\ll x^8 \frac{x^2}{\log^{1/2} x} = x^{10} \log^{-1/2} x,$$

as desired. □

7. Szpiro Conjecture

Denote by $E(a, b)$ the elliptic curve over $\mathbf{Q}$ given by the model $y^2 = x^3 + ax + b$. For any $K > 1$, define

$$S_0(A, B, K) = \left\{ E(a, b)\colon \begin{array}{l} |a| \leqslant A, |b| \leqslant B, p^4 | a \Rightarrow p^6 \nmid b, \\ \log |\Delta(E(a, b))| \geqslant K \log N_{E(a,b)} \end{array} \right\}. \tag{15}$$

Then [7, Thm. 2] states that

$$\lim_{A,B \to \infty} \frac{\# S_0(A, B, K)}{AB} = 0.$$

This is essentially Theorem 2(a), except that the Weierstrass equations in (15) need not be minimal at 2 and 3, and that Theorem 2 deals with semistable curves only. In light of Proposition 3, these requirements can be achieved by imposing congruence conditions on a and b in (15). The arguments in [7] readily adapt to such congruence conditions, from which Theorem 2(a) follows. Theorem 2(b) is an immediate consequence of the following Proposition.

PROPOSITION 6. *Let $S_f(x)$ be the set of elliptic curves $E/\mathbf{Q}$ of height $\leqslant x$ such that $\Delta(E)$ are square-free and are prime to 6. Then $\# S_f(x) \gg x^{10}$.*

Proof. The discriminant of the Weierstrass equation

$$y^2 = x^3 + 2^4 3^4 Ax - 2^4 3^6 B.$$

is $64A^3 + 27B^2$. If $3 \nmid A$ and $2 \nmid B$, then by Proposition 2 this equation has good

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

reduction at 2 and 3. Define

$$R_0(x) = \{(A, B) : 0 < A \leqslant x^4/2^4 3, 0 < B \leqslant x^6/2^3 3^3, 3 \not| A, 2 \not| B\},$$

$$R(x) = \{(A, B) \in R_0(x) : 64A^3 + 27B^2 \text{ is square-free}\}.$$

Thus $R(x)$ corresponds naturally to a subset of $S_f(x)$. We claim that $\#R(x) \sim x^{10}/2^7 3^3 \pi^2$, from which the Proposition follows. This is very similar to the proof of Theorem 1 so we will be brief.

For any integer $M > 0$, denote by $r(M)$ the number of integer pairs (A, B) which are incongruent mod M, such that $3 \not| A, 2 \not| B$, and that $64A^3 + 27B^2 \equiv 0 \pmod{M}$. Define

$$s_M(x) = \{(A, B) \in R_0(x) : 64A^3 + 27B^2 \equiv 0 \pmod{M}\},$$

$$R_1(x) = \{(A, B) \in R_0(x) : p^2 \not| 64A^3 + 27B^2 \text{ for any prime } p < \log x\},$$

$$R_2(x) = \{(A, B) \in R_0(x) : p^2 | 64A^3 + 27B^2 \text{ for some prime } p \geqslant \log x\}.$$

Then $\#R(x) = \#R_1(x) + \mathrm{O}(\#R_2(x))$. We now compute the size of these two sets.

The congruence conditions on A and B imply that $\#s_M(x) = 0$ if $4|M$ or $9|M$. Thus as m runs through square-free integers whose prime divisors are all less than $(\log x)/10$, we get

$$\begin{aligned}
\#R_1(x) &= \sum_m \mu(m) \#s_{m^2}(x) \\
&= \sum_{(6,m)=1} \mu(m) r(m^2) \left(\frac{2}{3} \frac{x^4}{2^4 3 m^2} + \mathrm{O}(1) \right) \left(\frac{1}{2} \frac{x^6}{2^3 3^3 m^2} + \mathrm{O}(1) \right) \\
&= \frac{x^{10}}{2^7 3^5} \sum_{(6,m)=1} \frac{\mu(m) r(m^2)}{m^4} + \mathrm{O}(x^6 \sum_m r(m^2)) \\
&= \frac{x^{10}}{2^7 3^5} \prod_{3 < p < \frac{\log x}{10}} \left(1 - \frac{r(p^2)}{p^4} \right) + \mathrm{O}(x^6 \sum_m r(m^2)).
\end{aligned}$$

For any prime $p > 3$ we have $r(p^2) = p^2$. Combined with the Chinese remainder Theorem, we get $r(m^2) \leqslant m^2$. Since $m \leqslant \prod_{p < \frac{\log x}{10}} p < x^{0.14}$, $\#R_1(x)$ is equal to

$$\begin{aligned}
&\frac{x^{10}}{2^7 3^5 (1 - 2^{-2})(1 - 3^{-2}) \zeta(2)} + \mathrm{O}\left(\frac{x^{10}}{\log^2 x} \right) \\
&= \frac{x^{10}}{2^7 3^3 \pi^2} + \mathrm{O}\left(\frac{x^{10}}{\log^2 x} \right).
\end{aligned}$$

Now, the error term $\#R_2(x)$ is at most $\sum_{\frac{\log x}{10} \leqslant p < x^6} \#s_{p^2}(x)$ By Proposition 5 this is $\ll x^{10} \log^{-1/2} x$. This completes the proof of Proposition 6. □

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

Remark. This argument can be refined to give an asymptotic formula for the size of $S_f(x)$, as we did for $S(x)$ and $S'(x)$. We do not require such a result and so will not pursue this.

8. Counting Frey Curves

Recall that a subset D of $\mathbf{R}^n$ is $(n-1)$-Lipschitz parameterizable if its boundary ∂D can be covered by the images of a finite number of functions $\varphi_i\colon [0,1]^{n-1} \to \mathbf{R}^n$, such that for each i, there exists a constant $\lambda_i > 0$, called the Lipschitz constant for φ_i, such that $|\varphi(x) - \varphi(y)| \leqslant \lambda_i |x-y|$ for any $x, y \in [0,1]^{n-1}$. The following Lemma is a straight-forward adaptation of the argument in [12, p. 128].

LEMMA 6. *Let D be a subset of $\mathbf{R}^n$ such that ∂D is $(n-1)$-Lipschitz parameterizable. Let $L \subset \mathbf{R}^n$ be a lattice with fundamental domain F. Fix an element $P \in L$. Then for any integer $m \geqslant 1$ and any $t \leqslant 1$,*

$$\#\big(tD \cap (P + mL)\big) = \frac{\mathrm{vol}(D)}{\mathrm{vol}(F)} \left(\frac{t}{m}\right)^n + \mathrm{O}(t^{n-1}),$$

where the O*-constant depends only on L, n and the Lipschitz constants, but not on m and P.* □

Recall that a Frey curve is a semistable curve corresponding to a Frey triple (A, B, C) as defined in the Introduction. Note that the sign condition in (3) uniquely pin down a Frey triple among its six permutations (astriples of numbers).

LEMMA 7. *Distinct Frey triples correspond to non-isomorphic Frey curves.*

Proof. Suppose that two Frey triples (A, B, C) and (α, β, γ) correspond to isomorphic curves. Then there is a $\mathbf{Q}$-rational change of variables

$$X = u^2 x + r,\ Y = u^3 y + u^2 s x + t$$

taking the Weierstrass equation $Y^2 = X(X+A)(X-B)$ to $y^2 = x(x+\alpha)(x-\beta)$. The latter equation does not have a xy-term or a y-term, so $s = t = 0$. Thus

$$x(x+\alpha)(x-\beta) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r+A}{u^2}\right)\left(x - \frac{r-B}{u^2}\right),$$

whence one of $r, r+A, r-B$ is zero. If $r = 0$, then the set $\{\alpha, \beta\}$ is equal to the set $\{A/u^2, B/u^2\}$. Since $(\alpha, \beta) = (A, B) = 1$, that means $u^2 = 1$. Since α, A are even and β, B are odd, it follows that $\alpha = A$ and $\beta = B$.

Now, suppose that $r + A = 0$. Then $\{\alpha, \beta\} = \{-A/u^2, (-A-B)/u^2\}$. Again $u^2 = 1$ and α, A are even, but $\beta \equiv -1 \pmod 4$ while $-A - B \equiv 1 \pmod 4$, a contradiction. A similar argument shows that $r - B = 0$ is impossible. □

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

Proof of Theorem 3. In view of Lemma 7, counting Frey curves of bounded height is equivalent to counting the size of the set

$$F'(x) = \{(A, B, C)\colon E_{A,B,C} \text{ is a Frey curve and } h_e(E_{A,B,C}) \leqslant x\}.$$

A minimal Weierstrass equation of the Frey curve $E_{A,B,C}\colon y^2 = x(x+A)(x-B)$ is

$$y^2 + xy = x^3 + \frac{A-B-1}{4}x^2 - \frac{AB}{16}x.$$

Thus

$$c_4(E_{A,B,C}) = A^2 - AB + B^2 \tag{16}$$

and

$$c_6(E_{A,B,C}) = (A+B)(A^2 + B^2 + 13AB/2).$$

Recall that $A \equiv 0 \pmod{16}, B \equiv -1 \pmod 4$, and $(A, B) = 1$. Let $M = A/2$, $N = B - A/2$, and denote by D the 2-dimensional region bounded by

$$3M^2 + N^2 \leqslant 1 \text{ and } (3M+N)(3M^2 + 15MN + N^2) \leqslant 1.$$

The boundary of D is clearly 1-Lipschitz parameterizable. Let $L = \{(8m', 4n')\colon m', n' \in \mathbf{Z}\} \subset \mathbf{Z}^2$ and let $P = (1, 0)$. Then we are reduced to count the number of points $(m, n) \in x^2 D \cap (P + L)$ with the additional property that $(m, n) = 1$. As l runs through all square-free integers whose prime divisors are $\leqslant \log x$, we get

$$\begin{aligned}
&\#\{(m,n) \in x^2 D \cap (P+L)\colon (m,n) = 1\} \\
&\quad = \sum_l \mu(l)\#\{x^2 D \cap (P + lL)\} + \mathrm{O}(x^4/\log x) \\
&\quad = \sum_l \mu(l)\#\left(\frac{\mathrm{vol}(D)}{32}\frac{x^4}{l^2} + \mathrm{O}(x^2)\right) + \mathrm{O}(x^4/\log x) \\
&\quad = x^4 \frac{\mathrm{vol}(D)}{32} \prod_{p \leqslant x^2} (1 - p^{-2}) + \mathrm{O}(x^2 \cdot x^2/\log x) \\
&\quad = x^4 \frac{\mathrm{vol}(D)}{32\zeta(2)} + \mathrm{O}(x^4/\log x).
\end{aligned}$$

Approximate D by rectangular grids and we get numerically $\mathrm{vol}(D) = 0.2233$. This completes the proof of Theorem 3(a).

LEMMA 8. *Let*

$$G(x) = \left\{ E_{A,B,C} \in F(x)\colon \begin{array}{l} |A|, |B| > x^2/\log x, |c_6(E)| > x^6/\log x, \\ |\Delta(E_{A,B,C})| > h_e(E_{A,B,C})/\log^3 x \end{array} \right\}.$$

Then

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

(i) $|c_4(E_{A,B,C})| \gg x^4/\log^2 x$.
(ii) $\#G(x) = \#F(x) + \mathrm{O}(x^4 \log^{-1} x)$.

Proof. Since $c_4(E_{A,B,C}) = A^2 - AB + B^2$ is a positive definite quadratic form in A and B,

(iii) if $h_e(E_{A,B,C}) \leqslant x$ then $|A|, |B| \ll x^2$;
(iv) we have $|c_4(E_{A,B,C})| \gg x^4/\log^2 x$ provided that

$$|A|, |B| > x^2/\log x. \tag{17}$$

This gives (i).

For any fixed $\gamma \in \mathbf{R}$, the number of pairs of integers $|A|, |B| \ll x^2$ satisfying (17) and $|A + \gamma B| < x^2 \log^{-1} x$, is $\ll_\gamma x^4 \log^{-1} x$. In light of (iii) and the factorizations

$$c_6(E_{A,B,C}) = (A+B)\left(A - \frac{-13+\sqrt{153}}{4}B\right)\left(A - \frac{-13-\sqrt{153}}{4}B\right),$$

$$\Delta(E_{A,B,C}) = \left(\frac{AB(A+B)}{16}\right)^2,$$

we get (ii). □

LEMMA 9. *Denote by $r(M)$ the number of pairs of integers (A, B) incongruent* mod M *such that $AB(A+B) \equiv 0 \pmod{M}$. Then there exists an absolute constant $C > 0$, independent of M, such that $r(M) \leqslant CM$.*

Proof. Hensel's lemma plus the Chinese remainder theorem. □

We now tackle Theorem 3(b). If $E \in G(x)$, then the condition $\Delta(E_{A,B,C}) > h_e(E_{A,B,C})/\log^3 x$ plus the crucial relation (4) imply that

$$h_F(x) \leqslant \frac{1}{12}\log|\Delta(E)| + \mathrm{O}(\log\log x)$$

with an absolute O-constant. Since

$$\Delta(E_{A,B,C}) = \left(\frac{AB(A+B)}{16}\right)^2 \tag{18}$$

and since $N_{E_{A,B,C}}$ = square-free part of $\Delta(E_{A,B,C})$, we need to show that for any $\alpha > 1/6$, the number of Frey curves in $F(x)$ for which $N_E^{6\alpha} < |AB(A+B)|$ has density zero. Set $\xi = \log^{1/2} x$. We have to consider three cases:

(i) $p^2 | AB(A+B)$ for some prime $p \geqslant x^3$;
(ii) $p^2 | AB(A+B)$ for some prime p with $\xi \leqslant p < x^3$;
(iii) if $p^2 | AB(A+B)$ then $p < \xi$.

Proof. Since $(A, B) = 1$ and $|A|, |B| \ll x^2$, case (ii) is handled as we did with the first sum in Proposition 5, and case (i) is already handled by Gouvêa and Mazur

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

[9, §8]. These together yield an upper bound $\ll x^4/\xi$ with an absolute O-constant. For case (iii), write $|AB(A+B)| = p_1^{a_1}\cdots p_r^{a_r}$ and let $m = \max\{a_i : p_i < \xi\}$. The prime number theorem gives $\sum_{p\leqslant x}\log p = x + o(x)$, so

$$\mathrm{e}^{m\xi} \gg \Bigg(\prod_{p_i\leqslant\xi} p_i\Bigg)^m \geqslant \prod_{p_i\leqslant\xi} p_i^{a_i} \geqslant \frac{|AB(A+B)|}{N_E}$$
$$\geqslant |AB(A+B)|^{1-\frac{1}{6\alpha}} \gg \left(x^{12}\log^{-2}x\right)^{1-\frac{1}{6\alpha}},$$

where the O-constants are absolute. Thus there exists an absolute constant $c > 0$ such that $m > c\left(1-\frac{1}{6\alpha}\right)\xi$. For every Frey curve $E_{A,B,C}$ in case (iii) we can then find a prime $p < \xi$ such that $AB(A+B)$ is divisible by $p^{[c(1-\frac{1}{6\alpha})\xi]}$. The number of such case (iii) curves is then at most

$$\ll \sum_{p<\xi} r\left(p^{[c(1-\frac{1}{6\alpha})\xi]}\right)\left(2x^2p^{-[c(1-\frac{1}{6\alpha})\xi]}\right)^2$$
$$\ll x^4\sum_{p<\xi}p^{-[c(1-\frac{1}{6\alpha})\xi]} + \mathrm{O}\Bigg(x^2\sum_{p<\xi}1\Bigg) \ll x^4/2^{[c(1-\frac{1}{6\alpha})\xi]},$$

where the O-constants are absolute. This completes the proof of Theorem 3(b).

Finally, for part (c) it suffices to show that a positive portion of the Frey curves have fouth power free discriminants. Since $16|A$ and $2\nmid B$, by (18) it suffices to show that $\alpha\beta(16\alpha+\beta)$ is square-free for a positive portions of integer pairs (α, β). This follows immediately from [9, Thm. 3]. This completes the proof of Theorem 3.□

Proof of Corollary 1. By [15, §3], for any constants $\lambda > 1$ and $C_\lambda > 0$ there exists a constant C'_λ depending on C_λ only, such that $SZ(\lambda, C_\lambda)$ is true for a Frey curve $E_{A,B,C}$ if and only if $ABC(6\lambda/5, C'_\lambda)$ is true for the Frey triple (A, B, C). By (16), we have

$$\max(|c_4(E_{A,B,C})|^{1/2}, |c_6(E_{A,B,C})|^{1/3}) \gg\ll \max(|A|, |B|)$$
$$\gg\ll \max(|A|, |B|, |C|)$$

since $A+B+C=0$. Apply Theorem 3(b) and we are done. □

9. Root Numbers of Elliptic Curves

For any finite prime p and any elliptic curve $E/\mathbf{Q}$, denote by $W_p(E)$ the local root number of $E/\mathbf{Q}_p$. Then the global root number of $E/\mathbf{Q}$ is given by $W(E) = -\prod_p W_p(E)$.

LEMMA 10. *Suppose $E/\mathbf{Q}$ has multiplicative reduction at $p > 2$. Then*

$$W_p(E) = -\left(\frac{-c_6(E)}{p}\right).$$

Proof. If E is multiplicative at p, then $W_p(E) = -1$ if and only if E is split multiplicative at p [16, Prop. 3], and the latter holds if and only if$-c_6(E)/c_4(E)$ is a square in $\mathbf{Q}_p^\times$ [18, p. 441]. Since E is multiplicative at p, we have $p \nmid c_4(E)$ [17, p. 180]. Thus if $p > 2$, the relation $c_4^3 - c_6^2 = 1728\Delta$ implies that $c_4(E)$ is a square (mod p) and that $p \nmid c_6(E)$. The Lemma then follows. □

LEMMA 11. *For any curve $E/\mathbf{Q}$, we have $c_4(E_{-1}) = r^4 c_4(E)$ and $c_6(E_{-1}) = -r^6 c_6(E)$, where*

$$r = \begin{cases} 1 & \text{if both } E \text{ and } E_{-1} \text{ have additive reduction at } 2; \\ 2 & \text{if } E \text{ is good or multiplicative at } 2; \\ 1/2 & \text{if } E \text{ is additive at } 2 \text{ and } E_{-1} \text{ is good or multiplicative at } 2. \end{cases}$$

Proof. The Weierstrass equation $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$ is a model of $E/\mathbf{Q}$ [17, p. 42], so $y^2 = x^3 - 27c_4(E)x + 54c_6(E)$ is a model of $E_{-1}/\mathbf{Q}$. The c_4, c_6 and Δ of the latter equation is $2^4c_4(E), 2^6c_6(E)$ and $2^{12}\Delta(E)$, so

$$c_4(E_{-1}) = \left(\frac{2}{t}\right)^4 c_4(E), \qquad c_6(E_{-1}) = \left(\frac{2}{t}\right)^6 c_6(E),$$

and (19)

$$\Delta(E_{-1}) = \left(\frac{2}{t}\right)^{12} \Delta(E),$$

for some positive integer t not divisible by any odd prime.

Case I. E and E_{-1} both have additive reduction at 2.

By Proposition 3, E being additive at 2 implies that $v_2(c_4(E)) \geqslant 4$, so if $t = 1$ then (19) implies that $v_2(c_4(E_{-1})) \geqslant 8$. By Proposition 3 again it then follows that $v_2(c_6(E_{-1})) = 6, 7, 8,$ or 10. By (100) that means $v_2(c_6(E)) = 0, 1, 2,$ or 4, contradicting Proposition 3. If $4|t$, then by Proposition 3, E_{-1} being additive at 2 implies that $v_2(c_4(E)) \geqslant 8$ and $v_2(c_6(E)) \geqslant 11$, which is impossible. Thus $t = 2$.

Case II. E is good or multiplicative at 2.

If E has good reduction at 2, then E_{-1} has additive reduction at 2. From the third relation in (19) we see that $t = 1$.

Now, suppose E is multiplicative at 2. Then there exists an element $d \in \mathbf{Q}_2^\times$ such that E_d is the Tate curve over $\mathbf{Q}_2$; note that $\mathbf{Q}_2(\sqrt{d})/\mathbf{Q}_2$ is unramified. Twisting by $-d$ then takes E_{-1} to the Tate curve over $\mathbf{Q}_2$. This time $\mathbf{Q}_2(\sqrt{-d})/\mathbf{Q}_2$ is ramified, so by [16, Prop. 3(ii)] E_{-1} is additive at 2, and hence 2 divides $c_4(E_{-1})$ by [17, p. 180]. On the other hand, E is multiplicative at 2, so $c_4(E)$ is odd. Invoke (19) and we done.

Case III. E is additive at 2, and E_{-1} is good or multiplicative at 2.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

This follows from case II above, once we note that $(E_{-1})_{-1} = E$. This completes the proof of the Lemma. □

LEMMA 12. *Suppose $E/\mathbf{Q}_2$ has additive reduction, and that $j(E)$ is a 2-adic unit. Then*

$$W_2(E)W_2(E_{-1}) = -1.$$

Proof. This is an immediate consequence of Proposition 4 and [16, Prop. 2(iii)]. □

COROLLARY 4. *Let $t = \pm 1$. Then for $E \in S_t(x)$, we have $W(E_{-1}) = -t$.*

Proof. Since $E/\mathbf{Q}$ is semistable for $p > 2$, so does E_{-1}. By Lemma 10, the root number of E_{-1} is equal to

$$\begin{aligned} &- W_2(E_{-1}) \prod_{\substack{p|\Delta(E_{-1})\\ p>2}} \left(\frac{-c_6(E_{-1})}{p}\right) \\ &\quad = -W_2(E_{-1}) \prod_{\substack{p|\Delta(E_{-1})\\ p>2}} -\left(\frac{-c_6(E)}{p}\right)\left(\frac{-1}{p}\right). \end{aligned}$$

If $p > 2$, then p divides $\Delta(E)$ if and only if it divides $\Delta(E_{-1})$. Thus

$$\begin{aligned} W(E_{-1}) &= -W_2(E_{-1}) \prod_{\substack{p|\Delta(E)\\ p>2}} W_p(E)\left(\frac{-1}{p}\right) \\ &= W(E)W_2(E)W_2(E_{-1})\left(\frac{-1}{\delta_E}\right). \end{aligned}$$

Apply Lemma 12 and we are done. □

Let P, Q be coprime, nonzero integers with Q odd but possibly negative. Define the extended Jacobi symbol via

$$\left(\frac{P}{Q}\right) = \begin{cases} \text{the usual Jacobi symbol } (P/|Q|) & \text{if } |Q| > 1; \\ 1 & \text{otherwise.} \end{cases}$$

Suppose P is also odd; then the law of quadratic reciprocity takes the following form [3, p. 73]:

$$\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2} + \frac{sgn(P)-1}{2}\frac{sgn(Q)-1}{2}}\left(\frac{Q}{P}\right),$$

where $sgn(d) = d/|d|$. For future reference we compute the symbol $(-c_6/\Delta)$ for those pairs (c_4, c_6) corresponding to elliptic curves in $S'(x)$ such that $\gcd(6, c_4c_6) = 3$. Similar formula can be obtained easily in the other cases.

So, suppose $\gcd(6, c_4c_6) = 3$. By Propositions 2 and 3 we can write $c_4 = 3\gamma_4$, $c_6 = 3^n\gamma_6$ with $n \geqslant 3, 3 \nmid \gamma_4\gamma_6, \gcd(\gamma_4, \gamma_6) = 1$, and $\Delta = (\gamma_4^3 - 3^{2n-3}\gamma_6^2)/4^3$. Since

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

$c_6 \equiv -1 \pmod 4$, we get

$$\begin{aligned}\left(\frac{-c_6}{\Delta}\right) &= (-1)^{\frac{sgn(c_6)+1}{2}\frac{sgn(c_4^3-c_6^2)-1}{2}}\left(\frac{\gamma_4^3 - 3^{2n-3}\gamma_6^2}{-c_6}\right)\left(\frac{4^3}{-c_6}\right)\\ &= (-1)^{\frac{sgn(c_6)+1}{2}\frac{sgn(c_4^3-c_6^2)-1}{2}}\left(\frac{\gamma_4}{-3}\right)\left(\frac{\gamma_4}{\gamma_6}\right)\end{aligned} \tag{20}$$

10. Proof of Theorem 4

The odd part of the discriminant of any elliptic curve over $\mathbf{Q}$ is invariant under twist by -1. If $E \in S_t(x)$, then by Lemma 11 the height of E and E_{-1} are the same. Consequently, $E_{-1} \in S_t(x)$ as well, and the first part of Theorem 4 then follows from Lemma 12. We now tackle the second part.

Given nonzero integers m, n with $n > 1$, we write $n||m$ if $n|m$ and if $\gcd(n, m/n) = 1$. Note that if $E/\mathbf{Q}$ has height $< x$, then $p^2|\Delta$ implies that $p < x^6$. As n runs through all perfect squares such that every prime divisor of $n$is $< \log x/10$, we have the decomposition

$$\begin{aligned}&- \sum_{E\in S'(x)} (-1)^{\omega(E)} W(E)\\ &\quad = \sum_{c_4,c_6}\left(\frac{-c_6}{\Delta}\right) - \sum_{n}\sum_{\substack{c_4,c_6\\ n||\Delta}}\left(\frac{-c_6}{\Delta}\right) + \sum_{n}\sum_{\substack{c_4,c_6\\ n||\Delta}}\left(\frac{-c_6}{\Delta}\right)\prod_{p|n}\left(\frac{-c_6}{p}\right) +\\ &\qquad + \mathrm{O}\left(\sum_{\frac{\log x}{10}<p \leqslant x^4\sqrt{\log x}}\ \sum_{\substack{c_4,c_6\\ p^2|\Delta}} 1\right) + \mathrm{O}\left(\sum_{x^4\sqrt{\log x}<p<x^6}\ \sum_{\substack{c_4,c_6\\ p^2|\Delta}} 1\right),\end{aligned} \tag{21}$$

where c_4, c_6 run through all pairs of integers $|c_4| \leqslant x^4, |c_6| \leqslant x^6$ corresponding to curves in $S'(x)$. We now show that each of the five terms on the right side of (21) is $\ll x^{10}\log^{-1/2} x$, from which the second part of Theorem 4 follows. Note that the last two terms are covered by Proposition 5.

The first term in (21): We break down the sum into four pieces, depending on the value of $\gcd(6, c_4c_6)$. We will work out the details only for the case where the gcd is 3; the other three cases are handled in the same way.

So, consider the first term in (21) taken over pairs (c_4, c_6) such that $\gcd(6, c_4c_6) = 3$. We will call this the restricted first term. By Proposition 2, we have

- $c_4 = 3\gamma_4, c_6 = 3^m\gamma_6$, with $3 \not| \gamma_4\gamma_6$ and $n \geqslant 3$;
- c_4, c_6 satisfy conditions (f,g) of Proposition 2;
- $p \not| (c_4, c_6)$ for any prime $p > 3$.

To compute this restricted first term, we invoke the root number formula (20) according to the sign of $c_4^3 - c_6^2$.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

If $c_4^3 - c_6^2 < 0$, then by (20) the root number is

$$(-1)^{\frac{sgn(c_6)+1}{2}}\left(\frac{\gamma_4}{-3^m\gamma_6}\right) = (-1)^{\frac{sgn(c_6)+1}{2}}\left(\frac{\gamma_4}{-3}\right)^m\left(\frac{\gamma_4}{\gamma_6}\right).$$

Note that Proposition 2(f,g) imposes conditions on $\gamma_4 \pmod{2^7}$ and $\gamma_6 \pmod{2^6}$. Fix one such set of congruence conditions, say $\gamma_4 \equiv a \pmod{2^7}$ and $\gamma_6 \equiv b \pmod{2^6}$. Denote by φ the Euler-φ function. Then the restricted first term becomes

$$\frac{1}{\varphi(2^6)\varphi(2^7)}\sum_{\chi_4}\sum_{|\gamma_4|\leqslant x^4/3}\chi_4(\gamma_4/a)\sum_{m=3}^{\infty}\left(\frac{\gamma_4}{-3}\right)^m \times$$
$$\times\sum_{\chi_6}\sum_{\frac{|\gamma_4|^{3/2}}{3^{m-3/2}}<|\gamma_6|\leqslant x^6 3^m}(-1)^{\frac{sgn(c_6)+1}{2}}\chi_6(\gamma_6/b)\sum_{|\gamma_4|\leqslant|3^{m-1}\gamma_6|^{2/3}}\left(\frac{\gamma_4}{\gamma_6}\right),$$

where χ_4 (resp. χ_6) runs through all primitive Dirichlet characters of conductor 2^7 (resp. 2^6) plus the trivial one. The product $\chi_4(\cdot)\left(\frac{\cdot}{\gamma_6}\right)$ is a Dirichlet character of conductor dividing $2^6 \cdot 4\gamma_4$. Since $\gcd(6, \gamma_6) = 1$, if this product of characters is trivial then γ_4 must be a square, for which there are $\leqslant \sqrt{x^4/3} \times 2$ possibilities, each contributing $\ll x^6/3^m$ to the inner-most sum. If this product of characters is nontrivial, then the Polya–Vinogradov inequality [4, p. 135] plus the trivial estimate shows that the inner-most sum is $\ll \min(\sqrt{|\gamma_4|}\log|\gamma_4|, x^6/3^m)$. In addition, since 3^m divides $|c_4| \leqslant x^6$, we have $m \leqslant 6\log x/\log 3 < 6\log x$. Consequently, the whole expression above is

$$\ll \sum_{|\gamma_4|\leqslant x^4}\sum_{m=3}^{6\log x}\sqrt{|\gamma_4|}\log|\gamma_4| + \sum_{\substack{|\gamma_4|\leqslant x^4\\ |\gamma_4|=}}\sum_{m=3}^{\infty}x^6/3^m$$
$$\ll \log x\int_2^{x^4}\sqrt{t}\ln t\,\mathrm{d}t \quad\ll\quad x^6\log^2 x + x^8 \quad\ll\quad x^8.$$

If $c_4^3 - c_6^2 > 0$, then the inner-most γ_6-sum is now taken over the interval $|\gamma_6| \leqslant |\gamma_4|^{3/2}3^{3/2-m}$. The Polya–Vinogradov argument still applies, yielding the same upper bound $\ll x^8$.

Proposition 2(f,g) imposes finitely many congruence conditions on γ_4 and γ_6 at 2, so in the end the contribution to the first term in (21) from those pairs (c_4, c_6) with $\gcd(6, c_4c_6) = 3$ is $\ll x^8$. The same goes for the three cases of $(6, c_4c_6)$, so the total contribution of the first term in (21) is $\ll x^8$.

The second term in (21): Write $n = p_1^{2m_1}\cdots p_r^{2m_r}$. Then $n||\Delta$ if and only if $p^{2m_i}||\Delta$ for every i. Thus to achieve $n||\Delta$ it suffices to impose congruence conditions on c_4 and c_6 1 (mod $p_i^{2m_i+1}$) for every $p_i > 3$ as well as congruence conditions at 2 and 3, as prescribed by Proposition 2. As before we will discuss only the case where $\gcd(6, c_4c_6) = 3$, and we will fix one set of congruence condition $\gamma_4 \pmod{2^7}$ and

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

$\gamma_6 \pmod{2^6}$. Recall that $\sum_{p<A} \log p < (2\log 2)A$ for any $A \geqslant 1$ [10, p. 341]. For any prime $p > 3$ and any integer $m \geqslant 1$, induction gives

$$\#\left\{(\alpha,\beta) \in (\mathbf{Z}/p^{m+1}\mathbf{Z})^2 \colon \begin{array}{l} p^m \| (\alpha^3-\beta^2) \\ \text{and } p \not| \, \alpha\beta \end{array}\right\} = p^m(p-1)^2. \tag{22}$$

Thus for any given n as above the total number of possible congruence conditions at the primes > 3 is

$$\leqslant \prod_{i=1}^{r} p_i^{m_i}(p_i-1)^2 \leqslant \sqrt{n} \prod_{p<\frac{\log x}{10}} p^2 < \sqrt{n}x^{\frac{4\log 2}{10}} < \sqrt{n}x^{0.28}. \tag{23}$$

Also, let

$$n_4 = 2^7 \prod_{p_i>3} p_i^{2m_i+1} \leqslant 128nx^{0.14}, \quad n_6 = 2^6 \prod_{p_i>3} p_i^{2m_i+1} \leqslant 64nx^{0.14}. \tag{24}$$

Fix one such collection of congruence conditions $a \pmod{n_4}$, $b \pmod{n_6}$. Then the restricted second term is

$$\frac{1}{\varphi(n_4)\varphi(n_6)} \sum_{\chi_4} \sum_{|c_4| \leqslant x^4} \chi_4(c_4/a) \sum_{\chi_6} \sum_{|c_6| \leqslant x^6} \chi_6(c_6/b)\left(\frac{-c_6}{\Delta}\right), \tag{25}$$

where χ_4 and χ_6 run through all primitive Dirichlet characters mod n_4 and n_6, respectively, plus the trivial one. When $c_4^3 - c_6^2 < 0$, combine formula (20) with (25) and we get

$$\frac{1}{\varphi(n_4)\varphi(n_6)} \sum_{\chi_4} \sum_{|\gamma_4| \leqslant x^4/3} \chi_4(\gamma_4/a) \times$$
$$\times \sum_{m=3}^{\infty} \left(\frac{\gamma_4}{-3}\right)^m \sum_{\chi_6} \sum_{\frac{|\gamma_4|^{3/2}}{3^{m-3/2}} < |\gamma_6| \leqslant x^6/3^m} (-1)^{\frac{sgn(\gamma_6)+1}{2}} \left(\frac{\gamma_4}{\gamma_6}\right)$$

This time the product of characters $\chi_6(\gamma_6/b)\left(\frac{\gamma_4}{\gamma_6}\right)$ has conductor dividing $4n_6\gamma_4$. Furthermore, under the hypothesis $\gcd(6, c_4c_6) = 3$ and $n \| \Delta$, we see that $\gcd(n_6, \gamma_4) = 1$. Thus if this product of characters is trivial, then up to a factor

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

dividing 4, each of γ_4 and n_6 is a square. Consequently, the expression above is

$$\begin{aligned}
&\ll \frac{1}{\varphi(n_4)\varphi(n_6)} \sum_{\chi_4,\chi_6} \Bigg(\sum_{|\gamma_4| \leqslant x^4} \sum_{m=3}^{6\log x} \sqrt{|\gamma_4| n_6} \log(|\gamma_4| n_6) + \sum_{\substack{|\gamma_4| \leqslant x^4 \\ |\gamma_4| =}} \sum_{m=3}^{\infty} \frac{x^6}{3^m} \Bigg) \\
&\ll \frac{1}{\varphi(n_4)\varphi(n_6)} \sum_{\chi_4,\chi_6} \big(\sqrt{n_6} x^6 \log x + x^8\big) \qquad \text{since } \log(n_6) \ll \log x \\
&\ll \sqrt{n_6} x^6 \log x + x^8 \\
&\ll \sqrt{n} x^{6.07} \log x + x^8. \qquad \text{by (24).}
\end{aligned}$$

We get the same estimate too when $c_4^3 - c_6^2 > 0$.

To recapitulate, for any perfect square n whose prime divisors are all $< \log x$, if we restrict c_4, c_6 to those with $\gcd(6, c_4 c_6) = 3$ and satisfy a given congruence condition given by (22) for every prime $p > 3$ dividing n, then the restricted second term in (21) is

$$\ll \sqrt{n} x^{6.07} \log x + x^8.$$

By (23), the total number of congruence classes is $\ll \sqrt{n} x^{0.28}$, so the total contribution of the second term in (21) for $n < x$ is

$$\begin{aligned}
&\sum_{\substack{n=1 \\ n=\square}}^{x} \big(\sqrt{n} x^{0.28}\big)\big(\sqrt{n} x^{6.07} \log x + x^8\big) \\
&\quad \ll x^{6.35} \log x \sum_{t \leqslant \sqrt{x}} t^2 + x^{8.28} \sum_{t \leqslant \sqrt{x}} t \ll x^{9.28}.
\end{aligned} \tag{26}$$

On the other hand, the contribution of the second term in (21) for $x < n \leqslant x^6$ is

$$\begin{aligned}
\ll \sum_{\substack{x<n \leqslant x^6 \\ n=\square}} \sum_{\substack{c_4,c_6 \\ n||\Delta}} 1 &\ll \sum_{\substack{x<n \leqslant x^6 \\ n=\square}} \big(\sqrt{n} x^{0.28}\big) \left(\frac{2x^4}{n_4} + \mathrm{O}(1)\right)\left(\frac{2x^6}{n_6} + \mathrm{O}(1)\right) \\
&\ll \sum_{\substack{x<n \leqslant x^6 \\ n=\square}} \big(\sqrt{n} x^{0.28}\big) \left(\frac{x^{10}}{n^2 \prod_{p<\frac{\log x}{10}} p^2} + \frac{x^6}{n \prod_{p<\frac{\log x}{10}} p}\right) \\
&\ll \sum_{\substack{x<n \leqslant x^6 \\ n=\square}} \left(\frac{x^{10.28}}{n^{3/2}} + \frac{x^{6.14}}{\sqrt{n}}\right) \\
&\ll x^{10.28} \sum_{t>\sqrt{x}} t^{-3} + x^{6.14} \sum_{t<x^3} 1/t \quad \ll \quad x^{9.28}.
\end{aligned} \tag{27}$$

Combine (26) and (27) and we see that the total contribution of the second term in (21) is $\ll x^{9.28}$.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

The third term in (21): The extra factor $\prod_{p|n}(-c_6/p)$ is a character of conductor $\leqslant \prod_{p<\frac{\log x}{10}} p < x^{0.14}$, so the argument for the second term now yields an upper bound$\ll x^{9.28+0.14} = x^{9.42}$ for the third term in (21), which is acceptable.
Since the last two terms in (21) are handled by Proposition 5, we have verified that every term in (21) is$\ll x^{10}\log^{-1/2} x$. This completes the proof of Theorem 4.

Remark. Theorem 4 clearly holds for logarithmic height. To see that it holds for the Faltings height we need to prove (5). From the proof of corollary 2.3 in [19, p. 259], we get the relation

$$\mathrm{O}(1) \leqslant h_l(E) - h_F(E) \leqslant 6\log\big(1 + \log\max\big(|j(E)|, |j(E)\Delta(E)|\big)\big).$$

Since $j(E) = c_4(E)^3/\Delta(E)$, the relation (4) follows immediately.

11. Lower Bounds For Other Ranks

Proof of Theorem 5. Let $E/\mathbf{Q}$ be a modular curve of conductor N, and let $L(E, s)$ be its L-function. It follows from the Rankin–Selberg method that there exists an absolute constant $c > 0$ such that, as D runs through all fundamental discriminants such that the root number of the twisted curve E_D is $+1$, we have the lower bound [8, p. 76]

$$\sum_{D \leqslant N^2} L(E_D, 1) > cN^2.$$

In particular, there exists a twist with $D \ll N^2$ such that $L(E_D, 1) \neq 0$. By the work of Kolyvagin *et al.*, it follows that the Mordell–Weil rank of $E_D(\mathbf{Q})$ is zero. Apply these remarks to the curves in Proposition 6, which are modular by the work of Wiles and Taylor–Wiles, and we obtain the first part of Theorem 5. To prove the second part, note that the hypothesis there implies that for every $\varepsilon > 0$ there exists an absolute constant $c(\varepsilon) > 0$ independent of E, such that [8, p. 77]

$$\sum_{D \leqslant N^{\varepsilon}} L(E_D, 1) > c(\varepsilon)N^{\varepsilon}.$$

Continue as before and we get the second part of Theorem 5. □

Proof of Theorem 6. The reduction mod 3 of the Weierstrass equation

$$E_{a,b}\colon y^2 = x^3 + 3ax^2 - (1 + 3a)x + 9b^2 \tag{28}$$

is $y^2 = x^3 - x$, which is nonsingular over $\mathbf{F}_3$, so $E_{a,b}$ defines an elliptic curve over $\mathbf{Q}$ for any integers a, b. Now $E_{a,b}(\mathbf{F}_3) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and is generated by the image of the $\mathbf{Q}$-rational points $P_1 = (0, 3b)$ and $P_2 = (1, 3b)$.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

LEMMA 13. *Let* $a \equiv b \equiv 1 \pmod{11}$*; then* P_1 *and* P_2 *generate a free, rank 2 subgroup of* $E_{a,b}(\mathbf{Q})$.

Proof. Suppose otherwise; then $t_1P_1 + t_2P_2 \in E_{a,b}(\mathbf{Q})_{tor}$ for some integers t_1, t_2,not both zero. Moreover, we can assume that at least one t_i is odd. If $a \equiv b \equiv 1 \pmod{11}$, then $E_{a,b}$ has good reduction at 11, so the prime-to-11 part of $E_{a,b}(\mathbf{Q})_{tor}$ injects into $E_{a,b}(\mathbf{F}_{11})$. On the other hand, if $a \equiv b \pmod{11}$, then $\#E_{a,b}(\mathbf{F}_{11}) = 11$, while Mazur's Theorem implies that $E_{a,b}(\mathbf{Q})$ has no 11-torsion. Thus $t_1P_1 + t_2P_2 = 0$. Since P_1 and P_2 generate $E_{a,b}(\mathbf{F}_3) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and at least one t_i is odd, this is a contradiction. □

Proof. Replace x by $x - a$ and the Weierstrass equation (28) becomes

$$y^2 = x^3 + (-3a^2 - 3a - 1)x + (2a^3 + 3a^2 + a + 9b^2). \tag{29}$$

Now, $3a^2 + 3a + 1$ is square-free for a positive portion of the integers $a \equiv 1 \pmod{11}$ (cf. [11, p. 62]*), so for such a and any $b \equiv 1 \pmod{11}$, the Weierstrass equation (29) is minimal at every prime (including 2 and 3). Consequently for such a and b, we have $c_4(E_{a,b}) \gg\ll a^2$ and $c_6(E_{a,b}) \gg\ll \max(|a|^3, b^2)$. At most four pairs of integers (a, b) give rise to the same equation (127), so the number of $E_{a,b}$ of height $\leqslant x$ and with Mordell–Weil rank $\geqslant 2$, is $\gg x^2x^3 = x^5$. This completes the proof of Theorem 6. □

Acknowlegements

I would like to thank Professor Silverman for useful comments and for bringing to our attention the work of Kraus and of Fouvry *et al.*; Professor Hoffstein for useful discussions regarding nonvanishing theorems; and Professor Mazur for suggesting that we study the density aspect of the Szpiro Conjecture. Part of the paper was written during my visit to Queens University. I would like to thank Professor R. Murty for his invitation, and Queens' mathematics Department for their hospitality.

References

1. Brumer, A.: The average rank of elliptic curves. I, *Invent. Math.* **109**(3) (1992), 445–472.
2. Brumer, A. and McGuinness, O.: The behavior of the Mordell–Weil group of elliptic curves, *Bull. Amer. Math. Soc. (N.S.)* **23**(2) (1990), 375–382.
3. Cox, D.: *Primes of the Form* $x^2 + ny^2$, Wiley, New York, 1989.
4. Davenport, H.: *Multiplicative Number Theory*, 2nd edn, Springer-Verlag, New York, 1980.
5. Ellison, W. J. and Ellison, F.: *Prime Numbers*, Wiley-Interscience, New York, 1985.
6. Frey, G.: Links between stable elliptic curves and certain diophantine equations, *Ann. Univ. Saraviensis* **1** (1986), 1–40.
7. Fouvry, E., Nair, M. and Tenenbaum, G.: L'ensemble exceptionnel dans la conjecture de Szpiro, *Bull. Soc. Math. France* **120** (1992), 485–506.

*The method cited there readily extends to cover the extra congruence condition.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press

8. Goldfeld, D. and Szpiro, L.: Bounds for the order of the Tate–Shafarevich group, *Compositio Math.* **97** (1995), 71–87.
9. Gouvêa, F. and Mazur, B.: The square-free sieve and the rank of elliptic curves, *J. Amer. Math. Soc.* **4**(1) (1991), 1–23.
10. Hardy, G. H. and Wright, E.: *An Introduction to the Theory of Numbers*, 5th edn, Oxford Univ. Press, 1979.
11. Hooley, C.: *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Univ. Press, 1976.
12. Lang, S.: *Algebraic Number Theory*, Springer, New York, 1986.
13. Kraus, A.: Quelques remarques á propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.* **54**(1) (1989), 75–80.
14. Massar, D.: Note on a conjecture of Szpiro, In: *Astérique* **183** (1990), 19–23.
15. Oesterlé, J.: Nouvelles approches du théorème de Fermat, In: *Séminaire Bourbaki*, exposé 694, 1987–88.
16. Rohrlich, D.: Variation of the root number in families of elliptic curves, *Compositio Math.* **87** (1993), 119–151.
17. Silverman, J.: *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
18. Silverman, J.: *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
19. Silverman, J.: Heights and elliptic curves, In: *Arithmetic Geometry*, Springer, New York, 1986, pp. 253–265.
20. Szpiro, L.: Discriminant et conducteur des courbes elliptiques, In: *Astérique* **183** (1990), 7–18.
21. Tenenbaum, G.: *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, 1995.

https://doi.org/10.1023/A:1017514507447 Published online by Cambridge University Press